# CPS: Medium: Collaborative Research: Multi-Objective Mitigation Strategies for Viability and Performance of Cyber-Physical Systems

Bruno Sinopoli, Sanjoy Baruah (Washington University in St. Louis), Ilya Kolmanovsky (University of Michigan)

## Challenge:

This project aims to bring control theory, automotive & aerospace application domain-knowledge, and real-time resource allocation, to bear on the problem of run-time mitigation when complex CPSs operating in uncertain environments confront with unanticipated viability-compromising situations.

## Proposed solution:

Establish a systematic, general, and broadly applicable framework to approach failure mode effects management (FMEM) development for advanced autonomous systems:

- **Fault Detection**: Faults should be detected as soon as they happen (or are potentially likely to happen)
- **Multi-Mode Control**: Pointwise-in-time state and control constraints should be enforced at all times despite the presence of faults.
- **Effective Resource Reallocation**: Computing resources should be appropriately reallocated in a timely manner upon detection of faults to executing the corresponding control strategies
- **Mitigation Coordination**: Once a fault is detected, a set of strategies should be provided to the multi-mode control module and the resource allocator to assure system viability.

## Scientific impact:

- Providing a framework for formalizing the concept of "continuing operation" in the face of a variety of contingencies.
- Defining a set of mitigation strategies that addresses a broad range of contingencies that arise in several important applications.
- Obtaining a better understanding of emergent problems that arise from the interaction of resource-allocation and control strategies, and propose devising optimal (or near-optimal) strategies for dealing with such problems with guaranteed performance in the presence of uncertainty.

## Broader impact:

- Analysis techniques, algorithms and implementation methodologies developed in this project can support the automotive industry to develop safe advanced/autonomous vehicles.
- This project provides unique opportunities for students to develop expertise across the different areas.

## Proposed framework:

### Fault Detection

- LTI systems with $F$ fault scenarios can be expressed as $F$ distinct LTI systems with different system matrices.

$$\begin{cases} x(t+1|\mu) = A_\mu x(t|\mu) + B_\mu v(t) + \omega(t) \\ y(t|\mu) = C_\mu x(t|\mu) + \zeta(t) \end{cases}$$

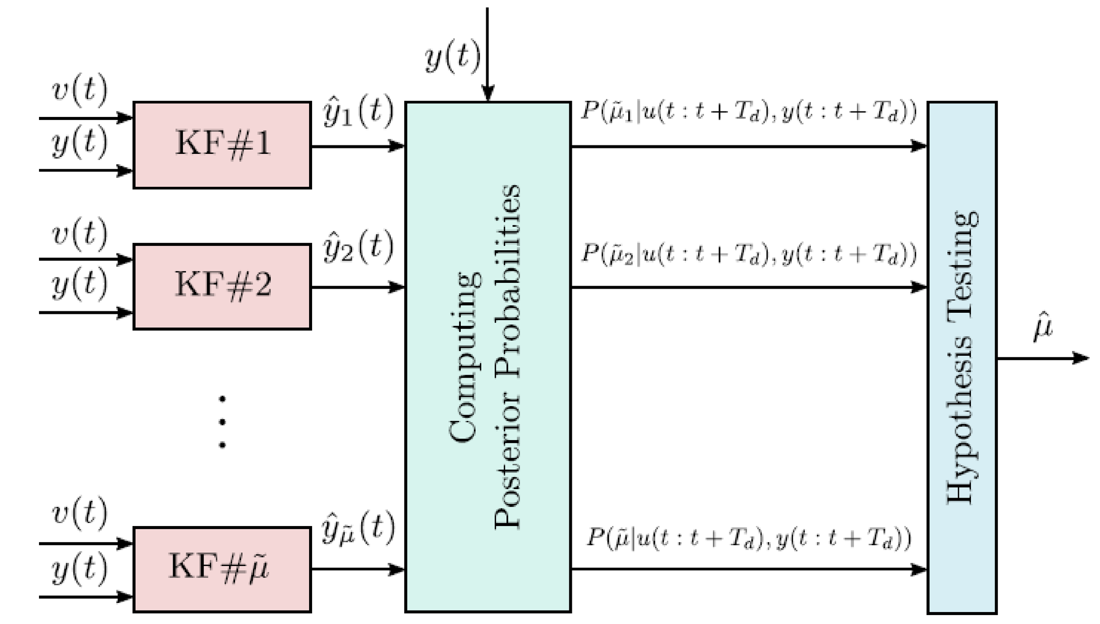
- When the system is operating in mode $\mu$, its state and reference have to satisfy constraints

$$\begin{cases} \mathbb{E}[z_1(t|\mu)] \in \mathcal{Z}_1 \\ \mathbb{P}(z_2(t|\mu) \in \mathcal{Z}_2) \geq \beta \end{cases}$$

- The Multi-Model Adaptive Estimator (MMAE) uses residual signals to identify the actual mode of the system.

$$\hat{\mu} = \arg\max_{\tilde{\mu}} \mathbb{P}(\tilde{\mu}|y(t:t+T_d), v(t:t+T_d-1))$$

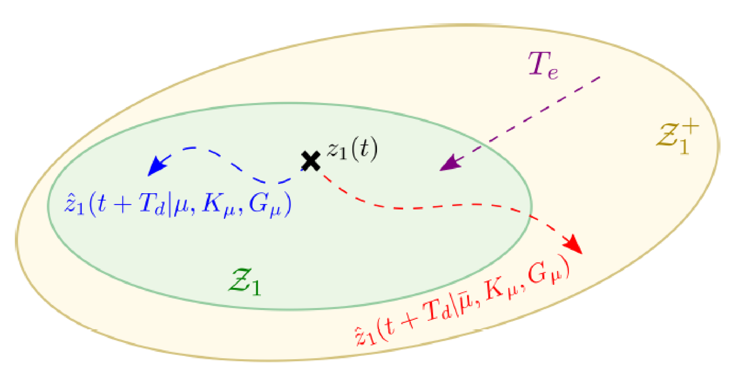
with $y(t:t+T_d) = [y(t)^\top \cdots y(t+T_d)^\top]^\top$ and $v(t:t+T_d-1) = [v(t)^\top \cdots v(t+T_d-1)^\top]^\top$




- The control sequence $v(t:t+T_d-1)$ can be determined via a suitably designed optimization problem so to improve detection performance without violating constraints

$$v^* = \arg\min_{v} \sum_{\tilde{\mu}} \sum_{\check{\mu}} \sqrt{\mathbb{P}(\tilde{\mu})\mathbb{P}(\check{\mu})} e^{-\rho_{\tilde{\mu}\check{\mu}}}$$

with $\rho_{\tilde{\mu}\check{\mu}}$ as a quadratic function in the control sequence $v(t:t+T_d-1)$.



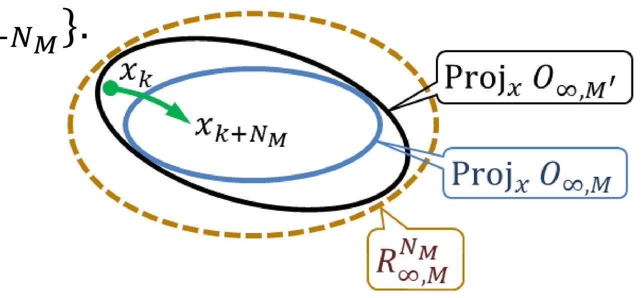

### Multi-Mode Control

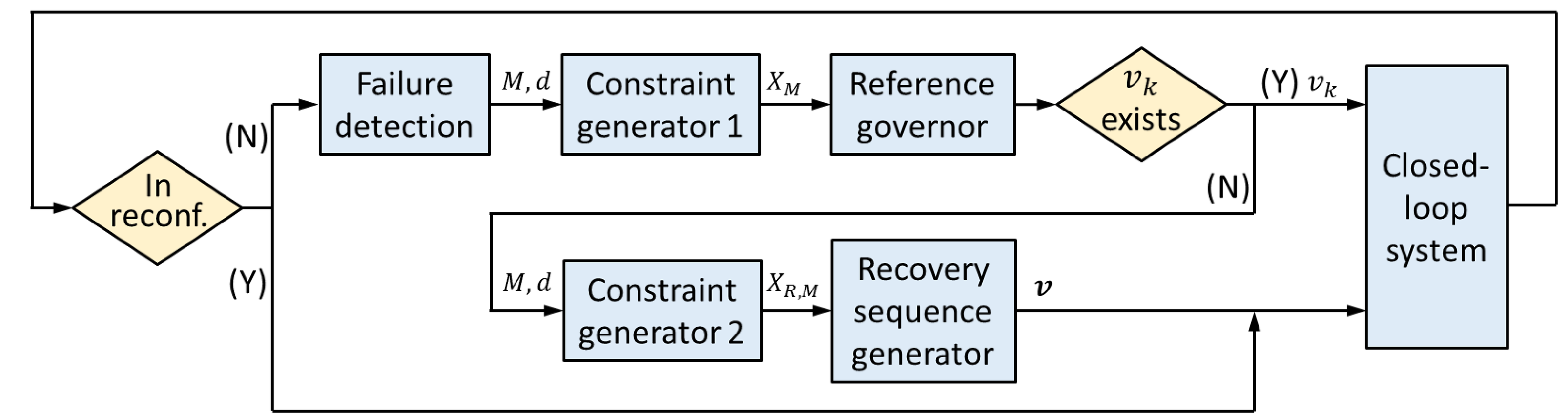
#### Set-theoretic failure mode reconfiguration

- Exploits nesting between constraint admissible sets $O_{\infty,M}$ and recoverable sets $R_{\infty,M}^{N_M}$ to ensure there exists a recovery sequence $\boldsymbol{v} = \{v_k, \ldots, v_{k+N_M}\}$.
- Reconfiguration condition for mode $M$:

$$\text{Proj}_x\, O_{\infty,M'} \subseteq R_{\infty,M}^{N_M} \quad \forall M' \in \text{pred}(M)$$

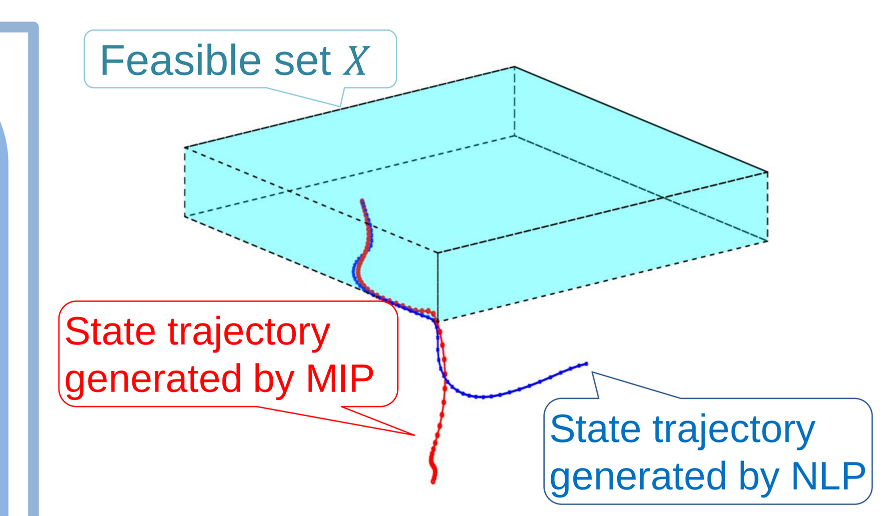
- Apply reference governor for reference tracking while imposing constraints.




#### Viability maximization and failure mode management

- State trajectory may eventually drift outside a desired operating region $X$.
- Maximize the time before trajectory exiting operating region $X$ (violating constraint).



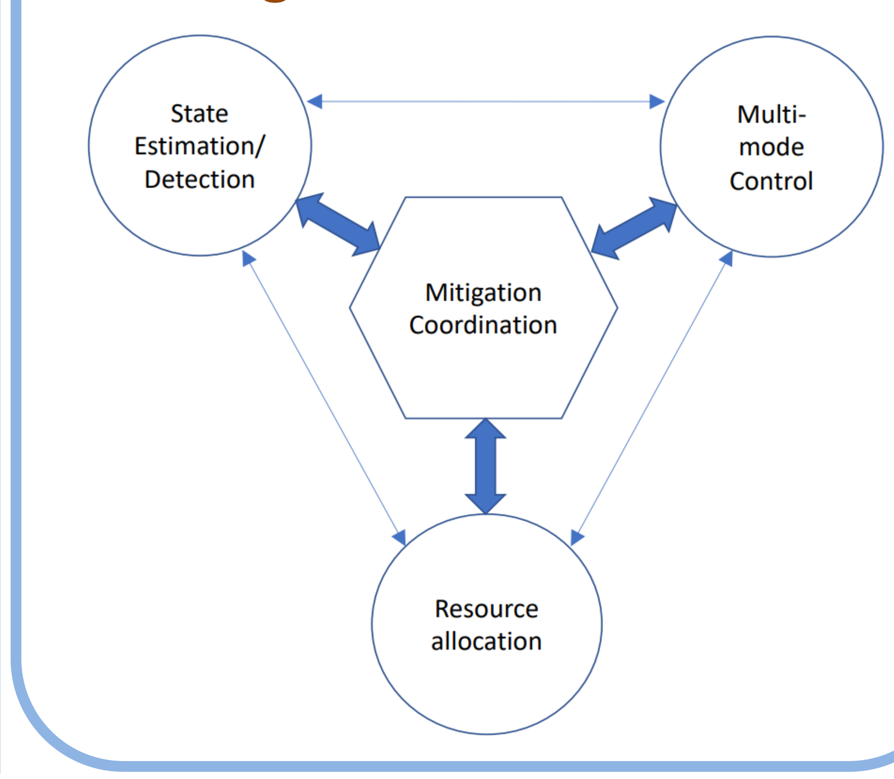

Continuous nonlinear programming (NLP) approach based on exponential weighting

$$\min_{\{u_k\}_{k=0}^{N-1}, \{\varepsilon_k\}_{k=0}^{N}} \sum_{k=0}^{N} \boldsymbol{\theta^{N-k}\varepsilon_k}$$

Subject to
$$x_{k+1} = f_d(x_k, u_k)$$
$$u_k \in U$$
$$0 \leq \varepsilon_k \leq \varepsilon_{k+1}$$
$$H(x_k) \leq h + \mathbf{1} M \varepsilon_k$$

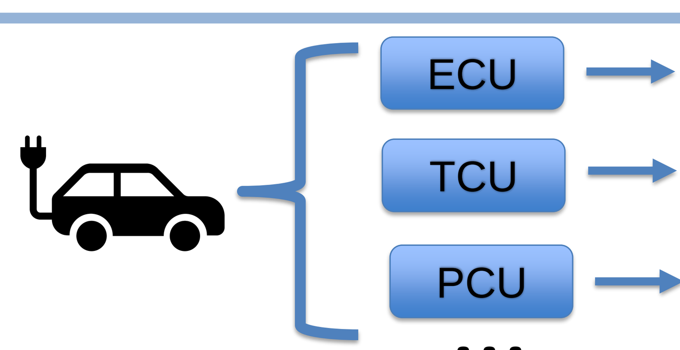
- Same "time-before-exit"
- Significantly improved computation efficiency over mixed-integer programming (MIP) approaches

### Mitigation Coordination




### Resource Allocator

Responsible for marshalling and allocating the available platform computing resources




2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: ECCS-1931738 and ECCS-1932530