Model-Based Engineering with AADL: Transitioning Research to Practice

Sam Procter
Outline

The Problem: Safety-Critical Embedded Software Systems
  • Part of the Solution: AADL Framework

How AADL Helps Solve Problems
  • Our Current Project
  • Zooming Out: Safety Work Done by the MBE Team
  • Zooming Out, Again: A Holistic View of Research Using AADL

DoD Impacts: Army AADL Success Story
  • Not Just DoD: How AADL Supports Transition

Alignment with Digital Engineering Strategy
Model-Based Engineering with AADL: Transitioning Research to Practice

The Problem: Safety-Critical Embedded Software Systems
The Safety-Critical Embedded Software System Challenge

**Problem:**
- Software increasingly dominates safety and mission-critical system development
- Issues discovered long after they are created

**Goal:**
- Early discovery of system-level issues through virtual integration and incremental analytical assurance

**Solution:**
- **Language** standardized via SAE International & matured into practice through pilot projects & industry initiatives
- **Tooling** available under open source license continually enhances analysis, verification, and generation capabilities
- Direct alignment with DoD Digital Engineering Strategy

A critical task: Reducing safety and security risks through early analytical assurance
Like a lot of models that engineers draw every day on their whiteboards, AADL consists of boxes and lines.

The difference between AADL and a whiteboard is that AADL has precise semantics.

This box represents a computer process - a protected region of memory and a space where we can allocate individual threads.
Those threads are also boxes – but they have very precise meanings.
AADL Overview

We can connect the threads together using lines to represent different types of intra-process communication.

We add more semantics via *properties* – they are useful for both system analyses and to guide code generation.

This box shows a periodic thread – it is dispatched regularly according to some clock.

And this thread is sporadic – it is dispatched whenever a message arrives at a specified port.
How AADL Helps Solve Problems
Integrated Safety and Security Engineering (ISSE)

- Architecture-Led System Assurance
- Tooling
  - EMV2 Library
  - GATSE Extensions
  - Safety Patterns
  - HAMR / Slang, Flow Derivation, Simulator
  - ASAP
- SAFE
- Stable ----> Mature ----> Prototype
- Security Annex
- Off-Nominal Behavior
- Error Model (EMV2)
- Language

RESEARCH REVIEW 2020
AADL and Safety: The Work of the Model-Based Engineering Team

2006: Error Model (v1)

2014: Error Model (v2)

2016: Arch. Led System Assurance

2018: Security Policy Enforcement

2020: Safety and Security

Increasingly Autonomous Systems

Architecturally Integrated Safety & Security
A Holistic View of Lines of Research Enabled by AADL

- Code Generation
  - Ocarina
  - MAPs
- Virtual Integration
  - CAAS Study
  - Stepper Motor
  - SAVI
  - FVL
- Resource Budgeting & Latency
  - Apache ATAM
  - NASA JPL
- Behavior
  - DARPA HACMS
  - DARPA CASE
- Requirements
  - Apache
  - CH-47F
  - Wheel Brake
- Complexity
- Tradespace
- Security
- Autonomy
Model-Based Engineering with AADL: Transitioning Research to Practice

DoD Impacts: Army AADL Success Story
Helping to Revolutionize Army Aviation

Over many years, the SEI has had an outstanding partnership with the U.S. Army, which is at the vanguard of applying AADL and ACVIP to the Army’s future vertical lift challenge.

Benefits of AADL & ACVIP (via Alex Boydston)

- Decreased fielding time by finding problems early
- Early risk reduction by discovering performance issues early
- Increased cybersecurity by using AADL/ACVIP to improve system security
- Decreased development costs and support for MOSA and certification by transforming procurement supporting MBE and ACVIP

Virtual integration of software, hardware, and system supports verification, airworthiness, safety, and cybersecurity certification

Image source: army.mil
Impact

Finding Problems Early (AMRDEC/SEI)
Summary: 6-week virtual integration of health monitoring system on CH47 using AADL
Result: Identified 20 major integration issues early
Benefit: Avoided 12-month delay on 24-month program

Improving System Security (DARPA/AFRL)
Summary: AADL applied to unmanned aerial vehicles & autonomous truck
Result: AADL models enforced security policies and were used to auto-build the system
Benefit: Combined with formal methods verification, prevented security intrusion by a red team

Transforming Procurement (Joint Multi-Role)
Summary: Industry/DoD process demonstration
Result: Pre-integration fault identification
Benefit: 10X reduction integration test cost

Makes complex capabilities possible through Agile analytic and virtual integration of real-time safety- and security-critical cyber-physical embedded systems

All image sources: army.mil
How AADL and SEI Research Enable Transition

Research
- SEI
- K-State
- Telecom Paris
- UMinn
- GTRI
- Adventium

DoD & Industry
- Army
- ANSYS¹
- Dassault
- Ellidiss
- Physical Optics Corp
- Innovative Defense Technologies

“Valley of Death”

¹ https://www.ansys.com/blog/create-models-architecture-analysis-design-language-aadl
Model-Based Engineering with AADL: Transitioning Research to Practice

Alignment with Digital Engineering Strategy
June 2018 – Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Michael Griffin (former USD(R&E)): “Those implementing the practices must develop the “how” – the implementation steps necessary to apply digital engineering in each enterprise.”


Boydston et al.: “ACVIP plays a key role in addressing issues in cyber-physical systems (CPS) and can be a key contributor to the U.S. Department of Defense (DoD) Digital Engineering Strategy.”


Image source: DoD Digital Engineering Strategy, June 2018
For More Information

Contact Us
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web:  www.sei.cmu.edu
Email:  info@sei.cmu.edu