

A composite image of the solar system. On the left, a large portion of Earth is visible, showing blue oceans and white clouds. A satellite is in orbit around Earth. In the center, the Sun is a bright orange and yellow sphere. The Moon is a smaller, grey sphere in the middle ground. To the right, Mars is a reddish-brown sphere. In the bottom right, Jupiter is a large, striped sphere. The background is a dark space filled with stars and a nebula.

V&V of Fault Management: Challenges and Successes

L. Fesq, Jet Propulsion Laboratory, California Institute of Technology

K. Costello and D. Ohi, NASA IV&V Facility

T. Lu, TASC

M. Newhouse, CSC/NASA MSFC

Infotech@Aerospace, August 19-22, 2013, Boston, MA



FM V&V: Challenges and Successes

- Summary of special Breakout Session held at 2012 IV&V Workshop
- IV&V in unique position
 - Interacts with projects across all NASA domains
 - Capture FM approaches to better understand how FM concepts, principles and architectures are applied throughout NASA
- Session enabled IV&V teams to uncover common FM V&V themes, challenges and recommendations



Introduction

- FM responsible for protecting space asset and ensuring mission success even in presence of faults
- Portion of FM implemented in software keenly scrutinized by a project's IV&V team
- NASA's space exploration goals* → increased capability, complexity, robustness → increased need to predict, detect, diagnose, prevent, respond to off-nominal conditions
- Comet Surface Sample Return, Lunar South Pole-Aitken Basin Sample Return, Saturn Orbiter, Mars Sample Return, Venus In Situ Explorer, Io Observer, Lunar Geophysical Network, Mars Cache (MAX-C), Jupiter Europa Orbiter (JEO) – EHM, Uranus Orbiter and Probe
- Human mission to deep space



*Identified in the NRC's "Visions and Voyages for Planetary Science in the Decade 2013-2022"



FM V&V Breakout Session

Goals and Topics

- Session Goals
 - Convene engineers who have analyzed NASA's FM software;
 - ID FM architectures/characteristics that made V&V challenging;
 - Share approaches that were applied to analyze FM architectures, including insights on what worked, as well as what did not work;
 - Capture Findings and Recommendations
- Topics
 - Human-rated/long-duration: ISS
 - Planetary Lander/Rover: MSL
 - Lunar/L2 Robotic: JWST
 - Human-rated crew vehicle: MPCV
 - Earth Orbiter Robotic: JPSS



Common themes in FM IV&V

- FM is a critical element of NASA's Flight Systems
- Current FM IV&V approaches have dealt only with spacecraft
- IV&V still in learning phase (as are many developers)
- Mission domains had similar approaches to architecting FM
 - Detection/monitors
 - Persistence
 - Responses
 - Levels/tiers
 - Priorities
 - Detection-response many-to-one relationships



Common FM IV&V Challenges

- System complexity and changing mission reqs driving need for more/better FM architectural strategies, design principles, patterns
 - FM is a SE discipline – needs consistent implementation
 - Ambitious goals -> more robust, capable features; e.g., humans to deep-space
 - Increasing role of software drives more HW/SW interactions



Common FM IV&V Challenges – cont.

- Interactions between different FM tiers in the system generate complexity
 - Systems that have local and system responses introduce separate zones of FM control that could conflict with one another; e.g., race conditions
 - Special analyses needed to verify complex, integrated, tiered FM systems
- Priorities introduce challenges
 - IV&V's role becomes more complex due to need to understand potential response interrupts/interferences



Common FM IV&V Challenges – cont.

- FM information not centralized
 - FM reqs, architecture, design, V&V information often are scattered among many artifacts
 - IV&V usually must search through a wide array of artifacts to piece together comprehensive FM view
 - Leads to FM information that is not consistent or cohesive
 - E.g., low-level FM behaviors added during design phase but not fed back into reqs spec



Common FM IV&V Challenges – cont.

- Differences in FM terminology across artifacts within a development project
 - Occurs across subsystems and components due to development by different contractors
 - Creates additional complexity since terms may be interpreted differently
 - Leads to implementation of incorrect behaviors





Common FM IV&V Recommendations

- It is NOT true that the FM architecture needs to be delayed until the nominal system has been designed
 - Assess FM drivers early in a project life
 - Mission characteristics
 - Required fault tolerance
 - Unattended operations requirements
 - Redundancy requirements
 - Early FM framework
 - allows the IV&V Team, as well as the development team, to reason about the planned FM approach
 - Example: monitor design pattern introduced late





Common FM IV&V Recommendations – cont.

- Focus on & monitor FM design throughout lifecycle
 - Evaluate FM at major milestone reviews
 - FM engineer identified on the program?
 - FM reqs properly defined and flow down to subsystem?
 - FM architecture defined?
 - FM architecture helps avoid coupling, race conditions, and retriggering FM responses?
 - System-level & local-level FM detailed-designs defined; e.g., coding patterns, HW vs. SW dependencies?
 - Are test plans/procedures traced to system FM reqs?
 - Are there test reports for all system FM testing?





Common FM IV&V Recommendations – cont.

- FM requires a system perspective
 - Not merely a subsystem responsibility
 - Understand responses to faults, potential for interactions between fault responses, how responses affect other processes
- When performed only at the subsystem level, system-wide view of fault behavior and response interactions become challenging
 - Capture comprehensive view of faults to enable analysis of end-to-end responses
 - Dynamic analyses needed to understand interactions





Common FM IV&V Recommendations – cont.

- Successful solutions to FM V&V are using models to represent end-to-end FM detection mechanisms and responses.
 - E.g., simple spreadsheets - > relational databases
 - Models offer verification benefits
 - Facilitates ability to support top-to-bottom consistency checking throughout lifecycle
 - Enables querying to ensure constraints are met
 - Provides systematic approach to manage/track FM data across disparate sets of artifacts
- Establish standardized set of terminology, design principles and patterns



Summary

- Key FM V&V Themes and Recommendations from 2012 IV&V Workshop Breakout Session
- Undisciplined FM discipline causes rippling effects
- IV&V and projects would benefit from NASA guidelines on designing, developing, testing, operating FM for different mission types
 - Establish FM as discipline would promote FM info to be organized/centralized
 - Facilitate cohesive, system-wide view of FM elements
 - Support assurance of system safety
 - Allow IV&V analyses to better align with project tasks

