Integrative Challenges of Cyber-Physical Systems Verification

André Platzer

Computer Science Department
Carnegie Mellon University
Pittsburgh, PA
USA
aplatzer@cs.cmu.edu

Abstract. Cyber-physical systems integrate cyber elements with physical elements, thereby combining the computing and physics regimes. This integration has exciting prospects as a basis for advanced systems that solve big technical, societal, economical, and ecological challenges. When designing, understanding, and analyzing these cyber-physical systems, however, we also face big integrative challenges. Challenges of integrating CPS. Challenging of integrating dynamics. Of integrating theories, technologies, and tools. And even challenges of integrating different disciplines. As a way to tackle those challenges, we advocate logical analysis of cyber-physical systems, including a logical verification approach of hybrid systems and of distributed hybrid systems.

1 Cyber-Physical Systems

The notion of *cyber-physical systems* (CPS) is used for systems that tightly integrate cyber elements and physical elements. The cyber elements use computing and communication technology. And the physical elements control physical processes. CPS integrate both regimes, e.g., when computers control physical processes and are communicating with each other over a wireless network. CPS applications come from many different domains, including the automotive, aerospace, factory automation, chemical or physical process control, medical devices, and smart grid energy systems. Because of the impact that CPS have on our physical world, safety-criticality and reliability are extremely relevant aspects of CPS.

Think of, for instance, a car that is driving down the road. Of course, a car uses advanced computer technology for navigation, electronic stability control, adaptive cruise control, lane change assistants, and many other parts of the system design. The car is also very physical and it is important that we understand how it moves on a street. We always want to understand how other cars may move around us so that we can drive safely among them. In order to make sure that the cyber elements work together well with the physical movement, we need to understand the combined CPS aspects of the system. Just looking at the physics will not tell us what the impact of computer decisions in the adaptive cruise control system would be on the car dynamics. And just looking at the computer would not enable us to understand how the physical car is evolving. And we would really like to understand CPS very well in order to make sure that we can certify and trust that the CPS will always operate safely and reliably.

With today's strong sensor, communication, and computation capabilities, it seems like it should be possible to devise smarter car safety assistance systems that uses the full range of technology to prevent accidents. This is exactly what constitutes a full-blown CPS, and exactly what several companies, research projects, and initiatives are working on. The author has recently laid the foundation for the first verification technology that can handle systems like those [4], which are known as distributed hybrid systems.

This is really just one example out of many other CPS applications. Because the CPS model is so general, applications arise in many different forms from various application domains. It is probably even hard to predict which domain will not be effected by CPS ideas.

2 Integrative Challenges

CPS applications abound, because modern technology can help advance several aspects of system design in numerous application domains. Yet, CPS bring along new challenges that need to be addressed.

Integrating CPS First of all, CPS themselves integrate cyber elements and physical elements. They integrate discrete with continuous effects. *Hybrid systems* [1], for instance, are prominent mathematical models for those CPS that integrate discrete and continuous dynamics. The discrete dynamics typically comes from the discrete control decisions and digital controllers. The continuous dynamics comes from the physical process elements of the CPS.

Hybrid systems are a very useful and well-established class of system models. Substantial research has been conducted in the field and the HSCC is a very successful conference series focusing on hybrid systems developments and advances.

Nevertheless, hybrid systems do not model all aspects of all CPS. Distribution effects, for instance, are neglected by hybrid systems models. Multi-agent hybrid systems where multiple hybrid agents coevolve are not captured by hybrid system models. More generally, these systems form *distributed hybrid systems* with discrete dynamics, continuous dynamics, and distributed dynamics. For distributed hybrid systems, verification and analysis has been a long-standing challenge, but a recent breakthrough has shown that verification is still possible for distributed hybrid systems [4].

Integrating Theories, Technologies, and Tools On the level of technical implementations, CPS integrate different technologies from mechanical design, sensor manufacturing, and computer programming techniques. There is an even greater number of technologies that have to be combined in order to understand, analyze, and design CPS. This includes combinations of techniques from logic, from mathematics, from control, and from electrical engineering.

In a heterogeneous world with very different CPS for different problems, it is not surprising that different tools with different strengths need to be integrated for different parts of the solution. Recurring themes include the need to handle arithmetic data, differential equations, and either a form of abstraction, or iteration, or induction. The author is one of the lead developers behind the verification tool KeYmaera [5], a theorem prover for hybrid systems. KeYmaera integrates numerous techniques for automated theorem proving, fixedpoint procedures, decision procedures for nonlinear real arithmetic [6], computer algebra, SMT, and other parts of the verification problem.

Integrating Disciplines CPS integrate many insights from computer science, mathematics, and electrical and mechanical engineering. Those disciplines need to work together in order to solve the integrative challenges of CPS. Today's system design is still too much dominated by teams working independently on cyber aspects, and other teams working working independently on physical aspects. CPS challenges need joint solutions for the combined problems.

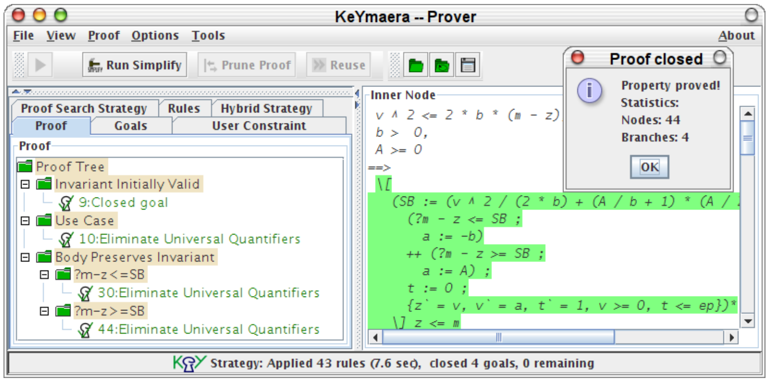
3 A Logical Approach to CPS Verification

As a solution for the verification challenges arising in CPS, we advocate a logical approach to CPS verification. We have developed a logical analysis and verification approach for hybrid systems [3]. This approach is based on a strong logical and mathematical foundation. Its theoretical properties have been analyzed in detail and the approach has been shown to possess important properties like soundness and relative completeness [3, 2]. The approach has been implemented in the verification tool KeYmaera[1] [5]; see Fig. 1.

The logical verification approach has also been used successfully in a number of case studies, including verification of collision freedom in flight collision avoidance maneuvers, collision freedom of the cooperation protocol for the European Train Control System, and verification of a distributed car control system. These application scenarios have different characteristics, ranging from implicit communication overapproximations to explicit communication and from ideal-world dynamics to system models with disturbance. They include both applications with complicated safety-critical spatio-temporal constraints and with dynamic partitioning into regions. These applications consider systems with small, medium, or large and varying number of participants.

The underlying system models cover fundamentally different mathematical characteristics, including linear dynamics, nonlinear dynamics, and distributed dynamics. With that range of different characteristics, we hope that a good range of usability in verification has been demonstrated concerning the flexibility of

[1] Available at http://symbolaris.com/info/KeYmaera.html



Proof

```
Proof Tree
⊟ Invariant Initially Valid
    9:Closed goal
⊟ Use Case
    10:Eliminate Universal Quantifiers
⊟ Body Preserves Invariant
  ⊟ ?m-z<=SB
      30:Eliminate Universal Quantifiers
  ⊟ ?m-z>=SB
      44:Eliminate Universal Quantifiers
```

```
 v ^ 2 <= 2 * b * (m - z)
 b >  0,
 A >= 0
==>
 \[
   (SB := (v ^ 2 / (2 * b) + (A / b + 1) * (A / 
     (?m - z <= SB ;
       a := -b)
     ++ (?m - z >= SB ;
       a := A) ;
     t := 0 ;
     {z` = v, v` = a, t` = 1, v >= 0, t <= ep})*
   \] z <= m
```

Proof closed

Property proved!
Statistics:
Nodes: 44
Branches: 4

Strategy: Applied 43 rules (7.6 sec), closed 4 goals, 0 remaining

Fig. 1. Verification tool KeYmaera for hybrid systems

models. There are other aspects of usable verification that would benefit from further investigation, including scalability, out-of-the-box automation, and ease of use.

4 Biographical Information

André Platzer is an Assistant Professor in the Computer Science Department at Carnegie Mellon University, Pittsburgh, PA. Among several other awards, he received the ACM Doctoral Dissertation Honorable Mention Award 2009 and the Brilliant 10 Young Scientists Award by Popular Science in 2009. His research interests include logic, hybrid systems, distributed hybrid systems, and CPS verification.

References

1. Thomas A. Henzinger. The theory of hybrid automata. In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society.
2. André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reas.*, 41(2):143–189, 2008.
3. André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, Sep 2010.
4. André Platzer. Quantified differential dynamic logic for distributed hybrid systems. In Anuj Dawar and Helmut Veith, editors, *CSL*, volume 6247 of *LNCS*, pages 469–483. Springer, 2010.
5. André Platzer and Jan-David Quesel. KeYmaera: A hybrid theorem prover for hybrid systems. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *IJCAR*, volume 5195 of *LNCS*, pages 171–178. Springer, 2008.
6. André Platzer, Jan-David Quesel, and Philipp Rümmer. Real world verification. In Renate A. Schmidt, editor, *CADE*, volume 5663 of *LNCS*, pages 485–501. Springer, 2009.