V&V of Fault Management: Challenges and Successes

Lorraine Fesq

Jet Propulsion Laboratory, California Institute of Technology

NASA IV&V Annual Workshop

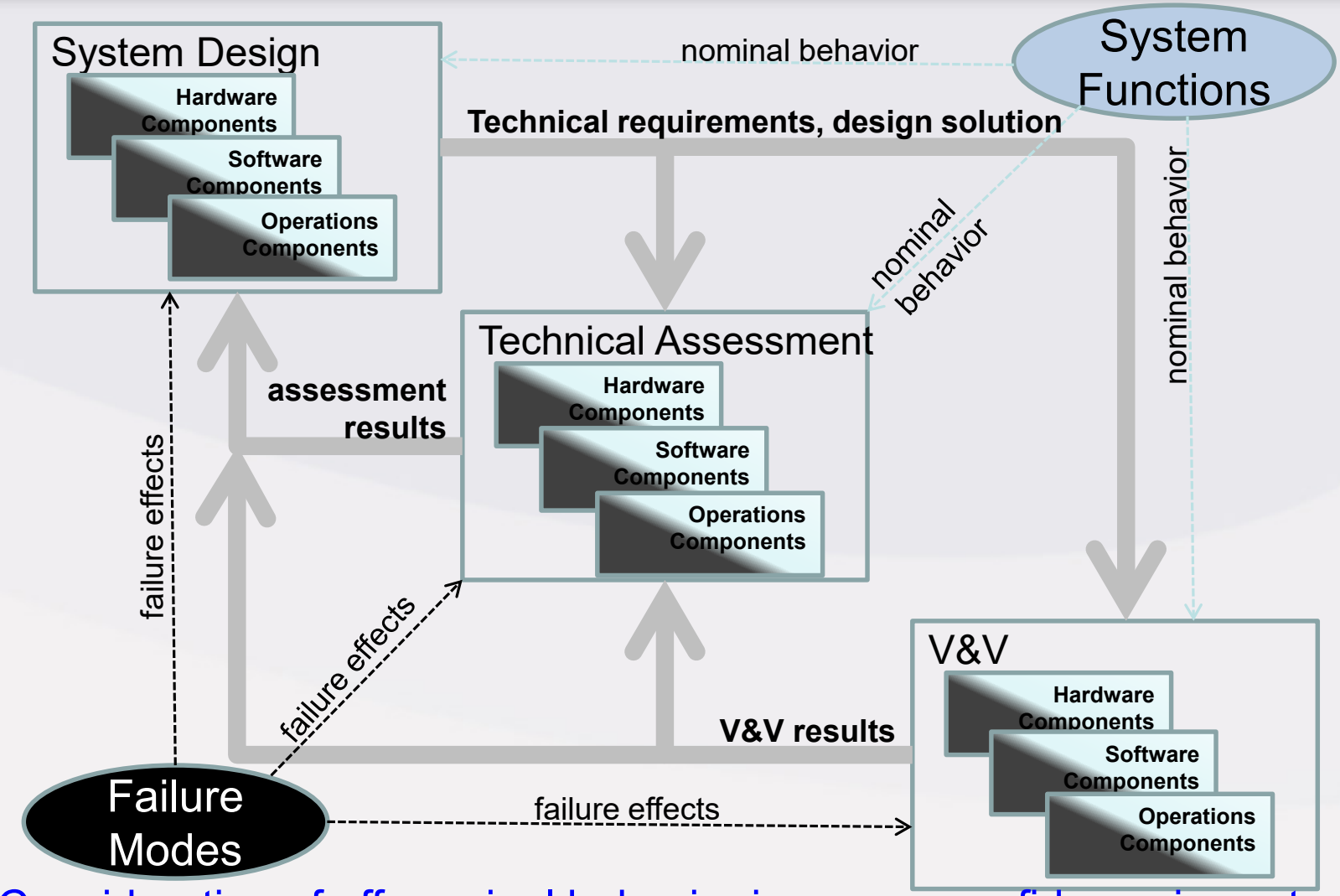
September 11-13, 2012

Copyright 2012 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.

Agenda

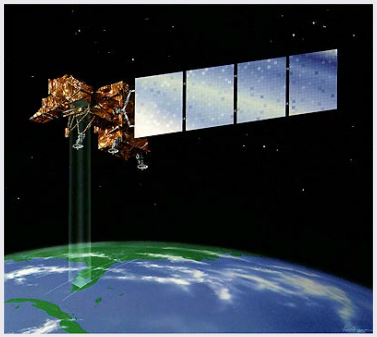
- Scope of Fault Management (FM)
- Current FM Issues Plaguing Missions
- Addressing FM Architecture
- Goals of the Breakout Session – Round Table
- Logistics – US Persons Only
- Acknowledgements

FM in the Development Process

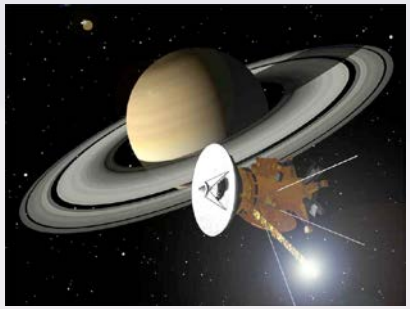


Consideration of off-nominal behavior improves confidence in system performance and improves system robustness.

2012 Scope



- Names for this discipline: FM, ISHM, FP, IVHM, SHM, FDIR, RM, HUMS
- 2012 focus: EO, DS, HSF, OSMA
- Future focus: Aeronautics, GS, MS



Recommendations to Resolve Current FM Issues

NASA has 12 Recommendations for improving FM designs on its missions

1. FM should be “dyed into design” vs “painted on”
2. Find a home for FM within Project organization
3. Standardize FM Terminology
4. Identify FM representation techniques and FM design guidelines
5. Establish FM Metrics
6. Apply Continuous Process Improvement to FM
7. **Assess mission-level requirements’ affect on FM complexity**
8. **Assess if FM architecture is appropriate for Mission**
9. Establish and maintain mission-level risk posture
10. **Be skeptical of inheritance claims**
11. Provide adequate testbed resources
12. Capture and understand FM cultural differences among aerospace organizations

NASA’s FM Community has been working together to address these issues

5

NASA's 2012 Spacecraft Fault Management Workshop Overview

Summary:

- Sponsor, Lindley Johnson, NASA SMD/PSD Discovery Program Executive
- 115 attendees plus 60+ via Live WebCast
- >30 organizations from government, industry, academia

Objective: In contrast to the 2008 FM Workshop which identified *problems*, this Workshop concentrated on *solutions*.

Goals:

- Document key findings and make recommendations for future missions
- Mature the contents of the NASA FM Handbook
- Build the NASA FM Community

NASA's 2012 Spacecraft FM Workshop Held April 10-12, 2012

Approach: Assemble key FM players across NASA, industry, government, academia, to

- **Identify FM Capability Gaps**
  - Develop Strawman FM Capabilities Roadmap (Rec #6)
- **Assess FM Architecture Fitness**
  - Perform a FM architectural trade study to enable future missions to assess appropriateness of FM architecture (Rec #7, Rec #8, Rec #10)
- **Work Toward Common Understanding**: Handbook Summit
  - Terminology (Rec #3)
  - FM's relation to SE and to OSMA
  - Panel on "Integrating FM: How does it fit?"
  - Expose how FM is addressed outside of NASA

Breakout Session 2: FM Architecture Assessment

Goal of FM Architecture Assessment Session

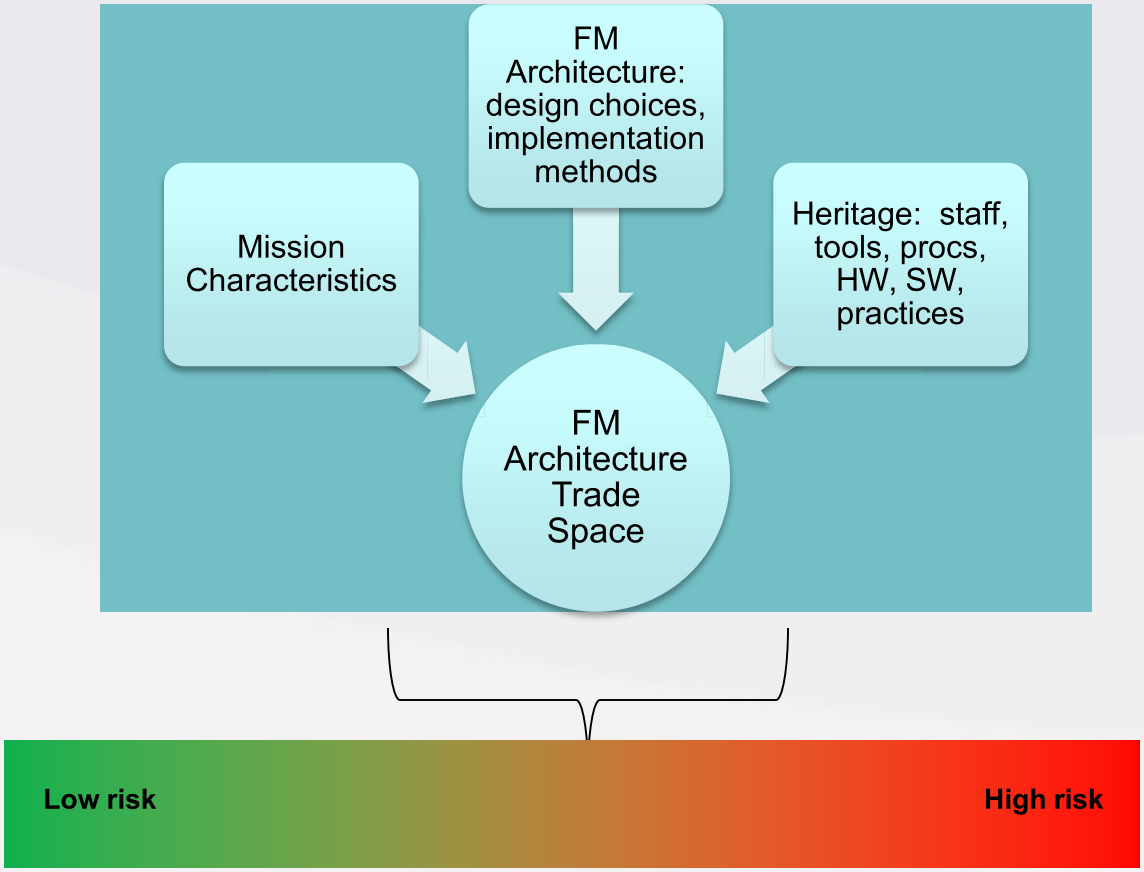
- Provide a way for projects to Assess risk incurred by using a particular FM architecture on a mission

Approach

- Introduce a proposed approach for correlating mission/design/implementation characteristics with quality outcomes
- 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

Architecture Trade Study Approach

- **<u>Concept</u>: Develop an online database to help future projects determine the appropriateness of a FM architecture to a mission**



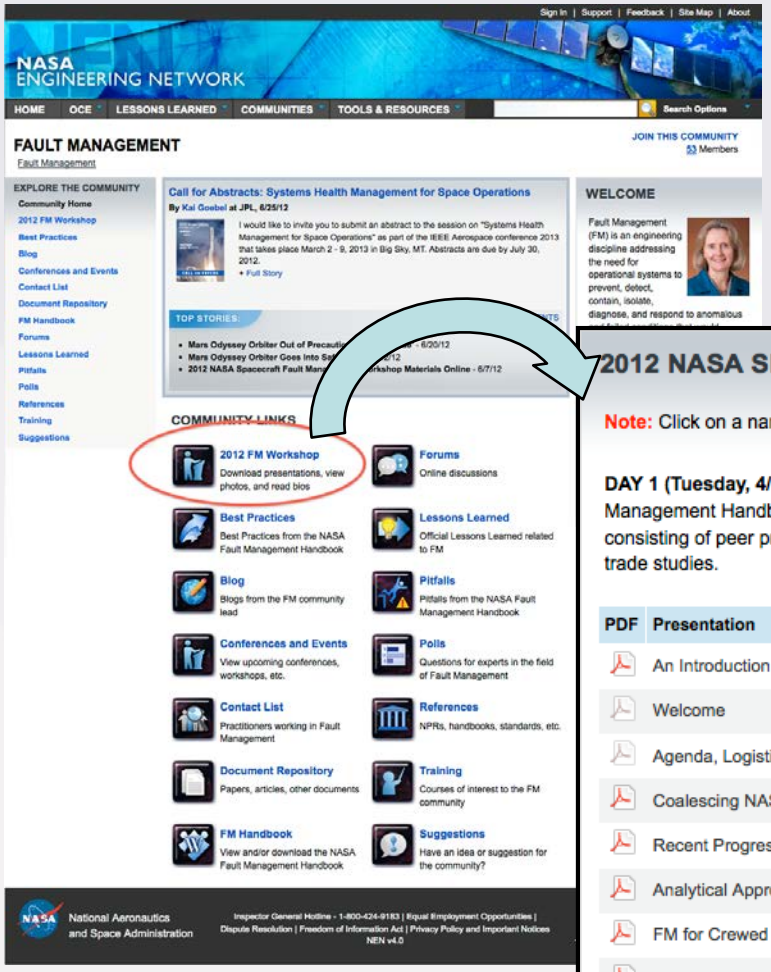
FM Architectures Expressed Through Case Studies

- Enlightening discussions on descriptions of the missions and fault management design solution:
  - *Cassini*, 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)
- 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*

FM Architecture Session Conclusions

- Developing a FM Architecture assessment tool would 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 – 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 optimize QA1, then QA2 and QA3 may be negatively affected"
    - These could be included in a future version of the FM HB
  - Include architecture assessment as an explicit process step in FM development

2012 FM Workshop Presentations/Videos on NEN



FM CoP Home Page on NEN

- Workshop Presentations posted on NEN FM CoP
  - Download Presentation material
  - Watch videos of presentations
  - See photographs from the Workshop
  - Read Speakers' bios

2012 NASA SPACECRAFT FAULT MANAGEMENT WORKSHOP

Note: Click on a name to read more about a speaker.

DAY 1 (Tuesday, 4/10) focused on recent developments, progress and successes in the field of FM. To begin, the draft NASA Fault Management Handbook was presented and discussed, and opportunity was given for community feedback. There were also case studies consisting of peer presentations on new technology developments, on recent mission "success stories," and on recent FM architecture trade studies.

PDF	Presentation	Speaker	Affiliation	Presentation
	An Introduction to the 2012 NASA FM Workshop	Lorraine Fesq	JPL/Caltech	Watch
	Welcome	Lindley Johnson	NASA/HQ	Watch
	Agenda, Logistics, FM Handbook Status	Lorraine Fesq	JPL/Caltech	Watch
	Coalescing NASA's Views of Fault and Health Management	Brian Muirhead	JPL/Caltech	Watch
	Recent Progress in FM	Kris Fretz	JHU/APL	Watch
	Analytical Approaches to Guide Space Launch System FM Development	Jon Patterson	NASA/MSFC	Watch
	FM for Crewed Missions	Carlos Garcia-Galan	NASA/JSC	Watch
	Independent Assessment of NASA Fault Management System Architectures	Phillip Schmidt	Aerospace Corp	Watch
	State Awareness and Decision-Making Architecture	Mark Derriso	AFRL/W-P	Watch
	Fault Management using MBSE Tools and Techniques	Michael Aguilar	NASA/GSFC	Watch

Today's Round Table Goals

"V&V of Fault Management: Challenges and Successes"

Background: FM is typically characterized as "Critical" software, and can measure ~50% of the total flight software

Questions: How are FM architectures evaluated/V&Ved? What techniques are used to V&V this portion of the FSW?

Goals:

- Meet with engineers who have V&Ved FM software on NASA's missions
- Describe unique FM architectures/characteristics that made V&V challenging
- Share approaches that were used, and insights on what worked, what didn't
- Capture Lessons Learned and Best Practices

Today's Round Table Logistics

"V&V of Fault Management: Challenges and Successes"

- Special Breakout Session with emphasis on FM architectures
- Open to US Persons only, to promote open and lively discussions
- Will meet in side room, 3:00pm-5:00pm
- Informal presentations
  - Human-rated: ISS by Sarma Susarla
  - Planetary Lander/Rover: MSL by Shirley Savarino
  - Lunar/L2 Robotic: JWST by Joe Woo
  - Human-rated: MPCV by David Ho
  - Earth Orbiter Robotic: JPSS by Tiffany Lu
- Out-Brief on Day 3, during the Open Program

Backup

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