Formal Verification of Transportation Cyber Physical Systems

Ashish Tiwari*

SRI International, Menlo Park, CA 94025, tiwari@csl.sri.com

1 Introduction

Transportation systems – automotive, aviation, and rail – involve interactions between software controllers, communication networks, and physical devices. These systems are among the most complex cyber physical systems being designed by humans, but added time and cost constraints make their development a significant technical challenge. Automated technologies for verification and validation are now indispensable for quickly developing safe and reliable transportation systems.

Formal verification technology complements the traditional simulation-based approach for testing models of cyber physical systems by providing comprehensive and exhaustive coverage. Automated formal analysis can also be used to improve support for design, testing, and code generation. Formal techniques are increasingly being recognized as being essential in saving time and money. Formal approaches for verification are beginning to be accepted as certification arguments (cf. DO178C).

2 Requirements and Technical Challenges

New formal verification and validation technology is required to address the following specific challenges posed by the transportation sector.

Complexity. Transportation systems are complex systems and current formal verification technology does not scale to the sizes of these systems. These systems need to be analyzed at several levels of abstraction. It is unlikely that a single verification technique will suffice at every level. A collection of techniques with suitable integration of the results is required.
Transportation systems are time-critical systems. Safety of these systems depends on the ability to generate responses with real time guarantees. Specification and verification of timing requirements adds to the complexity.
Transportation systems consist of embedded control systems inside the vehicle (V) and the surrounding infrastructure (I), as well as, the interaction between vehicles (V2V) and between vehicle and the infrastructure (V2I). The dynamics of these interactions increases complexity and poses new challenges for formal verification.

Unreliable or unknown components. Detailed models of some components of the transportation system may not be available because, for example, they are built by external suppliers or they are part of some legacy subsystem. Guaranteeing reliability and robustness of the system obtained by integrating incompletely specified components is a challenge for compositional verification.

* With input from other members of the formal methods group at SRI International

Flexibility. Transportation systems are expected to evolve. They can be updated, as well as, extended with new external components. We need techniques to provide assurance that these modified systems continue to meet their correctness specification at the system level.

3 Research Challenges

Traditional formal verification approaches based on model checking and theorem proving are insufficient for dealing with the complexity of transportation cyber physical systems. New mathematics and new computational support for dealing with **hybrid state spaces** and for reasoning on combined linear, nonlinear, Boolean, and finite-domain constraints is required. New tools and approaches for hybrid (discrete+continuous) systems are needed as existing ones are not scalable.

The verification of complex cyber physical systems requires a portfolio of techniques – from **lightweight** and **invisible methods** that verify shallow properties of the detailed model to **heavyweight methods** that verify deep properties of an suitable abstraction of the model. Moreover, **static formal verification techniques** that validate the model, design, or implementation once need to be complemented with **dynamic techniques** that monitor the system as it is running. Formal runtime techniques can (probabilistically) guarantee lifetime safety.

Compositional verification is an important approach for verifying complex systems consisting of several interacting components. Compositional verification is based on analyzing individual components and then verifying the system by composing the analyses of the components. Compositional analysis is enabled if components specify their **interfaces** – the constraints (or assumptions) on their inputs and the properties (or guarantees) on their outputs. A component needs to be verified against its specification, which includes **timing specification** and interface specification. These specifications, in the form of interfaces and **invariants**, can range from being very simple to very complex. Formal techniques for generating and checking both interfaces and invariants is required. Simpler interfaces and simpler invariants are easier to compute and compose.

Simulation-based testing and formal verification need to complement each other. Formal verification techniques use slow symbolic methods, but provide exhaustive coverage, whereas simulation-based approaches use fast numerical solvers, but provide limited coverage. Formal techniques can be used to develop new approaches for **automated test vector generation** – for both unit and system level – and thus improve coverage of testing. Conversely, verification and invariant generation tasks could be guided by simulation results.

A crucial approach for building and verifying complex transportation byber physical systems will be based on preserving **separation**, or more generally least privilege, in the inter-component interactions.

Simulation models of cyber physical systems contain several details of low-level dynamics that are not always required for verifying high-level control algorithms. Model reduction and abstraction is the process of simplifying a simulation model to a more abstract (for example, reduced order) model for use in verification and other analysis. Performing **automated model abstraction** of large high-dimensional hybrid systems, and characterizing and quantifying the approximation and/or the abstraction function used to create the simpler model

are challenging technical tasks. The abstract formal models, in contrast to simulation models, are simpler, yet more robust, and are better suited for verification. Automated techniques for model abstraction are also required to support **multi-scale modeling**.

4 Conclusion

Transportation cyber physical systems are now being designed using computer-aided control system design tools, such as Matlab. Analysis is currently supported only in the form of simulation. To increase confidence in the safety and reliability of the designed system and that too in the limited development time available, it is imperative that a portfolio of new formal technologies be developed that can support the design, testing, and implementation of complex cyber physical systems. However, to deal with the complexity of transportation systems, these novel approaches for verification and composition should be tunable so that they can provide increased assurance with investment of more resources.

Biography

Ashish Tiwari received his B.Tech and Ph.D. degrees in Computer Science from the Indian Institute of Technology, Kanpur and the State University of New York at Stony Brook in 1995 and 2000, respectively. He is currently a member of the formal methods group in the Computer Science Laboratory at SRI International. His research interests are in symbolic techniques, automated deduction, decision procedures, program analysis, and formal technologies for analysis and verification of hybrid system models of embedded software and biological systems.

Dr. Tiwari co-chaired the International Workshop on Hybrid Systems in 2006 and the workshop on Automated Deduction: Decidability, Complexity and Tractability in 2007. He has served on the program committee of all the major conferences on automated deduction, verification, logic, and hybrid systems. His list of publications are available online at `http://www.csl.sri.com/~tiwari/`.