Fault Management Architectures and the Challenges of Providing Software Assurance

Presented to the 31st Space Symposium
Date: 4/14/2015

Presenter: Rhonda Fitz (MPL)
Primary Author: Shirley Savarino (TASC)
Co-Authors: Lorraine Fesq (JPL/Caltech),
Gerek Whitman (TASC)

Table of Contents

- Introduction to NASA IV&V
- IV&V Philosophy and Methodology
- Challenges with FM and the FM Handbook
- FM Architectures SARP Initiative
- FM Assurance Statements
- Conclusions

NASA IV&V Facility

NPR 7150.2, NASA Software Engineering Requirements

The program manager shall ensure that software IV&V is performed on the following categories of projects:

- Category 1
- Category 2 that have Class A or Class B payload risk classification
- Projects specifically selected by NASA Chief of Safety and Mission Assurance

IV&V = Independent Verification and Validation [of Software]

Independence:

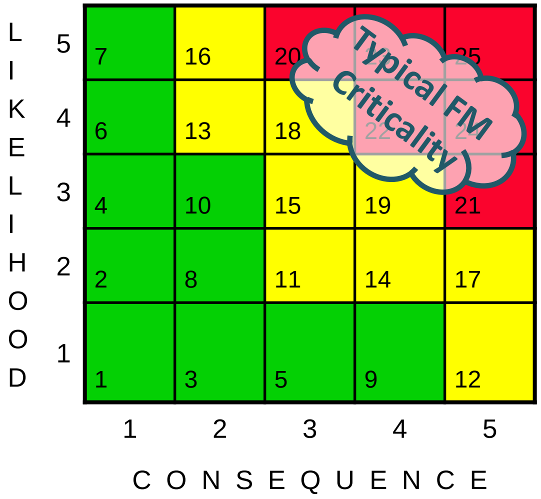
- Technical Independence
- Managerial Independence
- Financial Independence

NPR 7120.5E defines Categories; NPR 8705.4 defines classification of payload risk

IV&V Methodology

Criticality analysis assesses likelihood and impact of failed behaviors

- Plotted on a risk matrix
- Establish priorities and focus for analysis
- Generally, FM is high criticality



5	7	16	20	23	25
4	6	13	18	22	24
3	4	10	15	19	21
2	2	8	11	14	17
1	1	3	5	9	12
	1	2	3	4	5

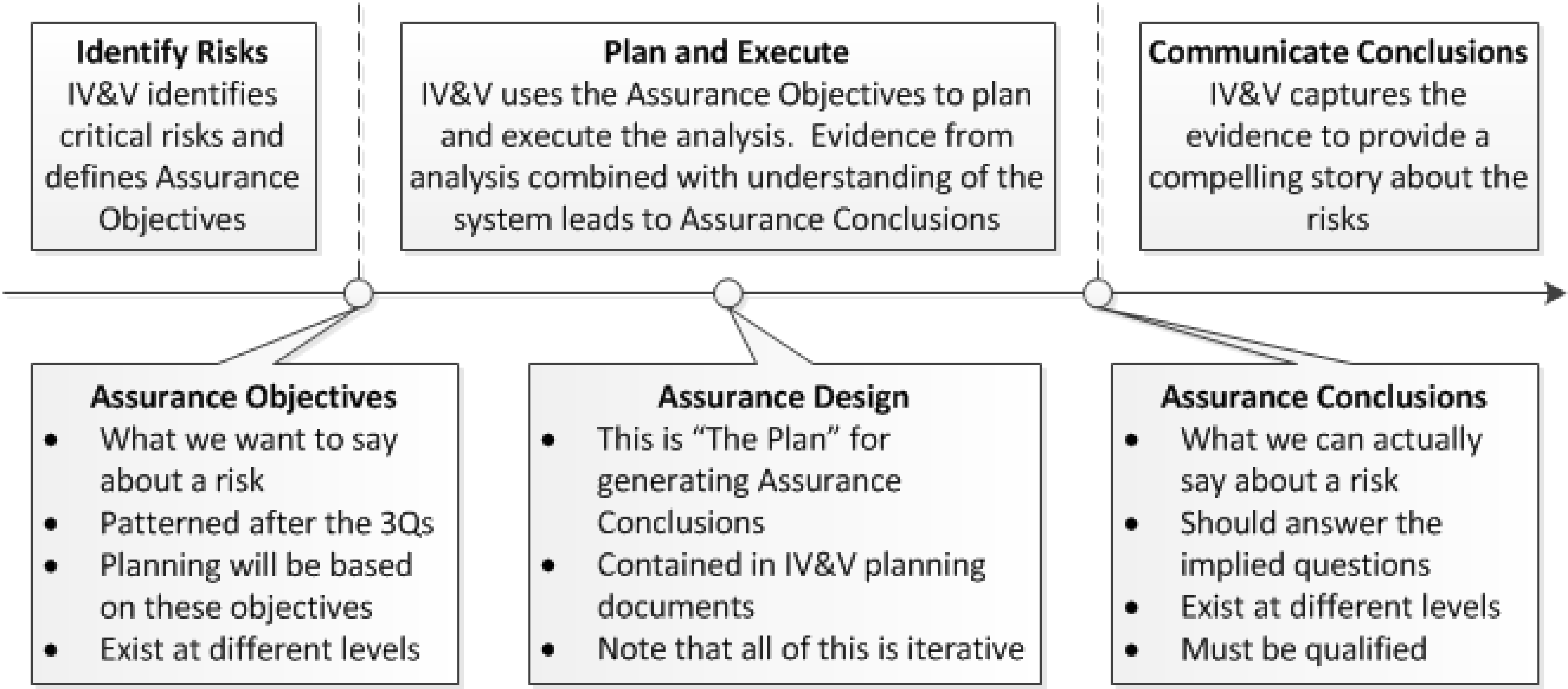
The goal of each IV&V project is to assure mission success by assuring that the critical software (mission-critical and/or safety-critical):

- Does what it is supposed to do
- Does not do what it is not supposed to do
- Performs appropriately under adverse conditions

a.k.a. "The 3 Questions"

IV&V assures mission success by validating and verifying critical software.

Assurance Strategy



Identify Risks

IV&V identifies critical risks and defines Assurance Objectives

Plan and Execute

IV&V uses the Assurance Objectives to plan and execute the analysis. Evidence from analysis combined with understanding of the system leads to Assurance Conclusions

Communicate Conclusions

IV&V captures the evidence to provide a compelling story about the risks

Assurance Objectives

- What we want to say about a risk
- Patterned after the 3Qs
- Planning will be based on these objectives
- Exist at different levels

Assurance Design

- This is "The Plan" for generating Assurance Conclusions
- Contained in IV&V planning documents
- Note that all of this is iterative

Assurance Conclusions

- What we can actually say about a risk
- Should answer the implied questions
- Exist at different levels
- Must be qualified

Challenges with Fault Management

- 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

- Continuous improvement for software assurance practices is attained by leveraging the IV&V FM Community of Interest to identify FM architecture commonalities/strategies across NASA missions

FM Handbook

Goal

•Ameliorate schedule/cost/predictability challenges of testing/operating FM systems

•Improve reliability and safety of NASA's flight and ground systems

•Coalesce the FM field

Scope

- Outline scoped to address needs of Agency – crewed and robotic missions
- Robotic emphasis in Version 1, due to SMD co-funding
- Suggested use as "companion" to SE Handbook

Draft 1 Released July 2011

1113 comments (NTSPO record)

Current Status: Draft 2 released 4/9/12.

Lesson Learned: Diverse FM views across NASA. Comments cannot be dispositioned by one person or one Center – requires discussions/consensus among people in the discipline, across the Agency

Plans: Renewed effort to develop "chapter" for each mission type, to be incorporated into NASA FM Handbook

Take 2: Developing a Deep Space FM Robotic Guidebook

FM Architectures SARP 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

Survey Methodology

IV&V Analyst Subject Matter Experts were surveyed from each of eight chosen projects with a variety of mission types, developers, and relative complexity

Name	*Mission Type*
Mars Science Laboratory (MSL)	Deep Space Robotic
International Space Station (ISS)	Human Spaceflight
James Webb Space Telescope (JWST)	Deep Space Robotic
Multi-Purpose Crew Vehicle Exploration Flight Test 1 (MPCV EFT-1)	Human Spaceflight
Joint Polar Satellite System (JPSS)	Earth Orbiter
Magnetospheric Multiscale (MMS)	Earth Orbiter
Geostationary Operational Environmental Satellite R-Series (GOES-R)	Earth Orbiter
Solar Probe Plus (SPP)	Deep Space Robotic

Architecture Survey Questions

Category	*Description*
Structure 7 questions	Obtain a high level view of each architecture, and provide insight into size, complexity, and scale. • Address the structure and organization of the FM architecture. • Characteristics such as centralization or distribution, tiers of operation, interdependency, modifiability, and implementation within the overall flight software are addressed.
Concept 10 questions	Addresses the design process and major design ideas and themes of the FM architecture. • Considerations such as fault analysis, automation, mission phases, fault definition, redundancy, and fail-safe/fail-operational modes are addressed. • Establish a broad view of how the FM system is intended to accomplish its objectives, and why it is designed and structured in the way it is.
Implementation 13 questions	Technical implementation detail about how the FM architecture was built and how it works. • Number of monitors and responses, false positives and persistence, fault isolation, simultaneous responses, and subsystem inter-communication are examples of the low-level characteristics covered by this section. • Capabilities that some architectures have but others do not are important to uncover in order to help categorize and label the architectures as well as reveal potential strengths and limitations of various FM architectures.
Other Questions 5 questions	• This was the catch-all section for things the other questions may not have entirely covered • This section contained questions involving heritage and mission parameters in order to provide some additional context to frame the rest of the responses.

IV&V Survey Questions

Survey: IV&V Analysis Questions
• What were the key drivers to IV&V on this project?
• What were the critical errors that IV&V was focused on assuring against?
• What other assurance strategies were involved in IV&Ving this project?
• What kinds of artifacts did you get from the developer to use in the analysis, and how did the types of artifacts you received affect your analysis?
• Were there types of artifacts you did not receive or the developer did not generate that would have made analysis easier/faster/more complete?
• What kinds of technical reference(s) did you generate during your analysis?
• If the FM system was inherited or standardized, how did this influence your analysis?
• What language was used to write the FSW? How did this choice in language make analysis easier/more difficult?
• What was the highest benefit analysis? In retrospect, were there things you or the IV&V team would or should have done differently?

Sample FM Assurance Statements

Typical Assurance Objectives or Conclusions	Source Mission Type	3Qs Mapping
Concept Phase		
"The Hazards Report documents all known software-based hazard causes, contributors, and controls."	Deep Space Robotic	Q3
Requirements Phase		
"The system fault management requirements are of high quality and are consistent with acquirer needs as they relate to the system's software."	Deep Space Robotic	Q1
Design Phase		
"There are no monitor-response collisions – there are no concurrent responses that could cause harm or detrimental behaviors to the vehicle between any lower or higher level responses."	Deep Space Robotic	Q2
Implementation Phase		
"The fault management behaviors needed for the system during flight operations are correctly and completely being represented in the algorithms and fully satisfied in the implementation."	Earth Orbiter	Q1
Integration & Test Phase		
"The set of tests was comprehensive with regard to the Fault Management Design Document algorithms."	Human Spaceflight	Q1
Operations & Maintenance Phase		
"The added tests strengthened the developer's testing of the Power Management software and provided additional assurance that the software will perform as expected."	Human Spaceflight	Q1

Conclusions

- Completed an in-depth survey of several FM architectures that serve to structure the safety- and mission-critical software
- The NASA IV&V Program has found that FM systems are often ranked high in the risk-based assessment of criticality
- The Assurance Strategies that focus IV&V analysis provide value by identifying and mitigating risks across a variety of mission types, including Earth orbiters, human spaceflight, and deep space robotic missions
- Results of these efforts will feed into the updated NASA FM Handbook providing dissemination across NASA, other agencies and the space community
- Potential future efforts will be to extend our efforts to survey additional spaceflight projects; investigate projects within other domains such as launch vehicles, ground systems, or manned and unmanned aeronautics systems; as well as collaborate with OSMA and FM experts across the NASA agency

References & Contacts

References:

- NASA IV&V Website
- Fault Management Handbook (NASA-HDBK-1002) Draft 2
- Fault Management NASA Engineering Network
- IV&V Technical Framework (IVV 09-1) Version O

Contact Information:

Rhonda Fitz – rhonda.s.fitz@ivv.nasa.gov
Shirley Savarino – shirley.savarino@tasc.com
Lorraine Fesq – lorraine.m.fesq@jpl.nasa.gov
Gerek Whitman – gerek.whitman@tasc.com