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

Authors: Akshay Rajhans[1] and Bruce Krogh[2]
Dept. of Electrical & Computer Engineering, Carnegie Mellon University, Pittsburgh, PA.
Email: {[1]arajhans, [2]krogh}@ece.cmu.edu

Abstract
Current methods for design and verification of cyber-physical systems lack a unifying framework due to the complexity and heterogeneity of the constituent elements and their interactions. Because of the inherent heterogeneity, model-based development of such systems involves several models and specifications in different formalisms that are best suited for modeling and specifying different aspects of the systems. We propose an approach to managing the heterogeneity in modeling and specifications in terms of their behavioral semantic interpretations.

To develop the semantic approach to dealing with heterogeneity, we consider two cases – one where it is possible to define the semantics of all the constituent models and specification formalisms in a common universal behavior formalism in which they are compared and analyzed [1]; and a more realistic one where the semantics are defined in different behavior formalisms, but associations are defined across these behavior formalisms using mathematical relations called behavior relations [2].

To facilitate the use of several models and specifications, we propose a conjunctive construct in which each abstract model serves a different abstraction of the underlying model, and a disjunctive construct in which different models used to model different parts of the system behavior together cover the whole range of system behaviors. Arbitrary nesting of these conjunctive and disjunctive constructs lets the system designer build an arbitrary heterogeneous verification hierarchy.

We use parametric extensions of the conjunctive and disjunctive verification constructs for capturing inter-formalism interdependencies and for analyzing semantic consistency between a parent heterogeneous verification activity and its children activities to ensure that the different models used in a verification hierarchy make consistent semantic assumptions about each other and about the system [1,2]. Auxiliary constraints over parameters are a first step towards capturing the inter-formalism interdependencies, and capture static interdependencies across the different formalisms. Overapproximation of dynamic interdependencies can be captured in terms of the bounds on the valuations of the interdependency variables. The use of variable projection via existential quantification and implication provides a practical approach to defining and checking semantic consistency using SMT solvers or theorem provers. A prototype framework for semantic consistency analysis is being developed using the theorem prover KeYmaera.

In cases where the heterogeneous abstract and concrete models are composed of smaller interacting component models, we propose a compositional approach to heterogeneous abstraction analysis using behavior abstraction functions as the semantic mappings between the heterogeneous formalisms. This enables the use of independent local heterogeneous verification activities for the components that compose at the global system level, thereby facilitating a distributed model-based development from the independent development of the components to that of the system [3].

With our industrial partner, Toyota, we have been developing a case study in the area of cooperative intersection collision avoidance systems (CICAS). We illustrate the theoretical concepts using a CICAS for Stop-Sign Assist.

References
[1] Rajhans et al., *Using parameters in architectural views to support heterogeneous design and verification*, CDC '11.

[2] Rajhans, Krogh, *Heterogeneous verification of cyber-physical systems using behavior relations*, HSCC '12.

[3] Rajhans, Krogh, *Compositional heterogeneous verification*, MPM '12 (submitted).