André Platzer

Lecture Notes on Foundations of Cyber-Physical Systems

15-424/624/824 Foundations of Cyber-Physical Systems

Chapter 1
Cyber-Physical Systems: Overview

Synposis This chapter provides an informal introduction to cyber-physical systems, setting the stage for this textbook. The primary purpose is a light-weight overview of the technical and non-technical characteristics of cyber-physical systems, some of their application domains, and a discussion of their prospects and challenges. The chapter also informally outlines and explains the approach taken in this book to address safety challenges in cyber-physical systems.

1.1 Introduction

This chapter provides a light-weight introduction to *cyber-physical systems* (*CPS*), which combine cyber capabilities (computation and/or communication as well as control) with physical capabilities (motion or other physical processes).

Note 1 (CPS) Cyber-physical systems *combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone.*

Cars, aircraft, and robots are prime examples, because they move physically in space in a way that is determined by discrete computerized control algorithms that are adjusting the actuators (e.g., brakes) based on sensor readings of the physical state. Designing these algorithms to control CPSs is challenging due to their tight coupling with physical behavior. At the same time, it is vital that these algorithms be correct, since we rely on CPSs for safety-critical tasks like keeping aircraft from colliding.

> How can we provide people with cyber-physical systems they can bet their lives on? – Jeannette Wing

Since cyber-physical systems combine cyber and physical capabilities, we need to understand both to understand CPS. It is not enough to understand both capabilities only in isolation, though, because we also need to understand how the cyber

and the physics work together, i.e. what happens when they interface and interact, because this is what CPSs are all about.

1.1.1 Cyber-Physical Systems Analysis by Example

Airplanes provide a rich source of canonical examples for cyber-physical systems analysis challenges. While they are certainly not the only source of examples, airplanes quickly convey both a spatial intuition for the motion and an appreciation for the resulting challenges of finding out where and how to fly.

Fig. 1.1 Aircraft example: Which control decisions are safe for aircraft collision avoidance?

If a pilot has gotten into a situation where her airplane is too close to other aircraft, see Fig. 1.1, then it would be immensely helpful to give the pilot good advice about how to best maneuver to resolve the situation. Of course, such advice needs to be given quickly and safely. There is not enough time to carefully plan out every possible trajectory of the ownship and all other intruder aircraft, but a quick response is needed right away, which is what computers are good at. But the advice also has to be safe such that it reliably separates the aircraft always under all relevant scenarios of when and how exactly the pilots will respond to the advice. For the ownship (following the blue trajectory), Fig. 1.1 gives a schematic illustration of unsafe zones (in shades of red) resulting from given intruder aircraft (gray).

More generally, this begs the question which control decisions are safe for aircraft collision avoidance. How can one predict right away whether given control decisions for the aircraft and intruders are guaranteed to be safe or whether they could possibly lead to a collision? How can a computer control program be designed that reaches safe decisions and gives good advice to pilots sufficiently quickly? What would constitute a safety argument for such a pilot decision support system, which justifies why the system always suggests safe collision avoidance advice?

1.1.2 Application Domains

Cyber-physical systems provide prospects of improved safety and efficiency in numerous application domains [2, 29, 30, 58]. Examples include both autonomous self-driving cars and improved driver assistance technology for cars such as lane keeping assistants or distance keeping assistants [1, 12, 32, 35], where computer control technology helps people drive cars more safely and more efficiently. Both pilot decision support systems [23, 24, 55, 64] and full autopilots for unmanned aerial vehicles (UAVs) fall under this paradigm. In the former, the computer focuses on an advisory role where it gives decision support to pilots who are ultimately in

charge. But autopilots also automate the flight during certain well-defined phases of the flight, such as in normal cruise flight or during landing. The case of UAVs provides more comprehensive automation where the computer is in primary control of the UAV for extended periods of time and remote pilots limit themselves to only providing certain control decisions every once in a while. Other applications include train protection systems [56], power plants [14], medical devices [25, 30], robots that operate in the vicinity of humans [36, 41], or robotic surgery systems [7, 26]. Autonomous underwater vehicles (AUVs) also need computer control for sustained operation since their operating conditions only provide infrequent opportunities for human intervention. Many other application domains are of relevance, though, because the principle of using computer control to help physical systems is quite general.

1.1.3 Significance

Cyber-physical systems can help in many ways. In cars, computers support the human driver by taking control of the car either in full or partially for a certain period of time. For example, the computer can help prevent accidents by keeping the car on the lane in case the human driver is inattentive and/or decelerates when the driver fails to notice that the car in front is braking. Of course, the tricky bit is that the computer needs to be able to reliably detect the circumstances where a correction of the car's trajectory is in order. In addition to the nontrivial challenges of reliably sensing other cars and lanes, the computer needs to distinguish user-intended lane changing from accidental lane departures, for example based on whether the driver signaled a lane change by a turn signal, and apply steering corrections appropriately.

In aerospace, computers can not just support pilots during fair weather phases of the flight such as cruise flight, but can also help by providing pilots with quick collision avoidance advice whenever two or more aircraft got too close together. Since that is a very stressful situation for the pilots, good advice on how to get out of it again and avoid possible collisions is quite important. Likewise remote pilots cannot necessarily monitor all flight paths of UAVs closely all the time, such that computer assistance would help prevent collisions with commercial aircraft or other UAVs. Besides detection, the primary challenges are the uncertainties of when and how exactly the respective aircraft follow their trajectories and, of course, the need to prevent follow-on conflicts with other aircraft. While already quite challenging for two aircraft, this problem gets even more complicated in the presence of multiple aircraft, possibly with different flight characteristics.

For railway applications, technical safety assistance is also crucial, because the braking distances of trains exceed the field of vision such that the brakes need to be applied long before another train is in sight. One challenge is to identify a safe braking distance that works reliably for the current train and track conditions without reducing the expected overall performance by braking too early. Unlike a maximum

use of the conventional service brake, full emergency brakes on a train may also damage the rails or wheels.

1.1.4 The Importance of Safety

Wouldn't it be great if we could use computers to leverage the advances in safety and efficiency in the CPS application domains? Of course, the prerequisite is that the cyber-physical systems themselves need to be safe, otherwise the cure might be worse than the disease. Safety is paramount to ensure that the cyber-physical systems that are meant to improve safety and efficiency actually help. So, the key question is:

How do we make sure cyber-physical systems make the world a better place?

Because the world is a difficult place, this is rather a difficult question to answer. An answer needs enough understanding of the world (in a model of the relevant part of the world), the control principles (what control actions are available and what is their effect on the physical world) and their implementation in a computer controller, as well as the requisite safety objectives (what precisely discriminates safe from potentially unsafe behavior). This leads to the following rephrasing [53]:

How can we ensure that cyber-physical systems are guaranteed to meet their design goals?

Whether we can trust a computer to control physical processes depends on how it has been programmed and on what will happen if it malfunctions. When a lot is at stake, computers need to be guaranteed to interact correctly with the physical world.

The rationale pursued in this book argues that [53]:

1. Computers would perfectly earn our trust to control physics if only they came with suitable guarantees.
2. Safety guarantees require appropriate analytical foundations.
3. A foundational core that is common to *all* application domains is more useful than different mathematics for each area, e.g., a special mathematics for trains.
4. Foundations have already revolutionized the digital parts of computer science and, indirectly, the way our whole society works.
5. But we need even stronger foundations when software reaches out into our physical world.

These considerations lead to the following conclusion:

Because of the impact that they can have on the real world, cyber-physical systems deserve proofs as safety evidence.

As has already been argued on numerous other occasions [2–6, 10, 11, 13, 19, 20, 27, 28, 33, 34, 37–40, 42, 43, 45, 58, 61–63, 66], the correctness of these systems needs to be verified, because testing may miss bugs. This problem is confounded, though, because the behavior of a CPS under one circumstance can radically differ from the behavior under another, especially when complex computer decisions for different objectives interact. Of course, due to their involvement of models of reality, the safety evidence should not be limited to proofs alone either, but needs to include appropriate testing as well. But without the generality resulting from mathematical proofs, it is ultimately impossible to obtain strong safety evidence beyond the isolated experience on the particular situations covered by the test data [49, 54, 67].

1.2 Hybrid Systems versus Cyber-Physical Systems

While the defining criterion that cyber-physical systems combine cyber capabilities with physical capabilities makes it easy to recognize them in practice, this is hardly a precise mathematical criterion. For the characteristic behavior of a system, it should be mostly irrelevant whether it happens to be built literally by combining an actual computer with a physical system, or whether it is built in another way, e.g., by combining the physical system with a small embedded controller achieving the same performance, or maybe by exploiting a biochemical reaction to control a process.

Indeed, cyber-physical systems share mathematical characteristics, too, which are in many ways more important for our endeavor than the fact that they are built from cyber components and from physical components. While a full understanding of the mathematical characteristics of cyber-physical systems will keep us busy for the better part of this book, it is reasonably straightforward to arrive at what is at the core of all mathematical models for cyber-physical systems. From a mathematical perspective, cyber-physical systems are (at least) hybrid systems:

Note 2 (Hybrid systems) Hybrid systems *are a mathematical model for dynamical systems that combine discrete dynamics with continuous dynamics. Their behavior includes both aspects that change discretely one step at a time and aspects that change continuously as continuous functions over time.*

For example, the aircraft in Fig. 1.1 fly continuously along their trajectories as a continuous function of continuous time, since aircraft do not jump around in space with discrete jumps. Every once in a while, though, the pilot and/or autopilot reaches a decision about turning in a different direction to avoid a possible collision with

intruder aircraft. These discrete decisions are best understood as a discrete dynamics in discrete time, because they happen one step after another.

Similarly, a car controller would decide to accelerate or brake, which is best understood as a discrete dynamics, because there is a discrete instant of time where that decision is reached and scheduled to take effect. The car's continuous motion down the road, instead, is best understood as a continuous dynamics, because it changes the position as a continuous function of time.

In the most naïve interpretation, the cyber components of cyber-physical systems correspond to the discrete dynamics of hybrid systems while the physical components of cyber-physical systems correspond to the continuous dynamics of hybrid systems. While possibly a good mental model initially, this view will turn out to be too simplistic. For example, there are events in physical models that are best described by a discrete dynamics even if they come from the physics. For instance, the touchdown of an airplane on the ground could be considered as causing a discrete state change by a discrete dynamics even if the runway that the aircraft touches down on is quite physical and not a cyber-construct at all. Conversely, for some purposes, some of the computations happen so frequently and so quickly that we best understand them as if they were running continuously even if that is not entirely true. For instance, a digital PID controller for an inner loop flight controller could sometimes be considered as having a continuous effect even if it is implemented as a digital device.

In fact, this is one of the liberating effects of understanding the world from a hybrid systems perspective [53]. Since the mathematical principles of hybrid systems accept both discrete and continuous dynamics, we do not have to either coerce all aspects of a system model into the discrete to understand it with discrete mathematics or force all system aspects into a continuous understanding to analyze it with continuous techniques. Instead, hybrid systems make it perfectly acceptable to have some aspects discrete (such as the steps of a digital controller) and others continuous (such as continuous-time motion), while allowing modeling decisions about ambivalent aspects. For some purposes, it might be better to model the touch-down of an aircraft as a discrete state change from in-the-air to on-the-ground. For other purposes, such as developing an autopilot for landing it is important to take a more fine-grained view. Hybrid systems enable such tradeoffs.

Overall, hybrid systems are *not* the same as cyber-physical systems. Hybrid systems are mathematical models for complex (often physical) systems, while cyber-physical systems are defined by their technical characteristics. Nevertheless, exhibiting a hybrid systems dynamics is such a common feature of cyber-physical systems that we will take the liberty of using the notions cyber-physical system and hybrid system quite interchangeably at least in the first parts of this book.

Despite this linguistic simplification, you should note that hybrid systems can be nontechnical. For example, certain biological mechanisms can be captured well with hybrid system models [63] or genetic networks [18] even if they have nothing to do with cyber-physical systems. Conversely, a number of cyber-physical systems feature additional aspects beyond hybrid systems, such as adversarial dynamics (studied in Part III), distributed dynamics [47], or stochastic dynamics [46].

1.3 Multi-dynamical Systems

Owing to the fact that cyber-physical systems can have more dynamical aspects than just that of hybrid systems, this book follows the more general multi-dynamical systems principle [48, 53] of understanding cyber-physical systems as a combination of multiple elementary dynamical aspects.

Note 3 (Multi-dynamical system) Multi-dynamical systems *[48] are mathematical models for dynamical systems characterized by multiple facets of dynamical systems, schematically summarized in Fig. 1.2.*

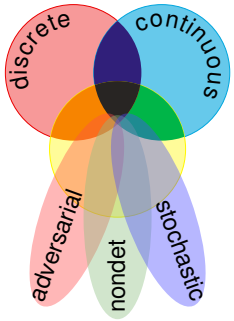


Fig. 1.2 Multi-dynamical systems aspects of CPS

CPSs involve computer control decisions and are, thus, *discrete*. CPSs are also *continuous*, because they evolve along differential equations of motion or other physical processes. CPSs are often *uncertain*, because their behavior is subject to choices coming from either environmental variability or from intentional uncertainties that simplify their model. This uncertainty can manifest in different ways. Uncertainties make CPSs *stochastic* when good information about the distribution of choices is available [46]. Uncertainties make CPSs *nondeterministic* when no commitment about the resolution of choices is made. Uncertainties make CPSs *adversarial* when they involve multiple agents with potentially conflicting goals or even active competition in a game [52]. Verifying that CPSs work correctly requires dealing with many of these dynamical features at the same time. Sometimes, CPSs require even more dynamical features, such as *distributed* dynamics [47].

Hybrid systems are the special case of multi-dynamical systems that combine discrete and continuous dynamics and will be considered in Parts I and II. *Hybrid games* are multi-dynamical systems that combine discrete, continuous, and adversarial dynamics, which will be studied in Part III. *Stochastic hybrid systems* are multi-dynamical systems that combine discrete, continuous, and stochastic dynamics, but are beyond the scope of this book [8, 46]. *Distributed hybrid systems* are multi-dynamical systems combining discrete, continuous, and distributed dynamics [47].

Multi-dynamical systems study complex CPS as a combination of multiple elementary dynamical aspects. Throughout this book, we will come to appreciate how this approach helps to tame the complexity of CPS by understanding that their complexity just comes from combining lots of simple dynamical effects with one another. The overall system is quite complex, but each of its pieces is better-behaved, since it only has one dynamics as opposed to all of them at once. What miracle translates this *descriptive simplification* of a CPS described as a combination of multiple dynamical aspects into an *analytic simplification* of multiple dynamical systems that can be considered side-by-side during analysis? The descriptive simplification is a helpful modeling advantage to disentangle different dynamical aspects of the system into separate aspects of a model. But the biggest impact of multi-dynamical systems is in how they enable an analytic simplification of studying and analyzing the individual dynamical aspects separately. How does the descriptive advantage carry over to an analytic advantage?

The key to this mystery is to integrate the CPS dynamics all within a single, compositional logic [48, 53]. Compositionality means that the meaning of a construct is a simple function of the meaning of the pieces [59]. For example, the meaning of the logical conjunction operator $\wedge$ (read as "and") is a simple function of the meaning of its pieces. The formula $A \wedge B$ (read as "A and B") is true exactly if A is true and B is true, too. Another way to say that is that the set of states of a system in which formula $A \wedge B$ is true is exactly the intersection of the set of states in which A is true with the set of states in which B is true, because it is this intersection of states in which both A and B are true.

Since compositionality is an intrinsic feature starting from the very semantics of logic [15, 17, 21, 22, 57, 60], logics naturally reason compositionally, too. For example, a proof of the formula $A \wedge B$ will consist of a combination of a proof of A together with a proof of B, because the two of those proofs together justify that A and B are both true.

With suitable generalizations of logics to embrace multi-dynamical systems [42, 44, 46, 47, 49, 51, 52], this compositionality generalizes to CPS. We just need to make compositionality work for the CPS operators, which are, of course, are more complicated than a mere logical and. Verification works by constructing a proof in such a multi-dynamical systems logic. The whole proof verifies a complex CPS. Yet, each proof step only reasons separately about one dynamical aspect at a time, for example, an isolated discrete assignment or the separate local dynamics of differential equation, each captured in a separate, modular reasoning principle.

Multi-dynamical systems also impact and simplify the presentation of the Foundations of Cyber-Physical Systems. The compositionality principles of logic and multi-dynamical systems considerably tame the conceptual complexity of CPS by making it possible to focus on one aspect at a time without losing the ability to combine the understanding attained for each aspect. This gradual approach effectively conveys the principles for a successful separation of concerns for CPS.

1.4 How to Learn about Cyber-Physical Systems

There are two primary ways of learning about cyber-physical systems.

Onion Model

The *Onion Model* follows the natural dependencies of the layers of mathematics going outside in, peeling off one layer at a time, and progressing to the next layer when all prerequisites have been covered. This would require the CPS advocate to first study all relevant parts of computer science, mathematics, and engineering, who can then return to CPS in the big finale. This would turn this book into at least requiring the first part on real analysis, the second part on differential equations, the third part on conventional discrete programming, the fourth part on classical discrete logic, the fifth part on theorem proving, and finally the last part on cyber-physical systems. In addition to the significant learning perseverance that the Onion Model requires, a downside is that it misses out on the integrative effects of cyber-physical systems that can bring different areas of science and engineering together, and provide a unifying motivation for studying them in the first place.

Scenic Tour Model

This book follows the *Scenic Tour Model*, which starts at the heart of the matter, namely cyber-physical systems, going on scenic expeditions into various directions to explore the world around as we find the need to understand the present subject matter. The textbook directly targets CPS right away, beginning with simpler layers that the reader can understand in full before moving on to the next challenge. For example, the first layer are CPS without feedback control, which allow simple finite open-loop controls to be designed, analyzed, and verified without the technical challenges considered in later layers of CPS. Likewise, the treatment of CPS is first limited to cases where the dynamics can be solved in closed form, such as straight line accelerated motion of Newtonian dynamics before generalizing to systems with more challenging differential equations that can no longer be solved explicitly. This gradual development where each level is mastered and understood and practiced in full before moving to the next level is quite helpful to tame complexity. The Scenic Tour Model has the advantage that we stay on cyber-physical systems the whole time and leverage CPS as the guiding motivation for understanding more and more about the connected areas. It has the disadvantage that the resulting gradual development of CPS does not necessarily always present matters in the same way that an after-the-fact compendium would treat it. This textbook compensates by providing appropriate technical summaries and highlighting important results for later reference in boxes, with a list of theorems and lemmas in the table of contents.

Besides the substantial organizational impact of this "CPS first" approach throughout the presentation of this book, the Scenic Tour Model is most easily noticeable

in the Expedition boxes that this textbook provides. Every part of this textbook is written in a simple style bringing mathematical results in as needed, and with an emphasis on intuition. The Expedition boxes invite the reader to additionally connect to other areas of science that are of no crucial relevance for the immediate study of CPS, but still provides a peculiar link to another area, in case the reader happens to be familiar with it or finds this link as an inspiration to explore that other area further.

Prerequisites

Even if deliberately light on prerequisites, this textbook cannot start from zero either. Its primary assumptions are some prior exposure to basic programming and elementary mathematics. Specifically, the textbook assumes that the reader has had some prior experience with computer programming (such as what is covered in a first semester undergraduate course taught in any programming language to understand concepts like if-then-else conditionals or loops).

While Chap. 2 starts out with an intuitive as well as a rigorous treatment of differential equations and provides a few conceptually important meta-results in its appendix, this book is no replacement for a differential equations course. But it also does not have to be. The concepts required for CPS from differential equations will be picked up and expanded upon at a light pace. The textbook does, however, assume that the reader is comfortable with simple derivative and differential equation notation. For example, Chap. 2 will discuss how $x' = v, , v' = a$ is a differential equation, in which the time-derivative x' of position x equals velocity v, whose time-derivative v' in turn equals the acceleration a. This differential equation characterizes accelerated motion of a point x with velocity v and acceleration a along a straight line.

Most crucially, the textbook assumes that the reader has been exposed to some form of mathematical reasoning before (such as *either* in a calculus or analysis course *or* in a matrix or linear algebra course *or* a mathematics course for computer scientists or engineers). The particular contents covered in such a prior course are not at all as important as the mathematical experience itself with mathematical developments and proofs. This textbook develops a fair amount of logic on its own as part of the way of understanding cyber-physical systems. A prior understanding of logic is, thus, not necessary for the study of this book. And, in fact, the *Foundations of Cyber-Physical Systems* undergraduate course that the author teaches at Carnegie Mellon University counts as fulfilling a Logics/Languages elective or Programming Languages requirements.

1.5 Computational Thinking for Cyber-Physical Systems

The approach that this book follows takes advantage of Computational Thinking [65], just for cyber-physical systems [50]. Due to their subtleties and the intricate

interactions of complex control software with the physical world, cyber-physical systems are notoriously challenging. Logical scrutiny, formalization, and correctness proofs are, thus, critical for cyber-physical systems. Because cyber-physical system designs are so easy to get wrong, these logical aspects are an integral part of CPS design and critical to understanding their complexities.

The primary attention in this book, thus, is on the foundations and core principles of cyber-physical systems. The book tames some of the complexities of cyber-physical systems by focusing on a simple core programming language for CPS. The elements of the programming language are introduced hand-in-hand with their reasoning principles, which makes it possible to combine CPS program design with their safety arguments. This is important, not just because abstraction is a key factor for success in CPS, but also because retrofitting safety is not possible in CPS.

To simplify matters, the chapters in this book are also organized to carefully reveal the complexities of cyber-physical systems in layers. Each layer will be covered in full, including their programmatic, semantic, and logical treatment, before proceeding to the next level of complexity. For example, the chapters first study single-shot control before considering control loops, and only then proceed to systems with differential equations that cannot be solved in closed form.

1.6 Learning Objectives

The respective learning objectives are identified at the beginning of each chapter, both textually and with a schematic diagram. They are organized along the three dimensions *modeling and control*, *computational thinking*, and *CPS skills*. The most important overall learning objectives throughout this textbook are the following.
Modeling and Control: In the area of *Modeling and Control* (MC), the most important goals are to

- **understand the core principles behind CPS.** The core principles are important for effectively recognizing opportunities how the integration of cyber and physical aspects can solve problems that no part could solve alone.
- **develop models and controls.** In order to understand, design, and analyze CPSs, it is important to be able to develop models for the various relevant aspects of a CPS design and to design controllers for the intended functionalities based on appropriate specifications.
- **identify the relevant dynamical aspects.** It is important to be able to identify which types of phenomena of a CPS have a relevant influence for the purpose of understanding a particular property of a particular system. These allow us to judge, for example, when it is important to manage stochastic effects, or when a nondeterministic or adversarial model is more adequate.

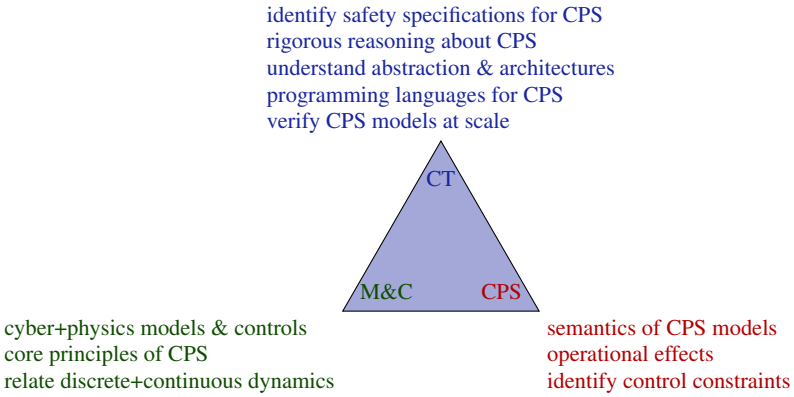
Computational Thinking: In the area of *Computational Thinking* (CT), the most important goals are to

- **identify safety specifications and critical properties.** In order to develop correct CPS designs, it is important to identify what "correctness" means, how a design may fail to be correct, and how to make it correct if it is not correct yet.
- **understand abstraction and system architectures.** Both abstraction and architectural insights are essential for the modular organization of CPS, and for the ability to reason about separate parts of a system independently. Because of the overwhelming practical challenges and numerous levels of detail, abstraction is even more critical than it already is in conventional software design.
- **express pre- and post-conditions and invariants for CPS models.** Pre- and post-conditions allow us to capture under which circumstance it is safe to run a CPS or a part of a CPS design, and what safety entails. They allow us to achieve what abstraction and hierarchies achieve at the system level: decompose correctness of a full CPS into correctness of smaller pieces. The fundamental notion of invariants achieves a similar decomposition by establishing which relations of variables remain true no matter how long and how often the CPS runs.
- **use design-by-invariant.** In order to develop correct CPS designs, invariants are an important structuring principle guiding what the control has to maintain in order to preserve the invariant. This guidance simplifies the design process, because it applies locally at the level of individual localized control decisions that preserve invariants without explicitly having to take system-level closed-loop properties into account.
- **reason rigorously about CPS models.** Reasoning is required to ensure correctness and find flaws in a CPS design. Both informal reasoning and formal reasoning in a logic are important objectives for being able to establish correctness.
- **verify CPS models of appropriate scale.** Formal verification and validation helps finding and fixing bugs and proving correctness, which is helpful in all stages of the CPS design. Formal verification is not only critical but, given the right abstractions, surprisingly feasible in high level CPS control designs.

CPS Skills: In the area of *CPS skills*, the most important goals are to

- **understand the semantics of a CPS model.** What may be easy in a classical isolated program becomes very demanding when that program interfaces with effects in the physical world. A precise understanding of the nuanced meaning of a CPS model is fundamental to reasoning, along with an understanding of how it will execute. A deep understanding of the semantics of CPS models is also obtained by carefully relating their semantics to their reasoning principles and aligning them in perfect unison.
- **develop an intuition for operational effects.** Intuition for the joint operational effect of a CPS is crucial. For example, it is crucial to understand what the effect of a particular discrete computer control algorithm will be on a continuous plant.
- **identify control constraints.** An operational intuition guides our understanding of the operational effects and, along with their precise logical rendition, their impact on finding correct control constraints that make a CPS controller safe.

This textbook will give the reader the required skills to formally analyze the cyber-physical systems that are all around us – from power plants to pace makers and everything in between – so that when you contribute to the design of a CPS, you are able to understand important safety-critical aspects and feel confident designing and analyzing system models. Other beneficial byproducts include that cyber-physical systems provide a well-motivated exposure to numerous other areas of mathematics and science in action.



1.7 Structure of This Book

This textbook consists of three main parts that develop different levels of the foundations of cyber-physical systems. You are now reading the introduction.

Elementary Cyber-Physical Systems

Part I studies elementary cyber-physical systems characterized by a hybrid system dynamics whose continuous dynamics can still be solved in closed form. Differential equations are studied as models of continuous dynamics, while control programs are considered for the discrete dynamics. Part I investigates differential dynamic logic for specifying properties and axioms for reasoning about CPS. It further investigates appropriate structuring principles for proofs and the handling of control loops via loop invariants and discusses both event-triggered and time-triggered control. This part provides an extensive introduction into the wonders and challenges of cyber-physical systems, but still isolates most of the reasoning challenges in the search for discrete loop invariants since their differential equations can still be solved explicitly. While enabling interesting and challenging considerations about

CPSs, Part I limits the level of interaction and subtlety in their safety arguments. The insights from Part I enable, for example, a comprehensive study of controllers for safe acceleration and braking of a car along a straight lane.

Differential Equations Analysis

Part II considers advanced cyber-physical systems whose dynamics cannot be solved in explicit closed form. Most crucially, this necessitates indirect forms for analyzing the safety of the CPS, because solutions are no longer helpful. Based on the understanding of discrete induction for control loops from Part I, Part II develops induction techniques for differential equations. In addition to developing differential invariants as induction techniques for differential equations, this part studies differential cuts that make it possible to prove and then use lemmas about differential equations. It also considers so-called differential ghosts, which can simplify safety arguments by adding extra variables (ghost variables or auxiliary variables) with additional differential equations into the dynamics for balancing out the expected invariant equations. Part II is required to handle safety arguments for CPS with nonsolvable dynamics such as robots racing on a circular race track or driving along curves in the plane or for aircraft flying along three-dimensional curves.

Adversarial Cyber-Physical Systems

Part III fundamentally advances the understanding of cyber-physical systems to cover hybrid games mixing discrete dynamics, continuous dynamics, and adversarial dynamics. Based on the understanding of hybrid systems models for CPSs from Part I and invariants for differential equations from Part II, Part III shifts the focus to an exploration of hybrid games, in which the interaction of different players with different objectives is a dominant aspect. Unlike in hybrid systems, in which all choices are nondeterministic, hybrid games give different choices to different players at different times. Part III is required to handle safety arguments for CPS in which multiple agents interact with possibly conflicting goals, or with the same goals but possibly conflicting actions resulting from different perceptions of the world.

TODO

Part IV

Online Material

The theory exercises provided at the end of the chapters are designed to actively check the understanding of the material and provide routes for further developments. In addition, the reader is invited to advance his or her understanding of the material by practicing CPS proving in the KeYmaera X verification tool [16], which is an aXiomatic Tactical Theorem Prover for Hybrid Systems that implements differential dynamic logic. For technical reasons, the concrete syntax in KeYmaera X has a slightly different ASCII syntax, but, other than that, KeYmaera X follows the theory of differential dynamic logic as presented in this textbook.

The Web page for this book is at the following URL:

`http://www.lfcps.org/fcps/`

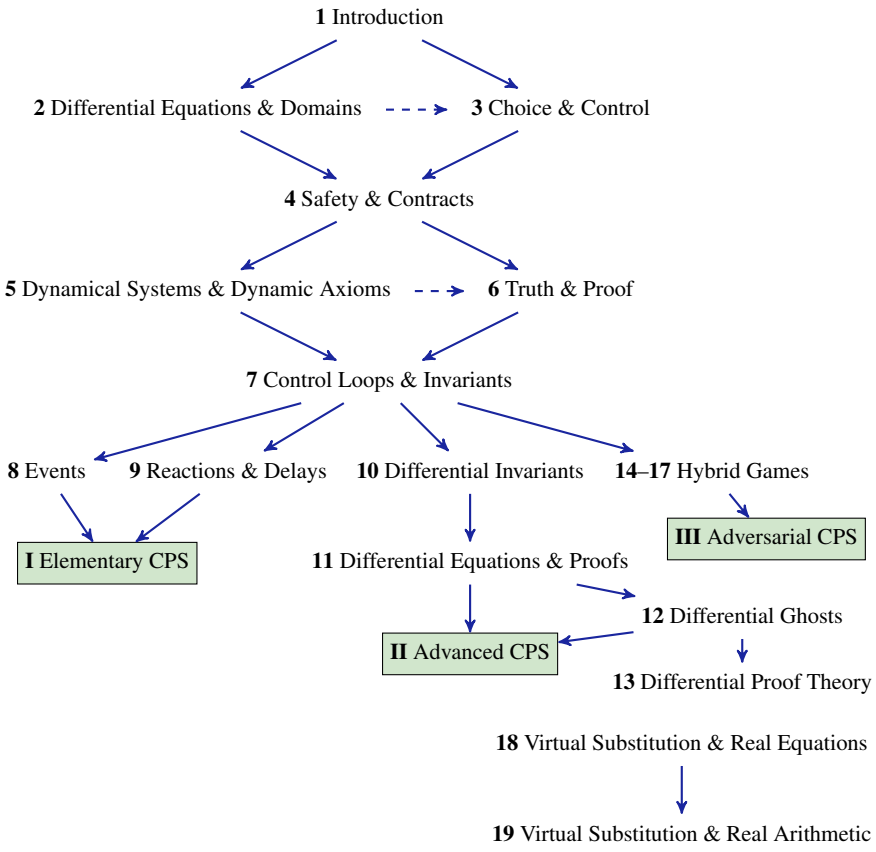


Fig. 1.3 Dependencies and suggested reading sequences of chapters

Suggested Reading Sequence

Even if the basic suggested reading order in this book is linear, this textbook can be read in many different ways. Except for most of the foundation developed in Part I, the other parts of this book are independent and can be read in any order. The dependencies among the topics in the chapters are shown in Fig. 1.3. Weak dependencies on some small number of concepts are indicated as dashed lines, so could be presented in a different order. The core of the textbook are the chapters that lead to elementary CPS Part I in Fig. 1.3, including either Chaps. 8 or 9 or both. An integral part for advanced CPS are Chaps. 10 and 11, along with an optional study of the topic of differential ghosts for advanced differential equations in Chap. 12.

Different reading sequences are possible for this textbook. The minimal core for an understanding of elementary cyber-physical systems always includes Chaps. 1–7 from Part I. A minimal course emphasizing an experience with system modeling covers the Chaps. 1–9 that lead to Part I on Elementary CPS in Fig. 1.3. For a minimal course emphasizing CPS reasoning Chaps. 1–7 would be followed by Chaps. 10–11 from Part II, possibly including Chap. 12 for advanced reasoning techniques. The other chapter sequences are independent. After Chaps. 1–9, any sequence of the other topics following the reader's interest are possible since the hybrid game chapters Chaps. 14–17 in Part III are independent from the virtual substitution topics in Part IV.

The textbook features an active development leading the reader through a critical and self-propelled development of the core aspects of cyber-physical systems. Especially at places marked as follows ...

Before you read on, see if you can find the answer for yourself.

... the reader is advised to work toward an answer before comparing it with the development pursued in the textbook. Of course, when comparing answers, the reader should keep in mind that there is more than one way of developing the material.

1.8 Summary

This chapter gave an informal overview of application domains for cyber-physical systems, which combine cyber capabilities such as communication, computation, and control with physical capabilities such as motion or chemical process control. It motivated the need for careful designs and comprehensive safety analyses, which will be developed in this book. Closely related is the mathematical notion of hybrid systems, which are dynamical systems that combine discrete dynamics with continuous dynamics. Despite the fact that both are different notions, since cyber-physical systems are based on the technical characteristics, while hybrid systems are a mathematical model, this textbook simplifies matters by using both notions interchangeably in Parts. I and II. More advanced models of cyber-physical systems

will be deferred to Part III after the hybrid systems model has been understood well in Part I and Part II.

This chapter set the stage for the multi-dynamical systems approach that this book follows. Multi-dynamical systems are characterized by multiple facets of dynamical systems whose compositionality in a logic of dynamical systems enables a separation of concerns for CPS. The multi-dynamical systems view directly benefits the presentation in this book as well, by making it possible to focus on one aspect at a time without losing the ability to combine the understanding attained for each aspect.

References

1. Althoff, M. & Dolan, J. Online Verification of Automated Road Vehicles Using Reachability Analysis. *Robotics, IEEE Transactions on* **PP,** 1–16 (2014).
2. Alur, R. *Formal verification of hybrid systems* in *EMSOFT* (eds Chakraborty, S., Jerraya, A., Baruah, S. K. & Fischmeister, S.) (ACM, 2011), 273–278.
3. Alur, R. *Principles of Cyber-Physical Systems* (MIT Press, 2015).
4. Alur, R., Henzinger, T., Lafferriere, G. & Pappas, G. J. Discrete Abstractions of Hybrid Systems. *Proc. IEEE* **88,** 971–984 (2000).
5. Alur, R. *et al.* The Algorithmic Analysis of Hybrid Systems. *Theor. Comput. Sci.* **138,** 3–34 (1995).
6. Branicky, M. S. *General Hybrid Dynamical Systems: Modeling, Analysis, and Control* in *Hybrid Systems* (eds Alur, R., Henzinger, T. A. & Sontag, E. D.) **1066** (Springer, 1995), 186–200.
7. Bresolin, D., Geretti, L., Muradore, R., Fiorini, P. & Villa, T. English. in *Coordination Control of Distributed Systems* (eds van Schuppen, J. H. & Villa, T.) 347–355 (Springer, 2015).
8. Bujorianu, L. M. *Stochastic Reachability Analysis of Hybrid Systems* (Springer, 2012).
9. (eds Chakraborty, S., Jerraya, A., Baruah, S. K. & Fischmeister, S.) *Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, part of the Seventh Embedded Systems Week, ESWeek 2011, Taipei, Taiwan, October 9-14, 2011* (ACM, 2011).
10. Clarke, E. M., Emerson, E. A. & Sifakis, J. Model checking: algorithmic verification and debugging. *Commun. ACM* **52,** 74–84 (2009).
11. Davoren, J. M. & Nerode, A. Logics for Hybrid Systems. *IEEE* **88,** 985–1010 (July 2000).
12. Deshpande, A., Göllü, A. & Varaiya, P. *SHIFT: A Formalism and a Programming Language for Dynamic Networks of Hybrid Automata* in *Hybrid Systems* (eds Antsaklis, P. J., Kohn, W., Nerode, A. & Sastry, S.) **1273** (Springer, 1996), 113–133.

13. Doyen, L., Frehse, G., Pappas, G. J. & Platzer, A. in *Handbook of Model Checking* (eds Clarke, E. M., Henzinger, T. A. & Veith, H.) chap. 30 (Springer, 2017).
14. Fourlas, G. K., Kyriakopoulos, K. J. & Vournas, C. D. Hybrid systems modeling for power systems. *Circuits and Systems Magazine, IEEE* **4,** 16–23 (quarter 2004).
15. Frege, G. *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens* (Verlag von Louis Nebert, 1879).
16. Fulton, N., Mitsch, S., Quesel, J.-D., Völp, M. & Platzer, A. *KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems* in *CADE* (eds Felty, A. & Middeldorp, A.) **9195** (Springer, 2015), 527–538. doi:10.1007/978-3-319-21401-6_36.
17. Gentzen, G. Untersuchungen über das logische Schließen. I. *Math. Zeit.* **39,** 176–210 (1935).
18. Grosu, R. *et al. From Cardiac Cells to Genetic Regulatory Networks* in *CAV* (eds Gopalakrishnan, G. & Qadeer, S.) **6806** (Springer, 2011), 396–411. doi:10.1007/978-3-642-22110-1_31.
19. Henzinger, T. A. & Sifakis, J. The Discipline of Embedded Systems Design. *Computer* **40,** 32–40 (Oct. 2007).
20. Henzinger, T. A. *The Theory of Hybrid Automata.* in *LICS* (IEEE Computer Society, Los Alamitos, 1996), 278–292. doi:10.1109/LICS.1996.561342.
21. Hilbert, D. Die Grundlagen der Mathematik. *Abhandlungen aus dem Seminar der Hamburgischen Universität* **6,** 65–85 (1928).
22. Hoare, C. A. R. An Axiomatic Basis for Computer Programming. *Commun. ACM* **12,** 576–580 (1969).
23. Jeannin, J. *et al.* A Formally Verified Hybrid System for Safe Advisories in the Next-generation Airborne Collision Avoidance System. *STTT*. doi:10.1007/s10009-016-0434-1 (2016).
24. Johnson, T. T. & Mitra, S. *Parametrized Verification of Distributed Cyber-Physical Systems: An Aircraft Landing Protocol Case Study* in *ICCPS* (IEEE, 2012), 161–170. doi:10.1109/ICCPS.2012.24.
25. Kim, B. *et al. Safety-assured development of the GPCA infusion pump software* in *EMSOFT* (eds Chakraborty, S., Jerraya, A., Baruah, S. K. & Fischmeister, S.) (ACM, 2011), 155–164. doi:10.1145/2038642.2038667.
26. Kouskoulas, Y., Renshaw, D. W., Platzer, A. & Kazanzides, P. *Certifying the Safe Design of a Virtual Fixture Control Algorithm for a Surgical Robot* in *HSCC* (eds Belta, C. & Ivancic, F.) (ACM, 2013), 263–272. doi:10.1145/2461328.2461369.
27. Larsen, K. G. *Verification and Performance Analysis for Embedded Systems* in *TASE 2009, Third IEEE International Symposium on Theoretical Aspects of Software Engineering, 29-31 July 2009, Tianjin, China* (eds Chin, W. & Qin, S.) (IEEE Computer Society, 2009), 3–4. doi:10.1109/TASE.2009.66.
28. Lee, E. A. & Seshia, S. A. *Introduction to Embedded Systems — A Cyber-Physical Systems Approach* (Lulu.com, 2013).

29. Lee, I. & Sokolsky, O. *Medical cyber physical systems* in *DAC* (ed Sapatnekar, S. S.) (ACM, 2010), 743–748.
30. Lee, I. *et al.* Challenges and Research Directions in Medical Cyber-Physical Systems. *Proc. IEEE* **100,** 75–90 (2012).
31. *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012* (IEEE, 2012).
32. Loos, S. M., Platzer, A. & Nistor, L. *Adaptive Cruise Control: Hybrid, Distributed, and Now Formally Verified* in *FM* (eds Butler, M. & Schulte, W.) **6664** (Springer, 2011), 42–56. doi:10.1007/978-3-642-21437-0_6.
33. *Handbook of Hybrid Systems Control: Theory, Tools, Applications* (eds Lunze, J. & Lamnabhi-Lagarrigue, F.) (Cambridge Univ. Press, 2009).
34. Maler, O. Control from computer science. *Annual Reviews in Control* **26,** 175–187 (2002).
35. Mitra, S., Wongpiromsarn, T. & Murray, R. M. Verifying Cyber-Physical Interactions in Safety-Critical Systems. *IEEE Security & Privacy* **11,** 28–37 (2013).
36. Mitsch, S., Ghorbal, K. & Platzer, A. *On Provably Safe Obstacle Avoidance for Autonomous Robotic Ground Vehicles* in *Robotics: Science and Systems* (eds Newman, P., Fox, D. & Hsu, D.) (2013).
37. Nerode, A. *Logic and Control* in *CiE* (eds Cooper, S. B., Löwe, B. & Sorbi, A.) **4497** (Springer, 2007), 585–597. doi:10.1007/978-3-540-73001-9_61.
38. Nerode, A. & Kohn, W. *Models for Hybrid Systems: Automata, Topologies, Controllability, Observability* in *Hybrid Systems* (eds Grossman, R. L., Nerode, A., Ravn, A. P. & Rischel, H.) **736** (Springer, 1992), 317–356.
39. NITRD CPS Senior Steering Group. *CPS Vision Statement* NITRD. 2012.
40. Pappas, G. J. *Wireless control networks: modeling, synthesis, robustness, security* in *Proceedings of the 14th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2011, Chicago, IL, USA, April 12-14, 2011* (eds Caccamo, M., Frazzoli, E. & Grosu, R.) (ACM, 2011), 1–2. doi:10.1145/1967701.1967703.
41. Plaku, E., Kavraki, L. E. & Vardi, M. Y. Hybrid systems: from verification to falsification by combining motion planning and discrete search. *Form. Methods Syst. Des.* **34,** 157–182 (2009).
42. Platzer, A. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reas.* **41,** 143–189 (2008).
43. Platzer, A. *Differential Dynamic Logics: Automated Theorem Proving for Hybrid Systems* Appeared with Springer. PhD thesis (Department of Computing Science, University of Oldenburg, Dec. 2008), 299.
44. Platzer, A. Differential-Algebraic Dynamic Logic for Differential-Algebraic Programs. *J. Log. Comput.* **20,** 309–352 (2010).
45. Platzer, A. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics* doi:10.1007/978-3-642-14509-4 (Springer, Heidelberg, 2010).

46. Platzer, A. *Stochastic Differential Dynamic Logic for Stochastic Hybrid Programs* in *CADE* (eds Bjørner, N. & Sofronie-Stokkermans, V.) **6803** (Springer, 2011), 431–445. doi:10.1007/978-3-642-22438-6_34.
47. Platzer, A. A Complete Axiomatization of Quantified Differential Dynamic Logic for Distributed Hybrid Systems. *Log. Meth. Comput. Sci.* **8.** Special issue for selected papers from CSL'10, 1–44 (2012).
48. Platzer, A. *Logics of Dynamical Systems* in *LICS* (IEEE, 2012), 13–24. doi:10.1109/LICS.2012.13.
49. Platzer, A. *The Complete Proof Theory of Hybrid Systems* in *LICS* (IEEE, 2012), 541–550. doi:10.1109/LICS.2012.64.
50. Platzer, A. *Teaching CPS Foundations With Contracts* in *CPS-Ed* (2013), 7–10.
51. Platzer, A. Differential Game Logic. *ACM Trans. Comput. Log.* **17,** 1:1–1:51 (2015).
52. Platzer, A. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reas.* doi:10.1007/s10817-016-9385-1 (2016).
53. Platzer, A. *Logic & Proofs for Cyber-Physical Systems* in *IJCAR* (eds Olivetti, N. & Tiwari, A.) **9706** (Springer, 2016), 15–21. doi:10.1007/978-3-319-40229-1_3.
54. Platzer, A. & Clarke, E. M. *The Image Computation Problem in Hybrid Systems Model Checking.* in *HSCC* (eds Bemporad, A., Bicchi, A. & Buttazzo, G. C.) **4416** (Springer, 2007), 473–486. doi:10.1007/978-3-540-71493-4_37.
55. Platzer, A. & Clarke, E. M. *Formal Verification of Curved Flight Collision Avoidance Maneuvers: A Case Study* in *FM* (eds Cavalcanti, A. & Dams, D.) **5850** (Springer, 2009), 547–562. doi:10.1007/978-3-642-05089-3_35.
56. Platzer, A. & Quesel, J.-D. *European Train Control System: A Case Study in Formal Verification* in *ICFEM* (eds Breitman, K. & Cavalcanti, A.) **5885** (Springer, 2009), 246–265. doi:10.1007/978-3-642-10373-5_13.
57. Pratt, V. R. *Semantical Considerations on Floyd-Hoare Logic* in *17th Annual Symposium on Foundations of Computer Science, 25-27 October 1976, Houston, Texas, USA* (IEEE, 1976), 109–121.
58. President's Council of Advisors on Science and Technology. *Leadership Under Challenge: Information Technology R&D in a Competitive World.* An Assessment of the Federal Networking and Information Technology R&D Program. Aug. 2007.
59. Scott, D. & Strachey, C. *Toward a mathematical semantics for computer languages?* tech. rep. PRG-6 (Oxford Programming Research Group, 1971).
60. Smullyan, R. M. *First-Order Logic* 176. doi:10.1007/978-3-642-86718-7 (Dover, 1968).
61. Tabuada, P. *Verification and Control of Hybrid Systems: A Symbolic Approach* (Springer, 2009).

62. Tiwari, A. Abstractions for hybrid systems. *Form. Methods Syst. Des.* **32,** 57–83 (2008).
63. Tiwari, A. *Logic in Software, Dynamical and Biological Systems* in *LICS* (IEEE Computer Society, 2011), 9–10. doi:10.1109/LICS.2011.20.
64. Tomlin, C., Pappas, G. J. & Sastry, S. Conflict resolution for air traffic management: a study in multi-agent hybrid systems. *IEEE T. Automat. Contr.* **43,** 509–521 (1998).
65. Wing, J. M. Computational thinking. *Commun. ACM* **49,** 33–35 (2006).
66. Wing, J. M. Five deep questions in computing. *Commun. ACM* **51,** 58–60 (2008).
67. Zuliani, P., Platzer, A. & Clarke, E. M. Bayesian Statistical Model Checking with Application to Simulink/Stateflow Verification. *Form. Methods Syst. Des.* **43,** 338–367 (2013).