Industrial Verification Using the KIND Model Checker

Lucas Wagner [*] Jedidiah McClurg [*] [†]

Abstract

The ability to quickly and effectively verify correctness of avionics software is essential in building safe and affordable aircraft. Many avionics software components can be modeled using synchronous dataflow languages, making them suitable for verification by model checking. We discuss a comprehensive approach for modeling and verifying such systems. The Rockwell Collins translator framework is a product family of translators that accepts models developed in Simulink/Stateflow or Scade/Esterel and targets a variety of formal analysis tools. We have recently integrated the open-source KIND model checker into the translator framework to enable k-inductive verification of safety properties. In this talk, we demonstrate results of successfully using this approach on industrial examples. We also discuss ways that we have improved the efficiency of our formal verification process through intuitive graphical control, visualization, and simulation. Finally, we present novel approaches to accelerating the verification of difficult, state-intensive problems through state minimization and automatic generation of mode and range invariants.

[*] Advanced Technology Center, Rockwell Collins, Cedar Rapids, IA 52492
{lgwagner, jrmcclur}@rockwellcollins.com

[†] Department of Computer Science, University of Iowa, Iowa City, IA 52242
jedidiah-mcclurg@uiowa.edu