CPS Forum Poster Proposal

Design and Analysis of Cyber-Physical System Architectures

Shang-Wen Cheng[1], David Garlan[1], Bruce Krogh[2], Akshay Rajhans[2], Bradley Schmerl[1], Bruno Sinopoli[2]
[1]Computer Science Dept.
[2]Dept. of Electrical and Computer Engineering
Carnegie Mellon University
Pittsburgh, PA 15213

We present an architecture-based approach and tool to support the principled design and evaluation of alternative architectures for cyber-physical system (CPS) applications. Today's models and methods for analysis and design of CPSs are typically fragmented along lines defined by disparate mathematical formalisms and dissimilar methodologies in engineering and computer science. While separation of concerns is needed for tractability, such analytical approaches often impose an early separation between the cyber and physical features of the system design, making it difficult to assess the impacts and tradeoffs of alternatives that cut across the boundaries between these domains. Architecture description languages (ADLs) support the description of annotated structural representations that facilitate the evaluation of design tradeoffs in terms of important quality features such as performance, reliability, security, and maintainability. In particular, the notion of *architectural style* describes a vocabulary of structural types, a set of properties and composition rules, and associated analyses to enable such tradeoffs [1]. The proposed approach builds on existing software architecture tools that have worked well for complex software systems by developing a new CPS style with certain basic component and connector types to model physical systems, their interconnections, and the interaction between physical and cyber components.

The poster will present
- a new vocabulary of basic architectural component and connector types for CPS, defined in the Acme ADL [3] using AcmeStudio [5]
- the implementation of two analysis tools implemented as ACME plug-ins for analyzing and verifying properties of CPS designs using Labelled Transition System Analyser (LTSA) [4] for verifying finite-state processes (FSP) [4] and PHAVer [2] for verifying linear hybrid automata
- an illustration using CPS ADL to model the architecture for a building HVAC system
- analysis results exposing potential errors in the architectural designs for the HVAC system
- methods for addressing design errors in the architectural description
- current research directions

References
1. G. Abowd, R. Allen, D. Garlan. Formalizing style to understand descriptions of software architecture. In ACM Transactions on Software Engineering and Methodology, 4(4):319-364, October 1995.
2. G. Frehse. PHAVer: Algorithmic verification of hardware systems past HyTech, Int'l Journal on Software Tools for Technology Transfer, 10:263-279, 2008.
3. D. Garlan, R. Monroe, D. Wile. ACME: Architectural description of component-based systems. In Foundations of Component-Based Systems, Cambridge Univ. Press, 2000.
4. J. Magee, J. Kramer. Concurrency: State Models & Java Programs (2nd ed.), Wiley, 2006.
5. B. Schmerl, D. Garlan. AcmeStudio: Supporting style-centered architecture development. ICSE 2004.