Endorsements

This excellent textbook marries design and analysis of cyber-physical systems with a logical and computational way of thinking. The presentation is exemplary for finding the right balance between rigorous mathematical formalization and illustrative case studies rooted in practical problems in system design.

Rajeev Alur, University of Pennsylvania

This book provides a wonderful introduction to cyber-physical systems, covering fundamental concepts from computer science and control theory from the perspective of formal logic. The theory is brought to life through many didactic examples, illustrations, and exercises. A wealth of background material is provided in the text and in an appendix for each chapter, which makes the book self-contained and accessible to university students of all levels.

Goran Frehse, Université Grenoble Alpes

[The author] has developed major important tools for the design and control of those cyber-physical systems that increasingly shape our lives. This book is a 'must' for computer scientists, engineers, and mathematicians designing cyber-physical systems.

Anil Nerode, Cornell University

As computing interfaces increasingly with our physical world, resulting in so-called cyber-physical systems, our foundations of computing need to be enriched with suitable physical models. This book strikes a wonderful balance between rigorous foundations for this next era of computing with illustrative examples and applications that drive the developed methods and tools. A must read book for anyone interested in the development of a modern and computational system science for cyber-physical systems.

George J. Pappas, University of Pennsylvania

This definitive textbook on cyber-physical systems lays the formal foundations of their behavior in terms of a single logical framework. Platzer's logic stands out among all other approaches because it provides a uniform treatment of both the discrete and continuous nature of cyber-physical systems, and does not shy away from their complex behavior due to stochasticity, uncertainty, and adversarial agents in the environment. His computational thinking approach makes this work accessible to practicing engineers who need to specify and verify that cyber-physical systems are safe.

Jeannette M. Wing, Columbia University

Foreword

I first met André when he was just finishing his PhD and gave a job talk at CMU (he got the job). I was a visiting researcher and got to take the young faculty candidate out for lunch. André talked about verifying cyber-physical systems (CPS) using "differential dynamic logic" and theorem proving. I was skeptical, for one because related approaches had only seen modest success, and also because my money was on a different horse. A few years before, I had developed a model checker (PHAVer), and was working on a second one, called SpaceEx. At the time, these were the only verification tools that, on the push of a button, could verify certain benchmarks from CPS and other domains involving continuous variables that change with time. I was quite proud of them and, for me, algorithmic verification was the way to go. But André was determined to make theorem proving work in practice, and indeed, he advanced the field to an extent that I did not think possible. André and his team first developed the logical framework, then built a very capable theorem prover for CPS (KeYmaera), successfully applied it to industrial case studies like airplane collision avoidance, and, finally, addressed important application issues such as validating the model at runtime.

The book in front of you provides a comprehensive introduction on how to reason about cyber-physical systems using the language of logic and deduction. Along the way, you will become familiar with many fundamental concepts from computer science, applied mathematics, and control theory, all of which are essential for CPS. The book can be read without much prior knowledge, since all necessary background material is provided in the text and in appendices for many chapters. The book is structured in the following four parts. In the first part, you will learn how to model CPS with continuous variables and programming constructs, how to specify requirements and how to check whether the model satisfies the requirements using proof rules. The second part adds differential equations for modeling the physical world. The third part introduces the concept of an adversary, who can take actions that the system can not influence directly. In a control system, the adversary can be the environment, which influences the system behavior through noise and other disturbances. Making decisions in the presence of an adversary means trying to be prepared for the worst case. The fourth part adds further elements for reasoning soundly and efficiently about systems in applications, such as using real arithmetic and – my favorite – monitor conditions. Monitor conditions are checked while the system is in operation. As long as they hold, one can be sure that not only the model but also the actual CPS implementation satisfy the safety requirements.

By now André and his group have handled an impressive number of case studies that are beyond the capabilities of any model checker I know. Fortunately for me and my horse, the converse is also still true, since some problems can in practice only be solved numerically using algorithmic approaches. If your goal is to obtain a rock-solid foundation for CPS from the beautiful and elegant perspective of logics, then this is the book for you.

Goran Frehse, Associate Professor, Université Grenoble Alpes, Grenoble, 2017