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

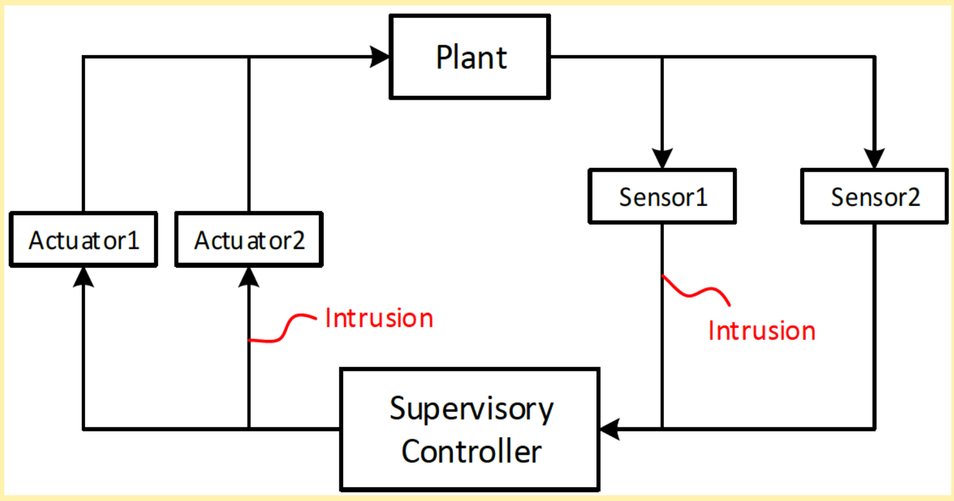
Stéphane Lafortune

https://wiki.eecs.umich.edu/stephane/index.php/CPS_Security

Objective: Develop novel methodologies to analyze and design cyber and cyber-physical control systems that can detect malicious attackers and protect against unsafe behavior after the system has been compromised.

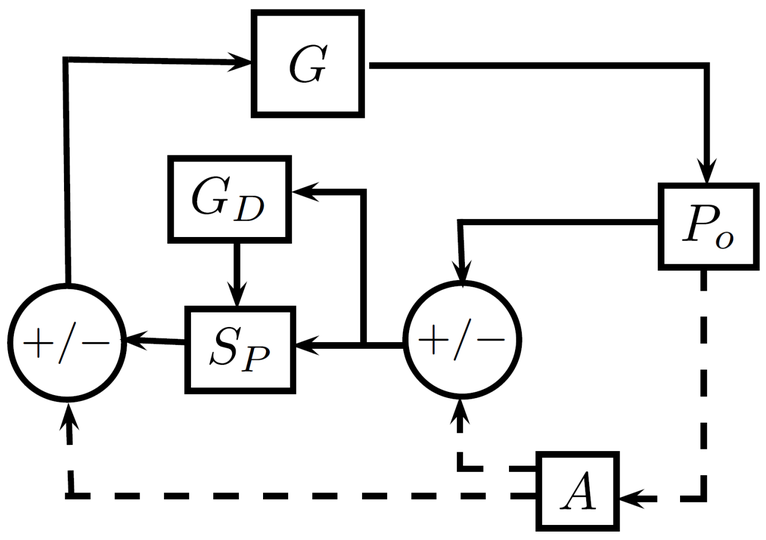
Approach and Goals:

- Discrete-event models of supervisory control systems with feedback loops
- Sensors and actuators are potentially vulnerable to malicious outside intrusion
- Defend the system by detecting intrusions and avoiding damage (unsafe states)



Supervisory control system

Detection and Mitigation of Actuator and Sensor Attacks



Closed-loop control system architecture under attack

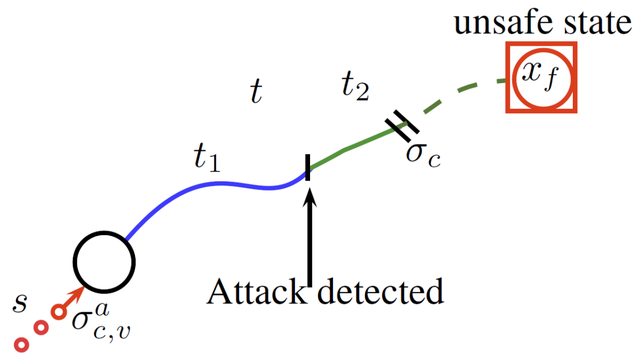
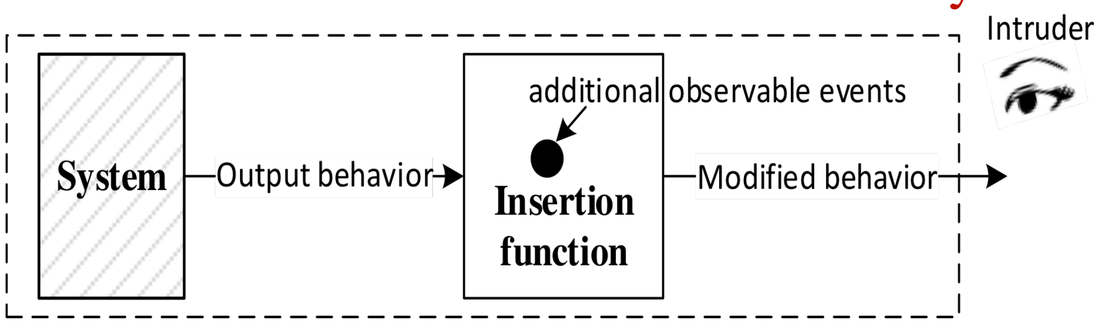


Illustration of safe controllability

- An attacker is assumed to gain control over a subset of vulnerable system actuators or sensors
- Analyze the worst-case scenario of "all possible attacks" from the attacker
- Attacker actions on actuators and sensors are modeled as fault events that are potentially unobservable
- The objective is to diagnose such attacks and intervene before an unsafe state is reached
- The diagnostic engine will trigger a switch to a "safe mode" of operation upon detection of an attack
- Characterization of the property of *safe controllability* and development of a test for it

Non-disclosure of System Secrets using Obfuscation



Obfuscation mechanism

The attacker is a malicious outside observer. It has full knowledge of the system structure and it attempts to infer system secrets from its observation of system behavior

- The defense mechanism is *obfuscation* of output behavior by the use of an *insertion function*
- By inserting fictitious events at the output of the system, the insertion function makes secret behaviors indistinguishable from non-secret ones for the intruder
- We consider both *private* and *public* insertion functions
- We developed a two-player game technique to synthesize insertion functions with the desired properties, when they exist

[1] L.K. Carvalho, Y.-C. Wu, R.H. Kwong, and S. Lafortune, "Detection and Prevention of Actuator Enablement Attacks in Supervisory Control Systems," in Proceedings of the 13th International Workshop on Discrete Event Systems, June 2016. (Journal version submitted)

[2] Y.-C. Wu, Y. Ji and S. Lafortune. Enforcement of opacity by public and private insertion functions. Submitted for journal publication, 2016

[3] X. Yin and S. Lafortune, "A Uniform Approach for Synthesizing Property-Enforcing Supervisors for Partially-Observed Discrete-Event Systems," IEEE Transactions on Automatic Control. Vol. 61, No. 8, August 2016, pp.2140-2154.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia