



IV&V of Autonomy

The current approach, and looking to the future

Ken Costello

Gerek Whitman (Engility)

Special thanks to:

Rhonda Fitz (MPL)

Shirley Savarino (Engility)

Scott Starn (Engility)

The IV&V process, abstracted



Capability Based Assurance and Follow-the-Risk

CBA: Decompose mission into mission, system, and software capabilities that become the scope for IV&V analysis

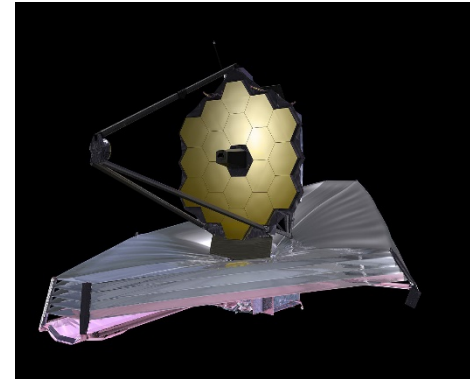
FTR: As understanding is gained, identify areas of risk or concern in order to inform prioritization of IV&V analysis and develop specific assurance objectives

Mission drivers for autonomy

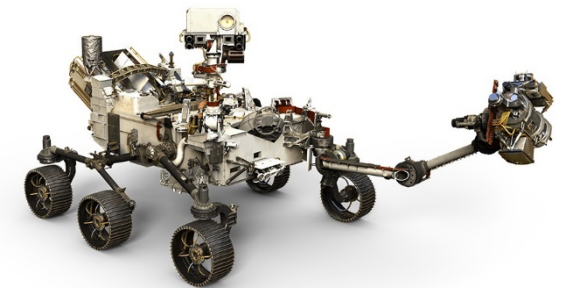
1. Communication constraints outgrow decision-making cadence
2. Time-critical decisions for control, health, or life support
3. Decisions can use rich on-board data
4. Local decisions could improve robustness & reduce complexity
5. Autonomy can reduce system cost or improve performance
6. Variability in training and proficiency is unacceptable in manual control

Missions supported by IV&V:

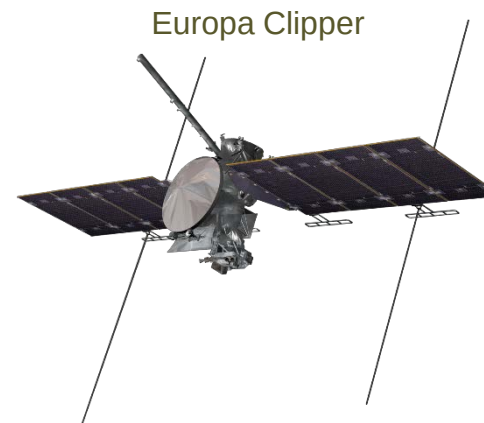
James Webb Space Telescope (JWST)



Mars 2020



Parker Solar Probe (PSP)



Identifying areas of autonomy risk

Functional

Requires understanding of mission goals and objectives

- What mission capabilities are supported by autonomy? Are they safety-critical?
- How does the autonomy capability make decisions?
- Are there cases in which it can make a bad decision?
- What are the mission conditions under which autonomous control is allowed?

JWST Example

- JWST requirement to operate for 4 weeks without ground intervention

Non-Functional

Requires understanding of system and software development

- How do the various parts of the autonomy architecture interact?
- What are the boundaries and constraints of allowed autonomous decisions?
- Can conflicting decisions collide?
- What is the interaction between humans and autonomy?

JWST Example

- Highly distributed JWST Fault Management (FM) architecture

Providing assurance for autonomy risks

- Assurance needs are developed from the identified risks and concerns
- Autonomy risks include increased system/software complexity (exploding state space), as well as multi-faceted, possibly non-deterministic, decision-making
- IV&V wants to assure that autonomous software used to perform mission- and safety-critical capabilities:
 1. Executes those capabilities as intended
 2. Does not introduce unwanted or unnecessary behaviors, and
 3. Responds appropriately to adverse conditions, including environments that are not well understood or difficult to model/simulate

JWST example

- IV&V wants to assure that the JWST software can operate autonomously over a period of 4 weeks while safely responding to any introduced faults
- IV&V wants to assure that any potential conflicts in JWST's distributed FM response behavior are not credible or appropriately mitigated

Identifying/developing tools and techniques

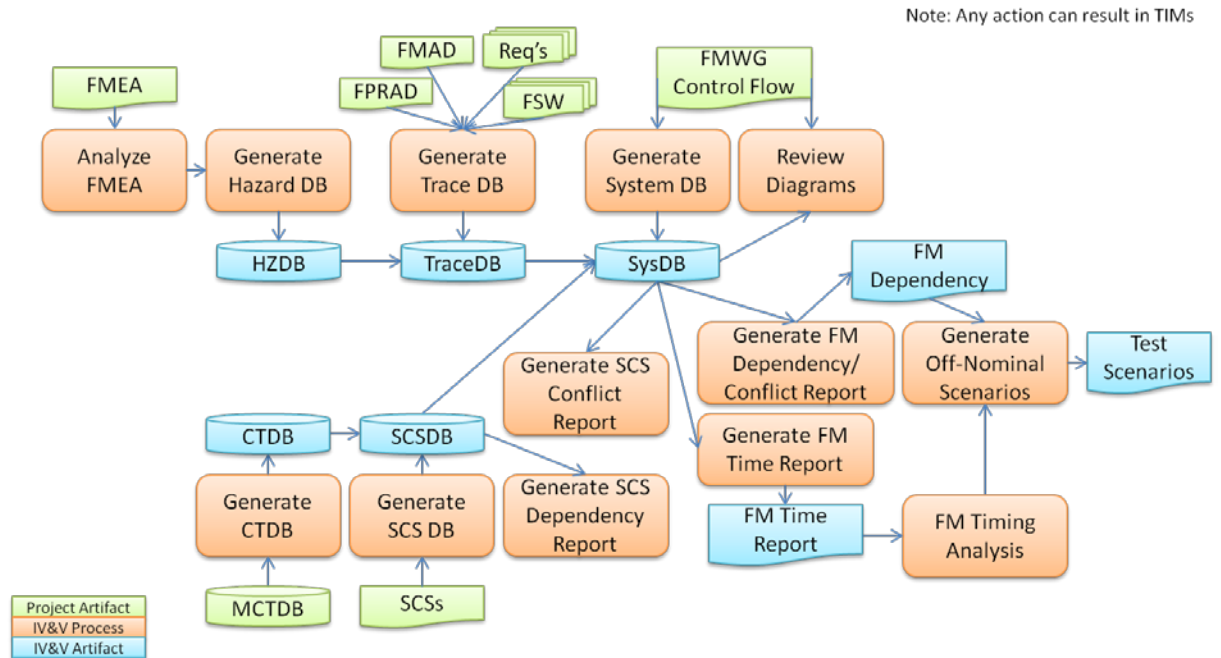
- Autonomous operations are often critical and require high rigor IV&V analysis to assure correct functionality
- Autonomy implementation almost always requires tailored work instructions for IV&V analysis to address non-functional considerations
- IV&V has a vast amount of experience to draw from in order to find the best way to get the evidence needed to address the identified risk
 - Catalog of Methods (COMPASS)
 - Adverse Condition Awareness Tool (ACAT)
 - Jon McBride Software Testing and Research Lab (J-STAR)
- When the tool or technique doesn't already exist, we create it or evolve it from an existing tool or technique

JWST autonomy assurance techniques

Long-duration testing in the JWST Integrated Simulation and Test (JIST) software-only simulator

Though developed by IV&V's J-STAR Lab, JIST was adopted by the JSWT developer to help mitigate test schedule risks

End-to-End FM verification through database development and analysis



The future of IV&V for autonomy

- High value, high risk NASA missions have thus far addressed the autonomy mission drivers with deterministic solutions
 - Complex and highly critical software functions operate using preloaded conditions to implement autonomy
 - IV&V efforts have therefore been ensuring that the autonomy software correctly and completely implements the desired capabilities without introducing emergent behaviors
- Future missions may use autonomy in a less deterministic manner, introducing more decision making (e.g. artificial intelligence) in the software
- Foreseen challenges:
 - Characterization of the environment has less certainty, with the software responding to environmental challenges (e.g. routing around an obstruction in a rover's path)
 - Use of Monte Carlo simulation and automated testing to exercise the full operational space
 - IV&V is heavily dependent on artifacts – what will future autonomy artifacts look like?
 - Achieving configuration management of self-modifying autonomous systems
 - The ability for IV&V to crack open the autonomous decision-making software and make it visible, understandable, and testable for IV&V analysts
 - Understanding the competing agendas in autonomous decision-making software
 - Autonomous systems will probably necessitate more validation methods as opposed to verification – what validation will be done by developers to assure their systems, and how does IV&V maintain independence?