# Compositionality and Reconfiguration for Distributed Hybrid Systems

André Platzer, Edmund M. Clarke, Sarah M. Loos

Computer Science Department

Carnegie Mellon University

This research project addresses fundamental challenges in the verification and analysis of distributed hybrid systems.  In particular, we are working to minimize the mismatch between the combinations of dynamics that occur in complex physical systems and the limited kinds of dynamics currently supported in analysis.  At present, the major mismatches in advanced cyber-physical systems for traffic applications are caused by scalability issues, nonlinearities in the system dynamics, and lack of modeling features. For instance, traffic control systems require maneuvers where there is a large and evolving number of participants depending on the local traffic situation. Verification does not scale to large systems like those yet.

We address the major scalability issues by working with a strictly compositional reasoning approach. We propose to develop hierarchical modularity principles in order to exploit the static structure of the system, which will generally be too big to handle or may change by communication links. By verifying the system with hierarchical reasoning principles, we generate a proof structure which is composed of many verified modules.  This has the added benefit of producing a verification which is highly resistant to modifications of the model, i.e., a change in the model is unlikely to require a complete revision of the verification, but rather only part of the verification would need to be regenerated.

To address the nonlinearities arising in system models, particularly the continuous dynamics, we propose to study differential invariants as a verification technique. Differential invariants are formulas that allow symbolic proofs about the dynamics of a system without having to solve the differential equations. This project will study the differential invariant problem and their generation.

This research presents a major improvement addressing the challenges of hierarchical composition, reconfiguration, and nonlinearity in system models.  It has significant applications in the verification and analysis of safety-critical properties in state of the art and next generation cyber-physical systems, e.g, robotic swarms and unmanned aerial vehicle cooperation schemes.  This research will build verification technologies for cyber-physical systems.