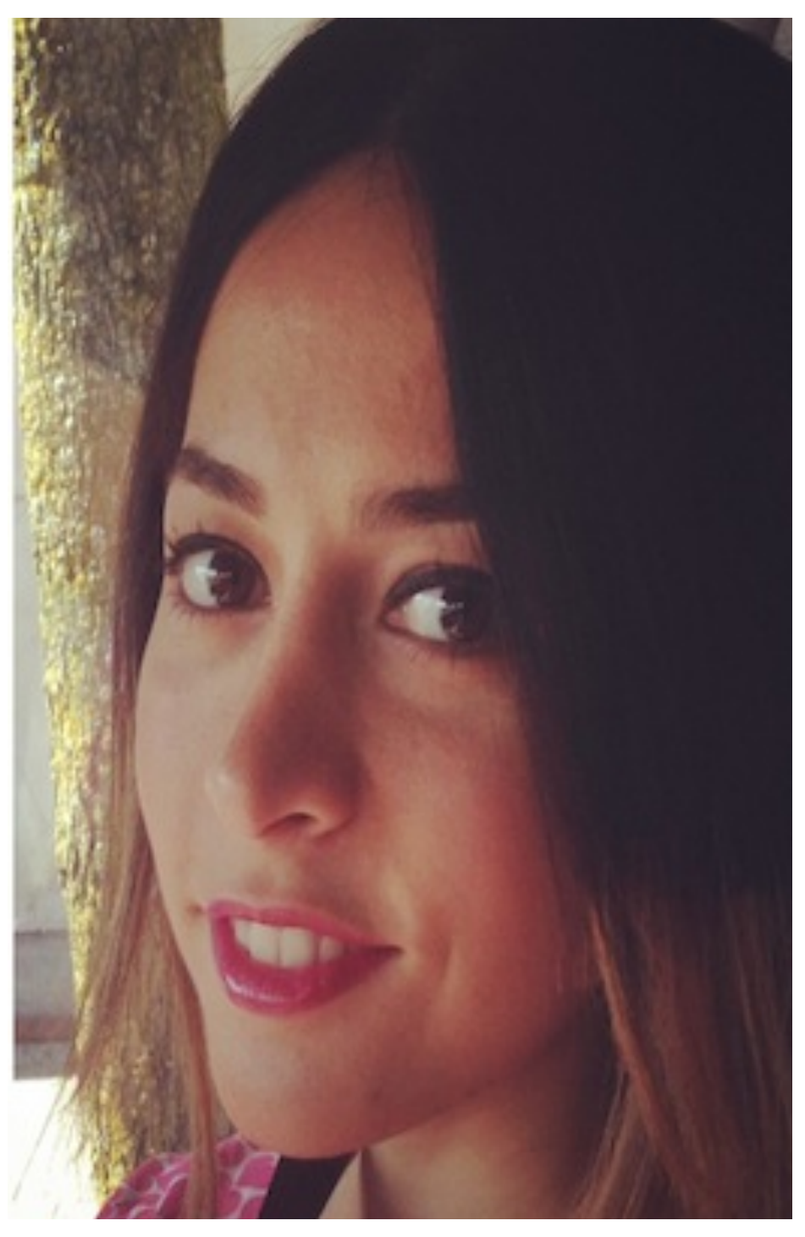
Formal Synthesis of Partially-Observable Cyber-Physical Systems



Niloofar Jahanshahi

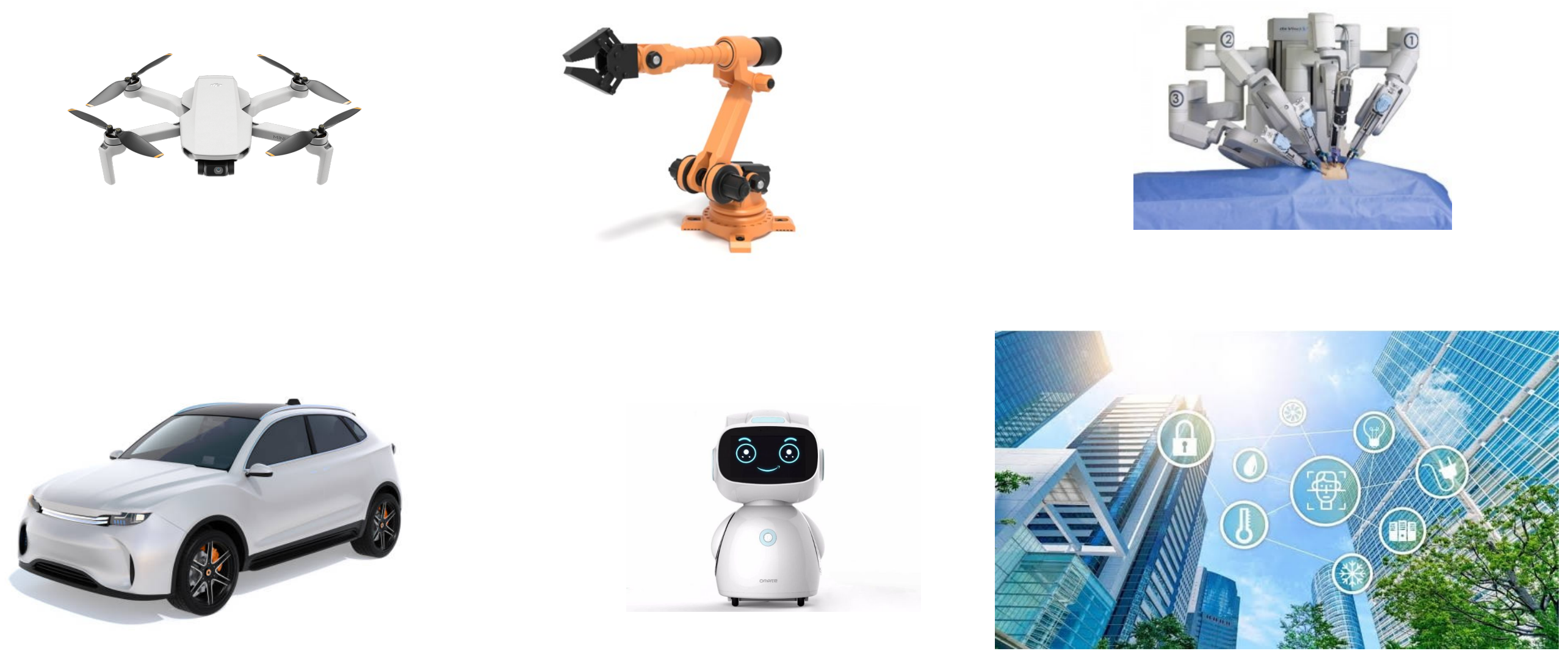
`jahanshahi.niloofar@sosy.ifi.lmu.de`

Supervisor: Majid Zamani & Matthias Althoff

Collaborators: Pushpak Jagtap & Abolfazl Lavaei

Cyber-Physical Systems

Cyber-physical systems: complex models consisting of both computational elements and physical entities.

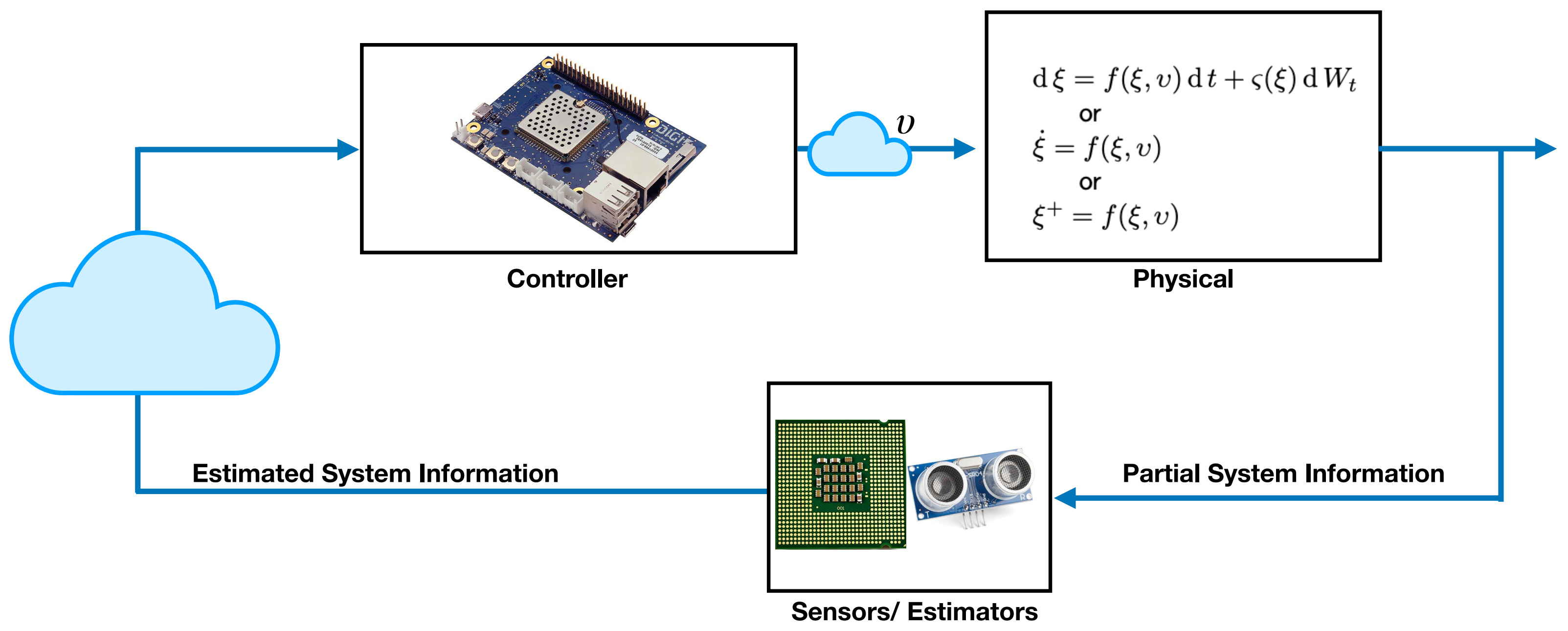


Challenges:

- Increasing complexity: interconnected large-scale systems;
- Complex control objectives: beyond the classical stability;
- Closed-form models: not available or too complex to be of any use.

Problem Statement

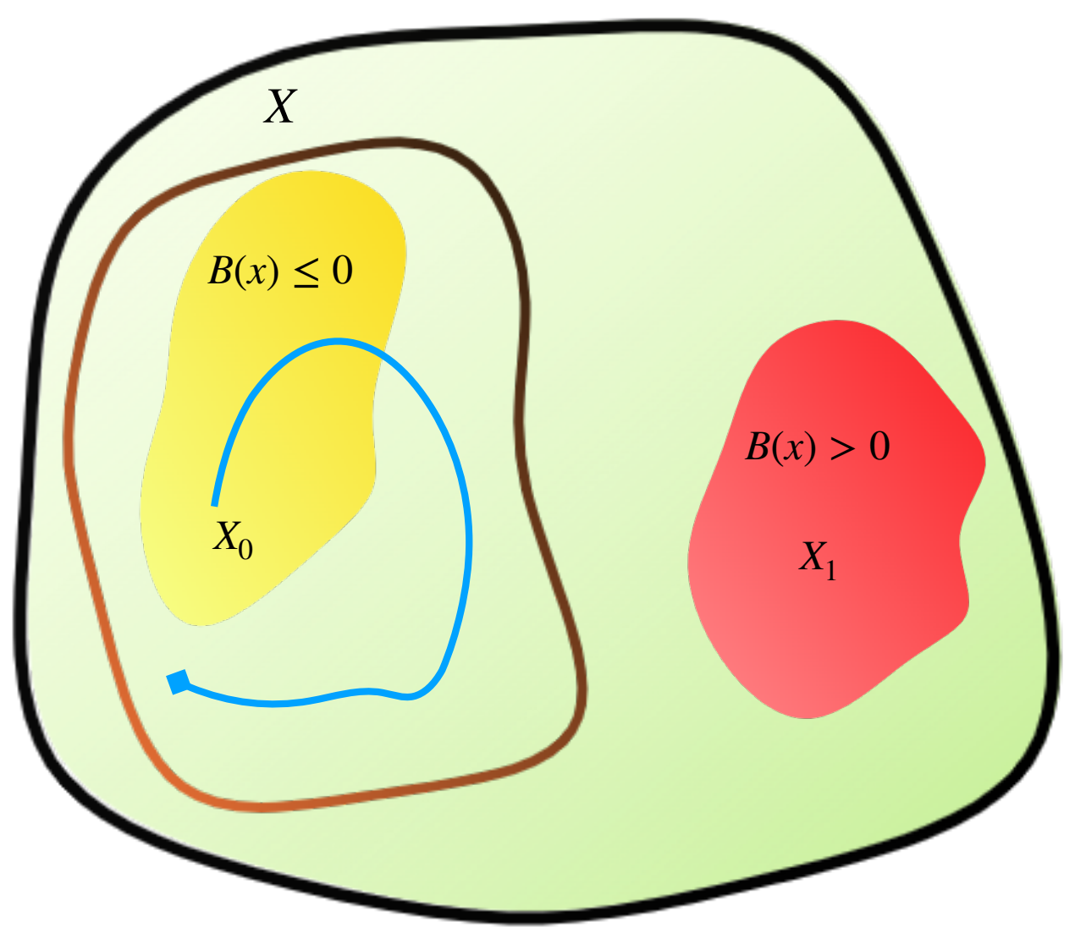
Can we *formally* design a controller such that a partially-observable stochastic control system satisfies a given *safety* specification?


Controller
υ
$\mathrm{d}\,\xi = f(\xi,\upsilon)\,\mathrm{d}\,t + \varsigma(\xi)\,\mathrm{d}\,W_t$
or
$\dot{\xi} = f(\xi,\upsilon)$
or
$\xi^+ = f(\xi,\upsilon)$
Physical
Estimated System Information
Partial System Information
Sensors/ Estimators

Control Barrier Functions (CBFs)

Dynamics of the system $\Sigma : \begin{cases} x^+ = f(x,\upsilon), \\ y = h(x), \end{cases}$

X: state space; X_0: initial set; X_1: unsafe set;



Control barrier function: $\mathcal{B} : X \to \mathbb{R}$

- $\forall x \in X_0, \;\; \mathcal{B}(x) \leq 0,$
- $\forall x \in X_1, \;\; \mathcal{B}(x) > 0,$
- $\forall x \in X, \exists u \in U, \; \mathcal{B}(f(x,u)) \leq \mathcal{B}(x).$

Theorem 1

Existence of a control barrier function $\mathcal{B}$ guarantees that a system starting from X_0 does not reach X_1 under the synthesized controller.

CBF for Systems with Partial Information

Assumption 1

The states of the system can be estimated by a proper estimator as follows:

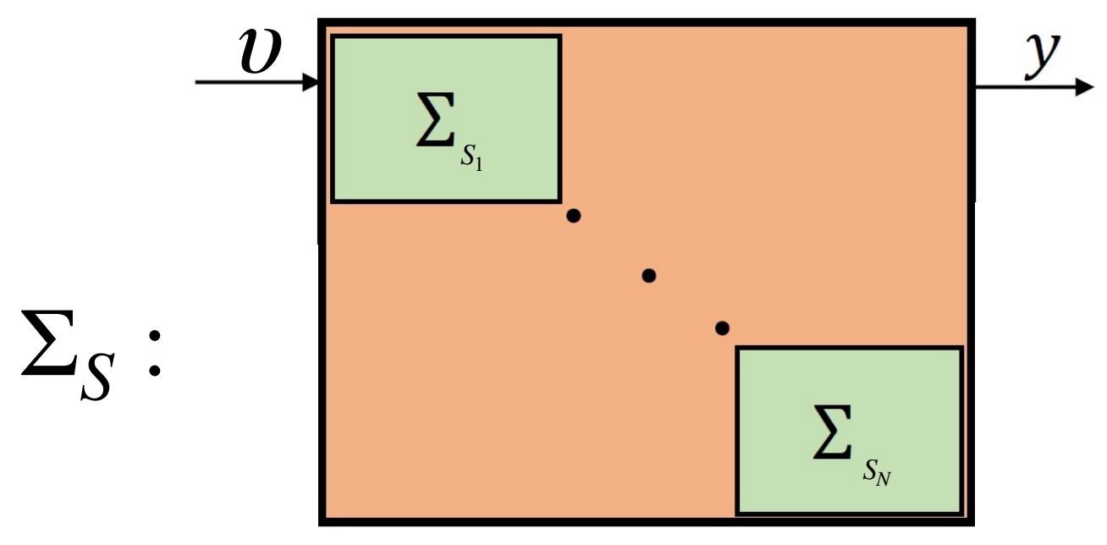
$$\widehat{\Sigma} : \hat{x}^+ = \hat{f}(\hat{x},\upsilon,y).$$

Control barrier function: $\mathcal{B} : X \times X \to \mathbb{R}$

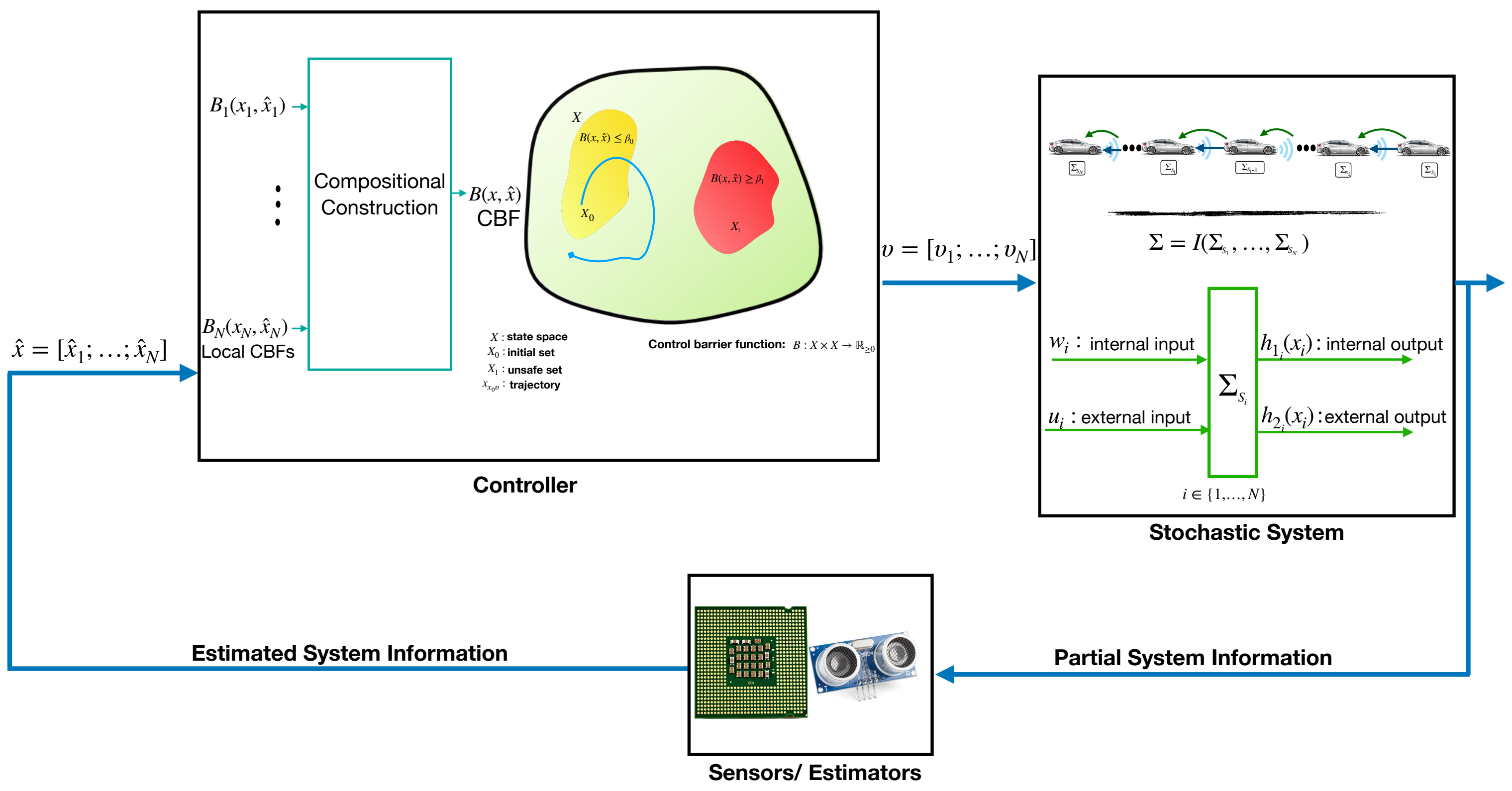
- $\forall (x,\hat{x}) \in X_0 \times X_0, \;\; \mathcal{B}(x,\hat{x}) \leq \beta_0,$
- $\forall (x,\hat{x}) \in X_1 \times X, \;\; \mathcal{B}(x,\hat{x}) \geq \beta_1, \;\; \beta_0 < \beta_1$
- $\forall \hat{x} \in X, \exists u \in U,$ such that $\forall x \in X,$ $\mathcal{B}(f(x,u), \hat{f}(\hat{x},u,y)) \;\leq \mathcal{B}(x,\hat{x}).$

Large-Scale Interconnected Control Systems

Synthesizing a controller for Σ_S monolithically is extremely complex and challenging, so rather than looking at Σ_S monolithically, we consider it as an interconnection of subsystems Σ_{S_i}.



CBFs for Interconnected Control Systems


$B_1(x_1,\hat{x}_1)$
$B_N(x_N,\hat{x}_N)$
Local CBFs
Compositional Construction
$B(x,\hat{x})$ CBF
X
$B(x,\hat{x}) \leq \beta_0$
X_0
$B(x,\hat{x}) \geq \beta_1$
X_1
X : state space
X_0 : initial set
X_1 : unsafe set
$x_{x_0\upsilon}$: trajectory
Control barrier function: $B : X \times X \to \mathbb{R}_{\geq 0}$
Controller
$\hat{x} = [\hat{x}_1; \ldots; \hat{x}_N]$
$\upsilon = [\upsilon_1; \ldots; \upsilon_N]$
$\Sigma = I(\Sigma_{S_1}, \ldots, \Sigma_{S_N})$
w_i : internal input
u_i : external input
Σ_{S_i}
$h_{1_i}(x_i)$: internal output
$h_{2_i}(x_i)$: external output
$i \in \{1,\ldots,N\}$
Stochastic System
Estimated System Information
Partial System Information
Sensors/ Estimators