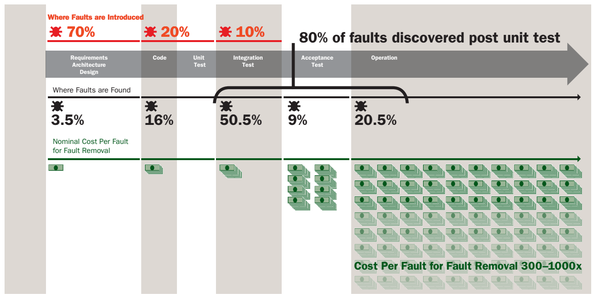
AADL Workbench for Virtual System Integration

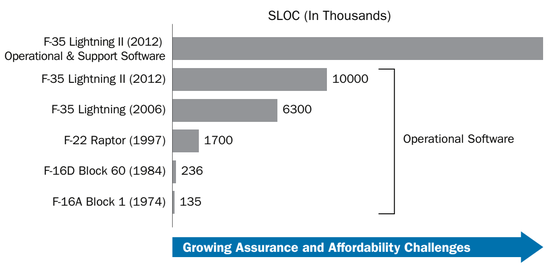
Safety and Mission Critical System Challenge

The traditional development lifecycle using existing methods of system engineering are not working for the latest generation of systems being developed. Requirements and architecture design introduce 70% of system issues, while 80% are discovered post unit test, when they are exponentially more expensive to fix.



Much of the growth in total system cost is interaction complexity and mismatched assumptions in embedded software, making systems increasingly unaffordable.

DoD Capabilities through Software

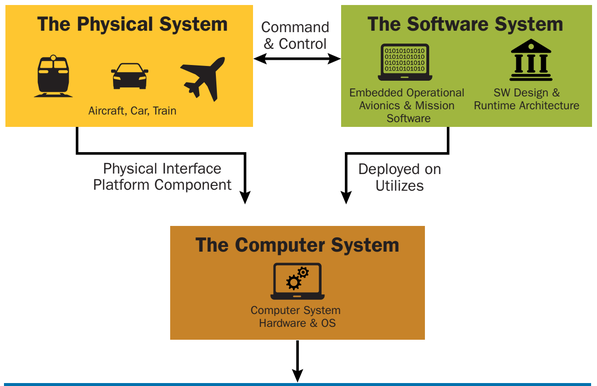


Source: Hagan/Sorenson, "Delivering Military Software Affordably", Defense AT&L, Mar-Apr 2013

Software as % of total system cost
1997: 45% ⟶ 2010: 66% ⟶ 2024: 88%

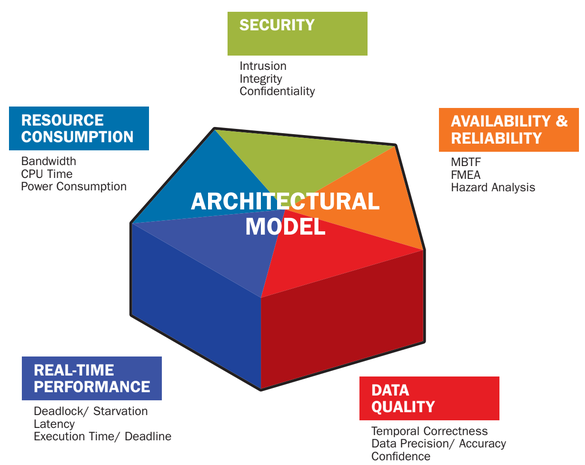
Virtual System Integration with SAE AADL

The SAE International AS-5506 Architecture Analysis & Design Language (AADL) standard suite has been developed to address this challenge through virtual system integration and analysis to discover system-level issues earlier in the life cycle.



AADL focuses on interaction between the three elements of a software-reliant mission and safety-critical systems

An Analyzable Architecture Modeling Notation. Well-defined timing semantics of a task and communication architecture deployed on distributed platforms, modeling of virtual channels, partitions, operational modes, end-to-end flows, fault behavior, and security characteristics lead to multi-dimensional analysis of virtually integrated systems and discovery of system level issues early in the lifecycle.



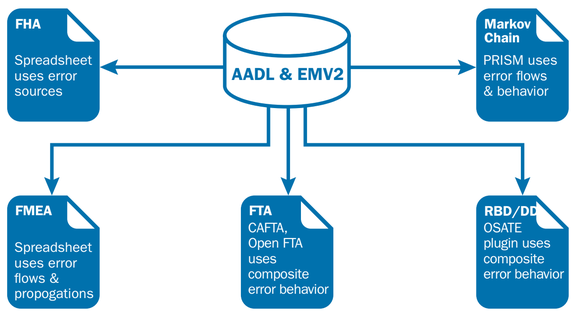
The Open Source AADL Workbench

The Open Source AADL Tool Environment (OSATE) provides a reference implementation of the SAE AADL standard suite notation and a prototyping platform for advancing research in architecture-centric system analysis and verification.

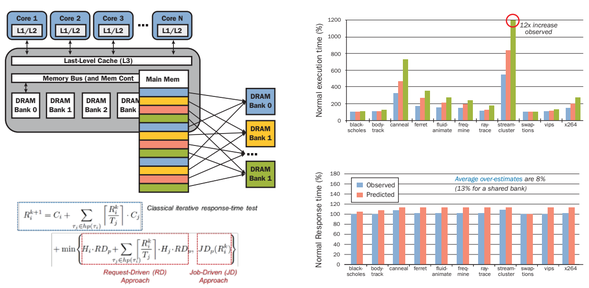
Open Source AADL Tool Environment (OSATE)

Modeling Capabilities	Analysis Capabilities	Usability Capabilities	External Contributions
AADL	Resource Budget	Context sensitive help	Resolute
EMV2	Latency	Role specific workflow	Agree
BA	Safety	Expanded Navig. Views	Ocarina Code Generation DeOS, VxWorks
Type Consistency	RMS/EDF Scheduling	Graphical Editor	MAST Scheduling
Semantic Consistency	Resource Allocation		Independent contributions
Team Mgmt	Functional Integration		
	ARINC653 Support		

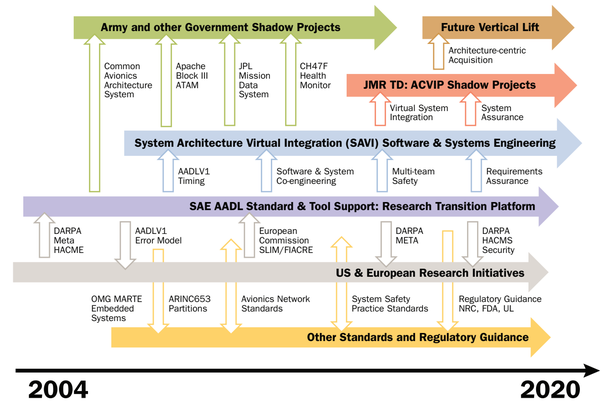
Support of SAE ARP4761 System Safety Assessment Practice



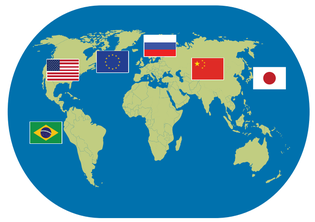
Rate Monotonic with Memory Partitioning



Towards an Architecture-centric Virtual Integation Practice (ACVIP)



International investment and engagement



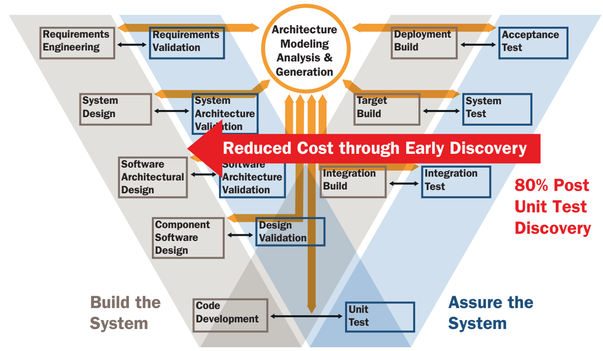
A Key Technology in the System Architecture Virtual Integration (SAVI) initiative by an international Aerospace industry consortium. Proof of concept demonstrations, return on investment, technology maturation, pilot applications, and process adapation in a multi-year self-funded effort.

TEES | AVSI AEROSPACE VEHICLE SYSTEMS INSTITUTE

BOEING · EMBRAER · AIRBUS · BAE SYSTEMS · Honeywell · GOODRICH · NASA

Software Engineering Institute | Carnegie Mellon University

Early Discovery through Virtual System Integration



Contact: Peter Feiler phf@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002837