FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

High Confidence Learning and Adaptive Systems for CPS

Claire Tomlin, EECS, UC Berkeley

Berkeley
UNIVERSITY OF CALIFORNIA

Massachusetts Institute of Technology

NSF

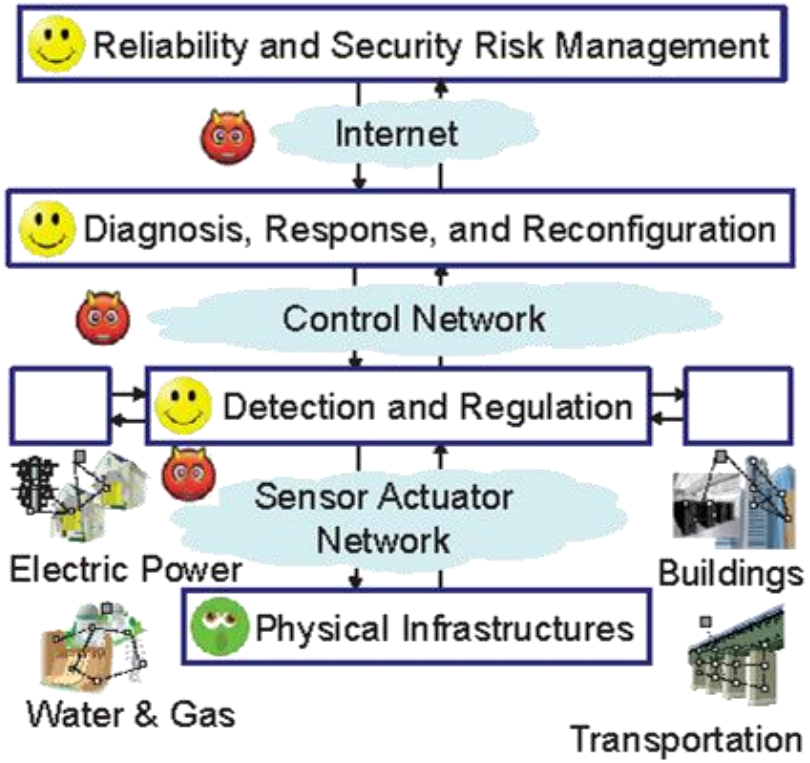
MICHIGAN

VANDERBILT UNIVERSITY

Economic Incentives

Game theory // Mechanism design // Interdependent risk management

Resilient CPS design



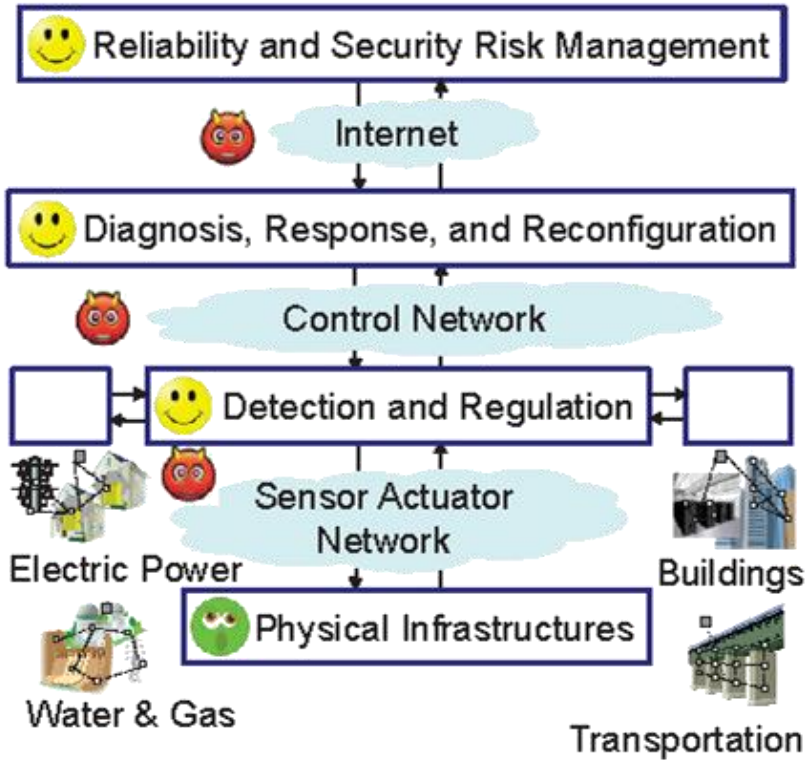
Robust Control

Fault/attack diagnostics // Control of ActionWebs // Model-based design

Economic Incentives

Game theory // Mechanism design // Interdependent risk management

Resilient CPS design



Residential DR

Secure Estimation for CPS
Fully decentralized policies

Distributed Power
UAV networks
Resilient Stormwater Mgmt

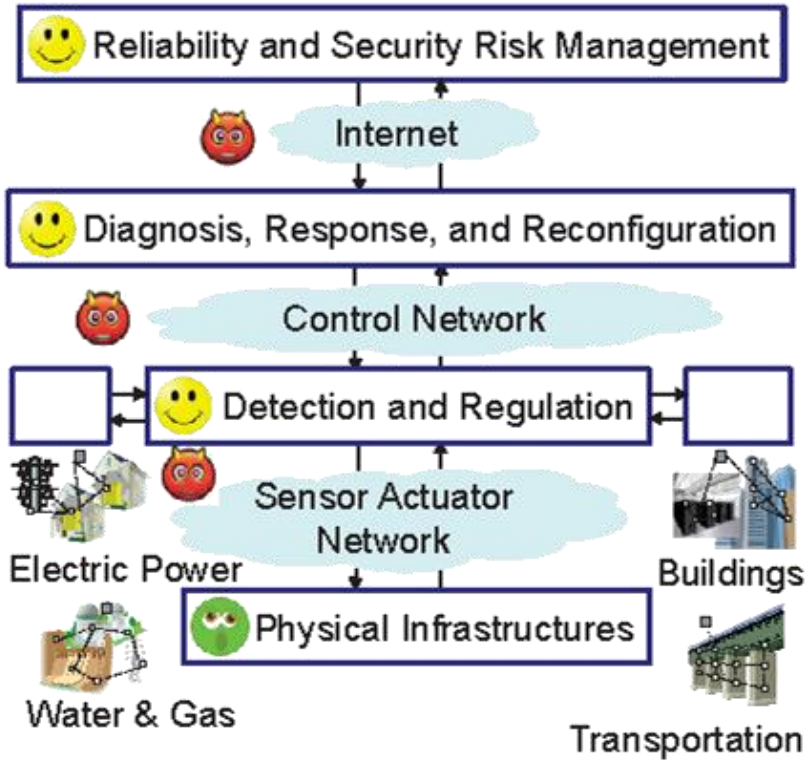
Robust Control

Fault/attack diagnostics // Control of ActionWebs // Model-based design

Economic Incentives

Game theory // Mechanism design // Interdependent risk management

Resilient CPS design

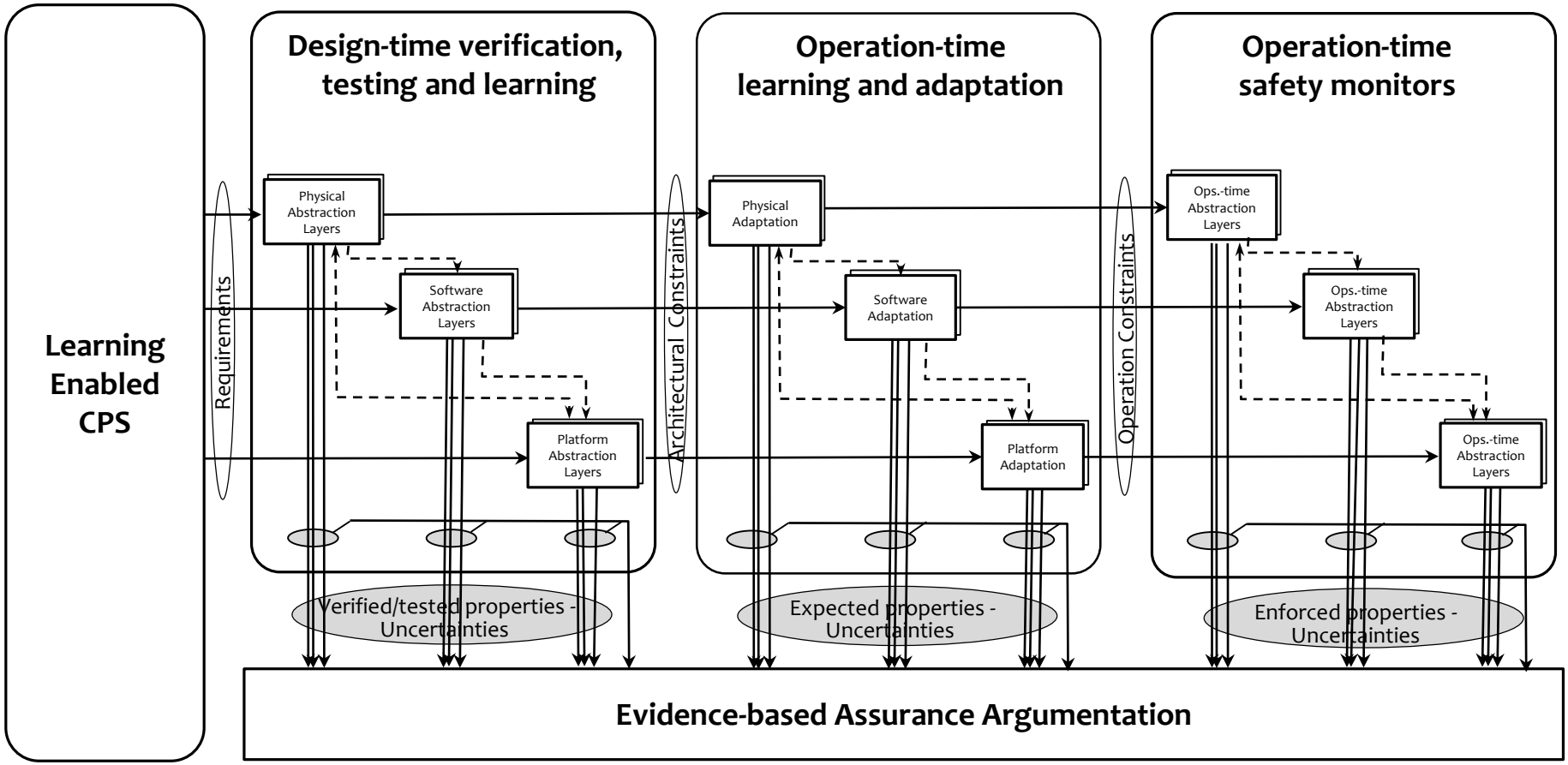


Learning-Enabled Components

Robust Control

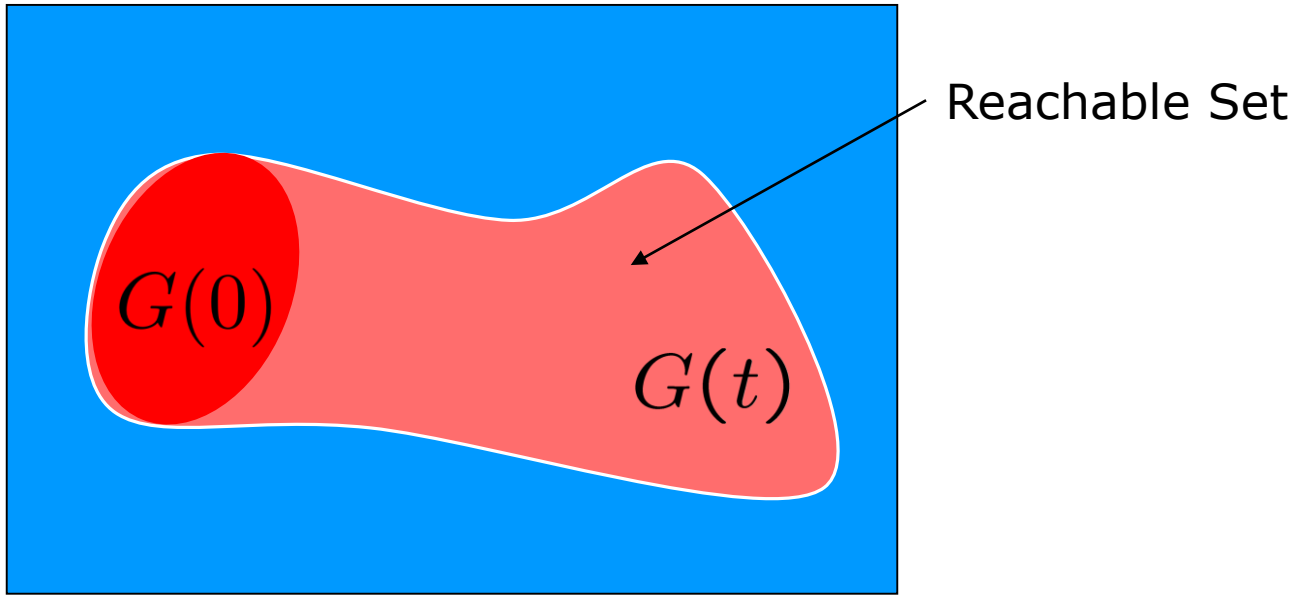
Fault/attack diagnostics // Control of ActionWebs // Model-based design

Designing high confidence systems that can learn

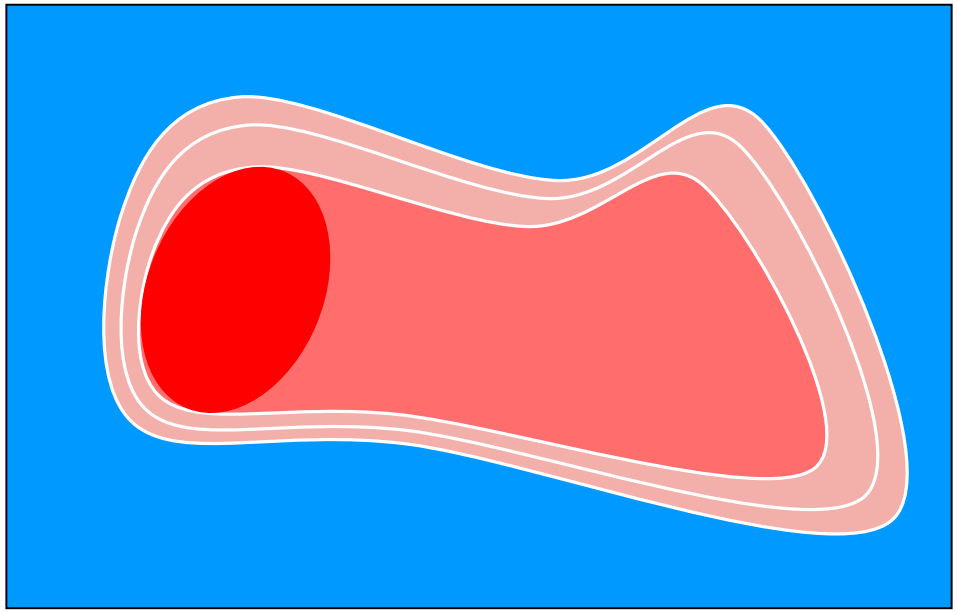


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

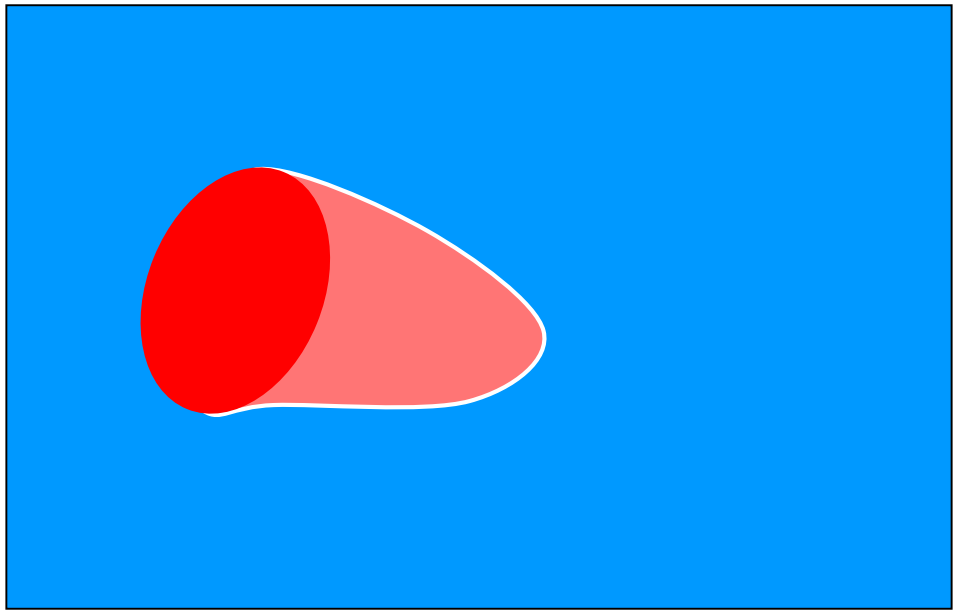
Model Checking using Reachability



Overappromixations as certificates



Learning can reduce conservatism



Scalability

- Impose practical constraints
  - Roads, highways, protocols…
- Approximations
  - Bisimulations (Girard, Pappas, Tabuada)
  - Linear, piecewise and multi-affine systems (Morari, Borrelli, Krogh, Johansson, Rantzer, Belta, Ozay, Darbon, Osher)
  - Ellipsoidal and polyhedral sets (Kurzhanski , Varaiya, Stipanovic)
  - Polynomial systems, barrier certificates (Parillo, Majumdar, Tedrake, Pappas, Papachristodoulou, Julius, Lall, Topcu, Frehse, Le Guernic, Donzé, Girard, Dang, Maler, Dreossi, Sankaranarayanan)
  - Decoupling disturbances (Chen, Herbert)
- Mathematical structure
  - Monotone systems (Sontag, Hafner, Del Vecchio, Arcak, Coogan)
  - LTL specifications (Kress-Gazit, Raman, Murray, Wongpiromsarn, Belta)
- Decompositions (Mitchell, Del Vecchio, Chen, Herbert, Grizzle, Ames, Tabuada)
- Machine learning (Lygeros, Djeridane, Niarchos, Seshia, Chen)

Learning a controller

Sinusoid + Yaw:

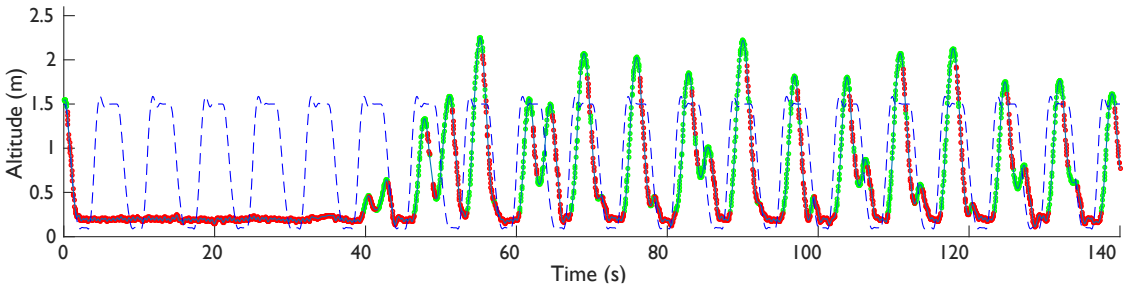
- Trained on each component separately
- Asked to fly combination
- Used Cascade FF neural net (ReLU), 2 layers, 3000 units

… but stay safe while learning

- **Safety:**
  - A nominal model with error bounds
  - Reachable sets computed to ensure safety in worst case
- **Performance:**
  - Use online learning to update model
  - Cost function used to generate control action within the safe set

Safe Policy Gradient Reinforcement Learning

The quadrotor first: drops



After about 1 minute,
it can roughly track the trajectory

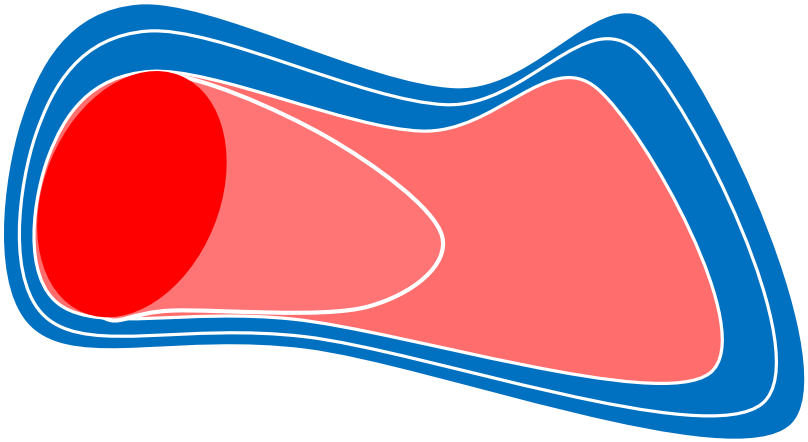
Soon, it starts experimenting

…but the safe controller steps in

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

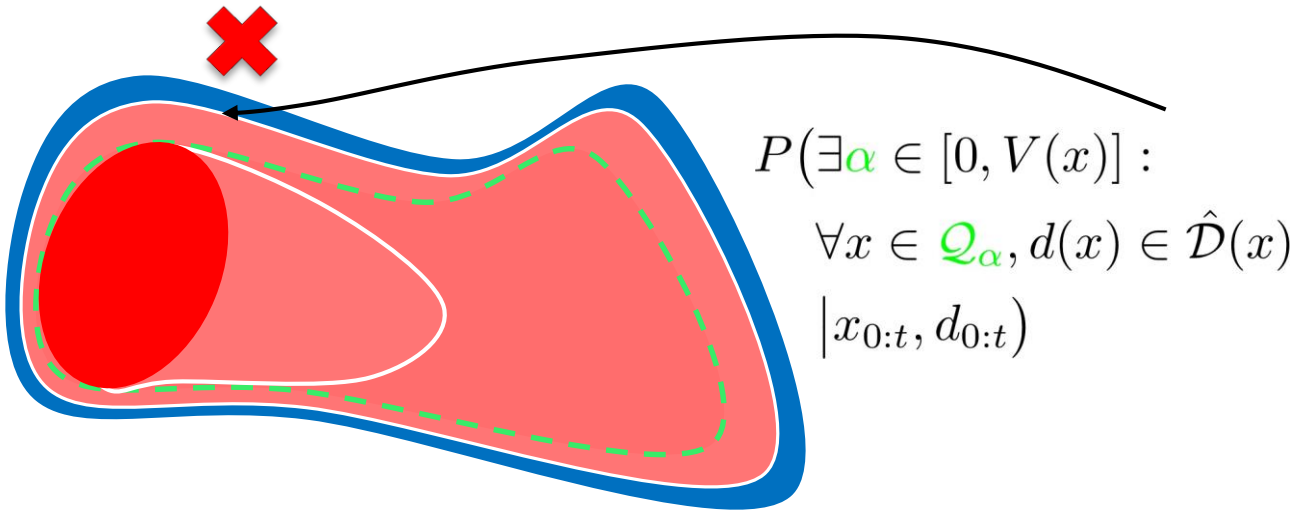
[PGSD: Kolter and Ng, 2009]

Online Safety Guarantee Validation



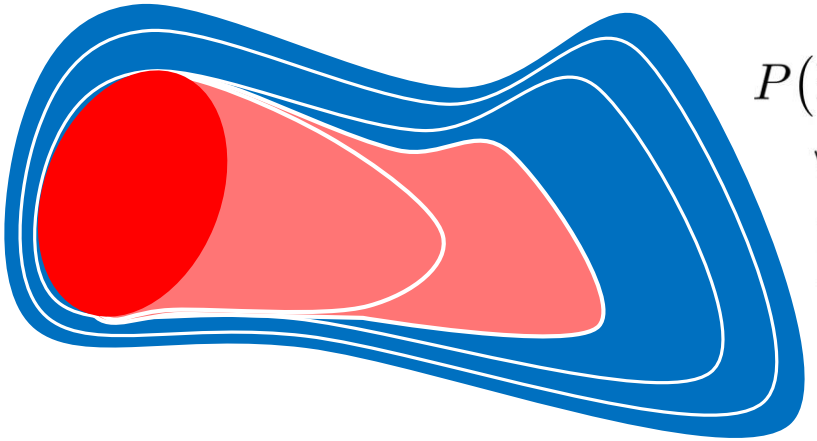
- Initialize active unsafe set = smallest candidate set

Online Safety Guarantee Validation



- Measure disturbance
- Compute Bayesian posterior on existence of a usable level set
- If posterior is low (weak safety guarantee), update unsafe set
- Update disturbance model

Online Safety Guarantee Validation

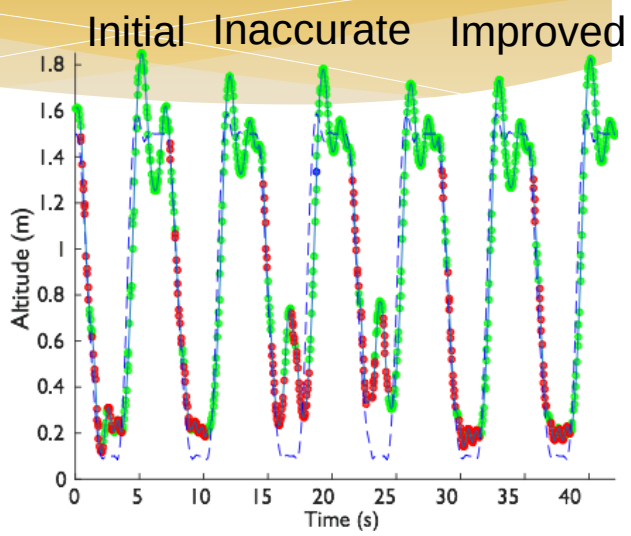


$$P\big(\exists \alpha \in [0, V(x)] : \forall x \in \mathcal{Q}_\alpha, d(x) \in \hat{\mathcal{D}}(x) \,\big|\, x_{0:t}, d_{0:t}\big)$$

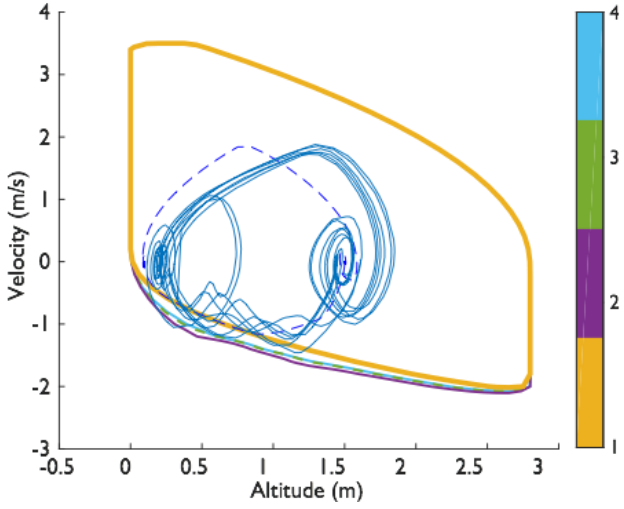
- Measure disturbance
- Compute Bayesian posterior on existence of a usable level set
- If posterior is low (weak safety guarantee), update unsafe set
- Update disturbance model

Safe Learning

First computed model is locally inaccurate



System detects inconsistency, slightly contracts safe set



Tracking resumes after a better model is computed

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS


Safe Learning
with online model validation
Berkeley
University of California

Research Challenges

* Models of unknown environments
* Scalability and compositional safety
* Safe exploration
* Sample efficiency: design-time vs operation-time
* Mixed initiative and collaborative learning
* Risk models

* Thanks: Kene Akametalu, Somil Bansal, Jaime Fisac
* FORCES: Max Balandat, Young Hwan Chang, Margaret Chapman, Roel Dobbe, David Fridovich-Keil, Qie Hu, Insoon Yang, Datong-Paul Zhou,