Fault-Tolerant Spaceborne Computing
Employing New Technologies

Reflections on NASA’s 2012 Spacecraft Fault Management Workshop

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

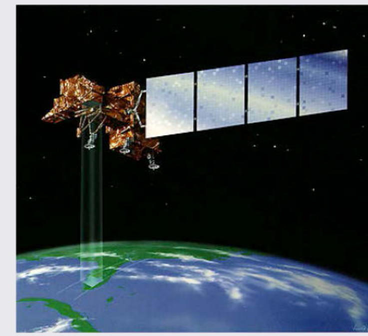
Sandia National Laboratories, Albuquerque, NM
May 31, 2012

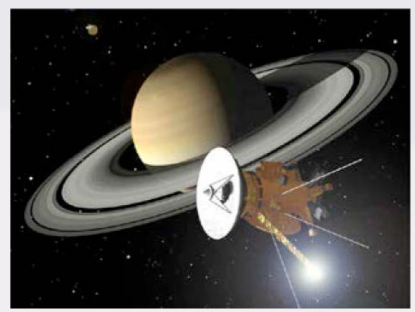
2012 Spacecraft Fault Management Workshop

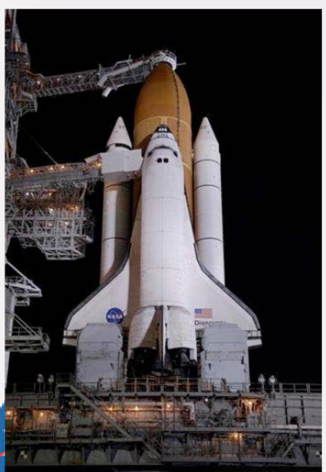
- 115 attendees plus 60+ via WebCast
- >30 organizations from government, industry, academia
- 4 NESC Technical Fellows and members of the SE TDT
- Sponsor, Lindley Johnson, NASA SMD/PSD Discovery Program Executive

2012 Scope

- FM, ISHM, FP, IVHM, SHM, FDIR, RM, HUMS
- HSM and OSMA focus this year
- Aeronautics, GS, MS next on the list







Recent FM Developments

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)

2008 | 2009 | 2010

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)

*

2011 | 2012

*

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

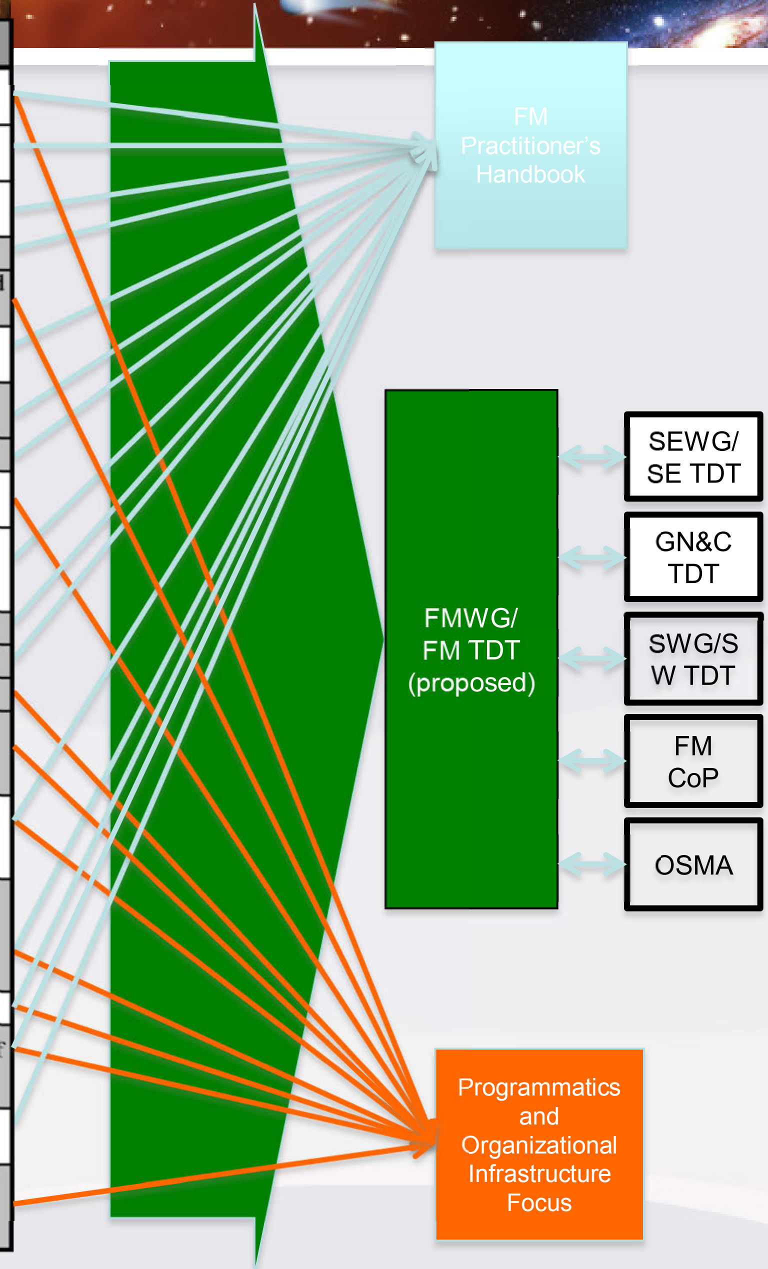
Oct '10: **FM CoP** established on OCE's NEN website – nen.nasa.gov (L. Fesq)

Jul '11: **FM Handbook Draft** delivered to NESC/SMD and NTSPO and Centers for review. OCE directs to "coordinate robotic, HSF and OSMA concepts next"

Apr '12: SMD/PSD sponsors **2nd S/C FM Workshop** (L.Johnson)

Allocation of Workshop Recommendations

#	Recommendation
1	a) Allocate FM resources and staffing early, with appropriate schedule, resource scoping, allocation, and prioritizing. Schedule V&V time to capitalize on learning opportunity.
	b) Establish Hardware / software / "sequences" /operations function allocations within an architecture early to minimize downstream testing complexity.
	c) Engrain FM into the system architecture. FM should be "dyed into design" rather than "painted on."
2	a) Establish clear roles and responsibilities for FM engineering.
	b) Establish a process to train personnel to be FM engineers and establish or foster dedicated education programs in FM.
3	Standardize FM terminology to avoid confusion and to provide a common vocabulary that can be used to design, implement and review FM systems.
4	a) Identify representation techniques to improve the design, implementation and review of FM systems.
	b) Establish a set of design guidelines to aid in FM design.
5	a) Identify FM as a standard element of the system development process (e.g., separate WBS) to promote innovative solutions and realistic estimates of complexity, cost, schedule.
	b) Establish metrics and process specification with milestones that will allow proposal evaluators and project teams to assess the relevance, merits and progress of a particular FM approach.
6	a) Design for testability: Architectures should enable post-launch and post-test diagnosis.
	b) Examine all observed unexpected behavior.
	c) Implement continuous process improvement for FM lifecycle.
	d) Catalog and integrate existing FM analysis and development tools, to identify capability gaps in the current generation of tools, and to facilitate technology development to address these gaps.
7	Review and understand the impacts of mission-level requirements on FM complexity. FM designers should not suffer in silence, but should assess and elevate impacts to the appropriate levels of management.
8	Assess the appropriateness of the FM architecture with respect to the scale and complexity of the mission, and the scope of the autonomy functions to be implemented within the architecture.
9	Define and establish risk tolerance as a mission-level requirement.
10	Examine claims of FM inheritance during proposal evaluation phase to assess the impacts of mission differences.
11	Develop high-fidelity simulations and hardware testbeds to comprehensively exercise the FM system prior to spacecraft-level testing.
12	Collect and coordinate FM assumptions, drivers, and implementation decisions into a single location that is available across NASA, APL and industry. Utilize this information to establish / foster dedicated education programs in FM.



Themes for 2012 FM Workshop

- Themes for 2012
  - *Architecture Fitness:* Perform a FM architectural trade study to enable future missions to assess appropriateness of FM architecture (Rec #5, Rec #8)
  - *Technology gaps:* Develop Strawman FM Capabilities Roadmap (Rec #6)
  - *Common understanding:* Hold Handbook Summit to address
    - terminology (Rec #3)
    - FM related to OSMA
    - FM's related to SE
  - Panel on "How FM Fits Within a Project"

Goals

- Bring FM LL and BP alive to benefit future missions
- Establish a vision for FM technology development
- Expose the different views/roles of FM on current missions
- Work toward consensus on key issues
- Approach
  - Collect and Assess past FM Architectures
  - Develop a FM Capabilities Roadmap
  - Discuss via a panel the role of FM on a Mission
  - Mature the contents of the NASA FM Handbook

Architecture Trade Study Breakout Session

- **Goal: generate trade space (database?) to help future projects determine the appropriateness of a FM architecture for a particular missions**
- Material needed
  - Exemplar FM architectures
  - Mission Characteristics
  - Metrics/Quality Attributes
  - Work with experts to generate exemplar FM architectures
    - Pull from FSW Complexity study – appendix contains Kevin's FM family tree
    - Infotech@Aerospace 2011 Special Session on FM Architectures
    - Solicit input from participants prior to workshop (RFWI)

Green = confirmed

Develop Strawman Capabilities Roadmap

- **Goal: Develop a FM Capabilities roadmap to identify near-term needs and long-term goals**
- Material needed: Strawman Gap Analysis and possibly Technology Roadmap
- The Plan to generate material
  - IV&V Facility to lead this effort. Independent, no biases
  - Team of Center Reps
  - Source material: OCT Roadmaps, NRC report, CxP FM Technology wish list, Opportunities for Investment from 2008 Workshop
  - Solicit input from participants prior to workshop (RFWI)

Note: NRC report on OCT roadmaps

NRC review captured some sense of the need for FM

"*Due to the potential for major mission improvements, strong alignment with NASA needs, and reasonable risk and development effort, **ISHM/FDIR/VSM are rated as high-priority technologies**.*"

What is happening in FM outside of NASA?

Program includes four Invited Speakers, whose role is to

- Help us understand how other communities are organizing and maturing the FM field
- Gain new perspectives by exposing us to alternate approaches and concepts

1. **Michael Aguilar, NASA GSFC (lunch-time speaker)**
   - NASA NESC Software Tech Fellow
   - "Fault Management using MBSE Tools and Techniques"
2. **Dr. Werner Dahm, Arizona State University (previously Air Force)**
   - Director, Security and Defense Systems Initiative
   - "ISHM: Applications and Challenges on the Horizon"
3. **Dr. Algirdas Avizienis, UCLA**
   - Distinguished Professor Emeritus, Computer Science Department
   - "Terminology Issues in Dependable Computing"

2012 NASA FM Workshop
Day 1 and Day 2 Observations

Common themes:

•FM technology advancement is crucial for the success of future human missions (Brian Muirhead, Jon Patterson, Carlos Garcia-Galan, Lee Morin)

•All but one of the afternoon talks recommended increasing model-based design using UML/SysML, TEAMS, IMS/AMISS (Mark Schwabacher, Robert Mah, Mitch Ingham, Dan Dvorak, Lui Wang, Mark Derriso)

•Three talks identified the importance for System States to be explicit (Dan Dvorak, Mitch Ingham, Mark Derriso)

•Goal-based control was mentioned by five speakers:

- Jon Patterson: "goal tree / success tree"
- Phillip Schmidt: “goal-oriented over component-directed monitoring”
- Dan Dvorak: "goal-based control"
- Mitch Ingham: "integrating goal-driven commanding, fault detection, diagnosis and recovery"
- Werner Dahm: "goal-driven context-aware systems”

Differing views:

•Stephen Johnson defined FM as *“A set of ‘meta-control loops’ that aim to restore the system to a state that is controllable by nominal (passive and/or active) control systems“* while Mitch Ingham and Dan Dvorak presented concepts that defined FM with the nominal activity

•APL and MSFC/SLS handled FM organization differently:

- “APL split FM functionality into two distinct roles: Fault Management and Autonomy” - Kris Fretz
- “Nominal and FM teams … have been combined for SLS” – Jon Patterson

•Terminology still needs to be worked, especially w.r.t. architecture, to address full range of health and fault management

Common Themes

- FM technology advancement is crucial for the success of future human missions
- Importance for System States to be explicit
- Goal-based control
- Importance of modeling at the architecture and system level and the need to include functionality including SW and FM functionality in the models.
  - Need to conduct an assessment (e.g. survey) of the tools and their usage to understand if the SOA is up to the challenge
  - Corollary question: have we seen where the tools have/are failing when used on big problems. Most likely need to go outside NASA (e.g. DOD, industry, automotive) to answer this question. Depending on the answer will need to get support to push capabilities in tools and trained operators/users.

Future plans and actions

- Write Workshop Report summarizing activities
- Complete the Handbook (help!)
- Updates to NPRs and other Handbooks (e.g., SE, SW)
- Develop a framework for SW architecting that includes HM/FM.
- Consider development of a more general and/or unifying term for HM/FM. e.g. health management, resilience management, dependability management, resilient control, resilient control management, mostly harmless
- Continuing discussions, especially panel topics. Use Forum on FM CoP?
- Next workshop: Agency-level sponsor? Joint with Aerospace Corporation?

Why a Roadmap?

- A roadmap can provide guidance to the maturation of the Fault Management discipline
  - Identify critical capabilities and technologies
  - Identify capability and technology gaps
  - Identify ways to leverage R&D efforts

- Varied and competing interests in NASA missions
  - Capability development is not straight-forward
  - Prioritization of capabilities unclear
  - Limited technology/capability development funding

Goals of Creating a Roadmap

- Connect and balance NASA's needs (pull) with Fault Management innovation (push)
  - Which envisioned NASA missions or systems will drive FM capability?
  - Which FM-related capabilities are needed to enable or enhance the envisioned NASA missions/systems?
  - Which FM technologies need to be developed to address the capability needs?
- Provide a clear framework for Fault Management innovation for
  - NASA policymakers
  - Mission/System Engineers
  - Researchers and Technologists
- Identify FM-related investment priorities for NASA Technology Programs, e.g., SBIR, OCT, Directorate tech programs

Domain Areas

- Aeronautics
- Launch vehicles
- Earth-orbiter human
- Earth-orbiter robotic
- Deep-space human
- Deep-space robotic
- Ground operations
- Mission operations

Note: this is an incomplete set of domains, but they represent the set we intend to target at this workshop. Other domains will be targeted post-workshop.

Accomplishments

- [Pre-workshop] Each Breakout Team Lead produced a starting point for their roadmap, by filling out the "Mission/System" timeline and exemplar Capabilities and Technologies that are driven by some of these Missions/Systems
- [At Workshop] Each Breakout Team:
  - revised the Mission/System timeline,
  - identified the set of Capabilities that are driven by each Mission/System, and
  - started to identify the set of technologies that are needed to provide the Capabilities.
- Highlights from each Domain Roadmap will be presented by the Breakout Team Leads.

•Note: Items in RED font are needed NOW!

Launch Vehicles – FM Needs

2012 | 2015 | 2018 | 2021+

Missions

- SLS PDR → SLS CDR → SLS EM-1 → SLS EM-2
- Commercial Crew → Commercial Crew - ISS
- J-2X Dev. & Testing → Advanced Booster → Second Stage Development
- Exp. SSME Cert. → RS-25E Dev. & Testing
- Lunar, Asteroid, Mars Missions
- Orbital Refueling

Capabilities

- •Auto- translation of S&MA & Design data to directed graph & state machine models
- •Software FM
- •Requirements Formalization
- •Semi-auto translation of directed graph models to real-time diagnostics
- •Automatic translation of model-based algorithms to flight software
- •Critical Flight data acquisition
- •Model-Based Connectivity to S&MA, SE&I
- •Auto-translation of directed graph models to real-time diagnostics
- •SHM/FM Function Analysis
- •SHM/FM Design Analysis including cost/benefit trades
- •Reduced FM Verification Cost & Expanded Coverage
- •FM Analysis-Design-V&V Integration
- •Cryogenic & high-temperature measurements
- •Anomaly detection
- •Deep-space FM
- •Engine Transient Modeling
- •Model-based Test Data Prediction
- •Model-based Test Data Reduction
- •Probabilistic Engine Redline Analysis

Technologies

- •Script-based data translation
- •Adaptive telemetry
- •Model-based data translation
- •Function Analysis Tool
- •FM Control Loop Tool
- •FM Verification Tool
- •Integrated SHM/FM Analysis/Design Tool Suite
- •Pattern recognition
- •Cryogenic & high-temperature sensors
- •Deep Space Cryogenic & high-temperature sensors
- •On-board diagnostics
- •WinPlot/Matlab-based analysis tools
- •LV Prognostics

2012 | 2015 | 2018 | 2021+

Next Steps

- Make distinct Domain Roadmaps more consistent in format and scope (e.g., enabling vs enhancing annotations, explicit links between Missions/Capabilities/Technologies)
- Complete Technology timelines in Roadmaps
- Review Capability and Technology Roadmaps, solicit more input
- Perform gap analysis (needs vs. current Technology efforts)
- Prioritize Capability developments and develop Technology investment recommendations
- Outbrief to technology portfolio managers (e.g., OCT)

General Observations

- Many common development-time capabilities (modeling, auto-generating FM-related products, automating V&V, etc.)
- Also several common run-time capabilities (on ground, e.g., prognostics; onboard, e.g., diagnosis)
- Enabling capabilities for one domain are often enhancing for others
- Probably worth investing in common framework developments for multi-domain capabilities, or at least coordinating our work
- Next time, take attendance! (Sorry, all!)
- How to keep up momentum and complete the job?

- ***Fun discussions! Thanks to everyone for your enthusiastic participation!***

Summary – Intent of Session

- Introduce notion of using quality attributes to assess FM architectures
- Introduce a proposed approach for correlating mission/design/implementation characteristics with quality outcomes
  - Obtain feedback from session on approach
  - Provide basis for additional applications to be added to an architecture database
- Use developed case studies to illustrate approach and spur discussion on assessing FM architectures
- Apply insights from discussions to determine quality attributes for a future mission
  - Human mission to a near-Earth asteroid

Quality Attributes

- A proposed set of quality attributes have been developed in advance
- As part of the discussion, these attributes will be assessed for:
  - Completeness
  - Applicability (to a given mission type)
  - Level of Abstraction
- Will also develop correlations between quality attributes and mission characteristics, design choices and implementation methods

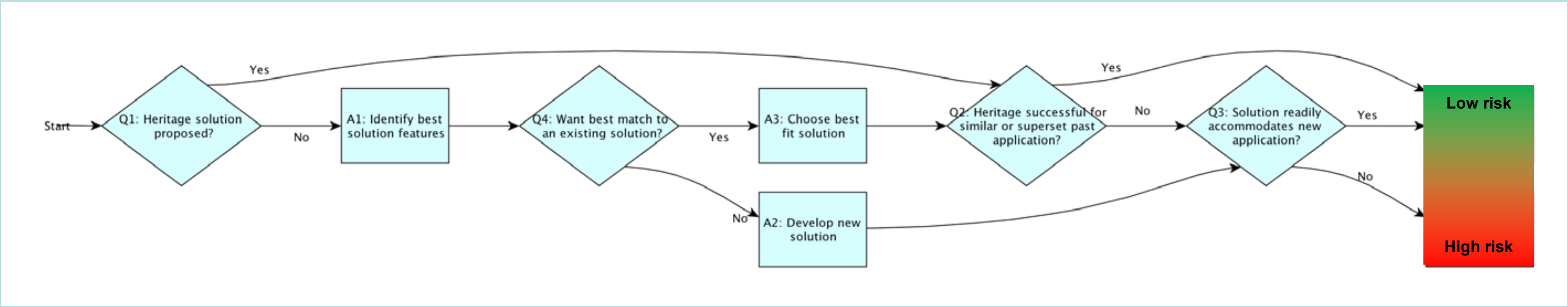
Analyzability
Appropriateness for Organization
Avoid Unnecessary Interruptions
Conceptual Applicability
Conceptual Integrity
Correctness
Cost For Development
Cost for Development Environment/Tools
Cost for Development Time and Testing
Cost for Operations
Cost For Repeated Work-Arounds
Cost for Training
Degrade Gracefully
Doesn't cause mission loss
Familiarity
Fault Coverage
Integrability
Interoperability
Modifiability during Development
Modifiability during Operations
Modifiability Mission-to-Mission
Modularity
Perceived Cost/Benefit
Preserve Resources and Opportunities
Reduce Recovery Time
Reliability
Reusability
Safety
Scalability
Testability
Thrustworthiness
Tolerate Modeling Errors
Usability/Operability

Assessment Process Overview

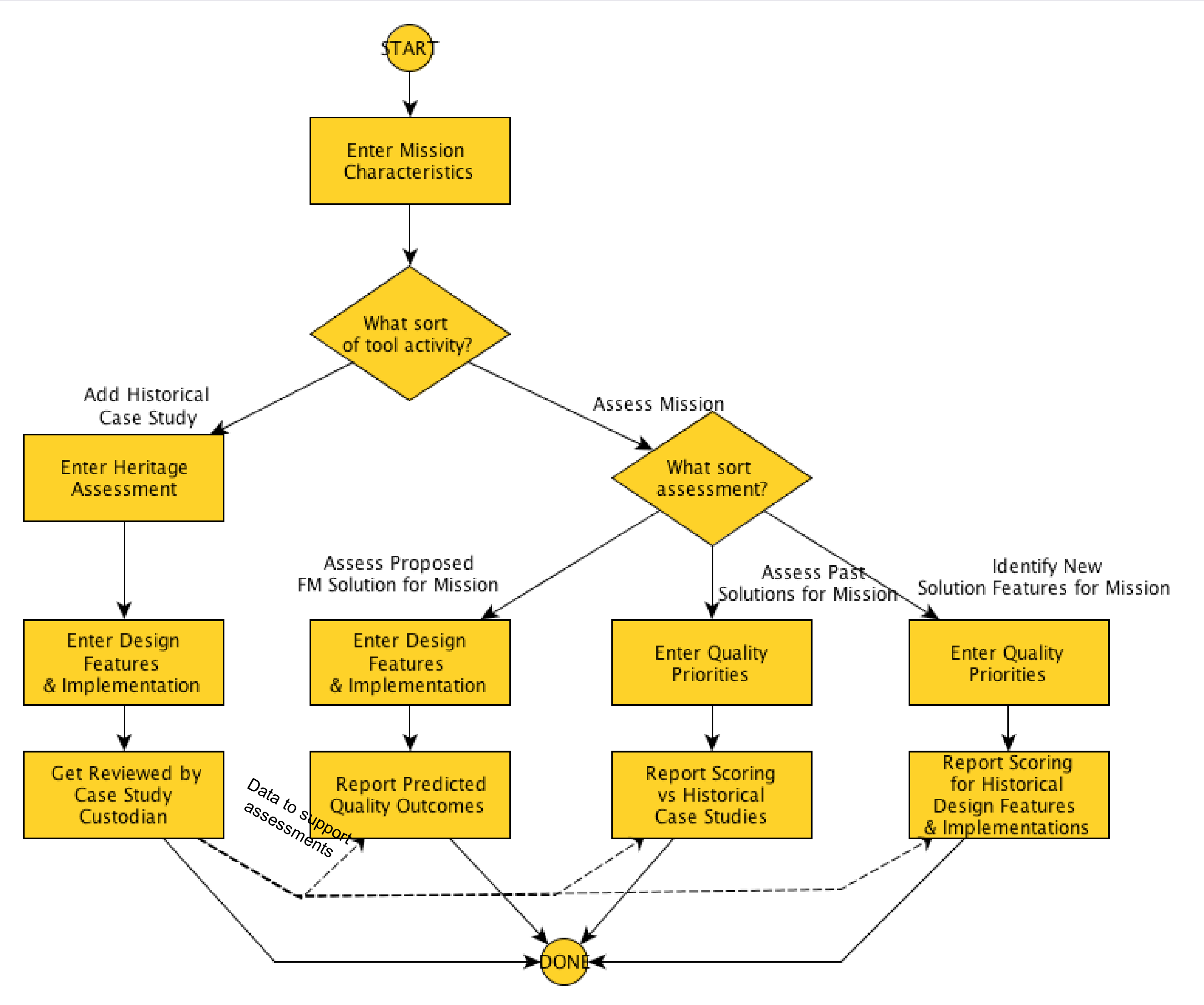
- The assessment process consists of two key elements:
  1. A top level process flow for examining the heritage risk story.
  2. An online database and reporting tool to ground the assessment in measureable data.

Heritage Risk Assessment Process

- We begin with a heritage risk assessment covering at least these areas of a fault management solution:
  - Staff
  - Analyses & design tools
  - Flight hardware
  - Engineering practices
  - Flight software
  - Mission design
- The figure below depicts the assessment flow.
  - Note that even a difficult-to-use solution, can be applied successfully to identical missions once it has been debugged sufficiently.
  - A project may also iterate this process across multiple aspects of the architecture and across multiple changes to the architectural approach.
  - Details for each box are now explained…



Flow for using the Database



Case Studies

- The following historical case studies were discussed in 3 breakout sessions:
  - Cassini Attitude Control FP, M. Brown (JPL)
  - Orion/MPCV, E. Seale (LM-Denver)
  - ISS Autonomous FDIR, B. O'Hagan (JSC)
  - Chandra, K. Patrick(NGC)
  - SSTI/Lewis, J. Tillman (NGC)
  - Dawn, J. Rustick (Orbital)

Insights from Case Studies – 1

- SSTI/Lewis. "faster, better, cheaper" mission with extreme cost constraints
  - Cost restrictions led to misapplication of heritage safing algorithm, and inadequate V&V (resulting in loss of mission)
- Dawn. Discovery Class, interplanetary mission to 2 asteroids. 10 year mission, includes significant periods of no communication
  - TMON table selected for cost reasons.
  - Easy to configure/re-configure, but hard to review, hard to communicate intent. Simple constructs, complex resulting behavior
  - FP FSW correctly identified and responded ~10 anomalies in-flight and several 'errors'
- Cassini. Flagship-class Saturn orbiter. Flying successfully for ~15 years.
  - Aspects of design that were goal-like worked well, and the things that weren't didn't work as well led to "gadgeteering"

Insights from Case Studies – 2

- ISS: interesting case study as a representative of class of systems (a) with various international partners, (b) that has evolved substantially over time, (c) that has a human crew. Key issues that come up in this class of system include
  - 1. How to provide coordinated FM across multiple independently implemented subsystems (ISS has some noted problems in this area)
  - 2. For such a long-lived system, how to prioritize FM upgrades given budget restrictions. Suggests the need for FM evolution management.
  - 3. How to understand the role of humans in the overall FM plan. What kinds of expertise can we assume they have, and to what extent does the answer to that question affect what we try to automate and how we automate it?
- Chandra:
  - Example of a system that made clear tradeoff in favor of safety over availability. Leads to a simpler FM system, but one that provides less overall utility.
    - Raises the issue of how you make a tradeoff between these two dimensions (a common issue, it seems, in NASA FM systems design).
  - Perceived need for a separate Attitude Control safing computer that in hindsight was probably not necessary.
    - However at the time the designers did not trust the software in the primary A-B redundancy in part because it was developed late in the process

Observations

- The idea of using quality attributes was not contested
  - However, there was not consensus on whether the proposed set of quality attributes was appropriate
  - It may be that defining a set of *a priori* quality attributes is a poor starting point
- But there was significant difficulty in mapping from quality attributes to mission and design characteristics
  - Although this appears feasible, it remains a research project to establish this mapping, especially to establish quantitative relations
- The bulk of the useful discussion came from the descriptions of the missions and fault management design solution, and not from walking through the spreadsheet
  - Being aware of past decisions is useful
  - Past design choices were made for various reasons, that had consequences that were not considered as part of the decision

Conclusions

- Continuing work on development of a tool appears to be useful
  - Concept of mission characteristics and architectural choices affecting quality attributes sound
  - But is hard, and a common approach may not be possible
  - Broaden scope to include missing aspects
    - e.g., organization, infrastructure, processes, prevention/design-time elements
- Other approaches are also likely to provide utility in assessing FM architectures:
  - Development of architectural guidance, stated in terms of quality attributes
    - “if you do A, you are likely to have consequences B, C, D”
    - “if you optimize QA1, then QA2 and QA3 may be negatively

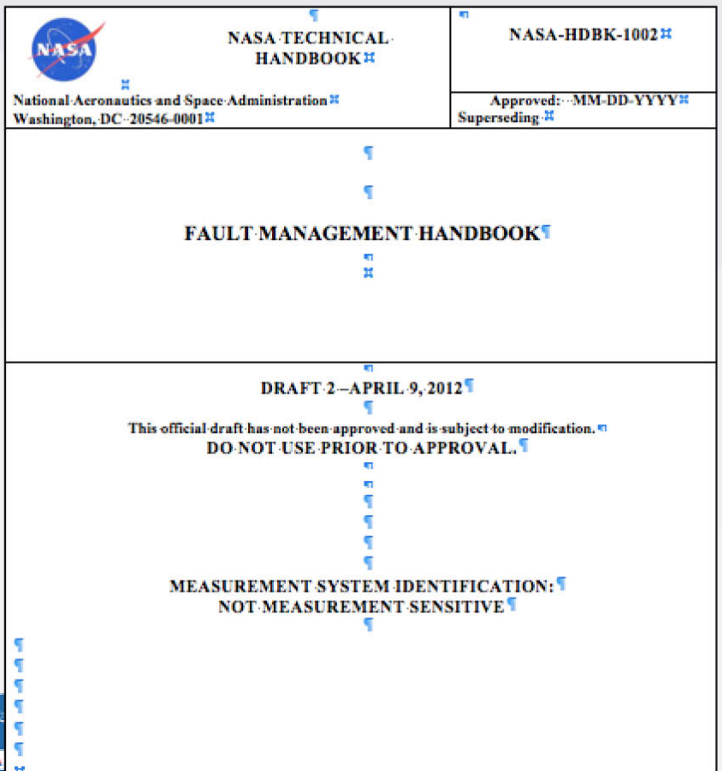
Acknowledgements

- Venue arrangements: Pauline Burgess and Michelle Hensen, NRESS
- Steering Committee
  - Lindley Johnson, HQ/SMD – sponsor for this workshop and FM Handbook
  - Neil Dennehy, GSFC/NESC – co-sponsor of FM Handbook
  - Steve Scott, GSFC/OCE
  - Brian Muirhead, JPL/OCE
  - George Cancro, APL
  - Pat Martin, HQ/OSMA
  - Tim Crumbley, MSFC/OCE and Standards Office Manager
  - Ken Ledbetter, HQ/OCE
  - Carlos Garcia-Galan, JSC/MOD
  - Jeri Briscoe, MSFC/DNF
  - Frank Groen, HQ/OSMA
- FM Architecture Trade Session Leads: Kevin Barltrop (JPL), David Garlan (CMU), John Day (JPL)
- FM Capabilities Roadmap Session Leads: Ken Costello (IV&V Facility), Mitch Ingham (JPL)
- Facilitators: Daria Topousis, Chris Eng, Alex Kadesh (JPL)

Backup

FM Handbook: [redacted]

http://www.nasa.gov/offices/oce/documents/2012_fm_workshop.html



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 9, 2012

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

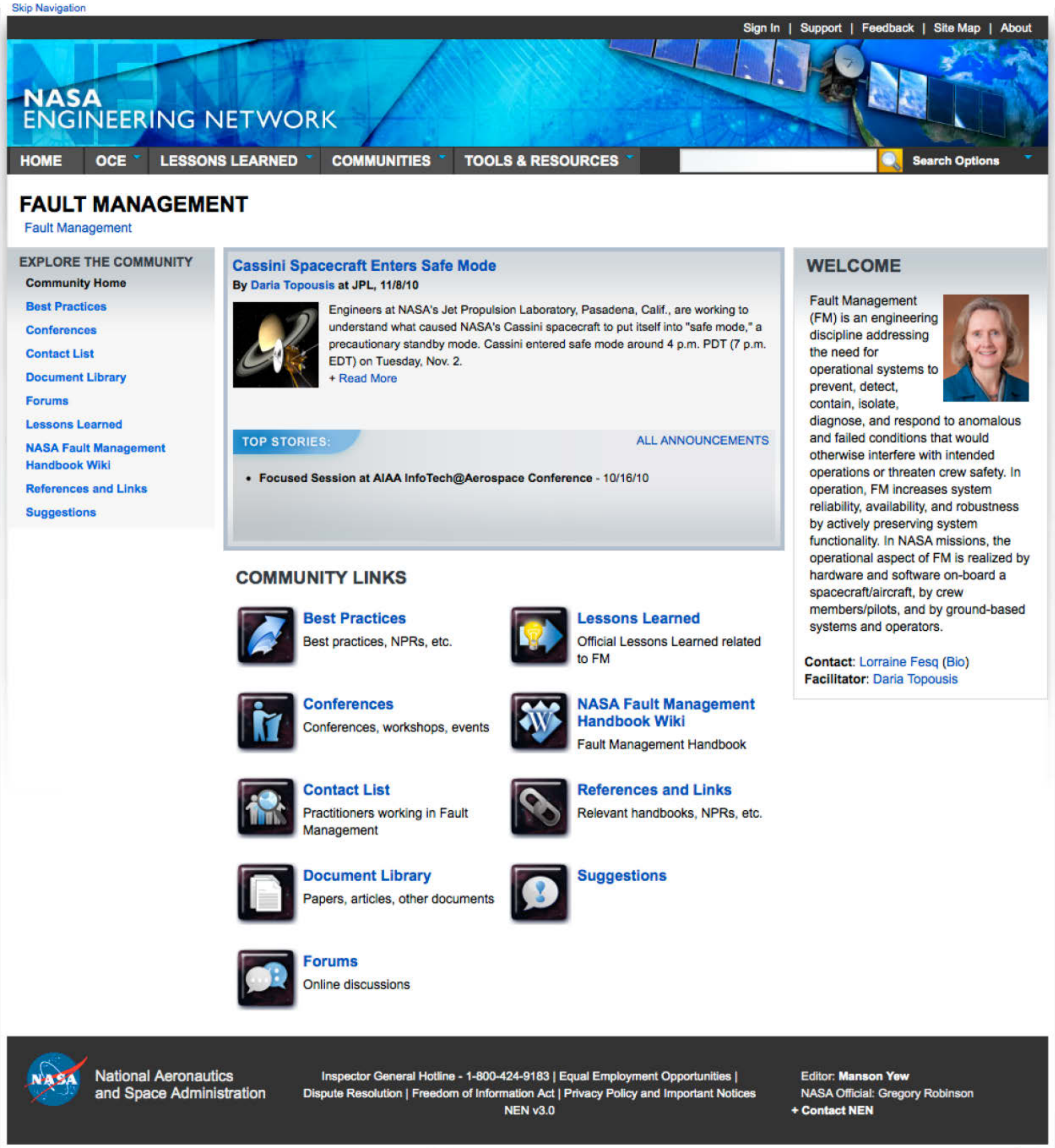
MEASUREMENT SYSTEM IDENTIFICATION:
NOT MEASUREMENT SENSITIVE

A community of practice is…

A group of people who "share a concern, a set of problems or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis."

-Etienne Wenger

NASA FM Community of Practice



Skip Navigation

Sign In | Support | Feedback | Site Map | About

NASA ENGINEERING NETWORK

HOME | OCE | LESSONS LEARNED | COMMUNITIES | TOOLS & RESOURCES | Search Options

FAULT MANAGEMENT

Fault Management

EXPLORE THE COMMUNITY

- Community Home
- Best Practices
- Conferences
- Contact List
- Document Library
- Forums
- Lessons Learned
- NASA Fault Management Handbook Wiki
- References and Links
- Suggestions

Cassini Spacecraft Enters Safe Mode

By Daria Topousis at JPL, 11/8/10

Engineers at NASA's Jet Propulsion Laboratory, Pasadena, Calif., are working to understand what caused NASA's Cassini spacecraft to put itself into "safe mode," a precautionary standby mode. Cassini entered safe mode around 4 p.m. PDT (7 p.m. EDT) on Tuesday, Nov. 2.

+ Read More

TOP STORIES: | ALL ANNOUNCEMENTS

- Focused Session at AIAA InfoTech@Aerospace Conference - 10/16/10

COMMUNITY LINKS

Best Practices
Best practices, NPRs, etc.

Lessons Learned
Official Lessons Learned related to FM

Conferences
Conferences, workshops, events

NASA Fault Management Handbook Wiki
Fault Management Handbook

Contact List
Practitioners working in Fault Management

References and Links
Relevant handbooks, NPRs, etc.

Document Library
Papers, articles, other documents

Suggestions

Forums
Online discussions

WELCOME

Fault Management (FM) is an engineering discipline addressing the need for operational systems to prevent, detect, contain, isolate, diagnose, and respond to anomalous and failed conditions that would otherwise interfere with intended operations or threaten crew safety. In operation, FM increases system reliability, availability, and robustness by actively preserving system functionality. In NASA missions, the operational aspect of FM is realized by hardware and software on-board a spacecraft/aircraft, by crew members/pilots, and by ground-based systems and operators.

Contact: Lorraine Fesq (Bio)
Facilitator: Daria Topousis

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
+ Contact NEN

Handbook Issues

- Terminology!
- What is the “science” that lies beneath FM?
- Confusion about FM vs OSMA responsibilities
- How does FM fit within a mission?
  - Part of SE’s responsibilities?
  - Separate subsystem like power, ACS and thermal?
  - Additional duty for subsystem engineers?