

META-II: Formal Co-Verification of Correctness of Large Scale Cyber-Physical Systems During Design

The code contained within the accompanying zip file enables the architectural synthesis and analysis of complex systems during the conceptual design phase. Our code involves the generation, translation, and analysis of complex systems following a model-based design paradigm. Code contained within the file is as follows:

- Designer Dashboard code that provides a graphical user interface to the workflow
- Concept generator code that allows a designer to explore the solution space using high-level components and specified design requirements, and design seeds and grammar rules for developing electrical power system and electro-mechanical ramp system concepts
- Component model library SQL code for installing a locally hosted version and a description of the library schema
- Automated model generator code that translates the conceptual designs created by the concept generator code into system-level models for analysis
- Functional verification code that evaluates the functional correctness and robustness of a conceptual design against functional requirements, and functional models in PRISM format
- Performance verification code that calculates the of probability of correctness to estimate how well each component as well as the overall system meets a set of performance requirements, and performance models in modelica format
- Reliability verification code that performs a system-level reliability analysis to assess the dependability of conceptual design architectures, and reliability models in matlab format

Our verification workflow tool chain is a heterogeneous set of software systems developed in five programming and modeling languages by four organizations across the United States. It includes significant legacy code bases and newly developed reasoning and integration code. The individual modules that comprise the verification workflow have been designed and developed to produce output that this in the format necessary to be the input for the next module in the tool chain. We have made an effort to seamlessly integrate the pieces of the workflow tool chain through the creation of the Designer Dashboard.

Delivered to the Government in Accordance with Contract FA8650-10-C-7079