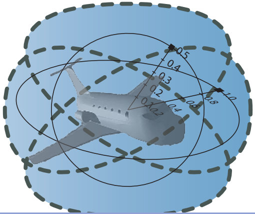
15-424/15-624: Foundations of Cyber-Physical Systems

01: Overview

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA

http://lfcps.org/course/fcps17.html
http://www.cs.cmu.edu/~aplatzer/course/fcps17.html



Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs
2. 15-424/624/824: Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Assessment
   - Labs
   - CPS V&V Grand Prix
   - Resources
3. Summary

Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs
2. 15-424/624/824: Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Assessment
   - Labs
   - CPS V&V Grand Prix
   - 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.

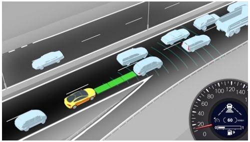
CPSs Promise Transformative Impact!

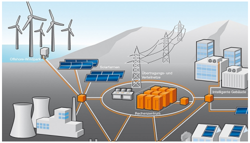
Prospects: Safe & Efficient

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

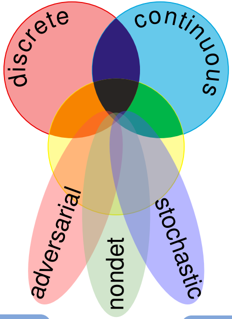
1. Safety guarantees require analytic foundations.
2. A common foundational core helps all application domains.
3. Foundations revolutionized digital computer science & our society.
4. Need even stronger foundations when software reaches out into our physical world.

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

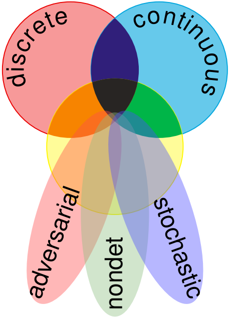
Exploiting compositionality tames CPS complexity.

Analytic simplification

CPSs are Multi-Dynamical Systems

hybrid systems

HS = discrete + ODE

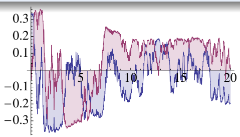


hybrid games

HG = HS + adversary

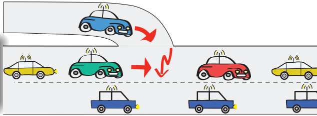
stochastic hybrid sys.

SHS = HS + stochastics



distributed hybrid sys.

DHS = HS + distributed

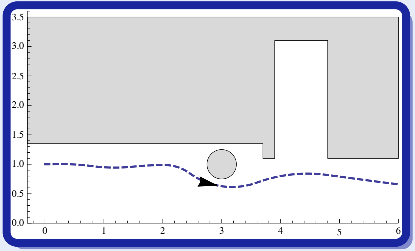


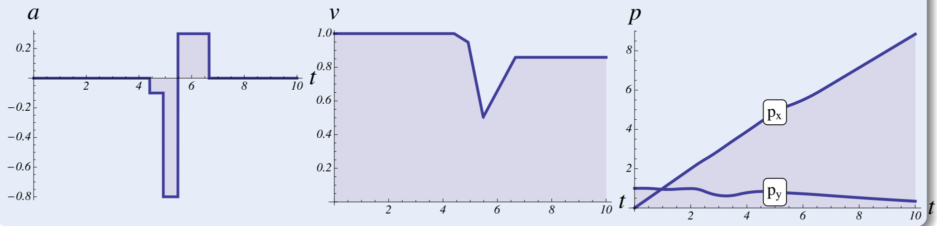
CPS Analysis

Challenge (CPS)

Fixed rule describing state evolution with both

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



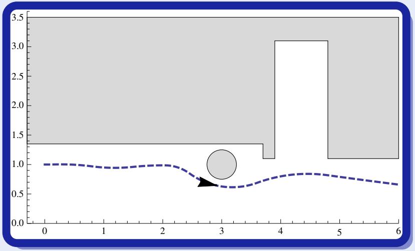


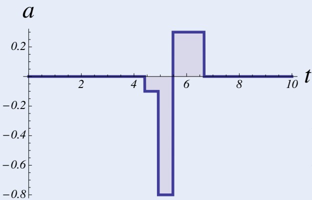
CPS Analysis

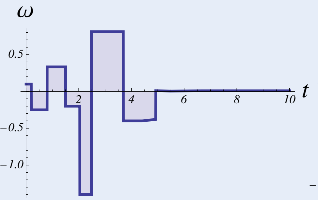
Challenge (CPS)

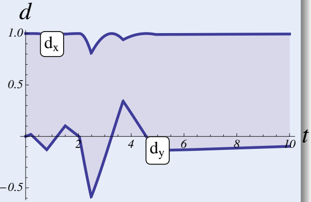
Fixed rule describing state evolution with both

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









Hybrid Systems & 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)

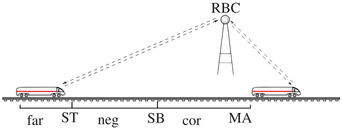
(Distributed network of) computerized control for physical system
Computation, communication and control for physics

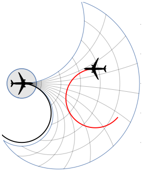
What CPS are around us?

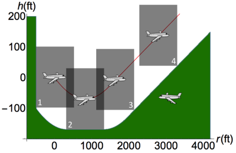
What CPS will be around us in the future?

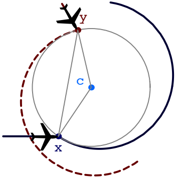
Which CPS do we trust with our lives?

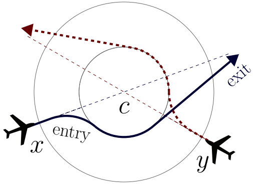
Verified CPS Applications

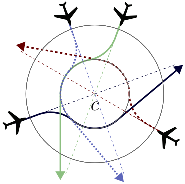


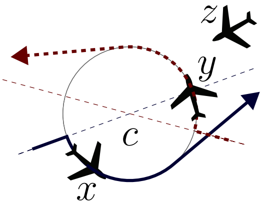


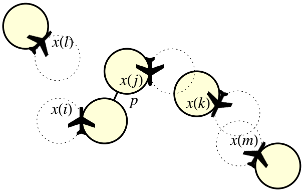


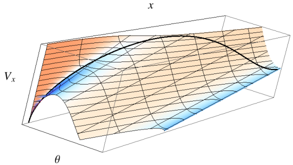






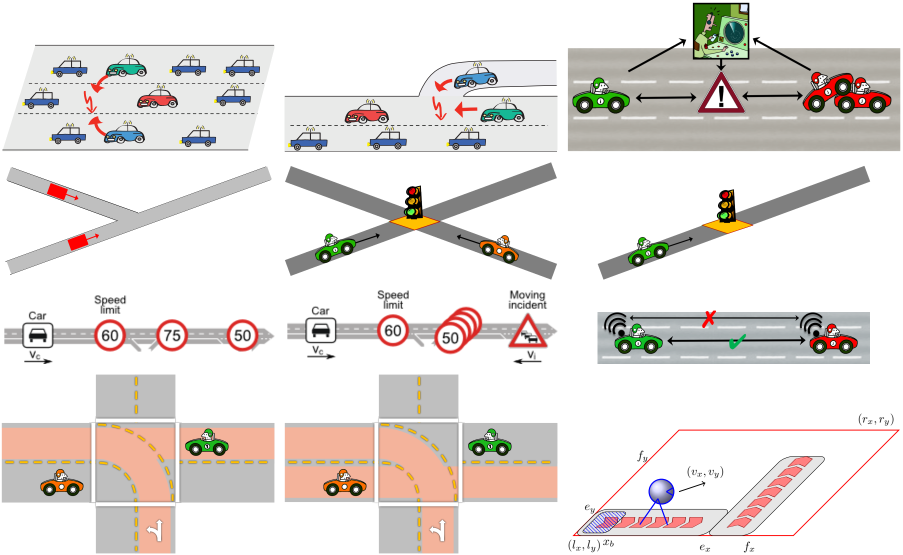






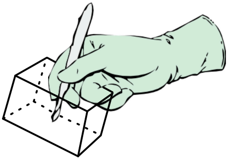
FEM'09,JAIS'14,TACAS'15,EMSOFT'15,CAV'08,FM'09,HSCC'11,HSCC'13,TACAS'14

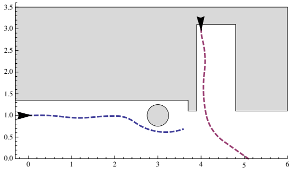
Verified CPS Applications

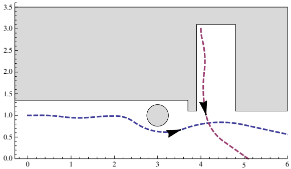


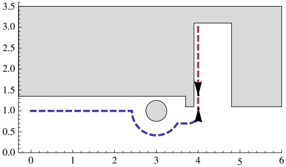
FM'11,LMCS'12,ICCPS'12,ITSC'11,ITSC'13,IJCAR'12

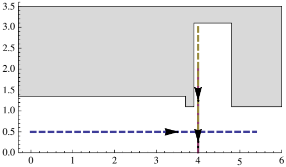
Verified CPS Applications

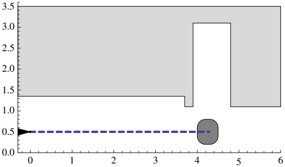


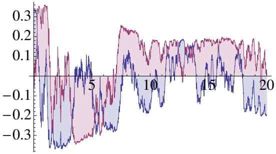


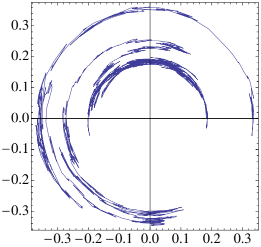


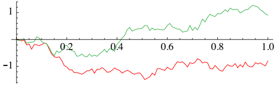






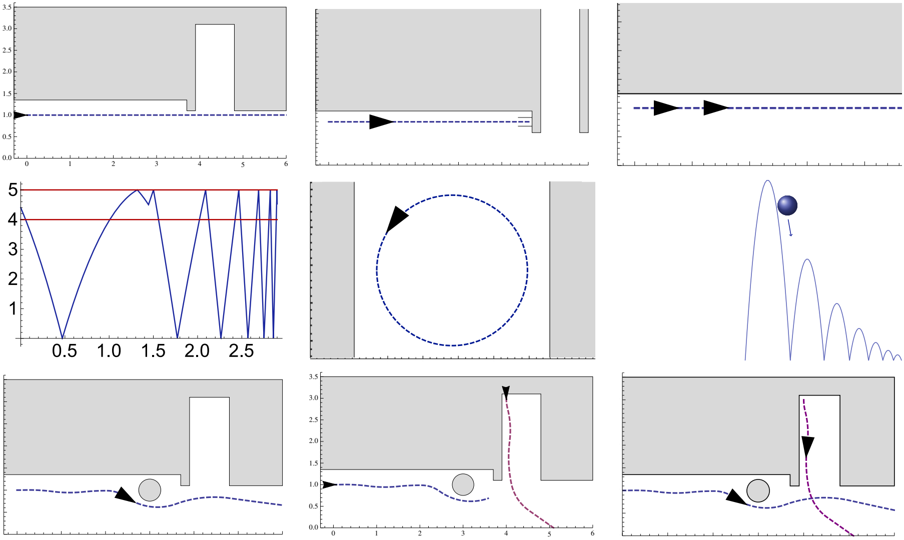






HSCC'13,RSS'13,CADE'12

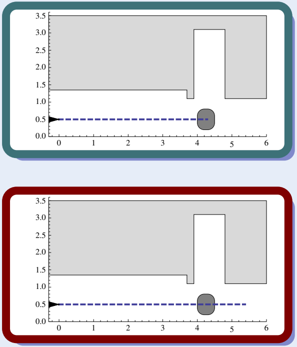
Verified CPS Applications



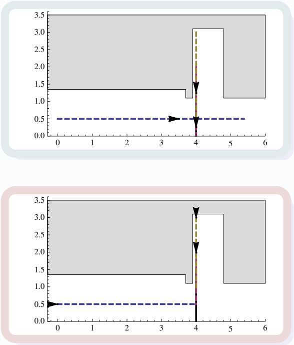
15-424/624/824 *Foundations of Cyber-Physical Systems* students

FCPS Labs

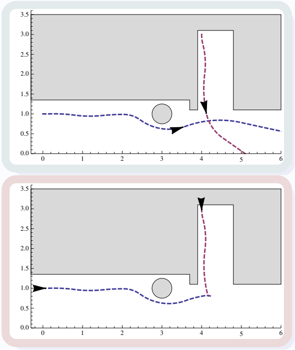
1: Charging Station



2: Follow the Leader



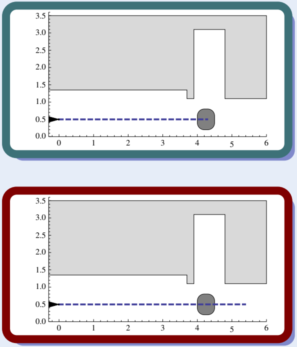
4: Obstacles



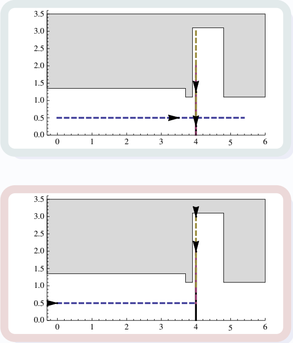
- ✓ Design, model
- ✓ Verify with KeYmaera X

FCPS Labs

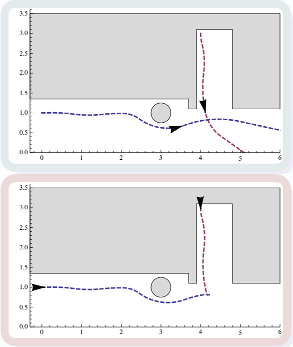
1: Charging Station



2: Follow the Leader



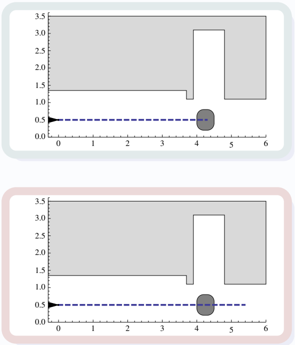
4: Obstacles



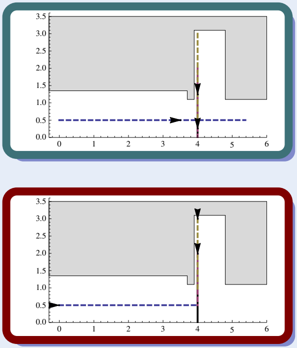
- ✓ Design, model
- ✓ Verify with KeYmaera X

FCPS Labs

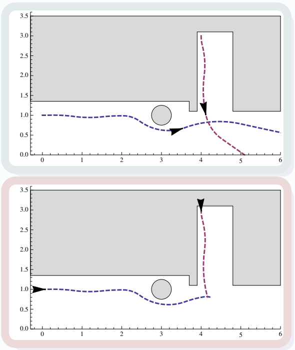
1: Charging Station



2: Follow the Leader



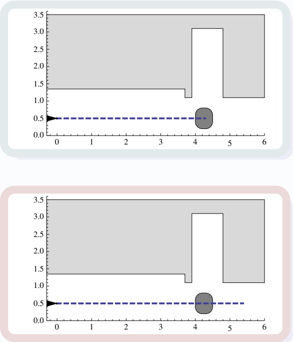
4: Obstacles



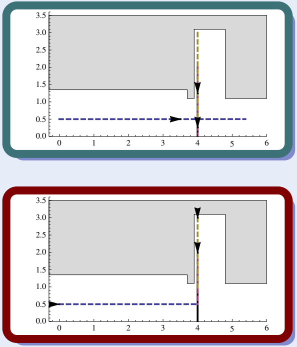
- ✓ Design, model
- ✓ Verify with KeYmaera X

FCPS Labs

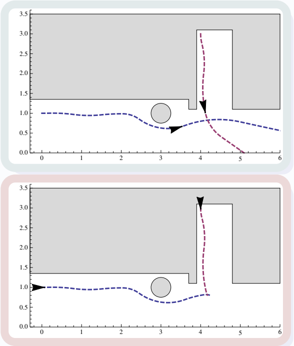
1: Charging Station



2: Follow the Leader



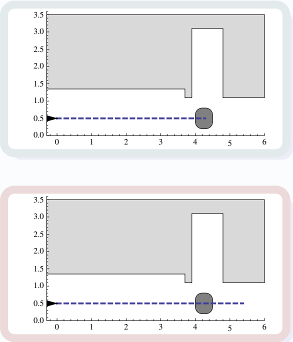
4: Obstacles



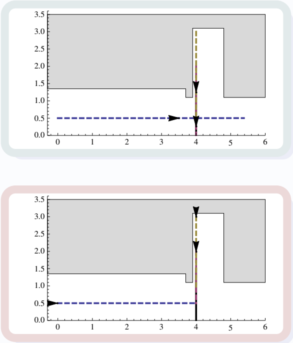
- ✓ Design, model
- ✓ Verify with KeYmaera X

FCPS Labs

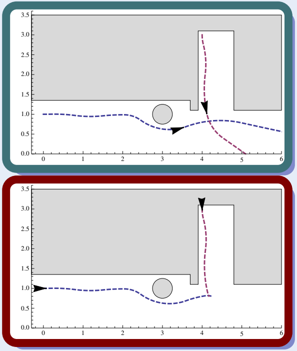
1: Charging Station



2: Follow the Leader



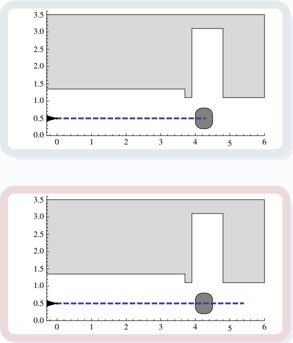
4: Obstacles



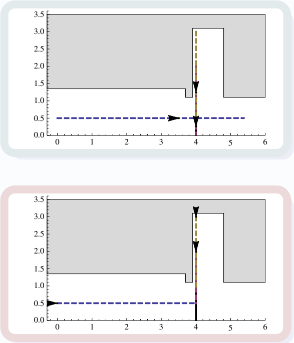
- ✓ Design, model
- ✓ Verify with KeYmaera X

FCPS Labs

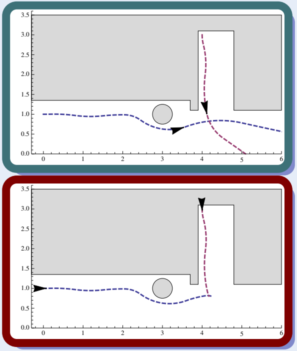
1: Charging Station



2: Follow the Leader



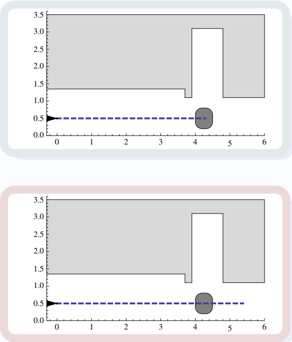
4: Obstacles



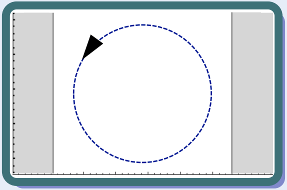
- ✓ Design, model
- ✓ Verify with KeYmaera X

FCPS Labs

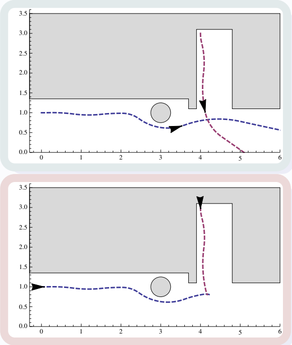
1: Charging Station



3: Racetrack



4: Obstacles



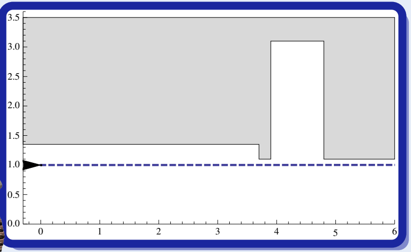
- ✓ Design, model
- ✓ Verify with KeYmaera X

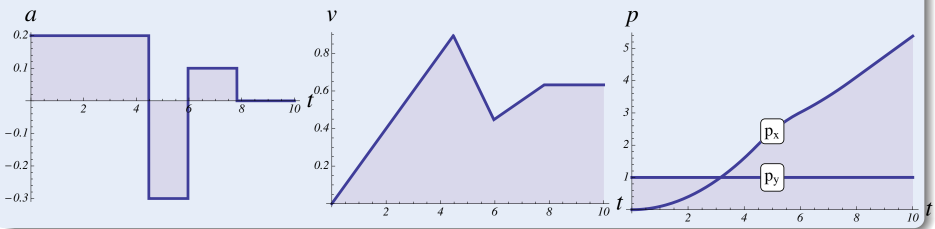
CPS Analysis & Design: Robot Lab

Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

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



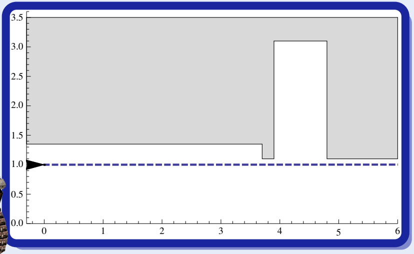


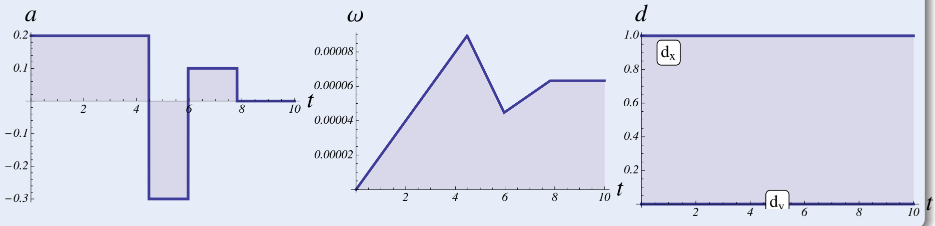
CPS Analysis & Design: Robot Lab

Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

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



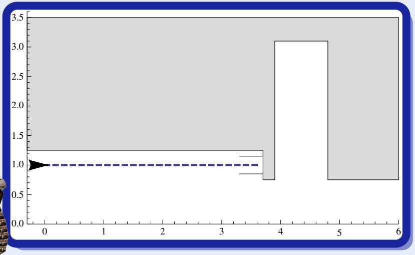


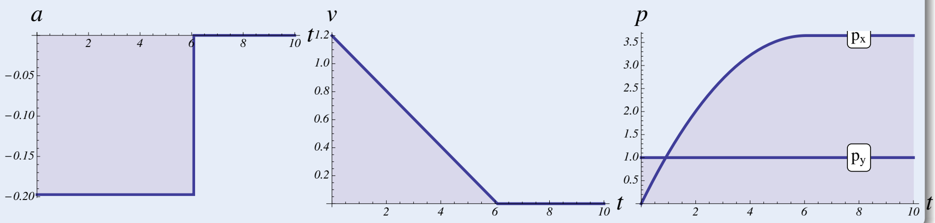
CPS Analysis & Design: Robot Lab

Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

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



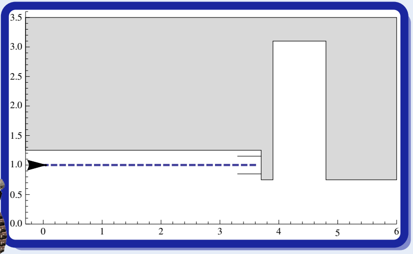


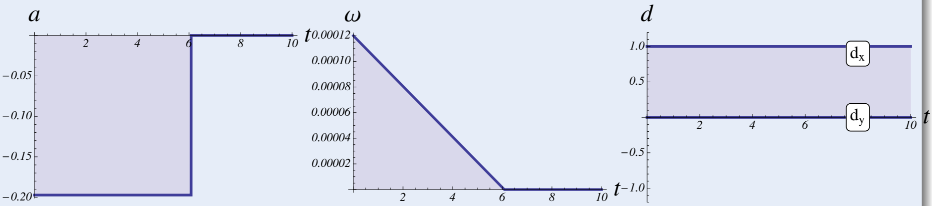
CPS Analysis & Design: Robot Lab

Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

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



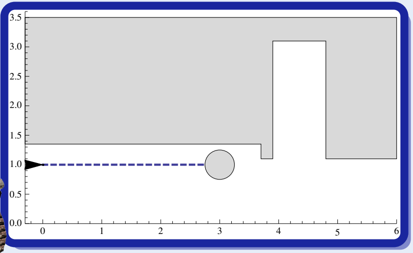


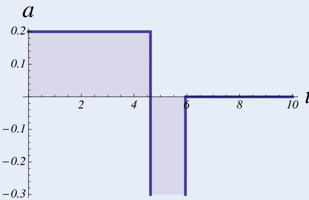
CPS Analysis & Design: Robot Lab

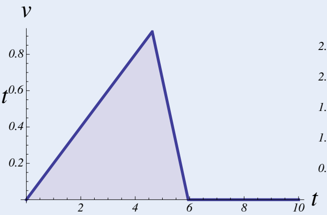
Challenge (Hybrid Systems)

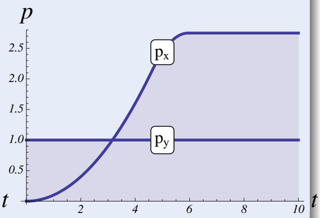
Design & verify controller for a robot avoiding obstacles

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







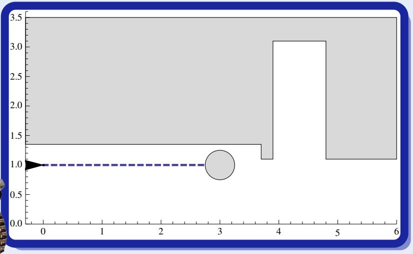


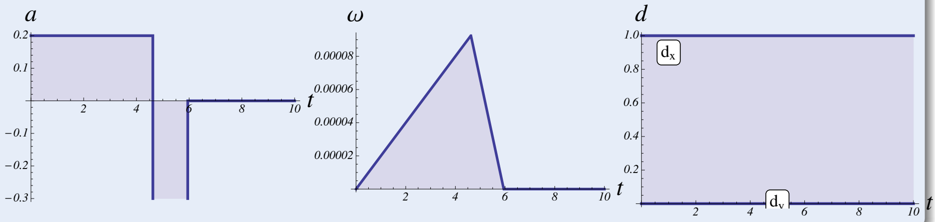
CPS Analysis & Design: Robot Lab

Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

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



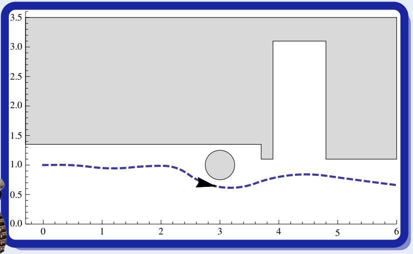


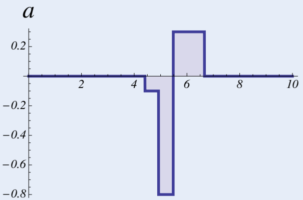
CPS Analysis & Design: Robot Lab

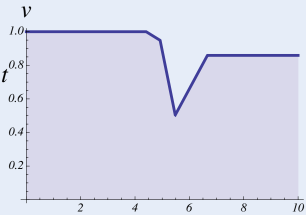
Challenge (Hybrid Systems)

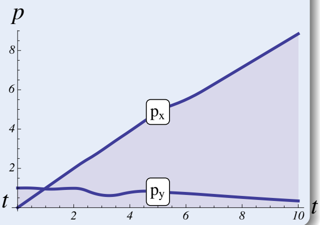
Design & verify controller for a robot avoiding obstacles

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







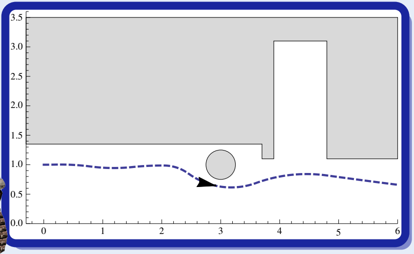


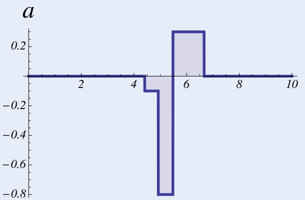
CPS Analysis & Design: Robot Lab

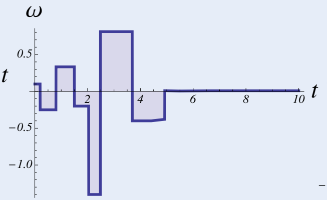
Challenge (Hybrid Systems)

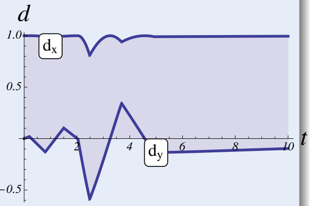
Design & verify controller for a robot avoiding obstacles

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

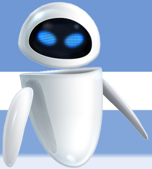








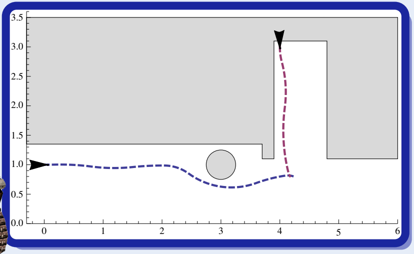
CPS Analysis & Design: Robot Lab

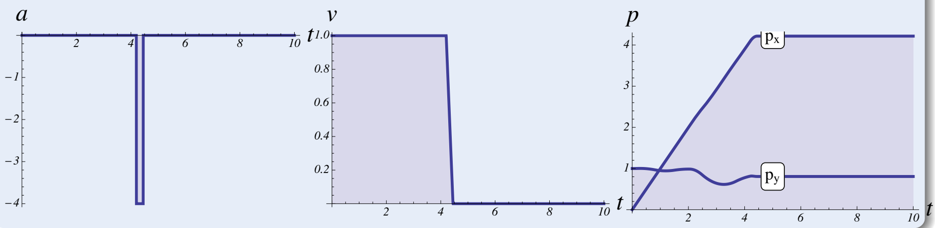


Challenge (Hybrid Systems)

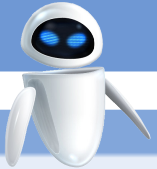
Design & verify controller for a robot avoiding obstacles

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





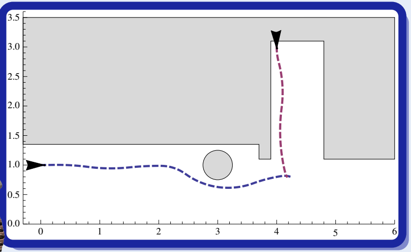
CPS Analysis & Design: Robot Lab

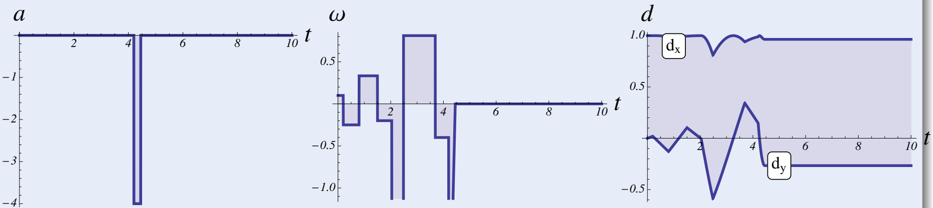


Challenge (Hybrid Systems)

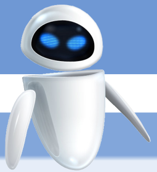
Design & verify controller for a robot avoiding obstacles

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





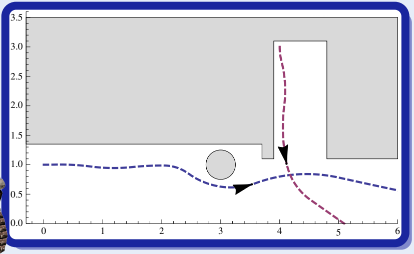
CPS Analysis & Design: Robot Lab

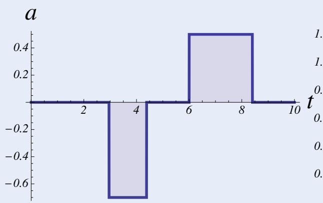


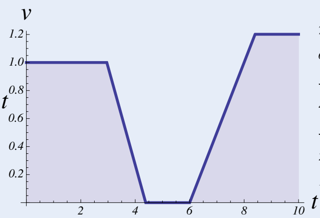
Challenge (Hybrid Systems)

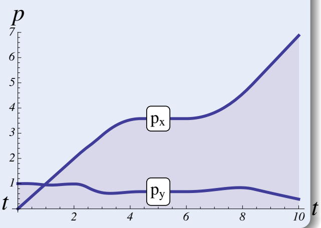
Design & verify controller for a robot avoiding obstacles

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

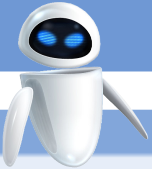








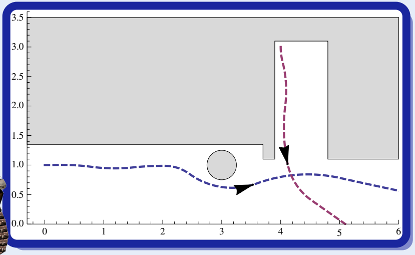
CPS Analysis & Design: Robot Lab

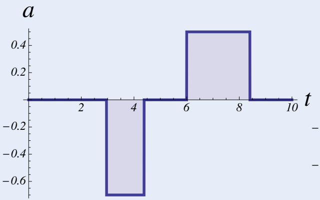


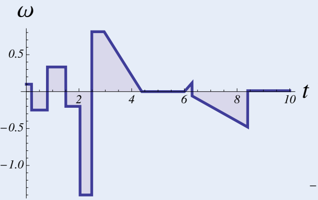
Challenge (Hybrid Systems)

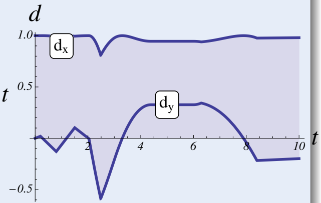
Design & verify controller for a robot avoiding obstacles

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



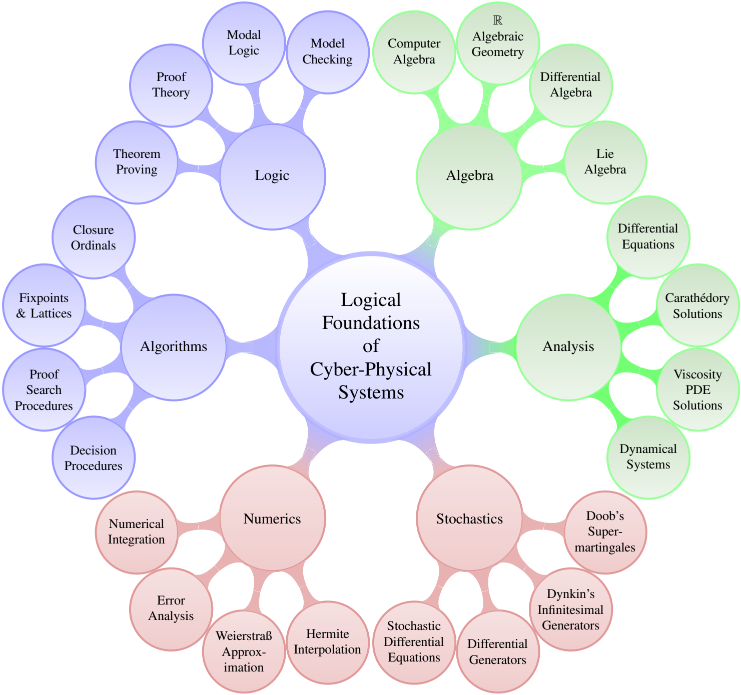






Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs
2. 15-424/624/824: Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Assessment
   - Labs
   - CPS V&V Grand Prix
   - Resources
3. Summary


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

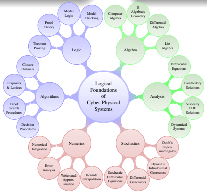
How to Teach Cyber-Physical Systems?

Onion Model

1. Going outside in
2. Unpeel layer by layer
3. Progress when all prereqs are covered
4. First study CS $\land$ math $\land$ 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



Computational Thinking for CPS

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

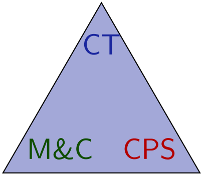
1. CPSs are so easy to get wrong.
2. These logical aspects are an integral part of CPS design.
3. Critical to your understanding of the intricate complexities of CPS.
4. Tame complexity by a simple programming language for core aspects.

About 15-424/624/824 Foundations of CPS

- ▸ 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 and system architectures.
  3. Learn how to design by invariant.
  4. Reason rigorously about CPS models.
  5. Verify CPS models of appropriate scale.
- CPS Skills
  1. Understand the semantics of a CPS model.
  2. Develop an intuition for operational effects.
  3. Use higher-level model-predictive control.
- Byproducts
  1. Exposure to numerous math areas in action.
  2. . . .

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

Course Outline

1. Cyber-physical systems: 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 & responses
9. Reactions & delays
10. Differential equations & differential invariants
11. Differential equations & proofs

---

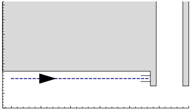
12. Robots / railway / air traffic / car CPS & applications
13. Hybrid systems & hybrid games
14. Distributed systems & hybrid systems
15. Virtual substitution & real arithmetic

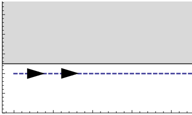
Assessment

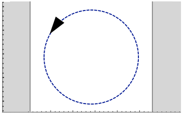
- TODO: Read Collaboration and Academic Integrity Policy ▸ Policy
- ≈22% Theory homework — Due at midnight
- ≈51% Labs, including ≈22% final project
  1. Betabot in first week — Due at **beginning** of lecture
  2. Veribot in second week — Due at midnight
- Whitepaper — For final project
- Proposal — For final project
- Term paper — Due with final project
- CPS V&V Grand Prix presentation — Thu May 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

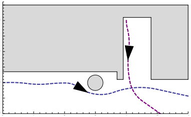
Robot Labs

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







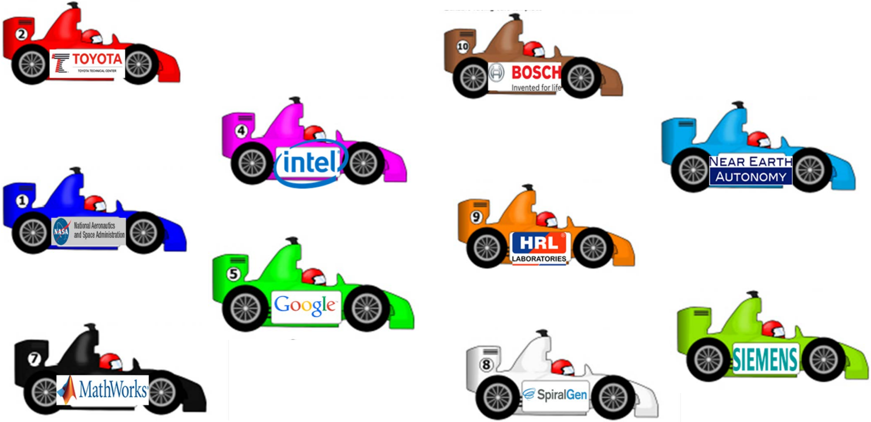


▸ CPS v&V Grand Prix

CPS V&V Grand Prix: Undergrad Course Competition

Carnegie Mellon University

May 5th, 2016



2 TOYOTA TOYOTA TECHNICAL CENTER
10 BOSCH Invented for life
4 intel
NEAR EARTH AUTONOMY
1 NASA National Aeronautics and Space Administration
9 HRL LABORATORIES
5 Google
7 MathWorks
8 SpiralGen
SIEMENS

Resources

Prerequisites

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

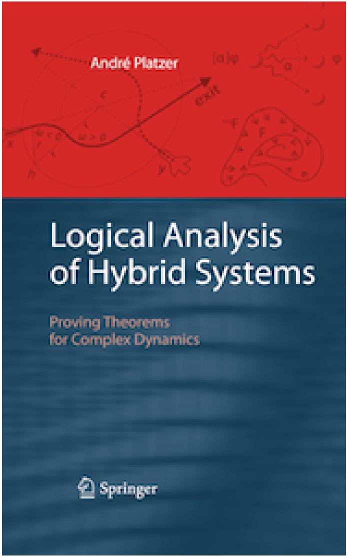
21-122 Integration, Differential Equations, and Approximation — x'

(15-251 Great Theoretical Ideas in Computer Science **or**
21-241 Matrix algebra **or**
18-202 Mathematical Foundations of Electrical Engineering) — Math proofs

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

  http://lfcps.org/course/fcps17.html
- KeYmaera X: aXiomatic Tactical Theorem Prover for Hybrid Systems
- Piazza
- Autolab
- Ask!

Lecture Notes and Book


André Platzer
Logical Analysis of Hybrid Systems
Proving Theorems for Complex Dynamics
Springer

- André Platzer.
  Foundations of Cyber-Physical Systems.
  Lecture notes.
  Computer Science Department
  Carnegie Mellon University.
  `http://lfcps.org/course/fcps17-schedule.html`

- André Platzer.
  Logical Analysis of Hybrid Systems.
  Springer, 426p., 2010.
  DOI 10.1007/978-3-642-14509-4
  `http://symbolaris.com/lahs/`
  CMU library e-book

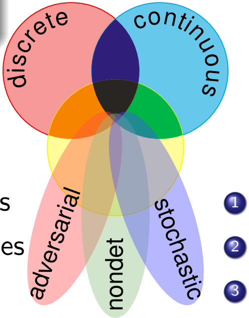
Outline

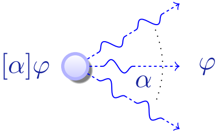
1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs
2. 15-424/624/824: Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Assessment
   - Labs
   - CPS V&V Grand Prix
   - Resources
3. Summary

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

differential dynamic logic

dL = DL + HP





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

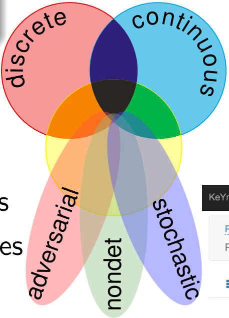
1. Multi-dynamical systems
2. Combine simple dynamics
3. Tame complexity
4. V&V cool challenges

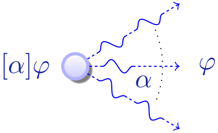
Numerous wonders remain to be discovered

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

differential dynamic logic

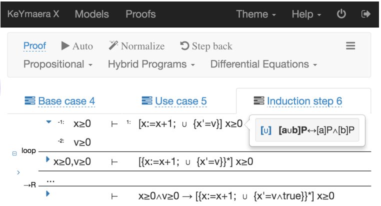
$$\mathrm{dL} = \mathrm{DL} + \mathrm{HP}$$





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

KeYmaera X



```
 -1:  x≥0        ⊢  1: [x:=x+1; ∪ {x'=v}] x≥0     [∪]  [a∪b]P↔[a]P∧[b]P
 -2:  v≥0
loop ─────────────────────────────────────────────
      x≥0,v≥0    ⊢     [{x:=x+1; ∪ {x'=v}}*] x≥0
     ─────────────────────────────────────────────
      ...
 →R  ─────────────────────────────────────────────
                 ⊢     x≥0∧v≥0 → [{x:=x+1; ∪ {x'=v∧true}}*] x≥0
```

Numerous wonders remain to be discovered

André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2017.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.

André Platzer.
Logics of dynamical systems.
In LICS [10], pages 13–24.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

André Platzer.
Differential dynamic logic for verifying parametric hybrid systems.
In Nicola Olivetti, editor, *TABLEAUX*, volume 4548 of *LNCS*, pages 216–232. Springer, 2007.

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.

J. Autom. Reas., 2016.

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481. Springer, 2015.

André Platzer.
Logic & proofs for cyber-physical systems.
In Nicola Olivetti and Ashish Tiwari, editors, *IJCAR*, volume 9706 of *LNCS*, pages 15–21. Springer, 2016.

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

📄 *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012*. IEEE, 2012.