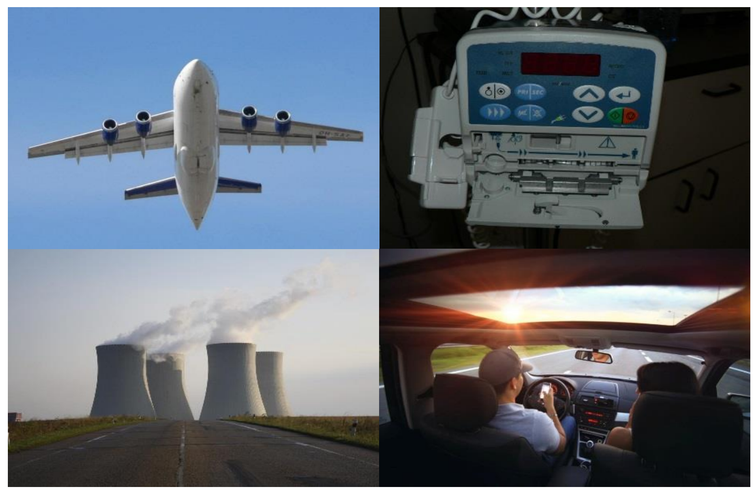
# Towards Synthesis of Nondeterministic Infinite State Reactive Systems

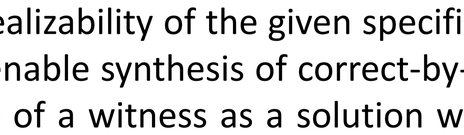
Andreas Katis
katis001@umn.edu

**Abstract :** We present our work on developing efficient algorithms related to the formal analysis of infinite state reactive systems. Our research focus is the discovery and implementation of decision procedures that can provide a formal proof regarding the realizability of the given specification, as well as the extension of these procedures to enable synthesis of correct-by-construction witnesses. Contrary to the traditional view of a witness as a solution with deterministic behavior, we strive for synthesis algorithms that allow more general solutions through nondeterministic designs.



## Synthesis of Infinite State Reactive Systems

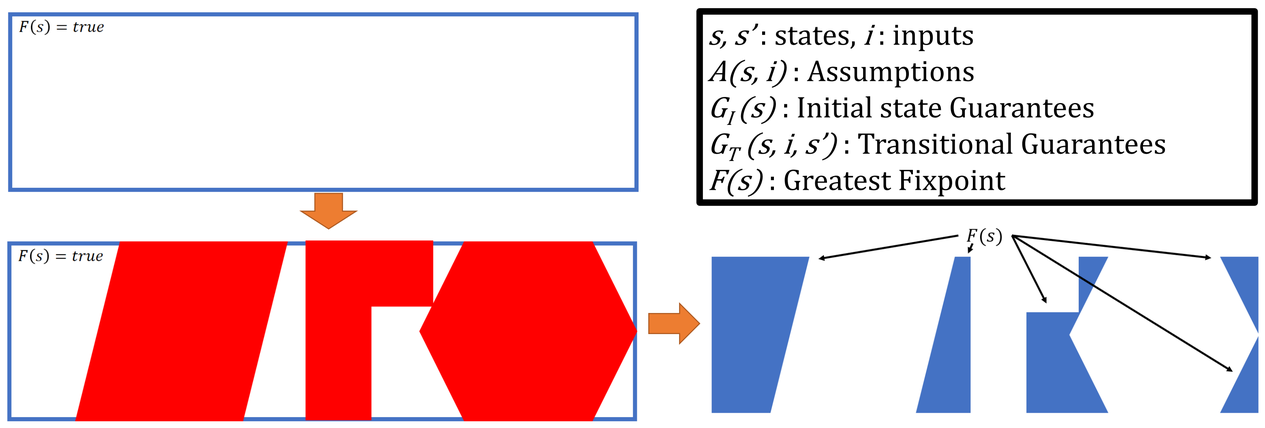
- **Reactive System**: Maintains an ongoing interaction with environment
  - Systems are defined in terms of *inputs* $i$ and *states* $s$.
  - A symbolic transition system is defined as: *(I, T)*
    - *Initial* states allowed by *I*
    - *Transitions* allowed by *T*




- A ***contract*** is a pair (A,G) with
  - **Assumptions**: A: (state x input) → bool
  - **Guarantees**: $G_I$ : state → bool , $G_T$ : (state x input x state) → bool

## Validity-Guided Reactive Synthesis

- $\forall s, i. \left(F(s) \wedge A(s,i) \Rightarrow \exists s'. G_T(s,i,s') \wedge F(s')\right)$
- $\exists s. F(s) \wedge G_I(s)$




## Achieving Synthesis of Nondeterministic Designs

- **Synthesis** : Compute $s_{init}, f(s,i)$, s.t.

$$G_I(s_{init}) \wedge \forall s, i. Viable(s) \Rightarrow Viable\big(f(s,i)\big)$$

- **Nondet. Synthesis** : Compute $s_{init}, F(s,i,r)$ s.t.

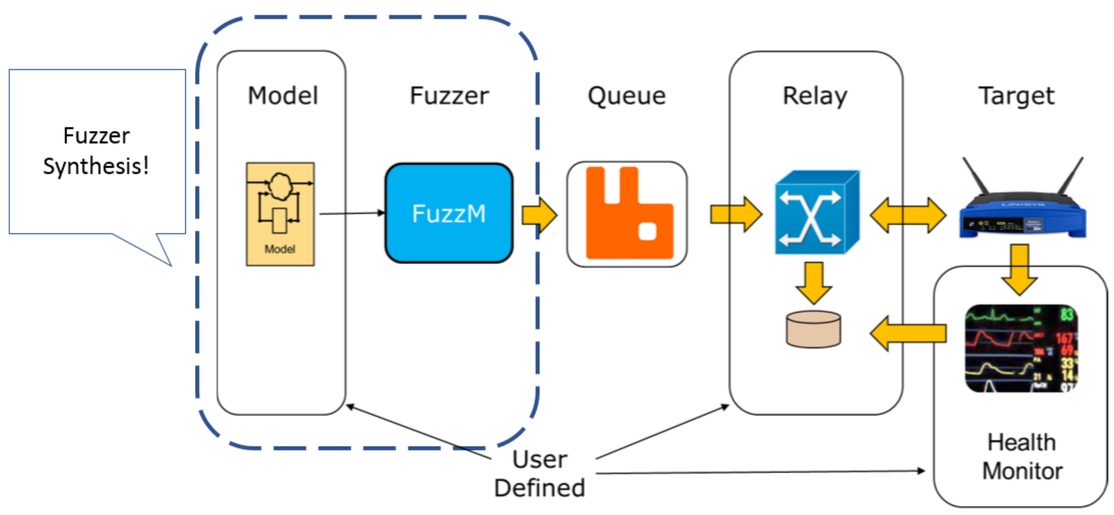
$$G_I(s_{init}) \wedge \forall s, i, r. Viable(s) \wedge B(s,i,r) \Rightarrow Viable\big(F(s,i,r)\big),$$

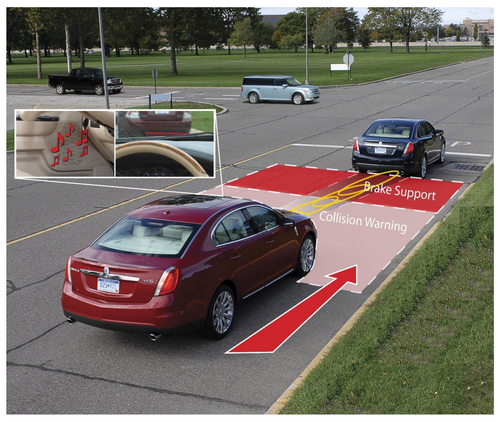
where $B(s,i,r)$ are assumptions on the random input $r$

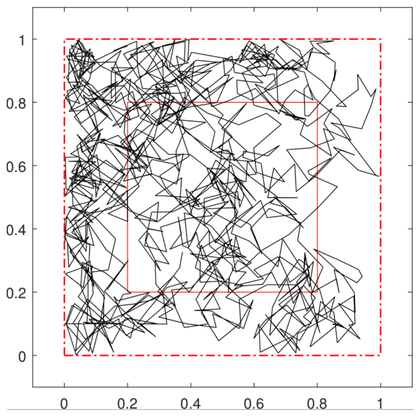
- **"Gold Standard"** :

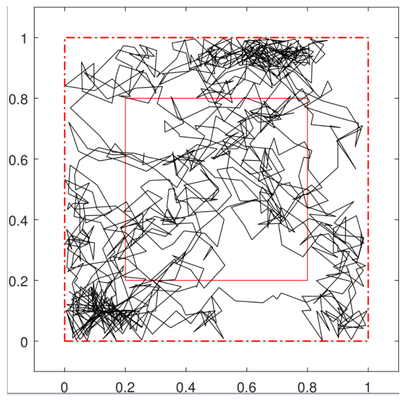
$$\forall s, i, s'. Viable(s) \wedge A(s,i) \wedge G_T(s,i,s') \wedge Viable(s') \Rightarrow$$
$$\exists r. B(s,i,r) \wedge F(s,i,r) = s'$$

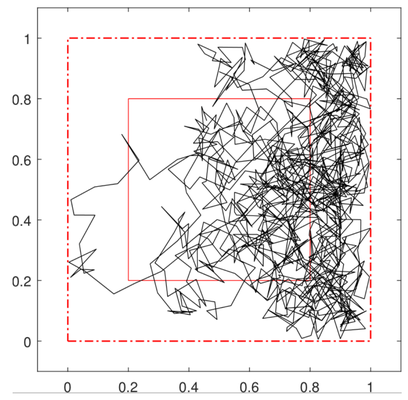
## Applications of Nondeterministic Reactive Systems

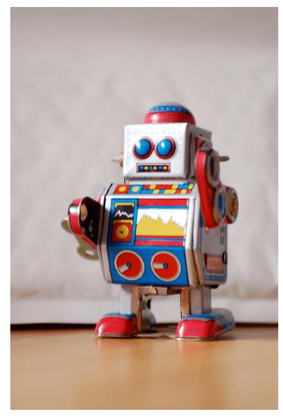








CriSys
UMN Critical Systems Group

fmcad.19