NASA’s Independent Verification and Validation (IV&V) Program and Gateway IV&V Project

August 14, 2019
Bill Stanton, Gateway IV&V Deputy Project Manager
Fairmont, West Virginia
www.nasa.gov/centers/ivv
What is IV&V?

- **Verification**
  - Are we building the system right?

- **Validation**
  - Are we building the right system?

- **Independent**
  - *IEEE Standard for System and Software Verification*, IEEE 1012, defines three important criteria for IV&V independence
    - Technical Independence - Different personnel; not the same people who build it
    - Managerial Independence - Planning and scoping control. Independent reporting path
    - Financial Independence - Funding from a source separate from project development
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.
IV&V Program budget covers all IV&V Program needs, including technical work, physical and IT infrastructure, security, etc.
Benefits of IV&V

- **Increased Safety and Dependability** - Greater confidence-delivered products are error free and meet user needs. Many IV&V-identified defects threaten loss of mission or loss of crew if not resolved.

- **Reduced Risk** - Increased likelihood high-risk errors are detected early, allowing time for the development team to evolve a comprehensive solution rather than a forced makeshift fix to accommodate deadlines.

- **Greater Management Insight** - Increased insight into project status and performance through independent perspective and objective evidence.

- **Reduced Cost** - Reduced development rework, reducing total program and project costs for a positive return on investment.

- **More Knowledge Transfer** – Increased communication across project teams and cross-project transfer of system and software engineering best practices.

**IV&V is an industry-proven approach to increase quality, reduce risk, gain development insight, reduce cost, and transfer knowledge.**
NASA’s IV&V Approach

- **Full Lifecycle** - Not just testing at the end. For NASA, IV&V starts near Mission SRR, continues up to, and sometimes beyond, launch.
- **Product Focused** – Not document or compliance focused. Examines concept, architecture, requirements, design, code, and test products.
- **Capability Based Assurance (CBA)** – Keeping the “big picture” in view when assessing the software details.
- **Follow the Risk** – Dynamically adapting plans to focus assurance activities where evidence indicates there is risk.
- **Use Multiple Perspectives for Analyses**
  - Add assurance the software will do what it is supposed to do.
  - Add assurance the software will not do what it is not supposed to do.
  - Add assurance the software will respond appropriately under adverse conditions.

**NASA IV&V** is a systems engineering process employing rigorous methodologies for evaluating the correctness and quality of software products throughout the SDLC for NASA’s highest profile missions.
IV&V Assurance Strategy: Concept

- The IV&V Assurance Strategy is the identification/selection of
  - Which mission capability and system software risk to target
  - Which IV&V techniques to use to help reduce the targeted risk
- IV&V techniques include assessments, analyses, evaluations, reviews, inspections, and testing of software artifacts during the entire development lifecycle that create evidence
  - Aligned with IEEE 1012
  - Documented in a Catalog of Methods
- How much evidence? → it is a trade-off between criticality of the system(s) 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 and type of evidence needed determines the rigor of the analysis
  - Analytical Rigor is the type and amount of IV&V techniques to use
How IV&V Uses Evidence

• Support recommendations for the developers that improve the quality (or reliability) of the system software
• Support assurance conclusions about the quality (or reliability) of the system software
• Adjust the IV&V Assurance Strategy to focus on the most critical software
• Gain insight into the progress of development
• Evaluate thoroughness of analysis
Establishing an IV&V Assurance Strategy

• The IV&V Program assesses a mission 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

• The IV&V Program’s process for this assessment 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 an IV&V Assurance Strategy (continued)

**Subsystem Criticality Profile**

- **Likelihood**
  - 5
  - 4
  - 3
  - 2
  - 1

- **Impact**
  - 5
  - 4
  - 3
  - 2
  - 1

**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** ...

---

**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 to more
Implementing an IV&V Assurance Strategy

- An IV&V Assurance Strategy is implemented by a set of Analysis Activities
  - Each Analysis Activity achieves one or more IV&V Project’s Assurance Objective
  - The IV&V Assurance Strategy informs the Technical Reference and which IV&V technique to use
  - An Analysis Activity generates the evidence for a specific Assurance Objective
- Possible outcomes of implementing the IV&V Assurance Strategy
  - Assurance Conclusions at varying levels of confidence and that are based on evidence from analyses performed
  - Findings or defects: “Issues”, a.k.a “TIM”s (Technical Issue Memorandum)
  - Candidate technical risks for adoption by the Program or Project
  - Refinement of the technical reference
  - Refinement of IV&V Assurance Strategy
1. Risk-Prioritize System Capabilities and Software for Assurance using PBRA/RBA and IVV S3106, and Develop High-Level Assurance Objectives (AOs)

   **Capability:** Entry, Descent, and Landing (EDL)
   **Entity:** Orion Timeline Vehicle Manager (TVM)
   **Objective:** Assure TVM correctly evaluates and detects critical events, to mitigate risk of inappropriate or missed event detection

2. Formulate Risk-Driven Assurance Design in Technical Scope and Rigor (TS&R), and Select and Tailor Analysis Methods using COMPASS and IVV 09-1

3. Develop IV&V Technical Reference, Studying Artifacts and Collaborating with Developers and IV&V Team to Identify IV&V Questions/Concerns to “Follow the Risk”

   **Learn and Understand:** IV&V created a flow diagram to model condition evaluation and event detection behavior, start to finish, capturing timing, data paths, and interfaces.

4. Execute Planned Analysis: IV&V traced expectations to TVM software and searched for answers to IV&V Questions/Concerns. IV&V noted differences in comparison logic between code methods intended to provide the same behavior, in critical event condition detection code.

5. Confirm Potential Issues: IV&V analyzed the logic and proved the code incorrect in 8 separate instances.

6. Evaluate Issue Significance and Document Issues: The incorrect code would have resulted in incorrect evaluation and detection of critical events, plausibly leading to Loss of Mission (LOM) during EDL, which relies significantly on event-driven behavior (Severity 1).

7. Communicate Issue and Track to Resolution: Orion accepted and resolved this significant issue.

8. **Condition Equivalent**
   
   $|x| < y \text{ (x < y) AND NOT (x <= -y)}$

9. **Incorrect Code in Critical Software Method**
   
   ```c
   584: case TVM Mission: LESS THAN:
   585: if (x <= -y) {LclRet = false;}
   586->: if (x < y) {LclRet = true;}
   587: break;
   ```
IV&V Communication Methods

- Interact with Program and Project staff in working group meetings to establish system understanding and communicate IV&V focus and status
- Communicate findings as soon as possible directly to the developer (e.g. during peer reviews of artifacts or software hosted by the Program, Projects or providers)
- Deliver reports at the completion of major work activities that summarize analysis approaches and results
- Communicate status of assurance objectives and summaries of assurance conclusions in presentations at Program and Project milestone reviews
- Communicate value of IV&V accomplishments in the IV&V Program’s weekly reports and monthly status reviews to the Agency
Status of Gateway IV&V

• First round of prioritizing the expected Gateway system capabilities and software and developing high-level Assurance Objectives (AOs) is complete and under internal review within the Program
  – Plan is to review results of the assessment with the Gateway Program and Module Projects
• Finalizing a risk-driven strategy to accomplish the assurance objectives that leverages the IV&V Program’s technical framework and applies appropriate analytical rigor
• Developing the IV&V team
• Supporting the Gateway Program’s efforts to certify Core Flight Software (CFS) for Gateway
Gateway IV&V Next Steps

• Continue to support CFS certification effort
• Finalize the initial Gateway IV&V Project Execution Plan (IPEP)
  – Identify which Assurance Objectives (AOs) to target and what techniques to use (e.g. exploring option to use formal methods for some AOs like those for assuring autonomous behavior)
  – Review the IPEP with the Gateway Program
• Begin executing according to the IPEP
  – Plan analysis activities that targets integrated Gateway system and software artifacts and Gateway module system and software artifacts as they mature and become available
  – Develop technical references in SysML for analysis activities by studying Gateway artifacts and collaborating with Program and Project staff to identify questions/concerns to target analysis (i.e. “Follow the Risk”)
  – Develop plan for establishing an independent Gateway VSM and software test capability for the Gateway IV&V Project
IV&V’s Goal is Mission Success
NASA’s Independent Verification and Validation Program

For More Information

https://www.nasa.gov/centers/ivv/program_flyers.html
QUESTIONS?
The IV&V Program’s mission is to provide our customers assurance that their safety and mission-critical software will operate reliably and safely.

- **System and Software Assurance**
  - Full Lifecycle IV&V
  - Independent Assessments
- **Safety and Mission Assurance (SMA) Support**
  - Common support infrastructure for assuring core Software Assurance functions across the Agency
  - Software Assurance Research Program (SARP)
- **Mission Protection Services (MPS)**
  - Cybersecurity Threat/Risk Assessment, Vulnerability Assessment, Information Assurance (IA) Support, CyberLab, FedRAMP
- **Jon McBride Software Testing And Research (JSTAR) Laboratory**
  - Independent Test Capability (ITC), Robotics
    - Simulation, Testing, Automation, and Virtualization
- **Partnerships, Collaboration, and Leadership**
  - MDA, International IV&V WG, WVANG, DOE, OSMA, FBI, NOAA, DOD/Army, CCSDS, OCIO, OCE, STF-1, GSFC Code 300, 400, 500, 700, 800
- **STEM Engagement**
How do IV&V Projects provide the most value to the Agency?

... by getting involved early in the SW development lifecycle
13 of 13 active IV&V projects started before mission SRR.

... by detecting defects in-phase with SW development
Overall phase containment by active projects: 92% over the past year.

... by detecting and submitting quality defects to the development teams
Overall issue acceptance for active projects was 95% over the past year.

... by ensuring our customers are satisfied with our products and services
ACTUAL: 2018 Annual Survey: 99.7% of all responses indicated a favorable (“Agree” or “Strongly Agree”) perception of the support being provided by the IV&V Program.