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.
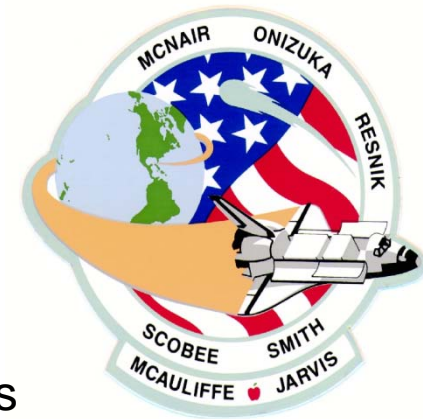
The Need for IV&V

NASA Decides That A Software Error Doomed The Mars Global Surveyor Spacecraft

By Keith Cowing   Posted Wednesday, January 10, 2007

During a meeting of the Mars Explorat[ion] Group Meeting in Washington Dc, yest[erday] McNamee, Mars Exploration Program [...] the recent failure of the Mars Global Surveyor (M[GS]) spacecraft.

Software Glitch Blamed for Turning Satellite Into Space Zombie

Peter B. de S[...]

Office of the Chief Engineer O C E

Reports

Text Size [+] [−]

Technical Excellence Initiative

NASA Study on Flight Software Complexity

In 2007 the NASA Office of Chief Engineer commissioned a multi-Center study of the growth in flight software size and complexity in NASA space missions. The

Software Glitch Means Loss of NASA's De[ep Impact] Comet Probe

timothy posted about 4 months ago | from Taco Cowboy ⭐

Taco Cowboy writes "'NASA is ca[...]
comet probe after a suspected so[...]

Inquiry Board Traces Ariane 5 Failure to Overflow Error

Readers of *SIAM News* may remember that on June 4, less than a minute into its first flight, the French rocket Ariane 5 self-[d...] des études spatiales) and ESA (the European Space Agency) to investigate the failure was chaired by applied mathematician [...]

Developing complex, safety and mission-critical software systems is inherently challenging, and that creates risk.

3

What is IV&V?

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?

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

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

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 <u>empirical evidence</u> 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 <u>empirical evidence</u> 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 <u>evidence</u>
  - 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 → 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)
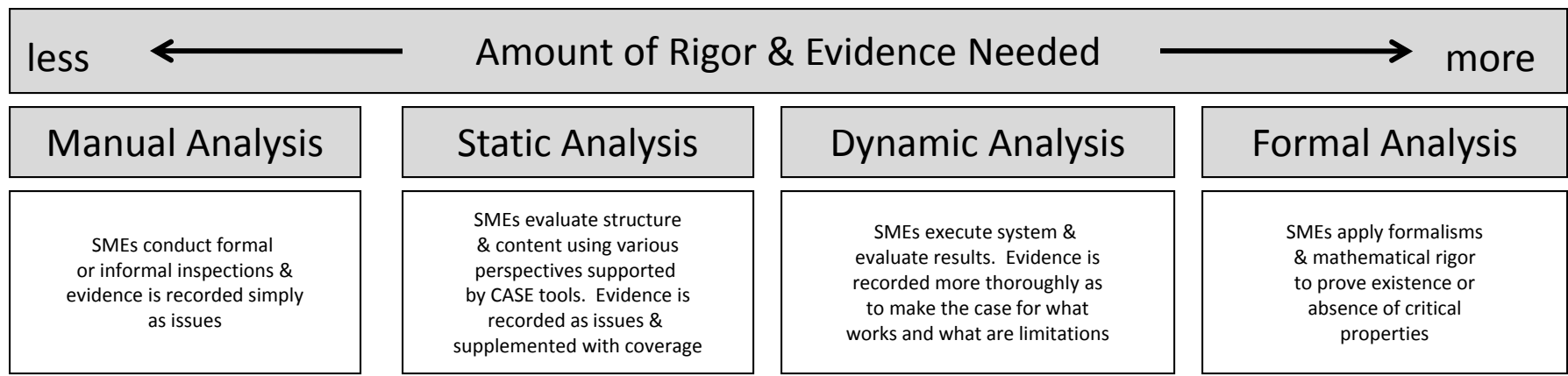
Establishing the IV&V Assurance Strategy (continued)

Responsible Subsystems

Desired Capabilities	Cruise - GNC	Cruise - Thermal (1)	Cruise - Telecom (2)	Cruise Power	EDL GNC (3)	Rover: Startup & Initialization	Rover: C&DH
Conduct habitability investigations							
Launch to Mars							
Cruise to Mars	x	x	x	x		x	x
Trajectory control	x		x				
Attitude Control	x		x				
Approach Mars					x		
Trajectory control	x				x		
Attitude Control	x						
Maintain flight systems							
Establish and maintain power					x		x
Establish and maintain thermal control		x					x
Perform fault detection							x
Establish and maintain communications			x				x
Gather engineering and housekeeping data	x	x	x	x	x	x	x
EDL							
Pre-EDL					x		
Entry					x		
Descent					x		
Landing					x		
Perform surface operations							
Traverse the Martian surface						x	x
Acquire and handle samples						x	x
Evaluate current position via TRS data							
Perform reconnaissance activity						x	x
Collect science data						x	x

Subsystem Criticality Profile

Likelihood (vertical axis: 1–5) vs Impact (horizontal axis: 1–5)
- Subsystem 1 at (2, 3)
- Subsystem 2 at (3, 3)
- Subsystem 3 at (4, 4)

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 …

---

less ←———— **Amount of Rigor & Evidence Needed** ————→ more

Manual Analysis	Static Analysis	Dynamic Analysis	Formal Analysis
SMEs conduct formal or informal inspections & evidence is recorded simply as issues	SMEs evaluate structure & content using various perspectives supported by CASE tools. Evidence is recorded as issues & supplemented with coverage	SMEs execute system & evaluate results. Evidence is recorded more thoroughly as to make the case for what works and what are limitations	SMEs apply formalisms & mathematical rigor to prove existence or absence of critical properties

Implementing the IV&V Assurance Strategy

- IV&V Assurance Strategy is implemented through the Assurance Design
  - The Assurance Design specifics 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

Ensuring Mission and Safety Critical Software and Systems Operate Reliably, Safely, and Securely

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 <u>products are error free and meet the user needs</u>.

- Increases likelihood of <u>uncovering high-risk errors early in the development lifecycle</u>.
  - 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 <u>chance to make early adjustments</u>.

- Reduces the need for rework from the developing contractor thereby <u>reducing total costs to programs and projects</u>.

- Facilitates the transfer of <u>system and software engineering best practices</u>.

IV&V leads to higher quality products, reduced risk, greater insight, reduced cost, and knowledge transfer.

QUESTIONS?

IV&V Services

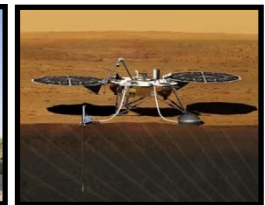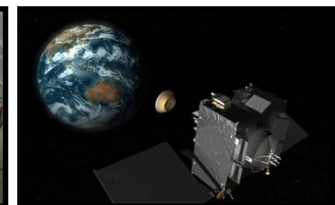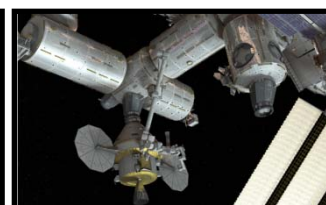IV&V plays a key role in a number of high-profile NASA and non-NASA missions.

Generic Look at IV&V

Needs Analysis & Concept Phase	**Concept Analysis** {validate selected solution, validate s/w reuse strategy, verify sys. architecture is complete, ensure security threats & risks are known}
Requirements Specification	**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	**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}
Implementation	**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 }
Integration & Test	**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}
Ops & Maintenance	**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}