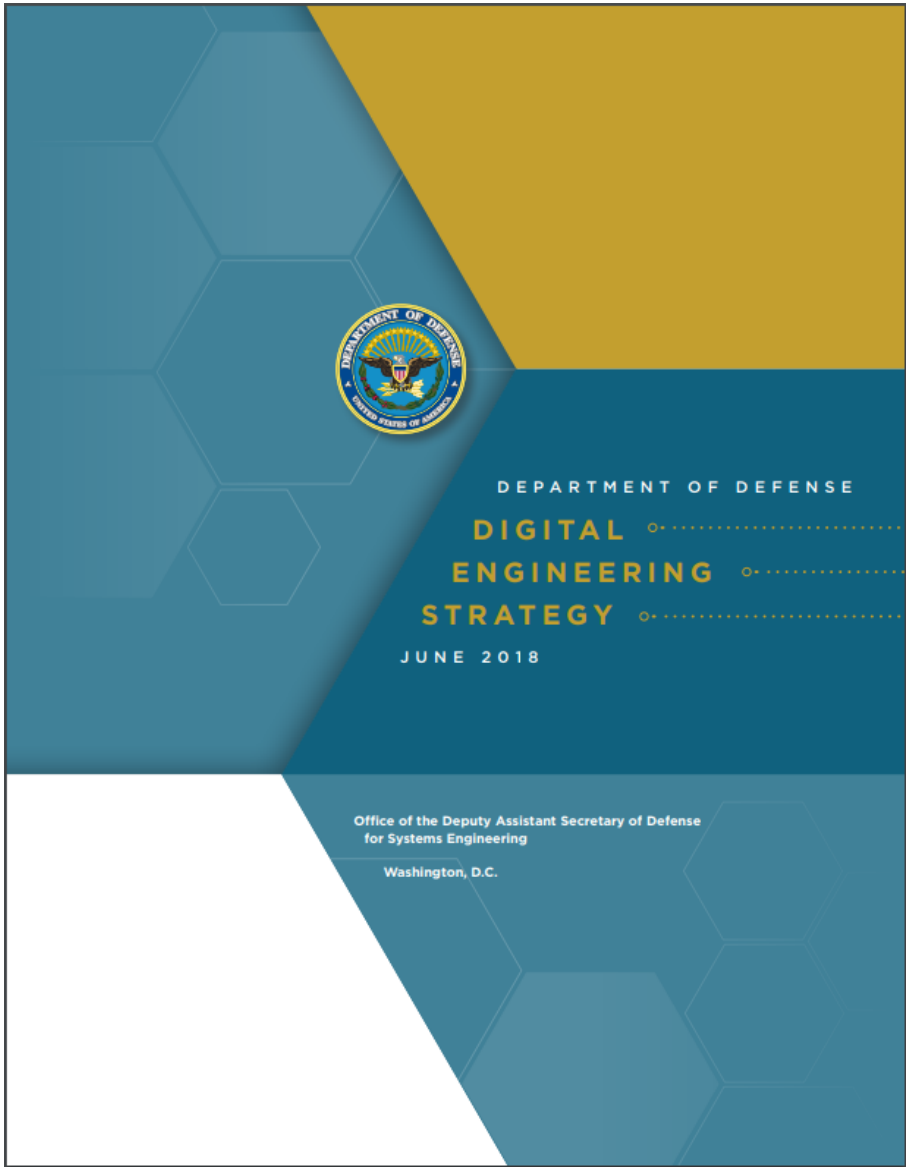
Formal Methods for Systems

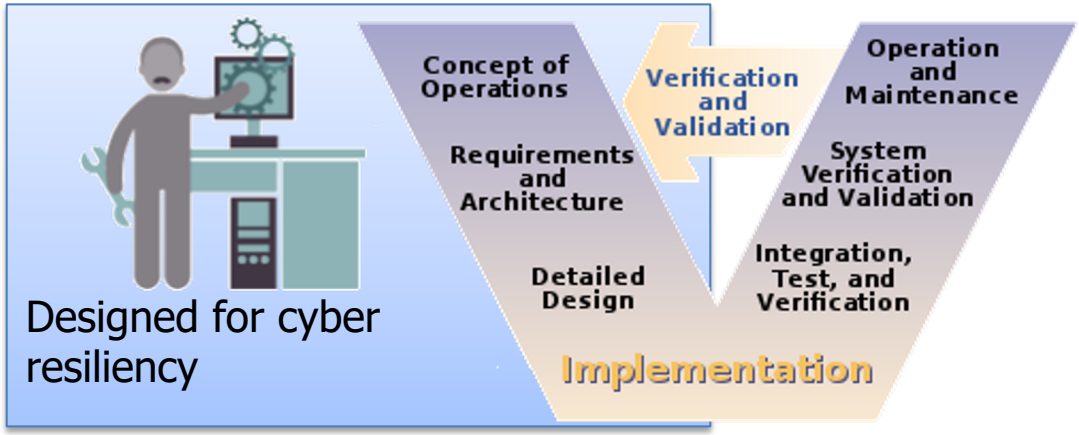
Dr. Ray Richards
I2O Program Manager

January 14, 2021

Digital Engineering Strategy



Cyber Assured Systems Engineering (CASE)



Explicit system properties

- Reliability
- Availability
- Maintainability
- Performance
- Safety
- many more…
- Cyber resiliency

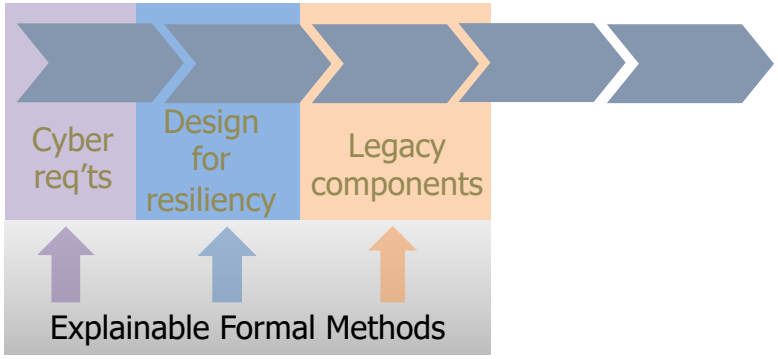
1. Shall…
2. Shall…
3. Shall…

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

- Resiliency is a property that cannot be verified through testing
- CASE is producing technologies to design and verify cyber resilient systems
  - Design-in cyber resiliency as an explicit property of the system
  - Enable informed design decisions when resiliency conflicts with other system properties
  - Provide formal methods tools to validate systems resiliency properties
  - Eliminate need for costly redesign

Explainable Formal Methods

Semantic translators that relate feedback from foundational analysis tools to the design domain

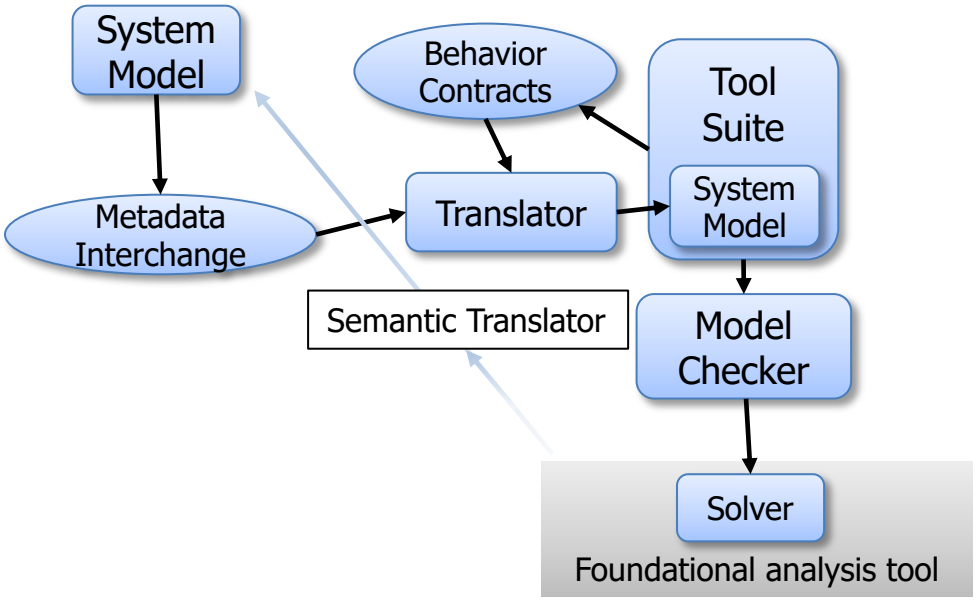


Challenges:

- Bridge the gap between the design domain and the analysis domain
- Increase scalability of component analysis tools

Approach:

- Specialize reasoning engines to scale in the problem domain
- Develop analysis approaches that scale under proper constraints
- Use contextual metadata to relate analysis feedback to design



www.darpa.mil