AADL is an Integration Focal Point

Adventium Labs

Aviation Development Directorate-Eustis Contract Number: W911W6-17-D-0003

This material is based upon work supported by the U.S. Army Combat Capabilities Development Command Aviation & Missile Center Aviation Development Directorate - Eustis under contract no. W911W6-17-D-0003. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of U.S. Army Combat Capabilities Development Command Aviation & Missile Center Aviation Development Directorate - Eustis.

tyler.smith@adventiumlabs.com camet-library.com

The Problem

Teams working on a safety critical systems often encounter challenges working together.

Different stakeholders have different

- Tools
- Workflows
- Standard practices
- Viewpoints

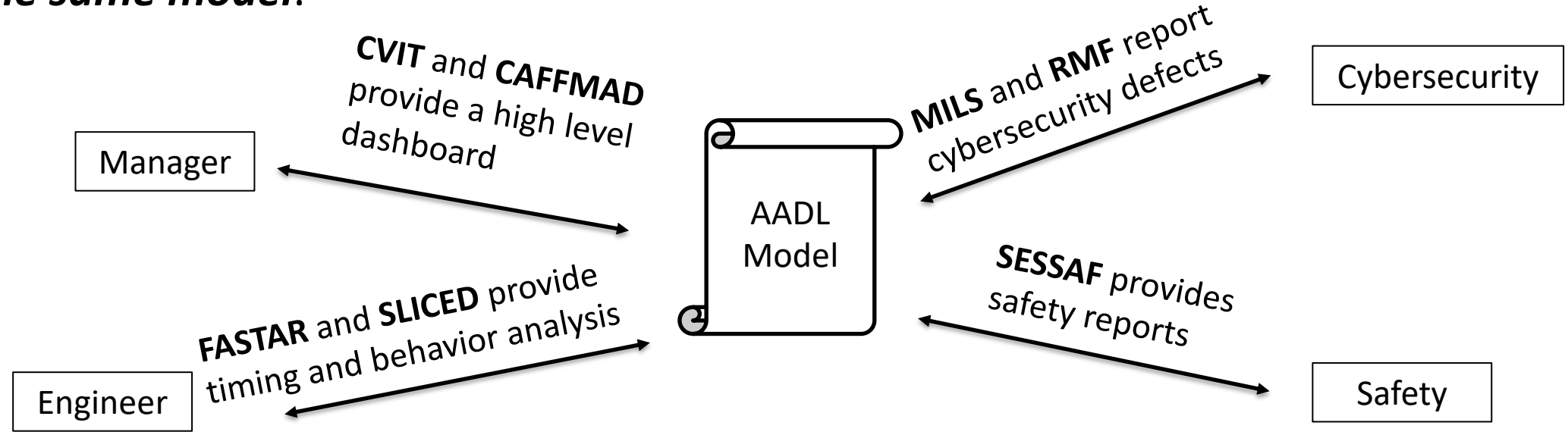
The result is often

- Duplicated information
- Degraded information quality
- Slow development iterations

The Solution

AADL is an **integration focal point** that brings embedded systems stakeholders together

- Adventium Labs builds tools that bring stakeholders together by leveraging AADL.
- With Adventium's CAMET library tools, Managers, Engineers, and Reviewers all use ***the same model***.



AADL is the Optimal Integration Focal Point

- It is not **vendor locked -** AADL models written in one tool will work in other AADL environments
- It is human **readable**
- It is designed to help identify **integration** issues in cyber-physical systems
- It enables **portable** analyses on the **compositional** architectures
- It is a **well defined** language for description and analysis of real time systems

CAMET Tools

The tools in Adventium's CAMET Library enable use of AADL as an integration focal point for multiple stakeholders.

- **SESSAF** brings systems engineers and safety analysts together around common AADL models.
- **MILS** and **RMF** ease coordination between engineers and cybersecurity analysts by highlighting architectural defects that pose a risk to cybersecurity qualification.
- **CVIT** provides a common operating picture for managers and engineers alike using AADL models and automated model analysis.
- **SLICED** detects behavioral incompatibilities between multiple software providers.
- **CAFFMAD** uses AADL's flexible type system to help engineers avoid locking onto a design trajectory too early and to provide systems engineers with a view of the design space.
- **ISOSCELES** uses AADL's consistent semantics to generate source code for safety-critical embedded systems, keeping software design consistent with system design.
- **FASTAR** evaluates constraints to ensure that software and hardware designs are mutually satisfactory.

Least Commitment Design Workflow

Models of Systems
(e.g., hardware, software, requirements)

AADL Models

SysML Models

(1) Designer specifies:
- Top level design
- Design variants to evaluate
- Parametric studies
- Analysis tools to apply

- Risk Management Analysis
- Systems-Theoretic Process Analysis
- Reliability Analysis
- Power & Weight Analysis
- Latency Analysis
- Schedulability Analysis

CAFFMAD

(2) As models are subsequently updated and refined during the design process, CAFFMAD:
- Automatically rebuilds design variants
- Applies analysis tools to each variant
- Tabulates results for trade study

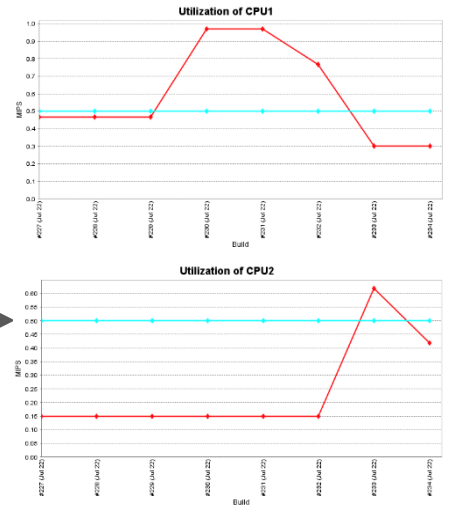
Design Space Explorer

Trade Space Explorer

Analysis Tools

	Instance	Property1	P2	P3	...	Result1	R2	R3	...
Design Variants	simplex								
	duplex								
	triplex								
	quad								
	n-version								
	ECC								
Property Variants	10 KWH								
	20 KWH								
	30 KWH								
	40 KWH								

Property Values | Analysis Results



CAFFMAD supports a **least-commitment** design approach

Safety Analysis

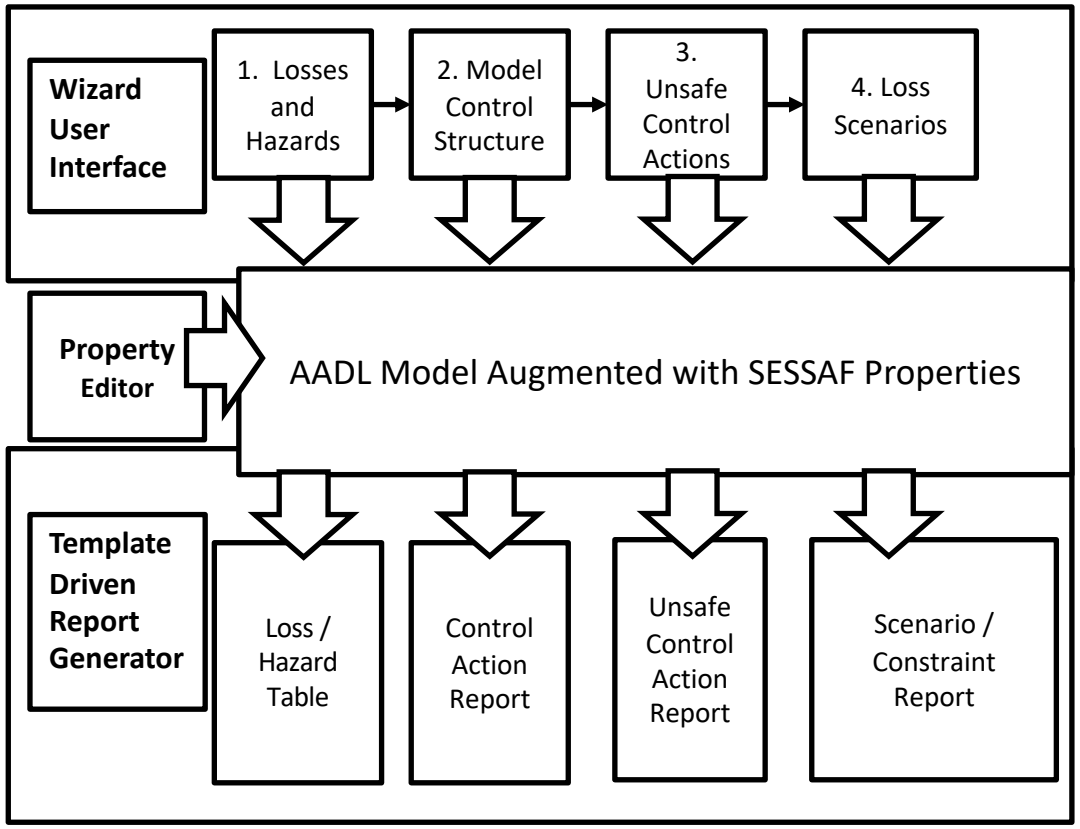
Supports top down safety and security risk analysis of embedded system models by Subject Matter Experts throughout the development process.

SESSAF Inputs:

- System Physical Architecture model
  - Mixed fidelity
- Control loops modeled as end-to-end flows

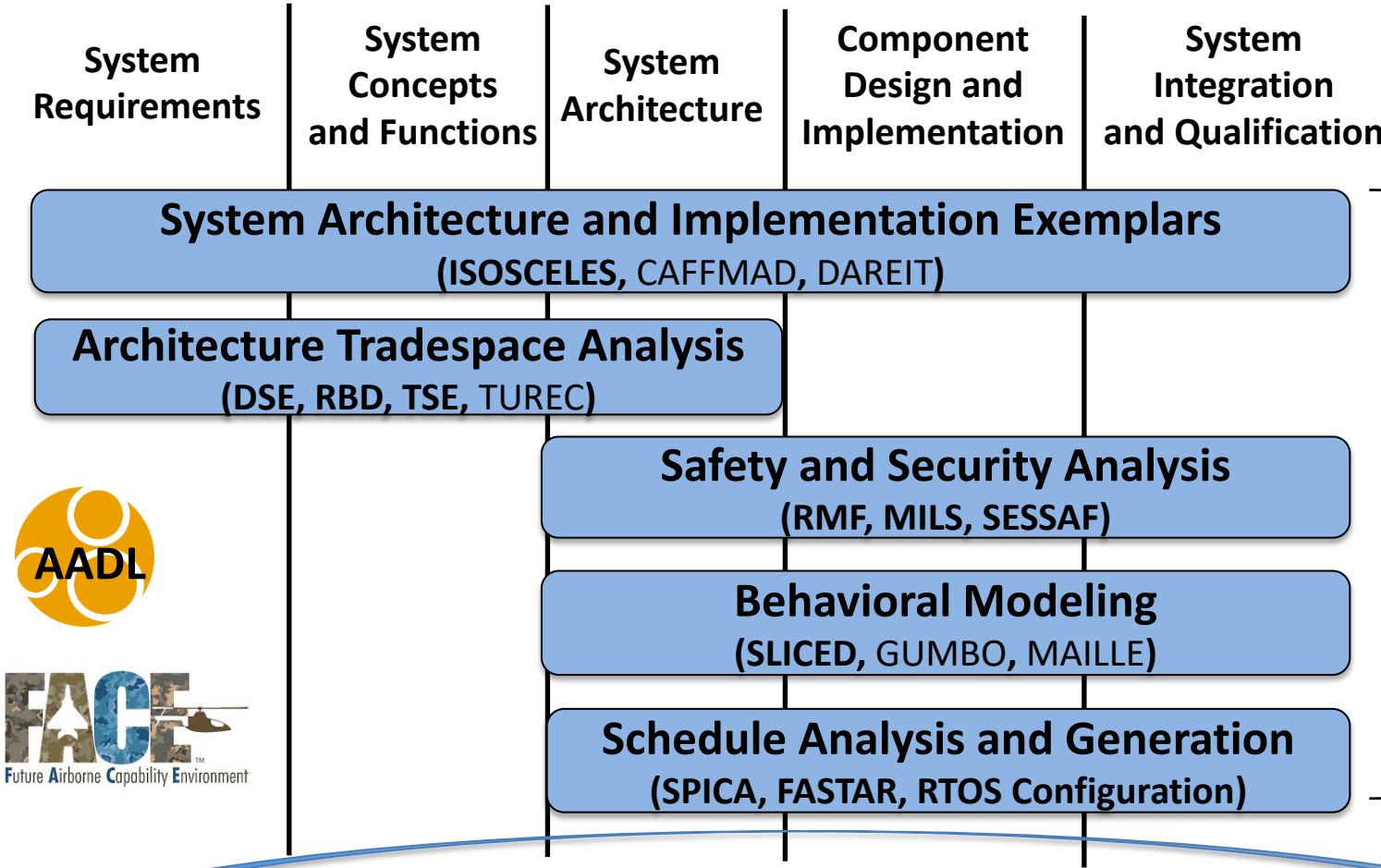
SESSAF Output Includes:

- Reports of unsafe control actions which lead to hazards and losses
- Reports assigning constraints to components to mitigate unsafe control actions
- Process status
- Reports and Mind Map



SESSAF brings safety and engineering closer together around common AADL models

Adventium Portfolio of Tools Supporting ACVIP



Boldface tools are available now.

Model-Based Digital Engineering Infrastructure

- Integration of multiple analyses into a shared workflow.
- Continuous virtual integration with mixed developer models.
- Automated model verification, report generation, and code generation.

Backup

Acronyms and Abbreviations

- AADL Architecture Analysis and Design Language
- ACVIP Architecture Centric Virtual Integration Process
- CAFFMAD Continuous Architecture Framework for Fault Management Assessment And Design
- CAMET Curated Access to Model-based Engineering Tools
- CASE Cyber Assured System Engineering
- CVI Continuous Virtual Integration
- DAREIT Design Analysis for Rapid, Effective Integration and Test
- DARPA Defense Advanced Research Projects Agency
- DHS Department of Homeland Security
- DoD Department of Defense
- DSE Design Space Explorer
- FACE Future Airborne Capability Environment
- FASTAR Framework for Analysis of Schedulability, Timing and Resources
- GUMBO Grand Unified Modeling of Behavioral Operators
- ISOSCELES Intrinsically Secure, Open, and Safe Cyber-physically Enabled, Life-critical Essential Services
- JMR Joint Multi-Role
- MAILLE Microkernel Application Information fLow with Logic-based Enforcement
- MBSE Model-Based System Engineering
- METAL-V Model-based Engineering Tools for an Affordable Lifecycle - Vertical
- MILS Multiple Independent Levels of Security
- MSAD Mission System Architecture Demonstration
- NASA National Aeronautics and Space Administration
- OSATE Open Source AADL Tool Environment
- RBD Reliability Block Diagram
- RMF Risk Management Framework
- RTOS Real-Time Operating System
- SESSAF Systems Engineering Safety and Security Analysis Framework
- SLICED State Linked Interface Compliance Engine for Data (SLICED)
- SPICA Separation Platform for Integrating Complex Avionics
- SysML System Modeling Language
- TD Technology Demonstrator
- TSE Trade Space Explorer
- TUREC Tooling to Understand Ripple Effect Costs
- VM Virtual Machine