

FM Workshop Panel

**Integrating Fault Management: How
Does It Fit?**

Comments to the FM Handbook indicated differing viewpoints concerning

- Scope of FM
- Integrating FM into engineering processes
- Assigning FM roles and responsibilities

Panel is intended to start a broader community discussion

1. How does a project strike a balance between the integrated system aspects of FM and the development and delivery of the required FM flight products?
2. How does a project manage the overlapping roles and responsibilities between FM, SE, and safety and reliability?
3. How does a project allocate the responsibilities of protecting against faults, predicting future failures, and post-facto analysis?
4. To what extent should mission type: human flight vs. robotic, single mission vs. repetitive flight; deep space vs. earth orbiter; mission size, duration, and complexity drive the approach to integrating FM?

Panel Agenda

		Duration	Total Duration
Overview (Purpose, format, panel introductions)	Moderator	5 minutes	5 minutes
Panelist Viewpoints	Panelists	7 minutes, each	42 minutes
Organizational comments (format and guidelines for audience participation)	Moderator	1 minute	1 minute
Audience Participation	Participants	Comments/Questions: 2 minutes each; Panelist response to question: 1 minutes each	40 minutes
Wrap-Up (summary of issues, follow up plans for continuing discussion via web, coming to closure, incorporating into the document)	Moderator	2 minutes	2 minutes

Panelists



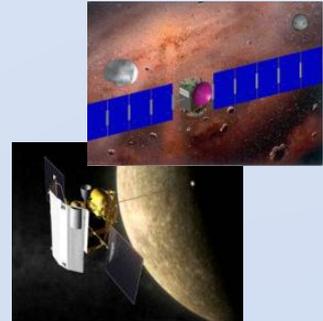
Michael Aguilar

- Manages the software program at Goddard Space Flight Center (GSFC)
- Serves as the NASA Engineering and Safety Center (NESC) Discipline Expert in Software Engineering
- Areas of interest: software development for spacecraft C&C systems, flight simulators, submersible robotics, nuclear reactor monitoring and control systems, and safety-critical embedded software
- Masters degree in Software Engineering, Carnegie Mellon University



George Cancro

- Manager for the MPCV Avionics, Power, and Software (APS) office at JSC
- Supported a variety of positions including Shuttle and Space Station assignments, primarily in the areas of avionics and software
- Areas of interest: flight avionics, flight software and data system, flight power and wiring systems, and the ground hardware, software, and labs required to test and verify these systems



Carlos Garcia-Galan

- Deputy Manager for Mission and Systems Integration of the MPCV project
- Supported multiple ISS-Shuttle assembly missions and ISS increment operations between missions as a flight controller
- Participated in multiple IR&D projects in the areas of IVHM, Intelligent systems and Mission Management for manned spaceflight applications at Honeywell.
- Technical Lead for the System Management function on the Lockheed Martin Orion design



Panelists (cont.)



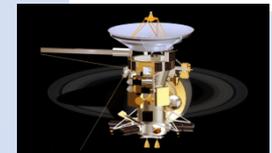
Stephen Johnson

- Associate research professor with the Center for Space Studies at the University of Colorado at Colorado Springs
- Analysis Lead for Mission and Fault Management in the Space Launch System program at MSFC
- Worked on developing practices and concepts for System Health Management and Fault Management since 1985
- General editor for *System Health Management: With Aerospace Applications* (2011)



Robert Rasmussen

- JPL Fellow, and the Architect for Europa mission studies at JPL
- Served as Chief Technologist and Chief Engineer in JPL technical divisions for software and systems engineering
- Worked Fault Management for the Voyager and led guidance and control systems engineering for Galileo and Cassini
- Doctorate in Electrical Engineering



Jonathan Wilmot

- Software architect for the Goddard core Flight Executive (cFE) and Core Flight System (CFS) software product lines
- Served in lead technical and software systems engineering roles ranging from helicopter avionics to lunar landers, including the Small Explorer series of spacecraft at NASA
- Bachelors degree in Computer Science, University of Maryland



The Fault Management “Waterfall”

Michael Aguilar

NASA Engineering and Safety Center

NESC Software Discipline Expert

NASA Technical Fellow in Software

Michael.L.Aguilar@nasa.gov

The Fault Management “Waterfall”

If the fault management (FM) process depends on all requirements and system designs to be completed before FM system development:

1. FM falls behind in PDR/CDR discussions/decisions
2. The FM system becomes an ad hoc layer over the already completed design
3. Modification of the implemented design to meet FM requirements occurs late in development

“Off..Off..Off with his Head!”

- Modify the NASA process to include an Architecture Review early, followed by PDR and CDR, etc.
 - Require the Architecture Review to detail the operation and use of the system
- Require PDR to demonstrate a system level understanding of the architecture and how it meets requirements
 - Fault management required to be at a specific level of maturity to pass PDR
- Require PDR to detail how the system is to be verified and integrated
 - “test it a lot” is not an acceptable answer
 - Even “test as you fly” is not acceptable answer
 - Simply checking boxes for a requirement’s verification method as Test, Analyze, Demonstrate, etc. is not enough
- Allow presenters to present directly from design tools and artifacts
 - Present actual Design Documentation
 - Present an appropriate level of complexity allowing “drill down” when needed
 - Reduce the PowerPoint “cartoon” efforts

Computer-Based Control System Safety Requirements

SSP 50038 Revision B (November 17, 1995)

It is acceptable for a unique set of computer based control system requirements to be used for the control of hazards, provided these requirements are reviewed by the SRP and found acceptable. The SRP will use appendix A as a tool to assess the acceptability of these requirements. Each item in appendix A shall be addressed with either compliance, or an explanation why an item does not apply. The following is a listing of the top level items:

- a) Separation of Commands/Functions/Files/Ports
- b) Interrupts
- c) Shutdown/Recovery/Safing
- d) Preventing/Precluding/Disallowing Actions
- e) Memory/Storage/Data Transfer
- f) Verification/Validation Checks
- g) Logic Structure/Unique Codes/Interlocks
- h) Monitoring/Detection
- l) Reasonableness Checks
- j) Initialization/Timing/Sequencing/Status Checking
- k) Operator Responses/Limitations
- l) Operator Notification
- m) General/Miscellaneous

George Cancro

Integrating FM: How does it fit?

- Start with Metrics (PM Level)
 - Cost – Ex: separate WBS!
 - Schedule – When is done? Ex: Faulted System Tests
 - Complexity – “After the fact” moving to “predictive”
- Allocation of Requirements and Roles
 - Begin Top down in everything (*fight tendency to get detailed...start with philosophy*)
 - Allocate FM roles – Ex: APL FM vs. Autonomy
 - Allocate Req to h/w, s/w, autonomy, ops
- Focus on Testing
 - Near Term: Critical Sequences (events) are unifying
 - Far Term: What limits our technology growth!!

Fault Management Scope in Theory and in Practice

Go to slides

Dr. Stephen B. Johnson
sjohns22@uccs.edu and
stephen.b.johnson@nasa.gov

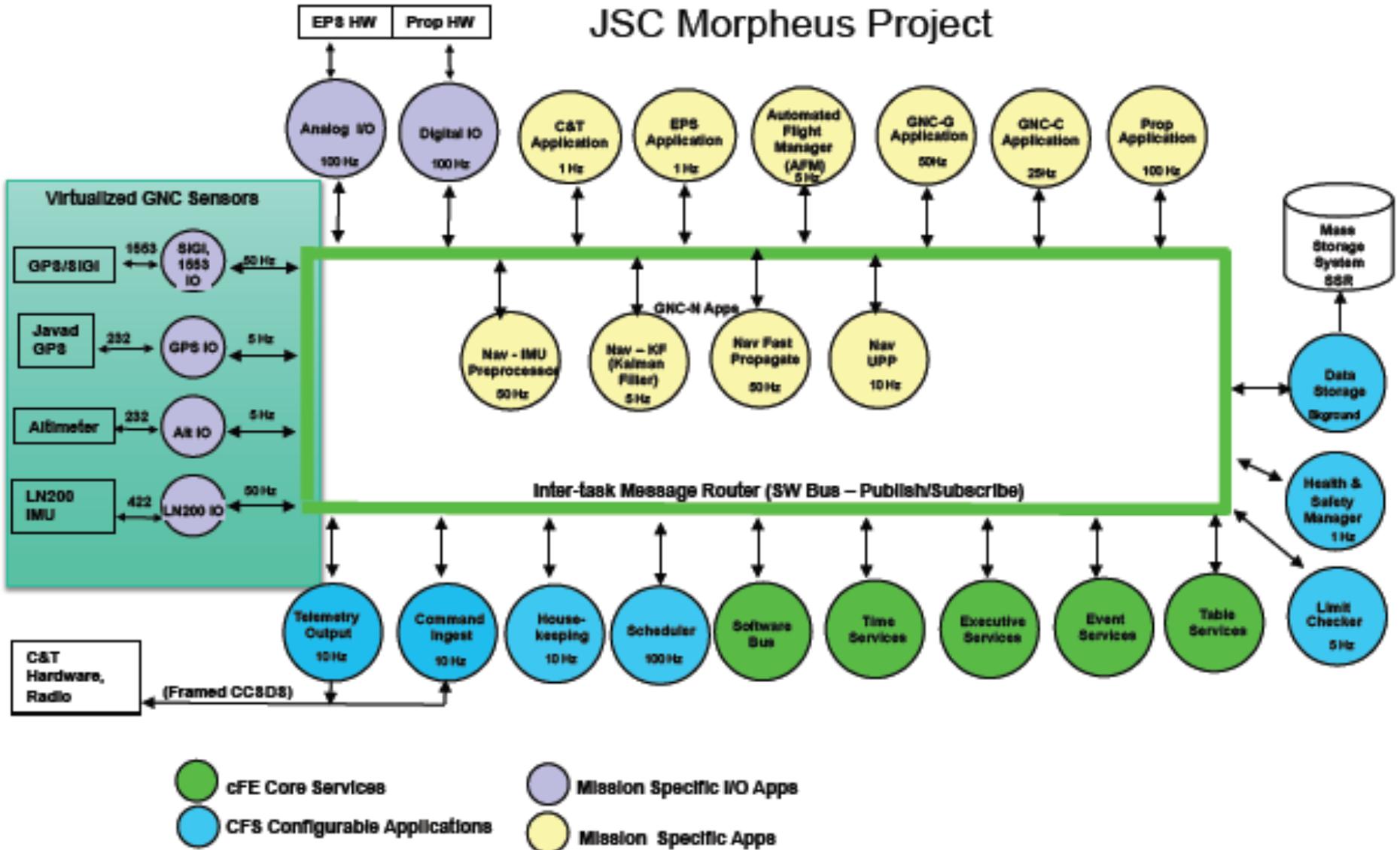
NASA MSFC EV43 Integrated System Health Management and Automation Branch

&

University of Colorado at Colorado Springs - Jacobs ESTS

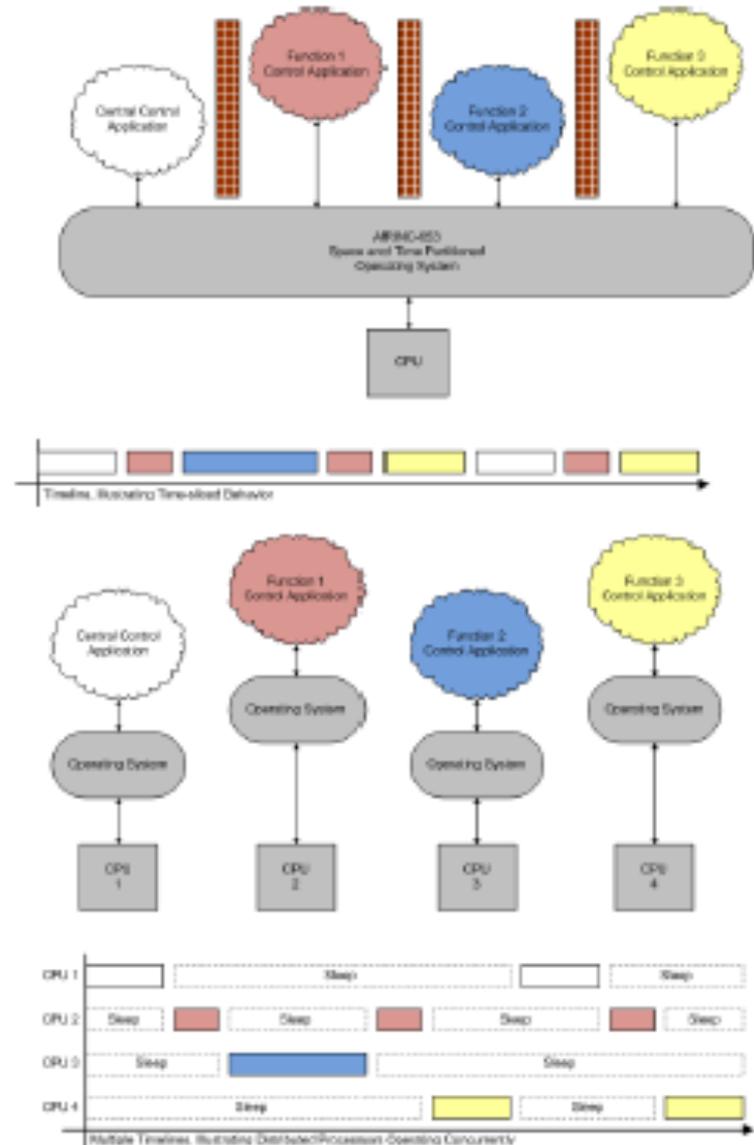
Jonathan Wilmot

System-Wide FM as Plug-ins



Partitioning and FM

- **Virtual partitioning:**
 - Single CPU:
 - CPU failure takes down everything
 - Partitioned into multiple virtual CPUs:
 - Space and time partitioning
 - Theory - prevents a software error in one application from affecting others
 - ARINC-653:
 - Purpose – to ease certification costs, when applications of varying criticality (e.g., Level-A vs. Level-E) reside on the same CPU
 - Requires a high-performance machine:
 - Increased power consumption
 - generally more SEU susceptible
- **Distributed partitioning:**
 - Multiple CPUs:
 - CPU failure has limited affectivity
 - Real partitioning:
 - Space - geographical separation
 - Time - TDMA system bus behavior
 - Machines can be scaled to requirements:
 - Low-power, rad-hard



Participant Guidelines

- We want to hear from as participants many as possible
- 2 minutes
 - Identify yourself and affiliation
 - Present question or comment
- Questions will be responded to by (optionally) all panelists; no more than 1 minute per response

Wrap-Up