Formal Verification with Reachability

Goran Frehse
ENSTA Paris

**Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel,
Rajat Kateja, Manish Goyal, Rodolfo Ripado, Thao Dang, Oded Maler**
UGA / CNRS – Verimag, France

Colas Le Guernic
DGA, France

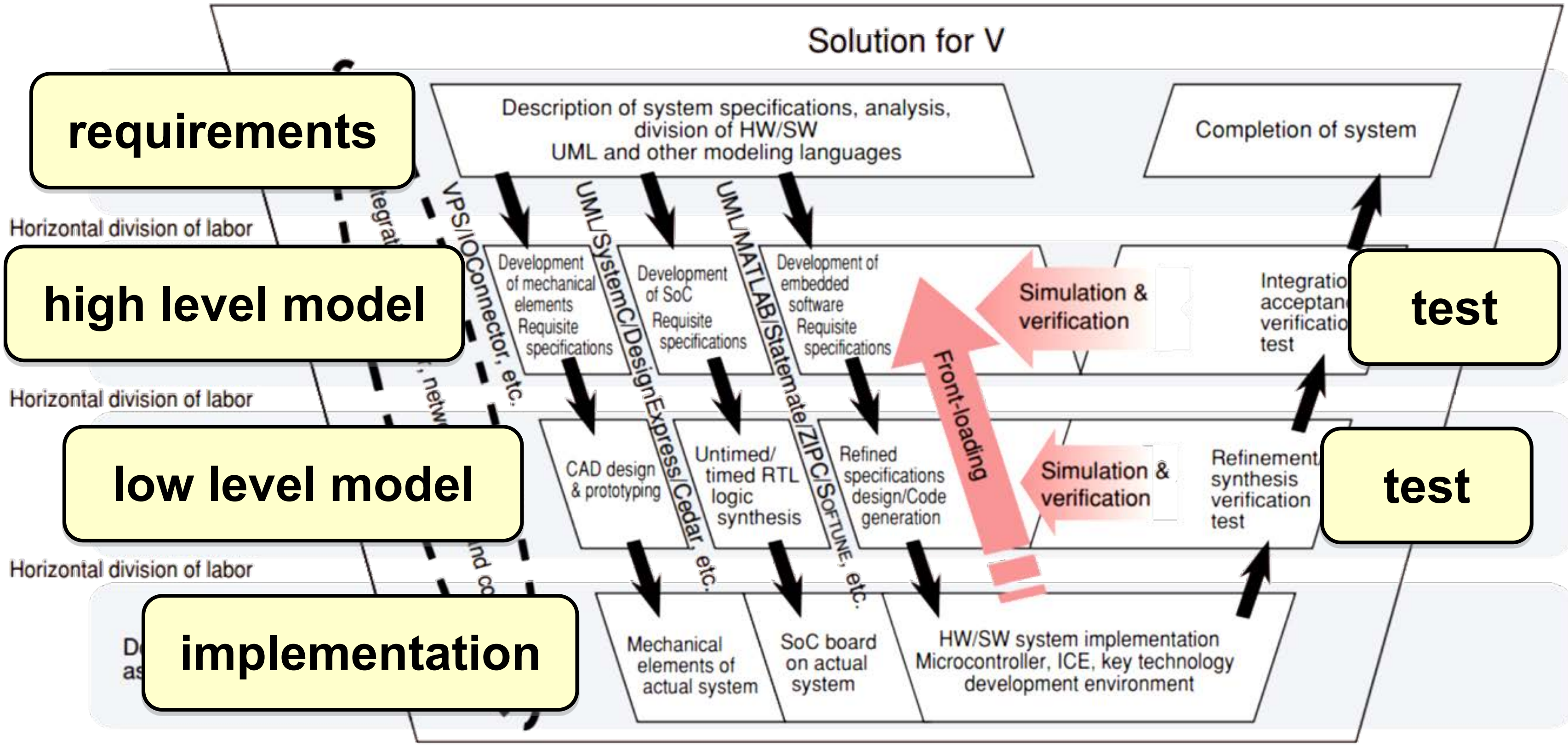
Antoine Girard
CNRS – L2S/CentraleSupélec, France

Séminaire IRT SystemX, Palaiseau, February 6, 2020

Outline

- **Modeling Complex Systems**
- **Set-based Verification vs Simulation**
- **Template Reachability in SpaceEx**
- **Dealing with Unpredictability**
- **Conclusions and Perspectives**

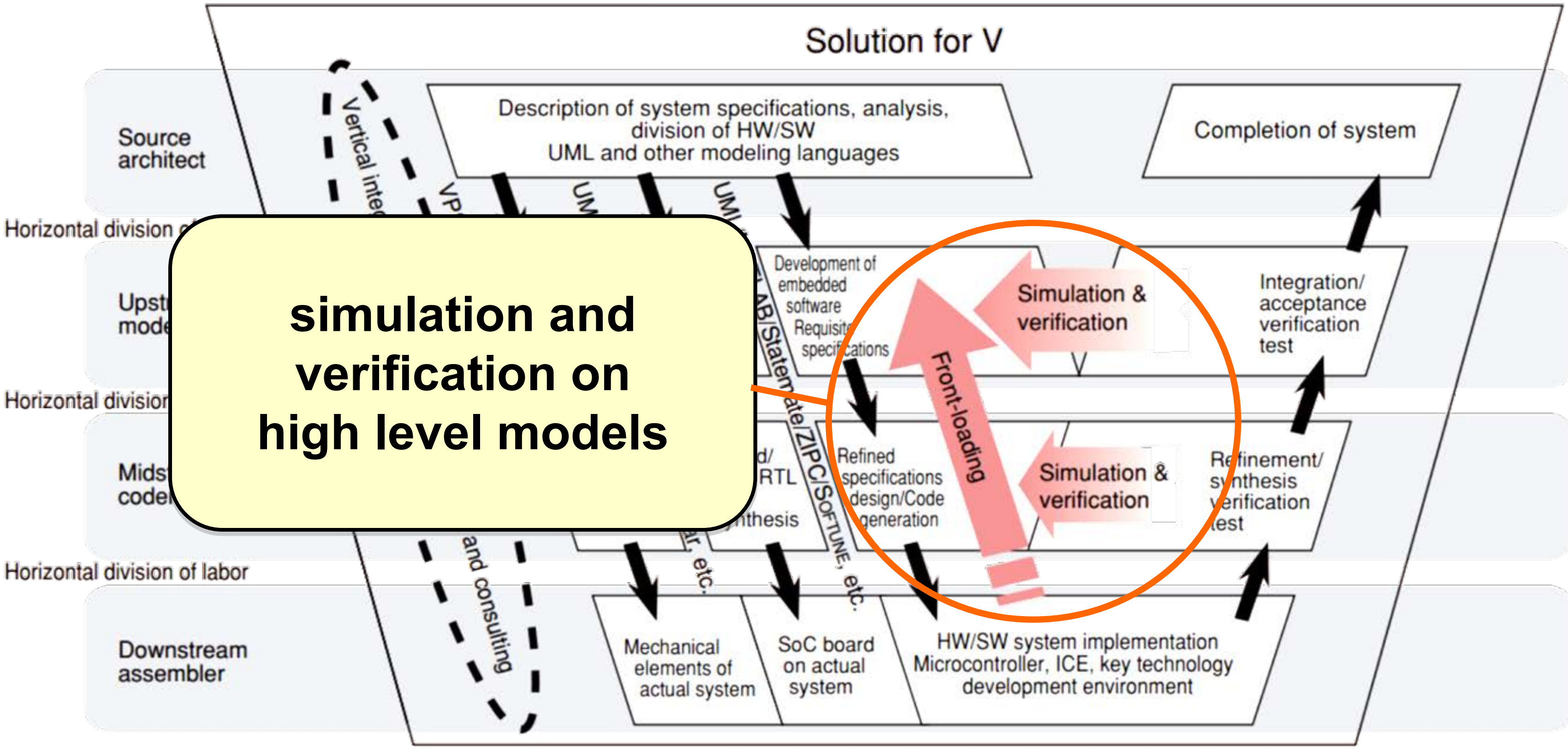
Model-Based Development



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

Formal Verification in Model-Based Design

How to guarantee absence of bugs (not just finding bugs)?

- continuous dynamic systems
- under bounded uncertainty (parameters, noise)
- under discrete events

Methods inspired from formal computer science

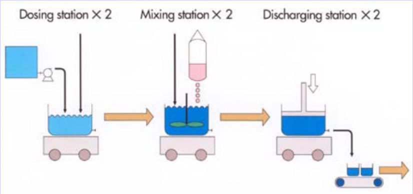
- abstract interpretation (Cousot & Cousot, '77)
- model checking (Clarke, Emerson, '80; Sifakis, '82)
- compositional analysis (Clarke et al., '89)

Variety of Application Domains

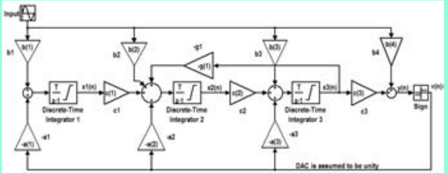
assisted and automated driving

human-robot interaction

smart buildings



chemical batch plants



analog mixed-signal circuits

autonomous drones

FP7 + H2020 projects **NANO 2017 project** **Collaborations**

1. Automated vehicle of Tecnalia 2. Sandwich assembly robot of R.U.Robotics Ltd. 3. http://www.itproportal.com/2012/12/21/smart-cities-smarter-buildings/ 4. MILOX™: Pipeless Production System http://www.toyo-eng.co.jp/en/product_line/medication/milox/index.html 5. Dang, Donzé, Maler. Verification of analog and mixed-signal circuits using hybrid systems techniques. FMCAD'04 6. Bitcraze Crazyflie

Modelling Complex Systems

First Principles

Tecnalia Twizy
UnCoVerCPS

ODEs kinematics
DAEs electrical, chemical, mechanical networks
PDEs heat, sound, fluids, elasticity

Modelling Complex Systems

First Principles

Data-Based

ODEs
DAEs
PDEs

Regression / Kalman
Gaussian Models
Machine Learning (NN)

Modelling Complex Systems

First Principles

ODEs
DAEs
PDEs

Data-Based

Regression / Kalman
Gaussian Models
Machine Learning (NN)

Communication

Events
Messages
Delays and Losses

Modelling Complex Systems

First Principles

ODEs
DAEs
PDEs

Data-Based

Regression / Kalman
Gaussian Models
Machine Learning (NN)

Communication

Events
Messages
Delays and Losses

Unpredictable Env.

People
Autonomous Vehicles

How to Verify Complex Systems?

Simulation Model → Mathematical Model

Simulation Model → Generalize

Mathematical Model → Simplify

Generalize

compute trajectories
identify equivalent neighborhoods

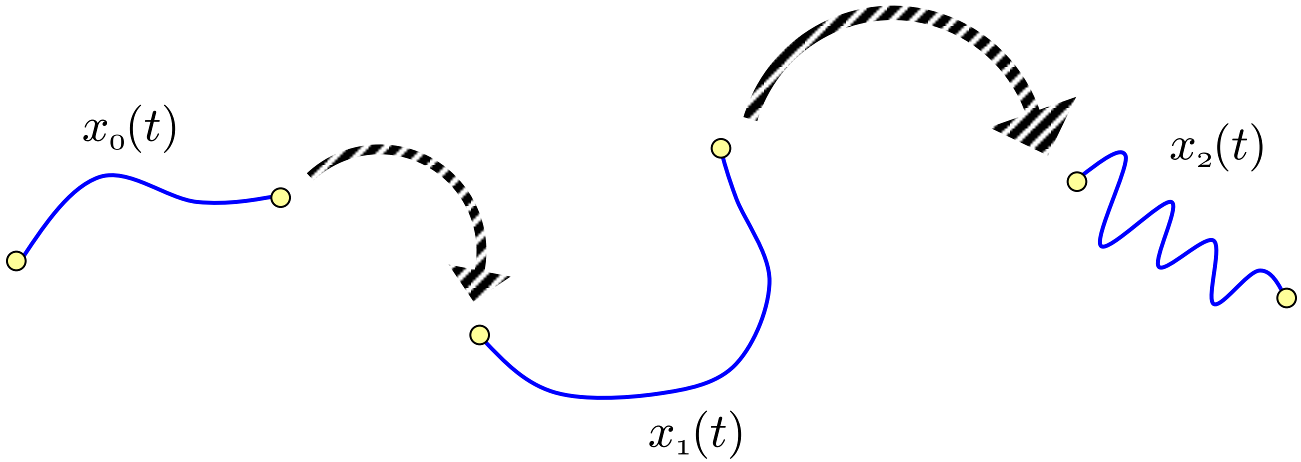
Simplify

abstract:
model-order reduction
projection
approximate bisimulation

this talk

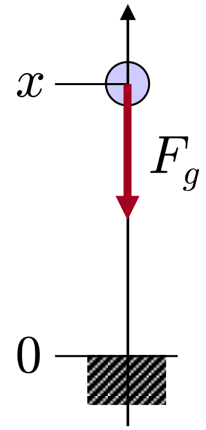
Hybrid Systems - Semantics

- **Continous/Discrete Behaviour**
  - evolution with time according to ODE dynamics
  - dynamics can switch (instantaneous)
  - state can jump (instantaneous)

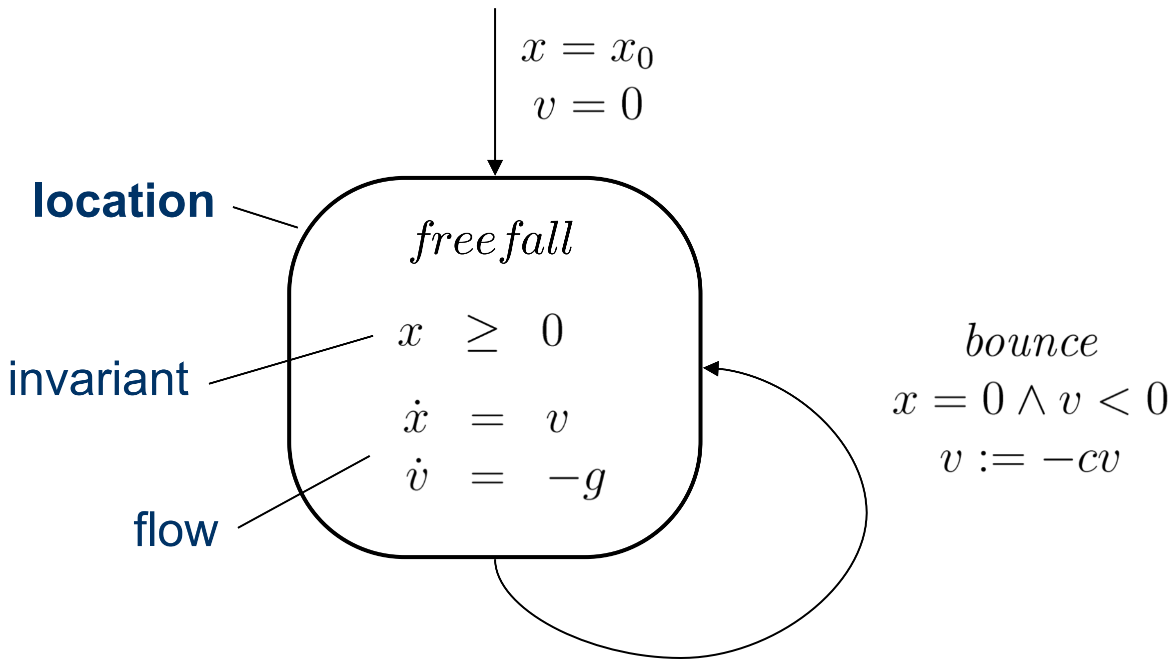


Modeling Hybrid Systems

- **Example: Bouncing Ball**
  - ball with mass m and position x in free fall
  - bounces when it hits the ground at $x = 0$
  - initially at position x_0 and at rest

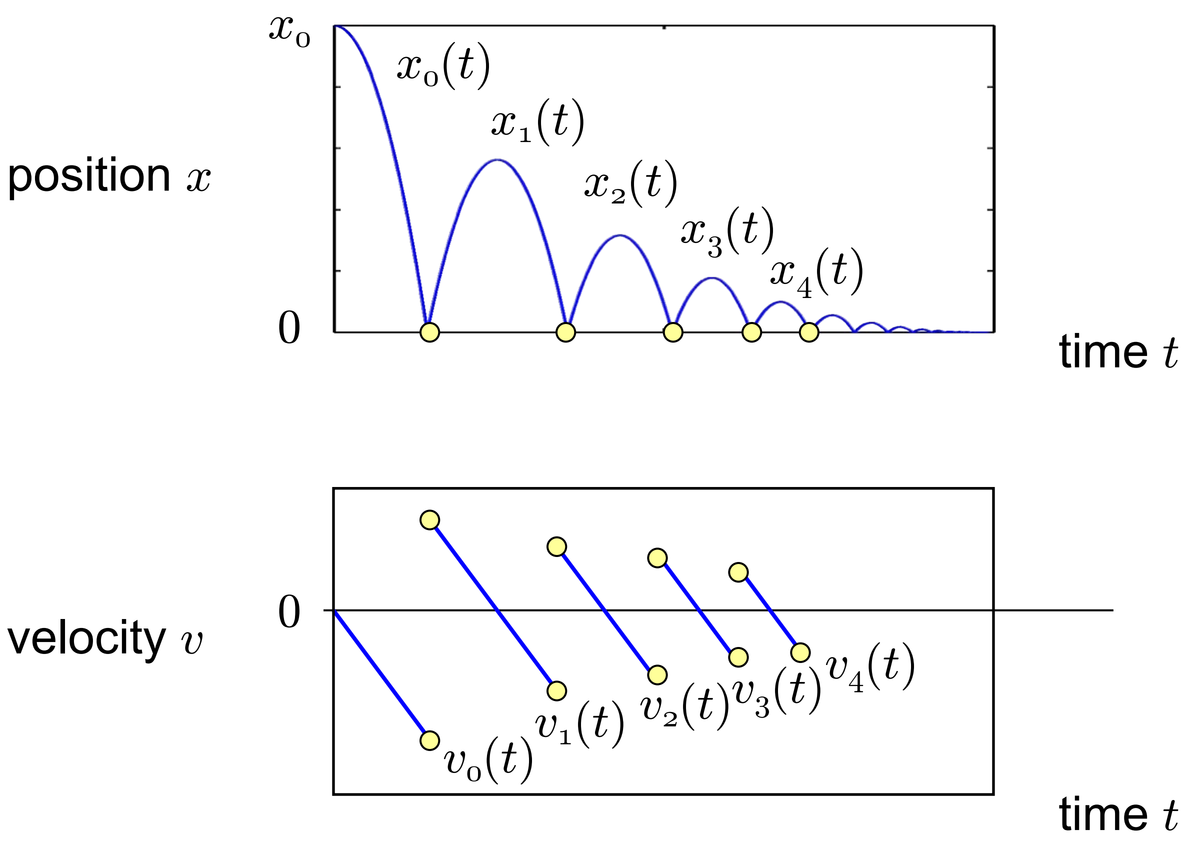


Hybrid Automaton Model



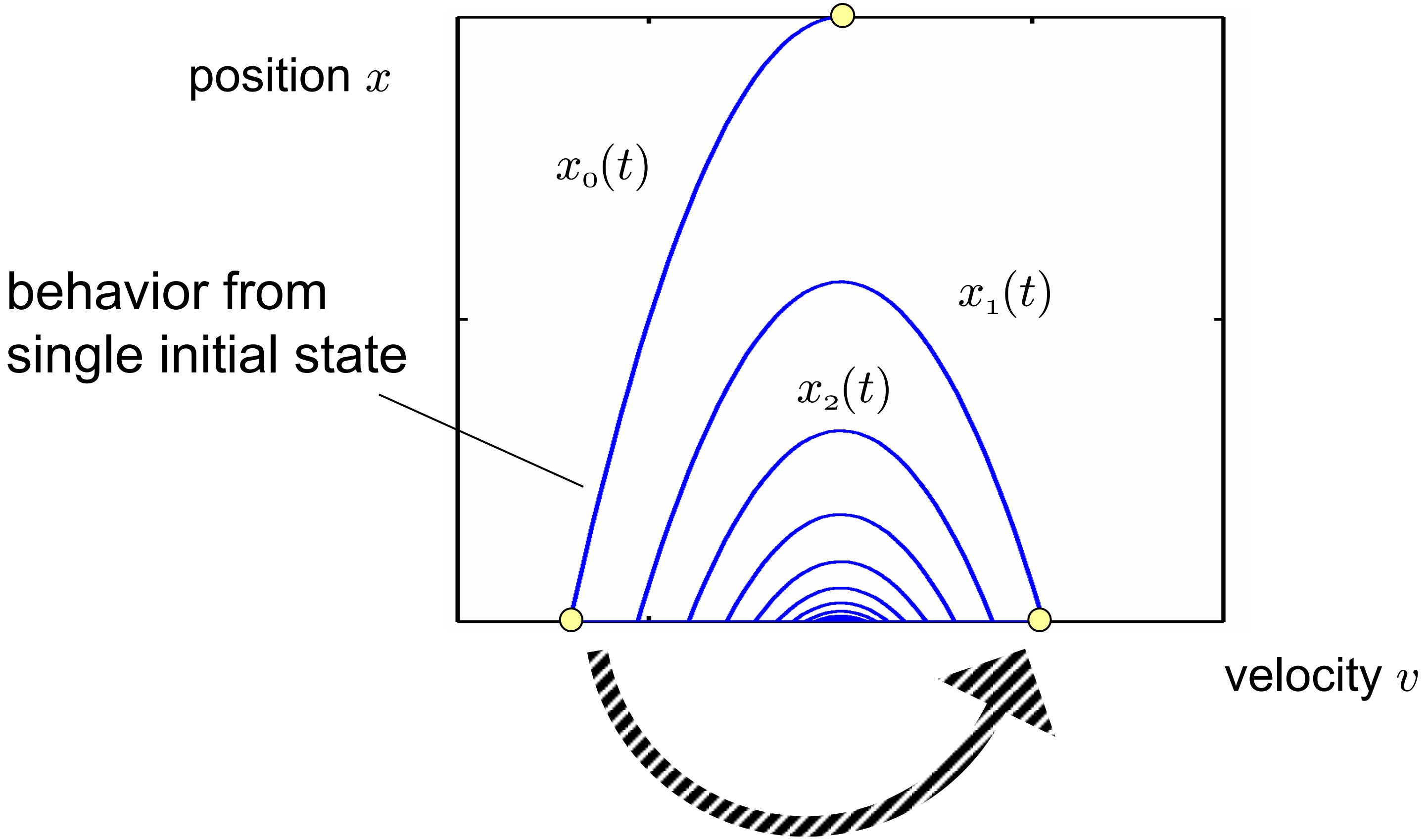
Example: Bouncing Ball

- **States over Time**



Example: Bouncing Ball

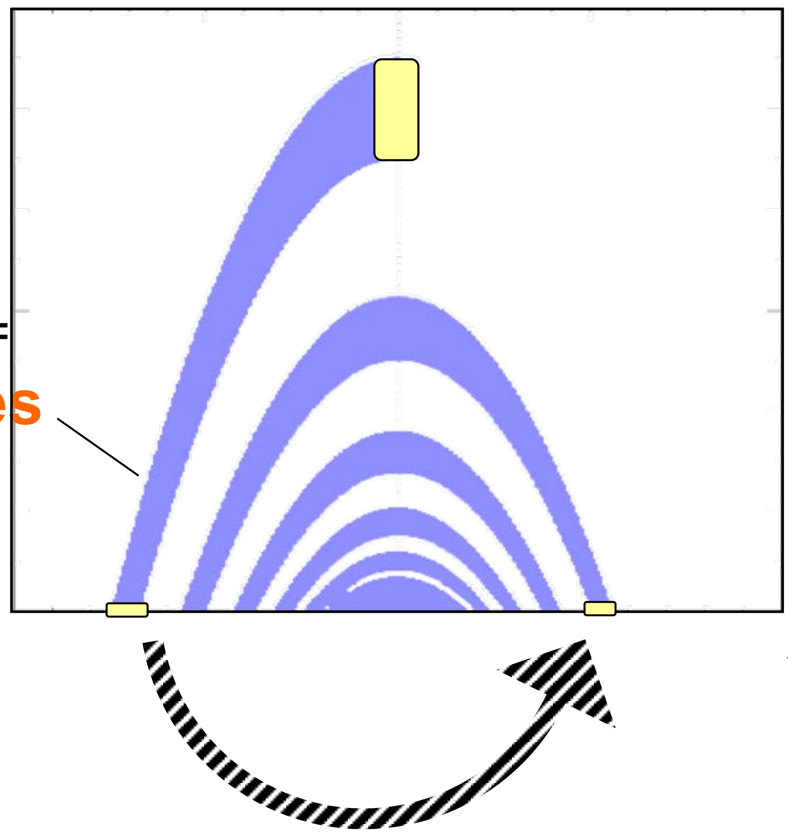
- **States over States = State-Space View**



Example: Bouncing Ball

- **Reachability in State-Space**

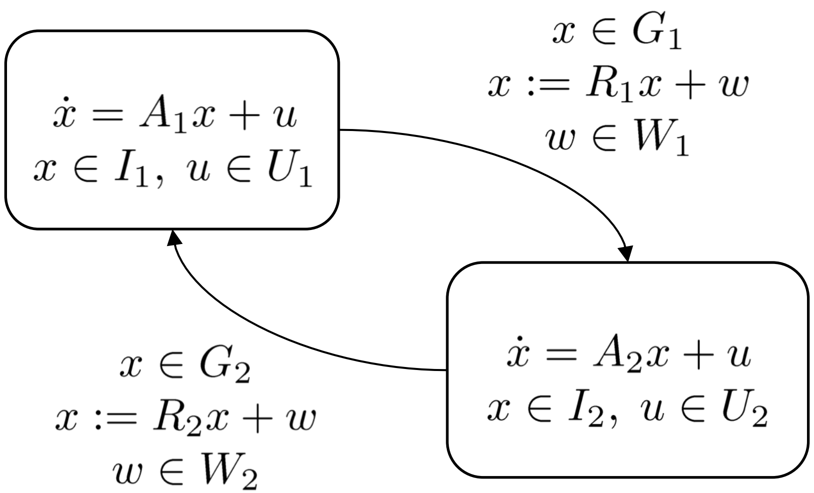
behaviors from
set of initial states =
reachable states

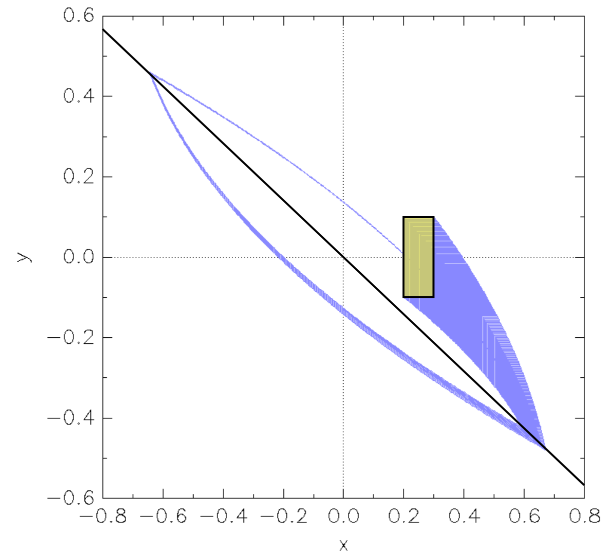


Outline

- Modeling Complex Systems
- **Set-based Verification vs Simulation**
- Template Reachability in SpaceEx
- Dealing with Unpredictability
- Conclusions and Perspectives

Hybrid Automata with Affine Dynamics





- **linear differential equations**
- **can be highly nondeterministic:**
  - additive "inputs" u,w model continuous disturbances (noise etc.)

Key: find approximation that is efficient but accurate for a large number of continuous variables

Reachability Operations

- **States reachable from initial Set R_0**
- **Fixpoint Computation**

$$R_{k+1} = R_k \cup \mathrm{post}(R_k)$$

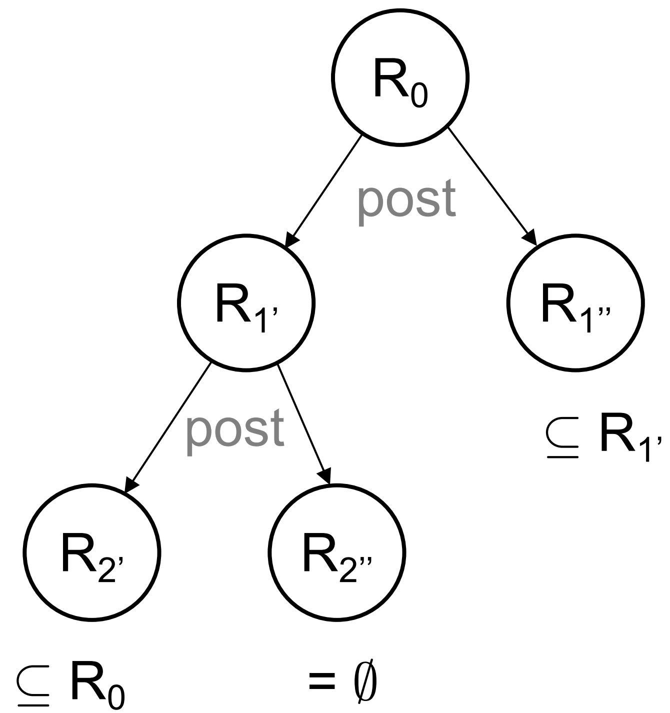
with post-operations

- time elapse
- image of discrete transitions

Fixpoint Computation

- **Checks Required for Termination**
  - Containment
  - Emptiness

- **Intersection with bad states**
  - optional



Time Elapse Computation

- **Continuous time elapse for affine dynamics**
  - efficient, scalable
  - approximation without accumulation of approximation error (wrapping effect)
- **Much heritage from prior work**
  - Chutinan, Krogh. HSCC'99
  - Asarin, Bournez, Dang, Maler. HSCC'00
  - Girard. HSCC'05
  - Le Guernic, Girard. HSCC'06, CAV'09

Affine Dynamics

- **linear terms plus inputs U:**

$$\dot{x} = Ax + u,\ u \in U$$

- **solution:**

$$x(t) = e^{At}x(0) + \int_0^t e^{A(t-\tau)}u(\tau)d\tau$$

matrix exponential

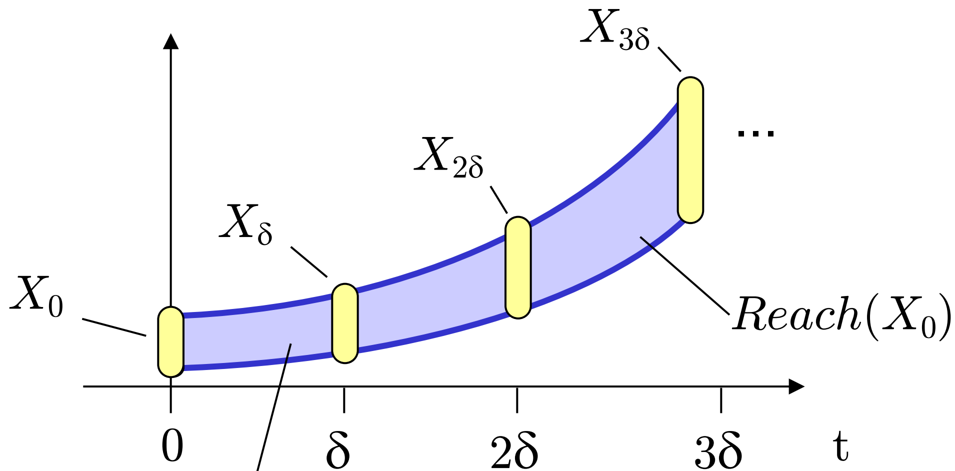
factors influence of inputs
(stable system forgets the past)

From Time-Discretization to Reach

- **States in discrete time:**

$$X_{k\delta} = (e^{A\delta})^k X_0 \oplus S_{k\delta}$$

integral over inputs

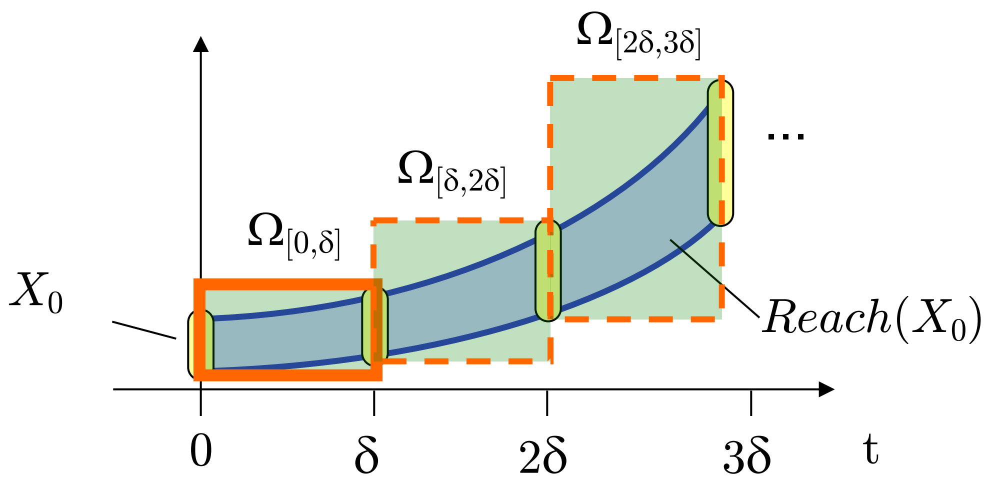


need to cover also states in between!

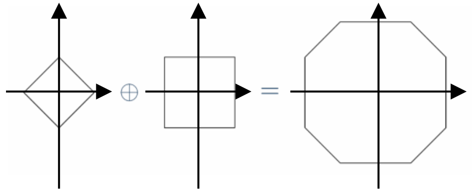
From Time-Discretization to Reach

- **Cover in discrete time:**

$$\Omega_{[k\delta,(k+1)\delta]} \quad = \quad (e^{A\delta})^k \Omega_{[0,\delta]} \oplus \Psi_{k\delta}$$

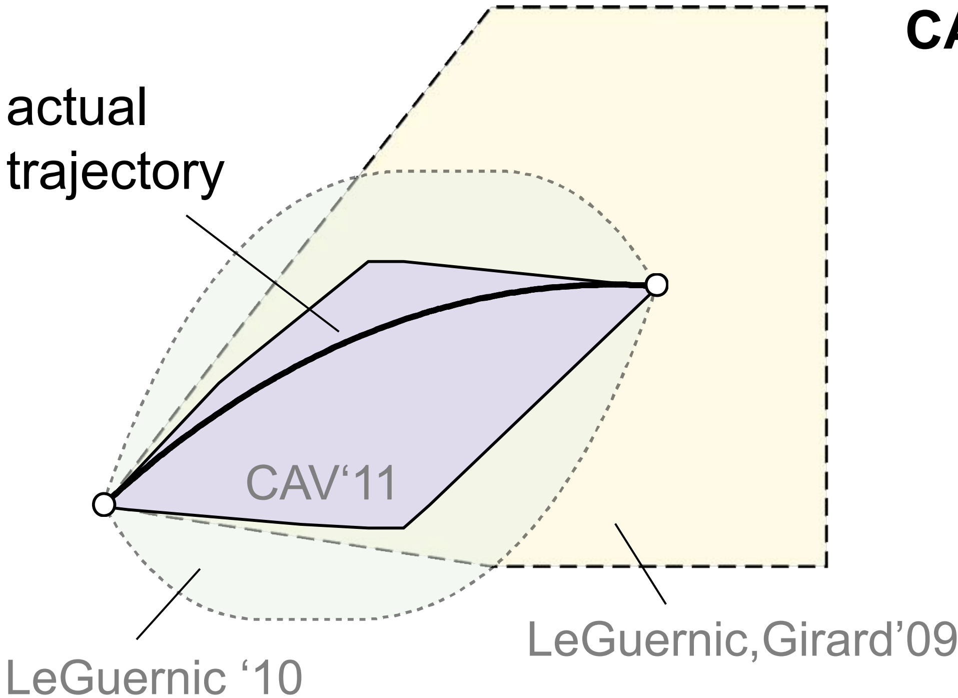


$\oplus$ Minkowski sum = pointwise sum of sets



From Time-Discretization to Reach

- **1st order Taylor approximation**
- **different bounds on the remainder**

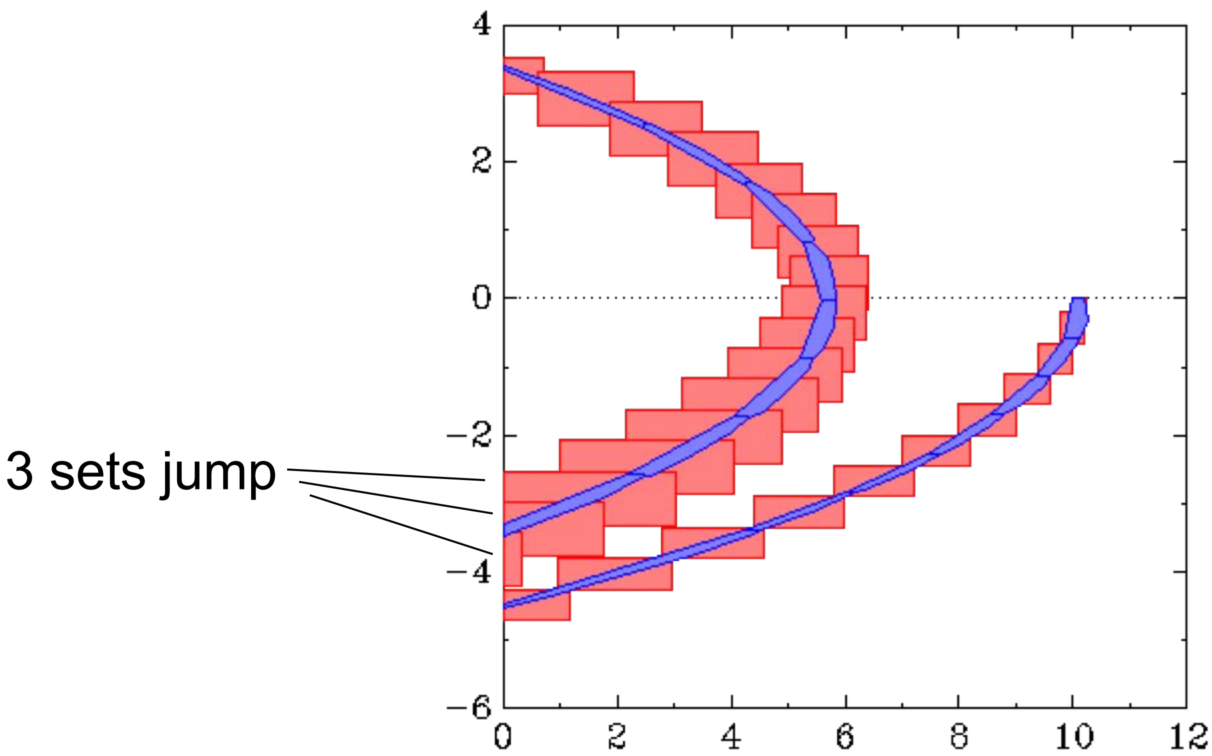


CAV'11: Complex Polytope

$$\Omega_{[0,\delta]} = \mathrm{chull}(\textstyle\bigcup_{0\leq t\leq\delta}\Omega_t)$$
$$\Omega_t = (1-\tfrac{t}{\delta})\mathcal{X}_0 \oplus \tfrac{t}{\delta}e^{\delta A}\mathcal{X}_0 \oplus \left(\tfrac{t}{\delta}\mathcal{E}_\Omega^+ \cap (1-\tfrac{t}{\delta})\mathcal{E}_\Omega^-\right) \oplus t\mathcal{U} \oplus \tfrac{t^2}{\delta^2}\mathcal{E}_\Psi$$
$$\Phi_2(A,\delta) = A^{-2}\left(e^{\delta A} - I - \delta A\right)$$
$$\mathcal{E}_\Omega^+(\mathcal{X}_0,\delta) = \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A^2\mathcal{X}_0\right)\right),$$
$$\mathcal{E}_\Omega^-(\mathcal{X}_0,\delta) = \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A^2e^{\delta A}\mathcal{X}_0\right)\right),$$
$$\mathcal{E}_\Psi(\mathcal{U},\delta) = \boxdot\left(\Phi_2(|A|,\delta)\boxdot(A\mathcal{U})\right).$$

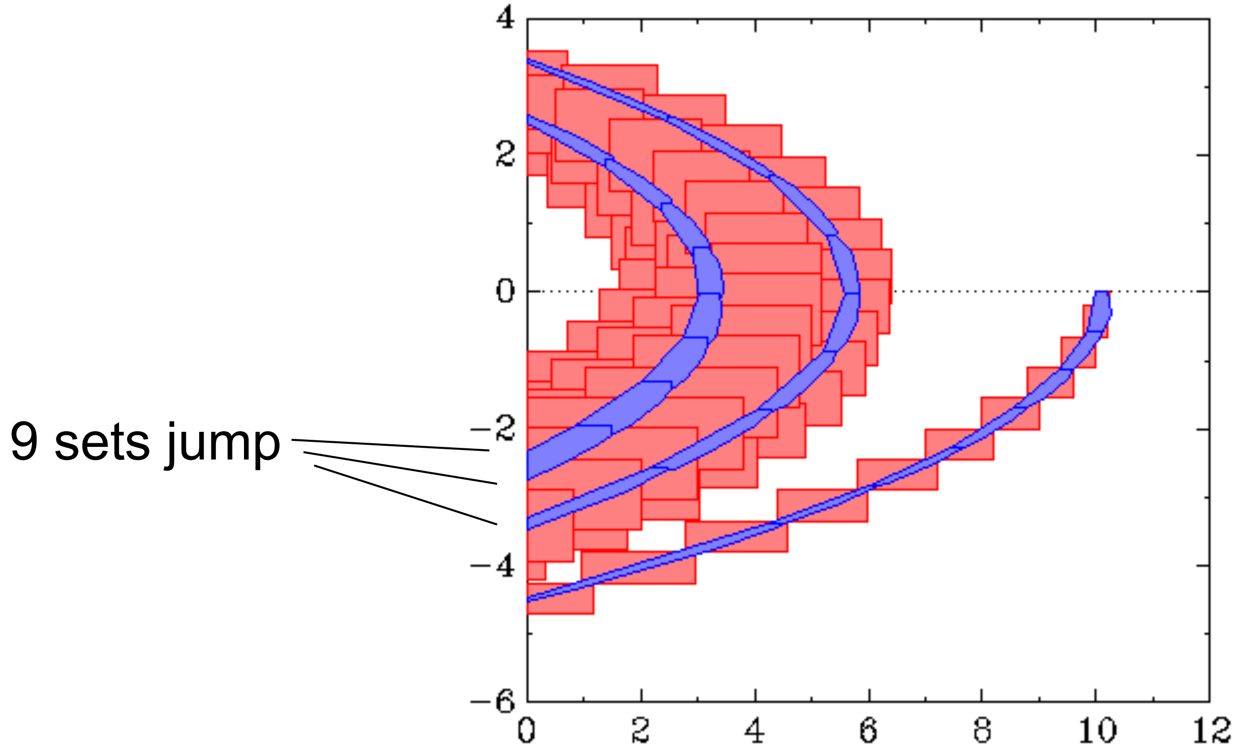
Problem: State Explosion

- **Bouncing ball example:**



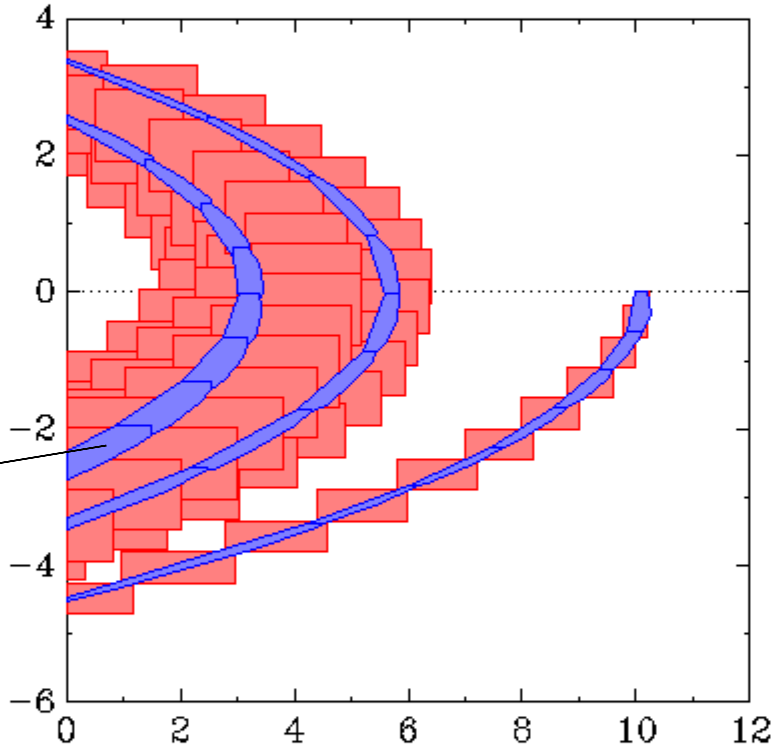
Problem: State Explosion

- **Bouncing ball example:**



Problem: State Explosion

- **Bouncing ball example:**



cover with
minimal number
of sets
[HSCC’13]

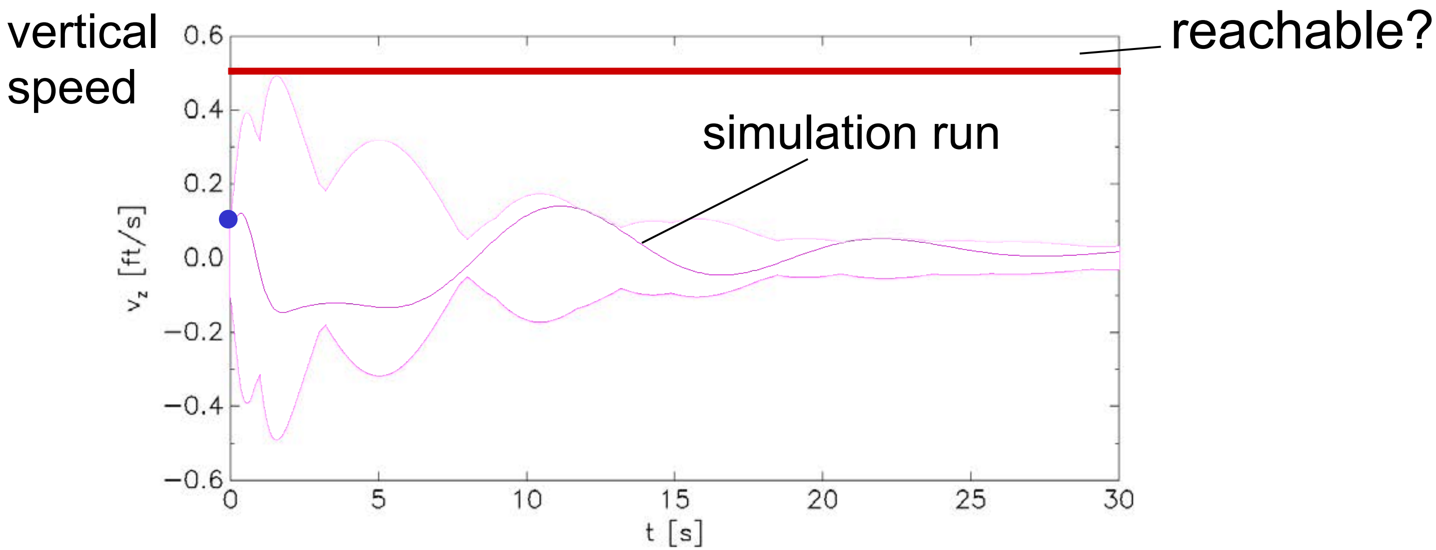
Example: Controlled Helicopter

- **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.

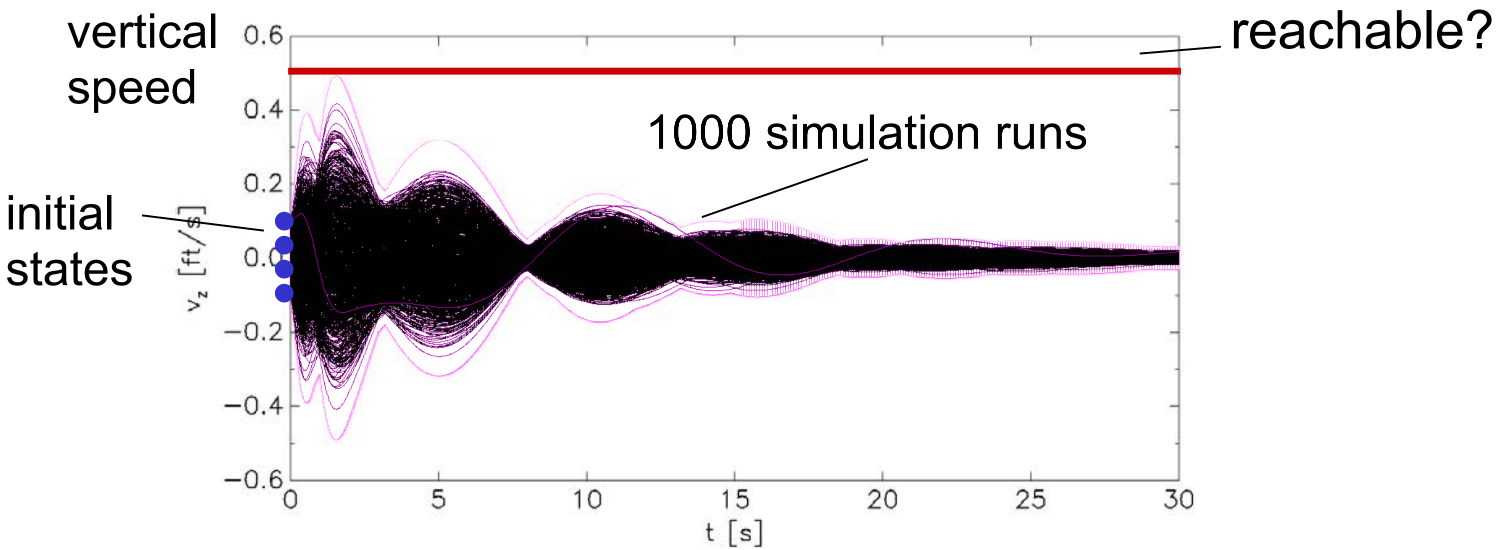
Simulation vs Reachability

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



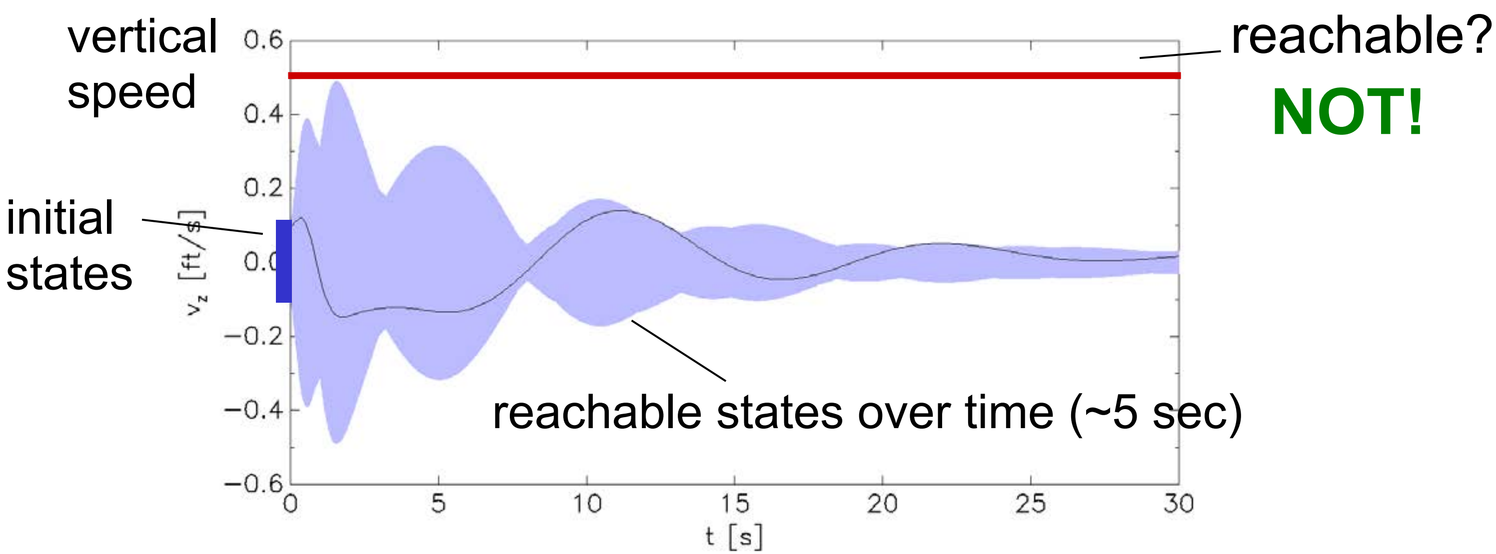
Simulation vs Reachability

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



Simulation vs Reachability

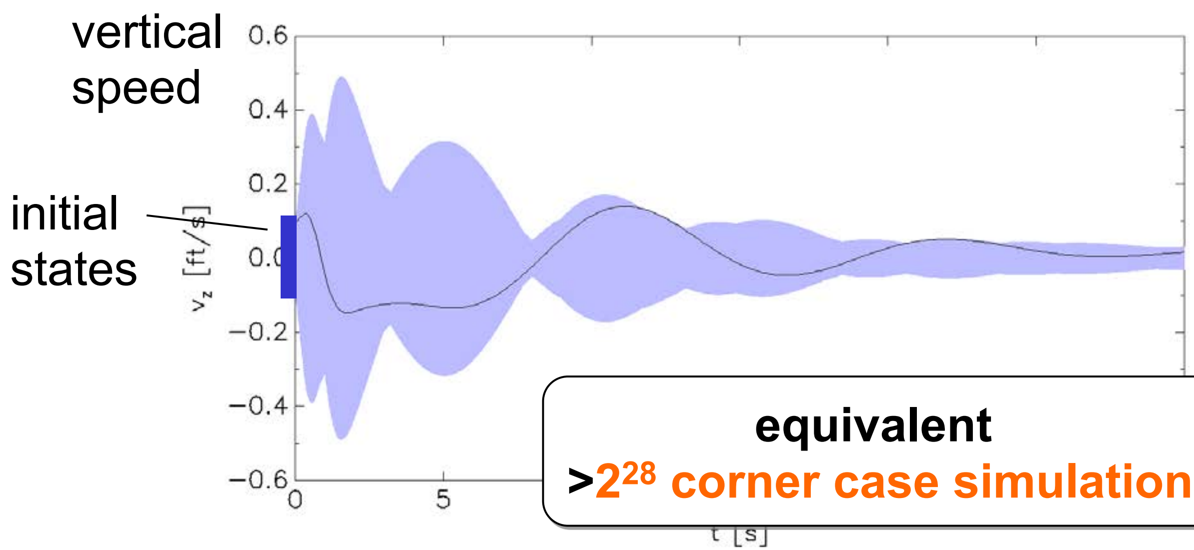
- **Simulation**
  - **single** behavior
- **Reachability**
  - cover of **all** behaviors



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



equivalent
>2^{28} corner case simulations

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^m vertices

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

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^m vertices

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

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

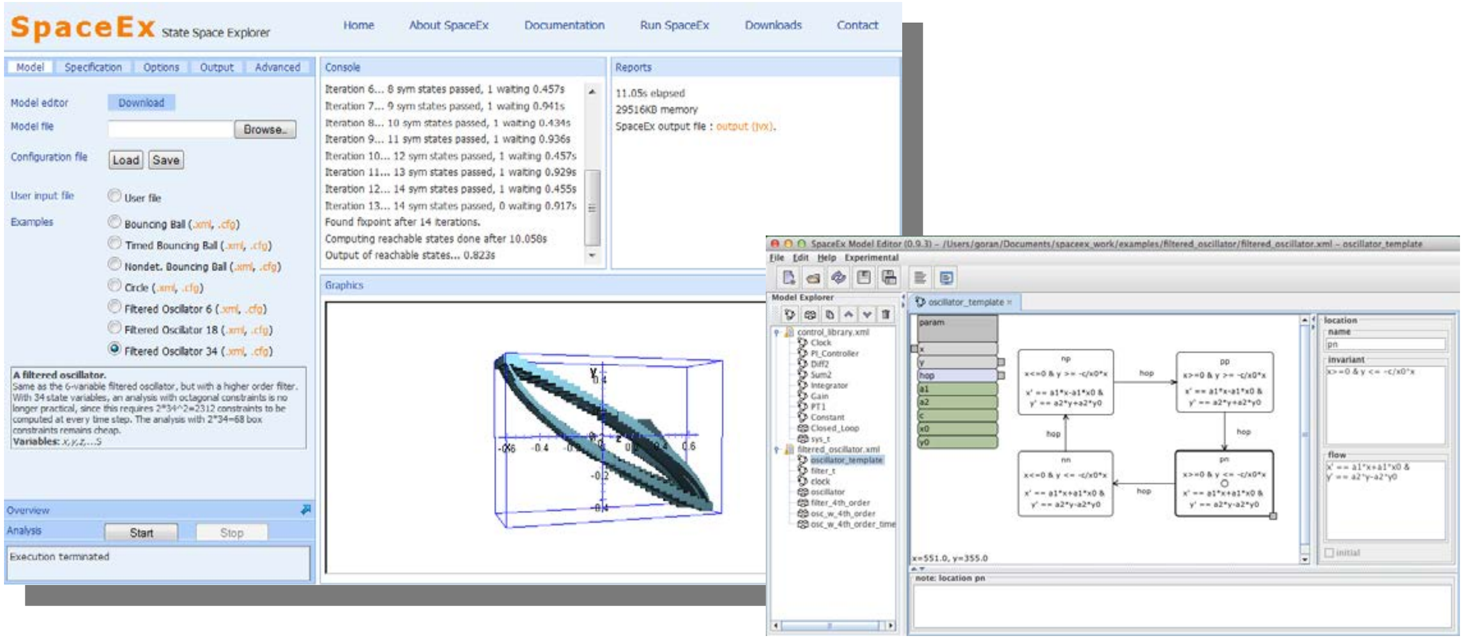
$T\, O(n^3)$ ***operations***

Outline

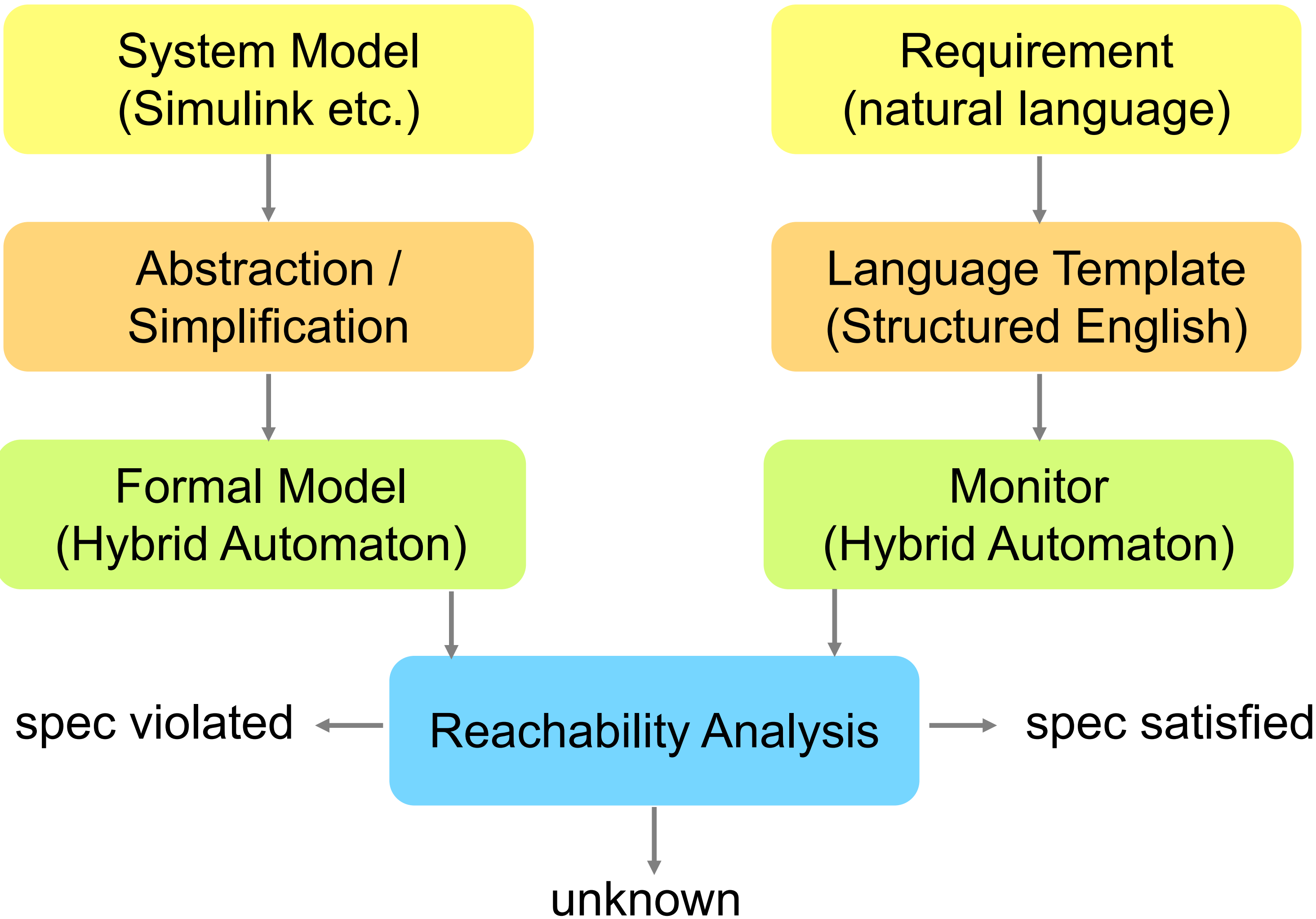
- Modeling Complex Systems
- Set-based Verification vs Simulation
- **Template Reachability in SpaceEx**
- Dealing with Unpredictability
- Conclusions and Perspectives

SpaceEx Verification Platform

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

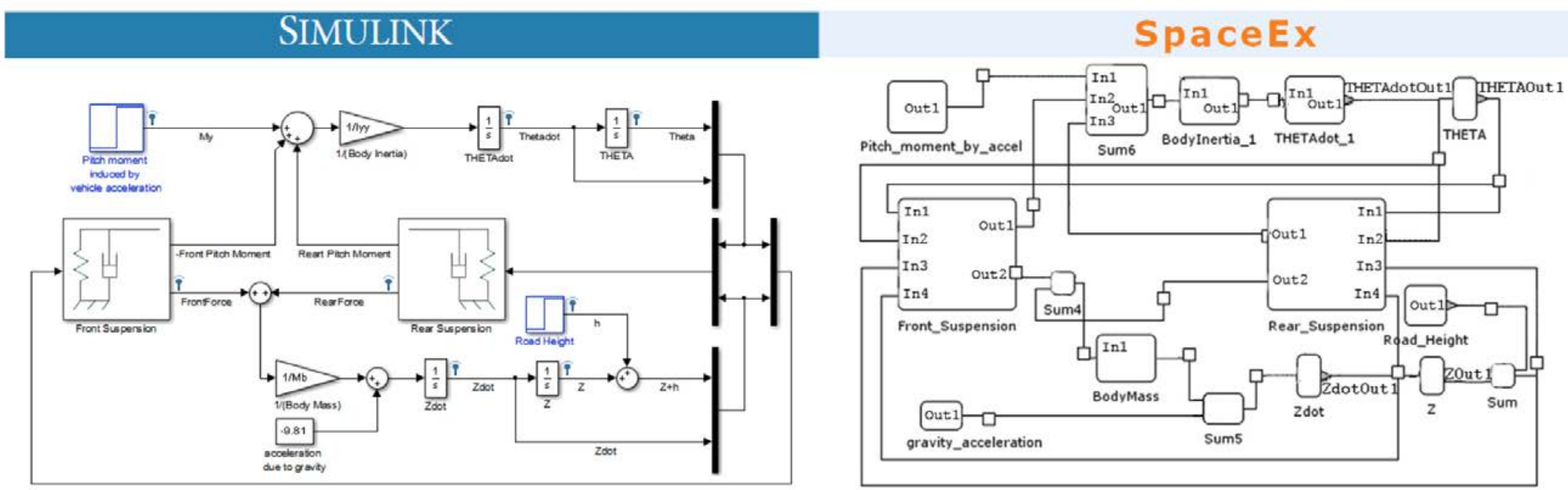


SpaceEx Verification Workflow



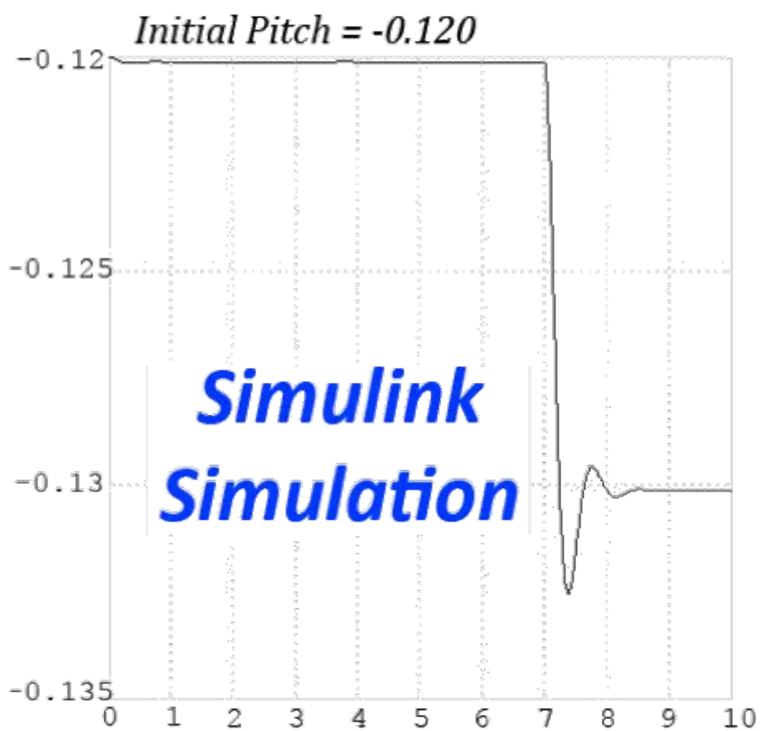
SL2SX: Translating Simulink to SpaceEx

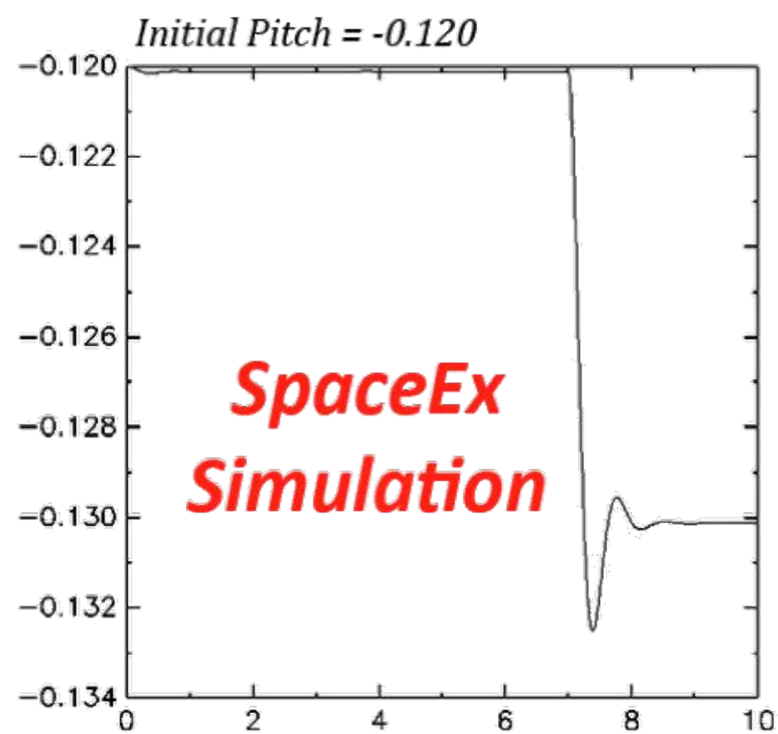
- **semi-automatic, gentle subset of Simulink**
  - continuous time linear blocks
  - steps, switches, etc.



Automotive Suspension from Simulink Example Library

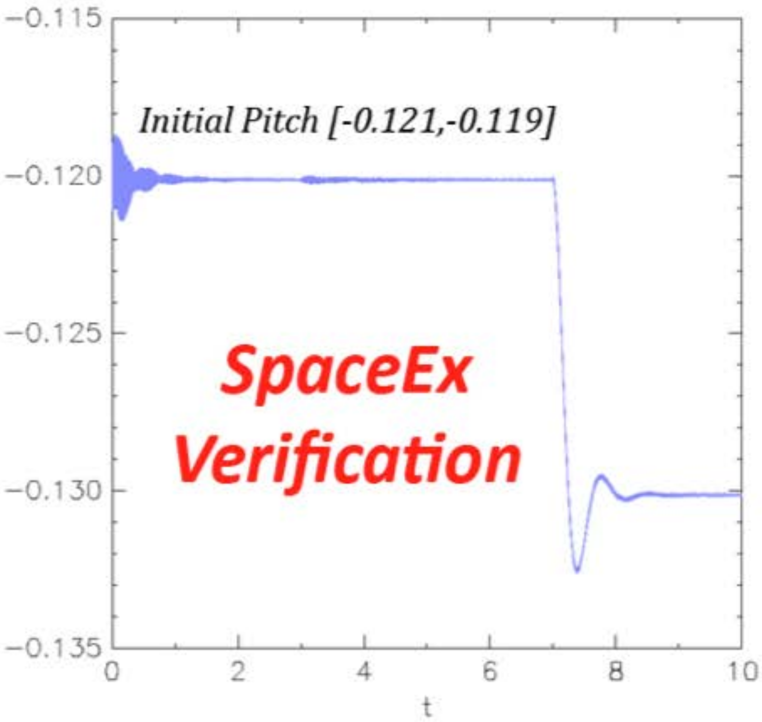
SL2SX: Translating Simulink to SpaceEx

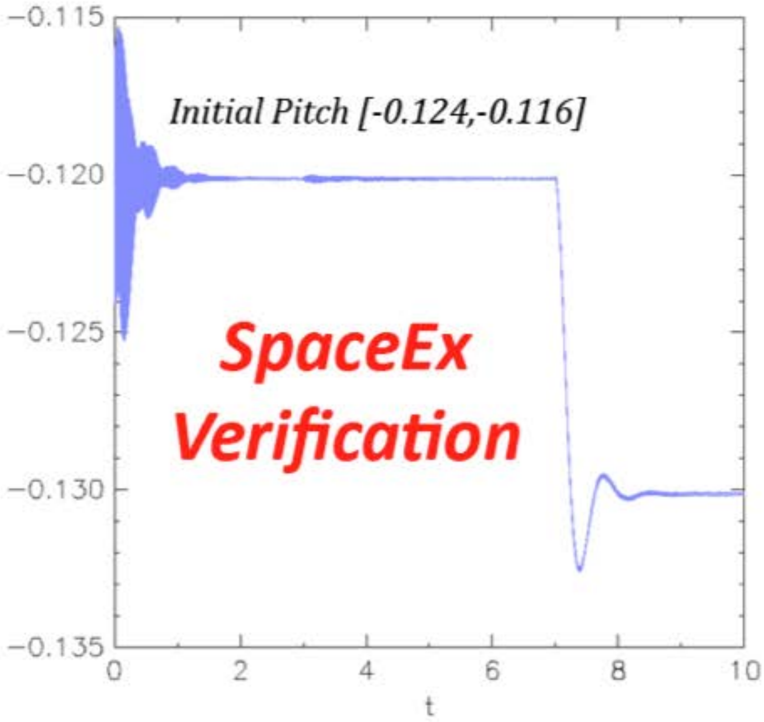




Automotive Suspension from Simulink Example Library

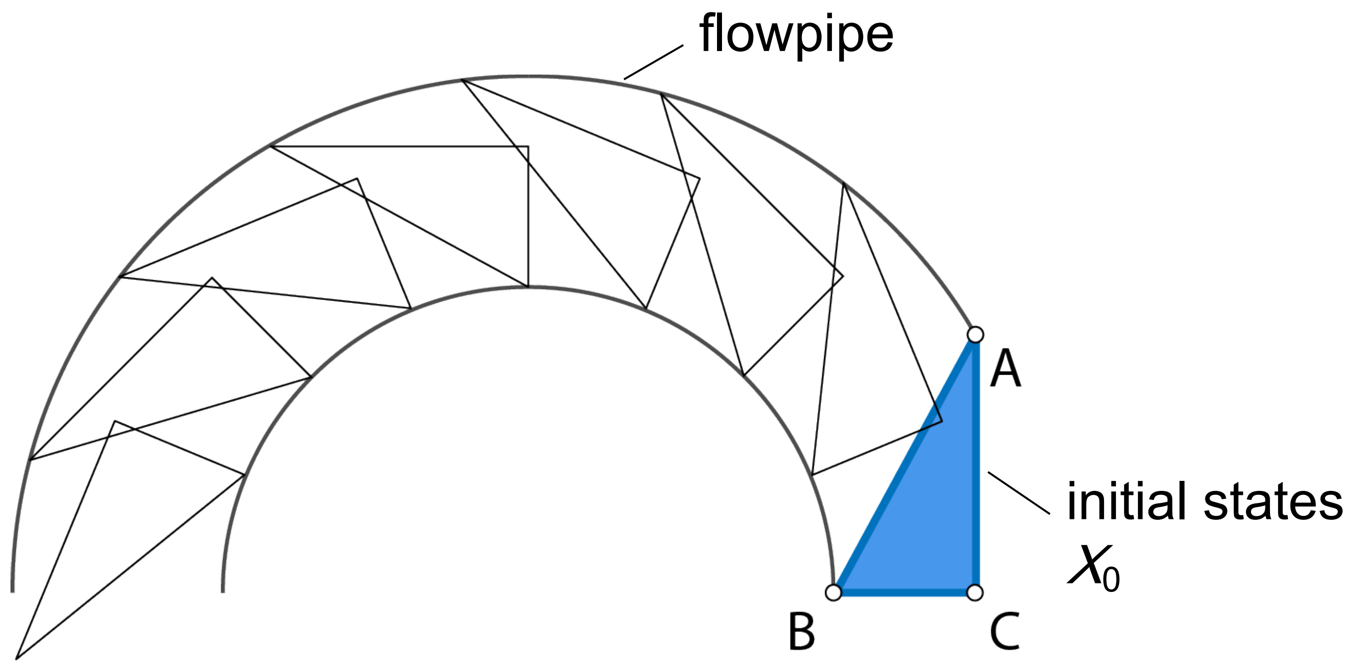
SL2SX: Translating Simulink to SpaceEx





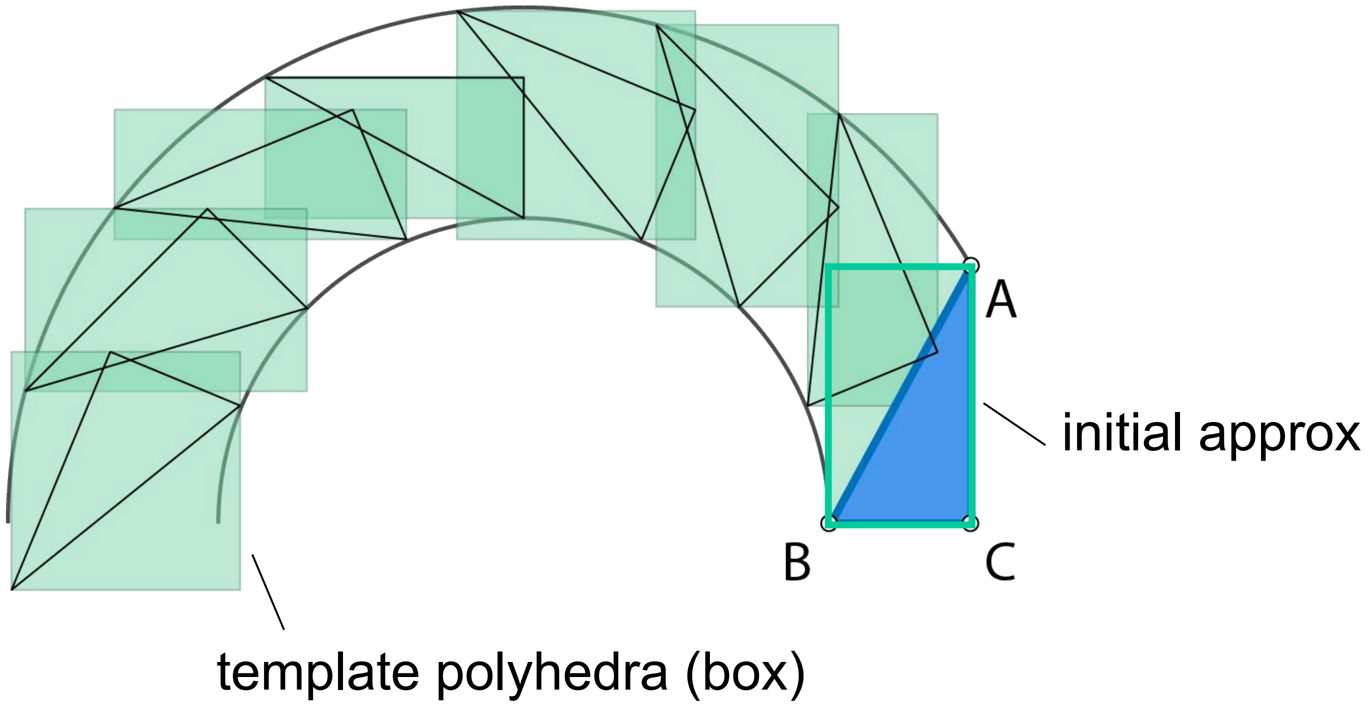
Automotive Suspension from Simulink Example Library

Reachable States over Time



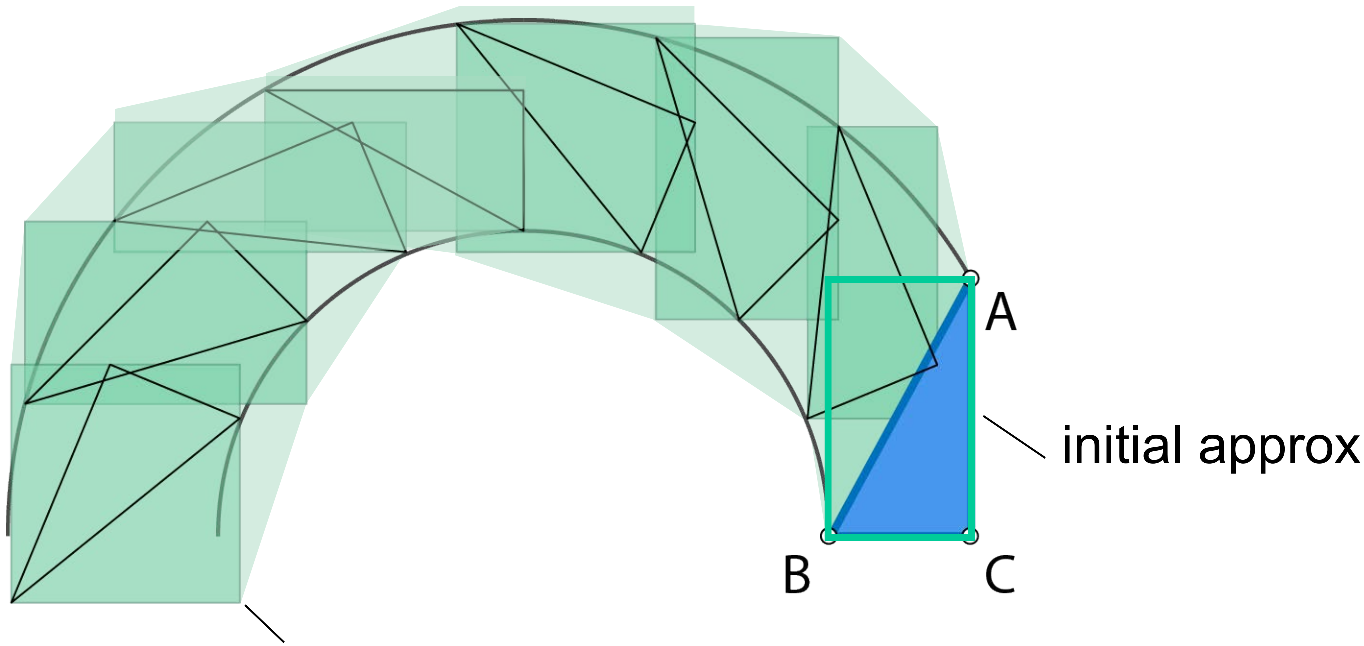
$$\dot{x}(t) = Ax(t) + u(t),$$
$$x(0) \in \mathcal{X}_0, u(t) \in \mathcal{U}$$

Template Reachability



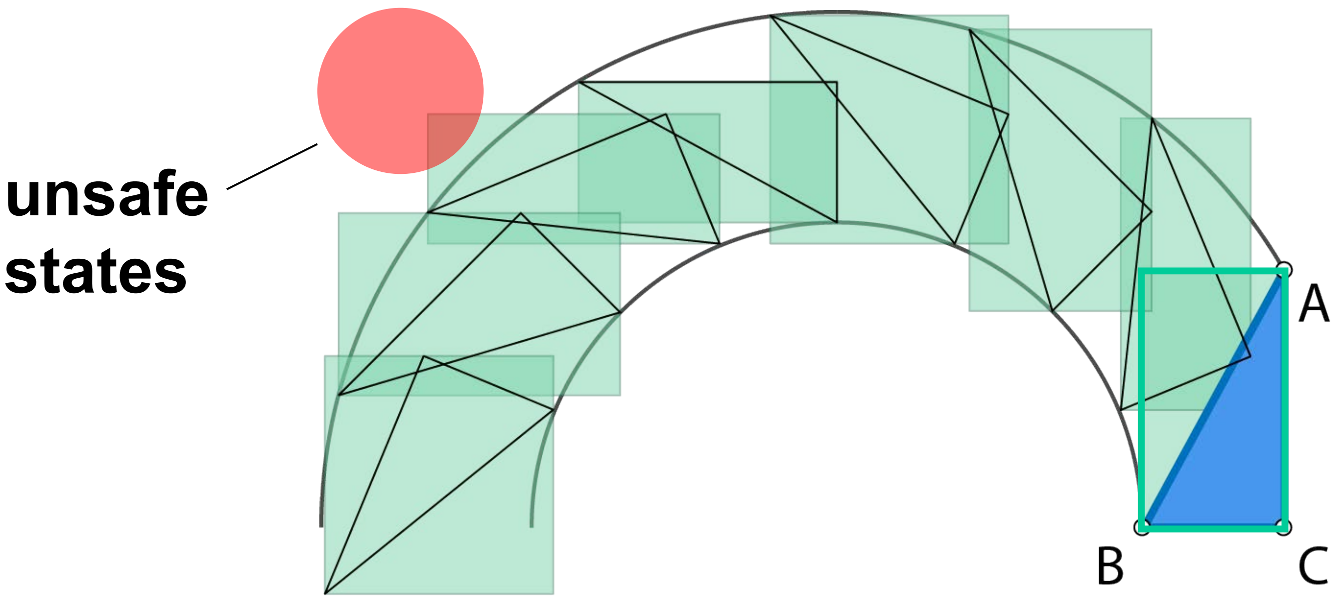
Girard and Le Guernic, 2008

Template Reachability



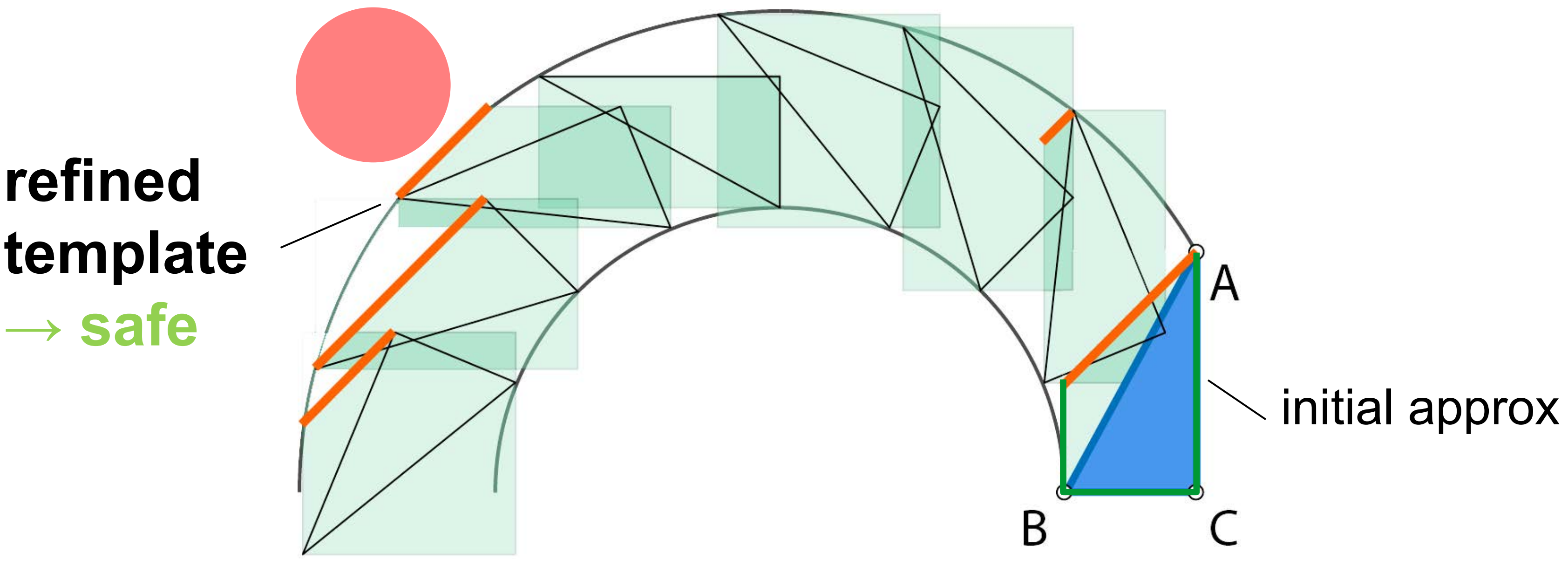
Girard and Le Guernic, 2008
Frehse, Le Guernic, Kateja, 2013

Template Reachability



Girard and Le Guernic, 2008

Template Reachability

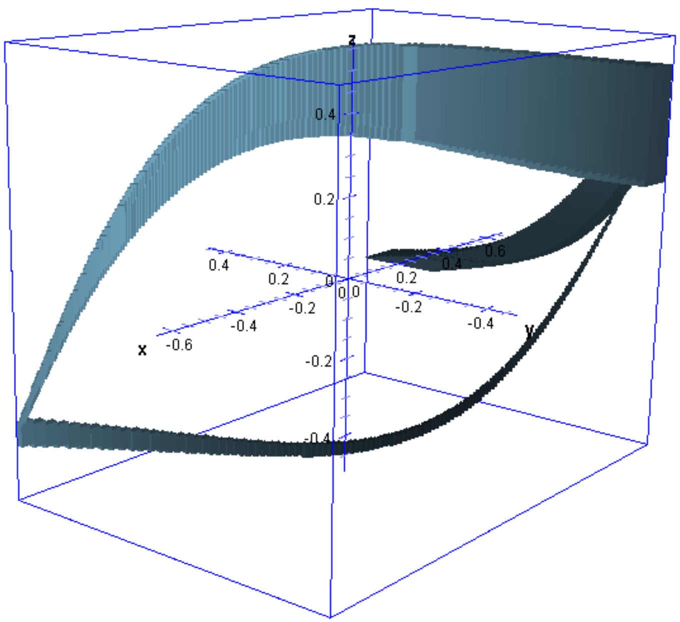


HSCC'15, TACAS'17, CAV'18

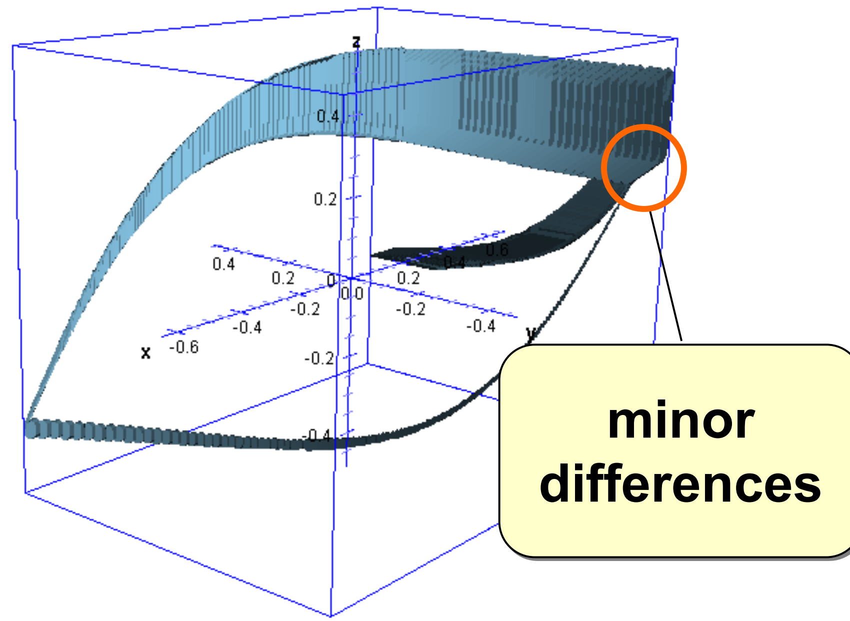
Example: Switched Oscillator

CAV'11

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



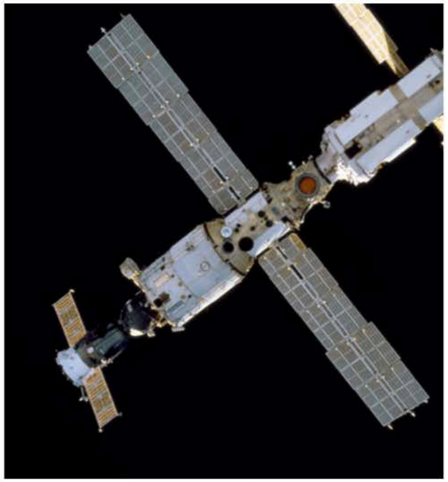
box directions

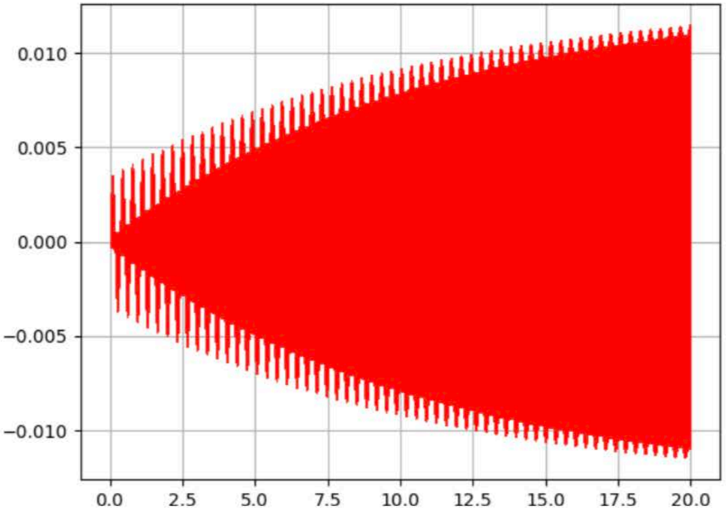


octagonal directions

6 x more work

Example: International Space Station





flexible body dynamics of Russian module of ISS[1]

270 variables, 3 nondet. inputs

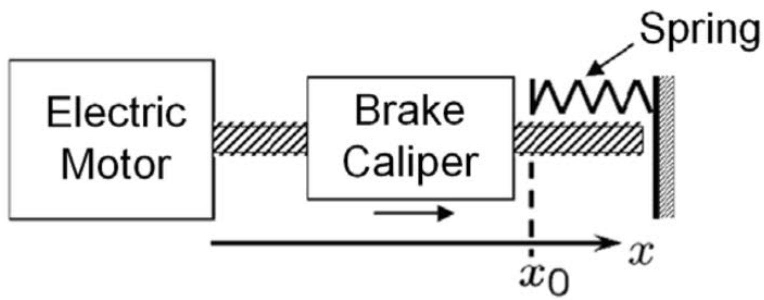
property with 1 variable: **40s**, with 270 variables: 45min

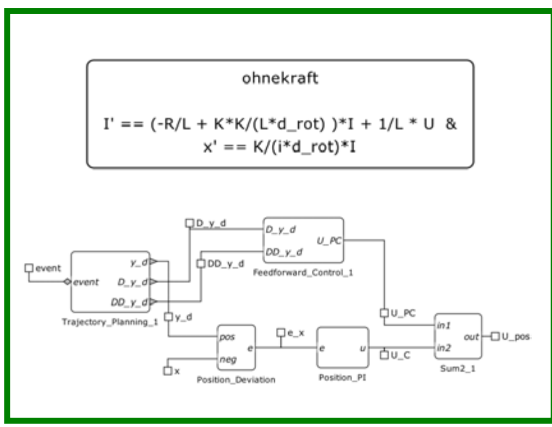
---

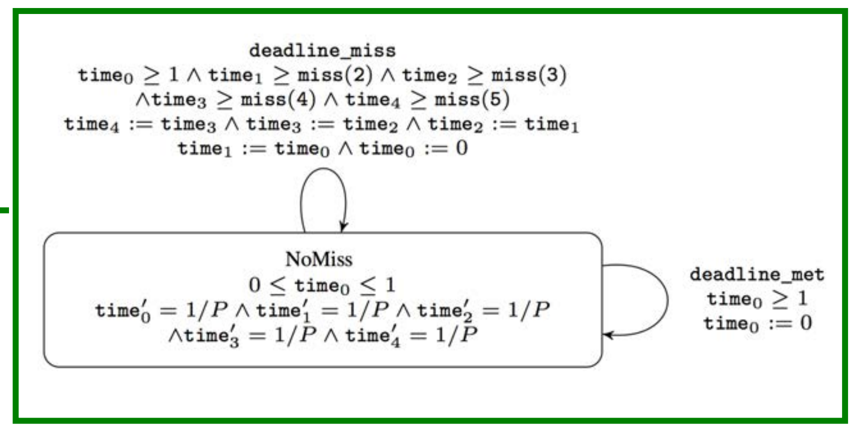
[1] Y. Chahlaoui and P. Van Dooren, "Benchmark examples for model reduction of linear time-invariant dynamical systems," in *Dimension Reduction of Large-Scale Systems*, Springer, 2005, pp. 379–392.

Case Study: Electro-Mechanical Brake

RTSS'14





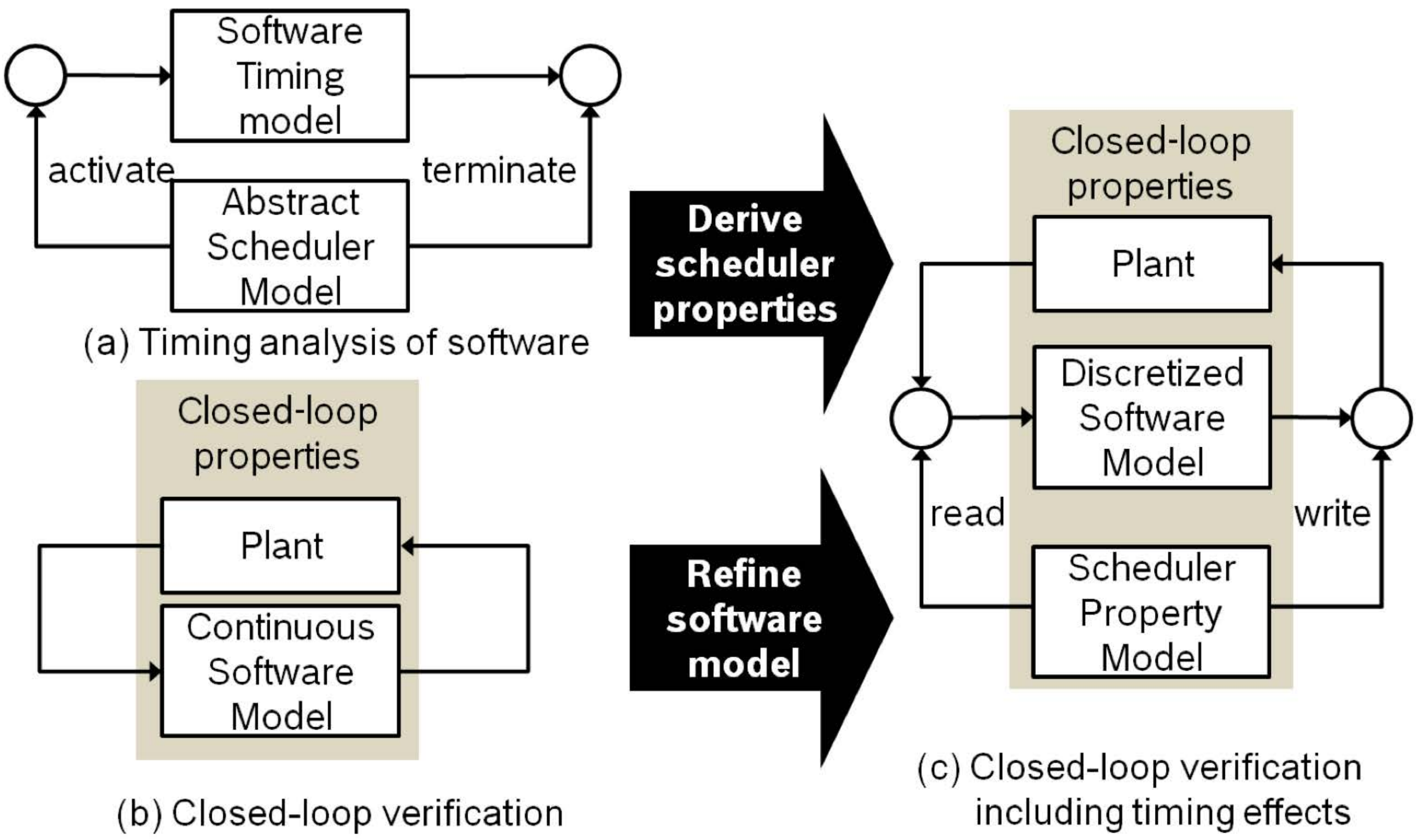


Plant & Controller

Scheduler (timed automaton)

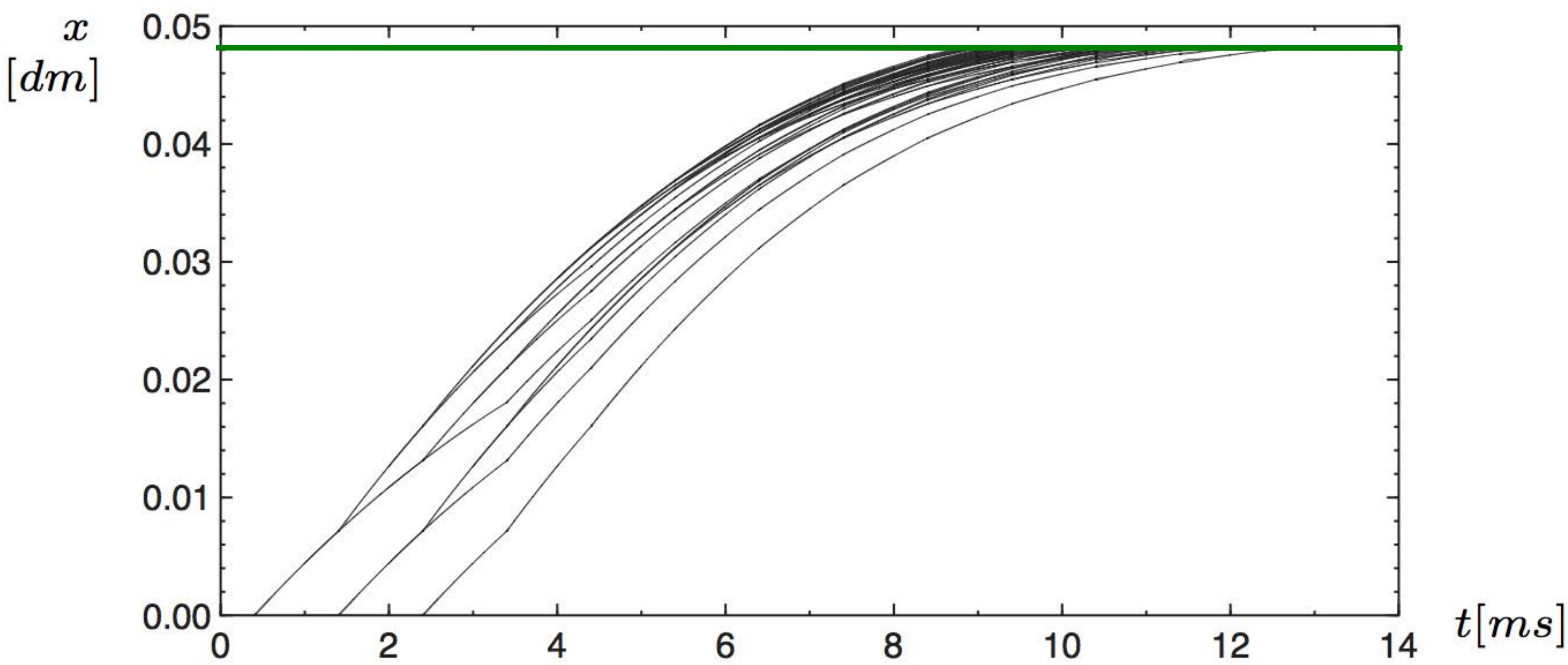
Frehse, Hamann, Quinton, Woehrle. Formal analysis of timing effects on closed-loop properties of control software. RTSS'14

Case Study: Electro-Mechanical Brake



Case Study: Electro-Mechanical Brake

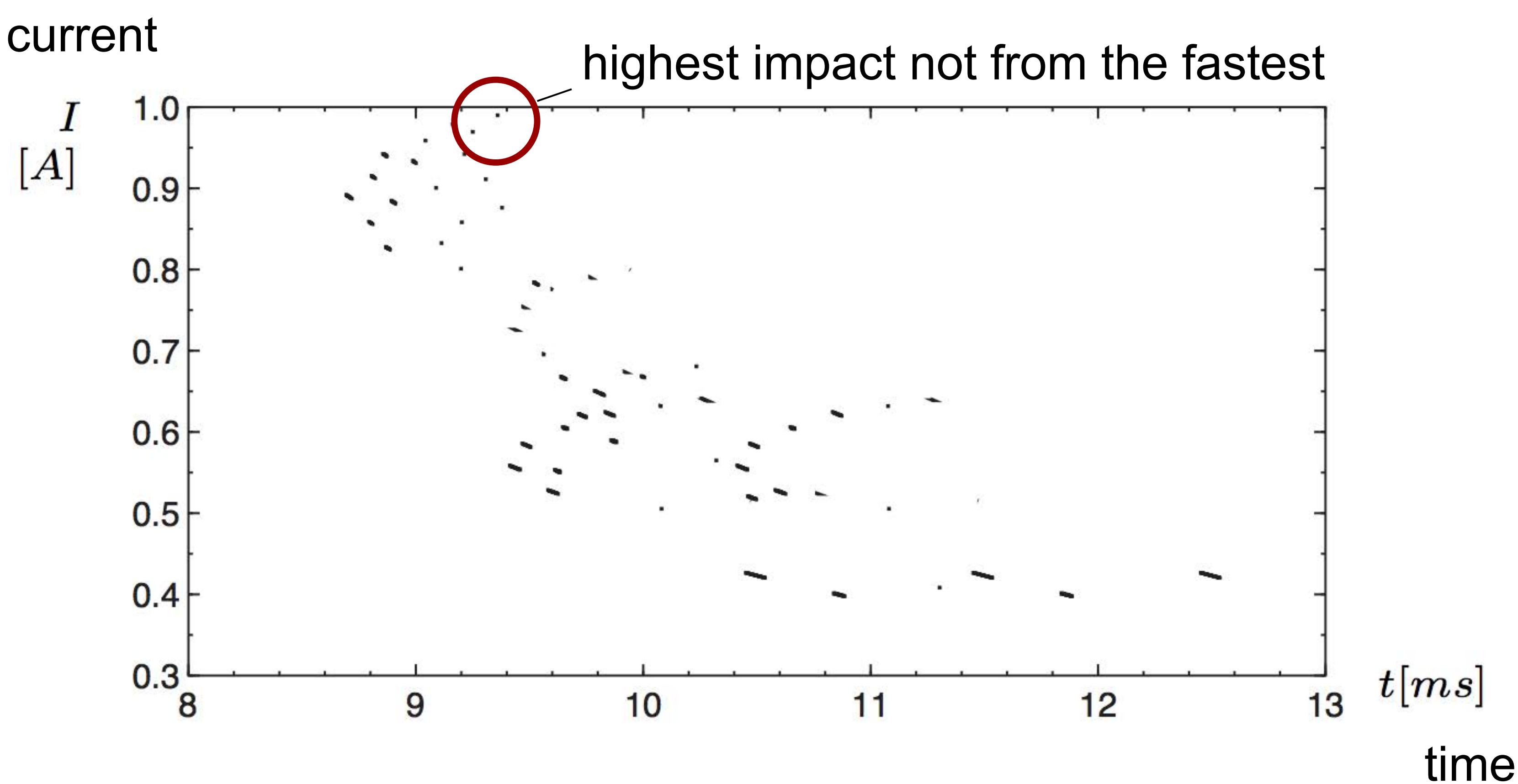
caliper position



verified: reaches target within 20ms

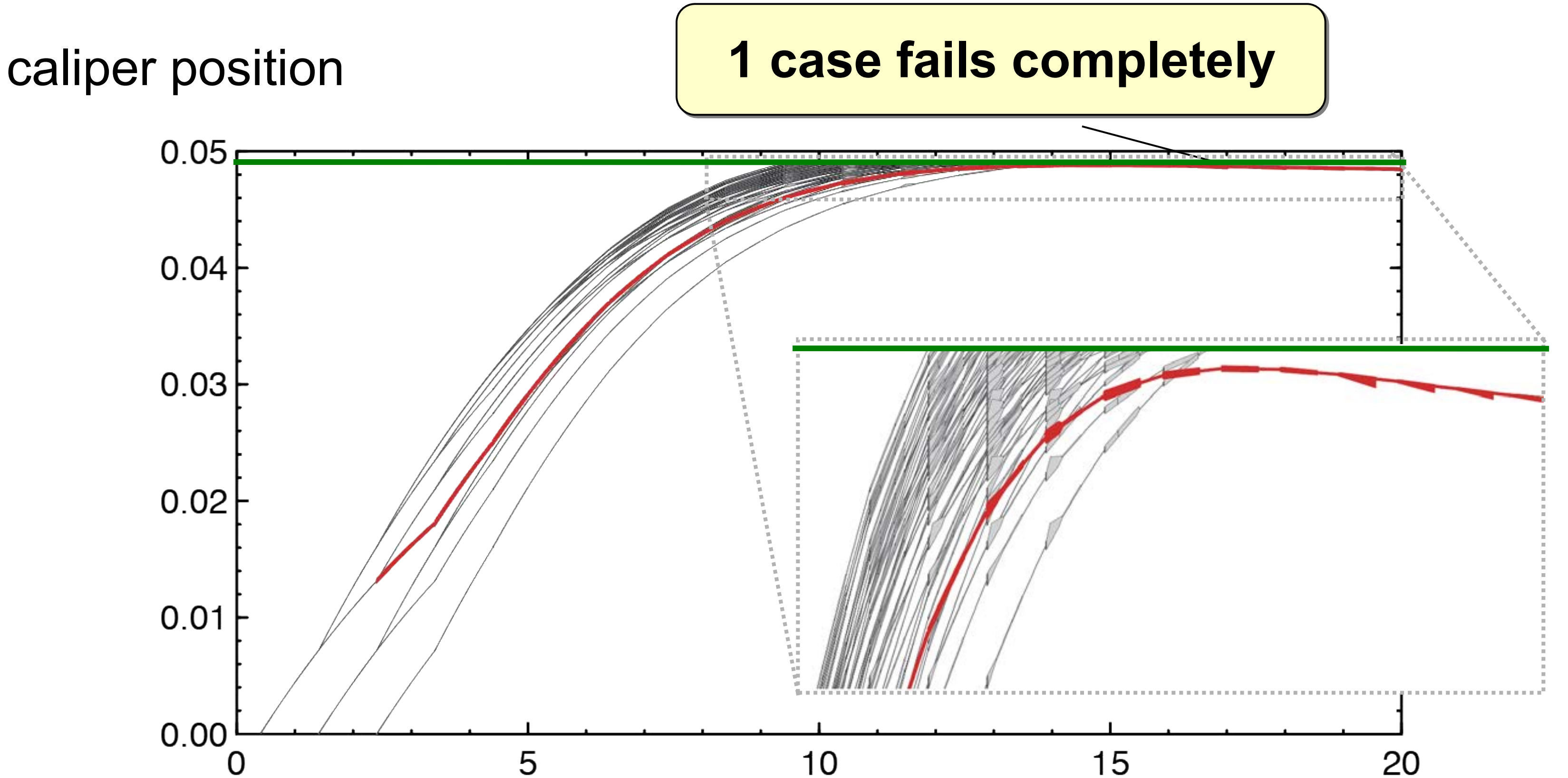
time

Case Study: Electro-Mechanical Brake



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

Case Study: Electro-Mechanical Brake



controller with (artificial) fault

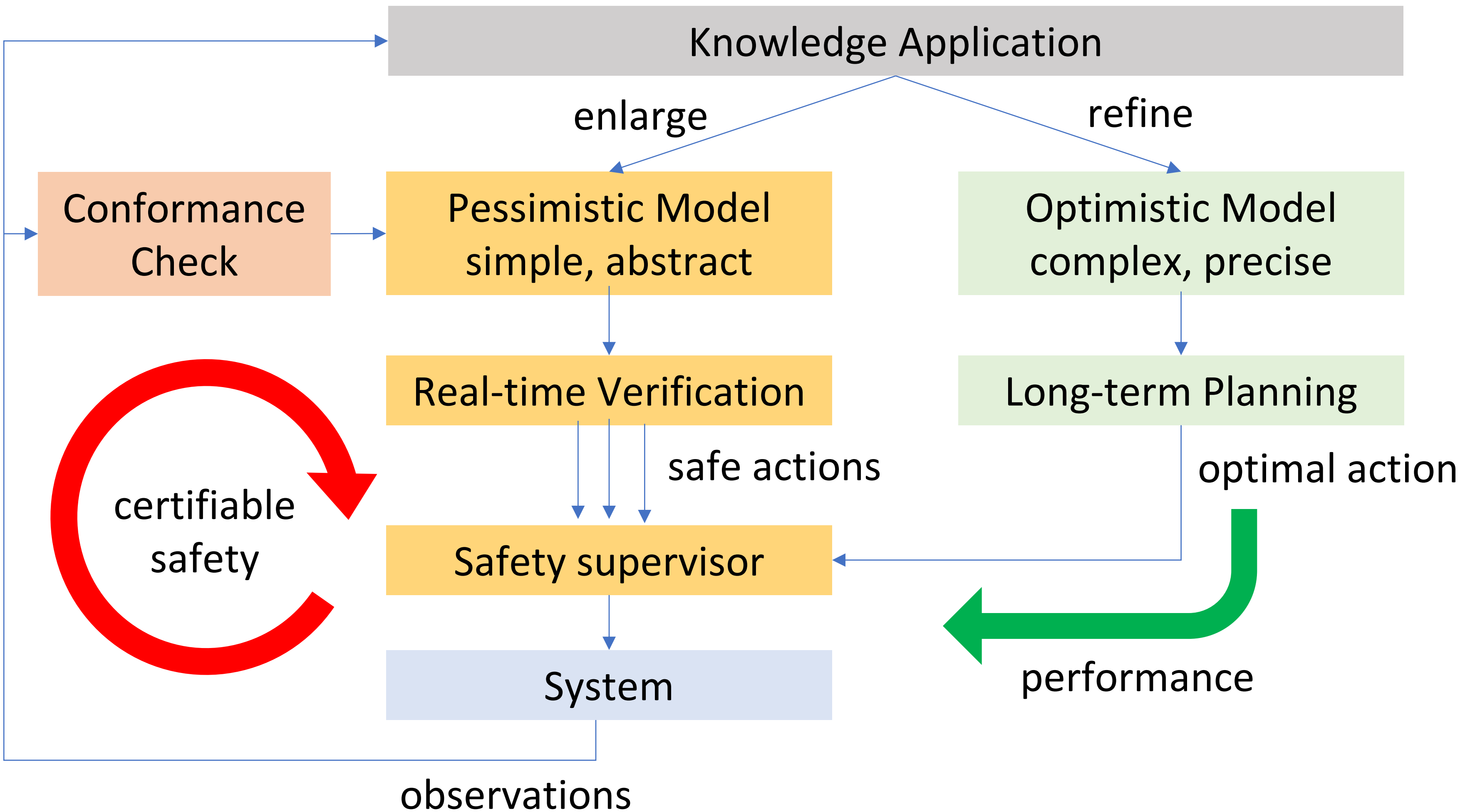
Outline

- Modeling Complex Systems
- Set-based Verification vs Simulation
- Template Reachability in SpaceEx
- **Dealing with Unpredictability**
- Conclusions and Perspectives

Unpredictability

- **How to deal with an unpredictable environment?**
  - **safe**
  - **adaptive**
  - **supervision**

Plan for the best, check for the worst



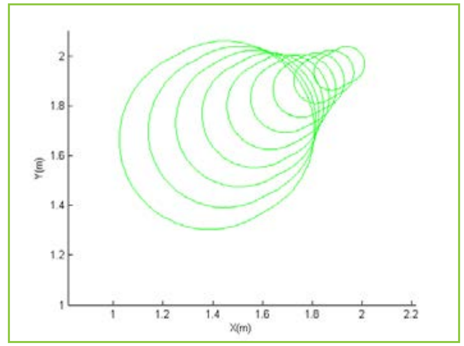
similar to QoS safety: Combaz, Fernandez, Sifakis, Strus. 2008
automated driving: Koschi, Althoff, 2017; Schürmann; Heß; Eilbrecht; Stursberg; Köster; Althoff, 2017

ONLINE REACHABILITY ANALYSIS

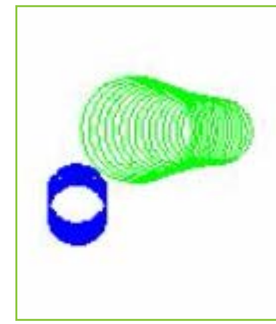
Althoff et al., 2018

$$\dot{p}_x = v_x$$
$$\dot{p}_y = v_y$$
$$\dot{v}_x = a_x$$
$$\dot{v}_y = a_y$$
$$\mathscr{U}_{ped}^{(a)} = \{(a_x, a_y) \in \mathbb{R} \times \mathbb{R} | a_x^2 + a_y^2 \leq a_{max}^2\}$$

Create Physical Model of Walking Pedestrian



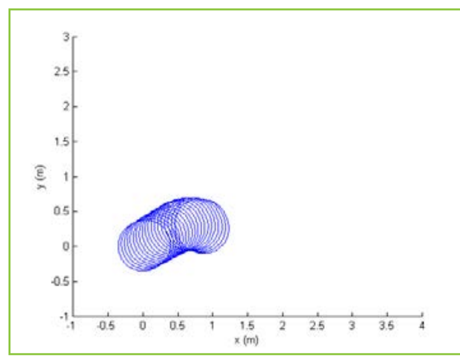
Compute Reachable Sets for each Pedestrian



Check for Possible Collisions

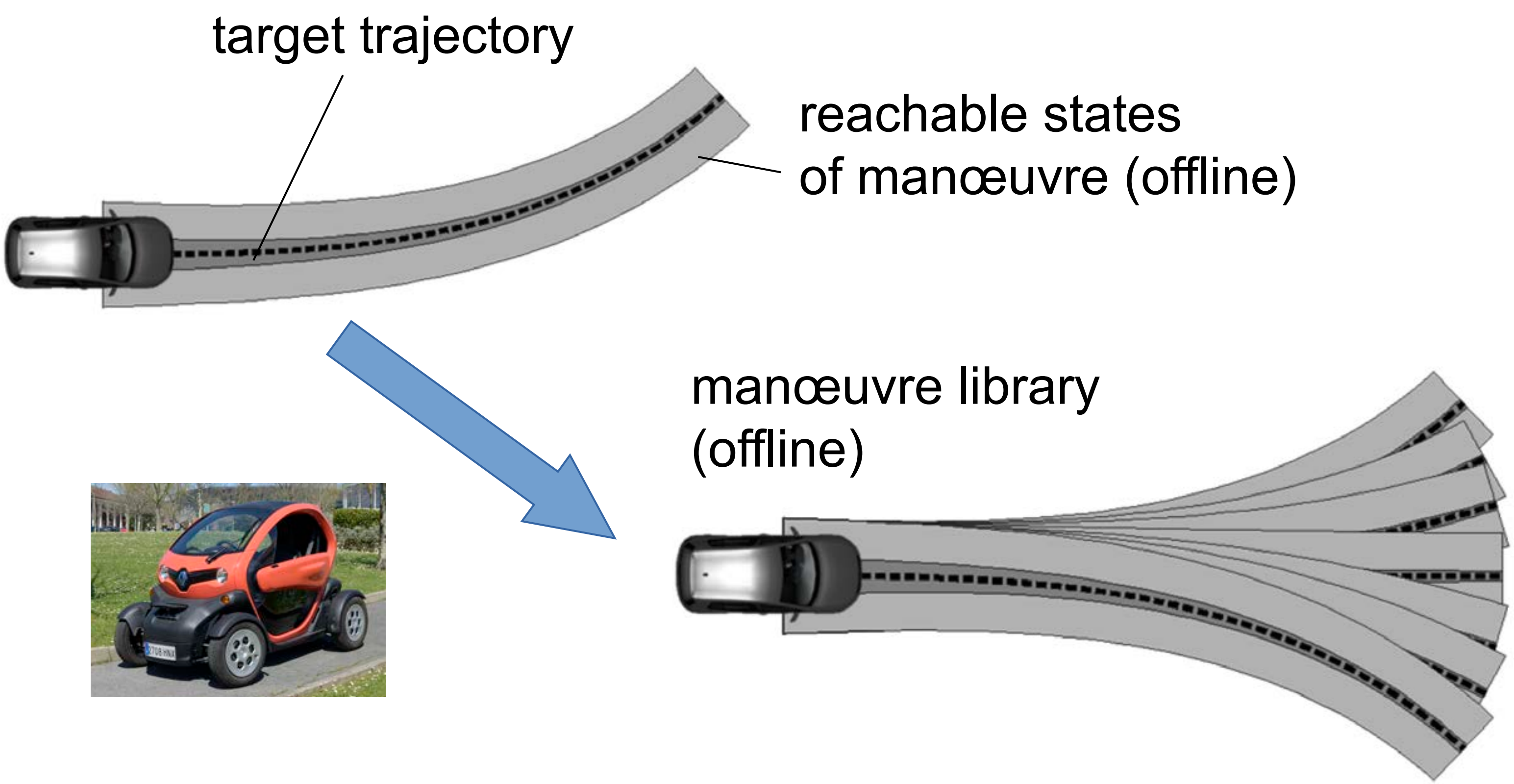
$$\dot{s}_1 = u_1 \cos s_3$$
$$\dot{s}_2 = u_1 \sin s_3$$
$$\dot{s}_3 = u_2$$

Create Physical Model of Robot



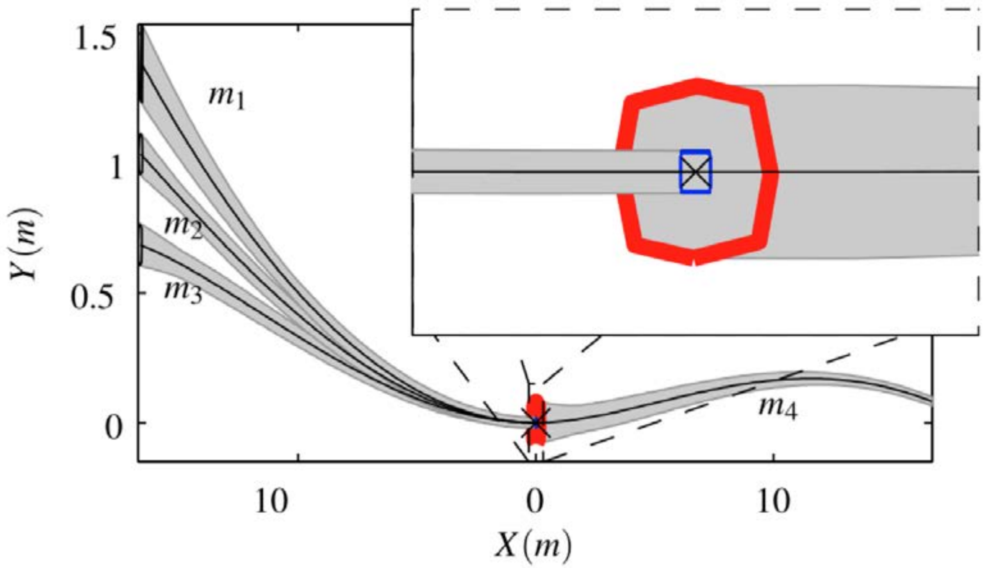
Compute Reachable Sets for Robot

Case Study: Automated Driving



Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016

Case Study: Automated Driving



reachability:
final states contained
in initial states

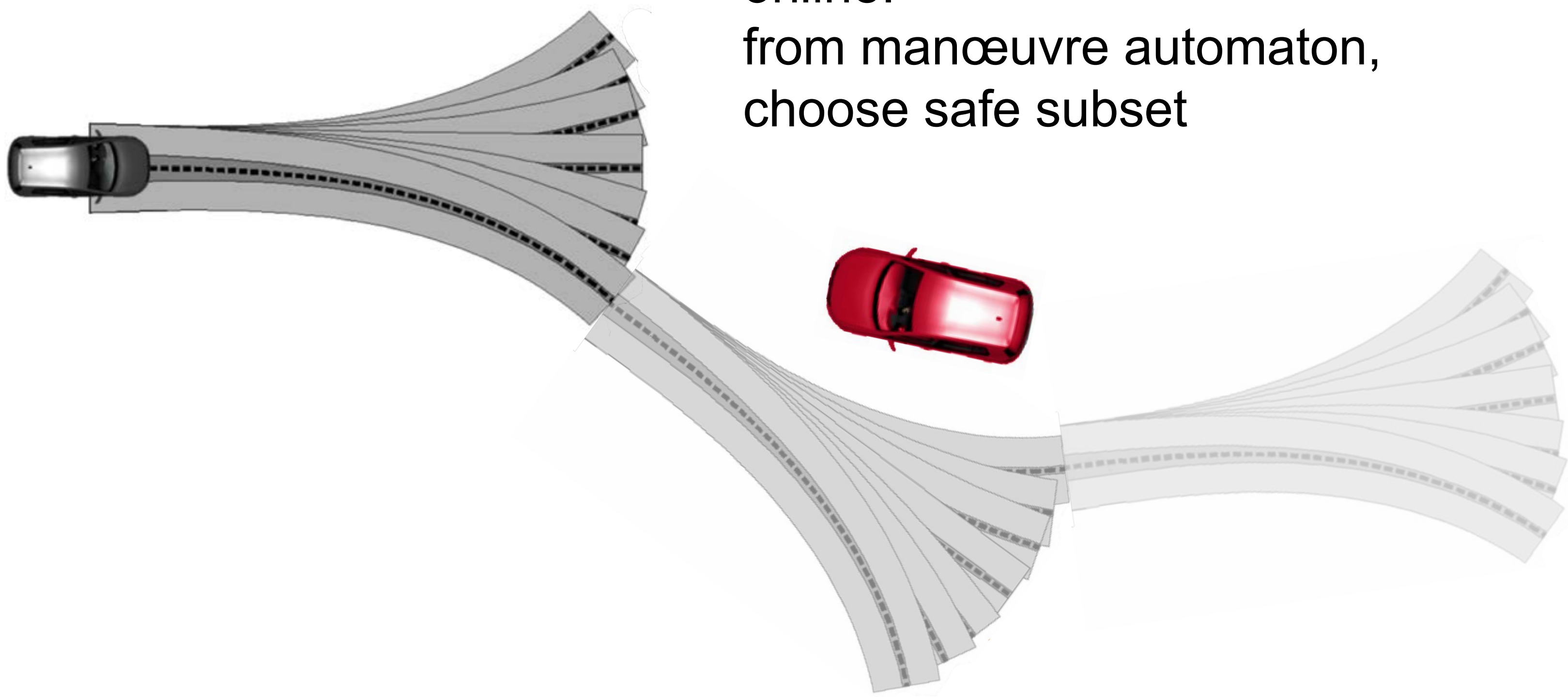
can be chained

manœuvre automaton

Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016

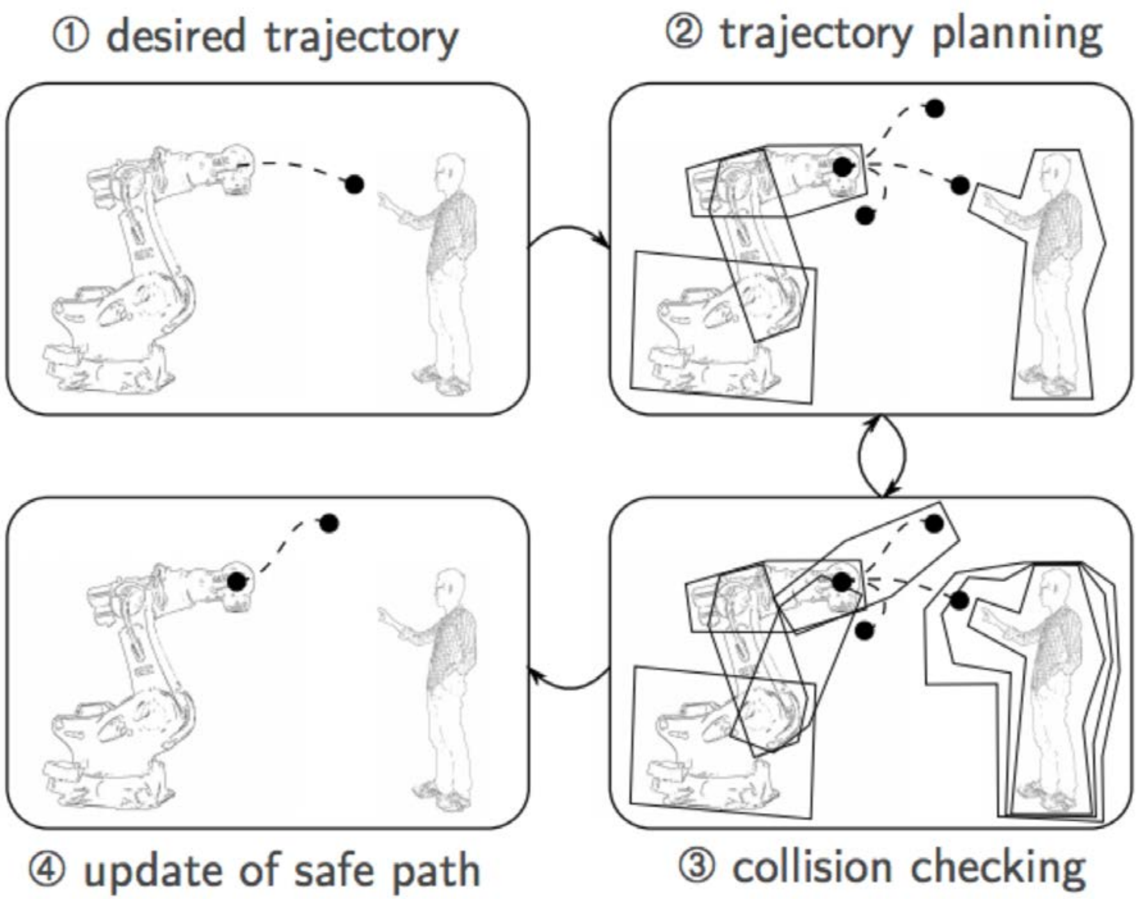
Case Study: Automated Driving

online:
from manœuvre automaton,
choose safe subset



Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016

Case Study:
Human-Robot Co-Existence

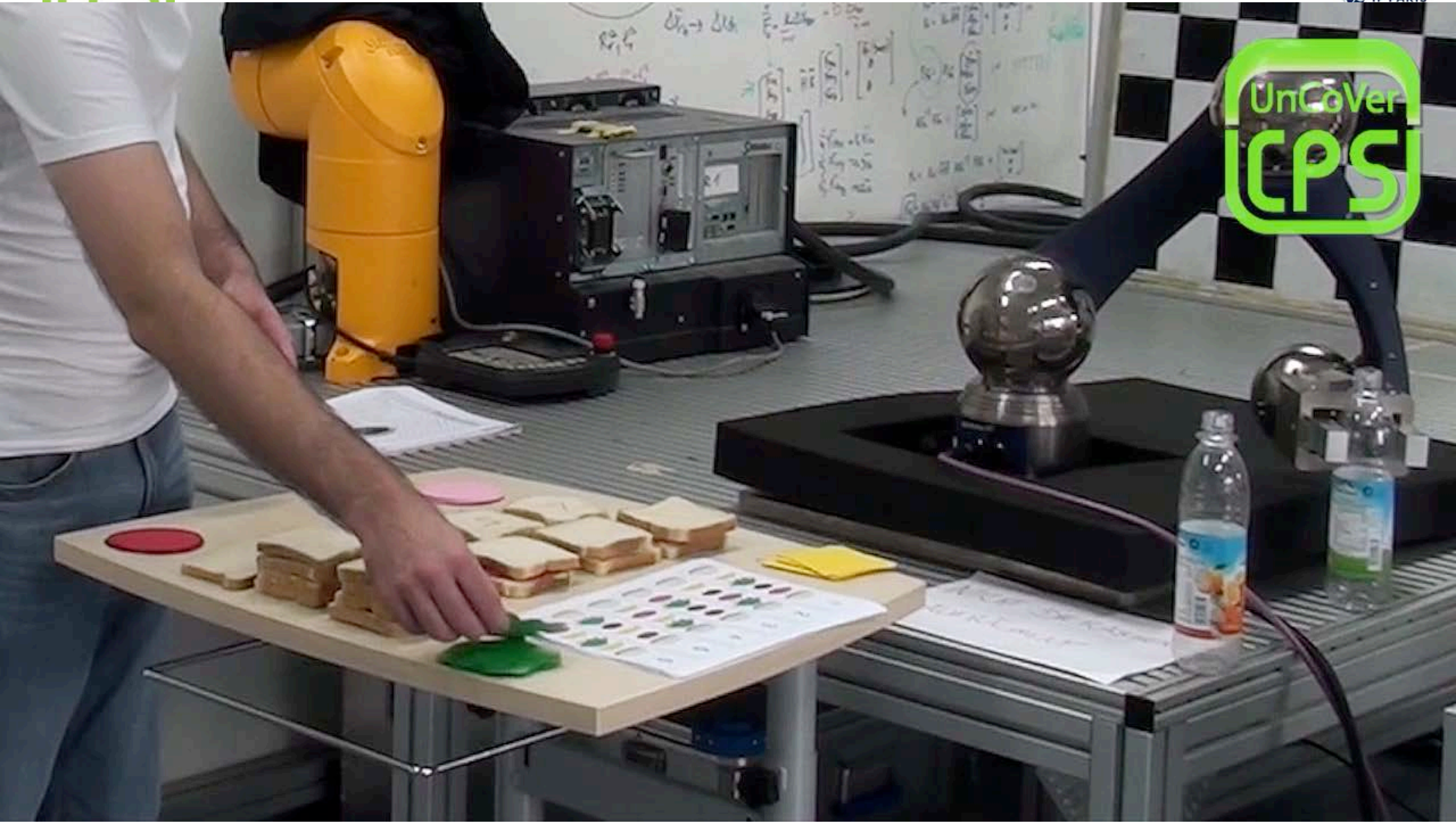


Matthias Althoff. Artemis Spring Event. http://road2cps.eu/events/wp-content/uploads/2015/10/UnCoVerCPS.pdf

Case Study:
Human-Robot Co-Existence

Experiment at TU Munich (Althoff et al.)

Case Study:



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

References

- Reachability
  - Chutinan, Krogh. Computing polyhedral approximations to flow pipes for dynamic systems.” CDC’98
  - Asarin, Bournez, Dang, Maler. Approximate reachability analysis of piecewise-linear dynamical systems. HSCC’00
  - Girard. Reachability of uncertain linear systems using zonotopes, HSCC’05
  - Le Guernic, Girard. Reachability analysis of hybrid systems using support functions. CAV’09
- SpaceEx
  - Minopoli, Frehse. SL2SX Translator: From Simulink to SpaceEx Verification Tool (Tool Paper). HSCC’16
  - Frehse, Le Guernic, Donzé, Cotton, Ray, Lebeltel, Ripado, Girard, Dang, Maler. SpaceEx: Scalable Verification of Hybrid Systems. CAV’11
- International Space Station
  - Althoff, Frehse, editors. ARCH19. Proceedings of 6th International Workshop on Applied Verification of Continuous and Hybrid Systems, EPiC Series in Computing, Volume 61, 2019, 219 pages
- Electro-Mechanical Brake
  - Frehse, Hamann, Quinton, Woehrle. Formal analysis of timing effects on closed-loop properties of control software. RTSS’14
- Online verification, Supervision
  - Combaz, Fernandez, Sifakis, Strus. Symbolic quality control for multimedia applications. Real-Time Systems, 40(1), 1-43.
  - Koschi, Althoff, Interaction-aware occupancy prediction of road vehicles. ITSC’17
  - Schürmann; Heß; Eilbrecht; Stursberg; Köster; Althoff, Ensuring drivability of planned motions using formal methods, ITSC’17
- Human-Robot Co-Existence
  - Matthias Althoff. Artemis Spring Event. http://road2cps.eu/events/wp-content/uploads/2015/10/UnCoVerCPS.pdf
- Automated Driving
  - Daniel Hess. Safe Vehicle Cooperation in UnCoVerCPS. 2016