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

Justin Smith

Independent Verification & Validation

John Bradbury

SAIC

Will Hayes

Software Engineering Institute
Carnegie Mellon University

Wes Deadrick

Independent Verification & Validation

NASA's IV&V Program

IV&V Program

- NASA's Independent Verification & Validation (IV&V) Program reports to the Office of Safety and Mission Assurance (OSMA)
  - Technically, Managerially, and Financially Independent
- Located in Fairmont, West Virginia
- IV&V perspectives structured around the following:
  - Does the software do what it is supposed to do
  - Does the software not do what it is not supposed to do
  - Does the software respond appropriately under adverse conditions
- IV&V's goal across all projects is to add assurance and mitigate risk
- Orion IV&V goal: Add evidence-based assurance that minimizes the overall risk of Orion software

Orion
Multi-Purpose Crew Vehicle

IV&V Program

Traditional Approach

IV&V Program

- 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
- IV&V has historically been more suited to a waterfall development lifecycle although it has always adapted as necessary
- Orion IV&V utilized a plan based off of a flight software risk assessment and planned twice a year for what assurance would be added
- Using this plan as a guide, Orion IV&V analyzed entities in their entirety, with some entities not considered risky enough to analyze at all

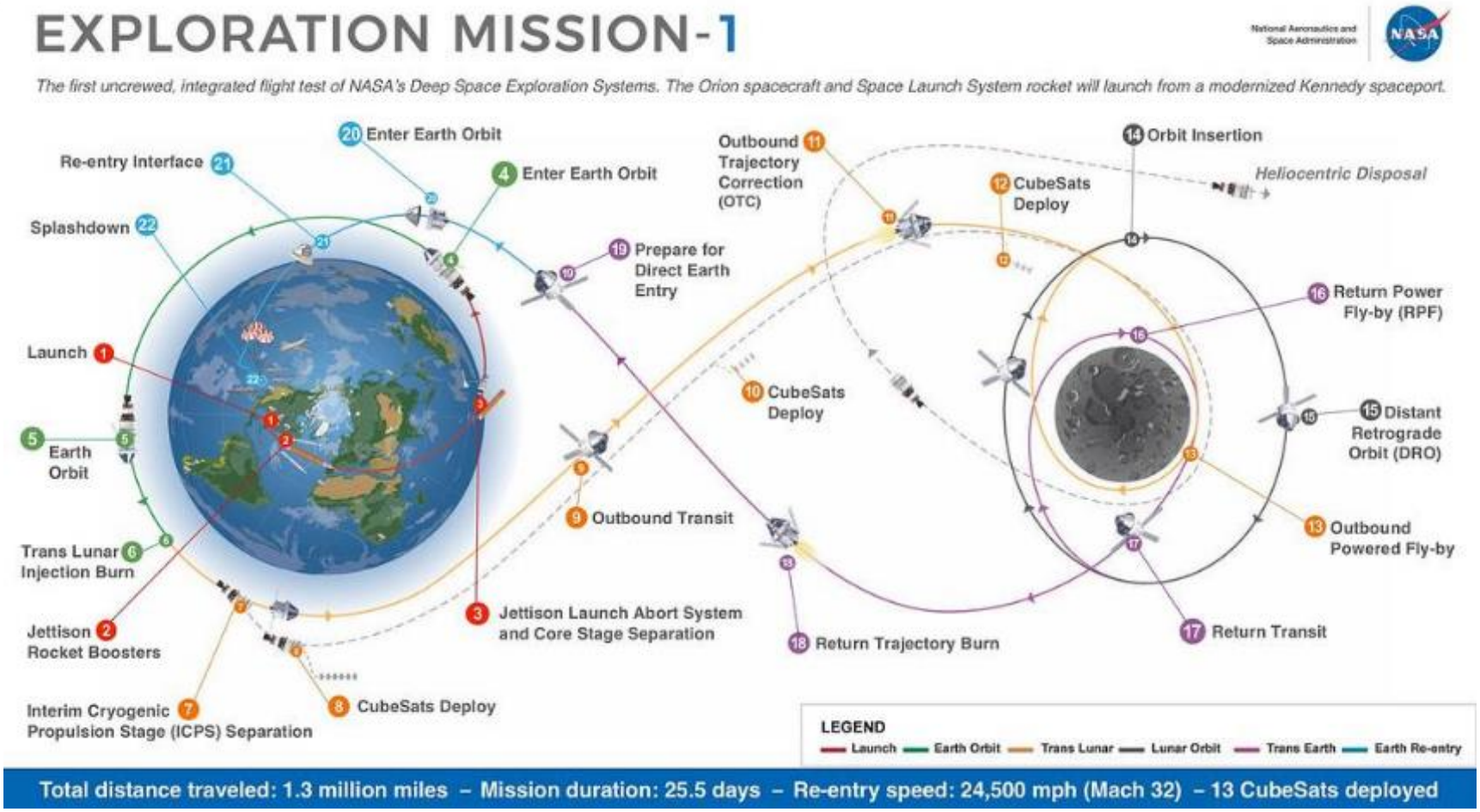
Challenges

IV&V Program

- Orion development environment is very dynamic
- Orion flight software for EM-1 is developed using an Agile development model which was very different for IV&V
- Team members could not perform the previous analysis without frustration
- In many cases IV&V provided inputs months out of phase with the developer
- Approach required IV&V to adapt much more than usual to perform effective analysis

Orion EM-1 Mission Overview

IV&V Program



Switch to Capabilities

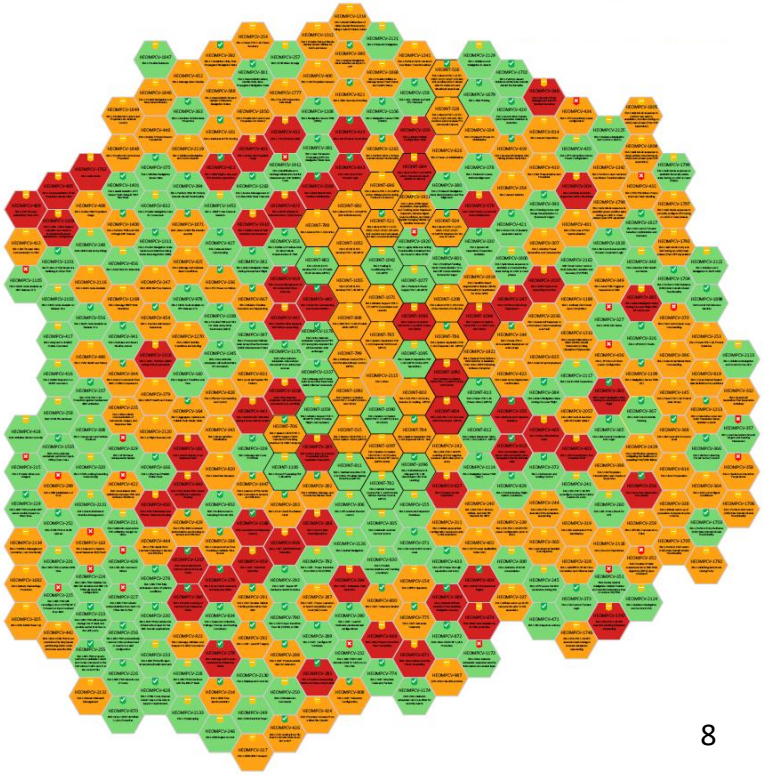
IV&V Program

- Orion IV&V was uncomfortable with the residual risk that would have resulted from the previous approach
- IV&V decided to make sure to analyze the highest risk mission capabilities regardless of their association to the entities
- IV&V now adds targeted assurance for specific capabilities and no longer focuses on everything within specific entities

Following the Risk

IV&V Program

- IV&V wanted to evaluate risk more dynamically, doing so much more frequently to match the changing risk landscape of the Orion Program
- Following the risk focuses the Orion IV&V team's effort on areas of highest concern – knowing their work will have an impact



Agile IV&V

IV&V Program

- To develop understanding of the Agile approach used by the Orion flight software developer, IV&V approached the Software Engineering Institute at Carnegie Mellon University
- IV&V learned Agile and Lean concepts that integrated logically with the Capability Based Assurance approach
- Agile IV&V is 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

Agile Principles

IV&V Program

- Retrospectives
- Small batch sizes of assurance work
- Fast integrated learning cycles
- Small self-organizing teams
- Frequent delivery
- Scrum / Scrumban
- Backlogs
- Daily stand-ups

Results

IV&V Program

- Communication improved in many areas
- The team embraced the continuous improvement mindset
- Orion IV&V changed delivery cadence from months to weeks
- Stakeholders were happy with the changes:
  - “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.”

Aspirations for Long Term

IV&V Program

- Build stronger team focus and increase collaboration among IV&V staff
- Improve the efficiency of IV&V analysis and delivery cycle
- Move toward greater synchronization with the development team
- Get comfortable with feeling uncomfortable
- Continue to add assurance and mitigate risk for Exploration Mission 1 and subsequent missions

Questions?

IV&V Program

Contact Information:

Justin Smith

NASA Independent Verification & Validation

Justin.L.Smith@nasa.gov

(681) 753-5217