



The Development of NASA's Fault Management Handbook

Lorraine Fesq

Handbook Team Lead

Jet Propulsion Laboratory, California Institute of Technology

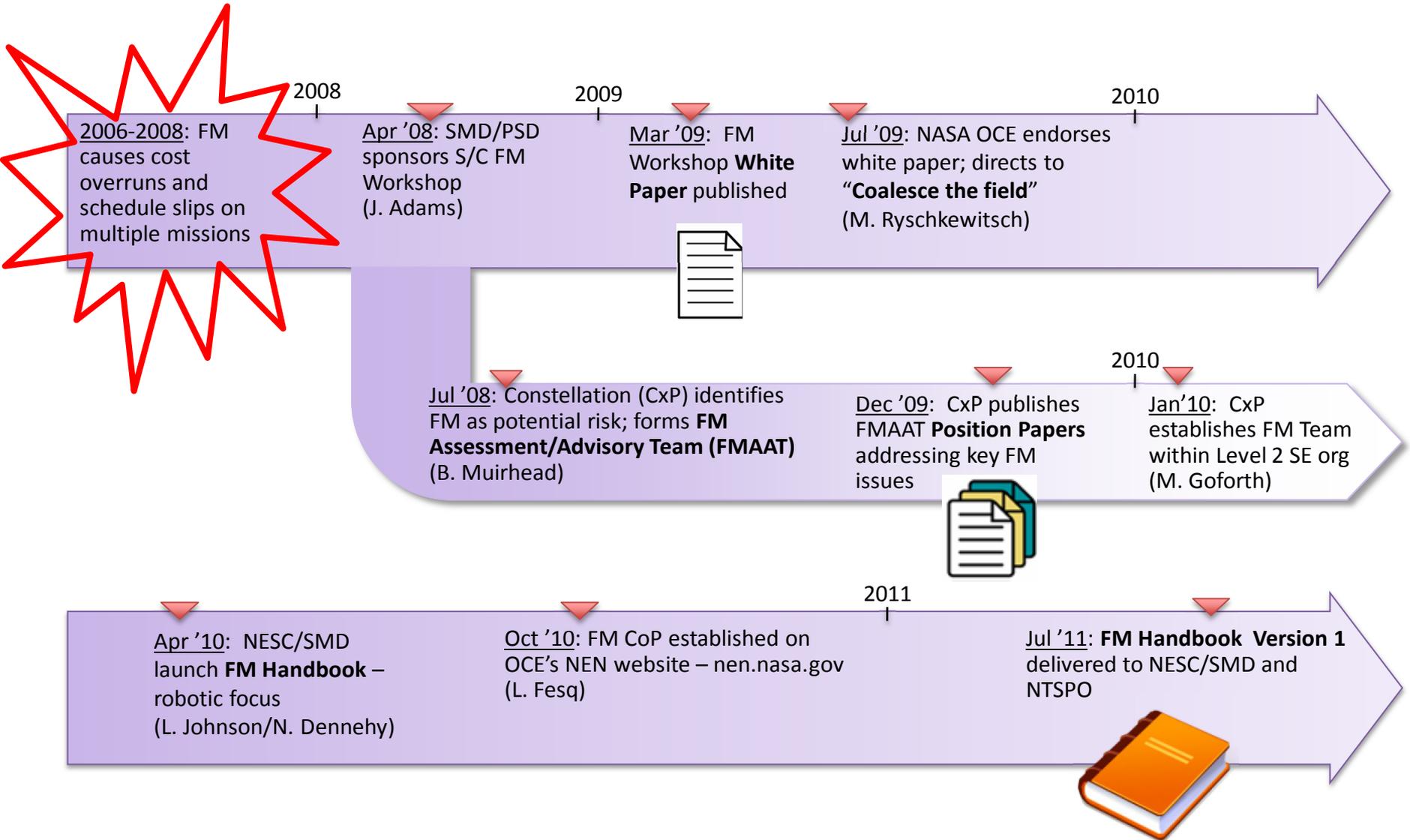
2011 Flight Software Workshop

JHU/APL

October 19-21, 2011

Copyright 2011 California Institute of Technology. Government sponsorship acknowledged. The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Recent Developments in FM

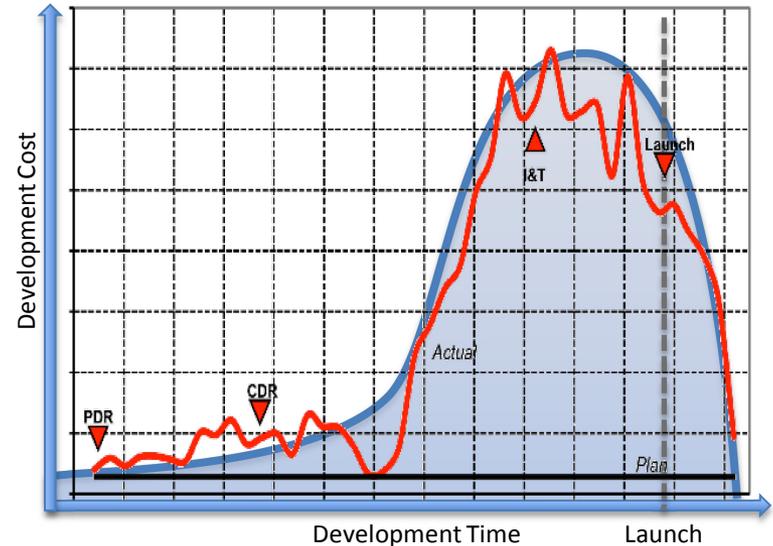


Fault Management Workshop



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 often are faced when building, testing, and operating FM systems
- Goals: Document key findings and 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.



FM Workshop Recommendations



[n] = Section in Handbook where Recommendation is addressed

2. Find a home for FM within Project organization

[5]

5. Establish FM Metrics

9. Establish and maintain mission-level risk req

11. Provide adequate testbed resources

[7,10]

6. Apply CPI to FM

7. Assess mission-level requirements on FM complexity

[7,8]

8. Assess if FM architecture is appropriate for Mission

[8]

10. Be skeptical of inheritance claims

[12]

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

[5,8]

4. Identify FM representation techniques and FM design guidelines

[8]

12. Capture and understand FM cultural differences Among aerospace organizations

3. Standardize FM Terminology

[3,4]

FM Handbook Goal and Approach



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/>

FM Handbook Scope

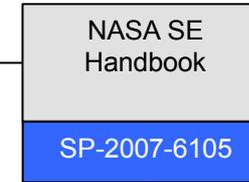
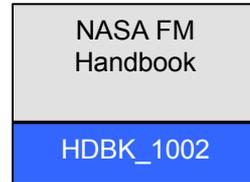


- **The envisioned users of the Handbook include:**
 - Top Level Management and Program managers
 - Systems and Subsystems Engineers
 - Mission Assurance/Reliability Leads
 - FM Practitioners
 - FM Trainees
 - Proposal Evaluators
- **Outline scoped to address needs of Agency – crewed and robotic missions**
- **Robotic emphasis in Version 1, due to SMD co-funding**
- **Suggested use as a “companion” to NASA Systems Engineering Handbook**

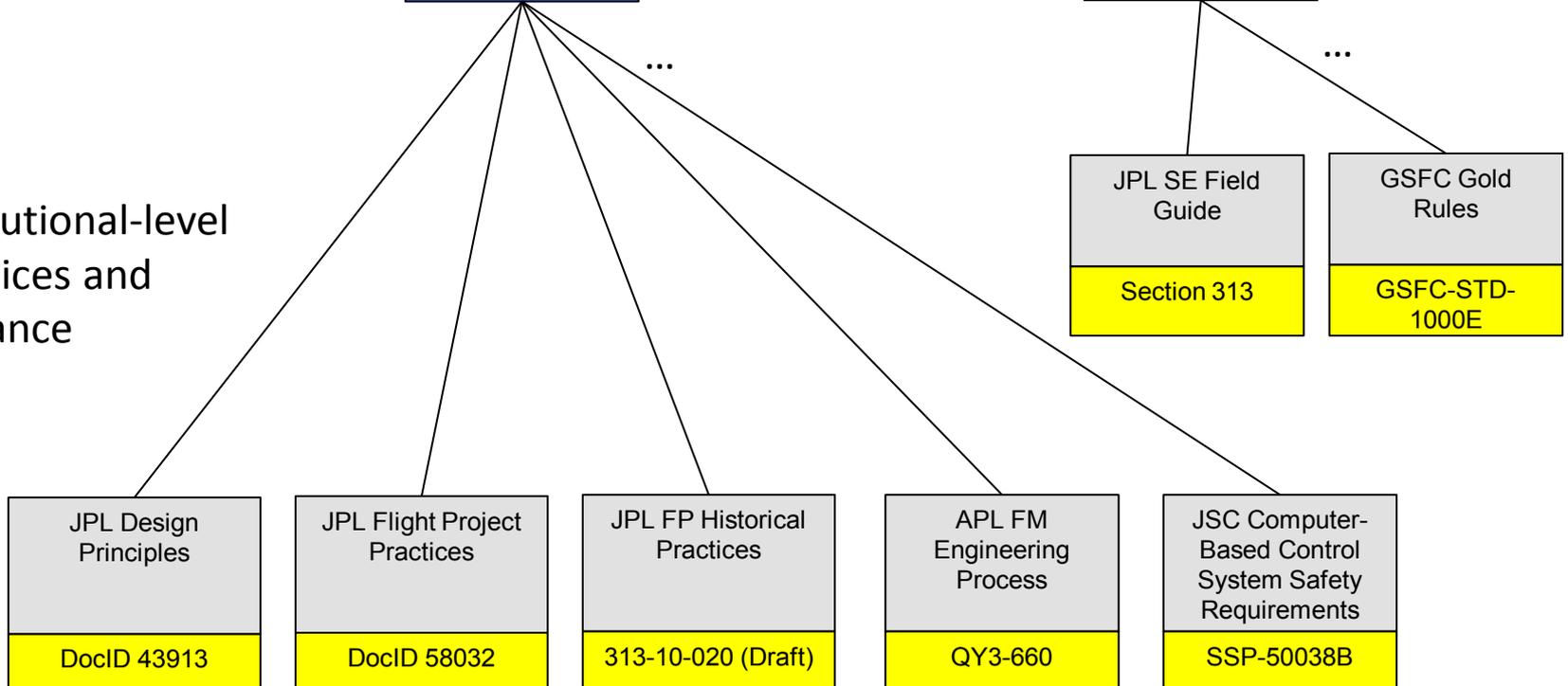
Use of NASA Handbooks and Institutional Practices



Agency-level
guidance and core
concepts



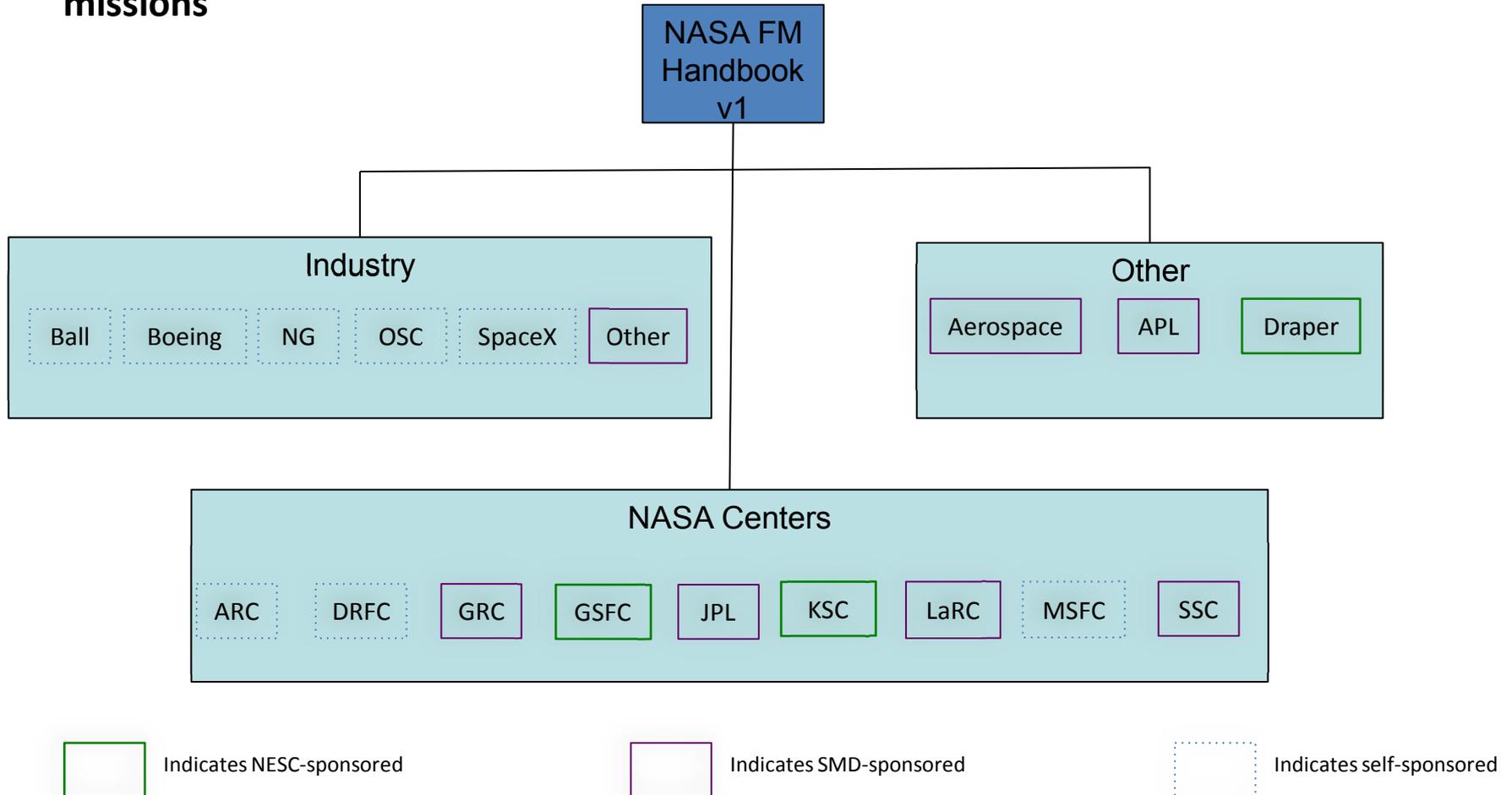
Institutional-level
practices and
guidance



FM Handbook Participation



Goal: To capture expertise across NASA and industry that would respond to needs identified in the FM Workshop Findings/Recommendations, to benefit future missions



FM Handbook Outline

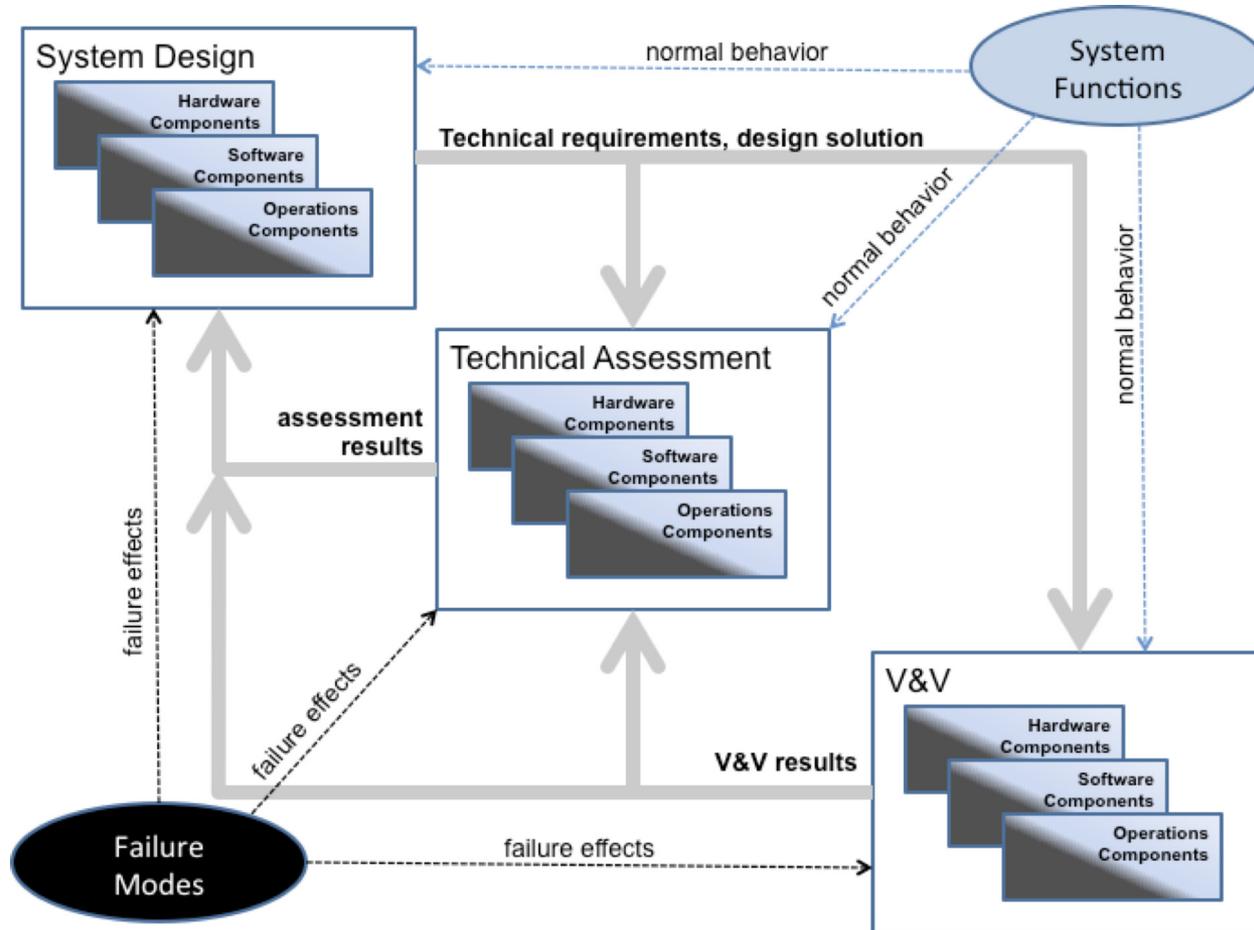


| Section | %* | Summary | Accomplishments & Challenges |
|-----------------------------|-----|--|---|
| Foreward | 100 | What does this Handbook provide? Why does NASA need a FM Handbook? | Fairly stable. Still debating whether FM includes Prognosis, and if FM = ISHM (or VSHM). |
| 1. Scope | 90 | What is FM? Relevance and Purpose; FM within NASA and institutional challenges; Structure of the Handbook; intended audience | |
| 2. Applicable Documents | 100 | List of documents sited in the text; approved documents | |
| 3. Acronyms and Definitions | 90 | Acronyms and abbreviations used throughout the document; Definitions of key FM terms | Team did not completely concur on definitions and concepts. Also, need to coordinate with OSMA (NASA-STD 8709.22) & Aerospace/DoD |

* 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



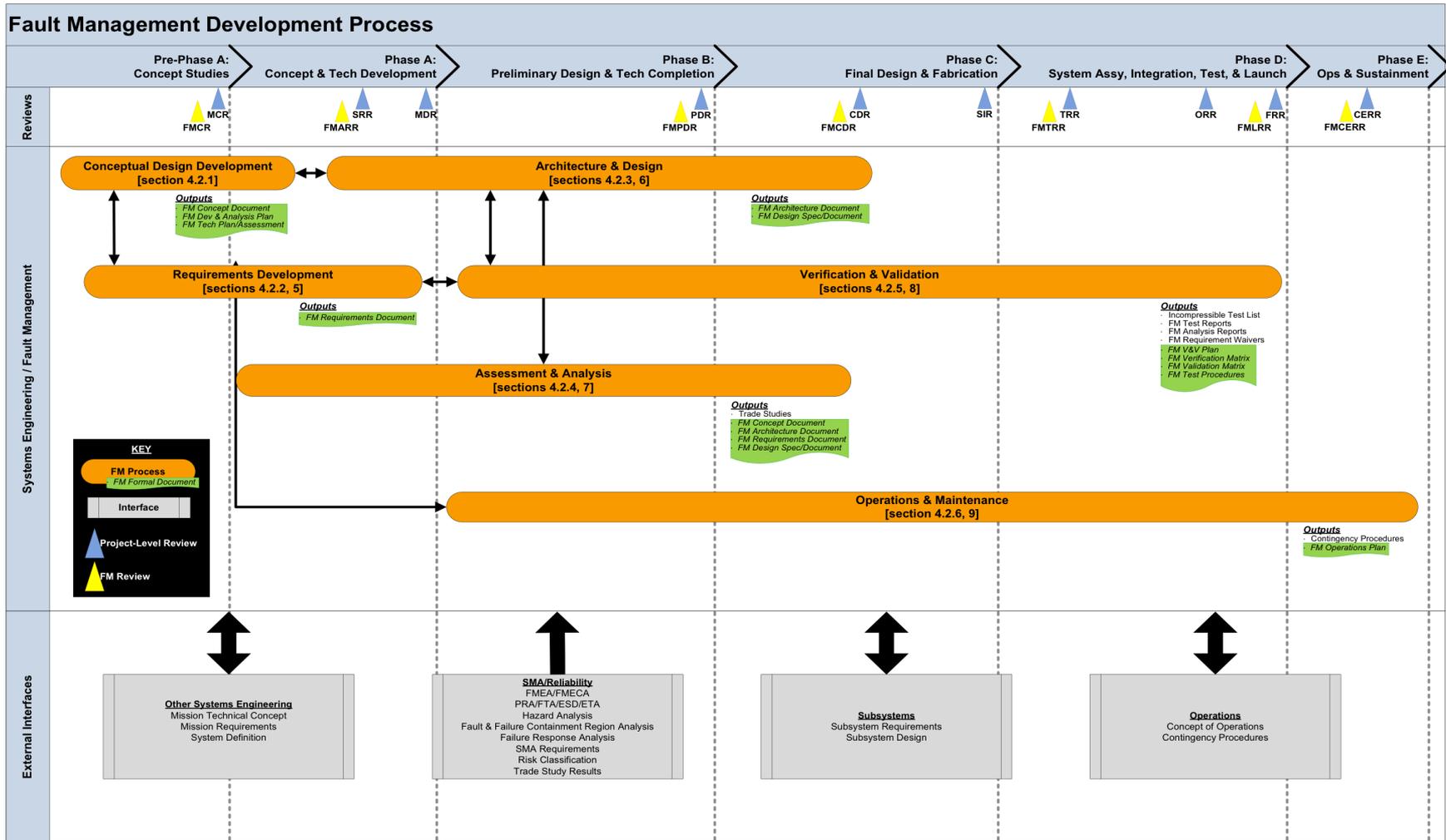
FM Handbook Outline (continued)



| Section | %* | Summary | Accomplishments & Challenges |
|--|----|--|--|
| 4. Concepts and Guiding Principles | 75 | Fundamental concepts and guiding principles grounding the field -- FM functions, FM as part of SE, FM goals: asset and function preservation | 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. |
| 5. Organization, Roles, and Responsibilities | 75 | Project organizational structure to support FM; interfaces; tasks | Fairly stable. Need to address different Mission classes (A, B, C, D). |
| 6. Process | 90 | Follows SE Process but focuses on FM products – Concept design, requirements, architecture, analysis, V&V, Ops and Maintenance | Came together nicely, once we adopted NASA SE Process as foundation. Agreement at a high level; further discussions still required to mature details. |

* 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 Process as Part of SE Process



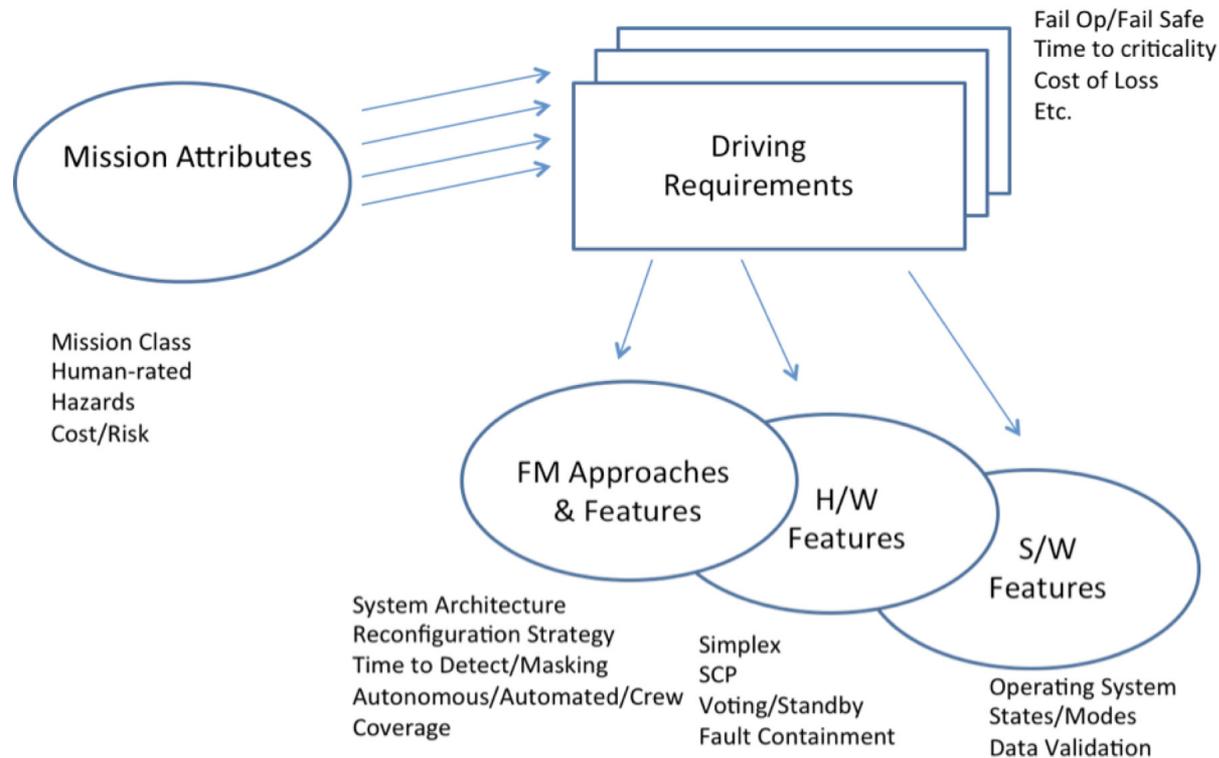
FM Handbook Outline (continued)



| Section | %* | Summary | Accomplishments & Challenges |
|-----------------------------|----|--|---|
| 7. Requirements Development | 90 | FM requirements categories; driving requirements; flow-down | Nice baseline identifying how to write FM requirements, with many examples and lessons learned provided. Currently deep-space-centric. |
| 8. Design and Architecture | 60 | Impacts of mission risk posture, goals, characteristics and FM priorities; FM architectures, design features and approaches; mission-specific considerations | 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. |

* 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 and FM Design



FM Handbook Outline (continued)



| Section | %* | Summary | Accomplishments & Challenges |
|---------------------------------|----|--|---|
| 9. Assessment and Analysis | 0 | To be expanded in later releases | |
| 10. Verification and Validation | 75 | Identifies FM V&V planning/preparation; how to perform FM V&V and analyze results; selection and prioritization of FM scenarios; simulators, test-beds and flight hardware testing | Fairly stable -- did not generate much controversy. Needs to address more Workshop Recommendations, like Design for Testability. Consider including Formal Methods. |
| 11. Operations and Maintenance | 0 | To be expanded in later releases | |

* 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 Handbook Outline (continued)



| Section | %* | Summary | |
|---------------------------|----|---|--|
| 12. Review and Evaluation | 90 | FM's presence in major milestone reviews; recommended FM-focused reviews; entrance and success criteria; key questions to ask at FM reviews | 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. |
| 13. Conclusion | 0 | To be expanded in future releases | |
| 14. Future Directions | 0 | Where this field is headed – new technology being developed that would offer technical solutions | Still debating if this Section should be included. |

* 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 Handbook Outline (continued)



| Section | %* | Summary | |
|------------|-----|---|---|
| Appendix A | 100 | References | |
| Appendix B | 0 | Work Product Templates (TBS) | |
| Appendix C | 95 | Relevant NASA Lessons Learned | 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. |
| Appendix D | 100 | Acknowledgements, historical background | |

* 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.

NASA FM Community of Practice



- 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

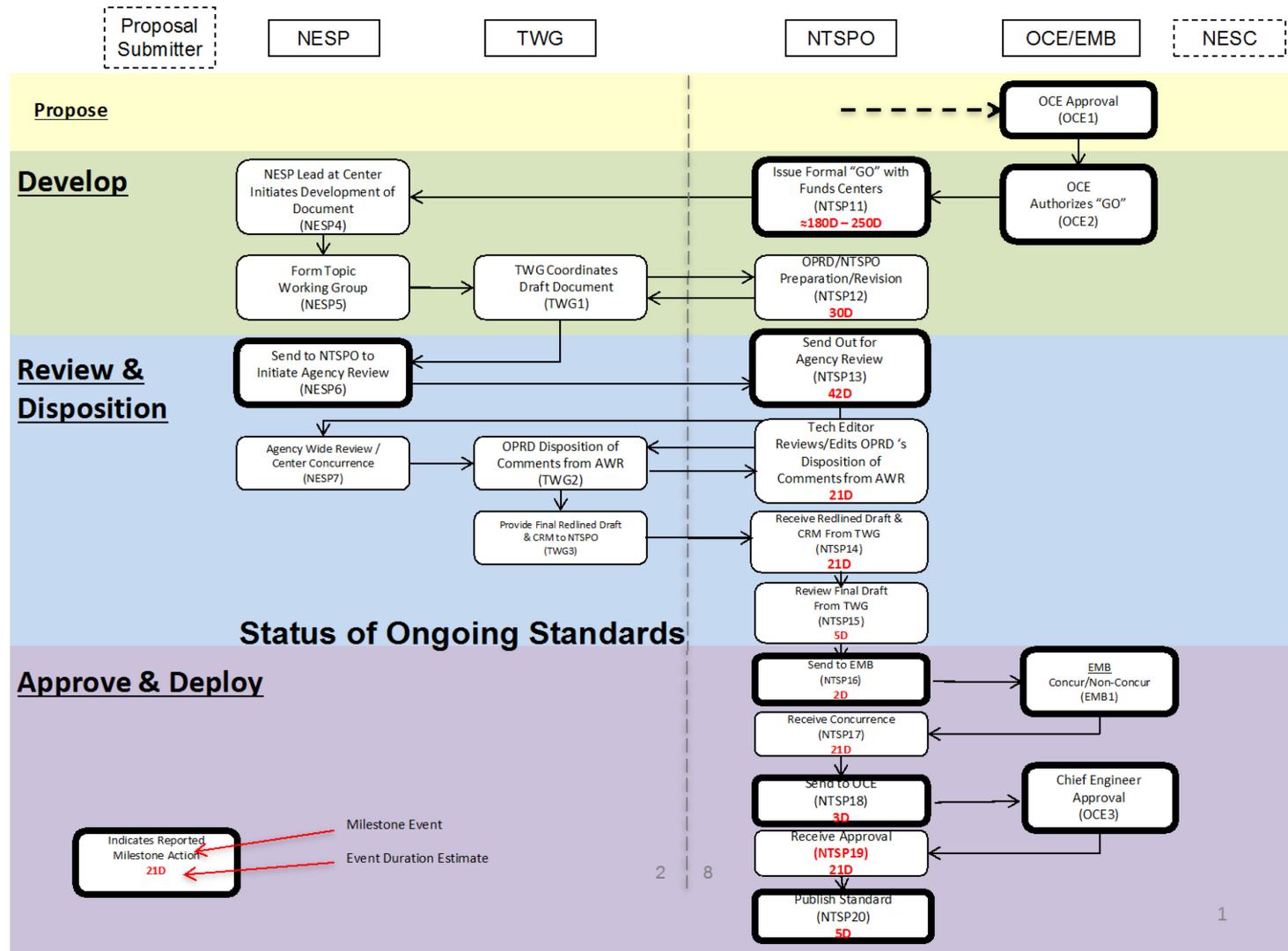
The screenshot displays the NASA Engineering Network (NEN) website interface for the Fault Management community. At the top, there is a navigation bar with links for Sign In, Support, Feedback, Site Map, and About. Below this is a main header for the NASA Engineering Network with a search bar and a menu containing HOME, OCE, LESSONS LEARNED, COMMUNITIES, and TOOLS & RESOURCES. The main content area is titled "FAULT MANAGEMENT" and includes a sub-header "Fault Management" with a "JOIN THIS COMMUNITY" button showing 23 members. On the left, there is a sidebar titled "EXPLORE THE COMMUNITY" with links for Community Home, Conferences, Contact List, Document Library, Forums, Lessons Learned, NASA Fault Management Handbook Wiki, References, Training, and Suggestions. The main content area features a featured article titled "ABSTRACT SUBMISSION DEADLINE EXTENDED: Integrated Systems Health Management in Boston July 2011" by Lorraine Fesq at JPL, dated 4/19/11. The article text states: "The deadline for abstract submission has been extended to May 10, 2011. Please consider submitting! This year, the Air Force Research Laboratory Air Vehicles Directorate will be hosting the Integrated Systems Health Management (ISHM) Conference on 19, 20 and 21 July 2011 in Boston, Massachusetts." Below the article is a "TOP STORIES" section with three items: "NASA Broad Agency Announcement (BAA): Unique and Innovative Space Technology - 3/2/11", "Kepler Anomaly Investigation - 2/16/11", and "Kepler Mission Manager Update: 64 Hour Safe Mode Ends - 2/10/11". To the right of the article is a "WELCOME" section with a photo of Lorraine Fesq and text describing the Fault Management (FM) discipline. Below the article and welcome section is a "COMMUNITY LINKS" section with icons and text for Conferences, Contact List, Document Library, Forums, Lessons Learned, NASA Fault Management Handbook Wiki, References, Training, and Suggestions. At the bottom of the page, there is a footer with the NASA logo, National Aeronautics and Space Administration, Inspector General Hotline - 1-800-424-9183 | Equal Employment Opportunities | Dispute Resolution | Freedom of Information Act | Privacy Policy and Important Notices | NEN v3.0, Editor: Manson Yew, NASA Official: Gregory Robinson, and Contact NEN.

Longer-term Vision



1. **Develop agency-wide FM Handbook, Version 2**
 - Engage Human Spaceflight Programs (ESMD), Mission/Ground Systems (SOMD), Aeronautics (ARMD), OSMA.
 - Address more Workshop Recommendations (e.g., representation techniques)
2. **Hold Workshop(s)** to bring NASA FM community together to achieve common understanding across Directorates (include SSME IVHM, Lunar Altair Lander, OSMA, Human Factors, etc.)
3. **Establish WG (part of SEWG?) or TDT to work through more challenging Recommendations (e.g., FM architecture trade space, metrics). Leverage FM CoP to identify potential members**
4. **Integrate/coordinate** FM concepts with other organizations (e.g., DoD, NRO) and with other documents (e.g., NASA Systems Engineering Handbook, NPRs)
 - Engage DoD, Aerospace Corp, NRO -- Contractors should be able to use consistent terminology, architectures, representation techniques regardless of customer
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

NTSPO Document Process



Conclusions



- **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
- **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's Office of the Chief Technologist: FM identified in seven of NASA's 14 Space Technology Roadmaps – opportunity to coalesce and establish thrust area to progressively develop new FM techniques
- **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.**



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**
- **Richard Larson, NASA DFRC**
- **Ken Lebsock, OSC (GSFC Affiliate)**
- **Steve Scott, GSFC Chief Engineer**