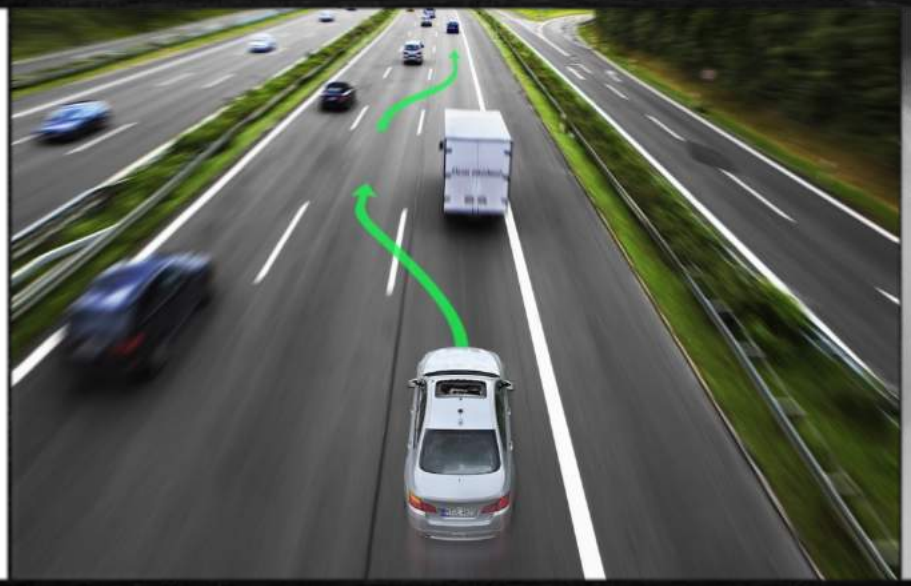
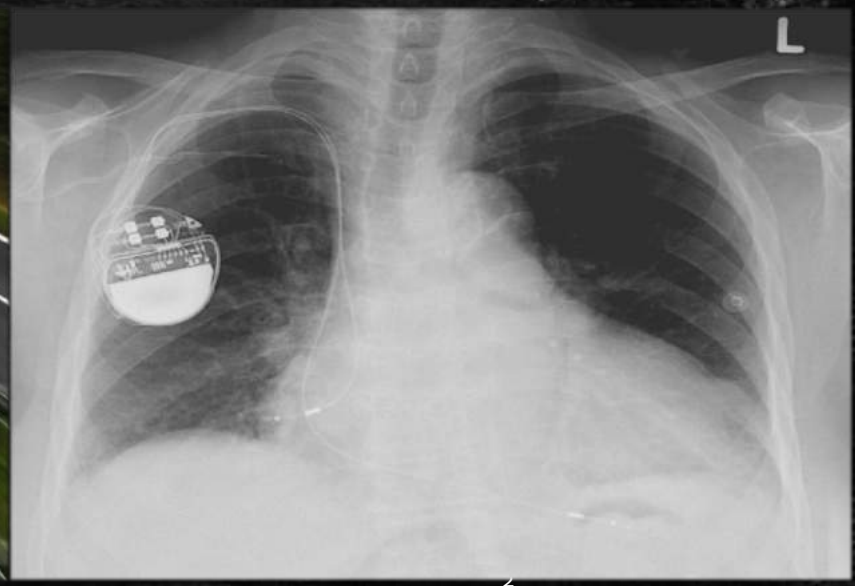
Automatic Reachability Analysis for Nonlinear Hybrid Models with C2E2

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

ILLINOIS
1867
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Safety verification problems in CPS





Inside look at the design process of CPS

- Control systems are designed using tools like MathWorks Simulink
- A typical model of a powertrain control systems [Jin 15]:

Closed loop Dynamics

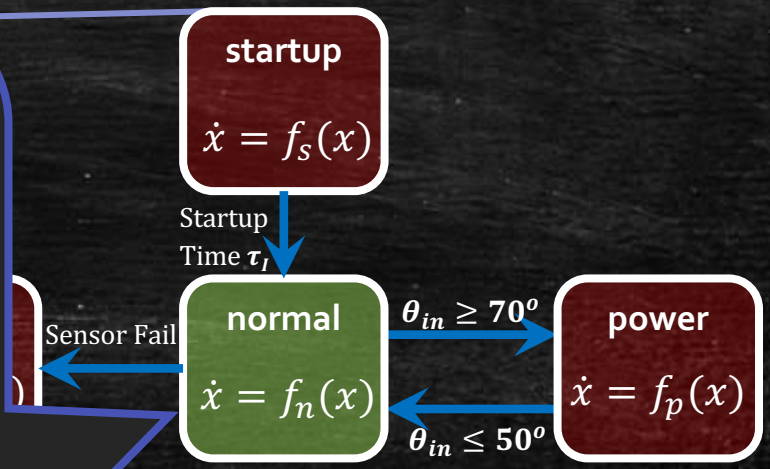
$$\dot{\theta} = 10(\theta_{in} - \theta)$$

$$\dot{p} = c_1(2\theta(c_{20}p^2 + c_{21}p + c_{22}) - c_{12}(c_2 + c_3\omega p + c_4\omega p^2 + c_5\omega^2 p))$$

$$\dot{\lambda} = c_{26}(c_{15} + c_{16}c_{25}F_c + c_{17}c_{25}^2F_c^2 + c_{18}\dot{m}_c + c_{19}\dot{m}_c c_{25}F_c - \lambda)$$

$$\dot{p_e} = c_1\left(2c_{23}\theta(c_{20}p^2 + c_{21}p + c_{22}) - (c_2 + c_3\omega p + c_4\omega p^2 + c_5\omega^2 p)\right)$$

$$i = c_{14}(c_{24}\lambda - c_{11})$$

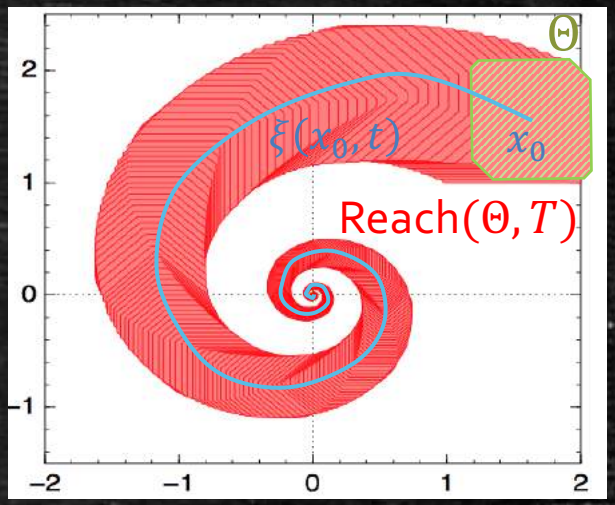


Safety Verification Problem of ODEs

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

Solution $\xi(x_0, t)$: state at time t from initial state x_0

Reach(Θ, T): all 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$(\Theta, \infty) \cap U = \emptyset$

Brief history of safety verification:

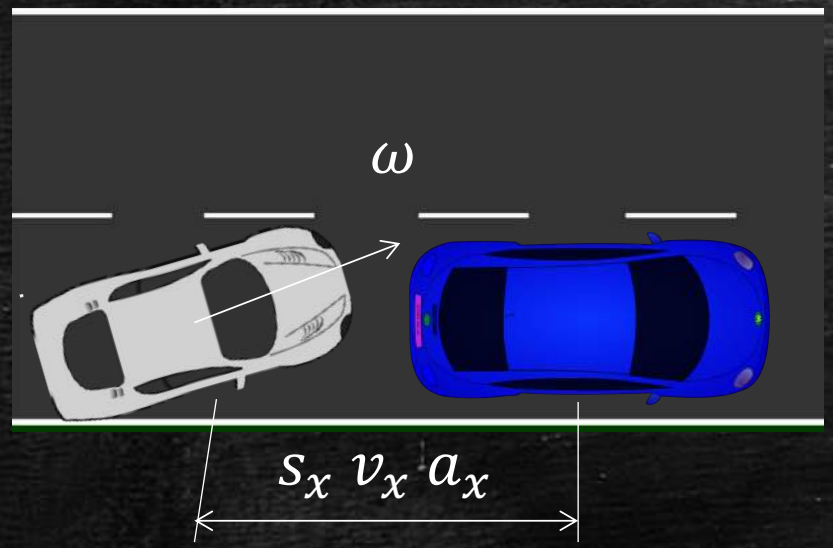
- Undecidable in general, even for rectangular dynamics, [Henzinger et al., 95]
- Bounded time verification for linear dynamics with over-approximation in existing tools: PHAVer [Frehse 05], SpaceEx [Frehse 11], d/dt [Asarin 01], Flow* [Chen 12], etc.
- Recent focus on nonlinear dynamics; our approach simulation-driven

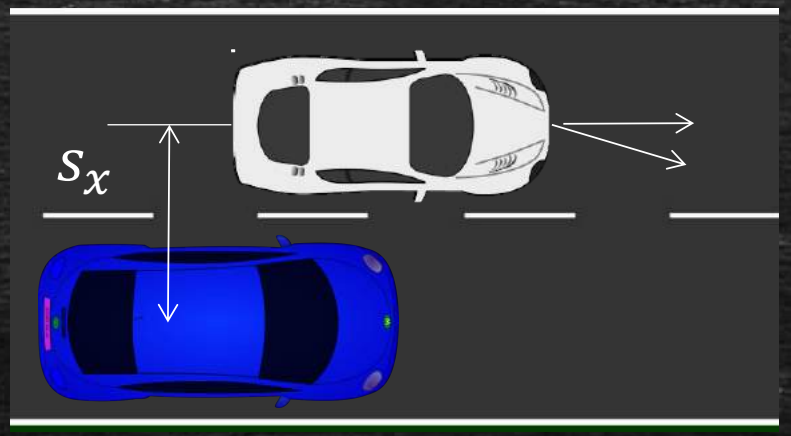
A Simple (Often The Only) Simulation-driven Strategy

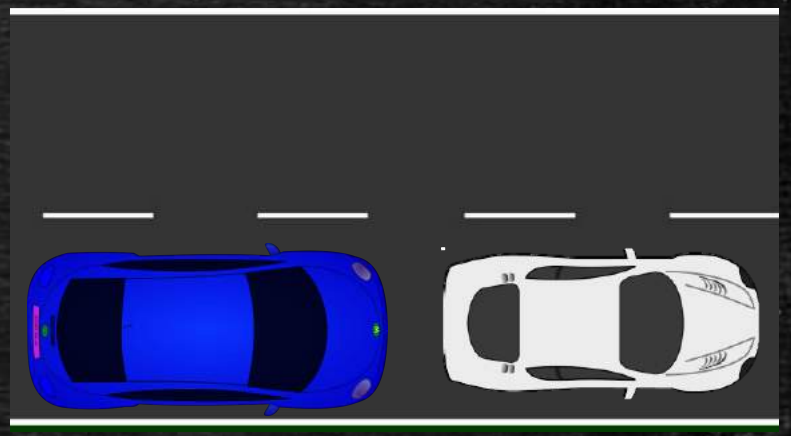
- Given start Θ and unsafe U
- Compute finite cover of initial set
- Simulate from the center x_0 of each cover
- **Bloat** simulation so that bloated tube contains all trajectories from the cover
- Union = over-approximation of reach set
- Check intersection/containment with U
- Refine

- ***Demo of the tool***

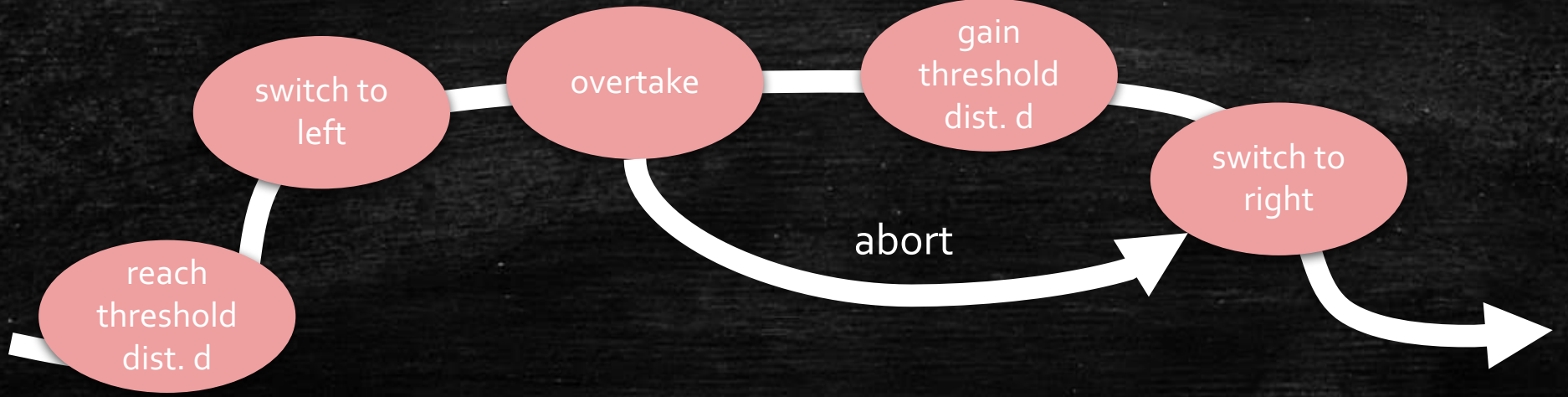
Auto-passing system



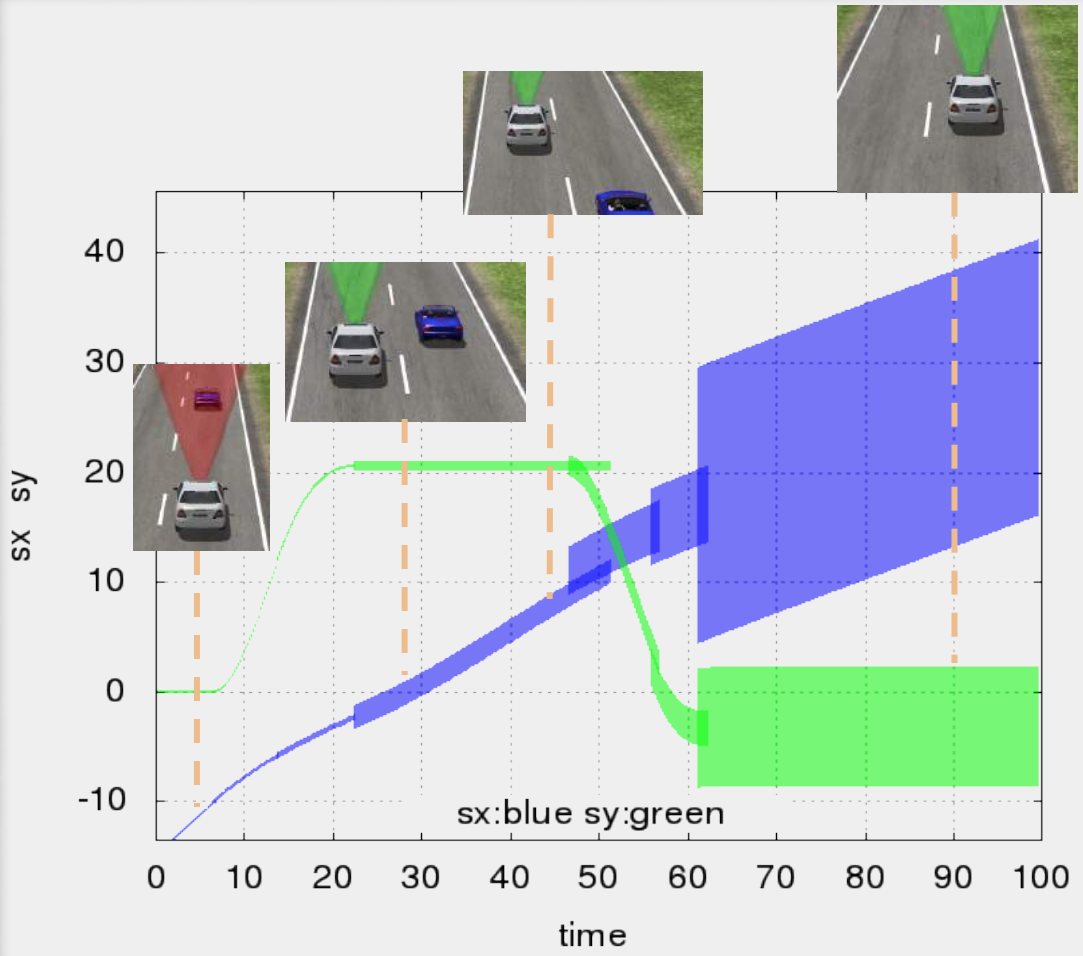


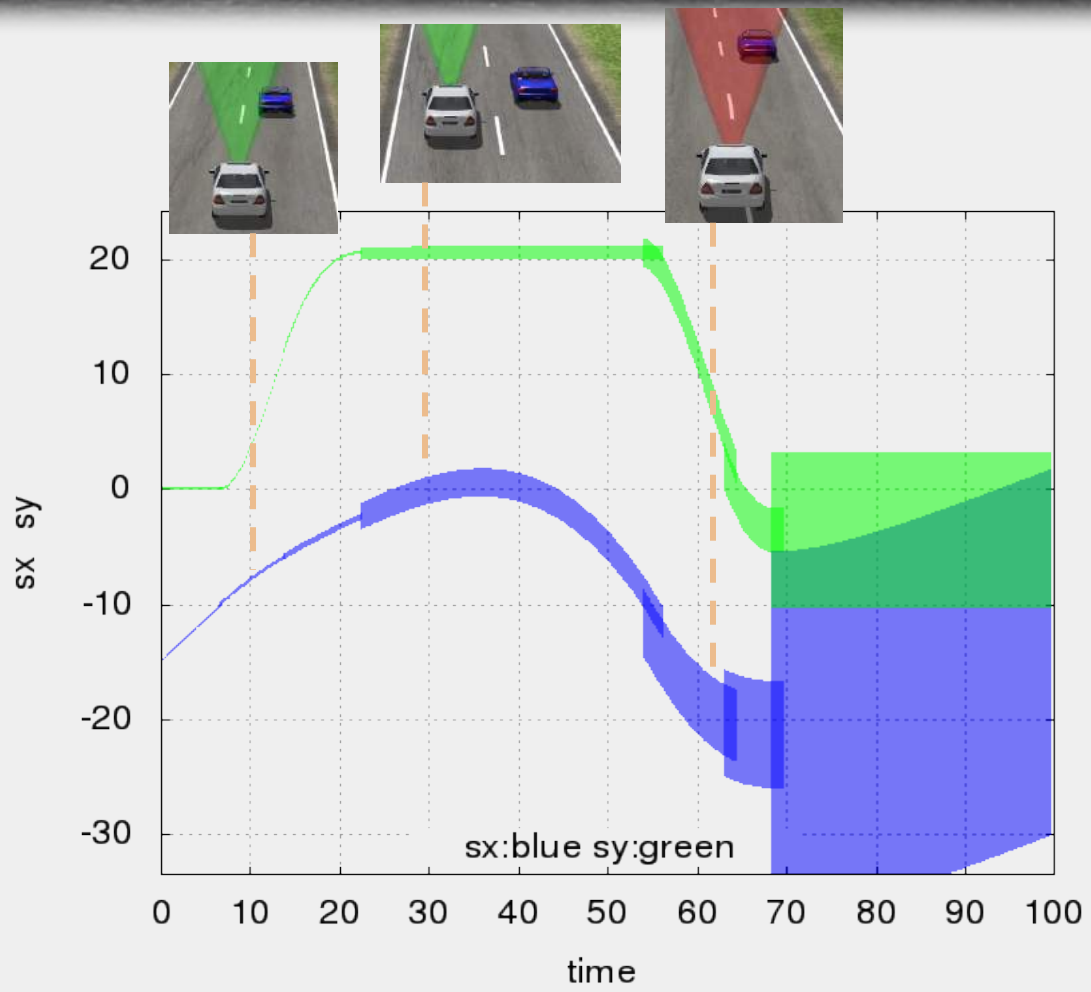


maneuver phases

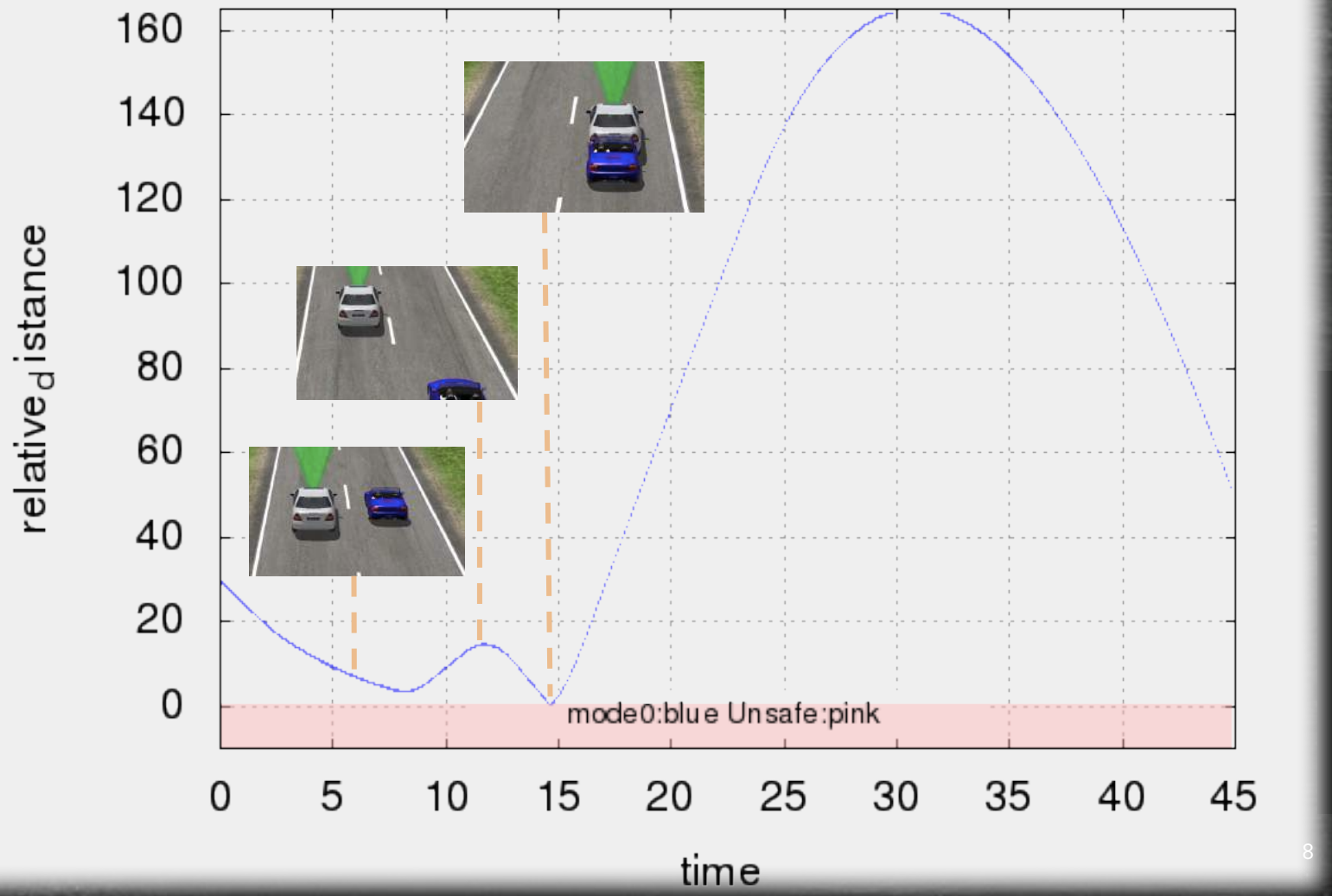


Auto-passing system





Auto-passing system – counter example



New features

Usability improvement*

- Automatic reach set computation using piece-wise on-the-fly discrepancy algorithm

Efficiency improvement

- Automatic check and handling of linear and nonlinear dynamics
  - Global discrepancy function for linear dynamics
  - On-the-fly discrepancy for nonlinear dynamics with coordinate transformation
- Automatic handling of constant dynamics

Others

- Testing script for installation checking
- Command line interface

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

- A promising tool that solves challenging problems---try it

Check out more examples at the C2E2 webpage

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