IV&V ASSURANCE CASE DESIGN FOR ARTEMIS II

Gerek Whitman
Gerek.A.Whitman@nasa.gov

Paul Amoroso
Paul.A.Amoroso@nasa.gov

Gregory Black
Gregory.J.Black@nasa.gov

Deneen Marculaitis-Granger
Deneen.M.Granger@nasa.gov

Justin Smith
Justin.L.Smith@nasa.gov

John Bradbury
John.W.Bradbury@nasa.gov

Wes Deadrick
Wesley.W.Deadrick@nasa.gov

NASA's Independent Verification & Validation Program
100 University Drive
Fairmont, WV 26554

Abstract— **As human-rated missions like those in NASA's Artemis program continue to grow in both size and complexity, and the role of software in achieving mission objectives expands dramatically, NASA's Independent Verification and Validation (IV&V) Teams face evolving challenges in assuring the safety and performance of the safety- and mission-critical embedded software that is essential to landing astronauts on the surface of the Moon by 2024. Key among these challenges is IV&V's desire to present a cohesive, integrated assurance statement to its stakeholders that encapsulates and summarizes our assurance positions across the integrated Artemis systems and their combined role in support of a safe and successful flight. In order to meet this challenge, the IV&V Teams have begun a transition to using formal assurance case concepts and documentation in the Goal Structuring Notation (GSN) to build an argument in support of software assurance. IV&V recognizes significant benefits to the logical argumentation structure provided by assurance cases and GSN over our current practices for documenting and managing assurance claims. In order to reap these benefits, IV&V is integrating the use of assurance case concepts with our paradigm of follow-the-risk capability based assurance. Because of this, assurance cases created and used by IV&V are distinct from the sort of assurance case created by a development project or embedded software assurance organization. IV&V's assurance cases depend much less upon standards and regulations, and more on evidence captured by IV&V regarding the environment, requirements, design, and implementation. IV&V constructs an independent network of claims based on an independent decomposition of arguments. Based upon the risk posture of these claims and their associated software and software artifacts, IV&V then develops and executes engineering analyses and testing, which provide evidence to either support or refute the claim. This emerging risk-informed assurance case methodology is being put into practice as IV&V plans for support of the Artemis II mission, the first flight of the Orion capsule and Space Launch System with astronauts on board.**

TABLE OF CONTENTS

1. INTRODUCTION

NASA is looking to return astronauts to the Moon by the end of 2024. The Artemis lunar exploration program will enable NASA to achieve this goal. The Artemis program is made up of various programs within NASA as well as collaborations with NASA's commercial and international partners. The Artemis program's next major milestone will occur in the fall of 2020. Artemis I will be the unmanned launch of the Orion spacecraft on the newly developed Space Launch System (SLS) from NASA's Kennedy Space Center where the Exploration Ground System (EGS) is located. This mission will send Orion to the Moon in order to test these three programs' abilities to support the next flight, Artemis II, which will occur in the fall of 2022, and will be the first time astronauts will fly on board Orion. That mission will fly humans around the Moon in preparation for the next flight,

Artemis III, which will utilize the Gateway and Human Landing System (HLS) to land astronauts on the surface of the Moon in 2024. [1]

The focus of NASA's Independent Verification and Validation (IV&V) Program is on assuring the safety- and mission-critical software that is essential to fly these missions and return our astronauts home safely. The Artemis missions utilize human-rated safety-critical software across many different platforms. Software is critical to prepare the SLS Launch Vehicle (LV) for launch on the ground within EGS and is crucial onboard the LV itself, controlling where the LV is flying. It helps Orion execute many capabilities during its journey to the Moon and back, executing critical mission events all the way until just after it splashes down. Software will be crucial in autonomous operation of Gateway, the habitable space for the astronauts to utilize while they are orbiting the Moon, and the HLS will rely upon software to travel to the surface of the Moon, and safely return to the Gateway. It is the backbone of the Mission Control Center (MCC) applications that will monitor and assist the crew while they are on their mission. IV&V has spent several years gaining system understanding in this extremely complex software across many of these platforms. In that time, the IV&V teams supporting the Artemis program have understood the risk associated with all the critical mission capabilities that will ultimately make these missions successful.

Due to the establishment of the Artemis program, IV&V will now be required on Gateway, HLS, and MCC in addition to EGS, SLS, and Orion. With the focus shifting to landing astronauts on the surface of the Moon in 2024, and the ramping up of development on Gateway and HLS, NASA IV&V felt the need to make a change. Prior to this change, the work on the EGS, SLS, and Orion IV&V teams was done in relative isolation. The teams would work with each other when appropriate, but IV&V added assurance at the project level, not the mission level. As NASA shifted toward a program vision to land astronauts on the surface of the Moon, IV&V needed to devise a way to operate as an assurance provider for the Artemis mission as a whole.

This change resulted in the creation of the Artemis IV&V Program. The Artemis IV&V Program is a team of approximately 70 people who are responsible for adding assurance for the software that executes the highest risk mission capabilities within EGS, SLS, Orion, Gateway, HLS, and MCC. The Artemis IV&V Program interfaces with each of the programs mentioned and remains in sync with development, focusing on how all of these capabilities from across several platforms ultimately come together and make the mission a success.

NASA IV&V will play a critical role in the agency's goal of landing astronauts on the Moon. In order to achieve the aggressive schedule of putting the first woman, and the next man, on the Moon by the end of 2024, the agency will have to accept some risk. The Artemis IV&V Team will help identify that risk throughout the development of the mission, as well as add assurance that the safety- and mission-critical software will do what it is supposed to do, not do what it is not supposed to do, and respond appropriately under adverse conditions. The next part of this paper focuses on how IV&V has built an assurance case and accompanying process in order to solve the problems the Artemis IV&V Team was encountering relative to the ultimate goal of adding assurance for the Artemis program.

2. Challenges of Assuring a Mission involving a System of Systems

The Artemis program contains several complex systems that need to work together safely to execute mission scenarios. Before the creation of the Artemis IV&V program, IV&V projects operated separately on the separate elements of EGS, SLS, and Orion. In addition to these three IV&V project teams was a Human Explorations and Operations (HEO) IV&V Integration Team, which sought to understand and assure the end-to-end perspective of the avionics and software interfaces between these systems.

Our means of generating software assurance are based upon the IV&V Capability Based Assurance (CBA) approach. In CBA, the mission, system, and software capabilities and their identified risks serve as the basis for planning what analysis activities are necessary to satisfy an assurance objective, while the IV&V Technical Framework [2] objectives, IV&V Catalog of Methods, and the available software artifacts are used as inputs to determine how this analysis should be conducted. IV&V uses the results of the analyses to draw conclusions of the software's ability to meet particular mission objectives, and come to an understanding of risk and the system itself to further sharpen the assurance design using a follow-the-risk approach.

Follow-the-Risk (FTR) is the approach by which IV&V understands, identifies, and prioritizes areas of risk within the projects' capabilities and software, in order to focus effort in the areas of highest risk. The goal of this approach is to reduce the residual risk across the entire risk landscape. Rather than reducing risk to "zero" in any given area, a follow-the-risk execution strategy moves the analysis effort to other higher risk areas when risk in a particular area is lowered sufficiently. IV&V assesses risk continuously, allowing focus to change as needed. Our decomposition of the Artemis mission capabilities uses the FTR approach to drive the identification of analysis needed to provide software assurance and drive down the risk.

In order to add assurance for a successful mission, IV&V examines system-to-system software behaviors with respect to mission capabilities. Specifically, the HEO Integration IV&V Team seeks to add assurance for the Functional and Operational Capabilities (FOCs) required to perform the mission. The HEO Integration IV&V Team focuses on these FOCs, which are a summary of applicable capabilities derived from the Concept of Operations and are allocated to each of the development programs supporting the Artemis program.

However, the other Artemis IV&V Teams worked separately, reported to different stakeholders, and communicated software assurance differently as compared to the HEO Integration IV&V Team. They focused on the individual system and software capabilities for their own role within the mission, and thus the objectives and goals for assurance were varied. In other words, the HEO Integration IV&V Team desired to collect and communicate assurance on cross-program and mission functionality, but the EGS, SLS, and Orion IV&V Teams performed analysis on software entities and system behaviors.

It was therefore very difficult at times for the four IV&V projects to align their assurances to the FOCs, and difficult to do a clean cross-program roll-up of mission scenario-level assurances. This caused challenges not just in reporting results, but also in communication across the projects, prioritization of analysis tasks, and allocation of resources to the riskiest parts of the software.

IV&V encountered gaps in assurance claims because the system-to-system integration arguments were not clearly integrated into the assurance hierarchy, and, more generally, because there was not a consistent methodology for organizing and decomposing assurance goals, establishing and documenting assurance strategies, and selecting and applying analysis methods.

At the time, the Artemis Teams used the bug tracking and task management tool Jira, developed by Atlassian, to hold the repository of assurance data, as well as to direct and manage the analysis tasks. In order to compile and report on combined IV&V software assurances, which included representing levels of confidence across the four projects, assurance conclusions had to be collected from each IV&V project and organized into groups relating to the FOCs. A hierarchy of "Assurance Goal" Jira tickets was used to "roll-up" assurance data to the parent assurance claims at the mission level.

This proved difficult to perform, because of both the inconsistency of assurance data capture across projects, as discussed above, as well as the fact that Jira is not an optimal tool for managing and comprehending a network of information. Furthermore, assurance arguments regarding the function from a system-of-systems perspective were difficult to identify and articulate within the sea of hundreds of Jira assurance tickets.

In spite of difficulties encountered in the assurance goal "roll-up" effort, the IV&V Projects were extremely effective in identifying software defects and driving positive change into the software. However, IV&V faced some challenges in cohesively communicating assurance at the Artemis level of abstraction. These challenges impressed the need to establish a unified assurance approach for all elements of the Artemis program, with the ability to extend the approach as new elements or projects are added, such as the Gateway and HLS elements in the near future.

Complex and subtle interactions between system elements may be overlooked in an assurance architecture. This is also true of operational dependencies and prerequisite conditions between transacting systems. It requires a broad scope of expertise in order to understand the convolutions and ramifications. Assurance goals are needed that represent mission operational capabilities and their corresponding behaviors, which emerge from the interactions between the individual systems. In addition to designing these goals, we want to gain confidence that hazardous and mission-ending emergent behaviors will not occur. A detailed understanding of each of the avionics and software subsystems that support the interchanges between the various Artemis program elements is required. Furthermore, knowledge about mission operations is needed to fill in the gaps between the mission level operational requirements and software subsystem requirements that support them. It usually takes members from a wide range of pertinent disciplines to help bring to light aspects of the integrated behaviors that are not visible when considering the separate system elements on their own. IV&V had to develop an approach to assurance that better enables this perspective and synergizes the inputs from each Artemis IV&V Team.

3. THE ARTEMIS IV&V LEAN EVENT

Artemis IV&V Leadership decided a multi-day Lean Six Sigma Event (“Lean Event”) would be an appropriate activity to begin to address these challenges of assuring the software for the Artemis “system of systems.” The benefits of a Lean methodology could be leveraged to increase speed and efficiency, and Six Sigma to increase consistency and quality. As noted by NASA’s Lean Six Sigma Program, applying these principles and methodologies can have the effect of consistently delivering high quality products and services by removing non-value added activities from existing processes, thereby reducing costs and increasing quality. [3]

The Lean Event was scheduled for three days in early June of 2019. The team consisted of twelve IV&V analysts,

representing all four Artemis IV&V Teams: EGS, SLS, Orion, and HEO Integration. Several of the team members selected traveled from their locations at other NASA centers or developer sites to include a variety of perspectives. Two IV&V Project Managers and a member of IV&V's Technical Quality and Excellence (TQ&E) Team, all of whom had experience or certification in Lean Six Sigma processes, facilitated the event.

The main objective of the Lean Event, best characterized as a Process Development Kaizen, was to determine an Artemis-wide IV&V workflow to support scoping, performing, capturing, and reporting assurance analysis - independent of mission - for Artemis II and beyond. This workflow would be required to support an agreed upon mission phase decomposition, support hierarchical decomposition of all assurance goals, be able to evaluate risk across the mission and systems, identify Artemis IV&V organizational structure, and establish how products would be logged, tracked, and reported in real time. A secondary objective was to plan a way to move away from using Jira as an assurance data repository and propose how the assurance data should be managed moving forward.

The driving Problem Statement read, "Our Artemis IV&V projects operate as four independent projects. The projects' outputs are varied in some form and make it difficult to communicate across projects, roll-up assurance to the mission level, and prioritize work and resources across projects. This approach results in numerous process inefficiencies and variation in the deliverables within Artemis IV&V." It was Artemis IV&V Leadership's view that by identifying and removing process inefficiencies and reducing variation of the outputs, a streamlined single process combined with standardized outputs could be utilized within Artemis IV&V resulting in a consistent message that can be delivered to various stakeholders at all levels.

The ground rules and assumptions imposed on the Lean Event included that team members, as well as leadership, would be open to new and possibly radical ideas, and the team would deliver an Implementation Plan with a corresponding Transition Plan at the conclusion of the Event. An additional constraint would be that the Artemis I software assurance evidence already in existence and/or currently being worked would be leveraged where appropriate, or discarded where it would present a hindrance.

The first day of the Lean Event kicked off with team introductions and IV&V project definition. Each Project's (SLS, EGS, Orion, and HEO Integration) process was defined and presented through a process map. This gave team members from the various projects insight into the various analysis procedures, product evidence types and cadence, and the IV&V and developer methodologies (CBA, Agile) in use. This activity allowed for a baseline review for each project, establishing boundaries and level of detail, process steps, sequence, and flow. Team members could also voice questions and comments on the other projects' processes to verify completeness.

The team continued this measurement and analysis activity by brainstorming potential problems and challenges to the current processes. Each project group had the opportunity to freely record ideas in a rapid-fire fashion using self-adhesive notes. After discussing the identified problems and challenges, day two began with a similar activity to brainstorm solutions that could meet the objectives of the Lean Event.

At each of these two stages, the team gathered these notes into Affinity Diagrams. Four main areas of focus ultimately emerged: Assurance Design, Risk, Roll-up, and Team Organization. The team then placed the notes assigned to each of these categories into a PICK chart, assigning each a classification:

- **P**ossible (easy to implement, low value)
- **I**mplement (easy to implement, high value)
- **C**hallenge (hard to implement, high value)
- **K**ill (hard to implement, low value).

Figure 1 shows samples of the PICK charts developed during this activity.

Day three focused on finishing the PICK chart activity, then developing the Implementation Plan and identifying and assigning Actions. At the conclusion of the day, the team out-briefed the results of the Lean Event and the Implementation Plan to the entirety of the Artemis IV&V Leadership and analyst community.

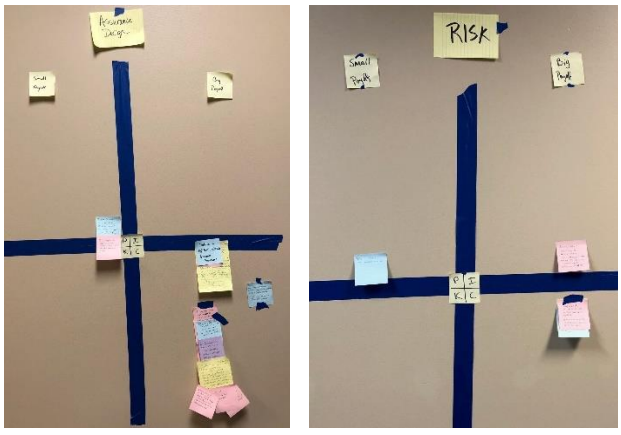

Figure 1. Two PICK charts developed during the Lean Event

The Implementation Plan

The Lean Event Team unanimously agreed that a formalized assurance case approach did possess the potential to solve

many of the challenges IV&V had been encountering previously. Utilizing assurance cases would allow each team to capture more clearly the structured argumentation and its underlying evidence and explicit assumptions supporting the claims IV&V desired to make. [4] However, the team did not know how to successfully implement such an approach in a way that would support the needs of all of the Artemis IV&V projects, as well as include the FTR approach to identify the correct focus areas across all of the Artemis software systems. The team laid out an Implementation Plan intended to continue the progress toward meeting the goals of the Lean Event.

The Lean Event Team tasked Artemis IV&V Leadership with establishing an Assurance Architecture Focus Group (AFG), a Risk Assessment Team (RAT), and an Assurance Case Pilot Team. These teams were expected to function for approximately three months following the Lean Event. The AFG would be tasked with laying the foundation for an Artemis Assurance Case, the RAT would identify risk criteria and develop an approach to apply them to the assurance case, and the Pilot Team would attempt to execute Assurance Case design within the assurance architecture and initial processes established by the AFG. Retrospectives led by Artemis IV&V Leadership were to be held at appropriate break points.

These teams would operate concurrently on their respective responsibilities, in order to move forward and solve problems quickly, but this would require regular interaction between teams and leadership to ensure the results were converging.

The Lean Event Team recognized a need to identify and/or develop various tools to support this new approach, assigning consideration of these to the AFG. The backbone would be an assurance case generation and management tool or system. Tools would also be needed to document workflow, such as daily work and progress logging, schedule tracking, and evidence and status reporting. IV&V had a number of tools already available that would need to be investigated.

Artemis IV&V Leadership was tasked with defining the reporting requirements for IV&V's stakeholders. Communication issues were identified as a fundamental obstacle throughout the Lean Event, so Artemis IV&V Leadership was also tasked with developing an Artemis IV&V Communication Plan. This plan would have the goal of providing a better understanding of expectations from the top down and bottom up, and improve communications horizontally across projects. In addition, the Lean Event Team made a recommendation to transition toward a single, integrated Artemis IV&V Team, as opposed to continuing to operate as four independent IV&V projects.

Finally, the Lean Event Team tasked Artemis IV&V Leadership with forward work to develop Artemis-wide training. This would include technical, process, and tool training, and would consider the need for establishing Working Groups to accomplish this undertaking. The team also suggested follow-on Lean Events focused on Resource Management and IV&V Evidence Collection. The Artemis IV&V Leadership saw potential in the results of the Lean Event process and Implementation Plan as presented. Leadership gave approval to proceed with building an Artemis Assurance Case.

4. BUILDING AN ARTEMIS ASSURANCE CASE

The outcome of the Lean Event indicated a direction the Artemis IV&V Team wished to move, but the team still had to commit the effort to take the first steps. From the recommendations by the Lean Event participants, team members were selected to participate in the AFG, RAT, and Pilot Team.

The Assurance Architecture Focus Group

The AFG began by defining the roles and responsibilities surrounding the new Artemis Assurance Case. The team identified the various roles for both analysts and leadership, and recognized the need for a new Assurance Architect role to persist beyond the achievement of the AFG's objectives, in order to provide oversight and management of the entire Artemis Assurance Case.

The AFG began to build on exploratory activities in assurance case design conducted earlier in the year in order to construct an architecture for the Artemis Assurance Case. They established the first few levels of decomposition of assurance claims, in order to uncover the claims that could map to the FOCs and other assurance objectives that were in focus for Artemis I analysis. Identifying how Artemis I assurance would map into the Artemis Assurance Case would be a key step in transitioning the team to the new approach later on. But the AFG also looked beyond the assurance approach used on Artemis I to include all desirable arguments and assurance strategies, even if not explicitly identified before. The resulting argumentation included mission scenario and functional decomposition, cybersecurity, safety, and code quality. The Artemis Assurance Case would need to contain the assurance generated for Artemis I, while also accommodating additional projects, such as MCC, Gateway, and HLS, as well as additional as-yet unknown future projects.

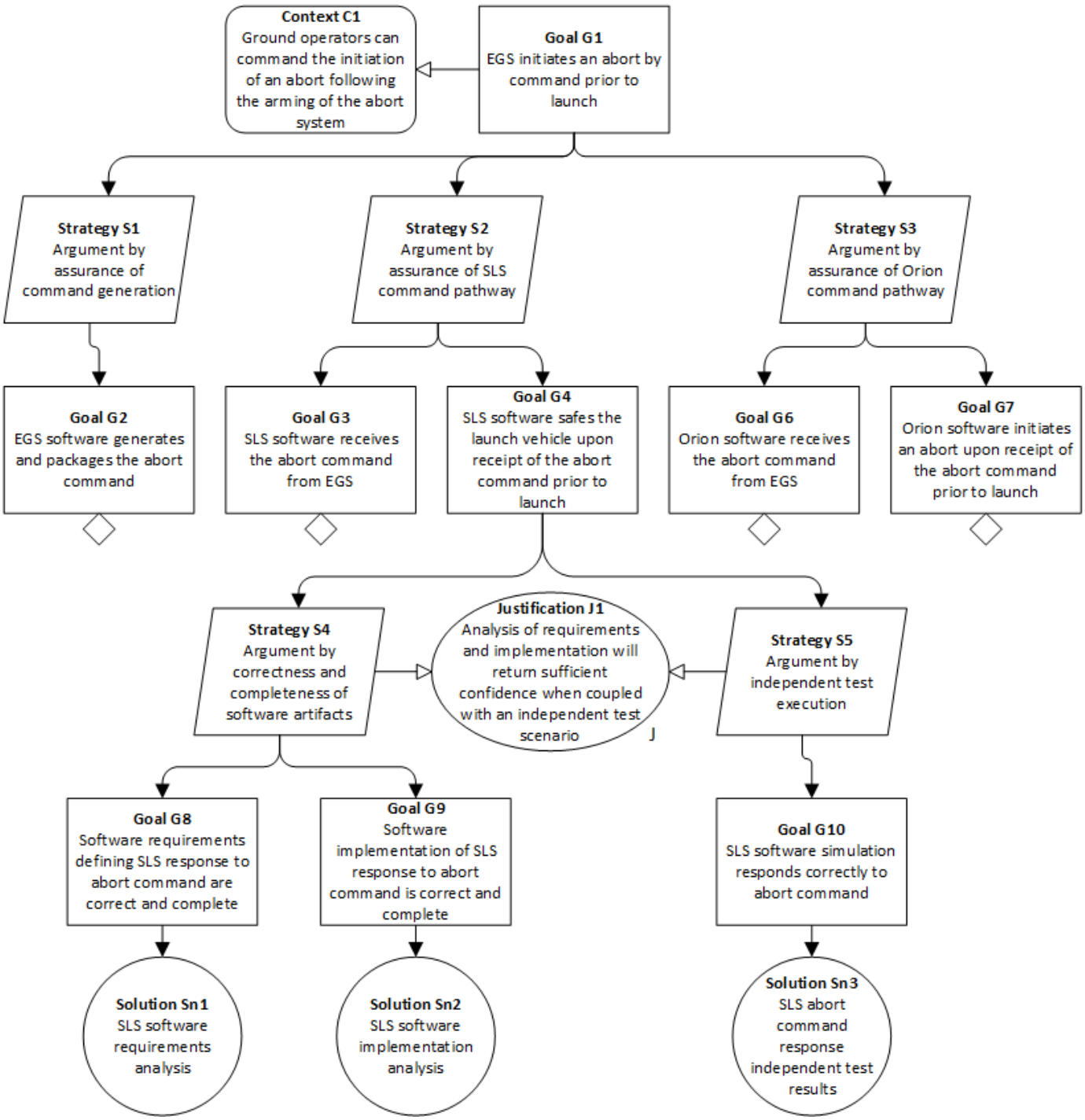

Figure 2. An Example IV&V Assurance Case Fragment

The AFG gravitated toward Goal Structuring Notation (GSN) [5] as the syntax in which they were writing assurance cases, for multiple reasons:

1. The GSN standard is both comprehensive and easily understandable.
2. The assurance case concepts presented by GSN are compatible with IV&V's approach to evidence-based assurance.
3. GSN syntax is broadly applicable to any desired IV&V assurance argument, and is extensible for managing a large, many-tiered assurance case.

The AFG took note of many examples of assurance case construction in published materials [6][7][8], from which we distilled a number of recommended practices in authoring assurance cases and using GSN syntax. In contrast with a quality assurance approach that might rely on adherence to

standards or requirements, IV&V's approach to assurance is based primarily on analysis and testing evidence generated by IV&V, independently of the development projects. It became apparent that IV&V assurance cases would have a unique flavor, describing the results of analysis executed by IV&V in response to perceived risk, as opposed to collecting and representing evidence provided by the development project. Figure 2 illustrates an example of what a capability-based, analysis-supported IV&V assurance case fragment might look like in the GSN syntax.

The AFG also began working to instantiate a meta-model in Enterprise Architect (EA), a model-based engineering tool developed by Sparx Systems, to define the GSN syntax and data fields necessary to manage the Artemis Assurance Case. The robust modeling environment of EA was at first intimidating, but provided much more control and insight over the diagram case, as well as a multi-user platform, which supports the large team size and geographic distribution.

As the implementation of assurance cases and GSN became clear, the AFG concluded by defining and documenting the process which the Artemis IV&V Team would follow to decompose the Artemis Assurance Case, as well as execute the analysis necessary to support it. This would be needed to train the Pilot Team and, eventually, the rest of the Artemis IV&V Team as we transition to the new assurance case approach.

The Risk Assessment Team

While the AFG developed the assurance case approach, the RAT worked in parallel on the other, equally important, piece to the puzzle – the risk assessment criteria for the entire Artemis IV&V Team to use. IV&V's FTR process necessitates the use of risk assessments to enable the comparison of priorities across all of the assurance targets in the Artemis Assurance Case. This was a challenging prospect, due to the disparate nature of all of the Artemis software systems.

As principal inputs, the RAT drew from two sources. The Project Based Risk Assessment (PBRA) is a risk assessment approach that is a key part of the IV&V project planning and scoping process. The Assurance and Safety Case Analytical Network (A-SCAN) tool is a recent addition to the IV&V toolset that applies risk assessments, styled after the PBRA, to a network of assurance claims to enable quantitative roll-up of risk and confidence scores, in order to fine-tune IV&V analysis effort. The RAT supplemented these with research in risk assessment methodologies from other applications.

The RAT recognized a need to develop risk criteria that could apply at various levels of argument or capability decomposition. What resulted was a multi-tiered, three-dimensional risk assessment approach, which imposed coarse risk criteria at the high level, gradually becoming more granular at lower levels of decomposition. At the top levels of the assurance case, we merely need to know if there is enough risk present to necessitate decomposing further. In contrast, at the lower levels of the assurance case, we need to prioritize the identified risks and decide which claims are most important to support with evidence, and how much evidence will be sufficient.

The risk assessment is three-dimensional because it includes the typical axes of likelihood and consequence, but also an additional consideration of software obligation. NASA IV&V's role is to assure software, so when assessing software risk on mission capabilities we must evaluate not just the likelihood and consequence of the failure of those capabilities, but also the role which software plays in mitigating failures or maintaining reliable operations.

The Pilot Team

After the AFG and RAT had established some preliminary products, the Pilot Team set out to test the execution. The AFG identified a limited scope in the Artemis Assurance Case – the pre-launch mission segment – for the Pilot Team to decompose down to solutions reflecting evidence obtained from IV&V analysis. This segment was chosen so that we could engage IV&V expertise in building assurance cases across all four IV&V teams at the time: EGS, SLS, Orion, and HEO Integration. The Pilot Team had to be introduced to and trained on assurance case concepts, but found them analogous to contemporary IV&V approaches in assurance design. The Pilot Team found that once they had acquired a base level of understanding of the capability or scenario for which they were building an assurance case, laying out an argument defining IV&V's approach to analyzing it was a straightforward task that exercised the skills they already had in planning and executing IV&V analysis.

The Pilot Team also found that in decomposing a scenario which involved contributions and interactions between multiple systems, the necessary assurance arguments for the integration between the systems naturally emerged while building the assurance case, or at least became obviously missing when reviewed by an analyst familiar with the interfaces.

As the Pilot Team worked, the AFG closely monitored their progress, in order to identify lessons learned and promising approaches as they defined the process the Artemis IV&V Team would adopt for building and maintaining the assurance case. The Pilot Team was able to experiment with a number of approaches for modularizing assurance cases, ultimately providing the recommendation that the appropriate number of Goal decomposition steps between assurance case

modules is usually only two or three. This prevents assurance case diagrams from becoming too explosive in size and difficult to understand, while still preserving enough context on a single diagram for analysts to comprehend it. The Pilot Team also uncovered potential pitfalls, such as decomposing from a systems architecture perspective too early, which can restrict an integrated assurance perspective, and make the assurance case more difficult to maintain when the systems change.

5. The Results

An intended outcome of this new approach is to achieve a structured and integrated message of IV&V's assurance for the Artemis missions overall, as well as to the individual development projects.

We anticipate that this new implementation of an integrated Artemis Assurance Case will drive a more cohesive and fluid IV&V Team structure, leading toward a more unified Artemis IV&V Team while still maintaining concentrations of subject matter expertise for the individual systems. The new organization will allow for a more holistic integration perspective, an easier flow of expertise between the component IV&V projects than previously achieved, and a more flexible allocation of resources to support the risk-based prioritization of assurance goals.

To guide the development and use of the Artemis Assurance Case, the team laid out an end-to-end process that consists of four distinct phases: Assurance Design, Analysis Planning, Analysis Execution, and Reporting and Tracking. Figure 3 shows a representation of this process, which is based on and expands upon the principles of the FTR processes already implemented for Artemis IV&V. A process workflow covers each phase, describing when and how the assurance case and other tools are used, the necessary review steps and transition decision points, as well as the actors and their responsibilities at each step.

The entire process is iterative, as the Artemis Assurance Case will be built up over time and some phases have internal iteration cycles. In Assurance Design, assurance cases decompose from the mission level down to the level at which software capabilities can be identified, based on the system understanding generated by analysts. As these assurance cases develop, they are reviewed and assessed for risk, allowing analysts to prune low risk branches from the IV&V focus areas and prioritize the rest. Risk assessments can also inform the selection and rigor of evidence or arguments used in the construction of the assurance case. After identifying individual software entities or behaviors in support of the decomposed capabilities, the Analysis Planning phase begins, during which analysts develop assurance cases that describe the analysis approach and identify the Solutions needed to produce the evidence to assure that capability.

Review of these assurance cases occurs before continuing. From the identified Solutions, analysis tasks are realized, and during the Analysis Execution phase analysts work these tasks. An analyst may determine that an alternate or additional analysis approach is necessary, or learn new information that influences the composition of assurance cases or risk assessments, thus feeding back to the previous two stages. Eventually, as analyses are completed, we enter the Reporting and Tracking phase, in which we report the results of analysis to our stakeholders, periodically assess our progress based on the identified risks and accumulated confidence, plan our priorities for the next work cycle, and hold retrospectives to identify what is and is not working and solicit feedback from team members. We anticipate the ability to take a snapshot of the Artemis Assurance Case and corresponding risk landscape at any given time, allowing us to communicate to our stakeholders about any areas of concern whenever there is an opportunity to do so.

A forthcoming challenge is the transition to this Artemis Assurance Case approach from the existing processes in use for assurance of the Artemis I mission. IV&V strives to maintain synchronicity with the development organizations and their product delivery schedules; however, those schedules will vary as the projects also transition work between missions. Currently, the Artemis I flight is scheduled for late 2020, and the Orion software developer is already working primarily on Artemis II products; SLS and EGS developers are expected to similarly transition at some, likely different, points in 2020. Thus, the transition at IV&V is similarly staggered, with an Orion IV&V Team making the first effort to implement the assurance case approach for Artemis II. IV&V Teams for the other systems are collaborating with the Orion Team to develop the argument structure at the system-to-system integration level. Later, at the points when other development projects and the IV&V assurance work on them is likewise transitioning from

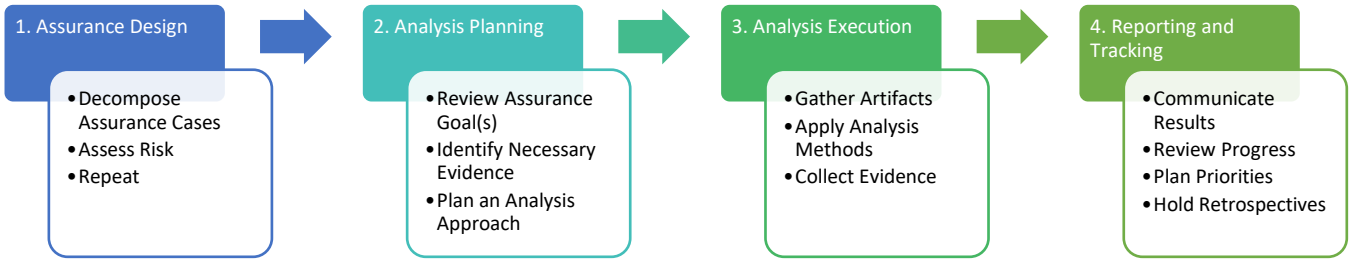

Figure 3: The Artemis Assurance Case Development Process

Artemis I to Artemis II, IV&V will continue to adopt this assurance case process and develop those respective system level and software arguments.

IV&V will also need to translate assurance conclusions and supporting evidence that can carry over from Artemis I assurance to the Artemis Assurance Case, as some software components and behaviors are likely to be reused with little-to-no modification. In general, the assurance structures of these two approaches are quite different, and it remains an open problem to determine how a transfer can be done efficiently and accurately while ensuring that nothing is lost in the process.

The MCC and Gateway systems are currently being added to the Artemis IV&V portfolio with their planning efforts now ramping up, and the HLS is expected to be added at a later date. IV&V expects that assurance case branches for these systems will integrate into the Artemis Assurance Case from their inception, without a need to transition any prior assurance structure.

IV&V uses a number of commercial and in-house tools for various non-technical tasks; for example, Jira for task tracking, an in-house database tool for tracking and reporting identified defects, and an in-house database tool for tracking and reporting identified project risks. For Artemis I, IV&V extended the use of Jira to capture and track the Artemis IV&V assurance network, but difficulties maintaining and visualizing the network and especially assessing the assurance posture at the high levels made this approach increasingly untenable. The different approaches each separate Artemis IV&V Team used to plan and assess assurance made any higher-level integrated assurance conclusions extremely subjective and lacking in a consistent viewpoint on risk determination.

As discussed in Section 3, to facilitate a more consistent approach for Artemis IV&V, it was determined that continued use of the Artemis I IV&V assurance toolset would be inadequate. Instead, the implementation for the Artemis Assurance Case will rely on two main tools: one to capture the assurance case, and one to perform the risk assessments and capture the assurance status and conclusions.

For the assurance network itself, a graphical modeling tool is desirable to aid in visualization of the network, and EA was chosen as the initial candidate. We found that, with some prior experience in using the modeling tool, we were able to customize a metamodel that supports all of the syntax and data structures we needed. The Pilot Team also proved that IV&V analysts were capable of learning the basic functions of EA within a short period, to a level of proficiency required to do their work.

For the risk assessment tool, we are adapting our in-house tool A-SCAN to implement the risk assessment approach defined by the RAT. A-SCAN will contain a representation of the Artemis Assurance Case, and allow analysts to apply risk assessments at the appropriate decomposition steps. Later, A-SCAN will collect the results from analysis evidence to feed a rollup calculation of confidence in support of an assurance objective and provide a consistent perspective on the overall assurance posture at any milestone. Eventually, we anticipate it will be desirable to have these two tools integrated or combined into a single tool solution that also interfaces with the other IV&V defect and risk tracking tools in order to reduce inefficiencies in the transfer of data and reduce maintenance effort. Artemis IV&V will continue to use Jira, but only as a task management and tracking tool, rather than as an assurance data repository.

6. CONCLUSION

The Artemis IV&V Team has made tremendous strides in the goal that they set forth for themselves in the Lean event. There is still a long way to go to get to where IV&V wants to be as a program and the assurance case that IV&V wants to have for the Artemis program, but the work described in this paper has the team pointed in the right direction.

One of the biggest takeaways from this experience was the value of Lean Six Sigma tools and holding a Lean event like the one described that occurred in June of 2019. The entire effort described in this paper is a result of the Lean event and the implementation plan that was developed by analysts from across the Artemis project portfolio at IV&V. The idea to build an assurance case was a grassroots effort dreamed up by the Artemis IV&V analysts after Artemis IV&V leadership gave high-level guidance of what problems needed to be solved.

Communication across the Artemis IV&V Program has also improved, and both analysts and leadership have identified this as one of the best things to come out of this effort. The increase in communication seems to have been due to a couple of specific reasons. The first was the Lean event in June that brought together twelve analysts from across the Artemis IV&V Program to address specific objectives laid out by management. With two Lean Six Sigma facilitators, the team was coached through addressing the challenges in front of them and in three days came up with an aggressive implementation plan that leadership could get behind. Throughout the entire event, the communication between the Artemis analysts increased day by day, and one could watch the transition from several independent IV&V Teams to a group of analysts that represented one common idea shared by a single team. The second reason communication has increased was due to the teams that were formed to work the implementation plan. These teams successfully achieved their goals laid out in the implementation plan, and communication across those teams was one of the main driving factors to their success.

Due in part to this increase in collaboration, the assurance case structure itself has turned out to be extremely useful and intuitive. All of those who have worked within the Artemis

Assurance Case to date, including the AFG and the Pilot Team, have reported an increase in system understanding of the entire Artemis mission. One of the main benefits reported is the visibility of system-to-system interactions and other various intricacies. This visibility then allows IV&V to better understand and communicate the risk within these cross-system interactions and plan more complete assurance activities in these areas.

Another benefit from the approach described in this paper is the promise of improved external communications. One of the challenges the Lean event participants were looking to address was the ability to communicate a cohesive story at the mission level. With all of the Artemis IV&V projects now working under an integrated assurance case, rolling up assurance at the mission level will occur more naturally. These Artemis program-level assurance statements can be communicated to various stakeholders both internal and external to IV&V including our primary stakeholder, NASA's Office of Safety and Mission Assurance. Not many entities within NASA are evaluating the combined capabilities of these systems prior to integrated testing. It is IV&V's hope that this work will help us communicate risk in integrated areas to decision makers earlier in order to help them avoid cost and schedule traps if these risks are realized during integration.

Moving forward, the Artemis IV&V Program wants to utilize the Artemis Assurance Case to help manage the work being done on all of the Artemis IV&V projects. As described above, the priority of each branch of the assurance case will be determined through the assessment process and this prioritization will be used to set the objectives of each work cycle for the Artemis IV&V Program. Currently, we are already developing and scoring assurance cases for Artemis II on Orion, along with MCC and Gateway. As the Artemis I launch approaches, the EGS and SLS teams will begin to transition their approach to using the Artemis Assurance Case. This will result in a unified assurance approach for Artemis II, the first mission for these projects with astronauts on board.

One of the major hurdles that needs to be cleared in the future is tooling. Currently, the team is using Enterprise Architect as described in the paper. IV&V would like to move toward a future tool, developed specifically to implement risk-driven assurance case development, built in-house at IV&V and adjusted to fit the needs of the Artemis IV&V Program.

There are still challenges and unknowns in the process described in this paper. Ultimately, IV&V is very much in the infancy of using assurance cases and has many more lessons to learn in the future. IV&V views this as a step in the right direction for how to add assurance for the mission that will enable astronauts to take their next steps on the Moon.

ACKNOWLEDGEMENTS

First and foremost, the authors would like to thank the members of the Artemis IV&V Program who were challenged back in the spring of 2019 to address the problems identified by leadership. Their participation in the Lean Six Sigma event as well as continued work throughout the summer has led to where the Artemis IV&V Program is today. The authors would like to thank NASA's IV&V Program leadership as well as IV&V contractor leadership for supporting the Lean Six Sigma effort and providing a safe space for the teams to take risks and innovate, allowing the team to come out of this experience with a better understanding of the structure that makes the most sense for the Artemis IV&V Program. Leadership has no guarantee that this effort will be a success, but the guidance and trust that has been given to the team will assure that these analysts will try their best, and continue to improve the process until it works for the Artemis IV&V Program.

REFERENCES

[1] NASA's Artemis Website: https://www.nasa.gov/what-is-artemis

[2] Independent Verification and Validation Technical Framework (IVV 09-1): https://www.nasa.gov/sites/default/files/atoms/files/ivv_09-1_independent_verification_and_validation_technical_framework_-_ver_p_-_10-25-2017.pdf

[3] NASA GSFC Lean Six Sigma (LSS) Overview PowerPoint presentation, Mark Bollard, Quality Assurance Branch, Safety & Mission Assurance Directorate, Goddard Space Flight Center.

[4] IEEE Standard Adoption of ISO/IEC 15026-1—Systems and Software Engineering—Systems and Software Assurance—Part 1: Concepts and Vocabulary

[5] Goal Structuring Notation Community Standard, Version 2, The Assurance Case Working Group: https://scsc.uk/r141B:1

[6] T. P. Kelly, "A Six-Step Method for Developing Arguments in the Goal Structuring Notation (GSN)" (1999).

[7] S. P. Wilson, J. A. McDermid, C. H. Pygott, & D. J. Tombs, "Assessing Complex Computer Based Systems using the Goal Structuring Notation" (1996).

[8] T. P. Kelly & R. A. Weaver, "The Goal Structuring Notation – A Safety Argument Notation" (2004).

BIOGRAPHIES

Gerek Whitman *received a B.S. in Aerospace Engineering from Pennsylvania State University in 2014. He has been supporting NASA's IV&V Program as a contractor for 5 years and is currently employed by SAIC Inc. He spent his first year with NASA IV&V assisting on a Software Assurance Research Program (SARP) initiative on Assurance of Fault Management Architectures. He joined the Orion Multi-Purpose Crew Vehicle (MPCV) IV&V team as an IV&V analyst in 2015, and served as an Orion IV&V Scrum Team Lead for six months in 2017. In 2018, while still on the Orion IV&V team, he served as a Capability Based Assurance (CBA) champion for the IV&V Office, assisting with the advancement of CBA on other IV&V projects.*

Paul Amoroso *is a senior software systems engineer with 35 years of experience working on DoD and NASA programs as a software developer, software systems architect and Software CPE. Twenty-four years of this time was spent employed by the Lockheed Martin Corporation. He is currently employed by TMC Technologies, working in NASA's Human Exploration and Operations IV&V projects, as a software integration analyst, reporting software assurances to the ESD Integrated Avionics and Software Integrated Task Team. Paul received a M. S. in Computer Science from the New Jersey Institute of Technology in 2005 and a B. S. in Physics from Montclair State University in New Jersey in 1982. He continues to support the NASA IV&V Program, doing cross-program software analysis and supporting the development of an Artemis Tri-Program emulation environment for dynamic independent testing.*

Greg Black *received a B.S. in Physics from the Massachusetts Institute of Technology (MIT) in 1991 followed by an M.S. and a Ph.D. in Astronomy from Cornell University in 1997. Afterwards he worked as a reseacher and instructor at the National Radio Astronomy Observatory (NRAO) and then the University of Virginia. He is currently employed by SAIC Inc. and has supported the NASA IV&V Program as a contractor since 2010. He has served as an analyst for teams providing software IV&V in support of various NASA missions; previously for the Orion Multi-Purpose Crew Vehicle (MPCV) including Exploration Flight Test-*

1 (EFT-1), the Global Precipitation Measurement mission (GPM), and the Magnetospheric Multiscale (MMS) mission. He currently continues in that role providing software IV&V support for the Space Launch System (SLS).

***Deneen Granger** received a B.S. in Computer Science from Chapman University in 1997, and is pursuing a Master of Aeronautical Science degree from Embry-Riddle Aeronautical University. She has been supporting government projects as a contractor for 18 years and is currently employed by SAIC Inc. She spent 13 years supporting the Western Range at Vandenberg Air Force Base in California as a software engineering analyst for the 30th Space Wing Range Safety IV&V and Performance, Evaluation, Test and Simulation (PET&S) contractors. There she worked on the Telemetry, Metric Data Processing, and Mission Flight Termination Ground Systems analysis tasks. She joined NASA IV&V in 2014 as a software engineer on the Exploration Ground Systems project, specifically as the lead IV&V analyst on the Launch Release Subsystem. She is currently the functional lead for the Electrical Ground and Flight Application Software IV&V efforts, as well as the EGS representative on the Artemis Assurance Architecture Team.*

***Justin Smith** received a M.S. in Aerospace Engineering from West Virginia University (WVU) in 2007. He also has B.S. degrees in Mechanical and Aerospace Engineering from WVU. He has been with NASA for 12 years as both a contractor and civil servant. He spent his first 4 years with NASA at Johnson Space Center as a data processing systems and navigation instructor for the Space Shuttle. Smith transitioned to civil service in 2011 with the Department of the Navy working submarine project management at the Washington Navy Yard. In 2013 he returned to NASA as a member of the Strategic Communications Office. He transitioned to the Orion IV&V Team in 2015 and has been the project manager since the summer of 2016.*

***John Bradbury** received a B.S. in Electrical Engineering from Texas A&M University in 1982 and a M.S. in Computer Science from the University of Houston – Clear Lake in 1987. He has been supporting NASA as a contractor for over 37 years and is currently employed by SAIC Inc. He spent his first 15 years supporting NASA at Johnson Space Center as a software requirements analyst and integrated system software tester for the Space Shuttle Primary Avionics Software System. Bradbury transitioned to IV&V in 1997 as the contractor project lead for Space Shuttle IV&V through the end of the Space Shuttle Program in 2011. He also served as the contractor project lead for International Space Station (ISS) IV&V in 2005 and 2006. In 2011 he began supporting NASA's Human Exploration and Operations IV&V projects as a technical and management lead. He served as the contractor lead for IV&V's Technical Quality and Excellence Team from April 2014 through March 2016. He transitioned to the Orion IV&V Team as its contractor project lead in March 2016.*

***Wesley Deadrick** received a M.S. in Software Engineering from West Virginia University in 2004. He has been with NASA for 17 years as a civil servant. During his time at NASA, he has worked as a researcher, an engineer, and a manager. He has worked on a number of NASA missions including Kepler, Juno, James Webb Space Telescope (JWST), Mars Science Lab, Mars Atmosphere and Volatile EvolutioN (MAVEN), International Space Station (ISS), Origins Spectral Interpretation Resource Identification Security Regolith Explorer (OSIRIS-REx), and the Constellation Program. He has also served as the office lead for several offices within the NASA IV&V Program and currently leads the IV&V Office which is responsible for the implementation of the IV&V Program's support to over fifteen science and human-rated NASA missions.*