C2E2: Simulation-Based Verification of Hybrid Systems

Parasara Sridhar Duggirala, Chuchu Fan, Matthew Potok, Bolun Qi, Sayan Mitra, Mahesh Viswanathan

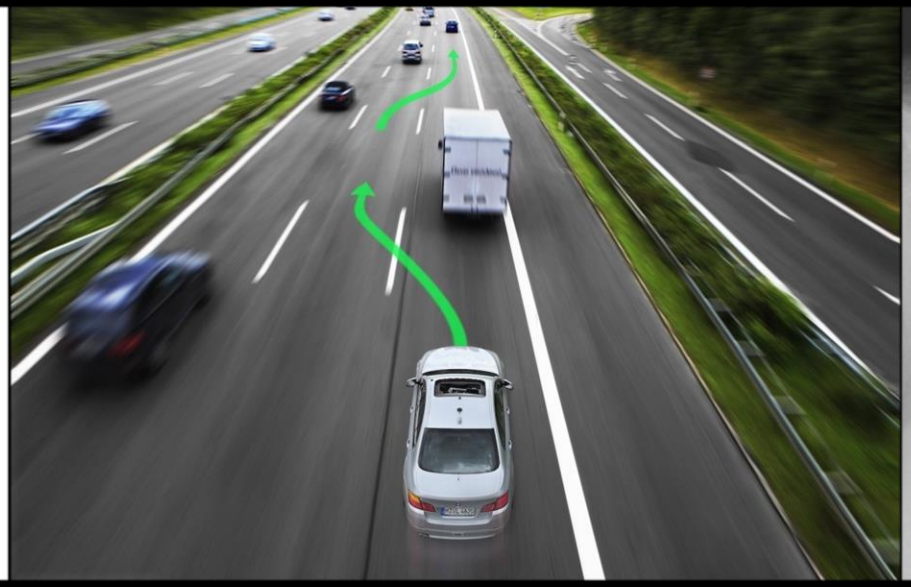
UCONN UNIVERSITY OF CONNECTICUT

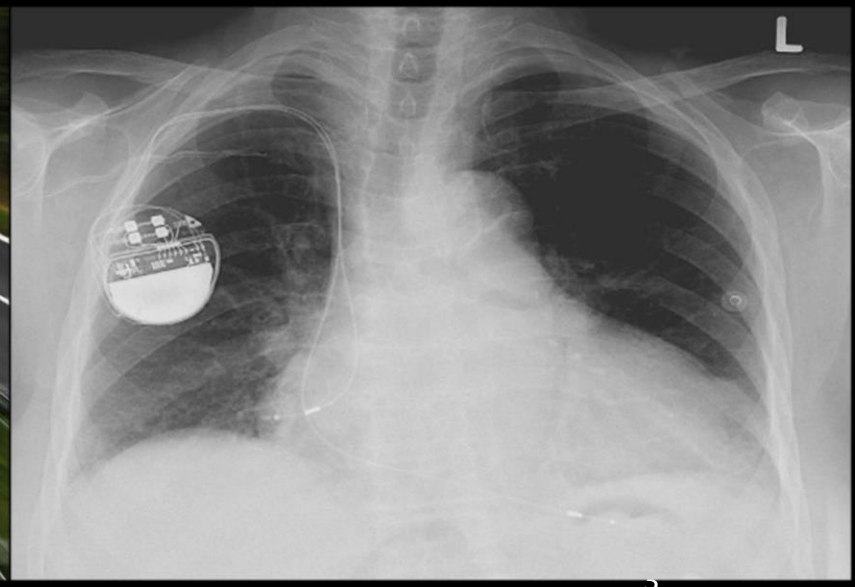
ILLINOIS UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Outline

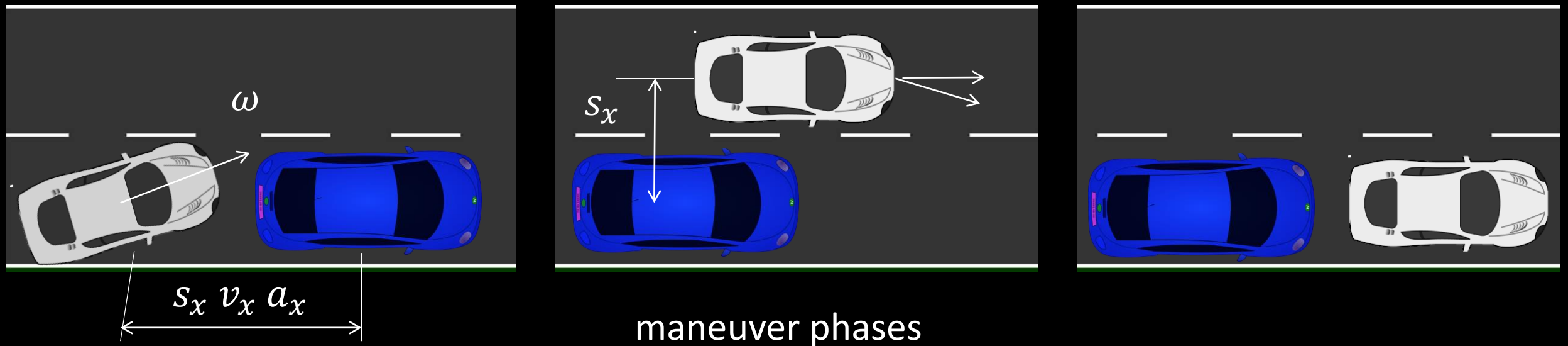
- CPS Verification – challenges
- C2E2 – simulation based verification technique for CPS verification
- Features of C2E2
- Demo

Safety verification problems in CPS

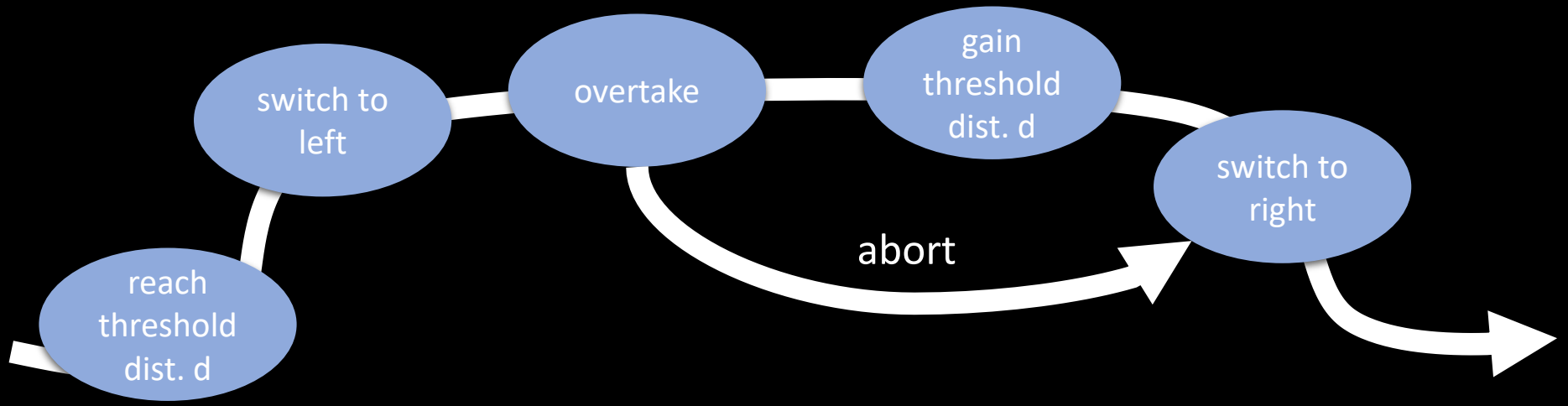




Auto-passing system



maneuver phases

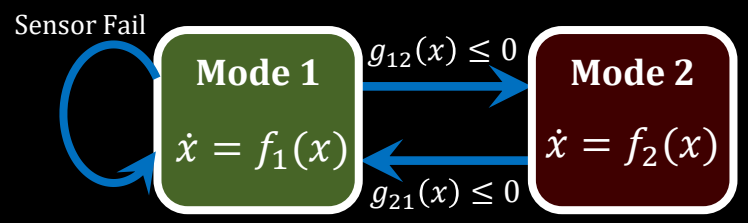


Safety verification problem of ODEs

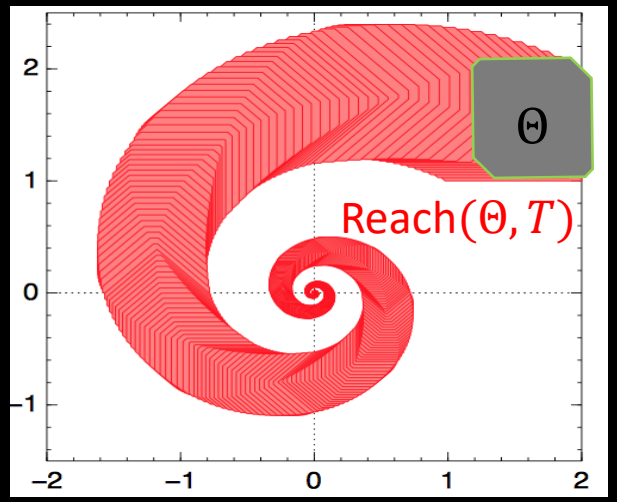
Consider an nonlinear ODE model $\dot{x} = f(x)$, $x \in \mathbb{R}^n$

Discrete transitions

Reach(Θ, T): states reachable from initial set $\Theta \subseteq \mathbb{R}^n$ up to time T



Safety verification problem: given initial set Θ, unsafe set U, time bound T, decide whether Reach$(\Theta, \infty) \cap \mathrm{U} = \emptyset$



Safety verification is undecidable in general [Henzinger et al., 95]

Bounded time verification with over-approximation in existing tools:

Linear dynamics: PHAVer [Frehse 05], SpaceEx [Frehse 11], d/dt [Asarin 01],

Nonlinear dynamics: Flow* [Chen 12], etc.

C2E2: bounded time verification for nonlinear hybrid systems

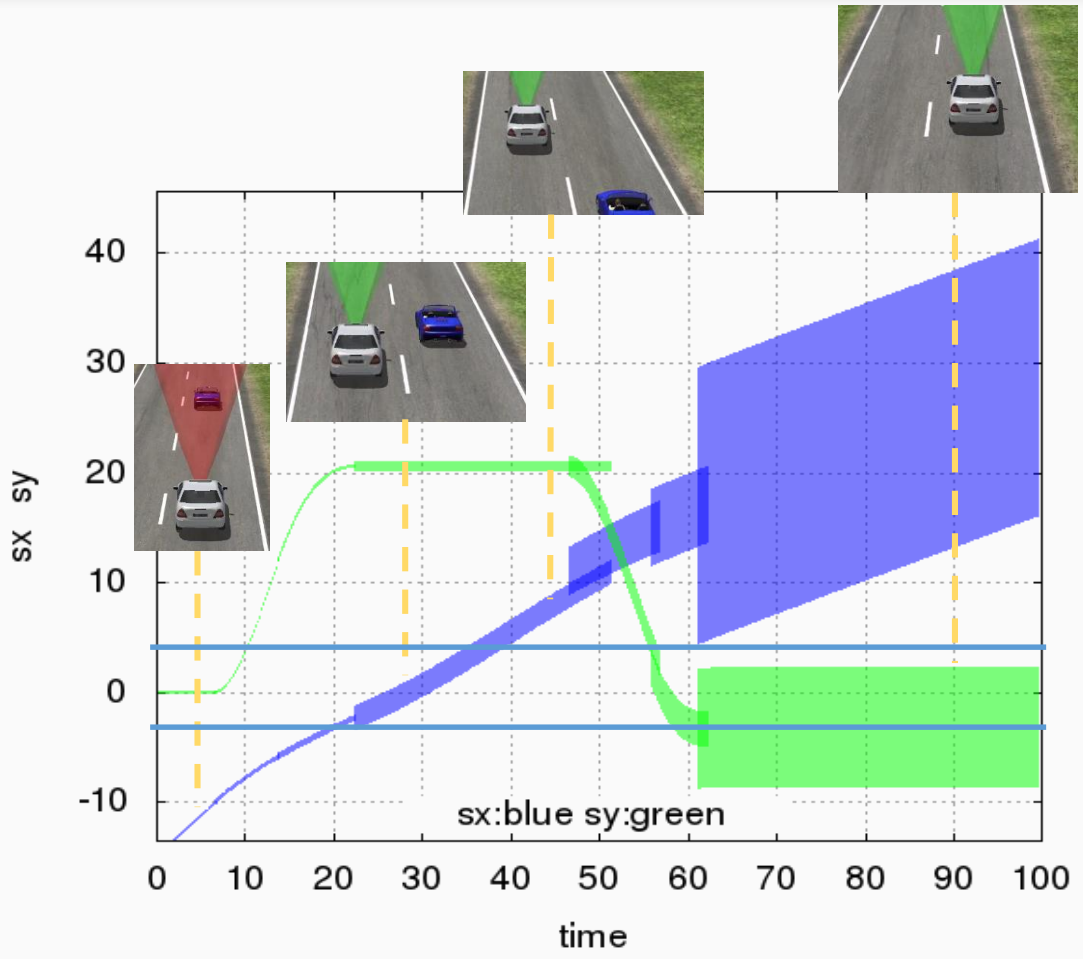
Simulation-driven approach

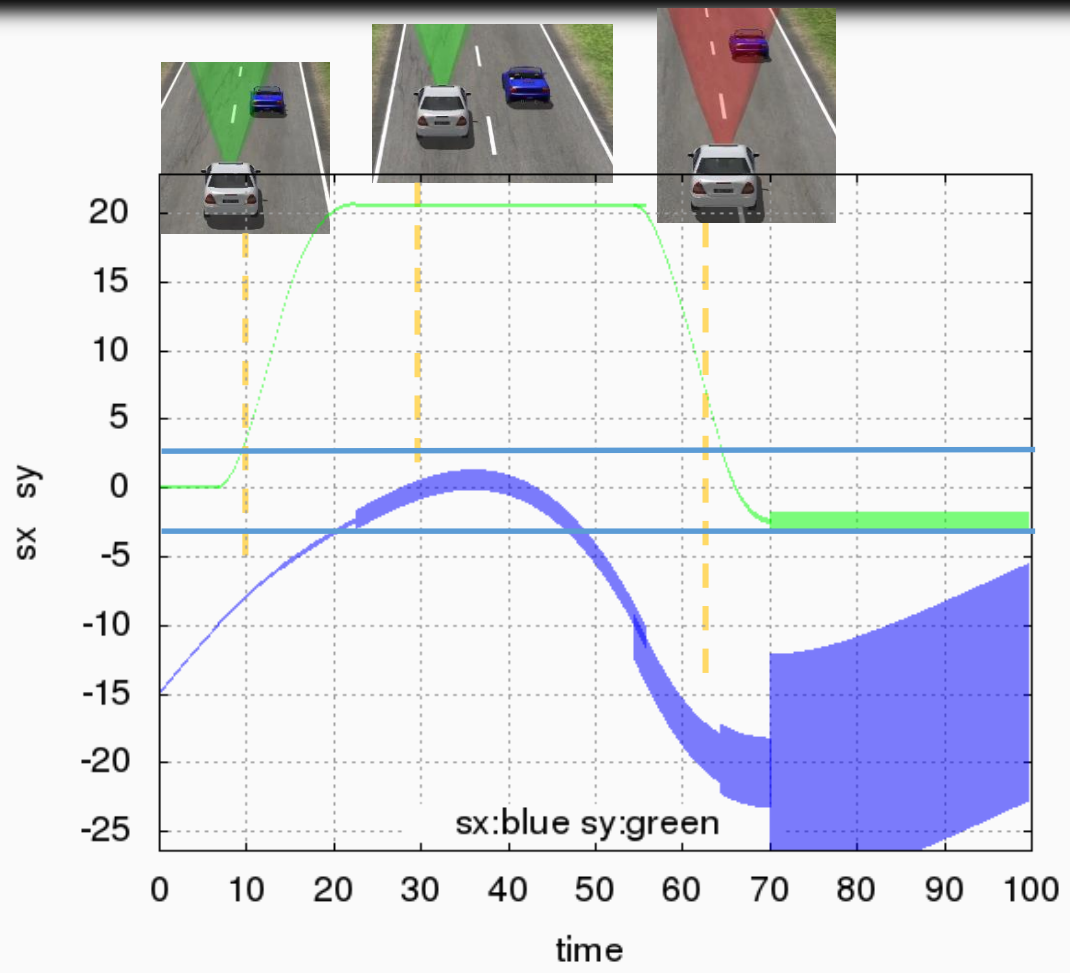
Provides soundness and relative completeness guarantees

Automatic simulation-driven strategy

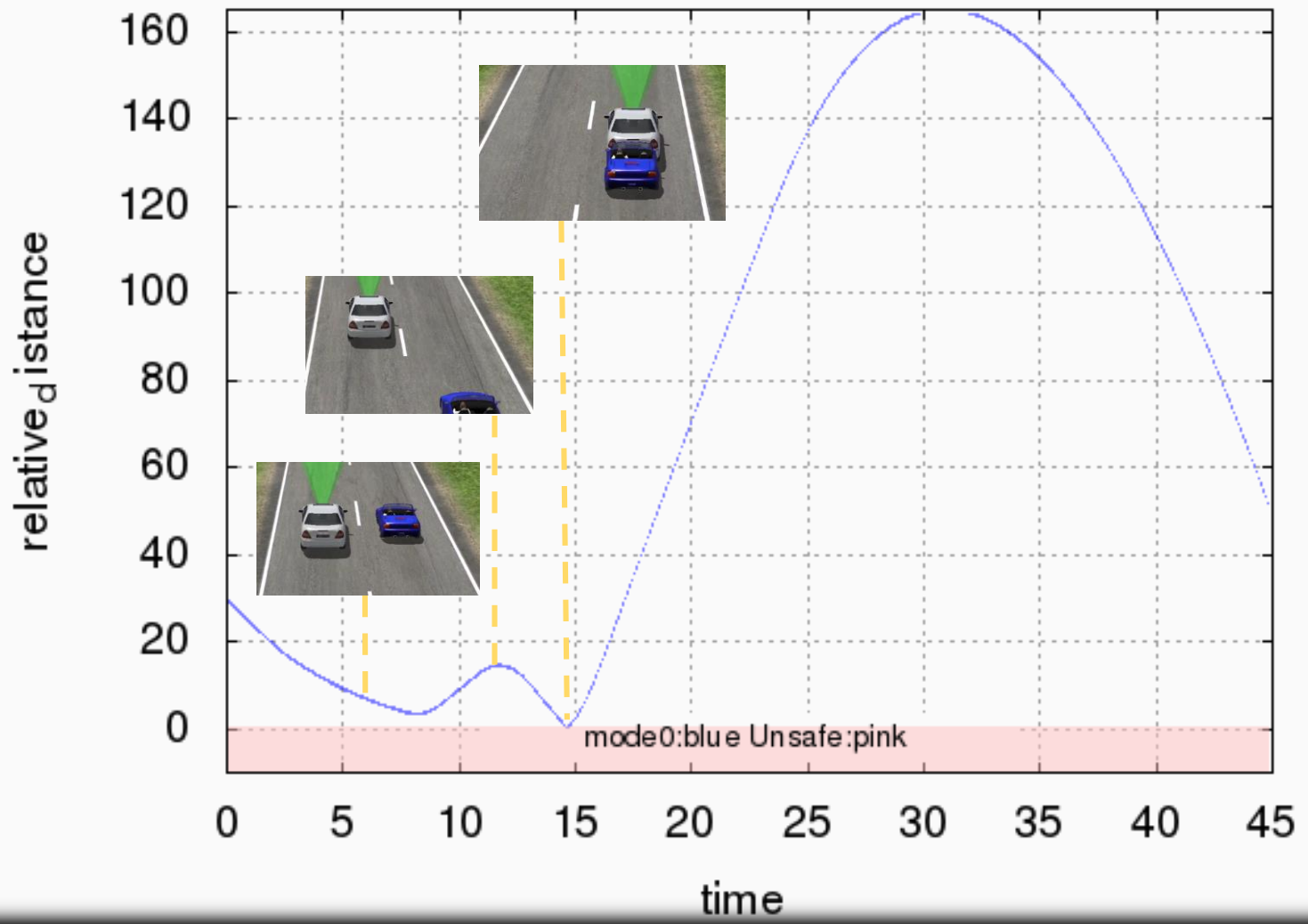
- Given start Θ and unsafe U
- Compute finite cover of initial set
- Simulate from the center x_0 of each cover
- **Bloat** simulation so that bloated tube contains trajectories from the cover
- Union = over-approximation of reach set
- Check intersection/containment with U and refine

Verification of auto-passing system





Auto-passing system – counter-example



New features in C2E2

Usability improvement

- Automatic reachability with piece-wise on-the-fly discrepancy algorithm

Efficiency improvement

- Automatic detection and handling of different classes dynamics
  - Global discrepancy function for linear dynamics $\dot{x} = Ax$
  - On-the-fly discrepancy for nonlinear dynamics $\dot{x} = f(x)$
  - Special handling of constant dynamics $\dot{x} = k$

New testing scripts and a command line interface

Demo

1. Website, downloading, and installation instructions.
2. C2E2 usability features.
3. Verification, results, and visualizations.
   - Cardiac cell
   - Autonomous vehicle passing
   - Powertrain control system
   - Robotic arms
4. Reachable sets, other data.

Conclusion

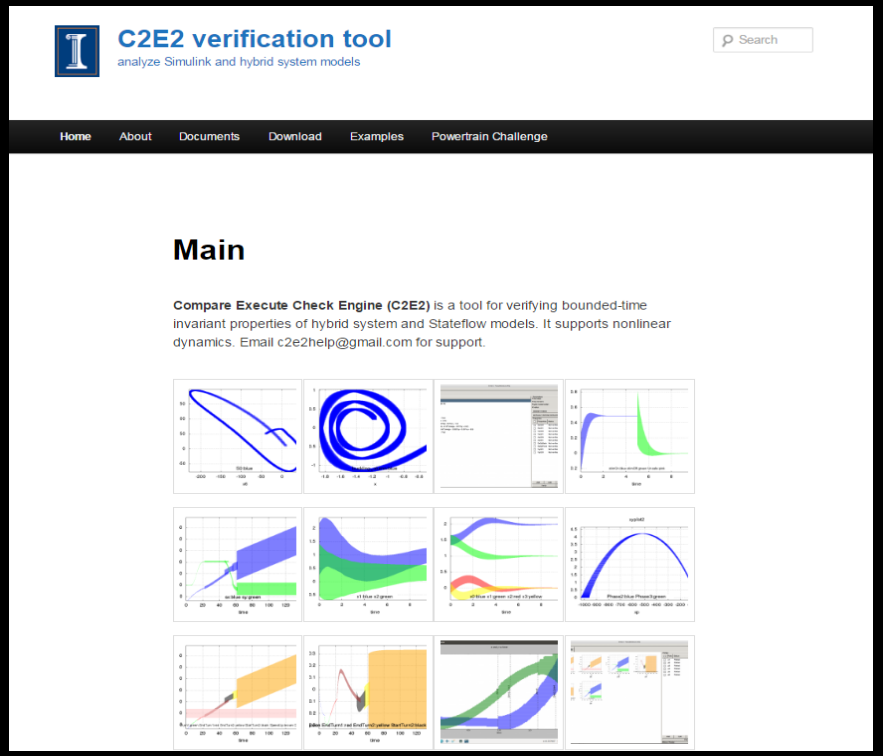
Simulation-driven verification can be used for safety analysis of CPS

- Automatic reachability analysis
- Provides *soundness* and *relative completeness*

C2E2: our invariant verification tool for hybrid systems is able to solve some hard problems--try it

Check out more examples at the C2E2 webpage

- **https://publish.illinois.edu/c2e2-tool/**



Questions?

Send an email to **psd@uconn.edu**, **cfan10@Illinois.edu** or **c2e2help@gmail.com**