

CPS Security Research at SUTD

Nils Ole Tippenhauer (SUTD)

CyPRO Protection of Cyber-Physical Systems

- ~5M SGD, collaborator PUB (water)
 - ▶ Access control in ICS, Remote attestation
 - ▶ Physical-layer attacks and resilient distributed computations
 - ▶ SWaT testbed

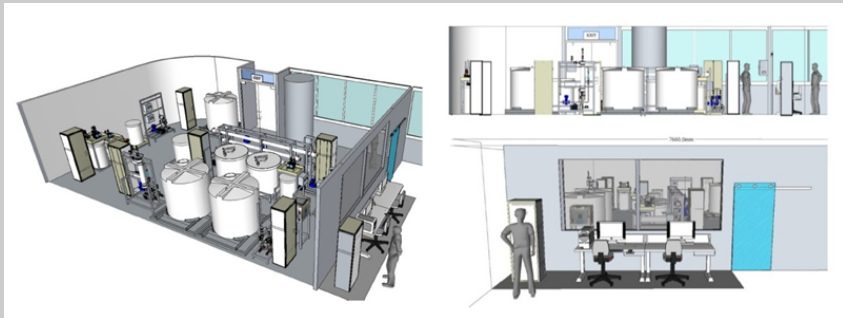
ASPIRE * Advancing Security of Public Infrastructure using Resilience and Economics

- ~6M SGD, collaborator SingPower Powergrid+PUB
 - ▶ Attacker models and layered defenses
 - ▶ Control Theoretic Defenses against Attacks
 - ▶ WADI and EPIC testbeds

ReSILIoT Research & Security Innovation Lab for Internet of Things

- ~5M SGD
 - ▶ Smart Home, Smart Nation infrastructure
 - ▶ IoT honeypots, IoT scanner, automatic testbed

- SWaT: Water treatment plant
 - ▶ 6 process stages, 5 gallons/minute
 - ▶ Distributed control, geographically centralized
- WADI: Water distribution testbed (opens soon)
 - ▶ 3 process stages: Reservoir, distribution, consumption
 - ▶ Centralized control, geographically distributed
- EPIC: Electric Power and Intelligent Control (in construction)
 - ▶ 4 process stages: Generation, distribution, micro-grid, load
- ReSILIoT: smart home testbed



- Software support for industrial protocol parsing
 - ▶ E.g. Scapy+Bro support for EtherNet/IP
- Complementary security solutions (L0,L1,L2 network)
 - ▶ Authenticated data collection
 - ▶ Traffic authentication
 - ▶ Attack detection (stateful, stateless)
 - ▶ Machine learning (physical process data)
 - ▶ Network traffic anomalies
- Cyber+Physical Simulation
 - ▶ MiniCPS
 - ▶ Formal models
 - ▶ Automatic learning of process models from data
- SCy-Phy Systems Week (yearly workshop)
 - ▶ Topic: CPS security (with hands-on)
 - ▶ itrust.sutd.edu.sg