Secure Algorithms for Cyber-Physical Systems, July 15, 2015

Jonathan Kimball and Bruce McMillin, Missouri University of Science and Technology
Mo-Yuen Chow, North Carolina State University

Challenge:

- How to provide a functioning CPS relying on Ground Truth of the system.

Solution:

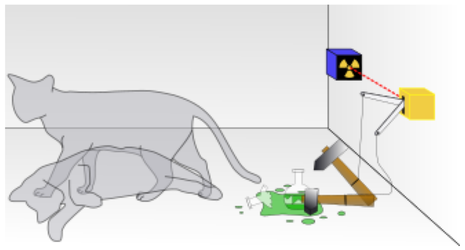
- Treat Cyber and Physical uniformly as Information
- Integrity Attacks are disruptions of flow to defenders
- Confidentiality Defense is disruption of flow to attackers
- Add more information to break the MSDND nondeducibility
  - Invariants on Program State
  - Physics Based
  - Algorithms Based
 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

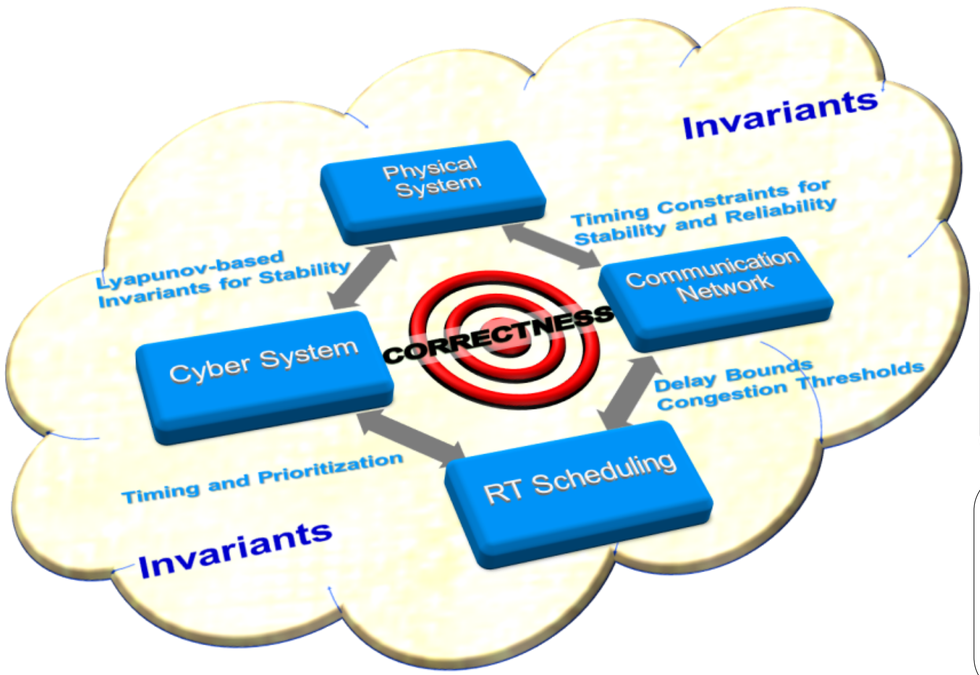
MSDND:

- Multiple Security Domain Nondeducibility
- A system is MSDND secure if it cannot be valuated whether a state x or y holds, or not, in a particular domain, i
- V_y^i is a valuation function in domain I over state y
- If MSDND secure, we cannot distinguish normal operation from attack

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

In the well-known Schrödinger's cat thought experiment, the cat's health is MSDND secure outside the box due to lack of valuation, but not MSDND secure from inside the box due to valuation.

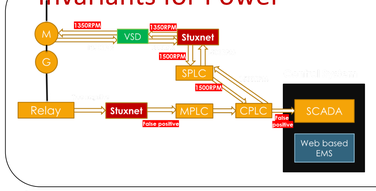




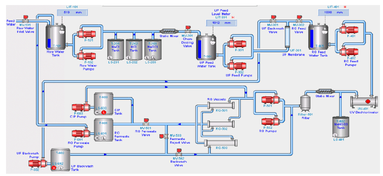
Scientific Impact:

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

Invariants for Power

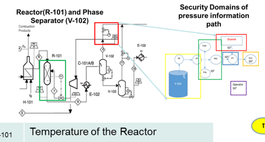


Invariants for Water Treatment



- Societal Resilience, water, power, chemical, aviation, transportation
- Smart Cities

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

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

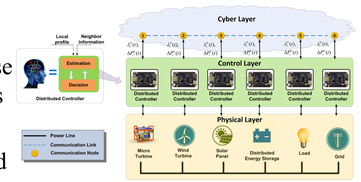
$$MSDND(ES) = \exists w \in W : [w \vdash \sqsupset f(s_{p1}, s_{p2}, s_c)] \wedge [w \models (\nexists V_1^{p1}(w) \wedge \nexists V_2^{p2}(w) \wedge \nexists V_3^{p3}(w) \wedge \nexists V_4^{p2}(w) \wedge \nexists V_5^{c}(w) \wedge \nexists V_6^{p3}(w) \wedge \nexists V_6^{p2}(w))]$$

Break MSDND → Add Inertial Navigation

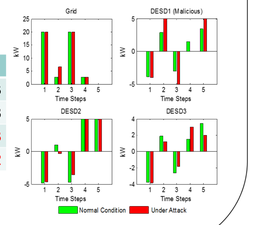
Cooperative Distributed Energy Scheduling (CoDES)

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



CNS-1505610/1505633