

Master's Thesis Internship

State of the Art of using Formal Methods for AADL Models Verification

Location: LTCI Laboratory, Telecom Paris, Institut Polytechnique de Paris, France

Duration: 6 months

Internship starting date: February 2025

Supervisors: **Dr. Dominique Blouin**

Associate Professor, Telecom Paris, Institut Polytechnique de Paris
ACES Research Group (Autonomous and Critical Embedded Systems)
LTCI (Information Processing and Communications Laboratory)

Dr. Aissam Belghiat

Associate Professor, University of Jijel
LaRIA Laboratory

Keywords

AADL, Architecture Description Languages, Formal Methods, Model-Based Systems Engineering, Model-Driven Engineering, System Architecture, Verification, Critical Systems

Context

The Architecture Analysis & Design Language (AADL) is an architecture description language (ADL) standardized by SAE (Society of Automotive Engineers). It has emerged as a crucial standard for specifying critical systems. Precisely, it is used to model and analyze the software and hardware architecture of embedded real-time systems. AADL is very rich in terms of constructs and semantics, but it has not been doted by a formal rigorous basis which hinders automatic verification of its models. AADL is widely used and the analysis of the languages and systems designed in it is a challenging research topic. Formal methods have become one of the main practices in software engineering for strict analysis and verification. The Formal methods can be used to find and resolve the problems early by describing the system with precise semantics and validating the system model. AADL has received a lot of attention, and numerous studies have been achieved in the literature trying to formalize this language using different formal techniques. The techniques were mainly based on Petri nets, Process algebras and Automata, but other methods were adopted.

This internship focuses on conducting a comprehensive literature review of formal methods applied to AADL. We aim to examine their capabilities, limitations, and potential areas for improvement.

Research Objectives

- Conduct an extensive literature review of formal methods approaches applied to AADL

- Study and categorize different formal properties that can be verified using these methods
- Identify limitations and challenges in current formalization approaches
- Study the scalability and applicability of existing solutions
- Propose potential directions for addressing identified limitations

Required Profile

We are seeking a motivated Master student with:

- Good background in formal methods and computer science in general
- Solid understanding of modeling languages and system architecture
- Knowledge of verification and validation techniques
- Knowledge on ADLs (architecture description languages)
- Familiarity with AADL or similar architecture description languages is a plus
- Excellent analytical and synthesis skills
- Good writing abilities in English
- Ability to work independently and as part of a research team

Skills

- Knowledge on formal methods
- Knowledge of formal verification tools
- Understanding of model-driven engineering
- Experience with technical documentation and academic writing

Expected Outcomes

- Comprehensive state-of-the-art report on AADL formalization
- Analysis of verification capabilities and limitations
- Recommendations for future research directions
- Potential conference paper submission

Application Process

Interested candidates should submit:

- Detailed CV
- Cover letter explaining your motivation and relevant experience
- Academic transcripts
- Any relevant research papers or projects
- References (optional)

Please send your application to:

dominique.blouin@telecom-paris.fr or aissam.belghiat@univ-jijel.dz

NB. The position is available immediately. Applications will be reviewed on a rolling basis until the position is filled.