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

Tool Expo Keynote Address – AADL Addressing Software Related Integration Issues and Costs

William Lewis, PhD

Director

Aviation Development Directorate

14 February 2019

Deliver collaborative and innovative aviation and missile capabilities for responsive and cost-effective research, development and life cycle engineering solutions.

~9,553
FY18 Strength

2,943
Civilian

23
Military

6,587
Contractor

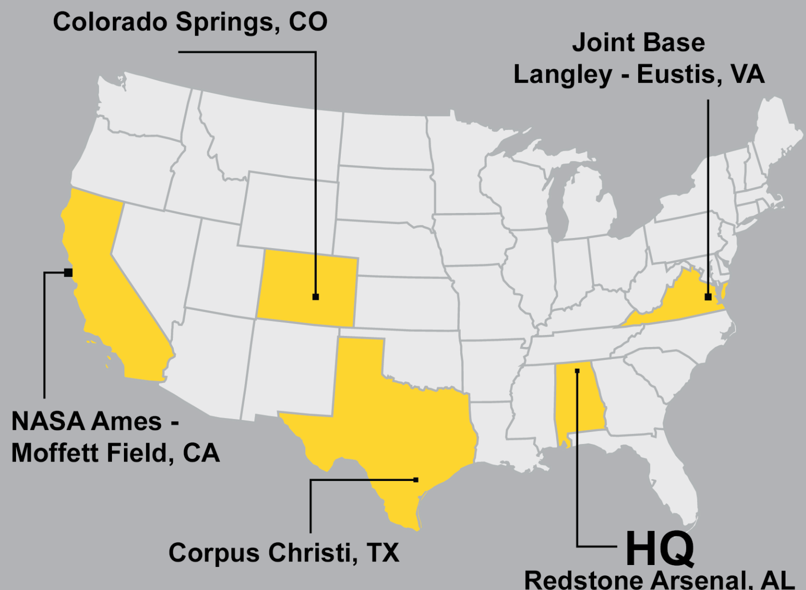
FY18 Funding
$3.4B

7%
Aviation S&T

8%
Missile S&T

58%
Army

27%
Other



Core Competencies

- Life Cycle Engineering
- Research, Technology Development and Demonstration
- Design and Modification
- Software Engineering
- Systems Integration
- Test and Evaluation
- Qualification
- Aerodynamics/ Aeromechanics
- Structures
- Propulsion
- Guidance/Navigation
- Autonomy and Teaming
- Radio Frequency (RF) Technology
- Fire Control Radar Technology
- Image Processing
- Models and Simulation
- Cyber Security

#1: Readiness

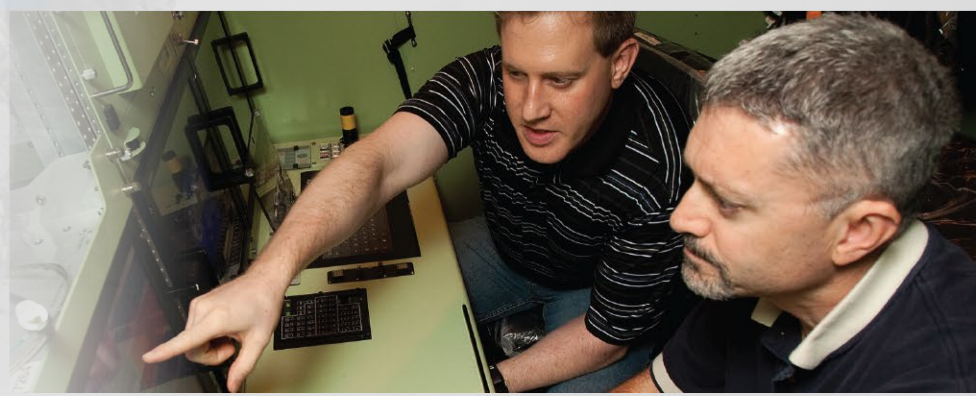
Provide aviation and missile systems solutions to ensure victory on the battlefield today.

#2: Future Force

Develop and mature Science and Technology to provide technical capability to our Army's (and nation's) aviation and missile systems.

#3: Soldiers and People

Develop the engineering talent to support both Science and Technology and the aviation and missile materiel enterprise



RAH-66 COMANCHE SOFTWARE REWORK & INTEGRATION LESSONS LEARNED

Photo Credit: Boeing-Sikorsky

In last year, multiple major software (SW) rebuilds occurred indicating significant integration issues

- **As high as 75% of SW replaced**
- **Routinely 50% of SW replaced / drop**

- ***In 1983, the Army planned to buy 5,023 vehicles at $12.1 million/copy.***
- ***Test schedule delays and increasing development costs scaled down the planned buy to 650 aircraft at $58.9 million/copy.***
- ***Technical challenges remained in software development, integration of mission equipment, radar and infrared signatures, and radar perf.***
- ***The first flight had been originally planned to take place during August 1995, but was delayed by a number of structural and software problems that had been encountered.***
- ***Key program elements, including development and integration of certain software capabilities, failed to foster confidence with Army overseers; several capabilities were viewed as having been unproven and risky.***
- ***Affordability became the issue. The anticipated consumption of up to 40% of the aviation budget by the Comanche alone for a number of years was considered to be extreme.***
- ***Complex spiral developments of the mission equipment package were never attempted due to termination of the program. Given earlier rework required, this more complex element would have involved significant rework.***

References:

- *http://www.defense-aerospace.com/articles-view/release/3/32273/pentagon-hit-over-comanche-failings-(jan.-23).html*
- *https://en.wikipedia.org/wiki/Boeing%E2%80%93Sikorsky_RAH-66_Comanche#cite_note-26*
- *https://en.wikipedia.org/wiki/Boeing%E2%80%93Sikorsky_RAH-66_Comanche#cite_note-Eden_p139-9)*

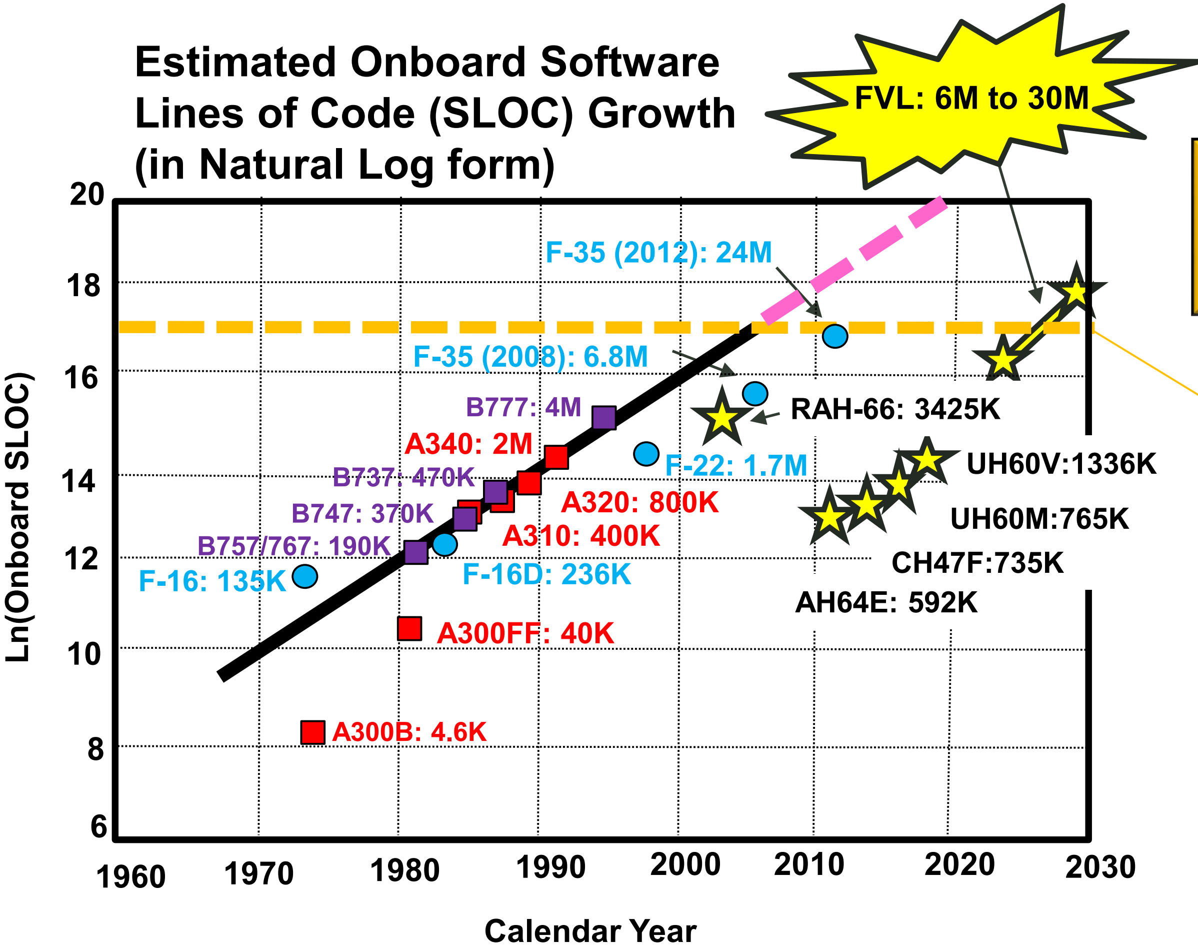
Integration and software rework were significant cost contributors. A cyber physical system development process was effectively non-existent

AVIATION SOFTWARE HAS REACHED AFFORDABILITY BARRIER LIMITING CAPABILITY

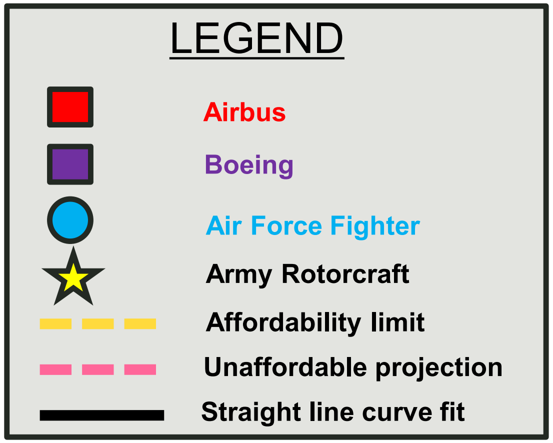
SAVI System Architecture Virtual Integration

A Commercial Aviation Industry Consortium

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

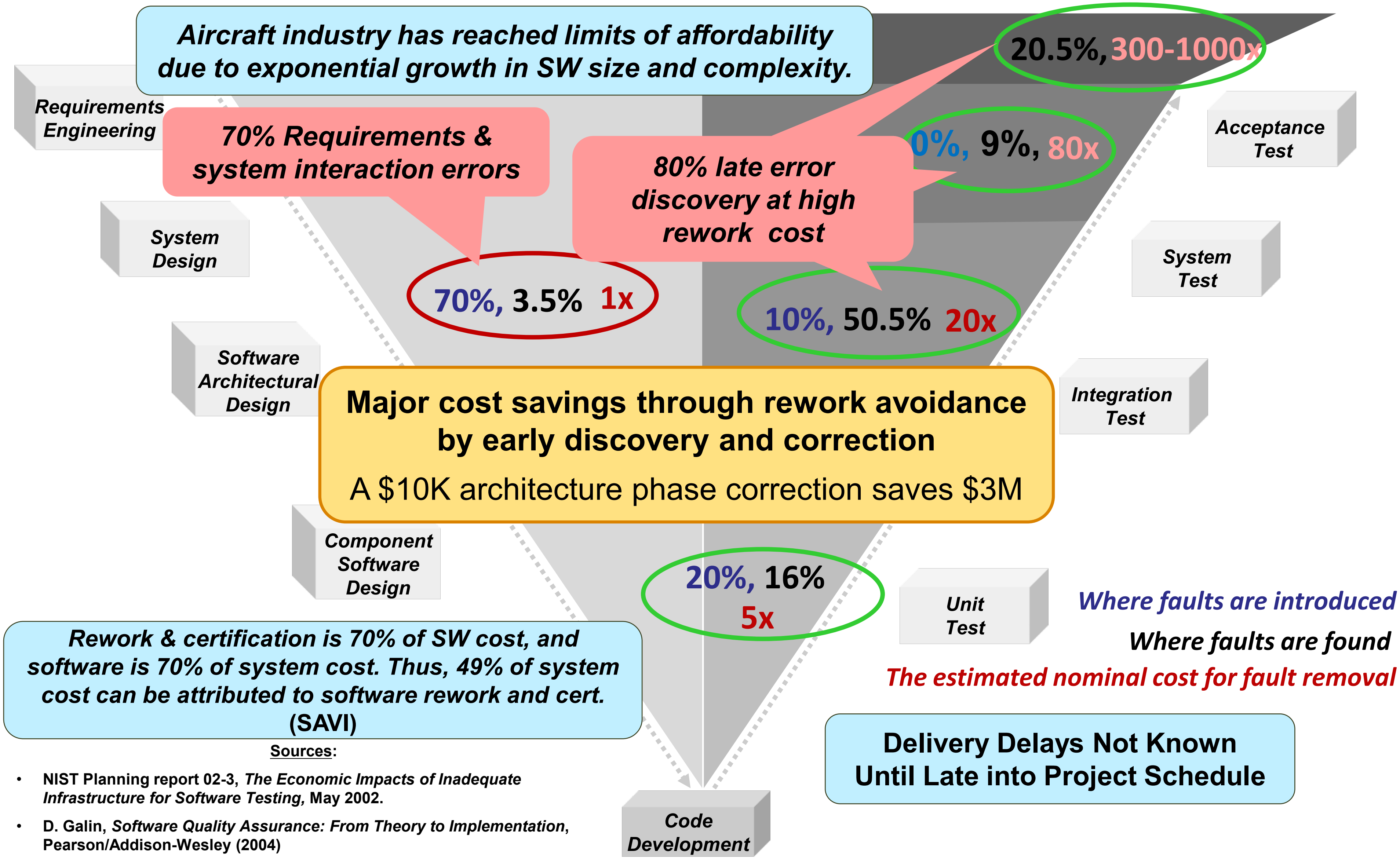


SAVI projects a limit of affordability at 27.5MSLOC or $10B in software costs



Both military and commercial aviation are facing an affordability limit with software and its integration

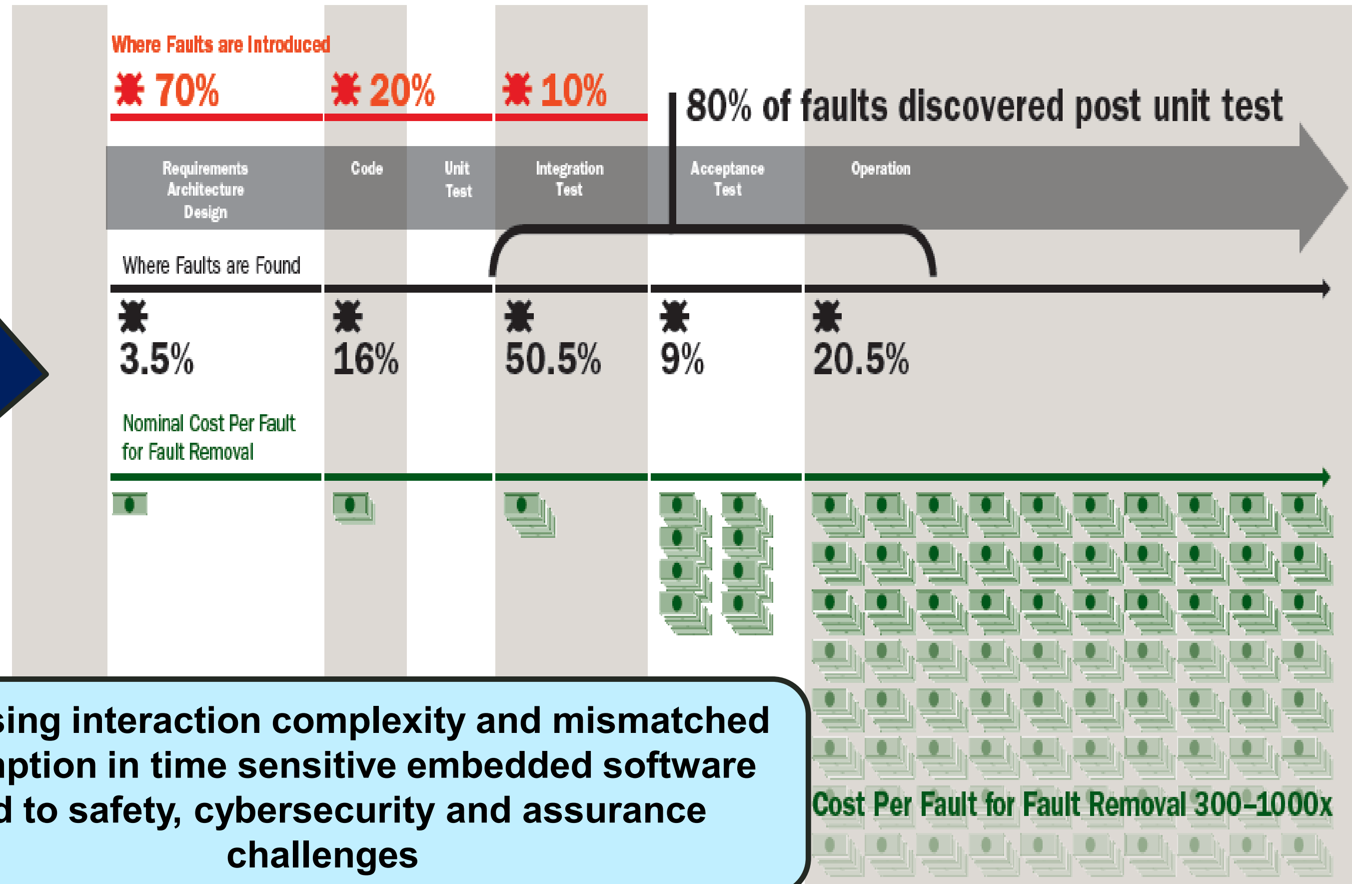
SOFTWARE REWORK HAS A MAJOR IMPACT ON SYSTEM COST



Sources:

- 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)

SYSTEM LEVEL NON-FUNCTIONAL ISSUES DRIVE REWORK COSTS



Increasing interaction complexity and mismatched assumption in time sensitive embedded software lead to safety, cybersecurity and assurance challenges

Need an ability to virtually integrate to detect design phase issues before physical integration

ANALYTICAL INTEGRATION FOR EMBEDDED SYSTEMS PROVIDED BY ARCHITECTURE ANALYSIS & DESIGN LANGUAGE (AADL)

DEVCOM AVIATION & MISSILE CENTER

The Physical System

Aircraft, Car, Train

Command & Control

The Software System

Embedded Operational Avionics & Mission Software

SW Design & Runtime Architecture

Physical Interface Platform Component

Deployed on Utilizes

SAE International

AS 5506 Standard Suite

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

The Computer System

Computer System Hardware & OS

SAVI System Architecture Virtual Integration

AVSI Aerospace Vehicle Systems Institute

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

AADL captures mission and safety critical embedded software system architectures in virtually integrated analyzable models to discover system level problems early and construct implementations from verified models

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

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

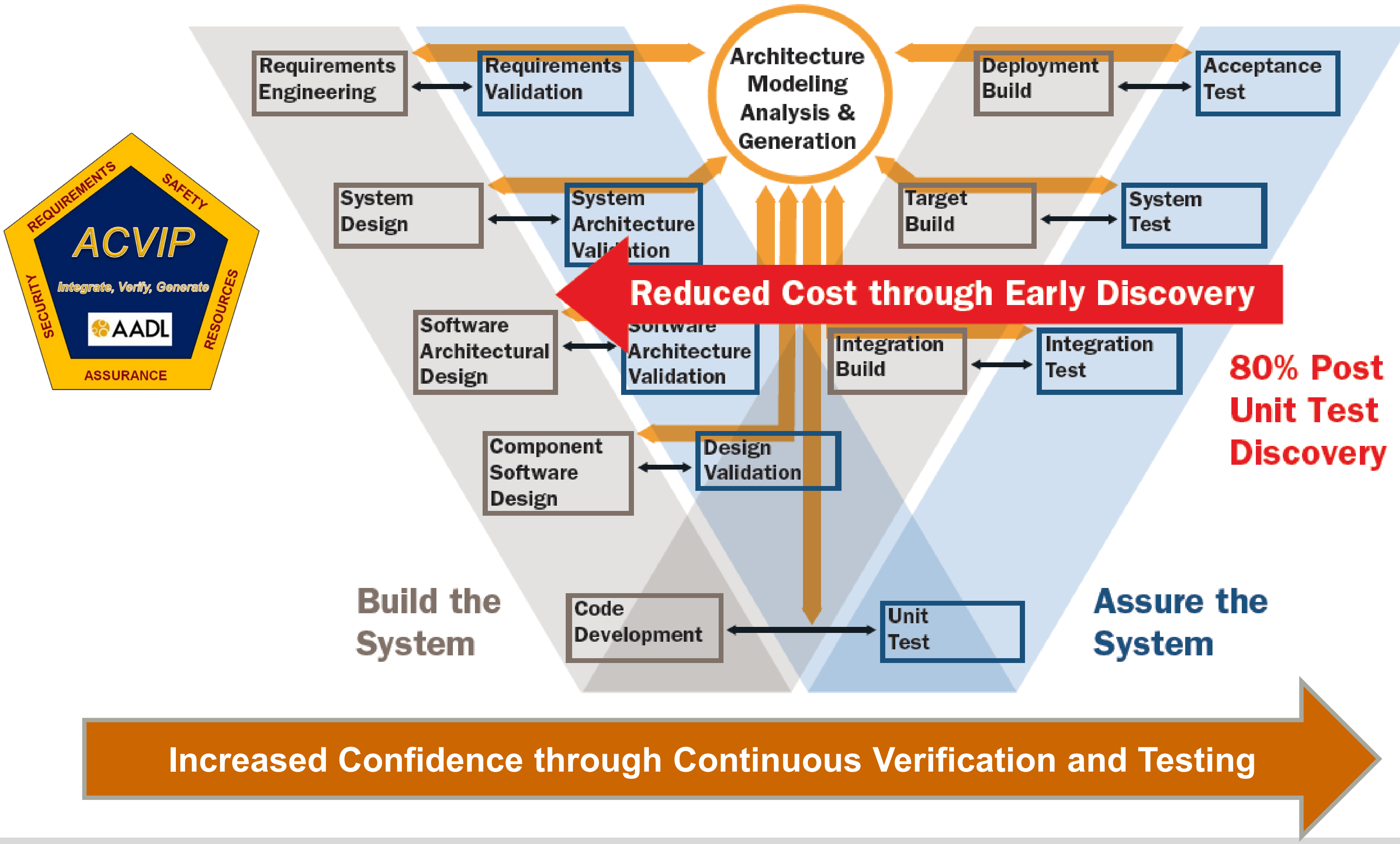
Virtual Integrated Software System
Analysis Uses AADL Model

- 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

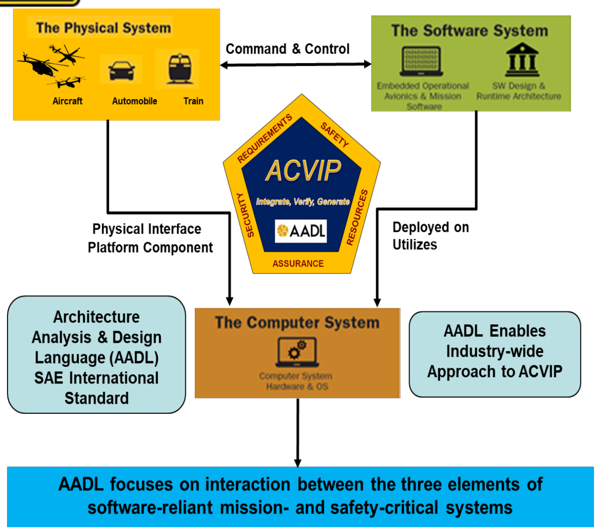
Change of Encryption From 128 bit to 256 bit
↓
Higher CPU demand
↓
Increased latency
↓
Affects temporal correctness
↓
Potential new hazard

Autocode generation from AADL Virtual Model is similar to Automated fabrication from CAD Virtual Model

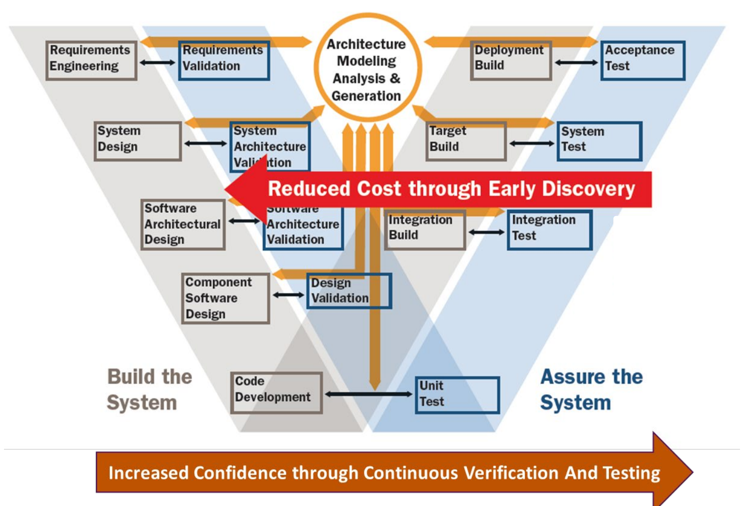
BENEFITS OF INCREMENTAL VIRTUAL SYSTEM INTEGRATION & CONTINUOUS LIFECYCLE ASSURANCE



ARCHITECTURE CENTRIC VIRTUAL INTEGRATION PROCESS (ACVIP)



Early Discovery through Virtual System Integration



- **Leverages** research from the AVSI **SAVI** consortium which used virtual integration to draw down costs in commercial aviation systems
- **Utilizes architecture models** to perform **virtual integration focusing on** software-intensive parts of real-time safety- and security-critical **computing systems** to **identify issues early before integration**
- **Process** (from ACVIP Modeling & Analysis Handbook)
  1) **Develop ACVIP Management Plan**
  2) **Establish Model Structure**
  3) **Define Model Content Needed for Analysis**
  4) **Incrementally Execute Analyses, Resolve**
  5) **Build System in Conformance to Models**
  6) **Support Certification and Readiness Reviews**
- **Supports architecture-based compositional modeling and analysis** of computing system properties
- Analytical results support **increasing assurance confidence** and compliments testing
- Provides an **"Authoritative Source of Truth"** embedded systems architectural model

Virtual Integration of Software, Hardware, and System supporting verification, airworthiness, safety and cyber security certification

U.S.ARMY

ACVIP MODELING & ANALYSIS EXERCISED ON JMR MSAD DEMONSTRATIONS

DEVCOM AVIATION & MISSILE CENTER

FY14				FY15				FY16				FY17				FY18				FY19				FY20			
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q

JCA Demo / ACVIP Shadow

ACVIP Related Tasks

- Scope limited to single component
- Model Based Acquisition
- AADL Modeling / Analysis
- JCA Model Refinement
- Lab Integration / Testing
- Report Generation
- Process Refinement

BOEING · SIKORSKY A LOCKHEED MARTIN COMPANY · Honeywell

ACVIP Integrate, Verify, Generate · AADL · REQUIREMENTS · SAFETY · SECURITY · RESOURCES · ASSURANCE

ACVIP Shadow on JCA Demo:
>85 Issues found via requirements, safety and timing analysis

Architecture Implementation Process Demonstrations (AIPD)

RFI BAA Award

Approach

- Government defined areas of emphasis and goals related to JCA, FACE™, ACVIP and MBE in general
- Efforts provided "evidence" of ability to meet USG business and process goals and are relevant to industry and Army aviation PM plans
- Model exchange and analysis and tools exercised
- Generated several lessons learned

BOEING · SIKORSKY A LOCKHEED MARTIN COMPANY · LOCKHEED MARTIN · GE Aviation · NORTHROP GRUMMAN · Honeywell · Rockwell Collins

ACVIP Integrate, Verify, Generate · AADL · REQUIREMENTS · SAFETY · SECURITY · RESOURCES · ASSURANCE

AIPD Lessons Learned wrt ACVIP:

- *Modeling Plan is crucial for success else modeling for sake of modeling*
- *Continue Tool maturation and addition of tools*
- *Authoritative Source of Truth needed*
- *Upfront modeling and analysis appears to* ***add significant value: ~3x increase to requirements and design activities, resulted in ~10x reduction on test and integration activities***

Mission Systems Architecture Capstone Demonstration

RFI BAA Award Award Award Award

Approach

- Implementation of a partial, notional mission systems architecture
- Multiple vendors
- Model Based Acquisition
- ACVIP Modeling / Analysis
- JCA / FACE Validation
- Scope of implementation limited by available resources (i.e. design only, limited lab implementation / test, etc.)

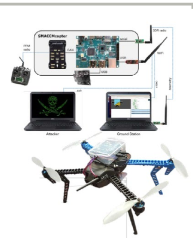
ACVIP is being applied across JMR MSAD Demonstrations

DEMONSTRATIONS OF EFFECTIVENESS IN USE OF ACVIP WITH AADL

Finding Problems Early (AMRDEC/SEI)

- Summary: 6 Week Virtual Integration of health monitoring system on CH47F using AADL
- Result: Identified 20 major integration issues early
- Benefit: Avoided 12-month delay on 24-month program

CH47 Chinook



Unmanned Quadcopter

DARPA

High Assurance Cyber Military Systems (HACMS)

TARDEC Autonomous Truck

Unmanned Little Bird

Improving System Security (DARPA / AFRL)

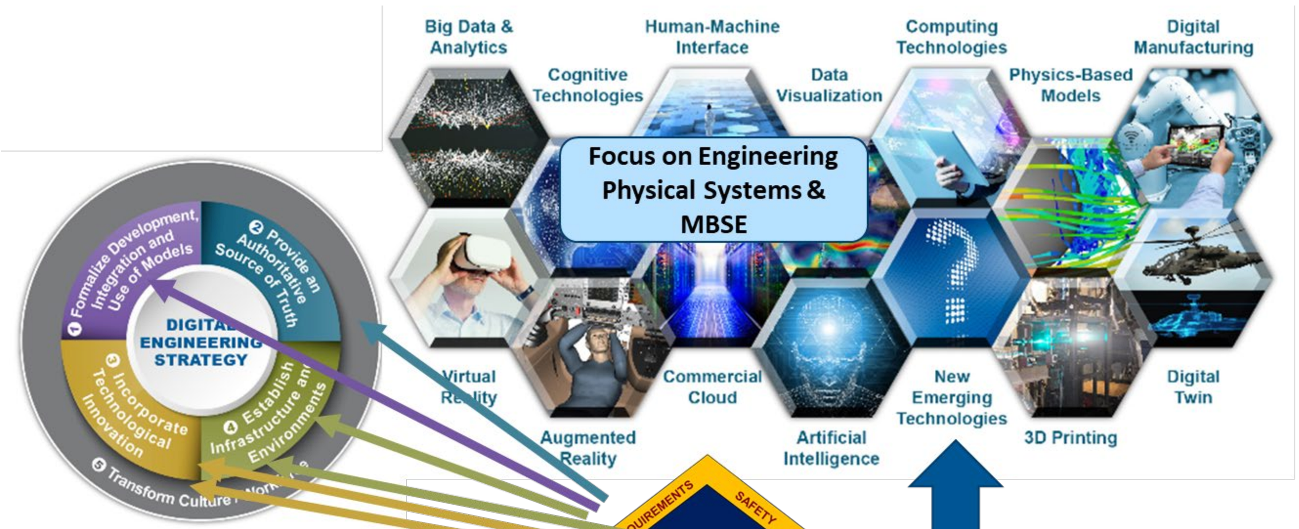
- AADL applied to Unmanned Aerial Vehicles & Autonomous Truck
- Result: AADL models enforced security policies and were used to auto build the system
- Benefit: Combined with formal methods verification, prevented security intrusion by a red team

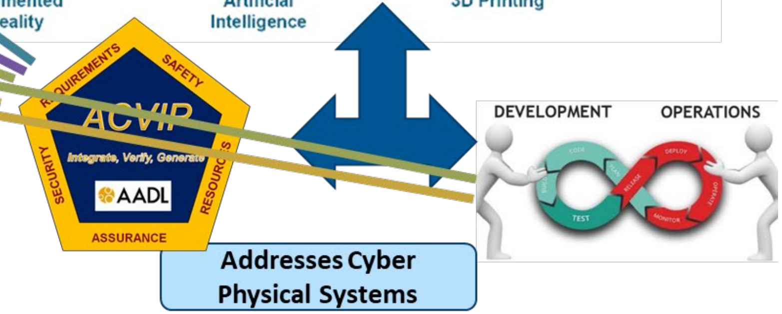
Transforming procurement (Joint Multi-Role)

- Summary: Industry/DoD mission system architecture demonstrations using ACVIP
- Result: Pre-integration fault identification
- Benefit: ~3x increase to requirements and design activities, resulted in ~10x reduction on test and integration activities

DOD DIGITAL ENGINEERING STRATEGY: ACVIP & AADL FOCUSES ON CYBER PHYSICAL SYSTEMS

“A Cyber Physical System (CPS) is a system that is controlled or monitored by computer-based algorithms, tightly integrated networks and its users. In cyber-physical systems, *physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a lot of ways that change with context*.”





Source: "US National Science Foundation, Cyber-Physical Systems (CPS)"

https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm

Benefits:
On Time - Faults found early
On Budget – Integration cost reduced
On Spec – Incremental Assurance
Driven by analytical models to verify

ACVIP with AADL is key for the modeling, analysis and generation of software intensive embedded and cyber physical systems

QUESTIONS?