C2E2

Verification Tool for Stateflow

ILLINOIS

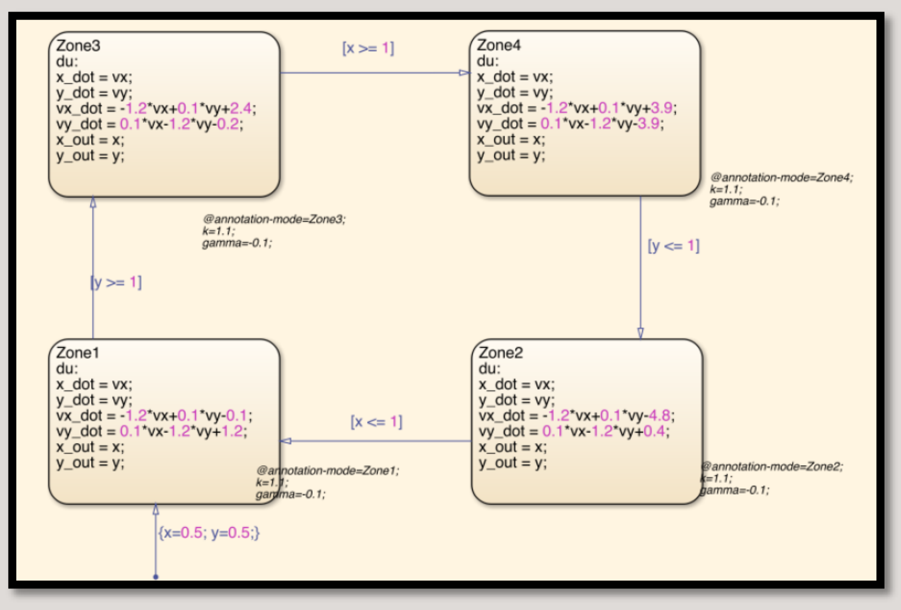
Duggirala ◦ Mitra ◦ Potok ◦ Viswanathan

Introduction

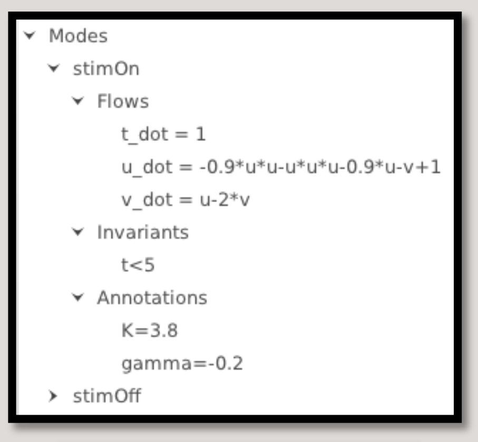
C2E2 a **verifier** for models of cyberphysical systems

- Nonlinear hybrid models. Supports Mathworks^{TM} Simulink Stateflow models and xml inputs
- Guards, resets, initial sets
- Bounded time invariants
- Counter-example generation
- Graphical user interface, visualizer
- Sound and relatively complete

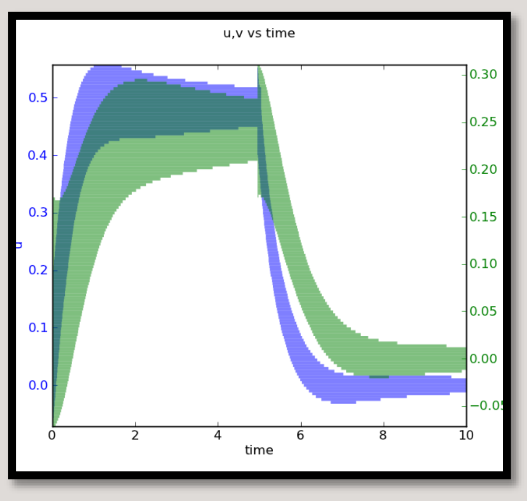
User Interface

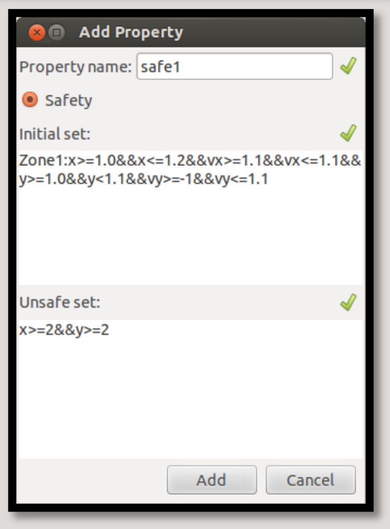


```
Zone3
du:
x_dot = vx;
y_dot = vy;
vx_dot = -1.2*vx+0.1*vy+2.4;
vy_dot = 0.1*vx-1.2*vy-0.2;
x_out = x;
y_out = y;

Zone4
du:
x_dot = vx;
y_dot = vy;
vx_dot = -1.2*vx+0.1*vy+3.9;
vy_dot = 0.1*vx-1.2*vy-3.9;
x_out = x;
y_out = y;

Zone1
du:
x_dot = vx;
y_dot = vy;
vx_dot = -1.2*vx+0.1*vy-0.1;
vy_dot = 0.1*vx-1.2*vy+1.2;
x_out = x;
y_out = y;

Zone2
du:
x_dot = vx;
y_dot = vy;
vx_dot = -1.2*vx+0.1*vy-4.8;
vy_dot = 0.1*vx-1.2*vy+0.4;
x_out = x;
y_out = y;

@annotation-mode=Zone3;
k=1.1;
gamma=-0.1;

@annotation-mode=Zone4;
k=1.1;
gamma=-0.1;

@annotation-mode=Zone1;
k=1.1;
gamma=-0.1;

@annotation-mode=Zone2;
k=1.1;
gamma=-0.1;
```



```
Modes
  stimOn
    Flows
      t_dot = 1
      u_dot = -0.9*u*u-u*u*u-0.9*u-v+1
      v_dot = u-2*v
    Invariants
      t<5
    Annotations
      K=3.8
      gamma=-0.2
  stimOff
```





Add Property

Property name: safe1

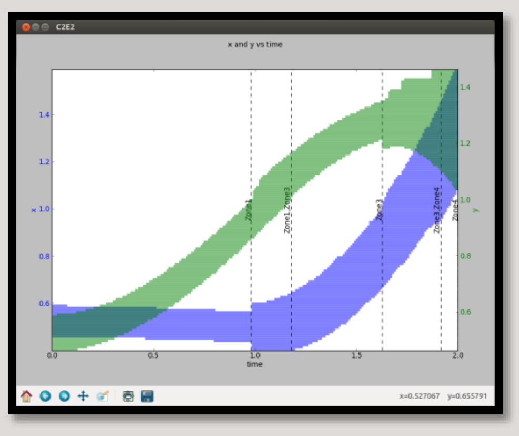
● Safety

Initial set:

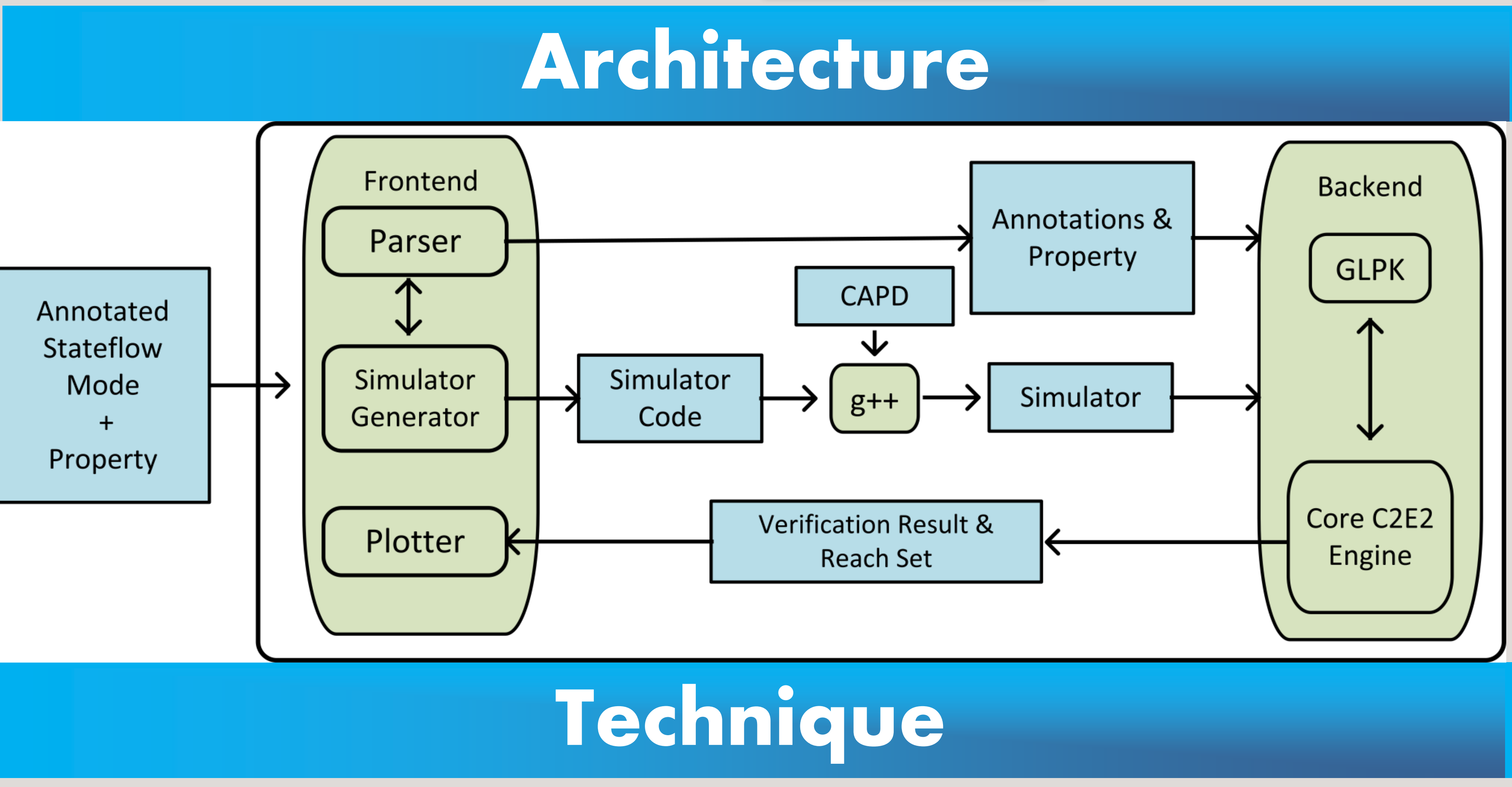
Zone1:x>=1.0&&x<=1.2&&vx>=1.1&&vx<=1.1&&y>=1.0&&y<1.1&&vy>=-1&&vy<=1.1

Unsafe set:

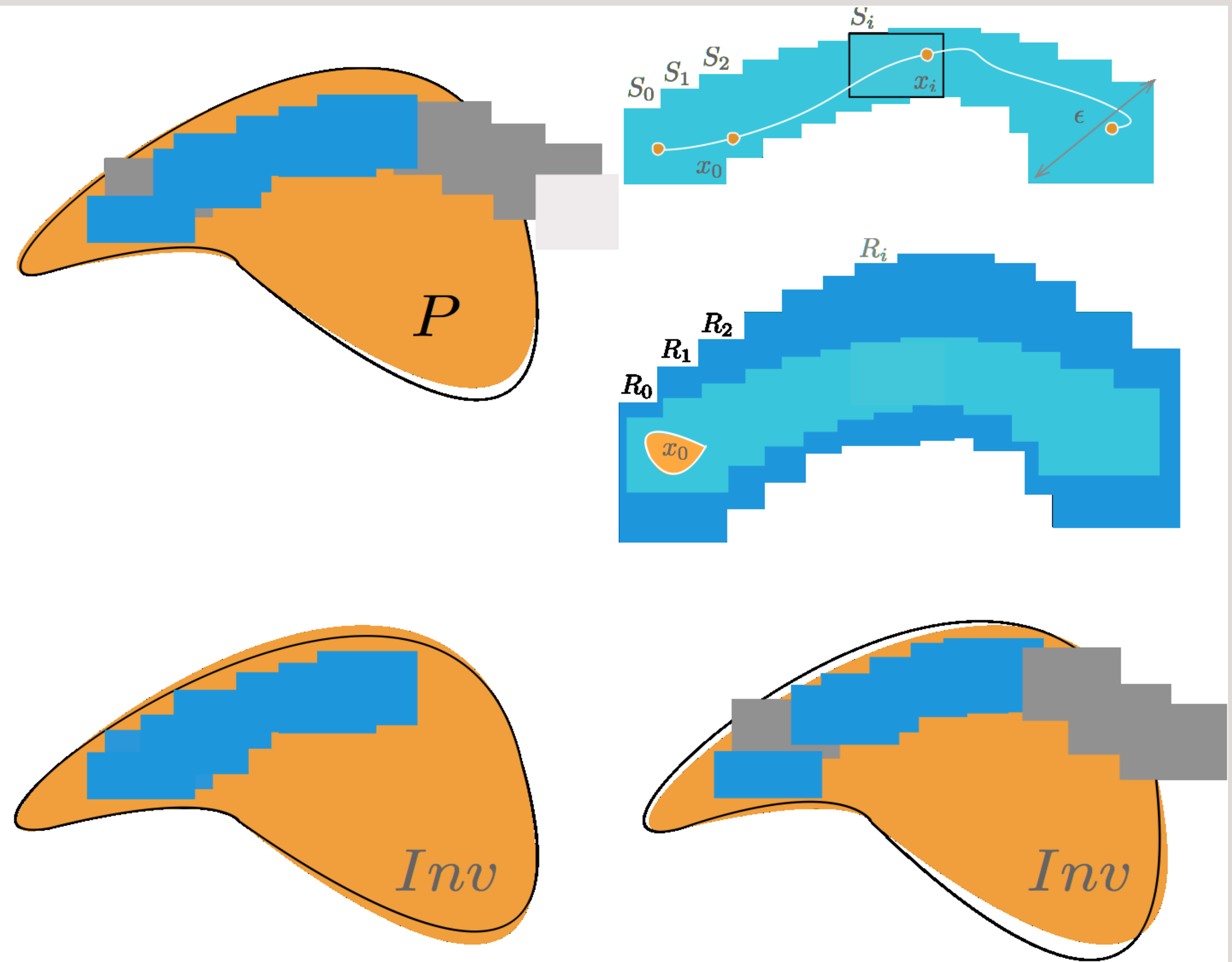
x>=2&&y>=2



Architecture



Technique



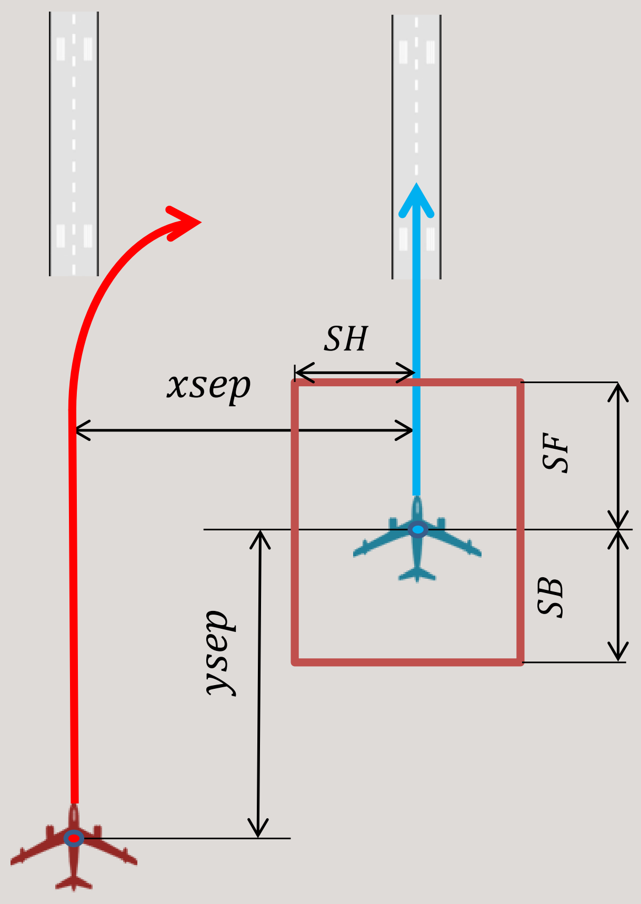
Soundness and Relative Completeness

Theorem. If returns safe or unsafe, then A is safe /unsafe.

Definition Given HA $A = \langle V, Loc, A, D, T \rangle$, an **$\epsilon$-perturbation** of A is a new HA A' that is identical except, $\Theta' = B_\epsilon(\Theta)$, $\forall \ell \in Loc, Inv' = B_\epsilon(Inv)$ (b) a ∈ A, $Guard_a = B_\epsilon(Guard_a)$. A is **robustly safe** iff $\exists \epsilon > 0$, such that A' is safe for U_ϵ upto time bound T, and transition bound N. Robustly unsafe iff $\exists\ \epsilon < 0$ such that A' is unsafe for U_ϵ.

Theorem. Terminates when robustly safe or robustly unsafe.

An application



Scenario	Alert $\preccurlyeq_4$ Unsafe	Running time (mins:sec)	Alert $\preccurlyeq_?$ Unsafe
6	False	3:27	2.16
7	True	1:13	–
8	True	2:21	–
6.1	False	7:18	1.54
7.1	True	2:34	–
8.1	True	4:55	–
9	False	2:18	1.8
10	False	3:04	2.4
9.1	False	4:30	1.8
10.1	False	6:11	2.4

Onward

Automatic Computation of Annotations

Temporal precedence properties

Compositional analysis, unbounded time properties

What's on your wish list?

References

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

C2E2 User's Guide. Duggirala, Mitra, Viswanathan, and Potok. 2014.

Verification of Annotated Models from Executions. Duggirala, Mitra & Viswanathan. EMSOFT 2013.

Temporal Precedence Checking for Switched Models and its Application to a Parallel Landing Protocol. Duggirala, Wang, Mitra, Munoz & Viswanathan, Formal Methods 2014.

Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells. Huang, Fan, Mereacre, Mitra & Kwiatkowska. CAV 2014

Supported by the National Science Foundation

Contact: c2e2help@gmail.com