Compositionality and Reconfiguration for Distributed Hybrid Systems

André Platzer   Edmund M. Clarke   Ping Hou   Sarah M. Loos

The objective of this research is to address fundamental challenges in the verification and analysis of reconfigurable distributed hybrid control systems. These occur frequently whenever control decisions for a continuous plant depend on the actions and state of other participants. They have not been supported by verification technology prior to this research project. The approach advocated here is to develop strictly compositional proof-based verification techniques to close this analytic gap in cyber-physical system design and to overcome scalability issues. This project develops techniques using symbolic invariants for differential equations to address the analytic gap between nonlinear applications and present verification techniques for linear dynamics.

This project aims at transformative research changing the scope of systems that can be analyzed. The proposed research develops a compositional proof-based approach to distributed hybrid systems verification in contrast to the dominant automata-based verification approaches. It represents a major improvement addressing the challenges of composition, reconfiguration, and nonlinearity in system models. This project also aims to implement an automated deductive tool with a user-friendly graphical interface for distributed hybrid systems verification and analysis.

This project has developed a system model for distributed hybrid systems that combines differential equations with assignments and dynamic dimensionality-changes. This project has introduced a dynamic logic for verifying distributed hybrid systems and presented a compositional proof calculus for it. The proposed research has used invariants for differential equations to develop the first formal verification technique that can handle the complicated nonlinear dynamics of distributed hybrid systems. This project addresses the problem of automated theorem proving for distributed hybrid systems and develops a new automated theorem prover called KeYmaeraD, which is the first formal hybrid verification tool for reconfigurable distributed hybrid systems.

The proposed research has significant applications in the verification of safety-critical properties in upcoming cyber-physical systems. This includes distributed car control, robotic swarms, and unmanned aerial vehicle cooperation schemes to full collision avoidance protocols for multiple aircraft. Analysis tools for distributed hybrid systems have a broad range of applications of varying degrees of safety-criticality, validation cost, and operative risk. Analytic techniques that find bugs or ensure correct functioning can save lives and money, and therefore are likely to have substantial economic and societal impact.

The proposed compositional verification techniques for distributed hybrid systems have been used successfully to verify a distributed car control system. Formal verification results guaranteeing collision freedom have been presented in a series of increasingly complex settings, culminating in a safety proof for distributed car control despite an arbitrary and evolving number of cars moving between an arbitrary number of lanes. Another successful case study for the proposed research is a formal verification for distributed roundabout collision avoidance maneuver for air traffic control. A formal proof has been presented to show that the distributed roundabout maneuver safely avoids collisions for arbitrarily many aircraft (even with dynamic appearance of new aircraft).