An Architectural Approach to Heterogeneous Modeling and Verification of CPS

I. Ruchkin[1], S. Mitsch[1], A. Rajhans[2], Jan-David Quesel[1], B. Krogh[2], D. Garlan[2], A. Platzer[1],
B. Schmerl[2], J. Kapinski[3], P. Ramachandra[3], K. Butts[3]
{[1]SCS, [2]ECE}, Carnegie Mellon University, Pittsburgh, PA [3]Toyota Technical Center, Ann Arbor, MI

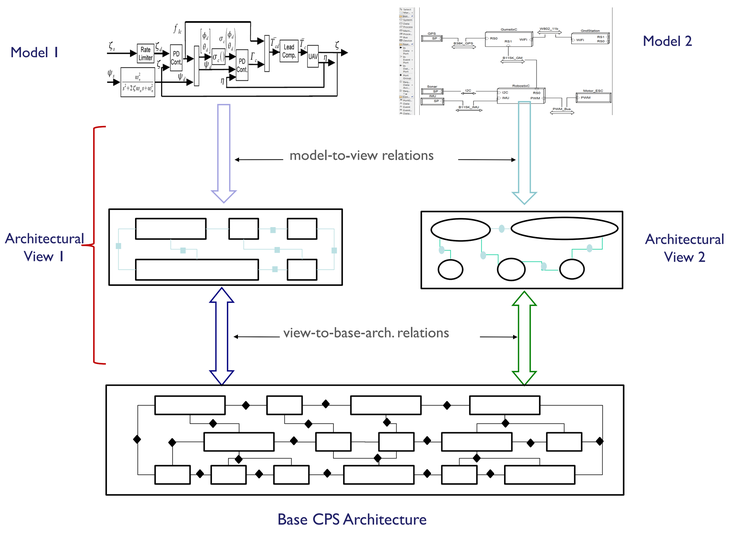
Award # 1035800
Medium GOALI

Objectives

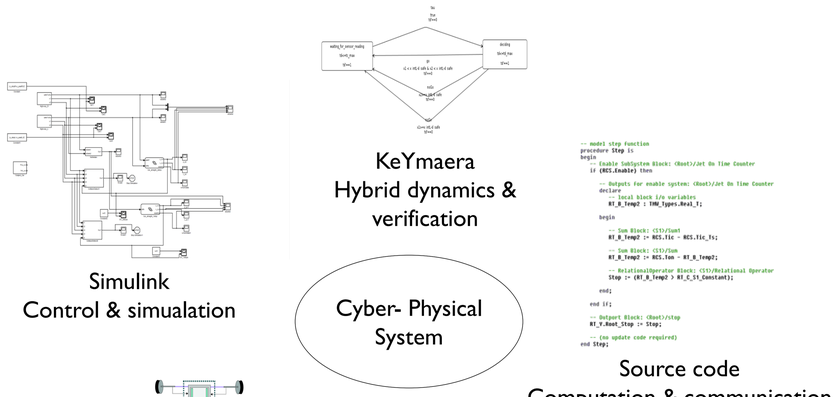
- Consistent representation of a system with multiple models
- Verification using heterogeneous models
- Tools to support CPS modeling and verification

Architectural Approach

We use architectural models (components and connectors) to represent common structural and semantic features to guarantee consistency.



Heterogeneous CPS Models

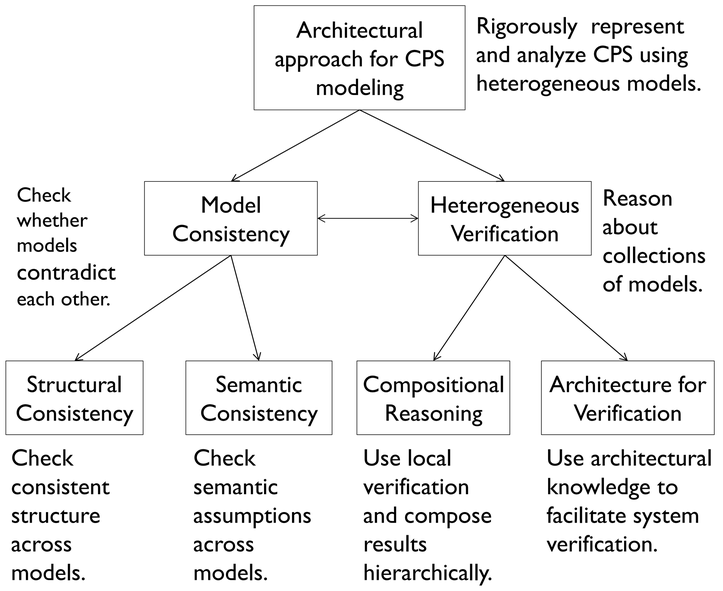


Heterogeneous models allow experts to address different aspects of the system design. Although convenient for the experts, creates two challenges: consistency and verification.

The challenges may occur because of:

- Timing: periods, events, determinism
- Movement: geometry, dimensionality
- Sensing and actuation: delays, precision
- …

Research Directions



Tools

AcmeStudio – architectural design environment for representation and analysis of architectural views.

- *AcmeMaps* – specification of relations between views.

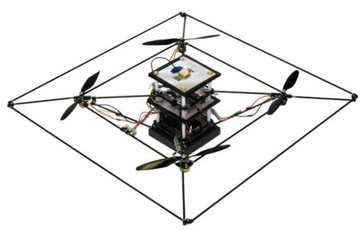
KeYmaera – hybrid program language and proof system for verification in differential dynamic logic

- *Sphinx* – a Graphical and Textual Modeling Tool for Hybrid Programs.

Case Studies

Quadrotor

Goal: ensure consistency of heterogeneous models for a STARMAC quadrotor.



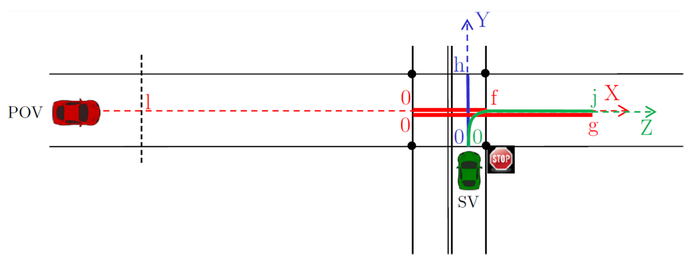
Results:

- Developed architectural modeling for structural consistency.
- Detected several inconsistencies in design.

A. Bhave et al. View Consistency in Architectures for Cyber-Physical Systems. ICCPS '11.

CICAS-SSA

Goal: verify a stop sign assist algorithm.



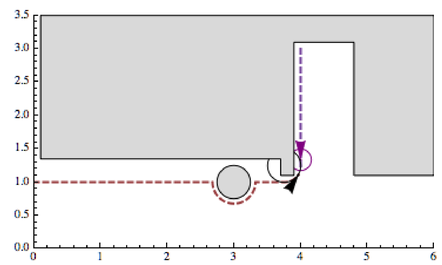
Results:

- Formalized heterogeneous model semantics using behavior relations.
- Developed a compositional approach to heterogeneous abstraction.

A. Rajhans et al. Heterogeneous verification of cyber-physical systems using behavior relations. HSCC'12.

Robot Collision Avoidance

Goal: verify a family of robot controllers for collision safety with obstacles.



Results:

- Proved safety for moving obstacles in presence of location and actuator uncertainty.
- Work in progress.

S. Mitsch et al. On Provable Safe Obstacle Avoidance for Autonomous Robotic Ground Vehicles. RSS' 13.