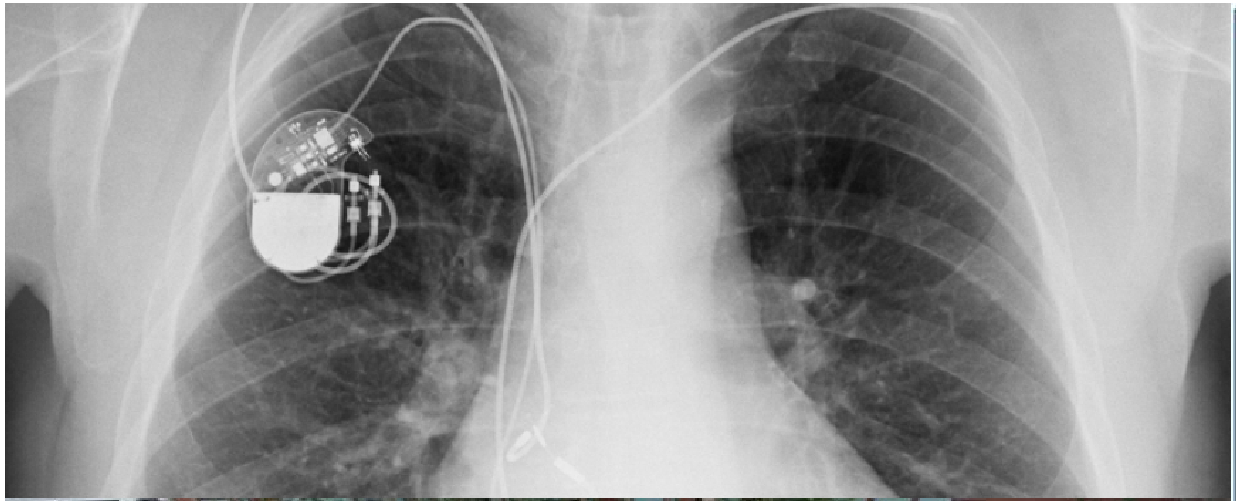
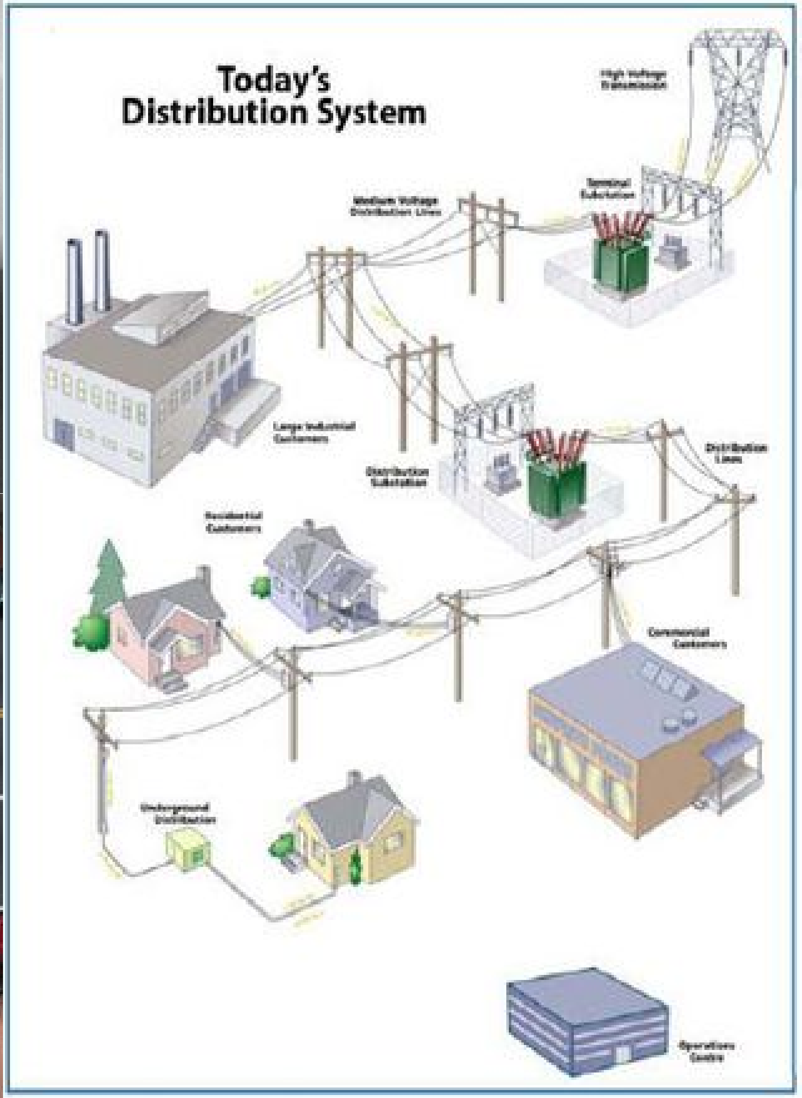
Verification from Simulations and Modular Annotations

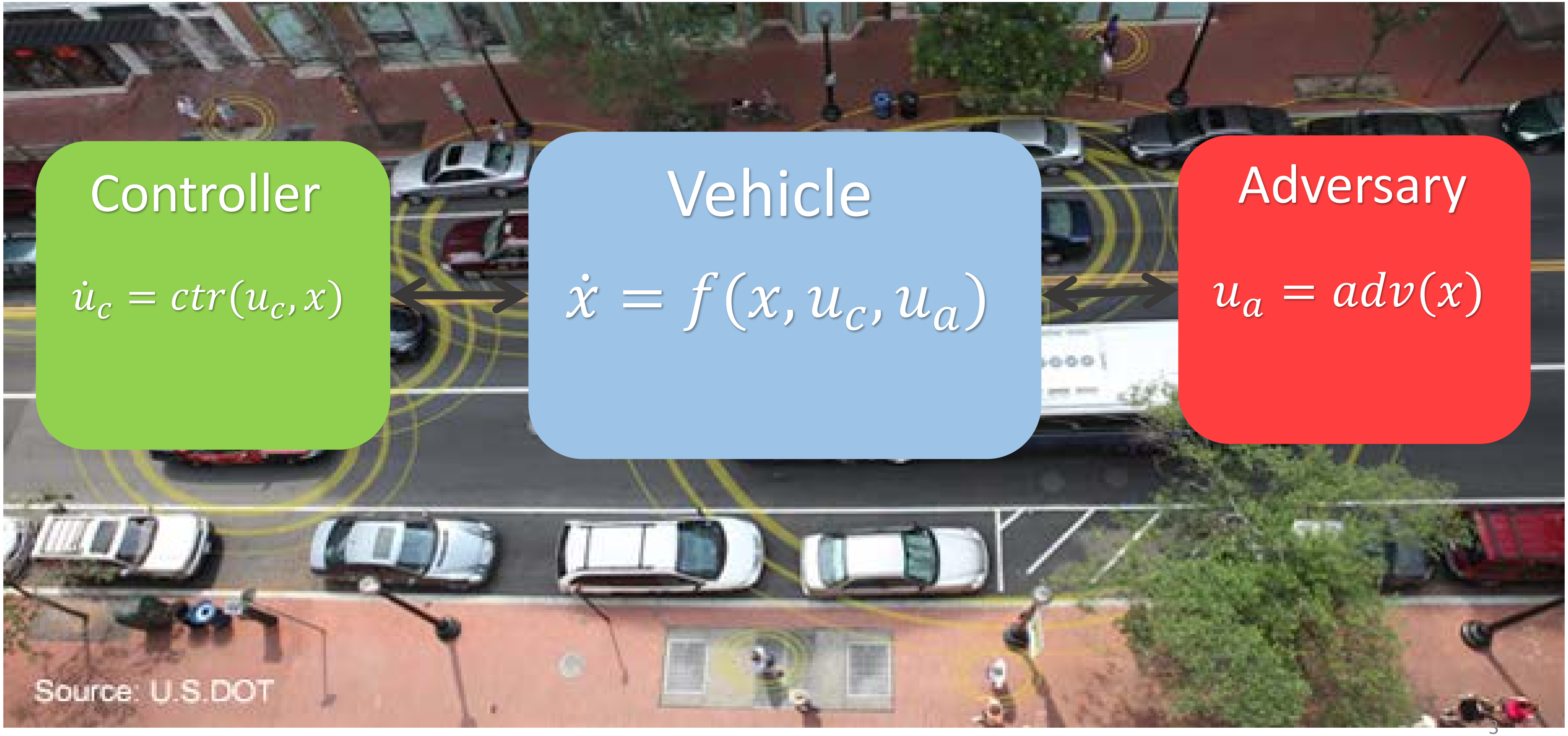
Zhenqi Huang, Yu Wang, Sayan Mitra and Geir Dullerud
Coordinated Science Lab
University of Illinois at Urbana-Champaign

Composed Safety-critical CPS





Safety under Adversary



Invariant Verification

Computing reach set exactly is undecidable [Henzinger]

- Over-approximations
- Bounded time

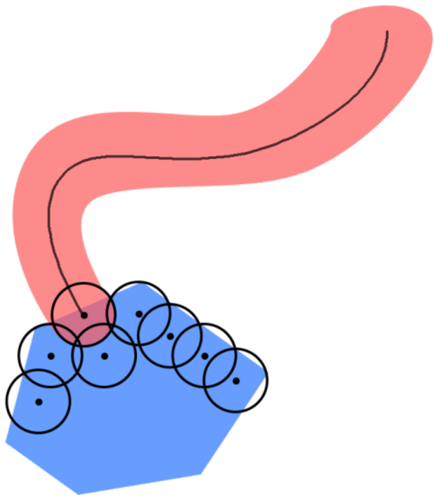
- Static analysis and symbolic approaches
  - E.g. HyTech[Henzinger97], CheckMate[Silva00], d/dt[Dang98], SpaceEx[Frehse11], flow*[Chen13]

- Dynamic+Static analysis using numerical simulations
  - E.g. Breach[Donzé10], S-TaLiRo[Annapureddy11], C2E2[Duggirala13]

Simulation-Based Bounded Reachability

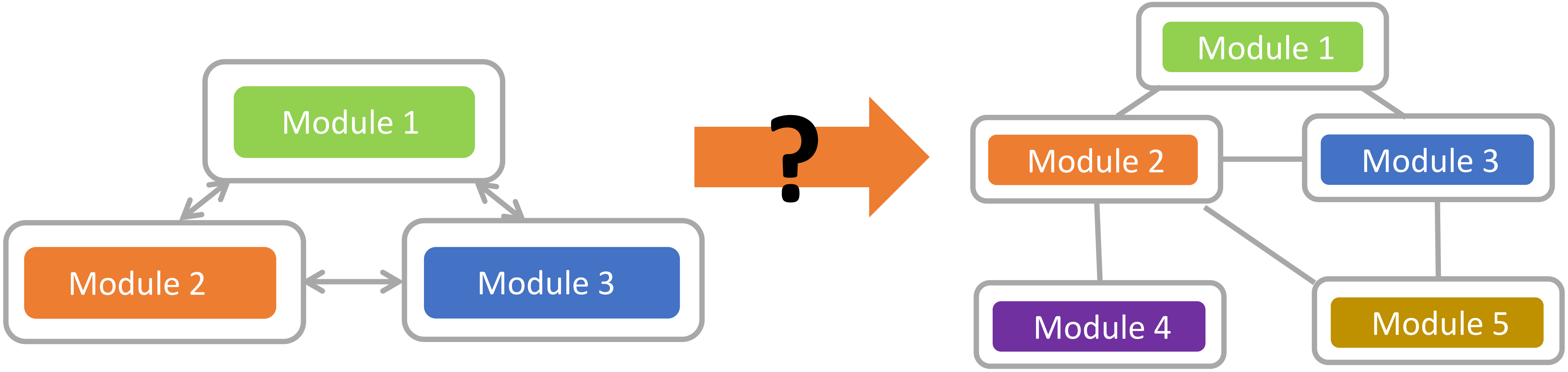
$$\dot{x} = f(x), \Theta \subseteq R^n$$

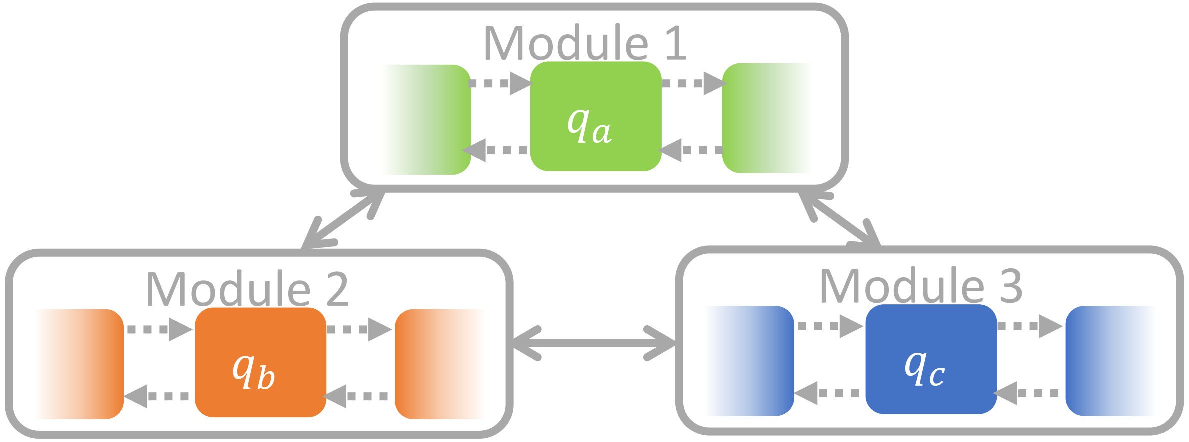
- Finite cover of Θ
- Simulate from the center of each cover
- Bloat the simulation with some factor, such that the bloated tube contains all trajectories starting from the cover
- Union of all tubes gives an over-approximation of reach set



The bloating factor can be computed using sensitivity analysis[Donzé07], or given as an annotation for the model[Duggirala13,Huang14].

Challenge

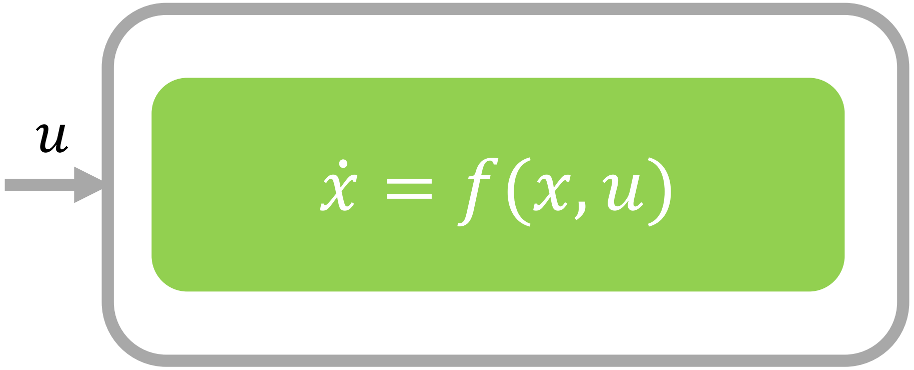


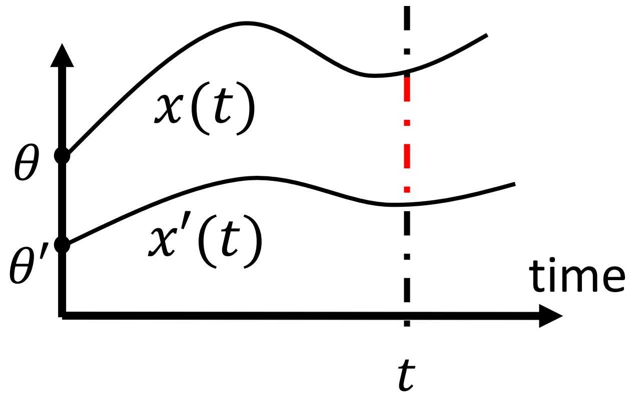


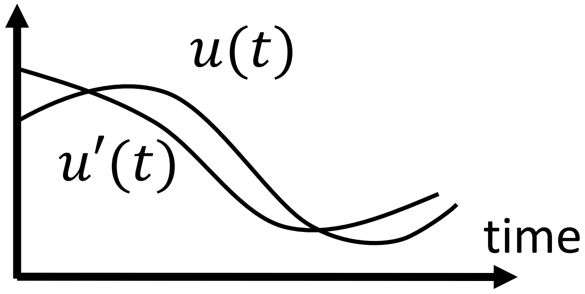
$$\begin{aligned} \dot{x}_1 &= f_a(x_1, x_2, x_3) \\ \dot{x}_2 &= f_b(x_2, x_1, x_3) \\ \dot{x}_3 &= f_c(x_3, x_1, x_2) \end{aligned} \quad \times L^N$$

We assume the network is annotated by the user per automaton per mode.

Annotation: Input-to-State (IS) Discrepancy





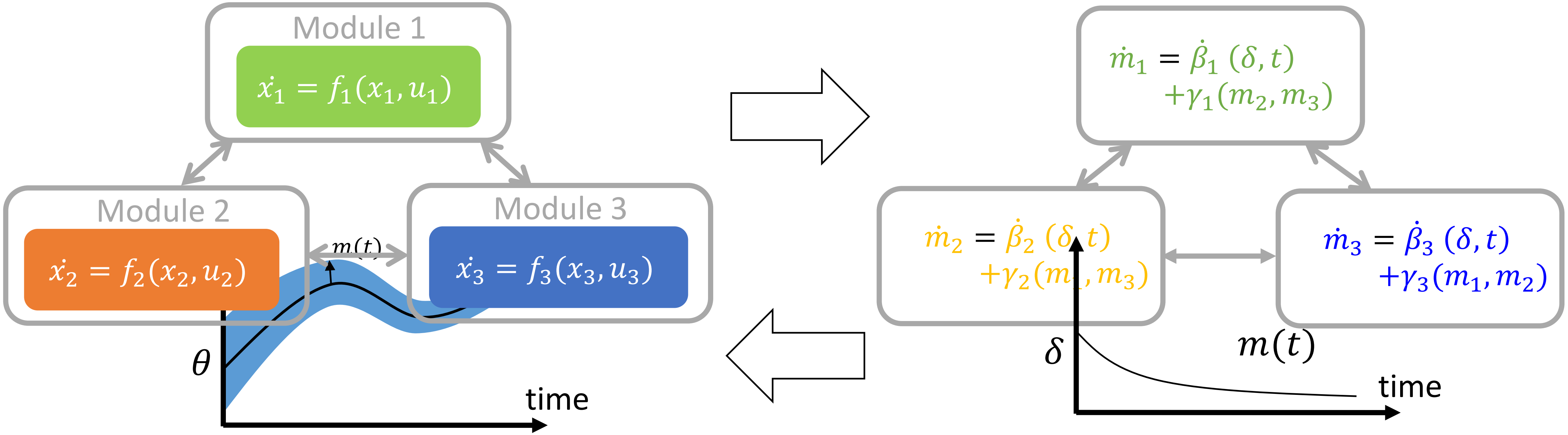


Definition[Duggirala13,Huang14]. IS discrepancy is defined by β and γ such that for any initial states θ, θ' and any inputs u, u',

$$|x(t) - x'(t)| \leq \beta(|\theta - \theta'|, t) + \int_0^t \gamma(|u(s) - u'(s)|)ds$$

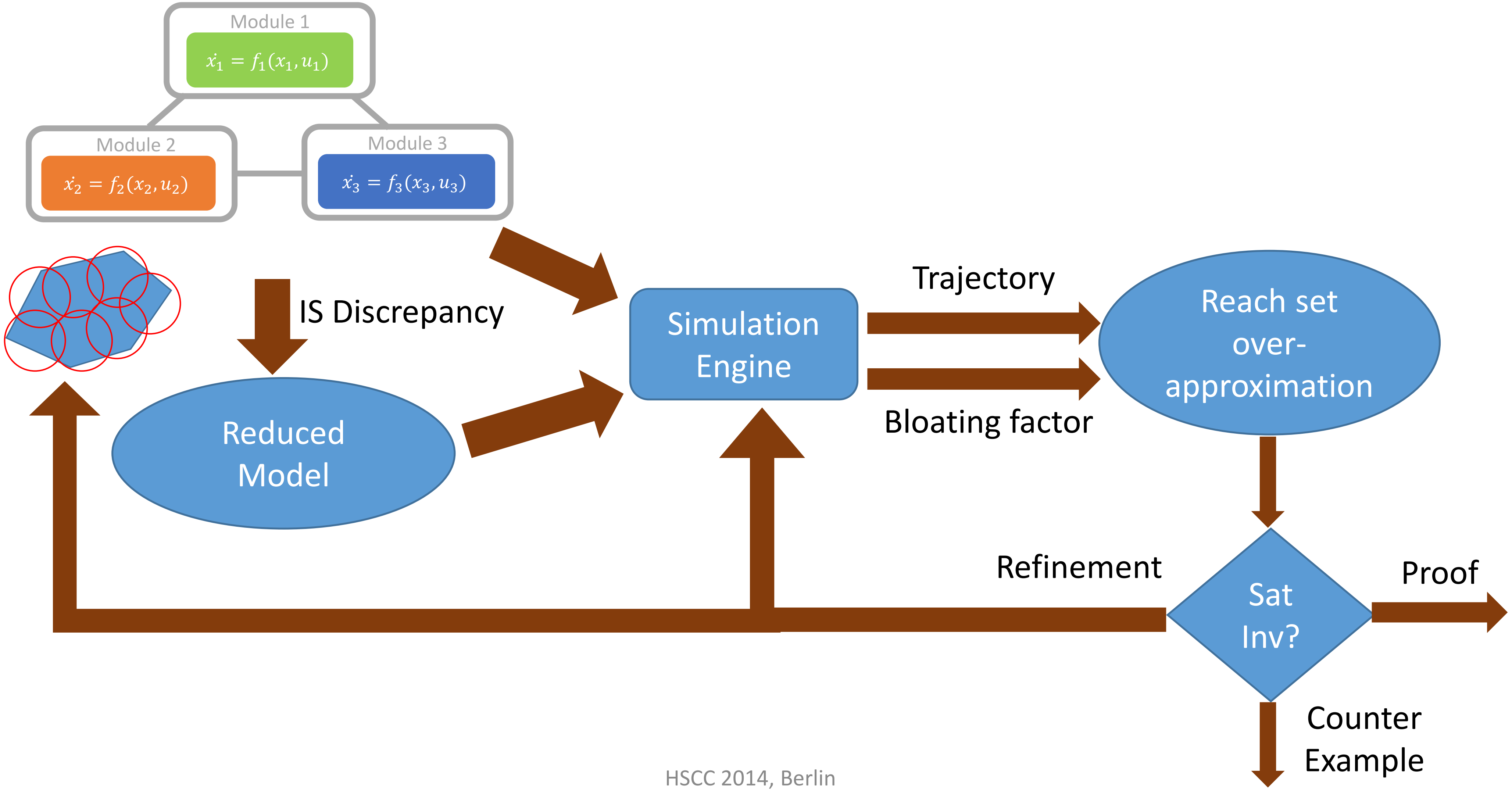
- $\beta \to 0$ as $\theta \to \theta'$, and $\gamma \to 0$ as $u \to u'$
- Linear $f()$: found automatically
- Nonlinear $f()$: several heuristics were proposed

Bloating a Trajectory with IS Discrepancy



- The bloated tube contains all trajectories start from the δ-ball of θ.
- The over-approximation can be computed arbitrarily precise.

Simulation & Modular Annotation $\Longrightarrow$ Proof

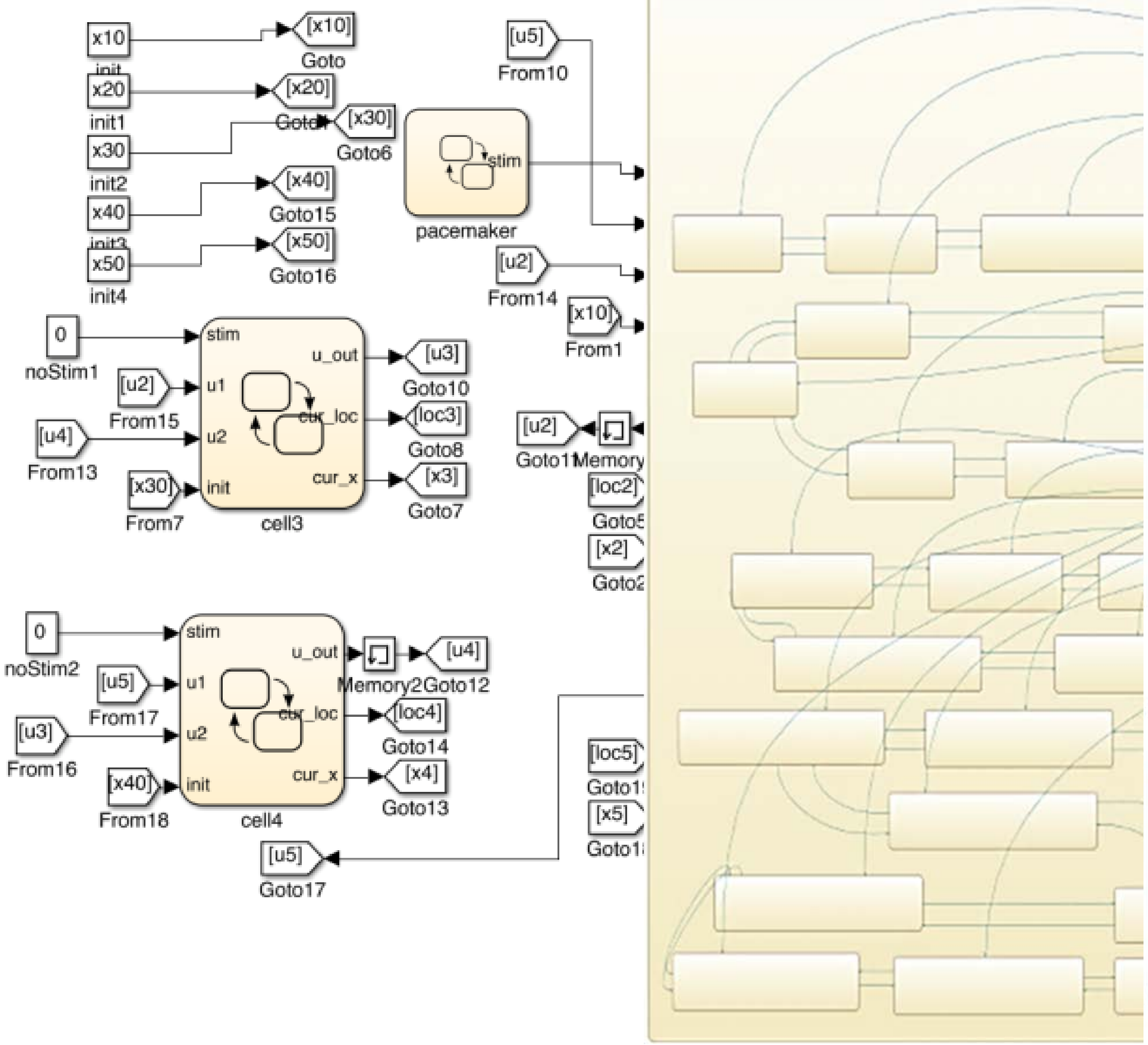


Soundness and Relative Completeness

- Definition. c-$\mathrm{perturb}(A)$ is the set of all HA A', such that A' and A are identical except that
  - The initial sets: $\mathrm{d_H}(\Theta_A, \Theta_{A'}) \leq c$, and
  - The differential equations in every module: $\mathrm{d}_\infty(f_A, f_{A'}) \leq c$
- Definition. A Robustly satisfies (violates) Inv iff there exists $c > 0$ such that all c-$\mathrm{perturb}(A)$ satisfy (violate) Inv.

- **Theorem**: the algorithm is sound and relatively complete.
  - i.e. the algorithm terminates if A robustly satisfies (violates) Inv.

Benchmark

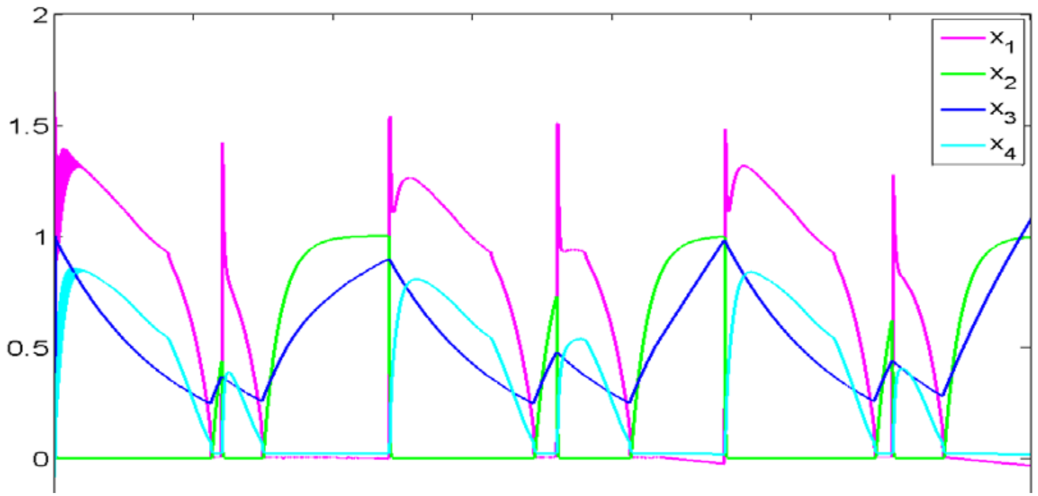


x10
[x10]
Goto
x20
[x20]
init1
x30
[x30]
Goto6
init2
x40
[x40]
Goto15
x50
[x50]
Goto16
init4
[u5]
From10
stim
pacemaker
[u2]
From14
[x10]
From1
0
noStim1
stim
u_out
[u3]
Goto10
[u2]
u1
From15
cur_loc
[loc3]
Goto8
[u4]
u2
From13
[x30]
init
cur_x
[x3]
From7
cell3
Goto7
[u2]
Goto11
Memory
[loc2]
[x2]
0
noStim2
stim
u_out
[u4]
Memory2
Goto12
[u5]
u1
From17
cur_loc
[loc4]
[u3]
u2
Goto14
From16
[x40]
init
cur_x
[x4]
From18
cell4
Goto13
[u5]
Goto17
[loc5]
[x5]

state1
du:
u_dot=-0.0025000000000000*u+D*(u1+u2-2*u)/(h*h)+stim;
v_dot=-0.0166666666666667*v+0.0166666666666667;
w_dot=-0.0726392130750601*u-0.0050000000000000*w+0.0050000000000000;
s_dot=0.0325954614796371*u-0.3657376929266330*s+0.0078827602517302;
u_out=u;
cur_x[0] = u;
cur_x[1] = v;
cur_x[2] = w;
cur_x[3] = s;
cur_loc=1;
[u<0.0032252252252252]
2
[u>=0.0032252252252252]
state2
du:
u_dot=-0.0025934648787471*u+0.0000003014452846+D*(u1+u2-2*u)/(h*h)+stim;
v_dot=-0.0166666666666667*v+0.0166666666666667;
w_dot=-0.0726392130750601*u-0.0050000000000000*w+0.0050000000000000;
s_dot=0.0342238163406254*u-0.3657376929266330*s+0.0078775084405570;
u_out=u;
cur_x[0] = u;
cur_x[1] = v;
cur_x[2] = w;
cur_x[3] = s;
cur_loc=2;
[u>=0.0059]
1
[u<0.0059]
1
state3
du:
u_dot=-99.8500002249997323*u+0.5891000013299984+D*(u1+u2-2*u)/(h*h)+stim;
v_dot=-166.6666666666666003*u-0.9486956521739127*v+157.9710144927535680*u*v+0.9999999999999996;
w_dot=1.2857135714285342*u-0.0050000000000000*w-0.0030142814285712;
s_dot=0.0000003317449342*u-0.3657376929266330*s+0.0080794269996715;
u_out=u;
cur_x[0] = u;
cur_x[1] = v;
cur_x[2] = w;
cur_x[3] = s;
cur_loc=3;
2

Experiments

Network	# Variables	# Modes	# Sims	Run Time (s)
8 cells (FH)	16	1	24	33
Lin. Sync	24	6	128	135.1
Nonli. WT	30	6	128	140.0
5 cells	20	2.1×10^7	170	945
8 cells	32	5.0×10^{10}	73	2377



Discussion

- A scalable technique to verify nonlinear hybrid automata networks using annotations
  - IS discrepancies are used to construct a reduced model of the overall network whose trajectory gives the bloating factor
  - Both original network and the reduced model
  - Sound and relatively complete algorithm

- Cardiac cell networks upto 8 cells, 32 var. and 29^8 modes are verified using 29 annotations

Ongoing: Synthesis