Formal Verification of Cyber-Physical Systems

An Invitation

Sriram Sankaranarayanan

University of Colorado, Boulder, CO

Pop Quiz

Solve this:

$$\frac{dx}{dt} = xe^{-t}$$

$$x(0) = 5$$

Dynamical Systems

- State: x
- Rule describing how to go from one state to next.

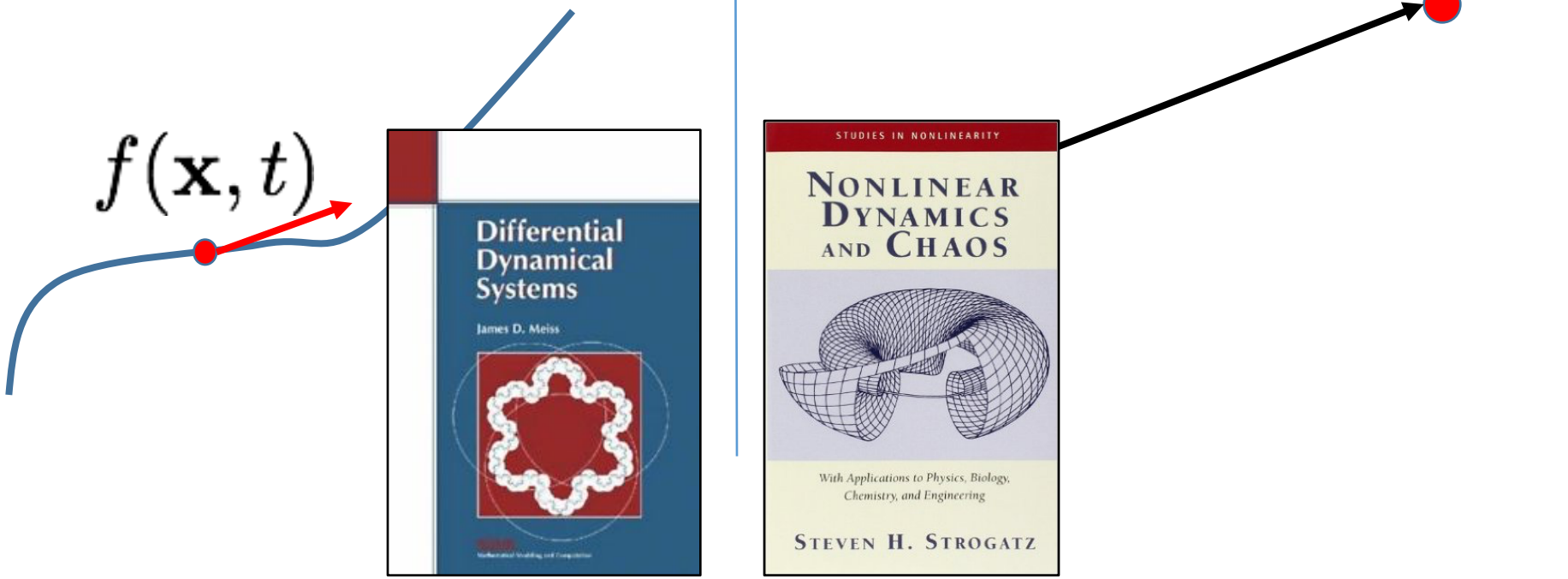
Continuous vs. Discrete Time

$$\frac{d\mathbf{x}}{dt} = f(\mathbf{x}, t)$$

$$t \in \mathbb{R}$$

$$\mathbf{x}(t+1) = f(\mathbf{x}(t), t)$$

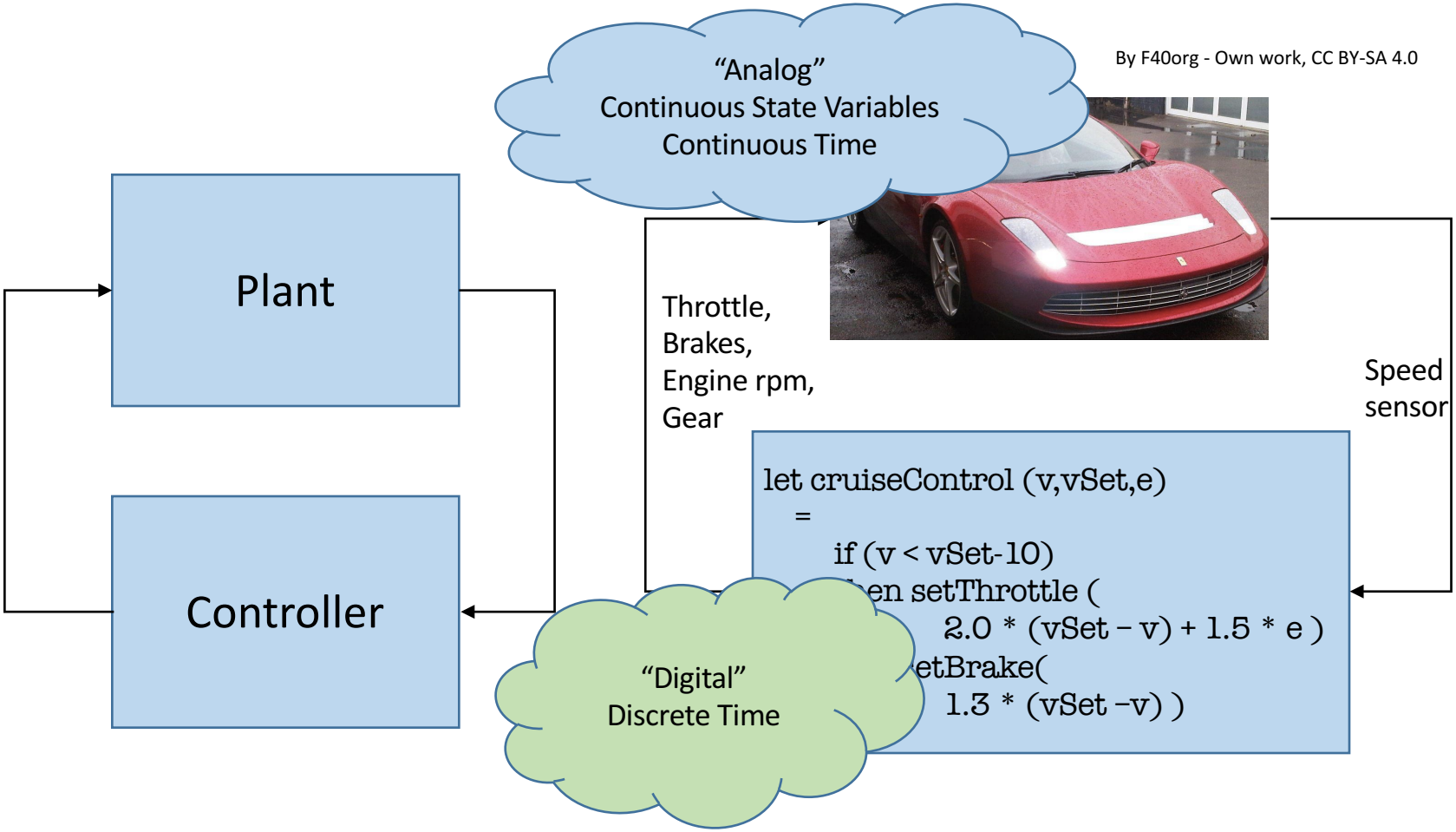
$$t \in \mathbb{N}$$



Outline

- Cyber-Physical Systems.
- Theoretical Challenges.
- Application Challenges.
- Research Directions.
- PhD in formal methods for CPS.

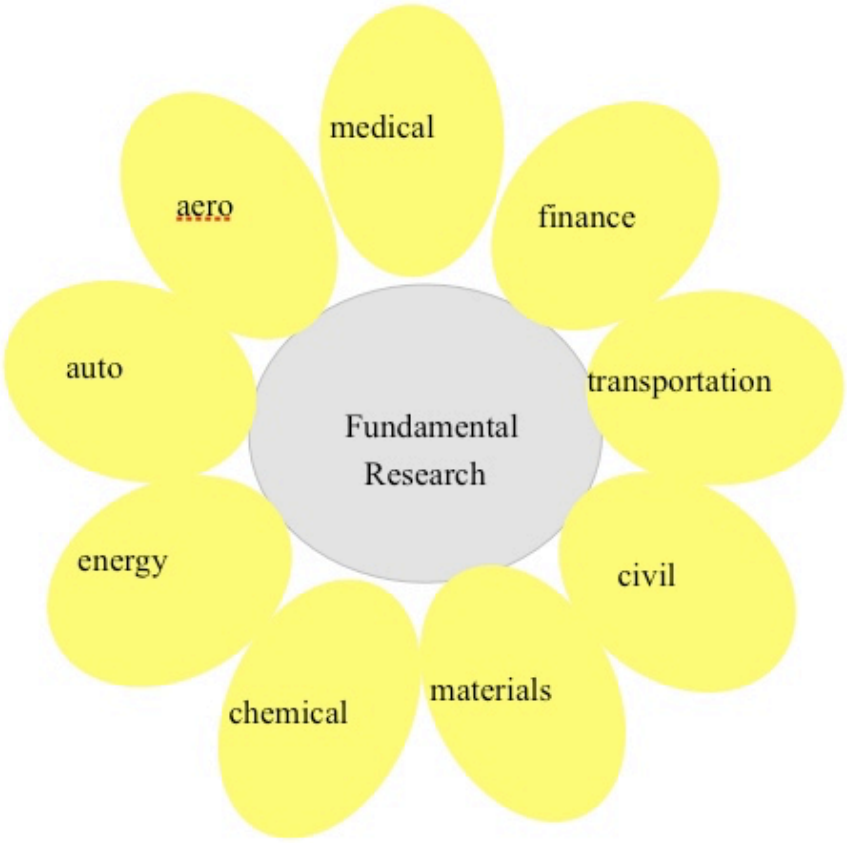
Control Systems



Cyber-Physical Systems (CPS)

- Computer Control of a Physical Process.
  - “Deeply” embedded, real-time computation.
- Discrete-time (digital) system interacting with continous time (analog) system.
- Natural systems: physics, biology, ecology, climate,..
- Common examples around us!

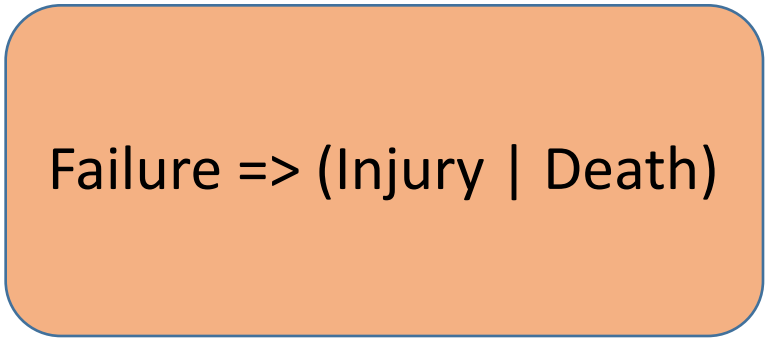
CPS Application Domains



Large variety of application domains.

“CPS Flower” by P.R. Kumar and Jeannette Wing.

Safety Critical Systems



Verification of CPS: Automotive Systems

NHTSA Campaign Number: 12V504000
BMW 7-series model years 2005-2007

Due to a software problem, the doors may appear to be closed and latched, but, in fact, may inadvertently open.

CONSEQUENCE:
The door may unexpectedly open due to road or driving conditions or occupant contact with the door.
The sudden opening may result in occupant ejection or increase the risk of injury in the event of a crash.

NHTSA Campaign Number: 11V248000
Honda CR-Z model year 2011

There is possibility that the engine control unit software may cause the electric motor of the hybrid system to move the vehicle unexpectedly in the opposite direction of the selected gear.

CONSEQUENCE:
Unexpected Vehicle Movement could increase the risk of a crash or personal injury to the persons in the path of the moving vehicle.

Source: safercar.gov

Cardioverter Defibrillators (ICD)

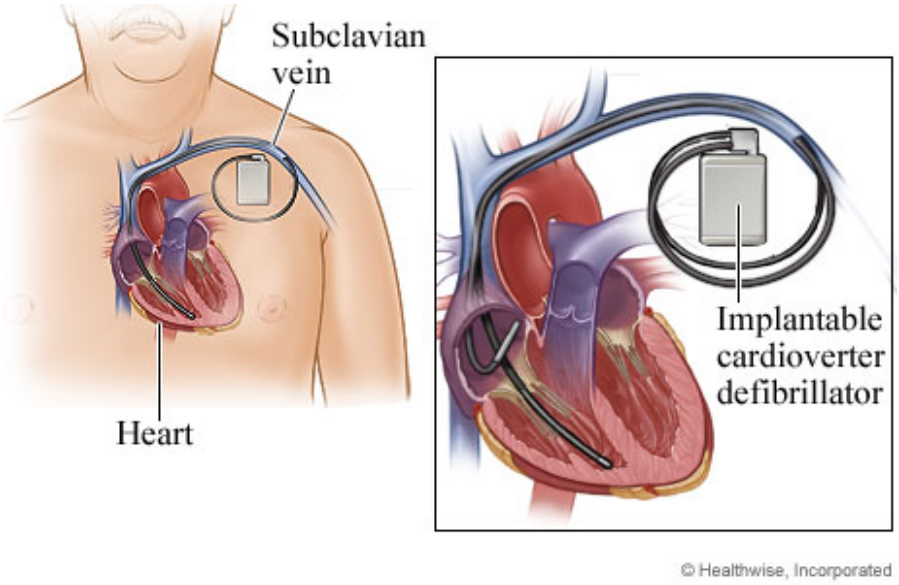


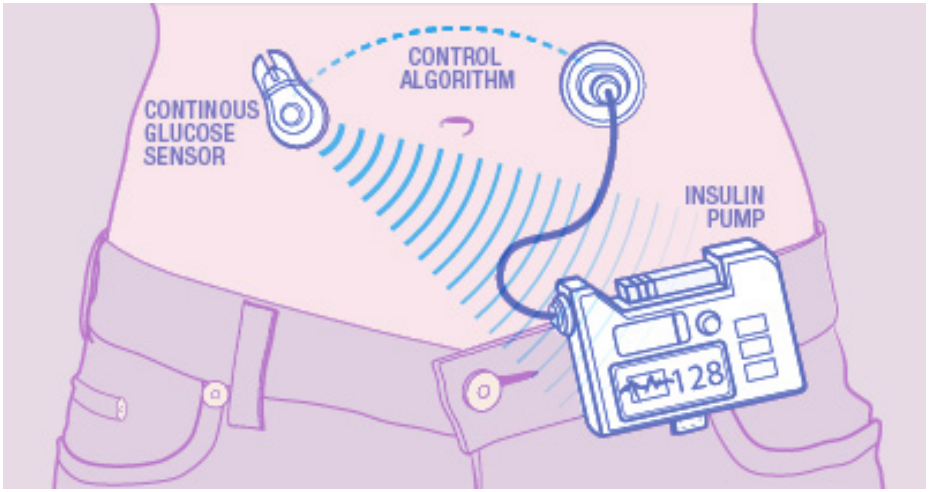
Image source: webmd.com

Injuries/Deaths due to

- Inappropriate shocks delivered.
- Appropriate shock not delivered.

[Smolka, Grosu et al., Mangharam et al.]

Artificial Pancreas



Source: MayoClinic.com

Too much insulin delivery:
loss of consciousness, coma, death.

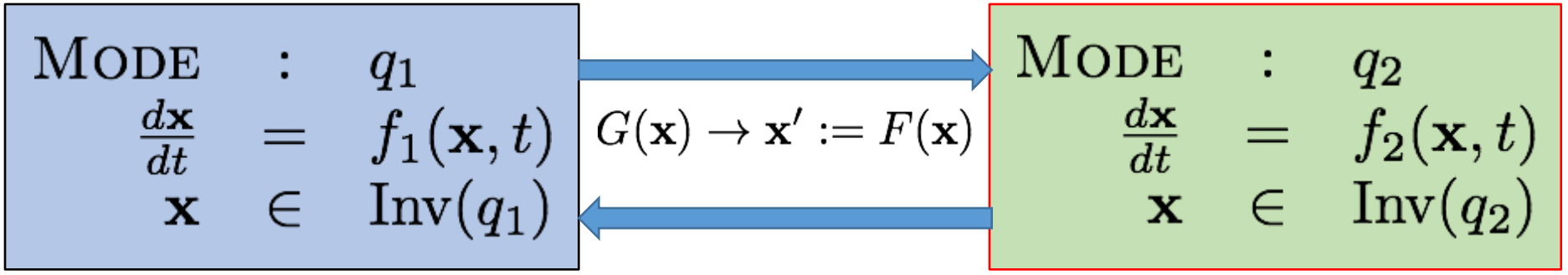
Too little insulin delivered:
diabetic ketacidosis

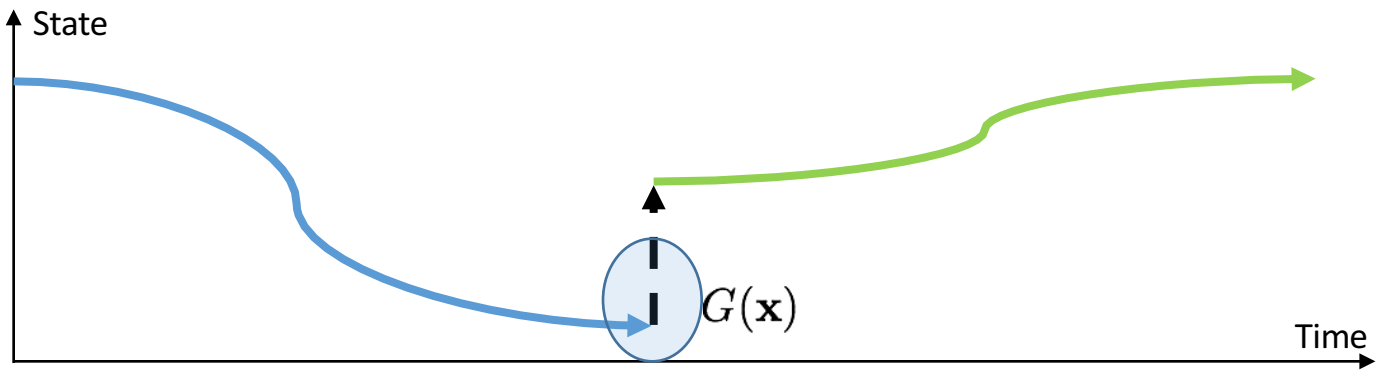
[Sankaranarayanan et al.'15,'16; Sanjian Chen et al.'15]

Foundations of CPS

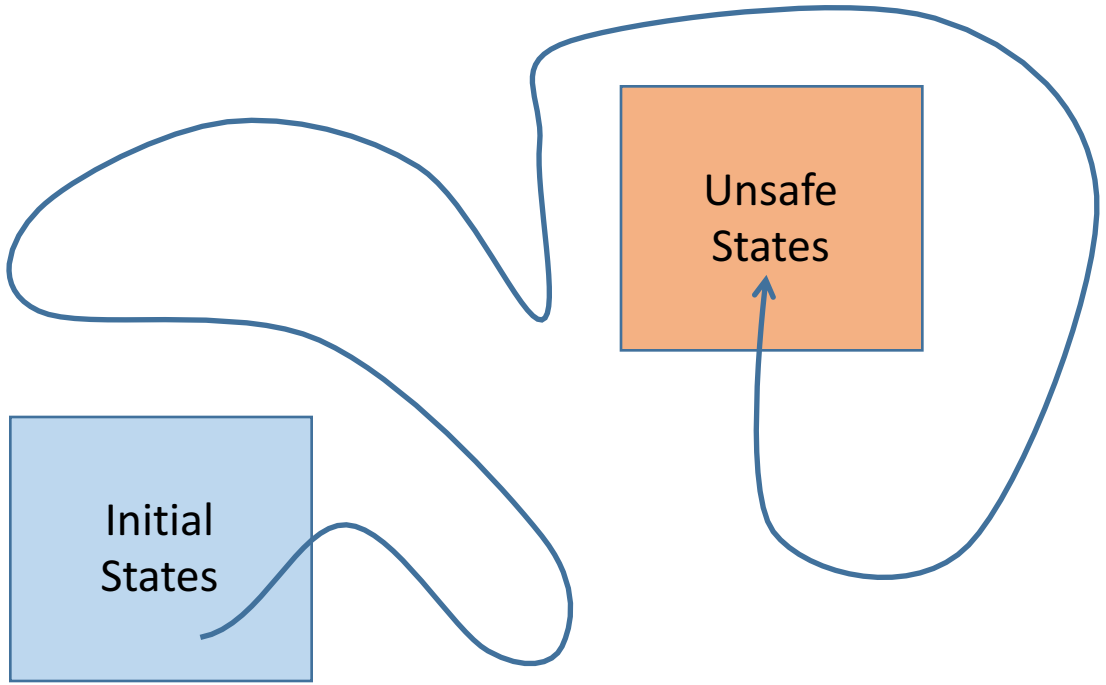
Hybrid Automata

[Alur, Henzinger,
Dill, Pnueli,
Manna, Maler,
Sastry, Lygeros, Tomlin,…]



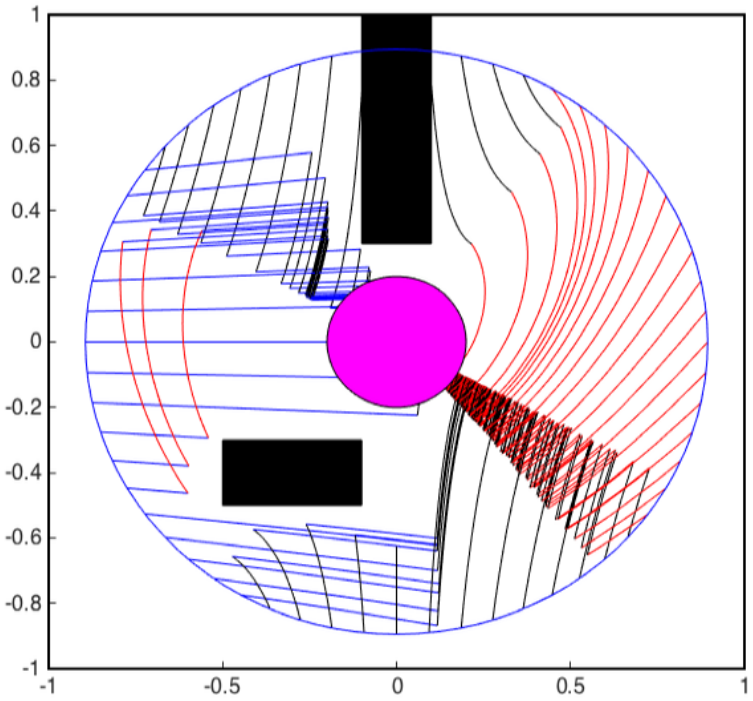


Specifications



Reachability: trajectory from initial to unsafe state?

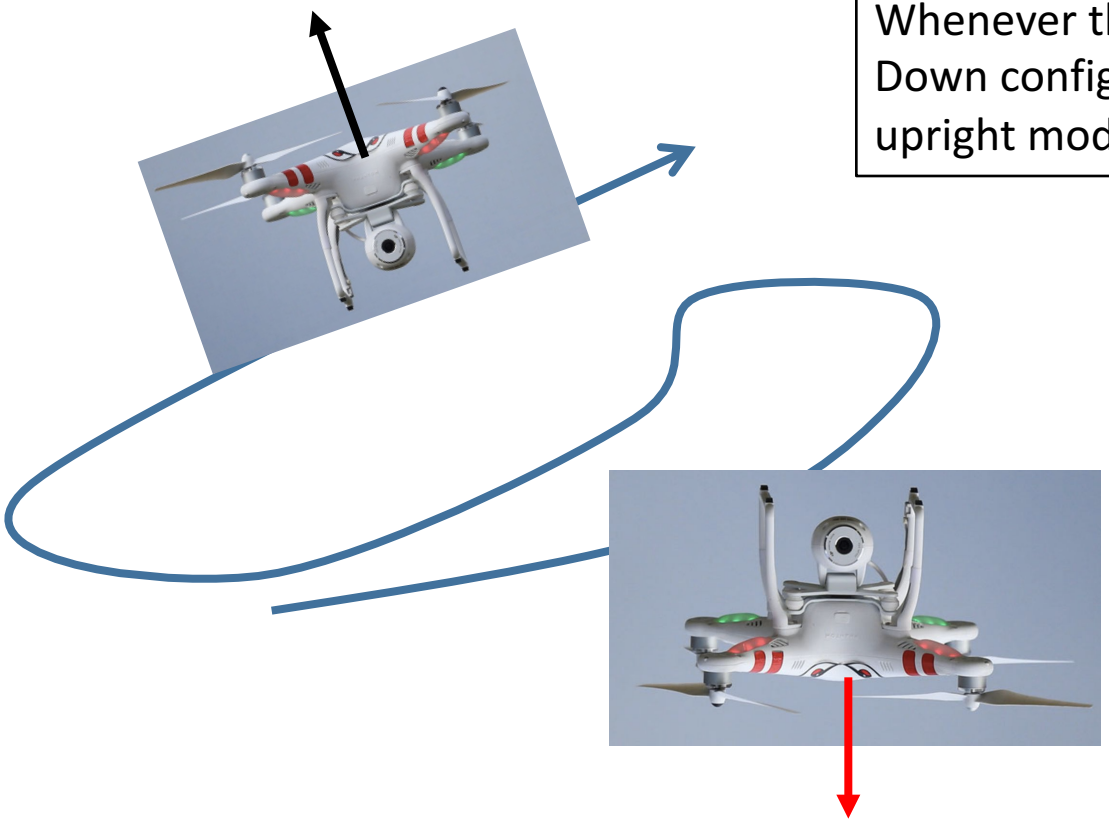
Stability



Stability

1. System converges towards an equilibrium
2. Trajectories that start close to the equilibrium remain close.

Real-Time Temporal Properties



Whenever the UAV reaches an Upside-Down configuration, it must reach an upright mode within 2 seconds.

Verification Techniques

Challenges

Murphy's Law for Hybrid Systems

Class of Hybrid Systems with "interesting" examples.

Verification Problems are Undecidable.

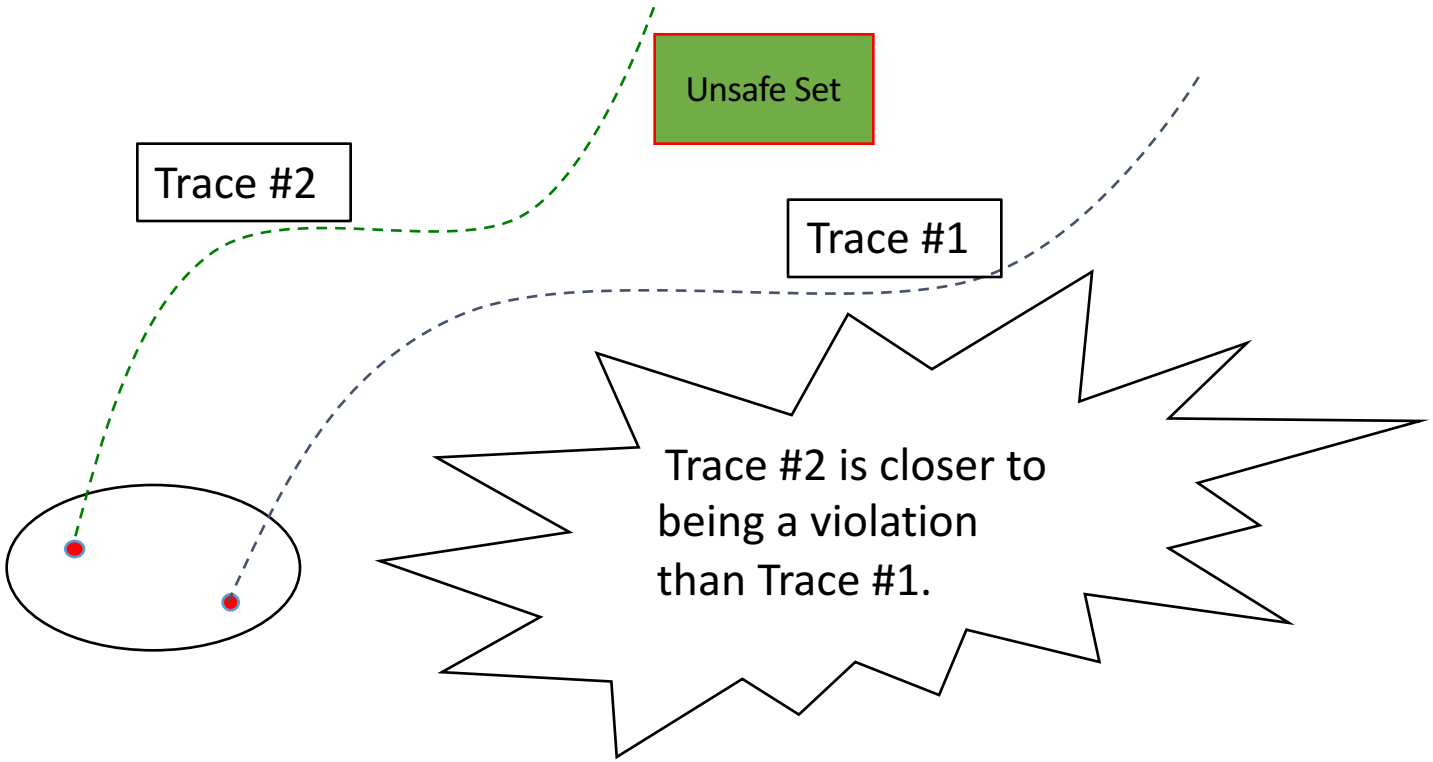
[Ken's One System Per Paper Syndrome]

Falsification Approaches

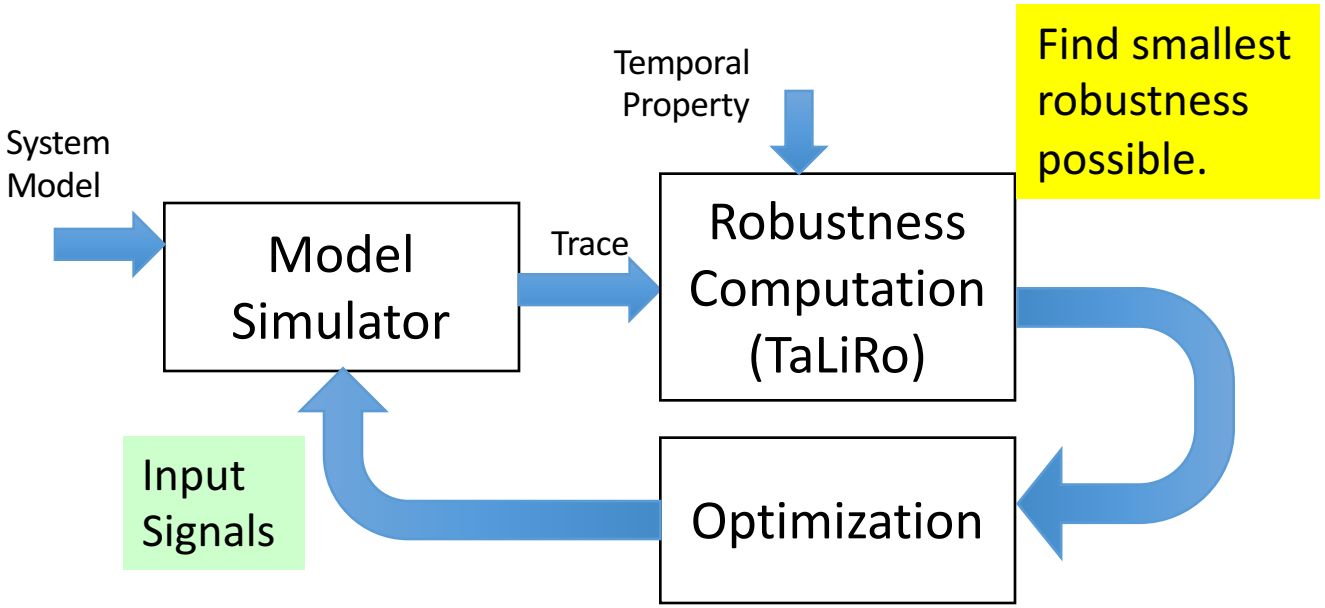
Lower Expectations, Throw away the Baby.

- Best effort search to find counterexamples.
- No correctness proofs.
- Falsification tools:
  - S-Taliro [Fainekos+S+Others],
  - Breach [Donze+Others].

Robustness: Idea

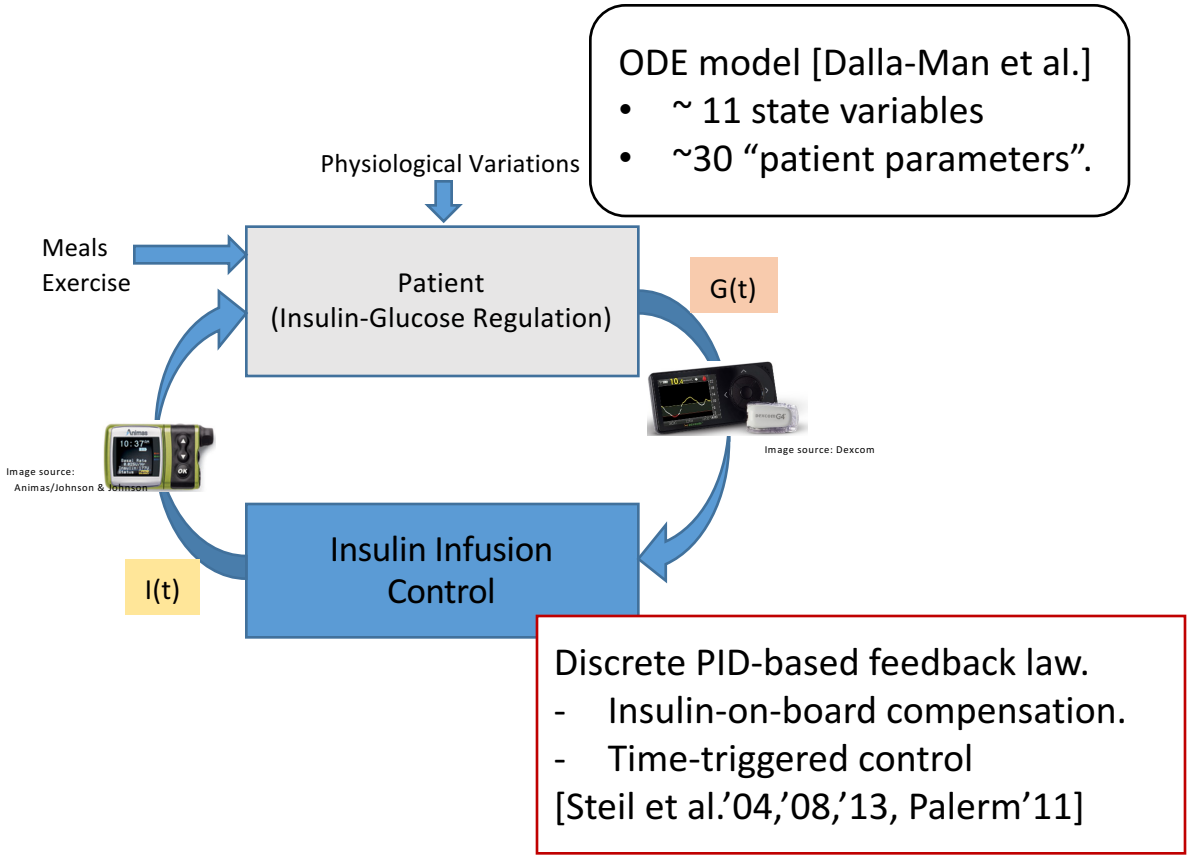


S-Taliro: Falsification Using Robustness



[Fainekos+S+Abbas+Ivancic+Gupta]

Case-Study: Artificial Pancreas Control.



S-Taliro Results

[Cameron et al.'15, S. et al. '16]

1. Hypoglycemia: Can blood glucose level go below 70 mg/dl?

   "Near" Violation!

2. Hyperglycemia: Can blood glucose level go above 350 mg/dl?

   Violation!

3. Insulin infusion below target: Can controller deliver insulin below target level of 90 mg/dl?

   Violation!

4. Can "wakeup" hyperglycemia above 200 mg/dl happen?

   No Violation!

5. Can the patient suffer a "prolonged" hyperglycemic episode?

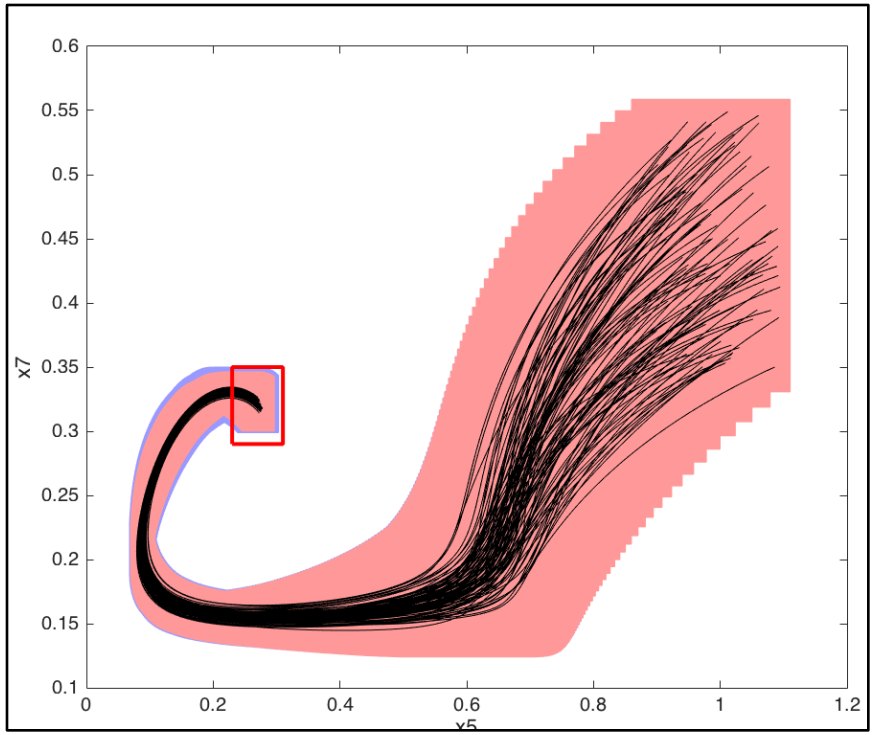
   Violation!

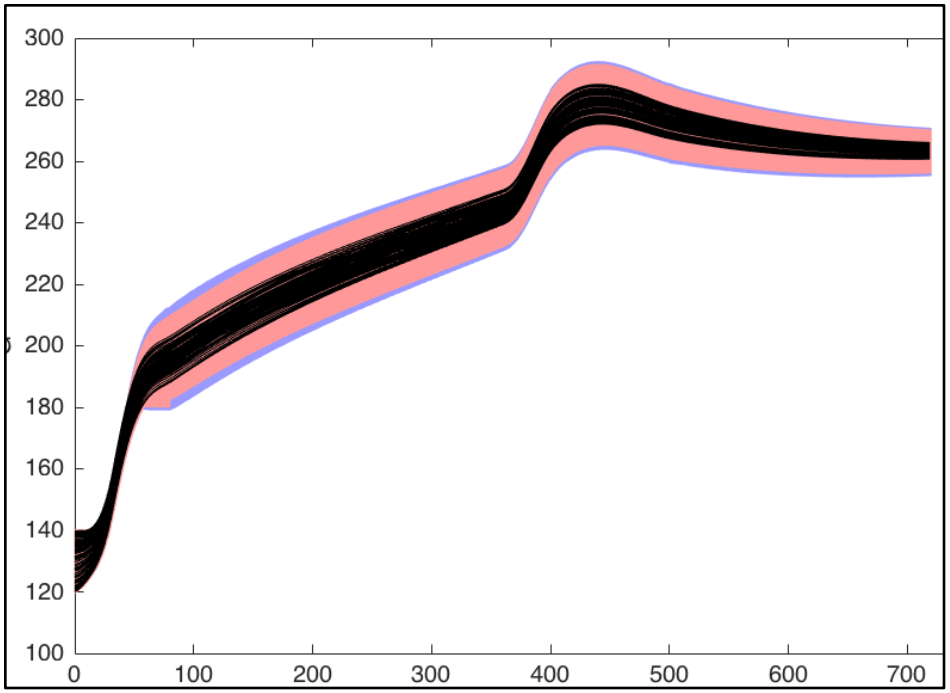
~ 3.5 hours of wall clock time.

Formal Verification

- Goal #1: Establish presence or absence of bugs.
- Goal #2: handle semantics with mathematical precision.

Approach #1: Flowpipe Construction





Goal: explore all reachable states up to a finite time horizon.

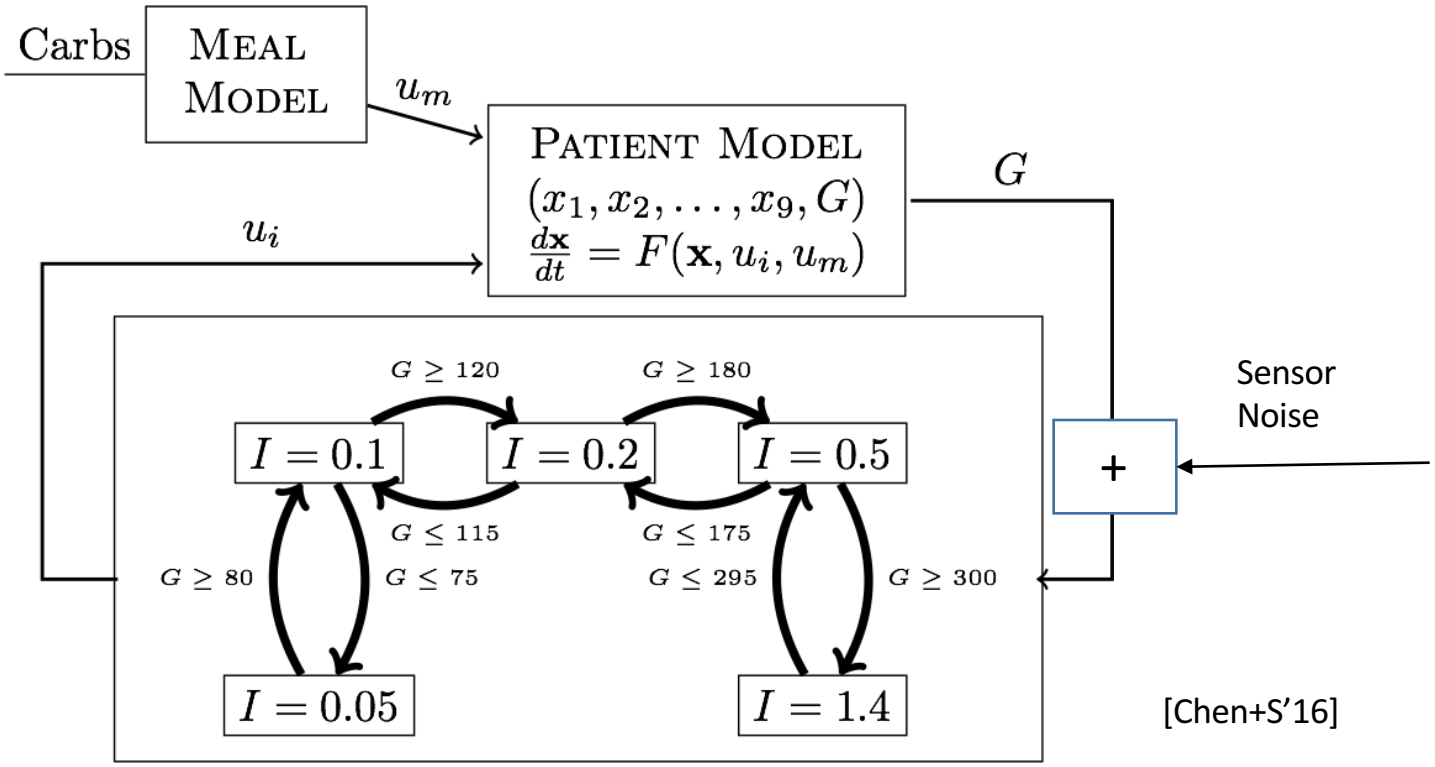
Symbolic Model Checkers For Hybrid Systems

- Linear hybrid systems:
  - SpaceEx [Frehse+Others, Verimag].
- Nonlinear hybrid systems:
  - Flow* [Chen+Abraham+**S**, Univ. of Colorado + RWTH Aachen University].
  - Cora [Althoff et al., TU Munich].
  - iSAT [Franzle+Others, Oldenburg].
  - dReach(*) [Gao+Kong+Clarke, MIT/CMU].

State-of-the-Art

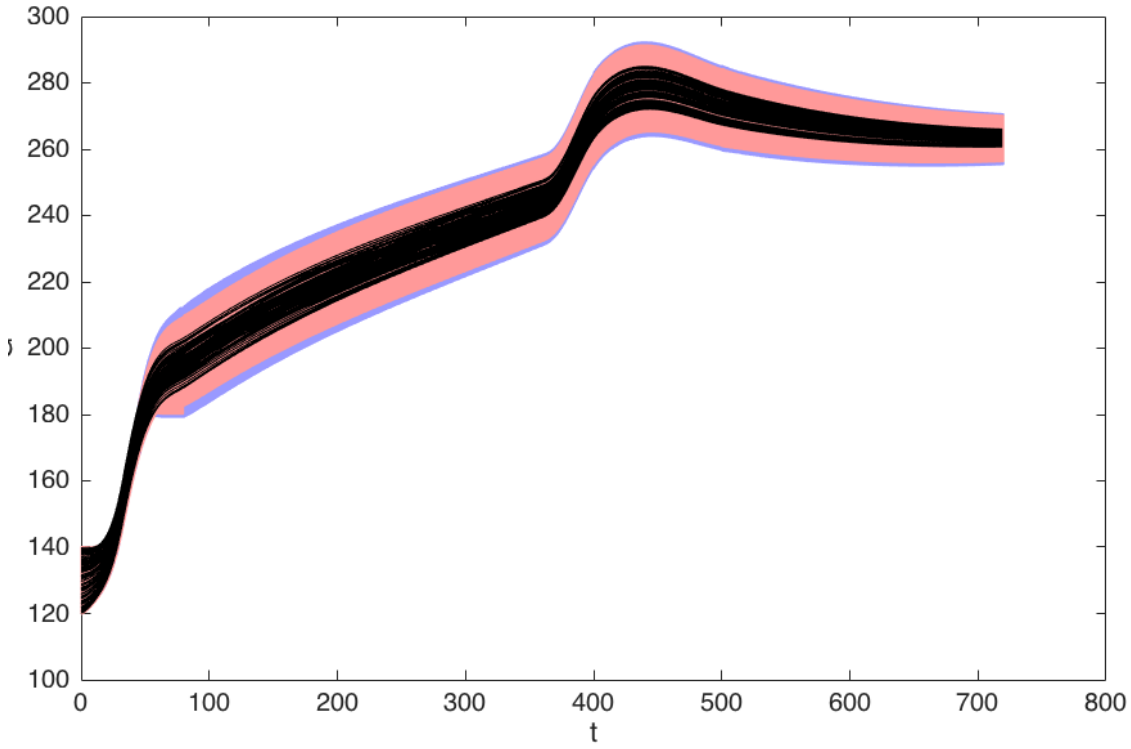
- SpaceEx: linear systems with 50+ state variables.
  - Interesting commercial applications at this scale.
- Nonlinear Systems:
  - Smaller systems: 5-10 variables.
- Recent work by Xin Chen + **S**:
  - 30+ variables if “structurally sparse”

Verification of Multi-Basal Artificial Pancreas System



[Chen+S'16]

Flow* Verification



- ✓ Absence of hypoglycemia
- ✓ No ketacidosis (G >= 300 mg/dl)
- ➢ Blood glucose does not settle inside range [70,180]

dReal/dReach

- Delta-Complete decision procedure over reals.
- Reason about type-2 computable real functions.
  - Solutions to Ordinary Differential Equations.
- Numerous applications:
  - Artificial Pancreas parameter selection [Chen+Lee'15]
  - ICD (Cardiac) Devices [Islam+Smolka+Grosu+Others]

Theorem Proving

- Early work on STeP Theorem Prover [Manna+Sipma..'90s]
- Keymera [Platzer+Others' CMU]
  - Differential Dynamic Logic.
  - Integrates with decision procedures over reals.
  - Extensions to concurrent and parameterized systems.
- Successes of KeyMera:
  - ACAS-X collision avoidance protocol verification.
  - Numerous application case studies.

Combining Simulations + Proofs

- C2E2 [Duggirala+Mitra + Viswanathan , UIUC]

- Testing + Proofs using discrepancy functions.
  - Compositional reasoning.
  - Inference of discrepancy functions from simulations.

  - Applications: medical devices, airtraffic management protocols, automotive systems.

Formal Synthesis

Formal Synthesis for CPS

- Interesting combination of CS + Control theory approaches for synthesis.
- Control approach: find feedback functions to obtain reachability/stability properties.
- CS approach: synthesize control for temporal objectives.

Tutorial Tomorrow

CAV 2016 tutorial on synthesis by Paulo Tabuada

Tomorrow afternoon.

“Hot” Research Directions

Foundations of CPS

- Understanding properties of hybrid systems.
  - Invariant Sets.
  - Lyapunov Functions.
  - Equivalences between systems.
- Efficient inference of properties.
  - Invariant Synthesis for nonlinear systems.
  - Nonlinear Lyapunov synthesis.
- Formal synthesis.
- Stochastic Hybrid Systems

From the model to implementation.

Throttle,
Brakes,
Engine rpm,
Gear

Speed
sensor

```
let cruiseControl (v,vSet,e)
   =
      if (v < vSet-10)
      then setThrottle (
                2.0 * (vSet – v) + 1.5 * e )
      else setBrake(
                1.3 * (vSet –v) )
```

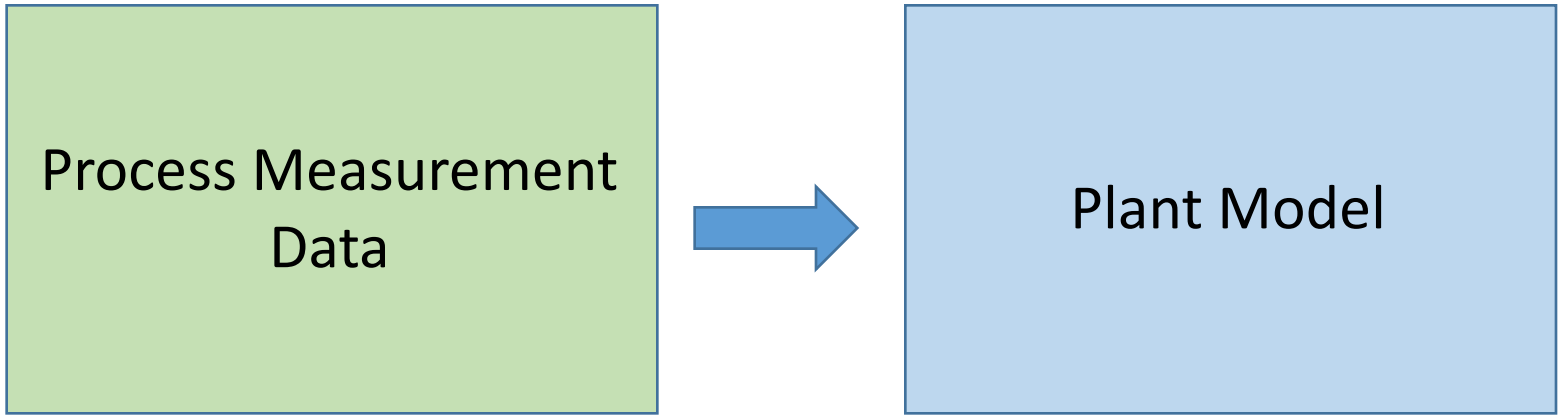
Goal

Integrate code analysis with models of physical dynamics.

[Jackson et al.'14, Zutshi+S+Deshmukh+Jin'16]

Constructing Models from Data

System Identification



Goal: Identify models more suitable for verification.

Reasoning about pattern recognition/machine learning.

Image Credit: google.com

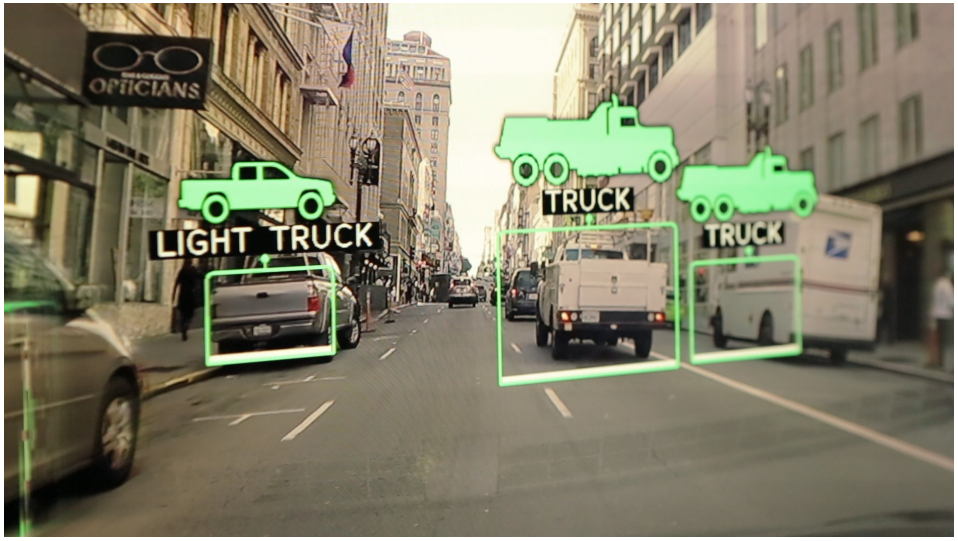


Image Credit: nvidia.com

Closed-Loop Medical Systems

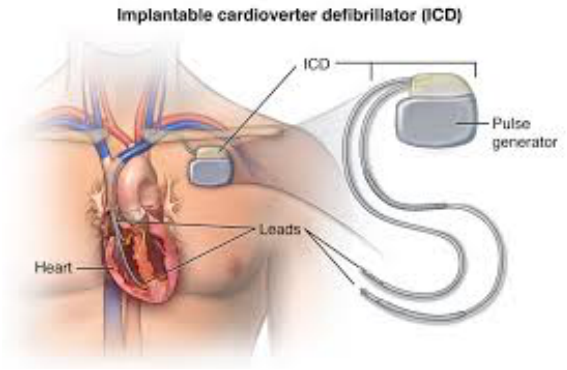
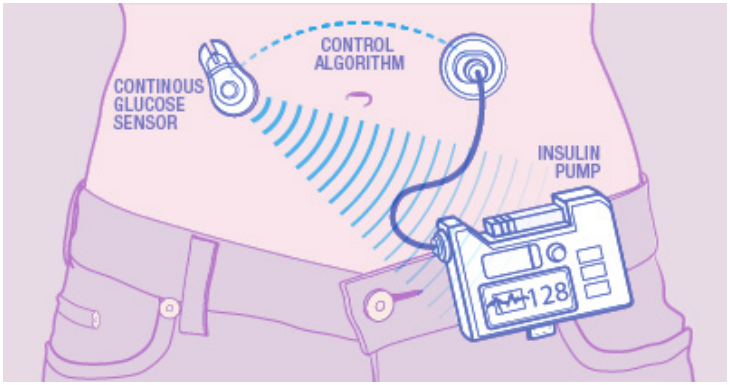
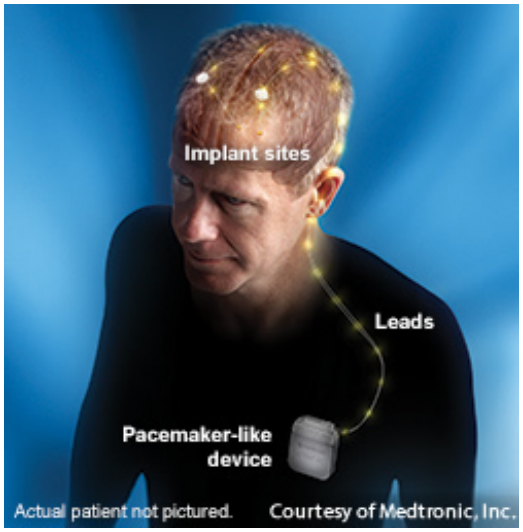


Image source: hopkinsmedicine.com



Source: MayoClinic.com



Resources for Closed Loop Medical Devices

https://www.cs.colorado.edu/~srirams/courses/clMedDevices-spr16/clDevices.html

Closed-Loop Devices

I have attempted to organize some basic references for various devices below. Your task for Week 1 is to expand and enlarge the list by doing a literature search.

Artificial Pancreas

The artificial pancreas is a great example of a closed loop medical device. A large portion of this class will focus on this device.

Scientific Survey Articles

- Claudio Cobelli, Eric Renard and Boris Kovatchev, Artificial Pancreas: Past, Present, Future, Diabetes November 2011 vol. 60 no. 11 2672-2682.
- B. Kovatchev, M. Breton, C. Dalla Man and C. Cobelli, In Silico Preclinical Trials: A Proof of Concept in Closed-Loop Control of Type 1 Diabetes, J Diabetes Sci Technol. Jan 2009; 3(1): 44–55.
- Francis J. Doyle, Lauren M. Huyett, Joon Bok Lee, Howard C. Zisser and Eyal Dassau, Closed-Loop Artificial Pancreas Systems: Engineering the Algorithms, Diabetes Care, May 2014 vol. 37 no. 5 1191-1197.
- Hovorka R, Canonico V, Chassin LJ, Haueter U, Massi-Benedetti M, Orsini Federici M, Pieber TR, Schaller HC, Schaupp L, Vering T, and Wilinska ME. Nonlinear model predictive control of glucose concentration in subjects with type 1 diabetes. Physiol Meas. 2004 Aug;25(4):905-20.

Videos

- Bruce Buckingham's TEDxDelMar Talk.
- Ed Damiano's TEDx Talk.

Press Articles

Human-in-the-loop CPS

- Many CPS are operated by humans in the loop.
- How do we reason formally about humans?
  - Modeling human behavior: ideas from psychology/cognitive science.
  - Collecting data about human actions and mistakes.

How to get started?

CPS-focused conferences

- CAV: plenty of papers on hybrid systems.
  - ETAPS/TACAS.
- CPSWeek: multiple conferences under single umbrella.
  - Hybrid Systems: Computation and Control (part of CPSWeek).
- ESWeek.
  - ACM/IEEE conference on Embedded Software (EMSOFT)
- RTSS:
  - IEEE Real Time Systems Symposium.

CPS Courses

- Formal Methods.
- Control Theory and Dynamical Systems.
- Real-Time and Embedded Systems.
- Convex Optimization.
- Robotics.

CPS Books

- Lee and Seshia, Introduction to Embedded Systems.
  - http://leeseshia.org
- Rajeev Alur, Principles of Cyber-Physical Systems.
  - https://mitpress.mit.edu/books/principles-cyber-physical-systems
- Andre Platzer, Logical Analysis of Hybrid Systems
- Handbook of hybrid systems (good reference).

Acknowledgments

- Thanks to Aarti, Andrey and Ruzica.

This work was supported by the US National Science Foundation (NSF) under Award # CPS-1446900.