U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND AVIATION & MISSILE CENTER

"Architecture Centric Virtual Integration Process (ACVIP) Overview"

for the 2022 ACVIP/Architecture Analysis & Design Language (AADL) User Day

Alex Boydston
FARA Program
Avionics/Software Engineer
US Army DEVCOM AvMC TDD-A

Tyler Smith
Program Manager/
Principle Investigator
Adventium Labs

Sholom Cohen
Program Manager/
Technical Lead
CMU SEI

02 June 2022

AGENDA

- **ACVIP Overview and Background – Alex Boydston – 10 minutes**
- **ACVIP Acquisition Management Guidance and the Open Source AADL Tool Environment (OSATE) – Sholom Cohen – 20 minutes**
- **ACVIP Modeling & Analysis Process and Curated Access to Model-based Engineering Tools (CAMET) – Tyler Smith – 20 minutes**

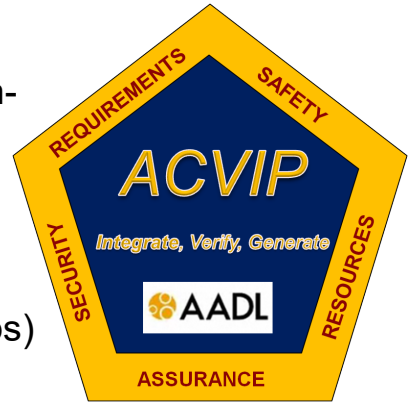
ACVIP Overview and Background

Alex Boydston, MSEE

Future Attack Reconnaissance Aircraft (FARA) Avionics & Software Engineer
US Army Development Command Aviation & Missile Center (DEVCOM AvMC)
Technology Development Directorate for Aviation (TDD-A)

ARCHITECTURE CENTRIC VIRTUAL INTEGRATION PROCESS (ACVIP) OVERVIEW

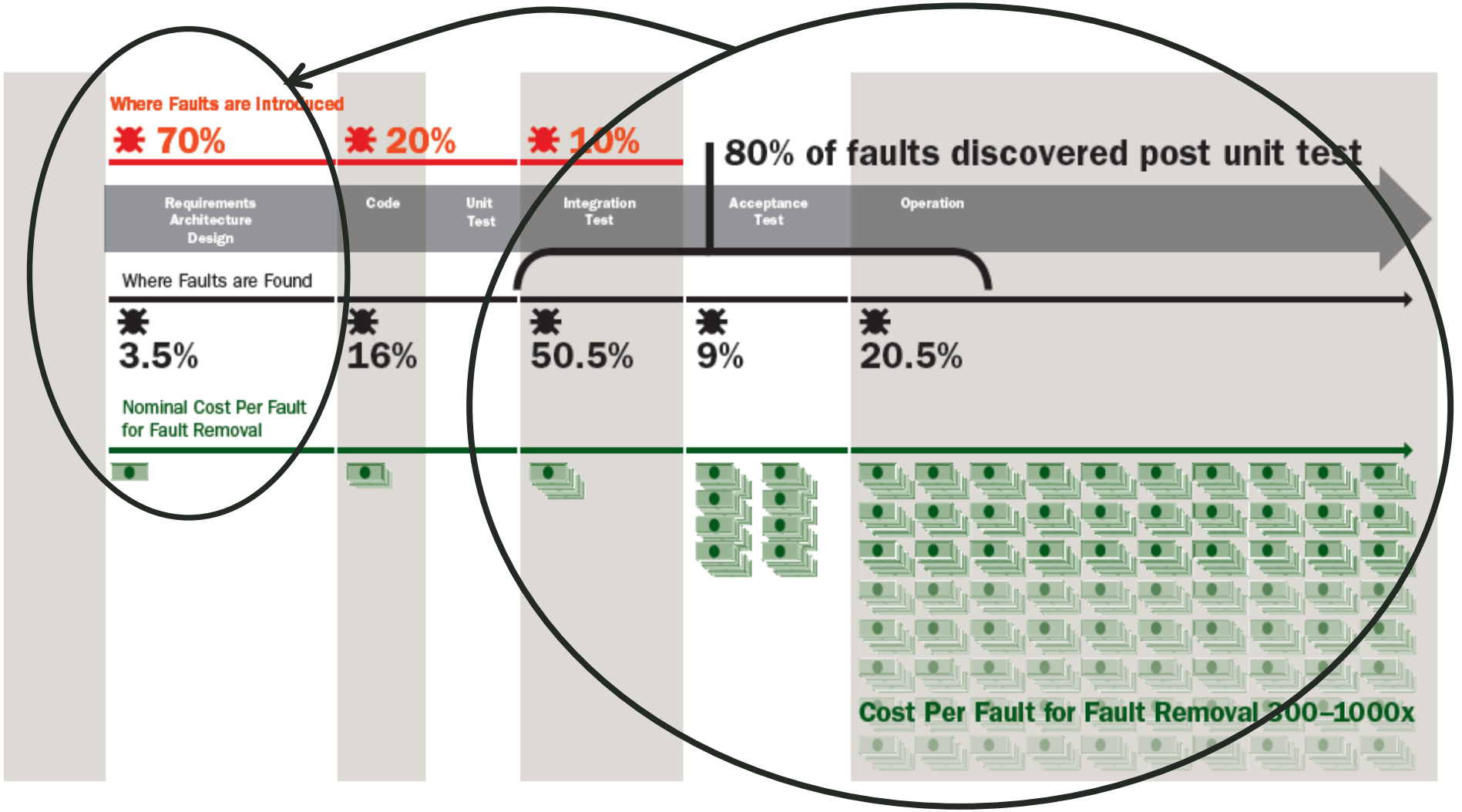
- **ACVIP addresses architectures for complex software-intensive embedded computing systems**
  - Engineers apply ACVIP during development and sustainment of these systems to reduce implementation and integration risks.
  - ACVIP provides the methods and tools to address system development where run-time sensitivity, safety, and cybersecurity are critical



- **ACVIP provides a virtual integration environment for early detection of defects not typically found until much later. This is accomplished using:**
  - Continuous verification throughout the development lifecycle (supports DevSecOps)
  - A consistent representation of the system by coordinating multiple models, languages, engineering domains, and design entities
  - The Architecture Analysis & Design Language (AADL)

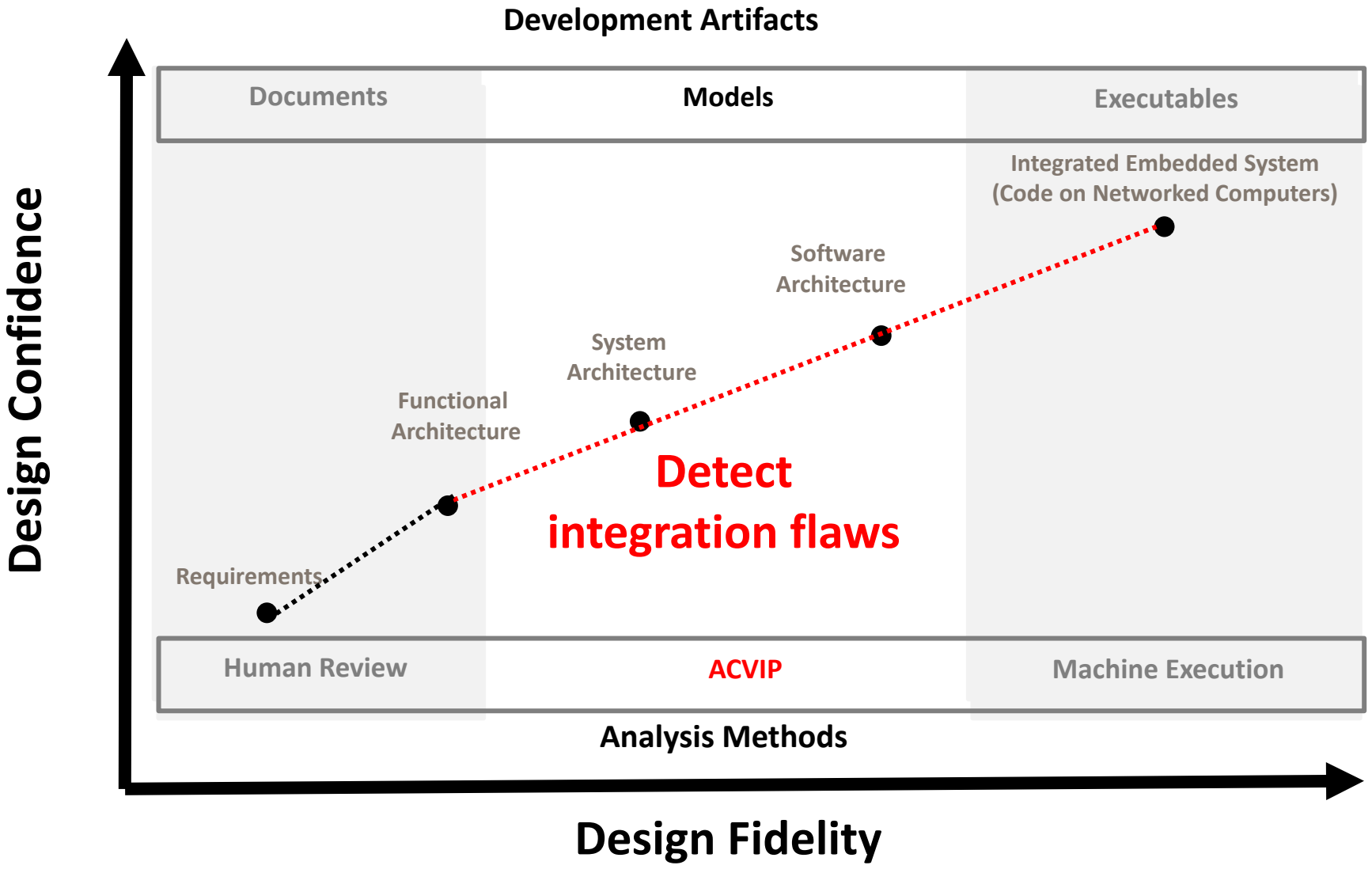
- **If the contractor performers do not take measures to make an early and iterative detection of software and hardware integration issues, then this will lead to expensive software rework costs as has been experienced on other prominent ACAT I programs**
  - For example, the recent GAO report (ref. gao-22-105128) on the F-35 Block 4 noted that 23% of the software defects were not found until flight test, there were still 11 unresolved flight safety critical issues, and over 800 unresolved other issues
  - The prior F-35 GAO report noted that the program schedule had slipped as much as 5 years as a result of the software integration issues

ACVIP ANALYSIS FINDS INTEGRATION PROBLEMS EARLY, WHEN LEAST EXPENSIVE TO FIX

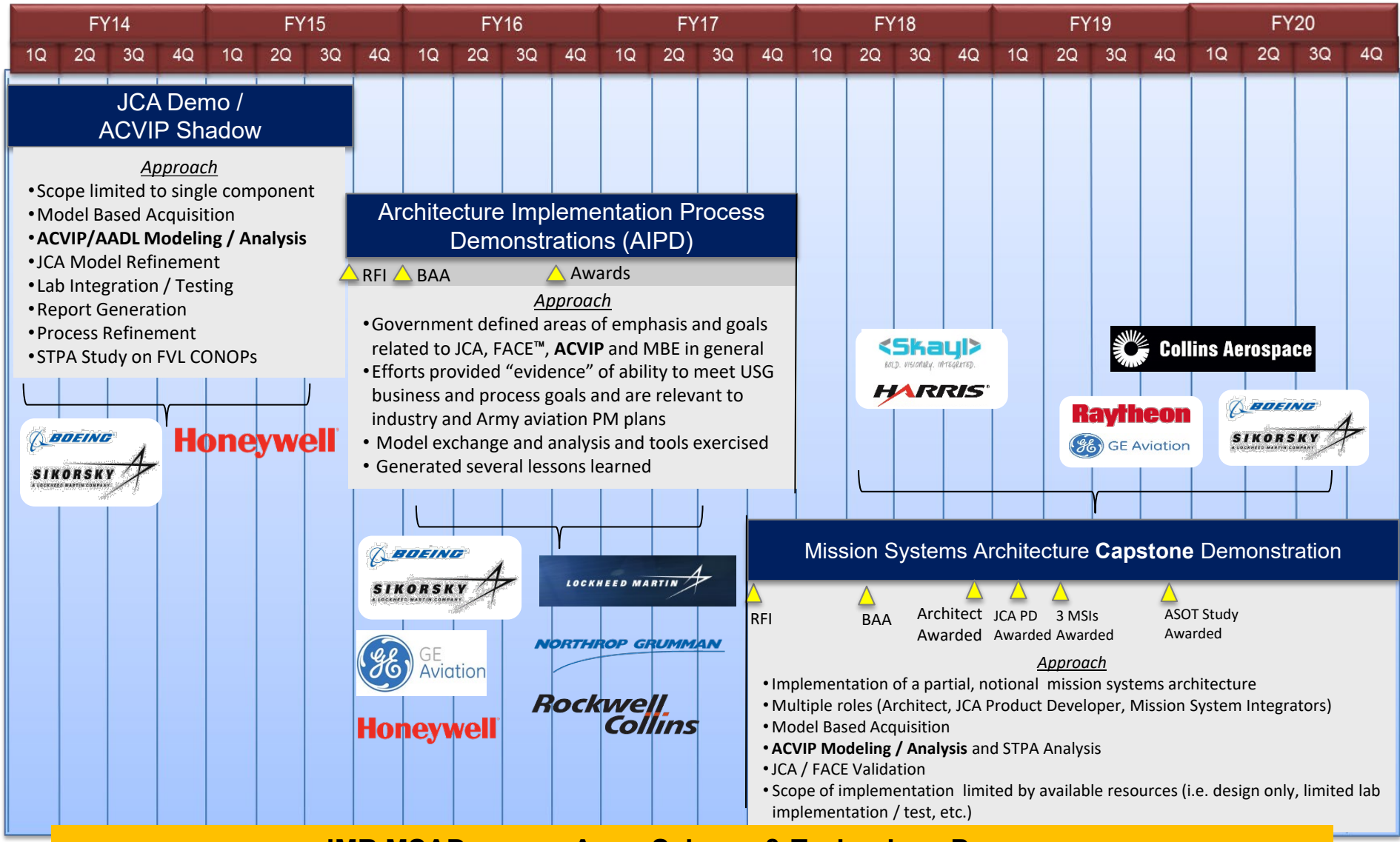


Goal: Find faults earlier through virtual integration, when significantly cheaper to fix

ACVIP INCREASES DESIGN CONFIDENCE



ACVIP PROCESS AND TOOLS WERE EXERCISED AND MATURED OVER JOINT MULTI-ROLE S&T PROGRAM



JMR MSAD was an Army Science & Technology Program of three increasingly complex software integration demonstrations.

ACVIP and AADL is Matured and Proven

The tools and process were exercised in Science & Technology Demonstrations

- ACVIP tools and process were developed, exercised and matured over the multi - year Joint Multi-Role Architecture Demonstration (JMR MSAD) 6.3 S&T Program for Future Vertical Lift (FVL)

- Evidence was achieved showing that ACVIP
  - ❑ Identified issues early (e.g., JCA Demo uncovered > 80 issues before integration)
  - ❑ MBSE & ACVIP reduced overall cost (e.g., 3x upfront effort reducing issues by 10x on AIPD, 30% reduction in integration on Capstone Demo)
  - ❑ Enabled an automated Continuous Virtual Integration approach supporting Agile
  - ❑ Is an integral part of an overarching Authoritative Source of Truth

- As a result of JMR MSAD, ACVIP guidance, training and requirements now exists in the FVL Architecture Framework (FAF)
  - ❑ Both FVL Programs (FARA and FLRAA) have requirements for ACVIP in the Statements of Work (SOW) and Systems Engineering Plans (SEPs)
  - ❑ The performer contractors are preparing to use ACVIP

ACVIP was created in anticipation of FVL and is transitioning as a requirement to FVL Programs

ACVIP Acquisition Management Guidance and the Open Source AADL Tool Environment (OSATE)

Sholom Cohen

Program Manager and Technical Lead

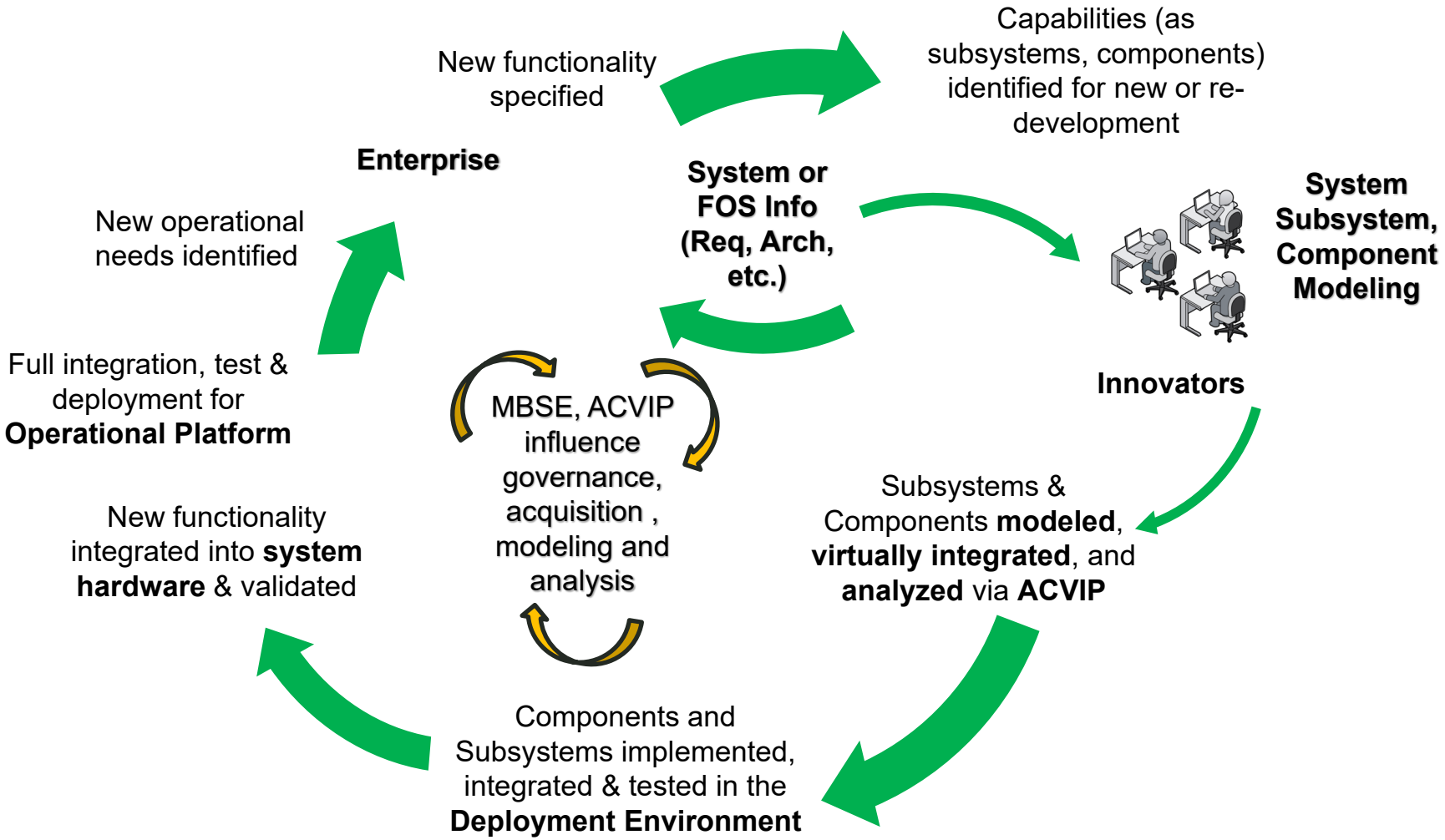
Carnegie Mellon University Software Engineering Institute

ACVIP RESEARCH, APPLICATION, AND IMPACT

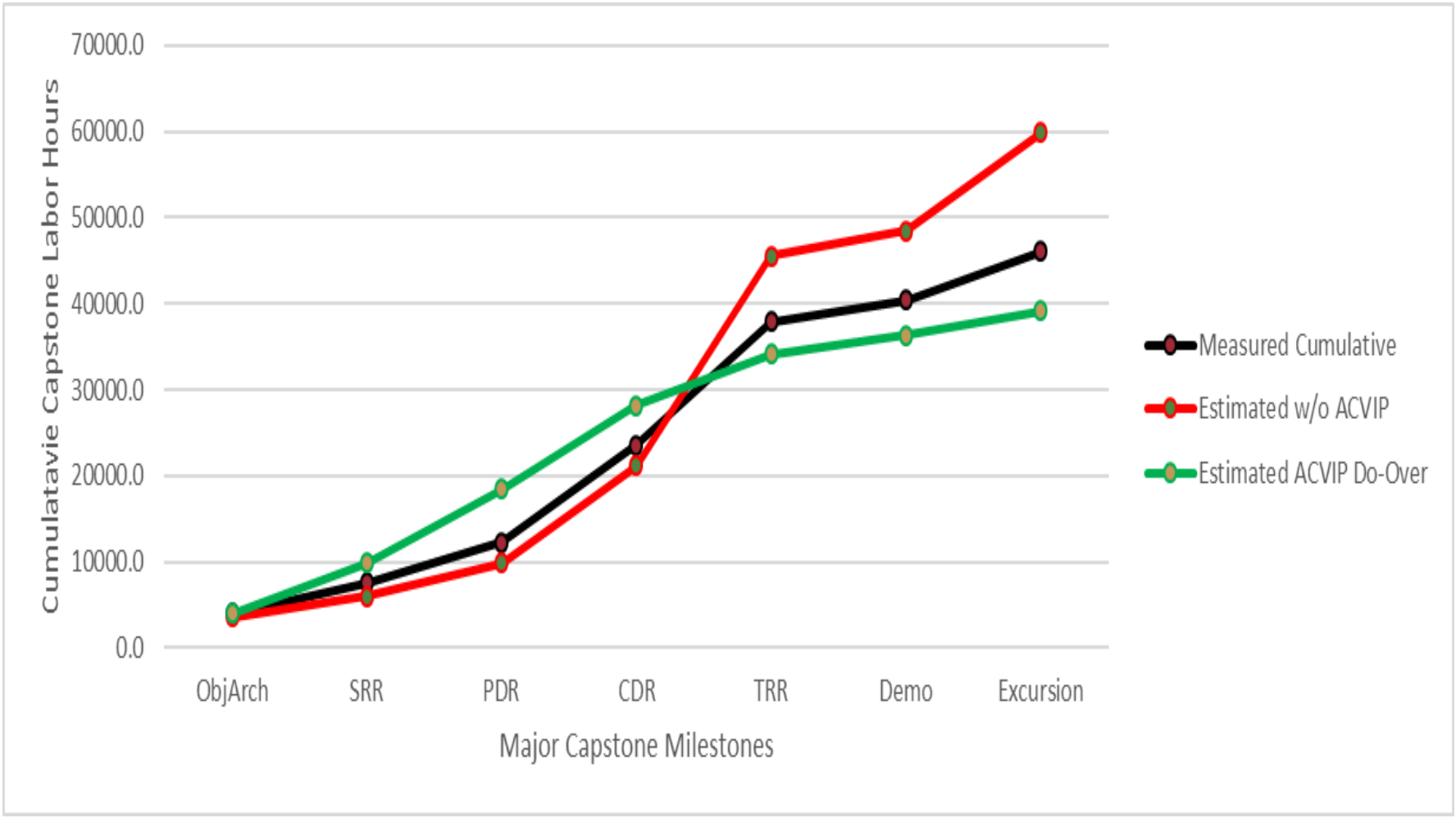
- July 2019, Dan Bailey, PM FARA Competitive Prototype, asks what must be accomplished to “get ACVIP on FARA Contract”

- SEI response:
  - Developed and matured tools and techniques in support of ACVIP for embedded computing systems software modeling with analysis
  - Integrated ACVIP into MBSE framework for Army Digital Engineering Transformation
  - Applied initiatives to provide proof-of-concept and prototype development to TRL-6 in multi-year SBIR and science & technology
  - Transitioned documentation, modeling, and tool support to acquisition, engineering, and operations for Major Army Acquisition

ROLE OF ACVIP IN ACQUISITIONS



ACVIP IMPACT REPORTED BY CAPSTONE MSI CONTRACTOR



CURRENT RESEARCH AND TRANSITION DIRECTION

- Integrate ACVIP and modeling with analysis into DoD digital transformation activities including MOSA, DEVOPS, Agile and other approaches
- Integrate with large scale acquisition and development programs
- Develop plan for applying ACVIP in new and emerging workflows and toolchains
- Apply modeling with analysis to product line development to achieve systematic reuse and other MOSA objectives
- OSATE maturation
  - Address new AADL standards
  - Improved graphics capabilities
  - New and validated introductory examples
  - Totally reworked analysis tools

WORKING WITH THE SEI

- Understanding our technology
  - Publications that document ACVIP for Digital Engineering transformation of acquisition and development
  - Acquisition Handbook (including generic ACVIP Plan and ACVIP Management Plan)

- Using our technology
  - Open-source tools, examples and case studies for download
  - Introductory webinars and examples
  - Web-based training

- Digital Engineering Transformation support

- Contact: Matt Milazzo mdmilazzo@sei.cmu.edu

Curated Access to Model-based Engineering Tools (CAMET) Base Pack

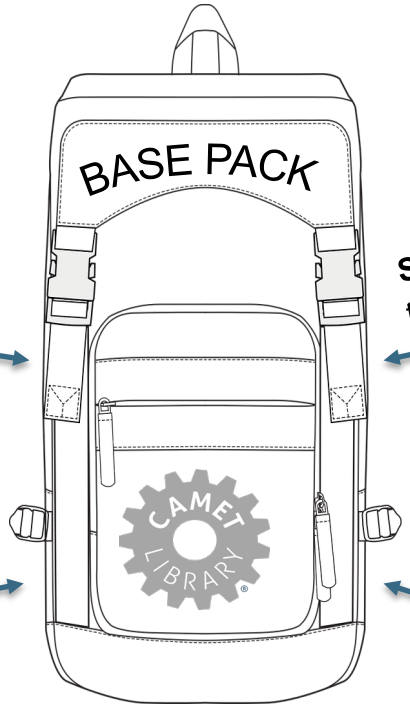
Five core tools for virtual integration and analysis with AADL

Tyler Smith

Program Manager and Principal Investigator

Adventium Labs

CAMET BASE PACK



Scheduling

FASTAR provides timing analysis

SysML to AADL Bridge translates models to AADL

Bridge to SysML

Domain Separation

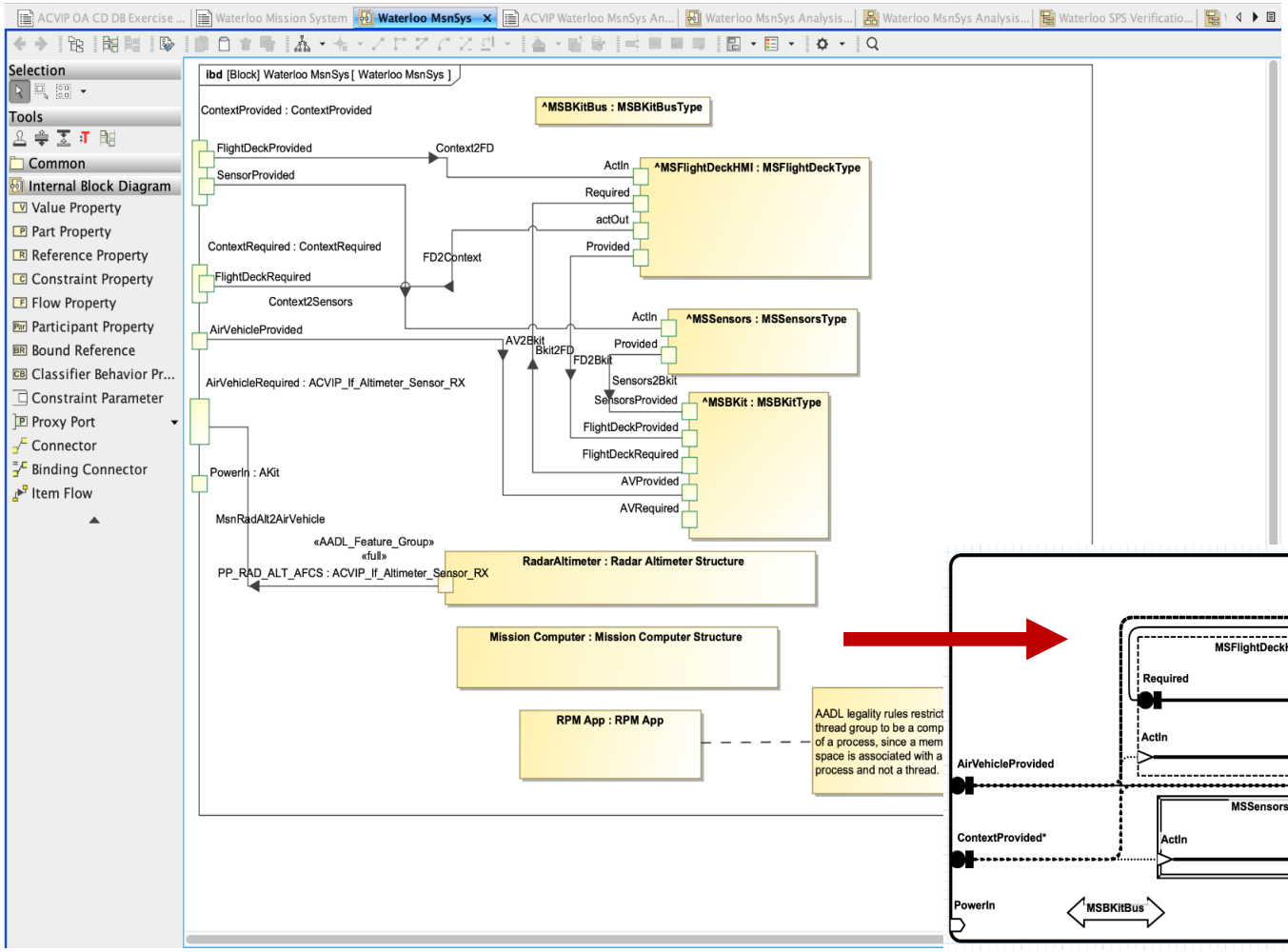
MADS assesses domain isolation

MILS and **RMF** report cybersecurity errors

Cybersecurity

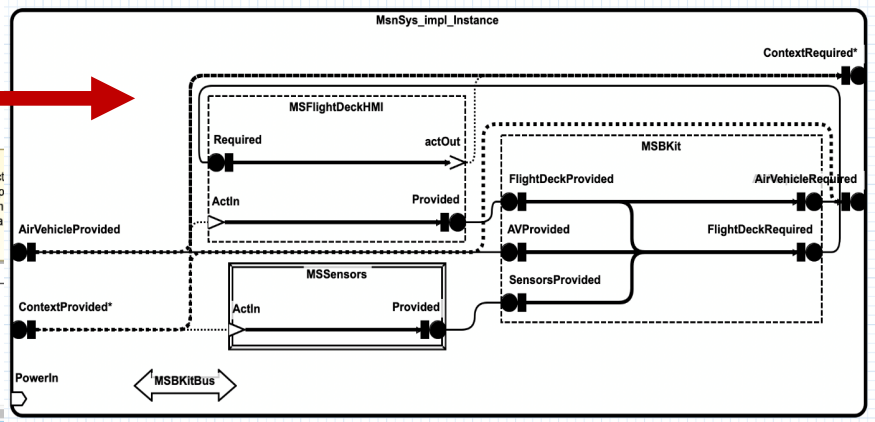
SYSML-TO-AADL BRIDGE (TRL 7)

SysML Model



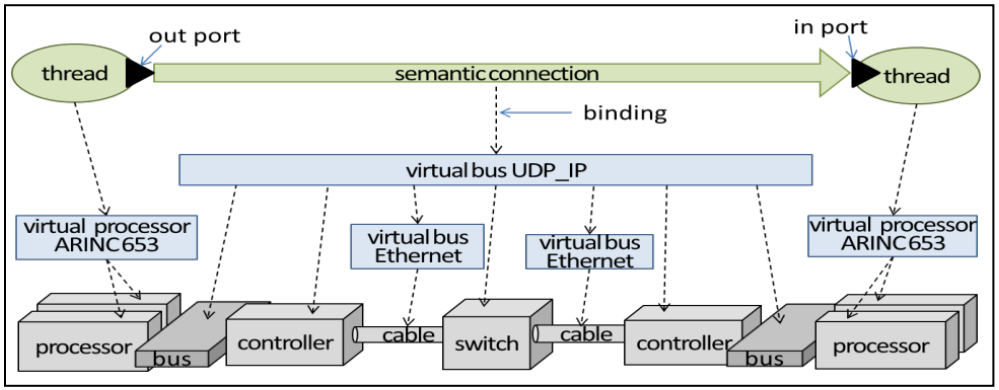
- MagicDraw/CAMEO
- Sparx Enterprise Architect

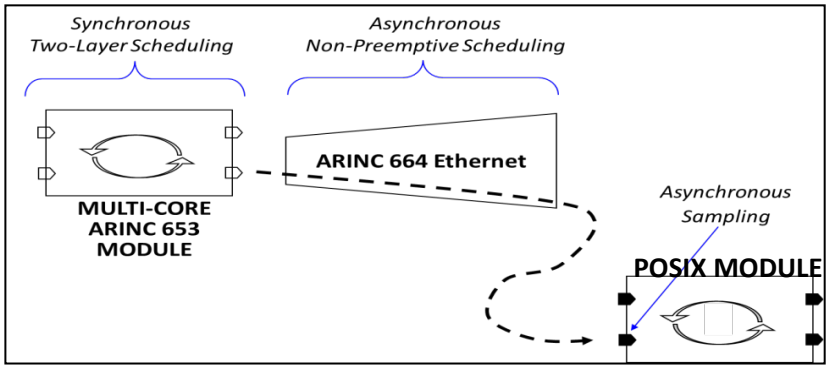
AADL Model



Included SysML Profiles enable virtual integration studies such as real-time performance, security, and safety.

FASTAR TIMING ANALYSIS AND SCHEDULE GENERATION (TRL 6)



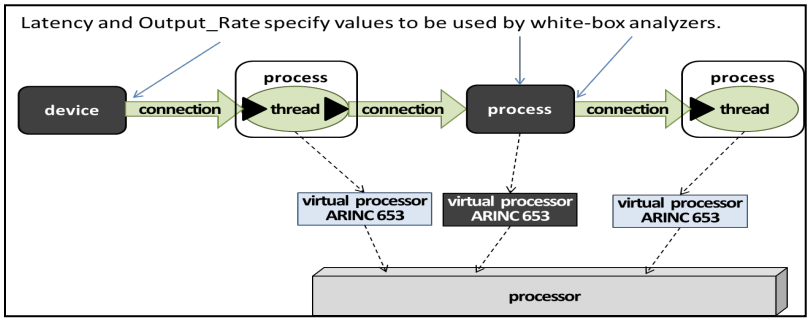


Layered Architectures

- Resource utilization analysis
- Latency and deadline analysis
- Blackbox & RMS timing analysis

Heterogeneous Architectures

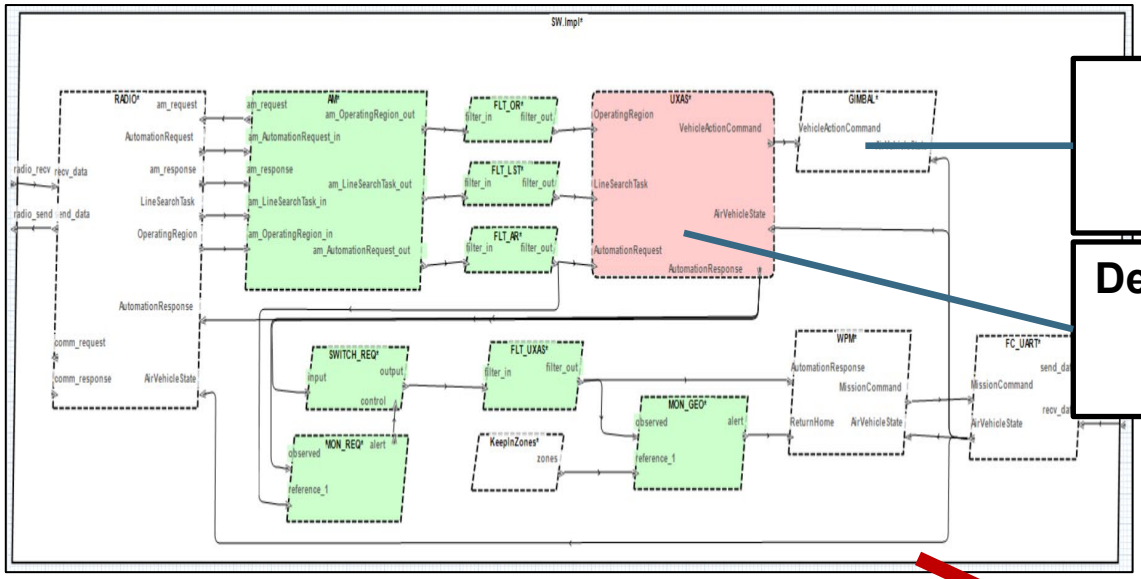
- Generate ARINC 653 schedule
- Framework can be extended with other analyzers & schedule generators



Mixed Fidelity Models

FASTAR analyzes resource needs and timing behaviors of complex, integrated system architecture models as they evolve through multiple development phases.

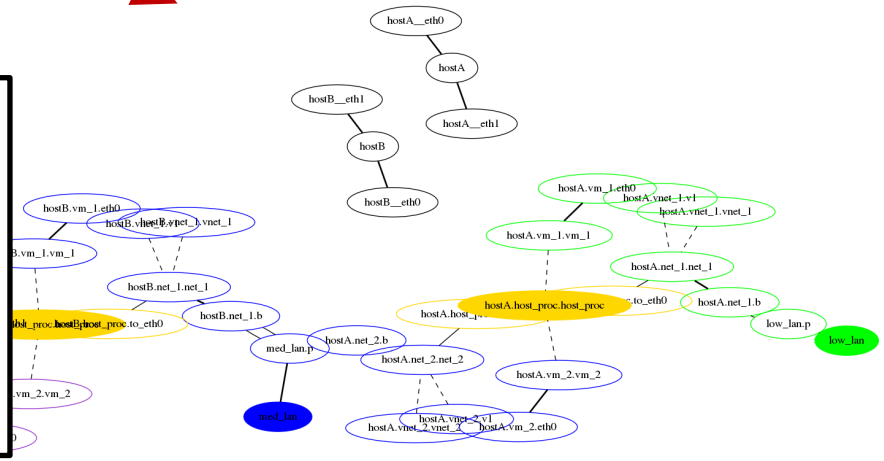
MULTIPLE INDEPENDENT LEVELS OF SECURITY (MILS) ANALYSIS (TRL 6)



Assign Security Levels to the system's hardware and software components

Designate which system components should represent Cross-Domain Solutions (CDS)

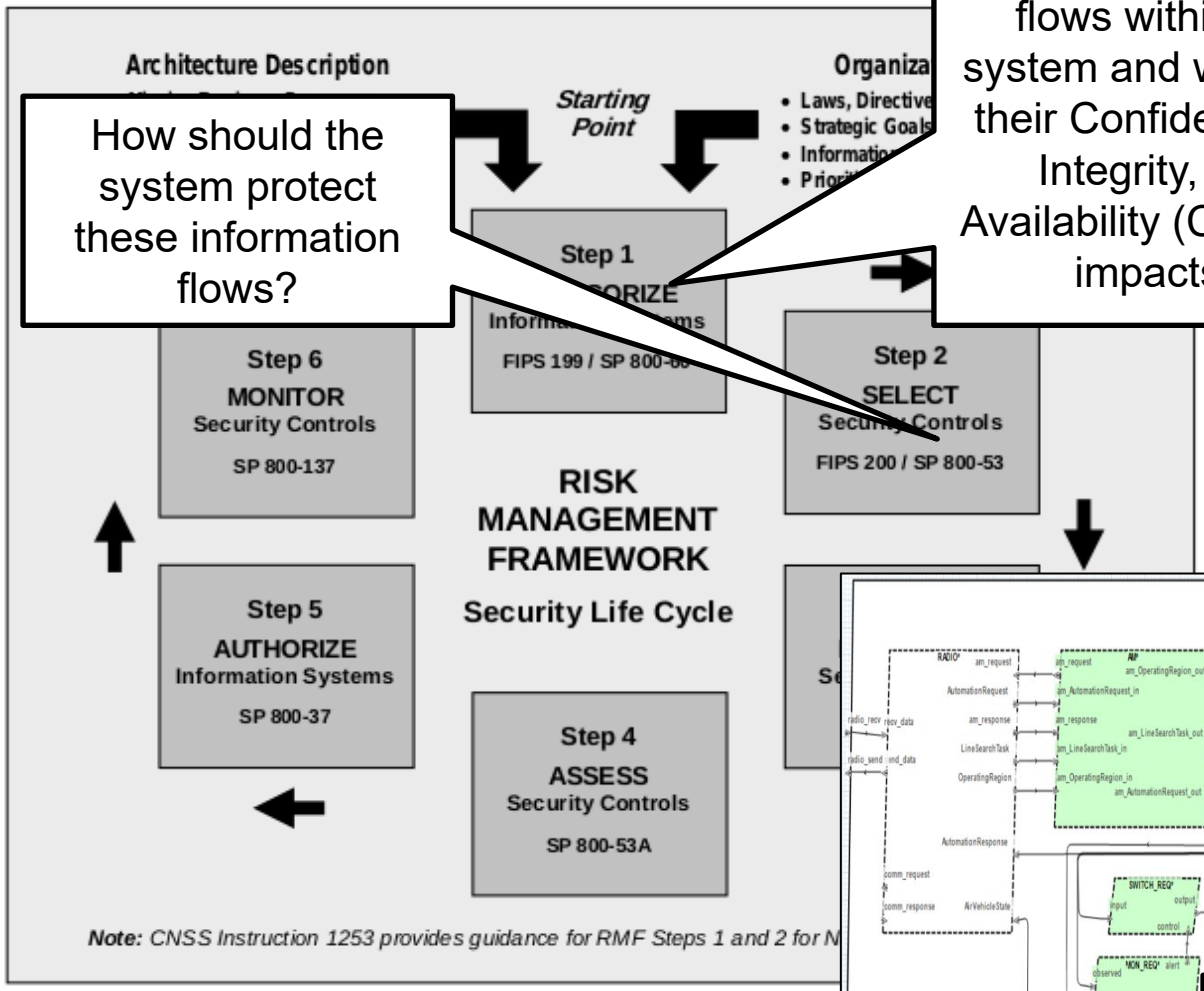
Analysis identifies if architecture hierarchy and hardware/software bindings violate security separation or if additional CDS components are necessary.



RISK MANAGEMENT FRAMEWORK (RMF) ANALYSIS (TRL 6)

What are the sensitive information flows within the system and what are their Confidentiality, Integrity, and Availability (CIA) loss impacts?

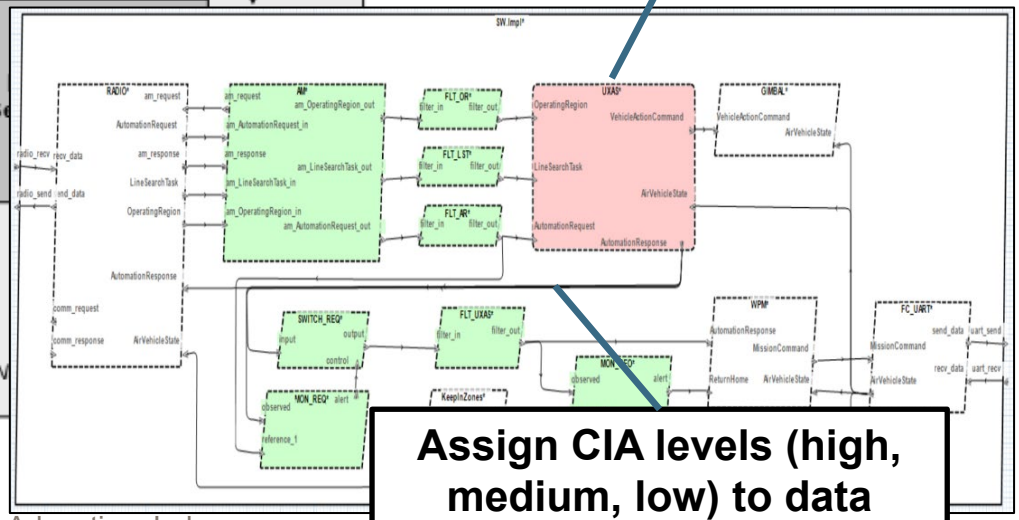
How should the system protect these information flows?



NIST Special Publication 800-37

Assign RMF controls to system components.

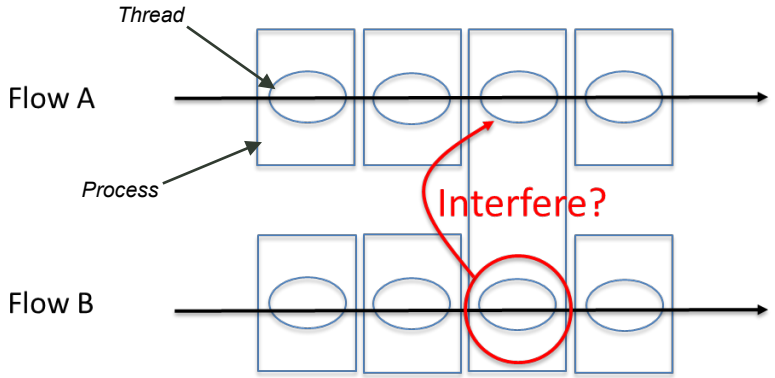
System Model



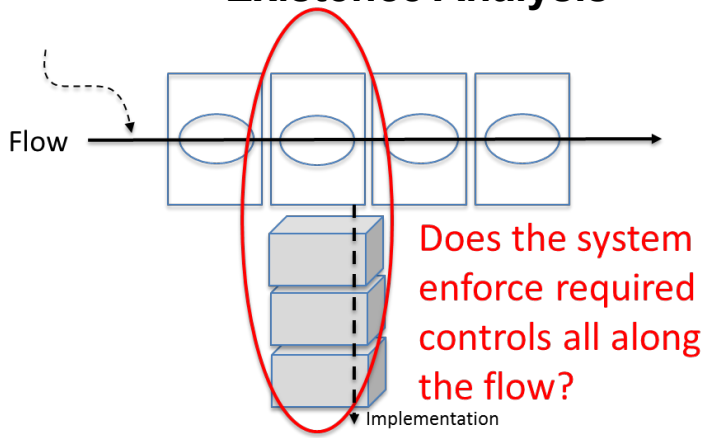
Assign CIA levels (high, medium, low) to data flows

RMF DATA FLOW ANALYSIS (TRL 6)

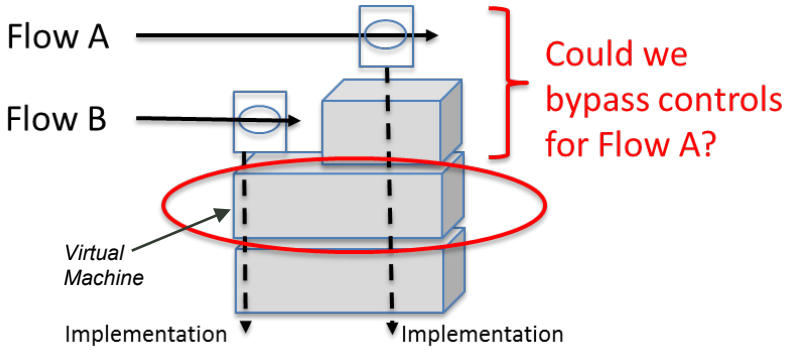
Mixed Criticality Analysis



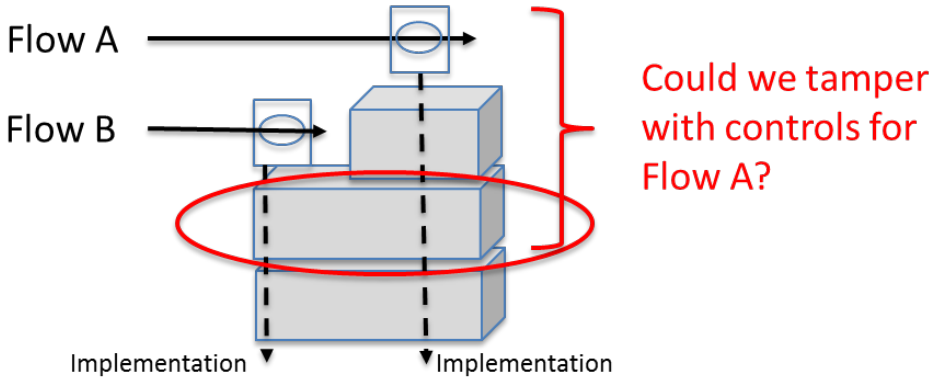
Existence Analysis



Non-Bypassability Analysis



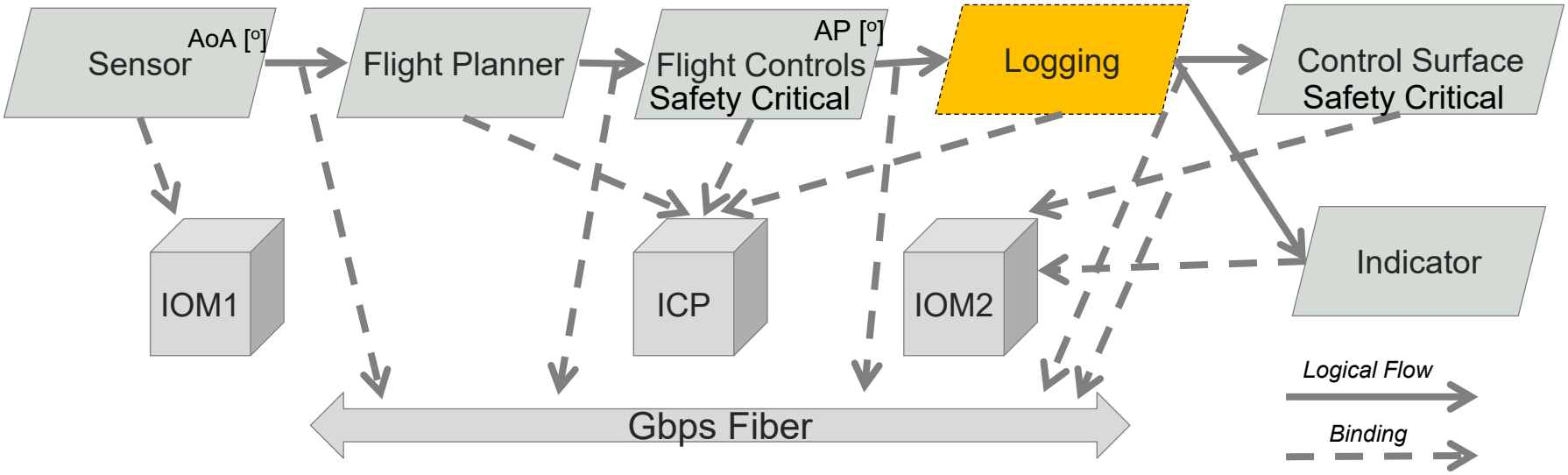
Tamper-Resistance Analysis



RMF Analysis indicates if any of the system data flows violate the controls put in place.

MULTIPLE ANALYSIS FOR DOMAIN SEPARATION (MADS) (TRL 5)

Consider information flow CA1 from Logging to control surface – risk of **integrity loss**:

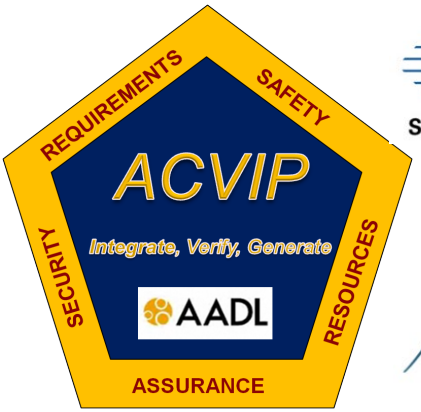


- Assume Logging is low safety criticality, no confidentiality, therefore comparatively low certification criteria
- Why is it allowed to participate in a critical information flow? This is a design error.
- Can it be on the same processor as the safety critical Flight Controls?

MADS Domain Separation Analysis detects invalid domain combinations

BACKUP CHARTS

ACVIP GUIDANCE & TOOLS MATURED DURING JMR



Software Engineering Institute

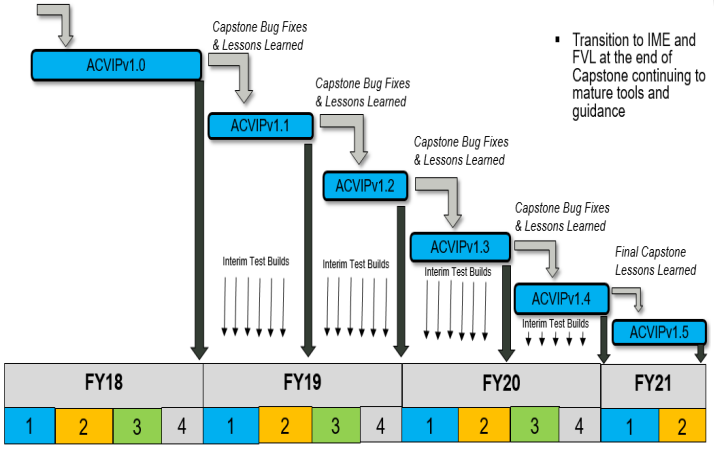
Adventium LABS

ACVIP VERSIONING RELEASE PLAN 2018-2021

- Biyearly Updates to:
  - OSATE & Plugin Tools by SEI & Adventium
  - ACVIP Handbooks

Note: Not all items get updated with each release

- Interim Test Builds will be available to address issues discovered during Capstone
- Transition to IME and FVL at the end of Capstone continuing to mature tools and guidance



AADL Based Tools Available for Capstone Demo

- Open Source AADL Tool Environment (OSATE)
- AADL Template for Analysis Requirements
- Architecture Led Integrated System Assurance (ALISA)
- Architecture Topology Analysis
- ARINC 653 Analysis & Generation Tools
- Behavior Analysis
- Computer Resource Analysis
- Continuous Virtual Integration Test
- Functional Integration Analysis
- Model Based Testing
- Security Analysis (MILS, RMF)
- Safety Analysis Support (MIL-STD-882, SAE ARP 4761 & STPA)
- Structural, Compositional and Formal Method Analyses
- System of Systems Simulation
- Translators and Translation Guidance (FACE-AADL, SysML-AADL)
- Timing, Latency and Scheduling Analysis

Plus new tools from multiple Sources:
* SBIRs
* DARPA
* Europe
* etc..

https://osate.org

https://www.adventiumlabs.com/our-work/products-services/model-based-engineering-mbe-tools

SAE INTERNATIONAL AADL Tool Expos

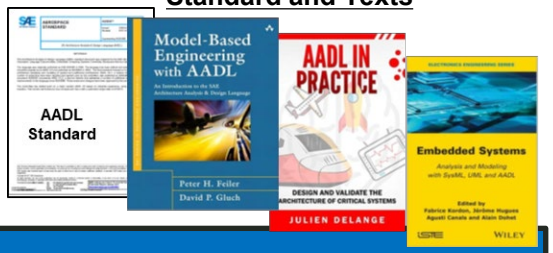
https://resources.sei.cmu.edu/news-events/events/aadl-user-day/

ACVIP/AADL Handbooks, Papers, Training and Texts

Handbooks & Papers

- Overview
- Modeling & Analysis
- OSD DEWG Overview
- Acquisition Management

Standard and Texts



Training

- https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V40
- https://www.adventiumlabs.com/our-work/products-services/acvip-training

ACVIP guidance and tools have been exercised, evaluated and matured on JMR MSAD to support legacy and future aviation systems

PRESENTATION ABSTRACT

The Architecture Centric Virtual Integration Process (ACVIP) addresses architectures for complex software-intensive embedded computing systems. Engineers apply ACVIP during development and sustainment of these systems to reduce implementation and integration risks. ACVIP leverages the Architecture Analysis and Design Language (AADL) to capture core design elements as a collection of models and a variety of analysis tools to detect integration errors and collect evidence the system meets key performance, safety, and security objectives. ACVIP is a part of the US Army S&T effort in preparation for the Future Vertical Lift (FVL) programs. Based on results from Army ACVIP research, ACVIP promises improved affordability, quicker time to field, improved adaptation to new mission scenarios, and opportunities for systematic reuse. In this talk the Army, the SEI, and Adventium Labs will introduce key ACVIP references, products, and support services: the ACVIP Acquisition handbook, the ACVIP Modeling handbook, ACVIP examples, and tool support through OSATE (by SEI) and CAMET (by Adventium Labs) along with in-class and online training material.

ACRONYMS

AADL	Architecture Analysis & Design Language
ACVIP	Architecture Centric Virtual Integration Process
AIPD	Architecture Implementation Process Demonstrations
ASOT	Authoritative Source of Truth
AvMC	Aviation and Missile Center
CAMET	Curated Access to MBE Tools
CDR	Critical Design Review
CDS	Cross Domain Solution
CIA	Confidentiality, Integrity and Availability
CMU	Carnegie Mellon University
CONOPs	Concept of Operations
DEVCOM	Development Command
DevSecOps	Development, Security and Operations
FACE	Future Airborne Capability Environment
FARA	Future Attack Reconnaissance Aircraft
FASTAR	Framework for Analysis of Scheduling, Timing and Resources
FLRAA	Future Long Range Assault Aircraft
FoS	Family of Systems
GAO	Government Accounting Office
GE	General Electric
JCA	Joint Common Architecture
JMR	Joint Multi-Role
MADS	Multiple Analysis for Domain Separation
MBE	Model Based Engineering
MBSE	Model Based Systems Engineering
MILS	Multiple Independent Levels of Security
MOSA	Modular Open Systems Approach
MSAD	Mission Systems Architecture Demonstrations
MSI	Mission System Integrator
NIST	National Institute of Science and Technology
OSATE	Open Source AADL Tool Environment
PDR	Preliminary Design Review
PM	Program Management
RMF	Risk Management Framework
RMS	Rate Monotonic Scheduling
SBIR	Small Business Innovative Research
SEI	Software Engineering Institute
STPA	System Theoretic Process Analysis
SysML	Systems Modeling Language
TDD-A	Technology Development Directorate for Aviation
TRL	Technology Readiness Level
TRR	Test Readiness Review
TS	Transport Services
US	United States
USG	US Government