SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

Cybersecurity for Critical Infrastructure

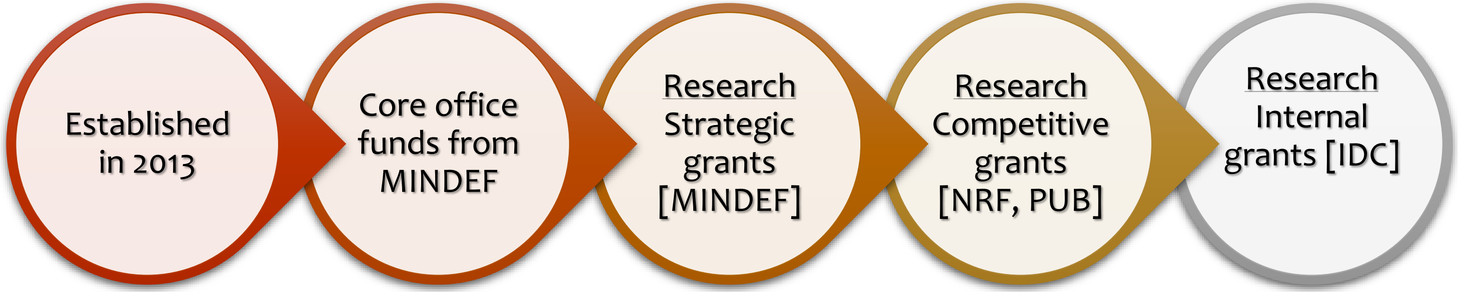
Prof. Jianying Zhou

SIEW’19@MBS, 1 November 2019

iTrust
Centre for Research
in Cyber Security

iTrust @ SUTD

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN


Established in 2013
Core office funds from MINDEF
Research Strategic grants [MINDEF]
Research Competitive grants [NRF, PUB]
Research Internal grants [IDC]

National Satellite of Excellence [NSoE]

Established in April 2019 by NRF

Focus: Design Science and Technology for Secure Critical Infrastructure [DeST-SCI]

A. Impactful research
B. Industrial partnership
C. Technology transfer

OUR MISSION

To advance the state of the art and practice in the design of secure complex interconnected critical infrastructure.

To improve the understanding of cyber threats to Cyber-Physical Systems and to develop and experiment with strategies to mitigate such threats.

https://itrust.sutd.edu.sg/

Testbeds @ iTrust

Secure Water Treatment (SWaT)

Water Distribution (WADI)

IoT Shielded Room

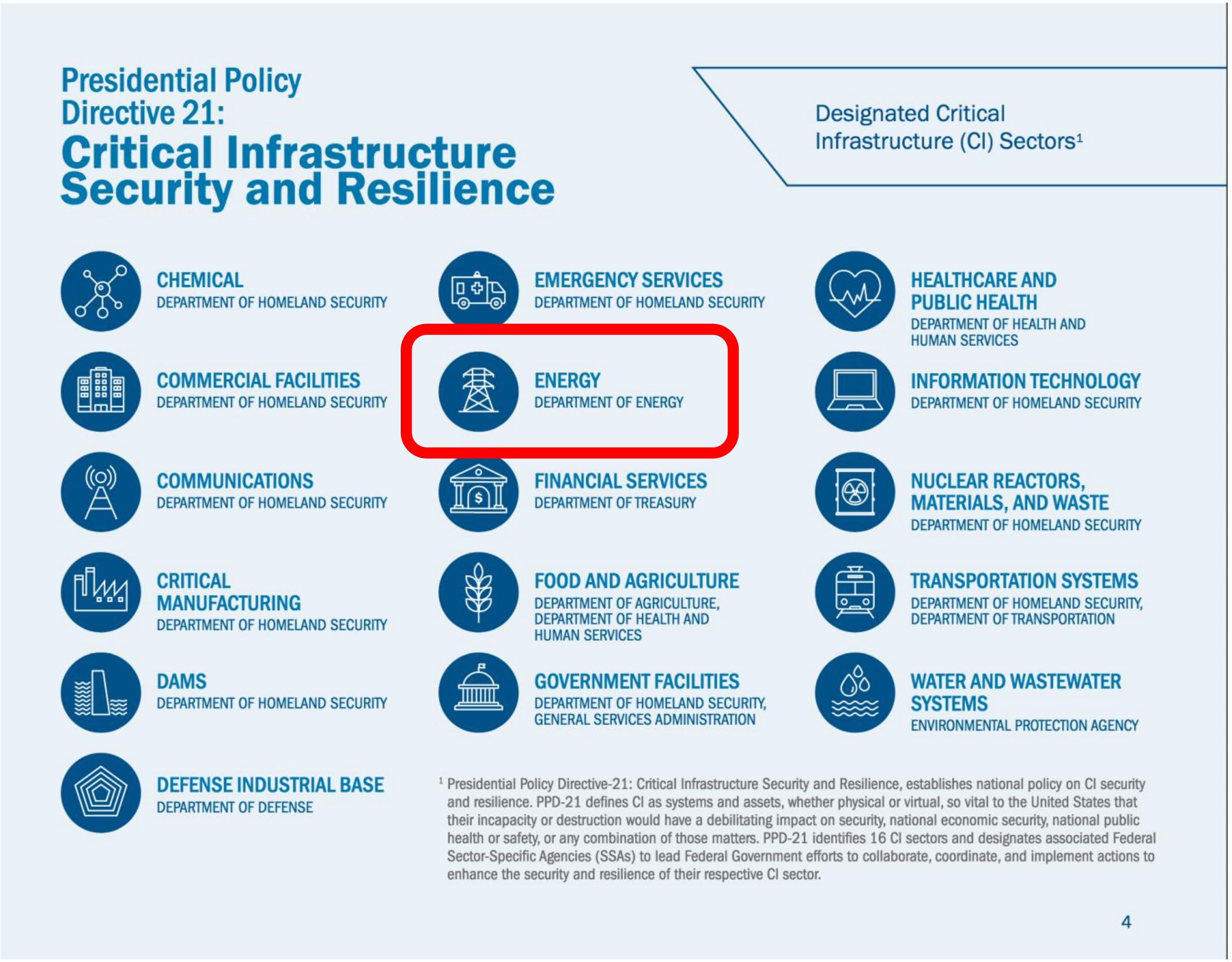
Transformer & inverters

Electric Power & Intelligent Control (EPIC)

Generators & programmable loads

Critical Infrastructure

NCCIC/ICS-CERT



Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

Designated Critical Infrastructure (CI) Sectors[1]

- **CHEMICAL**
  DEPARTMENT OF HOMELAND SECURITY
- **COMMERCIAL FACILITIES**
  DEPARTMENT OF HOMELAND SECURITY
- **COMMUNICATIONS**
  DEPARTMENT OF HOMELAND SECURITY
- **CRITICAL MANUFACTURING**
  DEPARTMENT OF HOMELAND SECURITY
- **DAMS**
  DEPARTMENT OF HOMELAND SECURITY
- **DEFENSE INDUSTRIAL BASE**
  DEPARTMENT OF DEFENSE
- **EMERGENCY SERVICES**
  DEPARTMENT OF HOMELAND SECURITY
- **ENERGY**
  DEPARTMENT OF ENERGY
- **FINANCIAL SERVICES**
  DEPARTMENT OF TREASURY
- **FOOD AND AGRICULTURE**
  DEPARTMENT OF AGRICULTURE, DEPARTMENT OF HEALTH AND HUMAN SERVICES
- **GOVERNMENT FACILITIES**
  DEPARTMENT OF HOMELAND SECURITY, GENERAL SERVICES ADMINISTRATION
- **HEALTHCARE AND PUBLIC HEALTH**
  DEPARTMENT OF HEALTH AND HUMAN SERVICES
- **INFORMATION TECHNOLOGY**
  DEPARTMENT OF HOMELAND SECURITY
- **NUCLEAR REACTORS, MATERIALS, AND WASTE**
  DEPARTMENT OF HOMELAND SECURITY
- **TRANSPORTATION SYSTEMS**
  DEPARTMENT OF HOMELAND SECURITY, DEPARTMENT OF TRANSPORTATION
- **WATER AND WASTEWATER SYSTEMS**
  ENVIRONMENTAL PROTECTION AGENCY

[1] Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, establishes national policy on CI security and resilience. PPD-21 defines CI as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. PPD-21 identifies 16 CI sectors and designates associated Federal Sector-Specific Agencies (SSAs) to lead Federal Government efforts to collaborate, coordinate, and implement actions to enhance the security and resilience of their respective CI sector.

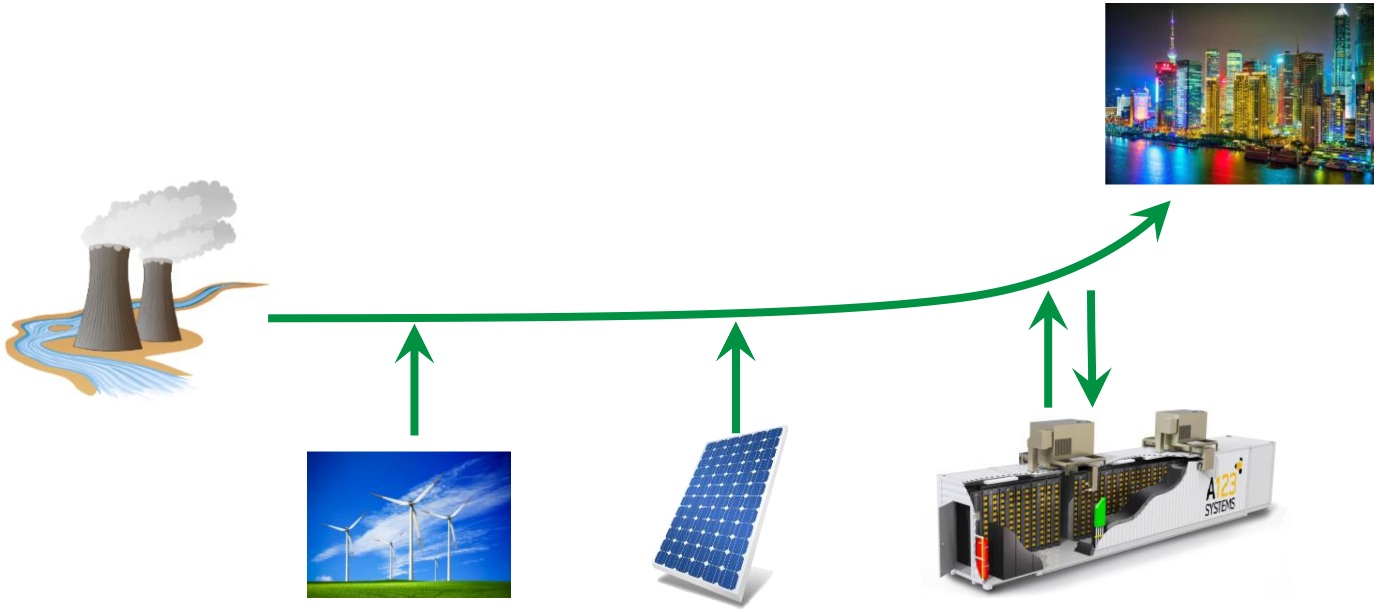
Cyber Attacks in Real World

Stuxnet (2010)

Ukraine power grid cyber attack (2015, 2016)

Attack Methods

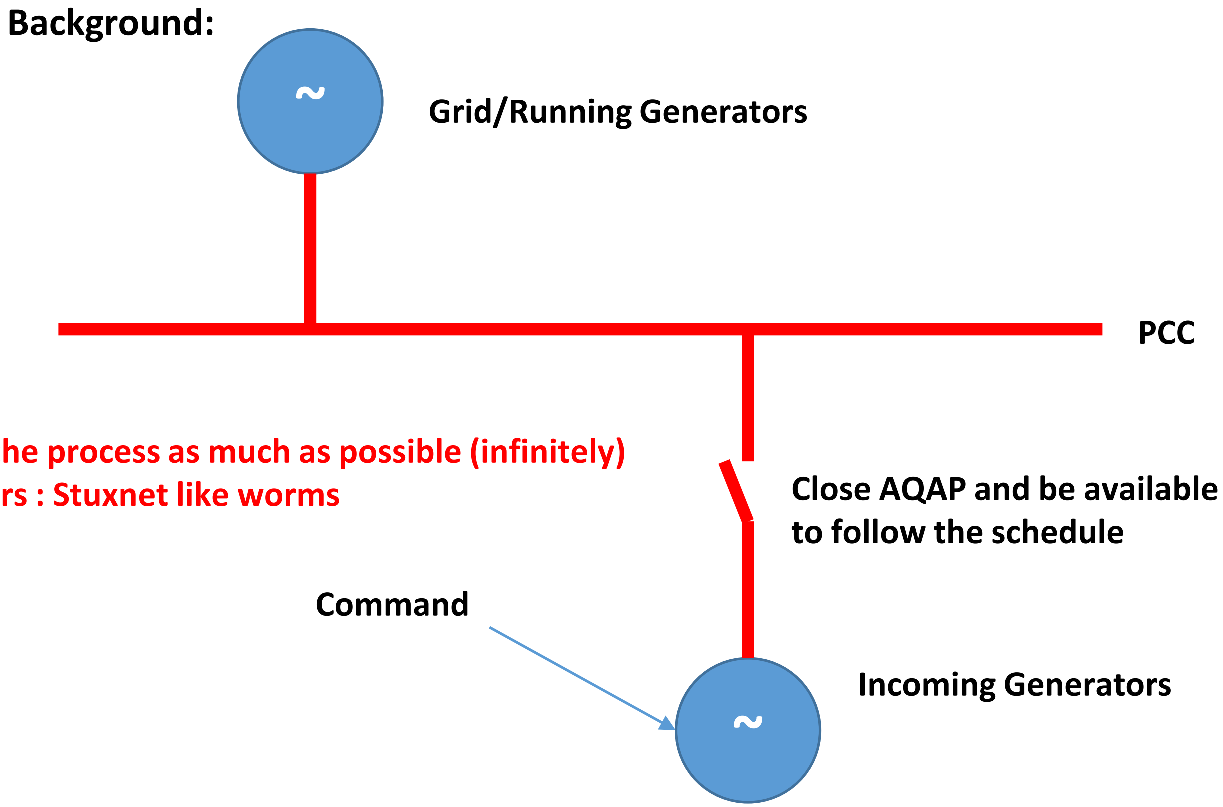
- Network scanning
- Command injection
- False data injection
- Malware
- Spear phishing



Social Engineering → Physical and Virtual Insider

An Example of Our Attack

Attacking Generator Synchronization



Background:

Grid/Running Generators

PCC

Close AQAP and be available to follow the schedule

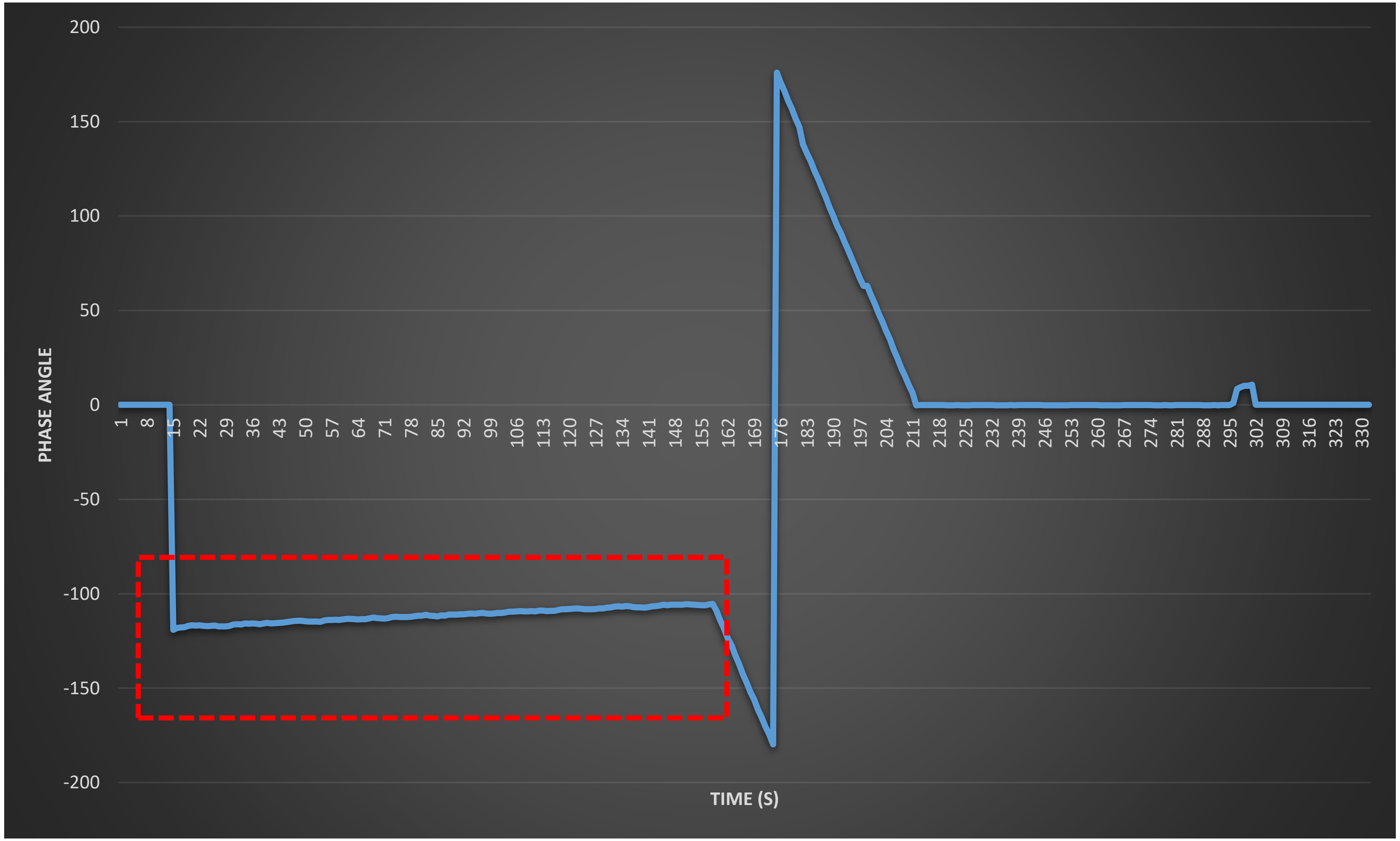
Command

Incoming Generators

Goal: Delay the process as much as possible (infinitely)
Attack Vectors : Stuxnet like worms

An Example of Our Attack

Attack Scenario: Prolonged sufficiently



Cyber Defense of Critical Infrastructure

Operational Technology [OT] centric:

- Detect process anomalies resulting due to an attack
- Avoid process anomalies that could be created due to an attack

Design Centric
(Physics/Chemistry)

Data Centric
(AI + ML)

Authentication &
Attestation

Modeling &
Analysis/Verification

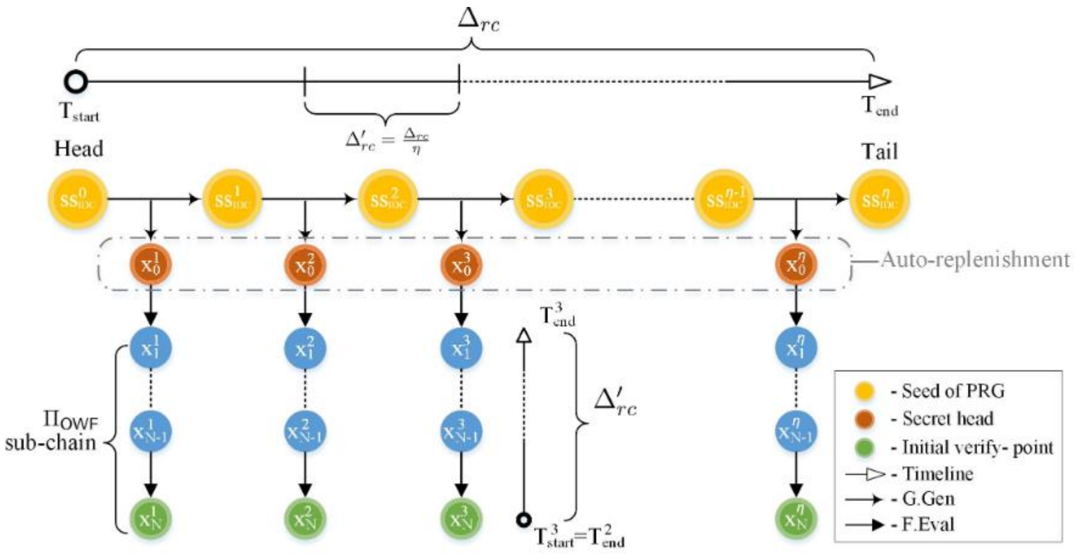
Proof of Aliveness (PoA)

Objective:

- Do real-time remote attestation whether a target device in CPS keeps operating.

Solution:

- Based on a novel multi-chain Time-based One-Time Password (TOTP).
- Target device continuously sends unforgeable proofs (e.g. one-time password) to a verifier (e.g., SCADA server) to show that the device is still alive.



Features:

- Fast & secure one-time password generation & verification
- Auto password replenishment: self-reinitialization

Reference:

- “Proof of Aliveness". **ACSAC'19** (patent pending)

NoisePrint

Objective:

- Identify devices (sensors and actuators) and detect anomalies in CPS.

Solution:

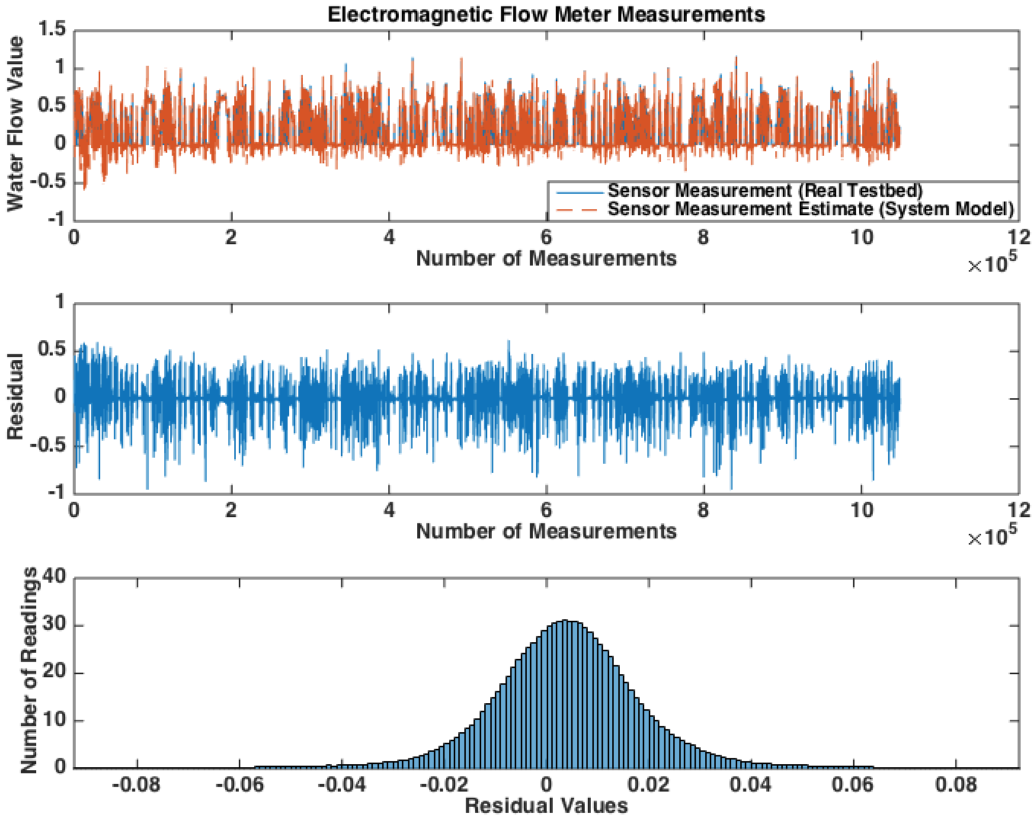
- Fingerprint two noise sources:
  - ✓ Device noise: comes from device manufacturing imperfections
  - ✓ Process noise: comes from the physical process of a system
- NoisePrint = device identification + attack detection

Features:

- High accuracy
- Non-intrusive detection

Reference:

- “NoisePrint: Attack Detection Using Sensor and Process Noise Fingerprint in CPS". **ACM AsiaCCS’18** (patent pending)



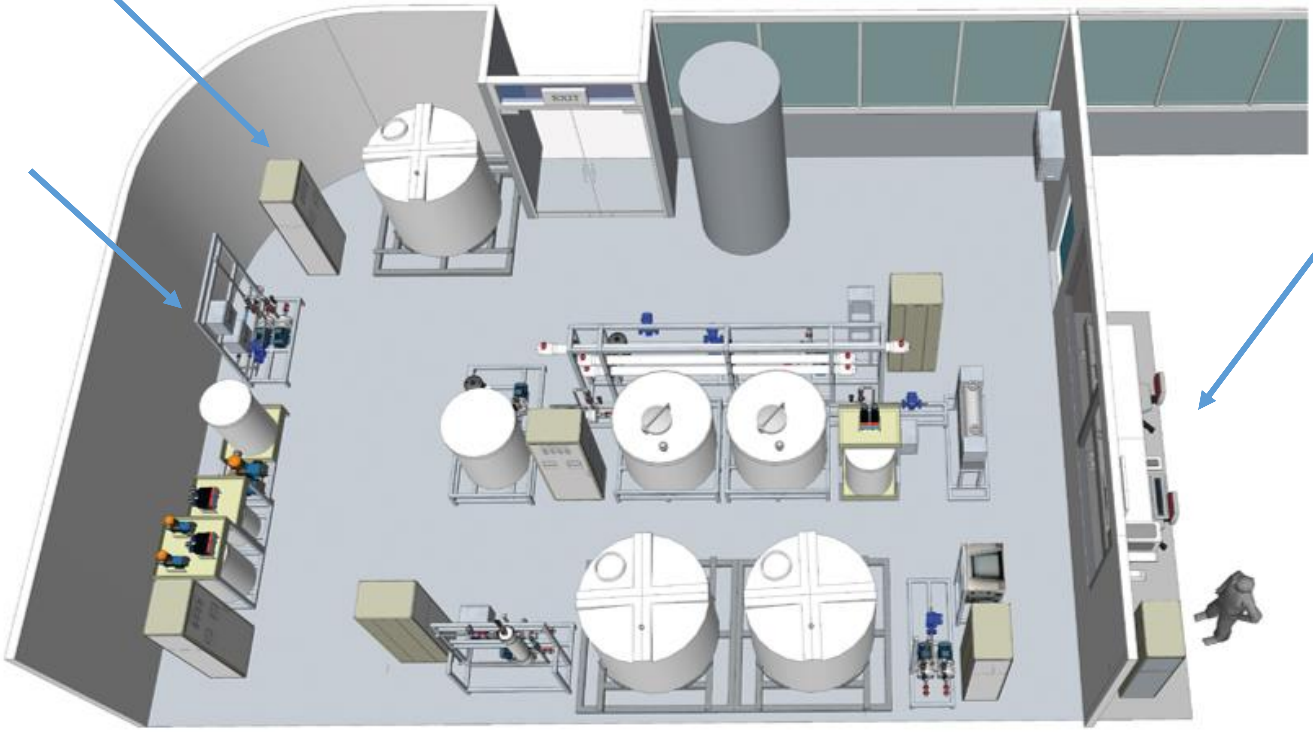
Technologies @ iTrust

Layer 1 (PLC)

- *DAD**
- *PoA**
- PLC code attestation

Layer 0 (Sensor/Actuator)

- *NoisePrint**
- *Black-box monitor**



Layer 2 (Historian)

- *ICS:BlockOps**

Critical Infrastructure Security Showdown (CISS) 2019

https://itrust.sutd.edu.sg/ciss-2019/

**Patent / patent pending*

Ongoing Research @ iTrust

- Attack benchmarking
- Command validation
- Metrics for resilience assessment
- ML-based rule/invariant derivation
- Digital twinning

iTrust
Centre for Research in Cyber Security

Thank You !

jianying_zhou@sutd.edu.sg

Welcome to visit iTrust.