ASSURANCE OF FAULT MANAGEMENT
RISK-SIGNIFICANT ADVERSE CONDITION AWARENESS

RHONDA FITZ, NASA IV&V PROGRAM
DECEMBER 13, 2016
Background

- **Approaches to FM** vary even among similar mission types
  - Deep Space Robotic, Human Spaceflight, Earth Orbiters, Launch Vehicles, Ground Systems
  - Large variance in approach, design, and terminology

- **As mission complexity increases, so does FM complexity**
  - FM may be handled on a subsystem basis on these large, complex missions under the flight software umbrella
  - FM system documentation is often relegated to various subdomain requirements and design artifacts
  - Architectural analysis enables FM capability assessment

- How can we improve **software assurance strategies** given the current visibility into these increasingly complex architectures?

**FM Architectures SW Assurance Research Program (SARP) Initiative**
**Challenges in Assurance of FM**

- Increasing FM complexity goes beyond traditional fault protection with the goal of not only averting catastrophe, but also maintaining capability.

- FM systems, many times architected as reactive components embedded within the overall software system, must be validated against higher-level system capability requirements.

- Off-nominal conditions are challenging to identify comprehensively, understand completely, and ascertain the optimal response to mitigate risk.

- Existing software development and assurance practices applied to FM systems need improvement to provide a high level of assurance.
FM Architectures Initiative

Description/Goals
- Analyze FM architectures from a varied set of NASA space missions to develop or expand upon the current FM architecture classification and its terminology
- Investigate IV&V methods and assurance strategies used on FM systems and their possible strengths and weaknesses
- Assess the visibility of FM architectures for a robust software assurance strategy

Products
- FM Architectures, with associated assessments of attributes and associated complexity, visibility
- IV&V Assurance Objectives and Analysis Techniques
- Final report

Value to NASA
- Technical Reference (TR) matrix of the high-level characteristics of select FM architectures and the IV&V methods used on them
- TR on the low-level features of FM systems specific to mission domain and/or developer
- Updates to the Architectures and V&V sections of the NASA FM Handbook
# Missions Investigated

<table>
<thead>
<tr>
<th>Name</th>
<th>Mission Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mars Science Laboratory (MSL)</td>
<td>Deep Space Robotic</td>
</tr>
<tr>
<td>International Space Station (ISS)</td>
<td>Human Spaceflight</td>
</tr>
<tr>
<td>James Webb Space Telescope (JWST)</td>
<td>Deep Space Robotic</td>
</tr>
<tr>
<td>Multi-Purpose Crew Vehicle (MPCV)</td>
<td>Human Spaceflight</td>
</tr>
<tr>
<td>Joint Polar Satellite System (JPSS)</td>
<td>Earth Orbiter</td>
</tr>
<tr>
<td>Magnetospheric Multiscale (MMS)</td>
<td>Earth Orbiter</td>
</tr>
<tr>
<td>Geostationary Operational Environmental Satellite R-Series (GOES-R)</td>
<td>Earth Orbiter</td>
</tr>
<tr>
<td>Solar Probe Plus (SPP)</td>
<td>Deep Space Robotic</td>
</tr>
<tr>
<td>Space Launch System (SLS)</td>
<td>Launch Vehicle</td>
</tr>
</tbody>
</table>
Early Goals Met, Exceeded

- Analyzed **FM architectures** from a small but varied set of current and former space missions to develop or expand upon the current FM architecture classification and its terminology
  - Consequence of various developers/domains is a broad range of FM architectures and styles
  - NASA FM Handbook should be regarded as a source of reference for common terminology
- Investigated IV&V methods and **assurance strategies** used on FM systems and their possible strengths and weaknesses
  - Resulting in TR that provides valuable insight to future software assurance and IV&V efforts
- Assessed the **visibility** of FM architectures for a robust software assurance strategy
  - Artifacts and insight into FM system provided by projects vary
- Determined benefits and limitations in the application of current software assurance methods and **IV&V techniques** across the lifecycle
  - Which methods work? Which don’t? Have methods been developed that are not documented and should be more widely used?
  - Captured recommended practices and pitfalls for updates or additions to FM Handbook
- Disseminated **results** via conference presentation and paper, final report, and input to the NASA FM Handbook/Community of Practice
  - Sharing results was the most crucial goal, in order to expand the discussion and formulate future direction for the FM community
Refined Improvement Goals

• Improve and expand upon the current analysis of NASA mission FM with a Technical Reference Suite for more comprehensive coverage of architecture, visibility, and assurance strategies
  – Analyze additional FM architectures, specifically from a Launch Vehicle space mission to expand upon the current FM architecture classification and its terminology
  – Further investigate SA and IV&V methods and assurance strategies used on FM systems to identify benefits and limitations in their application across the lifecycle
  – Learn more about the visibility of FM architectures within a nontraditional development environment, particularly within an Agile framework, using a model-based methodology
• Develop and refine the prototype Adverse Condition Database for access to IV&V project fault, failure, and hazard data for more rigorous assurance and risk reduction with Q3 analysis
• Disseminate results with FM SA Knowledge Exchange via conference presentations and papers, roundtables, and reports
FM Architectures Encore Initiative

Description/Goals

- Improve and expand upon the current analysis of NASA mission FM in a Technical Reference suite for more comprehensive coverage of architecture, visibility, and assurance strategies
- Develop and refine the prototype Adverse Condition Database for access to IV&V project fault, failure, and hazard data for more rigorous assurance and risk reduction with Q3 analysis
- Socialize products and findings with FM Software Assurance Knowledge Exchange

Products

- FM Architecture Matrix TR, FM Visibility Matrix TR, and dynamic FM Assurance Strategy TR with supporting IV&V methods employed across the development lifecycle
- Repository of NASA mission adverse conditions and associated project metadata
- Technical presentations, conference papers, and informal learning opportunities

Value to NASA

- Promoting FM knowledge for IV&V Program, SARP, and NASA Engineering Network
- Improved assurance from the provision of more comprehensive data
- More rigorous Q3 analysis from identification of off-nominal scenarios
- Increased efficiency of analyst workflow and broader test coverage
- Greater focus on FM and project areas of vulnerability or high risk
Research Thrusts

- **TR products** will be improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches
  - Investigate ways to integrate FY16 findings and products into SA and IV&V methods
  - Continue to develop a quick reference guide to improve TR usability for SA analysts across Agency
  - Capture challenges of Launch Vehicles, Agile development, and model-based FM
TR Suite Screenshots

FM Architectures Technical Reference

Created by Gorak Whittman, last modified on Sep 01, 2016

The TR suite generated by the SARP FMA Initiative consists of three distinct segments.

The Architecture Matrix

The Architecture Matrix is the result of a survey of nine IV&V projects, regarding the structural and functional features of their FM architectures. It is summarized by mission domain: Earth Orbiter, Deep Space Robotic, Human Spaceflight, and Launch Vehicles. The Architecture Matrix is accompanied with diagrams detailing the common structural and functional architecture types we have found in our investigations.

The Assurance Strategy Reference

The Assurance Strategy Reference Table is a collection of assurance objectives and conclusions related to FM from projects across IV&V in various lifecycle phases. It is intended for use as a reference guide of dos (and, in some cases, do-nots) for IV&V and other assurance projects planning and designing an assurance regimen of their FM systems.

The Visibility Matrix

The Visibility Matrix is an aggregation of observations, from research results and SMEs, of some of the typical challenges IV&V analysts face when trying to gain insight into the FM system and its architecture. These observations are associated with development artifacts (some specific, some more notional), and examples are provided of methods or strategies used by projects in the past to overcome visibility challenges.
The TR suite generated by the SARP FMA Initiative consists of three distinct segments.

**General Findings**

The Architecture Matrix was generated from survey responses gathered from FM SMEs on nine IV&V projects that fall into four broad mission domains. Results were aggregated on these domains to form generalizations on the trends seen in the architecture data during collection.

<table>
<thead>
<tr>
<th>Earth Orbiter Missions</th>
<th>Deep Space Missions</th>
<th>Human Spaceflight Missions</th>
<th>Launch Vehicle Missions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOES-R</td>
<td>MSL</td>
<td>ISS</td>
<td>SLS</td>
</tr>
<tr>
<td>JPSS</td>
<td>JWST</td>
<td>MPCV</td>
<td></td>
</tr>
<tr>
<td>MMS</td>
<td>SPP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The full architecture matrix is presented at the bottom of the page.
Research Thrusts

TR products will be improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches:
- Investigate ways to integrate FY16 findings and products into SA and IV&V methods
- Continue to develop a quick reference guide to improve TR usability for SA analysts across Agency
- Capture challenges of Launch Vehicles, Agile development, and model-based FM

TR suite has been improved and expanded for more comprehensive coverage and ease of sharing information:
- Populate AC Database with additional project data from IV&V and SSO projects
- Align with TRs enabling behavioral and hazard connections
- Continue to develop more efficient user interface for typical SA or IV&V analyst workflow scenario, based on user stories
- Develop AC Database user guide

Research findings and products will be socialized within the SA community to collaborate for the advancement of FM assurance across the Agency:
- Travel to select NASA centers for SA of FM knowledge exchange
- Consolidate results and document lessons learned and present to SA Working Group
Research Thrusts

• TR products will be improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches:
  – Investigate ways to integrate FY16 findings and products into SA and IV&V methods
  – Continue to develop a quick reference guide to improve TR usability for SA analysts across Agency
  – Capture challenges of Launch Vehicles, Agile development, and model-based FM

• The Adverse Condition Database prototype will be refined and productized for insight into off-nominal mission capabilities with focus on analyst usability:
  – Populate AC Database with additional project data from IV&V and SSO projects
  – Align with TRs enabling behavioral and hazard connections
  – Continue to develop more efficient user interface for typical SA or IV&V analyst workflow scenario, based on user stories
  – Develop AC Database user guide

TR suite has been improved and expanded for more comprehensive coverage and ease of sharing information.
Adverse Conditions

- Examining Q2 and Q3 are major challenges of FM software
- **Adverse Condition**: A subset of an off-nominal state that prevents a return to nominal operations and compromises mission success unless an effective response to the causal fault is employed
- How a system is **architected** to handle faults and adverse conditions is crucial for the satisfaction of functional and performance requirements for mission success
• Workshop focus was to better understand how the IV&V Program could most effectively utilize meaningful **Adverse Condition data** to enhance the software assurance provided

• **Q3 analysis**, “Will the system’s software respond as expected under adverse conditions?” brings high value to projects from an independent perspective, focusing on areas of high risk, and assessing the projects’ attention to off-nominal scenarios. As part of the SARP FMAE, an Adverse Condition Database is under development to augment the value of SA provided

• With this innovation, we had the following basic goals:
  – Create a database that centralizes a compilation of adverse conditions and related data from IV&V projects
  – Architect the fields such that there may be sharing of data between IV&V projects for more rigorous analysis

• This user story workshop was held to take theories of how the Program could use more rigorous Adverse Condition data and formulate these into “user stories” to inform the development process. Input was requested from all stakeholders and user groups that recognize that our Program will benefit from increased attention to Q3 and the rigorous identification of potential Adverse Conditions, related mitigations, and verifications of such

• As a <user type>, I want to <meet this goal>, so that <some value is created>
Entity-Relationship Diagram

IV&V Program

Entity-Relationship Diagram

Failure Type

Entity-Relationship Diagram

Hazard Type

Entity-Relationship Diagram

Hazard Type Map

Entity-Relationship Diagram

Custom Table

Entity-Relationship Diagram

Custom Data

Entity-Relationship Diagram

Domain

Entity-Relationship Diagram

Domain Name

Entity-Relationship Diagram

Domain ID Num

Entity-Relationship Diagram

Domain Description

Entity-Relationship Diagram

Domain Parent

Entity-Relationship Diagram

System

Entity-Relationship Diagram

System ID Num

Entity-Relationship Diagram

System Name

Entity-Relationship Diagram

System Phase

Entity-Relationship Diagram

System Description

Entity-Relationship Diagram

System Segment

Entity-Relationship Diagram

System_Map

Entity-Relationship Diagram

AC ID Num

Entity-Relationship Diagram

Domain ID Num

Entity-Relationship Diagram

Domain_Map

Entity-Relationship Diagram

AC ID Num

Entity-Relationship Diagram

Domain Name

Entity-Relationship Diagram

Domain Description

Entity-Relationship Diagram

Domain Parent

Entity-Relationship Diagram

Failure Type Map

Entity-Relationship Diagram

Failure Type_ID Num

Entity-Relationship Diagram

Failure Name

Entity-Relationship Diagram

Failure Description

Entity-Relationship Diagram

Failure Type_ID

Entity-Relationship Diagram

Hazard Type_ID

Entity-Relationship Diagram

Hazard Type Name

Entity-Relationship Diagram

Hazard Type Description

Entity-Relationship Diagram

Hazard Type_Map

Entity-Relationship Diagram

Hazard Type_ID

Entity-Relationship Diagram

AC ID Num

Entity-Relationship Diagram

adverse condition

Entity-Relationship Diagram

AC Identifier

Entity-Relationship Diagram

AC Name

Entity-Relationship Diagram

Open AC Name

Entity-Relationship Diagram

Desired Reaction System

Entity-Relationship Diagram

Desired Reaction Software

Entity-Relationship Diagram

AC Likelihood

Entity-Relationship Diagram

AC Result Timing

Entity-Relationship Diagram

Component Name

Entity-Relationship Diagram

Component Description

Entity-Relationship Diagram

SW Cause Indicator

Entity-Relationship Diagram

SW Cause Description

Entity-Relationship Diagram

SW Detection Indicator

Entity-Relationship Diagram

SW Detection Description

Entity-Relationship Diagram

SW Mitigation Indicator

Entity-Relationship Diagram

SW Mitigation Description

Entity-Relationship Diagram

SW Verification Type

Entity-Relationship Diagram

AC Origin

Entity-Relationship Diagram

Mission ID Num

Entity-Relationship Diagram

Mission Name

Entity-Relationship Diagram

Launch Date

Entity-Relationship Diagram

Development Start Date

Entity-Relationship Diagram

Description

Entity-Relationship Diagram

Ongoing

Entity-Relationship Diagram

Human Rated Notes

Entity-Relationship Diagram

Development Phase

Entity-Relationship Diagram

Mission Domain

Entity-Relationship Diagram

SBU Flag

Entity-Relationship Diagram

Capability

Entity-Relationship Diagram

Capability ID Num

Entity-Relationship Diagram

Mission ID Num

Entity-Relationship Diagram

Capability Name

Entity-Relationship Diagram

Description

Entity-Relationship Diagram

Entity

Entity-Relationship Diagram

Entity ID Num

Entity-Relationship Diagram

Capability Map

Entity-Relationship Diagram

AC ID Num

Capability ID Num

Entity-Relationship Diagram

Attachment ID Num

Entity-Relationship Diagram

Attachment

Entity-Relationship Diagram

Attachment ID Num

Entity-Relationship Diagram

FileName

Entity-Relationship Diagram

IV&V Info

Entity-Relationship Diagram

IV&V Info ID

Entity-Relationship Diagram

AC ID Num

Methods

Entity-Relationship Diagram

Associated IV&V Staff

Entity-Relationship Diagram

AC Used By Project

Entity-Relationship Diagram

Trace Requirement ID

Entity-Relationship Diagram

AC ID Num

Entity ID Num

Entity-Relationship Diagram

AC_ID Num

Entity ID Num

Entity-Relationship Diagram

Assurance of Fault Management

12/13/2016

Risk-Significant Adverse Condition Awareness
## AC Database Screenshots

<table>
<thead>
<tr>
<th>AC Identifier</th>
<th>AC Name</th>
<th>Open AC Name</th>
<th>Domain Name</th>
<th>Failure Type</th>
<th>Hazard Type</th>
<th>System Name</th>
<th>Component Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPCV-1012</td>
<td>CAUS6: A software-based control error could result in a loss of command and control capability to...</td>
<td>Electrical Power</td>
<td>Loss of Command / Control Capability</td>
<td>MPCV Crew Module; MPCV Service Module</td>
<td>CM: Electrical Power System, SM: Electrical Power Subsystem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-1013</td>
<td>CAUS4: Software Based Control Errors - Software errors could result in premature or inadvertent Spacecraft Structures and Mechanisms; Electrical Power Vehicle Structural Damage</td>
<td>MPCV Crew Module; MPCV Service Module</td>
<td>CM: Electrical Power System, SM: Spacecraft Structures and Mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-1015</td>
<td>CAUS6: Software Based Control Errors - Software errors could result in premature or inadvertent Spacecraft Structures and Mechanisms; Pyrotechnics; Numerical Incursions Degraded Vehicle Performance; Premature/Inadvertent Activation</td>
<td>MPCV Crew Module; MPCV Service Module</td>
<td>CM: Avionics, CM Electrical Power; SM: Spacecraft Structures and Mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-1019</td>
<td>CAUS7: Software-Based Control Error - Software commanding errors may cause separation of ECLS components Avionics / Command and Data Handling; Electrical Power</td>
<td>Hazardous Thermal conditions</td>
<td>MPCV Crew Module; MPCV Service Module</td>
<td>CM: Avionics, CM Electrical Power; SM: Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-1020</td>
<td>CAUS5: Software-Based Control Error - Improper software commanding of ECLS components Avionics / Command and Data Handling; Electrical Power</td>
<td>Habitat / Suit Depressurization; Loss of Control / Command</td>
<td>MPCV Crew Module</td>
<td>CM: Avionics, CM Electrical Power; SM: Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-1022</td>
<td>CAUS9: Software-Based Control Error - Software errors may cause generation of incorrect commands Spacecraft Separation; Pyrotechnics; Wiring; Avionics / Command and Data Handling</td>
<td>Loss of Control / Command Capability; Loss of Suitability</td>
<td>MPCV Crew Module; MPCV Launch Abort System</td>
<td>CM: Avionics, CM Electrical Power; SM: Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-1043</td>
<td>the vehicle loses all power Electrical Power</td>
<td>Loss of Command / Control Capability; Loss of Crew</td>
<td>MPCV Crew Module</td>
<td>CM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-3869</td>
<td>CAUS4: Software-Based Control Error - Software commanding errors may cause incorrect control Avionics / Command and Data Handling; Electrical Power</td>
<td>Crew Incapacitation, Illness, or Injury; Loss of Control / Command</td>
<td>MPCV Crew Module</td>
<td>CM: Avionics, CM Electrical Power; SM: Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-3870</td>
<td>CAUS9: Software-Based Control Error - Software commanding errors may cause incorrect control Avionics / Command and Data Handling; Electrical Power</td>
<td>Crew Incapacitation, Illness, or Injury; Hazardous Radiation</td>
<td>MPCV Crew Module</td>
<td>CM: Avionics, CM Electrical Power; SM: Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCV-3871</td>
<td>CAUS6: Software-Based Control Error - Software commanding errors may cause incorrect control Avionics / Command and Data Handling; Electrical Power</td>
<td>Crew Incapacitation, Illness, or Injury; Loss of Crew</td>
<td>MPCV Crew Module</td>
<td>CM: Avionics, CM Electrical Power; SM: Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IV&V Program**

12/13/2016

Assurance of Fault Management

Risk-Significant Adverse Condition Awareness
AC Database Screenshots

Mission Description
The Orion Multi-Purpose Crew Vehicle (MPCV) is a spacecraft intended to carry a crew of four astronauts to destinations at or beyond Low Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).

Mission Notes

AC Data
AC Origin
HR #: MPCV-FLT-035 Failed / Partial Deployment of

Document References
1.8 Electrical Power System - Redundant control power is provided to all the cards internal to the Power and Data Unit through the internal power supply (IPS) cards. SLS abort recommendation is received by PDUs - Power Management (PWM) domain software performs command processing for the power distribution subsystem. 1.3 Vehicle System Management - subset of vehicle functions that

Open AC Name
AC Domain Description

Component Name

Component Description

AC Likelihood

Edit AC

Domain Links

Domain Name
Add/Delete Domain
Electrical Power

Domain Description
Select 'Domain Name' to see Description

Failure Types

Failure Name
Add/Delete Failure

Failure Description
Select 'Failure Name' to see Description

Hazard Types

Hazard Name
Add/Delete Hazard
Loss of Command / Control Capability

Hazard Description
Select 'Hazard Name' to see Description

System Categorization

Add/Delete System
The Orion Multi-Purpose Crew Vehicle (MPCV) is a spacecraft intended to carry a crew of four astronauts to destinations at or beyond low Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).
Research Thrusts

• TR products will be improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches:
  – Investigate ways to integrate FY16 findings and products into SA and IV&V methods
  – Continue to develop a quick reference guide to improve TR usability for SA analysts across Agency
  – Capture challenges of Launch Vehicles, Agile development, and model-based FM

• The Adverse Condition Database prototype will be refined and productized for insight into off-nominal mission capabilities with focus on analyst usability:
  – Populate AC Database with additional project data from IV&V and SSO projects
  – Align with TRs enabling behavioral and hazard connections
  – Continue to develop more efficient user interface for typical SA or IV&V analyst workflow scenario, based on user stories
  – Develop AC Database user guide

TR suite has been improved and expanded for more comprehensive coverage and ease of sharing information

AC Database has been refined and productized for insight into off-nominal mission capabilities
Research Thrusts

• TR products will be improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches:
  – Investigate ways to integrate FY16 findings and products into SA and IV&V methods
  – Continue to develop a quick reference guide to improve TR usability for SA analysts across Agency
  – Capture challenges of Launch Vehicles, Agile development, and model-based FM

• The Adverse Condition Database prototype will be refined and productized for insight into off-nominal mission capabilities with a focus on analyst usability:
  – Populate AC Database with additional project data from IV&V and SSO projects
  – Align with TRs enabling behavioral and hazard connections
  – Continue to develop more efficient user interface for typical SA or IV&V analyst workflow scenario, based on user stories
  – Develop AC Database user guide

• Research findings and products will be socialized within the SA community to collaborate for the advancement of FM assurance across the Agency:
  – Travel to select NASA centers for SA of FM knowledge exchange
  – Consolidate results and document lessons learned and present to SA Working Group

TR suite has been improved and expanded for more comprehensive coverage and ease of sharing information
AC Database has been refined and productized for insight into off-nominal mission capabilities
Fault Management Architectures and the Challenges of Providing Software Assurance

Presented to the 31st Space Symposium
Date: 4/14/2015
Primary Author: Shirley Savarino (TASC)
Presenter: Rhonda Fitz (MPL)
Co-Authors: Lorraine Fesso (JPL), Gerek Whitman (TASC)

ABSTRACT
Fault Management (FM) is focused on safety, the preservation of assets, and maintaining the desired functionality of the system. How FM is implemented varies among missions. Common to most missions is system complexity due to a need to establish a multi-dimensional structure across hardware, software and spacecraft operations. FM is necessary to identify and respond to system faults, mitigate technical risks and ensure operational continuity. Generally, FM architecture, implementation, and software assurance efforts increase with...
Space Symposium Tech Track

31st Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 13-14, 2015

Fault Management Architectures and the Challenges of Providing Software Assurance

Primary Author
Shirley Savarino, shirley.savarino@tasc.com

Co-authors
Rhonda Fitz, rhonda.s.fitz@ivv.nasa.gov
Lorraine Freg, lorraine.m.freg@jpl.nasa.gov
Garek Whitman, garek.whitman@tasc.com

Abstract
Fault Management (FM) is focused on safety, the preservation of assets, and maintaining the desired availability of the system. How FM is implemented varies among missions. Common to most missions is system integrity due to a need to establish a multi-dimensional structure across hardware, software and spacecraft buses. FM is necessary to identify and respond to system faults, mitigate technical risks and ensure mission continuity. Generally, FM architecture, implementation, and software assurance efforts increase with...
Research Thrusts

- TR products will be improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches:
  - Investigate ways to integrate FY16 findings and products into SA and IV&V methods
  - Continue to develop a quick reference guide to improve TR usability for SA analysts across Agency
  - Capture challenges of Launch Vehicles, Agile development, and model-based FM

- The Adverse Condition Database prototype will be refined and productized for insight into off-nominal mission capabilities with a focus on analyst usability:
  - Populate AC Database with additional project data from IV&V and SSO projects
  - Align with TRs enabling behavioral and hazard connections
  - Continue to develop more efficient user interface for typical SA or IV&V analyst workflow scenario, based on user stories
  - Develop AC Database user guide

- Research findings and products will be socialized within the SA community for the advancement of FM assurance across the Agency:
  - Travel to select NASA centers for SA of FM knowledge exchange
  - Consolidate results and document lessons learned and present to SA Working Group
FY16 Advancements

- Finalized updates and migration of TR suite onto Confluence
  - Improved and updated the Confluence page for usability and to communicate the TR suite and other project advancements with enhanced HTML reporting feature
  - Launch Vehicle FM researched, summarized with inclusion of SLS data
- Finalized integration of project Adverse Condition data into AC Database
  - Fifteen IV&V projects include: GSDO, HEO Integration, ICESat-2, InSight, ISS, JPSS Flight, JPSS Ground, JPSS-2, JWST, Mars 2020, MPCV, OSIRIS-REx, SGSS, SLS, and SPP
  - Improvements made to the AC Database include core functionality (search, enter, edit), architectural changes, user interface changes, and automated import process
  - Capability Based Assurance workflow evolution enabled with additional fields
- Provided numerous outreach opportunities for knowledge exchange
  - Paper presented at 32nd Space Symposium, tech discussions, and workshops held
  - Held introductory courses on relational database architecture and management
  - Coordinated summer intern effort for assistance in AC Database development
- Collaborative deployment plans have been initiated
  - IV&V Senior staff support and direction for integration within Enterprise Architecture
  - Communication with tool developers for user-focused deployment is in place
  - Follow-on proposal activities have been accepted
Description/Goals

• Improve and expand upon the current analysis of NASA mission FM with a **Technical Reference Suite** for more comprehensive coverage of architecture, visibility, and assurance strategies
• Develop and refine the prototype **Adverse Condition Database** for access to IV&V project fault, failure, and hazard data for more rigorous assurance and risk reduction with Q2/Q3 analysis
• Disseminate results with **FM SA Knowledge Exchange** via conference presentations and papers, roundtables, reports, and informal learning opportunities

Value to NASA

• Promoting FM knowledge for SARP, IV&V Program, and NASA Engineering Network
• Improved assurance from the provision of more comprehensive data with specific guidance
• More rigorous IV&V analysis from identification of off-nominal scenarios and cross-project AC data sharing
• Increased efficiency of analyst workflow with focused methods and broader visibility and test coverage
• Greater focus on FM and project areas of vulnerability or high risk in terms of software reliability

FY16 Advancements

• Finalized updates and migration of TR suite onto Confluence with enhanced reporting feature
• Finalized integration of project Adverse Condition data from 15 IV&V projects into the AC Database
• Refined AC data import template, automated import process, improved usability and query timing
• Added functionality for capabilities and entities for Capability Based Assurance workflow evolution
• Collaborative deployment plans initiated

Planned Infusion

• TR suite has been improved and expanded upon for more comprehensive coverage of NASA mission types and non-traditional development approaches
• The AC Database has been refined and productized for insight into off-nominal mission capabilities
• Research findings and products have been and will continue to be socialized within the SA community to collaborate for the advancement of FM assurance across the Agency and the spaceflight community
Added Value

• Products and results are a step toward filling a number of gaps in the FM knowledge domain for SA community and IV&V across the Agency
  – TR suite provides cross-project, cross-agency **FM architecture** and software assurance knowledge sharing with practical application
  – Labor savings realized as analysts capitalize on deeper understanding of FM **Software Assurance strategies**, methods and tools in order to be efficient in providing domain specific FM assurance
  – Recommended techniques reduce risk of lack of **visibility** into FM architecture and boost assurance throughout the project lifecycle
**Added Value**

- Collaboration and infusion of results will continue as the TR suite and the **AC Database** are deployed, and methods are developed to take advantage of both as dynamic, living resources tailored to improve workflow
  - Improved assurance from the provision of more comprehensive **off-nominal data** with specific project examples available for guidance
  - More rigorous **Q2/Q3 analysis** from identification of off-nominal scenarios through cross-project AC data sharing and identification of relevant relationships
  - Increased efficiency of **analyst workflow** with focused methods and broader visibility and test coverage across the system for management of scope
  - Greater focus on **FM** and project areas of **vulnerability** or high **risk** in terms of software reliability in support of Capability Based Assurance
Additional Information

- FM NASA Engineering Network (NEN)
  - [https://nen.nasa.gov/web/faultmanagement](https://nen.nasa.gov/web/faultmanagement)
- SW Assurance Research Program products
  - [https://nen.nasa.gov/web/sarp](https://nen.nasa.gov/web/sarp)

• Contact:
  - Rhonda Fitz (rhonda.s.fitz@nasa.gov)
Architectural Views

- **Structural/Physical:**
  - How are individual components and entities related, joined, or positioned?
  - What groupings are used to encapsulate individual pieces?
  - What are the interfaces between different parts?

- **Functional:**
  - How does the architecture accomplish a purpose or goal?
  - How does the system get from Point A to Point B?
  - How does data flow through the system?

- **Centralized:**
  - Architectures with only one tier of FM activity at the system level, which has full control over all subsystems

- **Distributed:**
  - Architectures with at least one tier of FM activity that has no master controller directing individual entities

- **Hybrid:**
  - Architectures with multiple tiers of FM activity, where the highest tier is at the system level and can direct lower tiers
Centralized architectures are common in Earth Orbiters
Human Spaceflight and Deep Space Robotic missions commonly use hybrid architectures.
Hybrid FM Architectures

Structural Architecture

Main Computer / CSCI
- System FM
- Memory Storage

XYZ System Computer / CSCI
- Domain FM
- Memory Storage

ABC System Computer / CSCI
- Local FM
- Memory Storage

Hardware Layer
- Sensors
- Effectors

HW Components
- FP Routines
- Sensors
- Effectors

Software Layer
- To other sub-systems
- To hardware
Architecture Findings

- Some trends can be seen along mission domain: Earth Orbiter, Deep Space Robotic, Human Spaceflight
- Table and data-driven architectures are common, and enable more software re-use of FM engines
- Developers tend toward re-use even when architectures may not be intended for a particular mission type
- Implementation of FM capabilities typically lags behind other implementation, even when it would complement the nominal case
- FM architectures designed early and with intention reduce risk by:
  - Enabling more communication between development teams, as well as with stakeholders
  - Managing system complexity
Visibility Findings

- Availability and quality of artifacts has a large impact on analyst visibility
- Often, artifacts have sufficiently detailed information on FM, but are disorganized and scattered across many documents
  - Mining these documents for FM details may be necessary to develop a system understanding
- Model-based FM development may help to alleviate visibility challenges by imposing centralization of FM architectural design
- Development of a robust and well-maintained TR helps to mitigate visibility challenges as a project progresses