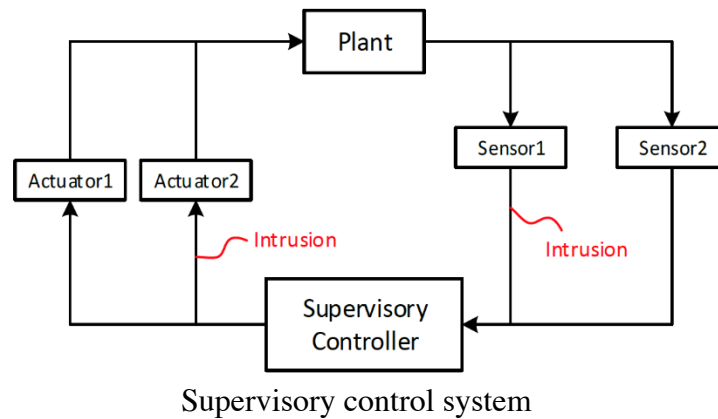


# Intrusion Detection and Resilience Against Attacks in Cyber and Cyber-Physical Control Systems



## Challenge:

- Sensors and actuators in networked feedback control loops are vulnerable to attacks that may inflict damage to cyber and cyber-physical systems



## Scientific Impact:

- Our approach will contribute to cyber and cyber-physical control systems that contain multiple feedback loops and interact with outside environment
- Design of intrusion detection module for compromised system components
- Characterization of notion of safe controllability under attacks

## Solution:

- Develop a game theoretic approach in the framework of discrete event systems to detect and characterize attacks and to synthesize suitable defense strategies
- Model-based approach; game theoretic formulation with attack scenarios and defense mechanisms

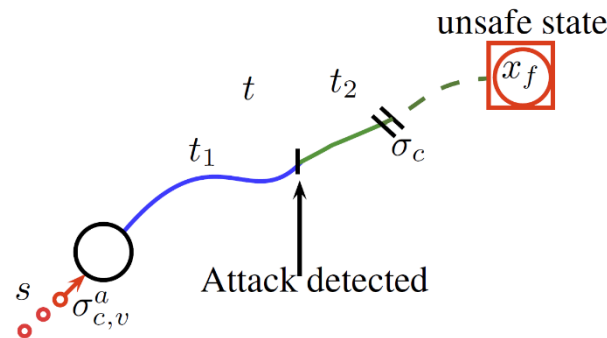
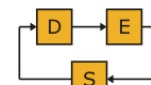


Illustration of safe controllability

CNS-1421122, University of Michigan  
Stéphane Lafortune (PI)  
stephane@umich.edu



## Broader Impact:

- Research at the interface of control engineering and cyber-security
- Combination of techniques from supervisory control, fault diagnosis, and reactive synthesis
- Multi-disciplinary training of students