Secure Algorithms for Cyber-Physical Systems

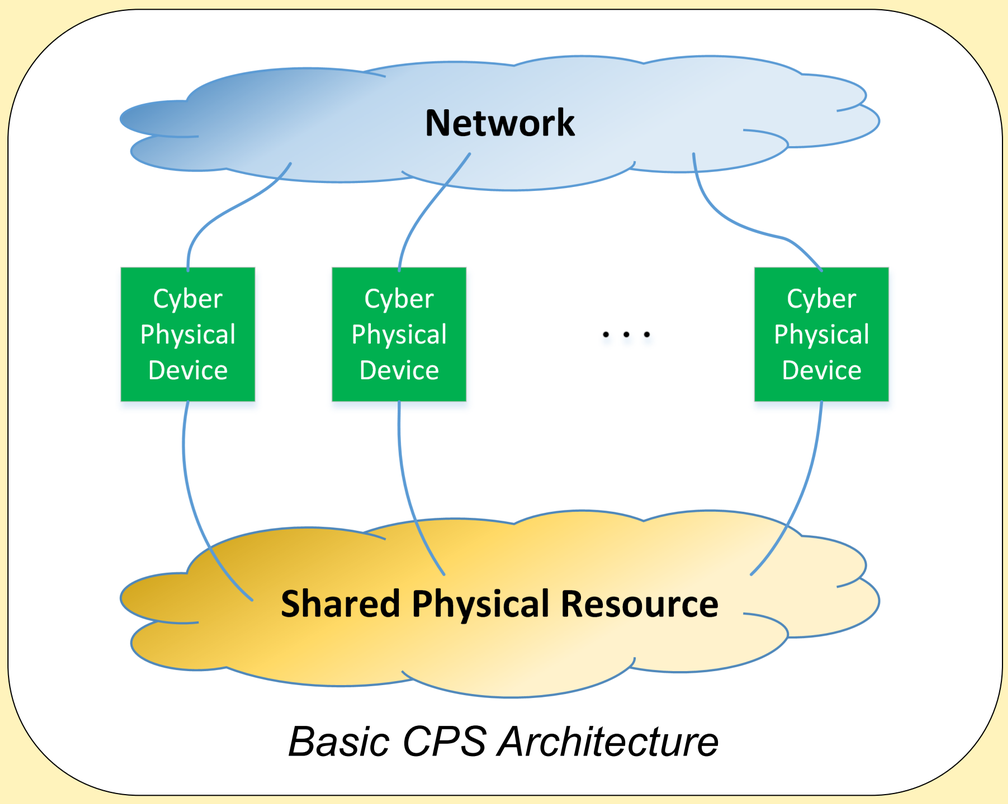
Jonathan Kimball (Missouri S&T), Bruce McMillin (Missouri S&T) and
Mo-Yuen Chow (North Carolina State University)

Invariants for Cross-Domain and Distributed Correctness

The objective of this project is to formulate and validate a methodology for creating secure algorithms in cyber-physical systems. The algorithms must be secure even when the devices do not trust each other.

A typical CPS is composed of many devices, each with both a cyber component and a physical component, interacting in a common physical system and communicating with their neighbors. The devices may be malicious and provide false information or fail to take actions as claimed, or the communication channel may be compromised.

Information flows between devices through both the network and the shared physical resource.



Basic CPS Architecture

Approach

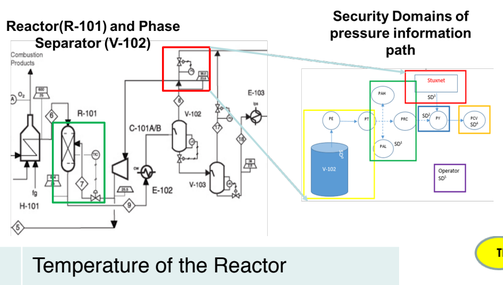
- Extend the Cyber World of logical Predicates to the Physical World
- Domain Experts Represent Physical Attributes (Chemistry, Physics)
- Distributed Run-Time Monitoring
- Correctness in the presence of threats and failures

Multiple Security Domains

- Use multiple domain nondeducibility (MSDND)
- Locate vulnerabilities
- Valuation functions $V_y^i(w)$ return the value of the corresponding state variable as seen by an entity in domain *i*.
- MSDND secure allows an attacker to go undetected.

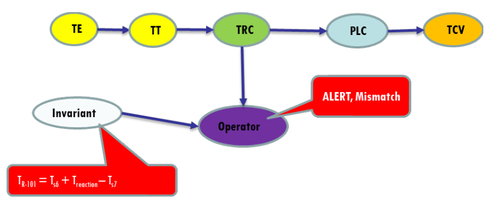
$$\text{MSDND} = \forall w \in W : w \vdash \left[s_x \ \mathbf{xor}\ s_y\right] \wedge \left[w \models \left(\nexists V_x^i(w) \wedge \nexists V_y^i(w)\right)\right]$$

Invariants for Chemical Plants

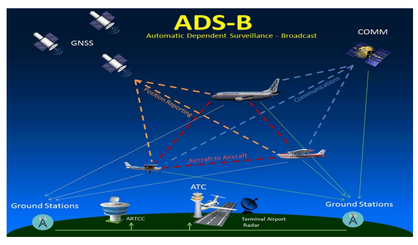


$T_{R\text{-}101}$	Temperature of the Reactor
T_{s6}	Temperature reduction due to pumping of H_2 (Stream 6)
$T_{reaction}$	Rise in temperature due to reaction
T_{s7}	Temperature of the inputs (Stream 7)

Invariant provides additional paths to break MSDND



Invariants for Air Traffic



$$MSDND(ES) = \exists w \in W: [w \vdash \Box f(s_{p1}, s_{p2}, s_c)] \wedge [w \models (\nexists V_1^{p1}(w) \wedge \nexists V_2^{p2}(w) \wedge \nexists V_3^{p1}(w) \wedge \nexists V_4^{p2}(w) \wedge \nexists V_6^{c}(w) \wedge \nexists V_6^{p1}(w) \wedge \nexists V_6^{p2}(w))]$$

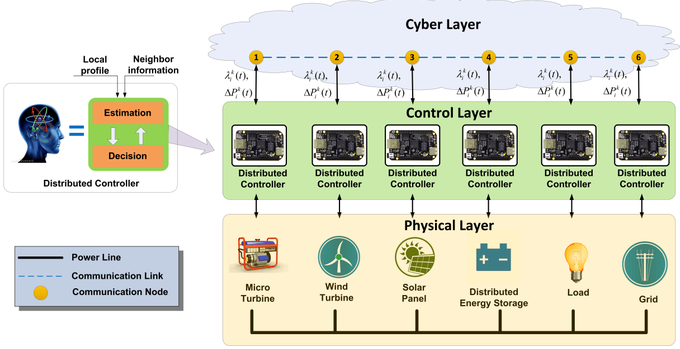
Pilot 1 and Pilot 2 are confused if no valuation exists over the 6 security domains

Break MSDND → Add Inertial Navigation

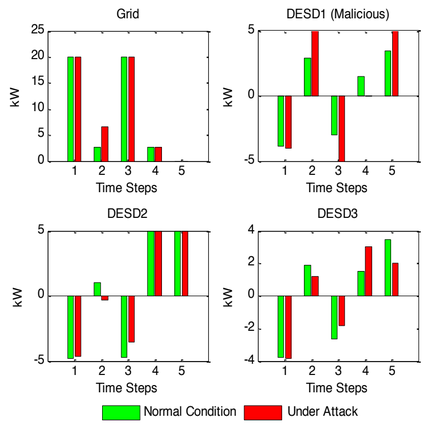
Cooperative Distributed Energy Scheduling (CoDES)

Data integrity attack can increase one node's profits

Add reputation function to defend



Benefit	Normal	Attacked	Change
Total Bill	187.02	208.55	21.53
DESD 1	26.08	34.06	**7.98**
DESD 2	38.56	35.98	-2.58
DESD 3	22.35	17.03	-5.32



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

Awards 1505610 and 1505633

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
January 9-11, 2017
Crystal City, Arlington, VA

National Science Foundation
WHERE DISCOVERIES BEGIN

MISSOURI S&T
NC STATE