Automated Testing and Verification for Cyber-Physical Transportation Systems

Georgios Fainekos* Sriram Sankaranarayanan†

Abstract

Small scale deployments of Cyber-Physical Transportation Systems have demonstrated tangible improvements in overall system safety and efficiency. Due to the safety-critical nature of these systems, verification and validation (V&V) methods are needed before such systems can be deployed in larger scales. Current V&V methods either provide solutions for restricted classes of systems or do not provide formal guarantees. There is a need for V&V methods that can scale-up to industrial size systems while at same time providing formal guarantees. Such methods can potential be adopted by certification standards.

1 Introduction

It is envisioned that new levels of efficiency and safety in our transportation systems can be achieved by enabling smart infrastructure and fully autonomous vehicles. The challenges in designing such Cyber-Physical Systems (CPS) are tremendous. The infrastructure-to-vehicle and vehicle-to-vehicle communication must be secure and reliable. The autonomous vehicle must be operating safely and efficiently. Efficiency is manifested at multiple levels of the hierarchy of such systems. For example, the freeway networks are efficiently utilized by platoons of high speed cars. Internal combustion engines must be regulated with complex control laws in order to meet strict environmental requirements while achieving the performance desired by consumers. At the same time, the overall system performance must be guaranteed in a wide range of operating conditions: from the deserts of Arizona to the heights of Alma in Colorado.

The complex system dynamics at all levels of the hierarchy and the strict safety and environmental requirements pose substantial challenges in the design of such systems. The quest for more efficient and safer transportation systems has lead designers to consider complex data fusion and control algorithms using several micro-controllers distributed over the system. The high complexity of these systems increases the probability of modeling, design and implementation errors. As a specific example, consider the modern automobiles. Numerous recalls are posted yearly due to software related errors. Such software related problems are pervasive across manufacturers. The software related recalls in the automotive industry mirror the historical developments in the aerospace industry. It is clear that such errors are critical for both human safety and public endorsement of autonomous technologies.

It is expected that as the vision of fully autonomous cars and aircrafts is being materialized, the software errors are going to exponentially increase. The fore and foremost reason will be the complexity of the software which is not only going to include low-level control functionality, but

*School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ. e-mail: fainekos@asu.edu

†Computer Science, University of Colorado at Boulder, CO. e-mail: srirams@colorado.edu

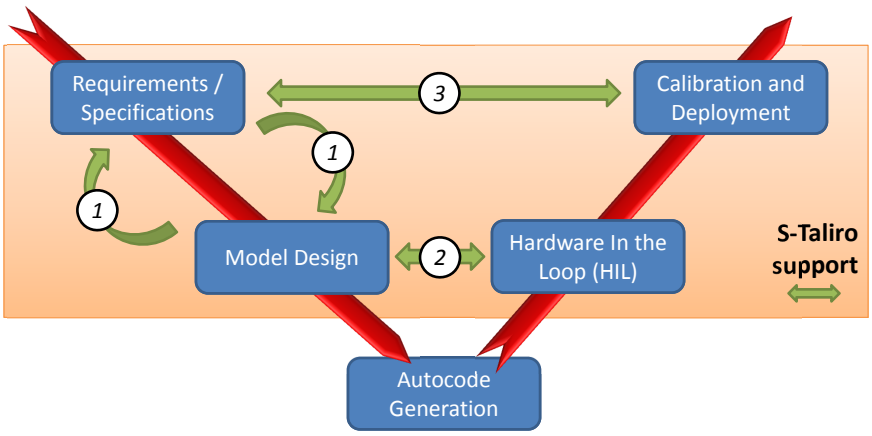

Figure 1: Required support in the Model-Based Development (MBD) of Cyber-Physical Systems (CPS). (1) Iterative development and testing of model; (2) Hardware/Processor-in-the-loop conformance testing; (3) Tuning and verification of prototype system.

also high-level decision making. Moreover, due to the highly non-linear nature of many CPS, it is possible that machine learning algorithms and adaptive control schemes are going to become necessary components of the control architecture. Currently, there are no verification and validation methods that will assess a complex fully autonomous CPS with respect to state and real-time requirements. Moreover, short development cycles are going to magnify the rate of software faults unless new requirements verification methods and technologies emerge for CPS.

2 Requirements

We need an ecosystem of software tools and development practices that support the principled engineering of complex CPS all the way from requirements and specifications to implementation (see Fig. 1). Tools for Model-Based Development (MBD) of CPS must be the central focus since they enable modeling, design and analysis of both the physical and cyber worlds in an integrated way. Currently, such an infrastructure does not really exist and MBD practices are not widely adopted by all sectors of industry. CPS software should be developed in collaboration with or by engineers who understand the properties of the system and not only the software. Thus, we need automatic tool support for engineers that will enable scalable and efficient testing and verification from the requirements phase to the implementation phase.

Beyond software reliability and correctness concerns, the government and industry are still facing certification challenges for adaptive control software. Adaptive control systems usually come with guarantees of asymptotic stability and convergence to the desired performance. However, their transient performance is usually unpredictable when new operating conditions or system modifications occur. Thus, we need a framework that can formally capture functional requirements for adaptive control systems. Moreover, the test cases that excite the worst system behaviors should be automatically discovered by software tools. The existence of such software tools will enable the certification of systems that could not be certified before.

3 Research Challenges

To address the aforementioned challenges, a comprehensive framework for automated testing, verification and validation of CPS developed under MBD practices is needed.

Confidence in Testing Results: Currently, the stochastic optimization methods for testing and falsification are best effort methods. Namely, when such methods are incorporated into the development cycle, they are run in the background – possibly overnight – trying to find a behavior of least robustness with respect to the system requirements. If the search terminates with a falsifying behavior, then this is a concrete counter-example to be used for system debugging and repair. However, when the worst behavior found is still correct, then there are no guarantees on system correctness – even probabilistic ones. Testing methods for CPS must be accompanied by probabilistic guarantees on the confidence on the results returned by the falsification algorithms. Moreover, suitable coverage metrics for CPS must be defined. Certification authorities must to able to quantify and propose coverage requirements on testing CPS the same way they can propose coverage requirements for software testing.

Simulation Explosion: While stochastic optimization methods for testing have had successes, better falsification procedures are necessary for large and complex systems. A major bottleneck of current techniques lies in the use of a large number of simulations to find violations. While the use of trace robustness and stochastic optimization helps reduce the number of simulations when compared to a blind choice of inputs, the number of simulations and time per simulation both increase for complex systems, making falsifications more time consuming. Therefore, there is a need for techniques that minimize the number of simulations required. We envision that by increasing the amount of information about the system, testing algorithms can better guide the testing process and reduce the overall number of tests.

Conformance Testing: A CPS model and its implementation are rarely going to exhibit exactly the same behavior given the same inputs. The parameters of highly complex nonlinear systems must be tuned on the real system in order to get the desired behavior. In other cases, the automatically generated code from the model needs to be modified to account for system artifacts that were not modeled. Finally, the noise in the system actuators and sensors might force the implementation and model to diverge under the same input. The challenge in addressing the conformance problem in an automatic way is to define a useful metric on hybrid (discrete-continuous) system trajectories and, thus, also on the distances between the trajectories of the model and the implementation. We argue that the conformance problem is application dependent and, thus, a number of appropriately defined cost metrics are needed.

4 Biographies

Georgios Fainekos is an Assistant Professor at the School of Computing, Informatics and Decision Systems Engineering at Arizona State University. He is director of the Cyber-Physical Systems (CPS) Lab and he is currently affiliated with the Center for Embedded Systems (CES) at ASU. He received his M.Sc. and Ph.D. in Computer and Information Science from the University of Pennsylvania in 2004 and 2008, respectively. He holds a Diploma degree (B.Sc. & M.Sc.) in Mechanical Engineering from the National Technical University of Athens. He was recipient of the 2008 Frank Anger Memorial ACM SIGBED/SIGSOFT Student Award.

Sriram Sankaranarayanan is an assistant professor of Computer Science at the University of Colorado, Boulder. His research interests include automatic techniques for reasoning about the behavior of computer and cyber-physical systems. Sriram obtained a PhD in 2005 from Stanford University. Subsequently he worked as a research staff member at NEC research labs in Princeton, NJ. He has been on the faculty at CU Boulder since 2009. Sriram has been the recipient of awards including the President's Gold Medal from IIT Kharagpur (2000), Siebel Scholarship (2005), the CAREER award from NSF (2009) and the Dean's award for outstanding junior faculty for the College of Engineering at CU Boulder (2012).