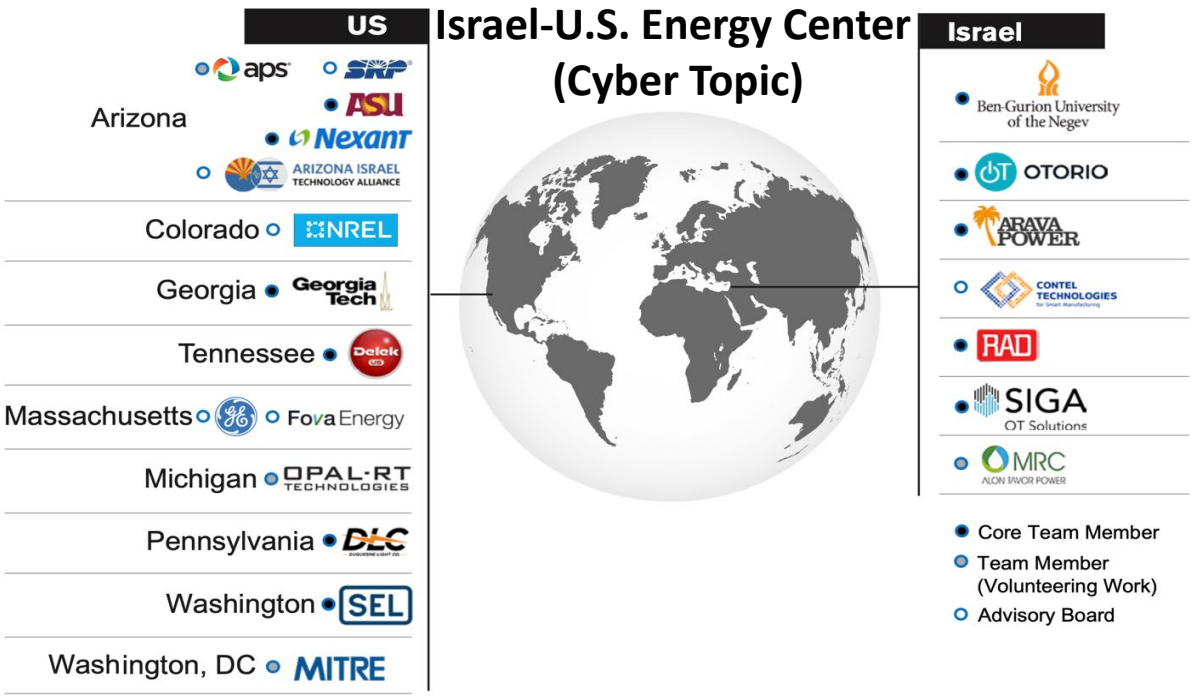
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Task7

Malware Threat Mitigation in ICS/SCADA/OT Environment

Quarterly Review Workshop II

Dr. Wenke Lee, Moses Ike
Georgia Institute of Technology
May 6, 2022

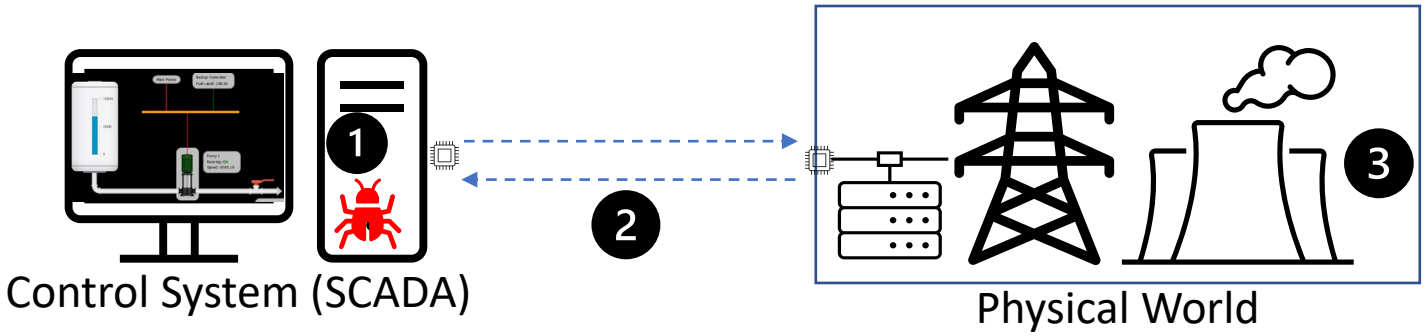
ICS Malware Attacks is a big problem in OT

- **2010 Stuxnet:** Iran centrifuge system
- **2014 Havex** (various organizations)
- **2016 Industroyer:** Ukrainian Power
- **2021 Oldsmar:** Water Treatment Plant
- **2021 Colonial Attack:** Oil and gas Pipeline
- **2022 Industroyer II**

Limitations of Existing Tools

1. Host System/API Call Behavior
   - Malware/Attacks use similar API calls
2. Statistical Traffic/Protocol Analysis
   - Only effective against obvious or noisy attacks (e.g., network scans, DoS, malformed protocols)
3. Physical Models (Sensor-based Deviations)
   - Raises many false alarms in practice due to benign deviation (e.g., faults/noise)

THREAT MODEL



Preliminaries: Value and Impact

- Practical Usability
  - Georgia Tech is leveraging ICS domain knowledge from its collaborations with Industry, such as Sandia National Labs, to develop techniques that is usable in practice

- New Insights
  - Georgia Tech has gained new insights on the ICS-specific nature of ICS malware behavior (e.g., Industroyer)
  - Lesson Learned and toolset will Impact ICS Industry

Objective

Correlating multiple “malware execution-relevant” datapoints

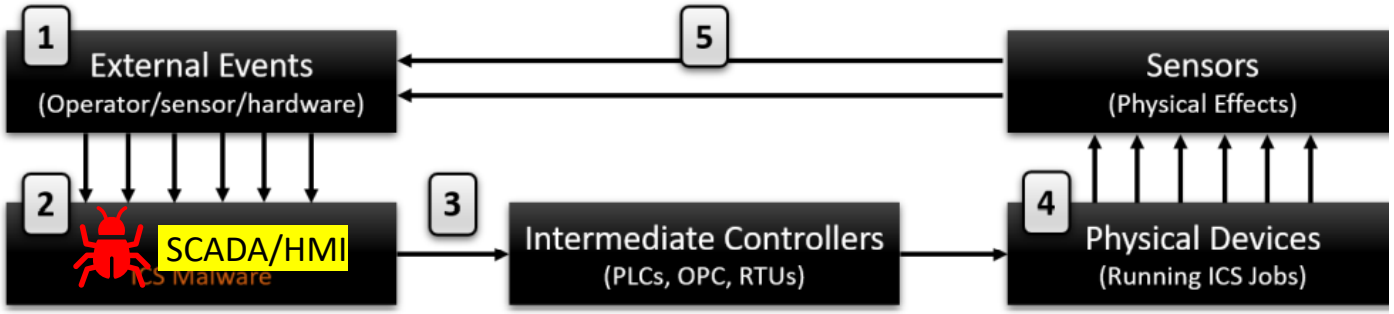


Figure 1: End-to-End ICS/SCADA process-control operation form a feedback control loop

Leveraging ICS Domain Knowledge

- SCADA execution follows an event-based mechanism
  - To blend with SCADA behavior, attackers/malware follow the same events to stay hidden

<u>Approach</u>: Model the **end-to-end** SCADA behavior triggered by physical events (sensor states)

- Develop a physical event-based behavior correlation algorithm

1 Sensor Data → 2 SCADA API Calls → 3 Control Commands

Initial Results: ICS Malware Host and Network Analysis

- 2016 Industroyer Malware Attack on Ukraine Power Grid
  - Industroyer sent malicious commands to circuit breakers and caused power outage

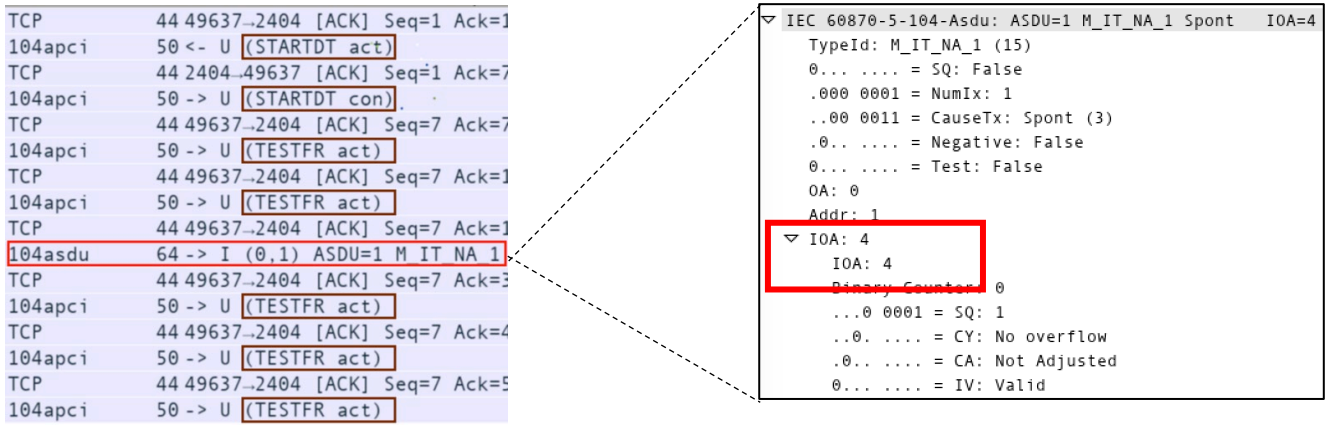
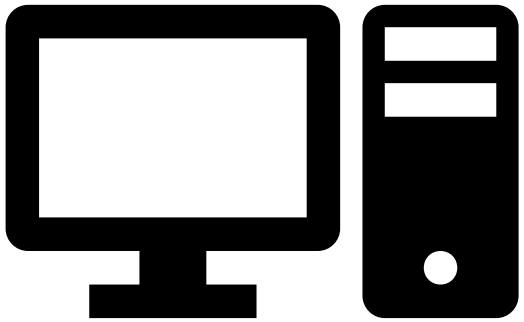
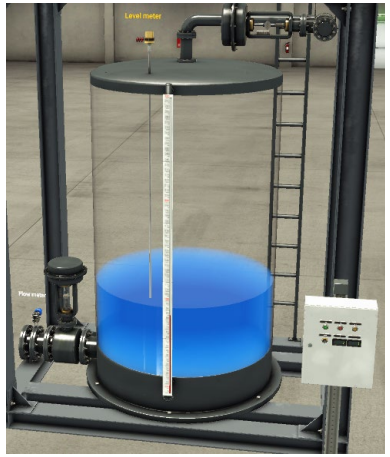


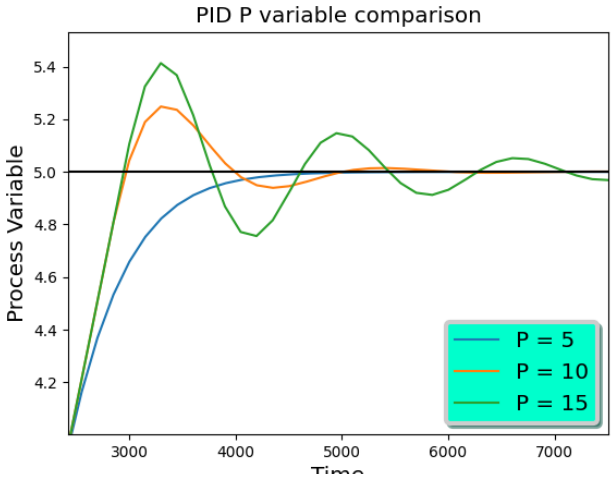
Figure 2: Industroyer Malware's ICS network behavior: Showing attack payload

- ICS-specific behaviors of Industroyer(Lesson learned)
  - Industroyer understood some physics of power systems
  - Terminated the legitimate SCADA program to hijack COM Ports to physical systems
  - Executed API calls may be anomalous to the core SCADA process-control
  - Sent Isolated commands not based on the physical dependences in the plant

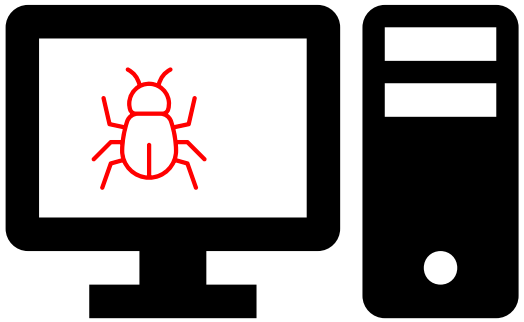
Modern ICS Attacks are Semantic (Physics) Based

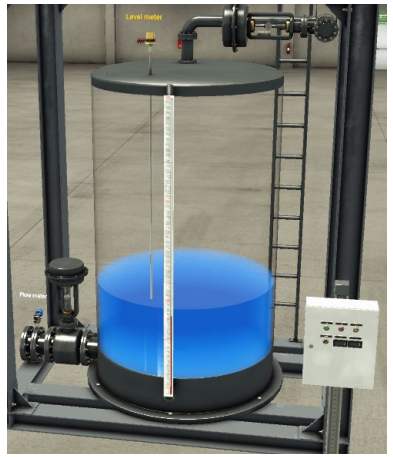


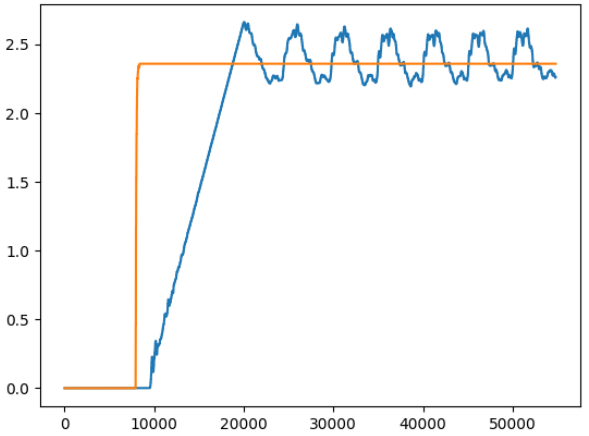




Benign Behavior







Attack Behavior

Adaptation of the 2021 Oldsmar Water Treatment Attack

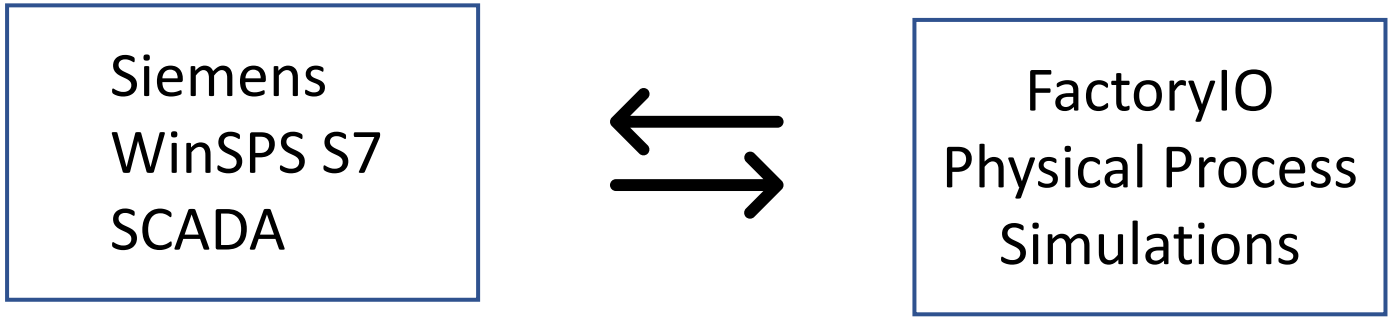
Analyzing Physical Ramifications in SCADA execution

- Execution-Phase Specific API Behaviors
  - Submitted Major Revision to S&P Oakland 2023

- Statistical and Temporal Physical Dependencies Telemetry
  - Submitted to CCS 2022

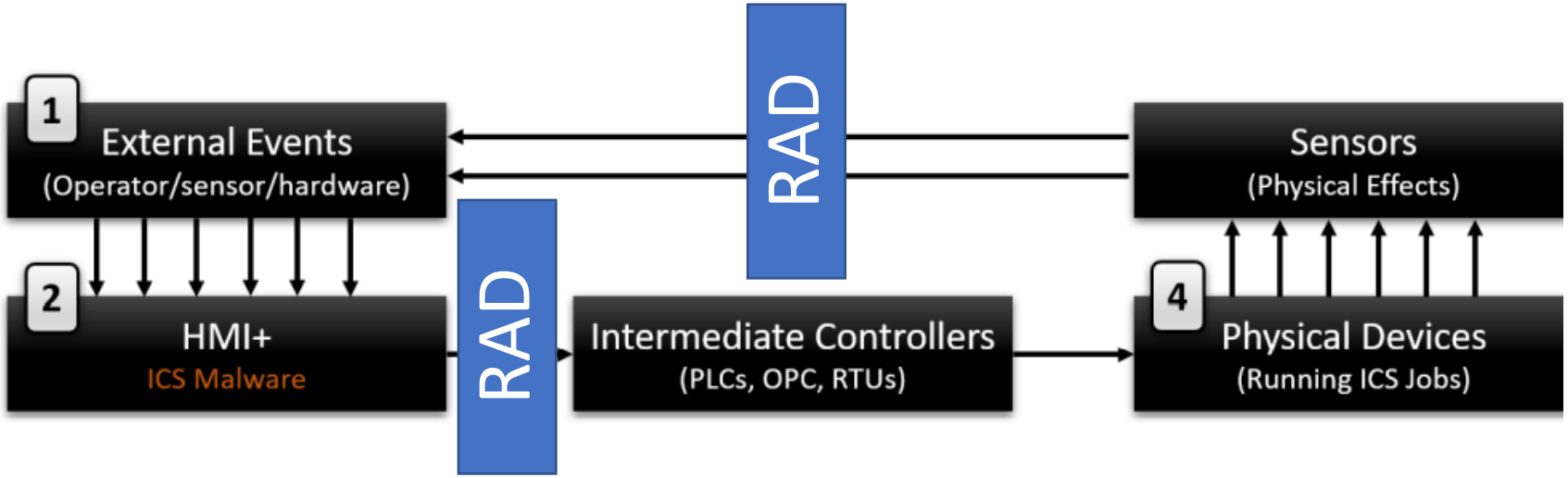
Tool Development

- **To Show Usability and Develop our Algorithm in Realistic Settings**
  - **Need to develop a SCADA Experimentation Testbed**
    - A virtual testbed, with a SCADA side and a physical world side



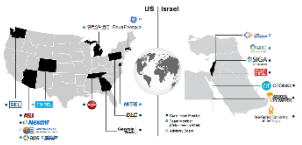
Commercialization

- Promising Integration opportunities with RAD Gateway
- Concrete Commercialization based on further use case analysis
  - Distributed or centralized data collection and analysis?
  - Offline or online detection ?



QUESTIONS

Cyber Security News



December 2019 — **Iranian** wiper malware was deployed against the network of Bapco, the national oil company of Bahrain.

January 2020 — A **Russian** hacking group infiltrated a Ukrainian energy company where Hunter Biden was previously a board member, and which has featured prominently in the U.S. impeachment debate.

April 2020 — Government and energy sector entities in **Azerbaijan** were targeted by an unknown group focused on the SCADA systems of wind turbines.

April 2020 — Suspected Iranian hackers unsuccessfully targeted the command and control systems of water treatment plants, pumping stations, and sewage in Israel.

May 2020 — **Israeli** hackers disrupted operations at an Iranian port for several days, causing massive backups and delays. Officials characterized the attack as a retaliation against a failed Iranian hack in April targeting the command and control systems.

May 2020 — **German** officials found that a Russian hacking group associated with the FSB had compromised the networks of energy, water, and power companies in Germany by exploiting IT supply chains.

July 2020 — Israel announced that two cyber attacks had been carried out against Israeli water infrastructure, though neither were successful.

August 2020 — **New Zealand**'s stock exchange faced several days of disruptions after a severe distributed denial of service attack was launched by unknown actors.

September 2020 — An electric utility in **Pakistan** that services 2.5 million customers fell victim to a ransomware attack by unknown actors. The attack did not disrupt the power supply but prevented customers from accessing their accounts and demanded almost $4 million in Bitcoin as ransom.

September 2020 — **French** shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks, though did not affect the moving of cargo.

October 2020 — Iran announced that the country's Ports and Maritime Organization and one other unspecified government agency had come under cyberattack.

. . .

CSIS, Significant Cyber Incidents, https://www.csis.org/programs/strategic-technologies-program/significantcyber-incidents