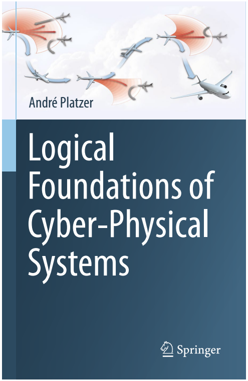
Logical Foundations of Cyber-Physical Systems

01: Cyber-Physical Systems: Overview



André Platzer

Carnegie Mellon University
Computer Science Department

Outline

Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs

2. Course: Logical Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Labs
   - CPS V&V Grand Prix
   - Assessment
   - Resources

3. Summary

Cyber-Physical Systems Analysis: Aircraft Example

Which control decisions are safe for aircraft collision avoidance?

Cyber-Physical Systems

CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.

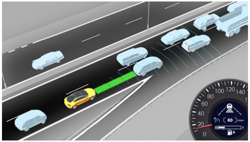
CPSs Promise Transformative Impact!

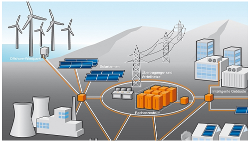
Prospects: Safe & Efficient

Driver assistance
Autonomous cars

Pilot decision support
Autopilots / UAVs

Train protection
Robots near humans




Prerequisite: CPSs need to be safe

How do we make sure CPSs make the world a better place?

Can you trust a computer to control physics?

Can you trust a computer to control physics?

1. Depends on how it has been programmed
2. And on what will happen if it malfunctions

Rationale

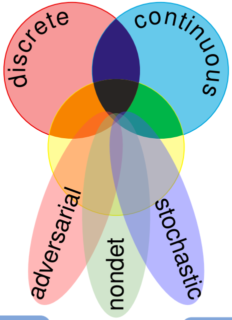
1. Safety guarantees require analytic foundations.
2. A common foundational core helps all application domains.
3. Foundations revolutionized digital computer science & our society.
4. Need even stronger foundations when software reaches out into our physical world.

CPSs deserve proofs as safety evidence!

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

Descriptive simplification

Tame Parts

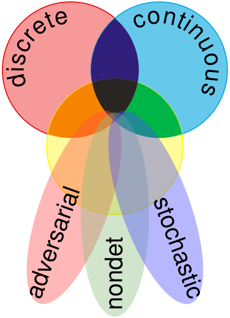
Exploiting compositionality tames CPS complexity.

Analytic simplification

CPSs are Multi-Dynamical Systems

hybrid systems

$\text{HS} = \text{discrete} + \text{ODE}$

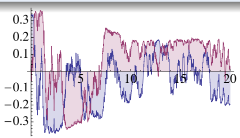


hybrid games

$\text{HG} = \text{HS} + \text{adversary}$

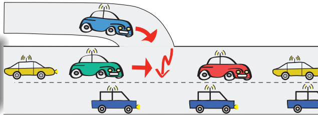
stochastic hybrid sys.

$\text{SHS} = \text{HS} + \text{stochastics}$



distributed hybrid sys.

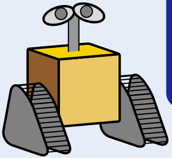
$\text{DHS} = \text{HS} + \text{distributed}$

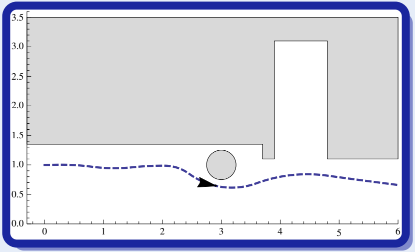


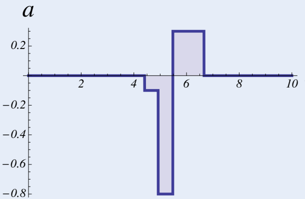
Challenge (CPS)

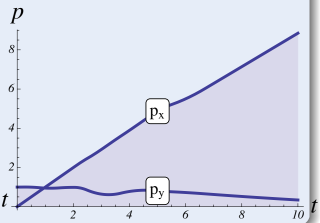
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)





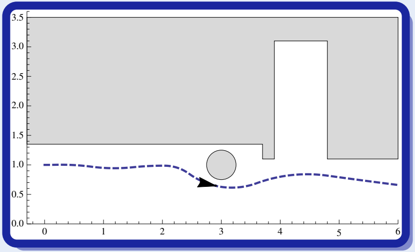


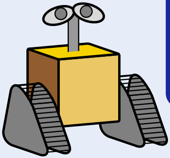


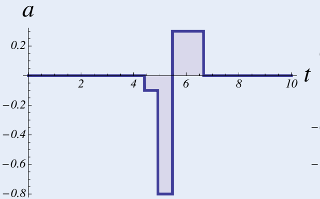
Challenge (CPS)

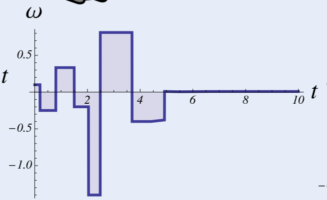
Fixed rule describing state evolution with both

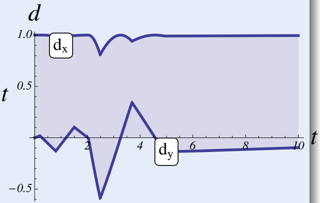
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)











Hybrid Systems Versus Cyber-Physical Systems

Mathematical model for complex physical systems:

Definition (Hybrid Systems)

Systems with interacting discrete and continuous dynamics

Technical characteristics:

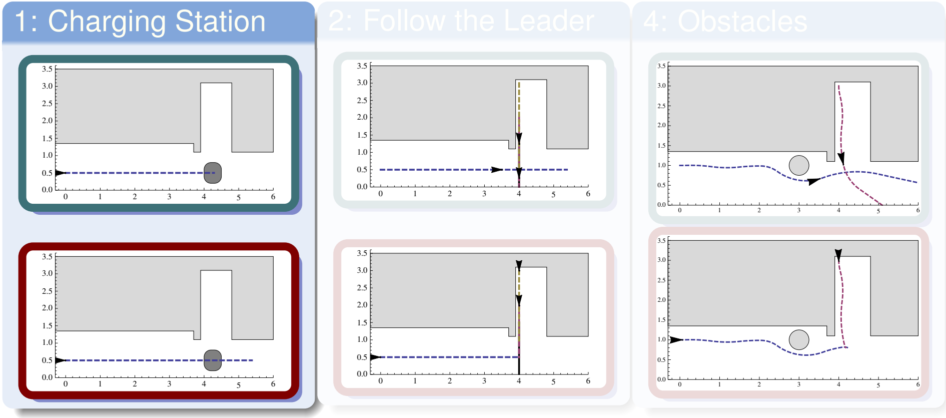
Definition (Cyber-Physical Systems)

(Distributed networks of) computerized control for physical system
Communication, computation, and control for physics

What CPSs are around us?

What CPSs will be around us in the future?

Which CPSs do we trust with our lives?



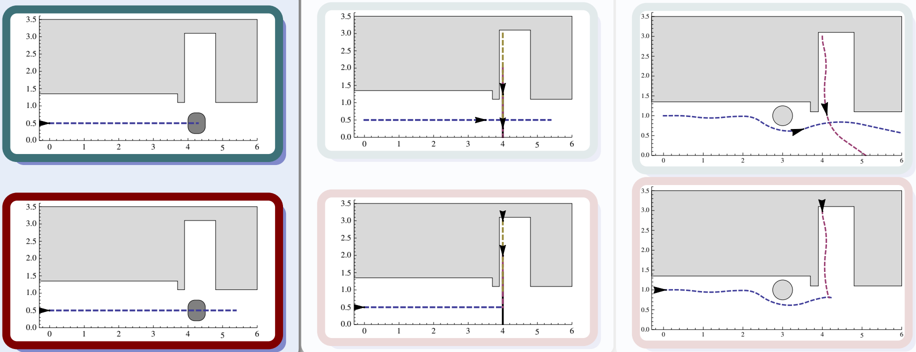
- ✓ Design, model
- ✓ Verify

LFCPS Labs

1: Charging Station

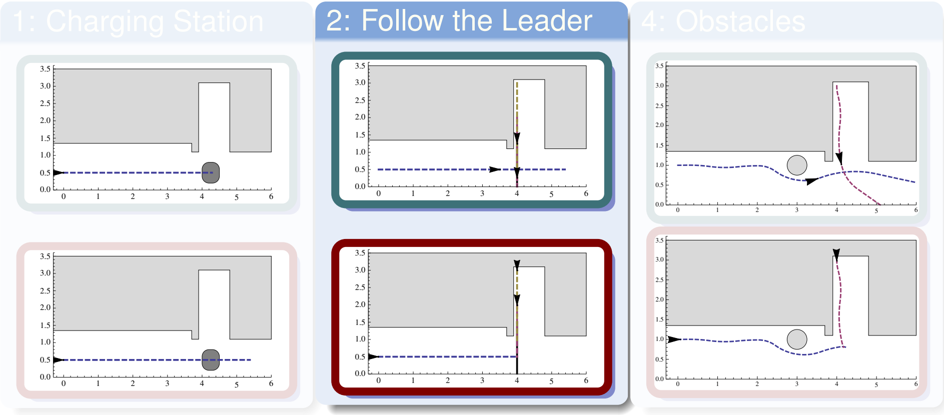
2: Follow the Leader

4: Obstacles



- ✓ Design, model
- ✓ Verify

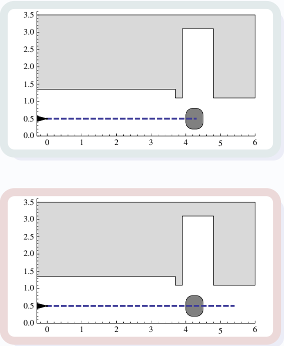
LFCPS Labs



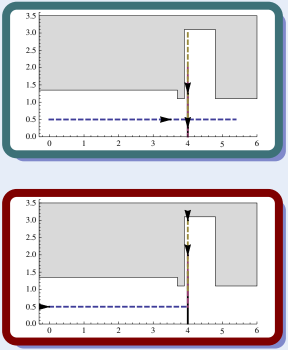
- ✓ Design, model
- ✓ Verify

LFCPS Labs

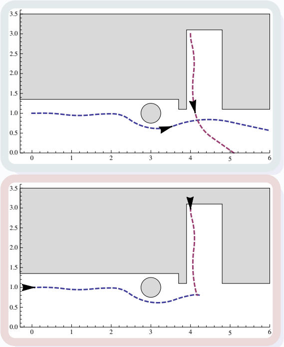
1: Charging Station



2: Follow the Leader



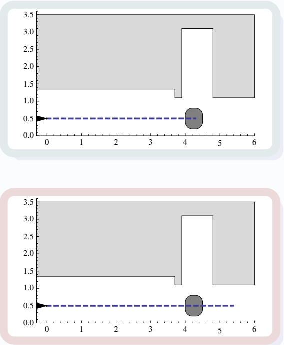
4: Obstacles



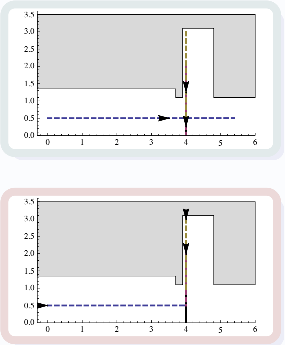
- ✓ Design, model
- ✓ Verify

LFCPS Labs

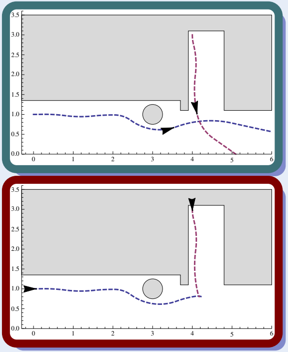
1: Charging Station



2: Follow the Leader



4: Obstacles

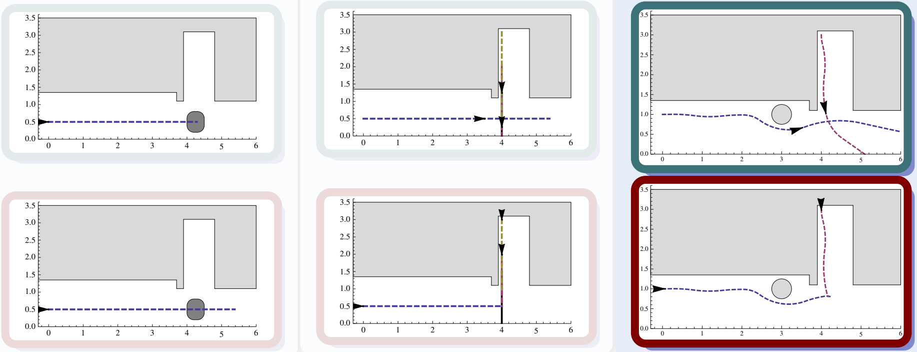


- ✓ Design, model
- ✓ Verify

1: Charging Station

2: Follow the Leader

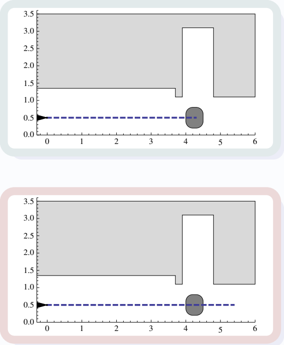
4: Obstacles



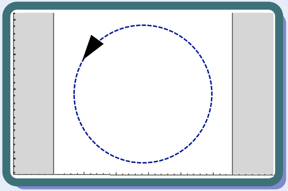
- ✓ Design, model
- ✓ Verify

LFCPS Labs

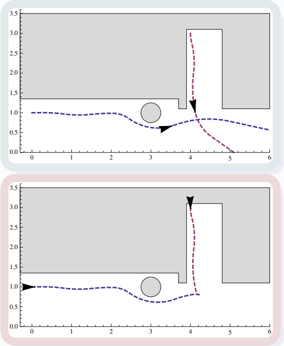
1: Charging Station



3: Racetrack



4: Obstacles

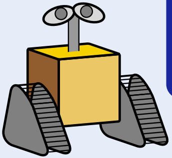


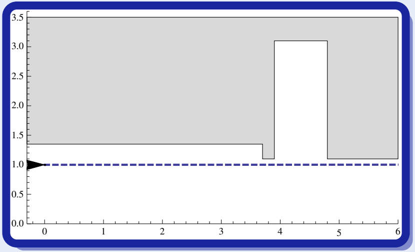
- ✓ Design, model
- ✓ Verify

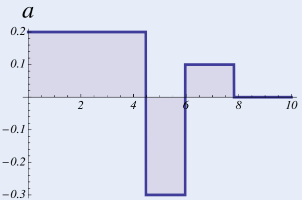
Challenge (Hybrid Systems)

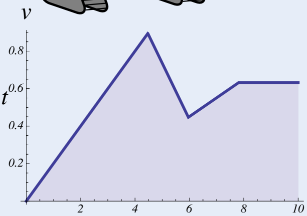
Design & verify controller for a robot avoiding obstacles

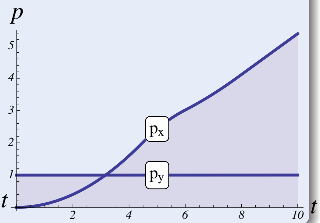
- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)







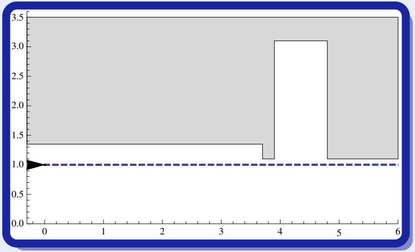


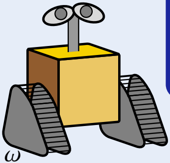


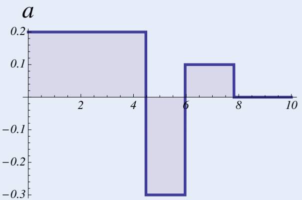
Challenge (Hybrid Systems)

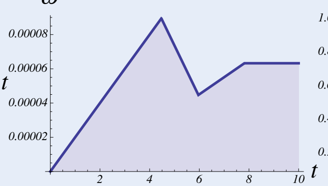
Design & verify controller for a robot avoiding obstacles

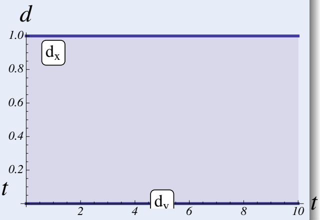
- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)







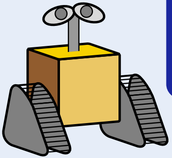


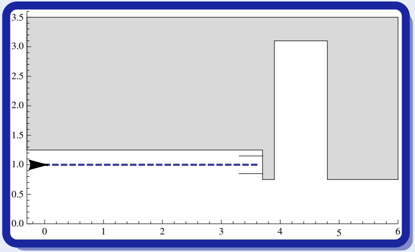


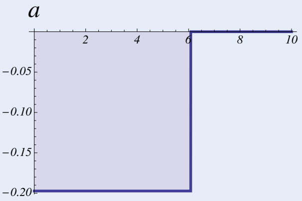
Challenge (Hybrid Systems)

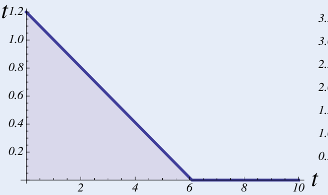
Design & verify controller for a robot avoiding obstacles

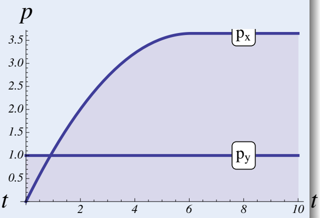
- Accelerate / brake / stop (discrete dynamics)
- 1D motion (continuous dynamics)









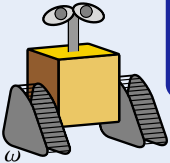


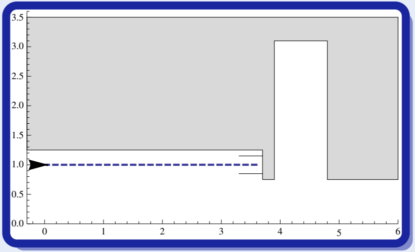
CPS Analysis & Design: Robot Lab

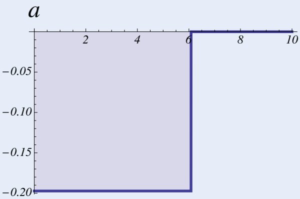
Challenge (Hybrid Systems)

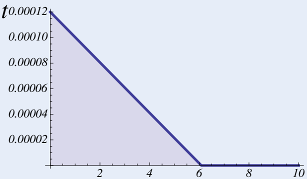
Design & verify controller for a robot avoiding obstacles

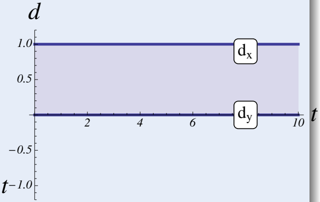
- Accelerate / brake / stop (discrete dynamics)
- 1D motion (continuous dynamics)







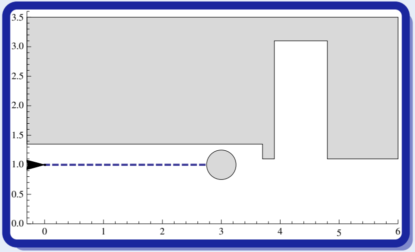


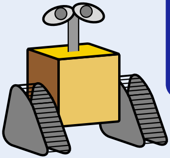


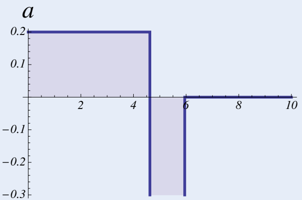
Challenge (Hybrid Systems)

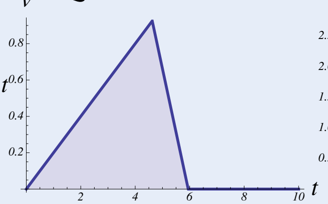
Design & verify controller for a robot avoiding obstacles

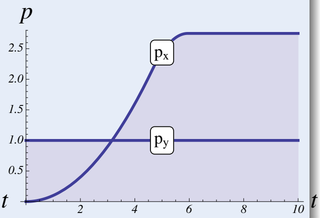
- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)







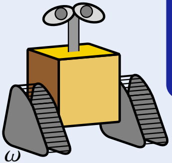


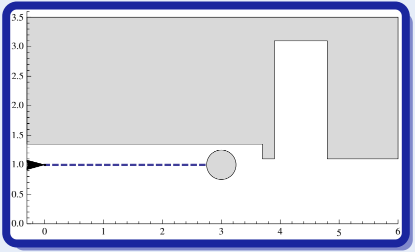


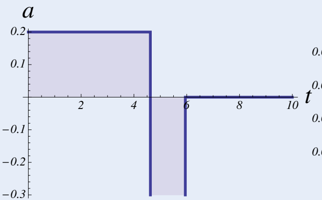
Challenge (Hybrid Systems)

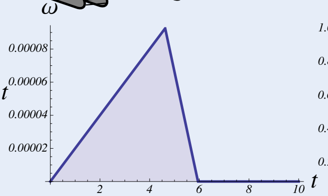
Design & verify controller for a robot avoiding obstacles

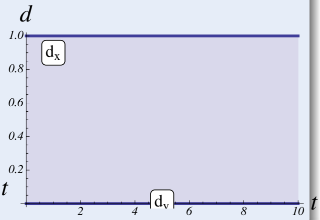
- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)







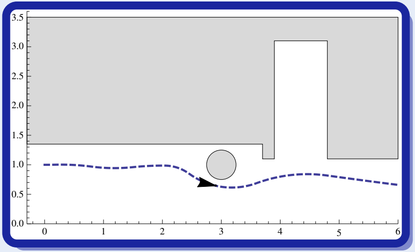


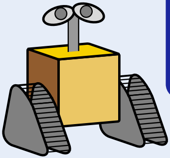


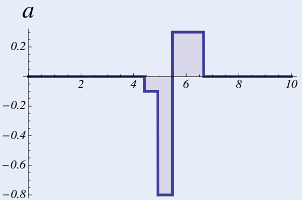
Challenge (Hybrid Systems)

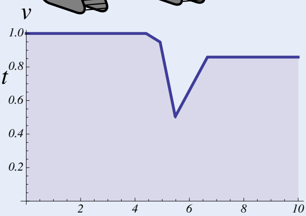
Design & verify controller for a robot avoiding obstacles

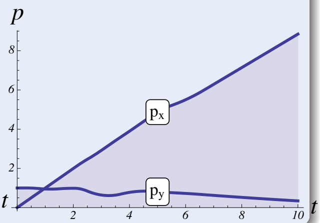
- Accel / brake / steer (discrete dynamics)
- 2D motion (continuous dynamics)







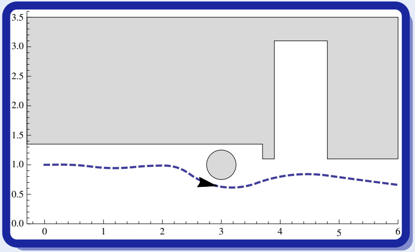


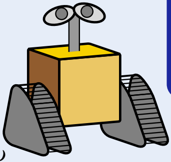


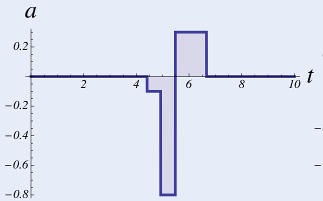
Challenge (Hybrid Systems)

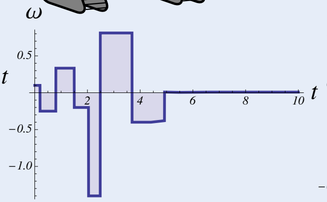
Design & verify controller for a robot avoiding obstacles

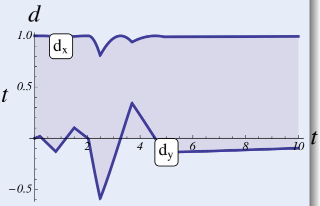
- Accel / brake / steer (discrete dynamics)
- 2D motion (continuous dynamics)









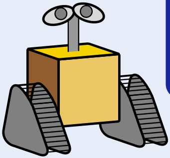


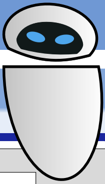
CPS Analysis & Design: Robot Lab

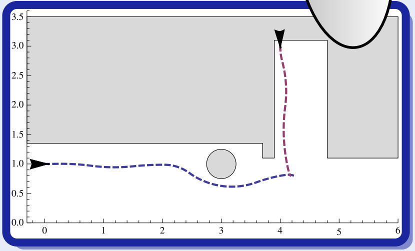
Challenge (Hybrid Systems)

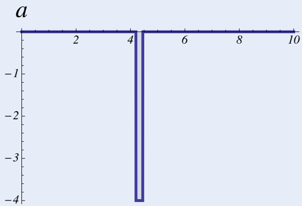
Design & verify controller for a robot avoiding obstacles

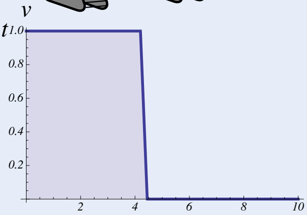
- Dynamic obstacles (other agents)
- Avoid collisions (define safety)

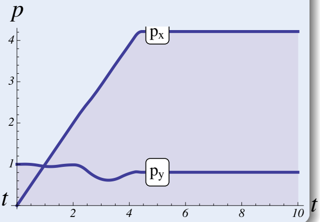


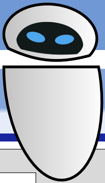








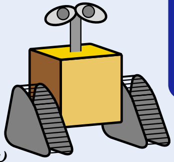


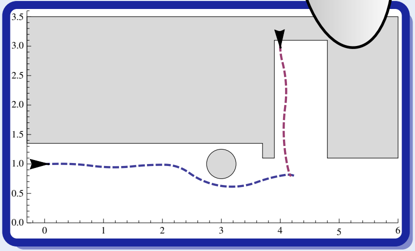


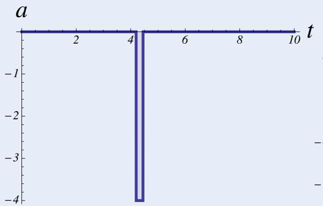
Challenge (Hybrid Systems)

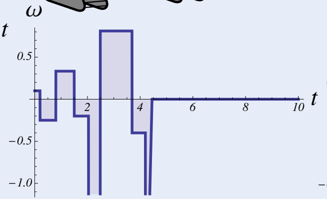
Design & verify controller for a robot avoiding obstacles

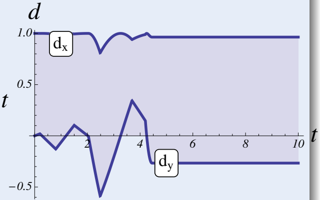
- Dynamic obstacles (other agents)
- Avoid collisions (define safety)

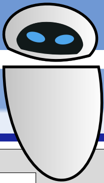








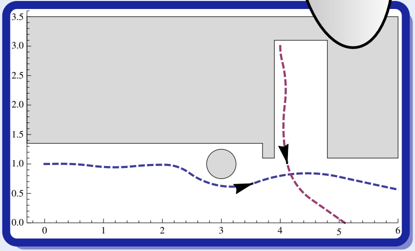


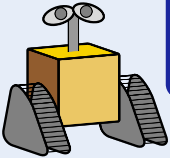


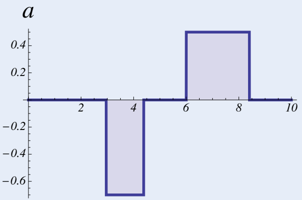
Challenge (Hybrid Systems)

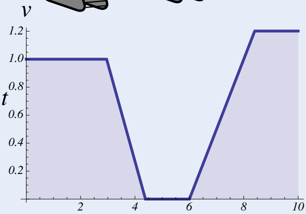
Design & verify controller for a robot avoiding obstacles

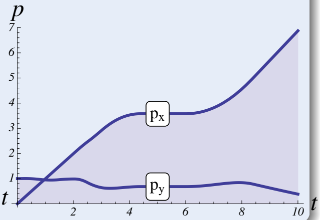
- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)

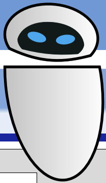








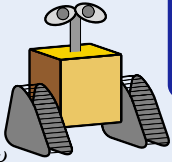


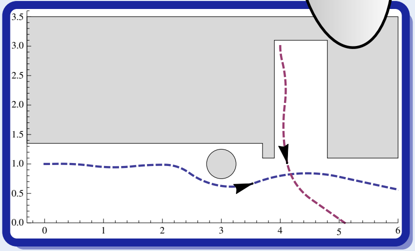


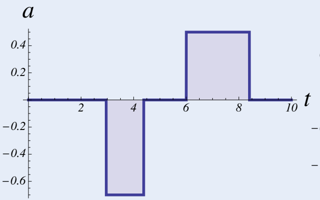
Challenge (Hybrid Systems)

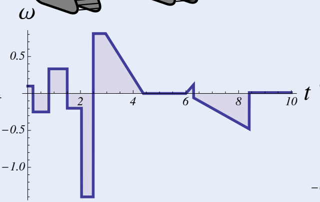
Design & verify controller for a robot avoiding obstacles

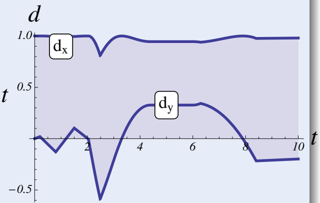
- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)



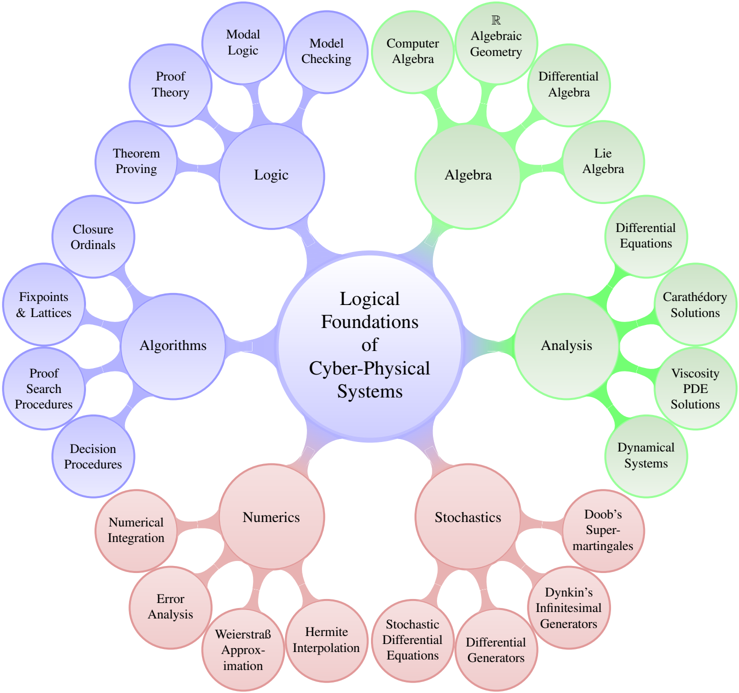








Outline


Logical Foundations of Cyber-Physical Systems
Logic
Modal Logic
Model Checking
Proof Theory
Theorem Proving
Algebra
Computer Algebra
ℝ Algebraic Geometry
Differential Algebra
Lie Algebra
Analysis
Differential Equations
Carathéodory Solutions
Viscosity PDE Solutions
Dynamical Systems
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search Procedures
Decision Procedures
Numerics
Numerical Integration
Error Analysis
Weierstraß Approx-imation
Hermite Interpolation
Stochastics
Doob's Super-martingales
Dynkin's Infinitesimal Generators
Differential Generators
Stochastic Differential Equations

How to Teach Cyber-Physical Systems?

Onion Model

1. Going outside in
2. Unpeel layer by layer
3. Progress when all prereqs are covered
4. First study CS $\wedge$ math $\wedge$ engineering
5. Talk about CPS in the big finale

Scenic Tour Model

1. Start at the heart: CPS
2. Go on scenic expeditions into various directions
3. Explore the world around us as we find the need
4. Stay on CPS the whole time
5. Leverage CPS as the guiding motivation for understanding more about connected areas

Logical scrutiny, formalization, and correctness proofs are critical for CPS!

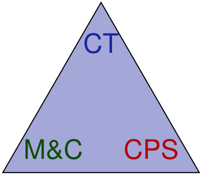
1. CPSs are so easy to get wrong.
2. Retrofitting CPSs for safety is not possible.
3. These logical aspects are an integral part of CPS design.
4. Critical to your understanding of the intricate complexities of CPS.
5. Tame complexity by a simple programming language for core aspects.

About Logical Foundations of Cyber-Physical Systems

- Foundations!
- Modeling & Control
  1. Understand the core principles behind CPSs.
  2. Develop models and controls.
  3. Identify the relevant dynamical aspects.
- Computational Thinking
  1. Identify safety specifications and critical properties of CPSs.
  2. Understand abstraction in system design.
  3. Express pre- and postconditions for CPS models.
  4. Use design-by-invariant.
  5. Reason rigorously about CPS models.
  6. Verify CPS models of appropriate scale.
- CPS Skills
  1. Understand the semantics of a CPS model.
  2. Develop an intuition for operational effects.
  3. Identify control constraints.
  4. Understand opportunities and challenges in CPS and verification.
- Byproducts
  1. Well-motivated exposure to numerous math and science areas in action.

Learning Objectives

identify safety specifications for CPS
rigorous reasoning about CPS
understand abstraction & architectures
programming languages for CPS
verify CPS models at scale



cyber+physics models
core principles of CPS
relate discrete+continuous

semantics of CPS models
operational effects
identify control constraints
opportunities and challenges

Textbook and Course Outline

I Part: Elementary Cyber-Physical Systems

2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays

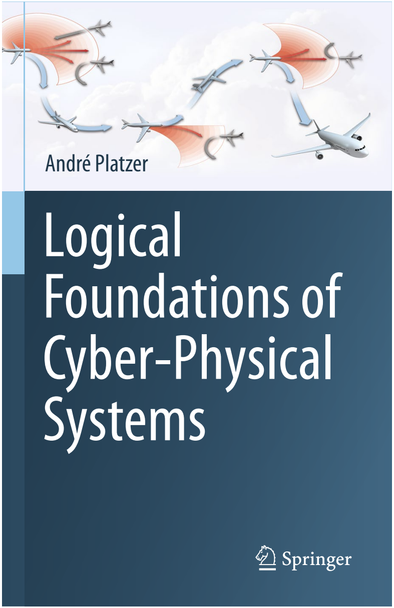
II Part: Differential Equations Analysis

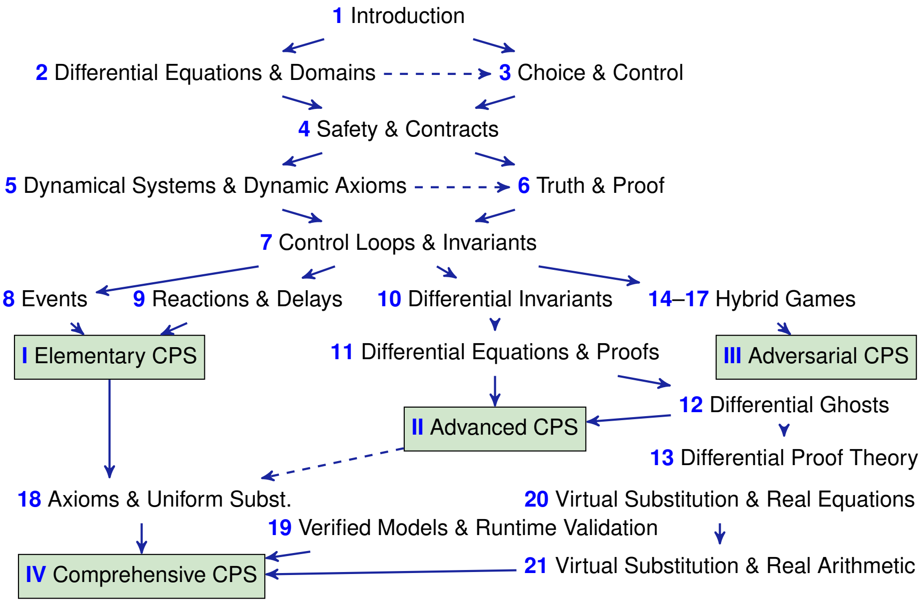
10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory

III Part: Adversarial Cyber-Physical Systems

-17. Hybrid Systems & Hybrid Games

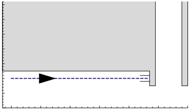
IV Part: Comprehensive CPS Correctness

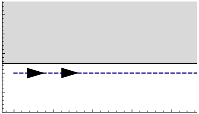


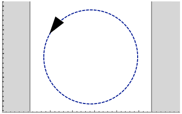

1 Introduction
2 Differential Equations & Domains
3 Choice & Control
4 Safety & Contracts
5 Dynamical Systems & Dynamic Axioms
6 Truth & Proof
7 Control Loops & Invariants
8 Events
9 Reactions & Delays
10 Differential Invariants
14–17 Hybrid Games
I Elementary CPS
11 Differential Equations & Proofs
III Adversarial CPS
12 Differential Ghosts
II Advanced CPS
13 Differential Proof Theory
18 Axioms & Uniform Subst.
20 Virtual Substitution & Real Equations
19 Verified Models & Runtime Validation
IV Comprehensive CPS
21 Virtual Substitution & Real Arithmetic

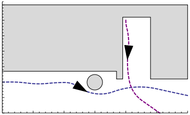
Robot Model Labs

1. Robot on Rails
   a. Autobots, Roll Out
   b. Charging Station
2. Robot on Highways: Follow the Leader
   a. with event-triggered control
   b. with time-triggered control
3. Robot on Racetracks
   a. stay on the circular racetrack
   b. slow down to avoid collisions
4. Robot in a Plane
   a. with obstacle avoidance
   b. Robot vs. Roguebot: don't collide with moving obstacles
5. Robot in Star-lab: self-defined final project
6. Final project presented at CPS V&V Grand Prix









▸ CPS V&V Grand Prix

CPS V&V Grand Prix: Course Competition

Assessment

- TODO: Read Course Policies ▸ Syllabus
- ≈22% Theory homework — Due at midnight
- ≈51% Labs, including ≈22% final project
  1. Betabot in first week — Due at **beginning** of lecture
  2. Veribot in second week — Due at midnight
- Whitepaper — For final project
- Proposal — For final project
- Term paper — Due with final project
- CPS V&V Grand Prix presentation — Tue Dec 11
- ≈11% Midterm — In class
- ≈11% Final — In class
- ≈5% Participation in class and in online comments
- Partner allowed for labs only and only starting in lab 2
- TODO: Theory 0 prep homework — Due this week

Resources

Prerequisites

15-122 Principles of Imperative Computation — if-then-else

21-120 Differential and Integral Calculus — x'

(21-241 Matrix algebra **or**

15-251 Great Theoretical Ideas in Computer Science **or** — Math proofs

18-202 Mathematical Foundations of Electrical Engineering)

Substitutes: 21-242 Matrix theory **or** 21-341 Linear algebra I for 21-241

- You are expected to follow extra material in the textbook.
- Further reading and background material on the course web page
- Check course web page periodically

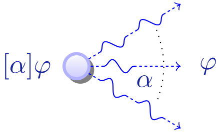
  http://lfcps.org/course/lfcps.html
- KeYmaera X: aXiomatic Tactical Theorem Prover for Hybrid Systems
- Piazza, Autolab, Ask!

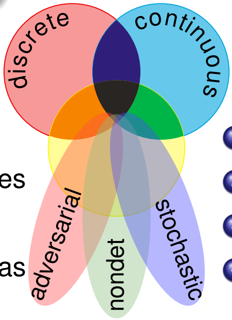
Outline

Logical foundations make a big difference for CPS, and vice versa

differential dynamic logic

$\mathsf{dL} = \mathsf{DL} + \mathsf{HP}$





- Strong analytic foundations
- Practical reasoning advances
- Significant applications
- Catalyze many science areas

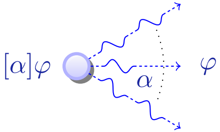
1. Multi-dynamical systems
2. Combine simple dynamics
3. Tame complexity
4. V&V cool challenges

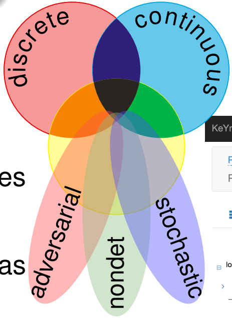
Numerous wonders remain to be discovered

Logical foundations make a big difference for CPS, and vice versa

differential dynamic logic

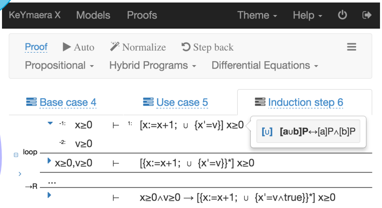
$$\text{dL} = \text{DL} + \text{HP}$$





- Strong analytic foundations
- Practical reasoning advances
- Significant applications
- Catalyze many science areas

KeYmaera X



Numerous wonders remain to be discovered

André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Switzerland, 2018.
URL: http://www.springer.com/978-3-319-63587-3,
doi:10.1007/978-3-319-63588-0.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.

André Platzer.
Logics of dynamical systems.
In *LICS*, pages 13–24, Los Alamitos, 2012. IEEE.
doi:10.1109/LICS.2012.13.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.
doi:10.1007/s10817-008-9103-8.

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.
J. Autom. Reas., 59(2):219–265, 2017.
doi:10.1007/s10817-016-9385-1.

André Platzer.
Logic & proofs for cyber-physical systems.
In Nicola Olivetti and Ashish Tiwari, editors, *IJCAR*, volume 9706 of *LNCS*, pages 15–21, Berlin, 2016. Springer.
doi:10.1007/978-3-319-40229-1_3.

André Platzer.
Differential game logic.
ACM Trans. Comput. Log., 17(1):1:1–1:51, 2015.
doi:10.1145/2817824.

André Platzer.
Differential hybrid games.
ACM Trans. Comput. Log., 18(3):19:1–19:44, 2017.
doi:10.1145/3091123.