Analyse fonctionnelle des systèmes cyber-physiques avec incertitudes

Goran Frehse

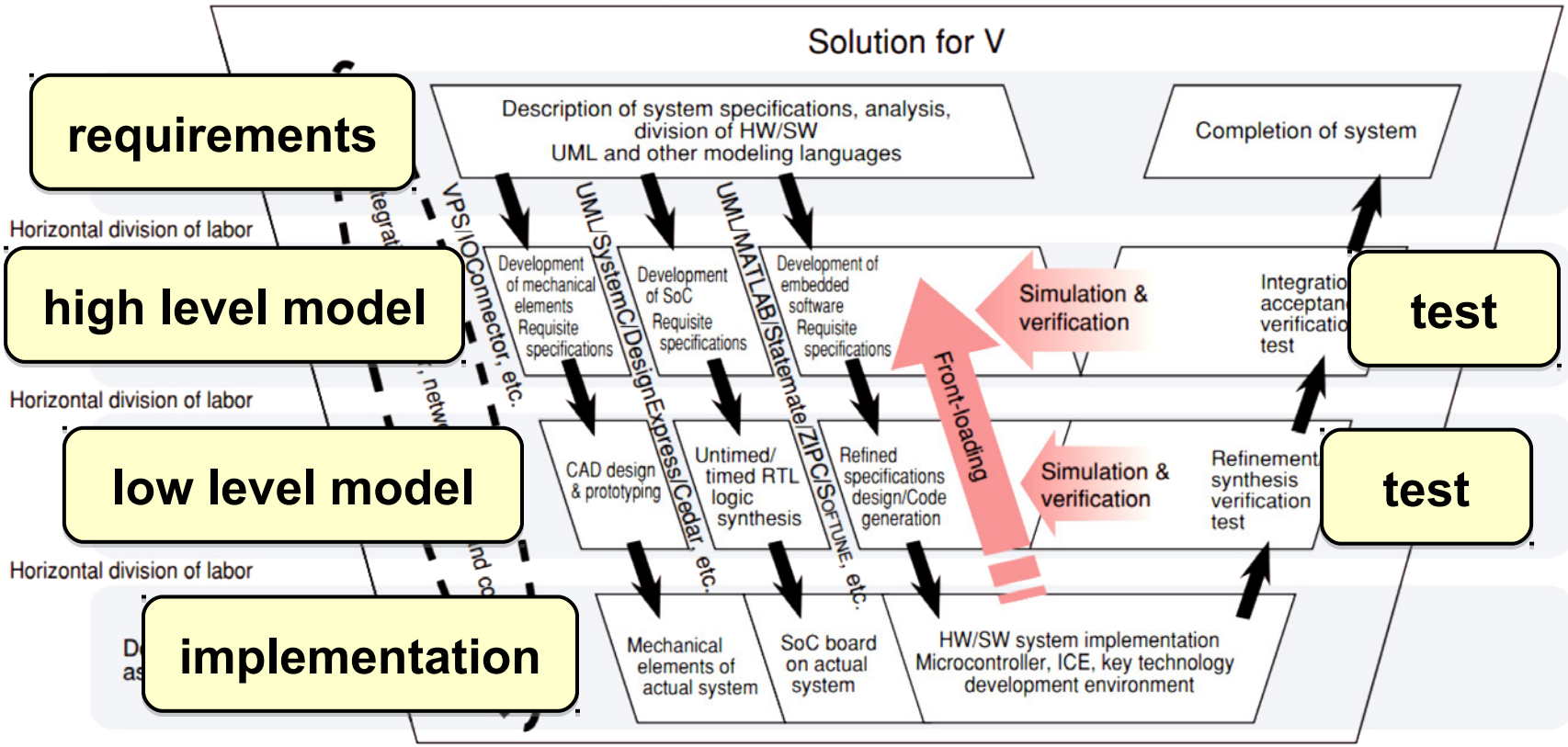
Univ. Grenoble Alpes / CNRS – Verimag, France

Forum Méthodes Formelles
Toulouse, 10 octobre, 2017

Outline

- Verification in Model Based Development
- Template Reachability in SpaceEx
- Applications
- Conclusions and Perspectives

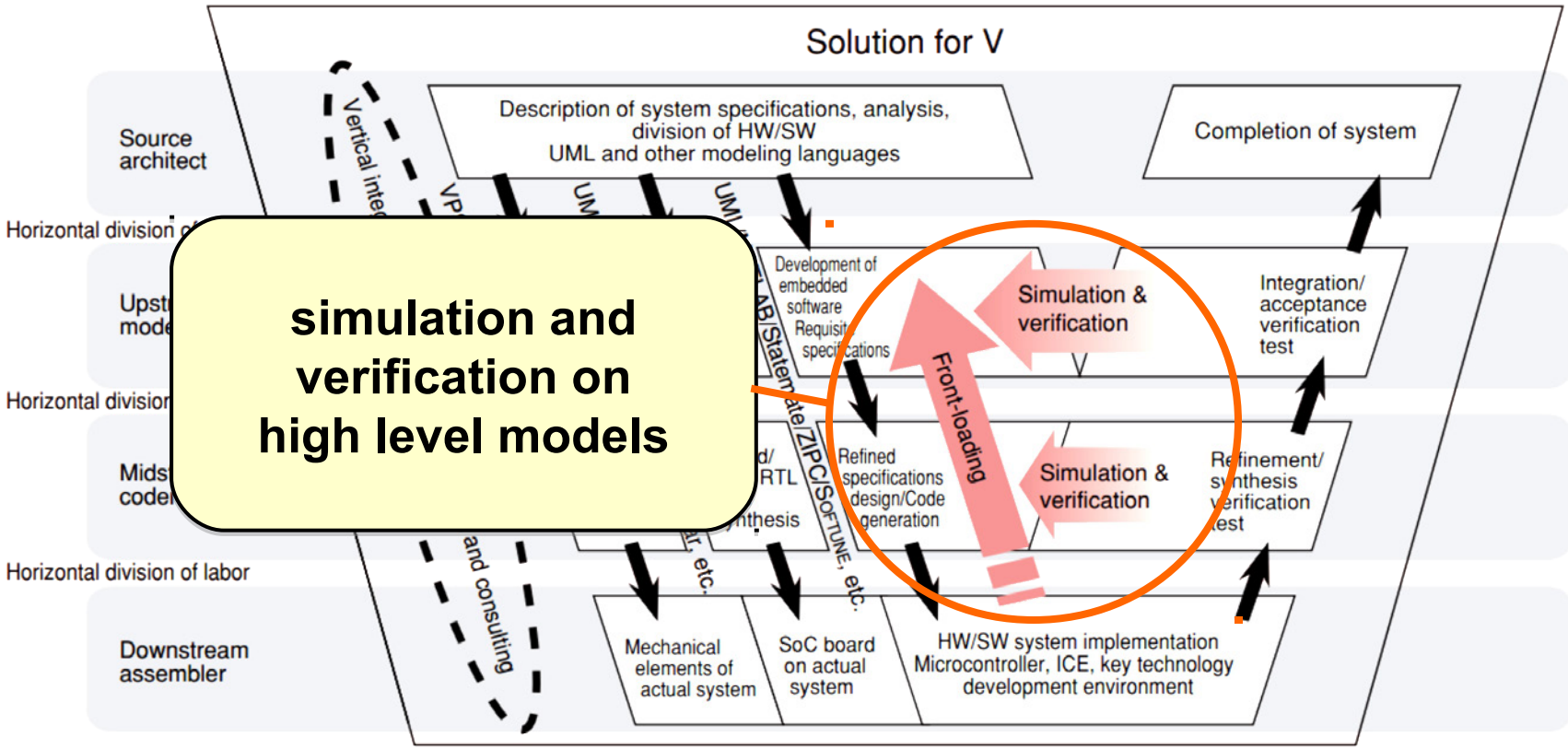
Model-Based Development



Development Vision for Systems Mixing Software, Circuits and Mechanics (Fujitsu 2006)

http://www.fujitsu.com/downloads/EDG/binary/pdf/find/24-1e/2.pdf

Model-Based Development



Development Vision for Systems Mixing Software, Circuits and Mechanics (Fujitsu 2006)

http://www.fujitsu.com/downloads/EDG/binary/pdf/find/24-1e/2.pdf

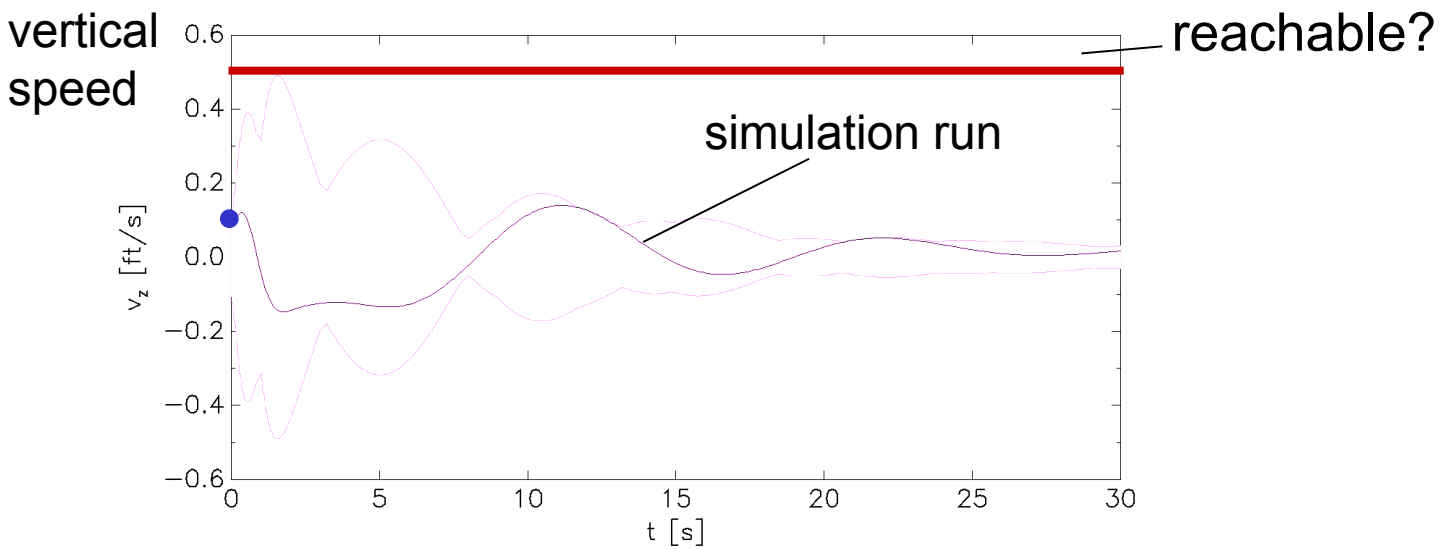
Example: Controlled Helicopter

- **28-dim model of a Westland Lynx helicopter**
  - 8-dim model of flight dynamics
  - 20-dim continuous H∞ controller for disturbance rejection
  - stiff, highly coupled dynamics

S. Skogestad and I. Postlethwaite, Multivariable Feedback Control: Analysis and Design. John Wiley & Sons, 2005.

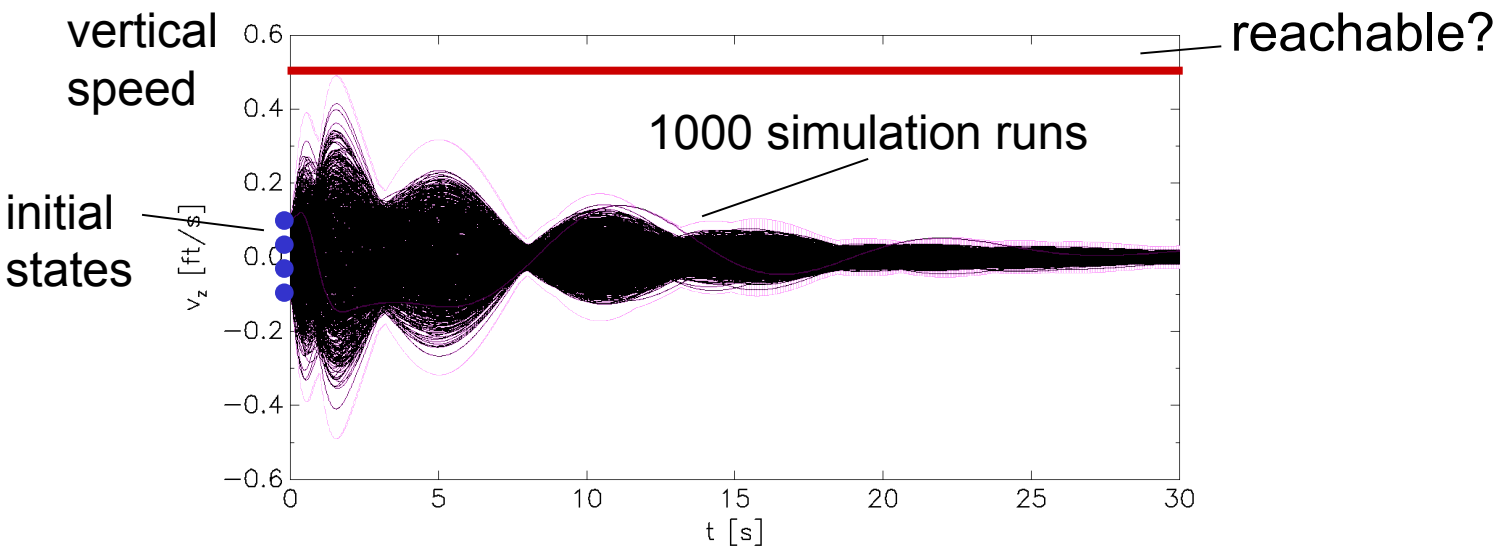
Simulation vs Reachability

- **Simulation**
  - **single** behavior



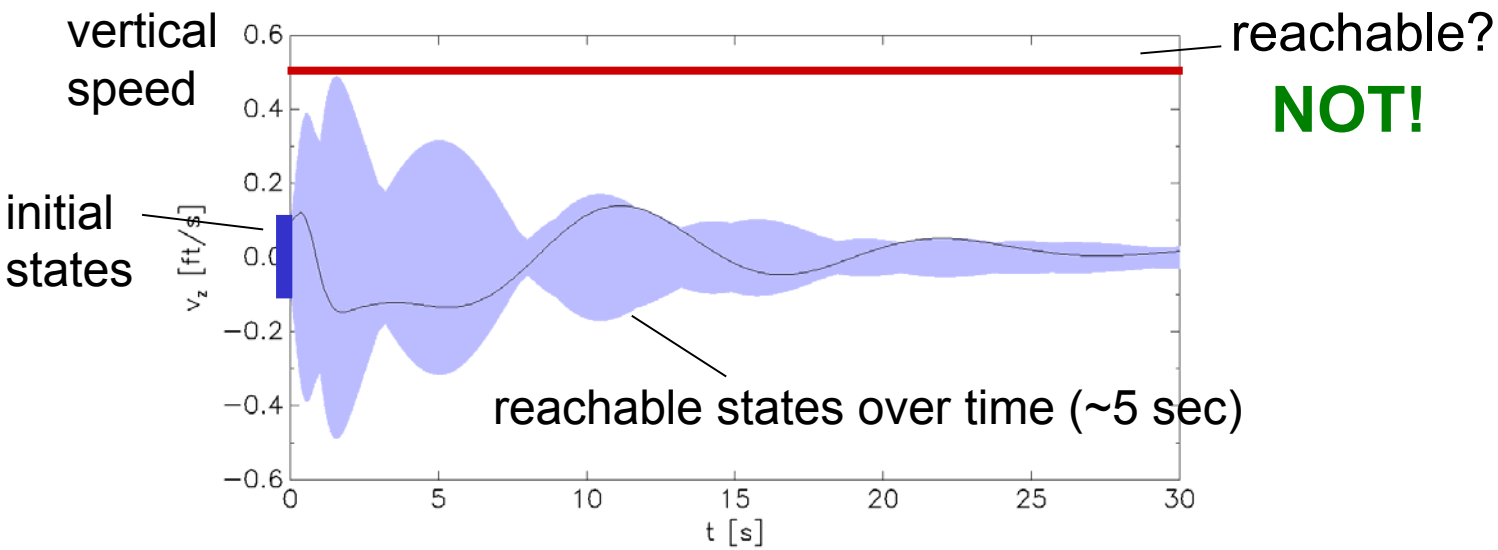
Simulation vs Reachability

- **Simulation**
  - **single** behavior



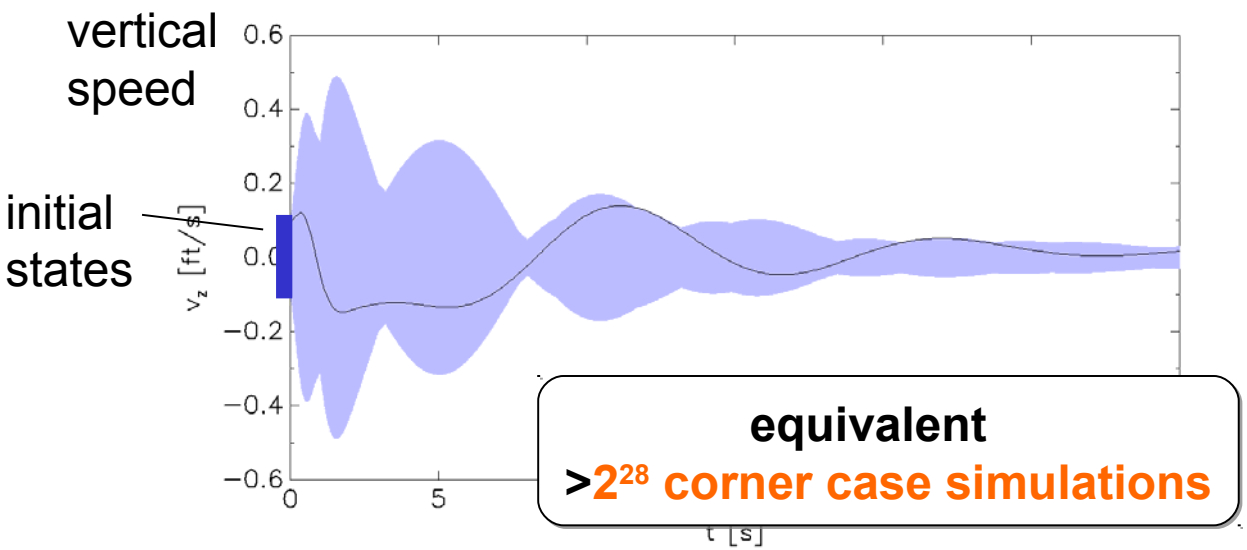
Simulation vs Reachability

- **Simulation**
  - **single** behavior
- **Reachability**
  - cover of **all** behaviors



Simulation vs Reachability

- **Simulation**
  - deterministic
    - resolve nondet. using Monte Carlo etc.
  - scalable for nonlinear dyn.
- **Reachability**
  - **nondeterministic**
    - continuous disturbances...
    - implementation tolerances...
  - scalable for linear dynamics



Simulation vs Reachability

- **corner case simulation: check all extreme points**
  - n variables, T time steps
  - initial set given by intervals = 2^n vertices
  - inputs given by intervals = 2^n vertices

$$2^n \, (2^n)^T \text{ trajectories}$$

initial set **inputs** **time steps**

Simulation vs Reachability

- **corner case simulation: check all extreme points**
  - n variables, T time steps
  - initial set given by intervals = 2^n vertices
  - inputs given by intervals = 2^n vertices

$$\mathbf{2^n\,(2^n)^T}\ \textbf{trajectories}$$

- **template reachability (interval enclosure):**

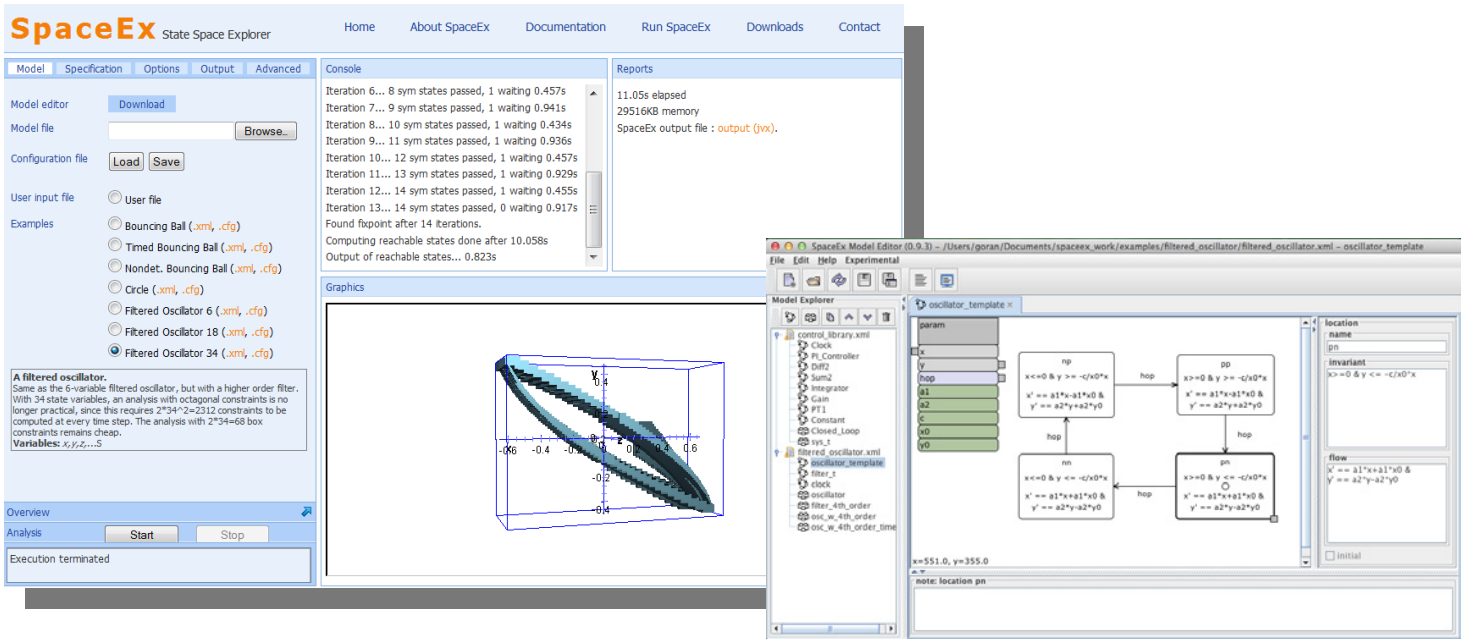
$$\mathbf{T}\ O(\mathbf{n}^3)\ \textit{operations}$$

Outline

- Verification in Model Based Development
- **Template Reachability in SpaceEx**
- Applications
- Conclusions and Perspectives

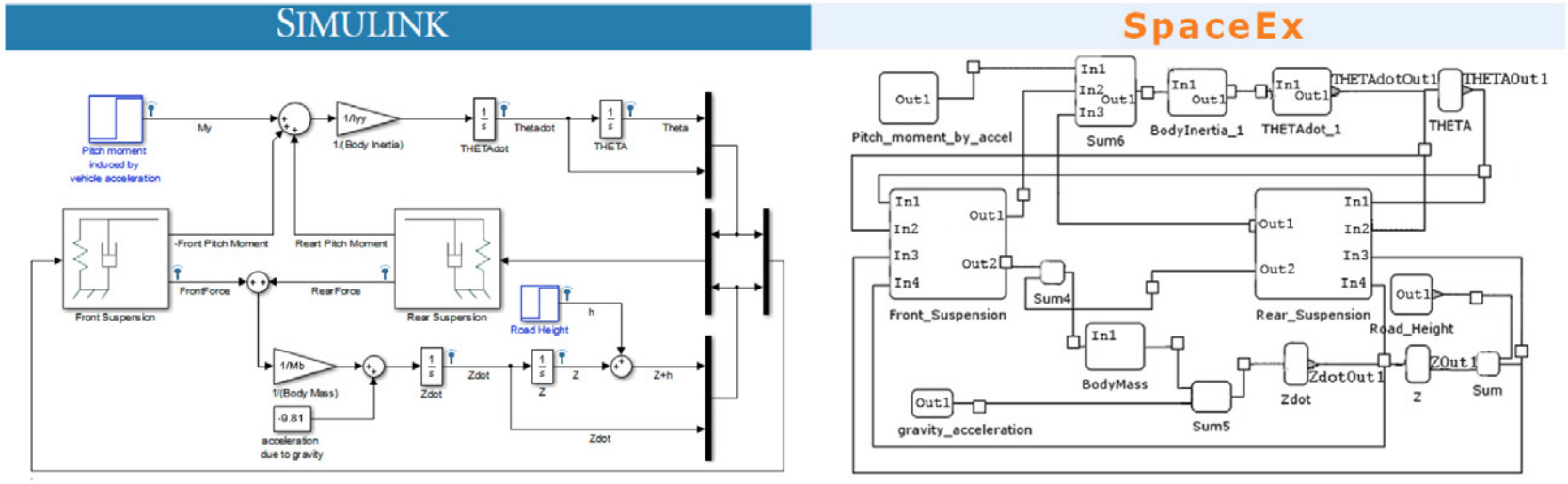
SpaceEx Verification Platform

- **reachability, monitoring, simulation**
  ADHS'09, ICTSS'11, CAV '11
- **open source: spaceex.imag.fr**



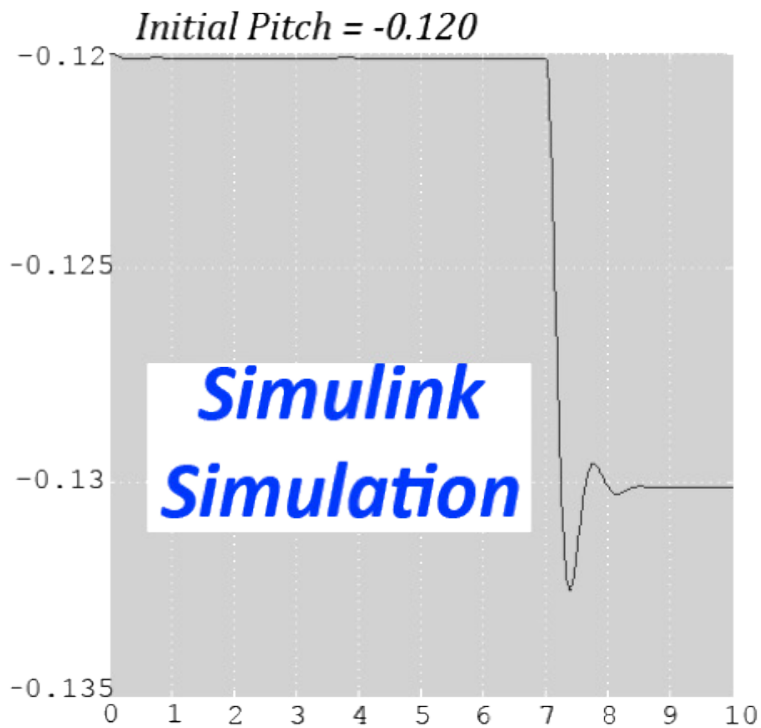
SL2SX: Translating Simulink to SpaceEx

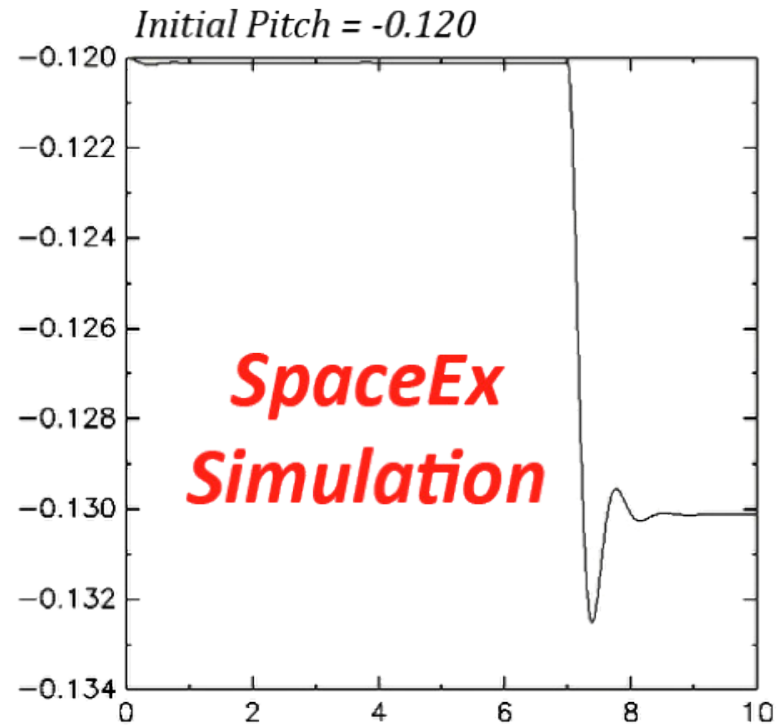
- **semi-automatic, gentle subset of Simulink**
  - continuous time linear blocks
  - steps, switches, etc.



Automotive Suspension from Simulink Example Library

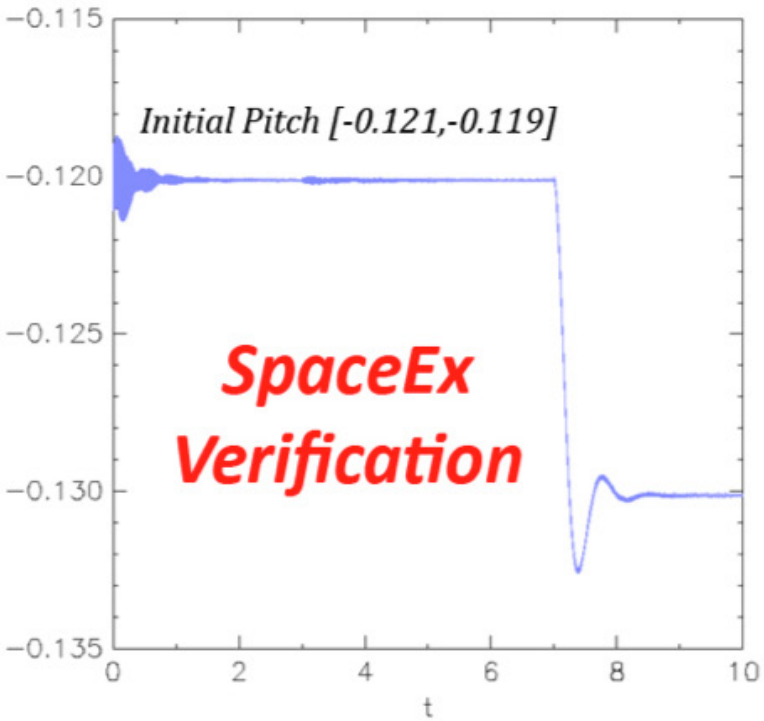
SL2SX: Translating Simulink to SpaceEx

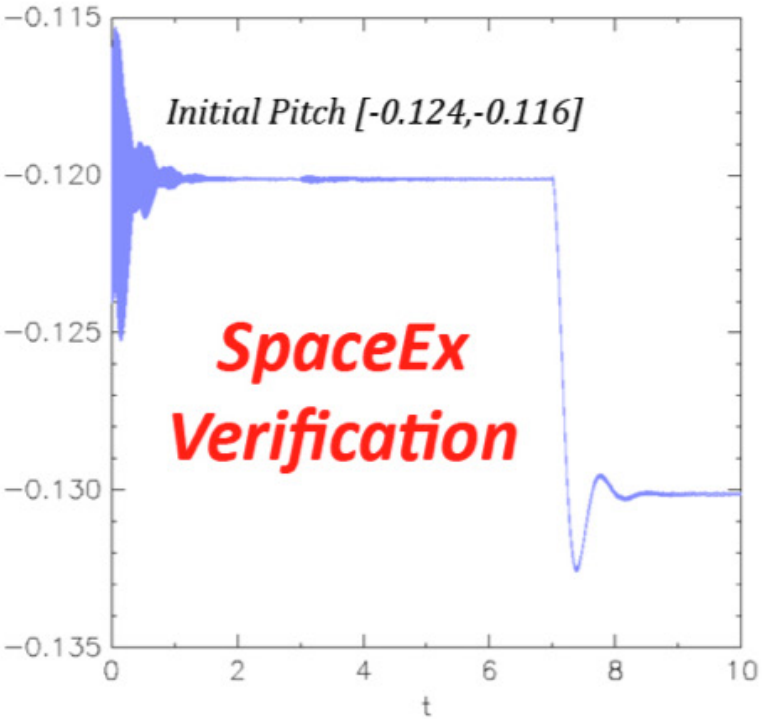




Automotive Suspension from Simulink Example Library

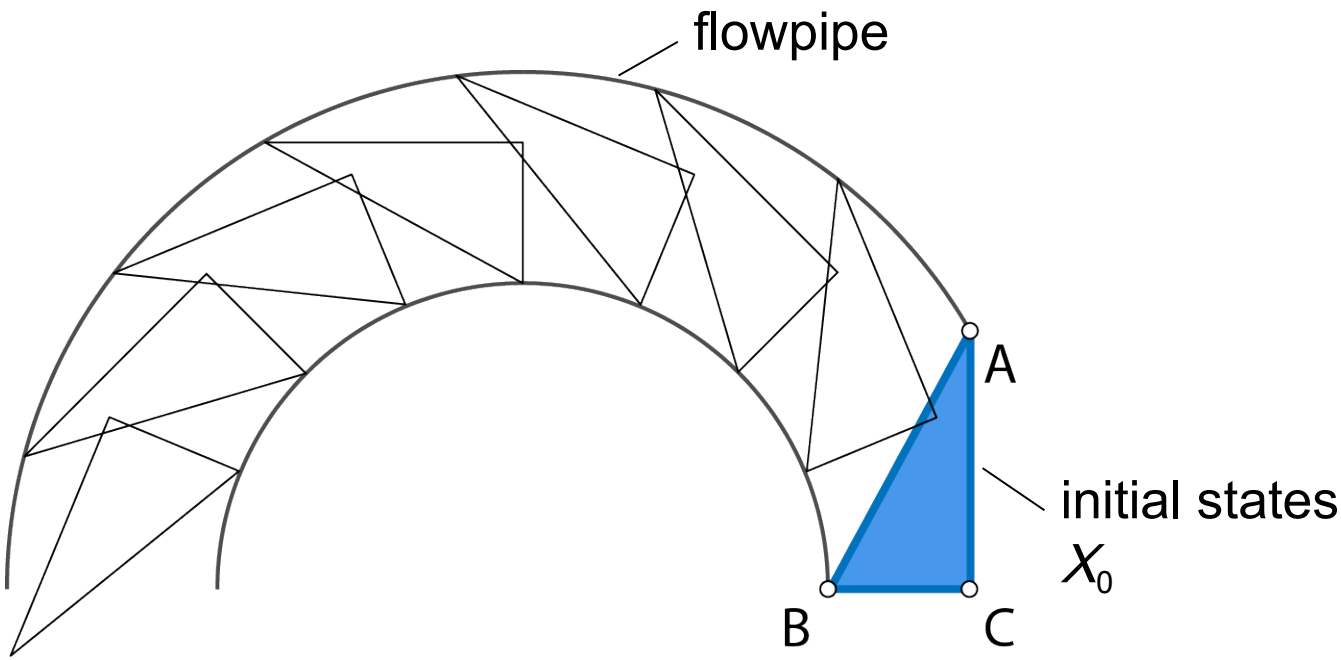
SL2SX: Translating Simulink to SpaceEx





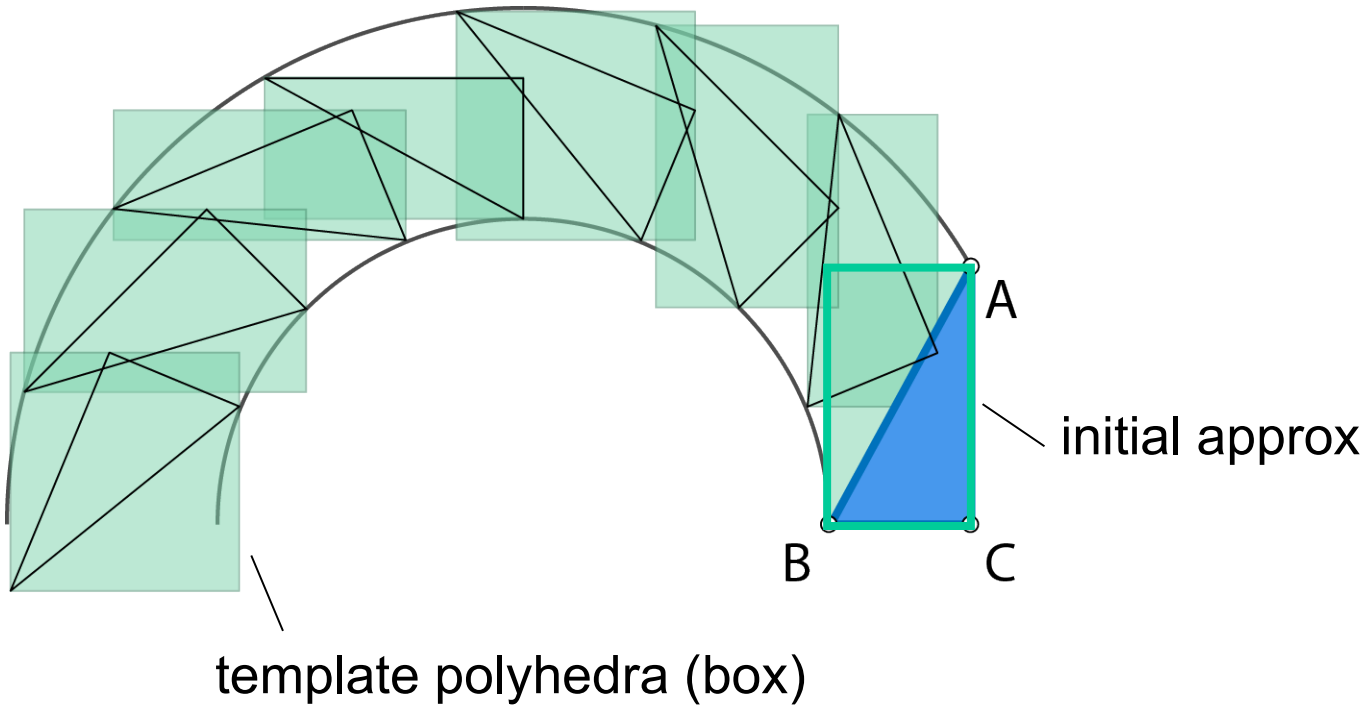
Automotive Suspension from Simulink Example Library

Reachable States over Time



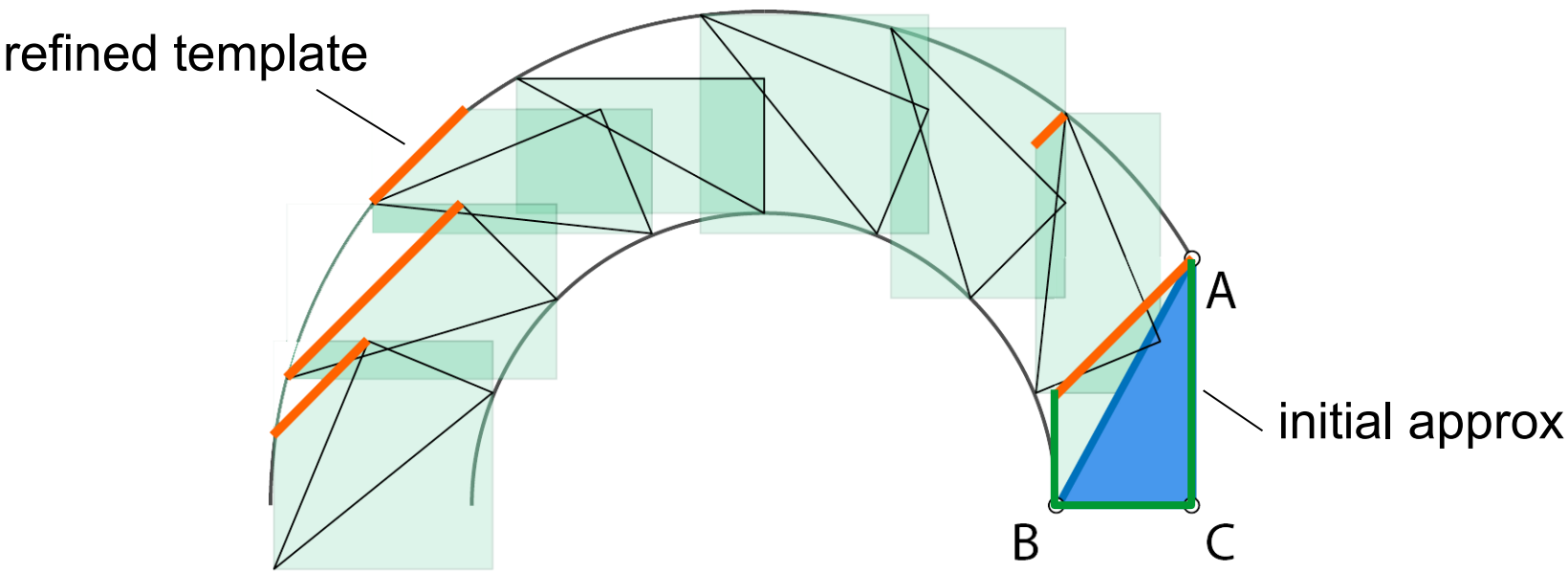
$$\dot{x}(t) = Ax(t) + u(t),$$
$$x(0) \in \mathcal{X}_0, u(t) \in \mathcal{U}.$$

Template Reachability



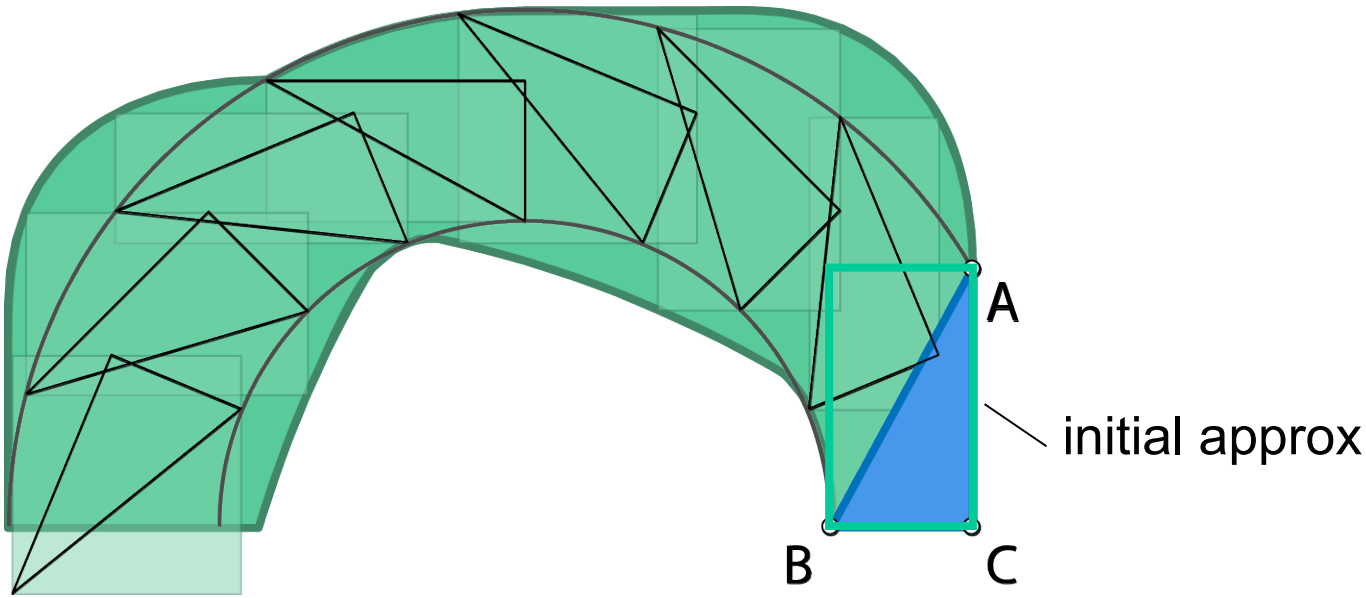
Girard and Le Guernic, 2008

Template Reachability



Girard and Le Guernic, 2008

Template Reachability

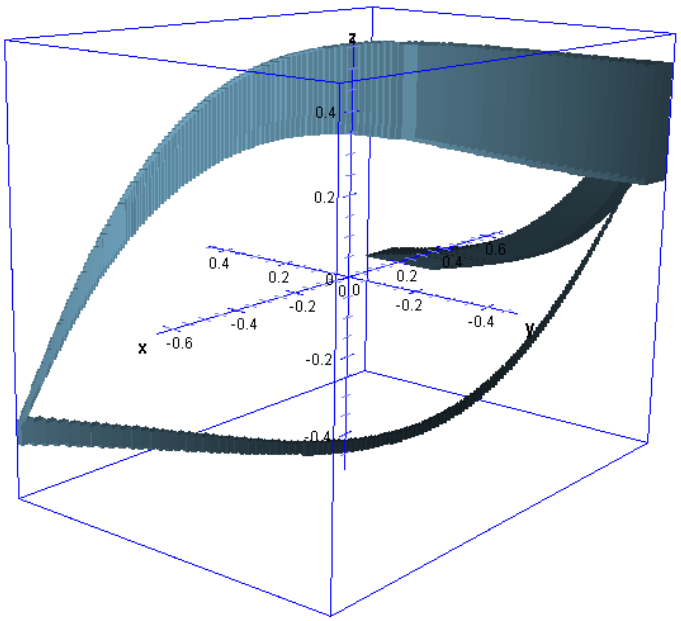


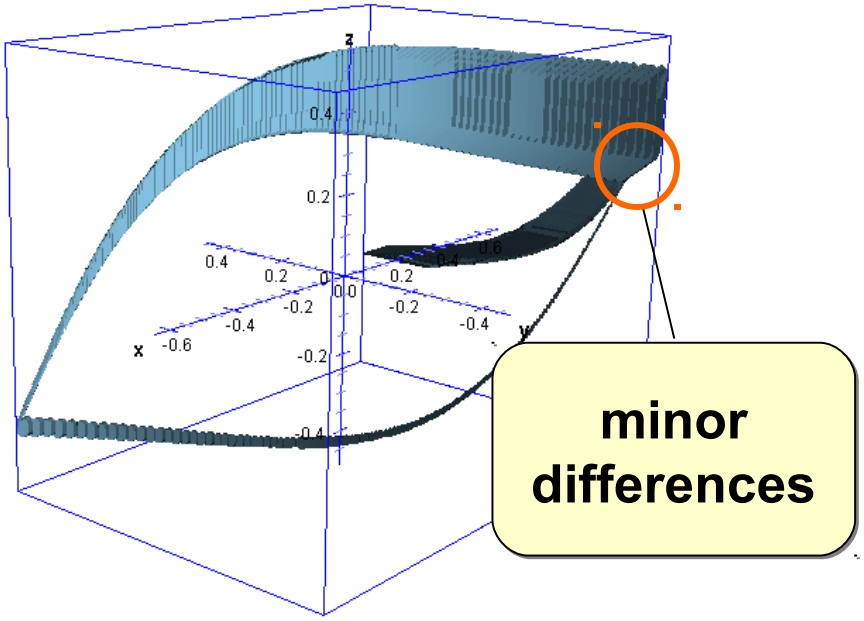
- extended over intervals of time (convex hull+bloating)
- approximation error bounded

Example: Switched Oscillator

CAV'11

- **Low number of directions sufficient?**
  - here: 6 state variables





box directions

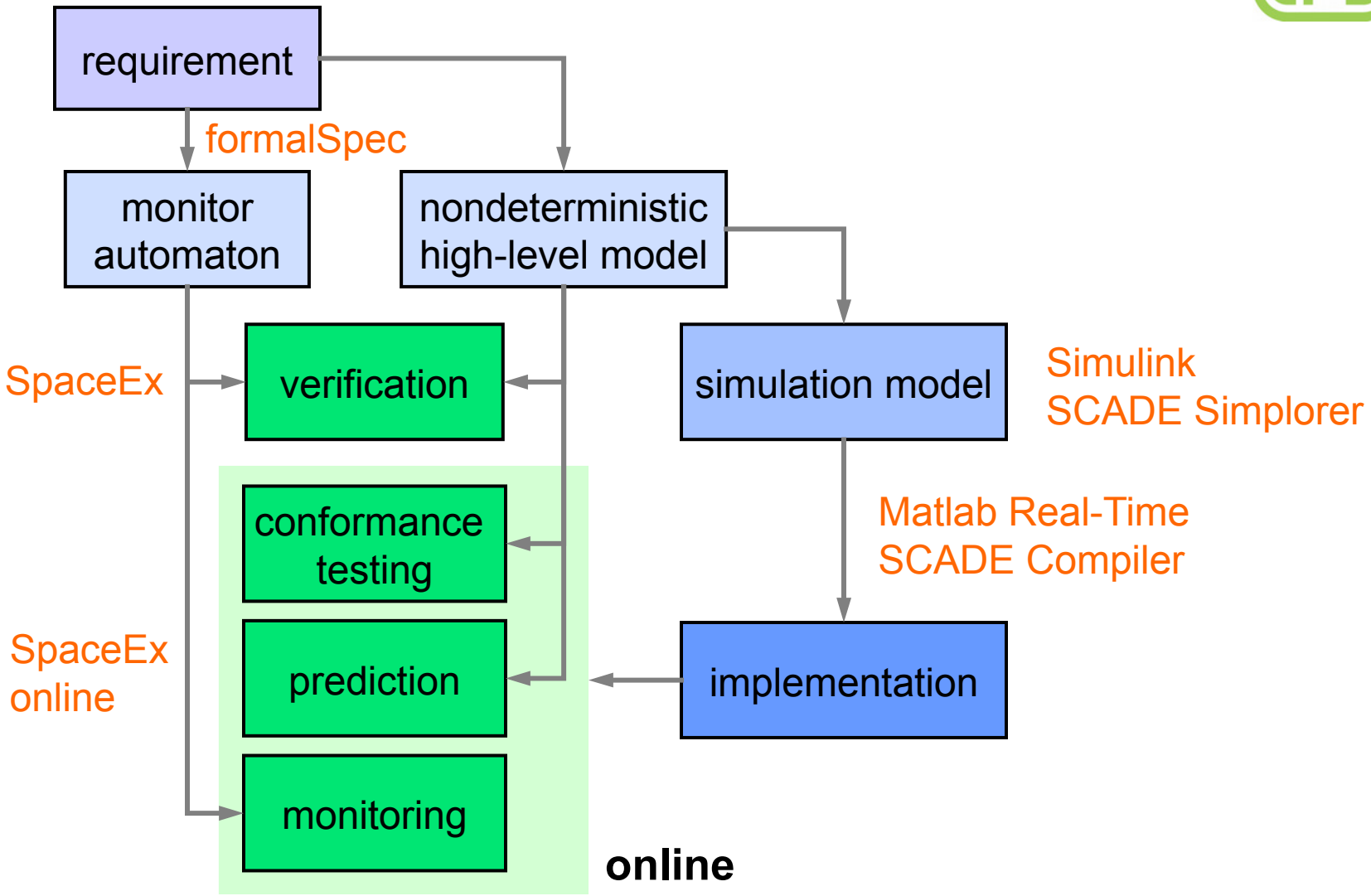
octagonal directions

6 x more work

Outline

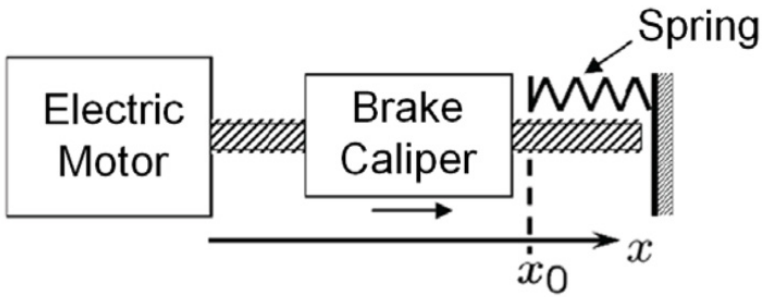
- Verification in Model Based Development
- Template Reachability in SpaceEx
- **Applications**
- Conclusions and Perspectives

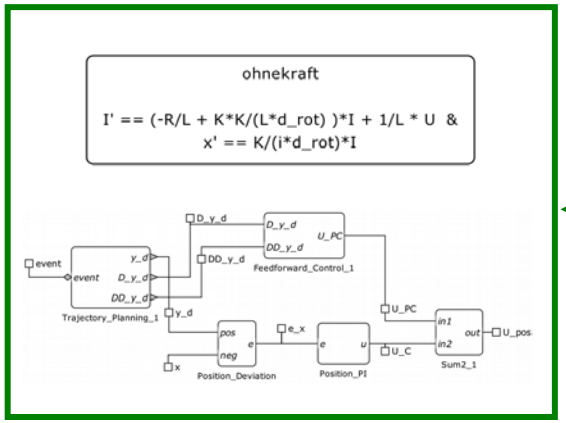
UnCoVerCPS – Design Flow

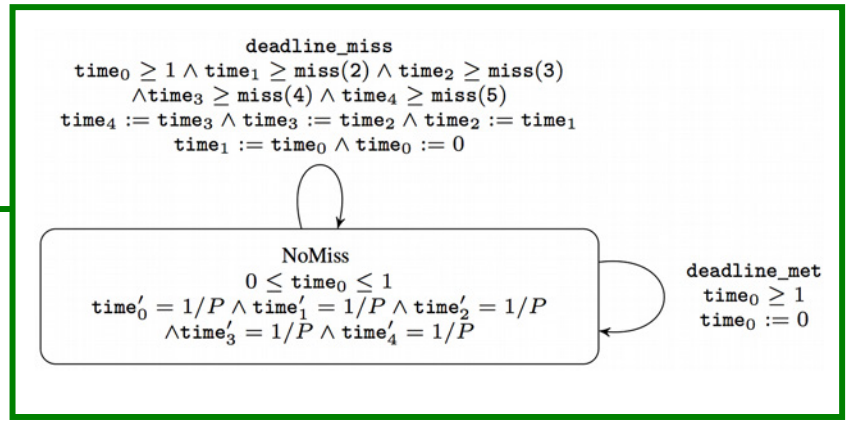


Case Study: Electro-Mechanical Brake

RTSS'14



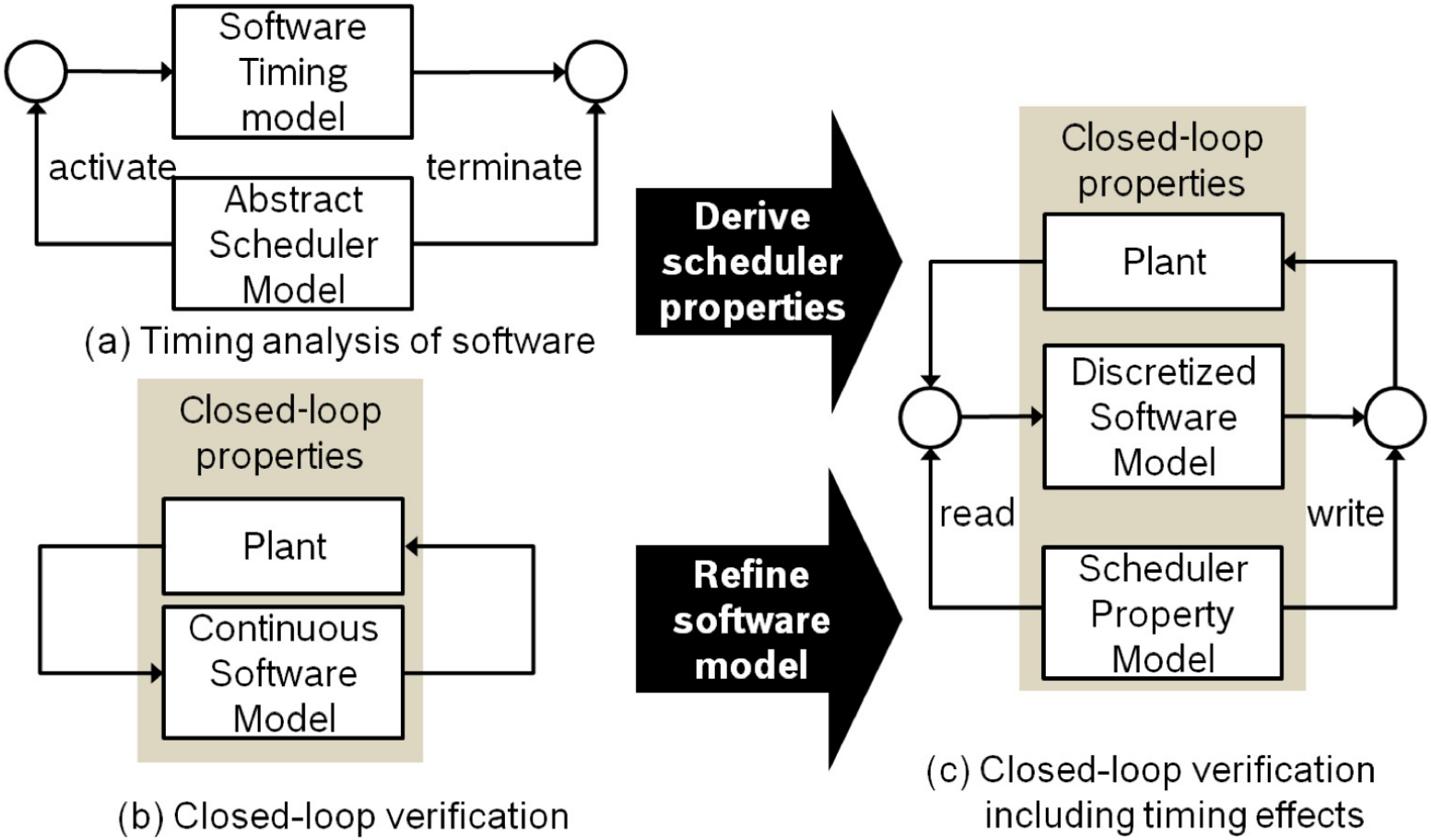




Plant & Controller

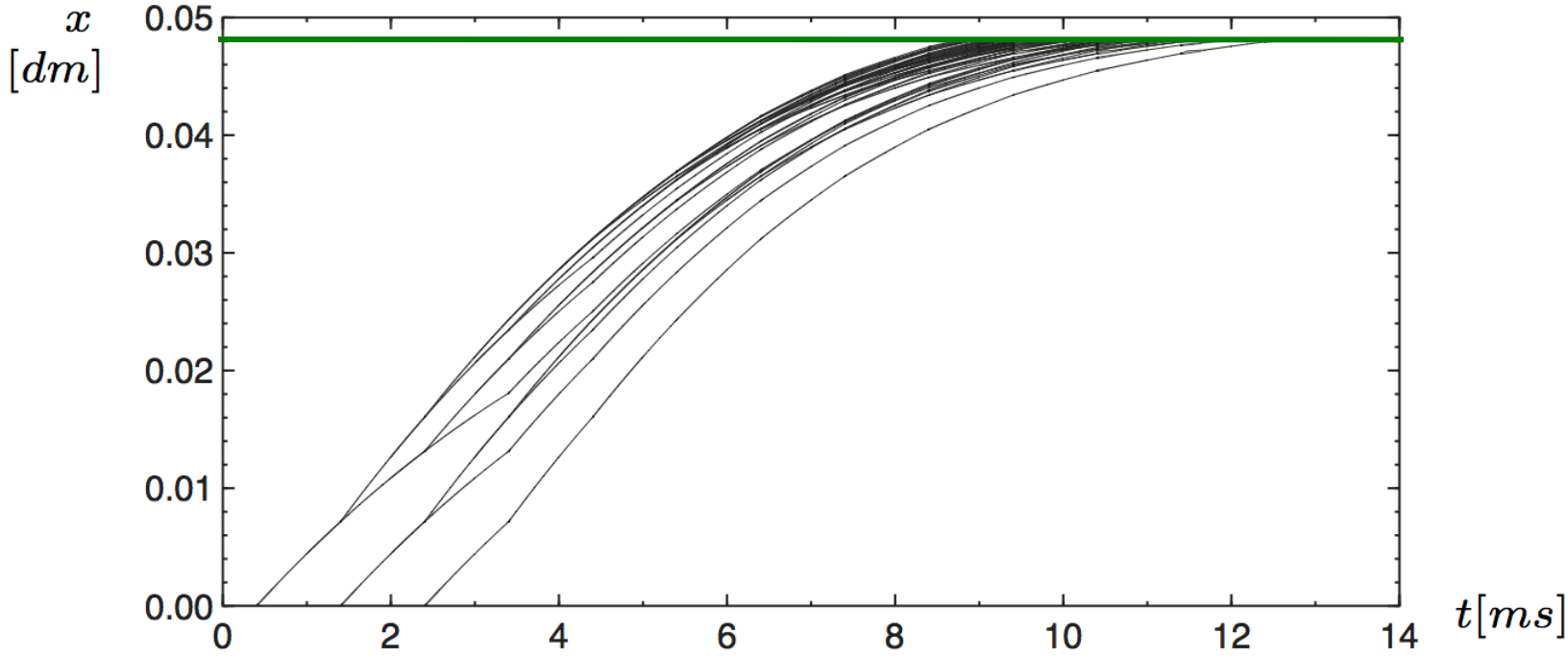
Scheduler (timed automaton)

Case Study: Electro-Mechanical Brake



Case Study: Electro-Mechanical Brake

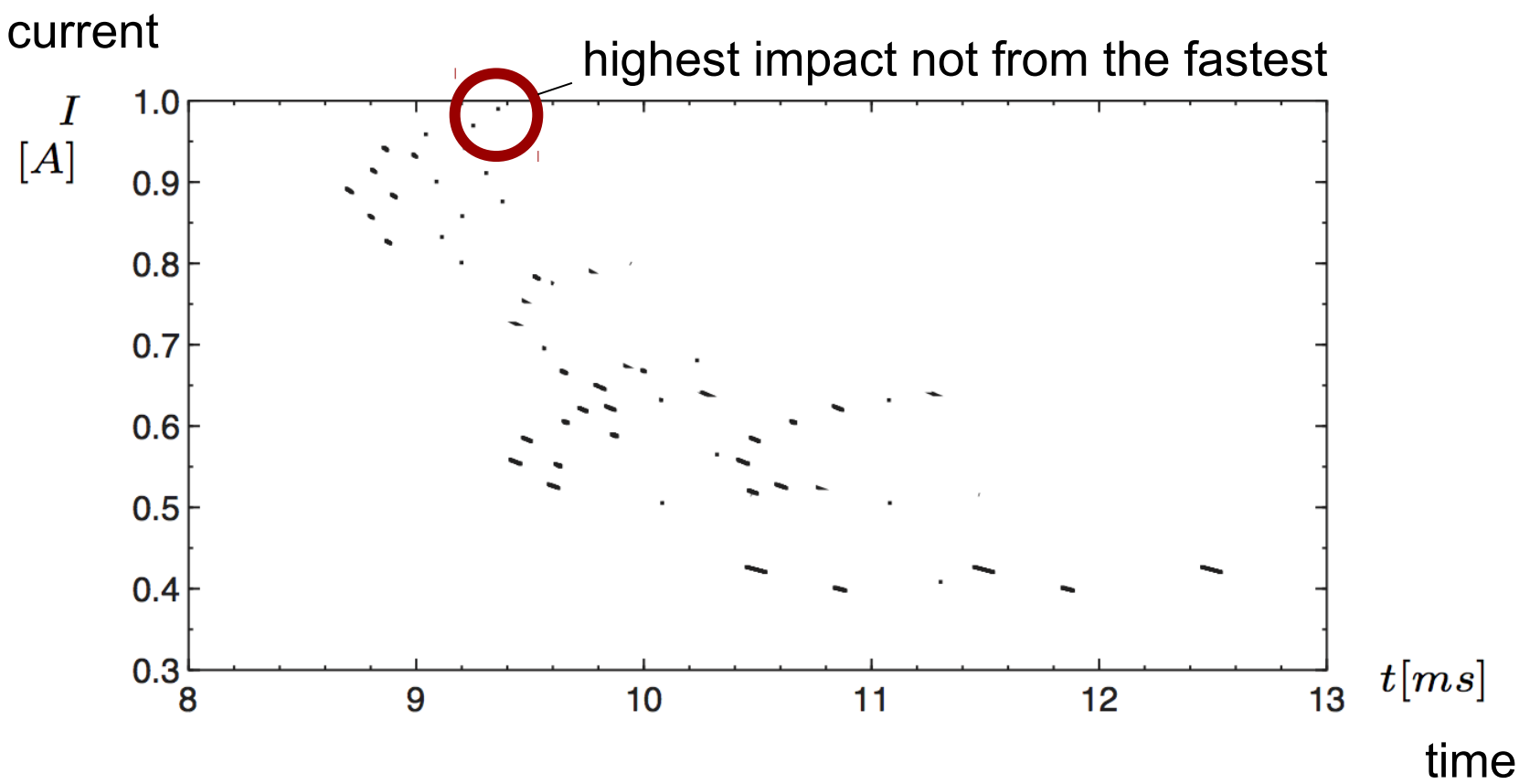
caliper position



verified: reaches target within 20ms

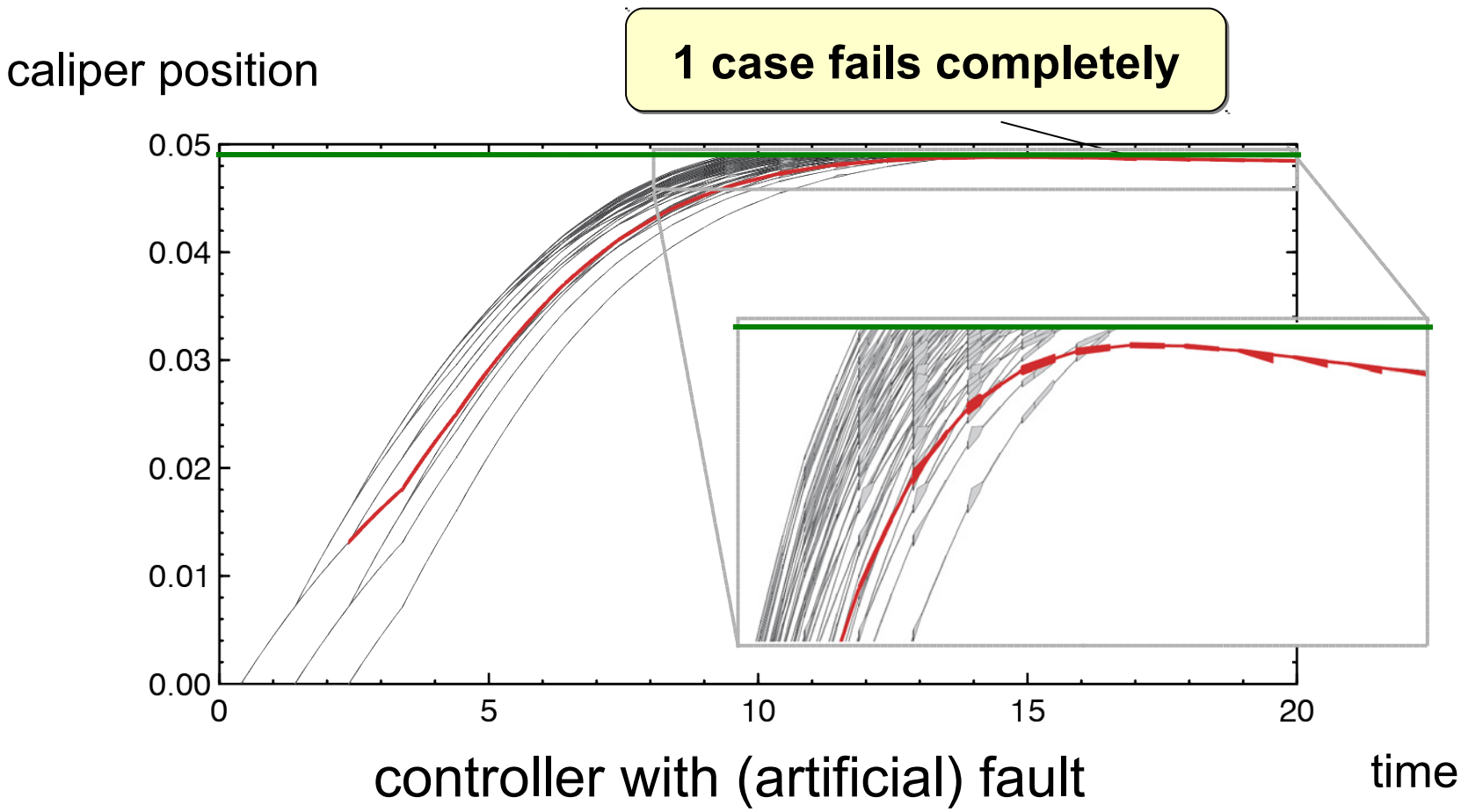
time

Case Study: Electro-Mechanical Brake

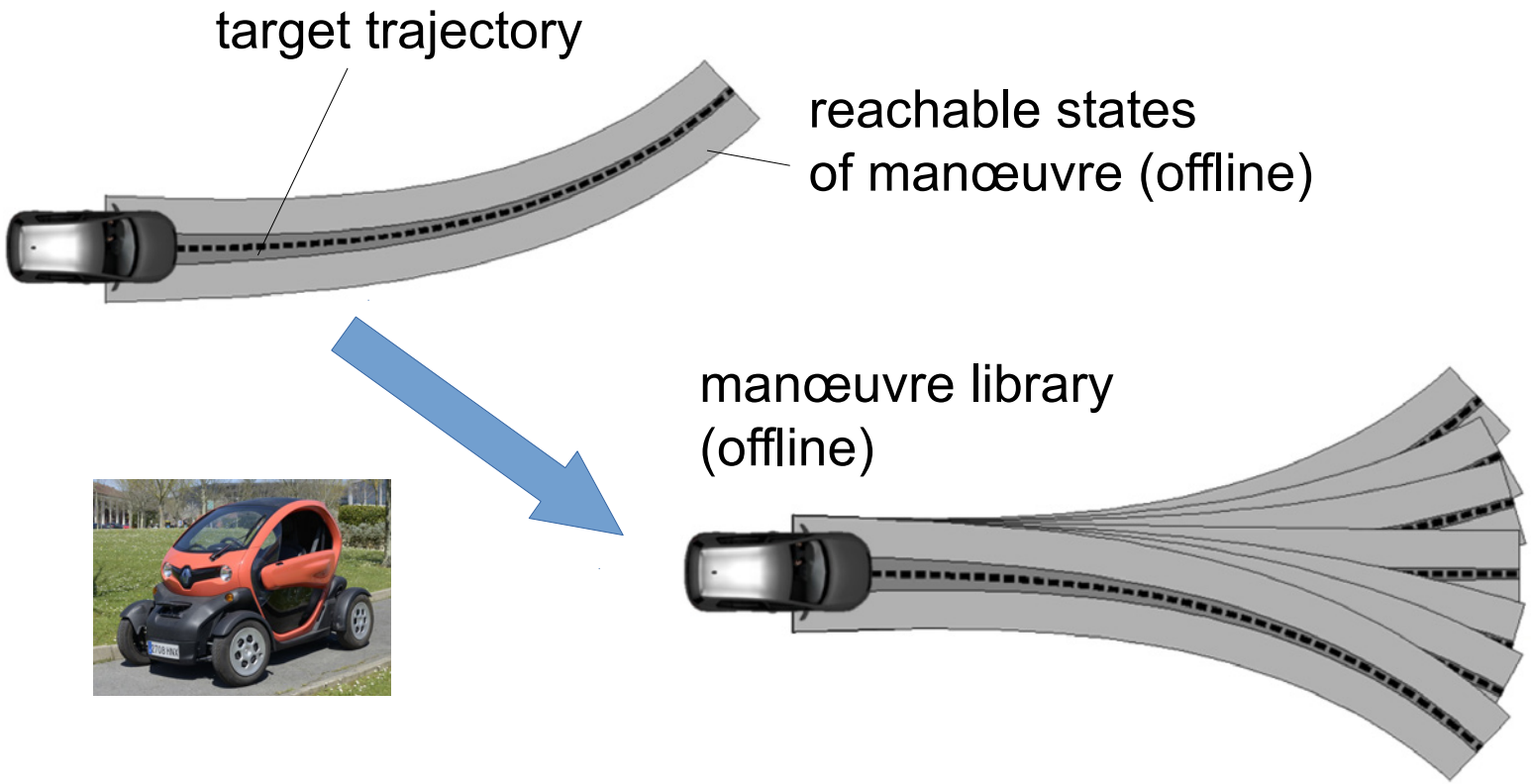


physical properties: maximum impulse on contact (measured via current)

Case Study: Electro-Mechanical Brake

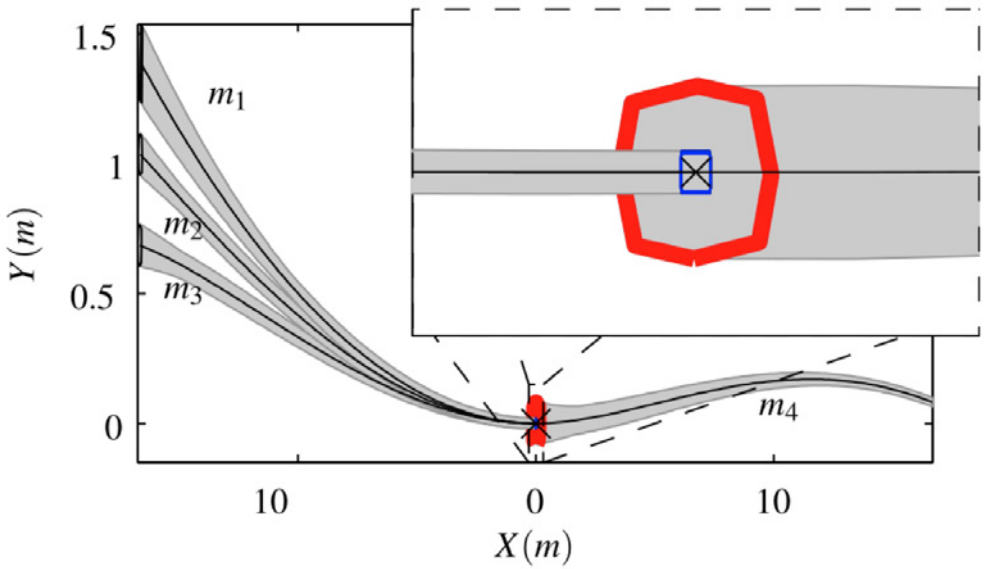


Case Study: Automated Driving



Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016

Case Study: Automated Driving



reachability:
final states contained
in initial states

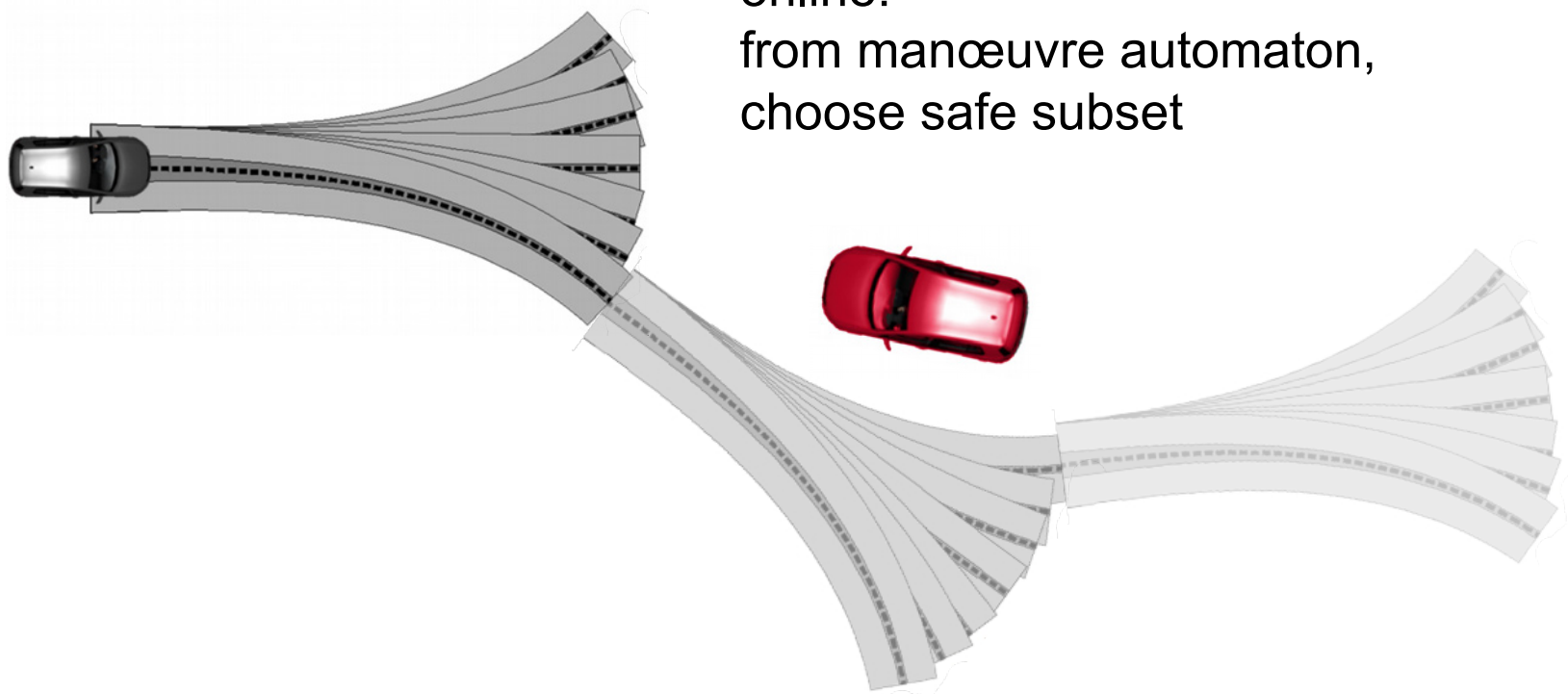
can be chained

manœuvre automaton

Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016

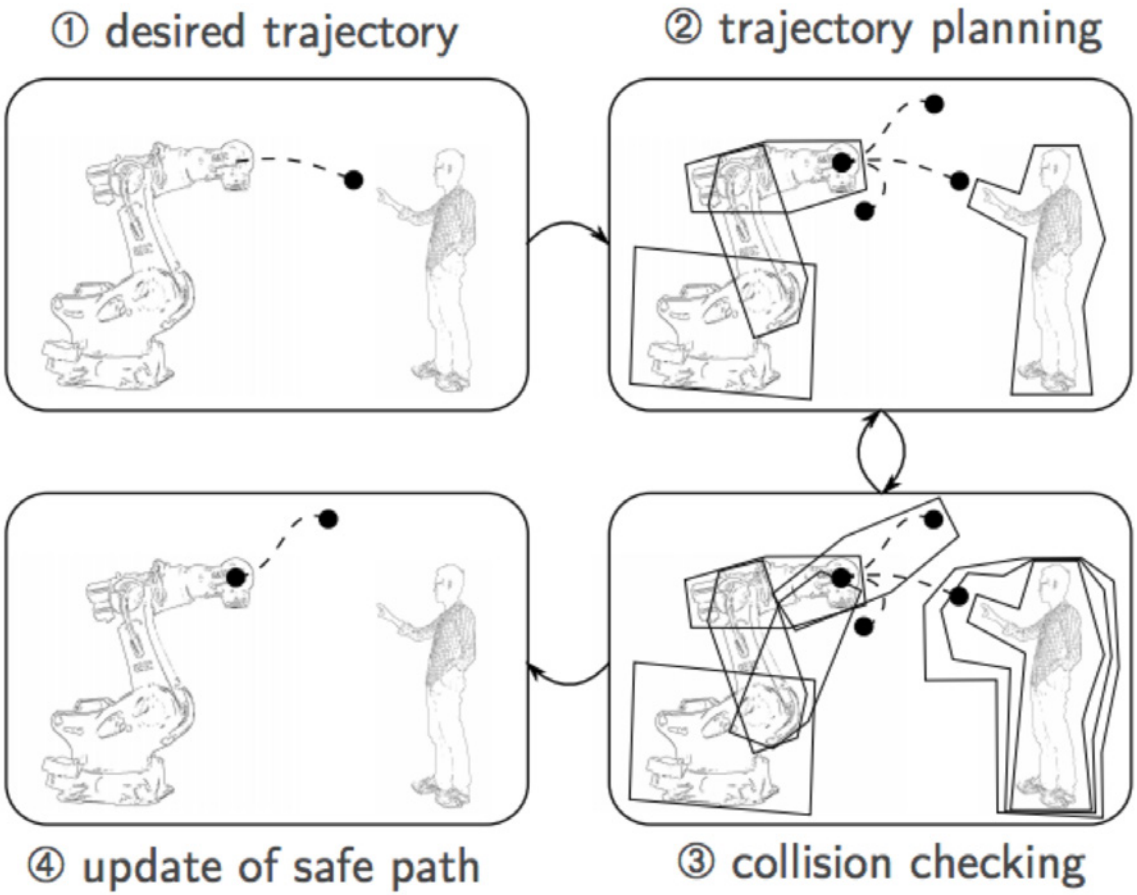
Case Study: Automated Driving

online:
from manœuvre automaton,
choose safe subset



Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016

Case Study: Human-Robot Co-Existence

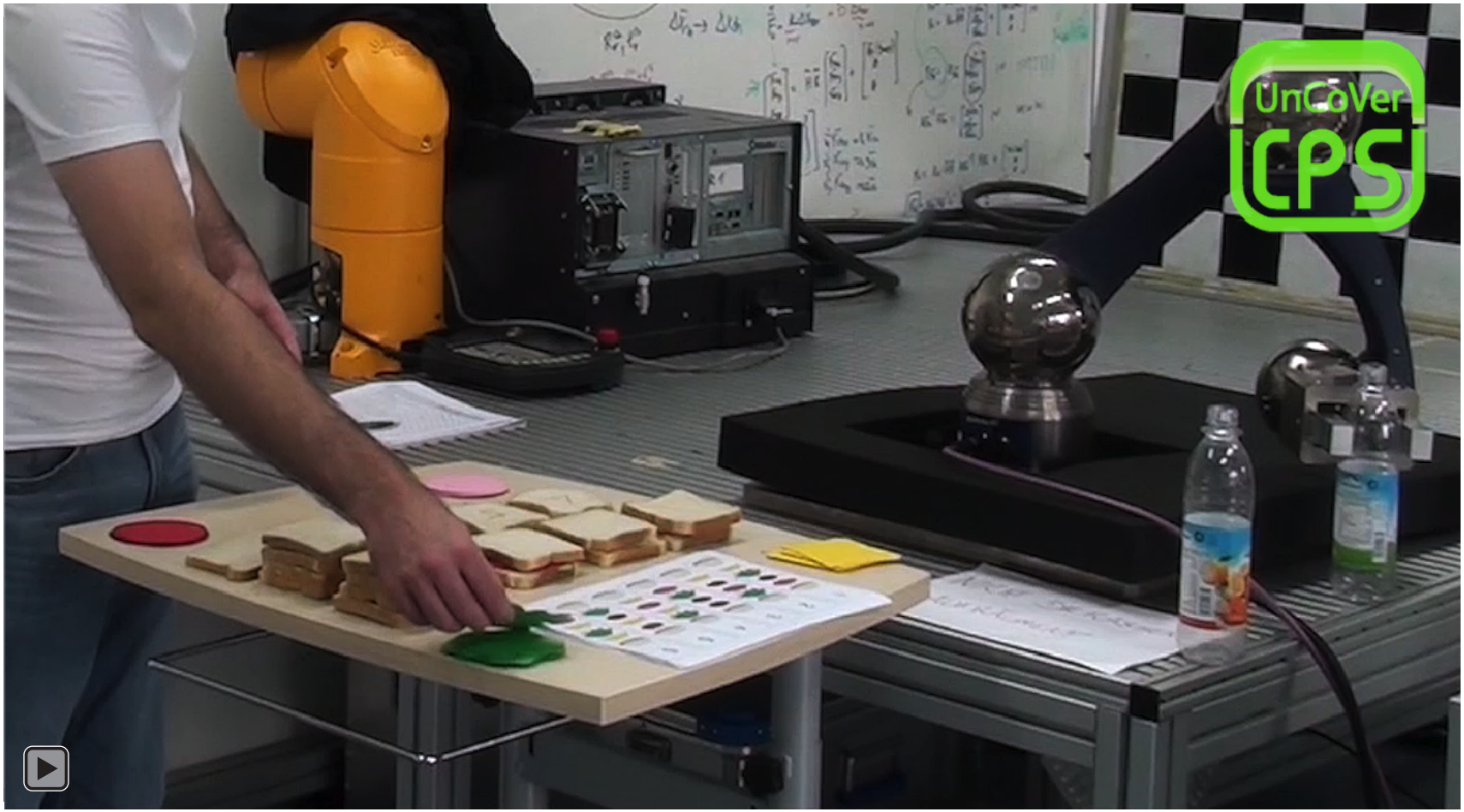


Matthias Althoff. Artemis Spring Event. http://road2cps.eu/events/wp-content/uploads/2015/10/UnCoVerCPS.pdf

Case Study: Human-Robot Co-Existence

Experiment at TU Munich (Althoff et al.)

Case Study:
Human-Robot Co-Existence



Conclusions and Perspectives

- **Set-based simulation: exhaustive envelope**
- **Can account for uncertainty**
  - modeling error, operating conditions
  - environment and user behavior
- **Huge potential for online use**
  - Verification: garantee safety
  - Monitoring: measurements conform to model
  - Prediction: trigger fail-safe in time