Agile approach to assuring the safety-critical embedded software for NASA's Orion spacecraft

Justin Smith
NASA's Independent Verification & Validation Program
100 University Drive
Fairmont, WV 26554
(681) 753-5217
Justin.L.Smith@nasa.gov

John Bradbury
Engility Corporation
100 University Drive
Fairmont, WV 26554
(681) 753-5210
John.W.Bradbury@nasa.gov
John.Bradbury@engility.com

Will Hayes
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213
(412) 268-6398
wh@sei.cmu.edu

Wes Deadrick
NASA's Independent Verification & Validation Program
100 University Drive
Fairmont, WV 26554
(304) 367-8329
Wesley.W.Deadrick@nasa.gov

Abstract—Human-rated missions like those in NASA's Orion Program continue to grow in complexity. The role of software in achieving ambitious mission objectives has expanded dramatically in the last few decades. Assuring the safety and performance of the embedded flight software is quickly growing beyond the reach of traditional methods and resource levels. The methods used to build these software-dominant systems evolve in an on-going attempt to keep pace with the scope of our ambitions. Agile software development is now commonplace. The long timelines and large batches of work associated with traditional methods are being replaced by rapid delivery of small increments – as system capabilities are realized in waves. Assurance of these critical software capabilities must therefore conquer an ever-expanding frontier of challenges, and do so with an approach matched to the evolving development methods. This paper recounts the journey of the Orion Independent Verification and Validation (IV&V) team as we addressed this dynamic environment. Widening our aperture to encompass a dramatically larger mission scope, while adjusting our cadence to synchronize with the rapid pace of agile software development, a new approach to IV&V is emerging. This approach is characterized by a sharper focus on mission capabilities, matched with a method to dynamically 'follow the risk' as the IV&V team delivers more compelling assurance data in waves. Traditional methods prevalent in IV&V tend to scope the work using artifacts of the development process as they evolve from preliminary to final versions, and the pace of delivery was synchronized with the development timelines prevalent in the waterfall lifecycle. That more static approach is out of phase with the demands of the new environment. Scoping work according to the critical capabilities of the system (rather than artifacts of development) and synchronizing with the rapid pace of agile development, we are moving toward more effective parity with the demands of the environment. We explain the concrete steps we took, the principles that motivated our choices, and the results we have achieved to date.

Keywords: Capability Based Assurance, Agile IV&V, Incremental Risk Assessment

TABLE OF CONTENTS

1. INTRODUCTION

NASA's Independent Verification and Validation (IV&V) Program plays a critical role for the highest profile missions within NASA's portfolio. IV&V adds 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 Orion Multi-Purpose Crew Vehicle (MPCV) is NASA's next human-rated space craft, a capsule designed to take humans farther into space than ever before. Orion is being designed to return Astronauts to lunar orbit, explore asteroids, and even Mars. With mission profiles such as the ones mentioned, Orion is exceedingly complex in terms of software's contribution to achieving mission objectives and that software is becoming more pervasive throughout the Orion systems. In addition, the software that resides on-board the Orion spacecraft is deemed human-rated safety-critical, thereby necessitating a broad scope of focus for the IV&V team's assurance efforts. This complexity, pervasiveness, and criticality creates a resource challenge for everyone whose job is to add assurance that the mission is going to fly safely and successfully.

The Orion flight software consists of over 800,000 lines of source code that is comprised of custom developed software, auto-generated software using multiple generators, and off-the-shelf software. This on-board software executes on a dozen processors with different architectures. In addition to the primary software, Orion is required to execute independently developed backup flight software due to the safety-critical nature of its operational objectives. Furthermore, Orion will be utilizing a real-time operating system which does not have the degree of flight heritage and data present on many other NASA missions. These are a small set of the unique characteristics of the Orion software that introduce added complexity to the assurance role of the Orion IV&V team. Prior to flying humans on board Orion in Exploration Mission 2 (EM-2), Orion will undergo two separate test flights. The first of these, Exploration Flight Test 1 (EFT-1), occurred in December 2014, launching Orion into a two-orbit flight to test various systems on board the vehicle. The second test flight will be EM-1, scheduled to launch in early 2020, which will send the Orion capsule to orbit the moon and spend close to three weeks in space. Orion's extended time in space will provide an opportunity to test out the capsule prior to the launch of EM-2. EM-2 will be a nine-day mission taking Astronauts around the moon and back approximately three years after the launch of EM-1.

As the software development for EM-1 matured, IV&V's Orion team noticed the negative effects of trying to add assurance for such complex and pervasive flight software with its current staffing level. The challenges ranged from keeping up with the pace of the flight software developer's agile development lifecycle to being unable to add assurance

for everything that had been identified as an area of concern. Traditionally, IV&V analyzes artifacts when they are received from the developer and delivers findings when the next group of artifacts are received or at major milestone events. Using an agile development approach, Orion didn't really have major milestone events and were incrementally developing the flight software over three years with new releases every three months. IV&V has historically been more suited to more traditional software development approaches, tending to scope the work using artifacts of the development process as they evolve from preliminary to final versions.

Orion's development environment is very dynamic, like nothing IV&V had seen before. The challenges were beginning to mount at a rate that was affecting the team's attitude towards their work and their ability to do their job effectively. The team members were not able to perform analysis without frustration. By the time the team members would review the artifacts and provide the analysis results to the developer, they had already either fixed the problem, or moved on to something very different and wouldn't return to address our findings until a later release. In many cases IV&V provided inputs months out of phase with the developer, which limits the effectiveness and impacts of the IV&V results. The developer was doing what they needed to do to build the flight software, and it was evident that these challenges would require IV&V to adapt much more than usual to perform effective analysis.

Orion IV&V needed to figure out how to operate moving forward. The IV&V team wasn't going to suddenly get an influx of resources, and the flight software developer wasn't going to slow down their aggressive development schedule. IV&V had to implement a change, something that would allow the Orion IV&V team to add assurance in the areas of highest risk to Orion flight software while at the same time allow flexibility to shift analysis focus rapidly if the areas of risk changed for whatever reason. The team needed a solution which would enable IV&V to continue to provide high value findings which could be identified early enough in the agile development lifecycle so that the developer could fix them at the appropriate time instead of fixing them in a later release increasing cost to an already resource constrained program.

2. PIECES OF THE PUZZLE

Follow-the-Risk Capability Based Assurance

Money wasn't falling from the sky. (It rarely, if ever, does.) The Orion IV&V team was set at its then-current level of 22 analysts. It was evident that there was too much work for the Orion IV&V team to perform IV&V against each safety-critical domain of the software, and Orion IV&V leadership had a sense that the team was wasting some of its effort on assuring relatively unimportant things due to the coarseness of its scoping approach which treated an entire domain of the software as either in-scope or out-of-scope. As a result of those concerns, along with the fact that IV&V had never provided services to a project using an agile development lifecycle, several decisions had to be made regarding how to move forward.

The first step began on a whiteboard in the summer of 2016. Orion IV&V leadership had been discussing ideas of how IV&V could make the biggest impact for the Orion Program with the analysts that were on the team. The team had lots of knowledge about the software capabilities that make up the Computer Software Configuration Items (CSCIs), or software entities, into which the Orion developers had organized the flight software because IV&V had been working on Orion for several years. What the team did not have was as much understanding of the broader mission capabilities necessary to carry out the various portions of the EM-1 mission, and they tended to be stove-piped in their area of expertise. An idea emerged for how to focus the Orion IV&V resources to target the areas of highest risk within the safety and mission-critical software capabilities of Orion, allowing Orion IV&V analysts to dynamically "follow-the-risk". These mission capabilities would represent how the vehicle is going to operate in the various phases of flight and would represent an integrated picture of how the various software domains would interact with each other to accomplish the mission capability. Figure 1 below details the nine step follow-the-risk process that was drawn on the whiteboard that day. The next several paragraphs will walk you through the process in more detail.

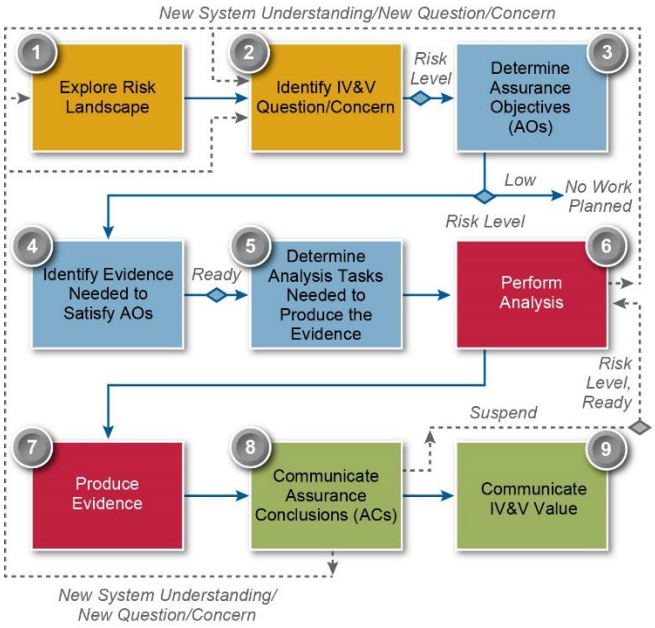

Figure 1: Follow-the-risk diagram

Following-the-risk begins with the analyst exploring the risk landscape in the area of the system or capability they would be analyzing, developing system understanding about that area of the system or capability, and identifying questions and/or concerns that they may have with the software based on the knowledge they have of how the software works and what kinds of things could go wrong, both software errors as well as adverse conditions that the software might experience during the mission.

The parts of the software involved in these questions and concerns would become the specific areas where Orion IV&V would focus its assurance effort. The belief was that if Orion IV&V analysts could find evidence to support that the software either did or did not address these areas of questions or concern in a satisfactory manner, then IV&V would be providing value to the Orion Program by reducing uncertainty and therefore reducing risk. IV&V then defined what we call assurance objectives, which, when satisfied by evidence resulting from IV&V analysis focused on those areas of risk, would address the question or concern.

The assurance objective would take on a pattern as the team began documenting them for each question or concern. That pattern was: "Orion IV&V adds assurance that [noun][action verb] to mitigate the risk / to avoid [question/concern]". As one can see with this pattern, there could be multiple assurance objectives needed for certain software behaviors or capabilities. The assurance objective represents the desired assurance conclusion that IV&V would like to be able to make at the completion of its analysis prior to the launch of EM-1. The bottom line is that the assurance objectives were written at a level of decomposition that it will be apparent what analytical evidence will need to be generated by the team members in order to satisfy them.

Once the assurance objective has been determined and the focused area of analysis has been determined, the analyst needs to identify what evidence they need to produce to show that the assurance objective has been satisfied. Once this evidence is identified, the analyst needs to develop a plan for the analysis that needs to be performed in order to produce the desired evidence. This could range from requirements tracing to independent testing of the software implementation and everything in between; it is up to the discretion of the analyst to come up with a plan.

The next step is where the analyst performs the analysis according to their plan. The primary goal for the analyst is to collect the aforementioned evidence needed to support the assurance objective. As the analysis is being performed, documents and code will be studied, issues can be discovered, and potentially new questions and concerns could arise resulting in new assurance objectives. Analysis would be performed with the specific capability identified in the assurance objective at the forefront, meaning analysts would be looking for evidence to support the software's ability to execute a specific capability. This was a very different approach than IV&V was used to in the past. This capability based assurance approach would take IV&V away from a more traditional IV&V approach derived from the IEEE 1012 Verification and Validation standard, to looking at artifacts and doing analysis with a specific mission capability, and the system and software capabilities that enable it, in mind.

One immediate thought when it came to capability based assurance was that it would reduce the total number of findings that IV&V identifies. Doing a more traditional technical framework approach exposes the analyst to an environment which can have many issues to be found, but the software defects found may not be as valuable as those specifically looking at a particular question or concern regarding a given mission capability. That's not to say the traditional approach won't work, it most definitely will work, it is that Orion IV&V didn't have the resources to do such an approach with adequate coverage of all safety-critical aspects of the software, and had to produce the most value for the Orion Program with the resources at hand.

No matter what the analyst discovers during their work, at the conclusion of the analysis, the evidence that they have found will be used to make an assurance conclusion. An assurance conclusion is used to communicate the current assessment for the mission capability that was analyzed. The assurance

conclusion conveys a level of confidence in the software's ability to correctly execute the capability or mitigate the question or concern from occurring. Ideally, the assurance conclusion is identical to the original assurance objective if there are no caveats or limitations on the evidence produced, but assurance conclusions can be caveated with various things if necessary. If the software isn't mature enough at a given point, or issues were found, this can all be communicated in an assurance conclusion. The assurance conclusions which are developed are one of the primary products which IV&V provides various stakeholders.

The process just described is the follow-the-risk process, but the process is not all completely new. Some of the things described like exploring the risk landscape, identifying evidence needed to satisfy questions or concerns, and performing analysis are things that IV&V already does. What is new and makes follow-the-risk so valuable is being able to adjust our focus "on the fly" as we reduce risk in one area and move on to addressing risk in another area, or as new risks are identified that either didn't exist or were not recognized previously. Prior to this approach on Orion IV&V and currently on most projects at IV&V, risk is usually only assessed a couple of times a year at semi-annual planning events. The risk levels that are determined as a result of those events are what drive the work over the entire year. This type of static risk assessment approach didn't seem to be appropriate for such a dynamic development environment as Orion's. Follow-the-risk would be a way that we could deal with such uncertainty moving forward, and adjust more easily to changes in the development environment.

Making the transition to the follow-the-risk, capability based assurance approach became a multifaceted event. The idea of taking a large team of 22 analysts and radically changing the way they would approach analysis didn't feel like the right thing to do at the time. The Orion IV&V leadership team discussed various options and determined that having a pilot team of select open-minded individuals would provide the best opportunity for success. Using a small subset of the larger team would provide a low-risk option to try different approaches and learn quickly from mistakes in order to innovate the changes necessary to make this idea work. Once the pilot team felt comfortable in the approaches they were using, their ideas could then be communicated to the remainder of the team for implementation.

The pilot team was assembled in August 2016 and consisted of four analysts of mixed backgrounds and experience. This pilot team was given freedom to experiment with capability based assurance and follow-the-risk concepts described earlier. The team would work together to explore these new concepts and test various ways to implement the ideas in the analysis they needed to perform. In order to have this freedom to explore, Orion IV&V leadership decided to stop analysis in the areas assigned to those four analysts. Leadership felt comfortable with this based on the fact that the software was in decent shape in their areas of expertise and that with the agile development approach that was being used, the software was going to be changing anyway, so IV&V felt that it could afford to skip looking at a single release of artifacts in those specific areas.

The pilot team worked with Orion IV&V leadership, discussing challenges which they needed help overcoming as well as solutions that they had discovered along the way. After about a month of experimenting, the team was ready to implement some ideas they had on previous areas of analysis that they had performed. The thought behind this was that the analyst could compare the new approach versus the previous approach they had used on those particular areas. The early results were very promising. The team performed the new analysis technique on previously analyzed documents in order to compare the results of their findings. Using capability based assurance the team found several very high severity issues that were missed during the application of the previous analysis approach because the mission capability was not being considered. The results spoke for themselves and in the eyes of the IV&V Program and Orion IV&V leadership, this was the type of analysis that the IV&V Program wanted to see more of in the future. Knowing that, the decision was made to transition the rest of the team to a follow-the-risk, capability based assurance approach.

Turning the ship and getting the entire team to embrace these new concepts would be challenging. The Orion IV&V team was a large team spread across multiple locations and time zones composed of analysts with various levels of experience and backgrounds. This was not a unified front moving forward; the decision to transition to follow-the-risk, capability based assurance was met with some resistance, which was encouraged by Orion IV&V leadership. The dissenting opinions were how the Orion IV&V team was going to understand the potential weaknesses and pitfalls. The challenge was getting the team to adopt a growth mindset to help make it work. The results of this type of analysis were too promising to management, and the desire to make this type of shift in the type of analysis were too strong not to at least try this method. Not doing follow-the-risk, capability based assurance was not an option; the options were finding various ways that the team could tweak what the pilot team had learned into making it work for everyone and discovering things that the pilot team missed along the way. This type of thinking led to innovation that IV&V had been seeking for quite some time.

Starting the Transition

Turning the team's world upside down had to have a plan. The first step of transitioning the way IV&V was doing work to the new way which was desired by leadership was getting the remainder of the team on the same playing field as the pilot team. The rest of the team had seen what the pilot team had been doing, and had heard the results. They needed an opportunity to experiment with the new approaches just like the pilot team had done. In order to implement capability based assurance and begin following-the-risk, it quickly became obvious that the team needed to define its assurance objectives before it could do much else. The remainder of the team were given approximately 10 weeks to study their respective areas of the Orion software, to explore the risk landscape and gain greater system understanding than they have ever had. This system understanding allowed the team to come up with all the questions and concerns they had regarding the software in that particular moment, with the knowledge they possessed. Since the team already had a significant amount of knowledge and understanding of what things could be particularly risky, the assurance goal network was built from the bottom up. This might seem counterintuitive to what a new project would do, identifying all the high level capabilities and then decomposing them. After some feedback from the team, they though it made the most sense taking their insight into what questions and concerns they had regarding critical mission capabilities and rolling them up to high level mission capabilities.

From these questions and concerns the first set of nearly 300 Orion assurance objectives were born. These assurance objectives were areas of concern that the team had deemed worthy enough to add assurance for, and provide their confidence in the flight software to the Orion Program based on the evidence they would collect. The timing of this action would take us through the end of the calendar year. January 1, 2017 would mark a new time for IV&V, with the entire team ready to storm into action on their newly created assurance objectives. This would also introduce the new vision for how IV&V would be conducted on Orion.

Now that the team had defined the "what" they would be doing, they needed the opportunity to practice the "how". The team was given the entire month of January 2017 to pick any assurance objective that was considered critical to the mission and to perform analysis with that specific capability in mind. This had never been done before by any analysts other than the pilot team, and was new territory for analysts of all levels of experience. The results were mixed after the first month; some analysts picked up on the concepts and execution of the new approach very quickly, often analysts who were relatively new to IV&V. Other team members struggled with these new concepts, particularly some of the more experienced analysts who were acclimated to the traditional IV&V approach. It was up to the entire team to understand why analysts were struggling with the new concepts and help them along as we wanted "No Analyst Left Behind".

Another thing that some members of the team struggled with was the amount of freedom this approach provided them. Leadership was asking the team to take an adaptive approach to IV&V and to "do what makes sense and don't do what doesn't make sense". Previous approaches to IV&V did not encourage such freedom at the analyst level and the need for dynamic decision making. Some analysts viewed it as a good thing that they had the opportunity to decide what to do, but others viewed the need to apply critical thinking to decision making as a bad thing; they appeared to prefer to be given specific direction as to what analysis to conduct rather than figure it out themselves. Still others were hesitant to exercise the freedom they were given, not fully believing at first that the previous constraints had really been released.

The overall effort regarding these implementation challenges brought forth how important teamwork would be moving forward. No longer can analysts just go do analysis in a vacuum or stovepipe and depend on leadership to piece all of this analysis together to make a statement about the current state of the software. In this new way of approaching our work, this would be a team-first environment; the Orion IV&V team would succeed or fail as a team.

Agile IV&V

The word Agile has a dirty feel to it around the halls of NASA IV&V; it makes everything more challenging in the world of an IV&V analyst. Agile had a different meaning to Orion IV&V leadership after working with a consultant from Carnegie Mellon University Software Engineering Institute. Mr. Will Hayes was hired by IV&V in the fall of 2016 to help the Orion IV&V project gain a better understanding of how Lockheed Martin, the Orion developer, was using Agile principles to develop Orion's flight software for EM-1 so that Orion IV&V could execute its new follow-the-risk capability based approach. As Mr. Hayes dove deeper into what IV&V was attempting to do using and following-the-risk, he educated Orion IV&V leadership on the benefits that Agile and Lean principles could bring to what was looking to be accomplished.

Mr. Hayes has extensive experience in the implementation of Agile development methods at scale, including the method used by Lockheed Martin – the Scaled Agile Framework (SAFe). We initially engaged the Software Engineering Institute to help us understand Agile Software Development. This engagement evolved quickly to an application of these concepts to our own work. Mr. Hayes took the Agile and Lean principles and put them in terms of assuring software instead of developing it. Out of this engagement there was a homework assignment which asked Orion IV&V leadership to write ourselves a "letter from the future" about what we wanted the team to look like six months from then. Our response to the homework assignment became the foundation for the Orion IV&V vision which we would come to use as a guiding light for leadership. This vision was communicated to the team in early January 2017. It made sense to provide leadership's vision to the team as they were transitioning to the new approaches described previously.

The assurance objectives that the team was defining were like little projects on their own, and could be broken down even further into smaller pieces of work which could be accomplished during a Sprint cycle. These smaller pieces of work are called "analysis activities" and describe the work that the analyst is planning on doing in order to gain the evidence needed for the assurance objective. At this point it seemed clear that the best way to approach the new way Orion IV&V was choosing to do analysis was through the fast integrated learning cycles which Agile provided. If something wasn't working, or something was working very well, this approach provided ample opportunity for the team to discuss the results and either course-correct or share the successes in order to help the other members on the team.

At the same time as the transition to follow-the-risk, capability based assurance, Orion IV&V leadership decided the team would adopt a few select Agile and Lean principles, but only the ones that made sense to be used given the objectives and nature of IV&V. Agile IV&V was going to be the application of those relevant Agile and Lean principles in the planning, management, and performance of IV&V, not an orchestrated adoption of some branded framework or tool. Mr. Hayes's next task was putting the finishing touches on the ideas of what Agile and Lean principles were viewed as relevant and developing the training for how they could be implemented in an assurance environment. Putting all three pieces of the puzzle together, it was determined that the entire team would make a formal shift to a follow-the-risk, capability based assurance Agile IV&V approach together as a team in early February 2017.

Agile IV&V was a modified SAFe model which utilized Scrum based analysis, working within a Scrum team breaking the work down into small meaningful pieces. Knowing that the team was currently too large to be a single Scrum team, we decided to create two self-organizing teams, each with their own Scrum Lead. Other aspects that seemed very valuable were setting up sprints and assurance releases. An assurance release is IV&V's version of a development release, and would last 12 weeks and contain four 3-week sprints. The sprints within the assurance release provided the team an opportunity to take back control of what IV&V wanted to work on. The team would have the ability to work on whatever high priority assurance objectives they wanted to, as opposed to simply being reactive to the various documents the developer provided.

The availability of software development artifacts can be a problem for a new project, but because the Orion Program had been going for almost ten years, there were plenty of artifacts available to support analysis, even if they were initial versions that were going to be updated. Using a release and sprint structure also provided an opportunity to insert retrospectives. At the end of each sprint, the team would hold a retrospective to discuss what went well and what didn't go well during that sprint. After the retrospective, the team would then plan the next sprint. At the assurance release level, the retrospectives were a time for all the scrum teams to stand down from work and bring everyone together to discuss how everything was going, to discuss what went well and what didn't go well at the release level. These retrospectives also provided an opportunity to discuss things that the team thought needed to be changed, as well as dive deeper into the various analyses being used and how the team could improve upon them.

Agile IV&V would also utilize the use of stand-ups, which would provide a daily status of each team member's status to the Scrum Lead. Typically a stand-up would last 15 – 20 minutes and would focus on what work the analyst had completed since the last standup, what work they were planning on completing before the next standup, and what help did they need overcoming any challenges they may be having. The Scrum Leads would then meet with Orion IV&V leadership in order to communicate up the status of how work was going. These Scrum Lead level meetings not only allowed leadership to have insight into what work was occurring, it provided leadership an opportunity to efficiently communicate things to the team through the Scrum Leads without the need to schedule another team meeting.

Assembling the Puzzle

January had come and gone, and it was time to put all of these early action steps together and introduce our Agile IV&V principles. The first Assurance Release Planning meeting

would provide an opportunity for the rest of the team to be coached in the relevant agile principles that would comprise the Agile IV&V approach described previously. Over the course of three days with the majority of the team co-located in Fairmont, West Virginia, the Orion IV&V team had a new plan of attack. Two new Scrum teams, one focused on the Entry, Descent, and Landing (EDL) mission phase and one focused on mission-phase-independent "infrastructure" such as Command and Data Handling, Communications and Tracking, and Electrical Power, were formed and were trained by Mr. Hayes on how to execute all the new processes. During this first week, the teams used the knowledge they had just obtained and planned their first Assurance Release down to each sprint. The team selected their work from the network of assurance objectives they had compiled as their backlog, starting with the highest priority assurance objectives. From there the team was able to begin operating in this new regime, continuously improving along the way.

The team learned lessons throughout the first 12-week Assurance Release and individuals adapted to the new ways of doing business. Agile principles had never been applied to an IV&V project at NASA. At first, everyone was very uncomfortable with the new processes – it took them out of their comfort zone. This was something the team had to get used to - as a leadership team we recognized that when the team is uncomfortable, they need to pay attention because they are about to learn something new. They needed to start getting comfortable with being uncomfortable.

Whatever the challenge was, the team helped each other and continuously communicated through the process to help clarify any missing information that was needed. In time, everyone adjusted to the new principles at different rates, which was expected given the dramatic changes that had been made. Throughout the early months of the transition it was crucial that leadership exhibited patience through this learning curve. The challenges the team was facing from figuring everything out were great enough without leadership breathing down their necks. The leadership team recognized that change is hard, change takes time, and we needed to have realistic expectations.

Retrospectives were crucial to the team's success early on, both at the sprint level and the Assurance Release level. These times provided an opportunity to discuss what was challenging for folks and to learn from others' successes. Retrospectives are a way to highlight the fast integrated learning cycles that Agile IV&V offered the team. Prior to holding an Assurance Release retrospective, team leadership solicited topics to discuss through one-on-one tag-ups with team members, as well as anonymous suggestions. These topics, as well as other topics that leadership thought were important to discuss, would be the focus of the three-day retrospective events. One thing that the retrospectives improved for Orion IV&V was the trust level among the team. The team quickly realized through openly discussing what wasn't going well publicly with the team, including leadership, without repercussions that they could trust each other. The team wanted to help each other get better, and evidence of that demonstrated the trust that they had for each other allowing for greater conversation and problem solving at all levels of the team.

One major adjustment came after the second assurance release, and was discussed at great length at the Assurance Release retrospective in early August 2017. The team had spoken up and they wanted to move away from Scrum toward Kanban or Scrumban. This suggestion was well thought out by the team; the team found it too difficult to break up the analysis activities into small enough pieces of work which could be consistently completed in three-week sprints. It was also determined that there was no value in remaining in a Scrum mentality since people weren't helping others complete their work once they had finished their own. This was due in part to the specialized domain expertise needed to analyze certain assurance objectives in many areas. It wasn't very efficient to have somebody who had little to no knowledge of what that person was working on to try to get up to speed and develop the system understanding in order to be able to help. By the time the person would be ready to help, the other person will have just ended up completing the work. The team also tried a collaborative "gang-tackle" approach to working an assurance objective, which they found to be ineffective.

Upon conclusion of the Assurance Release retrospective, the team had worked out the details of what would be a Scrumban approach, combining aspects of Scrum and Kanban. What would be eliminated was the time boxing of the sprint cycles and most of the ceremonies that come with sprints. Everything else mostly remained and was viewed as valuable: the team still had retrospectives, stand-ups, and assurance releases. The work was still broken down into smaller analysis activities and the analysts remained in small teams. A couple of principles which were adopted from Kanban were the use of a Kanban board in JIRA, and work in progress (WIP) limits. The introduction of the Kanban board in particular has been a tremendous improvement for the team. Being able to see the board and understand what any given person is working on is great insight to have. There were a few other things that were adopted along the way, most notably the use of a triage, which would help hold the team accountable to wrapping things up prior to the end of the assurance release. The team highlighted successful

aspects of the new Scrumban approach at the following Assurance Release retrospective.

Another struggle the teams had was operating as a self-organizing team. Leadership wanted to continue to foster growth in this area, so a third team was created, resulting in three smaller teams of 6-8 people. Another change was that the Scrum Lead position was now a rotational position, with the responsibilities lasting no more than two Assurance Releases. The thought process behind this was to give more people an opportunity to learn the position and gain some leadership experience, while continually promoting the idea of self-organization.

Seeing the Results

Since the transition to our follow-the-risk capability based agile approach in February 2017, the team continues to perform very well. All levels of stakeholders, from NASA IV&V leadership up through NASA's Office of Safety and Mission Assurance and the Orion Program are extremely impressed by the quality of the work that Orion IV&V is performing. The Orion IV&V team is continually being used as examples of excellence within the IV&V Program. The praise in their performance is not only coming from internal sources. Quotes from Orion Program personnel have also been coming into the IV&V Program through customer satisfaction surveys. One such quote: "IV&V's capability based approach and "follow-the-risk" strategy allows them to have relevant opinions on the most difficult issues the program is facing. Their recommendations and conclusions are well researched and obviously vetted internally. They consistently bring coherent communication and clarity to discussion and I highly value their opinion". Another quote from a member of the Orion Program: "I think IV&V has incredibly increased their value by going to this approach".

So how have we increased IV&V's value that is being provided to our stakeholders? By delivering impactful issues to the developer helping them identify deficiencies in their requirements, design, code, or testing with respect to critical capabilities for the Orion spacecraft. IV&V has seen the rate of the highest severity issues double in one year, while the overall rate of issue discovery has decreased. What that data supports is that the Orion IV&V program is not inundating the developer with low impact software defects and trivial issues, but is delivering evidence-based risk-driven critical issues that the Orion Program may not have otherwise found.

Another aspect of value that the IV&V team is adding is one of positive assurance. Previously there wasn't an effective method of communicating the "goodness" of the software, as most communication was focused on the issues and risks associated with what IV&V had analyzed. Since Orion IV&V has made the change to our new approach, we have been providing not only negative findings (issues and risks) but also positive findings, assurance conclusions that confirm the flight software's ability to do what it is supposed to do, not do what it is not supposed to do, and respond appropriately under adverse conditions. This provides a more balanced assessment of the condition of the software than simply providing the negative findings as in the past. IV&V's assurance conclusions provide all of our stakeholders insight into IV&V's confidence in the software. Having this type of insight allows decision makers to understand the level of risk perceived by an independent outside entity.

We are also able to deliver our assurance conclusions, issues, and risks at a much faster cadence. Under the old approach it was noted that IV&V was delivering products months out of phase with the developer. Since the changes have been made we have improved our delivery cadence from months to weeks, becoming more in sync with the developer which is crucial to make IV&V worth the investment when dealing with a project using agile development methods.

3. CONCLUSION

In conclusion, the Orion IV&V team has seen a tremendous amount of value-added change in a short time span. This change was not always easy at times, but the amount of growth which occurred for all members of this team was tremendous. The IV&V Program believes that the changes that the Orion IV&V team have implemented is a step towards the future of IV&V at NASA. In time it is hopeful that the Orion IV&V team will be able to learn from others who attempt a similar type of analysis approach.

If a project you are working on is either struggling with something, or is undergoing change, think about the benefits that agile principles could provide you. One of the primary benefits that can be provided is increased communication across the team. There are great advantages to having frequent communication at the worker level about how things are going and how to make them better. This type of communication also can provide great insight into the day-to-day operations for leadership. An agile approach also helps with accountability and planning for responsibilities, things that most projects could benefit from if they don't already have that in place.

The approaches in this paper worked for the Orion IV&V team after many adjustments along the way. What was described was one way of doing things, not the right way or the only way. It was the response of a team with numerous challenges, from agile developed safety critical software, to not knowing how all of the areas of risk were going to be addressed. Think about the challenges your team is facing and embrace that feeling of being uncomfortable. Challenge your team to find a solution that works for everyone to get the results that the customer is seeking.

4. ACKNOWLEDGEMENTS

The authors would like to first and foremost thank the members of the Orion IV&V team. Much was asked of them through this transition, and this team's success is a result of their ability to innovate and persevere through the myriad of changes described in this paper. The authors would like to thank NASA's IV&V Program leadership as well as IV&V contractor leadership for supporting the changes that were proposed by the Orion IV&V team. The investment leadership has made into these approaches described in the paper will hopefully shape the IV&V Program for the foreseeable future. The authors would like to thank the Orion Program for their patience and understanding as we made a radical change in the way IV&V performed its work. At the time these changes were being proposed, Orion IV&V leadership had no guarantees that we would be successful, but the Orion Program was supportive of our independence and trusted that we were making the best decision in the long run. The authors would also like to thank Carnegie Mellon University Software Engineering Institute for agreeing to help the Orion IV&V team deal with the challenges they were facing dealing with a software developer using an agile development model.

BIOGRAPHIES

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 10 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 36 years and is currently employed by Engility Corporation. 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.*

Will Hayes *is principal engineer with the Continuous Lifecycle Solutions Initiative at the Software Engineering Institute (SEI) of Carnegie Mellon University. Will currently supports very large scale programs striving to achieve rapid incremental delivery of systems driven by embedded software. He helps programs to effectively interact with development teams using innovative approaches, and to apply the necessary due diligence (e.g., exercise oversight, report metrics and incentivize desired performance) in ways that support –rather than hinder– successful use of continuous lifecycles. Throughout his 28 years at the SEI, Will has supported numerous commercial, government and defense organizations, providing consultation and coaching for a wide range of roles from engineers to CEOs.*