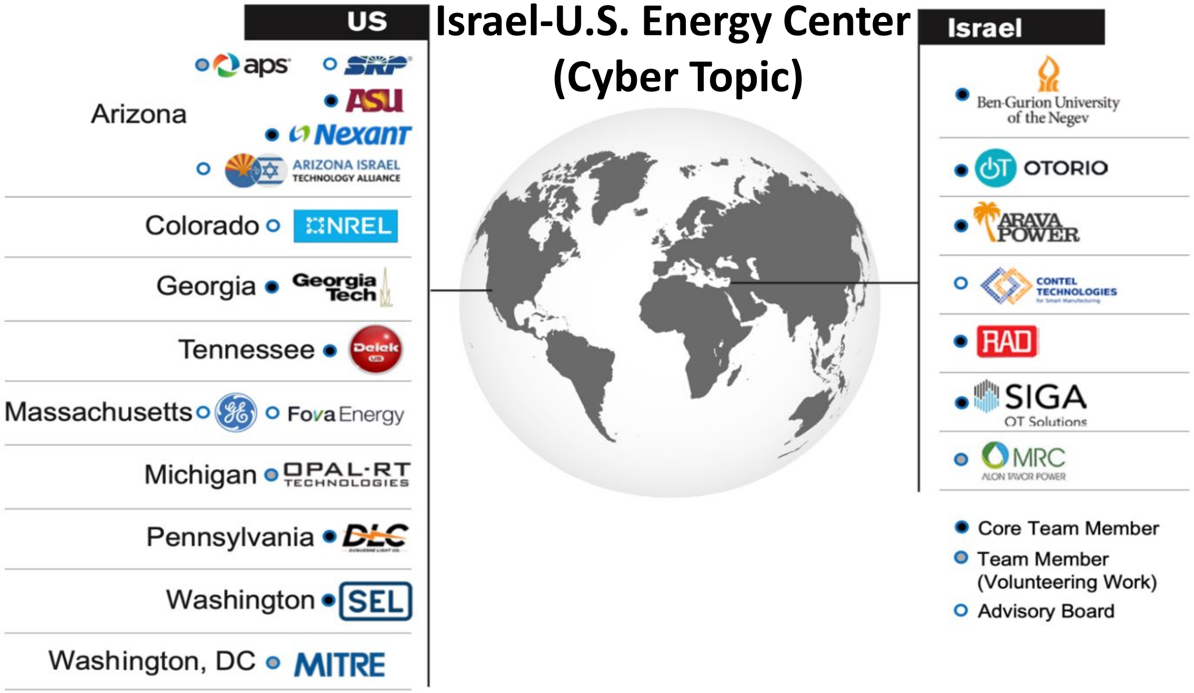
Progress on Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Summary of Task 9 and 18 Progress

Qiushi Cui, Yang Weng, Napoleon Enriquez, Corey Mai, Zhihao Ma

Prepared for

BIRD Foundation

Mar. 2023

Outlines

ARIZONA STATE UNIVERSITY

1. **False data injection review and our study**
2. **Other cyberattacks**
3. **Hardware-in-the-loop validation**

New Vulnerabilities on the Grid

Modern grid data-driven outlook → **New cyber-attack menaces**

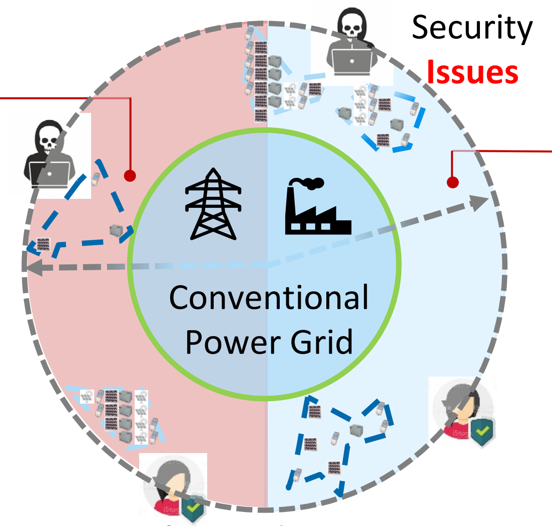
➢ New sensing devices

✓ Enhances situational awareness

✓ Enhances situational awareness

✗ New cyber-attack menaces

False Data Injection Attacks!



➢ New active devices

✓ High penetration of VRES

✓ Reducing carbon emissions

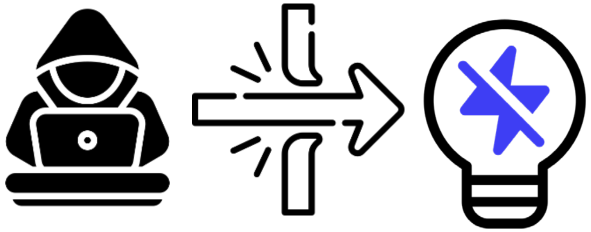
✗ Uncertainties for system operation

Vulnerable Power System

What is a FDIA?

False Data Injection Attacks:

- An attacker intercepts and maliciously changes the system measurements
- The objective is to cause harm in the real world
- For instance, a cyber-attack in a power system could cause a system operator to take wrong control actions causing a blackout.
- While these cyber-attacks can cause dire consequences, they are hard to be deployed practically due to unrealistic settings or assumptions.



False Data Injection Attacks

A successful FDIA requires:

1. Create a **corrupted** measurement vector, $\hat{\mathbf{z}} = \mathbf{z} + \mathbf{a}$ 

2. Pass the chi-squared test, $\mathrm{J}(\mathbf{x}) = \|\mathbf{z} - \mathbf{h}(\mathbf{x})\|^2 \geq \tau$ 

Problem: Power system model is not known, $\mathbf{h}(\cdot)$ → Access only to the observed measurements, $\mathbf{z}$

Alternative: Learn the underlying power system measurement distribution, $\hat{\mathbf{z}} \sim p_\theta(\hat{\mathbf{z}})$ 

Different FDIAs

- *Traditional* model-based attacks → **Require grid information**
  - ✘ Line parameters
  - ✘ Grid topology
  - ✘ State estimator model

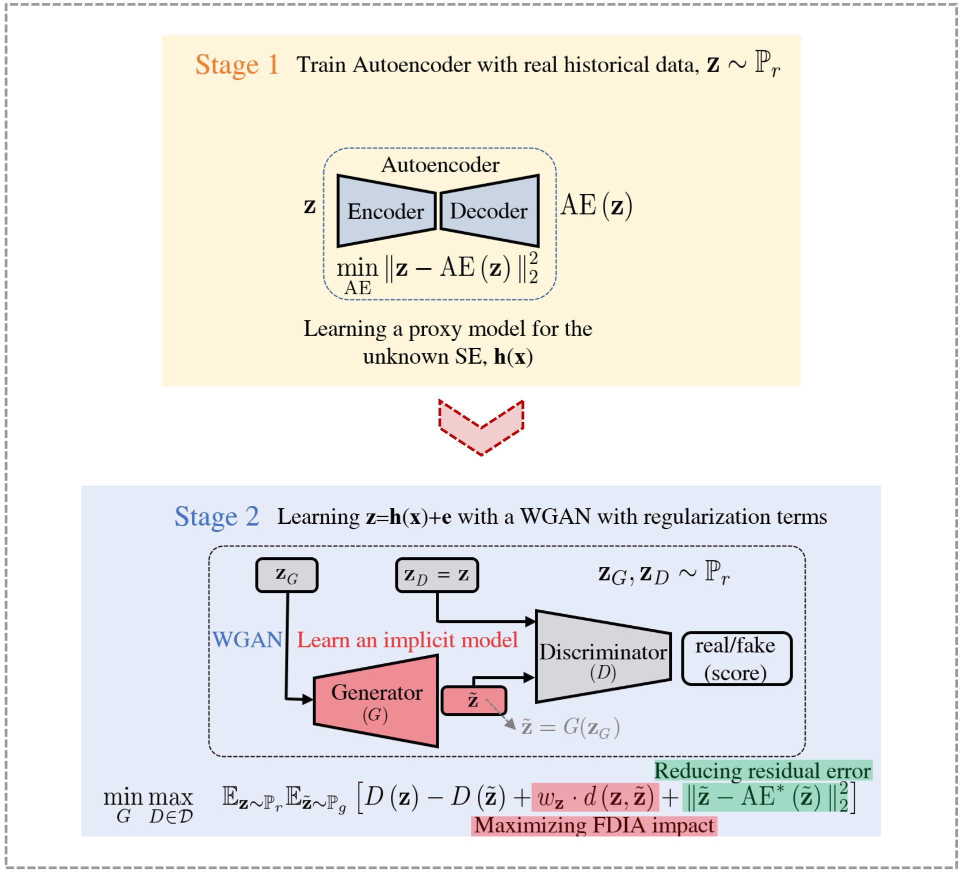
  } Carefully held!

Difficult to deploy an attack:

Lack of grid information + No performance guarantee

Proposed Framework:

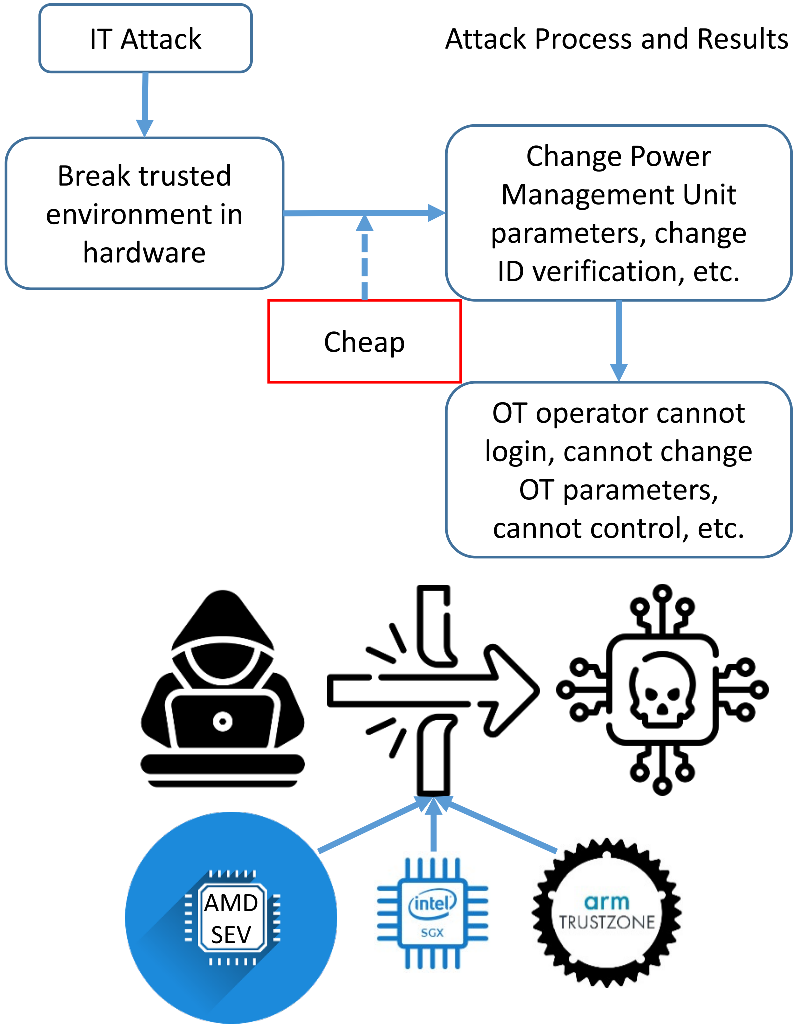
Learning the underlying power system model through data



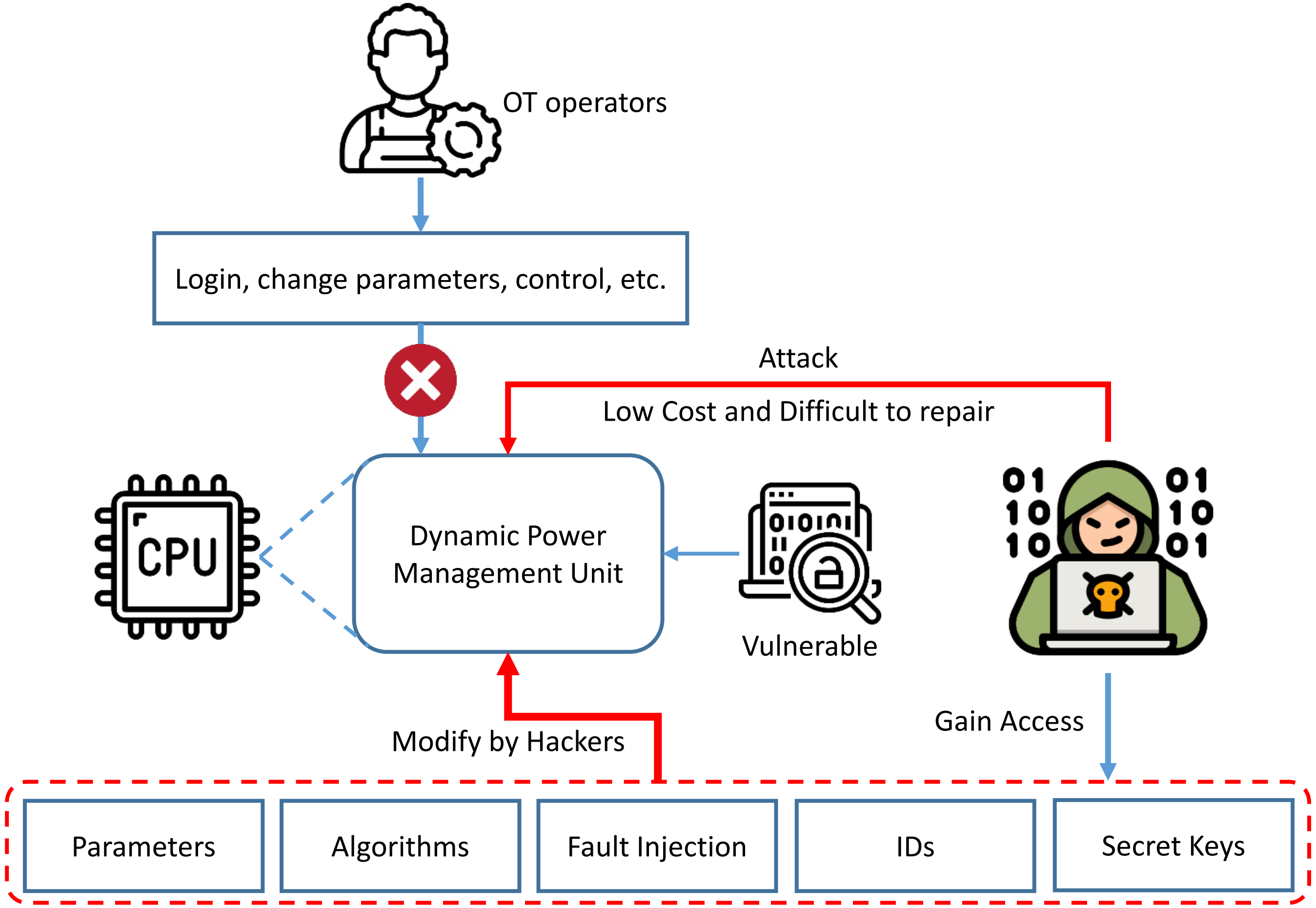
Outlines

1. False data injection review and our study
2. **Other cyberattacks**
3. Hardware-in-the-loop validation

Cyberattack on Hardware of Energy Internet



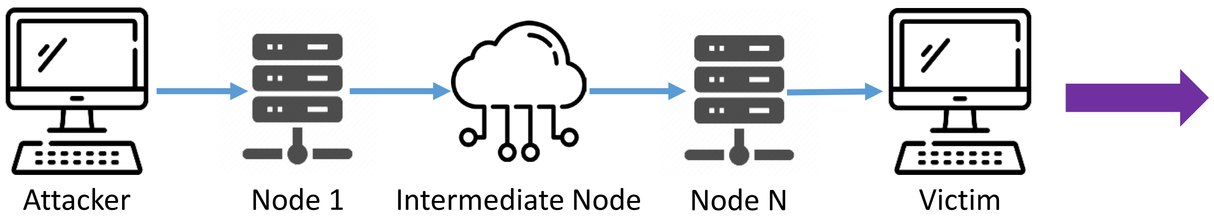
Trusted Execution Environments



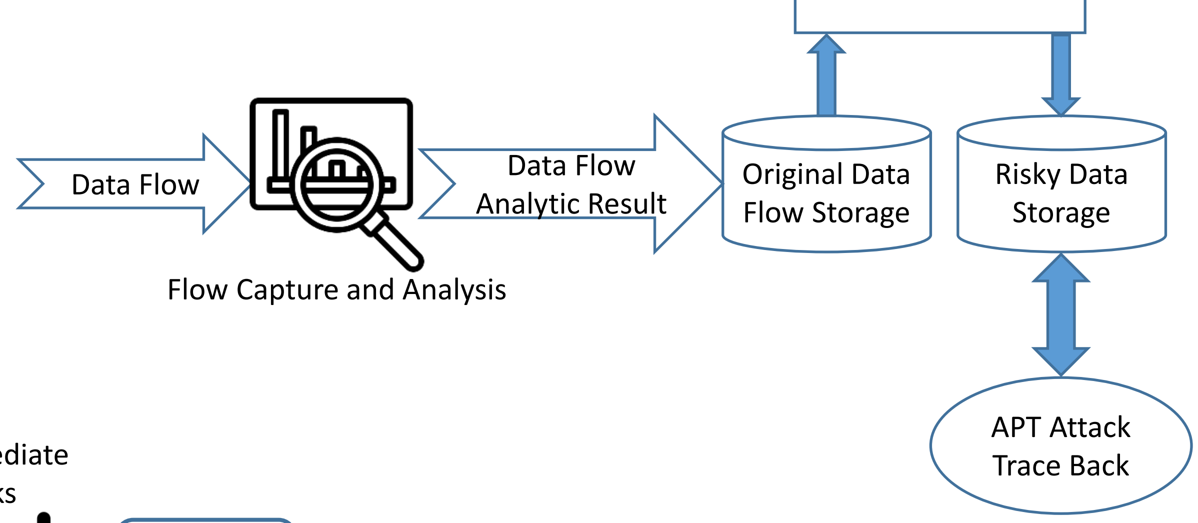
Cyber-Attack Recognition based on Data Flow to Avoid Traditional Advanced Persistent Threat

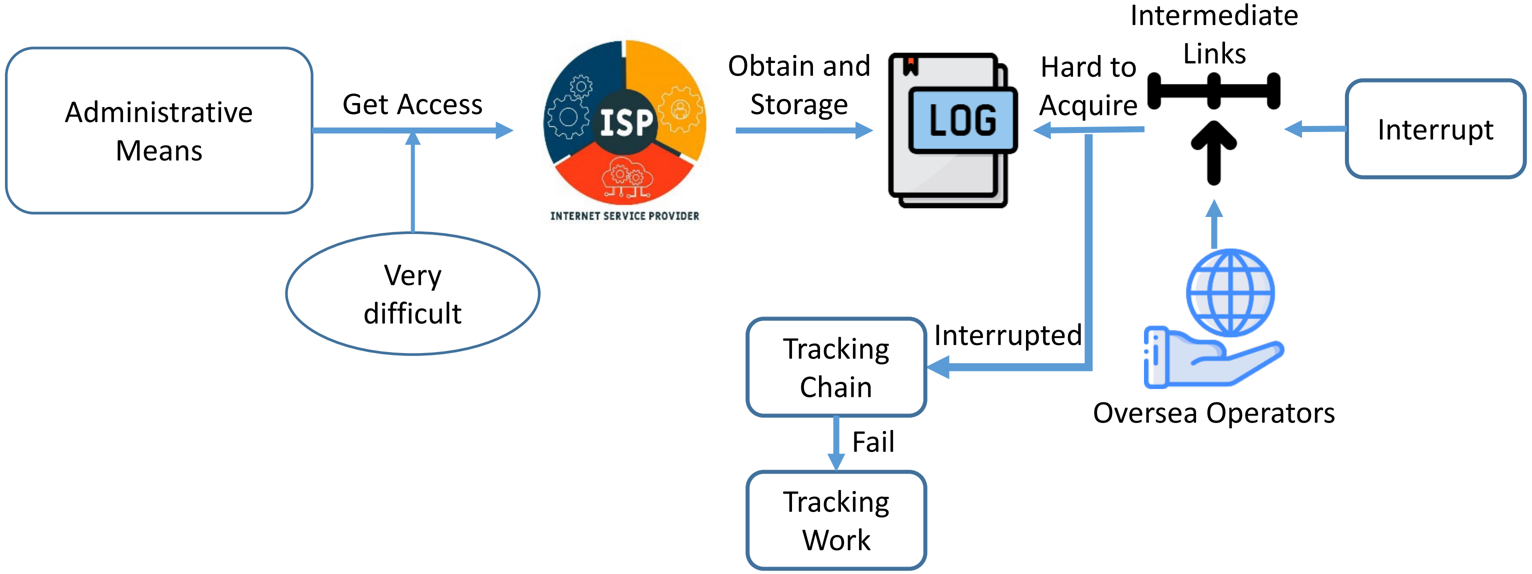
Arizona State University

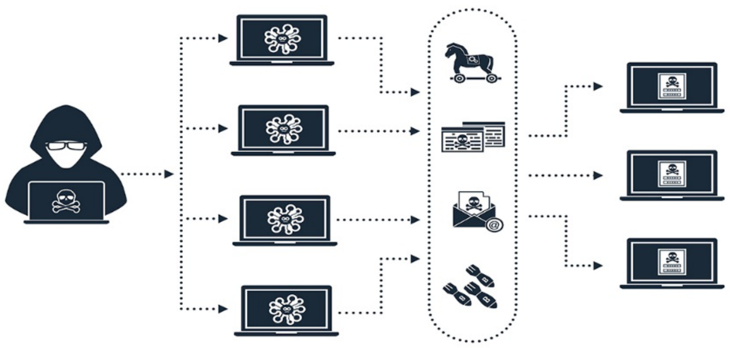
Cyber Attack Process Model



Traceability Method Framework Based on Network Flow Risk Data



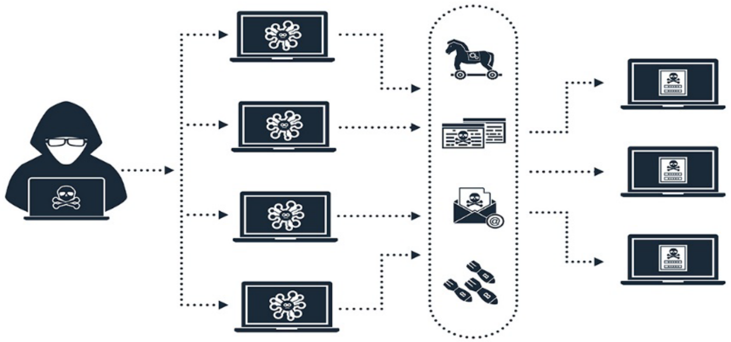




Botnet usage in cyber attack

Cyber-Attack Recognition based on Data Flow to Avoid Traditional Advanced Persistent Threat

ARIZONA STATE UNIVERSITY



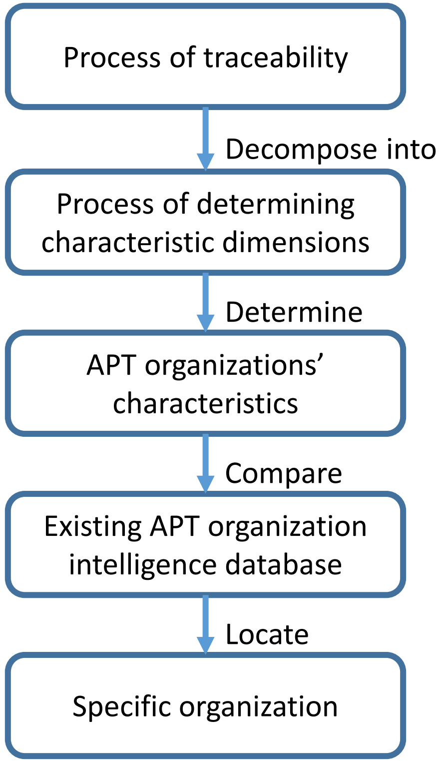
Botnet usage in cyber attack

Goal of APT attack source tracing:

- To locate the organization or individual who launched the attack

APT organizations characteristics:

- Associated with specific political entities.
- Can have different dimensions.
- Have relatively fixed attack targets:
  - Weapon arsenals.
  - Vulnerability libraries.
  - …



IT attacks on OT – An Example of DoS

Assumption 1 (DoS Frequency): For $t_1, t_2 \in \mathbb{R}_{\geq 0}, t_2 \geq t_1$, there exist $\eta \in \mathbb{R} \geq 0$ *and* $\tau_D \in \mathbb{R}_{\geq \underline{\Delta}}$ such that

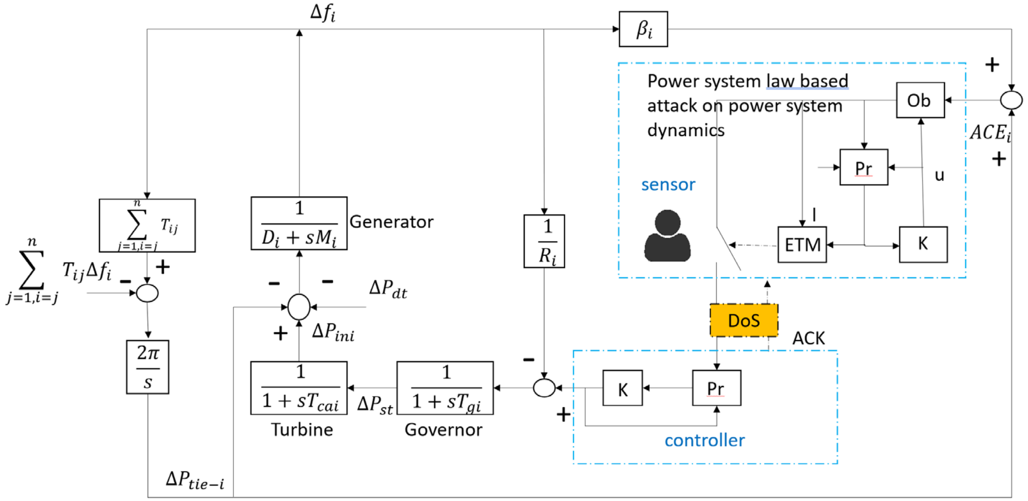
$$n(t_1, t_2) \leq \eta + \frac{t_2 - t_1}{\tau_D}$$

where η is the parameter and τ_D is the energy consumed by DoS conversion per unit time.

Assumption 2 (DoS Duration): For $t_1, t_2 \in \mathbb{R}_{\geq 0}, t_2 \geq t_1$, there exist $\varsigma \in \mathbb{R} \geq 0$ *and* $T \in \mathbb{R}_{\geq 1}$ such that

$$|\Xi(t_1, t_2)| \leq \varsigma + \frac{t_2 - t_1}{T}$$

where ς is the parameter and T is the energy consumed to maintain a DoS per unit time.

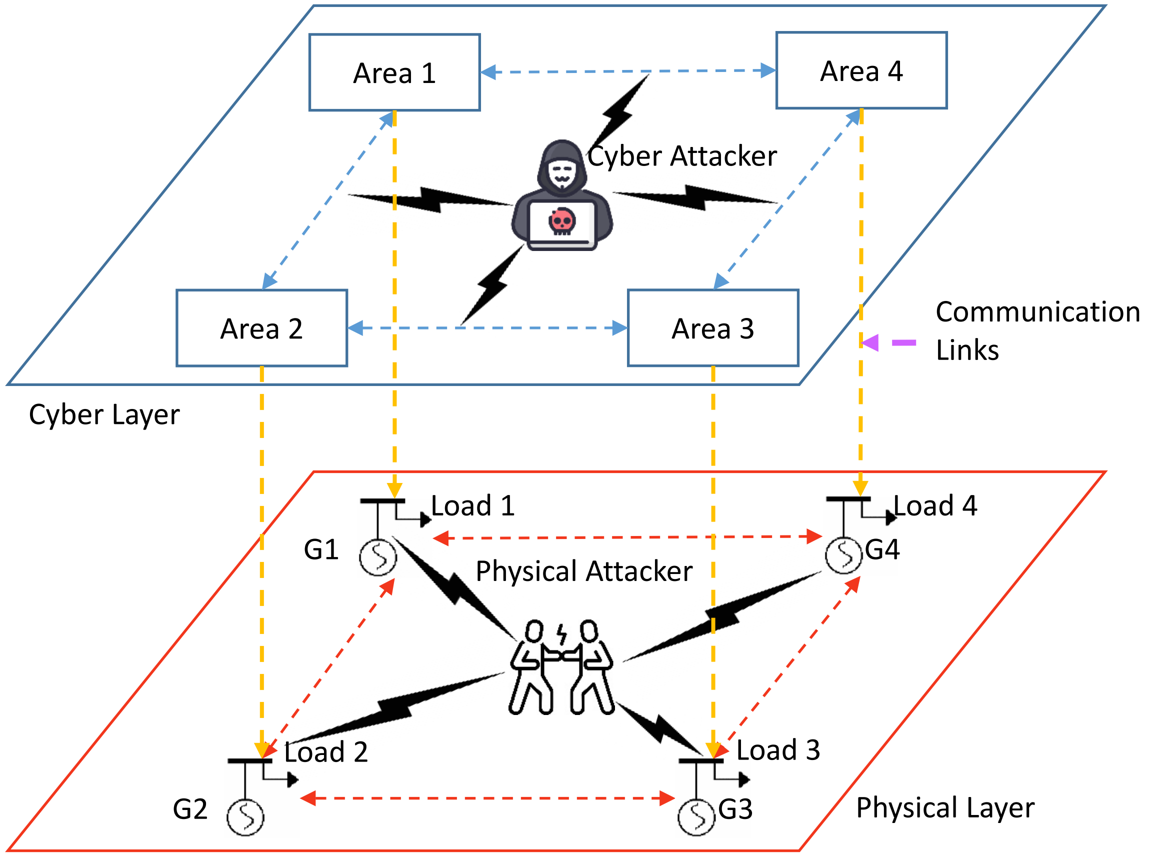


The ith load frequency control model

Cross-Layer Attacks: DoS and PMU Attacks

Cross-layer Attacks:

- Data transfer fail
- PMUs collect wrong data
- Control center makes wrong decisions

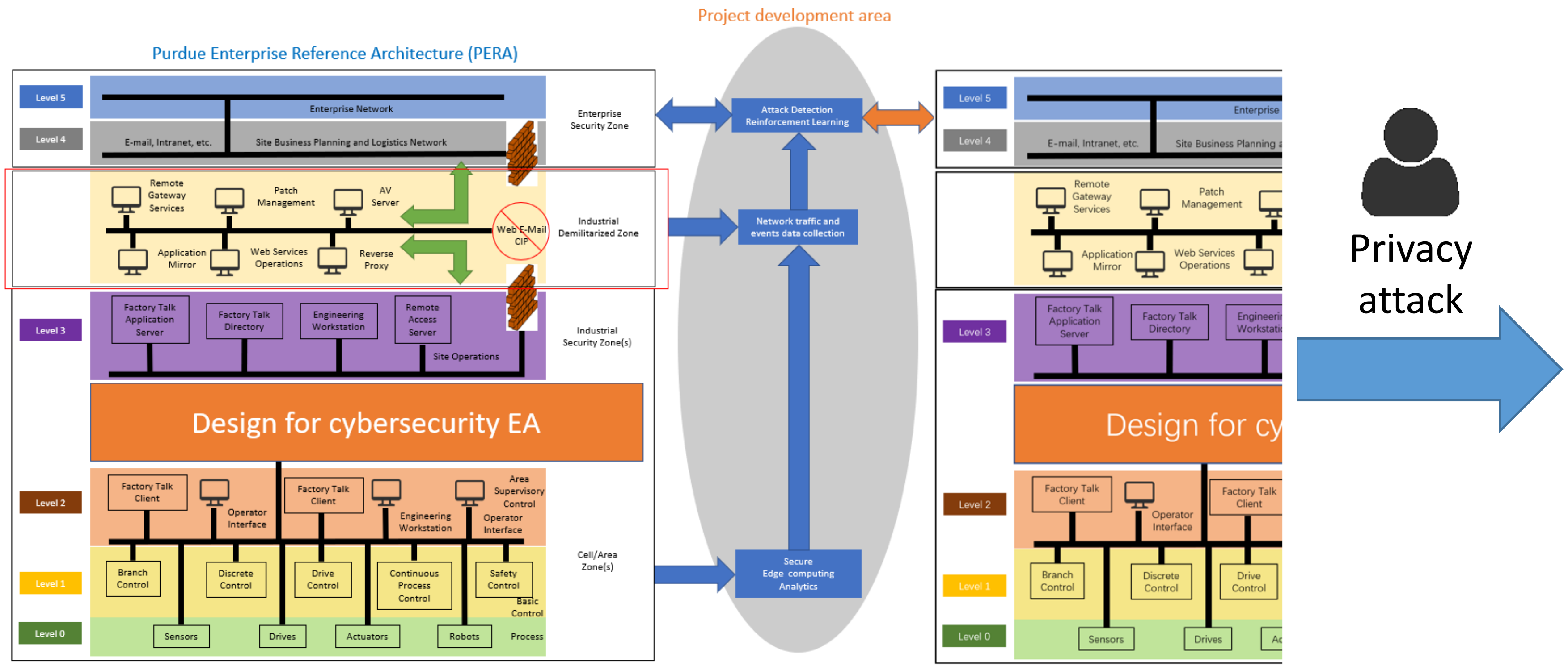


DoS attack in active distribution power system:

- False load shedding amount
- System frequency performance decrease

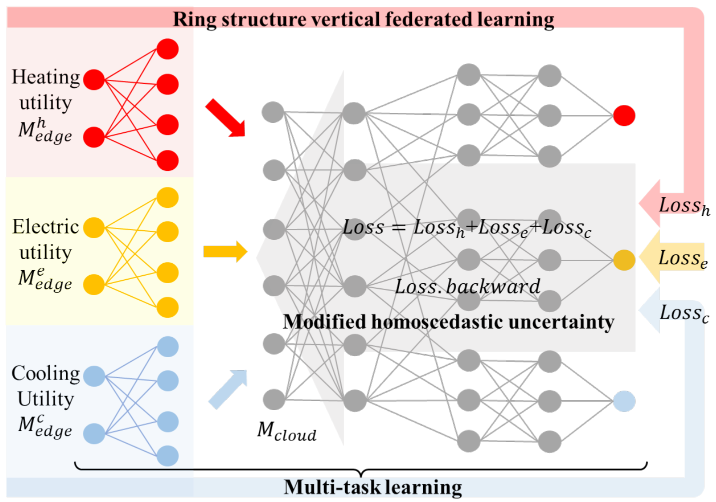
Security OT via Cyber Aware Energy Management Systems

Cyberattacks Detection of IT/OT Architecture—affect privacy of head, electric and cooling customer privacy—>national security



OT-Entity 1

OT-Entity 2



Outlines

1. False data injection review and our study
2. Other cyberattacks
3. **Hardware-in-the-loop validation**

Model-Free FDIA with a WGAN

Deploying a stealthy FDIA

- **Bad data detector**: Chi-square error test

$$\hat{\mathbf{x}} = \arg\min_{x} (\mathbf{z} - \mathbf{h}(\mathbf{x}))^{\mathrm{T}} \mathbf{W}^{-1} (\mathbf{z} - \mathbf{h}(\mathbf{x}))$$ State estimator

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^{m} (z_i - h(\hat{x}_i))^2 / \sigma_i^2$$ Chi-square test

- **Tampering measurements**: Dire consequences in the grid

Challenges:

- Pass the Chi-square test?
- Guarantee Convergence?
- Attack impact?

Proposed Solution:

- **Learn** a proxy SE model

Residual error test: $\mathbf{r} = \|\mathbf{z} - \hat{\mathbf{z}}\|_2^2$ → Proxy model: $\|\tilde{\mathbf{z}} - \mathrm{AE}^*(\tilde{\mathbf{z}})\|_2^2$

- **Learn** the sensor measurement distribution → Training a WGAN

$$\min_{G} \max_{D \in \mathcal{D}} \mathbb{E}_{\mathbf{z}_G, \mathbf{z}_D \sim \mathbb{P}_r} \mathbb{E}_{\tilde{\mathbf{z}} \sim \mathbb{P}_g} [D(\mathbf{z}_D) - D(\tilde{\mathbf{z}})]$$ WGAN conditioned on measurements

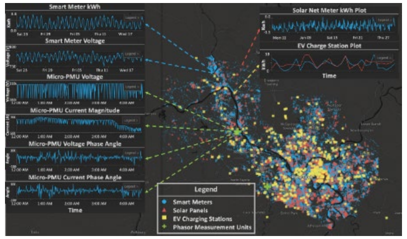
No grid information ✓

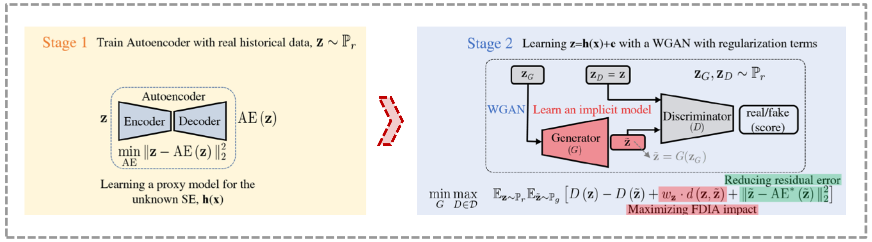
- **Embed** the proxy model into the WGAN

$$\min_{G} \max_{D \in \mathcal{D}} \mathbb{E}_{\mathbf{z}_G, \mathbf{z}_D \sim \mathbb{P}_r} \mathbb{E}_{\tilde{\mathbf{z}} \sim \mathbb{P}_g} [D(\mathbf{z}_D) - D(\tilde{\mathbf{z}}) + \|\tilde{\mathbf{z}} - \mathrm{AE}^*(\tilde{\mathbf{z}})\|_2^2 + w_z \cdot d(\mathbf{z}_G, \tilde{\mathbf{z}})]$$

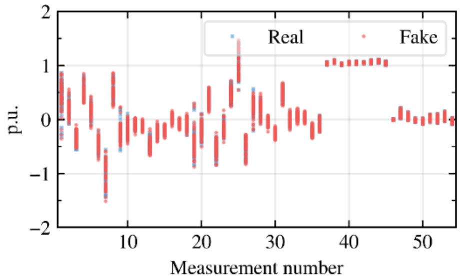
Numerical Results

Wealth of data from new sensing devices — Learning the underlying power system model through data — FDIA successfully deployed

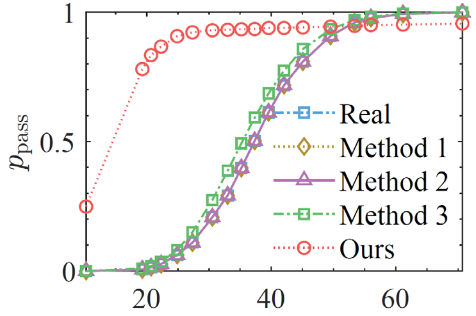




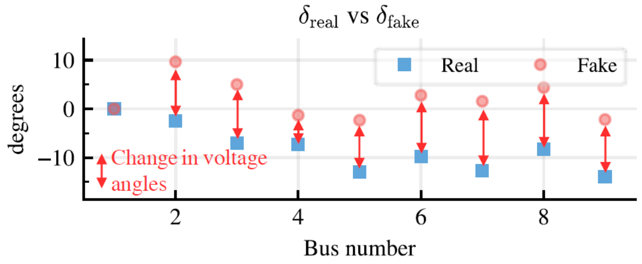
✓ Learned measurement distribution



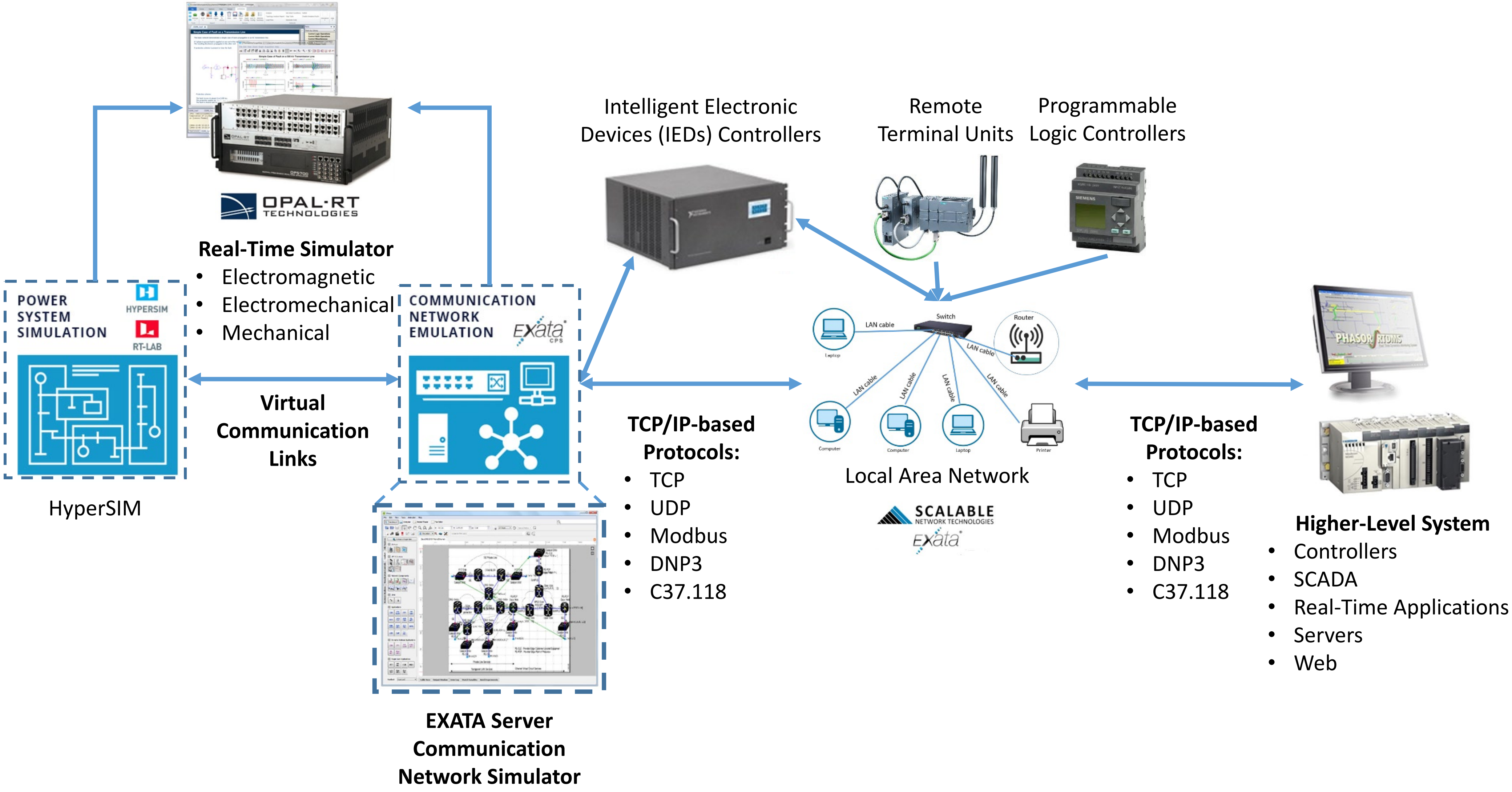
✓ Pass the Chi-square test



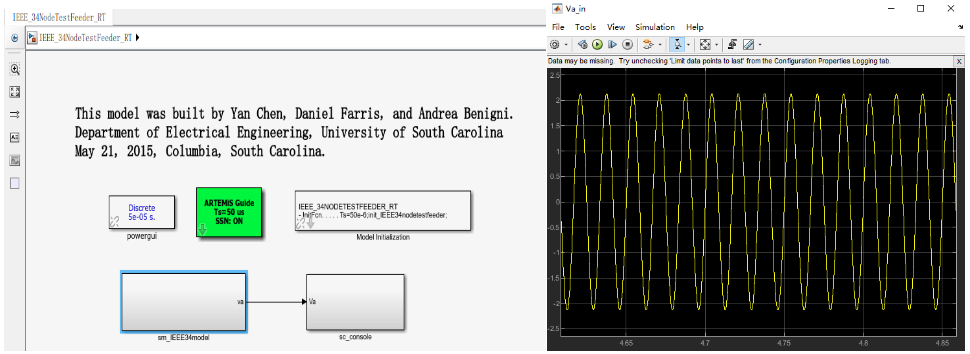
✓ It stealthy changes the underlying power system states



Cybersecurity Solution with HyperSIM and EXATA

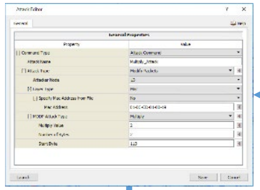


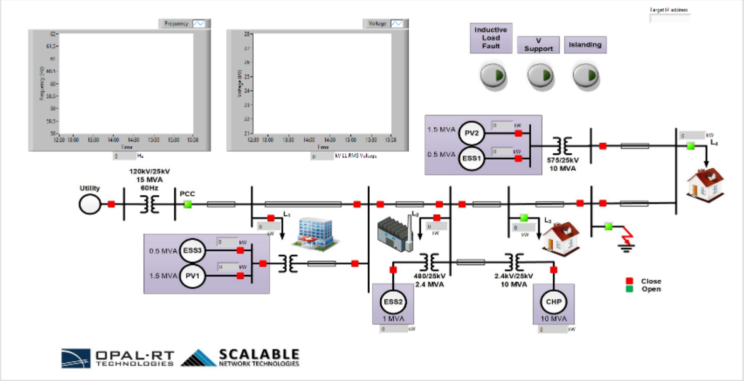
Cybersecurity Solution with HyperSIM and EXATA



EXATA Server Communication Network Simulator

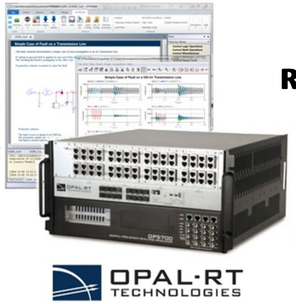
Attack Editor

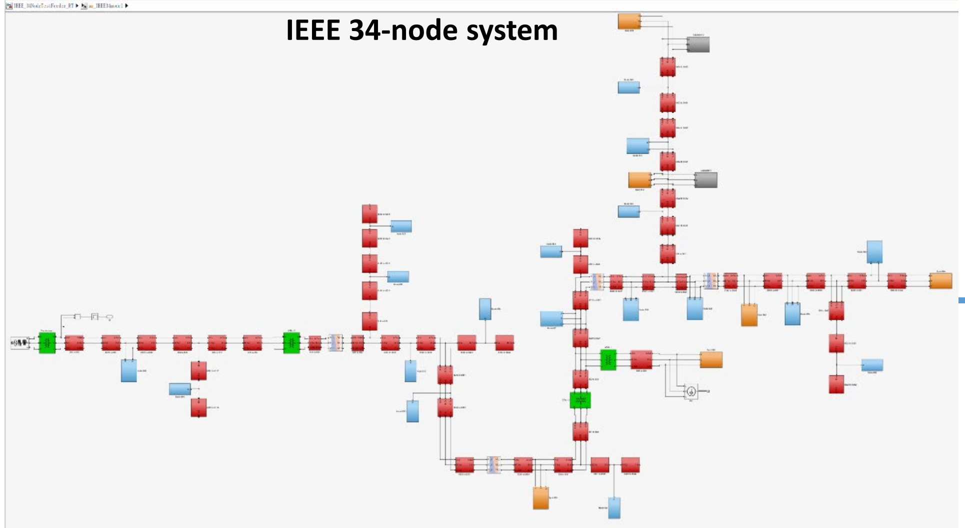




LabView

Real-Time Simulator





HyperSIM Simulator