AADL for DoD Systems

Dr. Raymond Richards
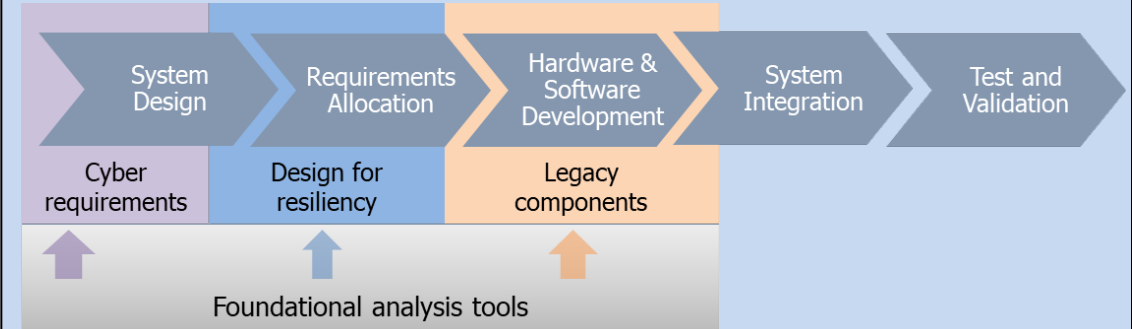Program Manager
DARPA/I2O

AADL Users' Days

November 14, 2019

DARPA Efforts in Digital Engineering

High Assurance Cyber Military Systems (HACMS)
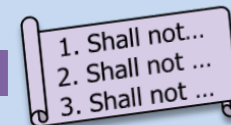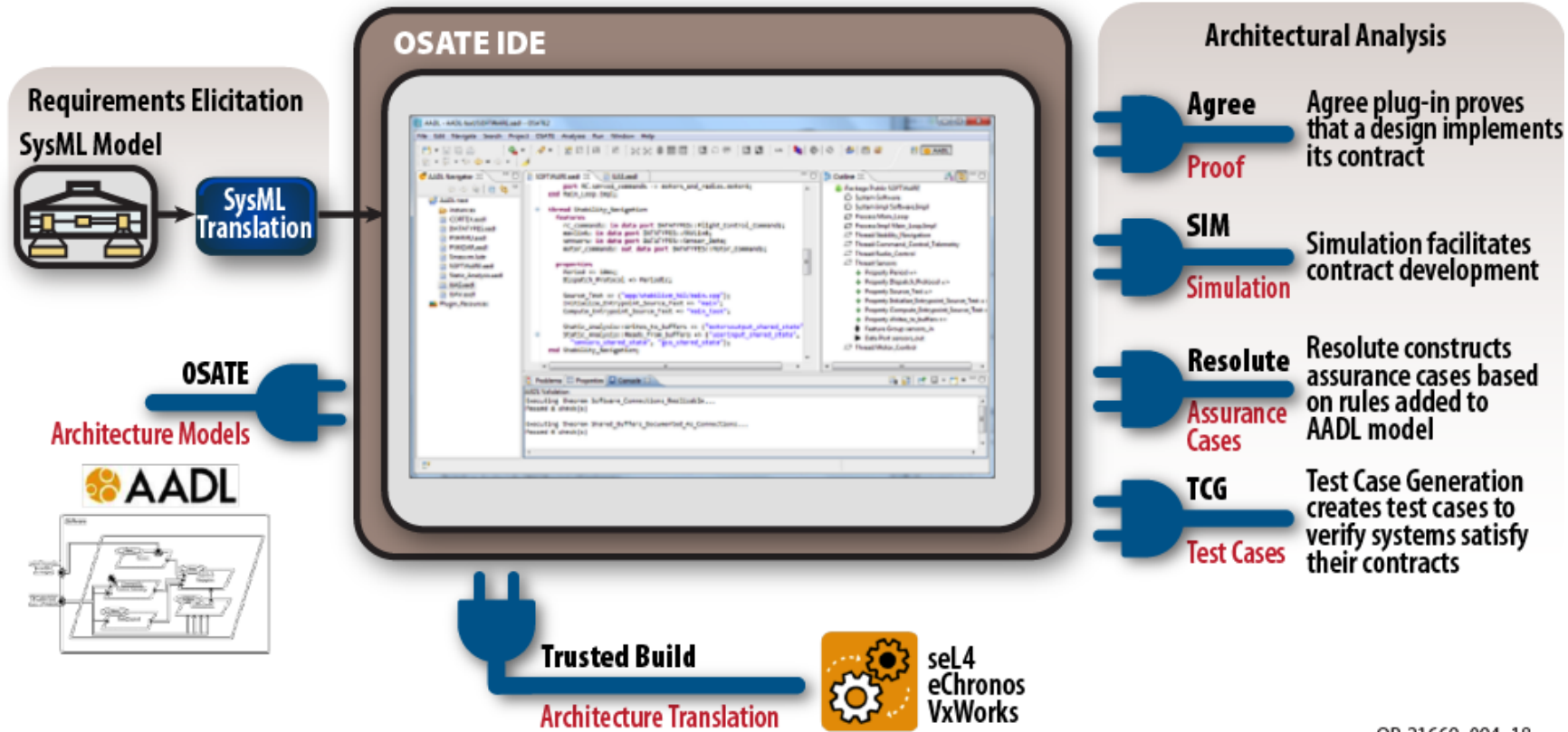Development of cyber hardened software for embedded systems

Architectural-Level Design
Compositional Reasoning

Application-Level Software
Generate from Specification, Correct by Construction, Software Verification, Robust Algorithms

Low-Level Software
Verified OS Kernels

Cyber Assured Systems Engineering (CASE)
Engineering systems for cyber resiliency

System Design	Requirements Allocation	Hardware & Software Development	System Integration	Test and Validation
Cyber requirements	Design for resiliency	Legacy components		

Foundational analysis tools

Explicit system properties
- Reliability
- Availability
- Maintainability
- Performance
- Safety
- many more...
- Cyber resiliency

1. Shall...
2. Shall...
3. Shall...

1. Shall not...
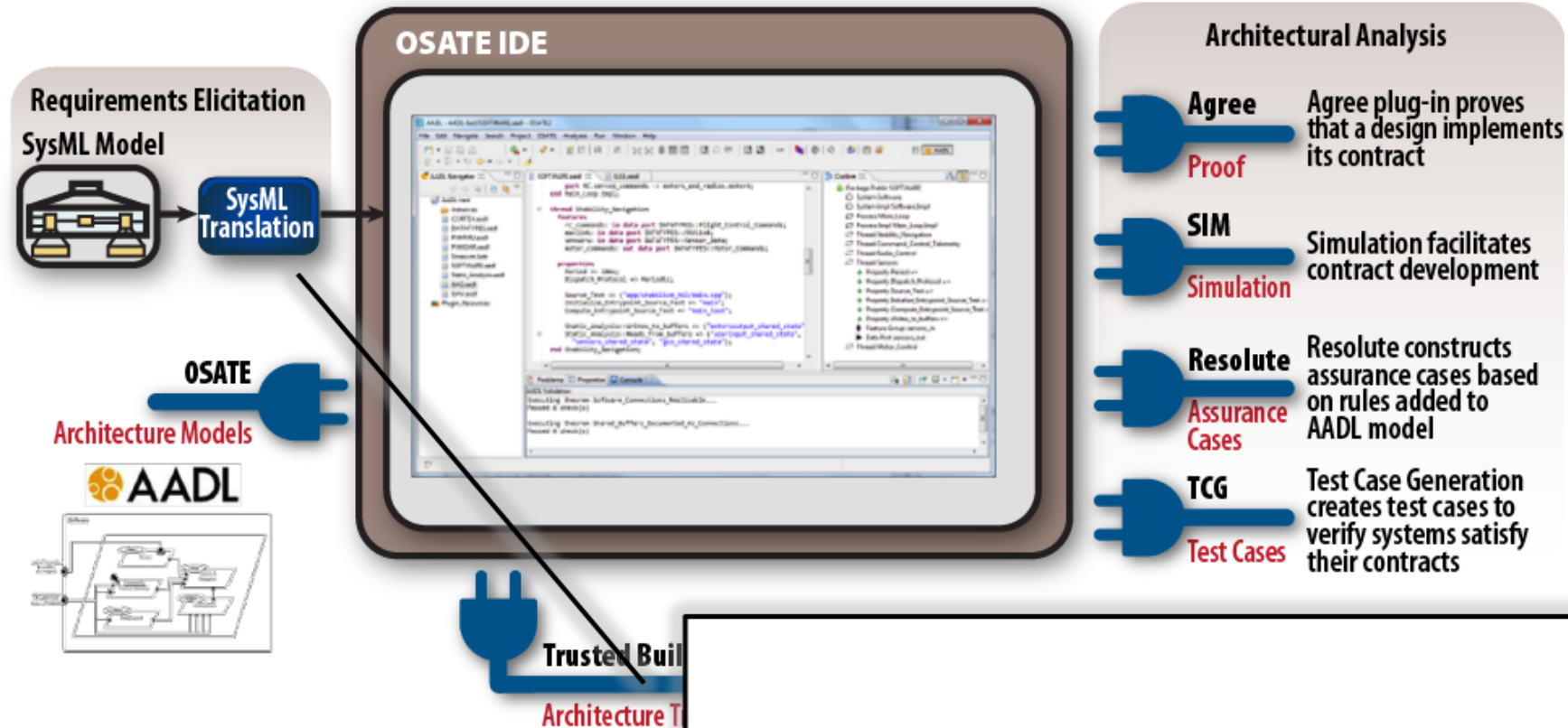2. Shall not ...
3. Shall not ...

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

Requirements Elicitation

SysML Model

SysML Translation

OSATE IDE

OSATE

Architecture Models

AADL

Trusted Buil...

Architecture T...

Architectural Analysis

Agree — Agree plug-in proves that a design implements its contract
Proof

SIM — Simulation facilitates contract development
Simulation

Resolute — Resolute constructs assurance cases based on rules added to AADL model
Assurance Cases

TCG — Test Case Generation creates test cases to verify systems satisfy their contracts
Test Cases

Translations and mappings between models are a must.

- New technologies are inserted into programs once it is demonstrated to be sufficiently mature
  - 'Risk burned down'
  - High TRL
  - Component-level C&A

- Resistance to adopt development approaches that require a restructuring of engineering processes
  - Introduces 'unacceptable risk' to programs

- Model-based tools insert into development process, not integrated into systems.
  - Is adapting MBE a sound business decision?
  - How to industry program managers view process change?
  - How do industry executives view process change?

Defense contractor program management's view

- Manage program for schedule and cost performance
    - Earned Value Milestone is a preferred style of program management for the defense industry
        - CPI, SPI
    - Requires cost, schedule, and execution predictability

- Risks and Opportunities
    - Events that have a probability of occurrence that if realized will increase (risk) or decrease (opportunity) program costs
    - PMs leverage MR to lower risk likelihood and increase opportunity likelihood
        - And to cover 'unknown risks'

http://www.managed-programs.com

- Front loaded modeling, analysis, and verification activity stresses cost and schedule metrics
    - Program may appear to be over budget and behind schedule when compared to traditional process
    - MR will be needed at integration

- Cost-benefit analysis
  - What are the benefits, measured in dollars
  - Capture new business
    - Substantiate with market analysis
  - Reduce costs (cost avoidance is a tough sell)
    - "If I never find a bug, then its free"
  - What is ROI?

    $$FMnre + \sum_i FMrc_i << \sum_i TRADrc_i$$

  - Understand all of the costs
    - How do Formal Methods tools integrate into complex engineering workflows?
    - What is the schedule impact? – with respect to earned value milestones
    - What is the cost impact? – with respect to earned value milestones
    - Training
    - Other costs

orgchanger.files.wordpress.com

Conclusion

- The near future will see a overhaul of the processes used to engineer complex systems
  - The traditional engineering 'V' will be replaced with "verify early, verify often'
  - Engineering artifacts will be design models
  - Required will be the ability to manage, analyze, and move data among models that span the system's lifecycle

- Design language technologies and tools will be the backbone of digital engineering processes
  - An interlocking mosaic of languages to specify and model all aspects of complex systems, across their lifecycles from conception to end-of-life will be needed
  - Research is required on how digital engineering processes can support systems during the sustainment phase of their lifecycle

- Transitioning to model-based engineering
  - Drive down risk by increasing the TRL of the model-based engineering workflow.
  - The MBE has to provide value
    - ROI
    - Direct evidence of costs and benefits of model-based approach is needed but is difficult to get
    - Compelling apples-to-apples numbers
  - Understand how to reliably predict cost and schedule expenditures though the development process

www.darpa.mil