The Development of NASA’s Fault Management Handbook

Science Mission Directorate

Lorraine Fesq, Handbook Team Lead
Jet Propulsion Laboratory, California Institute of Technology

2011 Flight Software Workshop
JHU/APL -- October 19-21, 2011
Agenda

- Historical Perspective
- Results of the 2008 Fault Management (FM) Workshop
- FM Handbook Goals, Scope and Contents
- Future Plans
- Acknowledgements
Recent FM Developments

2006-2008: FM causes cost overruns and schedule slips on multiple missions

Apr ’08: SMD/PSD sponsors S/C FM Workshop (J. Adams)

Mar ’09: FM Workshop White Paper published

Jul ’09: NASA OCE endorses white paper; directs to “Coalesce the field” (M. Ryschkewitsch)

Jul ’08: Constellation (CxP) identifies FM as potential risk; forms FM Assessment/Advisory Team (FMAAT) (B. Muirhead)

Dec ’09: CxP publishes FMAAT Position Papers addressing key FM issues

Jan’10: CxP establishes FM Team within Level 2 SE org (M. Goforth)

Apr ’10: NESC/SMD launch FM Handbook – robotic focus (L. Johnson/N. Dennehy)

Oct ’10: FM CoP established on OCE’s NEN website – nen.nasa.gov (L. Fesq)

Jul ’11: FM Handbook Version 1 delivered to NESC/SMD and NTSPSO

2011
SMD sponsored a workshop to uncover underlying causes of cost overruns on numerous missions

- Held April 14-16, 2008 in New Orleans, LA
- +100 attendees from 31 orgs – government, industry, academia
- Objective: Ameliorate schedule, cost and predictability challenges that occur when building, testing, and operating FM systems

- Goals: Document key findings, make recommendations for future missions
- Approach: Assemble key players in the spacecraft FM field across NASA, industry and other organizations, to
  - Capture current state of FM
  - Identify challenges associated with engineering/operating FM systems
  - Identify/describe issues underlying these challenges and propose steps to overcome/mitigate them
  - Discuss and document best practices and lessons learned in FM
  - Explore promising state-of-the-art technology and methodology solutions to identify potential investment targets.
2. Find a home for FM within Project organization

5. Establish FM Metrics

9. Establish and maintain mission-level risk req

11. Provide adequate testbed resources

6. Apply CPI to FM

7. Assess mission-level requirements on FM complexity

8. Assess if FM architecture is appropriate for Mission

10. Be skeptical of inheritance claims

1. FM should be “dyed into design” vs “painted on”

4. Identify FM representation techniques and FM design guidelines

3. Standardize FM Terminology

12. Capture and understand FM cultural differences Among aerospace organizations

[n] = Section in Handbook where Recommendation is addressed
Goal:
- Ameliorate schedule, cost and predictability challenges that often are faced when testing and operating FM systems
- Improve reliability and safety of NASA’s flight and ground systems
- Coalesce the FM field

Approach:
- Identify qualified team of FM practitioners and systems engineers
- Evaluate findings and recommendations from 2008 FM Workshop
  - Initial emphasis on foundational issues; e.g. establish common terminology
- Capitalize on existing material
  - ESMD’s Constellation Program’s Fault Management Assessment & Advisory Team’s (FMAAT) seven Position Papers and identified Risks
  - OCE’s FSW Complexity Task results (D. Dvorak)
  - Aerospace TOR: “Effective Fault Management Practices” (S. Hogan)
  - NASA’s Lessons Learned Database [http://llis.nasa.gov/offices/oce/llis/home/]
Co-funded by SMD and NESC (Neil Dennehy, GN&C Technical Fellow)

The envisioned users of the Handbook include:
- FM Practitioners
- FM Trainees
- Systems and Subsystems Engineers
- Mission Assurance/Reliability Leads
- Top Level Management and Program managers
- Proposal Evaluators

Outline is scoped to address needs of Agency – crewed and robotic missions

Robotic emphasis in Version 1, due to SMD co-funding

Suggested use as a “companion” to NASA Systems Engineering Handbook
NASA Handbooks vs Institutional Guidelines

Agency-level guidance and core concepts

Institutional-level practices and guidance

- JPL SE Field Guide
  - Section 313
  - GSFC Gold Rules
    - GSFC-STD-1000E

- NASA FM Handbook
  - HDBK_1002

- JPL Design Principles
  - DocID 43913

- JPL Flight Project Practices
  - DocID 58032

- JPL FP Historical Practices
  - 313-10-020 (Draft)

- APL FM Engineering Process
  - QY3-660

- JSC Computer-Based Control System Safety Requirements
  - SSP-50038B

- NASA SE Handbook
  - SP-2007-6105
Goal: To capture expertise across NASA and industry that would respond to needs identified in the FM Workshop Findings/Recommendations, for the benefit future missions.
<table>
<thead>
<tr>
<th>Section</th>
<th>%*</th>
<th>Summary</th>
<th>Accomplishments/Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Scope</td>
<td>90</td>
<td>What is FM? Relevance and Purpose; FM within NASA and institutional challenges; Structure of the Handbook; intended audience</td>
<td></td>
</tr>
<tr>
<td>2. Applicable Documents</td>
<td>100</td>
<td>List of documents sited in the text; approved documents</td>
<td></td>
</tr>
<tr>
<td>3. Acronyms and Definitions</td>
<td>90</td>
<td>Acronyms and abbreviations used throughout the document; Definitions of key FM terms</td>
<td>Team did not completely concur on definitions and concepts. Also, need to coordinate with OSMA (NASA-STD 8709.22) &amp; Aerospace/DoD</td>
</tr>
</tbody>
</table>

* Percent complete for Version 1 DRAFT. To develop a NASA-wide Handbook, all Sections need additional expertise/review, especially from HSF, GS/MS, Aeronautics and OSMA communities.
FM Domain

System Design

- Hardware Components
- Software Components
- Operations Components

Technical Assessment

- Hardware Components
- Software Components
- Operations Components

Technical requirements, design solution

nominal behavior

Failure Modes

nominal behavior

assessments results

nominal behavior

V&V

- Hardware Components
- Software Components
- Operations Components

V&V results

nominal behavior

failure effects

nominal behavior

nominal behavior

Failure Modes
<table>
<thead>
<tr>
<th>Section</th>
<th>%*</th>
<th>Summary</th>
<th>Accomplishments/Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.   Concepts and Guiding Principles</td>
<td>75</td>
<td>Fundamental concepts and guiding principles grounding the field -- FM functions, FM as part of SE, FM goals: asset and function preservation</td>
<td>Made some progress, but it was challenging to agree on terminology and guiding principles. This Section tended to generate lengthy academic/philosophical discussions. Still no unanimous agreement, and we expect more divergence before convergence, once we bring on additional practitioners and hear their definitions/viewpoints. But we now have a basic FM framework that we can use across NASA and with industry partners.</td>
</tr>
<tr>
<td>5.   Organization, Roles, and Responsibilities</td>
<td>75</td>
<td>Project organizational structure to support FM; interfaces; tasks</td>
<td>Fairly stable. Need to address different Mission classes (A, B, C, D).</td>
</tr>
<tr>
<td>6.   Process</td>
<td>90</td>
<td>Follows SE Process but focuses on FM products – Concept design, requirements, architecture, analysis, V&amp;V, Ops and Maintenance</td>
<td>Came together nicely, once we adopted NASA SE Process as foundation. Agreement at a high level; further discussions still required to mature details.</td>
</tr>
</tbody>
</table>

* Percent complete for Version 1 DRAFT. To develop a NASA-wide Handbook, all Sections need additional expertise/review, especially from HSF, GS/MS, Aeronautics and OSMA communities.
FA Process as Part of SE Process

Fault Management Development Process

Pre-Phase A: Concept Studies
Phase A: Concept & Tech Development
Phase B: Preliminary Design & Tech Completion
Phase C: Final Design & Fabrication
Phase D: System Assy. Integration, Test, & Launch
Phase E: Ops & Sustainment

Key
- FM Process
- FM Doc
- FM Interface
- FM Review

Outputs
- FM Concept Document
- FM Design Document
- FM Requirements Document

Requirements Development
[sections 4.2.2, 5]

Verification & Validation
[sections 4.2.5, 6]

Assessment & Analysis
[sections 4.2.4, 7]

Operations & Maintenance
[sections 4.2.6, 9]

Other Systems Engineering
- Mission Technical Concept
- Mission Requirements
- System Definition

FM Availability
- PRM:FMSSD7A
- Hazard Analysis
- Fault & Failure Containment Region Analysis
- Failure Response Analysis
- Design Requirements
- Risk Classification
- Trade Study Results

Subsystem
- Subsystem Requirements
- Subsystem Design

Operations
- Concept of Operations
- Contingency Procedures
<table>
<thead>
<tr>
<th>Section</th>
<th>%</th>
<th>Summary</th>
<th>Accomplishments &amp; Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Requirements Development</td>
<td>90</td>
<td>FM requirements categories; driving requirements; flow-down</td>
<td>Nice baseline identifying how to write FM requirements, with many examples and lessons learned provided. Currently deep-space-centric.</td>
</tr>
<tr>
<td>8. Design and Architecture</td>
<td>60</td>
<td>Impacts of mission risk posture, goals, characteristics and FM priorities; FM architectures, design features and approaches; mission-specific considerations</td>
<td>Hardest Section to write. It experienced many painful re-orgs/re-writes, so final version did not receive as much review as the other Sections. All practitioners know how to design, and agreed that it must be architected from the beginning since it permeates all levels of design; but no one approach is appropriate for all missions. Final incarnation in Version 1 expresses our realization that design is driven by mission requirements, and we then identified basic building blocks and guidance on how/when to use them. Open issues include establishing balance between distributed vs centralized, and between sub-system/low-level vs system-level. Trade space of mission characteristics and system design characteristics.</td>
</tr>
</tbody>
</table>

* Percent complete for Version 1 DRAFT. To develop a NASA-wide Handbook, all Sections need additional expertise/review, especially from HSF, GS/MS, Aeronautics and OSMA communities.
Mission Requirements Drive FM Design

**Mission Attributes**
- Mission Class
- Human-rated
- Hazards
- Cost/Risk

**Driving Requirements**

**FM Approaches & Features**
- System Architecture
- Reconfiguration Strategy
- Time to Detect/Masking
- Autonomous/Automated/Crew Coverage

**H/W Features**
- Simplex
- SCP
- Voting/Standby
- Fault Containment

**S/W Features**
- Operating System
- States/Modes
- Data Validation

Fail Op/Fail Safe
Time to criticality
Cost of Loss
Etc.
<table>
<thead>
<tr>
<th>Section</th>
<th>%</th>
<th>Summary</th>
<th>Accomplishments/Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Assessment and Analysis</td>
<td>0</td>
<td>To be expanded in later releases</td>
<td></td>
</tr>
<tr>
<td>10. Verification and Validation</td>
<td>75</td>
<td>Identifies FM V&amp;V planning/preparation; how to perform FM V&amp;V and analyze results; selection and prioritization of FM scenarios; simulators, test-beds and flight hardware testing</td>
<td>Fairly stable -- did not generate much controversy. Needs to address more Workshop Recommendations, like Design for Testability. Consider including Formal Methods.</td>
</tr>
<tr>
<td>11. Operations and Maintenance</td>
<td>0</td>
<td>To be expanded in later releases</td>
<td></td>
</tr>
</tbody>
</table>

* Percent complete for Version 1 DRAFT. To develop a NASA-wide Handbook, all Sections need additional expertise/review, especially from HSF, GS/MS, Aeronautics and OSMA communities.
<table>
<thead>
<tr>
<th>Section</th>
<th>%*</th>
<th>Summary</th>
<th>Accomplishments/Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Review and Evaluation</td>
<td>90</td>
<td>FM’s presence in major milestone reviews; recommended FM-focused reviews; entrance and success criteria; key questions to ask at FM reviews</td>
<td>Can be used stand-alone by any Review Team, for reviewing FM material at major milestone reviews and during FM-focused reviews. Need to scrub entrance/success criteria to make more FM-specific. Provide underlying mishap or motivation that led to questions.</td>
</tr>
<tr>
<td>13. Conclusion</td>
<td>0</td>
<td>To be expanded in future releases</td>
<td></td>
</tr>
<tr>
<td>14. Future Directions</td>
<td>0</td>
<td>Where this field is headed – new technology being developed that would offer technical solutions</td>
<td>Still debating if this Section should be included.</td>
</tr>
<tr>
<td>Section</td>
<td>%*</td>
<td>Summary</td>
<td>Accomplishments/Challenges</td>
</tr>
<tr>
<td>--------------------</td>
<td>----</td>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Appendix A</td>
<td>100</td>
<td>References</td>
<td></td>
</tr>
<tr>
<td>Appendix B</td>
<td>0</td>
<td>Work Product Templates (TBS)</td>
<td></td>
</tr>
<tr>
<td>Appendix C</td>
<td>95</td>
<td>Relevant NASA Lessons Learned</td>
<td>GSFC Gold Rules contain a number of FM-related rules. If these are based on Lessons Learned, capture them here. Suggest mining the Aerospace LL database.</td>
</tr>
<tr>
<td>Appendix D</td>
<td>100</td>
<td>Acknowledgements, historical background</td>
<td></td>
</tr>
</tbody>
</table>

* Percent complete for Version 1 DRAFT. To develop a NASA-wide Handbook, all Sections need additional expertise/review, especially from HSF, GS/MS, Aeronautics and OSMA communities.
### NTSPO Document Process

#### Propose
- **NESP**
  - NESP Lead at Center Initiates Development of Document (NESP4)
  - Form Topic Working Group (NESP5)
- **TWG**
  - TWG Coordinates Draft Document (TWG1)
- **NTSPO**
  - Issue Formal “GO” with Funds Centers (NTSP11) ≤1800 – 2500
  - OPRD/NTSPO Preparation/Revision (NTSP12) ≤300
  - Send Out for Agency Review (NTSP13) ≤420
  - Send to NTSPO to Initiate Agency Review (NESP6) ≤550
- **OCE/EMB**
  - OCE Approval (OCE3)
  - EMB Concur/Non-Concur (EMB1) ≤14
  - Chief Engineer Approval (OCE3) 210
  - Publish Standard (NTSP20) ≤50

#### Develop
- **NESP**
  - Form Topic Working Group (NESP5)
  - TWG Coordinates Draft Document (TWG1)
- **NTSPO**
  - OPRD/NTSPO Preparation/Revision (NTSP12) ≤300
  - Send Out for Agency Review (NTSP13) ≤420
  - Send to NTSPO to Initiate Agency Review (NESP6) ≤550
  - Issue Formal “GO” with Funds Centers (NTSP11) ≤1800 – 2500
- **OCE/EMB**
  - OCE Approval (OCE3)
  - EMB Concur/Non-Concur (EMB1) ≤14
  - Chief Engineer Approval (OCE3) 210
  - Publish Standard (NTSP20) ≤50

#### Ongoing Standards
- **Indicates Reported Milestone Action**
  - Milestone Event
  - Event Duration Estimate

<table>
<thead>
<tr>
<th>Milestone Event</th>
<th>Event Duration Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>210</td>
<td>28</td>
</tr>
<tr>
<td>210</td>
<td>8</td>
</tr>
<tr>
<td>210</td>
<td>1</td>
</tr>
<tr>
<td>210</td>
<td>1</td>
</tr>
<tr>
<td>210</td>
<td>1</td>
</tr>
</tbody>
</table>
   - Engage Human Spaceflight Programs, Mission/Ground Systems, Aeronautics, OSMA.
   - Address more Workshop Recommendations (e.g., representation techniques)
2. Hold another FM Workshop to focus on Solution Space – **SPRING 2012**!
3. Establish Agency-wide FM Board/WG/whatever to work through more Recommendations (e.g., FM architecture trade space, metrics)
4. Integrate/coordinate FM concepts with other organizations (e.g., DoD, NRO) and with other documents (e.g., NASA Systems Engineering Handbook, NPRs)
5. Training/Exposure -- e.g., NESC Brochure/Tech Update, Academy Online, JEO Workshop, NASA courses
6. Eventual standardization?
   - Update relevant NPRs to make FM requirements consistent, complete (Risk: 8705.4, R&M: 8725, PM: 7120.5E, SE: 7123.1A, SW: 7150.2)
   - Develop FM NPR (perhaps as a roadmap into FM items in other NPRs) or address as part of SE NPR
NASA Chief Engineer hosts Communities of Practice (~18 technical, 4 management) on NASA Engineering Network (NEN)

FM Community of Practice was established October 2010 on NEN website to coalesce the field
  - Provide a forum for subject matter experts, a library of collected FM material and a list of practitioners
  - nen.nasa.gov/web/faultmanagement
Final Thoughts

- Disciplined approach to FM has not always been emphasized by projects, contributing to major schedule and cost overruns
  - Often faults aren’t addressed until nominal spacecraft design is fairly stable
  - Design relegated to after-the-fact patchwork, Band-Aid approach

- FM Handbook will help ensure that future missions do not encounter same FM-related problems as previous missions
  - Version 1 of the FM Handbook is a good start.
  - Still need Version 2 Agency-wide FM Handbook to expand Handbook to other areas, especially crewed missions
  - Still need to reach out to other organizations to develop common understanding and vocabulary

- Handbook doesn’t/can’t address all Workshop recommendations. Still need to identify how to address programmatic and infrastructure issues.

- Progress is being made on a number of fronts outside of Handbook effort
  - Processes, Practices and Tools being developed at some Centers and Institutions
  - Management recognition – Constellation FM roles, Discovery/New Frontiers mission reviews
  - Potential Technology solutions – New approaches could avoid many current pitfalls
    - New FM architectures, including model-based approach integrated with NASA’s MBSE efforts
    - NASA Office of the Chief Technologist: FM identified in 7 of NASA’s 14 Space Technology Roadmaps – opportunity to coalesce and establish thrust area to progressively develop new FM techniques

Planning a 2nd NASA FM Workshop in Spring 2012, in New Orleans, LA. Look for announcements on the FM CoP Website!
Acknowledgements

Primary points of contact:
• Lorraine Fesq, Handbook Team Lead, JPL
• Neil Dennehy - Assessment Lead, NESC GN&C Tech Fellow

Authors:
• Timothy Barth, KSC, NESC Systems Engineering Office
• Micah Clark, JPL
• John Day, InSpace Systems (JPL Affiliate)
• Kristen Fretz, APL
• Kenneth Friberg, Friberg Autonomy (JPL Affiliate)
• Stephen Johnson, MSFC
• Philip Hattis, Draper Laboratory
• David McComas, GSFC
• Marilyn Newhouse, CSC (MSFC Affiliate)
• Kevin Melcher, GRC
• Eric Rice, JPL
• John West, Draper Laboratory
• Jeffrey Zinchuk, Draper Laboratory

Reviewers:
• Michael Aguilar, NESC Software Tech Fellow
• Michael Battaglia, NASA HQ, OCT
• Brad Burt, JPL
• Fernando Figueroa, SSC
• Steve Hogan, The Aerospace Corporation
• Brian Kantsiper, APL
• Richard Larson, NASA DFRC
• Ken Lebsock, OSC (GSFC Affiliate)
• Steve Scott, GSFC Chief Engineer