ADEPT Workshop 2023
AADL Intro and News

Bruce Lewis, AADL Committee Chair

Galois, Inc.

June 16, 2023

|galois|

Architecture Analysis & Design Language (AADL) History & Objectives

- Came out of 3 DARPA programs (12M) on Architecture Design Language
- Based on MetaH, Steve Vestal and ACME with Peter Feiler
- Experiments in Army Lab prove value so started SAE standard from MetaH
- SAVI adopted firming up ACVIP
- More DARPA programs leverage AADL for analysis, advanced tools many sources

- Key concepts from the beginning – Domain specific for RT embedded systems
  - Enable quantitative architectural analysis to virtually predict the effects of integrating software hardware and system components.
  - Enable generative approaches to build compliant systems from validated specs.
    (MetaH, OCARINA, TASTE, RAMSES, HAMR)
  - Provide standardized stable core concepts with well defined semantics to enable consistent exchange across contractors and interpretation by analysis & generation tools. (see Hughes SEI and Kiniry Galois presentations later)
  - Easy to understand engineering terms yet semi-formal specification of the underlying semantics (Hybrid automata, temporal logic, Behavior Annex).
  - Incremental refinement with analyzability of incomplete specs. (Key to ACVIP)
  - Flexibility to support new domains & analyses through annex sublanguage extensions and property sets.

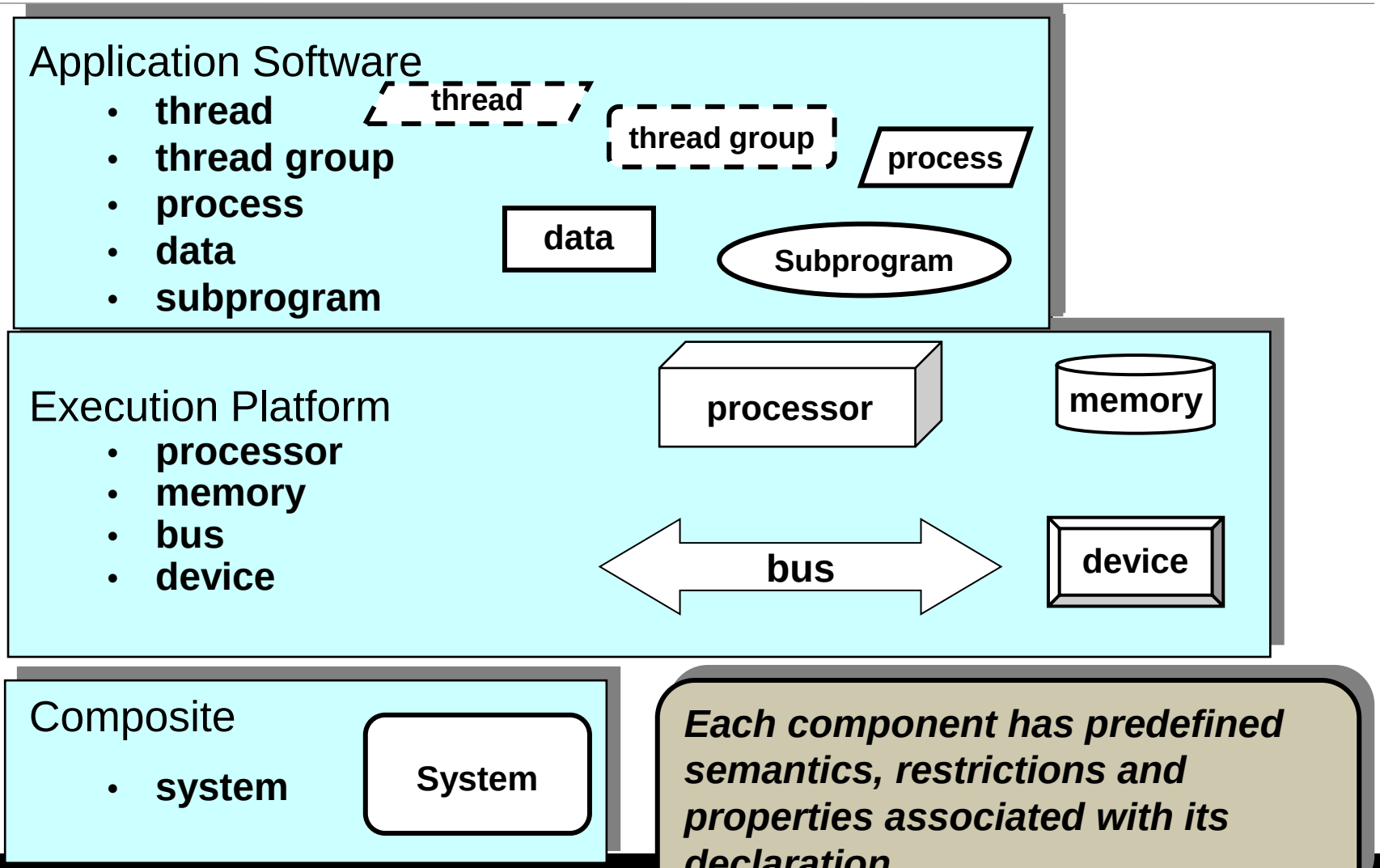
Architecture Analysis & Design Language

SAE International AS-5506 STANDARD SUITE

- **Core AADL language standard upgrades**
- **V1 [A) 2004, V2 (B) 2012, V2.2 (C) 2017, V2.3 (D) 2022**
  - For embedded & cyber physical software system modeling, analysis, and generative integration, - to predict integrated system runtime performance - Integrate then Build – then automate the build for conformance.
  - Strongly typed component based architecture language with well-defined, rich semantics for threads, processes on partitions, subprograms and processor, memory, bus, system and device components, sampled/queued, communication, modes, end-to-end flows
  - Textual and graphical notation, supporting incremental specification and analysis

- **Standardized AADL Annex Extensions**
- Error Model language for safety, reliability, security analysis [2006, 2015]
- ARINC653 extension for partitioned architectures [2011, 2015]
- Behavior Specification Language for components and interaction [2011, 2017]
- Data Modeling extension for interfacing with data models (UML, ASN.1, …) [2011]
- AADL Runtime System & Code Generation [2006, 2015, RTS refined in Core in 2022]

AADL Components



Each component has predefined semantics, restrictions and properties associated with its declaration.

Ports & Connections

Ports: directional transfer of data & control

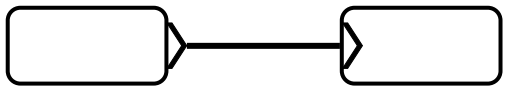
Data port: state, sampled data streams

Event port: Queued, thread dispatch & mode switch trigger

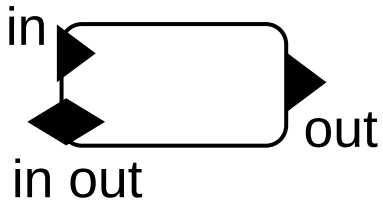
Event data port: queued messages

Port group: aggregation of ports into single connection point

Connection: connects ports in the direction of their flow



event port connection

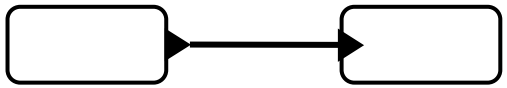


Data port

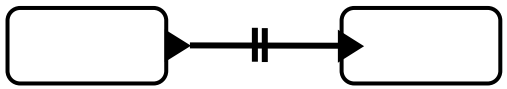
Event port

Event data port

Port group

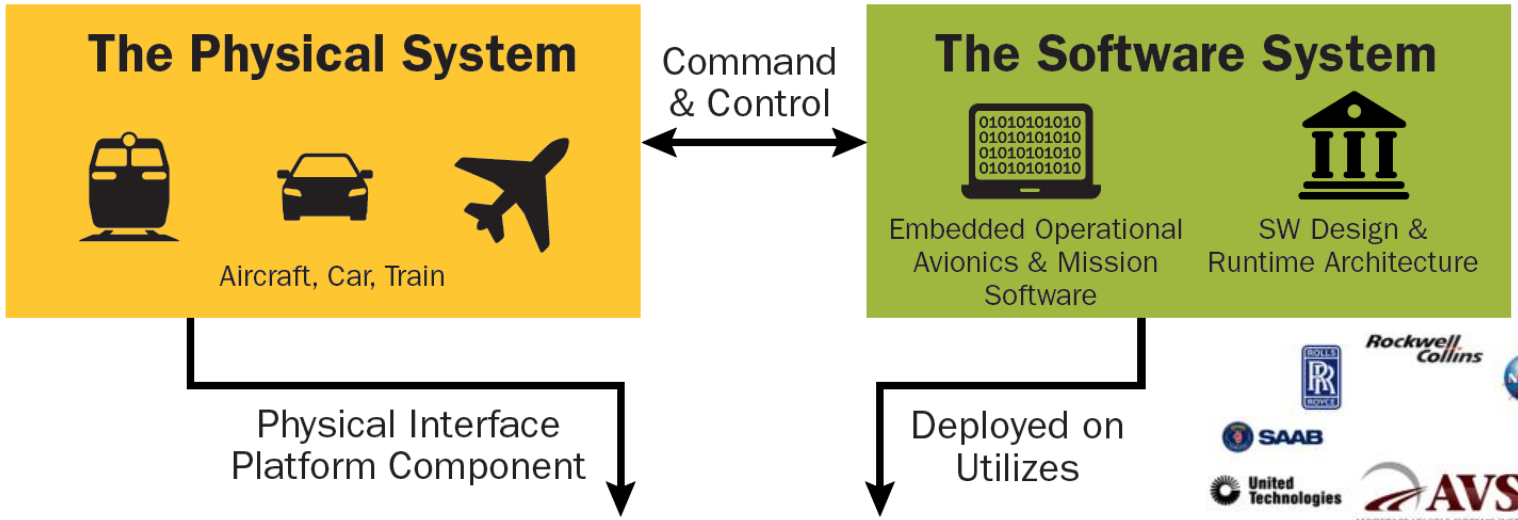


immediate



delayed

AADL ANALYTICALLY DESCRIBES THE REAL-TIME SYSTEM ENABLING VIRTUAL INTEGRATION



SAE International
AS 5506 Standard Suite

Standards provide long-term industry-wide solutions to support multi-organization model-based engineering

Rockwell Collins · NASA · SAAB · Honeywell · United Technologies · AVSI · AEROSPACE VEHICLE SYSTEMS INSTITUTE · aerospace valley · SAVI System Architecture Virtual Integration · EMBRAER · AIRBUS · BOEING · AIRBUS GROUP

In 2008 Aerospace industry initiative chose AADL over SysML and other notations as it specifically addresses embedded software systems

Standardized AADL captures mission and safety critical embedded software system architectures in virtually integrated analyzable models

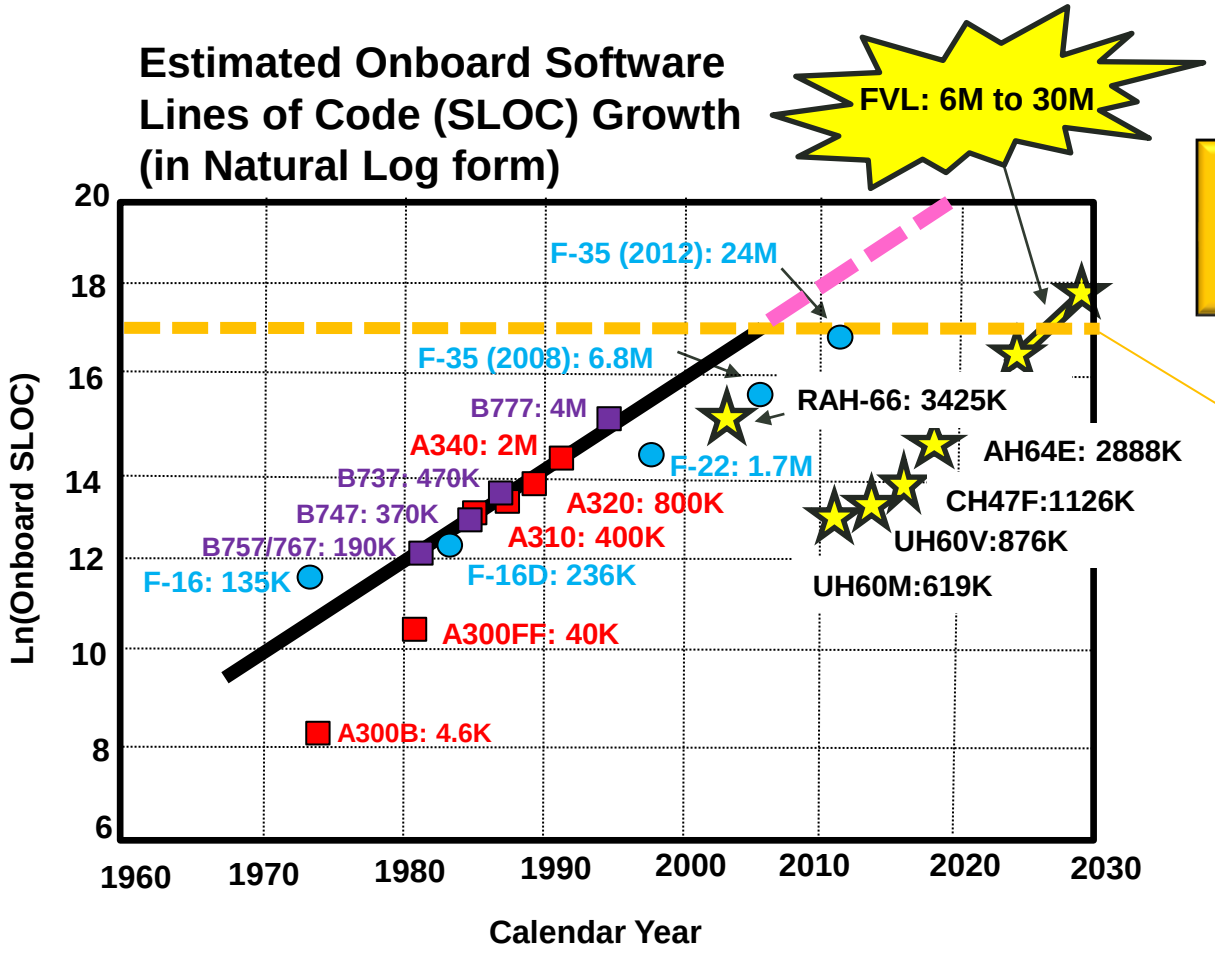
AVIATION SOFTWARE HAS ALREADY REACHED AFFORDABILITY BARRIER LIMITING CAPABILITY

DEVCOM AVIATION & MISSILE CENTER

SAVI System Architecture Virtual Integration

A Commercial Aviation Industry Consortium

Estimated Onboard Software Lines of Code (SLOC) Growth (in Natural Log form)



Per SAVI, software as % of total system development cost
1997: 45%, 2010: 70%, 2024: 88%

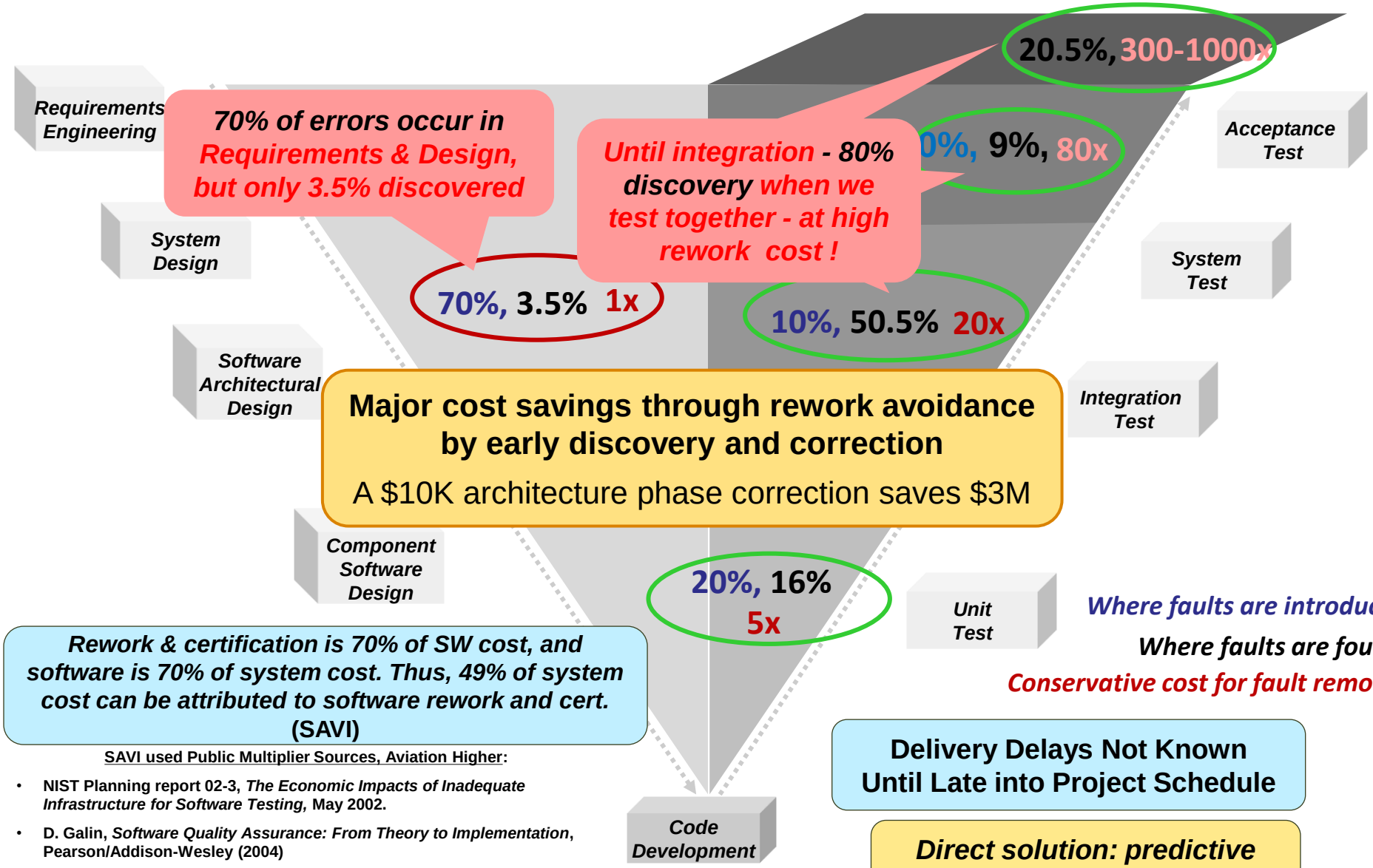
SAVI projects a limit of affordability at 27.5MSLOC or $10B in software costs

LEGEND

- Airbus
- Boeing
- Air Force Fighter
- Army Rotorcraft
- Affordability limit
- Unaffordable projection
- Straight line curve fit

Limiting SW capability directly impact strategic capabilities on weapon systems. Problem is getting worse. Leadership is key.

UNDERLYING CAUSE – INTERACTION REVEALED
LATE LARGE SOFTWARE REWORK COSTS



Rework & certification is 70% of SW cost, and software is 70% of system cost. Thus, 49% of system cost can be attributed to software rework and cert. (SAVI)

Delivery Delays Not Known Until Late into Project Schedule

Direct solution: predictive system virtual integration!

SAVI used Public Multiplier Sources, Aviation Higher:

- NIST Planning report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing,* May 2002.
- D. Galin, *Software Quality Assurance: From Theory to Implementation*, Pearson/Addison-Wesley (2004)
- B.W. Boehm, *Software Engineering Economics*, Prentice Hall (1981)

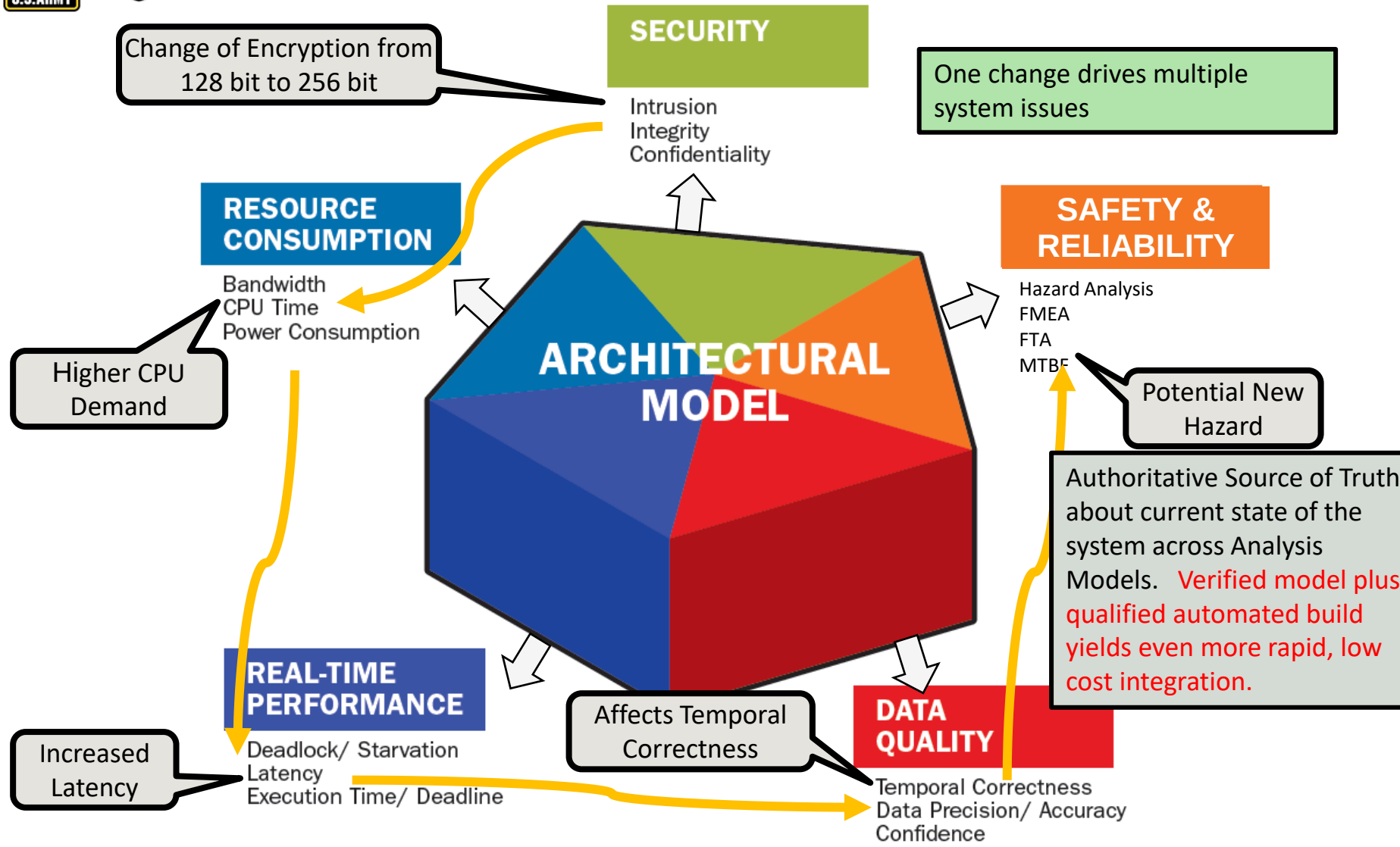
Late Error Rate on Current Development GAO F35 Report 2021

- Source: GAO-21-226: F-35 JOINT STRIKE FIGHTER, DOD Needs to Update Modernization Schedule and Improve Data on Software Development https://www.gao.gov/assets/gao-21-226.pdf

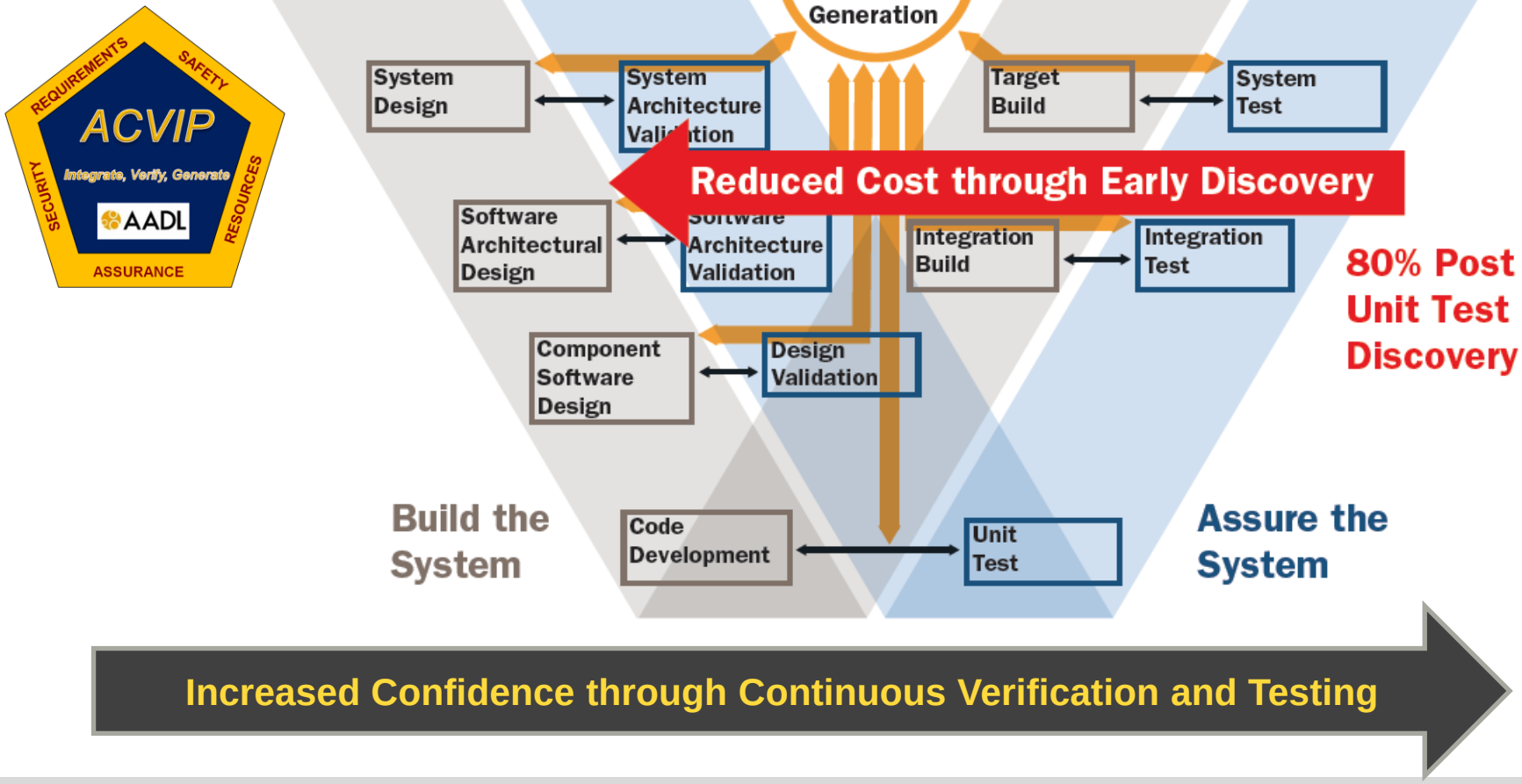
  - "Test pilots found 656 software defects which is 23% of total discovered defects (i.e.,2852 total). "Program officials released software to operational aircraft that included 386 software defects later found by pilots in the field. " Page 34.
  - "Ideally, according to the program office, the contractor would identify defects in the software lab or before the software is fielded to the developmental test aircraft." Page 33.
  - Total defects fielded to aircraft (656 + 386)/2852 = 37%
  - "DOT&E officials also stated that, as currently planned, the schedule does not provide adequate time to complete regression testing to identify and address defects….
    The contractor recognizes that late discoveries are a problem and is working toward identifying and fixing defects earlier in the development process." Page 38

  - Part of the solution - GAO F35 Report 2023 - Contractor moving toward …."Running additional static analysis checks, which allow developer more opportunities to identify any issues that the new capability might create for the current aircraft software"

AADL/ACVIP INCLUDES MULTIPLE DOMAINS OF ANALYSIS AGAINST AN INTEGRATED ARCHITECTURAL MODEL TO REVEAL EMERGENT EFFECTS



ACVIP PROCESS APPLIES AADL INCREMENTALLY TO CATCH INTEGRATION ISSUES EARLY



AADL SAE AS2C Committee Activities

- COVID made international travel difficult
- Currently two virtual meetings per month
  - Technology Updates – new tools, analysis methods
    - Typically Wed 10-11 AM Central Time, mid month
    - Video's available on request
  - Standards Update – working the core or annexes
    - Typically Thursday 10-11 AM Central Time, mid month
    - Working on updates to the EMV2 Annex now.
    - Next topic expected to be AADL modes
    - Other upgrades from formal language specification of AADL
- Expect to return to multiple face to face meetings/yr
  - Complete updates of annexes, consolidate to one
  - Meet at Aerotech meetings as well as present

Questions?

NEED FOR INTEGRATED ENGINEERING ANALYSIS OF EMBEDDED SOFTWARE SYSTEMS SIMILAR TO PHYSICAL

Virtual Integrated Physical System
Analysis Uses Computer Models (e.g. CAD)

- Aerodynamics
  - Aero elastics
  - Stall and Compressibility
  - Acoustics
- Structures
  - Static and Dynamic
  - Flutter and Vibration
  - Fatigue
- Drive Systems
  - Power Transmission
  - Wear and Fatigue
- Engine
  - Power Available
  - Fuel Required
- Mission Performance
  - Payload
  - Range
  - Speed

Change in # Rotor Blades from 2 to 4

↓

Increased Wt & Change in Vibrations

↓

Increased Power Transmission

↓

Increase in Fuel Flow

↓

Potential Loss of Capability

Virtual Integrated Software System
Analysis Uses AADL Model

- Security
  - Intrusion
  - Integrity
  - Confidentiality
- Resource Consumption
  - Bandwidth
  - CPU Time
  - Power Consumption
- Real-Time Performance
  - Execution Time / Deadline
  - Deadlock / Starvation
  - Latency
- Data Quality
  - Data Precision / Accuracy
  - Temporal Correctness
  - Confidence
- Safety and Reliability
  - MTBF
  - FMEA
  - Hazard Analysis

Change of Encryption From 128 bit to 256 bit

↓

Higher CPU demand

↓

Increased latency

↓

Affects temporal correctness

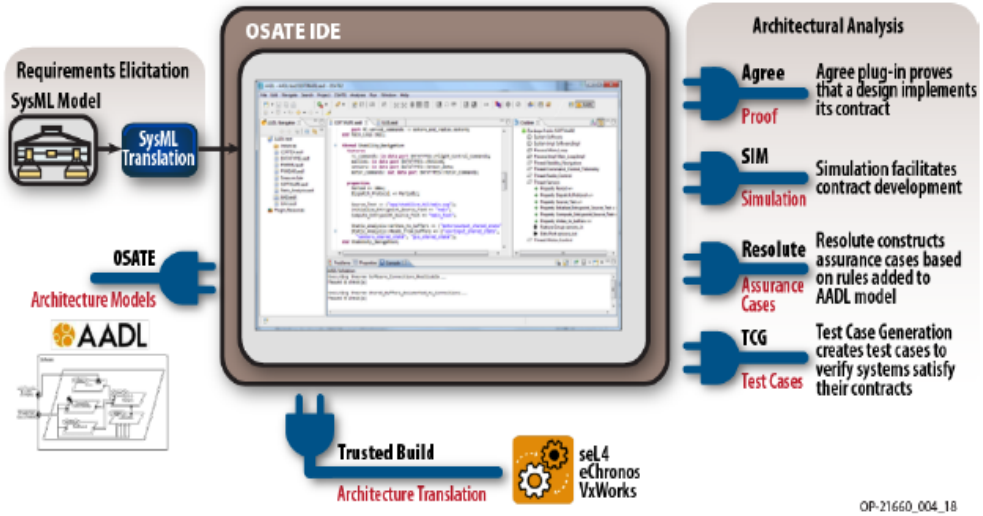
↓

Potential new hazard

Auto code generation from AADL Virtual Model is similar to Automated fabrication from CAD Virtual Model

DARPA: CYBER ASSURED SYSTEMS ENGINEERING (CASE) USING AADL

Architectural Modeling and Analysis



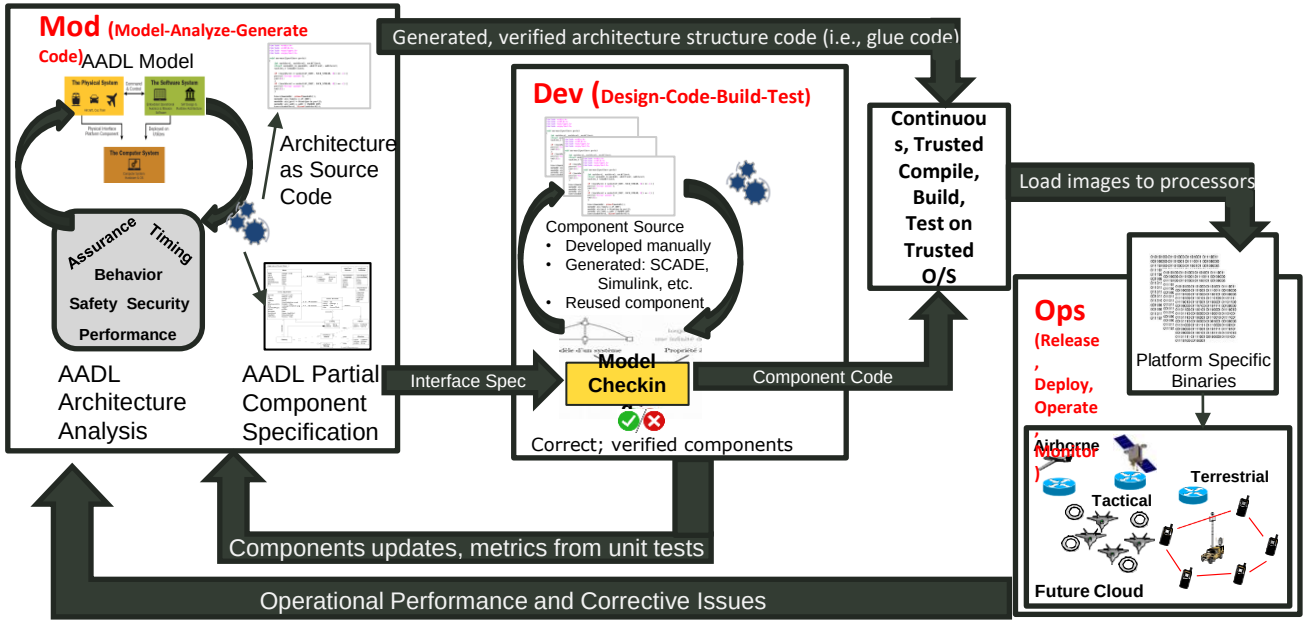
All too often architectures are modeled early in the engineering processes to be set aside and not leveraged to support design activities

From "AADL for DoD" by Ray Richards, I2O given at AADL Demo Day in DC, Nov 2019

3

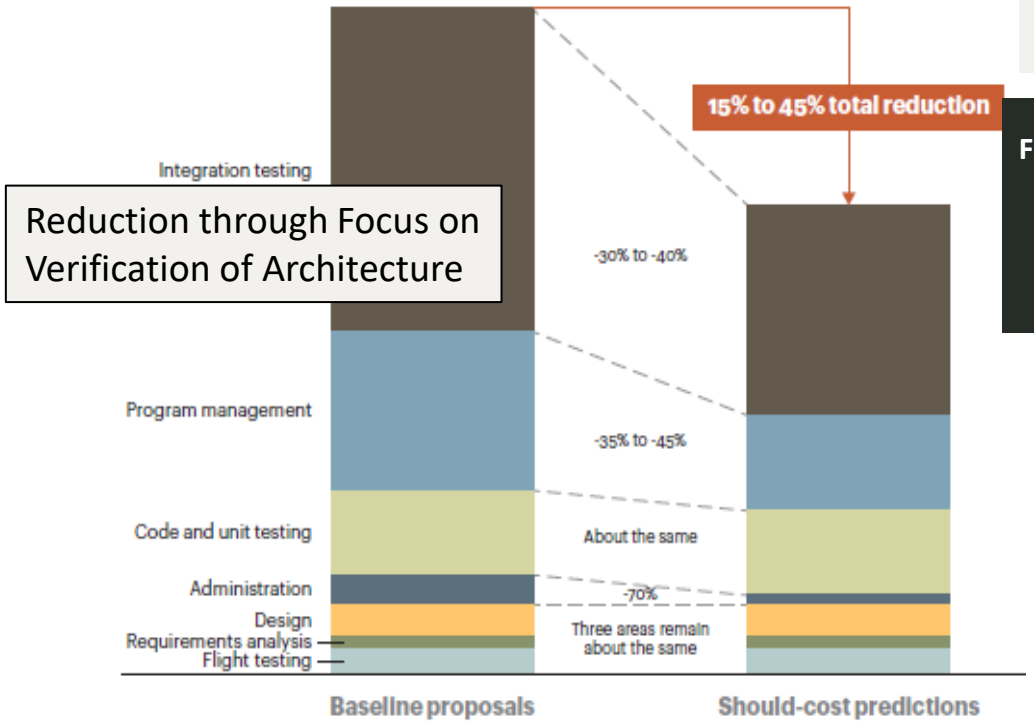
AADL/ACVIP Supports ModDevOps

- Predictive Modeling as a complement to DevOps
- Capture architecture, perform early integration analysis and synthesize middleware, leverage trusted build and execution infrastructure



SEI Research with Demo Exists Regarding TwinOps
(see https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651118)

COST REDUCTION POTENTIAL THROUGH VIRTUAL INTEGRATION OF EMBEDDED SOFTWARE SYSTEMS



Reduction through Focus on Verification of Architecture

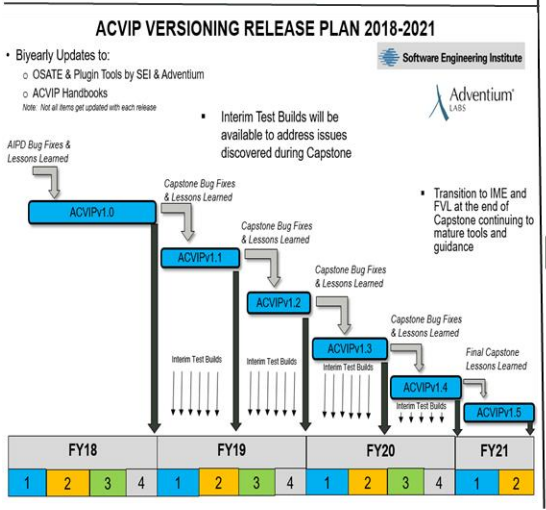
ATKearney "Software: The Brains Behind U.S. Defenses Systems"

ROI on AADL Pilot

For a 27.5 MSLOC system Nominal development cost reduction of 26%
(e.g., $2.4B out of $9.2B on a projected 2024 program)

Source: *ROI Analysis of the System Architecture Virtual Integration Initiative*
CMU/SEI-2018-TR-002

ACVIP GUIDANCE & TOOLS



AADL Based Tools Available for Capstone Demo as ACVIPv1.0

- 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
- Open Source AADL Tool Environment (OSATE)
- 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

AADL Tool Expo
https://github.com/saeaadl/userdays/tree/master/UserDays/2019-02/AADLToolFair

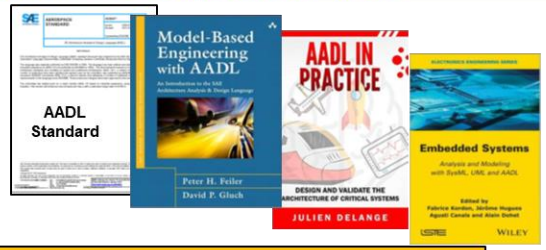
ACVIP/AADL Handbooks, Papers, and Texts

Overview

Modeling & Analysis

OSD DEWG Overview

Acquisition Management



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