UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Verification, Validation and Accreditation using AADL

RT21 Session at Annual SERC Research Review
Nov 9, 2010

Sue O'Brien
Acting Director
Rotorcraft Systems Engineering and Simulation Center
256-824-6133
obriens@uah.edu

Philip Alldredge
Technical Lead
Philip.Alldredge@uah.edu

SYSTEMS ENGINEERING
Research Center

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Agenda

- Problem and Objective
- Research Approach
- Method for the Research
- Benefits
- STIL and AADL Overview
- Deliverables
- Present Status
- Challenges

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Problem and Objective

Problem

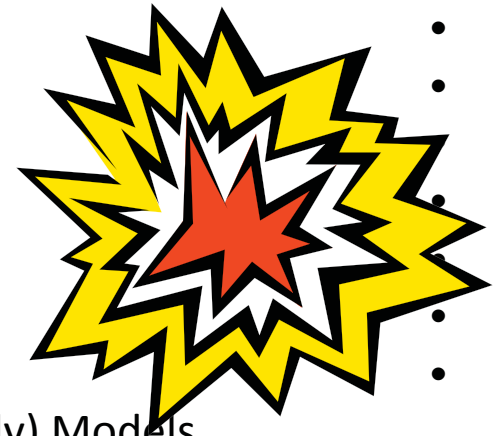
- Standard DoD Acquisition VV&A processes are not keeping pace with the emerging technologies being created to support development of complex DoD systems. Specifically the extensive use of models throughout the development lifecycle has progressed without commensurate means for establishing the soundness of these immediate design artifacts.

Objective for this Research

- Explore unique capabilities of a semantically strong architectural description language (ADL) for developing high confidence (verified and validated) models as part of a system development lifecycle.
- Exercise a selection of these capabilities on a real-world, representative system

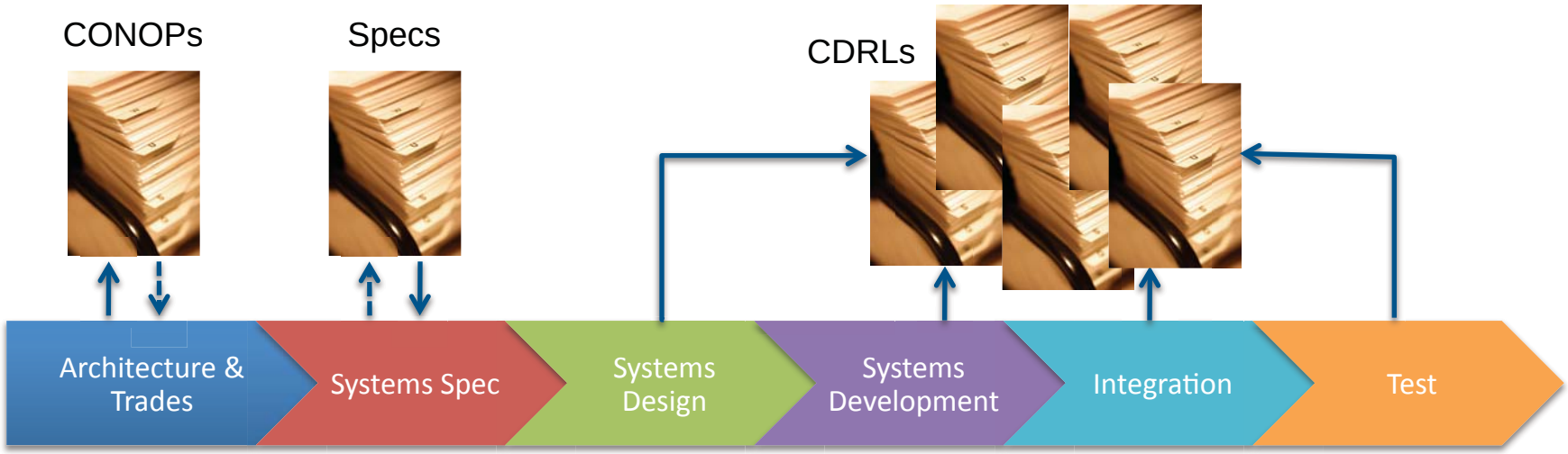
Model Explosion

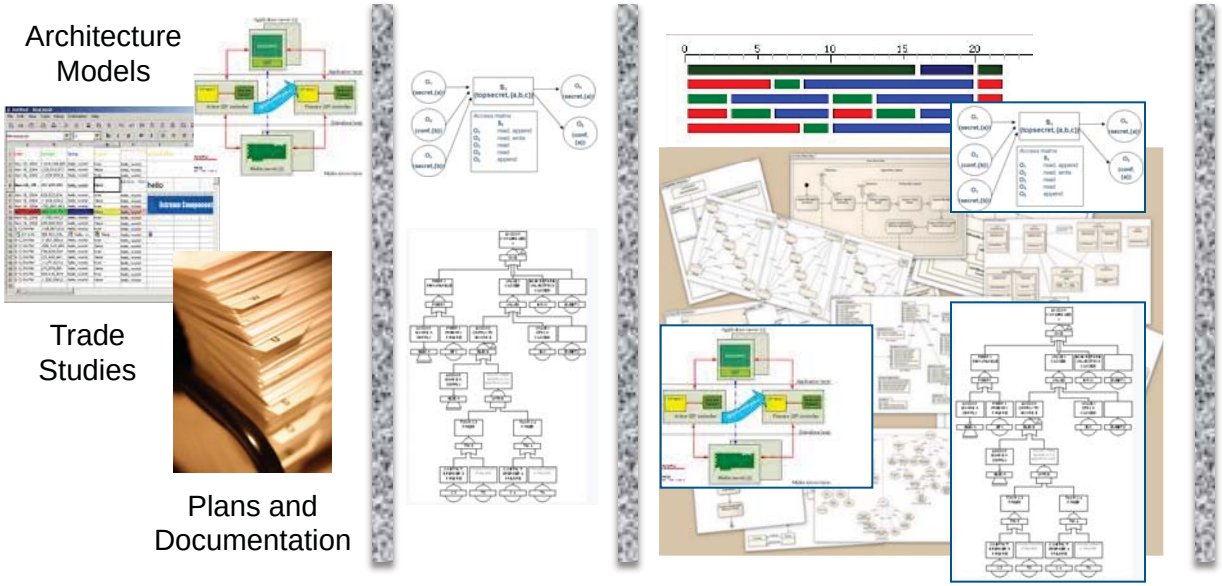
- Operational Models
- System Models
- Component Models
- Functional/Behavior Model
- Performance Model
- Structural/Component Model
- Cost Model
- Safety Model
- Security Model
- Reliability Model
- Maintainability Model
- Structural Model
- Mass Production Model
- Manufacturing (Assembly) Models



- Modeling Domains
- Ops/Mission Analysis
- System Design
- Algorithm Development
- Hardware Design
- Software Design
- Logistics Support
- Manufacturing
- Integration & Test
- Performance Simulation
- Engineering Analysis
- Human System Integration
- System Architecture Model (Integration Framework)
- Analysis Models
- Hardware Models
- Software Models
- Verification Models

Segmented Development Lifecycles Underachieve the Promise of MBSE

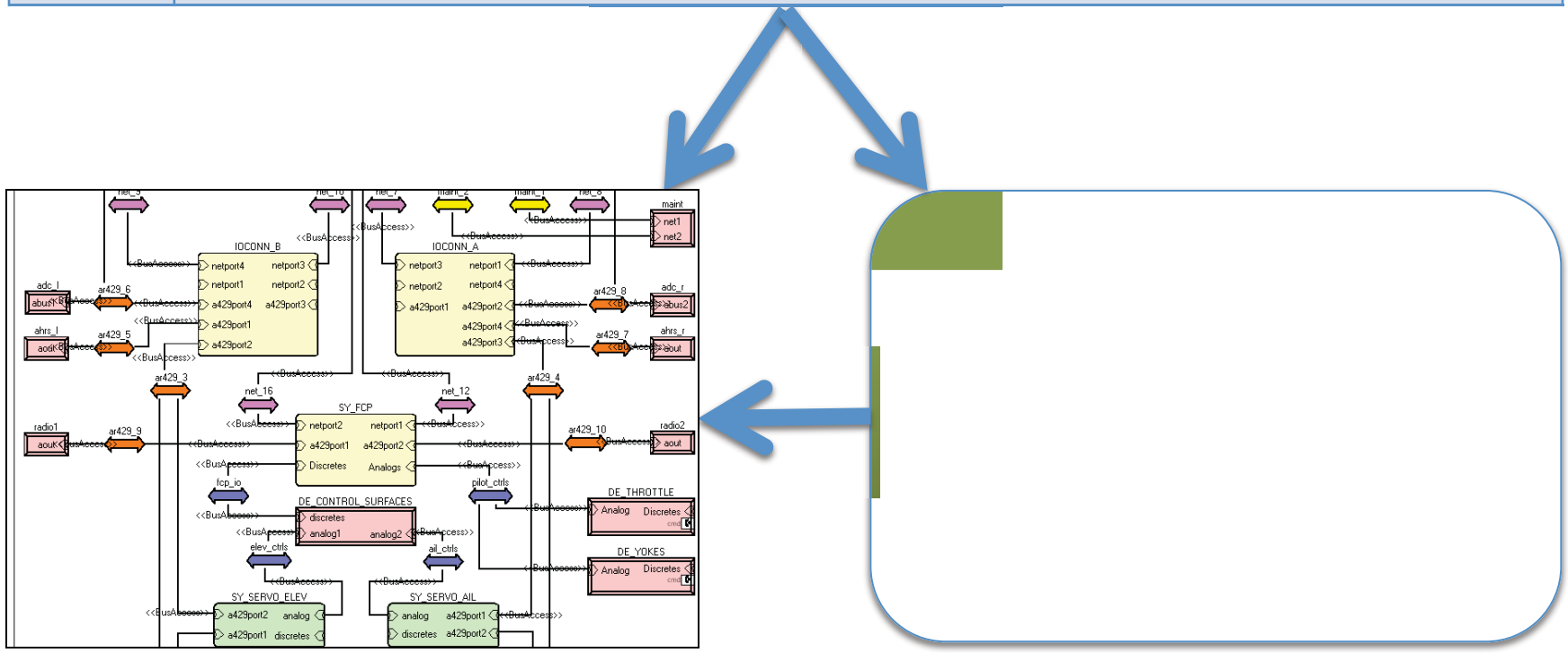




Verification

*Does the system do what it was **specified** to do?*

1.1	**The power supply bus capacity shall be 100 W.**
1.1.1	Any component attached to the power supply bus shall draw less than 20W.



Requirements-Based Testing

Verification

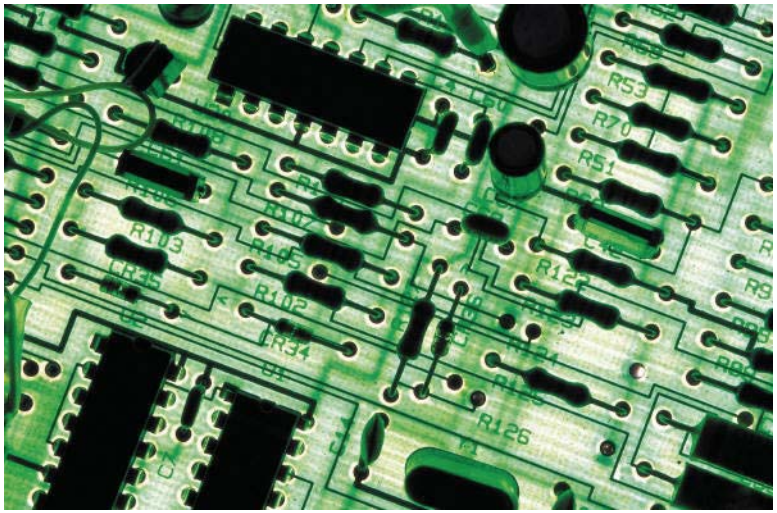
*Does the system do what it was **specified** to do?*

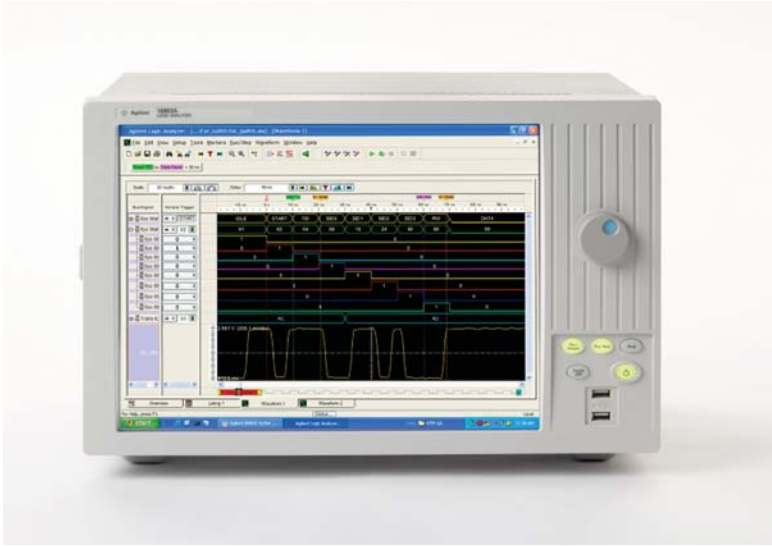
Current State	Future State
• Paper/English Specs	• Models as specs
• Paper/English Design documentation	• Model-based design documentation
• Paper/English Test Plans and reports	• Auto-generated test plans and reports
• Manual execution of test cases	• Automated testing and proofs

Most SE modeling languages/tools can help here.

Validation

*Does the system behave the way it was **intended** to behave?*

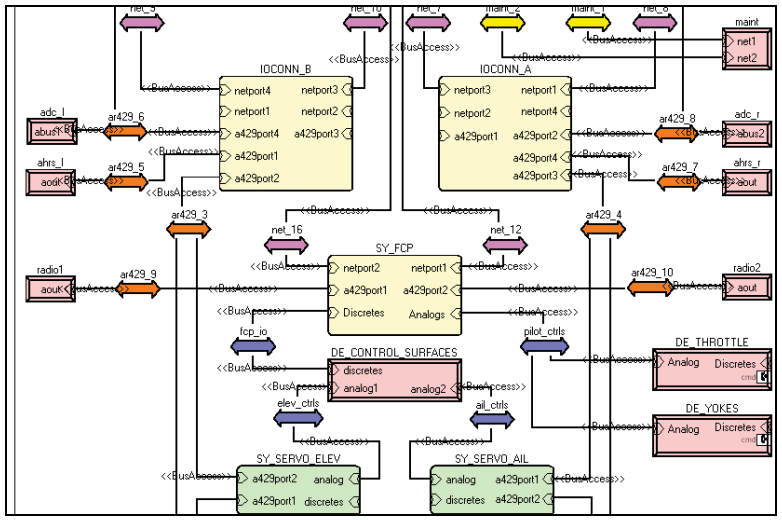




Functional Testing

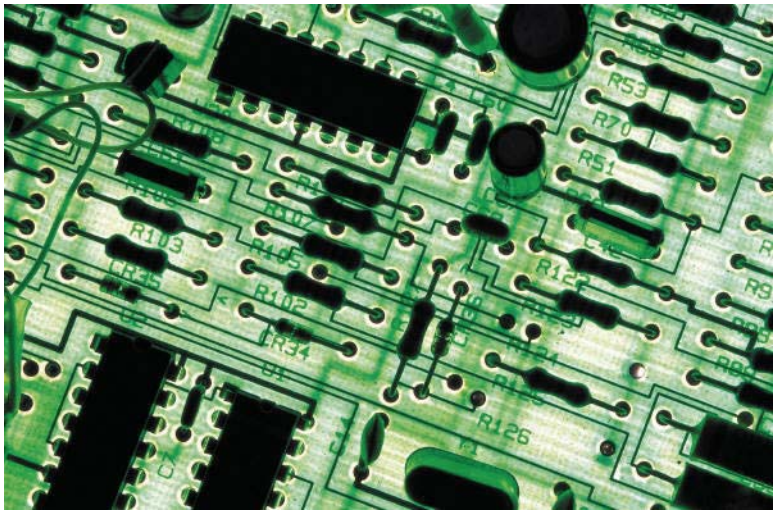
Validation

*Does the system behave the way it was **intended** to behave?*



?

=



Model Fidelity Testing

Validation

*Does the system behave the way it was **intended** to behave?*

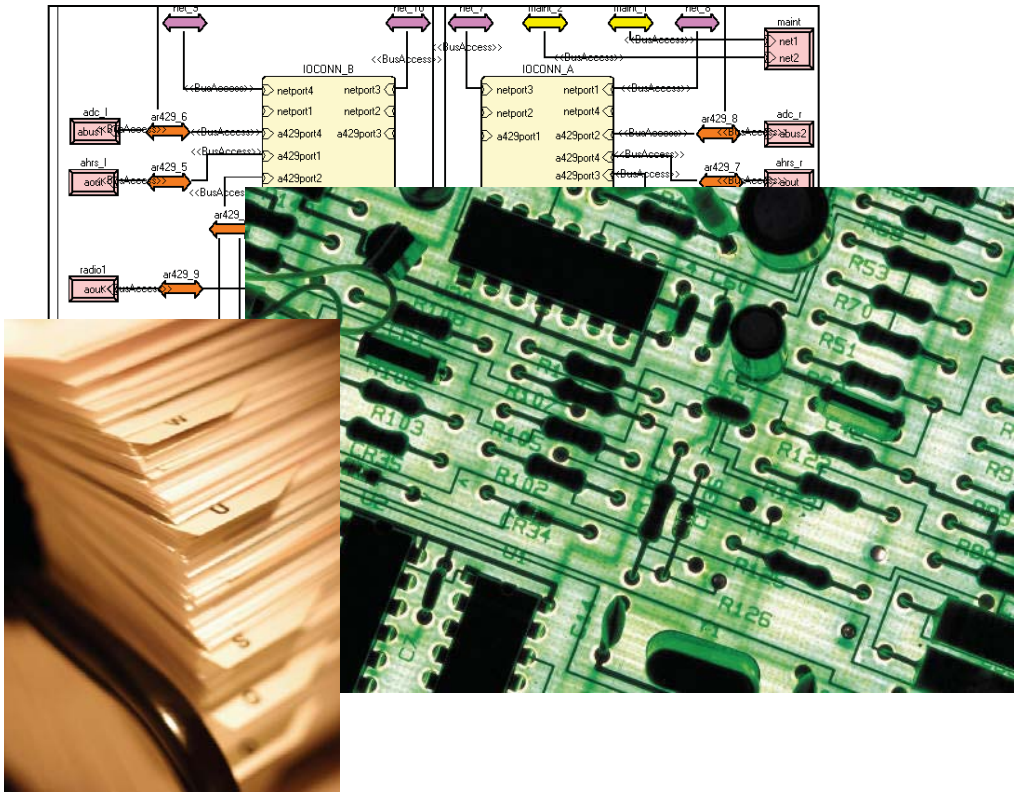
Current State	Future State
• Isolated, domain-specific models	• Integrated, domain spanning analytical capability
• Validated against physical prototypes after designs largely committed	• Validation in simulated environments
• Sporadic, manual use of correct-by-construction techniques	• Validation through broad use of correct-by-construction techniques

Will required semantic precise modeling languages to achieve full benefit.

Accreditation

*Is there sufficient **evidence** to demonstrate the **safety/effectiveness** of the system?*

- Are approved/controlled processes employed?
- Test artifacts
- Design artifacts



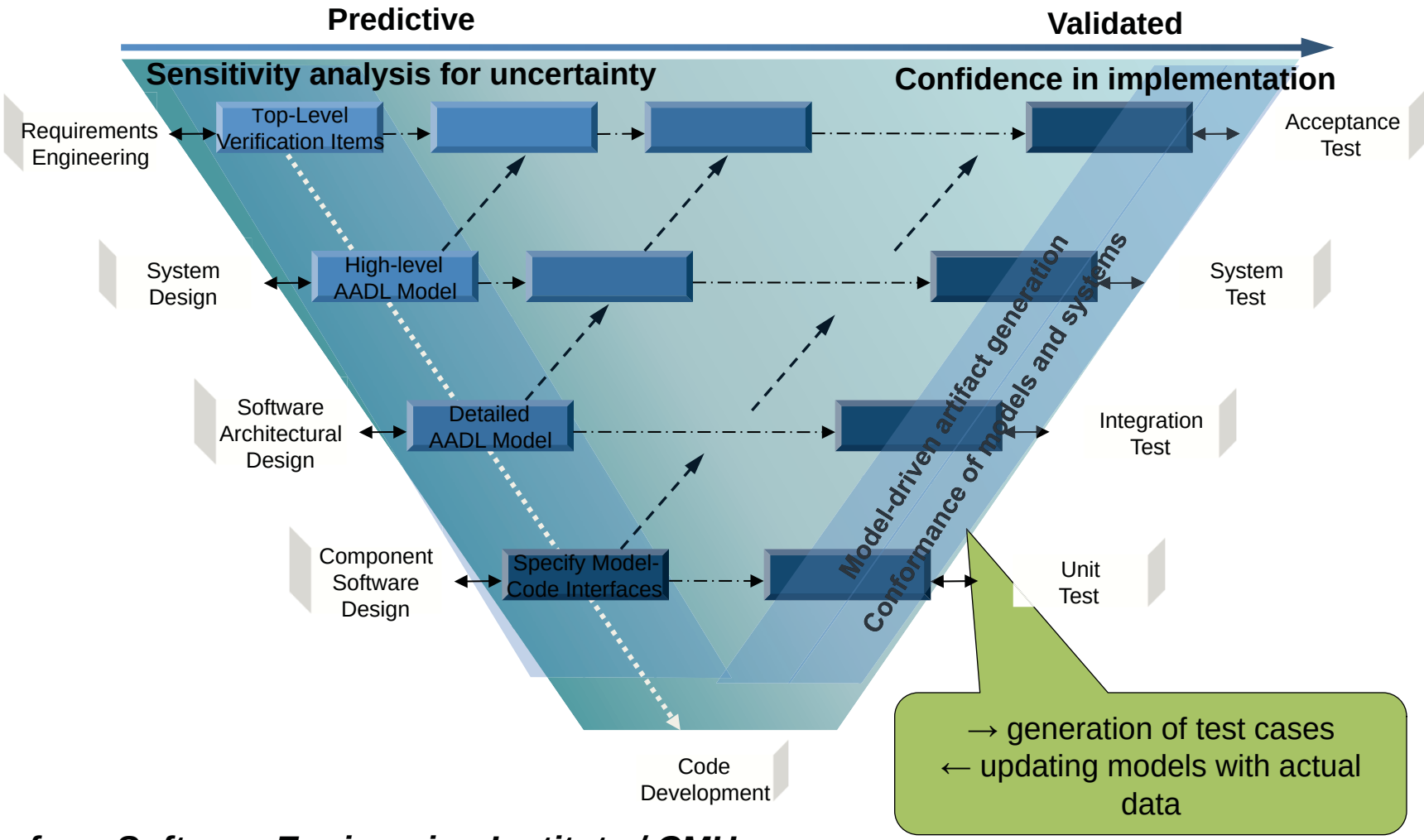
Accreditation

Is there sufficient evidence to demonstrate the safety/effectiveness of the system?

Current State	Future State
• Mountains of documentation that becomes shelfware	• Documented design products and processes as reusable models and tools
• Relies on extensive human review/evaluation	• Trusted evidence that generated using tools/ automation.
• Accredit only completed systems	• Incremental, component based accreditation of composable systems

Will required trusted models and V&V technologies matured in cooperation with certification authorities.

Incremental V&V is the Key



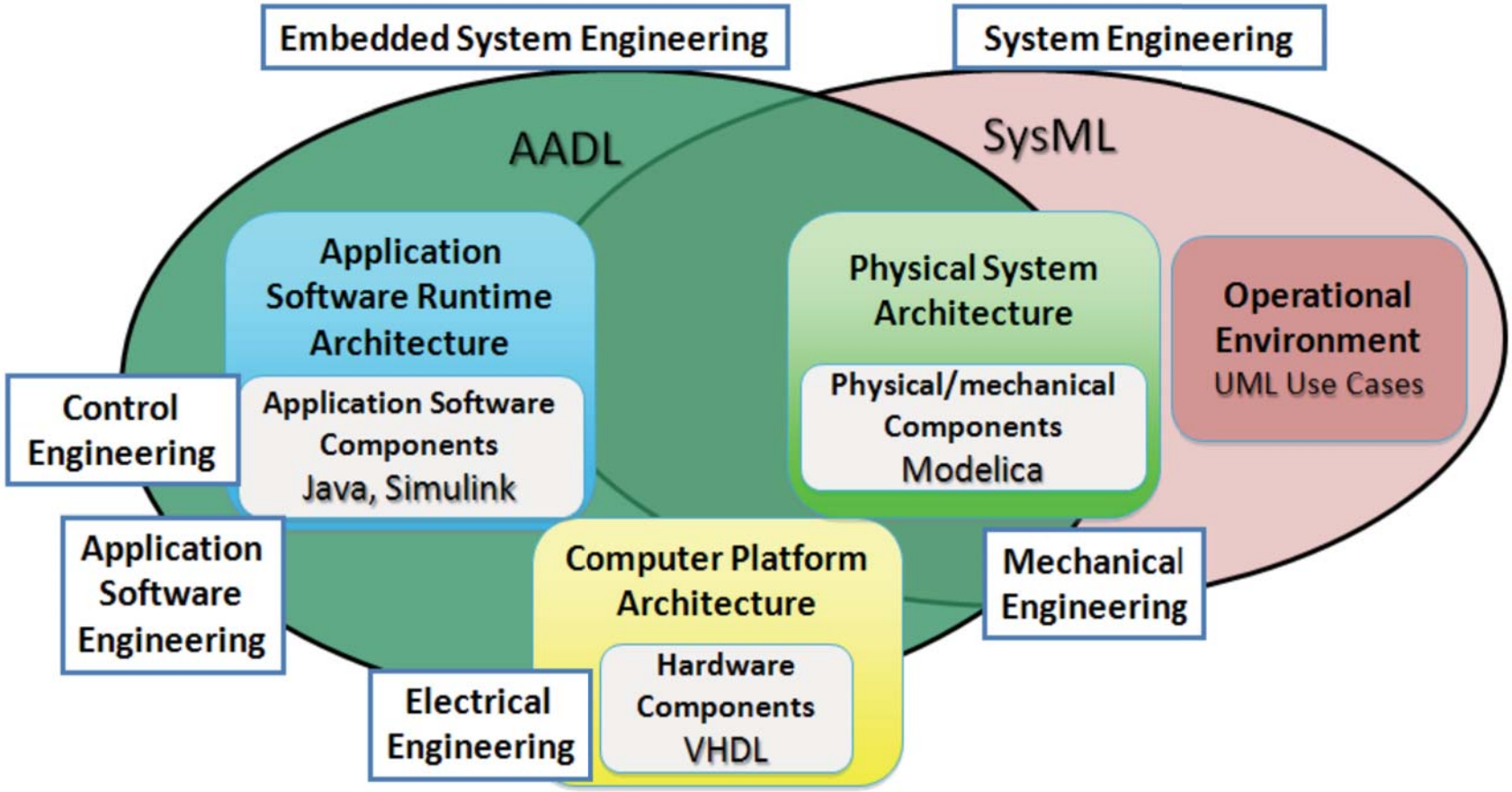
Slide from Software Engineering Institute / CMU

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

How does AADL help with all this?

- Verification
  - Strongly typed language and precise semantics remove the ambiguity of current English Language specifications and enables automation of verification testing
- Validation
  - Strongly typed language allows intrinsic consistency checking
  - Precise semantics allows common understanding of model components across multiple stakeholders
  - Formalism enables model checking analysis
  - Language annex process provides extensibility
  - Designed to accommodate incremental validation ("extends" construct)
- Accreditation
  - Auto-generation of artifacts

Multi-Notation Model Representation Approach with Minimal Information Replication



Slide from Software Engineering Institute / CMU

*Image and Data From: **Challenges in Validating Safety-Critical Embedded Systems,** Peter H. Feiler

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Research Approach

- Model a complex system to explore the benefits of using AADL for VV&A
- Research the viability and capability of AADL to perform early VV&A by modeling a software intensive multifaceted system
- Determine the ability to migrate toolsets to the user community (learning curve, challenges, tool maturity, etc.)

Method for the Research

- Evaluate application of incremental verification and validation process with AADL as it relates to development or qualification of a STIL facility to create an accreditation through analysis
- Develop an AADL initial iteration of the model focused on the critical path
  - Review system requirements
  - Design and model the system architecture at a high-level using AADL
  - Associate model elements with the system requirements using AADL properties
  - Perform analysis using the OSATE AADL toolkit and other tools to check the model for validity and to check if the modeled architecture violates system requirements
- Reiterate the process by refining the model down to a lower level by adding more detail
- At the end of each iteration, trace the system requirements to the model and verification will be performed via analysis
- Determine techniques to validate (and validate if possible)
- Investigate the challenges and advantages of AADL for assisting implementation of VV&A practices and as a mechanism to advance VV&A techniques
- Document evidence that AADL is beneficial for assisting implementation of VV&A practices and as a mechanism to advance VV&A techniques

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Expected Benefits of the Research

- Expand existing SAVI and AADL research in the area of incremental verification and validation on a model using the AADL language to demonstrate benefits for SILs and STILs
- Explore the impacts and benefits of using AADL for VV&A when modeling a complex system
- Consider how it might integrate into an overall process that includes virtual integration and enhanced use of qualified STILs
- Determine the ability to migrate toolsets to the user community (learning curve, challenges, etc.)
- Provide a foundation for this improved approach for future work in our lab and potential training for the community
- Develop a relationship with SAVI for future technology transition Document approach and benefits for OSD

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Why Choose AADL for Modeling Language

- Selected testbed is a hard real-time system, which AADL was created to model
- Strong semantics is well suited for VV&A of these systems
- Established SAE Standard with an active user community
- Availability of tools and support
- Growing capability
- Interfaces with other tools and languages

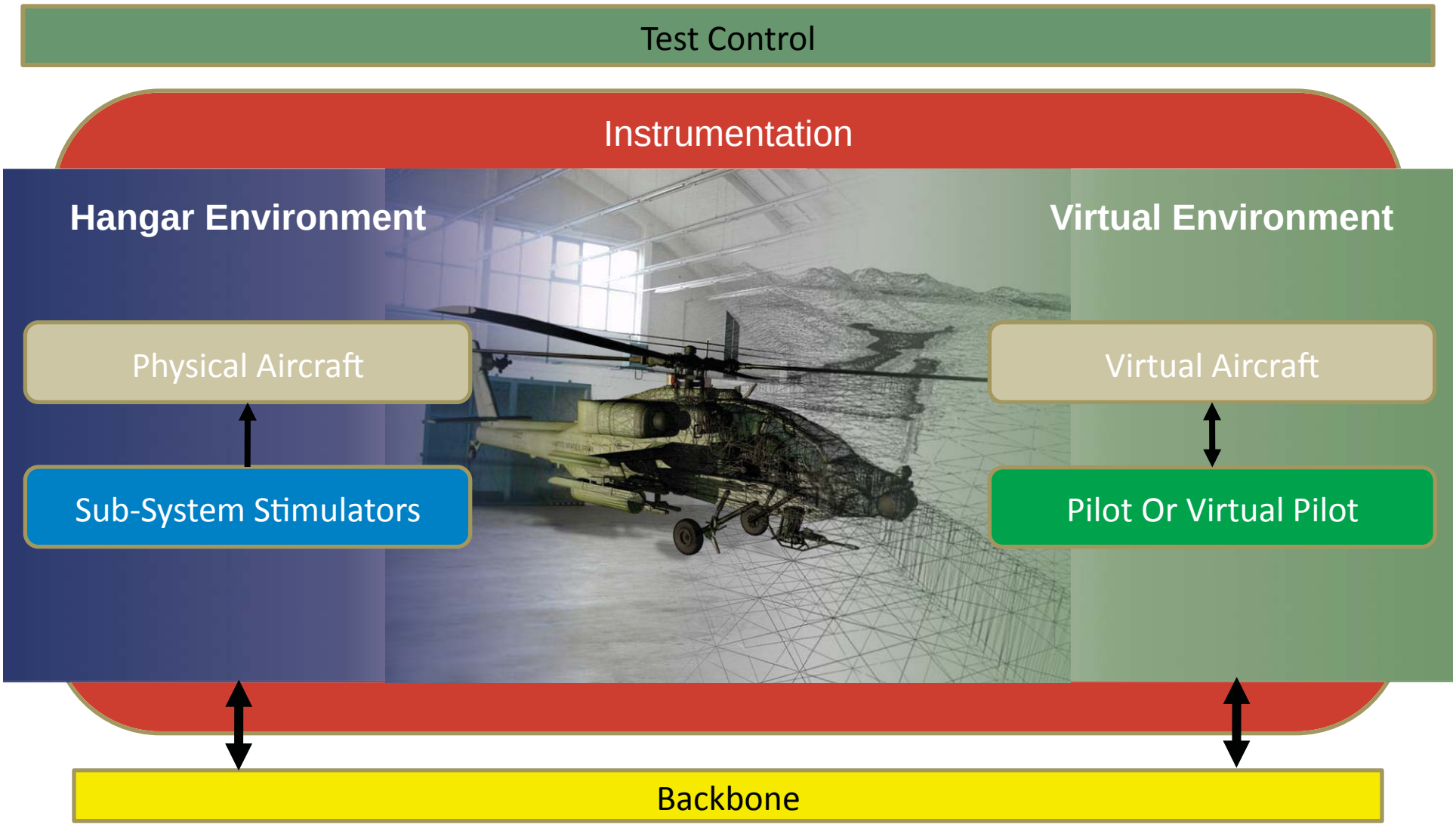
UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Why Model the STIL?

Redstone Test Center's System Test and Integration Laboratory (STIL)

- Provides a real-world problem of concern to DoD (Focus area 1)
- It is a software intensive distributed system that requires precise, and deterministic event ordering in order to meet requirements
- Possibility to incorporate existing models of helicopter systems from SAVI, Aviation Engineering Directorate, PM's or RSESC's research work for this effort or future efforts
- RTC, AED, SED and the PEO-Aviation Platform Offices interested in the STIL
- Users top concern is to not harm the aircraft, validation of the architecture could provide evidence to supporting a risk assessment

System to Model STIL



UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

AADL Overview

- AADL comes from a computer language tradition, rather than a diagrams tradition
- AADL was developed as a programming language not only to define the textual representation of software architecture but also (and more importantly) to formally define the syntax and semantics
- AADL, like its predecessor MetaH, produces language based modeling artifacts

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Why Choose AADL for Early VV&A

- AADL provides standardized, well documented semantics to underlay tools, enabling ease of integration of tools based on AADL
- AADL's strong semantics and textual notation enables integration of architecture specifications across entities. Loose or weak semantics require each user to add semantics which can be a major source of errors, inconsistency, and undefined assumptions
- AADL's well formed architectural behavior semantics cover nominal and fault management behavior, and allow assessment of faulty or incomplete models
- AADL provides incremental verification and validation leading to a qualified system
- At each stage starting with the requirements you validate that the requirements (and then their allocated constraints on the next level) are sufficient and verify the correctness of that level
- The ultimate result through all phases is a qualified system

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

How does AADL support VV&A?

- The AADL is designed for software intensive systems such as the STIL
- By using a standardized foundation (AADL) for the M&S, verification and validation time is reduced.
- Verification is supported by the AADL syntax checker and analysis tools that can find problems with the construction of the model
- Validation is supported by having a prebuilt simulator that will reduce errors caused by building a custom simulator. By generating software code using the AADL model, the implemented system is more likely to correspond to the model and simulation

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

VV&A for this Effort

- Verification
  - Analysis tools will be used to verify that the model compiles correctly, and that it meets its derived requirements for the architecture level above it
  - For instance, flow specifications will be used to verify that data and events flow through the system as planned and within time bounds and that processor and bus utilizations are within specification.
- Validation
  - Test cases will be produced and the expected results will be compared to the result of the simulation.
  - Model predictions will be calibrated against measurement on the STIL system and algorithms adjusted to enhance predictive capability from the models

Schedule and Deliverables

Date	Activity	Deliverables
—	1) Meetings	—
7/2010	a) Conduct Kickoff Meeting	Presentation
9/2010	a) Interim status review meeting	Presentation
—	a) Continue working with the Aviation Engineering Directorate (AED), the Software Engineering Directorate (SED) and the SAVI initiative by arranging regular meetings to leverage work that is presently being done and coordinate efforts.	—
12/2010	a) Status Meeting	Presentation
1/2011	a) Phase 1 Final Review	Presentation and demo
—	2) Demonstrate AADL-based VV&A capabilities in the context of conceptual architecture modeling	—
10/2010	a) Model Conceptual Architecture in AADL based on information from STIL POC.	AADL models with final report.
11/2010	a) Conduct verification of the conceptual model by tracing model to system requirements, using AADL tools, and working with STIL POC.	Results in final report
1/2011	a) Demonstrate how AADL can aid in conceptual architectural verification.	Presentation and demo

Schedule and Deliverables (cont)

Date	Activity	Deliverables
—	3) Demonstrate AADL-based VV&A capabilities in the context of runtime architecture modeling.	—
11/2010	a) Model a subset of the STIL Runtime Architecture focused on Time-Space-Position Information (TSPI) data flow.	AADL model with final report
12/2010	b) Perform runtime model verification using model traceability and AADL tools.	Analysis results in final report
12/2010	c) Perform validation of the STIL runtime architectural model.	Validation results in final report.
1/2011	d) Demonstrate how AADL can aid in runtime architectural validation.	Presentation and demo
1/2011	4) Develop Final Report	Phase 1 Final Report
	a) Description of tools and techniques used during the verification and validation process.	—
	b) Verification and validation results	—
	c) Provide drawings and overview description of each model	—
	d) Overall assessment of AADL and its impact on VV&A	

Deliverables

- Milestone Presentations
- AADL Demonstration
- Final Report

Demonstration

Demonstration will include:

- Overview of the task
- Automated units consistency
- AADL language checking
- Model constraints checking
- Analysis tools

Final Report

Final Report will include:

- Evaluation of VV&A capabilities of AADL
- Approach
  - AADL Description
  - Tools
  - Modeling process
  - Verification and validation techniques
- Models
- Results
  - Verification results
  - Validation results
- Conclusions

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

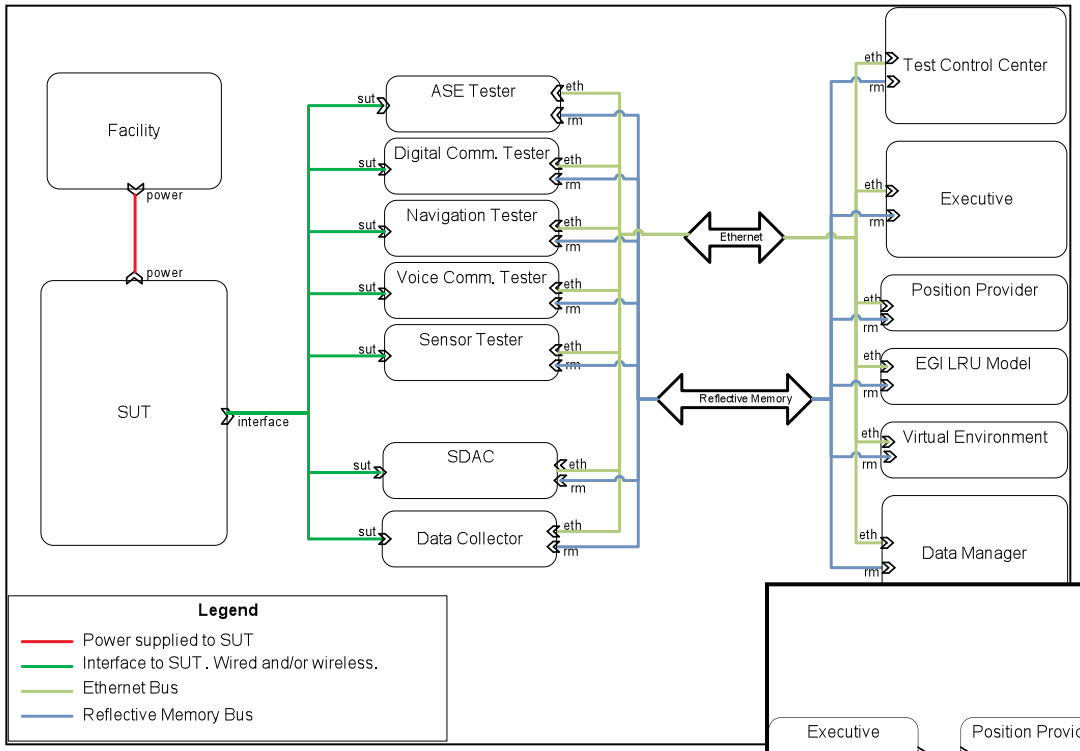
Present Status

- Currently creating model of the critical path
- The high level model will contain
  - Top level systems
  - Logical connectivity expressed using port groups
  - Physical connectivity expressed using buses

Critical Path

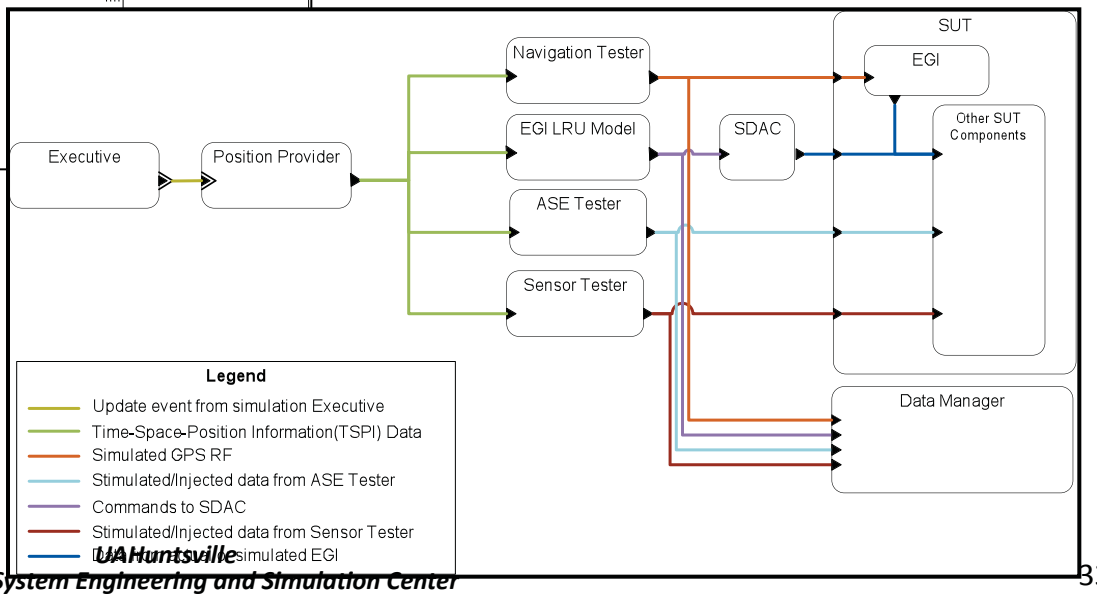
- Critical path for analysis is the Time, Space, Position Information (TSPI) data for the STIL
- Analysis will be performed on Reflective Memory versus Ethernet, the impacts of each configuration and how the STIL can be VV&A in regards to TSPI data

Current AADL Model



Conceptual Bus Connectivity

TSPI Data Flow Model



Challenges

- Complexity of the STIL
- Imprecise requirements for the STIL
- Maturity of the AADL tools
- Ability to make seamless two-way use of analysis tool results between this lower level and the architectural level

Future Work

- Continue expanding the STIL model to include other testers and subsystems to continue to explore
  - the benefits of using AADL for VV&A
  - can VV&A techniques be used on other existing models
  - combining AADL with SysML
  - the ability to model an entire system while including VV&A
  - integration of the STIL model with the Helicopter model
  - improving evidence from the STIL through a qualification for purpose through the architecture assessment and testing of the model to the environment
- UAHuntsville is in the process of creating new graduate programs in the Electrical and Computer Engineering department
  - First course will be in Software Safety Assurance,
  - Expansion of the model based design courses, where simulink as a modeling tool and produce real software (and/or hardware) from the model
  - Evaluating the inclusion of AADL as part of the degreed program
  - Explore improved methods to VV&A models and simulations

Acknowledgements

- PEO-STRI, PM-ITTS
  - Darrell Wright
  - Ken Porter
  - Jim Heinrich
- Dr. Bruce Lewis – US Army Research Development and Engineering Command, Software Engineering Directorate
- Dr. Peter Feiler - Software Engineering Institute, Carnegie Mellon University
- Dr. Dave Redman – AVSI, Texas A&M University
- Dr. Don Ward – AVSI, SAVI Program, Texas A&M University,
- AVSI SAVI Program Participants
- AADL Users Group
- PEO- Aviation Cargo Program Office – Mr. Jeff Langout
- Army Aviation Engineering Directorate – Mr. Alex Boyds and his staff
- AMRDEC – Dr. Jim Snider

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

References

- **The SAE Architecture Analysis & Design Language (AADL) Standard,** Peter H. Feiler, Software Engineering Institute, January 2008.
- **Challenges in Validating Safety-Critical Embedded Systems,** Peter H. Feiler, Software Engineering Institute, Copyright © 2009 SAE International, 09ATC-0271.
- **Diagrams and Languages for Model-Based Software Engineering of Embedded Systems: UML and AADL,** *Dionisio de Niz, Software Engineering Institute, Carnegie Mellon*
- **Multi-Dimensional Model Based Engineering for Performance Critical Computer Systems Using the AADL,** B. Lewis, P. Feiler, *ERTS 2006. 25-27 January 2006 . Toulouse.*
- **System Architecture Virtual Integration: A Case Study,** P. Feiler, L. Wrage, J. Hansson. *ERTS2010.*

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Questions

Contact Information

Sue O'Brien
Univ of Alabama in Huntsville
Acting Director RSESC
256-824-6133
obriens@uah.edu

Back-Up

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

AADL Overview

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

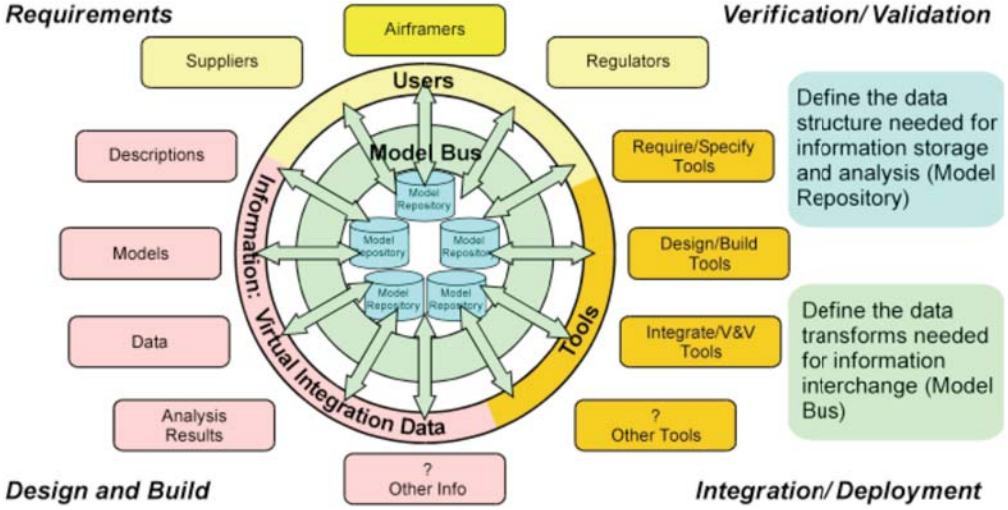
AADL VS UML

	UML	AADL
Origin	Diagrams Tradition	Language Tradition
Purpose	Depict functional structures	Define runtime behavior
Representation	Diagrams; graphic	Textual and graphic
Verification	----------	Automated analysis

Reference: **Diagrams and Languages for Model-Based Software Engineering of Embedded Systems: UML and AADL,** *Dionisio de Niz, Software Engineering Institute, Carnegie Mellon*

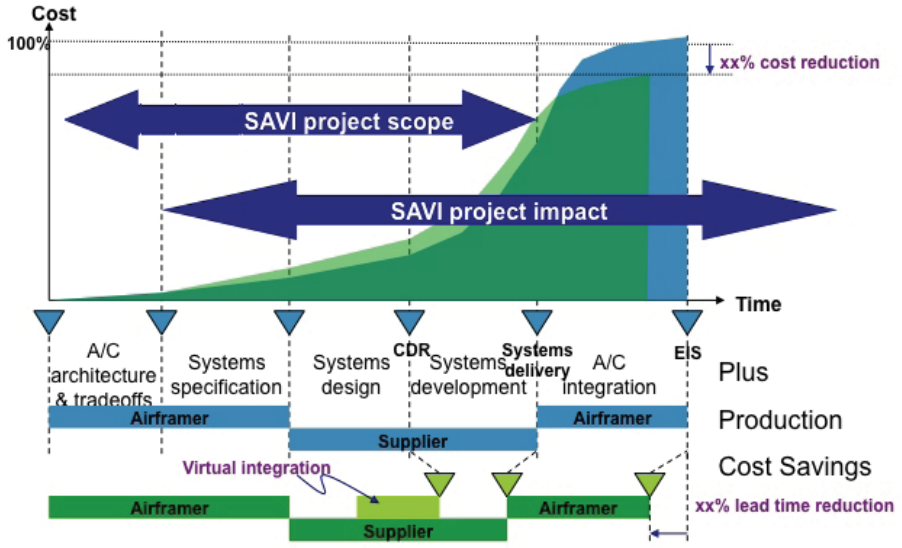
Virtual Systems Integration Uncovers Errors Earlier in Development

**** Slide Provided by the Aerospace Vehicle Systems Institute***



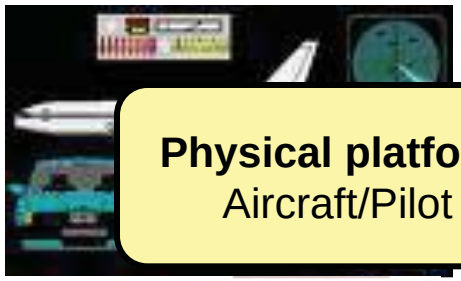
Standardized architecture language with strong semantics, the Model Bus and Model Repository concepts in SAVI enable…

... early validation of system and embedded software system behavior to reduce integration errors.



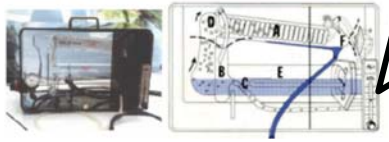
AADL: Focus on the Embedded Software System Architecture

The System



Physical platform
Aircraft/Pilot

Continuous Distiller

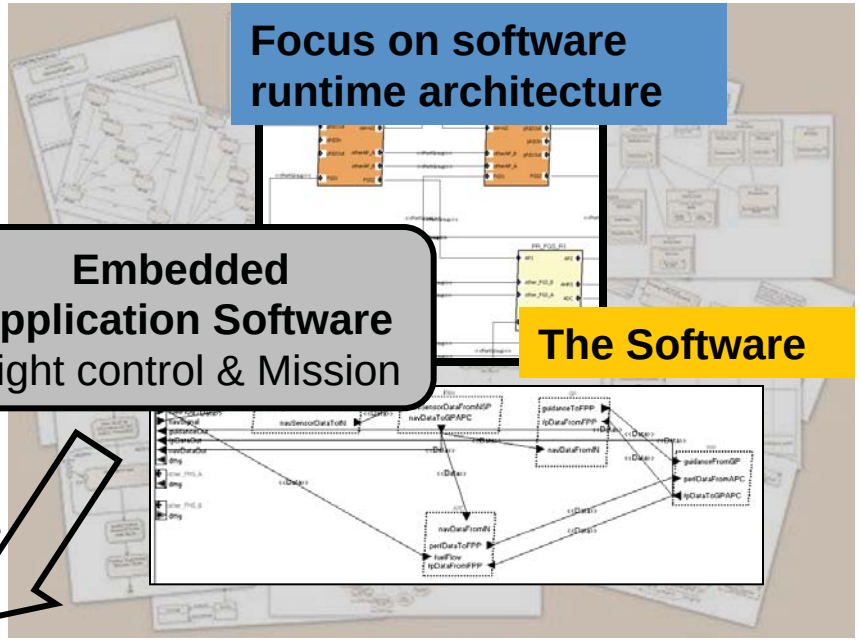


Physical interface
Platform component

Control
Guidance

Deployed on
Utilizes

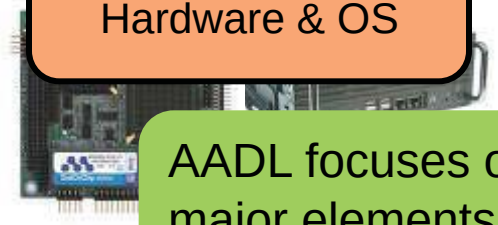
Focus on software runtime architecture



Embedded Application Software
Flight control & Mission

The Software

Computer System
Hardware & OS



The Computer System

AADL focuses on interaction between the three major elements of a software-intensive system based on architectural abstractions of each.

**** Slide Provided by the Aerospace Vehicle Systems Institute***

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Why Choose AADL for Early VV&A (cont)

- AADL offers strong potential for interfacing with analysis tools currently in use through a standardized XMI (extraction of data) and through user defined property sets (declaration in the model of data).
- AADL models are compiled, allowing full semantic checking for correctness (inconsistent specifications will not compile).
- AADL semantics provide a bridge to formal analysis and proof checking for correctness (AADLtoMaude, Alloy based verification, BLESS proof generation, AADL to FIACRE to Model checkers).
- AADL semantics support correct by construction approaches and precise generation for automated system integration (METAH, TASTE, OCARINA), a necessary capability for creating systems to the models without the risk of introducing new errors.
- AADL is constructed for incremental development, with incremental validation to higher level constraints (requirements at the top) and verification of correctness at each stage of system design, proceeding to a precise generative integration of the system. It supports layered evidence of correctness of from low level components to high level architecture through layered abstraction.
- Most systems considered complex are software driven, the integrated behavior of the system can not be understood in advance without understanding the software and the runtime system that drives it. This is the major issue driving up the cost of aviation systems.
- To understand integrated behavior, the physical hardware, the software and the computer system must all be part of the specification. AADL specifications capture all three elements for integrated analysis.

Sampling of AADL Experimenters/Users

- System Architecture Virtual Integration (SAVI) of AVSI Boeing, Airbus, Lockheed Martin, BAE Systems, Rockwell, GE, Goodrich, FAA, DoD, Army, NASA. Also potential members of SAVI looking at AADL - Embraer, Thales, Dassault, European Space Agency, Japanese Space Agency (JAXA), United Technologies and Sikorsky, Honeywell, world class automotive company
- Support for Predictable Integration of mission Critical Embedded Systems -SPICES - ITEA Project of 16 organizations in Europe including Airbus, Thales ...
- ASSERT - EU Project of 20 organizations in Europe including Thales and Astrium ...
- TOPCASED - European research program on Model Bus. Perhaps 30 organizations, some of which are using AADL.
- ARTIST II - 7 year European large scale research program, some using AADL.
- Open Group - International standardization organization looking to adopt AADL as a bridge to formal methods to evaluate correctness of systems. Many members (40-60).
- Open Group Japan (transition of key technology to Japan, involved in research across large Japanese companies), IPA (Govt equivalent of DARPA), JAXA
- Research community working Model-Based Development and advanced architecture based analysis - about 50 organizations across 200 plus papers using AADL.
- US Army - AMRDEC, Apache, CAAS, Reliability (and Safety) Framework, SBIR on error propagation and containment using AADL
- SEI - developing advanced analysis approaches for architecture centric development, Architect for AADL language, Developer of OSATE, the reference toolset for AADL.
- NASA - New IV&V approach developed using AADL, Architecture study of Robotic Vehicle with AI.
- Air Force, Wright Patterson, AFRL - Three trained in AADL from lab in advanced system development. SBIR's using AADL.
- Air Force, Eglin, AFRL - four trained in AADL in lab for weapons development, SBIR's using AADL.
- Aerospace Corporation - Developed and using Dependability Analysis toolchain based on AADL on AF satellite programs.
- ESA - Developed new system engineering toolset and has started to apply in lab demonstration programs, based on AADL and correct by construction concepts. Moving toward integration into ESA programs through demonstrations of redevelopment of current subsystems on satellites.
- META - New DARPA program focused on verification and validation during system construction of Cyber-Physical Systems. Using AADL, SysML and Modelica as starting points, strongly oriented to tight semantics for evidence of correctness and highly integrating and automating the process from system development to manufacturing.
- Four out of five government labs visited in France, including VERIMAG, LAAS, and INRIA, ANR were using the AADL.
- Key researchers in the US in the area of software/system verification in the US and Europe. See "Software Reliant System Qualification" by Peter Feiler to construct a list. See also Peter Feiler list of research papers.
- Various architecture description languages that incorporate parts of AADL (MARTE and EAST but both with loose semantics).
- China - level of interest may be significant.
- Other countries - AADL spreading via graduating PhD students. For instance, Professor in Saudia Arabia is developing our AADL Requirements Annex.

STIL
Overview

System Test and Integration Lab

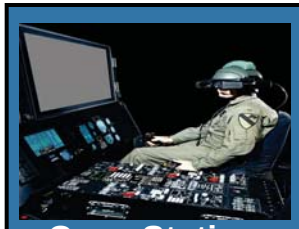
Test Control Center

Executive

Position Provider

EGI LRU Model

Virtual Environment



Crew Station Interface

Subsystem Testers Capabilities

- Navigation Systems
- Sensor Systems
- Aircraft Survivability Equipment
- Digital and Voice Comm Testing
- Test Support
- Modeling and Simulation
- Weapons and Armament Systems
- Human Factors Engineering
- Perform and Handling Qualities
- Crew Station Interface
- Aircraft Systems Testing

Facility

System Under Test

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

System Test and Integration Lab

- STIL will provide a synthetic environment capable of immersing an instrumented aircraft and its systems in a controlled, repeatable and distributed virtual environment to enhance test capability; augment open-air testing; mitigate program risk, cost, and schedule; and provide a collaborative environment for system of systems testing.
- STIL provides a real-world problem involving a software intensive distributive system that requires precise, deterministic event ordering in order to meet requirements.

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Aviation STIL
Key Performance Parameters

Capability	Block I	Block II	Block III	Remarks
KPP-1: Architecture				
a. Virtual Test Environment	P	X	F	Delivery of virtual environment for Navigation and ASE plus Multi-aircraft support for CH-47 and UH-60M. Delivery of virtual environment for Weapons, Sensors in Block III
b. Interfaces	P	X	F	Interface ASE to Architecture in Block I, NAV in Block II and Others in Block III
c. Allow for Human in the Loop	P	X	F	Prototype in Block I and Delivery in Blocks II and III
d. Exchange SUT data as required	P	X	F	Interface CH-47F in Block I, other SUTs in Blocks II and III
e. Expandability	P	X	F	Expandability
KPP-2: Bused Aircraft	P	X	F	Must be able to communicate with Bused Aircraft
KPP-3: Central Control or Stand Alone	P	X	X	Develop of central control that will be driven from TCC. Selected Stand Alone ASE for Block I. Delivery of Central Control and Stand Alone Navigation and ASE in Block II. Delivery of remaining Instrumentation based on priority and Funding
KPP-4: TCC Connect thru DREN	P	X	F	TCC-Lite (6 Workstations, Printer, two 50" displays) Delivery of Initial TCC DREN connectivity at 1Gb , Classified capability
KPP-5: Multiple Sensors		X	X	ASE and Navigation Remaining sensors based on Funding
KPP-6: Multiple Aircraft	P	X	X	Prototype with CH-47F Delivery of CH-47F and UH-60M AH-64D Block III, ARH, UAS : Not in Cost estimate

KEY: P = Preliminary capability X = Expanded capability F = Full capability

Why the STIL for VV&A?

- Provides a real-world problem of concern to DoD
- UML, PowerPoint, and other types of drawings of the STIL architecture already exist that can be used as a basis for an AADL model without starting from scratch.
- It is a software intensive distributed system that requires precise, and deterministic event ordering in order to meet requirements.