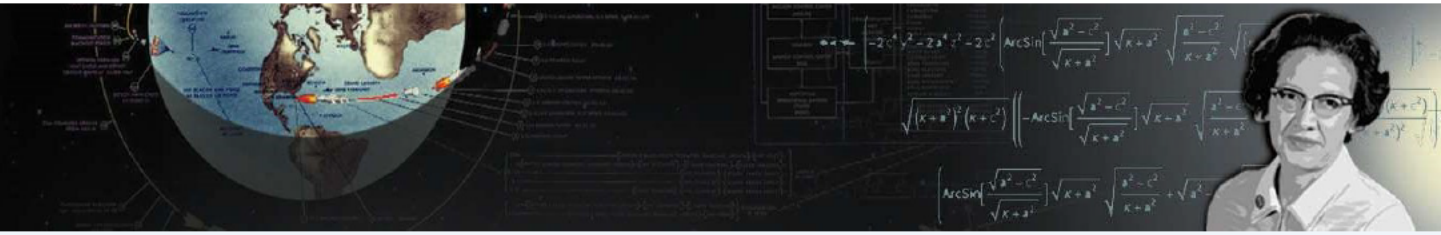
SAS2
NASA IV&V Overview

NASA Independent
Verification and Validation
(IV&V) Program

NASA's Independent Verification & Validation Program



NASA's IV&V Program was established 1993, triggered by Challenger accident.

Independent Verification & Validation 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.

- Category 1 and Category 2 (Payload Class A and B) missions.
- Currently supporting: EGS, Europa, Gateway, ISS, JPSS-2, JWST, Landsat 9, Lucy, Psyche, Orion, M2020, MCC, SLS, WFIRST, Roman Space Telescope
- NPD7120.4 Engineering & Program/Project Management policy is to use the IV&V Program as the provider of IV&V services; Criteria for determining which NASA projects are required to have IV&V are defined in NPR 7150.2

Functionally, we are part of OSMA, reporting to OSMA Chief, Terry Wilcutt.
Administratively we are GSFC Code 180 and receive support from Goddard.

We provide SMA (Safety & Mission Assurance) Support and outreach products and services to various Centers, Programs and Projects including Software Assurance and Mission Protection Services.

We provide cybersecurity assessments on the Agencies high value and supporting high value mission assets.

Our program maintains industry leading simulation and test labs including: JSTAR, CyberLab, and an MBMA Lab.

- The Jon McBride Software Testing and Research (JSTAR) lab is an independent test facility that provides software simulation and testing. It was awarded an Agency software of the year runner up (representing GSFC) last year, and previously received an honorable mention twice.

We provide WV students with STEM engagement. Through the combined efforts of our Education Resource Center, Robotics initiatives, and Education Outreach Specialists we reach students in all corners of the state.

Primary building recently renamed:
Katherine Johnson IV&V Facility

History of NASA's IV&V Program

NASA's Independent Verification & Validation (IV&V) Program was established as part of an agency-wide strategy to provide the highest achievable levels of safety and cost-effectiveness for mission critical software. NASA's IV&V Program was 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 disaster.

January 28, 1986

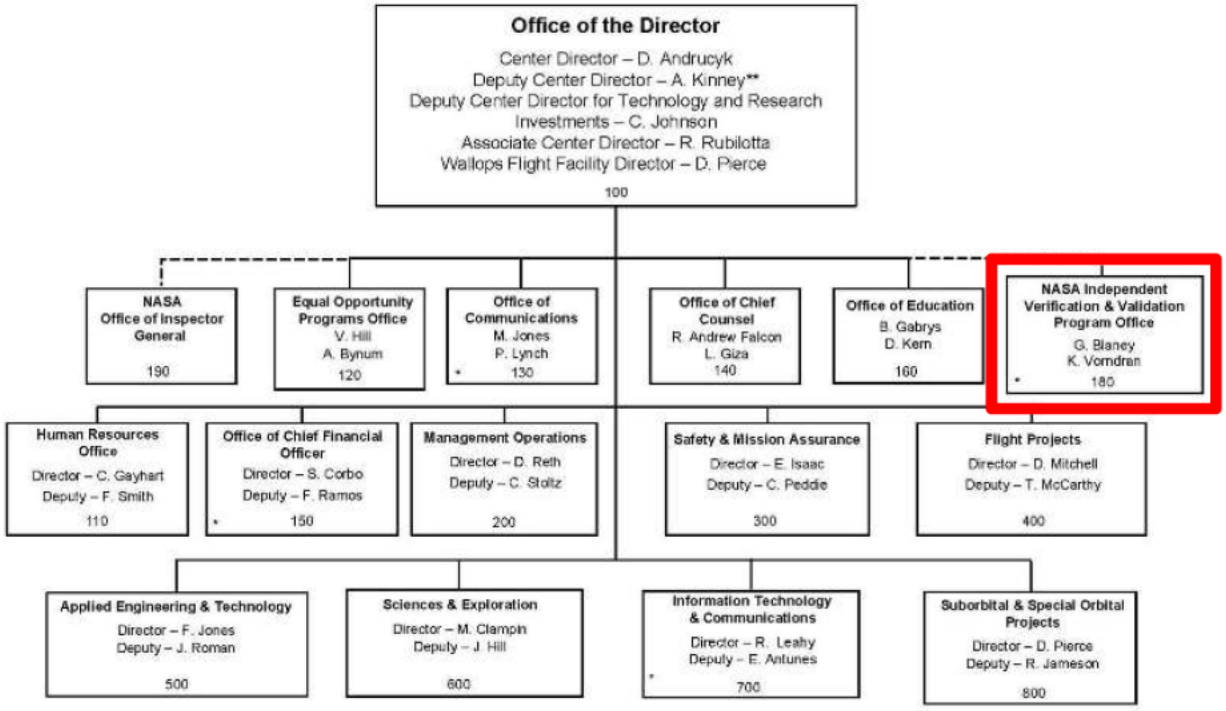
- 1991 - Grant to WVU to build IV&V Facility. Program assigned to HQ-OSMA
- 1994 - Space Station Program Implements IV&V through NASA's IV&V Program
- 1996 - Program assigned to AMES Research Center Focus = Research
- 1996 - Facility Omnibus contract: Enabled IV&V across all NASA Projects
- 1999 - Senior Management Council: IV&V mandate for all NASA software
- 2000 – Program transitioned to GSFC Focus = Applied
- 2003 - IV&V Funding changed to Corporate G&A
- 2003 – IV&V Program is functionally assigned to OSMA
- 2004 - IV&V Board of Advisors formed
- 2009 - IV&V added to NPR 7150.2A
- 2010 - Program reorganization to current org structure
- 2011 - Instantiation of JSTAR & Independent Test Capability
- 2012 - ISC Contract award – Single IV&V Service provider
- 2012 - IV&V Completed 22+ years of Space Shuttle IV&V
- 2012 - GO-SIM Software of the Year - Honorable Mention
- 2012 - ECTP Work began
- 2013 - Work with Commercial Crew partners began
- 2015 - Vulnerability Assessment Program (VAP) established
- 2015 - Released Secure Coding Portal (SCP) for the Agency
- 2016 - IV&V accredited as a FedRAMP 3PAO
- 2016 – JIST (JWST Simulator) Software of the Year - Honorable Mention
- 2018 – Cybersecurity Assurance Activities began
- 2019 – Office of Information Technology established
- 2019 – Naming of the IV&V Facility the Katherine Johnson IV&V Facility

OSMA

Office of Safety and Mission Assurance
CHIEF, SAFETY AND MISSION ASSURANCE
Terrence W. Wilcutt
Executive Assistant
Joyce Minor
DEPUTY CHIEF
Frank Groen, Ph.D.
Executive Assistant
Joyce Minor
NASA CENTER SMA DIRECTORS
• Ames Research Center: D. Demo
• Armstrong Flight Research Center: G. Graham
• Glenn Research Center: K. Martzaklis
• Goddard Space Flight Center: E. Isaac
• Jet Propulsion Laboratory: R. Nybakken
• Johnson Space Center: R. DeLoach
• Kennedy Space Center: J. Kunz
• Langley Research Center: F. Peri
• Marshall Space Flight Center: R. Burt
• Stennis Space Center: G. Benton
Resources Management Office
Paul Mexcur
Senior Safety and Mission Assurance Manager
P. Martin
Mission Assurance Standards and Capabilities Division
Dr. Matt Forsbacka
Administrative Specialist
LaChell Myles
Missions and Programs Assessment Division
Deirdre Healey
Secretary/Correspondence
Tierra Green
Institutional Safety Management Division
Grant Watson
Program Coordinator
Sue Roney
NASA Safety Center
Harmony Myers
Executive Assistant
Dennie Gonia
NASA Independent Verification & Validation (IV&V) Program
Gregory D. Blaney
Executive Assistant
David Runyon

GSFC

Goddard Space Flight Center Organization Chart

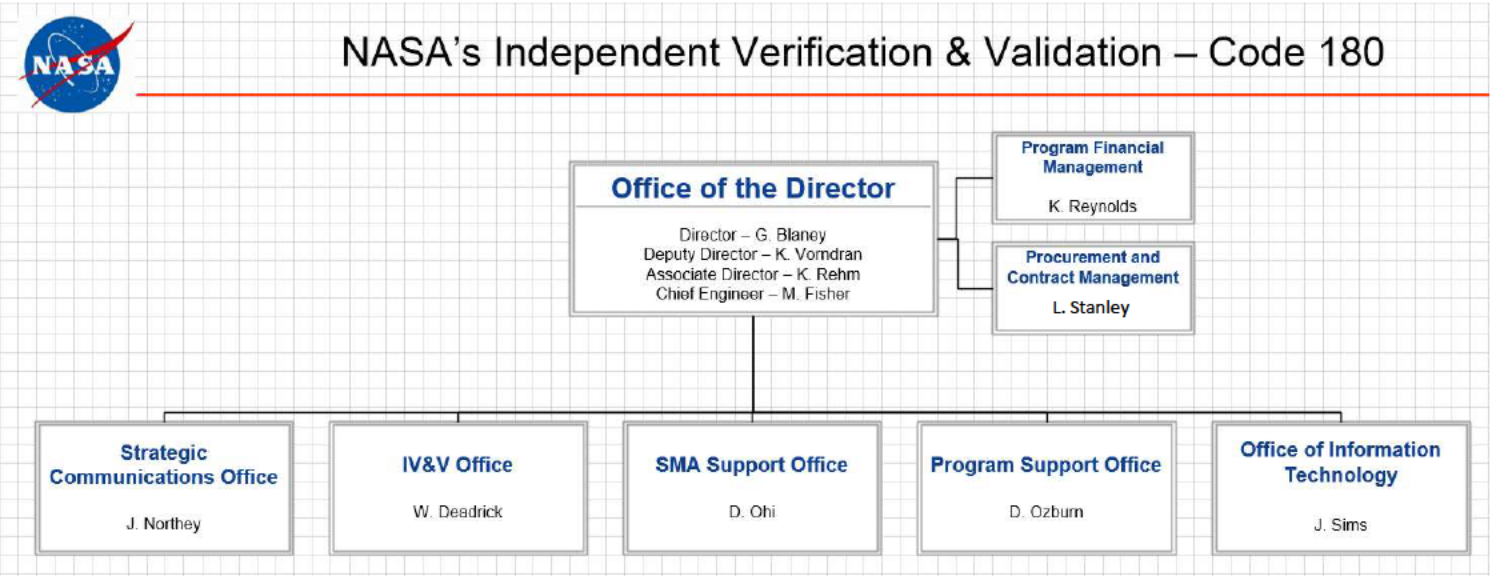


Updated: Sep. 2020

* Reports directly to NASA Headquarters
** as of May 24, 2020

IV&V Program

The NASA IV&V Program functions operationally under the guidance of the Office of Safety and Mission Assurance while receiving administrative support from GSFC [NASA IV&V is Code 180 (Center Director's direct report)]. The NASA IV&V Director serves as the NASA IV&V Program Manager and reports directly to the Chief, Safety and Mission Assurance.



NASA IV&V Program Strategic Plan: Vision and Mission

- **Vision -** Be a world leader in systems and software engineering that enables our customers' success.

- **Mission -** To provide our customers assurance that their safety and mission critical systems and software will operate reliably, safely and securely, and to advance the systems and software engineering disciplines. In doing so, we work to standards of excellence, focus on customer satisfaction, inspire and advance the next generation, and adhere to and demonstrate our core set of values: **safety, integrity, respect, teamwork, balance, innovation and excellence.**

NASA IV&V Program Values

Safety

We consider protecting ourselves and others from unnecessary harm as a cornerstone to success. We are committed, individually and as a team, to protecting the safety and health of the public, our team members, and those assets that the Nation entrusts to the Agency. With safety first, our commitment to all other values can be achieved.

Integrity

Our success is built on an environment of trust and ethical behavior. We exhibit sincerity and truthfulness in all actions.

Respect

We respect ourselves and each other, appreciating the creativity and broader perspective of a diverse team. This diversity is vital to our success.

Teamwork

We understand and believe that thinking, planning, decision-making and actions are better when done cooperatively. We recognize, and even assimilate, the belief that "none of us is as good as all of us." We recognize that our function exists to serve the bigger picture.

Balance

We believe in the importance of meaningful daily achievement and enjoyment in each of our four life quadrants: work, family, friends, and self.

Innovation

We cultivate creativity and seek knowledge that will strengthen our teams and ourselves. We recognize innovation as a way to energize our motivation and performance, leading to a sense of pride and personal accomplishment.

Excellence

We consistently look for ways to improve ourselves and our organization by promoting continual growth, learning and diversity of experience. We believe in providing high quality services that bring long term value to our customers.

NASA's IV&V Approach

- **Full Lifecycle -** For NASA, IV&V starts near Mission System Requirements Review (SRR), continues up to, and sometimes beyond, launch.
- **In Phase** - IV&V services are provide in-line with the system and software development to enable timely consideration and incorporation of IV&V issues, risks, and assurance results.
- **Mission Oriented** – IV&V strives to be a partner in mission success. Projects are viewed as key stakeholders. IV&V can not be successful without project buy in.
- **Product Focused** – Not process or compliance focused. IV&V concentrates efforts on the system and software products that are essential to constructing a system the fulfills mission goals and objectives (i.e., Level 1 requirements).
- **Capability Based –** Keeping the "big picture" in view when assessing the software details. Software functionality is evaluated within the context of the system capabilities they contribute to.
- **Risk Driven –** IV&V dynamically adapts plans to focus assurance activities where evidence indicates there is risk.

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.

NASA's IV&V Approach:
Observed Benefits

- **Increased Safety and Dependability** - Greater confidence that 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 to Safety and Mission Critical Software** - 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.
  - NASA IV&V has documented **536 valid Severity 1 or 2** (potentially mission ending) issues over the last 5 years alone.
- **Greater Management Insight** - Increased insight throughout the software development lifecycle through independent perspectives and objective evidence.
- **Increased Confidence –** IV&V generates empirical evidence as a complement to identified issues and risk which equate to greater confidence in the delivered software.
- **Reduced Development Cost** – IV&V reduces development rework, thereby reducing total program and project costs, for a positive return on investment.
- **Increased Knowledge Transfer** – Improves communication across project teams and cross-project transfer of system and software engineering best practices.
- **Reduces Cyber Events –** Provides security confidence and risk knowledge/management of cyber security risks.

IV&V is an industry-proven approach to increase quality, reduce risk, gain development insight, reduce cost, and transfer knowledge

IVVO Metrics Overview

- NASA IV&V captures and tracks metrics at various levels of abstraction; however, the following four metrics are viewed as top level leading indicators of IV&V effectiveness:

Early Lifecycle Engagement… by getting involved early in the SW development lifecycle

14 of 14 active IV&V projects started before mission SRR.

Phase Alignment… by detecting defects in-phase with SW development

Overall phase containment by active projects: **98%** over the past year.

Issue Acceptance… by detecting and submitting quality defects to the development teams

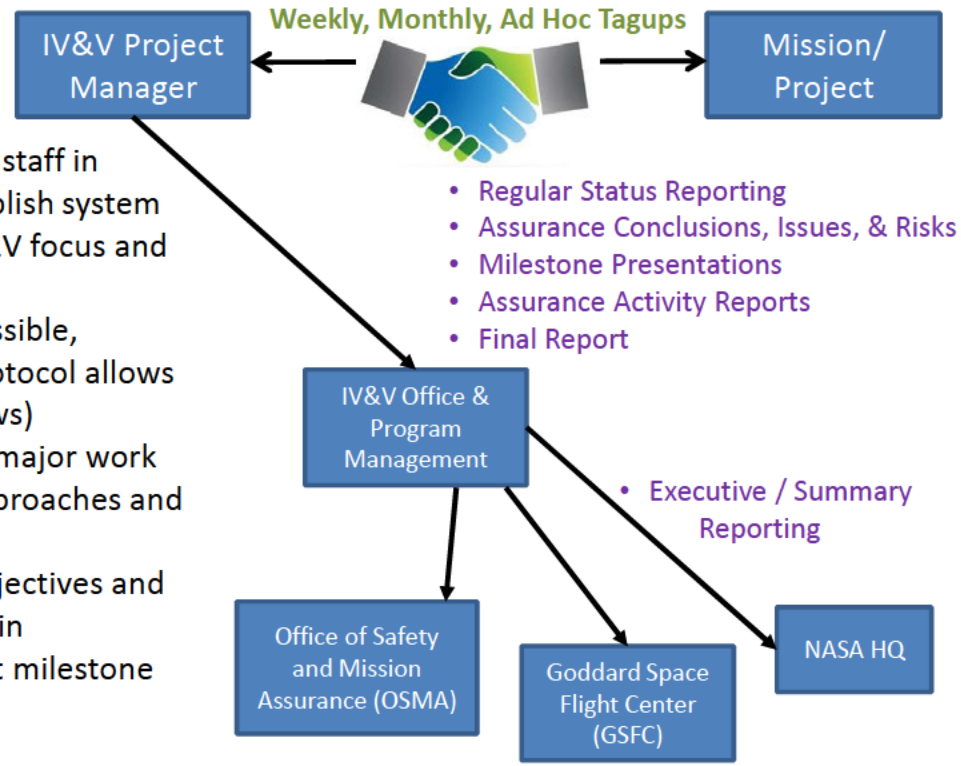
Overall issue acceptance for active projects was **97%** over the past year.

Customer Satisfaction… 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.

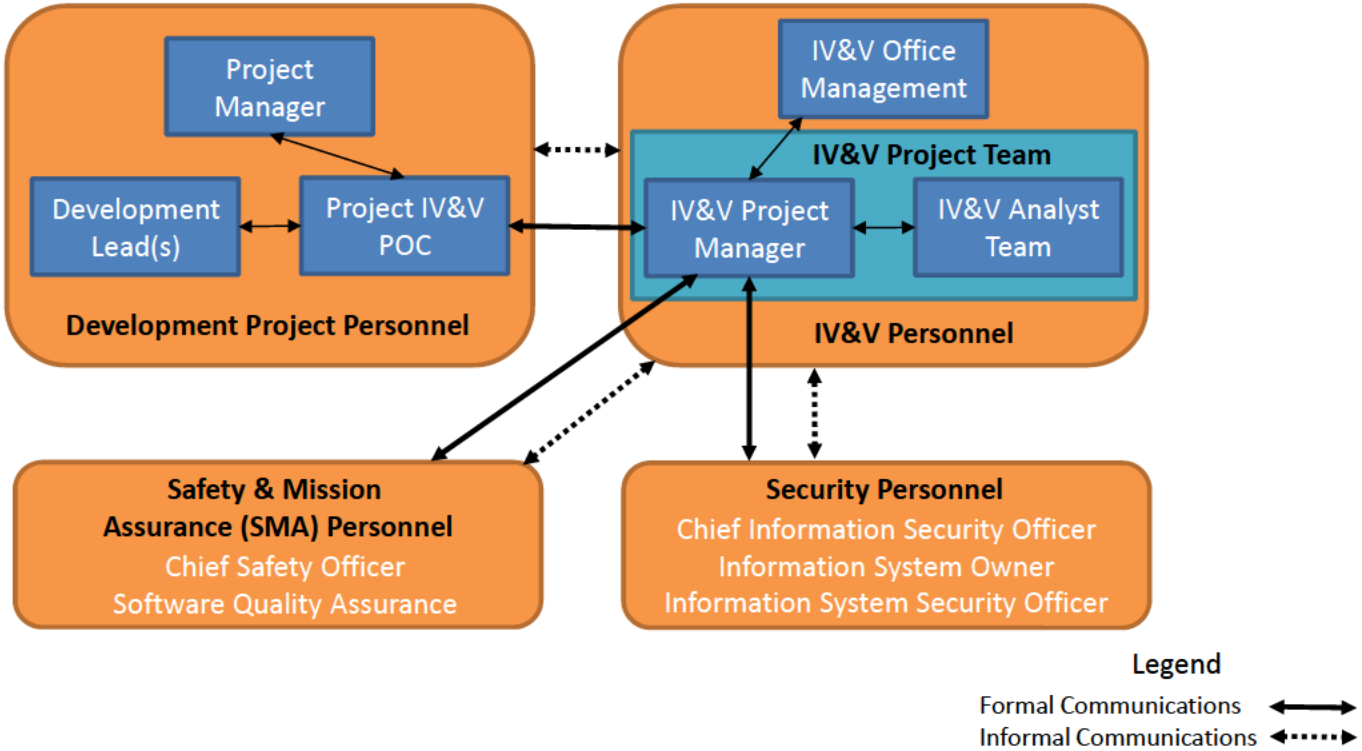
Communication & Reporting

- "No Surprises" Policy!
- IV&V personnel interact with Project staff in various development forums to establish system understanding and communicate IV&V focus and status
- Communicate findings as soon as possible, directly to the developer if policy/protocol allows (e.g. during development peer reviews)
- 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



IV&V provides actionable data to customers and stakeholders, both internal and external to the Project, that drives changes to system and software projects and informs key decision makers throughout the lifecycle

IV&V Project Interfaces: NASA Project Example I/Fs



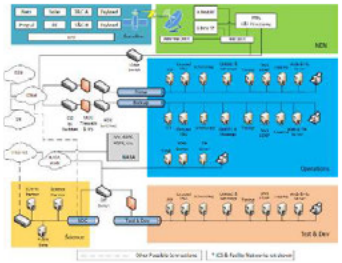
Within NASA Projects, the project level interfaces are tailored to optimize the information flow between key stakeholders throughout the development project

Mission Protection Services

- Mission Protection Services (MPS)
  - Multidisciplinary approach
  - Independent assessment of mission security risk
  - Focus on system and operational security risk factors
  - Informed by available threat intelligence

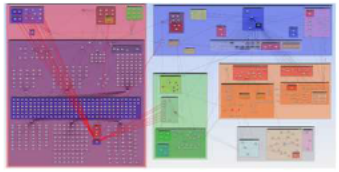
MPS Perspectives

Integrated end-to-end mission system	Mission system development and operations	Cybersecurity implementation assessment
(MPS-I)	*(MPS-L)*	*(CAT/BT-VAP)*



Combined perspectives provides optimal coverage

Targeted investigation of mission security risk across
- End-to-end mission system architecture
- Mission system development and operational lifecycles



SSO S&MA Services

Office of Safety and Mission Assurance

- Support for the Software Assurance Tech Fellow initiatives
  - Policy – updates to Software Assurance, Software Safety, and Formal Inspection Standards
  - Guidance – updates to SW Assurance Handbook and Guidebook
  - Training – development of cybersecurity training for software assurance practitioners and updates to IV&V training
  - Center Service Requests – range of services per request, including static code analysis, metrics and task management tools, and audit response.
- Software Assurance Research Program Management

Project Funded Services

- Commercial Crew Program
  - Software Quality Assurance, including equivalency of alternate standards, process mapping to standards, and process compliance auditing, evidence, and risk assessment.
  - Software Safety and Hazard Analysis, involving engineering analysis of requirements and design for protections against hazards, and verification evidence for hazard controls to support design certification.
- Wallops Flight Facility
  - Software Assurance, Software Safety, and V&V engineering analysis for range upgrade projects, including range and launch monitoring capabilities and ground- and flight-based safety destruct capabilities.
  - Additional project support services, such as risk assessment, modeling of system dependencies, and process assessment.

SSO Mission Protection Services Approach

MPS Integration Analysis
- Identification of mission dependencies on component systems
- End-to-end mission system data flow assessment
- Risk-driven mission security investigation
- Roll-up of mission security risk posture

MPS Threat and Vulnerability Research

MPS Lifecycle Support
- Analytical support for mission development projects
- Coverage of engineering and security artifacts
- In-phase feedback to engineering team
- Input to development milestone reviews
- Worked in conjunction with IV&V support

MPS Cybersecurity Assessment Team (CAT)
- Vulnerability Assessment of implemented mission systems and system security processes
- Mission-risk-focused penetration testing
- Identifies vulnerabilities, weaknesses and disconnects with system specifications and security and operations plans

OCIO Assessment and Authorization – FISMA Compliance & Authorization to Operate

SSO Metrics Overview

- The IV&V Program's SSO provides a range of different types of focused support per customer needs, as opposed to the full development life-cycle support provided by the IVVO. Therefore, SSO does not actively capture metrics to measure "getting involved early" or "phase containment." SSO continuously monitors the quality of their findings and customer satisfaction.

Issue Acceptance... by detecting and submitting quality issues to our customers

Cumulatively, SSO has achieved **95%** Issue Acceptance over the past year.

Customer Satisfaction... by ensuring our customers are satisfied with our products and services

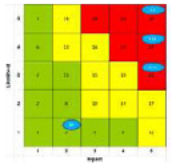
Cumulatively, the SSO Customer Satisfaction rating was **98**% over the past year.

NASA IV&V ITC Overview

- The NASA Independent Test Capability (ITC) resides within the Jon McBride Software Testing and Research (JSTAR) Lab and was established to develop software-only spacecraft simulation environments for NASA IV&V-supported missions
  - NASA Simulation Warehouse: Actively developing and maintaining environments across the Agency including Human Exploration, Science Missions (JPL, GSFC), and Small Satellite Missions
  - Develops and maintains an open-source small satellite simulator (NOS^3). www.nos3.org (*runner-up for 2019 NASA SW of the Year*)
  - Auto-provisioning of complete software simulation environments
  - Custom Software Tools to Simplify Usage, Analysis and Testing
    - Memory Dumps, Fault Scenarios, etc.
- ITC provides software integration services for multiple NASA projects
- ITC works closely with the Mission Protection Services (MPS) team to provide a simulation environment to support advanced cyber security testing (CyberSim)

IV&V Assurance Strategy: Implementation Process and *Example*

1. Risk-Prioritize System Capabilities and Software for Assurance using PBRA/RBA and IVV S3106, and Develop High-Level Assurance Objectives (AOs)



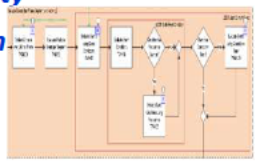
Capability: *Entry, Descent, and Landing (EDL)*
Entity: *Orion Timeline Vehicle Manager (TVM)*
Objective: ***Assure TVM correctly evaluates and detects critical events, to mitigate risk of inappropriate or missed event detection***

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 (Technical Framework)

Plan: ***Selected methods M-2, M-3, M-6, M-36, M103 to cover correctness and completeness, emergent behaviors, hazards and dependability***

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.***



IV&V Technical Reference

Condition	Equivalent
|x| < y	(x < y) AND NOT (x <= -y)

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.***

Incorrect Code in Critical Software Method

```
584: case TVM_Mission::LESS_THAN:
585:   if ( x <= -y ) {LclRet = false;}
586->: if ( x < y ) {LclRet = true;}
587:  break;
```

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.***

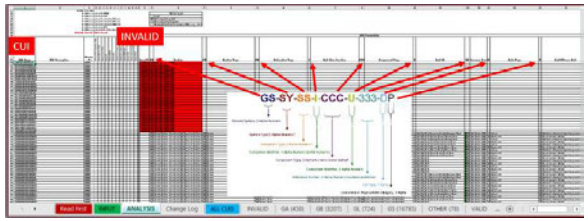
IV&V Assurance Strategy: Follow the Risk *Example*

IV&V Assurance Strategy evolves as system understanding grows, resulting in new concerns/risks, new areas of focus, and specialized analysis activities.

1. **Reevaluate Risk/Priorities**: IV&V lifecycle analysis activities include validation of Compact Unique Identifiers (CUIs), which are unique identifiers used for commanding between and within Exploration Ground Systems (EGS), the Space Launch System (SLS), and the Orion crew capsule, and monitoring telemetry data within and across these systems. IV&V observed a trend in invalid CUIs throughout system and subsystem artifacts in all three programs.

2. **Risk**: Incorrectly defined CUIs could lead to unintended commanding or inappropriate use of critical Human Exploration and Operations (HEO) system data; Either outcome could result in hazardous conditions, catastrophic failure, and/or loss of mission/vehicle/life.

3. **Learn and Understand**: IV&V studied the three programs' CUI Specifications, which define the naming conventions that must be followed in the establishment of CUIs for command and measurement parameters, and then developed a custom tool to aid in the analysis of hundreds of thousands of CUIs.



4. **Execute Planned Analysis**: IV&V executed the tool against ~85,000 EGS CUIs, ~30,000 SLS CUIs, and ~90,000 Orion CUIs.

5. **Confirm Potential Issues**: The tool identified over 77,000 CUIs that did not meet the Specification.

6. **Evaluate Issue Significance and Document Issues**: This was a systemic issue affecting all three Programs & their many subsystems. Although the software may have executed properly using the invalid CUIs, these unspecified CUIs could have led to unintended commanding or inappropriate use of critical system data, with devastating consequences.

7. **Communicate Issue and Track to Resolution**: The Issue was communicated to the CUI Specification product owners to be resolved at the Program Level. The Program updated the CUI Specs to include unspecified CUI fields and definitions, and revised the CUI management processes to ensure new CUIs are compliant. These changes resolved IV&V's concerns.

In order to achieve mission success, it is critical that operations personnel communicate using common nomenclature that unambiguously and uniquely defines all hardware/software items that may be monitored or commanded. This IV&V analysis has greatly increased the confidence that these systems will operate as an integrated mission.

19

IV&V Independent Testing: Increasing Confidence in SLS Critical Events *Example*

Driving Principles:

- Successful execution of a robust IV&V approach necessitates the use of both static and dynamic analysis techniques.
- IV&V focuses dynamic analyses and independent testing on complex functionality that can not be adequately evaluated in a static environment.
- IV&V focuses dynamic analyses and independent testing on complex functionality to add assurance and mitigate risk to the FSW.
- In some cases specific low level risks requiring mitigation may not be identified until during the execution of IV&V – in these instances IV&V approaches will be tailored and plans will be adjusted to allow mitigation of newly identified risks.

Example (SLS – Space Launch System):

- IV&V identified a risk: ability of the SLS FSW to detect and report internal errors.
- Due to the complex and dynamic nature of error reporting IV&V asserted that static analysis alone would not adequately verify the fully implemented capability.
- IV&V utilized the IV&V developed S3 tool to conduct independent testing
- Upon verification of 482 errors out of 852 possible error conditions, IV&V concluded that the associated SLS FSW functionality was behaving as intended and not introducing any adverse or unexpected behaviors
- IV&V testing augmented the developer's FSW testing which cannot easily trigger low-level types of errors in the test environment using the actual flight computer hardware

IV&V performed independent testing of critical communication and reporting capabilities, increasing confidence that FSW will behave as desired in the event of errors

Overarching Lessons Learned

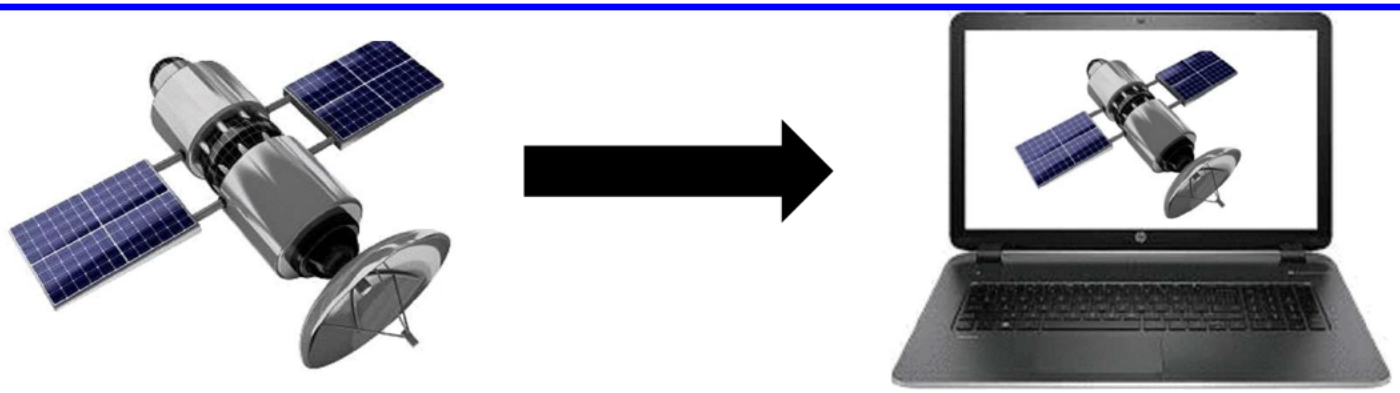
- Independence is fundamental (all three aspects): Financial, Managerial, Technical
- Policy must be established to define and institute IV&V requirements
- Be a partner with the project and focus on Mission Success
- In-phase issue detection and low false positive rates are critical to maintaining customer satisfaction
- Tailor communication channels, frequency, and content based on Project need
- Anchor IV&V Process in industry standards and best practices
- Full life-cycle IV&V is most effective
- Be adaptive: Risk is dynamic
- Emphasize, promote, and embrace a learning organization culture

Lessons Learned capture, management, and dissemination has been a foundational component of the IV&V Programs evolution over the past 25 years!

IV&V's Goal is Mission Success

Backup

Software-only Simulation



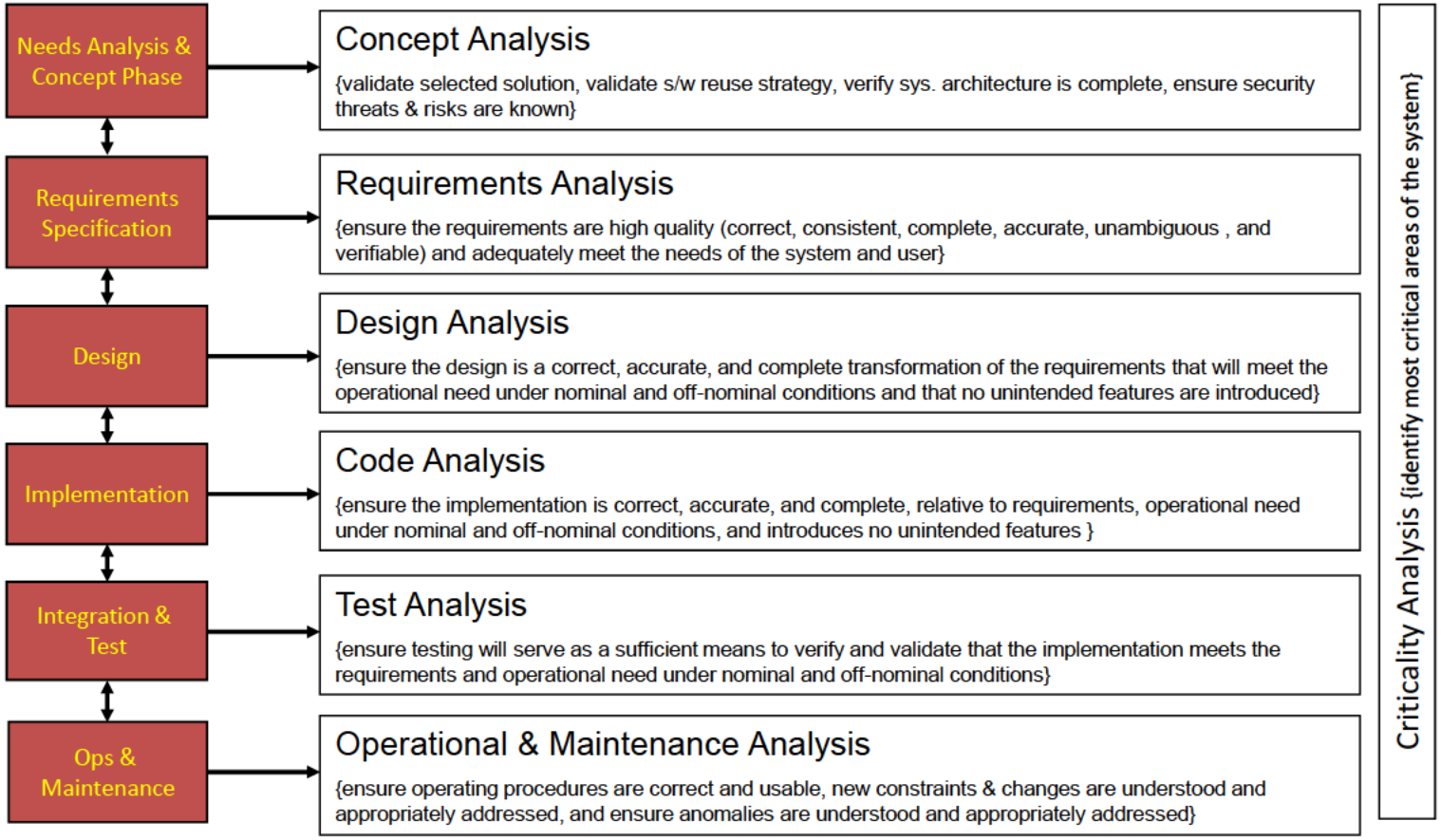
- Condense Entire Flight "System" to a Laptop
  - Sensors/Actuators are Simulated
  - Flight Computer Hardware is Emulated to create Virtual Platform
  - Flight Software binaries executed as delivered.
  - Ground Operations Integrated.
- "Software-only Flatsat"

Agency Directives & Requirements Relevant to IV&V Program and Project Selection

- NPD 7120.4E, *NASA Engineering and Program/Project Management Policy* (Section 1, 5, C):
  - It is NASA policy to use the NASA Independent Verification and Validation (IV&V) Program as the provider of IV&V services. The criteria used to determine which NASA projects are required to have IV&V are defined in NPR 7150.2.

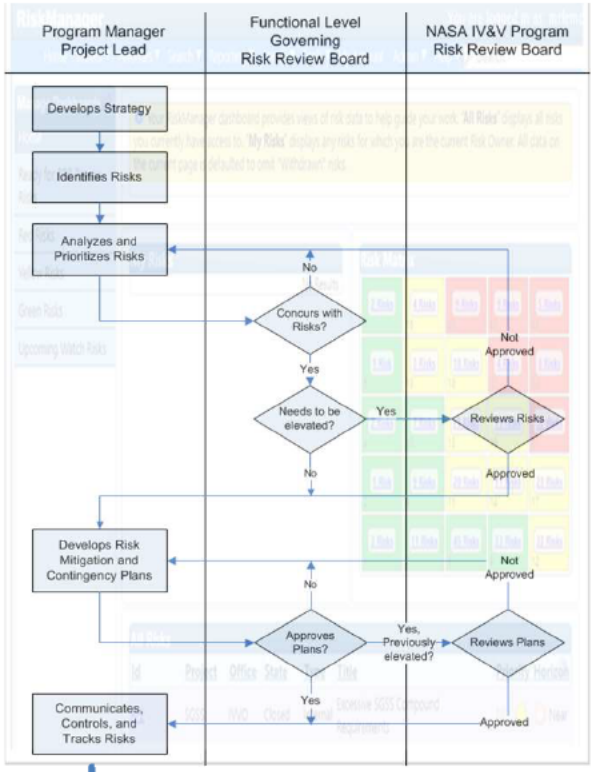
- NPR 7150.2C, *NASA Software Engineering Requirements* (Chapter 3.6):
  - The program manager shall ensure that software IV&V is performed on the following categories of projects:
    a. Category 1 projects as defined in NPR 7120.5.
    b. Category 2 projects as defined in NPR 7120.5 that have Class A or Class B payload risk classification per NPR 8705.4.
    c. Projects specifically selected by the NASA CSMA to have software IV&V.

IV&V Tech Framework Abstraction

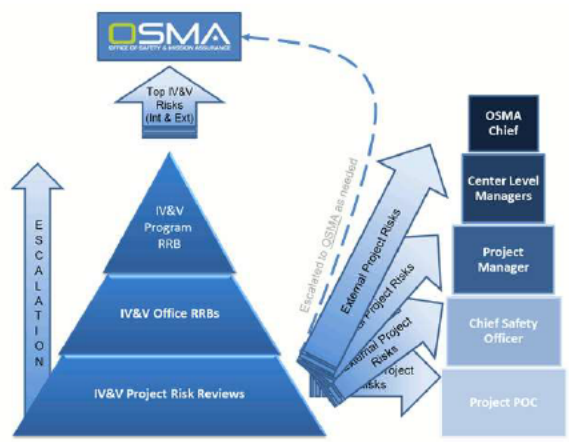


IV&V Risk Management

IV&V Risk Management Process



- Aside from Assurance Statements and Issue (TIMs) development and resolution, IV&V identifies external risks (risks to the development effort) and communicates those risks to the development POCs
- IV&V RM best practices for external risks:
  - Utilize Development Project scoring criteria
  - Encourage adoption of risks into developer's formal risk management process
  - Monitor to closure even if developer's have closed or placed risk in watching state
  - Communicate residual risk at milestones for still active external risks



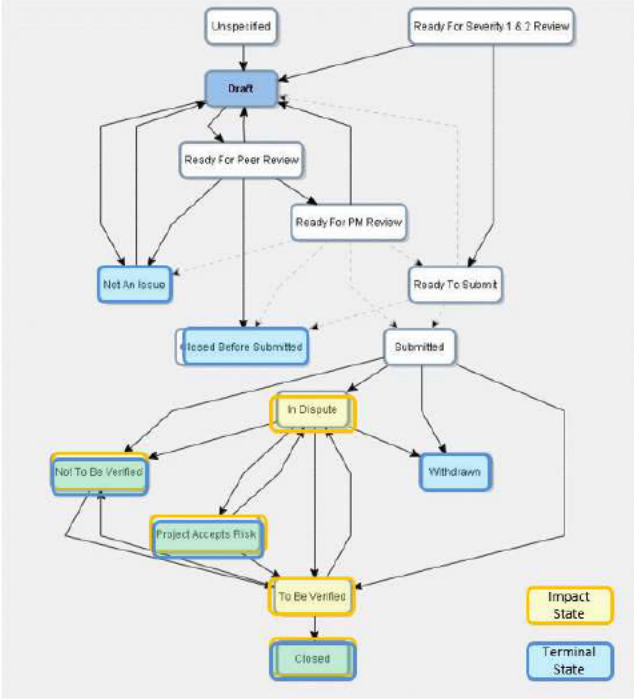
IV&V Risk Reporting Best Practice-Escalation Protocol

IV&V's RM process provides additional identification/mitigation of SW dev risks

IV&V TIM (Issue) Process

- Issues are deficiencies (defects) identified through analysis of artifacts
- Issues are documented in Technical Issue Memorandums (TIM)
  - TIMs are one of the primary communications tools used to share issues with the development projects
  - TIMs are used to communicate the work being performed across the program and the value of IV&V
- Critical required fields include:
  - Subject
  - Description
  - References
  - Impact
  - Severity
  - Phase Introduced/Found
  - Recommended Actions
  - Comments/Resolution Chronology

IV&V TIM State Machine (Tool enforced)



IV&V's TIM process has been refined through the interactions with multiple project and development stakeholders to ensure defects are communicated properly and the impacts of those defects are well known

IV&V TIM Severity Summary

Severity	Capability Affected	Success Criteria	Safety	Test	Cost/Schedule	Other
1-Catastrophic	Loss of essential capability or complete loss of mission critical asset	Inability to achieve minimum mission success criteria	Causes loss of life or injury	N/A	N/A	N/A
2-Critical	Degradation of an essential capability or Damage/destruction to mission asset which affects performance	Impact to the accomplishment of a mission objective	N/A	Essential capability not tested	Significant cost increases or schedule slip resulting from immediate or downstream development impacts	Significant reduction to requirements margins or design margins
3-Moderate	Degradation of system dependability or Loss of a non-essential capability	Impact to the accomplishment of extended/optional mission objectives	N/A	Essential capability inadequately tested	Moderate cost or schedule impact resulting from redesign, reimplementation, and/or retest	Degradation of an essential capability or inability to accomplish mission objective, but with a known workaround
4-Minor	Degradation of a non-essential capability	N/A	N/A	Non-essential capability inadequately tested	Defect impacting maintainability on current mission or reuse on future missions	Creates inconvenience for operators, crew or other projects' personnel
5-Editorial	Defect impacting documentation and communication clarity and poses no risk to the Mission Project					