Assuring NASA’s Safety and Mission Critical Software

Wesley Deadrick
IV&V Office Lead
NASA’s Independent Verification and Validation Program
Fairmont, WV
Origins of IV&V within NASA

- 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.
The Need for IV&V

Developing complex, safety and mission-critical software systems is inherently challenging, and that creates risk.
Independent Verification and Validation (IV&V) is an objective examination of safety and mission critical software processes and products.

**Independence:** 3 key parameters:
- Technical Independence
- Managerial Independence
- Financial Independence

**NASA IV&V perspectives:**
- Will the system’s software…
  - Do what it is supposed to do?
  - Not do what it is not supposed to do?
  - Respond as expected under adverse conditions?

**IV&V Technical Approaches:**
- Aligned with IEEE 1012
- Captured in a Catalog of Methods
- Spans the full project lifecycle

**Systems Engineering:** Determines if the right system has been built and that it has been **built correctly**

**IV&V Assurance Strategy**
The IV&V Project’s strategy for providing mission assurance
Assurance Strategy is driven by the specific needs of an individual project
Implemented via an Assurance Design
Communicated via Assurance Statements
What is IV&V? (continued)

• The IV&V Assurance Strategy is the selection and implementation of IV&V validation and verification processes
  – Implementation of the IV&V processes are driven by the IV&V Project’s risk assessment and unique characteristics
  – The Assurance Strategy is tailored to the needs of the individual projects

• The validation process provides empirical evidence that engineering products:
  – Satisfy system requirements allocated to software
  – Solve the right problems
  – Satisfy the intended use and user needs in expected operational environments

• The verification process provides empirical evidence that engineering products:
  – Conform to requirements (for example: for correctness, completeness, consistency, accuracy) during all life cycle phases (requirements, design, code, test)
  – Satisfy standards and best practices
  – Establish a basis for assessing the completion of each life cycle phase, and initiating other life cycle phases
What is IV&V? (continued)

- IV&V processes include assessments, analyses, evaluations, reviews, inspections, and testing of software artifacts during the entire development lifecycle that create evidence
  - Evidence is used to formulate recommendations that improve the quality (or reliability) of the system software
  - Evidence is used to make conclusions about the quality (or reliability) of the system software
  - Evidence is used to gain insight into the technical progress
  - Evidence is used to judge how thorough you’ve critiqued the system
- How much evidence \(\rightarrow\) it is a trade-off between criticality of the system being acquired/deployed
  - Life-sustaining subsystems would warrant an evidence package that clearly & objectively shows the software will operate safely (or clearly shows that it won’t)
  - Data management subsystems may warrant less of an evidence package
- The amount of evidence needed determines the rigor of the analysis
  - Analytical Rigor is the type and amount of IV&V processes to use for analysis
Establishing the IV&V Assurance Strategy

• The IV&V Program assesses the system to determine:
  – The inherent risk associated with the system capabilities
  – The role of software in those capabilities
  – Which software elements of the system warrant IV&V analysis
    – Software elements are generally the focal point of IV&V analyses; however, other lifecycle artifacts (for example: concept documentation, system design, etc…) are utilized to inform lower-level analyses

• Our process is called “Portfolio Based Risk Assessment” (PBRA)
  – Results in scores for impact (a measure of the effect of a problem) and likelihood (the potential for the existence of errors) for each system capability and software element
  – Enables informed decision making regarding:
    • What parts of the system should IV&V work on
    • What analytical rigor should IV&V apply (for example: dynamic analysis should be conducted to thoroughly test the implementation of the protocol used for communications)
Establishing the IV&V Assurance Strategy (continued)

<table>
<thead>
<tr>
<th>Subsystem Criticality Profile</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Subsystem 1** – do not recommend IV&V
**Subsystem 2** – recommend IV&V utilizing Static Analysis
**Subsystem 3** – recommend IV&V utilizing Dynamic Analysis
**Subsystem n** …

### Responsible Subsystems

<table>
<thead>
<tr>
<th>Subsystem Criticality Profile</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Subsystem 1** – do not recommend IV&V
**Subsystem 2** – recommend IV&V utilizing Static Analysis
**Subsystem 3** – recommend IV&V utilizing Dynamic Analysis
**Subsystem n** …

### Desirable Capabilities

**Launch Phase**
- Launch Abort
  - Launch Abort Systems
  - Trajectory Control
  - Attitude Control
- Approach Abort
  - Trajectory Control
  - Approach Abort Systems

**Maintain Flight Systems**
- Establish and maintain power
  - Power and Maintain Power
  - Perform Fault Detection
- Establish and maintain communications
  - Gather Engineering and Housekeeping Data
- Establish and maintain systems
  - Establish and maintain systems
  - Perform Fault Detection

**EOL**
- Pre-EDL
  - Entry
  - Descent
  - Landing

**Perform surface operations**
- Traverse surface
  - Traverse the Martian surface
  - Acquire and handle samples
  - Evaluate current conditions via TPS data
  - Perform reconnaissance activity
  - Collect science data

### Manual Analysis

- SMEs conduct formal or informal inspections & evidence is recorded simply as issues

### Static Analysis

- SMEs evaluate structure & content using various perspectives supported by CASE tools. Evidence is recorded as issues & supplemented with coverage

### Dynamic Analysis

- SMEs execute system & evaluate results. Evidence is recorded more thoroughly as to make the case for what works and what are limitations

### Formal Analysis

- SMEs apply formalisms & mathematical rigor to prove existence or absence of critical properties

### Amount of Rigor & Evidence Needed

- less
- more

**Subsystem Criticality Profile**

- 5: High
- 4: Medium High
- 3: Medium
- 2: Low
- 1: Very Low

**Impact**

- 5: Critical
- 4: High
- 3: Medium
- 2: Low
- 1: Very Low
Implementing the IV&V Assurance Strategy

- IV&V Assurance Strategy is implemented through the Assurance Design
  - The Assurance Design specifies the Technical Reference, inputs, analysis techniques, and objective evidence necessary to achieve the IV&V Project’s Objectives
  - Like the Assurance Strategy, the Assurance Design is specific to the needs of an individual project
    - Constructed to allow the IV&V Project to generate evidence to assure the critical capabilities and mitigate system risk
    - Areas of risk identified in the PBRA are key inputs into the development of the Assurance Design

- Assurance Statements are utilized to communicate the results of the implementation of the IV&V Assurance Strategy
  - A statement of the assurance that is being provided (or intended to be provided) by IV&V to a stakeholder or stakeholders on a system or subsystem
    - Assurance statements are typically formulated at the beginning of a IV&V Project and refined as necessary throughout execution
Tools for Implementing the IV&V Assurance Strategy

- NASA’s IV&V Program strives to continually develop new capabilities to support the execution of the IV&V Assurance Strategy
  - IV&V Techniques are documented in a Catalog of Methods (CoM)
  - Techniques are continually refined and tailored to the needs of the projects
- To maintain relevance, the IV&V Program selectively invests in new technologies necessary to assure NASA’s safety and mission critical software
  - NASA’s IV&V Program is advancing the state of the practice in Cybersecurity / Information Assurance and Independent Testing
    - Advanced techniques and capabilities are being developed to enable the program to keep pace with current development trends and emerging risk factors
    - Information Assurance and Independent Testing are becoming an increasingly prominent component of IV&V Project’s Assurance Strategies
Cybersecurity / Information Assurance


**Threat and Risk Assessment**
- FISMA Compliance
- Life-cycle
  - Provide mission security assurance throughout design, development, implementation, operation, maintenance, and disposition
  - Assessment and Authorization (A&A)
- Authority to Operate (ATO)

**Vulnerability Assessment / Penetration Testing**
- Implementation of Security Controls
- Monitoring of Security Controls
- Static Code Analysis (SCA)

**IV&V In-Phase IA Support**
- Build security in “from the ground up.”
- Security Architecture Verification
- IV&V Methods

**CyberLab**
- Component of ITC JSTAR Lab
- Virtualized servers
- Penetration Test tools
- Cybersecurity Knowledge Base
- Cybersecurity Training Program
- Mission System Virtualization and Testing
Independent Testing

Develop, maintain, and operate adaptable test environments for NASA’s IV&V Program that enable the dynamic analysis of software behaviors for multiple NASA missions.

**Simulation**
- Functional Software-only Simulators
- NASA Operational Middleware (NOS)
  - Common emulation software
  - Middleware
- Spacecraft Simulators
  - Ground systems, instruments, spacecraft dynamics
- Small Sat
- Integrate many technologies to create solutions

**Automation**
- Simulation Verification
- Increase Testing
  - Unit Testing
  - System Testing
- Automated Installations and Simulator Deployments

**Testing**
- Provide evidence-based assurance to customer
- Risk-focused independent testing
- Focused on testing adverse conditions
  - Fault injection, back-to-back scenarios, etc.

**Virtualization**
- Heavy reliance on virtualization technologies
  - Development
  - Simulator Releases
  - Rapid Deployment
  - Evaluation Environments
Summary
Benefits of IV&V

- Yields higher confidence that delivered products are error free and meet the user needs.
- Increases likelihood of uncovering high-risk errors early in the development lifecycle.
  - Allows time for the design team to evolve a comprehensive solution rather than forcing them into a makeshift fix to accommodate deadlines.
- Delivers ongoing status indicators and performance reporting to decision makers (e.g. program managers).
  - The customer is provided an incremental preview of system performance with the chance to make early adjustments.
- Reduces the need for rework from the developing contractor thereby reducing total costs to programs and projects.
- Facilitates the transfer of system and software engineering best practices.

IV&V leads to higher quality products, reduced risk, greater insight, reduced cost, and knowledge transfer.
QUESTIONS?
IV&V plays a key role in a number of high-profile NASA and non-NASA missions.
Generic Look at IV&V

- **Concept Analysis**
  - (validate selected solution, validate s/w reuse strategy, verify sys. architecture is complete, ensure security threats & risks are known)

- **Requirements Analysis**
  - (ensure the requirements are high quality (correct, consistent, complete, accurate, unambiguous, and verifiable) and adequately meet the needs of the system and user)

- **Design Analysis**
  - (ensure the design is a correct, accurate, and complete transformation of the requirements that will meet the operational need under nominal and off-nominal conditions and that no unintended features are introduced)

- **Code Analysis**
  - (ensure the implementation is correct, accurate, and complete, relative to requirements, operational need under nominal and off-nominal conditions, and introduces no unintended features)

- **Test Analysis**
  - (ensure testing will serve as a sufficient means to verify and validate that the implementation meets the requirements and operational need under nominal and off-nominal conditions)

- **Operational & Maintenance Analysis**
  - (ensure operating procedures are correct and usable, new constraints & changes are understood and appropriately addressed, and ensure anomalies are understood and appropriately addressed)

- **Criticality Analysis**
  - (identify most critical areas of the system)