11-2008

Analysis and Verification Challenges for Cyber-Physical Transportation Systems

Edmund M. Clarke
Carnegie Mellon University

Bruce Krogh
Carnegie Mellon University

Andre Platzer
Carnegie Mellon University

Raj Rajkumar
Carnegie Mellon University

Analysis and Verification Challenges for Cyber-Physical Transportation Systems

Edmund M. Clarke[1], Bruce Krogh[2], André Platzer[1], and Raj Rajkumar[2]

[1] Computer Science Department, Carnegie Mellon University, Pittsburgh, PA
[2] Electrical & Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA
{emc|krogh|aplatzer|raj}@cmu.edu

Abstract. Substantial technological and engineering advances in various disciplines make it possible more than ever before to provide autonomous control choices for cars, trains, and aircraft. Correct automatic control can improve overall safety tremendously. Yet, ensuring a safe operation of those control assistants under all circumstances requires analysis techniques that are prepared for the rising complexity resulting from combinations of several computerized safety measures. We identify cases where cyber-physical transportation systems pose particularly demanding challenges for future research in formal analysis techniques.

1 Cyber-Physical Transportation Systems

Cyber-physical systems are becoming more important in the supervisory and safety control functions of rail-based, airborne, and automotive transportation systems that have typically been performed by human operators before. Improvements in sensor accuracy, computational resources, and their understanding enable manufacturers to assist drivers and pilots on a level of sophistication that has never been possible before. Transportation assistance technology has most impact when supporting safety-critical driver or pilot decisions to prevent fatal accidents. It is of ultimate importance that these safety-critical control decisions are correct.

Control assistance technology can influence the actual control choices that take effect in the transportation system in several ways:

1. Pure alerting functions in lane change assistants for cars, the traffic alert and collision avoidance system (TCAS) for aircraft;
2. Fine-grained adaptations of human control actions like stuttering and selective force distribution in anti-lock braking systems and electronic stability control for cars; and
3. Semi-automatic control by speed supervision controllers on rails and car parking assistants.

Fully automatic proactive control has become feasible. Recent examples of this kind include the automatic train protection unit of the European train control system (ETCS) and auto pilot control for various aircraft maneuvering modes. Similar advances have been achieved in radar-based adaptive cruise control for cars that brake autonomously when approaching the end of a traffic jam. Recent robotic applications even allow completely driverless vehicle control. More generally, it turns out that nearly all modern transportation technology depends on a tight coupling with computer control. This makes them *cyber-physical systems* (CPS) and *hybrid systems* with interacting discrete and continuous dynamics.

Soon, there will be a complete coverage of assistance technologies for important driver and pilot decisions. Simultaneously, the need for analysis techniques has become more pressing. Either, verification techniques have to ensure correct functioning of such safety-critical control devices or detect errors in their design before they cause fatal injuries. Tragic accidents

indicate that the rising complexity of transportation systems makes it impossible for humans to understand their effects and side effects under all circumstances. This includes flaws in the warning system that led to the frontal train collision in Chatsworth 2008, deficiencies in some adaptive cruise controllers for cars from 2005, and unfortunate human-controller interactions causing the fatal mid-air collision in Überlingen in 2002.

Several large research projects have been launched already in Europe, including AVACS, ARTIST-2, HYCON, Minalogic, and SPEEDS. We need major initiatives for the US to take a lead in advancing the state of the art in CPS analysis.

2 Important Research Challenges for CPS Transportation

The increasing need for analysis techniques that scale to today's tightly integrated transportation control imposes several research challenges for CPS analysis and verification.

Scalable Analysis with respect to Complexity and Dimensionality: The most pressing need today are analysis techniques that actually scale to the full complexity of real applications. The two most fundamental limitations today are that most analysis techniques can only handle fairly limited classes of system dynamics (usually only linear or even constant dynamics) and that the dimension of the continuous state space they can handle is low (around 3-8). Most applications are governed by more complicated differential equations (e.g., flight dynamics) and have substantially higher dimensions (models of the environment).

Beyond any doubt, the major challenge for handling realistic traffic systems is to develop techniques that scale reliably both in the dimension and complexity of the system dynamics. Even today's high precision analyses would already need non-linear dynamics for hundreds of variables. If future research advances are not able to solve the scalability problem, the growing complexity of CPS cannot be managed any more. Without significant technological advances, we are convinced that a thorough safety analysis will never become possible!

Large-scale Verification Architectures for Cyber-Physical Systems: To speed up the verification process with good scalability properties for industrial settings, we envision the development of layered architectures. Rather than verifying each new transportation system from scratch, we consider it more economic and probably even more tractable to devise domain-specific verification frameworks. In much the same way as, e.g., cars are designed as instances of a product family, their safety and failure-robustness analysis should be conducted as a special instance of the general verification framework for ground transportation. For such a framework, a common parametric setup can then be pre-verified once and for all. Each design of a specific traffic agent would then only need to be re-analyzed with respect to a correct instantiation of the more general verification pattern. Ultimately, we conceive the forming of Verification Engineering as a new discipline devoted to the systematic development and use of corresponding domain-specific verification plans.

Dynamic Networks of Cyber-Physical Systems: A different research challenge results from the overwhelming increase of wireless communication in transportation and the resulting consequences for the overall system scope. Already in current implementations of ETCS, GSM-based wireless is the exclusive communication channel for establishing consent as to which train is allowed to move how far on which track. Similarly, the upcoming CAR2CAR

standard for co-operative car communication strives to use wireless adhoc networks to prevent road accidents and circumvent traffic jams. Consequently, we no longer find a fixed static setup of traffic agents. Instead, traffic agents form a fully dynamic network of physically moving hybrid systems with dynamically changing logical communication topology.

The primary research challenge caused by CPS with dynamic topology is that the number of participants can change over time, so that not even the dimension of the system state space remains constant during its evolution. New verification techniques are in order that can handle arbitrary dimensionality adjustments during system transitions. Without these advances, analysis techniques will never be applicable to next generation transportation systems, so that the high potential of modern communication technology could never be used for safety-critical transportation.

Probabilistic Effects in Cyber-Physical Transportation: A further challenge is automatic stochastic analysis of the likelihood of a certain event happening when taking the probability distribution of the corresponding transitions in the CPS into account. For instance, a train in ETCS may stop moving completely when all wireless communication channels suffer from 100% packet loss so that the train cannot receive movement negotiation messages. This is extremely unlikely, though. The question is: Is there an automatic algorithm for determining the probability of a train reaching its destination in time, given, e.g., a certain message loss probability and a particular repetitive sending scheme. More generally, is there an automatic tool that can prove that the failure probability in a stochastic CPS is bounded? Likewise, can we analyze stochastic environment models and sensor failure probabilities? The primary research challenge for stochastic CPS verification is to find analysis techniques that can handle their coupling of stochastic and hybrid dynamic system behavior by analyzing the transformation of appropriate probability distributions during hybrid evolutions. This technology will be of tremendous importance for conducting a formal risk analysis in future CPS for transportation.

3 Biographical Information

Edmund M. Clarke is a University Professor at Carnegie Mellon University and FORE Systems Professor in the School of Computer Science. Among several other awards, he received the ACM Kanellakis Award, the IEEE Harry H. Goode Memorial Award, the ACM Turing Award, and the CADE Herbrand Award.

Bruce Krogh is a Professor in the Department of Electrical and Computer Engineering at Carnegie Mellon University. He was the founding Editor-in-Chief of the *IEEE Transactions on Control Systems Technology*. Dr. Krogh is a Distinguished Member of the IEEE Control Systems Society and a Fellow of the IEEE.

André Platzer is an Assistant Professor in the Computer Science Department at Carnegie Mellon University, Pittsburgh, PA. Among other awards, he received the best paper award at TABLEAUX 2007 and the Woody Bledsoe Award at IJCAR 2006.

Raj Rajkumar is a Professor in the Department of Electrical and Computer Engineering at Carnegie Mellon University. He is Director of the Real-Time and Multimedia Systems Lab and Co-Director of the General Motors-Carnegie Mellon Collaborative Research Labs on Information Technology and on Autonomous Driving.