
NASA
How NASA's Independent Verification and Validation (IV&V) Program Builds Reliability into a Space Mission Software System (SMSS)
http://www.nasa.gov/centers/ivv/home/index.html

Acknowledgements

- Kristin Wortman for inviting the NASA IV&V Program to participate in this workshop
- The NASA IV&V Program (especially Marcus Fisher, Jeff Northey and Wes Deadrick) for their contributions to this presentation

NASA IV&V Program

- **Mission:** To provide our customers assurance that their safety and mission-critical software will operate **reliably** and **safely**
- Assurance is focused on:
  - Confidence that the software will do what it is supposed to do
  - Confidence that the software will not do what it is not supposed to do (ensure fault avoidance)
  - Confidence that the software will appropriately act/react to/under adverse conditions (ensure fault tolerance)
- Technical Issue Memorandums (TIMs) are provided to the developer when evidence suggests that any of the above assurance statements cannot be made
- Risks are proposed to the developer for adoption when evidence suggests the development process puts software quality (incl. reliability) at risk
- Reliability is increased when TIMs are resolved or risks are mitigated. (assist in fault removal and fault prevention)

What is IV&V?

IV&V, as a part of software assurance, plays a role in the overall NASA software risk mitigation strategy applied throughout the life cycle, to improve the safety and quality of software.

Software Assurance "umbrella", described in NASA's Software Assurance Standard (NASA-STD-8739.8)

Introduction to IV&V

- Software Verification and Validation (V&V) is a systems engineering discipline.
  - V&V is more than testing, just like development is more than coding!

- The purpose is to help the development organization build quality (e.g. reliability) into the software **during** the software life cycle.
  - Some objectives of performing V&V:
    - Facilitate early detection and correction of software errors,
    - Enhance management insight into process and product risk,
    - Support the software life cycle processes to ensure compliance with program performance, schedule, and budget requirements.

- As part of Software Assurance at NASA, and utilizing IEEE standards, IV&V is differentiated from V&V because it is managerially, technically, and financially separated from developers

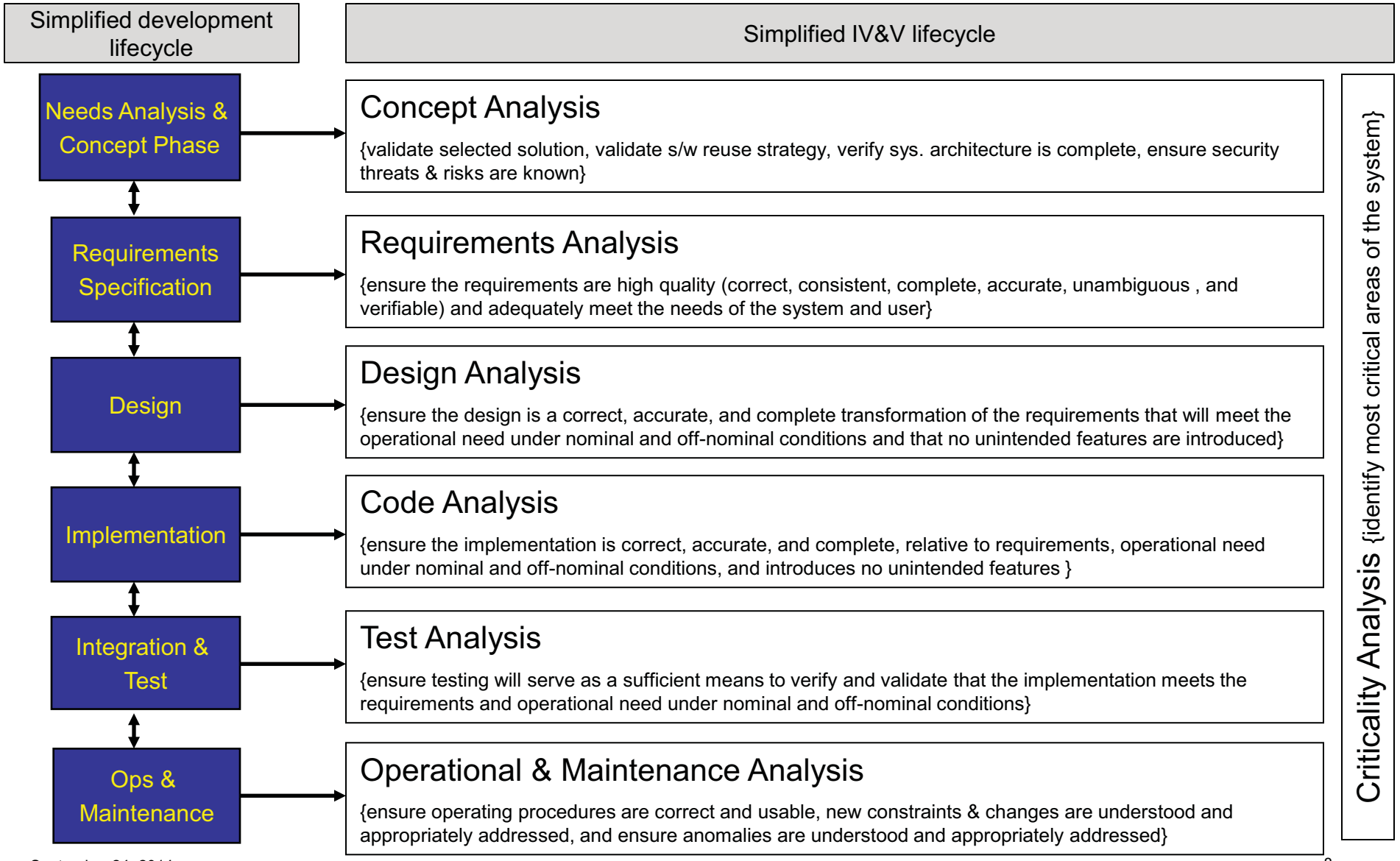
Introduction to IV&V (cont)

- IV&V processes determine if development artifacts of a given activity conform to the requirements of that activity, and if the software artifacts satisfy the intended use and user needs.
- The validation process provides empirical evidence that engineering products:
  - Satisfies system requirements allocated to software
  - Solves the right problem
  - Satisfies the intended use and user needs in expected operational environment
- The verification process provides empirical evidence that engineering products:
  - Conform to requirements (e.g., for correctness, completeness, consistency, accuracy) during all life cycle phases (e.g., requirements, design, code, test),
  - Satisfy standards and best practices,
  - Establish a basis for assessing the completion of each life cycle phase and for initiating other life cycle phases.

Introduction to IV&V (cont)

- 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 (e.g. reliability) of the system software
  - Evidence is used to make conclusions about the quality (e.g. 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 methods to use for analysis

Generic Look at IV&V

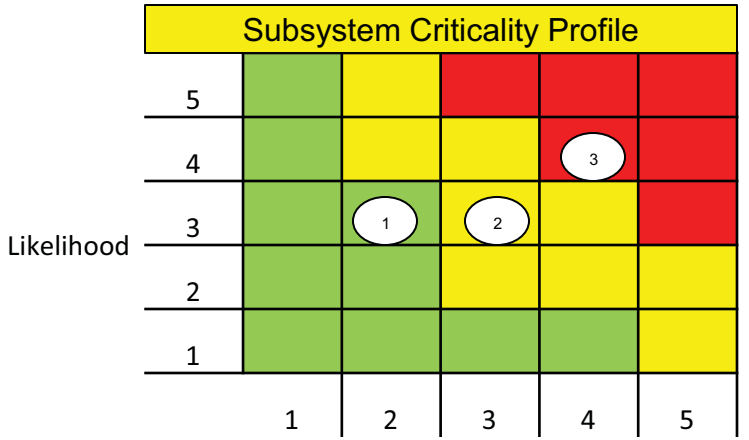


Determining the IV&V Assurance Strategy

- The IV&V Program assesses the system to determine
  - which capabilities of the system warrant IV&V analysis
  - the role of software in those capabilities
  - which software elements of the system warrant IV&V analysis
- The 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 decisions to be made regarding:
    - What parts of the system should IV&V work on
    - What analytical rigor should IV&V apply (e.g. dynamic analysis should be conducted to thoroughly test the implementation of the protocol used for communications)

Determining the IV&V Assurance Strategy (cont)

Desired Capabilities	Cruise - GNC	1 Cruise - Thermal	2 Cruise Telecom	Cruise Power	3 EDL GNC	Rover: Startup & Initialization	Rover: C&DH
	Responsible Subsystems						
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 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

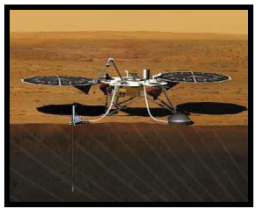
Subject Matter Expertise

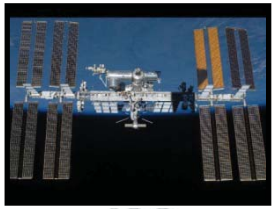
- IV&V Processes are applied by individuals with subject matter expertise in
  - The analysis method
  - The application of the software under analysis
  - The technologies and methods use to develop the software under analysis
  - The types systems that the software under analysis will be integrated with
- IV&V Program Leverages over 20 years of experience providing IV&V services to the NASA

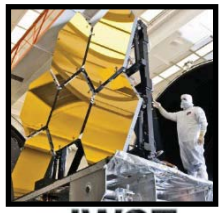
Current SMSS IV&V Projects


•GOES-R

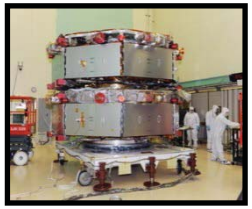

•ICESat-2

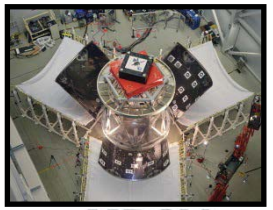

•InSight

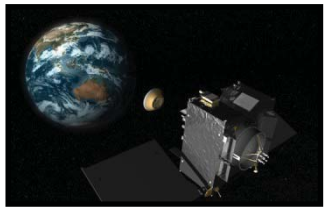

•ISS

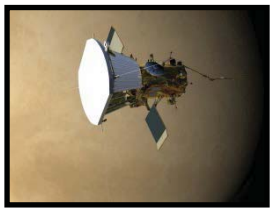

•JWST

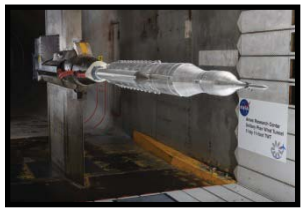

•JPSS


•MMS


•MPCV

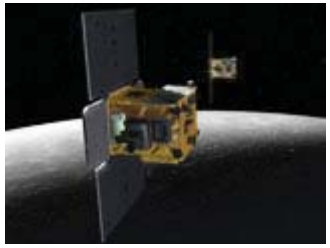

•OSIRIS-REx


•SPP


•SLS

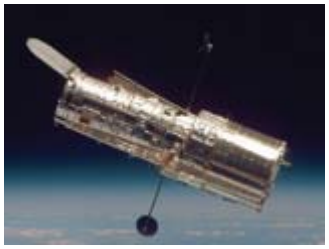
Past SMSS IV&V Projects

(not exhaustive)

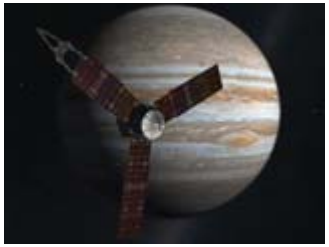


•GRAIL

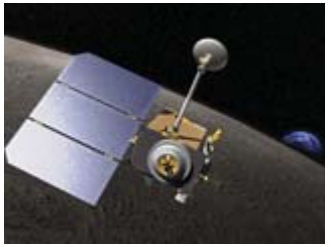
•GPM



•HST

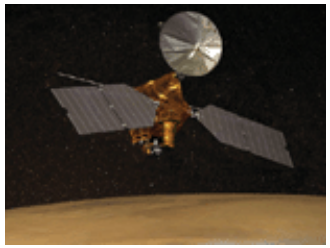


•Juno



•LRO

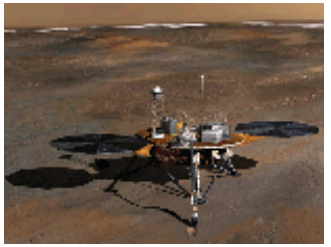
•MAVEN



•MRO

•MSL

•New Horizons



•Phoenix

•SSP

Summary

- IV&V helps build reliability into SMSSs by
  - Increasing the likelihood of discovering and removing critical defects throughout the development lifecycle
  - Focusing analyses on ensuring correct and complete fault avoidance, and fault tolerance
  - Applying best practices in its assessments, analyses, evaluations, reviews, inspections, and testing of software artifacts