



Fault-Tolerant Spaceborne Computing Employing New Technologies



Preliminary Findings from NASA SMD/PMD Planetary Spacecraft Fault Management Workshop

Lorraine Fesq

Presented by Kirk Reinholtz

Jet Propulsion Laboratory,
California Institute of Technology

5/29/08

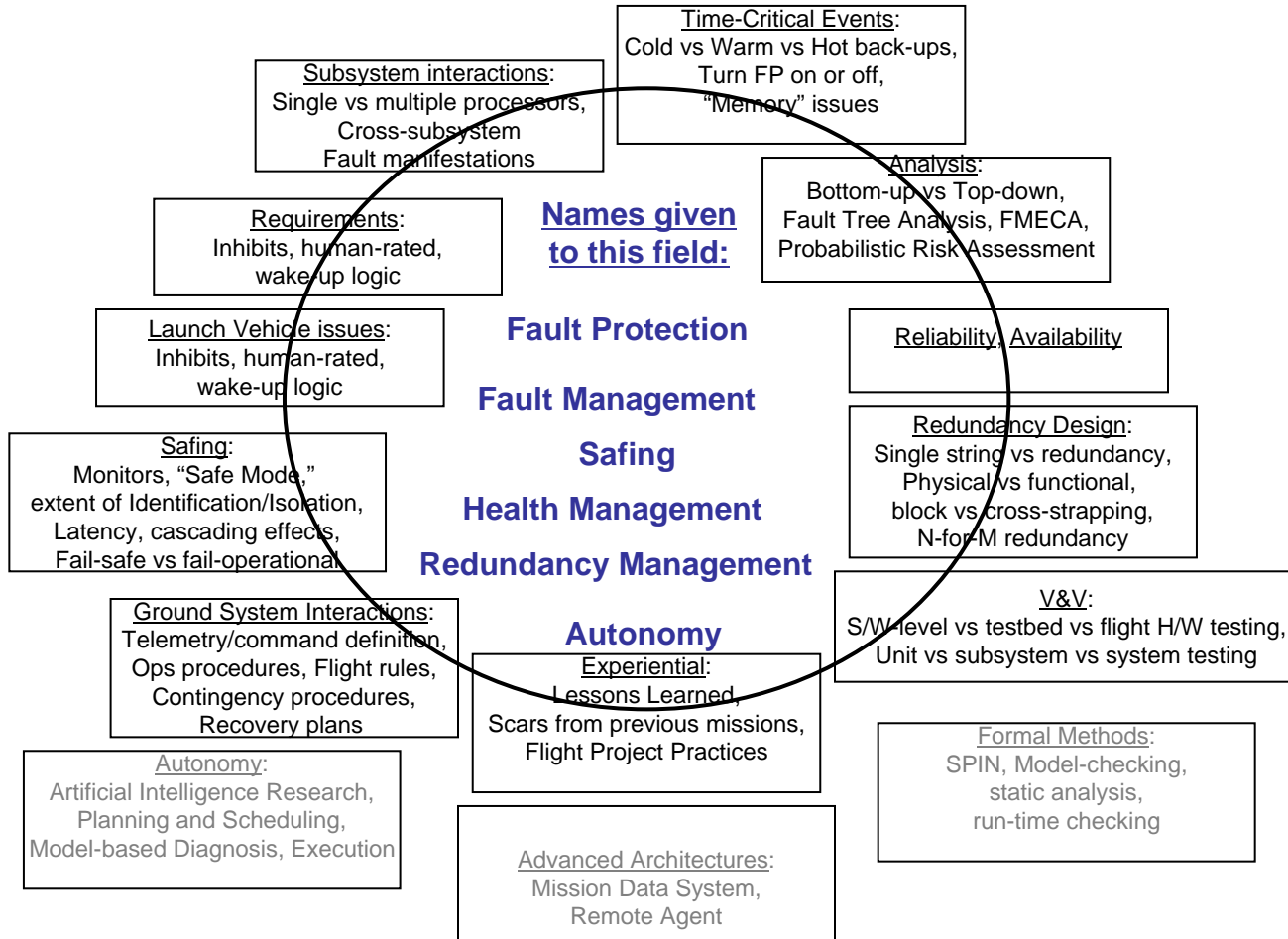
Albuquerque, NM



What is Spacecraft Fault Management?



Note: Workshop covered only a subset of these topics





The Vision



Conveyed by Jim Adams, Deputy Director, Planetary Science Division

- Objective: Ameliorate schedule, cost and predictability challenges that often are faced when testing and operating FM systems.
- Goals: Document key findings and make recommendations for future missions
- Approach: Assemble key players in the spacecraft fault management 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.
- Product: White paper to assist future missions
- Scope: Deep space and planetary robotic missions



Overview of FM Workshop



- Steering Committee
 - John McDougal - MSFC
 - Chris Jones - JPL
 - Steve Scott/Ray Whitley - GSFC
 - George Cancro & Dave Watson - JHU/APL
 - Technical Coordinator: Lorraine Fesq - JPL
- Held April 14-16, 2008 in New Orleans, LA
- >100 attendees from 31 organizations -- government, industry and academia
- Three days of activities
 - Expose Current State of FM through Case Study presentations
 - Identify and characterize cardinal issues via Breakout Sessions
 - View Future Directions via Poster Sessions and Invited Speakers



FM Workshop Goals



- Identify issues plaguing Fault Management in unmanned, autonomous spacecraft today
- Provide guidance for future programs and technology development
 - **Lessons Learned**
 - **Best Practices**
 - **Opportunities for investment**
- Target Audience: Current and future practitioners (FM, SE, SWE, V&V, etc.), proposal evaluators to assess viability of proposals, reviewers and program managers to evaluate credibility of program plans
- Not looking to produce a recipe or a set of standards. Instead, expectations associated with different approaches
- Rise above institutional preferences!

**This workshop was intended to start the discussions.
“First annual”**



FAULT MANAGEMENT WORKSHOP

Agenda



April 13, 2008	CDT	Day 1 - April 14, 2008	CDT	Day 2 - April 15, 2008	CDT	Day 3 - April 16, 2008				
6pm - 8pm: Registration & Pre-event Reception	7:00	Registration				7:15	Poster Session			
	8:00	Welcome/Introductions/Logistics	8:00	Parallel Break-out Sessions: Logistics						
	8:15	Why Are We Here? - Jim Adams, HQ	8:15	Architectures Session Chair - George Cancro, APL	V&V Session co-Chairs - Ray Whitley, GSFC & Chris Jones, JPL	Practices, Processes, Tools Session Chair - Dave Watson, APL	8:15	Future Directions: "New Directions in V&V: Evidence, Arguments, and Automation" - invited speaker John Rushby, SRI		
	8:30	Scope/Goals of the Workshop - Lorraine Fesq, JPL							9:15	Session Report - Architectures
	9:00	Current State: Case Studies from Recent Missions							9:45	Session Report - V&V
	9:15	"MER FLASH Anomaly" - Glenn Reeves, JPL	9:45	BREAK + Poster Setup			9:45	Session Report - Practices, Processes, Tools		
	9:45	"Dawn Lessons Learned" - Jonathan Rustick, OSC	10:00	Architectures Session	V&V Session	Practices, Processes, Tools Session	10:15	BREAK + Poster Session		
	10:15	"TRMM Power System FM Case Study" - Kris Naylor, CSC					10:45	Future Directions: "Model-based Monitoring of Complex Systems" - invited speaker Brian Williams, MIT		
	10:45	BREAK					11:00	Lunch		
	10:55	"Case Study Results/Findings from SMC Flight Software Projects" - Douglas Buettner, Aerospace Corp	11:30	Lunch		Session Chairs Meeting	Noon	Steering Committee Meeting		
	11:15	"MRO In-Flight Articulation Anomaly" - Wayne Sidney, LM; Tim Halbrook, LM; Todd Bayer, JPL	12:30	Architectures Session	V&V Session	Practices, Processes, Tools Session	1:00	Group Discussion - Integration of Findings		
	Noon	Lunch - "Spacecraft Fault Management, a Historical Perspective" - invited speaker Gentry Lee, JPL					3:00	Closing Remarks - Adjourn		
	1:00	"FM Organizational and Process Issues" - Stephen Johnson, MSFC	2:00	BREAK + Poster Session			3:15	Steering Committee and Session Chairs Meeting		
	1:30	"Hubble Space Telescope FM Lessons Learned" - Brian Vreeland, Space Systems Integration	2:15	Architectures Session	V&V Session	Practices, Processes, Tools Session	3:45			
	2:00	"JWST Architecture and Processes" - Judy Tillman, NGST								
	2:30	"STEREO AHEAD IMU Anomaly" - Mike Trela, APL	3:30	Future Directions: "Improving System Quality through Software Architecture" - invited speaker David Garlan, CMU						
	2:50	BREAK	4:30	Poster Session		Steering Committee Meeting				
	3:00	"Overview of FM Concepts Used on Typical Ball Spacecraft" - Christian Meyer, Ball Aerospace	5:15							
	3:30	"New Horizons Autonomy -- Path to Launch" - Adrian Hill, APL								
	4:00	"Cassini Leaking Regulator Anomaly" - Brad Burt, JPL								
	4:30	Breakout Session Descriptions - Session Chairs								
	5:00	Steering Committee Tag-up								
	5:15	Breakout Session sub-committee meetings								

Room Legend
French Quarter Bar - 3 rd floor
Salon 3 - Ballroom Level
Salon 1 - Ballroom Level
Crescent View - 12 th floor
Acadia - Ballroom Level
Broadmoor - Level 1
Salon Foyer (Posters & Breaks)



FAULT MANAGEMENT WORKSHOP

Invited Speakers



A Different Point of View

Program included four Invited Speakers, whose charge was to

- Help us understand how we arrived at our current situation
- Expose us to fundamental concepts to help us gain perspective and organize our field
- Introduce alternate approaches
- **Gentry Lee, Jet Propulsion Laboratory, California Institute of Technology**
 - Chief Engineer, Solar System Exploration Directorate
 - “Spacecraft Fault Management, a Historical Perspective”
- **David Garlan, Carnegie Mellon University**
 - Professor, Computer Science; Director, Software Engineering Professional Programs
 - “Improving System Quality through Software Architecture”
- **John Rushby, SRI International**
 - Program Director for Formal Methods and Dependable Systems, Computer Science Laboratory
 - “New Directions in V&V: Evidence, Arguments, and Automation”
- **Brian Williams, Massachusetts Institute of Technology**
 - Professor of Aeronautics and Astronautics; Director, Autonomous systems Laboratory (ASL); Member, Computer Science and Artificial Intelligence Laboratory (CSAIL); Member, Space Systems Laboratory (SSL)
 - “Model-Based Monitoring of Complex Systems”



FAULT MANAGEMENT WORKSHOP

Results (1/2)



- **Preliminary Key Findings**

- Standard Terminology and Design Representation required - FM systems are difficult to review and to communicate
- Lack of FM Consideration in Early Mission Phases is Partial Cause of Unplanned Cost/Schedule Growth during System Development.
 - FM must be considered from Day 1 on a project, not as an add-on at the end
 - FM should be “dyed into design” rather than “painted on”
- FM needs to be recognized as a discipline -- or maybe not....
 - Needs the attention of an individual discipline - create a WBS element for FM
 - Inherently tied to the rest of the system architecture – is a system’s engineering function
 - Explicit consideration of FM as proposal evaluation criterion
- Practices, processes, system definition & analysis tools haven’t kept pace with increase in complexity
- Must agree to risk tolerance posture early in the program
 - “Single fault tolerant” has varying definitions (single fault or error, fault plus error, etc.)
 - Design against possibility vs. Design against probability
- Indications of problems are usually there, but we don’t see them
 - During testing: Schedule pressure => did the test pass the given criteria? vs looking at what a test tells us about the system
 - In-flight: Don’t have visibility through telemetry
- Flexibility: friend or foe?



FAULT MANAGEMENT WORKSHOP

Results (2/2)



- **Opportunities for Investment**

- Establish common FM vocabulary and taxonomy
- Trade space of existing and future FM architectures -- how each handles complexity, flexibility, growth, risk and testability.
- Collect metrics to substantiate findings - e.g., staffing profile through I&T
- Establish FM performance metrics -- e.g., reliability, coverage, operational availability, autonomy
- Consensus on FM stance for different classes of missions
- Establish design criteria for FM systems and Principles with Rationale & Examples
- Produce a roadmap or “decadal survey”
- Create a complexity analysis tool for use in Concept Development and Requirements Definition
- Guidance across NASA for when you need various degrees of autonomy and/or complexity in FM system
- Technology Demonstration Program to validate FM technology for future missions
 - Need someone to accept the cost-risk of using a new technology to move forward



Current/Future Plans



- Develop secure website: presentations, findings, white paper development
- Digest all materials -- Case study presentations, Survey findings, poster presentations, academic points of view, Break-out Session results
- White Paper capturing Lessons Learned, Best Practices and Opportunities for Investment
- Determine a way forward - How can we make use of these findings?
 - Keep the dialog going
 - Website to share Workshop material
 - Monthly Steering Committee meetings
 - NASA FM Working Group to continue discussions?
 - Future workshops or sessions at related conferences?
 - Technical journal or special issue of an existing journal focused on FM?
 - Explore standardization opportunities -- are there areas that NASA should standardize? (e.g., terminology and taxonomy)
 - Training/Education -- within our community and students for pipeline
 - Collect Schedule and Cost metrics to form bases of estimates
 - Opportunities for in-flight Technology Demonstrations (e.g., via extended missions)
 - Show the business case (return on investment possibilities) in terms of reducing technical and programmatic risk by utilizing some of these techniques
- Review feedback from participants and incorporate improvements for next Workshop



L³ and Take-Away Messages



- Architecture: Surprisingly similar across organizations.
 - Rule-based FM architectures don't scale. Time for a change?
 - Not sure if rule base increasing due to additional complexity or unmanaged rule population
 - New approaches in the cue
 - Need business case - cost/risk to use vs cost/risk to not use
- V&V: Updated tools & approaches ready now
 - Static analyzers beginning to take root. Everyone should use them
 - Model checkers in the pipeline
- Practice, Processes and Tools: Communication is key
 - Terminology Standardization is low hanging fruit
 - Explicit Consideration of FM as Proposal Evaluation Criterion
 - Elevate the attention and scrutiny
 - Could help with metrics collection
 - Representation methods needed. SysML?
 - References needed - teaching text, Practitioner's Handbook