Pervasive Formal Verification in Control System Design

Lee Pike
Galois, Inc.
Email: leepike@galois.com

I. Motivation

Control systems design is a multifaceted field, drawing not only on control theory, but on results from computer science, electrical engineering, mechanical engineering, and physics. A controller often must satisfy regimented size, weight, power, and timing constraints, integrate with the overall system, and perform properly in a variety of harsh environments. Furthermore, control systems are arguably the lynchpin of safety in critical embedded systems, ranging from nuclear reactors to avionics to medical devices.

Progress has been made in the formal verification of aspects of control system design. Advances in hybrid system verification show promise in automating the verification of abstract models of dynamical systems. Advances in software and hardware formal verification may contribute to ensuring the correctness of implementations. Nevertheless, industrial uptake of these advances is still in its infancy, particularly as compared to disciplines such as digitial hardware design.

This panel will address the impediments to the adoption of formal verification techniques in industrial control system design. Furthermore, the panel will address what research topics would most benefit the adoption of formal verification in industry.

II. Panel Organization

The panelists will primarily be drawn from industry, having first-hand knowledge of the state-of-the-art in control system design practices.

This panel discussion will address the following questions:

- How can formal verification compliment current simulation and testing procedures?
- What will control system design look like in 10 years? 20 years?
- Can formal verification help build safer "intelligent" control systems?
- Where can the greatest impact be made in improving control system quality and reducing design costs? Better hybrid system verification tools? Better languages? More compiler assurance? Easier timing analysis? Automated power analysis?
- Could more aggressive control systems (i.e., that save energy, reduce operational wear, reduce the need for redundancy) be pursued if better design assurance could be provided?
- What social and educational impediments are there to having control systems engineers use formal verification tools?