2017 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

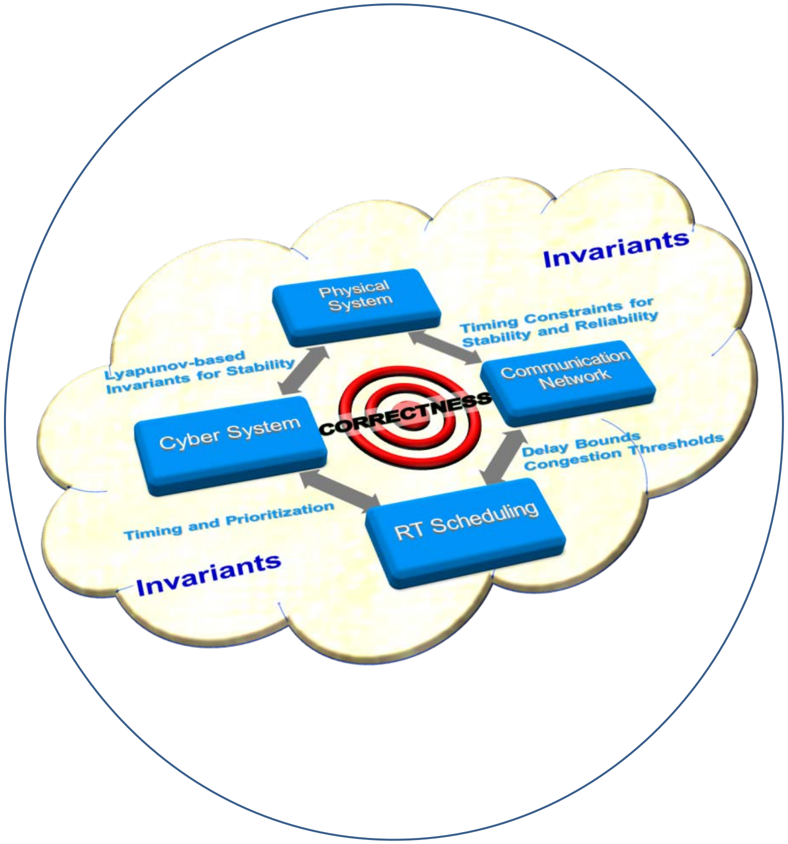
Secure Algorithms for Cyber-Physical Systems

- Jonathan Kimball (PI), Bruce McMillin (Presenter), Mo-Yuen Chow
- Missouri University of Science and Technology
- North Carolina State University
- mst.edu
- ff@mst.edu

- CNS-1505610

Create secure CPS applications without relying on trust

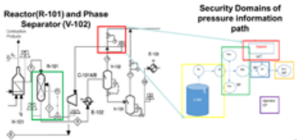
- Carve the CPS into multiple domains
- Treat Cyber and Physical uniformly as Information
    - Integrity Attacks are disruptions of flow to defenders
    - Confidentiality Defense is disruption of flow to attackers
- Add more information to break the MSDND nondeducibility
    - Invariants on Program State
    - Physics Based
    - Algorithms Based
    - Distributed
- Run-time evaluation


Invariants
Physical System
Timing Constraints for Stability and Reliability
Lyapunov-based Invariants for Stability
Communication Network
CORRECTNESS
Cyber System
Delay Bounds Congestion Thresholds
Timing and Prioritization
RT Scheduling
Invariants

$$\text{MSDND (ES)} = \exists w \in W \vdash [(s_x \oplus s_y)] \wedge [w \vdash (\nexists V_x^i (w) \wedge \nexists V_y^i (w))]$$

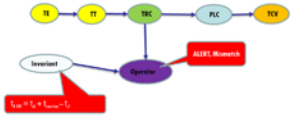
Findings

Invariants for Chemical Plants


Reactor(R-101) and Phase Separator (V-102)
Security Domains of pressure information path

Invariant provides additional paths to break MSDND

T_{R-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)



Invariants for Air Traffic

ADS-B
ATC
Ground Stations
Ground Stations

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

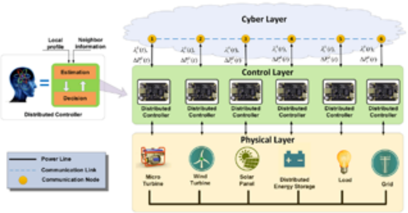
$$MSDND(ES) = \exists w \in W : [w \vdash \Box f(s_{p1}, s_{p2}, s_c)] \wedge [w \models (\nexists V_1^{p1}(w) \wedge \nexists V_2^{p2}(w) \wedge \nexists V_3^{p1}(w) \wedge \nexists V_4^{p2}(w) \wedge \nexists V_6^{c}(w) \wedge \nexists V_6^{p1}(w) \wedge \nexists V_6^{p2}(w))]$$

Break MSDND → Add Inertial Navigation

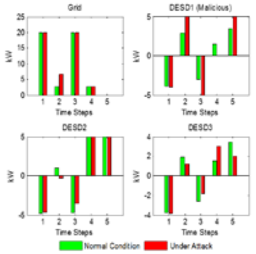
Cooperative Distributed Energy Scheduling (CoDES)

Data integrity attack can increase one node's profits

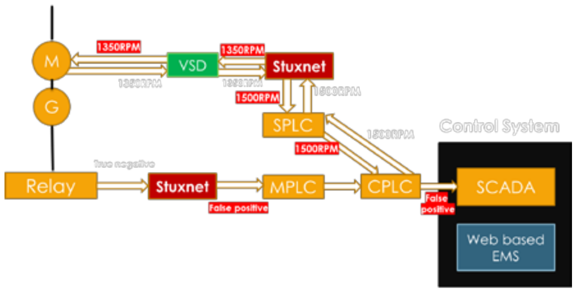
Add reputation function to defend



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

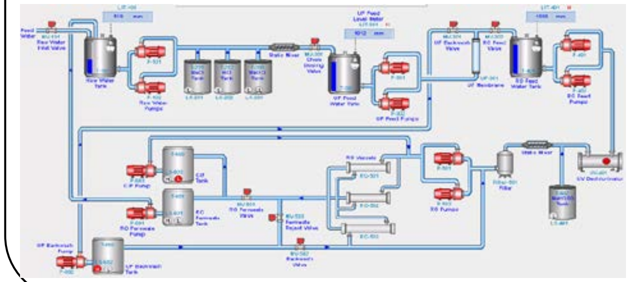


Invariants for Power



$$MSDND = \nexists\, V_{RR}^{SCADA} \wedge \nexists\, V_{\sim RR}^{SCADA} \wedge \nexists\, V_{RPM}^{SCADA} \wedge \nexists\, V_{\sim RPM}^{SCADA}$$

Invariants for Water Treatment



Scientific Impact:

Duality of information flow and deducibility protects both confidentiality and integrity of cyber and physical flows with the same model.