“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

DISTRIBUTION STATEMENT A:
Approved for public release; distribution is unlimited.
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)
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

<table>
<thead>
<tr>
<th>Where Faults are Introduced</th>
<th>Requirements</th>
<th>Architecture</th>
<th>Design</th>
<th>Code</th>
<th>Unit Test</th>
<th>Integration Test</th>
<th>Acceptance Test</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>70%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where Faults are Found</th>
<th>Requirements</th>
<th>Architecture</th>
<th>Design</th>
<th>Code</th>
<th>Unit Test</th>
<th>Integration Test</th>
<th>Acceptance Test</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50.5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

80% of faults discovered post unit test

Nominal Cost Per Fault for Fault Removal

Cost Per Fault for Fault Removal 300-1000x

Goal: Find faults earlier through virtual integration, when significantly cheaper to fix
ACVIP INCREASES DESIGN CONFIDENCE

Development Artifacts

- Documents
- Models
- Executables

- Integrated Embedded System (Code on Networked Computers)
- Software Architecture
- System Architecture
- Functional Architecture
- Requirements

Analysis Methods

- Human Review
- ACVIP
- Machine Execution

Detect integration flaws

ACVIP

Design Fidelity

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.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
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
Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM22-0466
• 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

New operational needs identified

Full integration, test & deployment for Operational Platform

New functionality specified

System or FOS Info (Req, Arch, etc.)

System, Subsystem, Component Modeling

Innovators

Subsystems & Components modeled, virtually integrated, and analyzed via ACVIP

MBSE, ACVIP influence governance, acquisition, modeling and analysis

Components and Subsystems implemented, integrated & tested in the Deployment Environment

New functionality integrated into system hardware & validated

Enterprise
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 (CAMEET) Base Pack
Five core tools for virtual integration and analysis with AADL

Tyler Smith
Program Manager and Principal Investigator
Adventium Labs
CAMEX BASE PACK

**FASTAR** provides timing analysis

**MADS** assesses domain isolation

SysML to AADL Bridge translates models to AADL

Bridge to SysML

MILS and RMF report cybersecurity errors

Cybersecurity

Scheduling

Domain Separation

Copyright 2022 Adventium Labs
SYSML-TO-AADL BRIDGE (TRL 7)

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

- MagicDraw/CAMEO
- Sparx Enterprise Architect

Copyright 2022 Adventium Labs
FASTAR Timing Analysis and Schedule Generation (TRL 6)

Mixed Fidelity Models

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

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

Copyright 2022 Adventium Labs

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
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.

Copyright 2022 Adventium Labs

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
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?

Assign RMF controls to system components.

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

NIST Special Publication 800-37

Copyright 2022 Adventium Labs
RMF DATA FLOW ANALYSIS (TRL 6)

Mixed Criticality Analysis

Existence Analysis

Does the system enforce required controls all along the flow?

Non-Bypassability Analysis

Could we bypass controls for Flow A?

Tamper-Resistance Analysis

Could we tamper with controls for Flow A?

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

Copyright 2022 Adventium Labs
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

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

ACVIP/AADL Handbooks, Papers, Training and Texts

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

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