Bridging the gap between research and practice: Formal methods in the automotive domain

Jyotirmoy V. Deshmukh,
Toyota Technical Center, Gardena CA

Where: Jakob-Haringer-Str. 2, Room T03

When: Friday, September 25, 2015, 10:30 s.t.

Abstract: At the heart of an automobile are its engine and powertrain. The operation of these components is controlled by embedded software on an electronic control unit (ECU). The paradigm of model-based development (MBD) has become the de facto standard for designing such control software. MBD designs of control software range from feature-level models to application-level and even entire system-level models. On the other hand, models of the plant (e.g. the engine), can range from simple physics-based models to high-fidelity models incorporating test-data. The advantage of MBD is in its ability to design, validate, and analyze the closed-loop model of the plant and the controller, often well before the actual hardware components become available. Unfortunately, even the simplest closed-loop model of an automotive powertrain subsystem is a complex cyber-physical system with highly nonlinear and hybrid dynamics, and reasoning about the correctness of such closed-loop models is a formidable task. In this talk, we introduce two challenges in reasoning about industrial-scale closed-loop control models: (1) Scaling verification or bug-finding techniques to engine control software, and (2) formalisms to express correctness and performance requirements for such models. We survey some of the existing work done to address such questions, and present some promising directions for future work.

Jyotirmoy V. Deshmukh is a research engineer at Toyota Technical Center in Gardena (Los Angeles). His research interests are in the broad area of formal verification of cyberphysical systems, automatic synthesis and repair of systems, and temporal logic. His current focus is in the area of automotive control systems modeled as nonlinear and hybrid dynamical systems. Jyotirmoy got his Ph.D. in the area of verification for sequential and concurrent software at the University of Texas at Austin, and was a post-doctoral researcher at the University of Pennsylvania.

UNIVERSITÄT SALZBURG

Software Systems Center
Colloqium Series

host: Wolfgang Pree