MODEL BASED SYSTEMS ENGINEERING & SOFTWARE SYSTEM SAFETY WORKSHOP

2 & 3 MAY 2017

A-P-T RESEARCH, INC.
AN EMPLOYEE-OWNED COMPANY

4950 Research Drive, Huntsville, AL 35805 · www. apt-research.com · 256.327.3373

MBSE KEY POINTS

- MBSE is necessary for program consistency and understanding in complex systems
  - Consistent documentation
  - MBSE pulls together system of systems – integration
  - Leverages greater efficiencies
- Acquisition process/strategies needs to leverage current technologies
  - Have to validate strategy at acquisition level
  - MBSE gives you more than a set of requirements does
- Safety product integration (with requirements development)
- Tool selection and how they interface is important
- Achieve early buy in from all stakeholders
  - Program Offices may not understand MBSE yet
  - Applicable Boards – Joint Services
- Need to mature the MBSE common definitions
  - Partner with INCOSE?
  - Need good guidance/guidelines – best practices
- Assurance organizations need to define new roles, develop new skills, and define products for model based environment
  - Need to bring all the disciplines into this (safety, reliability, etc.) – build a business case
- Consider benchmarking – RTCA DO-331 is an industry standard.
- Develop metrics for evaluating the fidelity of the model over the lifecycle
  - Model selection
  - Model parameters

MBSE WORKSHOP FINDINGS

- MBSE and system safety can provide a beneficial approach for a safety program which improves understanding, creates efficiency, and identifies potential hazards; especially for large and complex systems.
- The disciplines (safety, software safety, reliability, maintainability, etc.) are aligned to the system model.
- Safety engineers must understand the relationship between the model and the safety objective, the model functionality, its inputs, outputs, and limitations, to properly use this approach.
- General concepts of how the tool works need to be understood.
- An important aspect is to include as a requirement for the system model the outputs that provide insight into the behavior of the system functionality and effect of potential system hazards. Potential pitfalls include:
  - Environments beyond system requirements
  - Malfunctions not modeled
- The model can assist in valuable safety tests including: fault tolerance, failure mode effects, fault insertion, failure immunity, and off nominal.