Model-Based Engineering of Dependable Systems with AADL

Presenter(s):
>David Gluch, SEI/Embry-Riddle Aeronautical U., USA (dpg@sei.cmu.edu)
>Bruce Lewis, Army AMCOM SED, USA

Tutorial Overview:

The tutorial provides experiences using the SAE Architecture Analysis & Design Language (AADL) standard for high dependability system analysis and design. Attendees will learn key elements of the AADL and how to apply them in the design and analysis of dependable computer systems. Representative avionics and related application examples using the Open Source AADL Tool Environment (OSATE) are used as demonstrations of the AADL in action. The capabilities to specify fault handling, redundancy, fault-tolerance, and related high dependability design aspects are highlighted. In addition, the AADL Error Model Annex Standard reliability modeling language and its application in dependable system design are presented.

Structure of the Tutorial:

The tutorial will be conducted in two sessions that focus on the high dependability design and analysis capabilities of the AADL and supporting toolset. In the sessions, the AADL is presented as part of model-based and architecture-driven development. A focus is maintained on how the AADL's precisely defined semantics can specify and facilitate the analysis of important performance-critical and dependability considerations such as timing, schedulability, fault and error handling, time and space partitioning, and safety properties.

Employing pedagogical examples, the initial sections of the tutorial introduce key AADL language constructs and demonstrate the features, capacities, and use of the open source OSATE toolset. Throughout the remainder of the tutorial, both slide presentations and examples are used to explore the specification, analysis, and prediction capabilities of the AADL. These demonstrate how AADL-based modeling and pattern-based architectural analysis can identify shortcomings in a design, provide a framework for fault-tolerance, allow trade-offs across multiple performance critical and reliability qualities of an architecture, and establish a foundation for model-based design and analysis throughout the lifecycle of a dependable system.

A laptop computer is not required. However, if a participant wishes to complete the examples with the instructor using a laptop, the OSATE software must be downloaded from the AADL web site (www.aadl.info) prior to the tutorial.

Who should attend:

If you are interested in model-based engineering of dependable systems and understanding the value and capabilities of a precise architecture description language, this tutorial will provide you a foundation to begin to apply these techniques. To gain the most benefit from this tutorial, you should have a basic knowledge of real-time and dependability design issues (e.g., scheduling, communications, redundancy, partitioning, fault tolerance).