Adaptive IV&V for Increasingly Complex Software Systems

NASA's Independent Verification and Validation (IV&V) Program
Fairmont, West Virginia
Wes Deadrick, IV&V Program Director

www.nasa.gov/centers/ivv

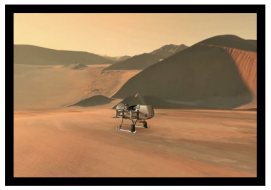
- **Established in 1993, driven by recommendation after Space Shuttle Challenger accident.**
- Based at the **Katherine Johnson IV&V Facility** in Fairmont, WV.
- Is the IV&V services provider for NASA and applied to the Agency's highest-profile missions
- Is risk driven.
- Employs rigorous analysis and testing methodologies throughout the Software Development Life Cycle (SDLC) to assure safety and mission critical systems and software will operate reliably, safely and securely.
- Strives to reduce the highest safety and mission software risks, inform decision makers, and provide confidence based on objective evidence.

Which NASA projects receive IV&V?

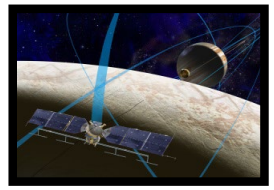
- NASA established IV&V as a requirement in NPR 7150.2, *NASA Software Engineering Requirements.* Per NPR 7150.2, IV&V is required on the following:
  - a. Category 1 projects as defined in NPR 7120.5.
  - b. Category 2 projects as defined in NPR 7120.5 that have Class A or Class B payload risk classification per NPR 8705.4.
  - c. Projects selected explicitly by the NASA Chief, Office of Safety and Mission Assurance to have software IV&V.

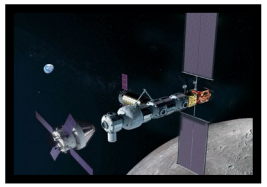
The result: IV&V is applied to projects that are human-rated, have lifecycle costs of several hundred million dollars or more, or have high priority and complexity.

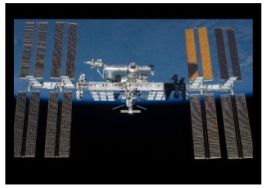
Artemis


Dragonfly


EGS


Europa


Gateway

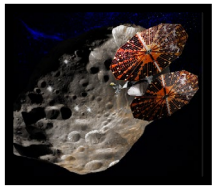

ISS

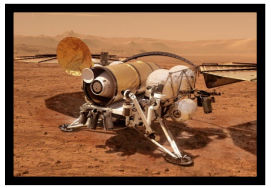

JPSS2


HLS

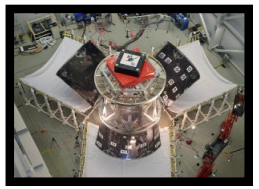

JWST


Landsat 9

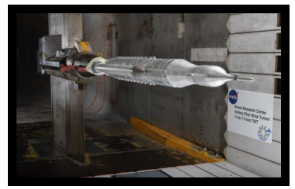

Lucy

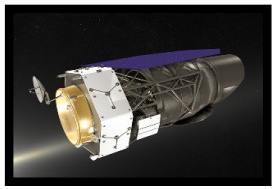

MSR


MCC


Orion


Psyche


SLS


Roman

The Growing Complexity NASA IV&V Faces

Increased reliance on data driven algorithms for mission critical software behavior

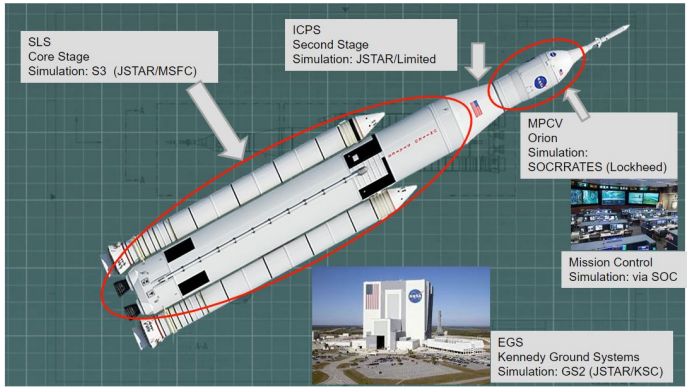
Overview: Data driven software has become more common, bringing with it new approaches to documentation and development for data content that differ from executable code. There also seems to be a growing tendency for systems to express complex software behaviors through data instead of code.

- Challenges:
  - Data is dynamic, less readable than code
  - Flight-like end-to-end system testing may be deemphasized
  - Further, segmentation of 'data' as the domain of Systems Engineering (while code is the domain of Software Engineering) introduces risk

System of Systems Integration Verification and Validation

Overview: NASA's Human Rated missions incorporate multiple complex and large systems, and the degree of risk relating to the interfaces and integrated behaviors is high

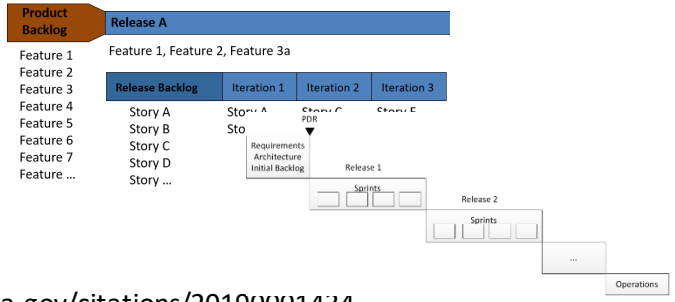
Challenges:
- Large complex systems
- Multiple developers and stakeholders
- Various domains



New and Emerging SW Development Lifecycle Models

Overview: Across the IV&V portfolio, development efforts follow many different processes. Agile development processes have been around the IV&V Program for multiple years at this point, but each tend to have various nuances in their approach (SAFE, Scrum, etc). New processes also continue to emerge, which require NASA IV&V to learn and adapt.

Challenges:
- Each development effort applies varying processes that produce different artifacts at different points along the timeline

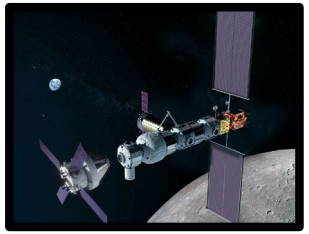


https://ntrs.nasa.gov/citations/20190001434

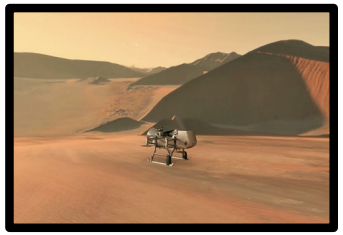
New technologies on the horizon: MBSE/MBMA, Machine Learning, AI

Overview: Engineering practices like true autonomy, MBSE and Machine Learning are right on the horizon for NASA IV&V practioners. How to verify the correct operations of such systems is an evolving area of research and the state-of-the-practice is still unclear. How IV&V analysis should be performed, from how to identify the existence of risk to what tools and techniques are needed, are currently in work

Challenges:
- Hard to prepare for V&V of True Autonomy
- Mixed approaches to MBSE

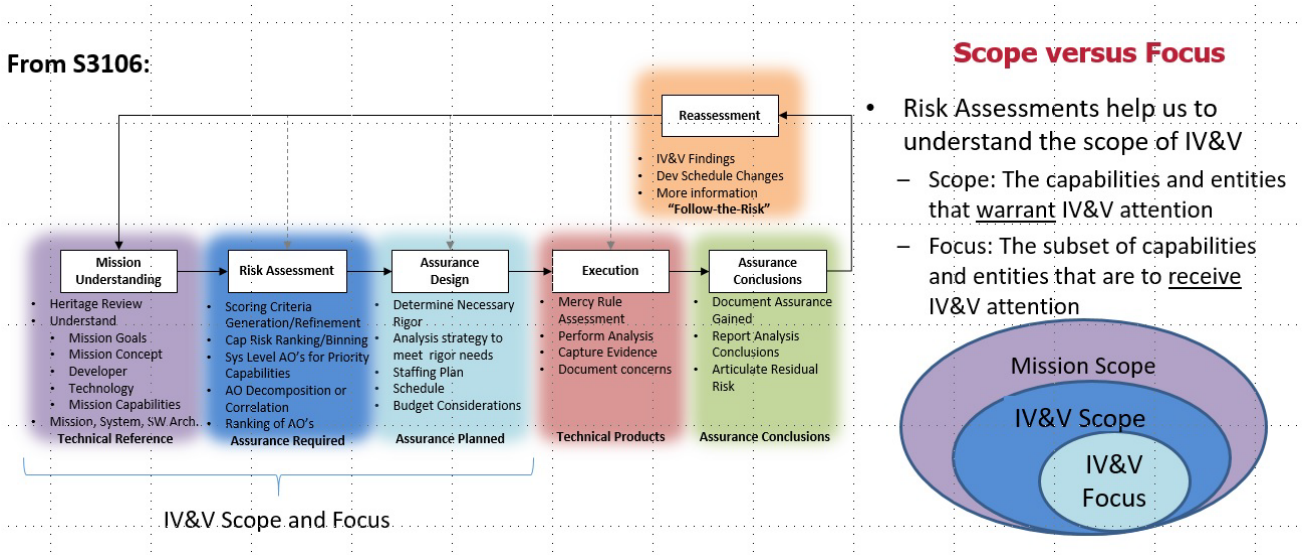


Gateway



Dragonfly

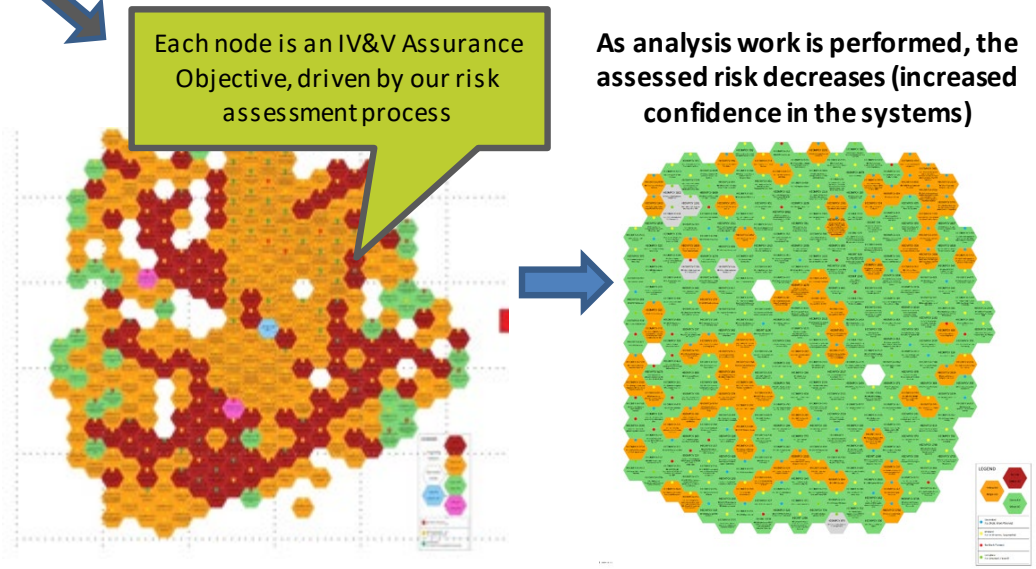
Why Adaptive IV&V is Necessary



Scope versus Focus

- Risk Assessments help us to understand the scope of IV&V
  - Scope: The capabilities and entities that warrant IV&V attention
  - Focus: The subset of capabilities and entities that are to receive IV&V attention

- Following the risk, is where the IV&V perception of risk adapts and grows over time to match the observed risk and allows the focus of the IV&V team's effort to shift to areas of highest concern
- The evolution of risks are monitored and adjusted throughout the execution of the IV&V Project

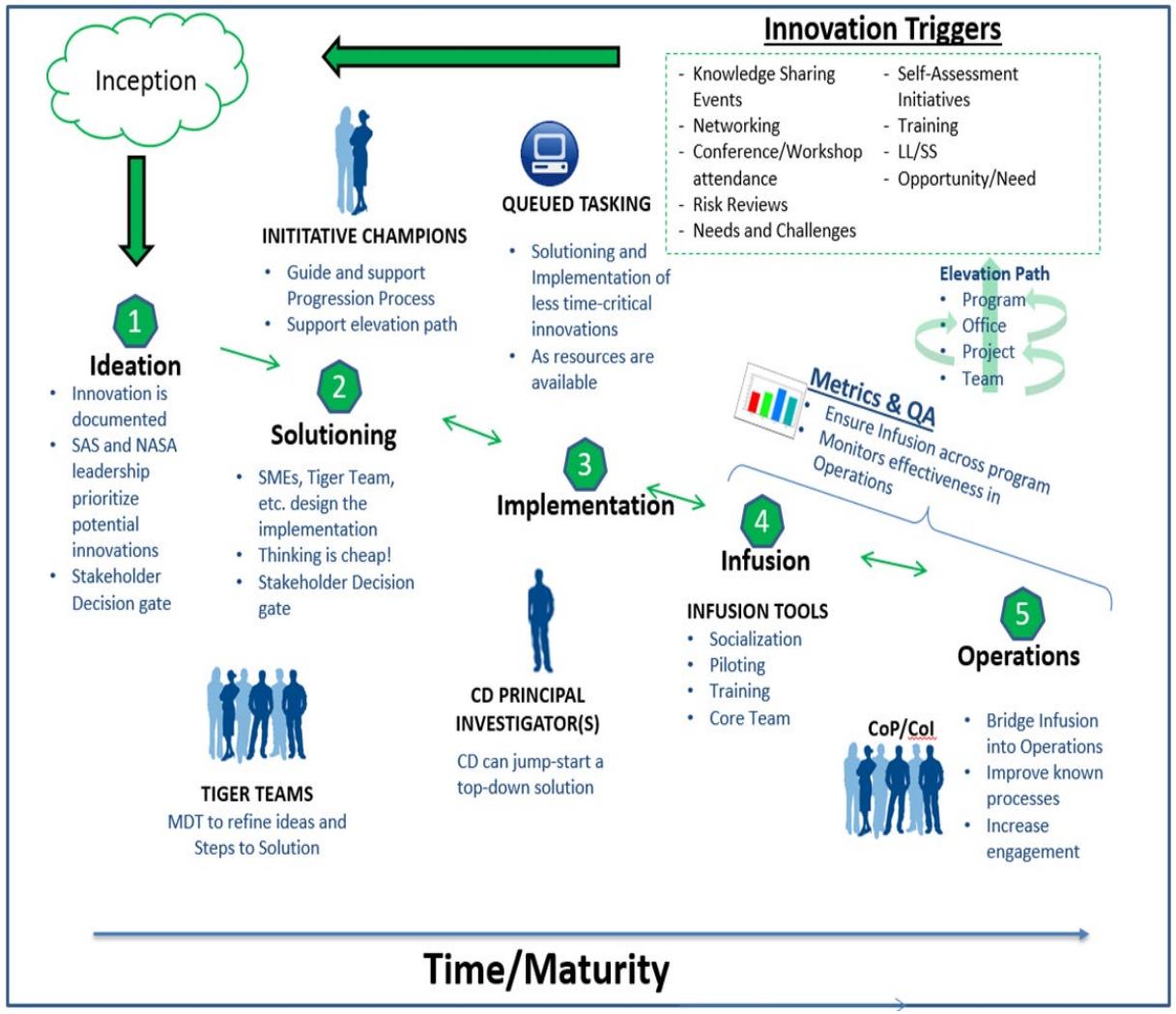


- IV&V collaboration with the Software Engineering Institute at Carnegie Mellon University
- Helped IV&V adopt Agile and Lean concepts that integrated logically with some of the ways we were trying to perform analysis and resulted in the following paper:
  - Agile approach to assuring the safety-critical embedded software for NASA's Orion spacecraft

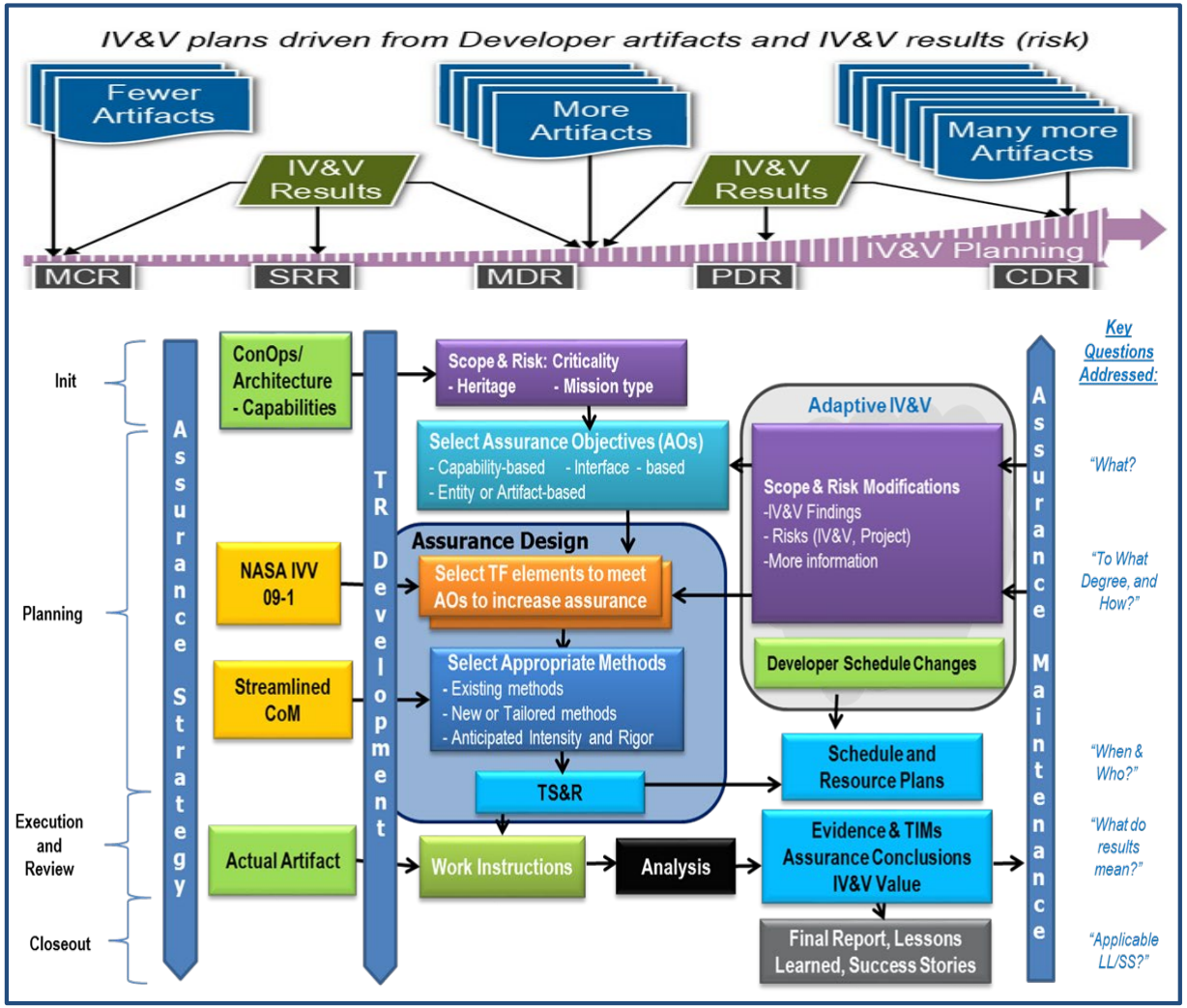
Risk is dynamic, IV&V's Risk Process adheres to the core IV&V principles, but utilizes adaptive measures to continuously update in response to changing risk

How the NASA IV&V Program adapts

Continuous Innovation



Continuous Evaluation



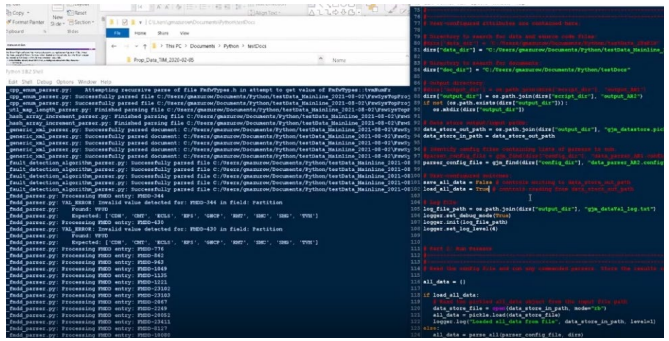
The two engines that power adaptation are innovation of new ideas and evaluation of effectiveness and risk posture.

IV&V Approaches to the Challenges

Increased reliance on data driven algorithms for safety and mission critical software behavior

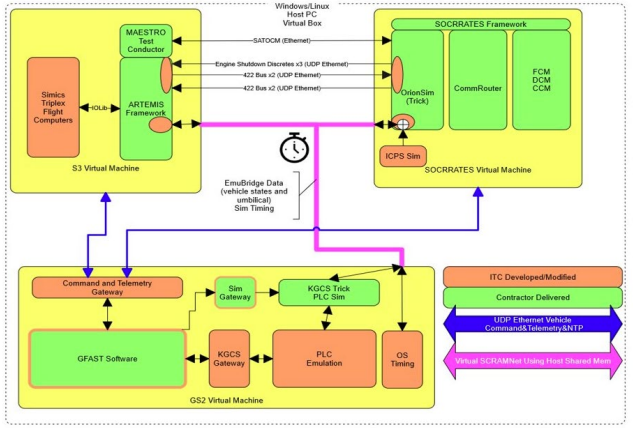
- Increase coverage and effectiveness of how we perform IV&V on data-driven systems
- Update/create our technical framework and methods to have more formal application
- Better understand the boundaries between software and data

- Tool development to aid our new approaches
  - One solution developed: a set of Python modules broken into 'parser' operations (which read and process data) and 'constraint' operations (to enforce constraints on data



System of Systems Integration Verification and Validation

- ARRISTOTLE was developed to facilitate risk-reduction testing of all phases for the Artemis return to the moon programs.
- Capabilities
  - Test as you fly
  - Fault injection across interfaces
  - Detailed post-processing log analysis tools
  - Ability to pause time and analyze states
  - Flight binaries



New and Emerging SW Development Lifecycle Models

- Agile IV&V for Agile development
  - Adoption of "Follow the Risk IV&V"
- The emergence of Analysis Threads to the IVV 09-1 Technical Framework application
  - Types of Threads
    - Correct and Complete
    - Traceability
    - Emergent Behavior
- Adaptive Assurance Design

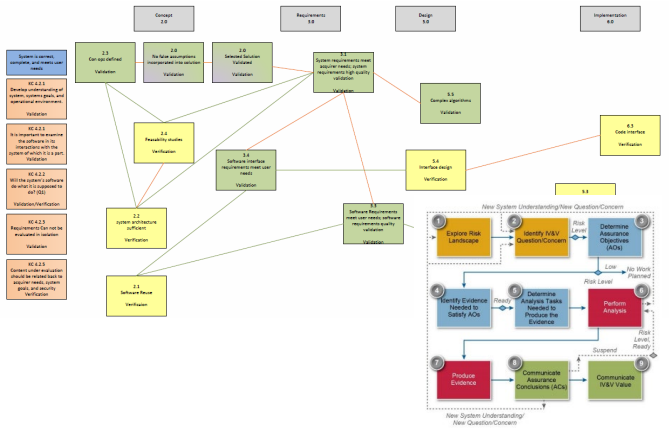


Figure 1: Follow-the-risk diagram

https://ntrs.nasa.gov/citations/20190001434

New technologies on the horizon: MBSE/MBMA, Machine Learning, AI

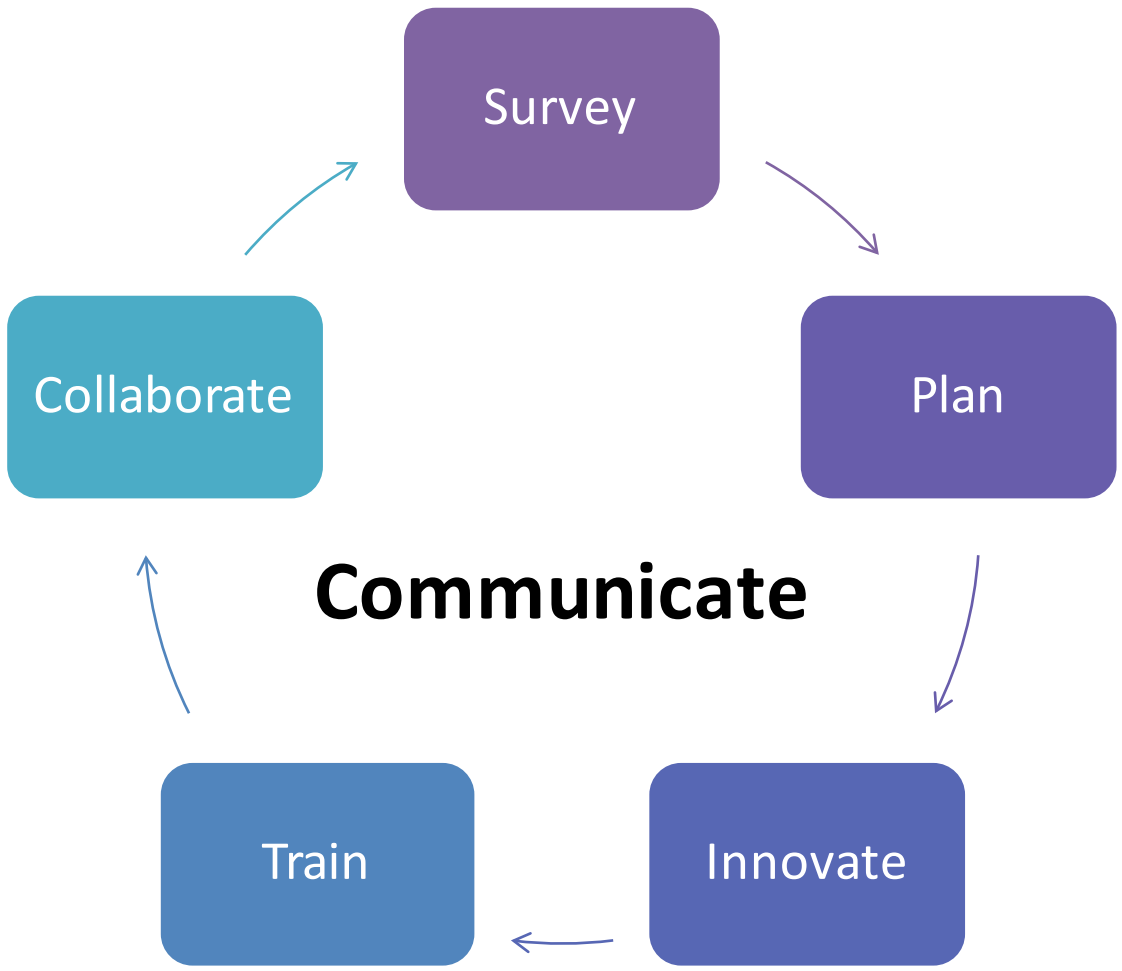
- Augmenting ATS Requirement Analysis Tool with Artificial Intelligence
  - Help prioritize analysis with application of AI machine learning
  - Results of the machine learning research can be integrated into the IV&V developed Analysis Tool Set (ATS)

- Capability Development efforts for developing approaches and tools required to assure safety-critical autonomous software systems

- JSTAR independent testing application of Machine Learning for Test Coverage

SBC Tasks / Main / Configuration / Utility Code Files

Acronym	Name	File	Line Coverage		Function Coverage	
SBS	Beam Steering Control	sbs.c	72.0 %	949 / 1318	84.3 %	70 / 83
SDI	Diagnostic	sdi.c	83.0 %	1343 / 1618	80.5 %	66 / 82
SIM	Instrument Manager	sim.c	66.3 %	555 / 837	79.3 %	23 / 29
SLA	Laser Control	sla.c	88.7 %	375 / 423	100.0 %	33 / 33
SMT	Main Computer Electronics Housekeeping and Telemetry	smt.c	76.2 %	214 / 281	66.7 %	14 / 21
SRT	Remote Terminal	srt.c	88.4 %	289 / 327	100.0 %	30 / 30
STH	Thermal Control	sth.c	85.6 %	664 / 776	97.4 %	38 / 39
SXP	Extrapolator	sxp.c	35.9 %	417 / 1161	60.6 %	20 / 33
SFM	File Manager	fm.c (common)	60.4%	462 / 765	76.9%	40 / 52
SHS	Health and Safety	hs.c (common)	84.7%	687 / 811	92.5%	49 / 53

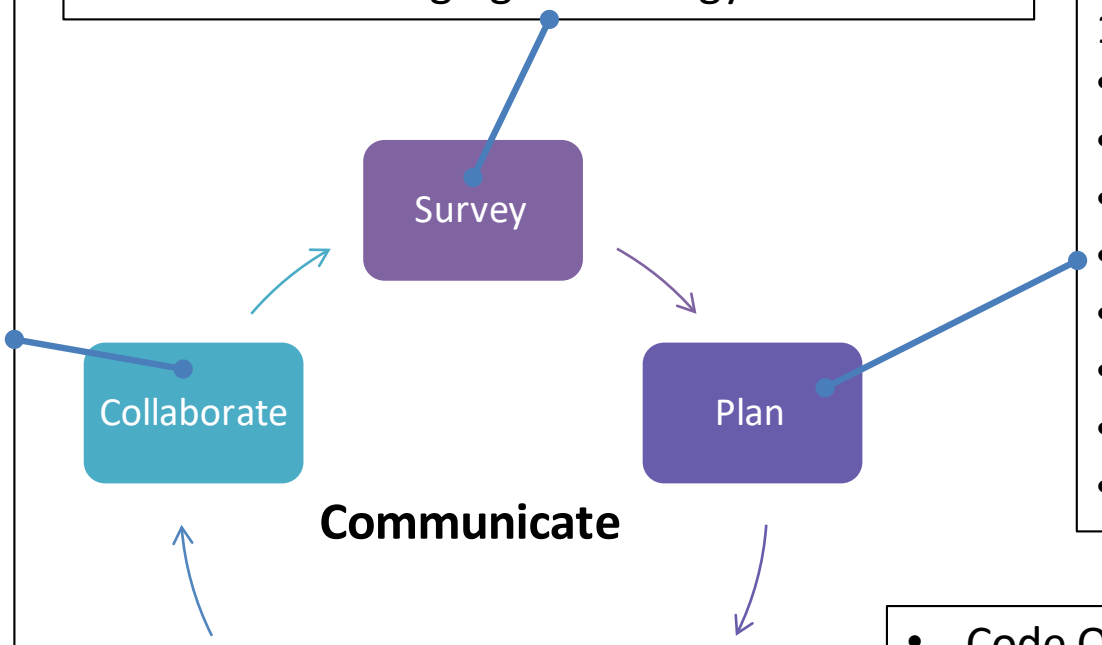


- Survey both the IV&V workforce and the state of the practice to identify trends and inform vision for IV&V
- Develop and maintain a strategic roadmap to achieve vision by mapping goals to a 1-3-5 plan
- Charter initiatives to achieve goals through innovation
- Prepare workforce for analysis of new and evolving technologies
- Collaborate with external communities to inform and validate our vision and achieve our goals
- Communicate at every stage and at every level to ensure commitment and support

Handling Evolution of Mission Systems: Current Approaches

- Technology and Strategic Roadmap Initiative
- New and Emerging Technology Studies

- Weekly Workshops
- Small communities of practice within the IV&V Program (e.g. SCAWG)
- NASA Engineering Network
- SARP
- MDA
- Interagency Science and Technology Partnership Forum (Trusted Autonomy)
- International IV&V Working Group
- IV&V Project Checkpoint Reviews



1-3-5 outlook:
- CBA/FTR/Agile IV&V
- Dynamic Analysis
- Integrated Analysis Toolset
- Automated SCA
- Late Lifecycle IV&V
- Team Readiness
- Deep Data Learning
- Formal Method Utilization

- IV&V Team Readiness Initiative
- Weekly Technical Discussions
- IV&V Boot Camp

- Code Quality Risk Assessments
- Data Analytics for Assessing System Risks
- Exploration of Techniques for Evaluating Binary Code
- Application of AI and ML to Requirements Analysis


NASA
NASA