NASA TECHNICAL HANDBOOK	**NASA-HDBK-1002**
National Aeronautics and Space Administration **Washington, DC 20546-0001**	**Approved: MM-DD-YYYY** **Superseding**

FAULT MANAGEMENT HANDBOOK

DRAFT 2 –APRIL 2, 2012

This official draft has not been approved and is subject to modification.
DO NOT USE PRIOR TO APPROVAL.

MEASUREMENT SYSTEM IDENTIFICATION:
NOT MEASUREMENT SENSITIVE

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Baseline		MM-DD-YYYY	Initial Release

FOREWORD

This Handbook is published by the National Aeronautics and Space Administration (NASA) as a guidance document to provide guidelines and recommendations for defining, developing, analyzing, evaluating, testing, and operating the Fault Management (FM) element of flight systems. It establishes a process for developing FM throughout the lifecycle of a mission and provides a basis for moving the field toward a formal and consistent FM methodology to be applied on future programs.

The NASA Science Mission Directorate's Discovery and New Frontiers Program Office and by the Office of the Chief Engineer's NASA Engineering & Safety Center (NESC) co-sponsored the development of this Handbook as an initial step toward an Agency-wide FM Handbook. As a result, the initial focus addresses FM required for science missions. It is recognized that FM is relevant to all NASA Directorates, and that ultimately this Handbook should address the needs of the Agency. In preparation for this broadened scope, the authors have strived to develop an outline that identifies FM-related needs and goals for all Directorates, with the intent that the content for the Aeronautics Research Mission Directorate and the Human Exploration and Operations Mission Directorate will be completed in a future revision of this Handbook.

NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers, approve this Handbook for use.

Requests for information, corrections, or additions to this Handbook should be submitted via "Feedback" in the NASA Standards and Technical Assistance Resource Tool at http://standards.nasa.gov.

_____ _____

Michael G. Ryschkewitsch
NASA Chief Engineer

Approval Date

TABLE OF CONTENTS

1. SCOPE

Fault Management (FM) is an engineering activity; it is the part of systems engineering (SE) focused on the detection of faults and accommodation for 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.

FM has emerged and developed along several paths in response to NASA's mission needs (e.g., deep space vs. earth orbiters vs. human spaceflight) as reflected by the different approaches used in many organizations (e.g., JPL vs. GSFC vs. JSC), 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 as described in section 4). However, present use of the term "fault management" is synergistic with usage in the field of network management, where the International Organization for Standardization[1] (ISO) defines FM as "the set of functions that detect, isolate, and correct malfunctions…." 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."

1.1 Relevance

FM provides a system's response to off-nominal conditions, which 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,

[1] International Organization for Standardization. *Information Technology — Multimedia Middleware — Part 6: Fault management, ISO/IEC 23004-6:2008.* Geneva, 2008.

and the targeted operating domain. Within NASA, FM is crucial to the development of crewed and robotic systems,[2] to the development of flight controls and maintenance of aircraft and spacecraft, and to the procurement, contractual oversight, and acceptance of commercial launch vehicles and orbital transportation services. NASA's historical concerns regarding FM are summarized in sections 1.1.1-1.1.4.

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 (see subsequent paragraphs in this section and Appendix B). 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 (see Appendix C). 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 (see section 4). FM follows an SE process, addressing the off-nominal design and responses to failures (see figure 2, FM Process as Part of SE Process). Mission and system characteristics, such as risk posture, response latency, fault tolerance requirements, and reliability requirements, drive the development process and the design, as described in section 4.

This handbook provides guidance for designing, developing, verifying, validating, and operating the FM element of a system within the context of NASA program and project life cycles, which produce derived requirements in accordance with existing systems engineering practices that flow down through the NASA organizational hierarchy. The guidance in this handbook is not meant to be prescriptive; instead, it is meant to be general enough to enable the reader to adapt the process to a particular mission and to each NASA Center. During system design and realization, FM activities take place within the context of the systems engineering technical processes enumerated in NPR 7123.1A and shown in Figure 1.

[2] NASA's robotic systems include terrestrial and non-terrestrial systems including aircraft, dirigibles, submersibles, rovers, rockets, satellites, space stations, space probes, telescopes, and other *in situ* platforms.

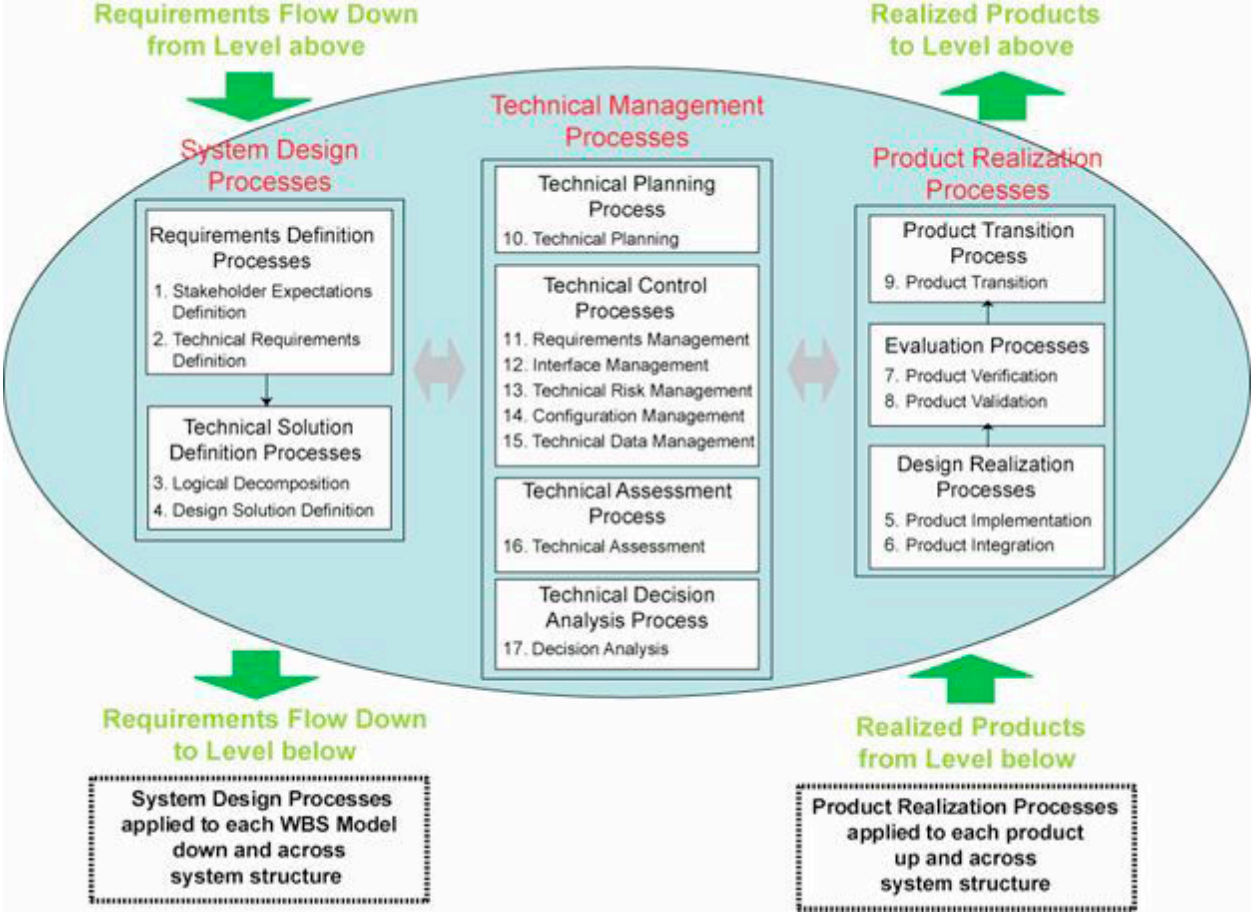

Figure 1— NASA's Systems Engineering Technical Processes

1.2 Purpose

The purpose of this Handbook is to integrate the collective knowledge and experience of FM lessons learned and best practices across the NASA community, FFRDCs, universities, and commercial partners, into guidance and recommendations that give footing for an Agency-wide, disciplined approach to FM. The goals of this Handbook are to:

- Recognize FM as an engineering discipline, a necessary element of project design and SE, and an essential factor affecting system safety, reliability and availability – Section 1.

- Establish foundational FM concepts, guiding principles, and terminology - Appendix C.

- Raise awareness of FM recommended practices to achieve consistency across the Agency – all Sections and Appendices.

- Promote organizational structures that facilitate effective FM development by noting institutional and programmatic factors that substantially affect FM -Appendix D.

- Delineate a FM development process and lifecycle consistent with the NASA Systems Engineering Handbook[3] (hereafter, referred to as the NASA SE Handbook) – Section 4.

- Articulate the purpose, process, work products, potential pitfalls, and recommended practices, and take advantage of FM lessons learned for each major development activity in the FM lifecycle – Sections 5-10, Appendix G.

This Handbook provides guidance and recommendations for defining, developing, analyzing, evaluating, testing, and operating the FM element of flight systems. This Handbook provides a process for developing FM throughout the lifecycle of a mission. It also provides the fundamental concepts and terminology needed to understand the FM discipline; captures the typical pitfalls experienced on missions when FM is not appropriately addressed; provides exemplars for how to write FM requirements; supplies the basic building blocks of FM architectures; provides techniques for assessing and analyzing FM designs, gives insights into the unique needs of FM during the verification and validation (V&V) phase; addresses FM operational considerations; and delineates reviews and evaluation criteria to ensure that a flight system's FM design is suitable for a mission, is staffed appropriately, and is progressing on schedule. Where appropriate, this Handbook provides recommended work products to be developed, technical and progress metrics, and lessons learned related to the particular development phase. This Handbook captures high-level concepts and FM fundamentals that are relevant to and common across all missions. Therefore, it is recommended that this Handbook be used in conjunction with Center-specific institutional best practices documents.

FM is an element of any SE approach, and as such, this Handbook should be used as a companion to the NASA SE Handbook, though it is not currently at the same level of maturity. Whereas the SE process typically concentrates on achieving nominal behaviors, this Handbook provides guidance on designing to accommodate faults and addressing off-nominal conditions. Both "nominal" and "off-nominal" behaviors have to be considered, addressed, and designed together, thus providing a cohesive, comprehensive, and robust system.

1.3 Applicability

This Handbook is applicable to NASA flight systems; in particular, it provides a disciplined approach to engineering how a flight system will prevent, detect, isolate, diagnose, and respond to anomalous and failed conditions that interfere with intended operations. The initial focus addresses FM required for science missions; however it is recognized that FM is relevant to all NASA flight systems.
NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers, approve this Handbook for use. This Handbook may also apply to the Jet Propulsion Laboratory or to other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in their contracts, grants, or agreements.

[3] NASA/SP-2007-6105 Rev. 1, Systems Engineering Handbook. Washington, DC, 2007.

This Handbook, or portions thereof, may be referenced in contract, program, and other Agency documents for guidance. When this Handbook contains procedural or process requirements, they may be cited in contract, program, and other Agency documents for guidance.

1.4 Intended Audience

This Handbook serves the needs of FM practitioners and lead engineers by coalescing collective experience and recommended practices from across NASA and industry. However, the information contained herein is not for FM practitioners alone. This Handbook is intended for use by a variety of FM stakeholders during diverse program/project formulation and execution activities. These stakeholders include the following:

- Proposal evaluators responsible for assessing appropriateness of proposed FM designs.
- Stakeholders with management and oversight roles, e.g., program and project management, safety & mission assurance (S&MA).
- Stakeholders with interaction roles, e.g., system and subsystem engineers.
- Stakeholders with ownership roles, e.g., FM engineers and trainees.
- Stakeholders with customer roles, e.g., operations.

Table 1, Relevant Sections for Handbook Stakeholders, relates these stakeholders and their activities to the relevant sections of this Handbook.

Table 1—Relevant Sections for Handbook Stakeholders

Stakeholder Roles	Activity	Key Sections	Frequency
Program/Project Managers	a. Proposal development and establishing organizational structure b. Managing program/project throughout lifecycle and holding reviews	1, 4–6, 8 10-12	During proposal phase At the beginning of a program or project and at major milestones
Proposal Evaluators	FM proposal assessment	1, 4–6, 8	During proposal evaluation period
Systems, Spacecraft, Subsystem, and Instrument/Payload Engineers (e.g., software; electrical power distribution; guidance, navigation and control)	Engineering the system	All	Ongoing throughout all phases, especially at major milestones
Review Board Members	Major milestone reviews and FM reviews	1, 4–6, 10	At all reviews
Safety and Mission Assurance Engineers (e.g., reliability, maintainability, quality assurance, probabilistic risk analysis, etc.)	Developing reliability products (e.g., Failure Modes and Effects Analysis) and monitoring processes	All	Ongoing
Test Engineers	V&V activities	1, 4, 7, 9-10	Phase C/D
Operations Personnel and Anomaly Teams (e.g., on-console operators; anomaly resolution teams, anomaly investigation boards)	Operations	1, 4, 6, 7, 9, 11	Ongoing throughout all phases, especially at major milestones and during phase E
FM Engineers, Practitioners and Trainees	All FM-related activities throughout mission life-cycle	All	Daily/weekly A reference source during all phases, including proposal development

2. APPLICABLE DOCUMENTS

2.1 General

The documents listed in this section are applicable to the guidance in this Handbook.

2.1.1 The latest issuances of cited documents shall apply unless specific versions are designated.

2.1.2 Non-use of specific versions as designated shall be approved by the responsible Technical Authority.

The applicable documents are accessible via the NASA Standards and Technical Assistance Resource Tool at http://standards.nasa.gov or may be obtained directly from the Standards Developing Organizations or other document distributors.

2.2 Government Documents

NASA

Columbia Accident Investigation Board	Columbia Accident Investigation Board Report, Vol.1.
Fesq, Lorraine (ed)	NASA White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate
GSFC-STD-1000E	Rules for the Design, Development, Verification, and Operation of Flight Systems (Rule No. 1.17)
NASA/SP-2007-6105, Rev 1	Systems Engineering Handbook
NPR 7123.1A	NASA Systems Engineering Processes and Requirements
NPR 7120.8	NASA Research and Technology Program and Project Management Requirements
NPR 8705.2B	Human-Rating Requirements for Space Systems
NPR 8705.4	Risk Classification for NASA Payloads
NPR 8705.5	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects
NPR 8715.3	NASA General Safety Program Requirements

U.S. Department of Transportation	Federal Aviation Administration, 2010 National Aviation

2.3 Non-Government Documents

International Standards Organization

ISO/IEC 23004-6:2008	Information technology — Multimedia Middleware — Part 6: Fault management

Other

The National Academies Press	Decadal Survey of Civil Aeronautics: Foundation for the Future, 2006 (Steering Committee for the Decadal Survey of Civil Aeronautics, National Research Council)
Joint Planning and Development Office	Next Generation Air Transportation System Integrated Plan

2.4 Order of Precedence

This Handbook provides guidance for defining, developing, analyzing, evaluating, testing, and operating FM functions of flight systems, but does not supersede nor waive established Agency requirements/guidance found in other documentation.

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

AC	alternating current
ASIC	application-specific integrated circuit
BFCS	backup flight control system
C&W	caution and warning
C3I	Command, Control, Communication, and Information
CALIPSO	Cloud-Aerosol Lidar and Infrared Pathfinder Satellite Observation
CDR	critical design review
CERR	critical event readiness review
CFE	critical failure effect
ConOps	concept of operations
CONTOUR	Comet Nucleus Tour
D&C	display and control
DFMR	design for minimum risk
EDAC	error detection and correction
EDL	entry, descent, and landing
ESMD	Exploration Systems Mission Directorate
ET	external tank
FAA	Federal Aviation Administration
FCR	failure containment region
FDIR	Fault Detection, Isolation, and Response
FEPP	failure effect propagation path
FFRDCs	Federally Funded Research and Development Centers
FM	fault management
FMARR	fault management architecture requirements review
FMCDR	fault management critical design review
FMCERR	fault management critical event readiness review
FMCR	fault management concept review
FMEA	failure modes and effects analysis
FMECA	failure modes and effects criticality analysis
FMLRR	fault management launch readiness review
FMPDR	fault management preliminary design review
FMTRR	fault management test readiness review
FRB	Failure Review Board
FRR	flight readiness review
FTA	fault tree analysis
FTE	Full-Time Equivalent
g	gravity
GN&C	guidance, navigation, and control
GSFC	Goddard Space Flight Center
HGA	high gain antenna
HITL	hardware-in-the-loop

HQ	Headquarters (NASA, Washington DC)
I&T	integration and test
ICD	interface control document
IRD	interface requirements document
ISO	International Standards Organization (International Organization for Standardization)
ISS	International Space Station
JPL	Jet Propulsion Laboratory
JWST	James Webb Space Telescope
KOZ	keep out zone
LEO	low Earth orbit
LOC	loss of crew
LOM	loss of mission
LOV	Loss of Vehicle
MC	mission class
MCO	Mars Climate Orbiter
MCR	mission concept review
MDR	mission definition review
MER	Mars Exploration Rover
MO	Mars Observer
MPL	Mars Polar Lander
MRO	Mars Reconnaissance Orbiter
MSE	Mission System Engineer
NESC	NASA Engineering and Safety Center
NextGen	next generation
NPR	NASA Procedural Requirements
ORR	operational readiness review
OSMA	Office of Safety and Mission Assurance
PDR	preliminary design review
POC	point of contact
POR	power on resets
PRA	probabilistic risk assessment
RCS	Reaction Control System
RPOD	rendezvous, proximity operations, and docking
RSDO	Rapid Spacecraft Development Office
S&MA	Safety and Mission Assurance
SCA	Sneak Circuit Analysis
SE	systems engineering
SEU	single event upset
SIR	systems integration review
SMD	Science Mission Directorate
SOHO	Solar Heliospheric Observatory
SOI	Saturn Orbit Insertion
SPF	single point failure
SRR	system requirements review
STP	Space Technology Program
SysML	systems modeling language
TBD	To be determined

TBR	To be reviewed
TRL	Technology Readiness Level
TRR	test readiness review
TTC	time to criticality
T-VAC	thermal-vacuum
V&V	Verification and Validation
VHA	vehicle health assurance
WIRE	Wide-Field Explorer

3.2 Definitions

Abort: The action to prematurely terminate a mission prior to reaching its mission destination.

Anomaly: The unexpected performance of intended function.

Behavior: The temporal evolution of a state.

Critical Failure Effect: A failure effect, which if it occurs, will irrevocably compromise one or more system objectives.

Error: The difference between the desired (ideal) state or behavior and the estimated state or behavior.

Expectation: The most likely predicted state or behavior.

Failure: The unacceptable performance of an intended function.

Failure Containment: Preventing a failure from causing further failures.

Failure Detection: Determining that something unexpected occurred. Also referred to as fault detection.

Failure Preclusion: Actively preventing a failure from occurring.

Failure Prognosis: Predicting the time of a future failure.

Failure Recovery: An action taken to restore functions necessary to achieve existing or redefined system goals after a failure.

Failure Response: An action taken to attempt to retain or regain the system's ability to control the system state in reaction to a failure.

Failure Response Determination: Selecting actions to mitigate a current or future failure.

Failure Tolerance: The ability to perform a function in the presence of any of a specified number of coincident, independent failure causes of specified types.

Fault: A physical or logical cause, which explains a failure.

Fault Avoidance: Passive prevention of faults and failures.

Fault Containment: Preventing a fault from causing further faults.

Fault Diagnosis: Determining the possible locations and/or causes of a failure.

Fault Identification: Determining the possible causes of a failure or anomaly.

Fault Isolation: Determining the possible locations of a hypothesized failure or anomaly cause, to a defined level of granularity.

Fault Management: The engineering discipline that encompasses practices that enables an operational system to contain, prevent, detect, isolate, diagnose, respond to, and recover from conditions that may interfere with nominal mission operations.

Fault Tolerance: A synonym for failure tolerance.

Function: The process that transforms an input state to an output state.

Goal Change: An action that alters the system's current objective.

Knowledge Error: The deviation between the estimated state and the ideal expected state.

Measurement: The process of determining a specific value of an observable variable or phenomenon, the outcome of which helps identify an estimated state.

Model Adjustment: Modifying the model of the system upon which expectations of future states and behaviors are based.

Nominal: An intended, acceptable state or behavior.

Normal Operations: The activity of controlling a system to a goal that leads to achievement of the system's intended purpose.

Objective: The purpose of one or more intended functions.

Observer: A human or a human-generated algorithm, which inherently includes human engineering judgment, which monitors the performance of operational and/or non-operational systems, subsystems, devices, or components.

Off-Nominal: A state or behavior beyond the boundaries of possible expected states or behaviors. There are three off-nominal states: anomalous, degraded, and failed.

Operational: A functionally active system, subsystem, device, or component. (For systems, subsystems, devices, or components requiring an input—e.g., electrical current for power—to function, the system, subsystem, device, or component becomes operational when the input is applied and received successfully.)

Prognosis: Prediction of future states or behaviors.

Redundancy: Duplicate functions or mechanisms.

Root Cause: In the chain of events leading to a failure, the first fault or environmental

cause used to explain the existence of the failure.

State: The value(s) of a set of physical or logical state variables at a specified point in time.

State Determination: Ascertaining the current states of the system.

System: A combination of interacting elements organized to achieve one or more stated purposes.

System State: The set of all states in the system at a specified point in time.

Time to Criticality: The time it takes for failure effects to propagate from the failure mode to the critical failure effect.

4. PROCESS

The purpose of this section is to provide an overview of the FM process that should be a part of any NASA flight program. This section provides a standard process in terms of a set of terminology and work products to properly develop FM capabilities. Key activities that are part of the FM process include conceptual design development, requirements development, architecture and design, assessment and analysis, V&V, and operations and maintenance. An overview of each of these activities is provided in this section, followed by detailed descriptions in the subsequent sections of this Handbook.

Figure 2, FM Process as Part of SE Process, depicts the FM process, which follows an SE approach and shows the activities, work products/outputs, and reviews associated with the FM process. The process is shown as a timeline with the mission phases (i.e., phases A–E), mission-level, and FM-specific technical reviews (see table 3, NASA Mission Phases and Reviews) depicted at the top of the diagram. Also shown are the various external interfaces with which FM interacts, either in the form of receiving inputs from those interfaces in order to support the FM function or by iterating details of FM functions with those who implement FM, or are impacted by FM design decisions.

Table 3 provides an overview of the mission phases as well as the associated reviews that require FM participation; FM-specific reviews are discussed in detail in section 8.

Recommended Practice: ***FM matures in parallel with the nominal system and subsystems developments.*** *The FM function cannot wait until the system is defined and be added post-facto. FM matures in parallel with the system and subsystems.*

Table 3—NASA Mission Phases and Reviews

Phase	Description	Mission-Level Technical Reviews
Pre-A	Concept Studies	Mission Concept Review (MCR)
A	Concept & Technology Development	System Requirements Review (SRR) Mission Definition Review (MDR)
B	Preliminary Design & Technology Completion	Preliminary Design Review (PDR)
C	Final Design & Fabrication	Critical Design Review (CDR) Systems Integration Review (SIR)
D	System Assembly, I&T, Launch	Test Readiness Review (TRR) Operational Readiness Review (ORR) Flight Readiness Review (FRR)
E	Operations & Sustainment	Critical Event Readiness Review (CERR)

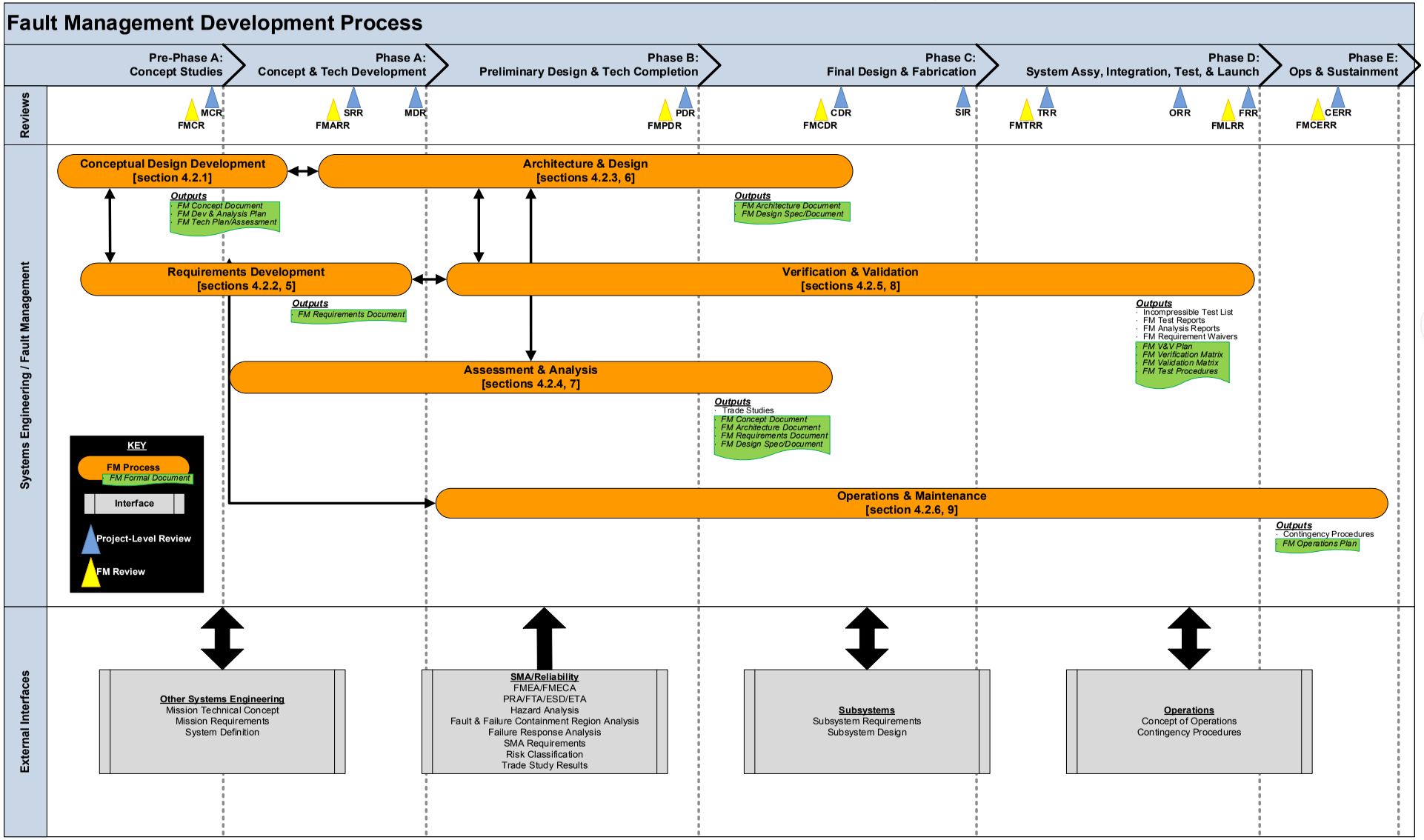

Figure 2—FM Process as Part of SE Process

4.1 Activities

4.1.1 Conceptual Design Development

FM conceptual design occurs in pre-phase A or early in phase A and is an iterative process that takes place simultaneously with, and is dependent on, the definition of mission requirements to ensure the customer's needs are met. The first step in the conceptual design is to define the FM boundary or scope, and to ensure that the size and complexity of the FM system matches the available resources and risk posture for the mission. The FM boundary is defined in the FM Concept Document and should encompass all elements of the system (i.e., hardware, software, and operations), all phases of the mission, all aspects of operating the system, the environment within which the system is required to operate, and the risk posture for the mission. All FM requirements should be cleanly derived from and traced back to the mission concept and risk assumptions outlined in the FM Concept Document.

The FM Concept Document is also used to provide a guiding focus for FM team members as well as to get buy-in on the FM ConOps from project management. The FM Concept Document contains the FM design principles that describe how FM will be applied, specifically to the given mission. The FM lead engineer develops FM ConOps and design principles by conducting science and engineering trade studies to develop a conceptual FM design that will be capable of detecting, preventing, correcting, and recovering from anomalies and failures that affect the ability to meet the mission goals and objectives of the customer within the resource constraints of the mission. The FM lead engineer works closely with system and subsystem engineers as they develop their requirements, conceptual design, and architecture in order to develop the FM requirements, conceptual design, and architecture in parallel. As programmatic assumptions and/or the development of mission requirements are refined, the conceptual FM design may undergo modifications. The conceptual-design development activity results in a baseline mission FM architecture that meets the goals and objectives of the mission and is capable of being implemented within the resources allocated to the project. Examples of the types of design principles that should be covered in the FM Concept Document include the sections that follow.

4.1.1.1 Unique Mission Design Characteristics

The first component of an FM philosophy is a complete analysis of the key mission design characteristics in order to identify unique mission challenges and unique advantages. Capturing distinctive mission design elements is critical in successful systems development, since it focuses the engineering team's mind on what needs to be done differently in comparison to past missions. At the same time, capturing the mission's risk category and approach ensures that FM will provide all required, and no unnecessary, risk mitigations.

4.1.1.2 Critical Events (Mission-Critical Activities)

Critical events refer to planned mission events (e.g., launch, orbit insertion, flybys, docking) or unexpected failure conditions that require a timely response to preserve level 1 mission science and/or the spacecraft itself (and a crew, if applicable). These events usually require a fail-operational response from onboard FM (as opposed to a fail-safe response). Compiling the list of critical events and understanding the constraints imposed by these events is important since the design of FM is driven by the need to survive these critical events.

4.1.1.3 Redundancy Philosophy

One of the most common methods to reduce mission risk (or improve mission reliability) is to add redundancy. Most often, redundancy is thought of in terms of hardware; however, functional/analytic and information redundancy should be considered. All NASA-sponsored missions with space payloads are required to adhere to the NASA Procedural Requirements (NPR) 8705.4, Risk Classification for NASA Payloads, which provides general guidance on the acceptability of single-point failure based on the mission risk classification. While guidance on single-point failures implies some direction on redundancy, the document leaves it to the engineering team to decide how best to implement redundancy requirements. The FM lead engineer uses the NPR as guidance regarding whether the mission will be fully redundant, selectively redundant, or non-redundant (i.e., single string); using trade studies, the FM lead engineer determines whether hardware, functional/analytic, or information redundancy is acceptable and, for hardware redundancy, determines the required level of cross strapping between components.

4.1.1.4 Safing Strategy

The spacecraft safing strategy is perhaps the most important design decision that the FM lead engineer makes to reduce mission risk. The term "safing" refers to a goal change from the current mission goal to another set of usually degraded goals (preserving some goals while jettisoning others) in order to preserve system assets. Depending on the type of mission, safing could be autonomous, ground initiated, or crew initiated. The safing strategy should present the following information to guide the FM system development process: 1) the safing strategy should clearly present the safe mode(s) and objectives; 2) the safing strategy should clearly state what classes of failure causes are expected to result in safing; 3) the strategy should show how a safing response will "safe" the vehicle from all identifiable situations, such as loss of attitude or loss of power, regardless of the cause, and even when faults cannot be hypothesized to cause these situations; 4) the safing strategy should show that "safety shall not be compromised" by the same credible fault that led to Safe [Mode] activation.[4] Further, it is important to realize that for each of these cases, there is an implied requirement on the operations team to be capable of diagnosing and recovering from these cases.

[4] NASA Goddard Space Flight Center. GSFC-STD-1000E, Rules for the Design, Development, Verification, and Operation of Flight Systems. Greenbelt, MD, 2009. Rule No. 1.17.

Pitfall: ***Projects often fail to adequately define and communicate mission attributes/concepts and function-preservation goals as a guiding philosophy.*** *As lower level FM decisions are made, they need to be made within the context of guiding FM philosophy and principles.*

Pitfall: ***Inheriting an FM system from a mission with a different level of complexity.*** *FM systems typically experience significant growth in complexity and cost late in the development cycle, often late enough to result in launch delays or delayed completion of all FM capabilities after launch. In particular, selecting a heritage system from a more complex mission for inheritance beyond the architecture level, or possibly design level, on a less complex mission may have unintended consequences on implementation, test, and operations. The time to analyze code or hardware paths may be significantly increased. The availability of options in the inherited approach may lead to acceptance of increased and unnecessary complexity. Even assumptions intended to simplify implementation and verification (e.g., stubbing out unnecessary paths) can actually increase the overall implementation resource requirements (e.g., by requiring additional verification to prove that all unnecessary or invalid responses have been adequately removed and that unwanted paths could not unintentionally be invoked).*

If any new technology is identified during the FM conceptual design development, the FM lead engineer documents it in the FM Technology Plan/Assessment. This new technology could be in the form of new FM technology required to protect mission functionality or new technology that supports FM development. This document defines the process for utilizing a new technology in the FM system or development. The assessment should include the technology descriptions, the plan to mature the technologies to technology readiness level (TRL) 6 by the PDR and fallback plans in the event the technologies do not reach TRL 6 by PDR.

Table 4, Summary of Inputs/Outputs of the Conceptual Design Development Activity, provides a summary of the inputs (i.e., documents, products, and activities) that feed into the conceptual design development activity as well as the outputs (i.e., documents, products, and activities) of the conceptual design activity.

Table 4—Summary of Inputs/Outputs of the Conceptual Design Development Activity

	Work Products	Description
Inputs	Mission Technical Concept	The technical approach and baseline mission architecture that meets the goals and objectives of the mission and that can be fabricated within the resources allocated to the project.
	Mission Requirements	List of mission science and engineering requirements necessary to meet the mission goals and objectives.
	Programmatic Assumptions	The program manager's allocation of project resources, such as schedule, budget, and launch vehicle options.
	Mission Design	Information on the specific mission design characteristics inherent to the mission. Special attention should be paid to those characteristics that can be utilized to simplify the FM conceptual design or that drive the FM conceptual design.
	Mission ConOps	The overall operations scenario that describes the end-to-end operation of the system after launch, including operational phases, payload operation/observation plans and schedules, ground communications schedule, data management, and other aspects of the day-to-day execution of the mission.
	Lessons Learned	Process improvement information for this phase from previous programs is incorporated into the implementation of this activity.
	Initial Risk Classification	The proposed risk classification for the mission and its associated justification.
	Analysis/Trade Studies	FM concept is developed, analyzed, and refined by using the output of scenario analysis; operational mode development; fault analysis, such as PRA, FTA, FMEA; and mission science and engineering trade studies.
Outputs	FM Concept Document	Defined in table 10.
	FM Development and Analysis Plan	Defined in table 10.
	FM Technology Plan/Assessment	Defined in table 10.

4.1.2 Requirements Development

FM requirements development begins in phase A, with final requirements being completed prior to the CDR. The FM requirements development/definition activity draws from the mission requirements that are derived by the Mission System Engineer (MSE) during the proposal phase as well as the S&MA requirements. The FM lead engineer, with the support of the SE team, examines initial project information to assess customer need and intent. FM requirements should be captured in the FM Requirements Document, which should present the FM requirements as a set of clear and concise mission-level engineering requirements allocated to systems (i.e., flight, ground, payload, and launch vehicle), and subsystems (i.e., hardware, software, mission operations, and crew, where appropriate).

The development of the FM requirements is an iterative process that takes place simultaneously with, and is dependent on, the development of the mission technical concept, the FM concept, and the fault tolerance, safety, reliability, and availability requirements. FM requirements are developed, analyzed, and refined by using the output of scenario analysis, operational mode development, fault analysis (usually begun in phase A and refined throughout phases B and C), and mission science and engineering trade studies. The input of these outside sources are used to formulate a series of mission-level FM requirements (see figure 3, Example FM Requirements Document Sections and Relationships to External Documents); these requirements usually begin with “The mission shall…” and define situations for which FM is responsible, the potentially bad things that should not happen, and the principles of the FM architecture developed in phase A. The requirements should not be one-to-one with faults identified in the FMEA process; rather, they should strive to demonstrate a reduction of potential faults into a smaller “failure symptom set” of required activities that the FM has to perform, required situations the system has to survive that handle all faults and failures in the analysis, and specific functions that are being protected/preserved without regard to the set of potential failure causes. In addition, requirements should not just be developed directly from the failure modes and effects analysis. Instead, requirements should describe a system-wide “safety net” that handles situations missed by failure modes and effects analyses. These “safety net” requirements may come from scenario analysis, operational mode development, engineering judgment, and lessons learned, but the primary driver for a “safety net” is the set of system functions that have to be preserved for a given mission/system. Finally, the FM lead engineer should consider requirements for test capabilities (e.g., fault injection in flight hardware and test benches) to ensure that test environments accommodate verification of individual FM software modules and failure scenario tests.

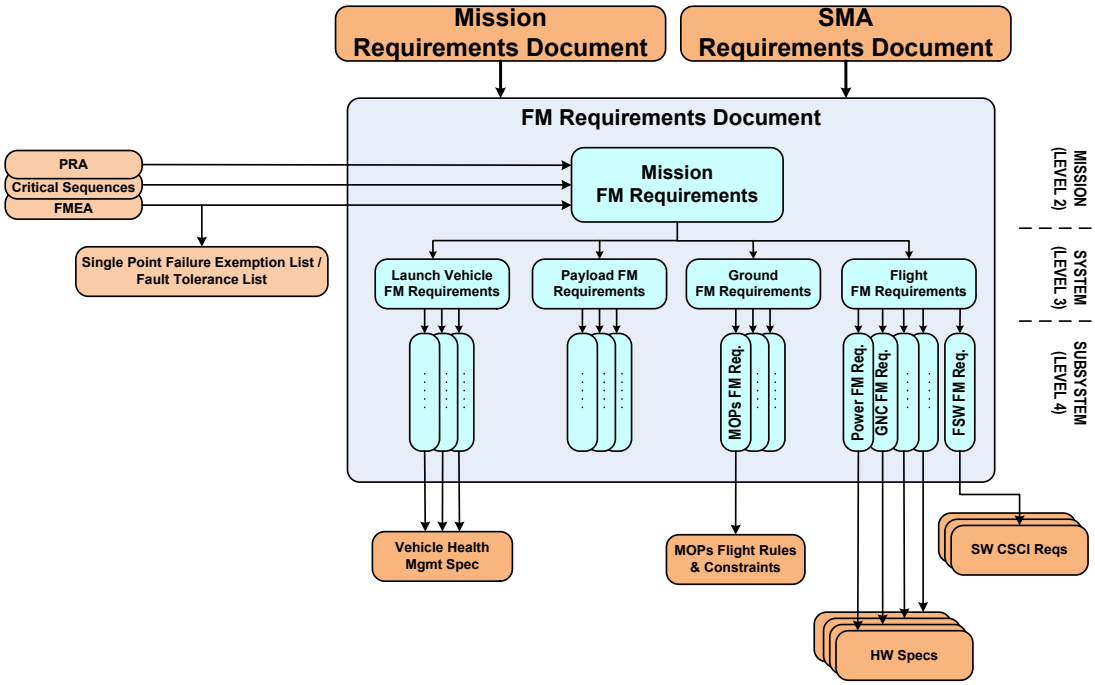

Figure 3—Example FM Requirements Document Sections and Relationships to External Documents

Once the mission-level FM requirements are developed, they are further broken down and, allocated to the various systems (e.g., flight, ground, payload), and then allocated to subsystems. The allocation of lower level FM requirements may be in whole (where one area takes full responsibility for the requirement) or in part (where multiple areas are required to take ownership in which the whole of all parts addresses the system-level requirement). During the allocation activity, the FM lead engineer works with other leads to determine the best and least risk area to take each requirement. Waiting too long to do this activity may deny allocation of requirements to certain areas, resulting in a less than optimal application of the prior FM experience and knowledge to the system design.

Table 5, Summary of Inputs/Outputs of the Requirements Development Activity, provides a summary of the inputs (i.e., documents, products, and activities) that feed into the requirements development activity as well as the outputs (i.e., documents and products) of the requirements development activity.

Table 5—Summary of Inputs/Outputs of the Requirements Development Activity

	Work Products	Description
Inputs	Mission Technical Concept	The technical approach and baseline mission architecture that meets the goals and objectives of the mission and that can be fabricated within the resources allocated to the project.
	Mission Requirements	List of science and engineering requirements necessary to meet the mission goals and objectives.
	S&MA Requirements	List of fault tolerance, safety, reliability, and availability requirements.
	FM Concept Document	Defined in table 10.
	Mission ConOps	The overall operations scenario that describes the end-to-end operation of the system after launch, including operational phases, payload operation/observation plans and schedules, ground communications schedule, data management, and other aspects of the day-to-day execution of the mission.
	Analysis/Trade Studies	FM requirements are developed, analyzed, and refined by using the output of scenario analysis; operational mode development; fault analysis, such as PRA, FTA, FMEA; and mission science and engineering trade studies.
	Initial Risk Classification	The proposed risk classification for the mission and its associated justification.
Outputs	FM Requirements Document	Defined in table 10.

4.1.3 Architecture and Design

The FM lead engineer begins developing the overall FM functions within the system in phase B, with the final design being completed prior to CDR. The development of the preliminary FM architecture and design is an iterative process that takes place simultaneously with, and is dependent on, the refinement of the FM requirements and the nominal system architecture and design. This activity results in refined technical FM functions within the system with the functionality and performance necessary to meet the goals and objectives of the mission within the resources allocated to the project.

During phase B, the preliminary design serves to expose the effects of multiple requirements interacting/interfering with one another (or otherwise negatively affecting the rest of the system) and to help define the mission ConOps. Under the direction of the FM lead engineer, functional analysis is performed and FM activities are allocated to transform the conceptual design developed in phase A into a technical system. The FM design process refines the FM requirements into a design that describes how failure conditions will be identified and what recovery steps will be taken. The FM lead engineer works with the SE and design teams to determine how each FM requirement should be implemented. This process may uncover

additional requirements needed to support the selected FM implementation. The preliminary design can take the form of timeline, state transition diagrams, or event sequence diagrams (often used in the scenario development associated with PRAs). Diagramming in this fashion forces development teams to consider how a system will react in the face of faults and to begin investigating the reaction responses in relation to what the mission has to accomplish during critical events. These high-level scenario diagrams enable early review of the off-nominal ConOps and provide an increased understanding of how the end system will function and provide context for test planning. The end result of this preliminary process is a technical specification called *FM Architecture Document,* which defines how all allocated FM responsibilities (defined in the *FM Requirements Document*) work together to form a complete system. It is important to nail down the hardware architecture to support FM goals/requirements during the preliminary design since it is difficult to change hardware after phase B.

Pitfall: ***Failure to consider test fidelity and resources early on in design planning.*** *When planning for an FM design, test platforms, a sufficient number of test platforms and adequate systems fidelity have to be planned early in the program because designing and building test assets takes time, and they need to be ready for early flight software testing. If it is discovered that there are inadequate test assets and fidelity at FM testing, it may be too late to avert a major schedule delay and cost growth. Suggestion: Build extra test assets and maximize fidelity as experience has shown that it will be used during the FM test "hump."*

Lesson Learned: ***(NASA Lesson Learned #0345) Mars Observer (MO), lack of system-level fault testing.*** *"From the analyses performed after the MO mission failure, it became apparent that the MO fault protection suffered from a lack of top-down SE in approach and design. Most fault protection was in the category of low-level redundancy management. It was also determined that the MO fault protection software was never tested on the flight spacecraft before launch. Design fault protection to detect and respond to excessive attitude control errors, use reaction control system (RCS) thrusters to control these errors, and always test fault protection software on the flight spacecraft before launch."*

Lesson Learned: ***(NASA Lesson Learned #1063) Lack of top-down SE in FM design introduces risk.*** *Lack of SE in the International Space Station (ISS) caution and warning (C&W) system design resulted in initiating a high-priority SE review of the C&W system to define a path for development and implementation of fully integrated alarm, situation assessment, countermeasure functions, and crew actions.*

The FM detailed design is finalized during phase C and consists of the allocation of FM functions to the different areas of the system and the proof that this allocation works at the system-level to lower the applicable risks of the overall system (e.g., risks of loss of mission (LOM) or loss of crew (LOC)). The detailed FM design is captured in the FM Design Specification/FM Design Document. Throughout phase C, the fidelity of the FM Design Specification/FM Design Document increases from descriptions of high-level interactions (i.e., between subsystems or between subsystem and ground) to detailed diagrams describing coordinated activities in terms of system/component states and detection, isolation, and reconfiguration schemes/algorithms for addressing faults and failures. The focus of this design activity is to identify adverse interactions, to define a system-level design that can implement the FM requirements, and to determine the adequacy of FM coverage. Ideally, the FM lead engineer

should "drive" the overall design and has ownership of the FM design. However, it is recognized that FM is a distributed function and that there will be overlap between information in the FM Design Specification/FM Design Document and individual subsystem specifications; however, these individual subsystem specifications should obtain information from and reference the FM Design Specification/FM Design Document.

To complete the FM detailed design, several existing products are updated based on the maturation of the overall design and several new products have to be created to capture all the activities of the planned FM system.

First, the fault analysis (e.g., FMEA) and scenario analysis (e.g., PRA) are refined based on modifications within the flight system and the FM Analysis Products associated with the "as-designed" system are created; this enables the revisiting of the single point failure (SPF) exemptions list/design for minimum risk (DFMR) list (or the fault tolerance list in the case of single string or limited redundancy system architectures), which should be finalized prior to the mission/project CDR.

Second, the FM Requirements Document is revised based on new fault/scenario analysis, new requirements, and/or increasing maturity of the FM concept. All allocation requirement sections within that document should be completed such that all mission-level FM requirements have been fully allocated to systems, and all systems-level FM requirements have been fully allocated to subsystems.

Third, modeling the system functions in a top-level fault tree or success tree and identifying the functional locations of the FM mechanisms, provides a means to assess the completeness of the FM design. The redundancy mechanisms identified in the tree specify the types of failures and faults that the FM mitigates, and just as importantly, cannot mitigate. When probabilistically summed, this provides a way for the FM practitioner to support the system probabilistic risk assessment (PRA). This information is needed by the system chief engineer and project manager to determine what risks are being mitigated by FM, and just as important, what risks are not being addressed by the current design.

Finally, the FM Design Specification/FM Design Document is updated with detailed descriptions and diagrams of the failure monitors and responses (if this approach is taken) and includes the assumptions, failure potential, potential hidden states within each design description, monitor/response prioritization (if applicable), and isolation and interaction prevention logic. The document contains the safing/abort design description, failure detection, isolation, and recovery algorithms, time critical sequences design descriptions, ConOps for the use of redundancy, and ConOps for pre-launch, ascent, post-launch and ground interaction, including diagnostics, repair, and recovery strategies, as appropriate.

Teams and individuals outside the FM team implement the majority of FM requirements, thus the act of forming a system-level FM design is a difficult activity with interaction between the FM team and other design and implementations teams. Again, it is difficult to avoid duplicate information with a distributed system, but the FM documentation (i.e., FM Requirements Document and FM Design Specification/FM Design Document) takes precedence and subsystem

documentation should refer to and reference the FM documentation. To ensure the success of the FM design and ensure that design and implementations of allocated FM requirements are suitable, the FM lead engineer has to perform oversight of the design and implementation of FM within all the allocated areas of the system. This oversight activity, which starts in phase C and continues until the implementation is complete, is a difficult and active role similar to the role defined in phase A of driving the architecture toward lower risk.
In this role, the FM lead engineer strives to understand the designs and implementations of allocated FM requirements sufficiently to do the following:

a. Question the implementations.
b. Understand the ramifications of the implementation on the system-level FM design.
c. Search for potential hazardous interactions between subsystem and system designs.

For example, many times subsystem leads cannot implement their subsystems as the FM requirements intended (e.g., due to cost, schedule, or technology limitations). Another example is the creation of new failure modes or revelation of new vulnerabilities based on the design or implementation of subsystems. In any case, performing oversight means the FM lead engineer has to actively work to provide the downstream effect of the design/implementation decisions, potentially define a new design/implementation that provides less risk at the system level, or take on new requirements to modify the FM concept and refer the potential change(s) to engineering review boards to discuss and approve cost and schedule changes.

Pitfall: ***Failure to appreciate overall cost-benefit of FM software/hardware infrastructure.*** *Often programs are scoped to meet FM requirements and not go beyond it. FM design and implementation infrastructure and flexibility are key areas where upfront investment can save significant downstream costs. Care needs to be taken to ensure that the flexibility does not degrade mission success or become untestable.*

Example 1 (software flexibility): A flexible FM implementation can allow for simple changes during the test phase, whereas a tangled interdependent inflexible design may require a complete re-V&V for what would be a simple change.

Example 2 (hardware infrastructure): Building in a fault tolerant hardware interface can simplify the possible failure modes to the nodes on either side of the interface rather than having to figure out if the interface itself may be at fault which could require a much more complex implementation.

Pitfall: ***Complexity due to absorbing the impact.*** *Design changes to other parts of a flight system can result in FM having to "absorb the impact." If FM is not involved with driving design decisions and does not have full involvement in subsystem-level designs and implementations, the FM design will be undermined, and will be vulnerable to an unsystematic approach that is difficult to test and to operate.*

Table 6, Summary of Inputs/Outputs of the Architecture and Design Activity, provides a summary of the inputs (i.e., documents, products, and activities) that feed into the architecture and design activity as well as the outputs (i.e., documents, products, and activities) of the architecture and design activity.

Table 6—Summary of Inputs/Outputs of the Architecture and Design Activity

	Work Products	Description
Inputs	System Definition	Definition of a technical system with the functionality and performance necessary to meet the goals and objectives of the mission and that can be fabricated within the resources allocated to the project.
	Mission Requirements	List of science and engineering requirements necessary to meet the mission goals and objectives.
	FM Concept Document	Defined in table 10.
	Mission ConOps	The overall operations scenario that describes the end-to-end operation of the system after launch, including operational phases, payload operation/observation plans and schedules, ground communications schedule, data management, and other aspects of the day-to-day execution of the mission.
	Analysis/Trade Studies	FM requirements are developed, analyzed, and refined by using the output of scenario analysis; operational mode development; fault analysis, such as PRA, FTA, FMEA; and mission science and engineering trade studies.
	FM Requirements Document	Defined in table 10.
Outputs	FM Architecture Document	Defined in table 10.
	FM Design Specification/FM Design Document	Defined in table 10.

4.1.4 Assessment and Analysis

Assessment and analysis supporting the FM effort may be performed by the FM team or by other teams depending on the project organization. A number of different analyses (including, but not limited to those listed in table 7, Summary of Inputs/Outputs of the Assessment and Analysis Activity) are used during the conceptual design development, requirements development, and preliminary design in phases A–C to identify possible faults/failures to be protected against and to identify possible response interactions or responses that may negatively impact another part of the system. Many of these analyses are iterative processes that take place simultaneously with, and are dependent on, the development of the mission technical concept and the FM conceptual design; these analyses are continually refined as more information about the system becomes available. The results of these analyses are used by the FM lead engineer to assist in the development of the requirements and the preliminary FM design.

Fundamentally, the FM lead engineer needs to know the following:

- What can go wrong?
- How often will it go wrong?
- What will happen if it does go wrong?
- What can be done to either avoid it or tolerate its effect?

To answer these questions, the FM lead engineer relies on assessment and analysis products to develop an understanding of failure scenarios as they propagate through the system. Various tools and techniques can be used to do the following:

a. Identify what can go wrong and where.

b. Examine the combinatorial effects of multiple failures and functional or physical dependencies and their impacts on the systems.

c. Explore the sequential nature of the system dependencies and timing.

d. Estimate or quantify system failure probability (NPR 8705.5).

This information allows the FM lead engineer to focus on failures that can propagate outside a system boundary, prioritize limited resources (both processes and development), and devise mitigations to alleviate identified concerns. These tools can also be used to reassess the implemented FM functions through updating with failure data discovered in test or on-orbit.

Table 7 provides a summary of the inputs (i.e., documents, products, and activities) that feed into the assessment and analysis activities as well as the outputs (i.e., documents, products, and activities) of the assessment and analysis activity.

Table 7—Summary of Inputs/Outputs of the Assessment and Analysis Activity

	Work Products	Description
Inputs	FMEA/Failure Mode, Effects and Criticality Analysis (FMECA)	The failure modes, effects, and/or criticalities of individual failure modes, generally in matrix form.
	PRA	The probability of LOC, loss of vehicle (LOV), or LOM, with sub-probabilities for various portions of the system in the fault trees and sequences used to perform the analyses. It is also used to identify major risk contributors.
	FTA	The identification of functional failures that the system has to protect against that are defined in the fault tree.
	Event Sequence Diagrams / Event Tree Analysis	Often part of the PRA; may be qualitative or quantitative. When quantified, the probabilities of occurrence of the various events in the sequences, usually fed into the PRA for overall system failure probability estimates. Identification of potential adverse system failure response interactions with each other and with the nominal control system.
	Hazard Analysis	Definition of the system's safety hazards and controls.
	FCR Analysis	Definition of the system's FCR boundaries and regions, with the specification of which faults and failures are contained at those boundaries.
	Failure Response Analysis	Quantitative (probabilistic) and qualitative assessments of the effectiveness of failure responses to mitigate the failures they are designed to address, including the timing race of failure response latencies versus failure effect propagations.
	FEPP Analysis	Identification of failure effects along all propagation paths associated with each failure modes, including groupings of failure modes that can produce specific effects that can cause loss of mission, vehicle, or crew.
	Failure Detection and Isolation Analysis	Qualitative and quantitative estimates of the effectiveness of individual and collective sets of failure detection algorithms, and vehicle sensors to detect failures and isolate faults.
	Failure Prognostics Analysis	Quantitative assessments of the effectiveness of prognostics designs intended to predict future failures, both in timeliness and accuracy.
Outputs	Trade Studies	Using the results from assessments/analyses listed above, trade studies are conducted to help with decision decisions.
	FM Concept Document	Defined in table 10.
	FM Architecture Document	Defined in table 10

	Work Products	Description
	FM Requirements Document	Defined in table 10
	FM Design Specification/FM Design Document	Defined in table 10

4.1.5 Verification and Validation

The FM V&V activity is started early in phase B and continues through phase D. In general, the FM lead engineer is responsible for the performance of the V&V of the system-level FM requirements and has oversight of the FM requirements allocated to various systems and subsystems. For the V&V of allocated requirements, the FM lead engineer has to evaluate the planning and procedures of the teams implementing the FM requirements and executing the activities.

The FM V&V Plan addresses the approach and risk posture to be taken for FM V&V. The plan documents guidelines, goals, and process steps for FM V&V actions. The planning effort should include test planning, plans for simulator development, test-bed certification, and identification of test assets and required fidelity. One important part of this definition is the identification and development of the FM Incompressible Test List (usually included in the FM V&V Plan). This list is a set of FM V&V actions that focuses on validating the core functionality of the FM system through realistic scenarios performed at the highest level of integration and defines the agreement between project management and FM on a list of tests that have to be completed successfully prior to launch. The incompressible test list may include both system and subsystem-level tests and defines the test venue (e.g., system, test bed, high fidelity simulator). It should be noted that the incompressible test list referred to here is the FM part of the overall project incompressible test list.

Additional support documentation is generated as part of the FM V&V process. First, the FM Verification Matrix describes the verification method(s) for each requirement and is created based on the completed FM Requirements Document. This matrix becomes the checklist for the FM lead engineer to ensure that all requirements have been verified. The verification method should specify who (NASA, contractor, etc.) is responsible for the test, what is needed for the test, and in what test bed or environment the test is to be performed. Second, the FM Validation Matrix is used to determine the set of failure scenarios and the validation method(s) for each failure scenario. Finally, for V&V performed by test or demonstration (at the system-level), 1) test procedures are developed with regard to the "Test what you fly, fly what you test" best practice, and 2) after test execution, test results are analyzed to determine if re-testing or regression testing is necessary and test reports are written. For V&V performed by analysis or inspection (at the system-level), reports or memos are written. Once the V&V assessment is complete, the FM lead engineer ensures that the V&V matrices are completed with the results of the V&V actions. At this point, the FM lead engineer determines and documents any necessary design changes or requirement waivers.

Table 8, Summary of Inputs/Outputs of the V&V Activity, provides a summary of the inputs (i.e., documents, products, and activities) that feed into the V&V activities as well as the outputs (i.e., documents, products, and activities) of the V&V activity.

Table 8—Summary of Inputs/Outputs of the V&V Activity

	Work Products	Description
Inputs	FM Design Specification/FM Design Document	Defined in table 10.
	FM Requirements Document	Defined in table 10.
Outputs	FM V&V Plan	Defined in table 10.
	Incompressible Test List	Defined in table 10.
	FM Verification Matrix	Defined in table 10.
	FM Validation Matrix	Defined in table 10.
	FM Test Procedures	Defined in table 10.
	FM Test Reports	Defined in table 10.
	FM Analysis Reports	Defined in table 10.
	FM Requirement Waivers	Waivers are written following any test or demonstration activity that shows a requirement was not met.

4.1.6 Operations and Maintenance

The allocation of FM responsibilities to operations and the incorporation of mission operations activities into the overall FM design should start as early as possible in the lifecycle. During the various other FM activities (i.e., conceptual design development, requirements, architecture and design), the FM lead engineer has to be cognizant of the influence the FM system has on the overall operations and maintenance of the project and has to coordinate closely with the operations team. A key area to focus on during phase B is the FM requirements allocated to mission operations. The FM lead engineer has to understand the ramifications and complexity of FM functions allocated to operations since in the past this has sometimes been performed in an inefficient, over-the-fence manner where requirements that are late or too costly for subsystems to implement are passed to operations without an appropriate trade study of the effect on overall lifecycle cost or mission risk. Assessing operability early can be a risk reducer for the mission and system in general, and for FM in particular.

Pitfall: ***Failure to consider impacts of deferring design functionality to operations.*** *FM has to consider implications of allocated FM functions to operations as FM requirement placed on operations can add complexity to the operations function. Table-based and script-based implementation strategies are very practical and flexible but can also lead to delayed requirements because tables/scripts can "always be added later."*

Pitfall: ***Failure to consider operations in nominal design.*** *An FM design that is not easy to operate may be cheaper in phases B and C, but phase D and phase E costs can significantly be increased due to complex, fragile procedures and operational sequences. An FM design has to consider the entire lifecycle cost and performance, not just near term milestones.*

Starting in phase A and continuing through phase C, the FM lead engineer works with operations staff to enumerate operational constraints and procedures that flow from the FM design or that will affect the FM requirements. By doing this, the FM lead engineer can understand the scope of the FM operations effort and can begin to understand the level of complexity and operability being imposed on operations. Conversely, operability considerations should flow back to the FM design as well as the overall system design. In addition, performing this activity in phases A-C enables the entire FM design (flight and ground) to be developed at the same time, enabling efficiency while also minimizing the possibility of design gaps. The FM lead engineer works with operations staff to develop detailed operations constraints and contingency procedures that implement the requirements allocated to ground and flight operations. Typically, contingency procedures are work products owned by the operations team; however, the FM team has significant input into these procedures and works with the operations team on their development. The development of the contingency procedures is an iterative design activity that uses the FM Requirements Document, FM Design Specification/FM Design Document, and engineering judgment to produce line-by-line procedures for interacting with the system during an unplanned or off-nominal event. The development of contingency procedures should start in phase C and may last into the early parts of phase E, if project schedules allow procedures and constraints required for later mission activities to be finalized during phase E. For ground operations and flight crew operations, these plans also include maintenance and repair procedures, including diagnostics as applicable to the system.

In phase D, the operations portion of the FM design can be completed in detail due to the increased fidelity of the implementation as well as complete command/telemetry dictionaries; and the FM team can complete the preparation of the FM system for operations. The FM team captures the day-to-day operation of the FM system from the vehicle operator's point-of-view in the FM Operations Plan. This plan addresses all mission phases, sequences, and modes when the FM system is used (e.g., pre-launch, launch, post-launch flight); FM transitions resulting from changes of phases, sequences, and modes; what needs to be done to perform check-out of the FM system; and plans for how to recover from safe modes or other off-nominal situations.

Finally, during phase E, the FM lead engineer supports activities, such as flight testing, calibration support, health and status monitoring, command script support, data handling support, and general support of science and program activities. The FM lead engineer is also involved with diagnosis and response to critical on-orbit anomalies and failures with the goal being to

support mission operations with solutions during off-nominal situations and gradually transfer oversight of FM from the FM team to the operations team.

Table 9, Summary of Inputs/Outputs of the Operations and Maintenance Activity, provides a summary of the inputs (i.e., documents, products, and activities) that feed into the operations and maintenance activities as well as the outputs (i.e., documents, products, and activities) of the operations and maintenance activity.

Table 9—Summary of Inputs/Outputs of the Operations and Maintenance Activity

	Work Products	Description
Inputs	FM Design Specification/FM Design Document[5]	Defined in table 10.
	FM Requirements Document[5]	Defined in table 10.
	Mission ConOps	The overall operations scenario that describes the end-to-end operation of the system after launch, including operational phases, payload operation/observation plans and schedules, ground communications schedule, data management, and other aspects of the day-to-day execution of the mission.
Outputs	FM Operations Plan	Defined in table 10.
	Contingency Procedures	Defined in table 10.

4.2 Summary of Work Products

As described in detail in the previous sections, various work products are developed during the FM process to support and describe the overall FM process. Table 10, FM Work Products, provides a list of work products to be produced during the various phases of the FM process. Not all of the work products listed in table 10 will be produced for a given mission. The risk posture of the mission drives the FM complexity and formality and, therefore, the cost and schedule. In addition, the document tree for a given project/program may dictate whether an FM work product is a separate document or is included as a part of another system-level document. It is recommended that projects have dedicated FM staffing in phase A. However, depending on the size of the program, the FM lead engineering position may not be staffed until phase B; in this case, phase A work products would be performed by a systems engineer.

[5] Although the FM Design Specification/FM Design Document and the FM Requirement Document are shown as inputs to the operations and maintenance activity, FM interacts with operations early in the FM process during both the development of the FM concept and FM requirements.

Pitfall: ***Budget and schedule deficiencies.*** *Failure to adequately budget and schedule for documentation, reviews, and spacecraft-level test preparation resources can lead to FM lagging the rest of the design instead of maturing in parallel with the system and subsystems. Addressing FM after the nominal system has been designed forces the FM system to become an added-on capability (which results in brittle designs that are difficult to test) rather than an integral part of the system.*

Table 10—FM Work Products

Work Products	Description	Phases
FM Development and Analysis Plan	Defines the process by which the FM functions within the system will be developed, taking into account both the size and complexity of the FM system and the available resources. The document should reference a defined process (i.e., an institutional-level document such as a FM Design Principles, Process, and Policies Document which documents that institution's FM process and the principles and processes extracted from lessons learned and disciplinary developments at that institution) and also describe any specific tailoring that has to be performed on the proposed project. This document outlines a high-level schedule of FM activities as well as tools and methods planned for use. This document also includes the type and description of all fault analysis activities that will be performed, how each of these fault analysis activities inter-relate, and how each of the activities will connect into the FM requirements.	A
FM Technology Plan/Assessment	Defines the process for utilizing a new technology in the FM design, development, or implementation. This document should include the technology description, the plan to mature the technology to TRL 6 by PDR, and fallback plan in the event the technology does not reach TRL 6 by PDR.	A
FM Concept Document	Defines the FM boundary, or scope, to ensure that the size and complexity of the FM functions within the system matches the available resources and risk posture for the mission. This document should include a description of the overall role of FM on the proposed project and key design elements including, but not limited to, unique mission design characteristics, critical sequences, redundancy philosophy, safing strategy, diagnostics architecture, failure recovery strategy, and maintenance/repair strategies.	A
FM Architecture Document	Documents the preliminary FM design that describes how the failure condition will be identified and what recovery steps are taken. This document includes timeline, state transition diagrams, and/or scenario diagrams to show how a system will react in the face of faults and the reaction responses in relation to what has to be accomplished in critical sequences.	B
FM Analysis Products	Products of the fault analysis activities. Depending on the project, these could include FMEA, FMECA, FTA, PRA, FEPP Analysis, Failure Detection and Isolation Analysis, Failure Response Analysis, Hazard Analysis, FCR Analysis, and Failure Prognostics Analysis.	A–C

Work Products	Description	Phases
SPF Exemptions List/Design for Minimum Risk List - Or - Fault Tolerance List	An SPF Exemptions List (also known as a Design for Minimum Risk List) or a Fault Tolerance List is generated depending on the level of redundancy of the project. For projects with redundancy, the SPF Exemptions List defines the agreement between project management and FM on a list of system components to which no FM will be applied. Note that any violation of the SPF list requires a project waiver with a thorough justification for class A missions (per NPR 8705.4, Risk Classification for NASA Payloads). For projects with limited or no redundancy, the Fault Tolerance List defines the list of functional or component redundancies that are applied to the system; all other items are SPFs that are accepted by the project.	B, C
FM Requirements Document	This document contains the system-level FM requirements as well as multiple sections of allocated FM requirements where FM responsibilities are allocated to subsystems, mission operations, and crew. Typically this is at level 2 (project dependent), though the level 1 mission-level requirement may have one or two basic FM top-level requirements.	B, C
FM Design Specification/ FM Design Document	Documents the FM technical system definition demonstrating how the FM responsibilities allocated to subsystems, operations, and crew (if applicable) will work together to keep the system safe and functional. The FM Design Specification (also called the FM Design Document) contains the design descriptions for the failure detection, fault diagnostics (fault isolation and isolation, whether automated or manual) as well as the failure responses including response sequences (e.g., safing, abort) and time-critical sequences (e.g., launch, orbit insertion), describes the assumptions, failure potential, and potential hidden states within each design description. Also described are the FM "engine," monitor/response prioritization, and isolation and interaction prevention logic. The design should be described in detail with pseudo-code and detailed design diagrams. This Handbook also contains the ConOps for the use of redundancy; and for pre-launch, ascent, post-launch diagnosis, and ground interactions, including contingency plans and maintenance/repair strategies.	B–D

Work Products	Description	Phases
FM Verification and Validation Plan	Defines the FM V&V approach, including the definition of what requirements are to be tested at what level of integration, the description of required regression testing, description of required post-test analysis, policy for when verification is complete and ready for launch, and policy in terms of test failure. This document outlines each of the planned system-level off-nominal tests, defines the testing environment required, and relates these tests to requirements and verification objectives. This plan also includes a description of how models and test beds used within the verification process will be validated. In addition, limitations to test-as-you-fly and their possible risks as it relates to FM verification should be documented.	B, C
FM Verification Matrix	Matrix of requirements and verification activities that demonstrates how each individual requirement in the FM Requirements Document will be verified. May be a separate document or included as part of the FM Requirements Document or FM Verification and Validation Plan. It has to include verification method, verification environment, person responsible for performing the verification, and person responsible for confirming the verification was properly achieved.	C
FM Validation Matrix	Matrix of FM functions and verification activities that demonstrates how each individual function will be verified. Typically, a large part is scenario-based testing with a high fidelity operational configuration with various injected faults.	C
FM Incompressible Test List	Defines the agreement between project management and the SE team on a list of FM V&V actions that have to be completed successfully prior to launch; these tests may include both system and subsystem-level tests. This list is often included in the FM V&V Plan; it should be noted that the incompressible test list referred to here is the FM part of the overall project incompressible test list.	B, C
FM Test Reports	Produced following each system-level test, these reports document the success/failure of the test, the requirements verified, and discussion of any discrepancies in the test or in the data collected during the test.	D
FM Analysis Reports	Document analyses that have been performed to verify FM requirements.	

Work Products	Description	Phases
FM Test Procedures	The set of associated test procedures (for the test and demonstration actions during the V&V process) that are developed. Note that the FM team may not be the developers of specific test procedures or perform the identified analyses, but in these cases, the FM team should have oversight of the test procedure generation process, and signature authority on the relevant procedures and analysis reports.	
FM Operations Plan	Defines how the FM system will be operated in flight. This document includes the configuration of the FM system for launch, flight, and other phases of the mission, a check out plan, a recovery from safing plan, a post-failure diagnostics plan, list of FM operational constraints, and maintenance and repair procedures.	D

5. REQUIREMENTS DEVELOPMENT

There is a saying that a project is no better than its requirements. Vague FM requirements are particularly problematic, because of the immaturity of the discipline and its historically inconsistent assumptions and expectations. Experience in robotic missions and reports in NASA Lessons Learned have shown that vague requirements carry the risk of omissions, inconsistent assumptions, and fragmented interpretation and implementation throughout the flow-down. In contrast, explicit, detailed FM requirements enables a clean, consistent flow-down and interpretation which allows for less design iterations, less disconnects and a more efficient V&V process resulting in lower lifecycle costs, and higher availability and robustness. Incomplete top-level FM requirements can force lower level subsystems and projects to make assumptions about key aspects of FM, posing a risk to the program level product (e.g., in terms of cost, schedule, safety and robustness). This section identifies some requirement categories to illustrate the breadth of issues that should be addressed. FM practitioners can use these recommendations and examples to develop better up-front FM requirements, which will facilitate a smoother and more deterministic FM implementation, with ultimately better coverage and effectiveness.

The purpose of this section is to provide guidance in the development of typical FM requirements that should be a part of any NASA program. Organizations that have designed many reliable systems have evolved a standard number of FM requirements, many of which are carried from project to project. These standard requirements and associated recommended practices and pitfalls often are documented in institutional guidelines and can be used as a starting point for FM requirements and provide context for avoiding deficiencies when developing FM requirements for new programs/projects. In addition, this section provides a few key placeholders and requirement categories to jump-start difficult project system-level FM requirements discussions with the goal to assist in developing high-level FM requirements.

The requirements and lessons learned captured in this section are collected from past NASA projects, and can help engineers and project managers assess the completeness and adequacy of their FM requirements. This section contains recommended FM requirements by describing example requirements, requirement types and rationale with some FM requirement flow down, based on other FM-intensive NASA projects. Note that this Handbook does not address the specific tailoring needed for any single program/project. The FM practitioner cannot simply cut and paste the example requirements shown here or from any other source. Actual requirements development requires a great deal of thinking, deliberation, and working through scenarios, implementations, and mission objectives (note, refer to section 6.1 for an overall mission risk posture and related requirement impacts discussion).

5.1 Writing Fault Management Requirements

How to write FM requirements can be summarized in a few general steps, as follows:

5.1.1 Know the Mission

Know the top-level mission class, risk posture (see section 6.1) and baseline assumptions on what the FM design is supposed to do; if that is not known, have discussions with program management and system engineers to build an initial consensus factoring in mission class, duration, critical events, and autonomous periods without ground contacts (if un-crewed). If other team members are not familiar with FM, a historical tutorial can help educate them. The FM risk posture should be consistent with allocated or at least available resources of all types: Personnel, budget, test beds, development, test time, etc.

Recommended Practice: ***Derive FM requirements from the mission concept and mission risk posture.*** *The FM requirements have to be clearly derived from the mission concept and risk posture and signed off at all levels, to control "requirements creep" as the project nears operation. Architecture and design decisions should trace directly to the FM requirements, based on a careful consideration of the complete FM life cycle.*

5.1.2 Consider Heritage

Most missions have heritage analogs, either in mission class and objectives or in specific hardware and software. Research similar mission requirements and evaluate them for completeness or holes. Note older missions tend to have fewer FM requirements than newer missions, mostly because the discipline is still maturing. Also, note that even if there is a heritage mission in terms of hardware and/or software that does not mean the heritage is applicable for the new mission. Early FM reviews should include heritage reviews in parallel or shortly after requirements are written (and before requirements are locked down) to ensure applicability. If a mission has new areas without precedent, focus extra effort in making sure the FM aspect and perspective of any areas are covered sufficiently.

Pitfall: ***Be careful of heritage requirements.*** *It is recommended to have centralized, top-down FM requirements defined in response to a mission's risk posture and unique objectives (as opposed to inheriting FM requirements without re-analysis); inherited requirements tend to be ill-fitted to new missions, and alone, bottom-up requirements development tends toward a disorganized set of distributed requirements with a difficult implementation, V&V, and ultimately performance shortfalls.*

5.1.3 Review All Categories

Next make an FM category list (see table 11, FM Requirement Categories) and expand it into subcategories until a list of candidate requirements is produced. As mentioned previously, it is typical to use other mission's example FM requirements and categories to initiate this process.

5.1.4 Determining Completeness

In order to determine and evaluate the FM requirements, the first step is to look for gaps while reviewing the categories and functional areas. Second, consider the system design. Think of all the hardware and software: What if it failed and what hardware, software, and functional redundancy are required? On this note, it is good to have FM architecture functional analysis at least started to aid in writing FM requirements. Finally, ensure that institutional policies,

practices, and principles are followed. It is recommended to write them explicitly as requirements, when applicable.

5.1.5 FM Requirements Checklist

When a set of FM requirements has been written, a checklist of things to consider when writing FM requirements is provided in the next sections. (Adapted from the NASA SE Handbook, Appendix C: How to Write a Good Requirement—a reiteration of the requirements validation checklist but populated with FM unique content instead of general system engineering content.)[6]

5.1.5.1 Clarity

Ensure FM requirements have one unique concept per requirement, as combination requirements are hard to split out at V&V time.

FM requirements are complex and the process of capturing all requirement rationales can be difficult as rationale paragraphs often get lost in requirements tools. However, the information is important and should be captured. With definitions used internally to a requirement (e.g., critical units), it is recommended that those be in-line with the requirement; or if there are many definitions, a separate glossary can be maintained. The risk is that a casual review will miss the subtleties of the term without the short explanation at the same place.

If all failure causes are the subject of a requirement, then the phrase "failure causes" should be used in writing the requirement instead of "faults." If the requirement pertains to internal causes, then the word "fault" is appropriate.

5.1.5.2 Completeness

a. State FM requirement assumptions whenever possible.

b. Capture TBD (To be Determined) and TBR (To be Reviewed) items in a complete listing maintained with the requirements. For example, if a system is being designed around a top-level critical, limiting constraint in a fault scenario such as power, rates, or thermal constraints, perform systems iteration as the design progresses.

5.1.5.3 Compliance

a. System-level requirements should be free of implementation specifics, but there may be core issues in FM that need upfront clarification from the top down, e.g., "There shall (or shall not) be a separate safe-mode computer," or " There shall be two of everything (versus internally redundant units).

b. No operations should be in FM requirements, but there may be core issues in FM that need up front clarification. For example, "the operator shall enable failure monitor X" is

[6] Also, see the NASA SE Handbook, sections 4.2 (Technical Requirements Definition) and 4.2 (Requirements Management).

something that belongs in ops procedures, not FM requirements, unless it is identifying/clarifying limitations on the level of automation provided by the FM system.

5.1.5.4 Consistency

a. FM requirements should be internally consistent. A mix of differing philosophies may result in inconsistent designs.

b. Consistent NASA FM terminology should be used.

5.1.5.5 Traceability

a. Differentiate between requirement needs and wants. If a requirement is not present, will the design work as intended, assuming the worst possible assumptions? This is often a difficult area in FM. Many requirements can seem extraneous, but without them, drastically different and unwanted design conclusions can be drawn and implemented without a contractual way to prevent it.

b. Ensure each FM requirement is accurately transferred and is traceable between all levels. Program engineers should ensure all levels meet the FM requirements.

Lesson Learned: ***Pay attention to the adequate flow of FM requirements to sub-contractors.*** *Projects may acquire components or entire systems from sub-contractors, which can lead to opacity in the FM system. Special attention needs to be paid to procured items to ensure that the FM requirements are adequately flowed to sub-contractors. One reviewer noted seeing inadequate FM requirements flow in projects ranging from the acquisition of an entire spacecraft down to individual components. For example, a spacecraft was purchased under the Rapid Spacecraft Development Office (RSDO) and during spacecraft I&T, it became clear that there was a significant disconnect between the FM implemented and the operations concept. It appeared the external supplier was solely concerned with development costs and delivered the spacecraft at launch +30 days without regard to operations complexity or system availability.*

5.1.5.6 Correctness

a. Are the FM requirements technically feasible given the program budget, schedule, and risk posture?

b. Are the assumptions of the FM requirements valid, e.g., level of redundancy, tolerance to SEUs, and operator errors?

5.1.5.7 Functionality

Are all the FM functions covered? At a minimum, failure detection, fault isolation (location), containment and response should be covered (see section 4.2 for a list of recommended FM functions).

5.1.5.8 Performance

a. Are all required FM performance specifications and margins listed (e.g., consider timing, throughput, storage size, latency, accuracy, and precision)?

b. Is each FM performance requirement achievable within technology and project constraints, and traceable to the mission attributes?

c. Are the tolerances overly tight or overly loose? Are the tolerances defendable and cost-effective? Ask, "What is the worst thing that could happen if the required tolerance, persistence, or threshold was doubled or tripled?" Also ask, "What is the worst thing that could happen if the required tolerance, persistence, or threshold was one half or one tenth?"

5.1.5.9 Interfaces

Are all the FM interfaces covered? Applicable items are FM hardware and software interfaces, FM Command, Control, Communication, and Information (C3I) interfaces, as well as test and operational interfaces.

5.1.5.10 Maintainability

Are there FM requirements for maintainability, be it flight code, ground procedures, threshold analysis models, or test files and revalidation scripts? This is particularly applicable for long duration missions or a product line that is gradually modified over time (e.g., components becoming obsolete or unavailable and so replaced with newer components or designs—the FM implications of a seemingly small change may be disproportionately large).

5.1.5.11 Verifiability

Ensure the FM requirements are verifiable. It is recommended to think of and document the V&V venue and method while writing and revising the FM requirements, as this will avoid rework later.

5.2 Fault Management Requirement Categories

FM requirements can be organized into categories for assessment, discussion, and understanding. Table 11, FM Requirements Categories, displays a set of FM requirement categories that can be used by programs and projects to assist in the determination of requirements completeness.[7] There are more categories and a lower level of subcategories, but the list shown in table 11 is an adequate set showing the typical areas of concern with respect to FM requirements. This set of requirements categories can also be used to develop a checklist to support the goal of requirements completeness.

A key point of the following categories is implicit/general versus explicit FM requirements. Explicit requirements can allow for a clean, consistent flow-down and interpretation, which

[7] Originally based on robotic missions but applicable to any NASA mission.

allow for less design iterations and disconnects, as well as a more efficient V&V process. Implicit or general requirements are not recommended as lower levels and subsystems may interpret these requirements in different ways, causing mismatched expectations, inconsistent implementations, and high likelihoods of missed functionality, which introduce a high level of risk to overall mission success.

Table 11—FM Requirement Categories

Category	Topic #	Included Topics	Comments
Scope	1.1	FM Robustness	Aspects of the design that make the design more robust, especially against unknown unknowns
	1.2	Environmental Tolerance	
	1.3	Autonomous Recovery	This can be a broad topic on what the true driving autonomy requirements are aside from requirements on fault tolerance.
	1.4	Fail Operational	Identifies fail operational specifics. These usually drive the limits of the FM architecture and design.
	1.5	Fail Safe	Fail safe versus fail operational requirements drive the FM response architecture and implementation.
	1.6	Fault/Failure Tolerance	Failure tolerance is a key category and contains most of the top-level, architecture driving requirements. Getting an agreed upon commitment to how a design will tolerate failures is key to having a clean, consistent FM design implementation.
	1.7	Required Functionality in the Presence of a Fault	Effectively a subset of failure tolerance, this usually is focused on spelling out specific items.
Functions	2.1	Allocation of FM Functions	This helps to clearly spell out who (onboard autonomy, ground, crew) is responsible for what in an FM design and implementation, the roles and responsibilities of an FM design.
	2.2	System Responsibilities	
	2.3	Failure Detection	Onboard detection generally required to level necessary for successful response.
	2.4	Fault Diagnosis	Includes isolation and identification. Isolation levels vary based on mission modes. During flight, isolation generally to level required for successful response (often, to the level of onboard redundancy). For pre-launch, or between flights for reusable systems, isolation typically to the line replaceable unit level. Identification is generally a ground-based function.

Category	Topic #	Included Topics	Comments
	2.5	Failure Effect Propagation	Failure effect propagation also relates to the fail safe and failure tolerance categories, but it is important to have baseline requirements on what failure effects are allowed to be since it can affect the design.
	2.6	Fault Isolation (Determine Location)	Refer to Topic 2.4 in this table.
	2.7	Failure Mitigation	
	2.8	Failure Notification	Relates to messages about critical failure conditions and system responses
	2.9	Fault Prevention	
	2.10	Failure Response (Recovery, Reconfiguration)	Responses retain (masking) functionality, recover functionality, or change system goals to achievable objectives.
Performance	3.1	False Negatives (Undetected Faults)	
	3.2	False Positives	False positives (or false triggers) focus on the mitigations and levels of robustness against false positives, i.e., accidental triggering of fault monitors. Most missions have this occur at least once. How it is dealt with can be as important to mission success as other key aspects. Note there is a related opposite category, false negatives (undetected failures).
	3.3	Acceptable Failure Effects	Sub-category of failure tolerance which includes the subset of design features where acceptable failure effects for cases that can have a wide variety of acceptable outcomes from a given standpoint, may have tight constraints from a mission perspective or other considerations.
	3.4	Availability	Places time constraints on system safing modes and recovery responses.
	3.5	Consumables	Knowing upfront what the allowable consumable depletion is in the presence of a fault can often be a key design driver in the sizing of consumable tanks, batteries, and cycle life.
	3.6	Degraded Operation	Safing modes, changed system goals

Category	Topic #	Included Topics	Comments
	3.7	Do No Harm	Ensuring that FM design mechanisms improve reliability, and do not create conditions worse than the failure effects that they mitigate
	3.8	Irreversible Action Robustness	
	3.9	Operability	This category includes only the subset of design features that affect operability. An FM implementation can meet all requirements but be very difficult to operate (in terms of prediction, reconstruction, real time, and non-real time telemetry) without clear requirements on operability. An operations section is not required, but it serves as a place to formalize expectations in FM operations.
	3.10	Reliability	One of the drivers of required risk levels.
Design	4.1	Design Feature	Design feature is a category for any requirement that places a specific FM design requirement on the design. For larger distributed projects with contracted-out FM implementation, this is a good way to set specific expectations of the FM design, which can prevent much unnecessary and possibly prolonged contract re-negotiations as well as ambiguous or unclear expectations as to what feature the customer is expecting from the FM implementation.
	4.2	Response Time	This category focuses on response time—or TTC for any area of the FM design.
	4.3	Safe Mode Design/Safing	
	4.4	Sanity Checking	
	4.5	Degrade Modes	Degraded modes include the safe mode example. Safe mode is a core FM defined safety mode for most unmanned missions and unmanned mission phases, but can also apply to manned phases and other degraded modes.
	4.6	Fault Containment Regions—Software Data	Limits the effects of FEPPs within computing systems

Category	Topic #	Included Topics	Comments
	4.7	Fault Containment	This category includes the subset of design features that address fault containment; i.e., the identification of FCRs and the requirement for containment of complex failure conditions. Note this is effectively a sub category of Failure Tolerance.
	4.8	Time to Criticality	FM mitigations have to operate faster than the TTC for each function to be protected.
	4.9	Parameter Determination	This category includes only the subset of design features that affect the determination of FM parameters, which can include threshold, persistence, mode, phase, and hardware configuration dependency.
Process	5.1	Analysis	Analysis requirements ideally should be part of an FM planning or practices document, but if that is not a contract deliverable, it can be better to formalize them as requirements.
	5.2	Operations	An operations section is not required, but it serves as a place to formalize expectations in FM operations.
	5.3	Testing	A test section is not required, but it serves as a place to formalize initial expectations in FM testing.

Pitfall: ***Requirements Formulation.*** *It is important to know if a set of requirements appears to be incomplete based on historical precedence. Some questions to ask in determining completeness:*

- *Is the number of top-level FM requirements less than expected when compared to other programs/projects of similar size/complexity?*
- *Are the FM requirements spread out among multiple documents?*
- *Are the FM requirements vague, ambiguous, too general, implicit, or abstract?*
- *Do most of the lower level FM requirements have insufficient detail and is flow-down inappropriate?*
- *Do the FM requirements address all of the FM functions? If not, they are likely missing something.*

Some key FM requirement categories are high-level fault tolerance policy, aspects of overall reliability, required functionality in the presence of a failure, redundancy management guidelines/approaches, failure effect propagation, allocation of fault classes (e.g., flight versus ground, random part failure, operator faults, design faults, transient versus permanent failures), use of redundant hardware, fault containment (see section 5.1).

Recommendation: The project FM requirement set should include key aspects of off-nominal strategy. Some examples are as follows:

- *What is the required functionality in the presence of a failure?*
- *What is the required response time given TTC (e.g., 0.1 sec, 1 sec, 1 orbit) for various faults?*
- *What are the performance requirements in the presence of a failure?*
- *What is the allowable consumable consumption after certain failures?*

Refer to section 5.1 above for a list of FM requirement categories that can help identify requirement deficiencies and omissions in the requirement set.

The existence of an appropriately broad set of FM requirements is proof that the necessary thought has been put into the preliminary design, the development of the architectural principles, and nominal/off-nominal ConOps. Absence of this broad set indicates that design and analysis areas may be under-explored.

5.3 Fault Management Driving Requirements

This section focuses on identifying key driving requirements. While section 5.2 discussed key requirements in many different areas, what sets this list apart as a noteworthy subset is that these few requirements completely drive the system design, the FM architecture as implemented in hardware, software, and operations.

Table 12, FM Mission Classes and Requirement Considerations, lists some FM requirement considerations of various mission classes (refer to section 6.1 for additional discussion).

Table 12—FM Mission Classes and Requirement Considerations

Mission Class (MC)	Mission Type and Risk Tolerance	Fault Tolerance Requirements and Approach
A	Flagship mission; low risk tolerance /high robustness; all practical measures taken to assure mission success.	Single fault tolerance; single fault and environmental effects; possibly select multiple fault tolerance; fully redundant systems with extensive FDIR.
B	Low risk /high robustness with select compromises where necessary	Single fault tolerance, or single fault and environmental effects with some exceptions; mostly redundant systems with select single-string elements and extensive FDIR
C	Medium risk; able to tolerate some risk to mission or degraded mission return.	Selected fault tolerance; mostly single string with select redundancy or graceful degradation; lower grade parts or exposure to failure conditions is permissible.
D	Medium to high risk; able to tolerate loss of mission objectives for failures.	Minimal fault tolerance where necessary; single string.

Table 13, FM Driving Requirement Areas and Examples, provides some of the typical driving FM requirements. This is not necessarily complete and does not account for unique project type requirements, but provides insights into driving requirements identified on numerous missions of various mission classes.

Table 13—FM Driving Requirement Areas and Examples

Legend Note: Column MC = Mission Class.
A mission class letter in italic means it may apply.

Driving Requirement Area	Driving Requirement Example	MC	Comments, Notes, and Definitions
Fault/Failure Tolerance	a. No single permanent hardware fault and one or more non-simultaneous recoverable faults shall cause a loss of mission. b. Any exceptions shall be separately exempted from this requirement via SPF/DFMR or other rationale.	A, B	For dual string missions. Due to the overarching scope of this top-level requirement, it is useful to define terms inline, e.g., "A recoverable fault can be an operator fault or environmental fault or software fault." "A hardware fault is a unique single fault—not a 'common cause' design error causing multiple hardware faults, which would be exempted."
Fault/Failure Tolerance	No single SEU or software fault shall cause an LOM.	C, D	For single string missions where redundancy does not exist, but onboard FM exists to reboot the system or system components.
Fail Safe/Fail Operational	The project shall fail safe for critical faults outside of critical events and shall have the ability to fail operational for critical faults during mission-critical events and fail operational for specific non-critical faults.	A, B	Critical faults are those that may endanger spacecraft health or mission objectives if not responded to. Mission-critical event examples: Launch, separation, deployments, orbit insertion, critical science periods, and entry, descent, and landing (EDL).
Time to Criticality and Response Time	The project shall respond to failures in a timely fashion before mission objectives are irrevocably compromised or non-recoverable damage is done.	A–D	

Table 13—FM Driving Requirement Areas and Examples

Legend Note: Column MC = Mission Class.
A mission class letter in italic means it may apply.

Driving Requirement Area	Driving Requirement Example	MC	Comments, Notes, and Definitions
Availability	The project shall be able to perform its mission requirements at least X percent of the time.	A–D	Alternatively, this can be phrased as a maximum outage duration and frequency.
Autonomous Recovery	The project shall be able to survive any single failure, without any ground assistance for at least the following. For Launch: TBD For Cruise: TBD For other Critical Events: TBD	A, B	Include notes with the requirements, e.g., "Note: Times for autonomous operation without ground contact are based on the duration to the next ground command plus additional time if initial ground contact fails."
Autonomous Recovery	The project shall be able to survive any one SEU or software fault, without any ground assistance for at least one ground pass duration.	C, D	Include notes with the requirements, e.g., "Note: Times for autonomous operation without ground contact are based on the duration to the next ground command plus additional time if initial ground contact fails."
Fault Containment	The project shall have hardware and software fault containment regions to prevent a single fault from impacting critical functionality or preventing use of multiple units or subsystems.	A, B	This category includes only the subset of design features that address fault containment—either the identification of FCRs or mandating containment of various non-straightforward failure conditions. Note this is effectively a sub-category of failure tolerance.
Operations	The ground is responsible for diagnosing and recovering all faults with a TTC greater than X.	A–D	Up-front specification on what operations' roles and responsibilities are with respect to FM can avoid cost and schedule overruns later in the development cycle.

Pitfall: ***Writing a small number of general high-level (or implicit) FM requirements (e.g., "protect against faults," or "do FM") in order to provide an implementer (i.e., a supplier or an in-house development team) with greater design freedom.*** *While seeming like a way to reduce paperwork or to allow designers to design unencumbered, it has many downsides, such as the following:*

- *Causing open-ended designs that can arbitrarily be declared finished, when, in fact the product is substandard. This can be especially difficult when projects are contracted out and resources are tight. The converse can also be true (typically with lower-mission classes). Poorly defined limits on the desired fault tolerance can allow designers to over-design, and end up with a system that is more complex or costly than strictly necessary to meet mission needs.*

- *The lack of detailed and specific requirements results in inadequate verification actions, and puts an inappropriate onus on the validation actions to certify the system behavior; specifically, the V&V matrix often has to be generated from scratch (at a significant downstream resource cost) because the framework was not developed upfront at the requirements stage.*

- *Design implementations overlook core driving requirements and functionality, e.g., a critical phase or activity that drives the entire architecture. The results of missing this can be catastrophic to an FM implementation schedule and to resource constraint.*

- *Subsystem design implementations can become inconsistent and may not work together or with the system FM design. The resulting interface and behavioral issues are usually only caught in system test, when the cost for making changes to the design is much more severe than in the design phase.*

Also, note a type of general requirement is a vague requirement. It may have more detail than a typical "general requirement," but a vague requirement can have many different, equally valid, interpretations. The example "protect against faults" does not define what a fault is, whether it includes environmental effects, such as SEUs, and whether it is single- or multiple-fault tolerant. Any of a number of solutions could be designed which meet this vague requirement.

Pitfall: ***Requirements are too specific.*** *Writing too many low-level specific FM requirements (e.g., "have a monitor X with response Y") in order to give an implementer (supplier or in-house) a very deterministic foundation upon which to implement, can seem like a way to reduce the uncertainty and to achieve a desired product, but it has many downsides such as:*

- *Design realities inevitably change through the project lifecycle, and even cookie cutter designs end up requiring unforeseen modifications that can cause specific requirements to break. In a dynamic design environment, precious resources can be spent continually fixing requirements instead of focusing on the implementation at the proper level.*

- *Requirements flow-down becomes a cut and paste exercise if top-level requirements are over-specified, thereby defeating the point of having levels of requirements,*

resulting in a single FM level of requirements being implemented. This can work if it is planned and consistently implemented that way, but implementing in this manner is very difficult.

- *Design is too rigid to mesh with heritage code and hardware; this is especially true with missions that use many heritage components. Existing subsystem code bases have to be opened up to shoehorn in the over-specified FM requirements.*

Recommended Practice: ***Determine top-level requirement strategy.*** *There are two main strategies to writing top-level requirements. For "in-house" designs where all designers are co-located and work to similar design principles and project practices, fewer number of general requirements may be sufficient, with the expectation that the detailed derived requirements will be in-family (i.e., like previous projects with similar systems and mission profiles, if applicable), and their implementation and interactions will be well-understood. (Note this strategy has risk, but in a constrained budget environment with limited FM team resources, this strategy can free up time that would be spent on detailed requirements and V&V matrices, for design, and implementation.)*

For "out-of-house" subcontracted designs where detailed requirements documents and interface requirements documents (IRDs) are essential for capturing all requirements and design assumptions, the requirement writers and designers cannot make assumptions on implemented design, especially when a contractor is responding to incentive contract realities.

Recommendation: If unsure, FM should use the minimum ambiguity "out-of-house" requirement strategy, because a lack of maturity in FM concepts and methodology becomes more evident in the "out-of-house" model, where assumptions and cultures regarding FM are likely to be different. In the "in-house" model there is more likely to be general agreement on the FM methodology, approach, and risk posture.

Pitfall: ***Issues with requirement interpretation.*** *Large programs with various subprojects (each with very different objectives) can have issues with project interpretation, causing potential problems and confusion. Below are two options to carry down project unique requirement specifics from top-level requirements documents to lower level requirements documents:*

Option One (Project specific): Carry sub-project specifics down from top-level, mission-level requirements, such as the following:

- *Project A shall be single fault tolerant.*
- *Project B shall be two faults tolerant.*

Option Two (phase specific): Carry mission-phase-unique specifics down from top-level, mission-level requirements, such as the following:

- *Phase A shall be single fault tolerant (note this would imply Project A).*
- *Phase B shall be two fault tolerant (note this would imply Project B).*

Pitfall: ***Institutions disagree about which faults and failures require protection (i.e., scope of FM).*** *Some institutions traditionally guard against only the most likely failures i.e., (a*

probabilistic approach) while others take a "possibility over probability," and thus try to account for all possible/credible failures. Given different tacit 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 typically is not 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 an FM system capable of handling critical events (i.e., fail-operational capabilities), which then leads to contract renegotiations and is a factor contributing to FM-induced cost overruns.

Pitfall: ***Use of probability in FM design.*** *Selecting faults based on probability can result in a system being less robust than expected, because experience has shown that low probability and unconsidered items are often the items that fail in-flight. Both the values and the uncertainties associated with probability estimates are frequently and significantly underestimated.*

Background: The Constellation Program FM Team determined that Constellation projects were using LOC/LOM probability metrics to help choose which faults to monitor and predict. Experiences from past in-flight failures has shown that most failures are in unexpected places and can be caused by design (software and hardware), parts and manufacturing faults often completely invalidating the upfront perceived reliability numbers for those components. Sole use of fault probabilities to decide which faults to protect against can lead to holes in the design and to a lower level of robustness than expected.

Recommendation: All electrical faults and all protectable mechanical faults[8] should be considered credible and appropriately protected against for the mission risk posture; since experience has shown that low probability items can fail in-flight. In addition, all critical active functions need a safety net protection to protect against unknown fault mechanisms. Example: It is often appropriate to not directly detect and respond to many low-level complex failure modes at the subsystem level, if it can be completely demonstrated that an adequate higher level safety net will meet mission FM requirements with no interaction or slow response time issues. Be careful when giving up lower level protection as safety nets have their limits and can get confused, especially in multiple or cascading failure event scenarios.

Pitfall Applicability: This pitfall is applicable to all projects attempting to use probabilistic methods to architect and selectively scope a FM design. Projects should design FM systems with clear top down principles and policies and protect core health and safety functions, especially electrical and redundant moving mechanical assemblies, regardless of the probability of failure, because design and manufacturing faults can often render those probabilities inaccurate in flight.

5.3.1 Test Platform Requirements

[8] For mechanical item classes that cannot be or are not readily able to be made redundant, factors of safety or Design For Minimum Risk (DFMR) practices are used to reduce credibility.

The FM team has to provide inputs early (early phase B) regarding what the FM fidelity requirements are for test resources, as well as FM test resource allocation to test platforms, using the FM Verification Matrix. Detailed input from the developers is required to determine the test-bed requirements. Issues that need resolution include:

- Who owns and maintains the test bed?
- What functionality and precision is required of the test bed?
- Who provides Configuration Management of the test bed?
- How long will the test bed be available?
- Will the test bed be available during the mission operation?

Below are a few test platform requirement categories and examples.

5.3.1.1 Fault Injection Requirements Category

a. **Concept:** Fault injection requirements are required so that test-bed venues (be it simulators, emulators, engineering models or flight hardware) are able to test the FM software (or hardware or firmware). The injection requirements should be broken down by sensor/actuator/subsystem and by FMEA failure modes of computers, interface buses, sensors, actuators, dynamics models (including deployment dynamics and propulsion), environment, power, thermal, instruments, radio frequency (when applicable) and harness (if not covered elsewhere). The injection of some faults may require intrusion into the sensor/actuator/subsystem, or may be damaging to the hardware. As such, the verification of the failure monitoring, fault identification, and failure response may need to occur on separate test beds at differing times of development. Not all fault injection can occur at system integration.

b. **Example Requirement:** The test-bed's attitude control system reaction wheel assembly model shall be capable of injecting all faults specified in the reaction wheel FMEA.

5.3.1.2 FM Functional Fidelity Requirements Category

a. **Concept:** FM functional fidelity requirements ensure that the test-bed venues (be it simulators, emulators engineering models or flight hardware) are able to test the FM (software, hardware or firmware) with sufficient functional fidelity. Example: A project may have planned to provide an open loop thermal power simulation at the simulator level to save resources, and the monitoring and response timing is non-critical.

b. **Example Requirement:** The thermal software simulator test-bed shall have the following models:

(1) Required sensors and actuators.
(2) Power.
(3) Thermal.
(4) Full dynamics.
(5) Be able to run flight code images.

5.3.1.3 FM Timing Fidelity Requirements Category

c. **Concept:** FM timing fidelity requirements ensure that the test-bed venues (be it simulators, emulators engineering models or flight hardware) are able to test the FM (software, hardware or firmware) with sufficient timing fidelity. Example: A project may have planned to provide an open loop guidance simulation at the simulator level to save resources, but the FM testing requires a highly accurate closed loop model to V&V key system scenarios. Fidelity examples include flight code treatment, interface bus treatment, simulated units and model commonality, and subsystem models and commonality.

d. **Example Requirement:** The software simulator test-bed for of telescope fine guidance verification shall have the following models:

(1) Required sensors and actuators.
(2) Full dynamics operating to specified timing jitter and accuracy.
(3) Be able to run flight code images.

5.3.1.4 FM Test Automation Requirements Category

a. **Concept:** FM testing requires many hundreds or even thousands of tests to perform a complete V&V. Running all these tests manually is not as efficient as automating the testing and data collection and perhaps even limited interpretation processes. Automation can better provide verification of test passes/failures, and/or accurate regression testing.

It should not be assumed that ground operations software meets these requirements. Test-bed operations supporting automation have differing requirements for scripting tests, pass or fail verification, and recording the results. Also, test-bed operations can require the proper initialization of the external test environment, such as proper power, thermal, pressure, and bus configurations.

b. **Example Requirement:** The Project's software simulation test bed shall be able to do the following:

(1) Automatically run FM tests.
(2) Collect the data.
(3) Generate an automated test report.

5.4 Requirements Development and Flow-Down

The FM requirements document contains the system-level FM requirements as well as multiple sections of allocated FM requirements where FM responsibilities are allocated to subsystems, mission operations, and crew. Depending on the scope and size of the project, this Handbook can be used at different levels. For example, the highest level requirement may be in a level 1 document, such as "the project shall be single fault tolerant," but the level 2 FM requirements document will capture most of the key requirements. If a project is split between a project

management center and a prime contractor, the FM Requirements Document may be split in this manner, e.g., higher level requirements at level 2 customer level, and the middle- level contractor-specific items at level 3, with level 4 having the detailed subsystem FM content.

Often, there is not just one FM requirements document as the only home for FM content. For example, some programs have embedded FM requirements in interface control document (ICDs) or IRDs. The system FM lead engineer should be responsible for one driving document that can be flowed down clearly to lower levels, and that document can be at different levels depending on the organization structure and the program size.

The following recommended practices and pitfalls are to be applied in the development and flow-down of FM requirements.

Recommended Practice: ***Centralize FM requirements.*** *It is recommended that emphasis is placed on FM requirements flow-down, traceability, and consistency.*

Recommended Practice: ***Methods to strengthen requirements statements and flow-down.*** *If FM requirements are found to be lacking, and it is impractical to recommend a requirement rework or reassessment at a later project phase (PDR or CDR), below are a few methods for optimizing a given a set of requirements. The following items identify options that will enable a project to improve the FM requirements given the existing set.*

- ***Search for gaps and overlaps.*** *Scrub existing requirements for gaps, overlaps and other inconsistencies. Create a virtual roll-up document and identify holes.*

- ***Determine the limiting constraints.*** *Analyze and determine the limiting constraints for requirements, and especially families of similar requirements, and establish consensus among all parties.*

- ***Consider targeted additions.*** *Where major omissions exist, consider adding new requirements or adding clarifications to existing requirements. This can be particularly helpful for key requirements that have extensive, implicit aspects—breaking them out explicitly can clarify and simplify the flow down as well as the FM V&V. A requirements parsing would help to determine what additional clarifications or requirements are required. For each FM requirement, it should be easy to identify who, what, where, when, how frequently, how long, how quickly, to report or respond to whom, and constraints to operating mode or mission phase.*

- ***Clarify ambiguity.*** *Where major ambiguity exists, and requirement modification or clarification is not feasible, establish consensus among all parties to the agreed upon interpretation and ensure that it is included in the V&V compliance matrix.*

Lesson Learned: ***(NASA Lesson Learned #1385) Lack of requirements to contractor led to loss of Comet Nucleus Tour (CONTOUR) mission.*** *Few requirements were imposed by NASA regarding the way contractors documented or performed work on CONTOUR, creating opportunities for contractors to adopt nonstandard engineering practices.*

Recommendation: Projects should establish clear and appropriate requirements for performing and documenting engineering work.

FM Lesson Interpretation: This lesson is applicable to out-of-house projects. These types of projects should establish FM SE processes and formal requirements for performing and documenting FM work.

Recommended Practice: ***Requirement flow-down should minimize parroting.*** *Try not to restate requirements. Anytime a requirement is restated during requirement flow down, sufficient detail needs to be added to justify the restatement.*

Recommended Practice: ***Avoid ambiguity.*** *Ambiguous requirements can be interpreted in multiple ways. If a program has different groups interpreting the same requirements in different ways, disconnects will likely occur.*

Recommendation: When terms or words are ambiguous, consider having in-line short definitions after the requirement to elaborate concepts more clearly. Alternatively, if appropriate, define the problematic terms in a project-approved glossary, if this glossary is used to enforce consistent interpretation.

If a requirement applies only to one part/aspect of a mission or vehicle, identify it as such so unintended parts do not attempt to comply with a requirement that was not meant for them.

Lesson Learned: ***(NASA Lesson Learned #1493) CALIPSO satellite Proteus propulsion bus, ambiguous fault tolerance requirements.*** *There were many interpretations of which specific document dictated the fault tolerance requirements for the spacecraft. Further, given a specific document, there were divergent conclusions over what the fault tolerance verbiage in each document imposed on the spacecraft design, checkout, and operations.*

Lesson Learned: Fault tolerance requirements should be clearly defined in appropriate Agency-level design standards and variance accepted only when accompanied by appropriate risk trades and supporting technical rationale.

Recommendation: NASA has to establish unambiguous requirements for fault tolerance in an Agency- level document (e.g., NPR 8715.3, NASA General Safety Program Requirements) and identify any exceptions.

FM Lesson Interpretation: Projects should identify and address ambiguous requirements expressed in multiple documents in the FM area.

Lesson Learned: ***(NASA Lesson Learned #2044) Mars Reconnaissance Orbiter (MRO), imprecise fault tolerance requirements.*** *MRO appendage keep out zone (KOZ) level 3 design requirements proved insufficient to prevent collision between an appendage and the spacecraft. Even faithful compliance with the "test-as-you-fly" rule does not cover all circumstances—in this case, motion associated with a unique geometric configuration.*

A requirement for a design implementation that would prevent penetration into a KOZ should have been written and verified. An early, relatively simple, parametric or systems modeling

language (SysML) diagramming activity would have quickly cleared up misunderstandings and led to correct and complete requirements.

Recommendation: Design and verification of kinematically complex systems, such as spacecraft appendage control, should observe the following principles:

Reaffirm the importance of precision in requirements language.

***Recommended Practice:* Identify institutional policies, practices, and principles.** *If a standard project policy, practice, or principle is effectively a requirement, then it should be formalized to minimize the potential for requirements creep.*

***Lesson Learned:* (NASA Lesson Learned #1162) Space Shuttle potential common mode failure, potential for hydraulic lines in close proximity to each other—common cause failure mode requirements.** *Redundant hydraulic lines for the three orbiter hydraulic systems are not adequately separated to preclude loss of all hydraulic power in the event of a single catastrophic failure of adjacent hardware.*

Recommendation: Provide the same degree of separation of redundant critical hydraulic lines as is given to redundant critical electrical wiring.

FM Lesson Interpretation: This lesson is applicable to all projects. Projects should establish FM principles and SPF guidelines, analyses, and requirements that can prevent these types of design disconnects.

***Recommended Practice:* Clearly identify goals.** *If a project has minimum requirements but wants to design to goals that are beyond the minimum requirements, these can be handled in a few ways, as follows:*

a. If the plan is to design a robust system, but be able to fall back to the minimum requirements in a severe case, then the goal value should be spelled out in all requirements, along with the minimum required value. Note this can vary with the requirement area.

***Example:** The vehicle shall fully reconfigure from any failure (excluding those listed on the SPF list) in X seconds, with a goal of Y seconds.*

b. If the plan is to design to bare minimum requirements only, but to document goal performance, then it is better to leave the goals out of the requirement system and instead, separately show actual performance margins via a separate V&V process on a best-effort basis, or in a margins management document, expanded to include certain performance margins.

***Recommended Practice:* Minimize overlapping requirements.** *If a top-level FM requirement and an IRD or other specification document covers the same subject, find the limiting constraint and formalize it clearly to avoid confusion downstream.*

Table 14, FM Requirement Counts, provides sample FM requirements counts from a selection of recent NASA projects of various classes (see table 12 in section 5.3e). These numbers are included to provide insight, and to offer a rough order of magnitude comparison for a candidate project. The key concern is not the exact number of requirements *per se*, but that more requirements are usually synonymous with more detailed FM phase-specific scenarios and robustness formulation and investigation at the system level.

Table 14—FM Requirement Counts

NASA Project	# Mission-level FM Requirements	# Spacecraft-level FM Requirements	Total	Comments
Project A: SMD Discovery/STP class	109	245	354	(1) Typically the higher the mission class, the more FM requirements.
Project B: SMD Discovery/STP class	147	138	285	(2) FM requirement counts have grown on recent missions as the FM discipline matures and FM requirement expectations become more formalized up-front. This factor needs to be taken into account (e.g., why flagship class is not at the top).
Project C: SMD Earth Orbiter class C	44	154	198	
Project D: SMD Flagship class A	30	122	152	
Project E: SMD Discovery/STP class	18	68	86	(3) Some missions are "in-house" vs. subcontracted out. In general, the more removed the contract/contractors, the more detailed FM requirements and interfaces should be to lower the chance of disconnects.
Project F: ESMD class A	2 (+15 with some FM content)	40	42	This is an example of a project that has a less than typical number FM requirements for the project of that complexity level.
Project G: SMD class D	20		20	The lower mission classes are generally expected to have less redundancy and fewer FM requirements.

5.4.1 Bottom-Up Requirements Development

Concurrent with the development and deployment of the mission-level FM requirements, bottom-up development is often in progress on the hardware and software subsystems. Due to schedule and hardware availability, development of computer systems, instruments, and interfaces can often be in progress before the mission-level FM requirements are completed.

To address this issue, the ISS developed a requirements document, SSP 50038B, Computer-Based Control System Safety Requirements, specifying mission independent safety requirements for initial boot sequences, bus and interface control, safe commanding, and anomalous conditions. Having a minimal set of mission-independent hardware and software safety

requirements allowed the low level development to proceed without negatively impacting the top-down mission-level requirements.

The James Webb Space Telescope (JWST) addressed the problem by defining a minimum set of safety requirements for each instrument and bus system. This defined a minimum set of safety monitoring and commanding to be available for use by the mission-level FM requirements. Some examples of these instrument and bus requirements follow.

- Each instrument was designed to allow power to be removed at any time without instrument damage.
- Each instrument was to provide a safe command that would initiate safing within the instrument.
- Each interface or bus was to provide a reset function to reset the interface or bus to a known safe state.
- Each instrument, interface, and bus was to provide monitoring and telemetry sufficient to identify their specific failures.

Allowing the engineers to design to the above requirements, they were able to proceed with the low-level design work, and provided valuable information to the FM team.

6. DESIGN AND ARCHITECTURE

While FM systems may vary widely from application to application, there are a handful of mission attributes that drive the needs of the operational FM. As mission designers and FM engineers define the mission and system, a number of priorities and constraints will arise that drive the FM design, including the application of redundancy, fault containment approaches, and hardware and software architectural choices. There will be features of the mission definition that clearly map to the FM effort, such as the mission risk posture and fault tolerance requirements. There will be mission and system characteristics that impact the FM design in less immediate ways, but that are common players in the decisions of the FM team.

The FM engineer will have the task of identifying goals, events, and constraints that have to be protected to accomplish the nominal mission, from which the engineer will derive the priorities of the FM system. Other features of the mission will constrain how the FM system can effectively meet those priorities, and will therefore constrain how the FM engineer can implement protective functions. To deploy FM throughout the system, the FM engineer will need to define hardware, software, and operational architectures that allow the implementation of protective functions that meet the priorities of the FM system. Figure 4, Mission Requirements and FM Design, illustrates the process of deriving FM requirements from mission attributes, and flowing them down to the architecture and design of operational FM.

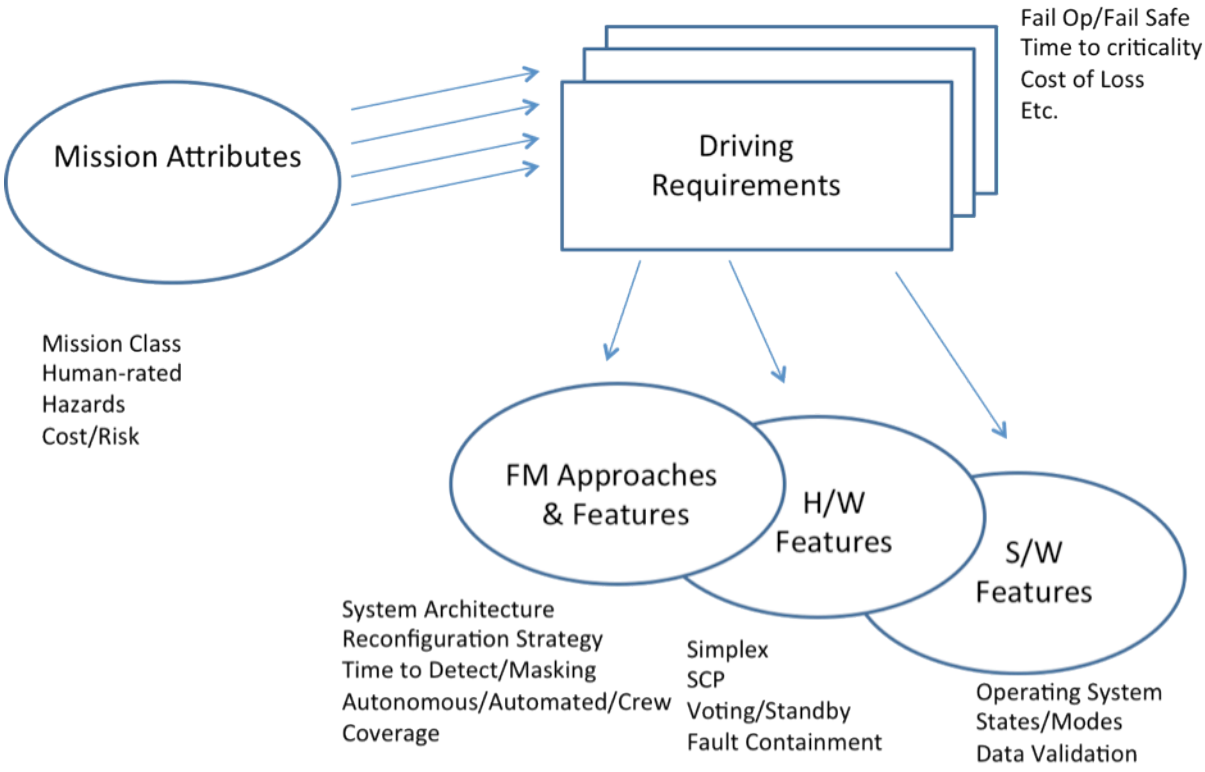

Figure 4—Mission Requirements and FM Design

Developing an early understanding of how these mission and system design choices drive the FM design from the top level down to the hardware and software architectures will help FM engineers define the correct set of strategies and functions to protect critical mission goals. It also will help project managers appreciate the scope of FM for their system and allocate appropriate resources to the effort. This section will guide the FM engineer to identify mission characteristics that drive the needs for FM, and will provide architectural considerations and building blocks that can be used to develop an FM design that will meet the needs of the mission.

6.1 Fault Management Objectives and Requirements

6.1.1 Mission Risk Posture

Two key steps in the mission definition determine the mission risk posture. First, the choice of mission classification, per NASA NPR 8705.4, defines the project's tolerance for risk, which in turn drives the FM approach to identifying and correcting failures. Low-risk missions require an FM approach that addresses the maximal set of possible failures and mitigations, while a higher tolerance for risk allows trades for smaller mitigated fault sets or riskier failure response strategies.

Second, the writing of fault tolerance requirements determines the risk tolerance approach for the mission in response to the mission class definition. Low risk missions will tend to have single- or even multiple-fault tolerance requirements across the entire system, usually against full mission success (e.g., “no single fault shall cause an LOM science return below full mission success.”). Single fault tolerance requirements tend to result in the highest quality, most expensive FM approach, with high quality parts requirements, full redundancy, thorough fault and failure containment, and extensive operational FM that can protect all functions against faults.

Higher risk tolerance missions have more room to define how risk is distributed. Fault tolerance requirements may be mixed or targeted: Single fault tolerance for core health and safety functions (e.g., pointing, power production), but not for science instruments or ancillary functions; partial fault tolerance with selective redundancy; smaller mitigated fault sets; lower-quality parts that are more prone to failure. Certain operational risks may also be more acceptable, where a low-risk class A mission might perform extensive analysis to show robustness to a failure condition in flight, a class C mission may choose to accept the risks and deal with the condition only if it arises.

For these higher risk missions, the FM engineer emphasizes managing risk and resources versus driving risk to a minimum. Risk is traded against resources to meet a tight cost constraint, rather than attempting to drive down the risk of failure at all costs. The FM team has to work closely with S&MA and project management to trade the likelihood and impact of failures to find the best places to apply limited resources. Table 12 in section 5.3 summarizes the mission types and risk tolerance for mission classes as defined in NASA NPR 8705.4 Risk Classification for NASA Payloads, and provides some applicable fault tolerant requirements and approaches that may be driven by the selection of the mission class.

Pitfall: ***FM is subject to changing priorities toward cost and risk over the course of system development, and implementation and operations.*** *FM complexity and cost can in part be traced to changing assumptions about the level of risk acceptable for a mission. Early in the project lifecycle, the primary concern is cost, which is reflected in low FM staffing levels and a late start to FM development. As projects near launch, however, project priority often switches to risk, which places additional strain on the FM system and designers. Should a failure occur during operations, e.g., a loss of redundancy, this too can impact risk posture going forward.*

Recommended Practice: ***Maintain a fault tolerance and risk policy statement that clearly articulates the project's risk posture and approach to mitigating failures.*** *A fault tolerance requirement that reflects the project's policy is necessary, but requirements are terse statements that often cannot capture the full range of nuances of a risk policy. A more detailed statement of project philosophy will help mediate disagreements about requirements interpretation later, and keep the FM effort focused.*

6.1.2 Mission Goals and Fault Management Priorities

Before FM can be defined for the mission, the goals, functions, and resources that need to be protected need to be identified. Any mission will include certain functions, events, or assets that are critical to achieving the mission's goals. Characteristics of the mission design will also levy implicit fault tolerance requirements. For example, availability or up-time requirements that flow from a science mission design will place a restriction on how much science operation time loss can be allowed when responding to a failure.

In general, the objective is to identify design drivers that place priorities on the FM functions of the system. Does the system need to autonomously recover full functionality and return immediately to executing mission goals (fail operational), or can the designers rely on more fail-safe strategies that allow operators to assess failures and implement thoughtful recovery actions? Does the system need to accommodate several FM strategies over the course of the mission, or can a single configuration work for all cases?

6.1.2.1 What Are the Mission Goals?

The FM engineer and mission designers should identify mission-level science, engineering, and service requirements that are central to the mission and define what it means for those requirements to be compromised. The following are important considerations:

- Science return requirements: Full versus minimum mission return. Are there opportunities for graceful degradation within mission requirements?
- Science collection events: Is there a single opportunity or a limited window in which a critical observation must be taken?
- One-time events and irreversible events that are critical to system health, such as critical deployments, orbit insertions, repair, maintenance, retrieval, landings,

docking: Can the event be cancelled and retried, or is there only one chance to get it right?

- Up-time or availability requirements: How long can the system be in a non-operational state or otherwise un-attendant to science goals?

Example: Consider a mission to perform a comet flyby. The primary objective of the mission centers on the encounter, which is a short, one-time event during which all science data is collected. The system has to remain operational or recover functionality quickly during the encounter to ensure that sufficient data is taken to meet the mission science goals. When paired with long ground-in-the-loop response times and a single fault tolerance requirement, this will drive an FM approach that is capable of fully autonomous recovery of most or all system functionality during the critical event.

Example: A contrasting mission would be a survey that has coverage or up-time requirements (e.g., "collect data over 95 percent of the surface of the earth five times"), but no critical science events. The up-time requirement may map to a maximum allowable downtime, but it will likely be acceptable to limit onboard autonomous or automated responses to actions that contain failure effects and protect system health (fail-safe strategy), and allocate recovery actions to operators on a longer time-scale.

6.1.2.2 Are There Critical Resources or Constraints FM has to Protect?

Many systems will have critical constraints, safety requirements, or finite resources that become priorities for FM. It is important to identify any unique resources or constraints that FM has to protect to maintain system health, safety of equipment or crew, or mission objectives. What conditions will violate a constraint or compromise a resource? Some examples are listed below.

- Consumables or other limited resources that directly support the mission (e.g., cryogen).

- Constraints that have to be maintained to avoid damage to a mission-critical assembly (e.g., pointing keep-out zones (KOZs), temperature constraints).

- Critical payload (e.g., sample return) that requires certain environments or other restrictions to protect integrity (e.g., temperature constraints, atmospheres, forces).

- Safe onboard survival conditions when there is a crew, and protection of resources minimally needed for the crew to access an acceptable safe haven.

In most cases, protection of a resource will place a critical constraint on a system. For example, a cryogenic telescope will require the protection of cryogen by keeping sunlight or other heat sources out of the telescope bore-sight, which places a pointing constraint on the system. The same constraint, however, may also exist by itself. A telescope may have a sun-pointing constraint to protect optics and detectors, resulting in a similar priority for FM, as does the cryogenic constraint. A critical payload poses similar challenges as a finite resource. If the

mission is to transport a payload (e.g., sample return), the system will have a set of functions or environmental conditions that have to be maintained to protect the integrity of the payload.

6.1.2.3 Which Functions Are Always to Be Maintained?

In addition to the above specific goals and constraints, a system design may also require that certain functions are continuously or near-continuously available. There may be functions that support the protection of one of the above constraints, or a minimal set of functionality required to keep the system safe while waiting for operators to perform a recovery (the safing design). If the system design includes limited redundancy, this set of functions will be an ideal place to apply physical or functional redundancy.

6.1.2.4 Varying Mission Phases and FM Strategies

When identifying modes of operation and critical events, it may become clear that different phases or events have different FM needs, which places another priority on the FM design: flexibility to implement different fault response strategies for different modes of operation. Where a mission with a single phase or mode of operation can implement static FM, a mission that has disparate phases will have multiple sets of FM, or FM functions that are reconfigurable depending on the activity.

Example: Unmanned aerial vehicle (UAV): Single mode of operation (fly) with similar, though varying goals (takeoff, land, navigate); most functions can be covered with a single FM strategy.

Example: Mars Rover: Four distinct mission phases with disparate goals (launch, cruise, landing, surface operations); disparate FM strategies.

Pitfall: ***Maintenance of "Core Operations" FM Support.*** *It may seem reasonable to focus FM efforts on the detection and response to failures. However, there is also a "core functionality" side within the FM capability that must be maintained. This includes setting FM parameters, spacecraft deployment sequencing, monitoring FM processing, reporting on FM actions, and supporting troubleshooting of both system and FM behaviors. The FM design also has to ensure that the information required to trace and resolve faults or failures is available in telemetry and preserved through a cascade of faults/failures in order to allow ground reconstruction and root cause analysis. These core FM functions are critical during V&V and operations, but can be overlooked in the FM design.*

6.2 Mission Characteristics

In addition to identifying the priorities of the FM task, the FM engineer will analyze the system architecture to find the mission characteristics that will drive the allocation of FM functions. In order to meet the priorities, FM functions will need to be distributed through the system, and the mission design places constraints on how or where those functions can be implemented.
A common driver of the allocation of FM function is response latency, particularly for deep space systems, or missions that have infrequent contact with the ground. *Response latency*, paraphrased from section 4.1.6, is the *time from the occurrence of a fault to the correction of the*

failure condition. In general, a response has to be clear or contain the failure effects before the failure propagates to a CFE; it has to be faster than the TTC of the failure. Because fault response can be implemented in multiple steps or in several different parts of the system, there may be several response latencies to consider. For instance, if the FM strategy includes software autonomous response that contains a failure by powering off an assembly, and then waits for ground operators to recover the function to continue with mission goals, there are two response latencies with different impacts. First, the time before the software response is a latency that impacts health and safety goals of the system—that response has to be designed to complete before a CFE permanently impacts health and safety. The second response latency is the time for operators to return the system to full functionality, and that response has to complete before affected mission goals are compromised by the loss of function—science observations are lost, too much time is spent in a mode of operation that consumes resources, and so on.

The response latency is built from the various mission and system characteristics that impact the execution of each of the core FM functions. Figure 5, FM Functions shows the set of FM functions identified in section 4.2.

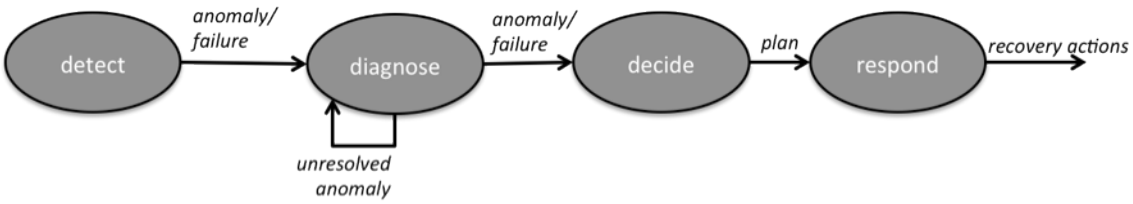

Figure 5—FM Functions

Viewed on a timeline, the milestones of FM functions can be expressed a little differently, as in figure 6, Breaking Down the Response Latency:

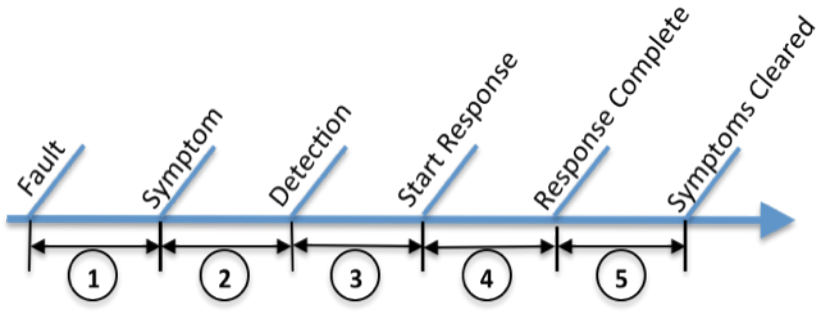

Figure 6—Breaking Down the Response Latency

(1) Observation latency: The duration from the occurrence of a fault to when the failure effects become observable.

(2) Detection latency: The duration from the observable failure effect to when a detection mechanism detects (and possibly identifies) the failure.

(3) Decision latency: The duration to diagnose the failure, decide on a response, and start execution of the response.

(4) Response execution time: The duration during execution of recovery activities.

(5) Recovery time: The duration from response completion to when failure effects are no longer present and mission/system status is restored to nominal.

For any system, there may be many elements that are capable of detecting, diagnosing, and responding to failures, including ground operators, ground software, crew, flight software, flight firmware, and flight hardware. For each element of the system that may implement one or more of the above FM functions, the response latency will be built from the characteristics of the systems involved.

In order for ground operators to implement some portion of the FM control loop, the entire information path from the point of failure to the eyes of the operator and back should be considered, and is often the longest response latency in the system. For example, a deep space mission may need to account for the following when assessing the ground response time:

- Data generation: The latency to observable failure effects, including data generation frequency (a telemetry value may be generated on a slow cycle).
- Data storage.
- Communications schedule: May be hours or days from the time data is generated and stored to the time it is played back for transmission.
- Data transmission latencies: Bandwidth available for the data volume, round-trip light time, bent-pipe transmission schemes in which data is stored and forwarded over another link.
- Data processing time: Demodulating, decoding, applying data number to engineering unit conversions.
- Analysis and display: Time to trend, display, or assess telemetry, including applying persistence and filtering to failure detection.
- Organizational and human response time: Time to understand, discuss, plan, generate commands, and approve transmission of a response.
- Communications schedule: Response may be delayed by available communication assets.

- Ground response execution time: Time it takes for operators to execute a response procedure.

- Transmission time: Latency of command transmission, including ground data system latency, round-trip light time.

- Onboard response execution time: Time for the target software or hardware to receive and process commands.
- Recovery time.

In the same example mission, an autonomous response implemented in flight software will have significantly lower response latency:

- Data generation: The latency to observable failure effects, including data generation frequency (a telemetry value may be generated on a slow cycle).

- Transmission of data to software: Subject to data bus latencies, software execution cycles, etc.

- Detection latency: Including data processing, persistence, and filtering.

- Decision latency: Software processing from detection to response execution.

- Response execution time.

- Recovery time.

Similar lists of sources of latency can be generated for each system that performs failure detection and response, tracing the path from the fault to the monitoring system and back.

When assessing the priorities of the FM system to protect particular functions, goals, or resources, the response latencies for the involved systems become key parameters in designing FM strategies. For example, in a deep space mission with limited computing resources, it may be desirable to take advantage of the flexibility of human-in-the-loop response, but the latency is intolerable. Where to split flight versus ground responsibility for failure detection, diagnosis, containment, and recovery is a common trade for robotic missions, and a common example of trades that will also consider hardware, software, crew, and operators as places to implement FM functions. Systems far from Earth, with a long round-trip light time and infrequent communications with the ground cannot rely on operators to intervene before the TTC for most failures. An event can be started and completed before data even reaches Earth. In these systems, the mission has to rely heavily on sophisticated autonomous or automated functions to execute the nominal event, to recover full functionality after a failure, and to survive after the event to return critical data. Conversely, an earth-orbiting system with frequent ground contacts can rely more heavily on ground interaction, and may be able to limit onboard automation. Similar considerations will be relevant when FM functions can be distributed through hardware or software, or across multiple interacting systems.

The decision of where to implement FM functions is, therefore, a trade against the mission characteristics that impact execution of FM. The mission design can be adjusted to support preferred FM strategies if the assessment is started early and performed proactively. Similarly, detection and response designs within the software and hardware are subject to the parameters of the system design; FM designers should be aware of the impact of the mission and hardware design on FM functions, and raise concerns where necessary to ensure that adequate resources are available to meet the priorities of the mission.

6.3 Fault Management Architectures, Design Features, and Approaches

[To be expanded in future versions]

6.4 Mission-Specific Fault Management Considerations

The scope and complexity of FM requirements imposed on a vehicle are strongly influenced by the mission's risk posture, the mission type, included phases, and some operational considerations. There are associated implications on strategies for achieving acceptable probability of LOM, LOV, LOC (if applicable), and/or an acceptable level of safety risk to the vicinity in which the vehicle operates. These factors are addressed in the following subsections, except for the range of NASA mission-risk postures, which are addressed in sections 5.3 and 6.1.1. Section 6.4.1 provides some tables that summarize relationships of mission characteristics to the primary FM design considerations, with more detail provided in subsequent sections. NASA mission types are identified in section 6.4.2 along with discussion of mission type-specific considerations that drive FM design. Sections 6.4.3 and 6.4.4 provide some detail about possible mission phases and operational considerations respectively that impact FM design. Finally, other mission-specific considerations that affect FM design are addressed in section 6.4.5.

6.4.1 Relationships Between Mission Characteristics and Primary Fault Management Design Considerations

The following tables summarize primary FM design considerations as a function of specific mission characteristics, with more detailed explanations in subsequent sections. Table 15, Primary FM Considerations by Mission Type, identifies FM considerations by mission type, with more details provided in section 6.4.2.

Table 16, Primary FM Considerations by Mission Category, addresses FM considerations by mission category, with more details provided in section 6.4.3.1. Tables 17-19 list FM considerations by mission phase for space vehicles, air vehicles, and surface vehicles, with more applicable details provided in sections 6.4.3.2, 6.4.3.3, and 6.4.3.4, respectively.

Table 15—Primary FM Considerations by Mission Type

Mission Type	Primary FM Design Consideration
Robotic	Prevent LOM.
With Crew	Prevent LOC.
Interacting Vehicles	Avoid causing harm to the other vehicle.

Table 16—Primary FM Considerations by Mission Category

Mission Category	Primary FM Design Consideration
Fixed-Phase	FM features applicable to the mission phase remain operative for the mission duration.
Multiphase	FM modes change with each mission phase.
Multifunction	If different FM is needed for different functions, then the FM architecture needs multiple phases.

Table 17—Primary FM Considerations by Mission Phase for Space Vehicles

Mission Phase	Primary FM Design Consideration
Powered Ascent to Space (Robotic)	Prevent harm to people and facilities on the ground.
Powered Ascent to Space (with Crew)	Prevent LOC while avoiding harm to people and facilities on the ground.
Orbit Insertion and Phasing	Assure successful completion of necessary orbit changes.
RPOD	Assure successful completion of RPOD maneuvers while preventing collision risks.
Free Flight in Space	Protect mission capabilities for subsequent use even if a safe mode has to be temporarily invoked.
Mated Flight in Space (Docked Vehicles)	Account for mated stack mass properties while protecting mission capabilities for subsequent use.
EDL	Assure success of essential EDL sequence events.

Table 18—Primary FM Considerations by Mission Phase for Air Vehicles

Mission Phase	Primary FM Design Consideration
Powered Takeoff	Enable safe return aborts.
Deployment to Powered flight (e.g., Mars Airplane)	Assure success of transition to powered flight.
Glider Deployment	Enable success of transition to gliding flight.
Balloon Deployment	Prevent payload from doing harm to people or facilities on the ground.
Aircraft Cruise, Glide	Maintain stable flight and a valid navigation state.
Balloon Drift	Sustain payload operations.
Aircraft Landing	Ensure safe touchdown (without airspace violations where applicable).
Balloon Landing	Enable intact payload return in a safe location.

Table 19—Primary FM Considerations by Mission Phase for Surface Vehicles

Mission Phase	Primary FM Design Consideration
Deployment	Assure success of each essential deployment step.
Stationary Operations	Protect mission capabilities for subsequent use even if a safe mode has to be temporarily invoked.
Mobility Operations	Protect mission capabilities for subsequent use even if a non-mobile safe mode has to be temporarily invoked.

6.4.2 Mission Type Considerations

NASA develops a variety of vehicles that operate in space, in the air, and on planetary surfaces. The details associated with a mission type and its intended range of operational environments can have a significant impact on the necessary FM capabilities. The following subsections review a representative set of NASA vehicle mission types, along with some applicable FM design considerations.

6.4.2.1 Robotic Missions

Robotic missions do not have humans onboard the vehicle, but may still have ground-based humans involved in the mission (and FM) decision loop. LOM is the paramount FM consideration for robotic space vehicles, with high FM importance also placed on LOM and LOV.

6.4.2.2 Missions With Crew

On a vehicle with a crew, LOC is the paramount FM consideration with high FM importance also placed on loss of mission or loss of vehicle.

6.4.2.3 Missions With Interacting Vehicles

One vehicle is deemed to interact with another vehicle when success of a mission or a particular activity becomes interdependent. During such interactions, one vehicle relies on another for specific services and has to respond to either its own failures or those known to exist on the interacting vehicle with insight regarding how they affect, or are affected by, the multivehicle interaction. Among the possible reasons for vehicle interactions are making a large velocity change burn, acquiring rendezvous targeting data, achieving latched docking, propellant transfer or obtaining power beamed from a generation platform. In the large velocity-change burn example, a vehicle with a crew may have to plot contingency separation maneuvers in the event that a propulsion vehicle is at risk of catastrophic failure, or the vehicle with crew may provide auxiliary attitude control during a burn if the propulsion vehicle fails to provide adequate control authority. For rendezvous and docking, the FM responses on a vehicle would first have to preclude risk that faults on either vehicle could jeopardize the safety of either vehicle due to collision, and secondarily would seek to limit risk to mission success. In the beamed power example, FM would have to act to prevent a spacecraft failure from enabling damage by incoming beamed energy that is not properly received.

In some cases, successful rendezvous and docking may be critical to assuring safety on a vehicle with a crew. This would be the case when a crew is transferring to a return vehicle after a human lunar/planetary landing mission. Under these circumstances, a vehicle with crew may need unique FM capabilities to overcome the adverse effects of faults, not just on the currently inhabited vehicle, but also on the interacting vehicle. Note that when two vehicles with crew interact, those interactions may require means for successful communication between crew members on both spacecraft, especially when there are significant failures.

6.4.3 Mission Phase Considerations

Each vehicle designed for a mission type will have to operate in one or more mission phases. The nature of vehicle activities pursued in a specific mission phase, and the environment in which it occurs, determine both what onboard equipment is essential to successful completion of that mission phase, and the TTC for component faults that may occur during that mission phase. Consequently, the FM design requirements for a vehicle are a union of the requirements associated with all the mission phases to be accomplished by a vehicle. Phase-related mission categories are discussed in section 6.4.3.1, and specific vehicle mission phases are addressed in sections 6.4.3.2–5. Some vehicle FM capabilities likely to be required for specific mission phases are identified in applicable subsections.

6.4.3.1 Some Mission Categories Based on Phase-Related Considerations

Missions can be categorized, in part, by the number and types of mission phases. Some specific phase-related mission categories are addressed in the following subsections.

6.4.3.1.1 Fixed-Phase

A fixed-phase flight vehicle system is one that maintains the same phase during mission operations. A vehicle with this mission feature does not have to change FM strategy modes based upon the sequence of the mission timeline. Examples of such flight system may be an on-station geosynchronous Earth orbit space vehicle or a flight element needed only during launch of a rocket for a given phase of ascent (e.g., a launch abort system). All FM requirements imposed on a fixed-phase vehicle system remain in effect for the duration of operation of the applicable flight system.

6.4.3.1.2 Multiphase

A multiphase mission/system is one that has to change its FM modes of response to events based on the differing phases for the given mission. The nature of required FM responses in a given mission phase are typically tied to the TTC metric. For example, the response to a failure on a crew transport vehicle during orbit phasing will be very different than the response during re-entry or touchdown because the time it takes for the consequences of a fault to become critical to mission or vehicle safety is generally much longer when on orbit than during an entry, descent, and landing sequence.

6.4.3.1.3 Multifunction

A multifunction mission/system is one that has two or more different functions that have to be coordinated. An example is a science mission that provides means for a variety of science-related functions that have to be managed in a way that is compatible with mission objectives while avoiding functional conflicts (e.g., a rover at a designated scientific target that has different operational and FM restrictions when grinding a rock surface as compared to imaging its current surroundings). In this scenario, spacecraft health has to be maintained while accomplishing observation coordination. For some missions, power usage and data throughput limits may come into play to decide if one function is more important than another function. Strategies for coordinating multiple functions of a given mission may dictate some required mission phases.

6.4.3.2 Some Specific Mission Phases for Space Vehicles

Space vehicles have to provide FM capabilities for mission phases during which they are active. That may, or may not include mission phases when the vehicle is a payload rather than a freely operating system. For example, a crewed space vehicle may be active throughout ascent atop a booster to have the situational awareness required in the event that there is need to initiate an abort. In contrast, many robotic space vehicles are mostly inactive payloads during their ascent to space. A space vehicle's FM design has to accommodate capability requirements only for the mission phase(s) during which it is active. The following subsections identify some typical space vehicle mission-phases, and some FM capabilities and/or issues unique to each of the identified mission phases.

6.4.3.2.1 Powered Ascent to Space

Space vehicles experience a powered ascent flight phase when leaving earth or departing the surface of another celestial body. During powered ascent, a vehicle will experience variable acceleration (possibly up to 8 g's), and the composite ascent system will undergo rapid changes in mass properties that affect control characteristics. In addition, if the ascent occurs in a sensible atmosphere, then there will be time-dependent aerodynamics forces acting on the vehicle, and lateral wind effects. The acceleration, rapidly changing system dynamics, and time-varied control characteristics that occur during powered ascent can make the TTC for a propulsion, navigation, or control fault very short—generally too short for ground control interaction or even onboard interaction by a crew (if humans are onboard). This means that the FM system has to be capable of rapid fault detection, isolation, and reconfiguration for all subsystems critical to successful powered ascent.

For a robotic vehicle, the primary objectives are as follows: First, to prevent harm to people or facilities on the ground; and second, to prevent LOM. If the first primary objective above is threatened, then destruction of the vehicle in a zone that can safely handle resulting debris may be preferred to impaired mission continuation that poses risk to people or facilities on the ground. If the secondary objective above is unavoidable, then either destruction of the vehicle or a goal change such as diverting the vehicle elsewhere (perhaps to a lower than intended orbit), is recommended. NASA's Range Safety policy is defined in in NASA NPR 8715.5, Range Safety Program.

For a vehicle with a crew, if significant threats to people or facilities on the ground develop or it is not possible to prevent LOM, then transition to an abort phase will occur (with aborts discussed in section 6.4.3.5). Note that it is typical for a vehicle with a crew to navigate its own state during powered ascent so it has independent means to determine if an abort is necessary, enabling transition to an abort without relying on getting state data transferred from the boost vehicle. For short TTC failures, however, the abort determination process may be autonomous without crew input. The determination of the need for an abort and the abort type is a special class of FM functionality.

Pitfall: *Powered ascent. Responsibility for executing powered ascent FM when there is a crew onboard has to be carefully partitioned between the launch vehicle and the spacecraft with the crew. The FM on the spacecraft with the crew has to be able to initiate an abort if there is a serious booster failure, regardless of whether there is notification from the booster regarding the failure. However, the abort trigger conditions for the FM on the vehicle with the crew also have to avoid inadvertently initiating an abort when one is not actually merited by booster and/or spacecraft conditions.*

Recommended Practice: ***Powered Ascent FM #1.*** *Implement automatic, very short response time FDIR for all subsystems critical to successful powered ascent.*

Recommended Practice: ***Powered Ascent FM #2.*** *Provide means for disposal of vehicles within a zone that can tolerate debris if significant threats to people or facilities on the ground develop or when LOM cannot be prevented. This disposal may zone may be land, sea, or space.*

6.4.3.2.2 Orbit Insertion and Phasing

A vehicle already placed into orbit may need to make significant changes to its orbit to enable realization of mission objectives. This will be accomplished by propulsion systems embedded in or attached to the vehicle. Part of the applicable FM functionality will be used to determine if necessary orbit changes have been realized. When they are not properly realized, the subsystem causing that fault has to be identified and isolated, with reconfiguration that not only applies an alternate subsystem to achieve the required orbit change, but when TTC is short, also provides means to determine new orbit change strategies that can recover mission objectives.

When the TTC for a failed orbit change is long, then ground control can provide the means to determine revised orbit change strategies. This may be the case when there will be cyclic opportunities to accomplish the desired orbit change over hours or days. However, some orbit changes cannot be postponed, which may be the case for a vehicle requiring orbit circularization after ascent to an unstable, low-perigee insertion orbit. In these short TTC cases, a failure to achieve a desired orbit change on an initial attempt will require rapid reconfiguration to a substitute subsystem that can enable the needed orbit change to occur, supported by onboard logic to determine how to apply the reconfigured vehicle capabilities to accomplish the necessary mission orbit characteristics.

Pitfall: ***Orbit Insertion and Phasing FM.*** *Automatic FM response to an orbit insertion and phasing propulsion failure has to avoid taking actions that cause irreversible loss or degradation of the mission when a detected failure is recoverable in a timely manner.*

Recommended Practice: ***Orbit insertion and phasing FM.*** *Provide onboard means to rapidly determine new orbit change strategies when FM fault recovery actions and TTC force use of alternate propulsion systems.*

6.4.3.2.3 Rendezvous, Proximity Operations, and Docking (RPOD)

RPOD is a series of maneuvers to bring one space vehicle into proximity, and then to attach itself to another space vehicle. (The term “proximity operations” is coming into frequent usage to describe robotic science operations near a primitive body. This section does not address such robotic mission scenarios yet.) After completing attached operations, RPOD can be reversed with the detachment and departure of a vehicle to go on to separate mission objectives (e.g., to return to Earth). The FM requirements on a vehicle during RPOD vary as a function of distance from a target vehicle and on whether the target vehicle has a crew.

At long range from the target, the primary FM objective is to prevent a failure from causing LOM. Relative navigation states have to be maintained, and rendezvous maneuvers have to be executed. TTC is generally long, so a failure during an applicable rendezvous step can be diagnosed by ground control where recovery steps can also be formulated.
Proximity operations have a much shorter TTC. Wrong actions resulting from component faults risk a collision of the maneuvering vehicle with the target within minutes. An FM system has to

provide means to detect and respond to failures with at least enough resulting vehicle capability to remove itself safely from the vicinity of the target vehicle.

During the docking phase, the maneuvering vehicle is in very close proximity to the target, and has to maintain very small relative velocities, along with very precise relative attitudes. Mechanical systems have to enable proper latching of the two vehicles. The TTC is very short (seconds), with collision a possible result of unmitigated faults. FM has to rapidly restore any fault-based loss of critical state information or control capability.

Note that berthing is an alternative to docking. In a berthing scenario, the arriving vehicle will go into free drift with relative rates nulled in close proximity to the target vehicle to allow a mechanical appendage to grab the arriving vehicle and subsequently to facilitate attachment of the two vehicles. In a berthing scenario, the target vehicle takes over much of the overall FM responsibility after the arriving vehicle is in free drift.

If the target vehicle has a crew, then preventing the risk of LOC due to collision during proximity and docking operations is a primary concern. It is not enough for FM to restore vehicle capabilities lost due to failures. The FM will have to facilitate termination of a rendezvous and safe separation of vehicles if the remaining fault tolerance of the maneuvering vehicle is too low. An exception to this rule may apply if the rendezvous is itself critical to avoiding LOC.

Pitfall: ***RPOD FM.*** *Unmanned vehicles performing rendezvous with a vehicle that has a crew will be expected to provide means for rendezvous/docking override by the crew. Sufficient FM situational awareness has to be made available to the crew, or there is risk that the crew will terminate a rendezvous due to a benign, but poorly understood fault or rendezvous trajectory perturbation.*

Recommended Practice: ***RPOD FM #1.*** *When the spacecraft is not at risk of either a collision with the target or causing docking collar damage, and a detected fault violates rules for completing the rendezvous, then a FM response should facilitate backing off to a safe hold point where reconfiguration options might enable another rendezvous attempt.*

Recommended Practice: ***RPOD FM #2.*** *If a detected fault in close proximity to the target violates docking rules or cannot be overcome by rapid reconfiguration, then FM has to quickly coordinate a safe separation maneuver to an acceptable distance and separated orbit condition. Once that has been achieved, application of the previous Recommended Practice rule can be considered.*

6.4.3.2.4 Free Flight in Space

Many space vehicles experience extended phases of free, unpowered flight, either in orbit or on an interplanetary trajectory. Some orbital spacecraft pursue their entire missions in such a phase. Under these flight circumstances, the TTC for most failures can be very long. There are possible failures that can have short TTCs during free flight in space (e.g., attitude control problems that allow unacceptable thermal stress on parts of the vehicle or that interfere with vehicle power-generation capability). For a free flight in space phase, FM response to failures with long TTCs

may be a vehicle default into a safe mode, awaiting ground control diagnosis and rectification of the cause of the failure. Furthermore, some rudimentary onboard FM control capabilities can be incorporated into a safe mode to prevent short TTC failure effects (e.g., providing for sun pointing in the safe mode to maintain power generation capability).

Recommended Practice: ***Free Flight in Space.*** *Always provide a safe mode option as a default FM response for when a detected failure is not directly addressed by a pre-determined fault isolation (and possibly reconfiguration) capability. A safe mode provides the ground or onboard crew with the time needed to formulate an effective failure response. To enable ground-directed recovery, commands from the ground have to be accepted and transmission of data as directed by the ground has to be accommodated when in the safe mode.*

6.4.3.2.5 Mated Flight in Space

Space vehicles that complete a docking operation may have extended operations mated to another space vehicle. Docked space vehicles generally rely on only one of the vehicles for orbit maneuver capability and orientation control (the active vehicle). The other docked vehicle operates in a passive state. The passive vehicle may also draw power and attitude knowledge from the active vehicle. In this scenario, an active vehicle operates much like a vehicle in a free-flight-in-space mission phase with similar FM design considerations (but with account for mass property effects of the mated vehicle on the stack control authority). A passive, mated vehicle will have many components in hibernation without active FM, but may also have some in warm standby mode, with long TTCs due to faults since they are not actively contributing to the mated stack functionality. Some "passive" mated vehicle systems may still actually be partly active during mated flight to sustain the intended function of the "passive" vehicle during docked operations (e.g., ISS visiting vehicles with a pressurized cargo volume in which the station crew can work may require active air circulation components).

Recommended Practice: ***Mated flight in space.*** *Exchange sufficient on-going FM information between mated vehicles to enable the following: Assured insight into the safety for subsequent use of a currently passive vehicle; wake up of idle subsystems on the passive vehicle, as needed, to protect it against loss of critical support services from the mated, active vehicle (including readying it for possible emergency haven use when a crew is involved).*

6.4.3.2.6 EDL from Space

Entry from space, as well as the descent to the surface, and safe landing are very dynamic flight phases whether involving a return of a vehicle to Earth or landing on another celestial body. Entry occurs during descent to a celestial body with a sensible atmosphere. Peak g-levels during entry can vary from less than 3 g's (e.g., Shuttle return to Earth), to 100s of g's (e.g., the Galileo probe entry at Jupiter). Descent can be under parachute, or guided aerodynamic flight at a planet with an atmosphere. Descent uses propulsive thrust when landing on a body without an atmosphere, or as an alternative pre-landing descent capability on a body with an atmosphere. G-levels during descent vary from that of the ambient celestial body g-field level to somewhat higher values, but with possible transient accelerations that are substantially higher when there is an atmosphere due to wind gust effects or due to parachute deployment dynamic effects.

Landing involves management of terminal touchdown devices under the following range of scenarios: Flared wheeled landing; splashdown; thruster "thump down"; airbag impacts; flared parachute landings; and thrusted deceleration to touchdown.

Failures during EDL have times of criticality ranging from short (seconds) to very short (milliseconds) depending on the specific vehicle dynamics. The general implication is that all FM capabilities for all flight-critical components during the EDL phases have to be onboard the vehicle and fully automated.

During an entry, dynamics of a healthy vehicle can vary substantially from nominal expected behavior both because of uncertainty in vehicle aerodynamics models and because of statistical variability in atmospheric characteristics. Consequently, FM methods used for failure detection and isolation during entry have to be robust enough to distinguish failure effects despite sensed vehicle behaviors that can be quite variable.

During descent under parachutes, FM failure detection and fault isolation methods have to avoid triggering false failure indications due to wind gust or parachute deployment-induced transient accelerations. Each phase of parachute deployment has to occur under proper dynamic pressure and Mach number conditions, which imposes FM requirements aimed at assuring sustained and accurate measurements of the states used to sequence parachute deployment events. During propulsive braking descent, special FM requirements will apply to the thrust control, including the throttle management, to assure that a safe vehicle velocity as a function of altitude always is followed.

During landing, special attention has to be applied to the monitoring of states that sequence controlled touchdown events, with FM-related reliability and robustness requirements on the applicable state measurement devices and landing system actuators. These components may include ground-relative altitude sensing devices, thrust cutoff indicators, and mechanical landing mechanism deployment devices (e.g., for landing gear drop, or airbag inflation). Vehicle orientation control at terminal touchdown may also be critical, requiring appropriate ground-relative attitude (and altitude) sensing and control redundancy with time-critical FM management of any associated component faults.

Pitfall: ***EDL from Space FM.*** *Analytic detection of propulsion failures can be very difficult during atmospheric entry when there are sizable uncertainties in atmospheric properties and vehicle aerodynamics.*

Recommended Practice: ***EDL from Space FM.*** *Because there is little tolerance to error during EDL, all fault sensitive functionality has to be either highly reliable, or redundant with rapid reconfiguration capability.*

6.4.3.3 Some Mission Phases for Air Vehicles

Air vehicles include powered aircraft, gliders, and balloons. They operate in a sensible atmosphere, but can deploy/takeoff from the ground, air, or space. All air vehicles may apply FM to achieve the desired probability of mission success, but air vehicles that fly over the Earth have to also apply FM to assure safety of people and facilities on the ground. The following

subsections identify typical air vehicle mission-phases, and some FM capabilities and/or issues unique to each of the identified mission phases.

6.4.3.3.1 Air Vehicle Takeoff or Deployment

Winged air vehicles that self-deploy from the ground have their own takeoff propulsion that carries them though a lifting ascent to their operational flight condition. Winged gliding vehicles need aid to deploy, carried to their release condition by a powered vehicle. Balloons that use buoyant lift from a lighter-than air gas are released from the ground or in the air to find equilibrium drift conditions.

A winged, powered aircraft has to use FM during takeoff (or during deployment following entry from space) to assure safe transition to flight. For a vehicle that takes off from Earth, possible takeoff abort or expedited return to landing criteria should be managed by an FM system to overcome problems that may occur during takeoff acceleration and climb-out. For a powered vehicle deployed following entry from space, FM will have to address extremely short TTC failures that can occur during very dynamic transition from an entry vehicle payload to an airborne, powered-flight vehicle.

A glider already released for its mission has to assess its own behavior to determine how well it is managing its potential energy to achieve flight objectives. Based on a glider's energy state, an onboard FM system has to discriminate when the vehicle can accomplish a safe flight completion or direct safe early termination of the gliding mission instead. FM actions also have to account for the state of a glider's control actuation devices.

For balloons deployed from Earth, a ground crew manages the deployment sequence, with the vehicle's onboard FM focus usually pertaining to the payload. Earth-based balloon FM facilitates successful payload mission execution, despite failures, and provides for safe payload recovery when the mission terminates. FM may also be used to manage systems that prevent an Earth-based balloon payload from landing in a location that is unsafe to people or facilities on the ground.

For balloons deployed to other planetary bodies, there will likely be a balloon/payload deployment sequence from a carrier vehicle during a carrier descent phase. There may be redundancy in components that are critical to successful balloon deployment and that have very short TTC after failure. For those components, applicable FM will have to be part of an automatic, onboard system.

Recommended Practice: ***Air vehicle takeoff or deployment FM.*** *Because there is little tolerance to error during takeoff or deployment of an air vehicle, all failure-sensitive functionality has to be either highly reliable or redundant, with rapid reconfiguration capability.*

6.4.3.3.2 Air Vehicle Cruise, Glide, or Drift

The mission operations phase for most NASA air vehicles involves cruise for a powered, winged vehicle; glide for an unpowered, winged vehicle; and drift for a balloon.

During cruise, a powered winged vehicle may have short TTC for propulsion and stabilization effector faults (seconds), but may have longer TTCs for navigation errors. However, TTC for navigation errors on Earth-based air vehicles may also be constrained by limits to aircraft situational awareness uncertainty that impacts the accuracy of path management in the airspace. For an Earth-based aircraft, onboard FM will require automatic means to address fault effects for any critical subsystems deemed to have short TTC, while faults that have criticality times in excess of 30–60 seconds may be managed by ground-based mission operators. Ground operator intervention is not an option for FM of any critical component on a cruising air vehicle in a planetary exploration application because of communication time lags that are large compared to faulted component TTC.

FM considerations for a gliding vehicle are similar to that for a cruising vehicle, but with the additional consideration that navigation faults have shorter TTC because navigation errors eat into glider energy management margins.

For drifting balloons, FM focuses on facilitating successful payload operations, with the TTC of many payload faults restricted only by the impact of the resulting loss of productive payload function time. Remaining mission life is impacted by the balloon integrity and the status of the buoyant gas supply. Subject to a compromised balloon condition, an FM response option for a recoverable payload could be ejection, to assure its safe return for future use. FM for the payload functionality during flight may be handled like an unmanned space vehicle in coasting flight, with extensive reliance on ground operators.

Recommended Practice: ***Winged vehicle cruise or glide FM #1.*** *Because there is little tolerance to loss of control effects on a winged air vehicle, and for loss of navigation in Earth air space, all failure-sensitive functionality during cruise or glide has to be either highly reliable, or redundant with rapid reconfiguration capability.*

Recommended Practice: ***Winged vehicle cruise or glide FM #2.*** *During cruise of a powered winged vehicle, FM can treat a multiengine propulsion system as redundant since cruise thrust requirements are much less than for takeoff.*

Recommended Practice: ***Drifting balloon FM.*** *Provide a safe mode as a default FM response when a detected failure is not directly addressed by a predetermined fault isolation and possibly reconfiguration capability. The safe mode should maintain the vehicle in a stable condition long enough to allow ground mission personnel to formulate an effective failure response. To enable ground-directed recovery, commands from the ground have to be accepted and transmission of data as directed by the ground has to be accommodated when in the safe mode.*

6.4.3.3.3 Air Vehicle Landing

All winged vehicles that seek an intact landing at designated sites have tight control requirements and bounded descent corridors that dictate response effectiveness and timeliness requirements for FM. The control requirements aim to maintain vehicle stability, and to keep the vehicle within corridor bounds that enable safe touchdown at a designated location. For landings on Earth, this has to be done without airspace violations, without hazards to external facilities, and

without risk to people on the ground. For a terrestrial aircraft, a controlled crash into an acceptable terrain location may be a better FM option than continued cruise flight that risks vehicle control loss with associated hazards to ground locations. An airplane used in planetary exploration may not have the same FM design constraints, possibly allowing an uncontrolled crash landing at the mission end. FM during aircraft landing will have to cover all effectors and navigation systems critical to successful terminal decent and landing. Short TTC for faults impacting landing system components mandates that the FM occur automatically onboard the vehicle.

Landing for a balloon payload aims to assure that it touches down intact. On Earth, the payload landing should occur in a safe, defined location where payload recovery can occur. FM requirements for landing pertain only to descent system components that directly contribute to proper payload touchdown conditions. Short TTC for faults affecting payload descent system landing-related components mandates that the FM occur automatically onboard the landing vehicle.

Air snatch intercepts descending reentry vehicles by air vehicle capture of parachute lines, and has the potential to reduce impact loads and contamination risks. Air snatch can also be performed away from populated areas, which reduces risk from impact of the vehicle, payload, and exposure to hazardous materials such as propellants and pyrotechnics.

Recommended Practice: ***Winged aircraft landing FM.*** *Because there is little tolerance to error during winged aircraft landing, all fault sensitive functionality has to be either highly reliable or redundant with rapid reconfiguration capability. This is especially true for all elements of the Guidance, Navigation, and Control (GN&C) subsystems, including applicable avionics and effectors.*

6.4.3.4 Some Mission Phases for Surface Vehicles

NASA surface vehicles operate on the ground of other celestial bodies. They are emplaced on a surface following a propulsive and/or aerodynamic descent. They can be stationary or mobile, and may operate intact in their landed configuration, or they may be released/deployed from within a carrier shell. The TTC for faults on surface vehicles is likely to be shorter for mobile vehicles than for stationary vehicles, influenced in part by the nature of possible surface obstacle hazards. Some of the applicable FM considerations are addressed in the following subsections.

6.4.3.4.1 Surface Vehicle Deployment

Deployment of a surface vehicle may be simple or complex. If a surface vehicle is not contained in a protective landing cocoon, then initial post-landing deployment may focus on specific appendages. These may include power systems (e.g., solar panels or radioisotope thermoelectric generators), communication antennas, observational devices, and robotic manipulation components. If a surface vehicle is contained within a landing shell, then many parts of the surface vehicle that are folded to fit within the cocoon may have to be extricated, and then opened or extended. Deployment steps generally result in successful latching of opened or extended components. Often, specific steps in a deployment sequence depend on success of the

prior steps. Consequently, fault in execution of each deployment step has to be detected, and rectification action taken before subsequent deployment steps can be safely attempted. Release and/or capture latches associated with deployment may require redundancy when the function of an individual latch can affect the success of the mission. In some instances, redundant latching may be attempted in parallel, where success with any one latch will enable success of that deployment step. In that instance, it may be necessary to determine if latching is accomplished, but may not be necessary to detect a fault in a particular redundant component. If only one latch at a time in a redundant set can be exercised, then detection of a latching fault is necessary to determine if a redundant component has to be exercised.

Recommended Practice: ***Surface Vehicle Deployment FM.*** *Provide either a) highly reliable or b) redundant deployment mechanisms and associated latching for each step of vehicle deployment, with means to verify the status during each of those steps. Include safe-hold modes to enable ground-directed recovery where possible during deployment for use when unanticipated faults are detected or when completion of an essential deployment step cannot be verified. Commands from the ground have to be accepted and transmission of data as directed by the ground has to be accommodated when in safe mode.*

6.4.3.4.2 Stationary Surface Vehicle Operations

Stationary operations of deployed surface vehicles may still require some onboard FM functionality. High data rate communications systems need to track either orbiting relay platforms or Earth. Failures of tracking elements need to be detected onboard so either a redundant component can be activated, or a lower bandwidth, less directional communication channel can be enabled to maintain critical data links. If the vehicle has robotic manipulators, then there will likely be unique FM requirements associated with either direct or functional component redundancy that prevent LOM due to manipulator component faults.

Recommended Practice: ***Stationary Surface Vehicle FM.*** *Provide a safe mode that puts the vehicle in a protective state as a default FM response when a detected fault is not directly addressed by a pre-determined fault isolation and possibly reconfiguration capability. The safe mode should prevent vehicle damage and minimize usage of (or allow generation of) vehicle power while ground mission personnel formulate an effective fault response. To enable ground-directed recovery, commands from the ground have to be accepted and transmission of data as directed by the ground has to be accommodated when in the safe mode.*

6.4.3.4.3 Surface Mobility Vehicle Operations

A robotic surface mobility vehicle has the option of terminating motion to provide ample time for assessment of necessary response to a detected fault. This would be comparable to a "safe mode" FM response used by a coasting spacecraft. The use of onboard, automated FM functionality on a robotic surface mobility vehicle is influenced by the relative value of the TTC for specific classes of faults. When the TTC is shorter than expected communication gap durations and/or communication signal time lags, then an automated FM capability is indicated over ground control response to a detected vehicle fault.

Recommended Practice: ***Surface Mobility Vehicle FM.*** *Provide a safe mode that puts the vehicle in a protective, stationary state as a default FM response when a detected fault is not directly addressed by a pre-determined fault isolation and possibly reconfiguration capability. The safe mode should maintain the vehicle in a benign stationary condition, with power minimized and/or generated if possible, while ground mission personnel formulate an effective fault response. To enable ground-directed recovery, commands from the ground have to be accepted and transmission of data as directed by the ground has to be accommodated when in the safe mode.*

6.4.3.5 Aborts

Space vehicles with crew have an FM priority to assure crew safety. Aborts are a special contingency form of FM response when the nature of a detected fault precludes FM restoration of nominal functionality, and the TTC of a fault precludes using a safe mode to provide opportunity to evaluate the fault implications. Flight phases where special abort modes are appropriate include powered ascent flight (launches), rendezvous operations (with respect to either another spacecraft or a small celestial body) when collision is a risk, and powered descent for extraterrestrial landings. Abort modes may also be invoked in response to a malfunction of a second vehicle's propulsion system that is used for a large velocity change burn applied to a space vehicle with crew (e.g., during Earth escape burns). Reentry to Earth is not a candidate for an abort, since it is generally an irreversible mission phase once initiated. However, transition from controlled entry to ballistic entry is an option for a capsule spacecraft following some major vehicle faults, but still, reentry continues in that scenario.

Aborts are initiated when a non-recoverable major fault occurs. Examples include when there is a major fault in an ascent propulsion system, or when full trajectory control can no longer be assured during rendezvous. Aborts may apply unique contingency systems (e.g., an ascent escape tower for a capsule, a launch abort system (LAS)), or may just apply alternative software functionality to systems that were already in use (as would generally be the case during a rendezvous abort).

In addition to preventing LOC during aborts, an FM system will be required to prevent harm to people and facilities on the ground. During aborts, special means may be applied to separate a passenger compartment/vehicle from an ascent booster to allow the booster to be destroyed in a safe zone while the crew attempts a survivable return. There may be unique control effector-related FM requirements during aborts to assure the highest possible likelihood of safe crew return given that LOM is already a given.

Pitfall: ***Abort capability implementation.*** *Crew displays of information to determine abort status can be complex, and may result in some scenarios where the proper response is ambiguous. Care has to be taken to assure that the crew will only command an abort when necessary.*

Recommended Practice: ***Abort capability implementation #1.*** *While providing for automatic aborts in all time-critical scenarios, always provide means for an onboard crew to designate, initiate, and/or override an abort capability.*

Recommended Practice: ***Abort capability implementation #2.*** *Whenever an abort mode may arise due to a fault on a second vehicle attached to a spacecraft carrying a crew, include independent means for the crew and the spacecraft carrying them to determine the health of the combined system function, providing sufficient insight to determine when a crew should initiate an abort.*

6.4.4 Operational Capability Considerations

6.4.4.1 Automated Operations

Automated robotic space vehicle operations provide a programmed set of sequences (including those related to FM) in the flight computer that are triggered by mission phase changes, detected/recognized events, or ground/crew command.

6.4.4.2 Human-in-the-Loop

Human-in-the-loop missions have requirements to enable interaction by humans in applicable mission decisions (either directly onboard the vehicle or by humans supporting the mission from the ground). FM functionality for systems with humans in the loop has to provide command paths into the onboard FM functionality for the required levels of human interaction. When there are crew members on board an applicable space vehicle, display and control (D&C) system functionality has to be provided to support the required levels of crew interaction.

6.4.4.3 Autonomous Operations

Autonomous vehicle operations provide the capability to determine a vehicle's own course of action independent of ground intervention, including in response to the vehicle's own assessment of sensed external factors. This assessment may be done by machine and/or by onboard crew. Onboard FM capabilities may be part of autonomous operations, including both fault detection and responses. Autonomous FM capabilities will be needed on a robotic vehicle when TTC for faults and/or communication constraints preclude reliance on ground controller intervention. On a vehicle with a crew, the following FM design considerations apply:

- When the TTC for a fault is too short for crew response, then automated FM functionality is provided.
- When the TTC allows for crew intervention, automated functionality may still be provided to limit crew workload.
- Generally, all onboard FM functionality will provide means for human oversight as well as intervention or override.

FM capabilities can be fully integrated into a vehicle's autonomous ConOps. Means for vehicle FM autonomy can be provided in combination with means for ground intervention and override of the vehicle's FM system when warranted, with the associated requirement for the vehicle to provide necessary telemetry to the ground to enable fully informed intervention or override by

ground personnel. The benefit of vehicle FM autonomy is that the vehicle is not dependent on the ground (with an associated time-delayed and possibly intermittent communication link) to address certain anticipated fault scenarios.

6.4.4.4 Ground Operations

6.4.4.4.1 Ground Operations Role

The ground role in the operations of robotic vehicles includes mission support, either in the form of commands or responses to failures. Ground operations may also take the raw data acquired onboard a vehicle and analyze it to provide necessary FM-related event response to a vehicle that does not have that FM capability onboard, or is in a configuration where such onboard FM authority is not granted.

An FM role for vehicles with crew may include procedural advice to the crew. However, ground operations may take the raw data and analyze it in more detail than is possible onboard, to help the crew or vehicle FM capability to determine the appropriate FM-related event response. This ground operations role may be applied under circumstances where the required event response analysis exceeds the onboard processing capabilities and/or puts too much workload burden on the crew.

6.4.4.4.2 Ground Response Latency and Telemetry Bandwidth Considerations

The planned role for ground interaction in vehicle FM operations must always account for communication restrictions involving gaps, delays, and/or communication link bandwidth limits. The latency associated with the ground detecting and responding to failures and the limits in the fidelity of data available to the ground are fundamental mission characteristics driving the required scope for in-flight FM autonomy. Where the ground is able to respond to failures quickly with high confidence in providing a proper response, little FM autonomy is needed to protect system health. However, as ground-in-the-loop response latency increases to the point that it exceeds the TTC of certain faults, then additional FM autonomy will be necessary to mitigate those failures as needed.

The following factors affect ground-in-the-loop response latency.

- *Delays in Ground Access to Spacecraft Data*: This includes the effects of contact schedules that are driven by spacecraft-to-ground-receiver visibility considerations; downlink time that is affected by signal transit times and bandwidth; data latency based on onboard data management protocols; and latencies in the ground's received-data handling system.

- *Analysis*: Spacecraft telemetry data has to be analyzed by ground personnel and/or software-based capability to detect unexpected or unacceptable vehicle/component behavior. This includes the time for data de-convolution and data processing by FM-support algorithms.

- *Operator Notification:* Ground operators with expertise in fault-impacted systems have to be reached and notified regarding FM analysis findings.

- *Operator Review of Data and Response Formulation*: The applicable ground operator(s) has to absorb and interpret the supplied fault analysis information and make response decisions. This has to be done in compliance with applicable response procedure protocols.

- *Delays in Response Data Uplin*k: This includes ground system uplink data processing and command execution latencies (that may include uplink data validity checks); the effects of contact schedules that are driven by spacecraft-to-ground-receiver visibility considerations; and uplink time that is affected by signal transit times and bandwidth.

Telemetry bandwidth is a major factor in determining ground confidence regarding insight into vehicle faults and resulting responses. Bandwidth limits can affect both the fidelity and completeness of supplied vehicle data needed to analyze the spacecraft and associated fault status.

6.4.4.5 Hybrid Operations

Hybrid refers to blending more than one kind of capability. Hybrid operations apply to robotic vehicles that have to accommodate both human intervention (i.e., via ground operations) as well as automated intervention during various parts of the mission. In the context of vehicles with crew, hybrid operations apply when there is a mix of means for machine and human mission management (from the ground or onboard). An FM system design for a vehicle with hybrid capabilities has to provide paths for ground operations and/or onboard crew to preempt or override onboard FM processes and actions.

6.4.4.6 Overrides

Vehicles generally are required to provide means for override of suspect automatic FM responses. This can be accomplished by the ground control, by onboard crew, or by crew at a remote in-space location (e.g., the ISS).

6.4.4.7 Onboard Displays and Controls

Space vehicles with crew have requirements to provide means for crew interaction and/or intervention in FM functionality. Providing means for crew interaction necessitates dedicated D&C functionality. The granularity and scope of the onboard D&C and associated crew access to FM functionality may not be as comprehensive as is available to ground control facilities based on display limitations and crew workload constraints.

6.4.5 Some Other Considerations

In addition to the risk posture, mission type, and mission phase consideration discussed previously, some other mission-unique factors can influence FM requirements and design choices. A few of those factors and their FM implications are discussed in the following subsections.

6.4.5.1 Launch Window Constraint Implications

Opportunities to launch spacecraft to other celestial bodies are constrained by the relative orbital placement of Earth and the target destination. Launches to a targeted lunar intercept may happen about one day a month. Launch to a planetary intercept may be possible during an interval lasting only weeks that occurs only once over a period of years. Each day that a launch window exists for these destinations, the launch window will be available for minutes. When launching on an Earth orbit rendezvous mission, an opportunity to launch lasts minutes each day, with many days precluded because of adverse expected lighting conditions during rendezvous. The following recommended FM practices can limit the likelihood that spacecraft faults and FM design complexity will prevent a constrained-window launch from occurring.

Recommended Practice: ***FM operability prior to constrained window launches.*** *FM functionality should be active long before launch so that latent vehicle faults that would violate launch rules can be detected and rectified before they impact a limited launch window opportunity.*

Recommended Practice: ***FM innovation limits for constrained launch-window missions.*** *For vehicles subject to planetary launch window constraints, with infrequent launch opportunities, any innovation demanded of the FM design and its implementation has to be limited to what can confidently be addressed within the baseline development schedule (to avoid risk that FM system development delays prevent meeting a given launch window cycle). Reuse of proven FM capabilities, design methodologies, and algorithms should be maximized under these circumstances.*

6.4.5.2 Reentry Constraint Implications

Reentry from orbit nominally occurs at a time that is nearly fixed upon initiation of maneuvers toward a de-orbit initiation point. Delay of de-orbit can only occur if the vehicle has the resources, such as propellant and power, and configuration, such as operational system components needed to continue its operation until another specific de-orbit opportunity is reached (which may be up to a day later). Also, a de-orbit sequence has to be completed after the orbit perigee has dropped below a critical point. A reentry sequence following a trajectory from deep space has to complete its execution at the designated time (which is determined when the trajectory toward the reentry target is initiated).

Recommended Practice: ***FM functionality for de-orbit and reentry from deep space.*** *For either reentry following a trajectory from deep space, or for de-orbit, the onboard FM system should have access to redundancy for components critical to reentry and/or de-orbit success, and should also have rapidly responsive, autonomous FM functionality with respect to the critical, redundant components.*

6.4.5.3 Cost Constraint Considerations

Implementation of an FM capability is an on-going part of a vehicle and mission system development program that can constitute a significant part of development cost. The assigned human resources for FM design and implementation, the subsystems that contain redundant components, and the supporting budget, should all be commensurate with the risk posture of the development program. Program risk postures that demand less risk require more FM development resources.

6.4.5.4 A Backup Flight Control System Option

A Backup Flight Control System (BFCS) is an FM design option for vehicles with crew that can provide protection against unanticipated faults with the primary avionics and software system, as well as the primary system's dedicated redundant components that may render the primary system unable to prevent LOC. The possibility of common mode faults that could simultaneously take out redundant primary system elements is a typical justification for considering a BFCS as part of FM. Potential sources of common mode faults include systematic component design flaws, major software functionality bugs, or accidents that simultaneously damage numerous vehicle components. The following are some of the considerations to address in deciding whether to include a BFCS:

- The added safety provided by including a BFCS should be deemed to exceed the safety gain that could be realized by applying the same resources to make the primary system more reliable. That requires consideration of how much primary system reliability gain can be realized, and at what cost, by more thorough component screening and testing; better system protection against environmental risks; more complete integrated hardware/software systems testing; and further physical separation of components with functional overlap.

- Inclusion of a BFCS would require that all aspects of its design be as independent as possible from the primary system. The software should be independently developed, coded, and verified. To the extent possible, processing and sensing resources should be distinct from the primary system. Also, while it will be impractical to have separate effectors, separate command paths to the effectors may be warranted. To realize all of these BFCS design factors, the BFCS developers should be a personnel team independent of the primary system development team. Consideration has to be given as to whether that is practical. Note also that an independent BFCS development team would have to coordinate the integration of a BFCS design into the vehicle with the overall vehicle integration team, which adds some work burden also to the vehicle integration team, too.

Measures also must be taken to prevent inadvertent, and possibly irreversible, in-flight selection of BFCS operations. The BCFS, as its name implies, represents back-up functionality, but must be invoked only in well-specified, agreed-on circumstances.

7. ASSESSMENT AND ANALYSIS

[This section will be expanded in later releases. The plan is to include the following topics.]

1. Quantitative versus Qualitative Analysis
   - 1.1. Safety Net
   - 1.2. Quantitative Buy-Down
   - 1.3. Qualitative "Patch-Up"
   - 1.4. Analysis for Design versus Verification/Validation
2. LOC, LOM, and Availability
   - 2.1. Fault Management Control Loop Effectiveness
   - 2.2. Single and Multiple-Fault Criteria
   - 2.3. Failure Effect Propagation
   - 2.4. Latent Faults and Failure Effect Interaction
3. Failure Scenarios
   - 3.1. Failure Scenario Criteria
   - 3.2. Failure Scenario Usage
4. Detection
   - 4.1. Coverage
   - 4.2. False Positive
   - 4.3. False Negative
5. Isolation and Identification (Diagnosis)
   - 5.1. Observability
   - 5.2. Isolation FP/FN
   - 5.3. Isolation for Repair and Recovery
   - 5.4. Identification for Root Cause Analysis
6. Failure Response Decision
7. Failure Response
   - 7.1. Race Conditions
   - 7.2. Response Interactions
8. Prognostics
   - 8.1. Remaining Useful Life
9. Models
   - 9.1. Goal Tree/Success Tree
   - 9.2. Fault Tree
   - 9.3. Discrete Events and State Machines
   - 9.4. Directed Graphs
   - 9.5. Physics-Based Models

8. VERIFICATION AND VALIDATION

FM V&V is part of the overall set of actions performed on a system. It is the set of V&V actions addressing system behavior in off-nominal situations. FM verification proves that the system design responds to failures as specified by system requirements, and FM validation proves that the reactions of the system preserve the assets and the intended functions. FM verification is an essentially bottoms-up, design-specific approach, and FM validation is essentially a top-down, intent-specific, system-wide approach.

Verification is the process of proving that a system conforms to its set of requirements.[9] The requirements are often in the form of a formal requirements specification for the system. In addition, requirements can be levied from other sources such as ICDs and IRDs.

Validation is the process of proving that a system conforms to the set of stakeholder expectations, as captured in the project/program ConOps document.[10] This process shows that the system is capable of accomplishing the desired system-level behavior under realistic nominal and off-nominal conditions and determines the effectiveness and suitability of the product for use in operations. It is focused on scenarios that exercise the system and analysis of the suitability of the resulting behavior without tracing specifically to system requirements.

This section describes FM V&V with respect to a "system"—both because system validation is a primary concern, and because the approach and process steps described here can be applied to any definition of "system." This is based on a given system boundary regardless of whether the defined system is a part, component, board, subsystem, vehicle, facility or combination of vehicles and facilities (e.g., a system of systems).

FM V&V is historically problematic, with many examples of inadequate resources (people, time, and budget) and/or unexpected problems. Many factors contribute to these issues, but the problem can be traced to a general lack of appreciation of system complexity. When considering a system, there are significantly more ways the system can fail (contingency paths) than ways it can succeed (nominal paths). Since the typical effort and planning for FM V&V is a small subset of the overall system V&V effort, it should not be surprising that these issues and inadequacies continue to occur. This section of the FM Handbook is intended to describe processes and best practices to enable managers and engineers to better define, scope and execute FM V&V.

8.1 Fault Management V&V Process Overview

The following section presumes familiarity with the system V&V process as described in the NASA SE Handbook. The process description here is intended to integrate and extend the ideas captured in the NASA SE Handbook, capturing differences, and providing more detail into FM V&V concerns and issues. The following subsections contain recommended practices, pitfalls,

[9] NASA SE Handbook, Section 5.3 (Product Verification).
[10] NASA SE Handbook, Section 5.4 (Product Validation).

and lessons learned specific to FM V&V, organized by the five V&V activities as defined in the NASA SE Handbook.

8.1.1 Fault Management V&V Planning

The execution of any FM V&V effort is preceded by a planning effort to determine and document the approach and risk posture to be taken for FM V&V. This effort is a subset of system V&V planning and should be undertaken at the same time. The material in the FM V&V plan has to be consistent with the project/program V&V plan. The FM V&V plan documents guidelines, goals, and process steps for FM V&V activities, as shown in the FM Process diagram in Figure 2. The planning effort should include test planning, plans for simulator development, test-bed certification, and identification of test assets and required fidelity. Often, necessary test resources and fidelity identified during FM V&V planning drives the scope of system V&V test assets, such as the number, fidelity, and fault injection capabilities of various test platforms. In some cases, this effort has required half of the total test asset planning time.

One key result of the FM planning effort is the determination of the scope of off-nominal scenarios to be considered in FM V&V, particularly for FM validation. The ability of the set of defined V&V actions to "cover" adequately the identified failure space, the as-implemented FM design, and the intended off-nominal behavior is a cost/risk trade that has significant implications to the project schedule and risk posture. Decisions on the approach and amount of V&V coverage should be made and documented early in the project lifecycle so that specific plans can be developed and costs estimated. Frequently, this aspect of FM V&V is given insufficient attention, and results in the cost and schedule impacts/overruns often seen during system test.

Pitfall: ***The Bump.*** *Many projects have experienced a significant increase in resources required to complete system-level FM V&V. This has been termed "the bump." Prepare for the FM V&V "bump" during testing by adequately planning the FM testing and accounting for integration issues, such as unplanned interactions or unexpected system behaviors. The size of the "bump" will be affected by the particular integration flow and the choice of system architecture and selected FM mechanisms.*[11] *The graphic in figure 7 illustrates a typical situation of planned effort (see black line) compared to the actual effort required (red line).*

[11] Future versions of this Handbook will address these points in more detail.

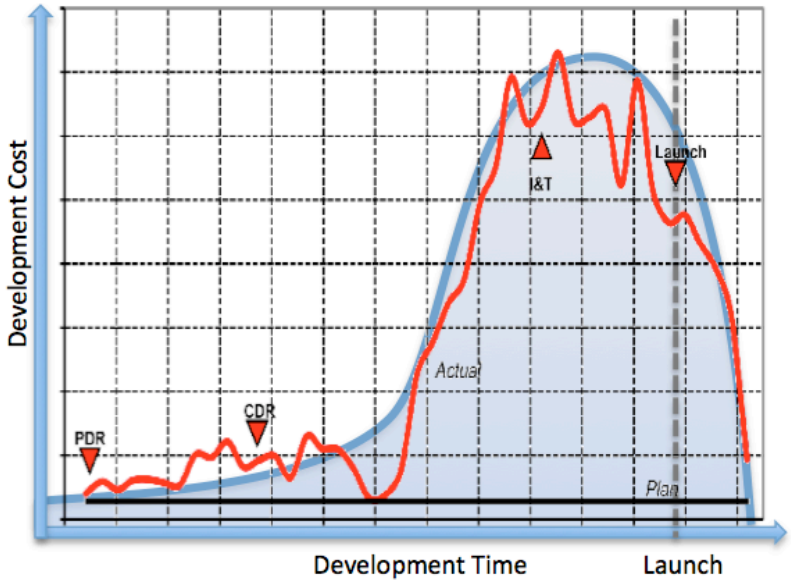

Figure 7—"The Bump" in Required FM Resources

Recommended Practice: ***FM V&V plan contents.*** *Include the following material in the FM V&V Plan: guidelines of verification approach, required test venues, approach for determining fault injection requirements, intended level of fidelity of models in test venues, scope of off-nominal scenarios for FM validation, coverage guidelines for FM validation (document resulting/intended risk posture), and policy on verification completeness.*

The results of the FM V&V planning effort should be documented in a formal project document. Depending on the size and document tree of a given project, the FM V&V material may appear in a separate FM V&V document, or be included in the project V&V planning document. Either option is acceptable, as long as there is a document that contains the FM V&V planning material.

Recommended Practice: ***Pass/Fail criteria.*** *When establishing pass/fail criteria for FM tests and demonstrations, the criteria should include the expected condition of all health-critical and mission-critical objectives. If these conditions are not part of the physical hardware or simulation used for the test or demonstration, analysis should be used to assess their behavior. This makes clear whether a given result during a test necessitates a retest.*

Recommended Practice: ***Account for sufficient resources.*** *Use the FM validation matrix to develop an estimate of the resources needed for performing off nominal (FM) V&V. See section 8.2.1 for additional discussion on the development of a FM validation matrix.*

Recommended Practice: ***Begin system validation planning early.*** *System validation planning for FM should begin during the design phase. The act of developing system-level validation tests often reveals inconsistencies in FM design and assumptions, such that the act of developing validation tests itself is a good early-on check (i.e., paper test) of the system. FM system engineers can still influence subsystem designs to ensure that they meet overall FM goals and*

identify inconsistencies and potential defects before they progress into the formal test program. Additionally, the FM engineers can determine if sufficient monitoring capability (e.g., test points, software telemetry interfaces) will be available during testing to validate the design.

Recommended Practice: ***Generate an "incompressible test list."*** *By the beginning of the test program, the test plan should have an "incompressible test list" which is, as it sounds, the absolute bare minimum list of tests that have to be run to qualify the design. Additionally, a standard set of FM regression tests (FM regression suite) should be generated when changes to the design (whether hardware or software) are made. (A further option is a minimal regression suite when just FM parameter changes are made. These are usually determined on a case-by-case basis, but identifying these upfront can stave off last minute disagreements.)*

8.1.2 Fault Management V&V Preparation

FM V&V implementation takes the FM V&V planning products and develops the specifics of the FM V&V approach. The difference in effort between one program and the next is dependent on the way in which the program has developed the FM requirements. In some programs, FM requirements are very specific and document each allocated FM function—in this case, the set of verification actions will be many. In other programs, the set of FM requirements is broad, perhaps referencing a lower level document or a database—in this case, the set of verification actions will be smaller. Depending on how the verification actions are performed, and the way in which the FM requirements are stated, the set of validation actions will vary as well.

The first step is the development of the V&V matrices, as illustrated in figure 8, Implementation—V&V Matrices.

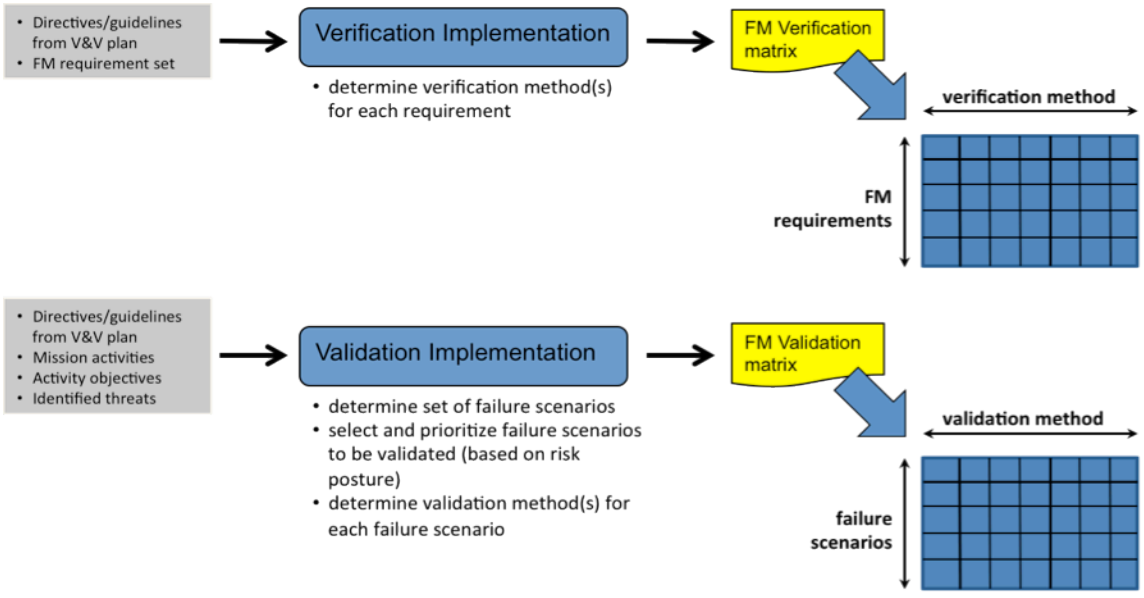

Figure 8—Implementation—V&V Matrices

Recommended Practice: ***Develop an FM system validation matrix.*** *Identify system tests that validate system performance ("Is the system doing the right thing?"). These tests should focus*

on system behavior and mitigate system risk. The plan should also include the test platform and resources needed for each test. Reviewing existing subsystem verification plans can help identify uncovered areas. The plan should then be developed into FM validation procedures. This notion of a validation matrix differs slightly from the description of the validation matrix in the NASA SE Handbook. The FM validation matrix is intended to be an extension of the validation matrix described in that document by including failure scenarios in the system validation matrix. For simplicity, this document refers to the FM portion of this validation matrix as the "FM validation matrix."

Recommended Practice: ***Prioritize requirements from a test perspective.*** *Not all requirements are equally important.*

Recommended Practice: ***Method selection.*** *While testing is typically viewed as the most desirable method for V&V, other methods may allow a more cost-effective solution that still meets the required risk posture. The selection of which method to use has to be weighed carefully in order to make use of V&V resources wisely. For example, analysis may be a more effective approach than development of complicated fault injection capabilities. Physics-based modeling can serve as a form of analysis and/or can be used to focus limited resources on the design of highly discriminatory tests. Future versions of this Handbook will provide additional information to guide FM practitioners in determining appropriate V&V method selection.*

Pitfall: ***Incremental verification.*** *Verification is usually performed "early" in the test program. Thus, it follows that low-level subsystem verification is often only exercised on individual subsystems in a standalone environment. External interfaces and external stimuli are either simulated or completely nonexistent. Even with a perfect subsystem-verification plan, there are potential problems that cannot be discovered from verification testing since there are likely to be dependent subsystem and system interactions that are not apparent to the developer of the subsystem.*

Pitfall: ***Limitations of testing.*** *When a requirement reads, "The system shall perform response action A," a verification test is developed to prove that the response action is taken under a specific set of conditions usually at the discretion of the verification engineer. In reality, there may be a number of scenarios due to initial conditions and the external effects of other subsystems where the requirement would not be met. However, the verification approach is typically "prove that requirement X is satisfied under conditions where we expect it to be met" as opposed to "find a condition where Requirement X is not satisfied." Once the requirement is provably met (perhaps under only a single initial condition), the box is checked off ("requirement verified"), despite the possibility that the requirement may not be met under other conditions. Then verification progresses to the next requirement. Avoid incomplete verification of requirements by considering all the scenarios under which the requirement is expected to be met. Additional tests and/or analyses may be necessary.*

Pitfall: ***Verification by allocation.*** *When the "Verification by Allocation" approach is used, system verification is reduced to a bookkeeping exercise of tracking higher-level requirements by checking off boxes as lower level subsystem requirements are verified. This approach is greatly flawed. If system A is made up of two subsystems B and C and both subsystems are fully verified, it is not enough to claim that system A is now verified by way of the "checkbox." Requirements*

can be allocated to lower level subsystems, but verification should not be allocated. Instead, perform verification of higher-level requirements by testing the combined system. This may require unique test equipment and facilities to support testing of the integrated product. In practice, this becomes more difficult for a multitier system of systems because as you move up the chain to higher-level integrated systems, (1) the requirements typically become less specific; and (2) the resources required to perform the test become more substantial. This is where validation can play a key role since validation can ensure that the allocation of requirements was correct.

Recommended Practice: ***Prioritize validation tests.*** *Identify an approach to prioritize the suite of validation tests giving highest priority to those that mitigate the most significant risks. As schedule and resource pressures build, there may be a need to reduce the amount of planned testing. By defining a methodical approach to assigning priorities to tests, this can be used to define a minimum set of tests required to certify FM (i.e., incompressible test list). In the end, an agreement between the FM SE team and project management has to be reached to establish minimum criteria to ensure that the FM team will perform sufficient testing and project management will not reduce testing in the face of schedule pressure without understanding the effect on risk. See sections 8.2.1–2 for specific recommendations on selection and prioritization of validation tests.*

Recommended Practice: ***Gremlin****. Establish a role within the FM V&V (or Project V&V) effort for a person with the appropriate mindset to identify numerous, unusual, especially pathological ways in which the system can fail. Integrate these identified scenarios into the prioritized set of validation tests. This explicit "think outside the box" approach can usefully extend the range of identified failure scenarios.*

8.1.3 Perform Fault Management V&V

The V&V actions are performed per the associated FM V&V plans. As a part of performing each test or demonstration action, a test report is written to document compliance and deviations from test objectives. The test report also lists any problem reports generated during the test. Inspection and analysis actions are documented in inspection memos and analysis reports. These activities, while performed to verify and validate FM functionality, are typical for execution of all V&V programs. More detail on the processes and outputs may be found in the NASA SE Handbook, sections 4.3.1.2 (Verification Process Activities) and 4.4.1.2 (Validation Process Activities).

Recommended Practice: ***Use formal modeling.*** *Leverage the ability of formal models and model checkers to perform some aspects of FM V&V, leaving a small number of validation cases for testing on flight hardware. Formal modeling is much more important for FM V&V than for V&V of nominal system behavior due to the exceptionally large number of possible failure scenarios, and for assessing the propagation of failure effects, which can only be done incompletely in tests and demonstrations. Formal models and simulations allow the exploration of many more states than are possible by test.*

Recommended Practice: ***Leverage features of system architecture.*** *Utilize system architectural features that allow well-behaved extrapolation of test cases by analysis. This enables test results*

from a given failure scenario to be extended to other failure scenarios that share the same architectural feature, increasing the coverage of the failure space, and grounding the analysis in actual test results.

Recommended Practice: ***Perform parameter reviews.*** *FM functionality is directly tied to a variety of parameters, such as failure or anomaly thresholds, weights that link responses to detections, and delay times associated with failure response TTC issues. Different behaviors often can result from changed parameter values, and thus parameters have to be rigorously reviewed, analyzed, and tested in V&V tests.*

Pitfall: ***Integration issues.*** *Integration of FM functionality is typically more problematic than nominal functions due to its far-reaching effects on the system behavior. When planning FM tests, or demonstrations in flight system testing, provide additional schedule margin to account for integration difficulties.*

Recommended Practice: ***Develop tools to assess pass/fail criteria.*** *In situations where there are a large number of FM test cases to assess, it is useful to develop tools or other means to assess automatically pass/fail criteria for each test. This enables a more effective test program by allowing FM practitioners to prioritize test review, focusing first on the tests that did not pass the automated checks. Developing such capability has the additional benefit of requiring success criteria for the tests to be crisply defined.*

Recommended Practice: ***Automated testing.*** *Use scripting and other similar means to automate FM testing. The large number of failure scenarios makes it very difficult to cover a significant fraction of these cases through testing. However, by incorporating automated testing practices to run (and provide initial assessments of) tests, the overhead associated with each test can be reduced, allowing many more test cases to be run. As an example, the Cassini Saturn Orbit Insertion sequence had tens of system tests, but to ensure the core attitude control FM logic worked with the Saturn Orbit Insertion (SOI) sequence, over 3000 tests were run in an automated environment. The upfront investment of developing the automated testing capability saved many work years of test effort, and in fact allowed an intractable problem to be successfully solved.*

Recommended Practice: ***Perform failure scenario walk-throughs.*** *Walk-throughs of failure scenarios can be very effective in the identification of problems with processes and FM responses, before these problems are found in test.*

Recommended Practice: ***Validation independence.*** *The team performing validation testing should be independent of the team that developed the design.*

8.1.4 Analyze Fault Management V&V Results

Upon completion of the V&V activities, assessment of the V&V actions is performed. Assessment in this context includes updating of the FM V&V matrices to record the completion of the V&V actions, as well as identifying any design changes or waivers needed. Frequently, the FM V&V results are also summarized separately in specific documents (e.g., an FM verification report and an FM validation report). As with the FM V&V execution step,

additional detail on this aspect of V&V is in the NASA SE Handbook, sections 4.3.1.2 (Verification Process Activities) and 4.4.1.2 (Validation Process Activities).

Recommended Practice: ***Analysis Independence.*** *All analyses should be reviewed by a "second set of eyes," preferably by a group independent of the design team.*
Recommended Practice: ***Use Test Results to Validation Analysis Assumptions.*** *Validate assumptions in analyses by comparing to results in test reports.*

8.2 Fault Management V&V Guidance

The following sections capture guidance along specific FM V&V topic areas.

8.2.1 Fault Management Validation—Selection of Failure Scenarios

The goal of FM validation is to develop proof that the system reacts as intended to the set of possible failures. FM validation consists of a set of actions that shows the behavior of the system in off-nominal situations. To perform FM validation, the FM practitioner needs both a definition of intent, and a definition of the failure space for the system.

The specification of intent is typically defined as a set of objectives for each system activity over the mission timeframe. Each objective is described in terms of performance of a system function (in a specified timeframe), and is categorized into one of three categories, as follows: First, safety-critical; second, mission-critical; or third, noncritical. This description of intent is ideally determined and documented as part of the standard SE or S&MA process, but the FM practitioner may need to collect and document this information.

Selection of the set of failure scenarios for FM validation has historically been a subjective and qualitative activity. Unlike the determination of the set of requirements for a verification matrix, the determination of the set of failure scenarios is not straightforward. This is due to the large size of the failure space, and the multitude of ways in which it can be organized. For systems of moderate complexity, the set of failure scenarios to consider could number in the thousands. As a rough rule-of-thumb, the number of failure scenarios expected in a given system is about an order of magnitude smaller than the number of failure modes.[12]

The set of possible off-nominal scenarios (failure scenarios) is the combination of all the unique failure conditions (the set of identified failure modes in the system, reduced to the smaller number of unique failure effects (since many failure modes produce the same effects/symptoms)), multiplied by the set of different system configurations over time. This generates a large set of failure scenarios, and for the vast majority of projects, the full set is not enumerated. In addition, it is impossible to know if all possible failure modes have been identified for systems of even moderate complexity. It is extremely likely (nearly certain) that unidentified failure modes exist for such systems -- the unknown unknowns. Nevertheless, in theory there exists a set of failure scenarios based on the combination of unique failure conditions and system configuration over time. Each of these failure scenarios can be analyzed

[12] The number of failure scenarios may vary from this rule, depending on whether the mission has a small number of mission activities, or a large number of varied activities.

to determine the associated failure effects (of each specific failure mode for each configuration and point in time).

Because of the large size of this set, it would be unreasonable to develop a validation plan and facilities to assess all the identified failure scenarios (or even, depending on the size of the project, to develop such a list). However, there are some approaches to reduce the set of failure scenarios to be assessed. Of relevance is that many scenarios have significant similarities to other scenarios, and these similarities can be used to extend the results of a given validation action. An FM practitioner can identify the small differences between scenarios, determine the effects of these differences (in many cases, this is simple and straightforward); and then state that, based on completion of the validation for "scenario A," that by similarity and analysis of the differences, "nearby scenarios" (e.g., B, C, and D) can be considered validated as well.

At issue is the method by which to identify a set of "important" failure scenarios that provide sufficient evidence that the system responds correctly to off-nominal situations. This is typically described as having sufficient coverage. In most cases, identification of this set of failure scenarios is based on the engineering judgment of the FM practitioner. This results in a set of failure scenarios that cannot be assessed quantitatively, and whose quality is in great part determined by the quality and experience of the FM practitioner. Furthermore, it is difficult to assess whether the identified set of the selected failure scenarios meets the risk mitigation posture of the project.

These issues may be addressed by using a top-down approach to the selection of failure scenarios. Specifically, the set of failure scenarios to be used for validation can be identified as follows:

a. Identify the set of mission activities for the system.

b. Identify the set of objectives to be performed in each activity (both mission-related, and related to the health of assets and/or crew and operator safety).

c. Select one or more failure case(s) that threatens each objective.

Since many projects use top-down failure analyses (e.g., FTA, PRA, success-tree analysis), this information is typically readily available, especially for mission-critical activities. For example, an FTA is usually performed for mission-critical activities. The branches of the FTA contain conditions that threaten the successful completion of the activity. These conditions ought to be used to define the set of failure scenarios to be considered for that activity. A set of failure scenarios prioritized from a well-defined top-down failure analysis will provide appropriate coverage of off-nominal behavior (since the top-down analysis illustrates the failure dependencies, while the set of identified causes for the off-nominal behavior is from the bottoms-up analyses). While the unique behaviors can only be determined from the characteristics of the design, the top-down, scenario-based approach provides a basis to assess coverage against the mission goals and objectives, which is one point of validation.

8.2.2 Prioritization of Failure Scenarios

While a top-down approach provides the information to select a set of failure scenarios for validation, the set so defined has to be "mappable" to the project risk posture, and match the resources of the project. Furthermore, there are distinctions that make certain failure scenarios more valuable in the reduction of project risk. For these reasons, it is also necessary to define a set of priorities for the failure scenarios. By delineating specific criteria in the definition of these priorities, a project provides the mapping between the set of failure scenarios and the stated risk posture. The criteria that define each priority level are typically definitions of coverage across a set of items, for example, time- and event-based items, such as critical events, mission phases, and mission activities; and design-based items, such as subsystems, hardware, or FM monitors/responses. Since validation is, foremost, an action to determine whether the system meets expectations (proof that "you have what you need"), it is more important than an assessment of "what you have." It is important to have activity or objective coverage (particularly mission-critical activity coverage) at a higher priority than design coverage (e.g., coverage of mission objectives ought to be a higher priority than coverage of all FM monitors/responses). For example, the four-tier priority scheme follows:

a. Required: Unacceptable risk in not performing these actions.
b. High: Significant risk in not performing these actions.
c. Medium: Some risk in not performing these actions.
d. Low: Acceptable risk in not performing these actions.

8.2.3 Using Test Beds for Fault Management V&V

The utilization of test beds for FM V&V is both beneficial and problematic. The benefits of using a test bed instead of the flight unit are greater visibility, additional time available, and an enhanced ability to inject faults. However, when using a test bed instead of a flight article, there is a greater reliance on modeling and analysis to determine the results of a given failure scenario. Models of hardware many times do not react in flight-like ways during failure scenarios. This section contains a set of recommended practices to assist in the planning and use of test beds in FM V&V.

Recommended Practice: ***Include all subsystems in test beds.*** *FM test models should include all subsystems (often power and thermal are short-changed causing many last minute or on-orbit surprises and anomalies). If there are insufficient resources for complete power subsystem hardware, then at a minimum, a detailed, high-fidelity, fully validated power simulation should be implemented. Thermal subsystems usually have to be simulated on test beds, but are validated in thermal-vacuum (T-VAC) testing. The test scope should not be partitioned into subsystems. FM is a system function, and all subsystems need to be fully involved irrespective of the organizational structure.*

Recommended Practice: ***Test-bed sparing.*** *If there is only one hardware test bed, it should have sufficient spares in case units are reworked during the design process. Projects are recommended to have at least one dedicated hardware test bed for FM testing.*

Recommended Practice: ***Hardware-in-the-Loop (HITL) testing.*** *A project should have at least one dedicated HITL test bed for FM software development and multiple high fidelity fully*

validated software simulations dedicated for FM activities. One key contribution of HITL is the acquisition of timing data. HITL test beds typically need to include the same physical redundancy as in the flight system, as simulated hardware many times has insufficient capability to support FM testing (e.g., a test bed for a dual-string system also needs to be dual-string).

Recommended Practice: ***Software simulation V&V.*** *Software models/simulations should be fully characterized against the hardware test beds and flight vehicle. Differences need to be fully documented and factored into the FM V&V test program. As new differences are understood, they should be updated throughout the test program.*

Recommended Practice: ***Database test procedures.*** *If running large numbers of tests, especially if automated, consider making the test procedures and the actual test run files the same to avoid duplicate resources and cumbersome test procedure maintenance.*

9. OPERATIONS AND MAINTENANCE

[This section will be expanded in later releases. The plan is to include the following topics.]

1.0 Introduction
2.0 Phase A
- 2.1 System Operation Guidelines
- 2.2 Develop FM operations approach

3.0 Phase B
- 3.1 FM Concept of Operations
- 3.2 Revise FM Operations Approach
- 3.3 Develop Operations Requirements

4.0 Phase C
- 4.1 Refine Operations Requirements
- 4.2 Detailed Operations Design
- 4.3 Response to Allocated FM functionality (result of flight/ground split)

5.0 Phase D
- 5.1 Operations V&V
- 5.2 Definition of Operating Constraints (e.g., flight rules)
- 5.3 Operator/Operations Team Certification
- 5.4 Contingency Planning

6.0 Phase E
- 6.1 Vehicle Operation
- 6.2 Anomaly Resolution
- 6.3 Updating System Behavior
- 6.4 Critical Events
- 6.5 Lessons Learned

10. REVIEW AND EVALUATION

To adequately review and evaluate FM functions within a system, three levels of reviews are recommended. FM is expected to be a topic in major program/project lifecycle reviews (i.e., MCR, MDR, SRR, PDR, CDR, SIR, and CERR, in accordance with NASA NPR 7123.1A, NASA Systems Engineering Processes and Requirements; and NPR 7120.8, NASA Research and Technology Program and Project Management Requirements) and system- and subsystem-level technical reviews (for those systems/subsystems that have been allocated FM functions). In addition, there should be dedicated FM technical reviews throughout the lifecycle to ensure an acceptable approach, plan, and FM design has been selected, FM meets the specified requirements, FM is ready for integration and test, and FM is ready for critical events.

Lesson Learned: ***(NASA Lessons Learned #1743) Mars Exploration Rover (MER).*** *The Mars Polar Lander (MPL) 1999 mission failure encouraged the MER project management to impose a healthy skepticism towards success. The MER project continuously demanded proof that the system would work, rather than assuming that risks were acceptable unless shown to the contrary.*

Dedicated FM technical reviews serve a number of purposes:

a. **Mind-Set:** In FM reviews, the participants, review board, and agenda are dedicated to asking "What if?" and "What is the required performance in the presence of a failure?" In non-FM focused reviews, there is little time for more than an occasional failure scenario walk-through as failure scenarios are a "tax" on a traditional nominal content-focused review schedule.

b. **Content:** FM review agendas have many specialized FM-centric topics covering the entire scope of a project's off-nominal behavior. It is a systems agenda, but key subsystems, such as flight software, GN&C, and power, are covered so that the interaction between the subsystem FM and systems FM can be fully appreciated and potential crosscutting issues can be realized. It is a unique opportunity and necessary step to formulating an integrated FM picture of the project.

c. **Logistics:** Having all FM issues presented in one place allows a review board consisting of FM experts in the NASA community to be assembled and to attend a focused, concise (1–2 day) review. Logistically, it can be difficult to assemble a 5–10 member review board of FM experts to attend a long (1–2 week) program/project review plus additional key system- and subsystem-level reviews. This issue also applies to the FM personnel on the project. Often, the FM personnel are too busy to be able to attend weeks of reviews, so they will not be able to participate in the FM-related discussions when they occur. Issues can be written down, but that is a poor substitute for a vigorous back and forth discussion between subject matter experts.

d. **Completeness:** A review of FM in piece parts makes it hard for anyone not in attendance at all presentations to integrate all the discussions and to identify gaps in the content. With no dedicated forum to walk through omissions and scenarios, it is almost certitude that items will be missed.

e. **Follow-Through:** FM reviews have action items. The follow-through, closure, and approval of those actions are well-established metrics for review confidence and success, and a key avenue for FM content to be modified as required for mission success.

f. **NASA Lessons Learned:** In the past, unmanned missions sometimes would hold informal FM reviews or critical event reviews. After years of experience and reflection on factors that led to failures and factors that supported the successes, the FM review process evolved. In recent projects, the FM review was the key forum where difficult system issues were discussed by FM experts, lead system engineers, and institutional chief engineers. Outcomes from such reviews were instrumental in identifying and correcting key disconnects as early in the design process as possible. The relatively high rate of success of recent missions has shown this process yields products that are more robust; and conversely, experience has shown that there will be gaps and holes without this FM-centric process.

Lesson Learned: ***(NASA Lessons Learned #1612) Assessing the human capital and facilities required for new Moon/Mars missions.*** *Bad habits (those contributing to failures) are not "un-learned" if personnel are not involved in thorough postmortem reviews of failed projects. The successes and failures of more recent missions, such as the X–vehicle programs and planetary exploration missions (such as MER), should be reviewed. In particular, understanding the successes should be a priority.*

The NASA SE Handbook provides general guidance on project-level lifecycle reviews, and it should be consulted for general entrance and success criteria for technical reviews. The purpose of this section is to provide a minimum set of recommended FM technical reviews for a successful low-risk program.

Table 20, Summary of Recommended Major Milestone Reviews, outlines the minimum list of recommended reviews for FM and provides a brief description of the review and the duration and timeframe for the review. For class C or class D missions, where the project team is relatively small, combining these dedicated FM reviews with associated project- or system-level reviews could be considered. However, all the FM-specific entrance criteria and success criteria listed for the various reviews should still be covered and careful consideration should be given prior to the removal, combining, or tailoring of FM reviews for a specific project.

Sections 10.1–7 detail the reviews listed in table 20 by providing the following for each review:

- Description: Short summary of the review.
- Entrance Criteria: Accomplishments and documentation that has to be complete prior to holding a successful review.
- Success Criteria: Criteria that will determine the success or failure of the review.

Note that additional reviews focused more on "quality control" than on the FM process, may also be useful based on project scope and specifics. These further reviews include the following:

- Fault analysis result reviews (e.g., PRA, FTA).

- FM phase/mode reviews (e.g., safe mode review, time-critical sequence reviews.).
- FM implementation peer reviews (e.g., FM flight software walk-through).
- Subsystem-specific reviews (e.g., GN&C FM reviews, power FM reviews).
- FM test procedure reviews.
- Other mission-specific FM reviews.

Table 20—Summary of Recommended Major Milestone Reviews

Review	Description	Duration [13]	Timeframe
FM Concept Review (FMCR)	The FMCR examines the FM boundary, or scope, to ensure that the size and complexity of FM matches the available resources and risk posture for the mission. The FMCR also examines the FM ConOps, the safing strategy, and the critical events list.	0.5–1 day	Prior to project MCR
FM Architecture/ Requirements Review (FMARR)	The FMARR examines both the architecture and mission- and system-level FM requirements to ensure that the architecture and requirements are in-line with each other and that the coverage provided by the requirements is sufficient and will satisfy mission requirements.	1–2 days	Prior to project SRR/MDR
FM Preliminary Design Review (FMPDR)	The FMPDR demonstrates that the preliminary design meets program requirements for FM with acceptable risk and within the constraints allocated. The FMPDR also demonstrates that the failure modes and effects of the preliminary system have been adequately analyzed and that an agreement has been reached between the FM team and the project on the set of FM policy and single fault tolerance exemptions. In addition, it ensures that all of the subsystem hardware/software is in place to support the FM requirements and architecture and is sufficient to support FM during critical events.	1–2 days	Prior to project PDR
FM Critical Design Review (FMCDR)	The FMCDR demonstrates that the maturity of the design is such that the implementation of FM mechanisms is ready to proceed. The FMCDR determines that the V&V plan, FM system-level test plan, and operability of the FM system are consistent with project constraints and overall risk level.	1–2 days	Prior to project CDR

[13] Duration of review varies based on NASA mission class and amount of FM coverage at project, system, and subsystem technical reviews.

Review	Description	Duration [13]	Timeframe
FM Test Readiness Review (FMTRR)	The FMTRR ensures that the FM system-level test plan is consistent with the program schedule and that all FM test procedures are ready for testing. The FMTRR also provides an opportunity to confirm that subsystem testing, results, and issues up to this point do not affect the FM system-level design.	0.5–1 day	Prior to project SIR/TRR
FM Launch Readiness Review (FMLRR)	The FMLRR assesses the adequacy of FM V&V performed to date, in order to determine if the system has sufficient FM maturity to launch.	0.5–1 day	Prior to launch
FM Critical Event Readiness Reviews (FMCERR)	The FMCERR reviews are held, as necessary, to verify the readiness of FM to support specific mission-critical event operations. These reviews focus on the mission-critical event operational timeline, the predicted behavior of the various platform subsystems, the predicted responses of FM during the event, and any operational constraints imposed by the FM functions.	0.5–1 day	Prior to critical events

10.1 Fault Management Concept Review

The FMCR examines the proposed FM concept including the definition of the FM boundary or scope, and ensures that the size and complexity of FM matches the available resources and risk posture for the mission. The design principles (e.g., unique mission design characteristics, critical events, redundancy philosophy, safing strategy) which describe how FM will be applied specifically to the given mission should be reviewed as well as the concept of FM operations (i.e., the FM ConOps), applicable technologies (along with the associated TRL estimates), and overall work plan, schedule and resources for FM. It is important that this review be held during phase A, prior to MDR.

Since concepts affect the way systems are architected/designed, built, and operated, it is of crucial importance to establish, define, and communicate this concept early during mission formulation. This review is primarily motivated by recognizing and appreciating that having a system concept that supports both nominal functionality and off-nominal (FM) functionality is important to practical aspects of defining the overall system design. Knowledge of the FM functions within the system, commonly shared among the overall team, will support a greater understanding of how those functions will interact with the host space platform system so that overall complexity can be minimized and undesired interactions can be avoided.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews and these general guidelines should be applied to FM-specific reviews. All concept reviews should confirm that the preliminary set of requirements satisfactorily provides a system

that will meet the mission objectives, with a technical plan that is sufficient to proceed to the next phase, and with cost and schedule estimates that are credible.

Pitfall: ***Use of legacy code in FM design.*** *Flight software source code is sometimes grandfathered in for use in a new program. This can be good and bad. The good part is there is a lot of testing completed and many bugs have been worked out. The bad part is that if there are undiscovered bugs, they are carried through to the next program. Also, there is a significant risk of new bugs related to interface, compiler or system differences, especially since heritage code rarely gets a detailed review and the experts that know the code the best are often not available to participate, or too much time has passed to recall logic subtleties well.*

Recommended Practice: ***Hold detailed FM code and logic reviews.*** *Cross-checking the FM code and logic against the FM description for completeness and correctness can alleviate issues, such as undiscovered bugs and bugs related to interfaces.*

Table 21, FMCR Entrance and Success Criteria, provides FM-specific entrance and success criteria for the FMCR. Table 28, FM Milestone Review Questions, provides relevant questions for reviews.

Table 21—FMCR Entrance and Success Criteria

FMCR Entrance Criteria	FMCR Success Criteria
FM Concept Document	FM Concept Document is complete and covers the content described in section 4.1.1. • The FM boundary/scope and role for FM is consistent with the program/project risk posture and NASA mission-risk classification and has been agreed to by the project. • The overall FM concept and description of how FM will apply specifically to the given mission to minimize risk of failures is reasonable/feasible given the project schedule and resources. • The redundancy and/or fault tolerance policy is consistent with the risk posture and NASA mission-risk classification. • The safing strategy and FM ConOps is consistent with the mission ConOps. • Critical events have been identified and ConOps exist for these events. • Preliminary analysis of FM timeliness is complete and is sufficient to understand FM flight-ground split and level of onboard FM. • Level of human/operator involvement in FM is defined. • Amount of interaction between nominal and recovery operations is defined.
FM Development and Analysis Plan	FM Development and Analysis Plan is complete and covers the content described in table 10. • FM Development and Analysis Plan is consistent with the program cost and schedule, is sufficient to determine faults given program risk posture and NASA mission-risk classification. • Detailed description of the fault analyses as planned, and how these analyses connect to FM requirements.
FM Technology Plan/Assessment	FM Technology Plan/Assessment is complete and covers the content described in section 4.1.1. • The use of technology agrees with overall program position, plan to achieve TRL 6 by PDR is feasible, and fallback options identified if technology does not reach TRL 6 by PDR.
Use of heritage hardware and	• Planned use of FM heritage is reasonable and

FMCR Entrance Criteria	FMCR Success Criteria
software in FM mechanisms	adequately matched to the mission characteristics and planned architecture. • Trade studies performed in order to justify approach and include comparison of heritage mission complexity and risk posture, operations environment, hardware complement, and software systems. • Assessment of areas of risk and approach to mitigation, including applicable FM lessons learned from heritage missions.

10.2 Fault Management Architecture Requirements Review

The FMARR examines both the architecture and mission- and system-level FM requirements to ensure that the architecture and requirements are in-line with each other and that the coverage provided by the requirements is sufficient to satisfy mission requirements. Reviewing the system architecture in terms of both its nominal and off-nominal (FM) functionality is important, so that complexity can be minimized and undesired interactions can be avoided. Critical information that should be reviewed includes, but is not limited to, the list of time-critical and/or mission-critical events that are design drivers for the FM functions within the system, lists of both hardware and software (both in flight and ground systems) that are envisioned to be needed by FM for diagnostics, expected ground response time to failures, and degree of ground interaction allowed/desired in failure responses. This review should be held during mid-to-late Phase B, prior to PDR. Note that larger programs may wish to have separate requirements and architecture reviews.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews. These general guidelines should be applied to FM-specific reviews, as follows:

a. All architecture and requirements reviews should confirm that there is a sound process for the allocation of requirements at all levels.

b. Requirements definition is complete with respect to top-level requirements and interfaces between external entities and major internal elements.

c. Requirements allocation and flow-down of key driving requirements have been defined down to subsystems.

d. Preliminary approach for how requirements will be verified and validated has been determined.

e. The architecture is reasonable, feasible, complete, and responsive to the mission requirements.

f. The system and subsystem design approaches and ConOps exist and are consistent with the requirements set.

Table 22, FMARR Entrance and Success Criteria, provides the FM-specific entrance and success criteria for the FMARR; table 28 provides relevant questions for reviews.

Lesson Learned: ***(NASA Lessons Learned #1385) CONTOUR Mishap Investigation, reliance of CONTOUR project on analysis by similarity.*** *Projects should conduct inheritance reviews (i.e., analyses by similarity) early in the project lifecycle and should assure that the analysis properly evaluates the inherited item's capabilities and prior use against all mission-critical requirements. The board felt that inadequate oversight was especially dangerous in combination with nonstandard engineering practices.*

Table 22—FMARR Entrance and Success Criteria

FMARR Entrance Criteria	FMARR Success Criteria
FM Requirements Document	FM Requirements Document is complete and covers the content described in section 4.1.2. • FM system-level requirements represent a complete flow down from project-level requirements and FM system-level requirements have been allocated down to subsystems. • System-level FM requirements demonstrate adequate coverage for faults determined by fault/scenario analysis and the project to be protected against by FM. • System-level FM requirements demonstrate a reduction of FM cases from the complete fault list determined by fault analysis (i.e., majority of requirements should be a one-to-many relationship with faults) and a safety net structure that guards against failures regardless of how they manifest (i.e., no explicit symptom-fault relationship).
Preliminary FM V&V Plan	Preliminary FM V&V Plan is complete and covers the content described in section 4.1.5. • Preliminary approaches for how FM requirements will be verified and validated have been determined (both for system-level scenarios and subsystem-level requirements); ownership of FM V&V activities identified and agreed to by system-level and subsystems.
FM Architecture Document	FM Architecture Document is complete and covers the content described in section 4.1.3. • The FM architecture is reasonable, feasible, consistent with the FM requirements, and testable, given the project schedule and resources. • The FM architecture clearly shows how failure conditions are identified and what recovery actions are taken. • Summary of analyses performed to ensure multiple requirements do not interfere/interact with one another or otherwise negatively affect the rest of the system.

10.3 Fault Management Preliminary Design Review

The FMPDR demonstrates that the FM preliminary design meets program requirements for FM with acceptable risk and is within the technical constraints and programmatic resources allocated. The FMPDR also demonstrates that the system has been adequately analyzed for potential faults and that an agreement has been reached between the FM team and project management on a clear and well defined set of faults that has to be managed. This design review should be held prior to the mission-level PDR. Some programs may wish to hold a pre-PDR peer review prior to the FMPDR; this may include limited review of fault analysis if separate reviews are not held.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews and these general guidelines should be applied to FM-specific reviews. All PDRs should confirm the following:

- That the top-level requirements are agreed upon, finalized, and consistent with the preliminary design.
- The flow-down of verifiable requirements is complete.
- The preliminary design is expected to meet the requirements at an acceptable level of risk.
- Adequate technical interfaces are consistent with the overall technical maturity and provide an acceptable level of risk.

Table 23, FMPDR Entrance and success Criteria, provides the FM-specific entrance and success criteria for the FMPDR; table 28 provides relevant questions for reviews.

Table 23—FMPDR Entrance and Success Criteria

FMPDR Entrance Criteria	FMPDR Success Criteria
Preliminary Fault/Scenario Analyses	• Summary of preliminary results from fault analyses identifying the faults/failures to be protected against and possible response interactions or responses that may negatively impact another part of the system; examining combinatorial effects of multiple failures and functional or physical dependencies and timing; exploring the sequential nature of system dependencies and timing. • Trade studies performed that demonstrate that the design selected and allocation of the design to subsystems is reasonable given program requirements and constraints. • Program accepted Design for Minimum Risk List/Single Point Failure Exemptions List or Fault Tolerance List.
Preliminary FM Design Specification/Document	Preliminary FM Design Specification/Document is complete and covers the content described in section 4.1.3. • Preliminary allocation of FM responsibilities to subsystems, software, operations constraint/procedure, or direct human crew/operator intervention is defined. • Safing design demonstrates how all systems/subsystems coordinate to produce “safe” end results; mode and mode transitions are defined. • Redundancy design and ConOps for usage of redundancy is defined. • Time-critical nominal and off-nominal sequence design demonstrating required success criteria, vulnerabilities, and fault recovery options defined. • Any required new technology has been developed to an adequate state of readiness (TRL 6).
FM V&V Plan, FM Verification Matrix, FM Validation Matrix	Refined FM V&V Plan, covering the content described in section 4.1.5. • Preliminary FM Validation Matrix developed using top-down techniques to define the off-nominal scenarios used to validate the system. • Preliminary FM Verification Matrix filled in with verification method, verifier assignment, verification objectives, and verification facility. • Preliminary analysis of test resource fidelity and

FMPDR Entrance Criteria	FMPDR Success Criteria
	time required demonstrate adequate test resources. • Preliminary FM incompressible test list identified.

10.4 Fault Management Critical Design Review

The FMCDR demonstrates that the maturity of the design is appropriate and consistent across all subsystems such that implementation of FM in multiple subsystems can proceed. FMCDR determines that the verification plan, FM system-level test plan, and operability (i.e., the ConOps) of the FM functions within the system are consistent with project constraints and overall program risk level. This design review should be held prior to the mission-level CDR. Some programs may wish to hold a pre-CDR peer review prior to the FMCDR.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews and these general guidelines should be applied to FM-specific reviews. All critical design reviews should confirm that the detailed design meets the requirements with adequate margins and at an acceptable level of risk, interface control documents are appropriately matured to proceed with fabrication, assembly, integration and test, the V&V requirements and plans are complete, and the testing approach is comprehensive.

Table 24, FMCDR Entrance and Success Criteria, provides entrance and success criteria for the FMCDR; table 28 provides relevant questions for reviews.

Table 24—FMCDR Entrance and Success Criteria

FMCDR Entrance Criteria	FMCDR Success Criteria
Final Fault/Scenario Analyses	• Summary of updated results from fault analyses and how these analyses tie into the FM design in terms of identifying the faults/failures to be protected against and possible response interactions or responses that may negatively impact another part of the system; examining combinatorial effects of multiple failures and functional or physical dependencies and timing; exploring the sequential nature of system dependencies and timing. • Summary of updated trade studies performed demonstrating that the design selected and allocation of the design to subsystems is reasonable given program requirements and constraints. • Program accepted Design for Minimum Risk List/ Single Point Failure Exemptions List or Fault Tolerance List.
Final FM Design Specification/Document	FM Design Specification/Document is complete and covers the content described in section 4.1.3. • Detailed safing definition demonstrates how all systems/subsystems coordinate to produce “safe” end results; mode and mode transitions are well defined. • Detailed FM design diagrams demonstrate both nominal and off-nominal responses and ConOps (including all subsystems and operations/crew) for time-critical events with defined success criteria and vulnerabilities. • Allocation of FM responsibilities to subsystems, software, operations constraint/procedure, or direct human crew/operator intervention is complete with adequate documentation to ensure interfaces and collaboration is well understood. • Detailed FM design is operable such that the operations teams understand the role in FM, the operations role is feasible given project resources, and operations can operate and recover during all planned nominal and predicted off-nominal situations.
FM V&V Plan, FM Verification Matrix, FM Validation Matrix	Completed FM V&V Plan, covering the content described in section 4.1.5. • Refined FM Validation Matrix developed using top-down techniques to define the off-nominal scenarios used to validate the system with plan for the validation of models, test beds, and any other test resources used

FMCDR Entrance Criteria	FMCDR Success Criteria
	to verify or validate FM requirements. • Refined FM Verification Matrix filled in with verification method, verifier assignment, verification objectives, and verification facility; completed burn-down plan for FM requirement verification at all levels. • Refined analysis of test resource fidelity and time required shows adequate fidelity and time for testing of FM requirements. • Refined FM incompressible test list

10.5 Fault Management Test Readiness Review

The FMTRR ensures that the FM system-level test plan is consistent with the program schedule and that all test procedures are ready for use in the test environment. The FMTRR also provides an opportunity to confirm that subsystem testing, results, and issues up to this point do not affect the FM system-level design. This review should be held prior to end of phase C.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews and these general guidelines should be applied to FM-specific reviews. All test readiness reviews should confirm that test plans are complete and approved, that identification and coordination of required test resources are complete, and that previous component, subsystem, and system test results form a satisfactory basis for proceeding into planned tests.

Table 25, FMTRR Entrance and Success Criteria, provides entrance and success criteria for the FMTRR; table 28 provides relevant questions for reviews.

Table 25—FMTRR Entrance and Success Criteria

FMTRR Entrance Criteria	FMTRR Success Criteria
FM, V&V Plan, FM Verification Matrix, FM Validation Matrix	• Component and subsystem-level FM verification activities are complete per FM Verification Matrix. • All known discrepancies/inconsistencies between subsystem implementation and testing and system-level FM design have been identified and have been either dispositioned or have an adequate plan to be disposed. • All issues generated from previous component and subsystem test results can be shown to have no adverse effect on meeting system-level FM requirements and executing the system-level FM design. • Verification of contingency procedures is proceeding according to requirement verification burn-down plan. • FM Validation Matrix is complete and incompressible test list finalized.
FM Test Procedures	• Objectives of testing have been clearly defined, documented, and reviewed, providing a reasonable expectation that the test objectives will be met. • FM Test Procedures in progress based on need dates.

10.6 Fault Management Launch Readiness Review

The FMLRR verifies the completeness of all testing, analysis, demonstrations, and contingency procedures ensuring that the FM functions within the system have sufficient maturity to launch. This review should be held prior to launch.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews, and these general guidelines should be applied to FM-specific reviews. All launch readiness reviews should confirm the following:

a. The system is ready for flight.
b. The flight and ground software elements are ready to support flight and flight operations.
c. The interfaces are checked out and functional.
d. Any open items and waivers have been examined and found to be acceptable.

Table 26, FMLRR Entrance and Success Criteria, provides entrance and success criteria for the FMLRR; table 28 provides relevant questions for reviews.

Table 26—FMLRR Entrance and Success Criteria

FMLRR Entrance Criteria	FMLRR Success Criteria
FM Verification Matrix, FM Validation Matrix	All activities documented in the FM Verification Matrix and the FM Validation Matrix are complete. • All known discrepancies/inconsistencies between system-level testing and system-level FM design have been disposed of or have an adequate plan to be disposed. • Required tests and analyses are complete and indicate that the system will perform properly in the expected operational environment. • All issues generated from system-level test results can be shown to have no adverse effect on meeting system-level FM requirements and executing the system-level FM design. • Refinement of FM analysis demonstrates that any new problems revealed during system test do not result in system failing to meet overall mission reliability requirements.
FM Test Procedures	• Any issues found during system-level tests have been analyzed to root-causes; then, either fixed and the original test successfully repeated, or risk has been accepted by the program. • Plan for future regression testing is reasonable given project schedule and remaining items that will be reconfigured or changed prior to launch.
FM Operations Plan	FM Operations Plan is complete and covers the content described in section 4.1.6.
Contingency Procedures	• All contingency procedures have been properly documented and signed off. • Contingency procedure test program has been successfully completed.

10.7 Fault Management Critical Event Readiness Review

The FMCERR reviews are held as necessary to verify the readiness of FM to support specific mission-critical event operations. Such mission-critical events would include, but not be limited to, orbital insertion propulsive maneuvers, rendezvous and docking operations, EDL operations, and flyby maneuvers. These reviews focus on the mission-critical event operational timeline, the predicted behavior of the various platform subsystems, and the predicted responses of FM during the event. Any operational constraints imposed by the FM functions within the system should be identified. All changes to the FM nominal configuration (e.g., a change to a fault detection threshold level) will be defined and supported with analytical, simulation, and test results. All

changes to the event timeline to accommodate FM configuration changes (both pre-event and post-event) will also be identified and incorporated into the final operational timeline.

The NASA SE Handbook provides general entrance and success criteria for program technical reviews and these general guidelines should be applied to FM-specific reviews. All critical event readiness reviews should confirm that the critical event design complies with the requirements and that the preparation for the critical event, including V&V, is thorough.

Table 27, FMCERR Entrance and Success Criteria, provides entrance and success criteria for the FMCERR; table 28 provides relevant questions for reviews.

Table 27—FMCERR Entrance and Success Criteria

FMCERR Entrance Criteria	FMCERR Success Criteria
FM Strategy	• Analytical, simulation and test results are complete and indicate that the FM system will perform properly during the mission-critical event. • Summary of FM changes necessary for conducting the critical event along with supporting analysis and simulation and test results. • A summary and an analysis of all applicable FM lessons learned from conducting similar mission-critical events. • Predicted behavior of the platform subsystems during the mission-critical event. • Nominal FM system flight configuration prior to critical event. • Pre-event FM reconfiguration plans, procedures, and timelines. • Post-event FM reconfiguration plans, procedures, and timelines. • FM contingency plans and procedures for potential use during the mission-critical event.
Contingency Procedures	• FM contingency plans and procedures for potential use during the mission-critical event. • All contingency procedures have been properly documented and signed off. • Contingency procedure test program has been successfully completed.

10.8 Relevant Questions for Fault Management Reviews

A set of relevant questions for FM milestone reviews is listed in table 28, FM Milestone Review Questions. These questions have a dual purpose. First, these questions identify specific detailed

areas for reviewers to probe. Second, the questions serve to provide another means to expose and highlight the underlying nature and the detailed aspects of the specific FM functions within the system being reviewed.

Table 28—FM Milestone Review Questions

#	FM Question	Applicable FM Review(s)
1	Are there any requirements with ambiguous wording?	FMARR
2	Should any requirement statements be split up?	FMARR
3	How will it be demonstrated that each requirement is met? Alternatively, can each requirement be verified that it is met?	FMARR
4	Are there any missing requirements?	FMARR
5	Have catastrophic failures that involved similar FM technologies been reviewed and understood?	FMARR, FMPDR, FMCDR
6	What is the plan to validate all models and tools used in the FM full lifecycle?	FMARR, FMPDR
7	Are the FM models and tools completely validated? How do you know?	FMCDR, FMTRR
8	Is reuse of FM models planned? If so, how will the reused models be validated?	FMARR, FMPDR
9	What are the plans to place the FM models and tools under configuration control?	FMARR, FMPDR
10	Have all critical FM models, tools, and analyses been placed under configuration control?	FMCDR, FMTRR
11	Do previous requirements and analyses from similar projects still apply?	FMARR, FMPDR, FMCDR
12	Is the heritage design well understood? Are the shortcomings and issues of heritage FM designs been fully understood before committing to use them, or are upgrades required? Are there any heritage elements where changes in application or environment will invalidate the expected performance? Was any qualification/acceptance testing requirements waived due to the application of heritage elements?	FMARR, FMPDR, FMCDR, FMTRR
13	Is there any analysis that cannot be verified because of contractor proprietary data or classified information?	FMPDR, FMCDR
14	Have all of the assumptions in the analyses been documented?	FMPDR, FMCDR
15	Can excessive thermal, structural, mechanical, or electrical loads occur for the component? What margins (above design environments) were applied in the design and analysis of the hardware? Are the margins adequate?	FMARR, FMPDR, FMCDR
16	Are contingency plans for on-orbit anomalies adequate?	FMLRR, FMCER

#	FM Question	Applicable FM Review(s)
17	Can a problem in a primary unit cause the same failure in its backup?	FMARR, FMPDR, FMCDR
18	Can a device damage its neighbors?	FMARR, FMPDR, FMCDR
19	Does the FM design allow in-flight upgrades and/or in-flight repair by crew?	FMARR
20	Is telemetry sufficient for all critical events? Is telemetry sufficient to distinguish among all known fault modes?	FMARR, FMPDR, FMCDR, FMCER
21	Are multiple safeguards available during early operation?	FMARR
22	Has FM been shown to be adequate?	FMLRR
23	Do the tests independently confirm development results?	FMLRR, FMCER
24	Have predictions been analytically established before testing?	FMCDR, FMTRR
25	Can a simple test be used to crosscheck an elaborate test?	FMTRR
26	Has all test data been reviewed for trends, oddities, “out-of-family” values, and other indicators of anomalies?	FMLRR
27	Are all test anomalies fully understood?	FMLRR
28	Have the test articles been fully inspected before and after testing?	FMLRR
29	Do the tests cover all operating modes?	FMLRR
30	Does the acceptance test plan screen for anticipated failure modes?	FMPDR, FMCDR
31	Is the test equipment compatible with the test conditions?	FMTRR
32	Does the system being tested represent the flight configuration? (Test as you fly.)	FMTRR
33	Does the test inject sufficient off-nominal conditions to ensure the equipment is robust?	FMTRR
34	What processes and standards are used in the design, analysis, and testing program?	FMARR, FMPDR, FMCDR, FMTRR, FMLRR
35	Have all the functional, performance, and interface relationships that exist between the various spacecraft's subsystems been rigorously searched out, recognized, identified, described, defined, and documented?	FMARR, FMPDR, FMCDR, FMTRR
36	Were all flight environments fully accounted for in the design?	FMPDR, FMCDR
37	What process was employed to validate/verify the flight simulations? What dispersions were considered?	FMPDR, FMCDR

#	FM Question	Applicable FM Review(s)
38	What testing and analyses were employed to define the flight environments? What is the pedigree of these tests and analyses?	FMPDR, FMCDR
39	Does the FM system design provide sufficient coverage for typical hardware anomalies (e.g., malfunctioning valves, shorted connecter pins, malfunctioning pyros, battery under-/over-charging, computer upset, etc.)? What device-level protections exist?	FMARR, FMPDR, FMCDR
40	Are launch integration and all ground crew operations thoroughly planned?	FMCDR, FMLLR
41	Is the selection and location of the FM sensors/instrumentation, as well as the associated display and alarms, sufficient to correctly and timely detect critical failures/events?	FMARR, FMPDR, FMCDR
42	Have redundancy switching analyses been performed to ensure a fail-safe transfer between multiple, or redundant, controllers? Have these analyses determined the effects on the redundancy switching process by considering all credible failure paths, such as part/component failures, start-up transients, latch-ups, overvoltage conditions, and electro-magnetic interference effects? What provisions are there in the FM system design to preclude glitches in one unit will not propagate across interfaces?	FMPDR, FMCDR
43	Can the onboard computer be safely reset? Can executable software be uploaded even if the computer locks up? Does the FM system architecture include a backdoor receiver with a default mode to overcome a computer lockup?	FMARR, FMPDR, FMCDR
44	Do the FM system tests accurately simulate time-dependent, especially start-up, behavior?	FMTRR
45	Is the power supplied to the FM system test bed monitored and recorded for abnormal transient voltage and current in the event of anomalies or failures?	FMTRR
46	Can unexpected time-dependent circuit behavior be accommodated by the FM system design?	FMARR, FMPDR, FMCDR
47	Is there a requirement for the FM system to accommodate the case where serial safety devices (e.g., thruster inhibits) fail simultaneously?	FMARR

#	FM Question	Applicable FM Review(s)
48	Will unexpected inputs cause the software to freeze or loop endlessly? Does the flight software ignore spurious inputs through filtering or limit checking? Does the flight software deliberately ignore faults if there is no possible recovery? Is the flight software precluded from resetting in response to input errors and to send error messages in telemetry instead?	FMARR, FMPDR, FMCDR
49	What happens if the software stops executing (hangs)?	FMPDR, FMCDR
50	Can the computer experience a fault during boot up?	FMPDR, FMCDR
51	Will it be possible to diagnose computer problems remotely?	FMARR, FMPDR, FMCDR
52	Is all critical FM software under configuration control?	FMCDR, FMTRR
53	How are FM software database parameters verified and placed under configuration control?	FMCDR, FMTRR
54	Are FM command scripts, both for ground test and in-space operations, formally controlled?	FMTRR, FMLRR, FMCER
55	Will testing exercise all logic branches? How will you know?	FMTRR
56	How are reused or modified FM software codes verified?	FMPDR, FMCDR
57	What is the plan to test FM flight software with high-fidelity hardware in the loop, in the flight configuration?	FMCDR, FMTRR
58	Has an analysis been performed to determine if a signal arriving earlier or later than expected can trigger unintended FM responses?	FMPDR, FMCDR, FMTRR
59	Will recovery from a computer crash return the system to the last known good state?	FMARR, FMPDR, FMCDR
60	What is the plan for independent verification of the fault protection logic?	FMARR, FMPDR, FMCDR
61	Does the FM design consider all operational possibilities?	FMARR
62	How will the autonomous FM system and the ground system both be provided with correct and timely information? How will synchronization of state information between flight and ground be maintained?	FMARR
63	Is the autonomous FM independent of all hardware and software that might be involved in either causing/diagnosing a fault so that the system itself can survive major anomalies?	FMARR

#	FM Question	Applicable FM Review(s)
64	Has a comprehensive and iterative architectural development process been conducted early in the system lifecycle that includes considerations, such as all potential hardware/software faults and degradations, safe hold/safe haven modes, and "design for test"?	FMARR
65	Have the GN&C analyses of all the spacecraft dynamics (e.g., aerodynamics, flexibility, damping, gyro dynamics, plume impingement, moving mechanical assemblies, fluid motion, and changes in mass properties) been factored in the FM design and parameters (especially fault monitors)?	FMPDR, FMCDR
66	Will the truth model used in the spacecraft's GN&C high-fidelity FM verification simulations be developed independently from the simulation models developed/used by the GN&C design team?	FMARR, FMPDR, FMCDR
67	Will sufficient FM HITL testing be performed to ensure proper and expected flight hardware-to-flight software interactions in all operational modes, during mode transitions, and during all mission-critical events?	FMARR, FMPDR, FMCDR, FMTRR
68	What basis or criterion has been relied upon to determine if the top-level FM system architecture is complete?	FMARR
69	What functionality is the FM system architecture intended to protect?	FMARR
70	What was the rationale for selecting either centralized or distributed FM system architecture?	FMARR
71	What was the philosophy for allocating between centralized FM functions and distributed FM functions?	FMARR, FMPDR, FMCDR
72	If there is a distributed FM architecture, how will interactional problems be addressed?	FMARR, FMPDR, FMCDR
73	Will the FM mechanisms operate fast enough to be effective at mitigating failures?	FMARR, FMPDR, FMCDR

APPENDIX A: REFERENCES

A.1 Purpose

The purpose of this appendix is to provide guidance and is made available in the reference documents listed below.

A.2 Reference Documents

A.2.1 Government Documents

Department of Defense

MIL-STD-1629A. (1980). Procedures for Performing a Failure Mode Effects and Criticality Analysis. Washington, DC.

NASA

Constellation Fault Management Assessment and Advisory Team (FMAAT).

——. *Position Paper #1.* (2009). Recommended Entry and Success Criteria for Fault Management Major Milestone Reviews. Washington, DC: NASA Exploration Systems Mission Directorate.

——. *Position Paper #2.* (2009). Recommended Fault Management Terminology. Washington, DC: NASA Exploration Systems Mission Directorate.

——. *Position Paper #3.* (2009). Recommended Fault Management Development Process. Washington, DC: NASA Exploration Systems Mission Directorate.

——. *Position Paper #5.* (2009). Recommended Fault Management Organization and Interfaces. Washington, DC: NASA Exploration Systems Mission Directorate.

——. *Position Paper #6.* (2009). Recommendations for Fault Management Verification and Validation. Washington, DC: NASA Exploration Systems Mission Directorate.

——. *Position Paper #7.* (2009). Example Fault Management Requirements. Washington, DC: NASA Exploration Systems Mission Directorate.

NASA Lessons Learned Database: http://llis.nasa.gov/offices/oce/llis/home/

——. (1995). Preferred Reliability Practices, Fault Protection, Practice No. PD-ED-1243. Washington, DC.

——. (1995). Preferred Reliability Practices, Fault Tolerant Design, Practice No. PD-ED-1246. Washington, DC.

——. (1999). Preferred Reliability Practices, Quantitative Reliability Requirements Used As Performance-Based Requirements For Space Systems, Practice No. PD-ED-1273. Washington, DC.

NASA/SP-2010-576 Ver. 1.1. (2010). NASA Risk-Informed Decision Making Handbook. Washington, DC.

NASA-GB-8719.13. (1995). NASA Software Safety Guidebook. Washington, DC.

NPR 7120.5D. (2007). NASA Space Flight Program and Project Management Requirements. Washington, DC.

NPR 7150.2A. (2009). NASA Software Engineering Requirements. Washington, DC.

NPR 8000.4A. (2008). Risk Management Procedural Requirements. Washington, DC.

NPR 8725.1-DRAFT. (2010). Reliability and Maintainability (R&M) Requirements for NASA Programs and Projects. Washington, DC.

NSTS/ISS 18798 Rev. B. (1997). Interpretations of NSTS/ISS Payload Safety Requirements. Washington, DC.

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. (2002). Washington, DC.

SSP 50038 Rev. B. (1995). Computer-Based Control System Safety Requirements. (ISS). Washington, DC.

A.2.2 Non-Government Documents

Cheng, P. (ed). (2005). TOR-2005(8617)-4204, 100 Questions for Technical Review. The Aerospace Corporation.

A.2.3 Suggested and Related Reading

Avizienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. (2004). “Basic Concepts and Taxonomy of Dependable and Secure Computing.” *IEEE Transactions on Dependable and Secure Computing* 1(1): 11–33.

Dvorak, D. (ed). (2009). NASA Study on Flight Software Complexity. Pasadena, CA: NASA Office of Chief Engineer /NASA Jet Propulsion Laboratory.

Federal Aviation Administration. 2010 National Aviation Research Plan. Washington, DC, 2010. Regulatory and Guidance Library: http://rgl.faa.gov/

Hallion, R. (ed). (2010). NASA/SP-2010-570, NASA's Contributions to Aeronautics. Washington, DC.

Hogan, S. (ed). (2009). *TOR-2009 (8591)-14, Effective Fault Management Guidelines*. The Aerospace Corporation.

Johnson, S.; Day, J. (2010). "Conceptual Framework for a Fault Management Design Methodology" (AIAA Paper #: 227006). AIAA Infotech@Conference. Atlanta, Georgia.

Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems* 4(3): 382–401. 1982.

Rasmussen, R. "GN&C Fault Protection Fundamentals." (2008). 31st Annual AAS Guidance and Control Conference. Breckenridge, CO.

Vaughan, D. (1996). *The Challenger Launch Decision*. Chicago, IL: University of Chicago Press.

APPENDIX B: FAULT MANAGEMENT CONCERNS WITHIN NASA

B.1 Purpose and/or Scope

The purpose of this appendix is to provide background on the relevance of FM to each of NASA's Directorates and to all of NASA's missions. 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.

B.1.1 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,[14,15] 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,[16] 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.[17] 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

[14] Federal Aviation Administration. 2010 National Aviation Research Plan. Washington, DC, 2010.
[15] 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.
[16] Joint Planning and Development Office. *Next Generation Air Transportation System Integrated Plan.* Washington, DC, 2004.
[17] Federal Aviation Administration. Regulatory and Guidance Library: http://rgl.faa.gov/

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.[18] In general, the aeronautics FM research that NASA conducts poses the following features and challenges.

B.1.1.1 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. Via a 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 in 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 common in today's commercial aviation systems.

B.1.1.2 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 determine, predict, mitigate, and manage the state of degradation for 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.

B.1.1.3 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.

B.1.1.4 Reliability Over a Long Lifetime With a High Number of Flight Cycles

[18] Hallion, Richard (ed). NASA/SP-2010-570, NASA's Contributions to Aeronautics. Washington, DC, 2010.

Aircraft are highly complex systems 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.

B.1.1.5 Large Existing Failure Modes and Effects Knowledge-base

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 and risks. This information collectively provides a large knowledge base to draw upon and enables FM designers to account for aircraft failure modes and effects.

B.1.1.6 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 allow their appropriate response to a range of conditions. Aeronautics missions have taken an inter-disciplinary 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.

B.1.2 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.[3].

B.1.2.1 Failure Tolerance Requirements do 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 [3]:

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 supporting 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.

B.1.2.2 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 [3]. 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.

B.1.3 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.

B.1.3.1 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.

B.1.3.2 High Reliability and Long Lifetime

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 dynamic environments. Lifetime and environmental factors dictate that individual components, and the overall system, have 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 limitations on the 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. An attendant difficulty, particularly for deep space missions, is the absence of any possibility to perform direct hardware maintenance or upgrading. Any needed evolution of functionality, whether related to faults or not, can be accomplished only through software.

B.1.3.3 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) often 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.

B.1.3.4 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. System complexity has increased recently due to (1) greater capability demands coupled with the need to minimize mass and power and hence the use of information and functional redundancy, and (2) the requirement to place many of these functions onboard for autonomous operations to reduce costs and to ensure mission success despite long communication latencies.

B.1.3.5 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.

B.1.4 Fault Management Concerns Within Space Operations

[To be expanded in later releases]

B.1.5 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 affect the execution of FM—the policies and ideals become institutional rationale for how FM should be performed. If these policies and ideals are not documented and communicated to other institutions, there exists 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.[19,20]

B.1.5.1 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.

B.1.5.2 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 "single fault tolerance" requirement. 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

[19] Fesq, Lorraine (ed). NASA White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate, Pasadena, CA: NASA Jet Propulsion Laboratory. 2009.
[20] Columbia Accident Investigation Board. Columbia Accident Investigation Board Report, Vol.1. Washington, DC, 2003.

example. Since FM is not typically identified as a proposal evaluation criterion, suppliers may 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.

B.1.5.3 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.

APPENDIX C: FM FUNDAMENTAL CONCEPTS AND PRINCIPLES

C.1 Purpose and/or Scope

The purpose of this appendix is to provide the underlying concepts and guiding principles that define and shape the FM field.

FM addresses the off-nominal states and conditions of a system, and must be developed in parallel to the nominal system design as shown in Figure 9. For a system to fulfill its goals and objectives, systems engineers define its functions. These mission functions should be analyzed to determine if the risk of their failure is acceptable, given the system design for that function. Where the risks of failure for a function are unacceptable, FM engineers design and deploy capabilities to preserve or recover that function, or to select one or more alternate goals that either do not require the failed function, or require less stringent performance.

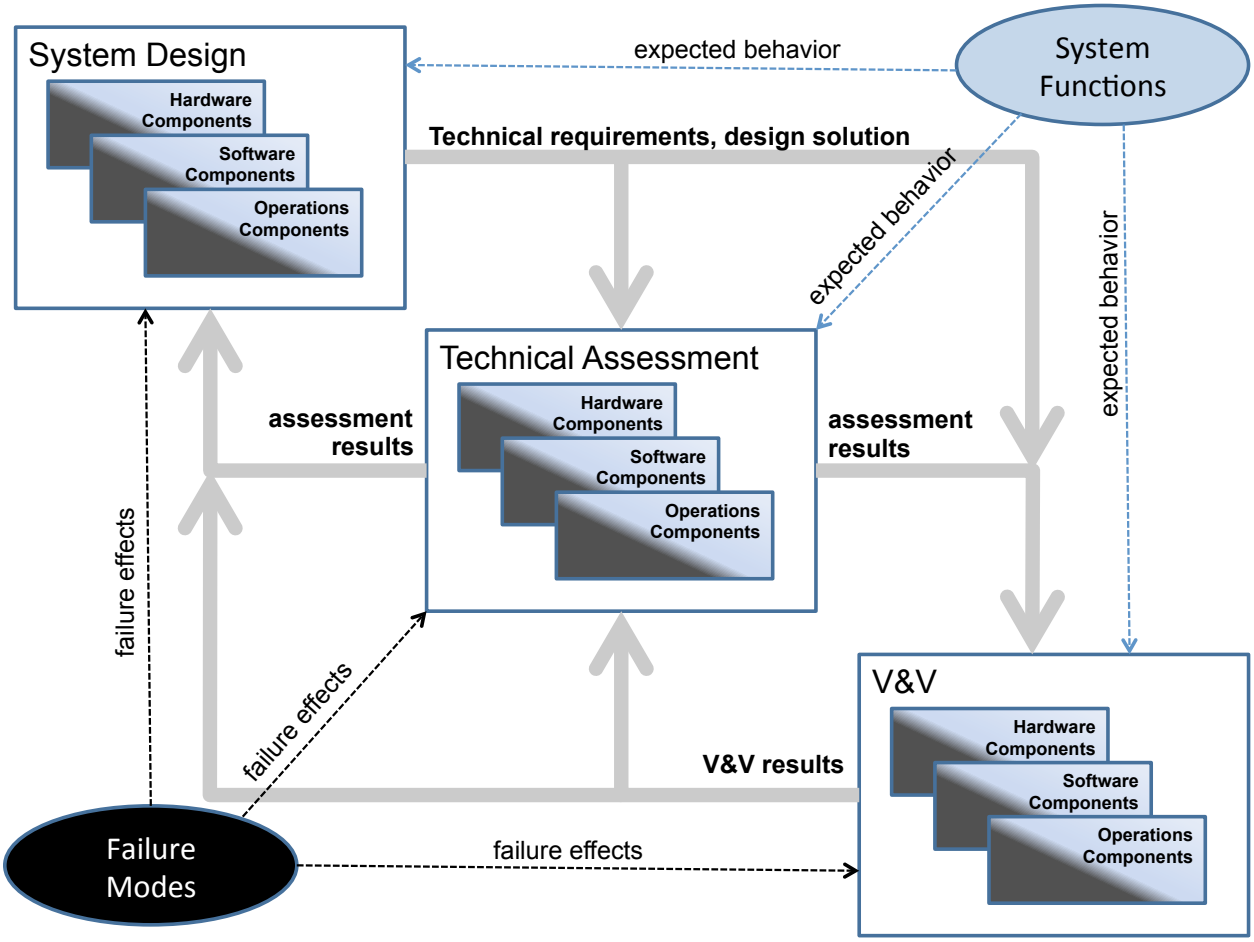

Figure 9 — FM follows a SE process, addressing off-nominal conditions/effects of failures (the "dark side" shown in the lower left) in parallel with activities to achieve nominal system functions (upper right).

In general, risks to mission functions are mitigated by one of five FM strategies, illustrated in figure 10, FM Strategies. In failure prevention, actions are taken to ensure that failures will not occur.

- Design-Time Fault Avoidance: Design function and FM capabilities to minimize the risk of a fault and resulting failure using, for example, stricter quality assurance processes, higher quality parts, or increased margin.

- Operational Failure Avoidance: Predict that a failure will occur in the future and take action to prevent it from happening, generally through repair, replacement, or operational changes that reduce the failure's probability or delay its occurrence**.**

In failure tolerance, failures are allowed to occur, but their effects are mitigated or accepted.

- Failure Masking: Allow a lower level failure to occur, but mask its effects so that it does not affect the higher level system function.

- Failure Recovery: Allow a failure to temporarily compromise the system function, but respond and recover before the failure compromises a mission goal.

- Goal Change: Allow a failure to compromise the system function, and respond by changing the system's goals to new, usually degraded goals that can be achieved.

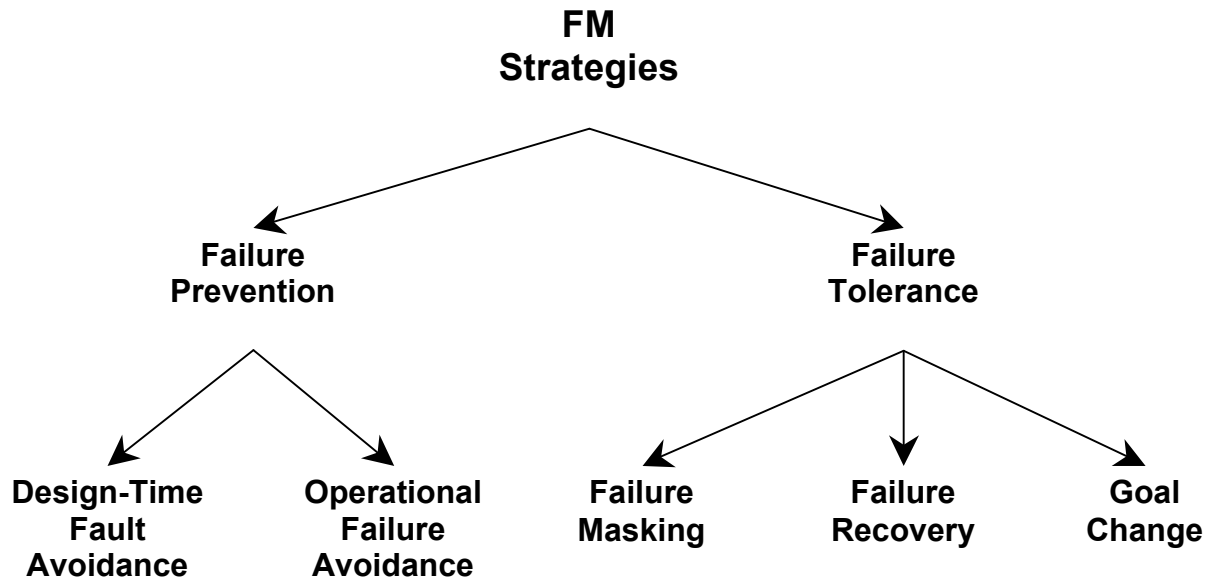

Figure 10—FM Strategies

Pitfall: ***Failure to Consider Alternatives.*** *It is easy to concentrate on one type of failure, e.g., random part failure, or one FM strategy, e.g., design-time fault avoidance, to the exclusion of all else. Different FM strategies are appropriate for different failure modes and mission types; different FM strategies are appropriate for different mission phases (design vs. implementation and operations). Selection of FM strategies, and ultimately the FM architecture and design, needs to consider the full mission life cycle, the required mission functionality, the available mission resources across the mission life cycle, and the accepted risk posture for the mission.*

FM draws from systems theory and SE by treating flight, ground, and operations as a collection of interacting parts whose relationships are open to analysis. This treatment is necessary because failures in one element of a system can propagate and have further failure effects in other, seemingly unrelated elements of the system, creating unexpected emergent behavior. FM also uses concepts from control theory by treating the active management of failures (e.g., detection, isolation, mitigation) as a problem of estimation and control.

C.2 Concepts

FM has evolved independently at multiple institutions and has a wide variety of interested stakeholders (see table 1). This section captures concepts and definitions for key terms that provide a common framework behind the guidelines and the best practices throughout this Handbook. The topics covered include the following:

- Definitions for failures, faults, and anomalies.
- The FM system scope and environment.

- States and behaviors.
- Hardware, functional, and informational redundancy.
- Failure effect propagation.
- Automation and autonomy in relation to FM.
- The primary FM functions (detection, diagnosis, decision, response, and adjust).

C.2.1 Failures and Faults

In FM, failure is defined as the "unacceptable performance of an intended function." Failure is by definition an effect, as opposed to a cause, because "performance" by its nature is assessed by the system's observable and predictable states and behaviors. Failure can result from causes internal to the system or external to the system (i.e., in the environment). Projects have responsibility for internal causes, and also for identifying an expected range of mission environments.

A fault is an internal cause of failure. Faults and failures are connected by their relationship as cause and effect. However, a "cause" from one perspective is often seen as an "effect" from another perspective, which is the event to be explained by a deeper cause. A root cause is the first event in a failure event chain; a proximate cause is the last causal event in a failure event chain. There can be several interacting root causes, or several interacting proximal causes, that together produce the failure. These concepts are intimately linked in a hierarchical and recursive fashion. Figure 11, Fault/Failure Event Chain, shows the conceptual relationship of faults, failures, and root causes.

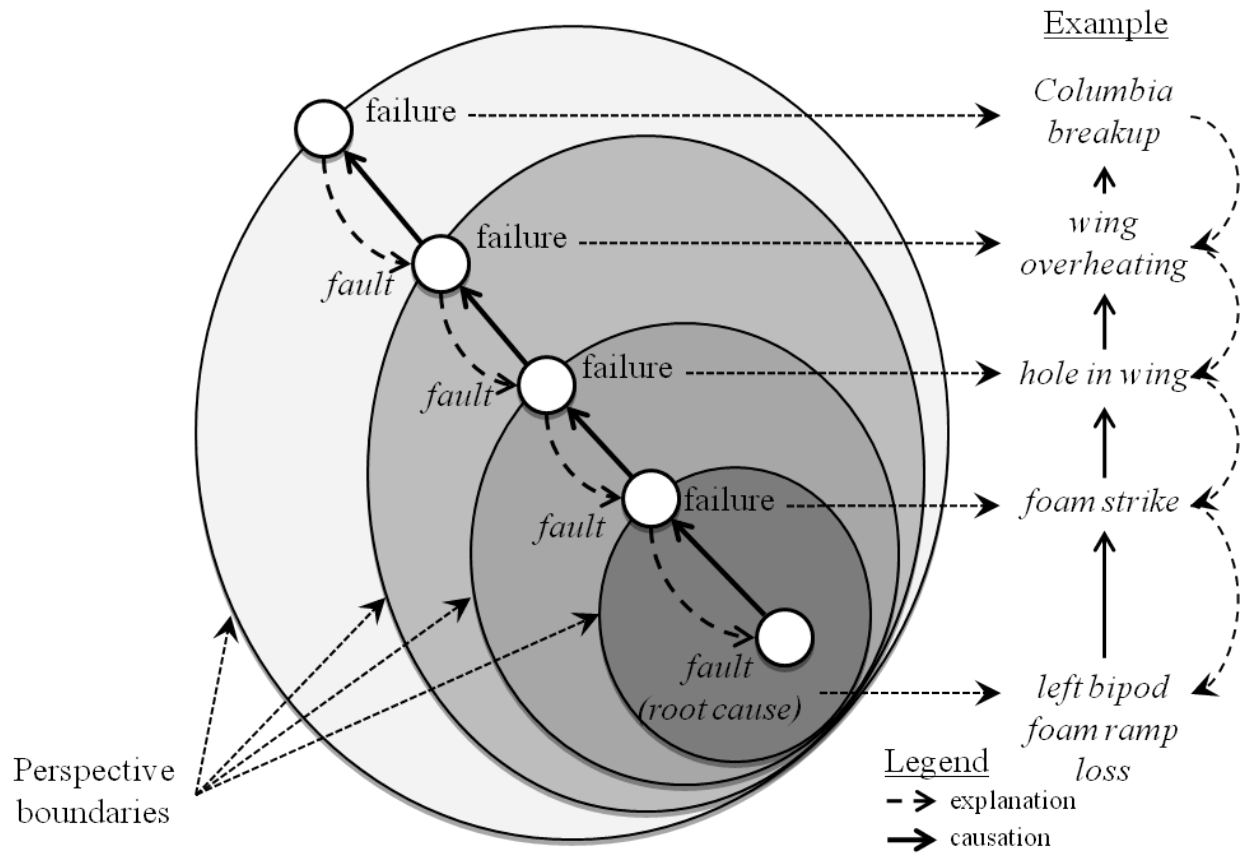

Figure 11—Fault/Failure Event Chain

A well-known example of this is the Columbia shuttle accident.[21] In the initial investigation into the cause(s) of the accident, the event to be explained was the breakup of the orbiter. This was soon explained by the weakening of the wing due to overheating, traced to a deeper cause, the external tank (ET) foam falling off during ascent and punching a hole in the wing's leading edge Reinforced Carbon-Carbon. For many, this was "the physical explanation," or "the physical cause" of the accident. For ET designers, and for the Columbia Accident Investigation Board, this cause was an effect that needed to be explained. In this example, as well as many others, a high-level cause is seen as a failure effect from a lower level, for which explanation is needed.

The root cause is defined as the first fault or environmental cause in the chain of events used to explain a failure. It is frequently true that there is more than one root cause for a mishap, so "root cause" in this sense implies that the failure investigation finds several paths of events that eventually combine to create the ultimate system failure. The first events of each of these paths are the root causes. Root causes lead to effects, some of which are identified as "proximate" causes, or causes that immediately precede the final failure in a chain of events. Contributing factors are just that, other considerations (possibly anomalies) that—while they do not represent unacceptable performance—allow a fault to occur, make a fault more likely to occur, or exacerbate the consequences of a fault.

[21] Columbia Accident Investigation Board. Columbia Accident Investigation Board Report, Vol.1. Washington, DC, 2003.

"Fault" is often used to describe the detected occurrence of undesirable performance. In this sense, a fault is an event to be explained. It may be the result of a failure, or it may be an indicator of a potential future failure. Alternately, analysis may determine that the event (fault) is simply an anomaly that does not materially affect system performance. From this perspective, FM engineering has the responsibility for defining the (hardware, software, and operations) processes to detect the event, and the ability to either tolerate or respond to the detected condition.

Pitfall: ***Contradictory Use of Fault and Failure in Requirements.*** *Cause and effect are inherently relative terms. This is addressed in FM terminology by identifying failure with effect (the thing observed) and fault with cause (the explanation for the thing observed). However, requirements are often written with contradictions between causes and effects, and hence between the words fault and failure. For the unwary, this can lead to different interpretations of requirements, and to latent faults in the design that can lead to catastrophic failure of the system in operations. The FM practitioner will frequently encounter confusion and arguments about causes and effects because of this conceptual and terminological confusion. The FM practitioner needs to define and use these terms consistently on a program; it is highly recommended to use the definitions in this Handbook.*

There is some historical terminology that the FM designer and operator should be aware of. Terms such as "fault diagnosis" could be described more accurately as "failure-cause diagnosis," because in-depth investigation may find that there was no design flaw or operator error. "Fault diagnosis" is historical shorthand, but the FM designer needs to be aware that causes are from both inside and outside the system boundary. Another issue is with "failure detection." Given the formal distinction between "faults" and "failures," the phrase "Fault Detection, Isolation, and Response" should be "Failure Detection, Fault Isolation, and Failure Response." However, this is cumbersome, and so the historical phrase is used.

C.2.2 Anomalies

An anomaly is defined as the "unexpected performance of an intended function." An anomaly should not be confused with a failure. Failures can exist without being anomalous, such as expected depletion of an expendable resource (e.g., cryogenic cooler). Conversely, anomalies that are not failures are also common, such as an unusual (unexpected) power signature that does not cause any loss of functionality.

Failures, not anomalies, are the primary focus of FM. However, the FM practitioner should consider the potential for anomalies as well as possible failure modes. Anomalies can be used as predictors for future faults, as in the case of an increase in temperature that is within the normal operating range but approaches the limiting value. Anomalies in one area can also lead to faults in other areas, as in the case of an increase in temperature in a component that causes overheating and failure of a neighboring component. However, anomalies that affect the FM functions themselves should be identified and, if possible, mitigated. FM capabilities should ideally remain independent and functional during all anomalies.

C.2.3 System and Environment

The placement of the system boundary is an essential concept for FM. The system boundary defines the bound of responsibility and/or interest, beyond which the team or engineer is not required to control faults. Outside of the boundary lies the environment, which the system cannot alter, but within which the system has to execute its mission. This can be a particular challenge when characteristics of the operating environment (and their effects on the behavior of the system) are at least partly unknown. Although the environment lies outside of the system, the FM practitioner has to understand the interactions of the system across the boundary to the environment to ensure the system functions properly within the environment. If the "environment" includes another engineered system, then the FM designer should work with the practitioners across that boundary to coordinate the design and operations across the boundary, though other teams or engineers are responsible for changes on the other side of the system boundary.

FM functionality is typically distributed across multiple elements of the system and multiple phases of use, with specific (and often redundant) capabilities assigned to hardware, software, and operational elements. All hardware, software, procedures, and personnel that are required for implementing, testing, and operating the mission are to be included within the FM boundary of the system. It may be acceptable for a subsystem designer, who is responsible for only a few (but not all) functions in the full FM scope of responsibility, to set his or her boundary at their subsystem boundary, as s/he is responsible only for items inside the boundary. However, the system-level FM designer has to address the entire FM scope, and should set the system boundary to encompass all mechanisms that perform FM functions.

Finally, the FM designer should carefully define and document the system boundary conditions that define the environment within which the system has to correctly execute its function(s). These boundary conditions not only define the physical environment (e.g., thermal, radiation, wind, landing surface), but the risk posture accepted for each mission, and the operating environment (e.g., time delays necessitating autonomous operations) within which the mission has to execute. This documented system boundary underpins the FM requirements and design, and helps control cost growth late in the development cycle.

C.2.4 States and Behaviors

System operation is characterized by changes to the system's states. The state of a system is defined by the value(s) of a set of physical or logical state variables at a specified point in time. The time evolution of states is called "behavior." Off-nominal operation of the system can be identified by monitoring these states and behaviors and comparing them to expected and intended states and behaviors, as defined by informal or formal models of the system. The failure/anomaly detection functions of FM perform these operations.

FM detection functions (failure detection and anomaly detection) can monitor either states or behaviors, or both. When these functions observe states in a single snapshot of time, then they monitor states. An example of this is human inspection of a photograph of a structure to identify a crack or deformity, or of the structure directly. For this detection mechanism to determine that

a failure (a crack or deformity) exists, there is no need for a "three strike" or "persistence" counter" to determine whether an observation is valid. Other detection mechanisms typical of real-time systems use such counters, to reduce the probability of a false positive detection. In this case, the failure detection mechanism is not just a single snapshot of a system's state (the attitude errors) at a single point in time; it uses multiple points to verify that the state is persistent. Although less common, FM detection functions can also monitor the time evolution (behavior) of a system.

FM detection mechanisms never directly observe the true (actual) states or behaviors of the system. Rather, the system contains mechanisms to measure certain phenomena, and these measurements will have some degree of precision, or conversely, some inherent inaccuracy. For observations of continuous phenomena, such as pressure, temperature, voltage, attitude, position, and the like, the numerical value provided will have uncertainty both in value and in time. In the best case, the precision will coincide with the significant figures of the digital measurement provided. More typically, the deviations between the actual state value and the measured value will be larger than this, to an amount that depends on the characteristics of the measurement device.

In addition to the inherent inaccuracy in any measurement, there is always the possibility of a failure that corrupts the data being observed, and thus other redundant measurement(s) or observation(s) can be used to determine if the digital measurement is accurate. Measurements are used in the FM detection and diagnosis functions to determine the true state with high probability, but no individual measurement by itself directly indicates the true state.

C.2.5 Redundancy

Redundancy is a fundamental aspect of FM designs and takes different forms based on the potential type of fault. Mistakes in design can become common-mode/design or systemic faults, in manufacturing they become "random part failure," and in operations they are considered "operator error."

There are four different approaches to redundancy, as follows: First, hardware identical; second, functional; third, informational; and fourth, temporal. Each of these approaches is better suited to handling different types of failures (e.g., common-mode/design faults, random part failure, or human error). When redundancy is included in the FM design, the full FM system analysis needs to consider the effectiveness of the approach in the FM design, limitations on it, and the mechanism(s) controlling the redundancy as part of the justification of the design.

C.2.5.1 Hardware Identical Redundancy

Hardware-identical redundancy can be used to mitigate random failures and expected lifetime limitations. A typical example of this type of mitigation is the inclusion of five identical reaction wheel assemblies, when a minimum of three is required for operations. However, while the hardware-identical redundancy mitigates random part failure in any of the redundant strings, it cannot mitigate a "common cause failure," a design flaw or manufacturing/assembly flaw common among all of the redundant strings. Hardware identical redundancy also can be utilized

both for failure detection and for failure responses. The voting mechanism in the triply redundant computing system is a mechanism for detecting failures in one of the computers and a fault isolation mechanism in that it determines the location of the originating fault as somewhere in the string that does not compare, and not in other strings.

C.2.5.2 Functional (Dissimilar or Analytic) Redundancy

Functional redundancy is the use of dissimilar hardware, software, or operations procedures to perform identical functions. Functional redundancy can be used for failure detection, by using non-identical measurements of related physical parameters (e.g., voltage, current, and resistance) to provide the same information content as a crosscheck on the validity of an individual measurement. It also can be used for failure prevention, by using multiple independent mechanisms for initiating critical activities (e.g., a database enable/disable flags, an operator confirmation, and separate hardware commands to arm and fire a pyro valve). Finally, it also can be used as part of a planned autonomous failure response (e.g., failover to a "safe mode" computer) or an unplanned workaround for an in-flight anomaly (e.g., use of a thruster to replace the function of a failed reaction wheel).

C.2.5.3 Informational Redundancy

Information redundancy utilizes extra information to detect and potentially to respond to certain types of failures. The most common example is error detection and correction codes (EDAC). In EDAC, extra bits are added to a message, such that if a cosmic ray or some other phenomenon causes one or more bits to flip (a single event upset (SEU)), then the receiving device can use the extra, redundant information to reconstruct the original message, in effect, "unflipping" the bit(s) that had been changed. In this example, information redundancy is used for detection, isolation, and response.

C.2.5.4 Temporal Redundancy

Temporal redundancy refers to the practice of repeating a function should it fail upon a single execution. A typical example is the use of several measurements over time of the same state variable, because any single measurement could be corrupted by an SEU. Another common example in computer processing is the checkpoint-rollback capability, when a series of computations have produced suspect results. In the checkpoint-rollback, the computer state is reverted (rolled back) to the computer state at a previous point in time that had been stored for potential future use (the checkpoint), and then re-started from the checkpoint to re-compute the original set of calculations.

C.2.6 Failure Effect Propagation and FM Latencies

FM is effective only if its responses execute fast enough to mitigate the effect of the failures to which each FM response applies. There is therefore a race condition between the latencies of the failure detection, fault isolation, and failure responses and the temporal evolution of the failure effects as they propagate through the system. Obviously, if the fault detection, isolation, and response (FDIR) latencies are such that the response completes only after the system function is

lost, then the FM mechanism in this case is only partially effective at best and useless at worst. This race condition has to be assessed for every FM mechanism that is included in the system. If humans are performing FM functions, then they are part of the FM mechanism and have to be included in the assessment.

C.2.6.1 Failure Effect Propagation Paths

FM is designed to mitigate failure effects, which spread from their point of origin at the fault (or in Failure Modes and Effects Analysis (FMEA) terminology, the "failure mode") along one or more failure effect propagation paths (FEPPs) through the system. Along these paths, the physics of the failure effects can change. For example, a mechanical fault in a liquid propulsion system valve can cause changes to the liquid pressure and quantity downstream of that valve. In turn, this abnormal pressure can lead to inappropriate temperatures of the fluid, and assuming for this example that this drives a turbine, to an incorrect turbine speed. The incorrect turbine speed may in turn create an off-nominal power level if the turbine is used to generate electrical power, which in turn affects avionic and mechanical components that depend on that power. If some of those components drive a hydraulic power system, then the hydraulic power levels will be incorrect, which in turn could cause a thrust-vector control actuator to lock up.

This example illustrates that there can be multiple effects of a single fault, and that it is not at all obvious how quickly these effects will propagate and to what ultimate effects. The temporal evolution of how they spread, and their relative effects, depends on the physics of each of the devices or the materials and mechanisms that propagate the effects. The timing and effects can also depend not just on the failure mode, but also on the specific physics of that failure mode, such that one failure mode as identified in the FMEA could have several possible effects and failure effect propagation times associated with those effects.

The point in an FEPP when a failure stops propagating is called a "failure containment boundary." A set of boundaries that stop a related set of failure effects define a "failure containment region" (FCR) or "failure containment zone" because the failure effects are contained within this region or zone. Containment of failures can be the result of passive designs or of active FM mitigations. Collectively, the placement of these boundaries and the definition of FCRs is a key aspect of designing FM architecture.

Historically, the analysis of FEPPs and effects has been underdeveloped. Recent efforts in this area, through methods such as directed graph modeling, have shown that both FMEAs and top-down fault tree analyses (FTAs) have significant gaps, and the informal methods used by FM designers have been only partially effective in addressing these gaps. Formal analysis of FEPPs shows promise to close these gaps.

C.2.6.2 Criticality of Effects

In general, failures start with some relatively innocuous cause, and then over time, whether milliseconds or decades, propagate to create effects that grow increasingly more serious. Ultimately, if not contained and/or mitigated, these effects may cause loss of life, the system, or the mission.

The "Critical Failure Effect" (CFE) is defined as a failure effect, which if it occurs, irrevocably compromises one or more system or mission objectives. The term "time to criticality" (TTC) is defined as the amount of time it takes for failure effects to propagate from the failure mode along FEPPs to the CFE. In general, the goal of the FM designer is to set the failure containment boundary far enough "upstream" (closer to the causal mechanism), that the failure responses can complete within the TTC and before the CFE can occur.

The TTC is not always the point in time when the mission actually fails. Rather, it is based on some intermediate effect, which if it occurs, has irrevocably compromised the mission, even if that ultimate mission failure or degradation will occur sometime further in the future. Consider a loss of propellant failure scenario in the cruise phase of a planetary probe. The effects of the propellant loss may not be ultimately manifested for months or years when the vehicle has to perform orbit operations to gather science data. The relevant time to measure for FM is the CFE, which in this case is "the amount of time, given the rate of loss of propellant based on the current (and projected) leak size, when there will be not enough propellant to meet mission objectives." When several CFEs occur for a given fault, then the CFE of relevance is the one to which the failure effects propagate soonest.

Pitfall: ***Worst Case Analysis.*** *A "worst case analysis" may not actually capture the worst case. For example, a severe "leak" in a propulsion system, which is often identified as the worst-case leak, is often much easier to detect than a smaller leak, and if the FM is improperly designed, the spacecraft could lose excessive propellant before the smaller (and seemingly less dangerous) leak is detected.*

C.2.6.3 Failure Response Latencies

The FM responses that are designed to mitigate the failure effects described in the previous sections should always operate fast enough to do so successfully. Several latencies have to be addressed, including sensor latencies (the measured value can have significant delays in reflecting the actual value of the measured physical phenomenon), data transmission latencies, computer processing cycle times, detection algorithm latencies such as "three-strike counters," decision latencies, and finally the latencies of the responses themselves. For each FM mechanism, these latencies have to be summed and compared to the time propagation of the failure effects to the critical effect they are intended to address.

As noted previously, the specific point in time by which the FM response has to complete is generally the time at which the CFE occurs. For example, in the case of a crew abort from an exploding launch vehicle, the abort has to be completed fast enough so that the crew vehicle is removed from the debris field of the exploding launch vehicle. This means that the ignition of the launch abort system has to occur early enough that the latencies of the solid rocket thrust and crew capsule acceleration are accounted for, and that the resulting crew capsule speed and trajectory are such as to enable successful escape from the debris field. In the prediction of when an aircraft's structure is no longer sufficient to ensure successful flight, the TTC is measured in decades, not milliseconds. The FM system has to detect failures at a low enough level of

functionality and early enough to prevent the spread of those low-level failures to larger-scale system failures, and the response has to be complete before the CFE.

Pitfall: ***FM Performance.*** *The FM designer has to design, and then prove, that detection, diagnosis, and response operate faster than the TTC (time from failure effect initiation to the CFE). If the FM control loop is not fast enough, then the FM designer has to determine the relative probabilities for success and failure of the FM control loop against the various failure effects it is designed to mitigate.*

C.2.7 Fault/Failure Tolerance

Fault tolerance and failure tolerance are synonyms, defined as "the ability to perform a function in the presence of any of a specified number of coincident, independent failure causes of specified types." Fault tolerance is unusual in that it is the ability to tolerate failures, but also is tied to the idea of a certain number of faults that cause failures that have to be tolerated. There have been many debates as to whether the term should really be fault tolerance, because it is a specified number of causes whose effects have to be tolerated, or failure tolerance, because it is the effects of the faults that have to be tolerated. The "answer" is that it is both, because 1) there are a specified number of causes; but 2) it is their effects that have to be tolerated. Thus, the terms fault or failure tolerance are both acceptable.

Failure tolerance is related to the terms "fail-operational" and "fail-safe." Fail-operational indicates that the system is designed to continue to operate without loss of functionality in the presence of a failure resulting from a specified number of faults. Fail-safe indicates that the system is designed to preserve some critical subset of functions in the presence of a failure resulting from the occurrence of a specified number of faults. There are occasional debates as to whether "fail-safe" is failure tolerance because not all system functions are preserved, and the pursuit of some mission objectives are suspended, but there is no argument that "fail-operational" is an example of failure tolerance.

As noted previously, failure tolerance and failure prevention are recursive, hierarchical concepts. Fault tolerance at a low level (or closer to the failure cause location) can enable failure prevention at a higher level (or further "downstream" from the causal location).

A given failure tolerance mechanism is valid only against certain types or classes of faults. For example, the triplex voting system handles regular "random part failures." This is a general characteristic of failure tolerance, that it is only valid against certain faults and failures, but not others. Specification of failure tolerance, without identifying what is being tolerated, is not only incomplete, but potentially dangerous, as it can mislead designers and managers into believing it is effective against all faults and failures, which is incorrect.

The locations of the failure tolerance mechanisms generally define the boundaries of an FCR. These regions are the zones in which certain failures, tied to certain classes of faults, can propagate, but not beyond the boundary of the FCR. FM designers, particularly for computing systems, often apply the FCR concept in the design process.

C.2.8 Automation and Autonomy

Automation (such as, function X is automated or automatic) refers to the allocation of system functions to machines (hardware or software) versus humans. If a function is implemented wholly by machines, then the function is fully automated, and conversely if implemented wholly by humans, then the function is not automated at all. Many functions are implemented by a mix of humans and machines in their implementation, and thus are identified as "partly automated." Autonomy refers to the relative locations and scope of decision-making and control functions between two locations within a system or across the system boundary. It is also frequently described as the "locus of control." Autonomy is relative in the sense that it is to be defined with respect to a specified location inside or outside the system, and then assessing the decision-making and control capabilities of other parts of the system with respect to that location. The most common example is the comparison of the flight segment versus the ground segment for a given system. The more decision-making and control capability that exists in the flight segment instead of the ground segment, the more autonomous the flight segment is said to be, from the perspective of the ground segment. For a robotic spacecraft, the flight segment usually consists of the spacecraft, so the most common autonomy comparison is between the spacecraft and the ground segment. For a crewed vehicle, an important autonomy comparison is between the ground segment and the joint vehicle-crew combination (the flight segment). One can also assess the relative autonomy of a vehicle from the perspective of the crew that is on the vehicle. The more decision-making and control authority that resides in the vehicle, as in cases where the crew cannot respond quickly enough to certain failures, then the vehicle is said to be autonomous from the crew for those decisions.

FM is closely linked to the concepts of automation and autonomy. Like many other functions, one can design the system with varying levels of FM automation and autonomy. Decisions regarding the application of automation and autonomy to FM functions are a trade between flight and ground segment complexity, flight and ground resource availability, response time requirements, and the risk posture of the mission. For example, a small, low-cost, low Earth orbit (LEO) mission may not be able to justify the need for a sophisticated onboard, automated FM system, while round-trip communication delays may force a deep space mission to implement autonomous onboard management of faults during critical operations (e.g., orbit insertion). On the other hand, it may be more cost-effective over the total life cycle of a small, low cost mission to automate FM capabilities (whether autonomously onboard or on the ground) to allow for "lights out" operation. These, and other considerations, need to be included in the requirements, architecture, and design of the FM system.

C.3 Fault Management Functions and Definitions

This section describes each of the operational FM functions shown in figure 12, Operational FM Functions.[22] These functions are active during the operational phase of the mission. The intent of FM is to preserve as much system functionality as possible, given the nature of the fault(s) to which it is responding and the risk posture of the mission. Preservation may mean that functionality is not compromised, or that functionality can be recovered when it has been compromised. If the system function cannot be preserved, an option may be to change the goal

[22] Note: Prognosis is not included in the diagram shown in figure 12, and is not yet addressed in this Handbook.

to another achievable goal that does not require that system function. The FM functions all contribute to the goal of preserving system functionality, though not all of the functions are always activated with any given failure. For example, it is frequently true that a failure response (failure recovery or goal change) may be initiated without the specific failure cause being identified. This is often the case, for example, when a spacecraft enters a "safe" state, thereby changing its goal from science data collection to asset preservation. There may be a later analysis to identify the failure cause, after the vehicle has implemented an autonomous response.

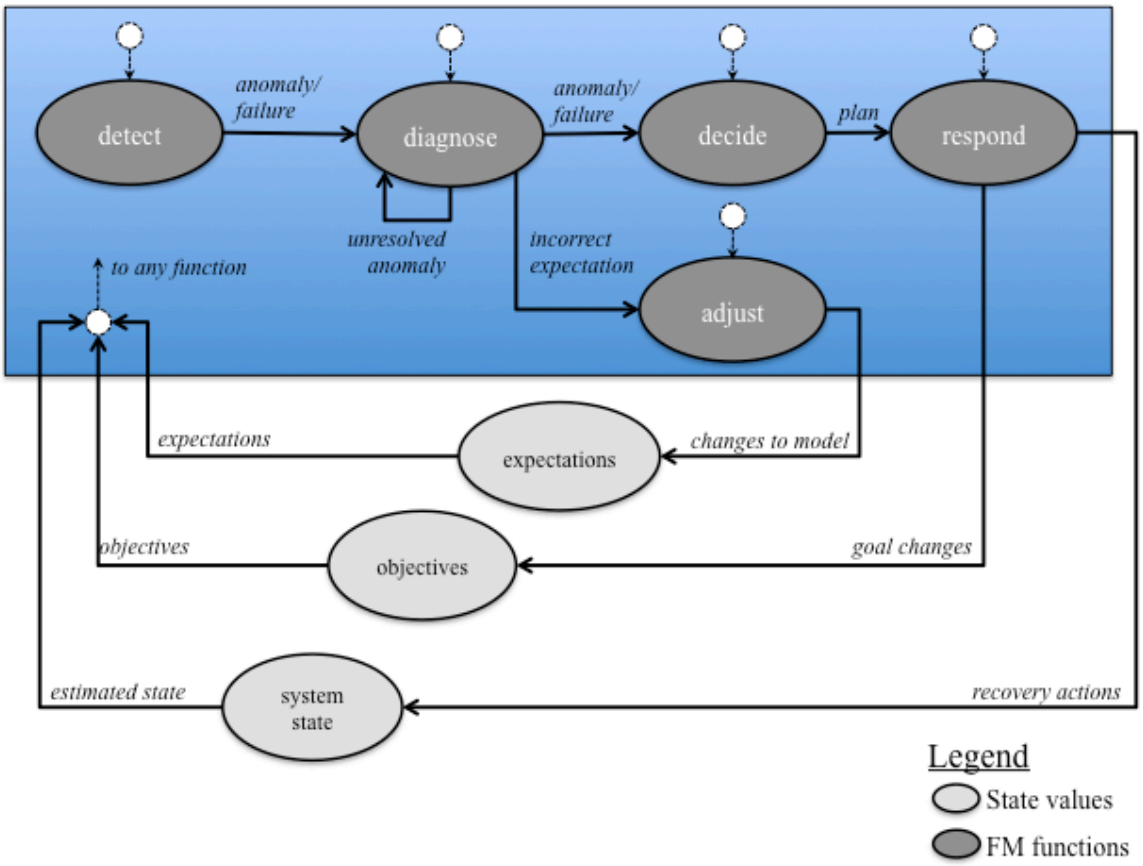

Figure 12—Operational FM Functions

When FM is needed to preserve functionality, it is the task of the FM designer to develop and implement mechanisms utilizing the relevant FM functions. The FM mechanisms deployed may include more than one function, or one function could be performed by more than one mechanism. For example, in a triplex voting computer system (known as triple modular redundancy), the triplex voting scheme includes failure detection, fault isolation, failure response determination, and failure recovery all in a single mechanism.

C.3.1 Detection

The FM function of detection comprises the detection of off-nominal situations, whether unacceptable (failure) or simply unexpected (anomaly). Their definitions, which are "deciding

that a failure exists" and "deciding that an anomaly exists," are straightforward extensions of the definitions of failure and anomaly.

Detection usually contains three sub-functions. The first is the implementation of a threshold of some kind to separate unacceptable/unexpected from acceptable/expected states and behaviors. The second is a filtering mechanism to determine if the threshold function is a false positive. This is often performed through mechanisms such as a "three-strike" counter or some other persistence evaluation to determine if the change in the measurement from previous measurements is valid and not corrupted by measurement noise or a SEU. Third, if the filtering mechanism determines that the measurement is valid, then notification of failure/anomaly is sent to other FM functions and/or other functions that need to know that a failure has occurred.

Failure detections can be based on knowledge of specific, known failure states and behaviors based on FMEA-identified failure modes, or they can be designed based on knowledge of what level of function compromise is unacceptable for achievement of the function's objective, regardless of the underlying failure mechanisms.

C.3.2 Diagnosis

Diagnosis is the term that encompasses the two FM functions of fault isolation and fault identification. It can be considered as a composite function that aims to determine the location and mechanism of the underlying failure cause(s).

Both fault isolation and identification are measured via ambiguity groups, which are groupings of components that cannot be distinguished from each other based on the detection signature provided by the detection functions. That is, if a specific set of detections occur, the underlying failure cause may exist in one of several possible components, and it is impossible to determine, with the given data, exactly which component contains the causal mechanism.

C.3.2.1 Fault Isolation

Fault isolation is the process of determining where the causal mechanism of a failure exists. The FM usage of the phrase "fault isolation" as a diagnostic function should not be confused with the use of the same phrase as a mechanism to prevent failure effects or causal mechanisms from spreading from one location to another (a common usage in electrical applications and electrical engineering). In FM terminology, preventing failure effects or causal mechanisms from spreading to another location is called "fault containment" or "failure containment."
The term fault isolation is historically used in FM and its predecessors, but includes determining the location not just of faults (causes of failure inside the system boundary), but also of environmental failure causes. It would be somewhat better termed "failure cause isolation," though for historical reasons we hold to the commonly used term "fault isolation." The fault isolation function determines the location of the failure cause, whether internal or external to the system.

C.3.2.2 Fault Identification

Fault identification, sometimes called "fault characterization," is the function of determining the possible causes of a failure or anomaly. Its implementation sometimes operates similarly to the fault isolation function in that automated diagnosis tools use similar techniques of forward and backward tracing of failure effects to determine the location of faults as it does to determine the possible failure modes that cause the observed failure. As with fault isolation, fault identification seeks for causes that can be inside the system boundary (faults), or outside the boundary in the environment.

It is frequently true that fault identification is not necessary for an effective failure response to be implemented. Often it only matters that the component in which the fault exists is removed from active use regardless of the particular failure mode in that component.

C.3.3 Decision

Decision is the FM function of determining the correct failure response to mitigate the current or predicted failure. It includes several key sub-functions, as follows: First, determining the compromises to system functionality that are occurring, how the failure could propagate, and how the compromised capabilities affect the system's ability to meet mission goals; second, identifying response options and determining the likely outcomes; third, selecting which response(s) to initiate; and fourth, notifying the system to implement the response(s).

Failure response determination can be implemented through automated mechanisms or human operators (ground or flight crew). When automated, the failure response determination is sometimes, though not always, seamlessly combined with detection and response functions. In these cases the "decision function" is not readily apparent, because the determination of what response to take is decided at design-time. A detected event immediately invokes execution of a response, because the decision of what response to take was pre-determined and built into the algorithm logic or into the hardware. In other cases, the decision logic is separated from the detections and responses.

C.3.4 Response

Failure response is a term that refers to three FM actions taken in response to a failure, as follows: First, goal change; second, failure recovery; and third, failure masking actions in response to a failure.

C.3.4.1 Goal Change

Goal change is defined as an action that alters the system's current goals. In the FM context, a goal change is activated to attempt to regain the system's ability to control the system state (achieve some function) in reaction to a failure. The most typical FM goal change is "safing." Usually the goal change is to a "degraded goal" or a subset of the system's original goals. For example, with spacecraft safing, the current science objectives may be abandoned while the spacecraft maintains the goals of ensuring a power-positive system and a communications link with Earth. In the case of a human-rated launch vehicle, an ascent abort abandons the goal of

achieving orbit, but protects the goal of keeping the crew safe. To do this, it specifies a different, achievable goal—to return the crew capsule and crew back to Earth.

Goal changes occur for many reasons, not just for FM. It is therefore not exclusively an FM function, but is shared with many other vehicle and mission functions and capabilities such as mission planning and operations, operational modes, and vehicle configuration controls.

C.3.4.2 Failure Recovery

Failure recovery is defined as an action taken to restore functions necessary to achieve existing or redefined system goals after a failure. In some cases, operations after recovery may be identical to operations prior to the failure, with no change of goals or functions. This would be the case for failover to an identical redundant hardware component or a computer reboot. However, in some cases, recovery to normal operation may require a new goal (one different from the original goal) for the system. An example of this would be turning off instruments to continue operations in a lower power configuration.

Failure recovery has been a label often applied to in-flight operational systems, and can be an autonomous recovery by the flight system or require intervention by the ground to achieve full recovery. However, failure recovery may also include maintenance or supportability actions as a part of the failure recovery. An example is a launch vehicle scrub. The failure recovery in this case may include repair and/or replacement of the failed component, reloading propellant tanks, and recycling the launch sequence to a point where it can be restarted.

C.3.4.3 Failure Masking

Failure masking is a variant of failure response in which failure effects are “hidden” from the rest of the system. The failure masking mechanism by definition prevents failure effects from moving past the mechanism, and thus it forms a FCR boundary dynamically. This can involve changing the system configuration to remove a failed component from active operation, or, alternatively, this can involve changing a goal to remove the need for a failed function. In the event that failure analysis proves that the failure response was inappropriate or unnecessary, failure masking can trap a fault without invoking any specific response, though possibly still reporting the occurrence. This is the case in a voting scheme in which a failed component is outvoted by other components and any effects from the failed component do not pass the FCR boundary.

C.3.5 Model Adjustment

FM practitioners use a variety of models and modeling practices, particularly for analysis of the performance and effectiveness of the FM design. These formal models, along with models of the system are produced by the various system designers and operators and are the basis for expectations of how the system will behave under failure conditions. Over the life of the program, these models often change as the system designers and operators learn how the system actually behaves in testing and operations. The FM practitioner has to plan for the adjustment of models based on operational experience, and the expected and observed degradation of performance over time. In addition, because these adjustments can lead to changes in what is

considered a failure or anomaly or conversely what behaviors are acceptable or expected, it is a crucial function for FM.

The most obvious example of model adjustment is upon diagnosis of anomalies. When anomalies occur, they are by definition unexpected, and an investigation is launched to understand where and what the causal mechanism might be for the unusual behavior. If the investigation is successful, then the anomaly is classified as either normal, expected behavior, as a degradation of function, or as a failure. In any case, there is a modification of the system model, so that future occurrences of this behavior will no longer be considered anomalous (or if they are rare, they will be very briefly considered unexpected in future occurrences, and then quickly resolved to be either failure or normal system behavior).

Pitfall: ***Normalization of Deviance.*** *Adjustment of a model has to be done with care. The FM practitioner should be wary of what has been called*[23] *"normalization of deviance," anomalies or anomalous behaviors that become classified over time as expected behaviors instead of remaining anomalies or unacceptable failures. The danger is one of complacency, that routine acceptance of anomalies can cause the FM practitioner to lose sight of the potential impacts of anomalies or faults that are danger signals of potentially much more catastrophic consequences, as was the case for both the Challenger and Columbia accidents.*

C.4 Guiding Principles

C.4.1 Crosscutting FM Interfaces

a. **Statement of Principle:** FM is a crosscutting engineering discipline that requires close coordination with SE, S&MA, and subsystem engineering teams.

b. **Commentary:** Implementation of FM functions is distributed across all elements of the project —hardware, software, and operations. As a part of a project's SE team, the FM engineer needs visibility into the nominal functionality of the entire system, in order to identify and plan appropriate responses to off-nominal behaviors. FM engineering utilizes the results of traditional reliability analyses, and as part of the parallel analysis of failure modes, FM engineers often have to force trades at various levels and across multiple subsystems. Therefore, a project's organizational structure and delegation of roles/responsibilities/authority has to support the flow of information to and from FM engineering, and allow trades to be clearly communicated and resolved across traditional subsystem and engineering disciplines. FM engineers need to be constantly aware of the global nature of engineering decisions that can affect FM and FM decisions that can affect overall system complexity and operations.

C.4.2 FM Development as Part of Systems Engineering

a. **Statement of Principle:** Design, analyze, verify, and validate FM with respect to the system's failure modes in parallel with development of the nominal system behaviors.

---

[23] Vaughan, D. 1996. *The Challenger Launch Decision*. Chicago, IL: University of Chicago Press.

b. **Commentary:** As shown in figure 9, every function of a system has both a "dark" side of potential failures and a "light" side of expected, nominal behaviors. The system's failure space is the set of possible failure behaviors, most of which will never occur in operation of the real system. Given the potential breadth of FM trades, crossing subsystem and component boundaries, decisions are often implicitly or explicitly made to postpone development of FM operational concepts, requirements, and designs. This then limits the trades available and can lead to more expensive, complex, or risky implementation approaches. To help control the complexity and ensure that the FM design is "dyed in" rather than "painted on," design and implementation of FM capabilities needs to progress hand-in-hand with the functions FM is expected to preserve. Figure 9 illustrates this parallel development of the nominal behaviors and failure modes throughout the implementation life cycle.

Pitfall: ***Heritage FM Systems.*** *FM designs often are inherited from previous missions without consideration of the applicability to the current mission of the heritage FM capabilities at each level (FM concept, architecture, design, implementation, and operations). FM is not "one size fits all." Do not assume that previous use or familiarity with a heritage FM design automatically conveys applicability to the current mission. Mission complexity and mission risk postures vary greatly. A heritage FM system from one application may or may not be suitable for another. The FM implementation for a 15-year flagship mission or a deep space mission with long return time delays will be more complex than that for a 1-year Explorer class mission in LEO. A simple mission with a single-string hardware design may require more onboard automation to meet mission goals and, therefore, a more complex software design, that a larger mission with significant hardware redundancy. FM requirements for human space flight are more extensive than for robotic "proof of concept" missions. In considering FM heritage, pay close attention to mismatches in inherent complexity and risk.*

C.4.3 System Boundary

a. **Statement of Principle:** Specify the system boundary so that it encompasses everything that detects, evaluates, and responds to failures as part of the system, including vehicle, crew, operators, and ground systems. The environment typically lies outside of the boundary; however, the system has to function within expected environmental conditions.

b. **Commentary:** FM design is an SE activity, and full analysis of FM requires placement of the system boundary around all elements that perform the FM functions. When scoping FM, consider all elements of the system (hardware, software, and operations); all phases of the mission (including V&V prior to launch); all aspects of operating the system (command and telemetry, reporting, troubleshooting, and analysis); the environment within which the system is required to operate; testing issues, such as fault injection capabilities; and the risk posture for the mission. Document the system boundary in such a manner that the FM requirements can be derived from and traced back to the mission concept and risk assumptions.

A typical problem with FM design is the incorrect specification of the system boundary that leaves the mission operators as "outside the system." It is common that for a full FM loop from detection through response and recovery, the mission operators and/or crew (for human spaceflight missions) perform essential FM functions. Likewise, for a subsystem or component,

it is common for subsystem organizations to draw their "system boundary" at the subsystem boundary. Although this is acceptable for them, the system FM designer has to allocate the subset of FM functions to that subsystem, and has to perform the full analysis using all the FM mechanisms, including those outside the subsystem boundary.

Finally, in the event of a major failure or loss of mission functionality, it may become important to a Failure Review Board (FRB) to distinguish between internal and external failures and assign responsibility for the resulting failure. For those failures whose cause is internal to or within the expected operating environment of the system, the system could potentially have been designed, implemented, or operated differently, and hence the system designers, builders, and operators (if part of the system) are likely responsible for faults that occur. However, for failures caused by unexpected conditions in the environment (e.g., the solar storm of the millennium or micrometeorite damage), it is possible that the design was done properly, and the mission just had bad luck in that the environment still caused failure. In either case, the careful documentation of the system boundary provides the FRB with the information required to understand the mission and its environment and can guide analysis of faults and failures and assignment of responsibility.

C.4.4 Function Preservation

a. **Statement of Principle:** Design FM to protect system functions when the risks of failure of that function are unacceptable. FM may be defined independently from known specific failure causes that can affect those functions.

b. **Commentary:** FM should be designed not only from the bottom up based on predicted failure modes (frequently identified in the FMEAs), but top-down based on an assessment of goals, objectives, and functions. A bottom-up design will often result in a complicated, incomplete, and potentially fragmented FM design.

Where the risks of failure for a function are unacceptable, FM is deployed to preserve or recover that function, or to select a new goal that does not require the failed function. To do this, identify functions that support mission goals, and analyze them to determine if the risk of failure of this function, given the system design for that function, is consistent with the project's defined risk posture. Deploy FM to improve the dependability of that function or to change the goal to an acceptable, achievable objective. In general, risks to functions are mitigated by one of five of the following strategies: Design-time fault avoidance; operational failure avoidance; failure masking; failure recovery; or goal change.

The FM design has to account for incomplete human understanding of the system's failure behavior, and for large uncertainties in probabilistic estimates, for failures of complex systems even when, or particularly when, these uncertainties have not been estimated. Humans can and do create systems beyond their full capability to understand. Aerospace systems exhibit this kind of complexity due to their disciplinary depth, large number of components, heterogeneity, and behavioral interactivity. It is impossible to know if all possible failure modes have been identified for systems of even moderate complexity.

Most FM mechanisms are designed against explicit, known failure causes, but the inherent incompleteness of knowledge implies that that some FM functions have to be deployed to protect system functions, independent of known specific failure causes that can affect those functions. These act as a "safety net" against non-predicted failure causes. Because these causes are not known, the FM designer can only be sure that the FM function will detect a problem affecting function, but cannot be certain that the corresponding responses will be fast enough to respond effectively in all cases. Detection capability is nearly assured because detection functions only need to detect deviation from nominal behavior without any knowledge of how that deviation occurred. However, analysis of the effectiveness of the failure response mechanisms implies the need to assess the race condition of the response versus the failure effects, and the failure effects cannot be known with certainty unless the causal mechanisms are understood.

Pitfall: ***Random Part Failure Bias.*** *Assessments of databases that trace failures to causes indicate that the percentage of system failures attributable to human faults is quite high, approximately 80-90 percent. The FM designer should not bias the design to focus on "hardware random part failure," but has to ensure that the full scope of the FM functionality includes software design and operational faults, since these are also likely causes of failure.*

C.4.5 Asset Preservation

a. **Statement of Principle:** Design and operate FM to preserve system assets when the risks of loss of that asset are unacceptable with respect to the goals of the mission. As with preservation of functions, FM may be defined independently from known specific failure causes that can affect the system mechanisms and assets.

b. **Commentary:** This principle is a corollary to, or sub-principle of function preservation, but is important enough to call out separately. For the system to achieve its goals and objectives, it has to perform required functions, and in turn, these required functions are assigned to specific assets. Assets span the hardware, software, and people, but also include entities such as power and expendables, e.g., propellant. In general, to preserve system function, one has to preserve its assets. To determine the proper strategy for preserving assets, the FM practitioner should refer back to the system's overall goals and objectives, the mission's risk posture, and the functions that have to be performed to achieve them.

For example, it is appropriate in many emergencies for the system to abandon some of its current functions to preserve assets for the long run. Spacecraft safing is the most important example. During cruise phase of a planetary mission, it is acceptable to abandon some current functions while preserving those functions that protect the vehicle and its assets by shedding loads, stopping the current mission activity, reducing functions to the very smallest and simplest set to enable pointing back to Earth so that mission operators can diagnose the fault and recover from the failure. This can be done because those stopped functions typically are not crucial to the long-term mission goal, in comparison to preserving mechanisms and assets for when they are needed in the science-gathering phase of the mission. The functions are restarted upon failure recovery and then are available at the appropriate mission time.

C.4.6 Risk Reduction

a. **Statement of Principle:** The FM implementation should always increase the reliability and safety of a system.

b. **Commentary:** FM is a tool used to reduce or manage overall mission risk. As such FM should deploy highly reliable and effective mechanisms that can be shown to reduce the overall mission risk, even though FM inherently adds more physical and logical mechanisms and hence potentially more failure modes and paths.

In the zeal to preserve functionality and assets, it is easy for the FM practitioner to be caught in a spiral of trying to protect the protection. Even the most simplistic case, where in the process of detecting and responding to a fault the FM design introduces an alternate fault path, the FM practitioner may be doing nothing more than increasing the overall complexity of the system. Each FM detection/response should be carefully evaluated to ensure it does not increase the risk posture of the mission, and that the benefit of the preservation of function or assets outweighs the increase in system complexity.

C.4.7 Design Mechanism Allocation

a. **Statement of Principle:** Allocate FM functions to the appropriate design mechanism types, including hardware, software, operations, or any combination thereof, keeping in mind the complexity of the evolving FM system and the risk posture and resource constraints for the mission.

b. **Commentary:** FM is often conceived as a purely software function. However, it can be (and often is) partly implemented in hardware design or as an operational procedure. Design mechanisms often, though not always, implement several FM functions simultaneously, such as fault isolation and identification, or failure detection and recovery. For example, propulsion systems sometimes have series-parallel valve combinations that detect, isolate, and respond to failures without any software or human intervention. In other cases, failures are detected, isolated, and recovered from exclusively by humans, with software only providing the base information for detection and executing human-specified commands to mitigate the failure. FM has to be allocated, designed, analyzed, verified, and validated in ways that cross specific implementation types. This means that FM should be organized as a set of system tasks and functions, and not merely in a disciplinary or subsystem fashion.

C.4.8 Tailoring Redundancy

a. **Statement of Principle:** Mission attributes drive the use of redundancy.

b. **Commentary:** Tailor redundancy (hardware, functional, or informational redundancy) to the specific needs of the mission. Hardware redundancy is not appropriate for all failure modes and all mission types. Informational redundancy may add unnecessary complexity for some missions. Consider needed recovery time, failure response strategies, failure containment architecture, system engineering margins (e.g., mass and power), and mission impacts of function outages and latencies associated with the redundancy architecture. When

modeling the FM implementation, show all redundancy mechanisms against specific classes of faults and/or failures.

FM implementations cannot be fully represented, analyzed, or understood unless all of the redundancy is represented, whether human operators, software algorithms, or hardware implementations. Human operators are often considered separate from the system, but if they are expected to perform an FM function for the system, including providing functional or informational redundancy, they are part of the system. When information redundancy is required, independent sources of knowledge may have inherently different uncertainties. FM designers should understand the consequences of these differences, and, when appropriate, model and account for the differences as part of the fault/failure detection or response.

APPENDIX D: CONTENT GUIDE FOR MANAGEMENT STRUCTURE

D.1 Purpose and/or Scope

The purpose of this appendix is to provide guidance in organizing a program/project to support successful FM design, development, testing and operations.

D.2. ORGANIZATION, ROLES, AND RESPONSIBILITIES

In the development of a flight system, responsibilities for various system elements—including FM are delegated to different project elements, organizations, and institutions. The design criteria and implications of FM cut across system elements and engineering disciplines (see section 4.3.1). Thus, in practice, FM requires coordination of multiple project elements and necessitates a clear definition of the roles, responsibilities, and interfaces of contributing organizations. Proper organizational roles and structure are needed to ensure efficient and well-understood programmatic interfaces, which in turn facilitate the development of robust and effective FM. Misunderstandings of programmatic interfaces, inadequate management structure, or insensitivity to institutional differences, contribute to substandard FM, for example, as in the following: First, gaps in fault and failure coverage; second, design defect discovery delayed until system integration; third, cost and schedule overruns; and fourth, increased safety risks.

The development of adequate and effective FM requires the coordination of engineering, S&MA, and operations organizations. Each organization has a specific role and brings specific expertise to the development of a robust and safe system. The organization(s) responsible for FM development should have cognizance over all system elements that perform FM functions, and should interface with other FM-related organizations (e.g., integration and test (I&T), S&MA). If the responsible organization has cognizance over only a subset, then there are increased risks of gaps and inconsistencies in the overall FM methodology and design.[24] These risks are greater when program and project organizations are distributed amongst different institutions.

Section 5.1 discusses recommended FM technical interfaces to establish in programmatic organization structures. Section 5.2 describes recommended FM roles and responsibilities within a project.

D.2.1 Programmatic Interfaces and Organizational Structure

[24] Unfortunately, responsibility for FM is typically diffused throughout multiple project elements and organizations. For example, some projects delegate FM to existing system engineers who have to balance this additional duty with their other nominal systems engineering activities—usually to FM's detriment. Other projects delegate FM to a separate engineering team (sometimes as a distinct subsystem). This project structure results in greater attention to issues of FM but runs the risk of isolating FM from the overall systems engineering effort. Still other projects delegate to subsystems without systems-level, engineering-led coordination. In most NASA projects, there is no single project-level system engineer with responsibility and authority over FM.

FM is a crosscutting discipline requiring a system-level view, and as such, should be positioned at the system level within program/project organization structures.[25] FM relies on hardware architecture and implementation, software algorithms, operational constraints and procedures, and S&MA inputs and feedback. For this reason, FM cannot be treated as residing within a single subsystem or functional component. While certain FM functions may be allocated to hardware, software, mechanisms, or operations, the overall FM approach and organizational topology should be directed from and coordinated at the system level. FM has to drive system design to ensure that FM is integral to the architecture with no gaps or inconsistencies.

To ensure adequate FM, an organizational structure that enables and promotes integration of FM processes across the entire program/project, with clear lines of communication between and allocation of roles and responsibilities across SE, FM, and the various subsystem disciplines should be defined. Furthermore, FM development cost and schedule as a formal engineering discipline should be estimated and tracked.

Pitfall: ***Poor integration of FM with SE leads to inadequate oversight.*** *When SE has no appreciable role in FM, there is a greater risk that FM will be an afterthought and that system-level reviews will overlook critical FM issues; this is exacerbated by the lack of an identified technical authority for FM. Even when SE is engaged in FM, there is still risk of inadequate oversight because FM design maturity depends on subsystem and component design maturity, which causes FM reviews to lag the pacing of system review milestones.*

Figure 13, Example Organization of FM Roles within a Program Structure, shows an idealized organization of FM roles within a generic tightly coupled or large single-project program (or system of systems) structure. The organization is hierarchical, with roles and responsibilities allocated among identified organizational elements. Figure 14, Example Organization of FM Roles within a Project Structure, elaborates the organization of FM roles in the project structure of a typical robotic mission.

[25] FM requires detailed knowledge of subsystem and component design (bottom-up knowledge; e.g., for failure analysis and failure detection design) as well as knowledge of overall system design and operational concept (top-down knowledge). Thus, there is a degree of confusion within projects—and a lack of consensus across institutions and projects—about where responsibility for FM ought to reside in a project's organizational structure.

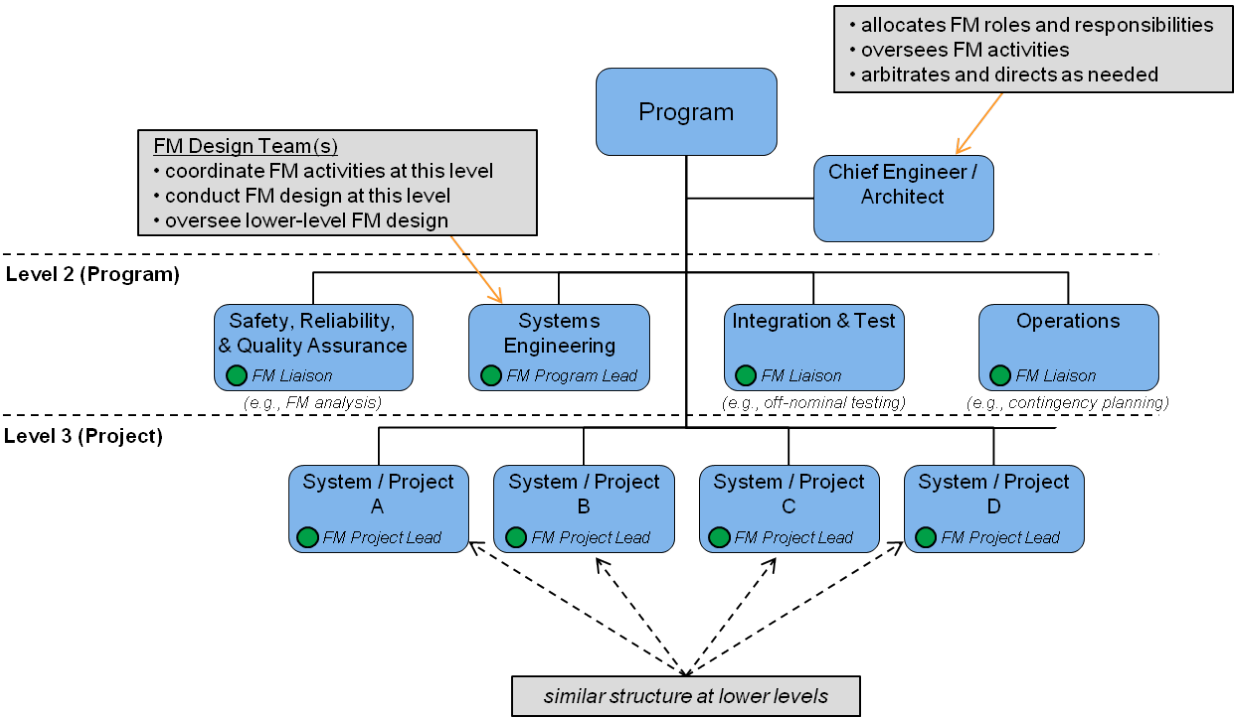

Figure 13—Example Organization of FM Roles Within a Program Structure

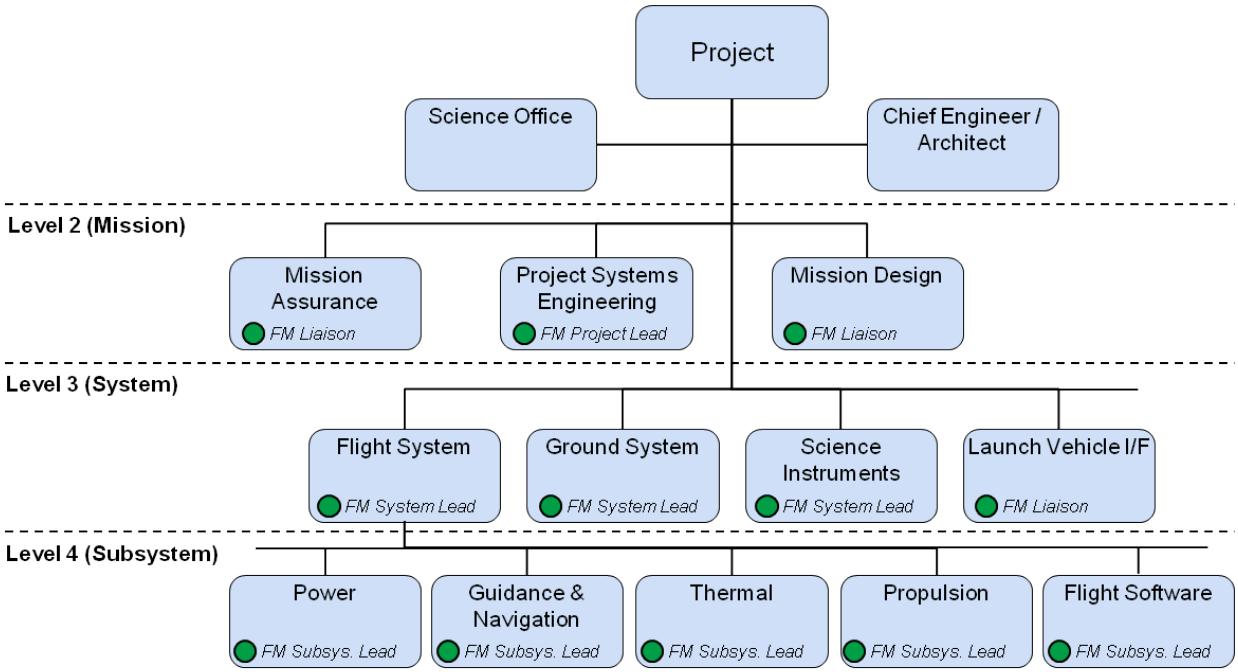

Figure 14—Example Organization of FM Roles Within a Project Structure

Implementation of FM is distributed across various deployments and system elements, e.g., flight and ground segments, hardware, software, and operations. Like SE, FM practitioners need

visibility into the nominal functionality of the entire system, in order to identify and plan for potential failures. In addition, FM can force trades at various levels and across multiple subsystems. Therefore, mission-development organizational structures and delegations of roles, responsibilities, and authority have to allow trades to be clearly communicated and resolved across traditional subsystem and engineering disciplines.

In the organizational structures illustrated above, FM responsibilities are defined and organized as a subset of SE responsibilities at each level in the organization. This ensures the appropriate scope for development and allocation of FM functions. Typical SE roles and responsibilities are performed with respect to FM by a hierarchical team of engineers specifically focused on FM, led by a project FM lead engineer. For a system-of-systems program, a program lead engineer coordinates FM work with the level 3 FM lead engineers, and between other level 2 organizations. The level 3 FM lead engineers perform similar coordination and design activities; each FM lead engineer has cognizance and authority to assess and allocate FM functions to project, system, or subsystem elements (depending on the level in the program hierarchy). The appropriate level of management resolves conflicts between peer organizations; e.g., in the case of level 2 organizations, either the program manager or the chief engineer resolves conflicts.

Recommended Practice: ***Identify FM as a standard engineering element of the system development process (e.g., separate work breakdown structure under SE); this will promote realistic estimates and measurements of complexity, cost, and schedule.*** *A historical collection of FM-engineering performance measures (e.g., cost, schedule) is needed for realistic future performance estimates.*

Recommended Practice: ***Establish a process to train personnel to be FM engineers.***

The following three properties are observed of the organization structures illustrated in figures 13 and 14, and are recommended for future mission-development organizations.

- FM is acknowledged as needing system-level perspective and requiring activities within engineering, S&MA, and operations.
- A team (or set of teams) is identified within the engineering organization as the focal point for FM analysis, design, and V&V.
- A team, board, or panel at an appropriate level is identified as the organization responsible for coordinating different areas of concern related to FM. At each level in the program organization, this team resides at a point in the hierarchy that has cognizance over engineering, S&MA, and operations activities (e.g., the Chief Engineer's Office).

The three observed properties reflect three principles for success in an organization, as follows: First, the organization's authority should match the scope of its responsibility or area of concern; second, the organization should have vertical structure and interfaces; and third, the organization should have horizontal integration with other interdependent organizations. These aspects are further described in the sections that follow.

D.2.1.1 An Organization's Authority

An organization's authority should match the scope of its responsibility or area of concern. For the organization responsible for FM, this means that its authority should include the set of possible system elements to which FM functions may be allocated, and cover all categories of possible design solutions. The team(s) responsible for FM functionality at each level in the organization should have cognizance over all aspects of FM allocation and design solutions, to prevent gaps, conflicts, and inconsistencies in the performance of FM. If there are multiple FM teams, these teams should be well coordinated, with formal interfaces and descriptions of roles and responsibilities.

Recommended Practice: ***Give the FM organization adequate budgetary and resource authority to effectively coordinate, design, and implement FM.***

Recommended Practice: ***Allocate FM resources and staffing early, with appropriate schedule, scope, and resource allocation and prioritization.***

D.2.1.2 Vertical Structure and Interfaces of an Organization

An organization should have vertical structure and interfaces. These interfaces should extend to organizations with similar responsibilities or areas of concern at both higher and lower levels in the program structure. Communication and coordination between organizations is typically achieved through leadership teams at each level (e.g., design teams to communicate and coordinate design), where each leadership team includes representatives from higher and lower levels. With respect to FM design and development, FM design teams should be formed to deal with issues at each level and these teams should have representatives from higher and lower levels (e.g., system representatives participating in subsystem design teams and subsystem representatives participating in the system FM design team). Without these teams, FM issues bubbling up from lower levels or flowing down from higher levels have no obvious forum for resolution—this can result in inconsistent issue resolution, ignorance of identified concerns, and ultimately gaps, overlaps, and inconsistencies in the practice and realization of FM.

Lesson Learned: ***Interactions with subsystem and S&MA engineers are paramount to assessing potential system failures and defining FM requirements.*** *In identifying and developing mission failure modes, some institutions tend to use a combination of FM failure analyses, safety, reliability, and mission assurance analyses, and subsystem engineer interviews. Other institutions use heritage failure modes updated with subsystem interviews, with some use of failure modes and effects analyses when available. A cavalier attitude toward the assessment of potential system failures (or toward specifying the scope and behavior of FM) does not to lead to success. For example, one project took a loose approach to the definition of the FM portion of the flight system—relying heavily on software architecture with no specific FM requirements, fault set, or definition of system behavior—and found that the resulting system had too many flaws to be operable. Moreover, the lack of system requirements to verify meant that small flaws were discovered too late when testing was more expensive and corrective action was more disruptive. Since many failures are caused by interactions of several component faults (where the components could be hardware, software, or people/procedures), or are created by the interaction of several components, each of which alone appears "fault-free," a purely bottom-up*

or heritage component-based assessment will miss a significant fraction of the most dangerous faults. Top-down and bottom-up assessments involving subsystem, system, S&MA and operations engineers, combined with "middle out" approaches by FM engineers (such as directed graph analysis and event-sequence-based failure scenario analyses), are all needed.

D.2.1.3 An Organization and Horizontal Integration with Other Interdependent Organizations

An organization should have horizontal integration with other interdependent organizations. Within a given program level, whether it be project, system, subsystem, or element, there are parallel organizations with dissimilar yet related responsibilities or areas of concern. These organizations should have identified roles and responsibilities, and formally documented interfaces between them to avoid overlaps and gaps. There should also be a coordinating organization at each level to mediate the distribution of responsibilities and interfaces, and to resolve issues between organizations. From a FM perspective, SE processes (e.g., requirements analysis and specification, design) should define the required nominal and off-nominal system capabilities, and the threats to these capabilities. The organizations responsible for these capabilities and functions should interface with the FM design organization(s). In addition, there should be a coordinating team or organization with authority over all aspects of FM—for example, this could be a system board or panel (for system issues). This coordinating organization should have cognizance over all aspects of FM, not just a subset—for example, there has to be a way to resolve conflicts that may arise between related teams working in a given level (e.g., teams responsible for engineering, V&V, integration and testing, safety and mission assurance, and operations).

Pitfall: ***Lack of clearly defined relationships and binding processes between FM and other independent organizations causes problems in FM design, implementation, and validation.*** *In particular, a poorly defined relationship with, or the late involvement of S&MA in FM development, has resulted in significant cost and schedule impacts and, in some cases, resulted in an inadequate FM design.*

The previous principles and suggested program/project organization structures are intended to recognize and promote FM as a system-level activity to be engineered in parallel with the nominal design.[26]

Pitfall: ***Inadequate, system-level consideration of FM during early project phases often causes unplanned cost and schedule growth during project development.*** *Project schedules often aim toward the most compact and compressed means to perform the range of functions needed to engineer, build, and test the intended system. Similarly, plans for V&V tend to represent a concise and fixed schedule that assumes everything will proceed successfully, accommodating anomalies and failures in system design and in the V&V process through overall schedule margin. However, by design, tests should push the system toward failure to see how it responds, which increases the likelihood of anomalies and uncovers design mistakes. In addition, system-level I&T is the best opportunity to understand and characterize how the system*

[26] Fesq, Lorraine (ed). NASA White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate, Pasadena, CA: NASA Jet Propulsion Laboratory. 2009.

operates as a whole. Therefore, this phase of the project lifecycle ought to be a primary recipient of resources, schedule, and staffing. Unfortunately, because the phase is late in the lifecycle, projects often "cut corners" to decrease resource and schedule consumption. Inadequate consideration of FM during project planning and early development phases contributes to insufficient V&V test plan coverage and resources; correcting deficiencies in FM test coverage drives, in part, late lifecycle cost and schedule growth. For example, one project allocated and planned for a constant FM staffing level of 0.5 full-time equivalents (FTE). In actuality, the project's FM staffing level peaked at more than 14 FTEs during system-level I&T (see figure 15, Unplanned "Bump" in FM Staffing Observed on Recent Missions).

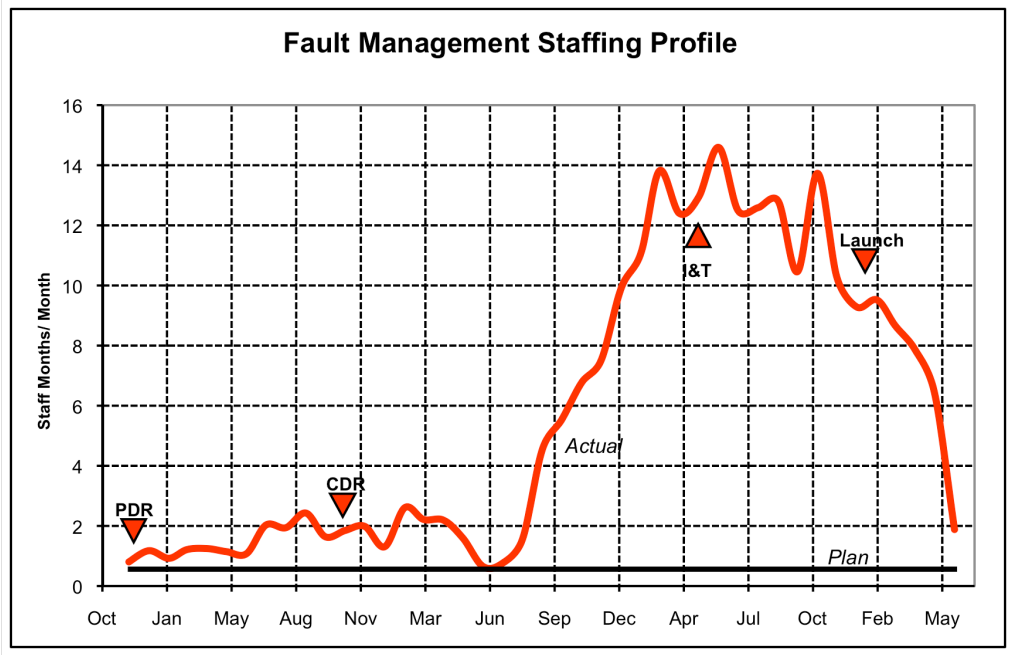

Figure 15—Unplanned "Bump" in FM Staffing Observed on Recent Missions

Discrepancies of similar magnitude between planned and actual FM staffing requirements have been observed on a number of NASA projects.[27] *This unplanned demand for increased staffing impacts budget, increases schedule risk, and introduces logistical and efficiency challenges—specifically, by burdening existing staff with the training of new staff.*

D.2.2 Project Fault Management Roles and Responsibilities

Within a project, the FM lead engineer is responsible for the cooperative design of flight and ground elements used to detect, contain, diagnose, and respond to anomalous and failure conditions within the system. The primary goal of the FM lead engineer is to reduce risks to mission and safety objectives within program resources and constraints; and by providing

[27] The generally observed pattern is that FM is initially viewed as a side responsibility of a single system engineer, increases to a full time responsibility as the mission progresses, and eventually requires an entire team to deal with problems, testing, launch, and early activation and checkout.

protection against potential faults/failures without designing an overly complex or cumbersome system. The responsibilities of the FM lead engineer include the following:

Programmatic:

- Be the team leader for the FM development function.
- Coordinate for the FM team interactions and interfaces between FM and other teams—e.g., SE, S&MA, and other subsystems.
- Represent FM in program reviews and in program-wide system design trades.
- Be responsible for roles, responsibilities, performance, and delivery of any sub-team FM lead engineers (see below).
- Write and/or oversee the generation and execution of the FM Development and Analysis Plan, the FM Verification and Validation Plan, and the FM Operations Plan (see section 6).
- Review hardware and software acquisitions.

Technical:

- Lead the architecture development, design evaluations, and trade studies necessary to develop the FM approach and overall mission concept of operations (ConOps).
- Apply FM-relevant institutional guidance, e.g., an institutional FM principles, process, and policies document.
- Participate in all system requirements and design activities (including subsystem trade studies) that affect the FM approach.
- Ensure completed analysis of potential faults and failures in the system.
- Ensure the preservation of flight system assets; i.e., ensure that safe mode is “safe” regardless of the fault, and that onboard, automated actions respond to off-nominal situations appropriately regardless of what caused the anomaly.
- Define the mission and system (and, occasionally, subsystem)-level requirements and capabilities necessary to implement the fault tolerance, detection, diagnosis, and recovery activities for the mission.
- Allocate the FM requirements to various ground and flight subsystems.
- Ensure completed design, implementation, testing and verification of the system features that satisfy the FM requirements across the multiple mission segments (e.g., flight and ground systems) and multiple spacecraft subsystems.

- Verify segment and subsystem compliance with FM requirements, including the review of test plans, procedures, and testbeds to ensure that the FM requirements will be thoroughly tested.

- Validate the overall system performance during off-nominal operations through the design, development, and execution of system-level scenario testing.

- Ensure adequate tools, processes, and techniques for use in the design, development, testing and operation of the FM system.

To accomplish the FM effort, a number of functional tasks have to be performed. Depending upon the size of the program and the scope of the FM effort, additional personnel may be needed to complete these tasks. These personnel can be grouped under the FM lead engineer or be on other teams depending on the project organization. Table 2, FM Functional Breakdown, identifies and describes the possible functional breakdown of the FM tasks. It is important to note that there is not necessarily a one-to-one correlation between tasks and personnel, as one person may be the technical leader of several tasks. In addition, each task may have one or more engineers supporting the effort.

Lesson Learned: ***(NASA Lessons Learned #1381) Mars Climate Orbiter (MCO).*** *"It is beneficial for a project to have a single point of contact (POC) whose job is continuously to ask the healthy question, 'What could possibly go wrong?' Formal analysis methods, such as FTA, FMEA, and FEPP analysis, should be employed in analyzing potential hazards and concerns."*

Table 2—FM Functional Breakdown

Functional Task	Description
Analysis	• Responsible for system- and subsystem-level failure analysis, e.g., hazards analysis, TTC analysis, failure scenario analysis, FEPP analysis. These analyses use and build on other component and subsystem analyses, e.g., PRA, FTA, FMEA.
Requirements	• Responsible for the development, allocation, and traceability of FM requirements.
Design	• Responsible for the FM design including active, onboard FM controllers (e.g., FM-specific flight software) and FM facets of the overall system's design (e.g., hardware redundancy).
Subsystem Coordination	• Responsible for oversight of subsystem development in accordance with FM requirements allocated to subsystems. • Responsible for ensuring that subsystem designs provide the capabilities and redundancy required to accomplish the FM objectives of fail-safe and fail-operational, where appropriate. • Provide programmatic and technical interface between system-level FM design and subsystem design and implementation. • Responsible for detecting inconsistencies between system-level design and subsystem design and implementation and providing recommendations to remedy inconsistencies at least cost and least risk to overall system. • Responsible for the development of onboard algorithms and logic that detects and responds to faults through the control of the overall vehicle configuration and component state. • Responsible for acceptance of FM-specific software.
V&V	• Responsible for the oversight of the V&V of FM requirements allocated to the subsystems and the V&V of FM system-level requirements through analysis of tests and development of tests reports. These activities are coordinated with test personnel and test managers (e.g., S&MA personnel).
Subsystem- and System-Level Test	• Responsible for subsystem- and system-level fault injection requirements, test planning, test procedure development, test execution, and test result analysis. • Responsible for requesting adequate tested resources and ensuring that adequate fidelity exists to perform V&V on the FM design.
Tool/Technology Development	• Responsible for the development of tools or new technology in support of the FM effort.
FM Operations	• Responsible for the oversight and/or development of nominal operational as well as contingency procedures, and the preparation and testing of these procedures for post-launch operations. • Responsible for identifying flight rules relevant to FM. • Responsible for FM-related activities during initial activation and checkout, including testing of safe-modes (if required).

APPENDIX E: WORK TEMPLATE

E.1 Purpose and/or Scope

The purpose of this appendix is to provide templates for the work products identified in this Handbook. These templates are presented as guidance for flight system missions.

[To be expanded in later releases]

APPENDIX F: RELEVANT NASA LESSONS LEARNED

F.1 PURPOSE

The purpose of this appendix is to provide a list of lessons learned that will guide FM practitioners and avoid repeating past lessons. The NASA Lessons Learned database[28] was mined for lessons relevant to FM. The lessons identified in this appendix were extracted from this database and are categorized to expose the higher level issues plaguing this field. All paragraphs in this appendix are direct quotes from the NASA Lessons Learned database.

F.2 FM LESSONS LEARNED CATEGORIES

F.2.1 Lack of Top-Down SE in FM Design Introduces Risk

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0345	Mars Observer Attitude Control Fault Protection	Description: From the analyses performed after the Mars Observer mission failure, it became apparent that the MO fault protection suffered from a lack of top-down system engineering design approach. Most fault protection was in the category of low-level redundancy management. It was also determined that the MO fault protection software was never tested on the flight spacecraft before launch. Design fault protection to detect and respond to excessive attitude control errors, use RCS Thrusters to control excessive attitude control errors, and always test fault protection software on the flight spacecraft before launch.	
1063	International Space Station (ISS) Program	Description: Lack of Systems Engineering in ISS Caution and Warning (C&W) System Design	Initiate a high-priority systems engineering review of the C&W

[28] NASA Lessons Learned Database: http://llis.nasa.gov/offices/oce/llis/home/

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
		LL: Although considerable progress has been made during past year in ISS C&W system design, systems engineering still not sufficiently evident in the whole spectrum of alarm and warning, situation assessment, and damage control and repair.	system to define a path for development and implementation of fully integrated alarm, situation assessment, countermeasure functions, and crew actions. Finalize and document C&W system design requirements.
1385	Comet Nucleus Tour (CONTOUR) Mishap Investigation:	LL II-2: Inadequate systems engineering process and specification of requirements. The board cited the fact that few requirements were imposed by NASA regarding the way contractors document or performed work on CONTOUR, creating opportunities for contractors to adopt nonstandard engineering practices.	
0369	Flight Software Deadly Embrace (Galileo)		#2: There should be a rigorous software verification and failure mode analysis conducted at the system level.

F.2.2 Projects Need a System-Level FM Engineer Who Continually Asks, "What could possibly go wrong?"

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
1381	ProSEDS Risk Review (MCO)	Description: Following the MCO mishap, the ProSEDS team decided to perform an in-depth review of the MCO mishap report to gather lessons learned and recommendations that could help prevent NASA from repeating past mistakes. LL 8: It is beneficial for a project to have a single point of contact whose job is to continuously ask the healthy question, "What could possibly go wrong?"	
0637	Wide-Field Explorer (WIRE) Mishap Investigation		#6: System and subsystem engineers should consistently evaluate functional designs and implementation to expose risk areas, particularly where multiple/complex interfaces exist. Projects with multiple components, i.e., spacecraft bus and a separate instrument, require complete team cooperation, openness, and the ability to penetrate and understand each other's design responsibilities in a timely manner.

F.2.3 A Rigorous Approach to FM with Experienced Designers is Key to a Successful Complex Mission

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
1743	Mitigating the Risk of Single String Spacecraft Architecture		Balance the risks of single string spacecraft architectures with effective risk management, ample fault tolerance, flight system flexibility, access to experienced designers, ample stress testing, use of proven designs, and a rigorous approach to fault protection.

F.2.4 Projects Need FM Related Reviews to Ensure FM Completeness, Consistency, and Minimum Risk

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0637	Wide-Field Explorer (WIRE) Mishap Investigation		#3: Peer reviews should be required by project management and held as often as necessary. #4: Peer reviews should consider the heritage capability and limitations of the support equipment to be used for testing the flight design. #5: Project review board members should consistently penetrate the system and subsystem functional design and

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
			implementation to expose risk areas, particularly where multiple/complex interfaces exist. Reviews should fully define spacecraft and payload interface requirements, and have a cognizant systems person from each program element review the other persons' test program and payload/spacecraft simulators for fidelity.
1385	Comet Nucleus Tour (CONTOUR) Mishap Investigation	LL Item II-1: Reliance of CONTOUR project on analysis by similarity. LL Item II-3: Inadequate review functions The board felt that inadequate oversight was especially dangerous in combination with nonstandard engineering practices.	#II-1: Projects should conduct inheritance reviews (i.e., analyses by similarity) early in the project lifecycle and should assure that the analysis properly evaluates the inherited item's capabilities and prior use against all mission-critical requirements.
1612 (HQ)	Cost Estimating: Assessing the Human Capital and Facilities Required for New Moon-Mars Missions	LL 2a: Bad habits (those contributing to failures) are not 'un-learned' if personnel are not involved in thorough postmortem reviews of failed projects.	#1a: The successes and failures of more recent missions, such as all the X-vehicle programs and planetary exploration missions (such as MER), should be reviewed. In particular, understanding the successes should be a priority.

F.2.5 FM Fault Responses Need to Handle All States; FM Fault Responses Should Not be Allowed to Interrupt Critical Activities

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0343	Mars Observer Inappropriate Fault Protection Response Following Contingency Mode Entry due to a Postulated Propulsion Subsystem Breach	Abstract: Following the loss of the Mars Observer spacecraft, simulations showed that a postulated propellant breach would have caused angular accelerations that could have inhibited downlink and caused multi-axis gyr saturation. In this case, fault protection features of flight software would have inhibited all momentum unloading and prevented the stabilization of the spacecraft. Ensure that fault protection takes proper action regardless of spacecraft state. Fault responses should not be allowed to interrupt critical activities.	

C.2.6 Fault Tolerance Requirements Should be Unambiguous

NASA Lesson #	Title	Description	Recommendation
1493	Ambiguous Fault Tolerance Requirements	CALIPSO Range Safety Regulations, NASA Safety Manual: Both documents [CALIPSO-Tailored Eastern and Western Range 127-1 Safety Regulations, Doc. TP2.LB.0.AQ.1836 ASC dated October 21-22, 2002; and NASA Procedural Requirement NPR-8715.3, "NASA Safety Manual"] contain sections related to fault tolerance requirements and there was debate over whether the fault tolerance requirements of either document were satisfied because of ambiguous wording. Even further, an unrelated but similar range safety document (ref. GSFC Wallops Flight Facility Range Safety Manual, RSM-2002) contained wording that seemed to conflict the GSFC engineering and safety offices' position. Fault tolerance requirements should be clearly defined in appropriate Agency-level design standards and variance accepted only when accompanied by appropriate risk trades and supporting technical rationale.	

F.2.7 Test Beds Need Flight Spare to Test Fault Scenarios and In-Flight Spacecraft Fault Recovery Procedures

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0284	In-Flight Spacecraft Fault Recovery) (Voyager 2)	Abstract: Voyager 2 suffered two potentially mission-catastrophic in-flight faults that were recoverable due to the availability of spare spacecraft hardware that was used to test workaround solutions. Maintain a functionally identical, properly configured, test bed of spare spacecraft hardware and associated support equipment, enabling detailed analysis of in-flight faults and candidate corrective actions. LL: The availability of spare spacecraft hardware and associated ground support equipment can mean the difference between restoring a lost spacecraft capability or flying with a reduced or lost capability due to the inability to adequately correct a fault.	

F.2.8 FM Operations Knowledge Should be Maximized, Procedures Should be Complete and Operations Complexity Should be Minimized for Minimum Operational Risk

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0664	SOHO Mission Interruption Joint NASA/ESA Investigation Board	Description: Loss of Contact with the Solar Heliospheric Observatory (SOHO) Spacecraft LL: The Board finds that the loss of the SOHO spacecraft was a direct result of operational errors, a failure to adequately monitor spacecraft status, and an erroneous decision which disabled part of the onboard autonomous failure detection. Further, following the occurrence of the emergency situation, the Board finds that insufficient time was taken by the operations team to fully assess the spacecraft status prior to initiating	

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
		recovery operations. The Board discovered that a number of factors contributed to the circumstances that allowed the direct causes to occur." FACTORS INDIRECTLY CONTRIBUTING TO THE FAILURE: 1. Ground Procedures (failure to control change; failure to perform risk analysis of a modified procedure set; Failure to communicate change). 2. Procedure Implementation (failure to properly respect autonomous Safe Mode triggers; Failure to follow the operations script; failure to evaluate primary and ancillary data; failure to question telemetry discrepancies). 3. Management Structure and Process (Failure to recognize risk caused by operations team overload; failure to recognize shortcomings in implementation of ESA/NASA agreements; emphasis on science return at expense of spacecraft safety; Over-reliance of flight operations teams on ESA and MMS representatives; dilution of observatory engineering support). 4. Ground Systems (Failure to resolve a critical deficiency report in a timely manner; failure to validate the planned sequence of events in advance)." [*Excerpt from core anomaly*]: Although the spacecraft remained Sun-pointing within nominal limits and was therefore in a power-positive and thermally-safe attitude, the state of the spacecraft was precarious at this point in time. It had an anomalous roll rate and was depending on a deactivated gyro for roll control in both ESR and ISA modes. The personnel on the ground were not aware of either of these facts at that	

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
		time. Gyro C was correctly configured to the ACU since the reconfiguration at ESR-5. Gyro B was active and on-line for fault detection, and it was correctly measuring the anomalous roll rate. A rapid decision was made that Gyro B was faulty because its output disagreed with the rate indicated by Gyro A. This decision led to the commanding off of Gyro B. During ESR-6 recovery, Ground Operations commanded the spacecraft to ISA mode. In ISA, the attitude control system resumed firing roll thrusters in an attempt to null the attitude error associated with the electrical rate bias term of the de-spun Gyro A. Gyro B and the associated fault detection were now inactive. The increasing roll rate eventually resulted in pitch and yaw Sun-pointing errors that exceeded a prescribed limit of five degrees, resulting in ESR-7 at 12:38 AM. Due to the gyroscopic cross-coupling torques caused by pitch and yaw thruster firings, and the absence of true roll rate indications, the ESR controller was no longer stable, and the spacecraft attitude diverged. The incorrect diagnosis of a Gyro B fault and the subsequent ground response to this diagnosis ultimately resulted in loss of attitude control, subsequent loss of telemetry, and loss of power and thermal control. Loss of telemetry occurred at 12:43:56 AM EDT, 6/25/98. At any time during the over five hour emergency situation, the verification of the spinning status of Gyro A would have precluded the mishap."	
0391	Galileo Spacecraft Safing Recovery Anomalies	Description: The Galileo mission twice experienced difficulties with recovery from safing errors due to a lack of a formal safing recovery plan and to software/documentation that had not been kept current on spacecraft states. Maintain and update an anomaly recovery plan, log spacecraft event updates, take care in reusing previously successful command packages, and identify nonstandard ground system configurations.	

F.2.9 FM Telemetry Should be Reviewed to Ensure Sufficient Visibility to Diagnose All Anomalies

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0560	Galileo Scan Platform Anomaly at Ida Encounter	LL 1: Establish "First, do no harm" as the overriding principle guiding both fault protection design and the ground response to in-flight anomalies. LL 2: Where it is not practical to record and downlink all telemetry, future missions should continuously buffer a small amount of high-rate telemetry as it is being down-linked at a lower rate. Should a fault occur, high-rate data for the period immediately preceding and following the fault could be stored for later retrieval. This would assist mission analysts in real-time diagnosis of the problem.	
1277	Ground Support Equipment (GSE) Fault Detection Robustness	Description: A critical cable connection fault was not observed during final checkout at the pad, due to insufficient flags in the ground support equipment. The problem resulted in a loss of a prime side instrument. LL: Important faults can be missed, if the GSE does not flag them to the operator.	A review of fault detection settings and telemetry in ground support and flight operations equipment should be incorporated into peer reviews.

F.10 FM Parameters/Configuration for Mission Events Should have Extra Scrutiny to Minimize the Risk of False Trips and Mission Failure

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0422	Particles Generated by Pyrotechnic Events (1967/76) (Viking Orbiter)	LL: Always take the precaution of placing the spacecraft in roll inertial and disabling any Canopus-loss fault protection software at and following a pyrotechnic event. At these times particles are shocked loose from parts of the spacecraft, from whence they drift through the Canopus tracker field of view.	Provide at least an hour's protection period following these events before returning the spacecraft to normal roll control. Bright objects resulting from a pyro event may also adversely affect other devices such as science instruments. A one-hour delay in operating these devices should be considered.

F.2.11 Mission-Critical Events Should have Extra FM Scrutiny and Hardware/Software Robustness to Minimize the Risk of Mission Failure

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0637	WIRE Mishap Investigation		#1: Independent, separate pyro inhibits should be considered for mission-critical events, particularly if all pyro functions can be simultaneously armed and enabled. Hence, activation of a pyro event would require two separate actions—one separate action to enable the inhibit and another to fire the pyros. This approach would preclude spurious transient pyro firings during turn-on and preclude sympathetic firings induced by sneak path and/or crosstalk/magnetic field

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
			interactions that may occur in cabling.

F.2.12 Verify all Redundancy Combinations to Ensure FM Testing is Complete

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0939	MPL Uplink Loss Timer Software/Test Errors (1998)	Abstract: Prelaunch tests and verification of software and hardware used to switch to a redundant string should include assumed failures in either string during all mission phases. MPL did not verify the ability of the Lander to switch to the redundant uplink string after landing assuming a failure in the primary string had occurred during earlier entry, descent and landing phases. Post mission testing of the uplink loss timer function demonstrated that an undetected logic error prevented the reconfiguration from the failed uplink hardware string to the backup string. Recognize that transitions to another mission phase are high-risk sequences and that database changes that impact logic decisions should be retested.	
0637	WIRE Mishap Investigation		#2: Testing only for correct functional behavior should be augmented with a significant effort in testing for anomalous behavior, especially during initial turn-on and power-on reset conditions.

F.2.13 FM Hardware Keep-out Zones Should be Understood and Embedded in Software to Avoid Hardware Damage and Error Conditions

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
2044	MRO Articulation Keep-Out Zone Anomaly	Abstract: An articulating solar array collided with the MRO spacecraft due to inadequate definition and verification/validation of system-level design requirements for implementing the appendage's keep-out zone in flight software. Mechanical resistance by the blanket caused motor rate errors that onboard fault protection interpreted as failure of both redundant gimbal motors, and fault protection commanded a warm reset of the flight computer and entry into safe mode. Construct models to ensure requirements discovery is complete, provide a robust appendage motion backstop capability, ensure precision in requirements language, and never ask control laws to exceed your control authority.	

F.2.14 Robustness and Reliability of Single Point Failure Items Should be Scrutinized to Minimize Risk, Especially with Late Design Changes

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0913	Space Mechanisms Reliability (JPL)	Abstract: Studies have shown that mechanical failures are more frequent and more likely to significantly affect mission success than are electronic failures. Spaceflight mechanisms are usually unique designs that lack the years of testing and usage common to electrical devices and in general cannot be designed with the same level of block of functional redundancy, or graceful degradation, common with electronic circuit design. The lesson provides a recommended checklist that contains 92 measures for enhancing the reliability, ease of fabrication, testability, maintainability, and robustness of mechanical designs.	

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0492	Galileo High Gain Antenna (HGA) Failure (1991)	Description: The Galileo spacecraft High Gain Antenna (HGA) was to open like an umbrella, but it never reached the fully deployed position. The failure was attributed to an inherited design of the rib retention mechanism. Recommendations involved the design of preloaded mechanisms, lubricant selection and use, hardware robustness, and fault tolerant design of one-shot, non-redundant, mechanisms. LL: Design changes intended to improve the reliability of inherited hardware may introduce new failure mechanisms. The mission impact of such design changes may best be understood through a 'physics of failure' approach to reliability analysis.	#3: Hardware should be inherently robust or redesigned to accommodate major changes in spacecraft system design, changes in spacecraft handling or the mission profile. Inheritance, design and peer reviews should fully consider the effect of such changes on known failure mechanisms. #4: One-shot, non-redundant, mechanisms should be designed for simplicity and fault tolerance—particularly where the mechanisms are preloaded prior to long-term storage, or where they endure extended periods under atmospheric and vacuum conditions prior to actuation."
0364	Galileo Retro Propulsion Module and Pyro Power System Interaction	Description: Galileo design optimizations over the years exacerbated interactions between spacecraft power and the propellant tanks. During the cruise phase, high power and heat dissipation near the propellant tanks combined with an enhanced tank load to increase the tank pressure. LL: Design of the various elements of a flight project (trajectories, science, mission operations, spacecraft design, spacecraft integration and test, etc.) is usually conducted in parallel. Although the designs are not	A thorough analysis should be conducted before changes are made to one or more of the flight project elements late in the development cycle where the test program is well advanced or actually may be completed for some of the elements. This analysis should be conducted in concert with designers of the other

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
		conducted independently, there are always subtle but significant interactions that can occur within one of the elements or between several elements.	elements. If discovered after changes are made, these interactions and couplings may (1) reduce the flexibility to make later changes necessary to recover from failures, or (2) negate the opportunity to enhance future science return, or (3) require complicated and costly operational workarounds.
0362	Magellan Radio Transmitter A Modulation Failure	Abstract: Loss of Magellan high rate X-band telemetry data was traced to moisture contamination due to a subcontractor's failure to use dry gas in the repackaging of an operational amplifier.	#1: Consider using a fault tree matrix during the design phase to identify critical telemetry parameters needed to analyze failures. #2: Match component screening and qualification to the mission, including any expected significant thermal cyclic excursions. #3: Minimize mission designed power cycling to reduce thermally induced stress. #4: Use of dry gas with moisture content below 5000 PPM in repackaging electronic components is a must.

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
1162	Space Shuttle Program	Description: SPF identification needs to take into account unit placement and proximity. LL: Redundant hydraulic lines for the three orbiter hydraulic systems are not adequately separated to preclude loss of all hydraulic power in the event of a single catastrophic failure of adjacent hardware.	Provide the same degree of separation of redundant critical hydraulic lines as is given to redundant critical electrical wiring.
0311	STS-56 High Rate Data Channel Failure Impact to ATMOS Experiment (payload high rate data failure)	LL 3: Functional redundancy is highly desirable for any single point failure subsystem. If functional redundancies for single point failure modes cannot be supplied, work-arounds should be established before the start of the mission.	

F.2.15 Flight Computers Should be Designed to Tolerate Errors Robustly

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
2041	MRO Spaceflight Computer Side Swap Anomalies [Export Version]	Abstract: A few months into its mission, MRO began experiencing unexpected side swaps to the redundant flight computer that placed the spacecraft into safe mode. The problem was traced to subtle inconsistencies between the MRO design implementation of an ASIC device and a known limitation of that device. Users of the RAD750 spaceflight computer should assure that the "PPCI Erratum 24" ASIC defect cannot cause excessive accumulation of uncorrectable SDRAM memory errors, and that the system architecture has robust error recovery capabilities. LL: The "Erratum 24" defect in the PPCI bridge ASIC represents a subtle failure mechanism for spacecraft employing a RAD750 SFC architecture that can be overcome by an operational workaround, but is best prevented through flight system design measures. LL: The ASIC defect can be overcome by an operational workaround, but is best prevented through flight system design measures. Specifically, processors need robust error checking, robust design measures for data salvage and should have a "clear-everything" capability for power on resets (PORs).	

F.2.16 Design out the Possibility of FM Software Deadly Embrace

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0369	Flight Software Deadly Embrace (Galileo)	Description: During a walk-through of the Galileo Spacecraft System fault protection implementation a possible "deadly embrace" in the flight software was uncovered. A deadly embrace is a continuous software looping operation that may preclude the achievement of an acceptable spacecraft state.	#1: A flight project should invoke a software policy that specifies that no single parameter error or single spacecraft malfunction can lead to a "deadly embrace" in the flight software. #2: There should be a rigorous software verification and failure mode analysis conducted at the system level. #3: One subsystem checking on another subsystem's functions should be used only when absolutely necessary. #4: "Try Again" responses may be undesirable unless a recovery mode is incorporated.

F.2.17 Always Use Watchdog Timers for Fault Robustness

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0559	Redundant Verification of Critical Command Timing (1995)	Abstract: When a new mission software release was uploaded to the spacecraft, the in-flight upload failed to include a software patch that had been written to fix a defective countdown timer. Because an independent "watchdog timer" was planned, but never implemented due to constrained project resources, the thrusters continued to fire after the desired shutdown time and the mission was terminated. Recommendations centered on the need for rigorous software configuration management, a watchdog timer to terminate operations, and test-bed verification of in-flight software updates. Description: Contributing Factors: 1. Inadequate Operational Configuration Management. The functions of configuration management and software performance analysis and repair lacked adequate staffing. 2. Inadequate Redundancy Design and Overflow Detection. Spacecraft hardware and software did not provide redundancy checking on the performance of software, such as fault protection monitors, to detect, diagnose and recover from an overflow condition. 3. Insufficient Processing Capability. The spacecraft computer was selected chiefly for its physical attributes— principally mass and radiation tolerance—rather than for its computational power. The decision to omit a watchdog timer was influenced by this hardware limitation. 4. Lack of Post-Launch Anomaly Analysis and Software Repair Capability. Only a single software development and simulation model was available for use by the flight project, and it was used continually after launch to generate flight sequences. This meant that the model was unavailable to generate software revisions to fix known bugs, so various software patches had to be uploaded throughout the mission.	

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation

F.2.18 Vehicle Interfaces Should be Subject to Failure Mode and Effects Analysis to Avoid Flight Hardware Damage

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0397	Viking Spacecraft Anomalous Power Turn-On	Description: While on the launch pad, Viking experienced an anomalous power turn-on that resulted in a total discharge of the spacecraft batteries. Failure analysis had not detected that discrete failure of a relay located in support equipment could have caused the problem. All interfaces with the spacecraft should be subject to failure mode analysis, status indicators or alarms should be used, and the spacecraft should not be left unattended unless periodic monitoring is conducted.	
0626	Inadvertent Powering of the Deep Space 2 Mars Microprobe (1998)	Description: During final assembly of the Deep Space 2 (DS2) Mars Microprobes, each of the two flight probes was inadvertently powered. The design of the mechanical switches was found to permit inadvertent ground paths during assembly, which could cause loss of mission due to undetected battery depletion prior to launch. System design must address hardware performance during assembly and test as well as during flight. Safing devices should be operational throughout assembly and test operations. Design analyses such as FMEA, SCA, and FTA must examine the electrical implications of mechanical/packaging design decisions.	
1529	Ensure Test	Abstract: When a GSE power meter registered zero due to an AC power	

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
	Monitoring Software Imposes Limits to Prevent Overtest (2003) (MRO)	glitch, the test monitoring and control software interpreted this as a loss of power and increased the test level past the maximum rating of the test article. This ground test error could have damaged flight hardware. Perform FMEA on test equipment to identify all potential GSE-induced failure modes. Either program the test control software or insert a limiting hardware device to prevent overtest.	

F.2.19 Do not Enable FM on Unused Components, Otherwise False FM Trips can Occur

NASA Lesson #	Title	Abstract/Description/Lessons Learned (LL)	Recommendation
0409	Voyager Gyro Swap During Launch Phase (1977)	Abstract: Because the Voyager failure protection logic was unnecessarily enabled during launch, transient gyro outputs triggered a series of alarming 'gyro swaps.' Careful attention should be given to preclude the possibility of spurious inputs triggering unwanted events when the protection logic is enabled. LL: It is suggested that failure protection logic be enabled only when the protected components or subsystems are required for spacecraft operation. Careful attention should be given to preclude the possibility of spurious inputs triggering unwanted events when the protection logic is enabled.	

APPENDIX G: ACKNOWLEDGMENTS

In 2008, the NASA Science Mission Directorate (SMD), Planetary Science Division, commissioned the first NASA FM Workshop[29] in response to a number of technical and programmatic issues surrounding FM experiences on recent missions. The workshop was h April 2008 in New Orleans, Louisiana. Although the workshop was to address a pattern of problems occurring across several planetary missions, the participants concluded that the challenges of adequate FM are present to a degree in all space missions. A primary recommendation from the workshop was the development of an FM Handbook that would benefit not only planetary missions but also all NASA missions. Both the NASA Chief En and the NASA Constellation Program Chief Architect endorsed the development of an FM Handbook.

The primary POCs for this Handbook are:

Lorraine Fesq, Jet Propulsion Laboratory, California Institute of Technology (JPL)
Neil Dennehy, NASA Goddard Space Flight Center (GSFC), NASA NESC Guidan Navigation, and Control Technical Fellow

The authors of this Handbook were:

Timothy Barth, NASA Kennedy Space Center and NESC Systems Engineering Off
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)
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
Jeffrey Zinchuk, Draper Laboratory

Reviewers for this Handbook were:

Michael Battaglia, NASA Headquarters, Office of the Chief Technologist
Brad Burt, Jet Propulsion Laboratory, California Institute of Technology
Tim Crumbley, NASA Marshall Space Flight Center, NESC Software Engineering Representative
Fernando Figueroa, NASA Stennis Space Center
Steve Hogan, The Aerospace Corporation
Brian Kantsiper, Johns Hopkins University, Applied Physics Laboratory

[29] Fesq, Lorraine (ed). *NASA White Paper Report: Spacecraft Fault Management Workshop Results for the Mission Directorate*, Pasadena, CA: NASA Jet Propulsion Laboratory. 2009.

Richard Larson, NASA Dryden Flight Research Center
Ken Lebsock, Orbital Sciences Corporation (GSFC Affiliate)
Steve Scott, NASA Goddard Space Flight Center

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.