Title: Formal Verification of Simulink/Stateflow Diagrams

Organizers: Naijun Zhan, State Key Lab. of Computer Science, Institute of Software, Chinese Academy of Sciences, email: znj@ios.ac.cn

Speakers: Naijun Zhan and Liang Zou, State Key Lab. of Computer Science, Institute of Software, Chinese Academy of Sciences, email: {znj,zoul}@ios.ac.cn

Abstract: Simulink is an industrial de-facto standard for building executable models of control systems and their environments, facilitating their validation by simulation. Stateflow is a toolbox used to model reactive systems via hierarchical statecharts within a Simulink model, extending Simulink's scope to event-driven and hybrid forms of embedded control. In safety-critical control systems, exhaustive coverage of system dynamics by formal verification would be desirable, complementing the inherently incomplete coverage that can be achieved from simulation. In this tutorial, we present such an approach to formal verification of Simulink/Stateflow (S/S) diagrams based on our work over the past few years. We will first introduce S/S, especially the basic notations and features related to hybrid system design, and then Hybrid CSP (HCSP), a formal language for modelling hybrid systems. We then present a deductive logic for reasoning about HCSP models, i.e. Hybrid Hoare Logic (HHL), as well as its implementation HHL Prover based on the interactive theorem prover Isabelle/HOL. We next show how to automatically encode S/S diagrams into HCSP models, and thus formal verification of S/S diagrams is enabled with the support of HHL Prover. We finally demonstrate the presented approach by two real-world case studies originating from the Chinese High-Speed Train Control System (CTCS-3) and the guidance-navigation-control (GNC) system of a lunar lander.