IV&V Program

ARTEMIS IV&V

Adaptive Independent Verification and Validation (IV&V) Reduces Risk of Software Impacting Safety in Artemis Missions

Gerek Whitman

Ryan Starn

SAIC

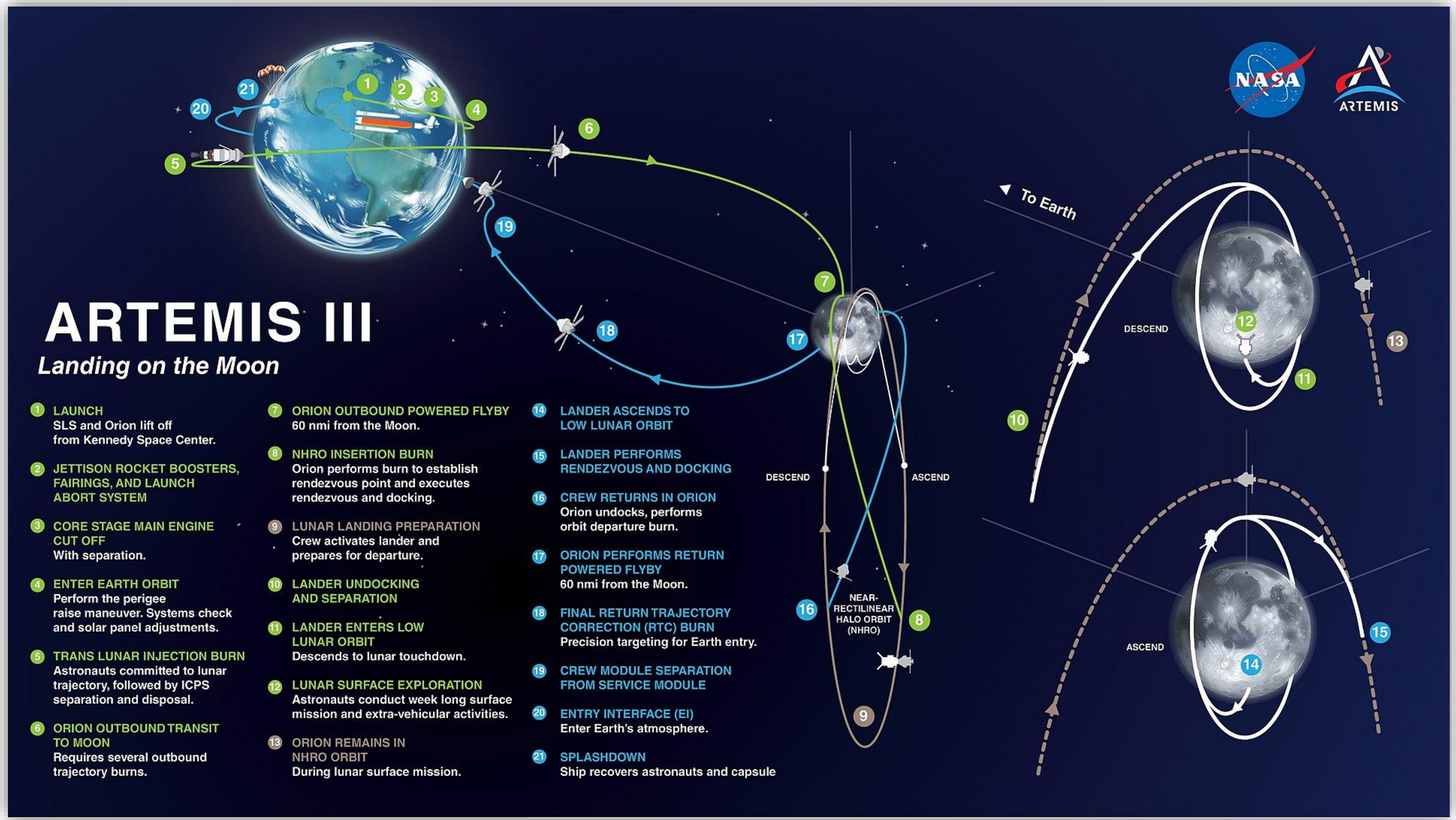
NASA’s IV&V Program

IV&V Program

- NASA’s Independent Verification & Validation (IV&V) Program reports to the Office of Safety and Mission Assurance (OSMA)
  - Technically, Managerially, and Financially Independent
- Located in Fairmont, West Virginia
- NASA IV&V employs systems engineering processes and rigorous methodologies for evaluating the correctness and quality of software products on NASA’s highest profile missions
  - Full Lifecycle
  - Mission Oriented
  - Capability Based
  - In Phase
  - Product Focused
  - Risk Driven
- NASA IV&V goal: Add evidence-based assurance that minimizes the overall risk of NASA mission software

NASA's Artemis Program

IV&V Program



ARTEMIS III

Landing on the Moon

1. LAUNCH
SLS and Orion lift off from Kennedy Space Center.

2. JETTISON ROCKET BOOSTERS, FAIRINGS, AND LAUNCH ABORT SYSTEM

3. CORE STAGE MAIN ENGINE CUT OFF
With separation.

4. ENTER EARTH ORBIT
Perform the perigee raise maneuver. Systems check and solar panel adjustments.

5. TRANS LUNAR INJECTION BURN
Astronauts committed to lunar trajectory, followed by ICPS separation and disposal.

6. ORION OUTBOUND TRANSIT TO MOON
Requires several outbound trajectory burns.

7. ORION OUTBOUND POWERED FLYBY
60 nmi from the Moon.

8. NHRO INSERTION BURN
Orion performs burn to establish rendezvous point and executes rendezvous and docking.

9. LUNAR LANDING PREPARATION
Crew activates lander and prepares for departure.

10. LANDER UNDOCKING AND SEPARATION

11. LANDER ENTERS LOW LUNAR ORBIT
Descends to lunar touchdown.

12. LUNAR SURFACE EXPLORATION
Astronauts conduct week long surface mission and extra-vehicular activities.

13. ORION REMAINS IN NHRO ORBIT
During lunar surface mission.

14. LANDER ASCENDS TO LOW LUNAR ORBIT

15. LANDER PERFORMS RENDEZVOUS AND DOCKING

16. CREW RETURNS IN ORION
Orion undocks, performs orbit departure burn.

17. ORION PERFORMS RETURN POWERED FLYBY
60 nmi from the Moon.

18. FINAL RETURN TRAJECTORY CORRECTION (RTC) BURN
Precision targeting for Earth entry.

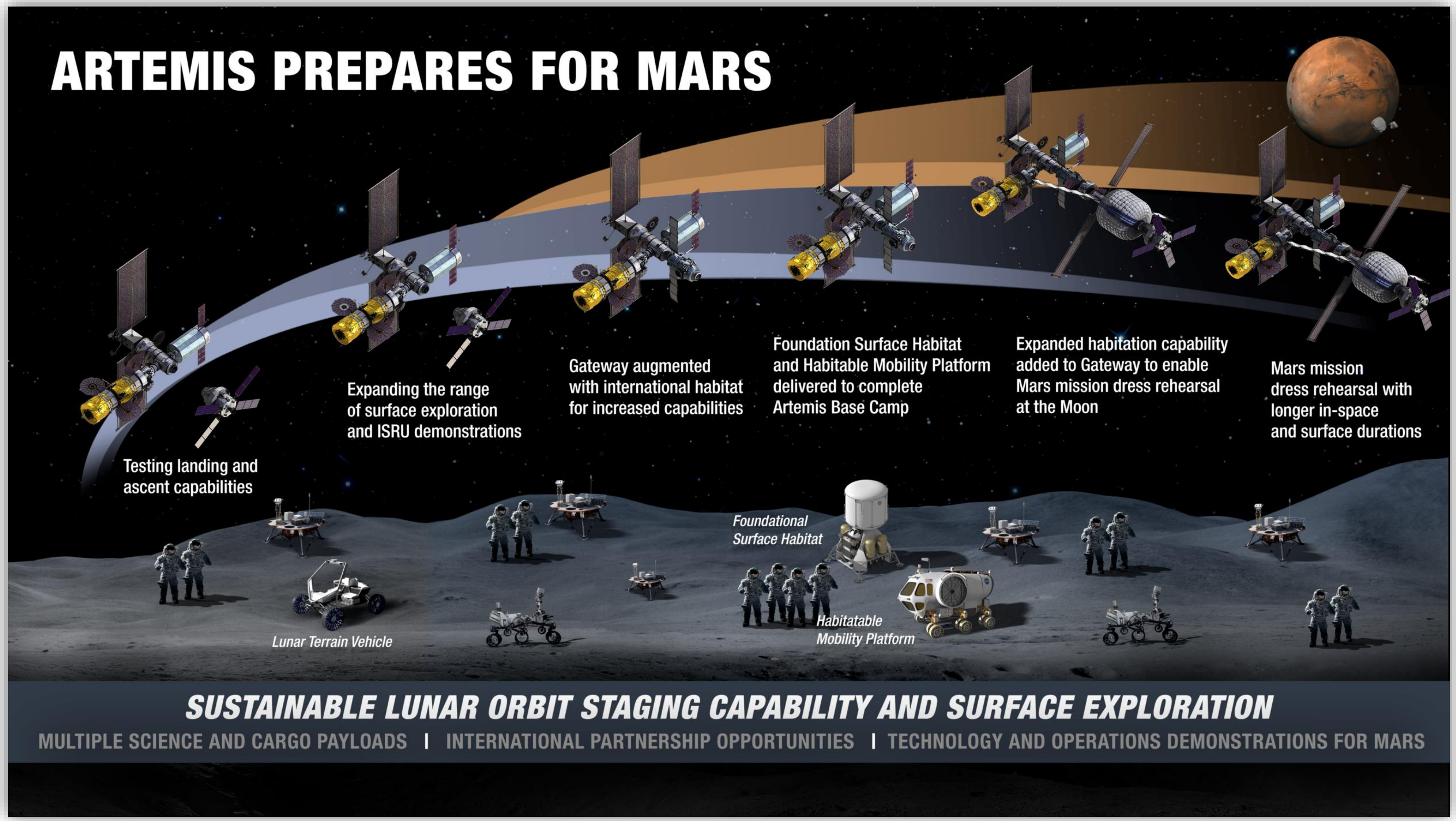
19. CREW MODULE SEPARATION FROM SERVICE MODULE

20. ENTRY INTERFACE (EI)
Enter Earth's atmosphere.

21. SPLASHDOWN
Ship recovers astronauts and capsule

NASA’s Artemis Program

IV&V Program



ARTEMIS PREPARES FOR MARS

Testing landing and ascent capabilities

Expanding the range of surface exploration and ISRU demonstrations

Gateway augmented with international habitat for increased capabilities

Foundation Surface Habitat and Habitable Mobility Platform delivered to complete Artemis Base Camp

Expanded habitation capability added to Gateway to enable Mars mission dress rehearsal at the Moon

Mars mission dress rehearsal with longer in-space and surface durations

SUSTAINABLE LUNAR ORBIT STAGING CAPABILITY AND SURFACE EXPLORATION

MULTIPLE SCIENCE AND CARGO PAYLOADS | INTERNATIONAL PARTNERSHIP OPPORTUNITIES | TECHNOLOGY AND OPERATIONS DEMONSTRATIONS FOR MARS

ARTEMIS

Artemis IV&V

IV&V Program

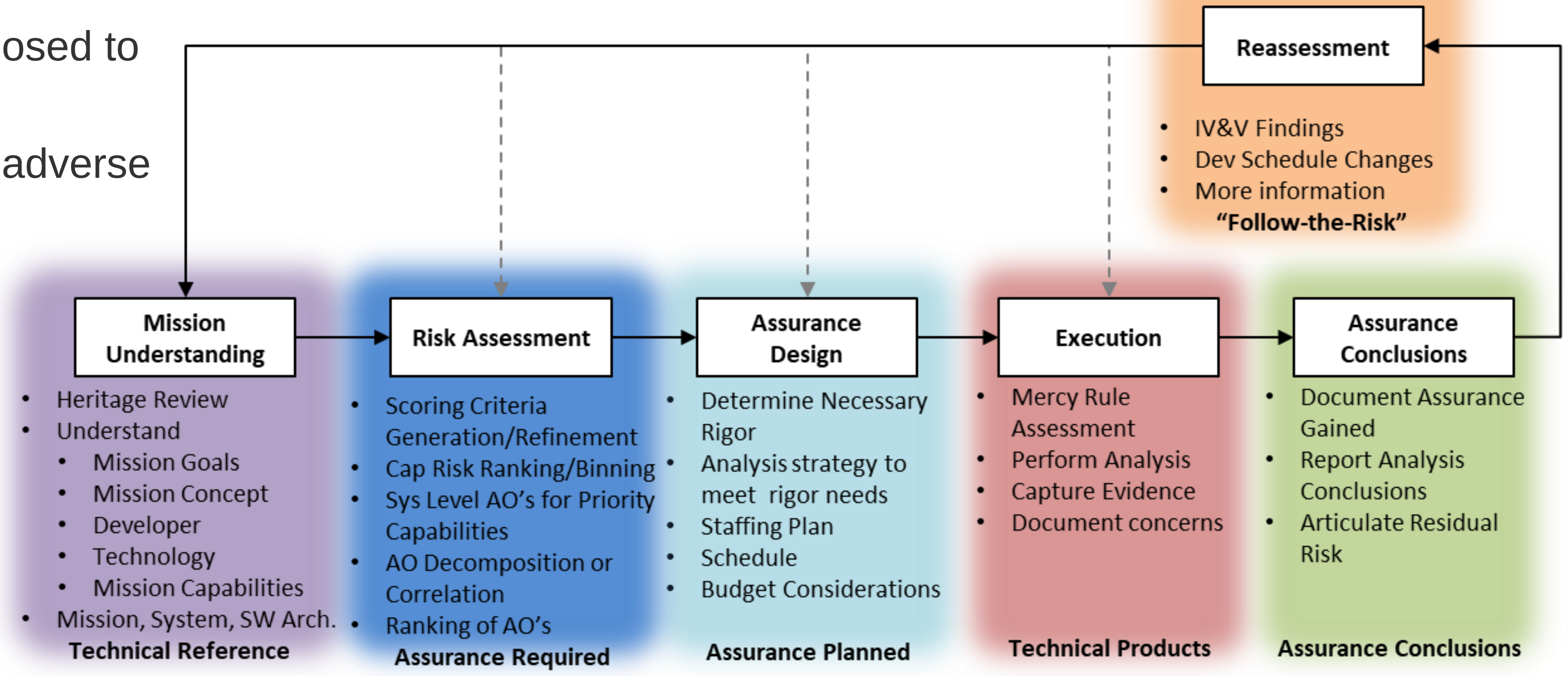
IV&V Assurance Strategy

Q1: Does the software do what it is supposed to do?

Q2: Does the software not do what it is not supposed to do?

Q3: Does the software respond appropriately to adverse conditions?

- Assurance Objective (AO): a targeted statement of a claim IV&V would like to make when analysis is complete
- Capability Based Assurance (CBA): the approach by which the mission, system, and software capabilities, not software components or entities, form the basis for identifying AOs and planning analysis activities



Reassessment

- IV&V Findings
- Dev Schedule Changes
- More information

"Follow-the-Risk"

Mission Understanding

- Heritage Review
- Understand
  - Mission Goals
  - Mission Concept
  - Developer
  - Technology
  - Mission Capabilities
- Mission, System, SW Arch.

Technical Reference

Risk Assessment

- Scoring Criteria Generation/Refinement
- Cap Risk Ranking/Binning
- Sys Level AO's for Priority Capabilities
- AO Decomposition or Correlation
- Ranking of AO's

Assurance Required

Assurance Design

- Determine Necessary Rigor
- Analysis strategy to meet rigor needs
- Staffing Plan
- Schedule
- Budget Considerations

Assurance Planned

Execution

- Mercy Rule Assessment
- Perform Analysis
- Capture Evidence
- Document concerns

Technical Products

Assurance Conclusions

- Document Assurance Gained
- Report Analysis Conclusions
- Articulate Residual Risk

Assurance Conclusions

- Follow-the-Risk (FTR): the approach by which IV&V understands, identifies, and prioritizes areas of risk within the projects' capabilities and software continuously, to focus effort in the areas of highest risk
- Adaptive IV&V: using critical thinking to alter assurance designs and analysis approaches rather than rigid adherence to a preconceived plan

Agile IV&V

Agile IV&V: An application of agile and lean principles appropriate to the planning, management, and performance of IV&V, rather than adoption of a branded framework or tool

Iterative Cycles – "Assurance Releases"

- Three-month planning cycles across Artemis IV&V
- Review completed assurance work and plan targets for next release
- Adapt to changes in project plans and available artifacts

Retrospectives

Discuss:

- What is going well
- What is not going well
- Potential process changes and improvements

Opportunity for team-building

Self-Organizing Teams

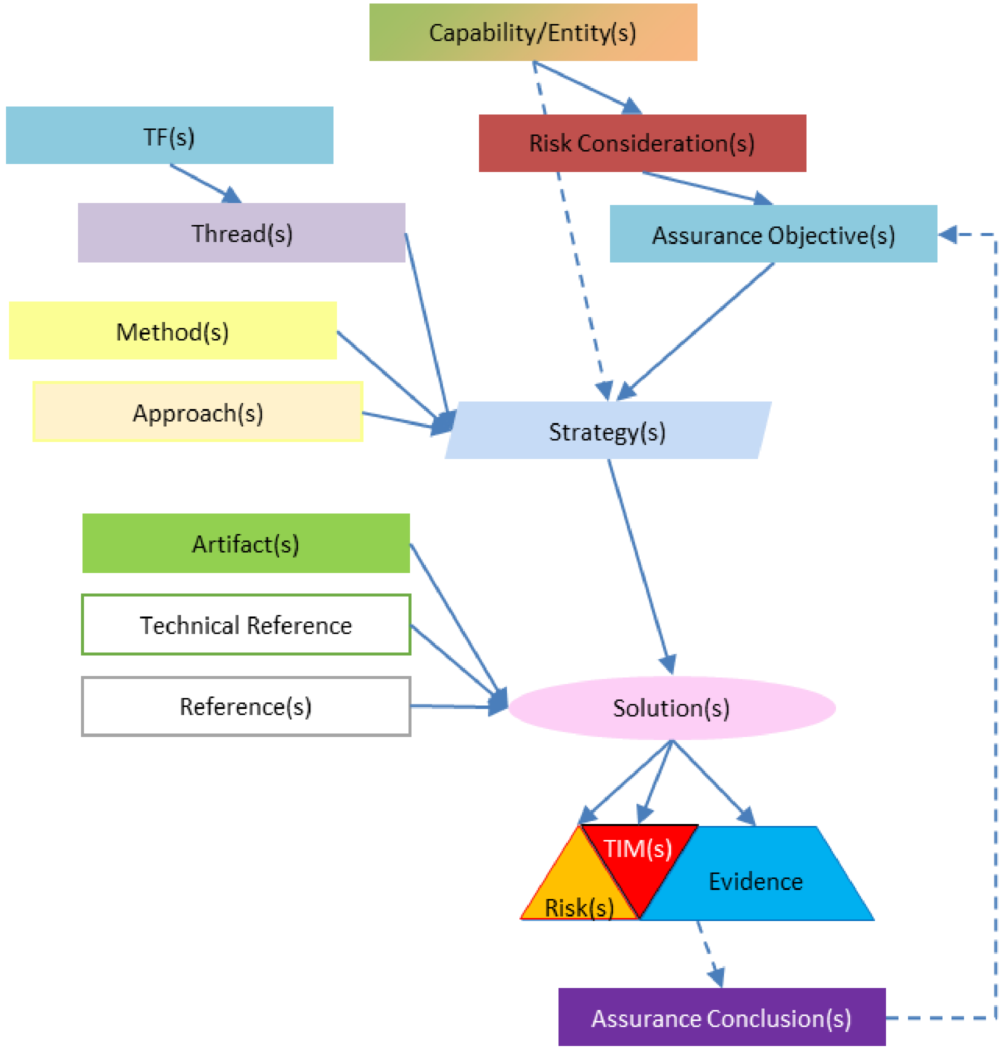
- Analysts have ownership of their areas of expertise
    - Prioritize, assess, and select assurance targets
- Team members interact regularly via stand-ups
    - Peers help each other overcome blockers

Kanban Task Management

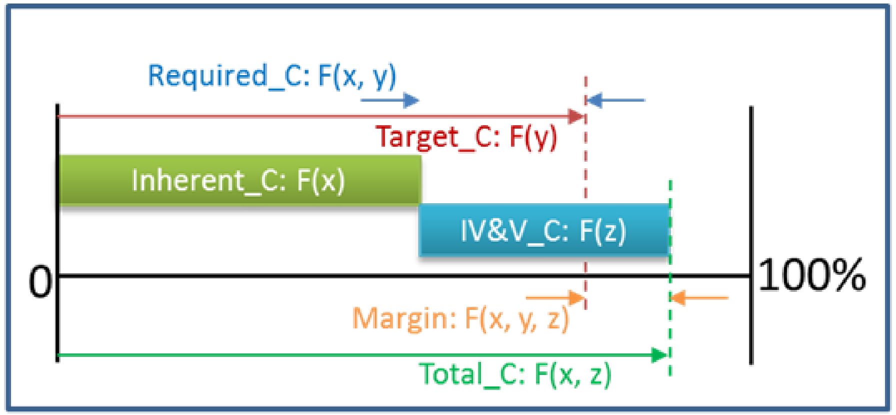
- Tasks are tracked on Kanban boards for team and stakeholder awareness
- Work-in-Progress limits lead to improvements in task size and turnaround time
- Triage incomplete tasks at end of release

Assurance and Safety Case Analytical Network (A-SCAN)

IV&V Program



- Confidence: A measure of positive assurance, or belief, in a claim or network of claims (AOs)
- By Dempster-Shafer Theory, there exists a mass of belief for a claim which is a summation of the mass of belief for its subclaims
  - Belief is based on evidence, and limited by doubt or uncertainty
- Target Confidence: “Enough IV&V” exists and can be measured based on the acceptable level of risk
- Inherent Confidence: Developer products will be correct, complete, and reliable to a certain degree without IV&V intervention
- Required Confidence: The relative deficit between target confidence and the inherent confidence of an assurance target
- IV&V analysis will increase total confidence that the system is correct, complete, and reliable
  - 100% confidence is the asymptotic maximum target



IV&V Program

A-SCAN: Intensity and Rigor

Intensity: the Breadth of Analysis

- The IV&V Technical Framework (TF) (derived from IEEE 1012) defines the activities that achieve assurance/confidence
- The application of more TF elements, each with their own confidence contribution (*$TFCC_i$*) produces broader sets of evidence from IV&V (*e_{IVV}*)
- TF Contribution to IV&V Confidence is not necessarily equal among the various TF Goals

Rigor: the Depth of Analysis

- TF Goals are achieved through Methods; however, not all methods are equally capable of achieving the TF Goal
- A Method’s rigor, or effectiveness to achieve a TF Goal (*Rig_i*) will impart a portion of the TF Contribution to Confidence

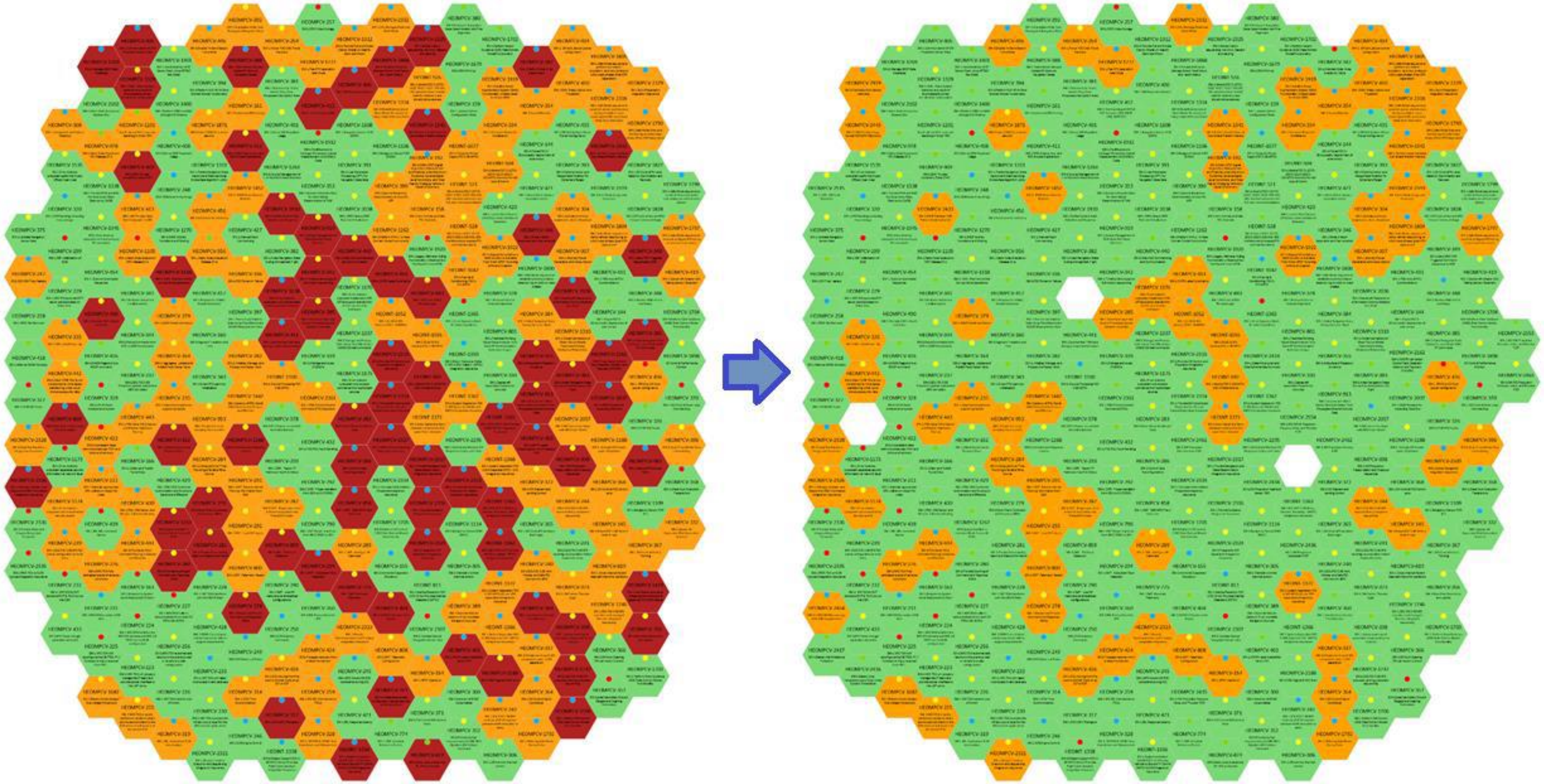
$$\sum e_{IVV} = \sum (TFCC_i \times Rig_i)$$

$$b(x) = \sum (TFCC_i \times Rig_i) \times (1 - \sum TSF_i)$$

Issues and Risks: Confidence “Defeaters”

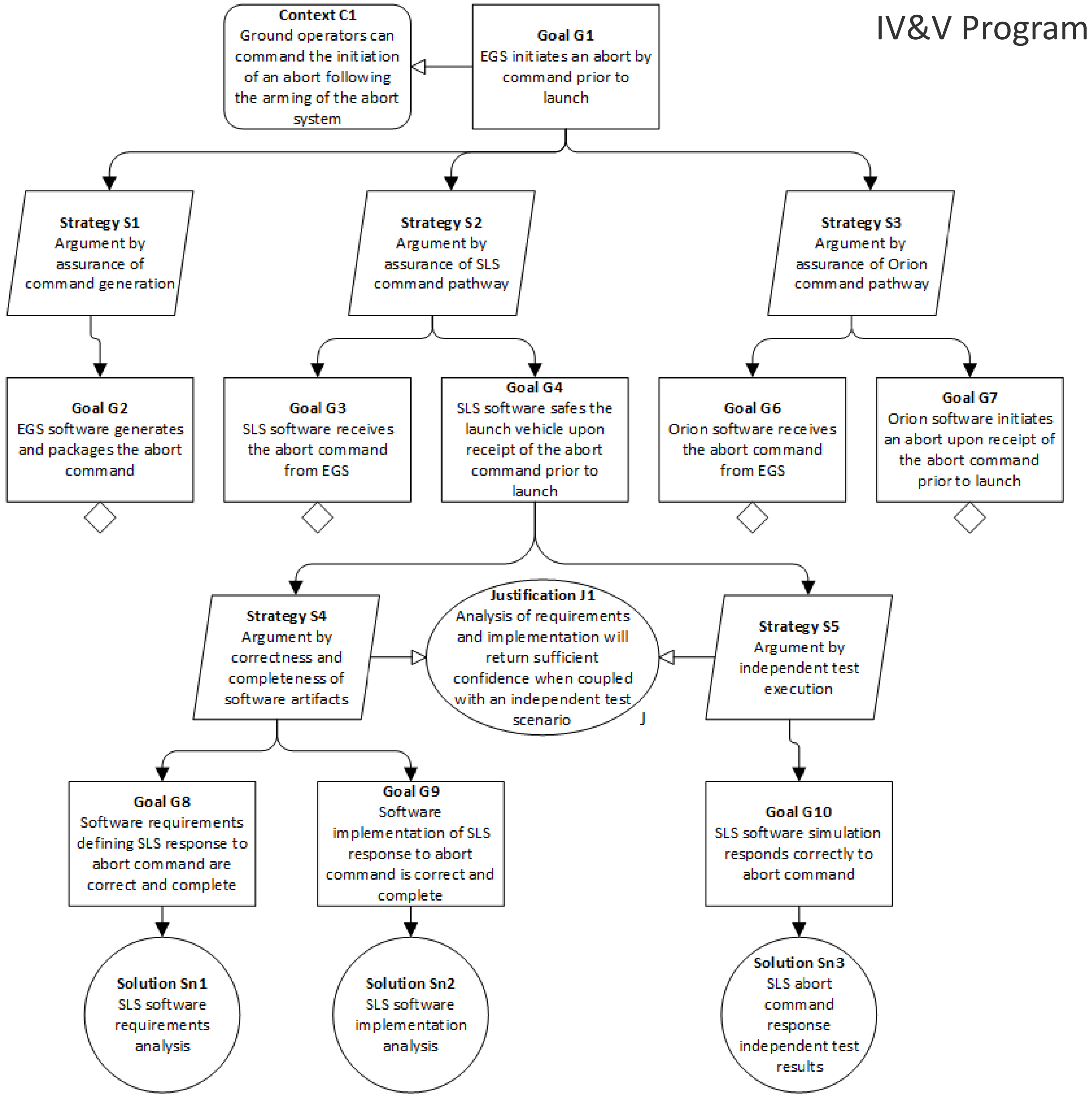
- Identified issues (TIMs) reduce confidence toward a claim until resolved
- TIMs represent direct doubt and detract from confidence based on number and severity (*TSF_i*)
- Risks are captured by Assumptions that increase uncertainty
- Both indicators can lead to changes in the original risk assessment

Tracking and Reporting Confidence



The Artemis Assurance Case

- A structured argument in GSN syntax composed of the claims and reasoning that makes up the assurance design for Artemis IV&V
- Largely capability-based in structure
  - Scenarios: Aborts, Separation Events, Docking
  - Cross-Scenario: ECLS, C&DH, GNC
- Promotes consistency and clarity of assurance argumentation
- Explicit and interrogatable for current and future missions



Context C1
Ground operators can command the initiation of an abort following the arming of the abort system

Goal G1
EGS initiates an abort by command prior to launch

Strategy S1
Argument by assurance of command generation

Strategy S2
Argument by assurance of SLS command pathway

Strategy S3
Argument by assurance of Orion command pathway

Goal G2
EGS software generates and packages the abort command

Goal G3
SLS software receives the abort command from EGS

Goal G4
SLS software safes the launch vehicle upon receipt of the abort command prior to launch

Goal G6
Orion software receives the abort command from EGS

Goal G7
Orion software initiates an abort upon receipt of the abort command prior to launch

Strategy S4
Argument by correctness and completeness of software artifacts

Justification J1
Analysis of requirements and implementation will return sufficient confidence when coupled with an independent test scenario
J

Strategy S5
Argument by independent test execution

Goal G8
Software requirements defining SLS response to abort command are correct and complete

Goal G9
Software implementation of SLS response to abort command is correct and complete

Goal G10
SLS software simulation responds correctly to abort command

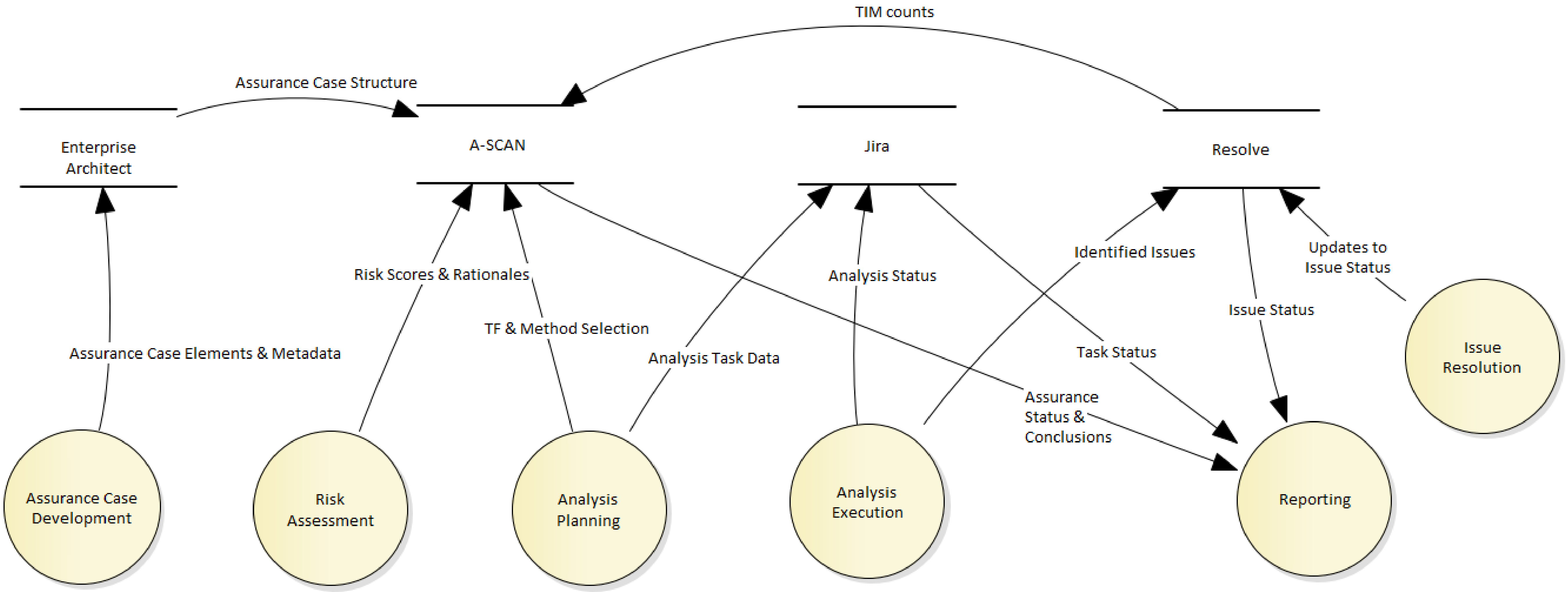
Solution Sn1
SLS software requirements analysis

Solution Sn2
SLS software implementation analysis

Solution Sn3
SLS abort command response independent test results

The Artemis Assurance Toolchain

IV&V Program

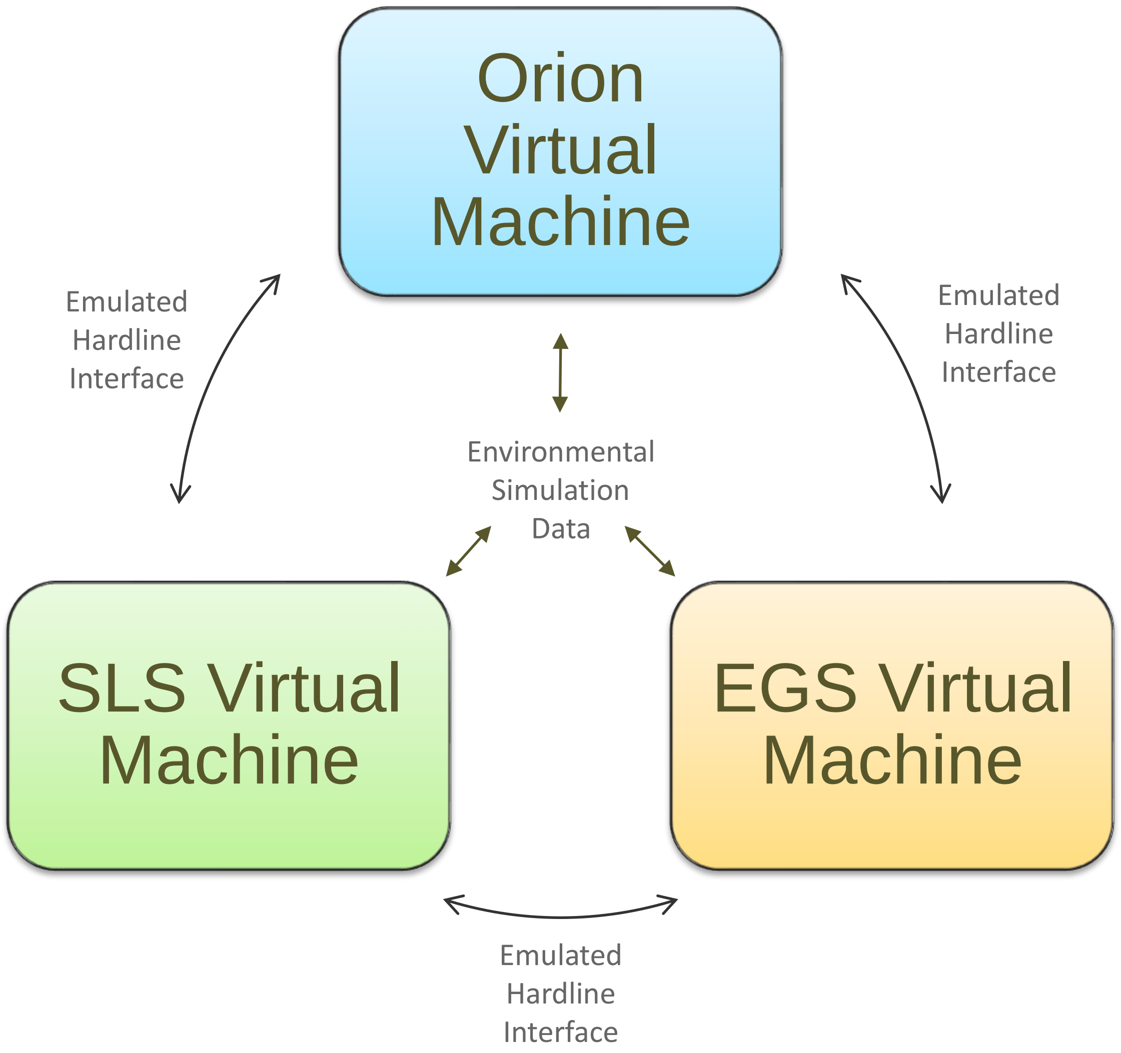


IV&V Program

ARRISTOTLE

Advanced Risk Reduction Integrated Software Test and Operations Tri-Program Lightweight Environment (ARRISTOTLE): An integrated independent test platform

- Includes emulations of Orion, SLS, and EGS, with plans to include emulations of Gateway, HLS, and MCC where possible for integrated testing on future missions
- Enables integrated scenario testing using actual flight and ground software that might be difficult or impossible to run on other test beds
- Executing test cases can often generate stronger evidence for correctness and reliability of data and command flows than other analysis methods, especially across interfaces
- Key test cases are high risk off-nominal scenarios involving interactions between Artemis systems (Aborts, Loss of Comms, System level faults, etc.)
- Produces evidence that directly supports the claims in the Artemis Assurance Case


Orion Virtual Machine
Emulated Hardline Interface
Emulated Hardline Interface
Environmental Simulation Data
SLS Virtual Machine
EGS Virtual Machine
Emulated Hardline Interface

IV&V Program

Conclusions

- Adaptive IV&V requires continuous improvement
  - Continue to identify and address needs and use cases via toolchain developments
  - Visualization, planning, tracking, and reporting, etc.
  - Assurance transfer from Artemis II to Artemis III
- Evolving approach is a direct response to the challenges of assuring software for a multi-mission program made up of large systems
  - Agile practices promote more adaptive task management and better turnaround cycles
  - Assurance Case methodology makes reasoning explicit and interrogatable
  - Artemis Assurance Case allows for distributed ownership and long-term maintenance of assurance design
  - A-SCAN provides consistent risk and confidence metrics across IV&V teams for right-sizing of assurance plans
  - ARRISTOTLE opens possibilities for producing robust evidence toward integrated scenarios

Keeping our astronauts and ground crews safe is the primary objective!

IV&V Program

Questions?