Risk-Significant Adverse Condition Awareness Strengthens Assurance of Fault Management Systems

NASA Office of Safety & Mission Assurance
Software Assurance Research Program
NASA's Independent Verification & Validation Program

Presented at the 33rd Space Symposium

Rhonda Fitz, Senior Systems Engineer
April 3, 2017

Contents

NASA's IV&V Program

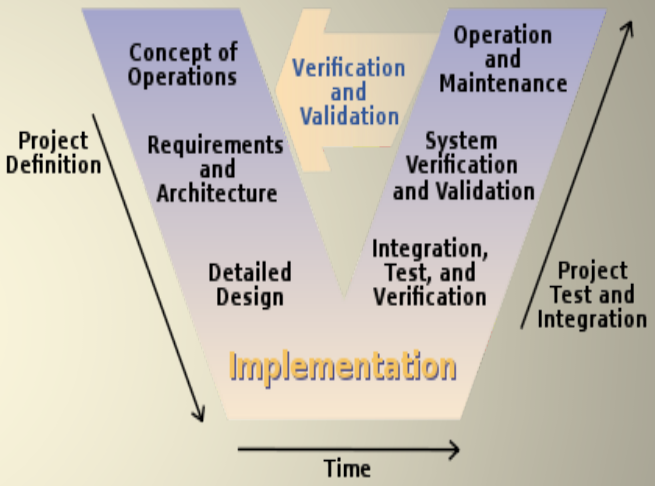
- NASA's IV&V Program: established in 1993
- Founded under the NASA Office of Safety and Mission Assurance (OSMA) as a direct result of recommendations made by the National Research Council (NRC) and the Report of the Presidential Commission on the Space Shuttle Challenger Accident
- IV&V is an objective examination of safety and mission critical system and software processes and products

Three Key Parameters:
- Technical Independence
- Managerial Independence
- Financial Independence

Three Questions (3Qs) of IV&V:
Q1 - Will the system's software do what it is supposed to do?
Q2 - Will the system's software not do what it is not supposed to do?
Q3 - Will the system's software respond as expected under adverse conditions?

IV&V Technical Framework

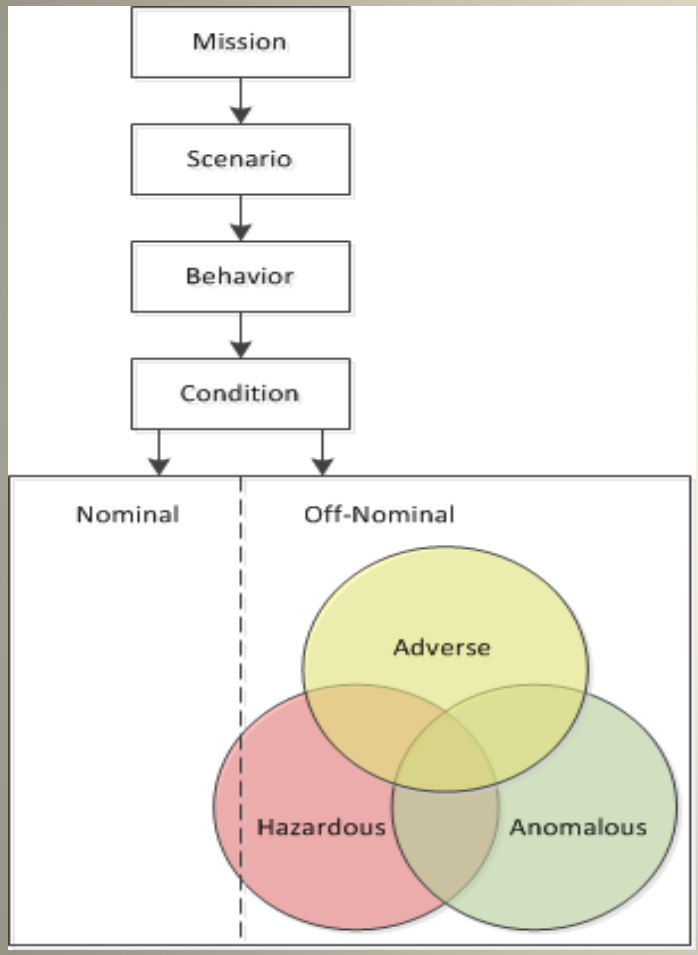
- Objectives include the verification and validation of:
  - Concept Documentation
  - Requirements
  - Design
  - Implementation
  - Test Documentation
  - Operations and Maintenance



- Risk-significant adverse condition awareness brings forth off-nominal analysis threads aligned with hazards, dependability, emergent behavior, security, and testing

IV&V plays a role in the overall risk mitigation strategy applied throughout the lifecycle to improve the quality, reliability, safety, and security of critical software systems

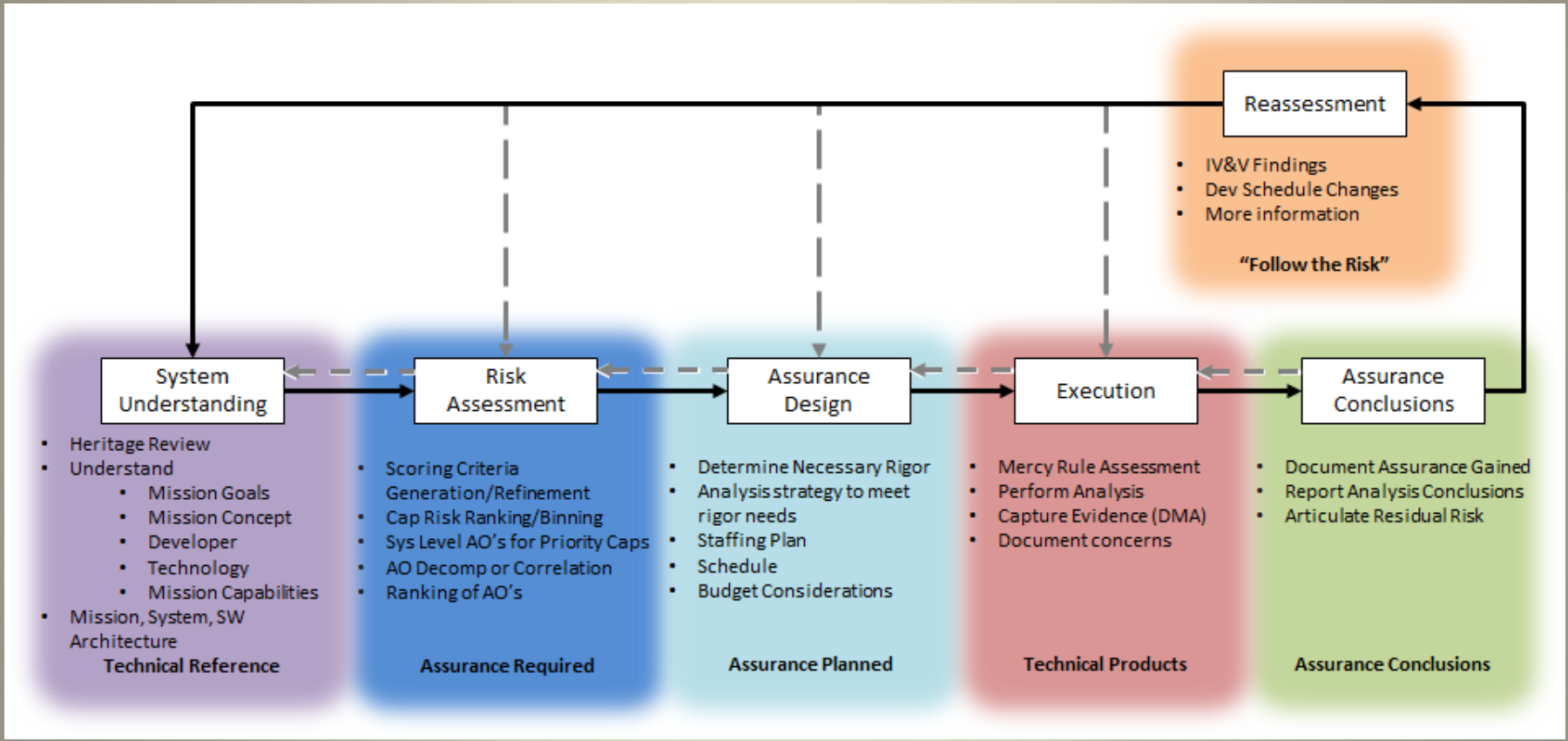
Adverse Conditions



- Examining Q2 and Q3 are major challenges of FM software
- An ***adverse condition*** is considered 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.

Adverse condition awareness strengthens software assurance

Assurance Strategy



Raising adverse condition awareness identifies areas of significant risk to apply an adaptive, iterative analysis approach for software assurance

Capability-Based Assurance

- Enables software assurance workflow in an adaptive, risk-informed manner
- Identifies IV&V scope and rigor by prioritizing and framing analysis
- Infuses agility in order to accommodate change
- Crosses all lifecycle phases
- Influences static and dynamic test coverage
- Communicates findings and assurance conclusions more comprehensively
- Provides the mapping of critical capabilities to adverse conditions or hazard causes that are prevented or mitigated by software controls and verifications
- Reveals dependencies or vulnerabilities in capabilities that may indicate missing requirements, weak design, incomplete implementation, or a need for expanded test coverage, either static or dynamic

The goal of defining capabilities at the mission level is to be able to adequately understand and mitigate the riskiest aspects of the mission

Hazard Analysis

- Maintaining the health and safety of a system, or fault management, is a cross-cutting capability that is an integral part of assurance
- A system's prevention, detection, isolation, response, or tolerance of multiple faults and failures maintains mission capabilities despite adverse conditions
- Assessing hazard causes, controls, mitigations and verifications is part of adverse condition awareness that can not be "done and forgotten" at the outset of a project, or worse, left to the end during system integration testing
- Evaluating multiple project artifacts, sources of adverse conditions to which the system should be capable of responding, occurs throughout the lifecycle
- Identifying unforeseen adverse conditions that may impede mission success or inhibit safety is an assurance service of great value to a project, ensuring that coverage is complete with respect to safety, security, and dependability

Independent analysis based on solid system understanding and experience with similar systems allows analysts to generate adverse conditions to be considered

Adverse Condition Database

- Centralizes and compiles a comprehensive listing of adverse conditions in a cross-project repository with correlated data relevant across NASA missions
- Incorporates adverse condition awareness into all phases or for all objectives of analysis, throughout the development lifecycle, expanding Q3 coverage
- Provides the ability to map critical capabilities to adverse conditions or hazard causes that are prevented or mitigated by software controls
- Improves analysis by tracking adverse conditions and allowing queries based on project, mission type, domain/component, causal fault, and other key characteristics for cross-project fault management knowledge sharing
- Alerts analysts of vulnerabilities, architectural design weaknesses, and unforeseen or undesirable system behaviors in reaction to faults
- Identifies risk-significant scenarios that may be selected for dynamic testing

The Adverse Condition Database promotes assurance at a higher level of rigor with the goal of reducing risk and increasing confidence in NASA mission success

Search Form

Search Form

Select Mission: MPCV [Clear]

Record Count: 12

Select Domain: Electrical Power [Clear]
Select Failure Type: [Clear]
Select Hazard Type: [Clear]
Select System: MPCV Crew Module [Clear]

Show as Datasheet | Add/Edit Mission | Import Data | Add a New AC | Close Database

AC Identifier	AC Name	Open AC Name	Domain Name	Failure Type	Hazard Type	System Name	ComponentName
MPCV-1012	CAUS6: A software-based control error could result in a loss of command and control capability to		Electrical Power		Loss of Command / Control Capability	MPCV Crew Module; MPCV Service Module	CM: Electrical Pov System, SM: Elect Power Subsyster
MPCV-1013	CAUS4: Software Based Control Errors - Software errors could result in premature or inadvertent		Spacecraft Structures and Mechanisms; Electrical Power		Vehicle Structural Damage	MPCV Crew Module; MPCV Service Module	CM: Electrical Pov System, SM: Stru SM: Mechanisms
MPCV-1015	CAUS6: Software Based Control Error 1) Failure of Timeline Management software to properly		Spacecraft Structures and Mechanisms; Pyrotechnics; Wiring; Avionics /		Degraded Vehicle Performance; Premature / Inadvertent Pyrotechnic	MPCV Crew Module; MPCV Service Module	CM: Avionics, CM Electrical Power S CM: Guidance, Na
MPCV-1017	CAUS17: Software Based Control Errors - A failure occurring within EPS controlling/ monitoring		Electrical Power		Loss of Crew; Loss of Power to Safety Critical Functions	MPCV Crew Module; MPCV Service Module	CM: Electrical Pov System, SM: Elect Power Subsyster
MPCV-1018	CAUS11: Software-based Control Errors - Software-related causes include: (1) The Electrical Power		Electrical Power		Fire / Explosion; Habitat / Suit Depressurization; Hazardous Gas /	MPCV Crew Module	CM: Electrical Pov System
MPCV-1019	CAUS7: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power ; Environmental		Hazardous Thermal Conditions	MPCV Crew Module; MPCV Service Module	CM: Avionics, CM Electrical Power S CM: Environment
MPCV-1020	CAUS5: Software-Based Control Error - Improper software commanding of ECLSS components		Avionics / Command and Data Handling; Electrical Power ; Environmental		Habitat / Suit Depressurization; Loss of Command / Control	MPCV Crew Module	CM: Avionics,CM: Electrical Power S CM: Environment
MPCV-1022	CAUS9: Software-Based Control Error - Software errors may cause generation of incorrect commands		Spacecraft Separation; Pyrotechnics; Wiring; Avionics / Command and		Loss of Command / Control Capability; Loss of Vehicle	MPCV Crew Module; MPCV Launch Abort System	CM: Avionics, CM Electrical Power S CM: Guidance, Na
MPCV-1043	the vehicle loses all power		Electrical Power		Loss of Command / Control Capability; Loss of Crew	MPCV Crew Module	CM
MPCV-3869	CAUS4: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power ; Environmental		Crew Incapacitation, Illness, or Injury; Loss of Command / Control	MPCV Crew Module	CM: Avionics, CM Electrical Power S CM: Environment
MPCV-3870	CAUS9: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power ; Environmental		Crew Incapacitation, Illness, or Injury; Hazardous Gas /	MPCV Crew Module	CM: Avionics, CM Electrical Power S CM: Environment
MPCV-3871	CAUS6: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power ; Environmental		Crew Incapacitation, Illness, or Injury; Loss of Crew	MPCV Crew Module	CM: Avionics, CM Electrical Power S CM: Environment

Adverse Condition Detail Form

AC Detail Form

AC Identifier: MPCV-1012

AC Name: CAUS6: A software-based control error could result in a loss of command and control capability to HDRMs or SADA necessary for solar array deployment. This would result in the inability to deploy the solar arrays in and inadequate power generation resulting in

Duplicate AC Record

Add a New AC

Close and Go Back to Search Form

Mission Data

Mission Name: MPCV

Launch Date: 2018-09-01

Development Start Date:

Ongoing: Y

Human Rated: Y

Mission Domain: HEO

Data Marked as SBU: N

Mission Type: Human Spaceflight

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 loe Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).

Mission Notes:

AC Data

AC Likelihood:

Edit AC

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: CM: Electrical Power System, SM: Electrical Power Subsystem

Component Description:

Domain Links

Add/Delete Domain

Domain Name: Electrical Power

Domain Description: Select 'Domain Name' to see Description

Failure Types

Add/Delete Failure

Failure Name:

Failure Description: Select 'Failure Name' to see Description

Hazard Types

Add/Delete Hazard

Hazard Name: Loss of Command / Control Capability

Hazard Description: Select 'Hazard Name' to see Description

System Categorization

Add/Delete System

System Name

Mission Form

Mission Form

Save Record | Cancel Changes | Close and Go Back to Search Form

Add/Edit Mission Data

Mission Name: MPCV

Launch Date: 2018-09-01

Development Start Date:

Ongoing: Y

Human Rated: Y

Mission Domain: HEO

Mission Type: Human Spaceflight

Data Marked as SBU (Y or N): N

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 loe Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).

Mission Notes:

Capabilities:

Capability Name	Description
Abort	Provides abort capabilities while systems are on the pad, during launch and ascent and on-orbit operations
Ascent Environment	Capability to withstand natural and induced environments experienced during ascent mission phases.
Attitude Control	Provide attitude control.
Auxiliary Comm	Auxiliary Voice Communication link capabilities.
Early Mission Termination	Provides early mission return capabilities while systems are performing in-orbit operations.
ECLSS and ECS Services	Maintain habitable atmosphere, partial pressure, humidity, temp control, trace contaminant, hazard detect
EDL and Recovery Environment	Capability to withstand natural and induced environments experienced during applicable recovery phases.
Entry Descent and Landing	Entry, Descent, and Landing Capabilities associated with MPCV and Mission Systems.
Fueling and Conditioning	Includes propellant loading storage and pressurizations capabilities.
Ground Processing	Provide ground operations capabilities for off-line processing, integrated operations, pad and launch opera
Guidance and Navigation	Determine state vector, targeting, and control functions.

Record: 1 of 30 | No Filter | Search

Entities:

Entity Name	Description
BEL	Backup Engage Logic
BFS	Backup Flight Software
CDH	Command & Data Handling
CFSW	Common Flight Software
CMT	Communicate & Track
CORE	Core Flight Software
DACF	Display and Control Formats
DACM	Display and Control Management
ECLS	Environmental Control & Life Support
EPS	Electrical Power Systems
GNCP	Guidance, Navigation, Control, and Propulsion

Value to NASA

- Collaboration and infusion of results will continue as the Adverse Condition Database is deployed to a wider audience and methods are enhanced to take advantage of the tool as a dynamic, living resource tailored to improve workflow in the ultimate goal of reducing risk and increasing confidence in NASA mission success
- As research progresses, the Adverse Condition Database and supporting assurance methodologies seek to:
  - Improve capability-based assurance from the provision of more comprehensive data
  - Provide more rigorous IV&V analysis from identification of off-nominal scenarios
  - Increase efficiency of analyst workflow and enable broader test coverage
  - Allow greater focus on FM and project areas of vulnerability or significant risk
  - Deliver support for reliability and resiliency for critical system safety

The complexity of fault management and the importance of effectively providing assurance that NASA safety- and mission-critical software will operate reliably, safely, and securely demands rigorous attention to risk-significant adverse conditions

References

- NASA's IV&V Program website

  https://www.nasa.gov/centers/ivv/home/index.html
- NASA Engineering Network: Fault Management

  https://nen.nasa.gov/web/faultmanagement
- Software Assurance Research Program products

  https://nen.nasa.gov/web/sarp

Contact Information

Rhonda Fitz ... rhonda.s.fitz@ivv.nasa.gov

Questions?


REACH
NEW
HEIGHTS
BENEFIT
ALL
HUMANKIND
REVEAL
THE
UNKNOWN