Title: CPS: Medium: GOALI: An Architecture Approach to Heterogeneous Verification of Cyber-Physical Systems (Award # 1035800)

Authors:

I. Ruchkin[1], S. Mitsch[1], A. Rajhans[2], J.-D. Quesel[1], B. Krogh[2], D. Garlan[2], A. Platzer[1], B. Schmerl[2], J. Kapinski[3], P. Ramachandra[3], K. Butts[3]
[1] School of Computer Science,
[2] Dept. of Electrical & Computer Engineering
Carnegie Mellon University, Pittsburgh, PA
[3]Toyota Technical Center, Ann Arbor, MI

{iruchkin, smitsch, jquesel, garlan, aplatzer, schmerl}@cs.cmu.edu
{arajhans, krogh}@ece.cmu.edu
{jim.kapinski, prashant.ramachandra, ken.butts}@tema.toyota.com

Abstract

Current methods for design and verification of cyber-physical systems (CPS) lack a unifying framework due to the complexity and heterogeneity of the constituent elements and their interactions. Heterogeneous models describe different aspects of a CPS at varying levels of abstraction and using different formal languages. This prevents engineers from detecting inconsistencies among models and reasoning at the system level to verify specifications at design time. Our architectural approach to CPS design and verification uses flexible architectural models to represent pertinent aspects of individual models to support consistency checking and verification at the inter-model level.

Our approach to CPS modeling prescribes the creation of architectural views for the constituent models. Each view abstracts out details that are irrelevant for relating models, and represents (part of) the system in a particular architectural style with appropriate types of components and connectors. For example, a software view may describe processes, threads, and shared memory segments, while the control view may show sensors, actuators, and controllers. To relate views to each other, we use a view mapping language [1], capable of expressing arbitrary constraints over view maps. Consistency between two views encompasses the structural aspect (non-contradictory components and connectors appear in the views) and the semantic aspect (the meanings of the views are not contradictory). A simple form of semantic consistency can be defined in terms of assumptions and guarantees over view parameters. We are extending these ideas for richer notions of consistency.

Verification of heterogeneous models for CPS is another challenge that we are addressing. For the case when the inter-model semantics are provided using behavior relations [2], we have developed a formal framework to verify heterogeneous models using abstraction, conjunctive, and disjunctive constructs [3]. This makes it possible to verify models locally and compose their specifications and invariants to prove system-level safety specification. This method, however, does not allow using the architectural knowledge in other models to aid local verification. We currently investigate how exploiting an architectural view might simplify verification.

We have refined our approach over the course of three case studies. The STARMAC quadrotor study served as a base to investigate structural consistency [1]. Multiple models of the quadrotor were abstracted into architectural views using the collection of CPS architectural styles, and were used to detect several inconsistencies in the quadrotor models. The CICAS-SSA study focused on modeling and verifying a stop sign assist algorithm using heterogeneous abstraction over behavior relations and functions [3]. Finally, the case study of robotic collision avoidance, currently in progress, targets furthering our knowledge in compositional hybrid model reasoning and verification.

References

[1] A. Bhave, *Multi-View Consistency in Architectures for Cyber-Physical Systems*, PhD Thesis. Carnegie Mellon University, 2011.
[2] A. Rajhans, B. Krogh, *Heterogeneous verification of cyber-physical systems using behavior relations*, HSCC '12.
[3] A. Rajhans, *Multi-Model Heterogeneous Verification of Cyber-Physical Systems*, PhD Thesis, Carnegie Mellon University, 2013.