Chapter 10

Conclusions and Future Work

This thesis investigates how the formal modeling and verification techniques of computer science can be used for the analysis of hybrid systems. The motivation behind such research lies in the inherent similarity of the hierarchical and decentralized control strategies of hybrid systems and the formal techniques used for the verification of distributed systems in computer science. The thesis focuses on the development of techniques that use hybrid I/O automata to model automated transportation systems and to verify that their protection subsystems enforce the desired safety properties. The long-term goal of such research is to develop a simple and scalable framework for modeling complex hybrid systems with stringent safety and performance requirements.

10.1 Summary

The thesis is split into two major parts. First, we develop an abstract model of a physical plant that is interacting with several protectors. Second, we specialize the abstract models of the physical system and the protectors to simplified versions of the PRT 2000™ and its overspeed and collision protection subsystems.

As indicated above, the first part of the thesis is devoted to the development of an abstract model of a physical plant and a number of protectors that guarantee particular safety or performance properties. Both the physical plant and the protectors are modeled as hybrid I/O automata. The protector automata communicate with the physical plant automaton through shared variables and discrete actions. If S, R, and G are subsets of the states of the physical plant, then a protector automaton A for the physical plant PP guarantees G from S given R provided that every finite execution of the composition $PP \times A$ starting in a state in S that only involves states in R ends in a state in G. It is shown that if two or more protectors do not rely on the correct operation of each other, *i.e.*, if the protectors are independent, then their composition guarantees the properties guaranteed by each of the protectors being composed. On the other hand, if the protectors rely on the correct operation of each other, their composition guarantees the properties guaranteed by each of the protectors being composed only under certain conditions.

The abstract protector is parameterized in terms of the physical plant PP, the start states S, the sets of guarantee G and reliance R, the port j through which it communicates with the physical plant automaton, and the sampling period d. It is defined as the composition of a sensor and a discrete controller, both modeled as hybrid I/O automata. The sensor automaton samples the output variables of the physical plant at intervals of d time units and the discrete controller automaton issues protective actions so as to ensure that the physical plant exhibits the desired safety properties. The correctness of the abstract protector reduces the correctness proof of a protector implementation to a simulation proof among the states of the implementation and the particular instantiation of the abstract protector.

The second part of the thesis involves the proof of correctness of overspeed and collision protectors for a simple model of an automated transportation system involving n vehicles. The overspeed and collision protectors are redefined for three types of track topology: a single track, a track involving a Y-shaped merge, and a general track topology comprised of Y-shaped merges and diverges.

In the case of a single track, the overspeed protector is defined as the composition of n protectors, each of which guarantees that a particular vehicle does not exceed the speed limit, provided that none of the vehicles collide among themselves. Conversely, the collision protector is defined as the composition of n protectors, each of which guarantees that a particular vehicle does not collide into any of the vehicles it trails, provided that none of the vehicles exceed the speed limit and that none of the other vehicles collide into any of the vehicles they respectively trail.

In the cases of the more complicated track topologies, although the overspeed protector remains unchanged, the collision protectors are restructured. They involve the composition of $n(n-1)/2$ protectors, each of which guarantees that a particular unordered pair of vehicles do not collide between themselves, provided that none of the vehicles exceed the speed limit and that the vehicles of all other unordered pairs of vehicles do not collide between themselves.

Due to the correctness proof of the parameterized abstract protector, the proofs of correctness of the overspeed protectors for the individual vehicles and of the collision protectors for either individual, or unordered pairs of vehicles, are straightforward. They simply involve demonstrating the existence of a simulation relation among the states of the particular protector implementations and the particular instantiations of the parameterized abstract protector.

The composition of the overspeed protectors is straightforward due to their independence.

The proof of correctness of the overspeed protection subsystem involves the application of the aforementioned composition theorems for independent protectors. In the case of the collision protectors, since the individual collision protectors rely on the correct operation of each other, the proof of correctness of their composition is more involved. It relies on the careful decomposition of the collision protection subsystem so that the failure of multiple collision protectors at the same instant in time is prohibited. Similarly, the correct operation of the composition of the overspeed and collision protection subsystems relies on the fact that the overspeed protectors and the collision protectors can only fail through trajectories and discrete actions, respectively.

10.2 Evaluation

The contributions of this thesis are twofold. First, we develop an abstract model of an automated transportation system comprised of a physical plant and an arbitrary number of protectors. Second, we specialize the abstract model so as to analyze and verify a particular automated transportation system and its overspeed and collision protection systems.

The abstract models that are developed include the physical plant and a number of protectors. The abstract protector is parameterized in terms of the physical system, its start states, its sets of guarantee and reliance, the port with which it communicates with the physical plant and the sampling period. Therefore, the specification of a particular automated transportation system involves refinement of the abstract model. Moreover, the proof of correctness of the abstract model leads to simple correctness proofs of the protector implementations for particular instantiations of the abstract model. Finally, composition of independent protectors is straightforward. The safety properties of the individual protectors are guaranteed by the composed protector. Such compositional assertions also hold for dependent protectors under certain conditions. The use of abstraction, modular decomposition, and composition is hoped to allow the scalability of the formal method analysis and the verification of large and complex hybrid systems.

In this work, we demonstrate how hybrid I/O automaton techniques can be applied to the specification and verification of a very general automated transportation problem. We believe that the techniques developed in this thesis complement more traditional safety analysis. For example, safety engineers typically perform a fault-tree analysis to identify possible causes of each system hazard and related dependencies among system components. In our work, we use composition of automata to formalize these dependencies: to yield a speed limited system, we compose the physical plant with a set of overspeed protectors, one for each vehicle, and assume that no collisions occur in the physical system; conversely, to yield a collision free physical system, we compose the physical system with a set of collision protectors, either one for each vehicle, or one for each unordered pair of vehicles, and assume that none of the vehicles exceed the speed limit. The composition of the physical system in such ways formalizes the independence of the overspeed protectors, the interdependence of the collision protectors and more importantly the interdependence of the overspeed protectors and the collision protectors. We believe a more comprehensive treatment in this style of all the protection subsystems would, as a by-product, yield a significant subtree of the fault-tree.

10.3 Future Work

In this thesis, the treatment of automated transportation systems is a case study in the use of hybrid I/O automata to formally model hybrid systems. The focus of the research is in the use of abstraction, modularity, and composition to develop an abstract model of automated transportation systems to be used in the analysis and verification of transportation systems in use or under development. The long-term goal is to see how the formal methods of computer science can be used to formally model hybrid systems in a modular and systematic way and to verify their safety or performance characteristics. However, issues that have yet to be addressed involve the topics of robustness, scalability, tractability, and the use of formal methods as part of the system design process.

The work in this thesis assumes an ideal system; that is, the communication among the various subsystems is assumed to be correct and reliable, and to occur in a timely fashion. Moreover, the sampling of the state of the physical plant is assumed to be exact and the effects of the protective actions are assumed to be precise. Since, these assumptions are far from realistic, future research could involve the development of formal methods for analyzing and verifying automated transportation systems that are robust with respect to communication delays and uncertainty. For example, the treatment of automated transportation systems of this thesis could be extended to allow delays in the communication between the plant and the protectors and uncertainty either in the sampling of the state, or in the effects of the protective actions. The treatment of automated transportation systems could also be extended to allow fault tolerance; for example, allowing the track topology to be dynamic so that vehicles are not allowed to travel on branches of the track that have failed either structurally, or due to unexpected accidents.

In this thesis, we develop formal modeling techniques that are based on abstraction, modularity, and subsystem composition. The motivation behind this approach is the intent to model and verify complex hybrid systems that involve hierarchical and decentralized control schemes. Therefore, it is imperative to examine the scalability and tractability characteristics of the formal modeling techniques developed. The success in modeling the overspeed and collision protectors of an automated transportation system in this thesis indicates that the modeling techniques that are based on hybrid I/O automata are scalable to larger and more complex systems. However, the study and formal analysis of more complex systems remains to be done. In particular, it would be interesting to examine how complex continuous-time dynamics affect the formal modeling tools developed in this thesis. Moreover, the lengthy correctness proofs, which were done by hand in this thesis, expose issues of tractability concerning the analysis and verification of complex transportation systems. In fact, they dictate that computer aided verification methods for hybrid I/O automata be developed.

The formal modeling techniques developed in this thesis are techniques intended for the analysis and verification of automated transportation systems. Future research could investigate the potential of using formal methods of computer science as an integral part of the design of the hierarchical and decentralized control schemes of automated transportation systems and of hybrid systems in general.