Model Based Systems Engineering with Architecture-Driven Assurance
NDIA Systems Engineering Conference
Dan Bliek – Principal Systems Engineer
Introduction - Change Drivers

- System Size and Complexity Continue to Grow
- Late Discovery of System-Level Errors Cause Major Cost and Schedule Impacts
- Fielding Times Have Become Unacceptably Long
- Increased Emphasis On:
  - Operational flexibility and technical superiority with rapidly composable heterogeneous systems
  - Dramatic reductions in system fielding times
  - Increased focus on efficient integration and verification

New systems development challenges with familiar overarching theme: “Better, Faster, Cheaper”
MBSE with Architecture-Driven Assurance

Transformational Change To System Engineering Processes And Tools

- **The Goal**
  - Rapidly ensure functionally correct, verifiably safe, and cyber-resilient components and systems

- **Architecture-Driven Assurance - Simple Definition**
  - Representing system structure (architecture) and formally expressed system behaviors (requirements) in analyzable models
  - Enabling early virtual analysis and integration of systems

- **Requires Tools That**
  - Express system architecture using a semantically rich, precise and standard notation
  - Enable formally expressing and analyzing system behaviors
  - Allow formalized requirements to be attached to system hierarchy
MBSE with Architecture-Driven Assurance

Five Precepts of Architecture-Driven Assurance

Provably Correct Requirements
- Behavioral properties formally expressed and analyzable
- Annotate system model components with assume/guarantee contracts
- Compete, correct and necessary

Architectural Model Is Correct
- Identifies system components, interfaces and interactions
- Ability to verify structural properties of the system

Components Are Correct
- Contracts are realizable (implementable)
- Implementation verified with test cases auto-generated from contracts
MBSE with Architecture-Driven Assurance

Five Precepts of Architecture-Driven Assurance

System Implementation Corresponds to the Model
- Build what you analyze
- Generate configuration data and code directly from the model

System Execution Conforms to the Model
- Operating system correctly enforces constructs defined by the architectural model
- Explicit constructs such as execution times, threads and schedules
- Implicit constructs such as no data flow unless explicitly specified
MBSE with Architecture-Driven Assurance

Tools for Architecture Modeling and Analysis
MBSE with Architecture-Driven Assurance

Benefits From Architecture-Driven Assurance

- Early Detection and Correction of Design Errors
  - Design time analysis with virtual integration
- Reduced Requirements Ambiguity with Early Validation
  - Formal expression and analysis of requirements
- Implementation Matches Architecture Models
  - Life-cycle cost savings; model retains value over time
- Hierarchical Models Separating the “What” from the “How” Via Contracts
  - Enabler for 3rd party integration, product-line approaches, and increased reuse
- Improved System/Product Life-Cycle Sustainment
  - Facilitate assessment of component replacement or technology insertions
MBSE with Architecture-Driven Assurance

Conclusions

- Technology Available Now
  - We have the technical capabilities to transform system engineering workflows

- Largest Impediments Are Environmental
  - Procurements based on models
  - Regulatory approvals
  - Inertia within industry to maintain status quo

Maintaining status quo for system engineering tools, methods and procurements will not support demands for increasingly complex systems with decreased fielding times.
Future Work

- Enhance and extend thru ongoing technology programs focused on:
  - Allowing systems engineers to design-in cyber-security throughout the development lifecycle
  - Model-based safety analysis to enable efficient verification and validation of complex safety-critical systems
  - Assurance of autonomous systems and behaviors

- Continue technology transition by applying methods and tools to relevant avionic systems
Questions?

- Contact Information:
  
  Dan Bliek  
  Rockwell Collins  
  [dan.bliek@rockwellcollins.com](mailto:dan.bliek@rockwellcollins.com)  
  (319) 295-8009