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

• Introduction to NASA IV&V
• IV&V Technical Framework
• Adverse Conditions
• Assurance Strategy
• Capability-Based Assurance
• Hazard Analysis
• Adverse Condition Database
  – Search Form
  – Adverse Condition Detail Form
  – Mission Form
• Value to NASA
• References
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?

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
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.
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.
<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>MPCI-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>MPCI Crew Module; MPCI Service Module</td>
<td>CM: Electrical Power System, SM: Electrical Power System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1013</td>
<td>CAUS4: Software-Based Control Error - Software errors could result in inappropriately</td>
<td>Spacecraft Structures and Mechanisms; Electrical Power</td>
<td>Vehicle Structural Damage</td>
<td>MPCI Crew Module; MPCI Service Module</td>
<td>CM: Electrical Power System, SM: Structural Power Subsystem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1015</td>
<td>CAUS6: Software-Based Control Error 1) Failure of Timeline Management software to properly</td>
<td>Spacecraft Structures and Mechanisms; Pyrotechnics; Methodologies; Avionics; CM</td>
<td>Degraded Vehicle Performance; Premature Uninhabitable Pyrotechnics</td>
<td>MPCI Crew Module; MPCI Service Module</td>
<td>CM: Avionics, CM: Electrical Power System, CM: Guidance, Navigatio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1018</td>
<td>CAUS11: Software-based Control Error - Software-related causes include: (1) The Electrical Power</td>
<td>Electrical Power</td>
<td>Fire / Explosion; Habitat / Suit Depressurization; Hazardous Gas</td>
<td>MPCI Crew Module</td>
<td>CM: Electrical Power System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1019</td>
<td>CAUS7: Software-Based Control Error - Software commanding error may cause incorrect control</td>
<td>Avionics / Command and Data Handling; Electrical Power; Environmental</td>
<td>Hazardous Thermal Conditions</td>
<td>MPCI Crew Module; MPCI Service Module</td>
<td>CM: Avionics, CM: Electrical Power System, CM: Environmental</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1020</td>
<td>CAUS5: Software-Based Control Error - Improper software commanding of EPS components</td>
<td>Avionics / Command and Data Handling; Electrical Power; Environmental</td>
<td>Habitat / Suit Depressurization; Loss of Command / Control</td>
<td>MPCI Crew Module</td>
<td>CM: Avionics, CM: Electrical Power System, CM: Environmental</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1043</td>
<td>the vehicle loses all power</td>
<td>Electrical Power</td>
<td>Loss of Command / Control Capability; Loss of Crew</td>
<td>MPCI Crew Module</td>
<td>CM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1066</td>
<td>CAUS4: Software-Based Control Error - Software commanding error may cause incorrect control</td>
<td>Avionics / Command and Data Handling; Electrical Power; Environmental</td>
<td>Crew Incapacitation, Illness, or Injury; Loss of Command / Control</td>
<td>MPCI Crew Module</td>
<td>CM: Avionics, CM: Electrical Power System, CM: Environmental</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1070</td>
<td>CAUS9: Software-Based Control Error - Software commanding error may cause incorrect control</td>
<td>Avionics / Command and Data Handling; Electrical Power; Environmental</td>
<td>Crew Incapacitation, Illness, or Injury; Loss of Command / Control</td>
<td>MPCI Crew Module</td>
<td>CM: Avionics, CM: Electrical Power System, CM: Environmental</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPCI-1071</td>
<td>CAUS6: Software-Based Control Error - Software commanding error may cause incorrect control</td>
<td>Avionics / Command and Data Handling; Electrical Power; Environmental</td>
<td>Crew Incapacitation, Illness, or Injury; Loss of Command / Control</td>
<td>MPCI Crew Module</td>
<td>CM: Avionics, CM: Electrical Power System, CM: Environmental</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Adverse Condition Detail Form**

**AC Detail Form**

**AC Identifier**: MPCI-1012

**Mission Data**

- **Launch Date**: 2018-09-01
- **Development Start Date**: Ongoing
- **Human Rated**: Y
- **Mission Domain**: HEO
- **Data Marked at SBU**: 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 Low Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).

**AC Data**

**AC Origin**: MPCI-FLT-015 Failed / Partial Deployment of

1. 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 PDU's - Power Management (PWM) domain software performs command processing for the power distribution subsystem. 1.7 Vehicle System Management - subset of vehicle functions that

**Domain Links**

- **Domain Name**: Electrical Power

**Failure Types**

- **Failure Name**: Add/Delete Failure

**Hazard Types**

- **Hazard Name**: Loss of Command / Control Capability

**System Categorization**

- **System Name**: Add/Delete System
Mission Form

**Add/Edit Mission Data**

- **Launch Date**: 2018-09-01
- **Development Start Date**: (Blank)
- **Ongoing**: Y
- **Mission Domain**: MEO
- **Mission Name**: MPCV
- **Mission Type**: Human Rated
- **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 low Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).

**Mission Notes**

**Capabilities**

<table>
<thead>
<tr>
<th>Capability Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort</td>
<td>Provides abort capabilities while systems are on the pad, during launch and ascent and on-orbit operations.</td>
</tr>
<tr>
<td>Ascent Environment</td>
<td>Capability to withstand natural and induced environments experienced during ascent mission phases.</td>
</tr>
<tr>
<td>Attitude Control</td>
<td>Provide attitude control.</td>
</tr>
<tr>
<td>Auxiliary Comm</td>
<td>Auxiliary Voice Communication link capabilities.</td>
</tr>
<tr>
<td>Early Mission Termination</td>
<td>Provides early mission return capabilities while systems are performing in-orbit operations.</td>
</tr>
<tr>
<td>ECLS and RCS Services</td>
<td>Maintain habitable atmosphere, partial pressure, humidity, temp control, trace contaminant, hazard detect.</td>
</tr>
<tr>
<td>Entry Descent and Landing</td>
<td>Capability to withstand natural and induced environments experienced during applicable recovery phases.</td>
</tr>
<tr>
<td>Fueling and Conditioning</td>
<td>Includes propellant loading storage and pressurization capabilities.</td>
</tr>
<tr>
<td>Ground Processing</td>
<td>Provide ground operations capabilities for off-line processing, integrated operations, pad and launch operations.</td>
</tr>
<tr>
<td>Guidance and Navigation</td>
<td>Determine state vector, targeting, and control functions.</td>
</tr>
</tbody>
</table>

**Entities**

<table>
<thead>
<tr>
<th>Entity Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEL</td>
<td>Backup Engage Logic</td>
</tr>
<tr>
<td>BFS</td>
<td>Backup Flight Software</td>
</tr>
<tr>
<td>CDH</td>
<td>Command &amp; Data Handling</td>
</tr>
<tr>
<td>CFSW</td>
<td>Common Flight Software</td>
</tr>
<tr>
<td>CMT</td>
<td>Communicate &amp; Track</td>
</tr>
<tr>
<td>CORE</td>
<td>Core Flight Software</td>
</tr>
<tr>
<td>DACF</td>
<td>Display and Control Formats</td>
</tr>
<tr>
<td>DACM</td>
<td>Display and Control Management</td>
</tr>
<tr>
<td>ECLS</td>
<td>Environmental Control &amp; Life Support</td>
</tr>
<tr>
<td>EPS</td>
<td>Electrical Power Systems</td>
</tr>
<tr>
<td>GNC</td>
<td>Guidance, Navigation, Control, and Relocation</td>
</tr>
</tbody>
</table>
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?