Formal Analysis of Cyber-Physical Systems using Inductive Approaches

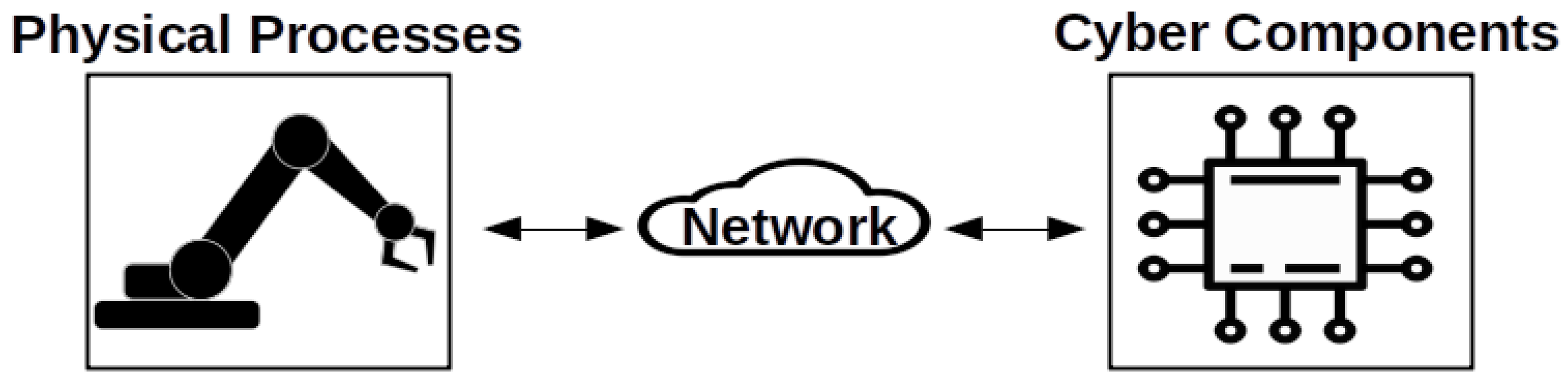
Mahathi Anand
mahathi.anand@sosy.ifi.lmu.de
Supervisors: Majid Zamani & Matthias Althoff
Collaborators: Vishnu Murali & Abolfazl Lavaei & Ashutosh Trivedi

CONVEY

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Motivation

Cyber-Physical Systems (CPS): Systems consisting interactions between physical and computational components



- Formal analysis of CPS is extremely important
- Inductive approaches provide an effective mechanism for safety analysis
- **Challenges**: Scalability, conservatism and analysis of complex logic specifications

Research Statement

- Utilizing inductive approaches using **barrier certificates** for the formal analysis of discrete-time stochastic CPS
- Tackling the scalability challenges using **divide-and-conquer** approaches
- Alleviating conservatism using k**-induction**
- Analyzing logic specifications using **automata-theoretic** approaches

System Definition

A discrete-time stochastic CPS S is a tuple (X, ς, f) where

- X is the state set
- $\varsigma := \{\varsigma(t) : \Omega \to \mathcal{V}_\varsigma,\ t \in \mathbb{N}\}$ is a sequence of independent and identically distributed (i.i.d.) random variables
- $f : X \times V_\varsigma \to X$ is the transition function such that for all $t \in \mathbb{N}$:

$$x(t+1) = f(x(t), \varsigma(t))$$

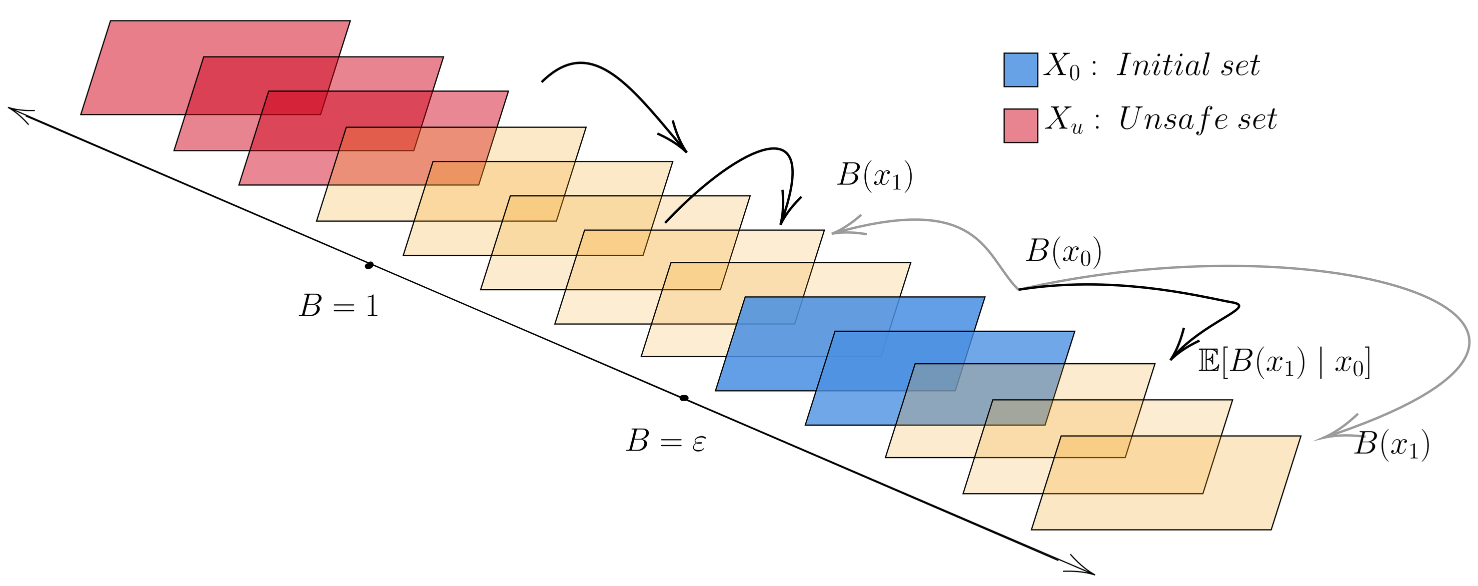
Safety by Induction

- $B : X \to \mathbb{R}$ is a barrier certificate for S with respect to a set of initial states X_0 and a set of unsafe states X_u if there exists $0 \le \varepsilon \le 1$ such that:

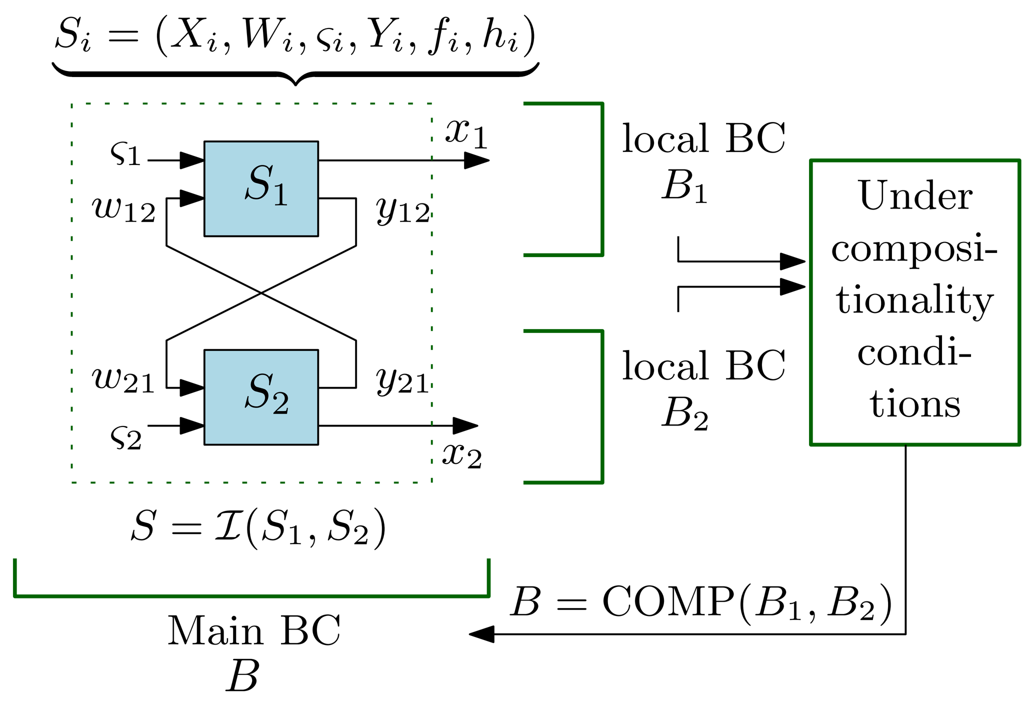
$$\begin{aligned}
&\forall x \in X_0 : \ B(x) \le \varepsilon\\
&\forall x \in X_u : \ B(x) \ge 1\\
&\forall x \in X : \ \mathbb{E}[B(f(x,\varsigma)) \mid x] - B(x) \le 0
\end{aligned}$$

- Existence of B means the system is safe with probability:

$$\mathbb{P}\{x(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0\} \ge 1 - \varepsilon.$$



Tackling Scalability: Compositional Framework



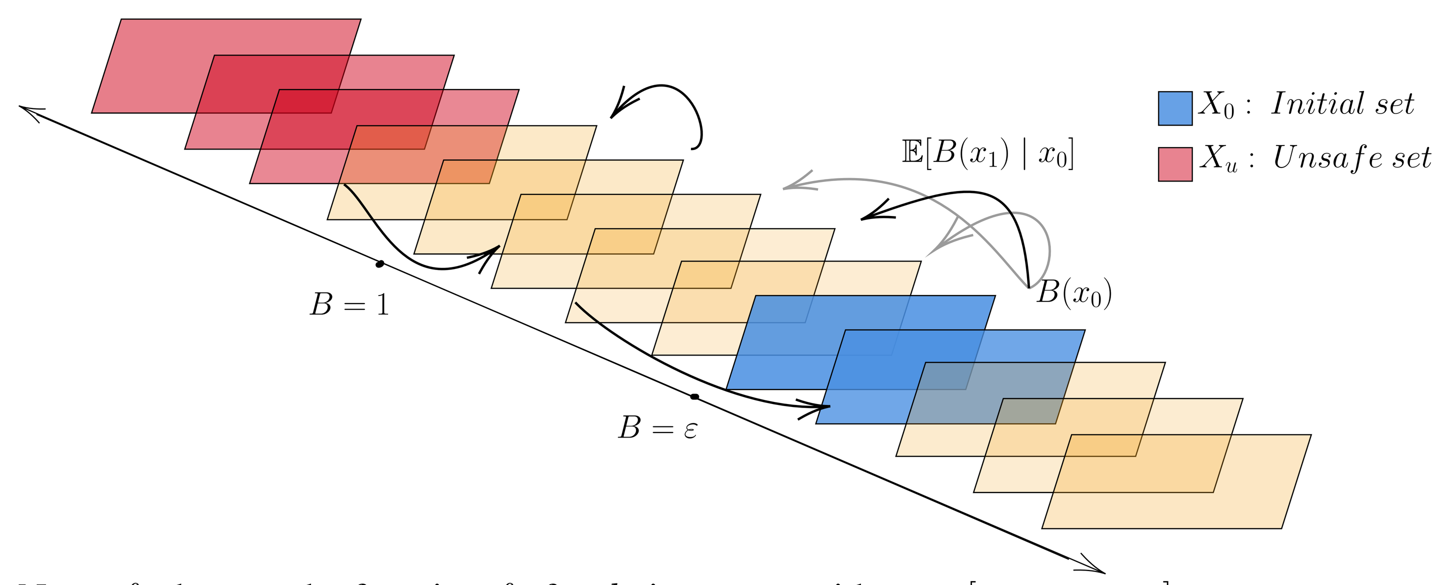
Tackling Conservatism: k-Induction

- $B : X \to \mathbb{R}$ is a k-inductive barrier certificate for S with respect to a set of initial states X_0 and a set of unsafe states X_u if there exists $k \in \mathbb{N}$, $0 \le \varepsilon \le 1$, and $c > 0$ such that:

$$\begin{aligned}
&\forall x \in X_0 : \ B(x) \le \varepsilon\\
&\forall x \in X_u : \ B(x) \ge 1\\
&\forall x \in X : \ \mathbb{E}[B(f(x,\varsigma)) \mid x] - B(x) \le c\\
&\forall x \in X : \ \mathbb{E}[B(f_k(x,\varsigma_k)) \mid x] - B(x) \le 0
\end{aligned}$$

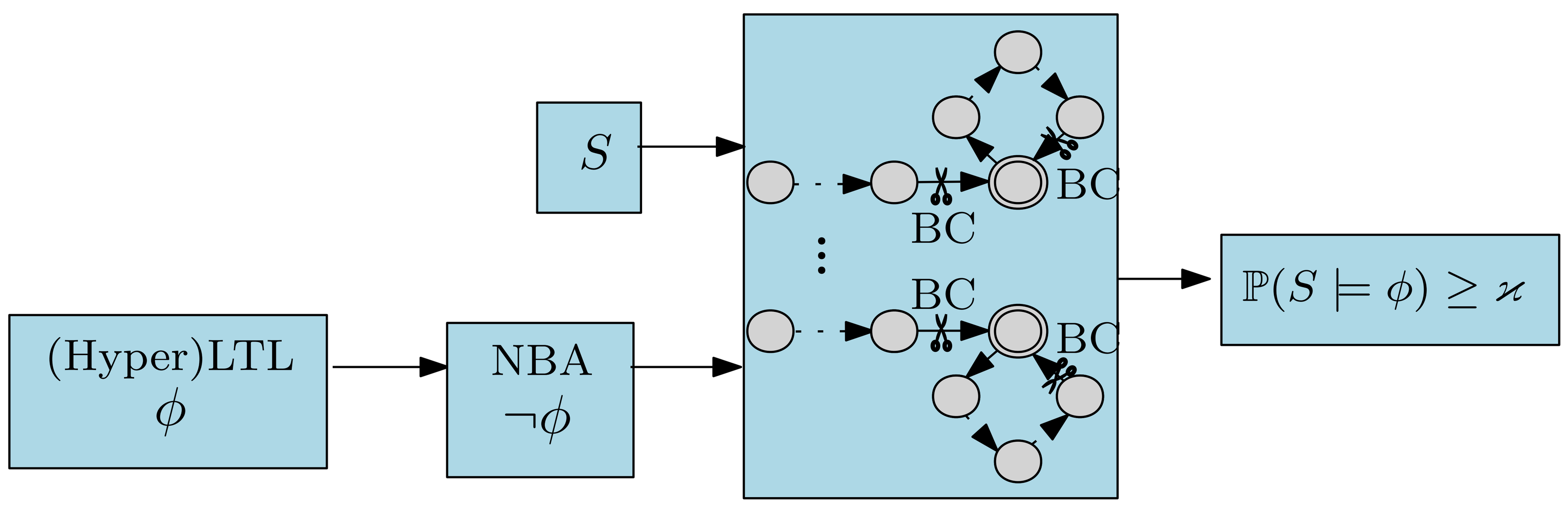
- Existence of B means the system is safe with probability:

$$\mathbb{P}\{x(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0\} \ge 1 - k\varepsilon - \frac{k(k-1)c}{2}.$$



Note: f_k denotes the function f after k time steps with $\varsigma_k = [\varsigma_1; \dots; \varsigma_{k-1}]$

Complex (Hyper)LTL Specifications



Relevant Publications

M. Anand, A. Lavaei, M. Zamani, From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems, IEEE TAC, 2022.

M. Anand, A. Lavaei, M. Zamani, Compositional synthesis of control barrier certificates for networks of stochastic systems against ω-regular specifications, *conditionally accepted*, NAHS 2023.

M. Anand, V. Murali, A. Trivedi, M. Zamani, k-Inductive barrier certificates for stochastic systems, HSCC, 2022.

M. Anand, V. Murali, A. Trivedi, M. Zamani, Verification of hyperproperties for uncertain dynamical systems via barrier certificates, *conditionally accepted*, IEEE TAC, 2023.

Gitub Repository for verification of hyperproperties:
https://github.com/mahathi-anand/CPS-Verification-against-HyperLTL