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

Authors:
Ajinkya Bhave[1], Ken Butts[3], Derek Caveney[3], David Garlan[2], Bruce Krogh[1], Sarah Loos[2], Andre Platzer[2], Akshay Rajhans[1], Prashant Ramachandra[3], Bradley Schmerl[2]

[1]Dept. of Electrical & Computer Engineering
[2]School of Computer Science
Carnegie Mellon University
Pittsburgh, PA.
[3]Toyota Technical Center, Ann Arbor, MI.
Email:
{jinx, arajhans, krogh}@ece.cmu.edu
{garlan, sloos, aplatzer, schmerl}@cs.cmu.edu
{ken.butts, derek.caveney, prashant.ramachandra}@tema.toyota.com

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. Our approach is to define relationships between system models at the architectural level, which captures the structural interdependencies and some semantic interdependencies between representations without attempting to comprehend all of the details of any particular modeling formalism. We present an extension of existing software architecture tools to model physical systems, their interconnections, and the interactions between physical and cyber components. A new cyber-physical system (CPS) architectural style is introduced to support the construction of architectural descriptions of complete systems and serve as the reference context for analysis and evaluation of design alternatives using existing model-based tools.

A system's base architecture (BA) models the system as an annotated graph of components and connectors. The components represent principal computational and physical elements of a system's run-time structure, connectors represent pathways of communication and physical coupling between components, and annotations represent properties of the elements. Each system model is related to the BA through the abstraction of an architectural view, which represents the architecture of the model as an abstraction and refinement of the underlying shared BA. Well defined mappings between a view and the BA can then be used as the basis for identifying and managing the structural and semantic dependencies between the models to evaluate mutually constraining design choices. We have implemented the CPS architectural style and architecture view mappings in the AcmeStudio design environment.

We address the issue of defining and evaluating consistency between architectural views imposed by various heterogeneous models and the BA. Architecture view consistency has both structural and semantic aspects. The notion of *structural consistency* ensures that the model elements adhere to the cyber and physical types and the connections between components present in the BA. Structural consistency checking between a model and the base architecture of the system is formulated as a labeled graph matching problem. The graph morphism consistency checker is implemented as an AcmeStudio plugin. The usefulness of the approach to check system connectivity assumptions is illustrated in the context of multiple heterogeneous views of a quadrotor air vehicle.

System-level verification requires some formal representation of the relationships and information interdependencies between the heterogeneous models. The notion of *parametric consistency* ensures that values of parameters used in each system model are mutually valid. We introduce the use of logical constraints over parameters in the architectural views to represent the assumptions underlying each model and the conditions under which the specifications verified for each model are true. Interdependencies and connections between the assumptions in the architectural views are managed in the BA using the first-order logic of real arithmetic to ensure consistency and correct reasoning.