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?

Control Barrier Functions (CBFs)
Dynamics of the system $\Sigma: \begin{cases} x^+ = f(x, u), \\ y = h(x), \end{cases}$ $X$: state space; $X_0$: initial set; $X_1$: unsafe set;

Control barrier function: $B : X \to \mathbb{R}$
- $\forall x \in X_0, \ B(x) \leq 0,$
- $\forall x \in X_1, \ B(x) > 0,$
- $\forall x \in X, \exists u \in U, \ B(f(x, u)) \leq B(x).$

Theorem 1
Existence of a control barrier function $B$ guarantees that a system starting from $X_0$ does not reach $X_1$ under the synthesized controller.

CBFs for Systems with Partial Information

Assumption 1
The states of the system can be estimated by a proper estimator as follows:
$$\hat{\Sigma}: \hat{x}^+ = f(\hat{x}, v, y).$$

Control barrier function: $B : X \times X \to \mathbb{R}$
- $\forall (x, \hat{x}) \in X_0 \times X_0, \ B(x, \hat{x}) \leq \beta_0,$
- $\forall (x, \hat{x}) \in X_1 \times X, \ B(x, \hat{x}) \geq \beta_1, \ \beta_0 < \beta_1$
- $\forall \hat{x} \in X, \exists u \in U, \ such \ that \ \forall x \in X,$
  $$B(f(x, u), f(\hat{x}, u, y)) \leq B(x, \hat{x}).$$

Large-Scale Interconnected Control Systems

Synthesizing a controller for $\Sigma_\Sigma$ monolithically is extremely complex and challenging, so rather than looking at $\Sigma_\Sigma$ monolithically, we consider it as an interconnection of subsystems $\Sigma_i$.

CBFs for Interconnected Control Systems