

# A Practical AADL Study in Aerospace Software: from Requirement to Implementation

Zhibin Yang

College of Computer Science and Technology,  
Nanjing University of Aeronautics and Astronautics, Nanjing, China

**Abstract:** Architecture Analysis and Design Language (AADL) is a standardized architecture description language for embedded systems, which is widely used in avionics and aerospace industries to model safety-critical applications. This talk is about an experiment to apply AADL in aerospace control software. It starts with an introduction of model-based development of safety-critical software and the capability of the AADL language. It also presents some of our new studies on AADL which aim to adapt the AADL capabilities to China industry, which includes: restricted Chinese natural language requirement modeling and its transformation into initial AADL architecture models, co-modeling with graphical AADL behavior annex and graphical synchronous language to support the specification of both control-flow and data-flow styles of functional behaviors, refinement of the initial AADL architecture models targeting code generation, automatically generating verification properties from restricted natural language requirements, C and Ada code generation by considering safety programming rules, reverse engineering from C source code to AADL models, etc. Then, we show the tool support we provide for these enhancements in the form of OSATE plug-ins and present an illustrative industrial case study. Finally, we conclude by the presentation of some learned lessons.

**Keywords:** Safety-Critical Software, AADL, Restricted Natural Language Requirements, Refinement, Compositional Verification, Code Generation, Reverse Engineering