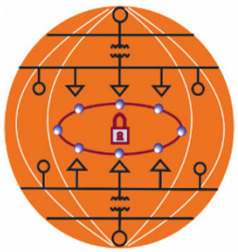



VIRGINIA TECH™

*Seminar at MPR, March 16, 2023*

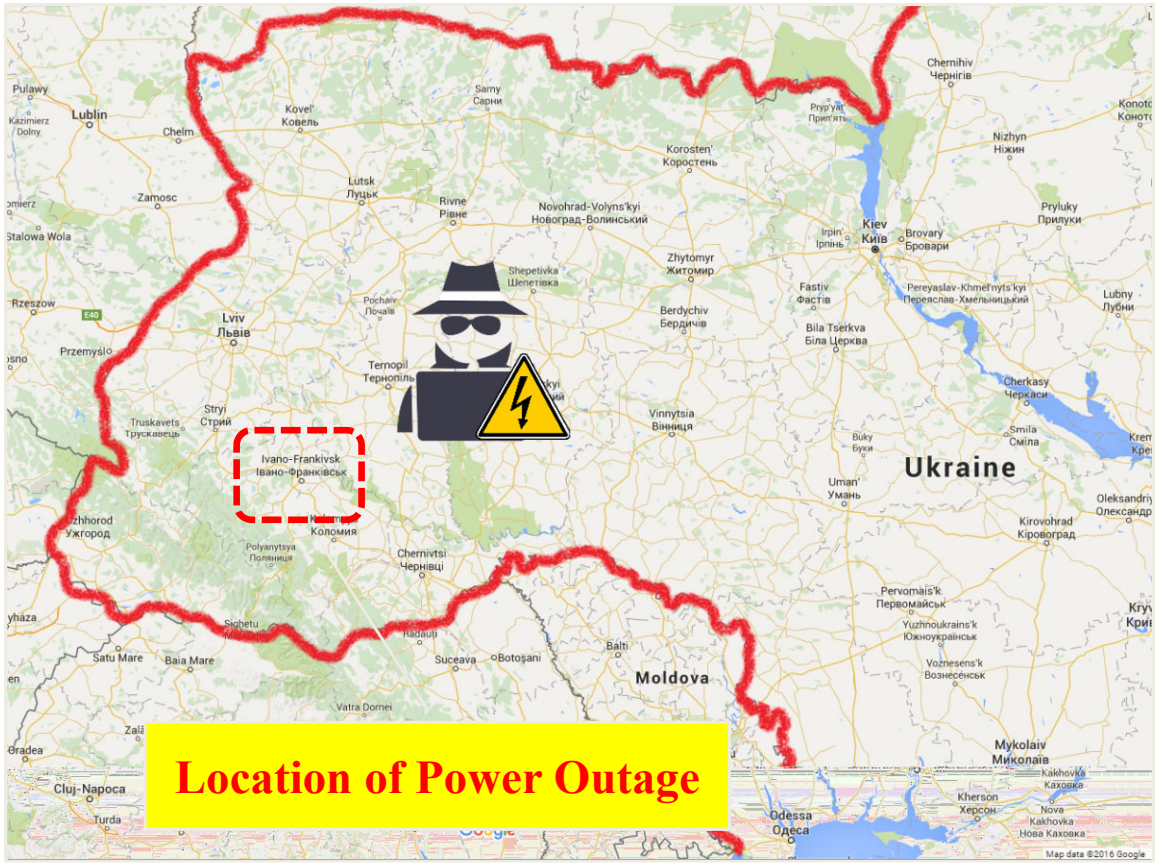
# *Cyber Security of SCADA, Substations, and Distribution Systems*

**Chen-Ching Liu**
**American Electric Power Professor**
**Director, Power and Energy Center**
**Virginia Tech**

Sponsored by U.S. National Science Foundation,
Department of Energy, Commonwealth Cyber Initiative (CCI), VA

# Cyber Attack in Ukraine's Power System

- **Attack on Ukraine's power grid**
  - ❑ December 23, 2015.
  - ❑ Malware installation.
  - ❑ Falsify SCADA data injection.
  - ❑ Flood attack on telephone system.
  - ❑ Trip circuit breakers in multiple substations.
- **Results**
  - ❑ Over 225,000 customers experienced power outage.

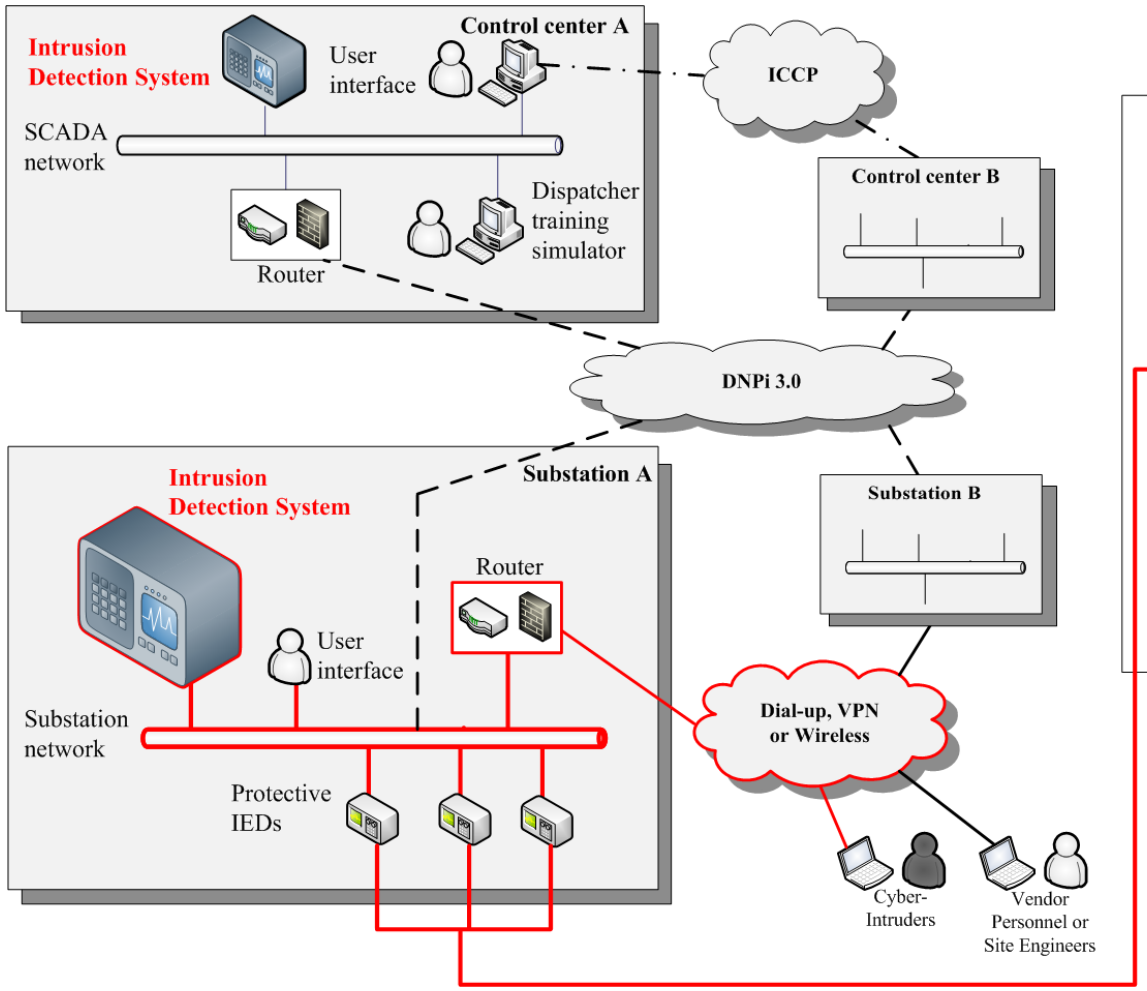


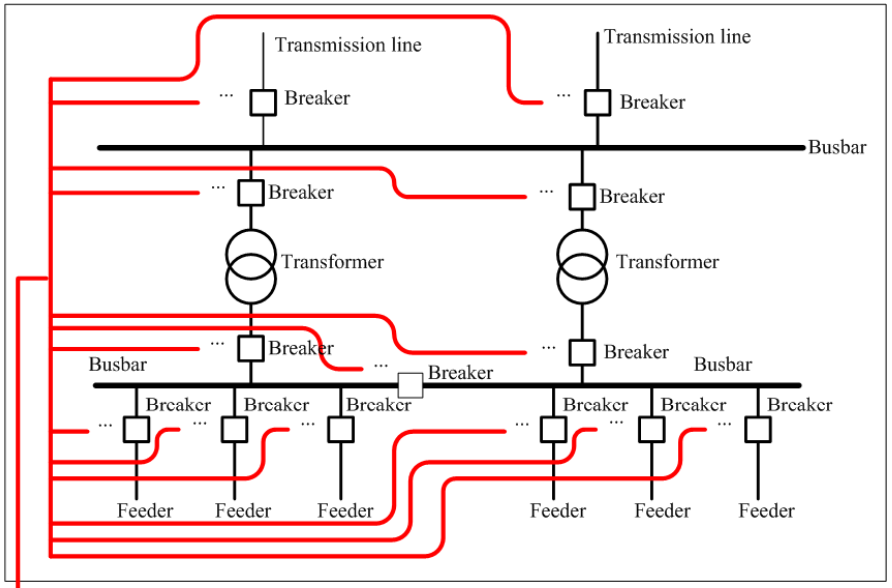

Source: Google map

# Escalating Cyber Security Factors

- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Constraints on use of existing security technologies and practices
- Insecure remote connections
- Widespread availability of technical information about control systems

# Cyber Systems in Power Infrastructure



# Cyber Security Standard for Supervisory Control and Data Acquisition (SCADA) NERC CIP 002-014

- 002 Critical asset identification (e.g. RTU, which support the reliable operation of a power system.)
- 003 Security management controls (e.g. How to manage the authentication, card or password, or both.)
- 004 Personnel training (e.g. Contrators and vendor must be authorized to gain access (cyber and physical), and training staff on security awareness.)
- 005 Electronic security perimeter (e.g. Periphery to protect all the cyber asset within.)
- 006 Physical security of critical cyber assets (e.g. Control policies on people who are authorized to have access to the critical cyber assets.)
- 007 System security management (e.g. Monitoring system events)
- 008 Incident reporting and response planning (e.g. Report to related authorities if necessary)
- 009 Recovery plans for critical cyber assets (e.g. When threat is over, recover the system and enhance the control policies)
- 010 Configuration change management and vulnerability assessments
- 011 Information protection
- 012 Communications between control centers
- 013 Supply chain risk management
- 014 Physical security

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection

# System Vulnerability

- A system is defined as the wide area interconnected, IP-based computer communication networks linking the control center and substations-level networks
- System vulnerability is the maximum vulnerability level over a set of scenarios represented by I

$$V_S = \max\left(V(I)\right)$$

* C. W. Ten, C. C. Liu, M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Trans. Power Systems*, Nov. 2008, pp. 1836-1846.

# Access Point Vulnerability

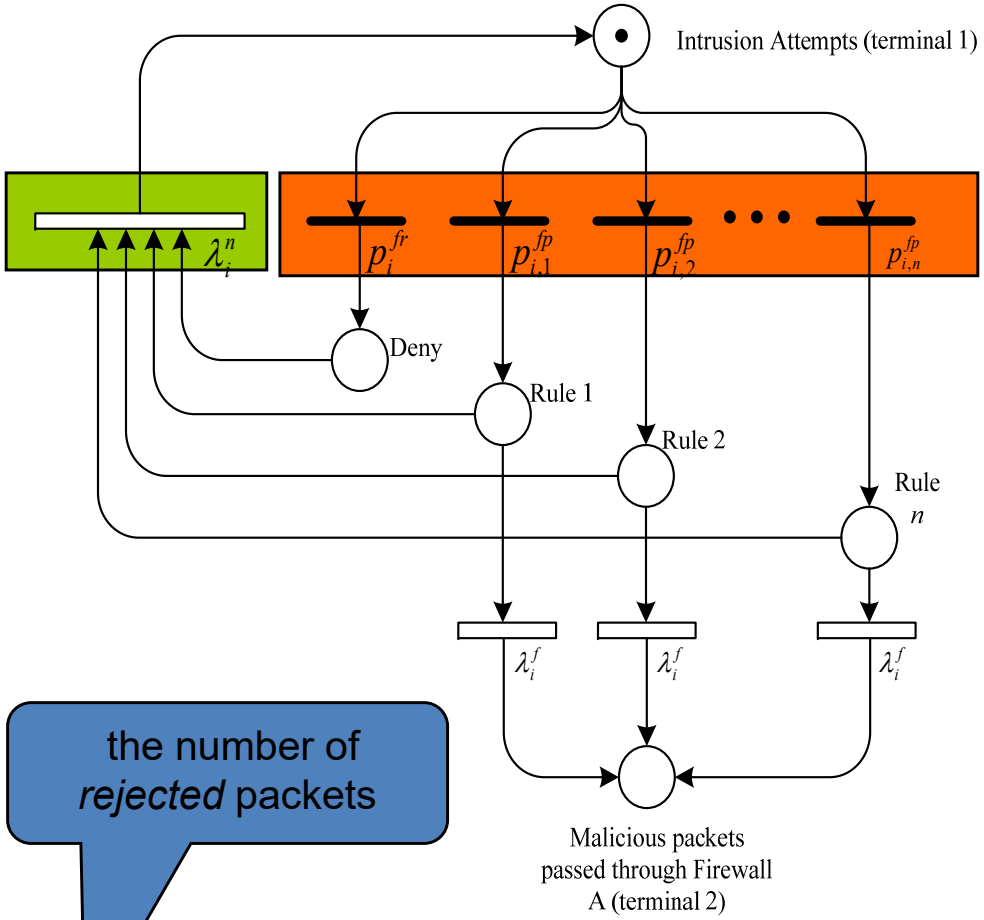
- Access point provides the port services to establish a connection for an intruder to penetrate SCADA computer systems
- Vulnerability of a scenario i, V(i), through an access point is evaluated to determine its potential damage
- Scenario vulnerability - weighted sum of the potential damages over the set S

$$V(i) = \sum_{j \in S} \pi_j \times \gamma_j$$

where $\pi_j$ is the steady state probability that a SCADA system is attacked through a specific access point *j*, which is linked to the SCADA system. The damage factor, $\gamma_j$, represents the level of damage on a power system when a substation is removed

# Firewall Model

- Firewall model
  - Denial or access of each rule
  - Malicious packets traveling through policy rule j on each firewall i is taken into account.




probability of malicious packets traveling through a firewall rule

denotes the frequency of malicious packets through the firewall rule

$$p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}$$

total record of firewall rule *j*.

the number of *rejected* packets

probability of the packets being *rejected*

$$p_i^{fr} = \frac{f_i^{fr}}{N_i^{fr}}$$

denotes the total number of packets in the firewall logs

# Modeling Integrated Cyber-Power System

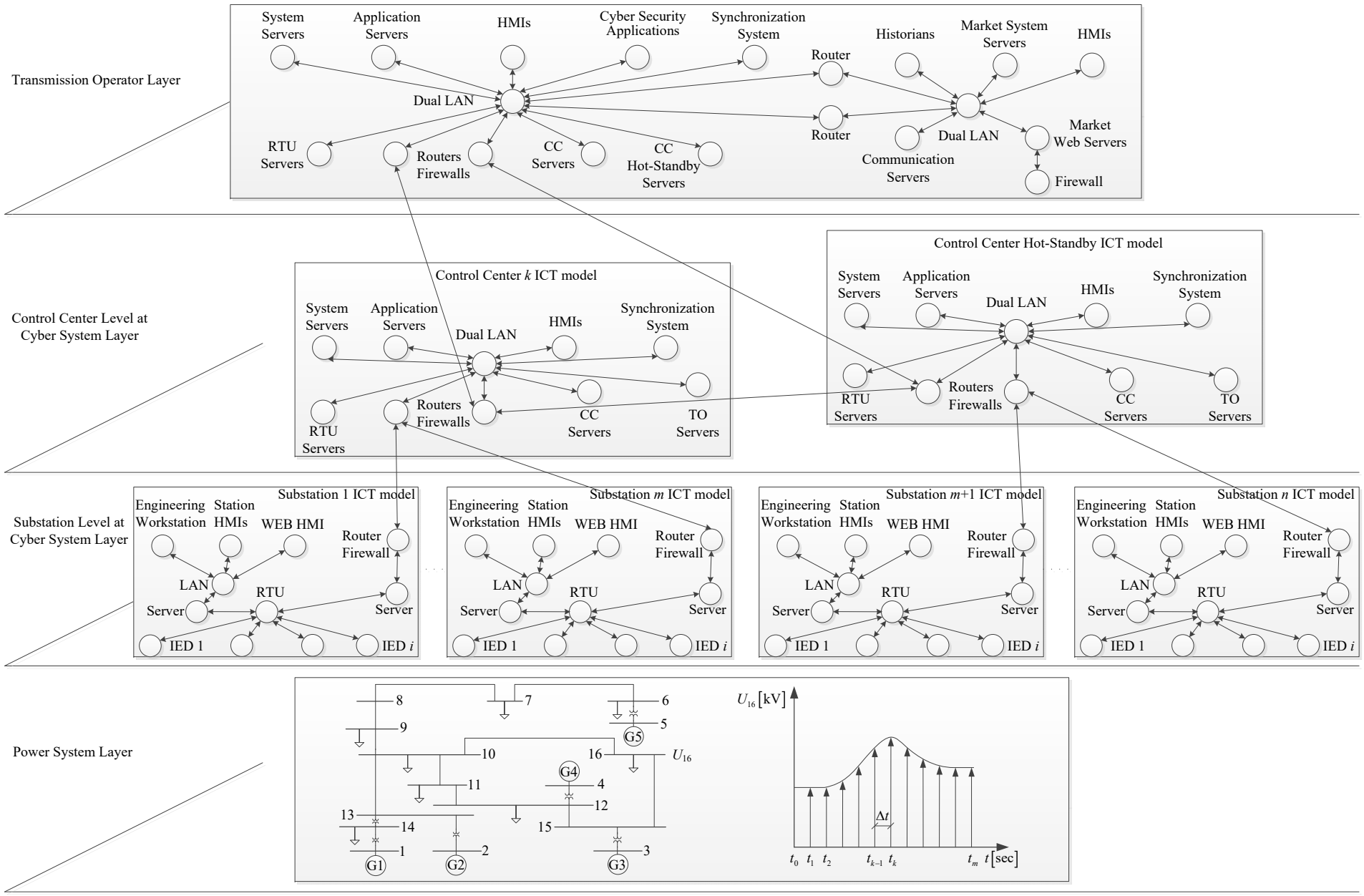
- **Methodology for CPS modeling of power systems**
  - Develop the ICT model of SCADA system
  - Integrate power grid model with ICT model for SCADA and grid control hierarchy
  - Dynamics of a power grid and its data infrastructure are combined

- **CPS tool used for assessment of SCADA communication performance**
  - Plan SCADA and ICT systems for power grids

- **CPS tool used for cyber security assessment in co-simulation environment**
  - Model cyber attacks and assess CPS security
    - Simulate cyber attacks at the cyber system layer
    - Perform impact analysis at the power system layer
    - Compute impact indices and attack efficiencies to disrupt power grid operation

* A. Stefanov, C. C. Liu, M. Govindarasu, "Modeling and Vulnerability Assessment of Integrated Cyber-Power Systems," *Int. Transactions on Electrical Energy Systems*, Vol. 25, No. 3, March 2015, pp. 498-519.

# Integrated Cyber-Power System Model



# Impact on Power System - Dynamics

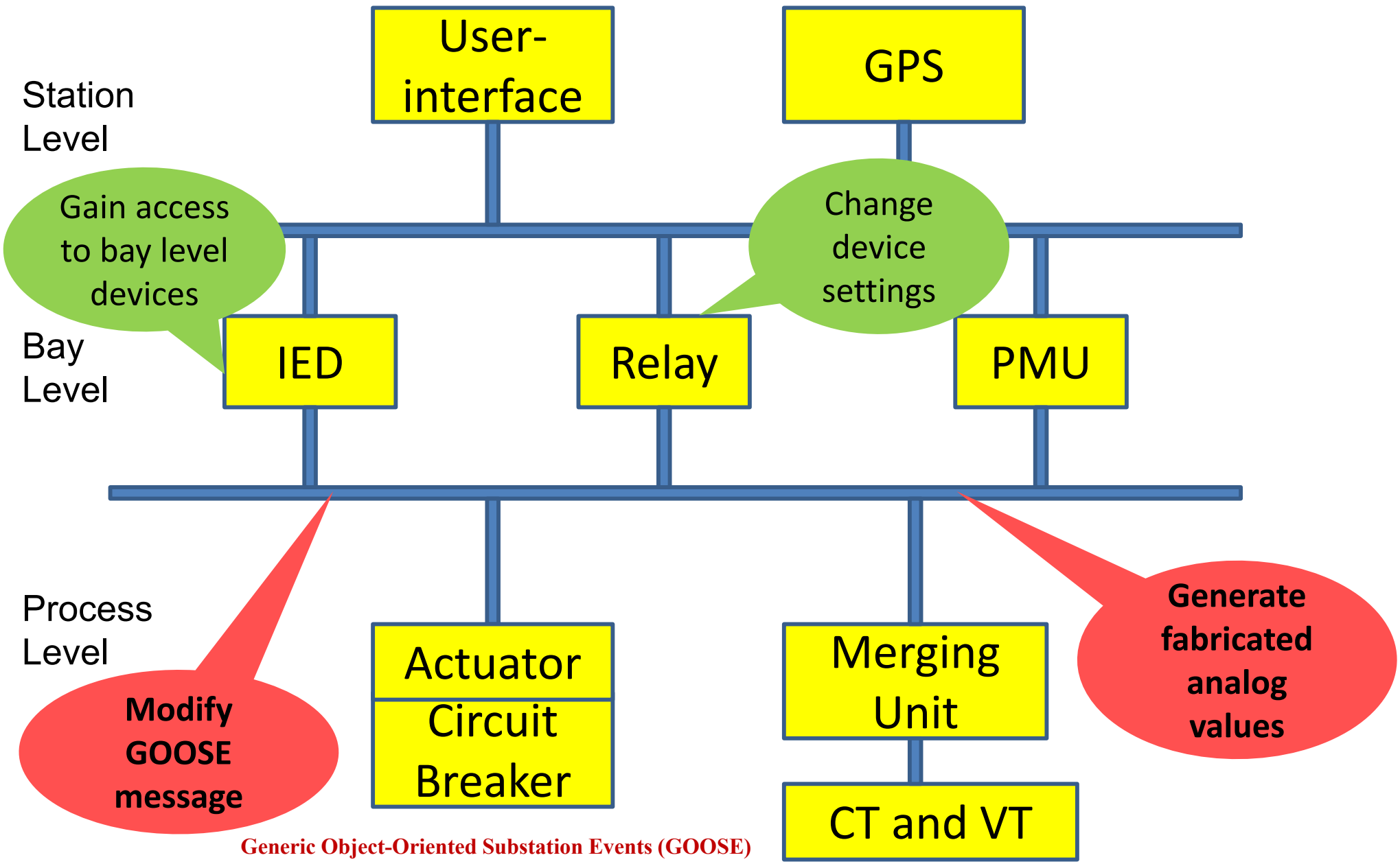
- **Cyber-Physical Security Assessment**

- Impact of the cyber attack is assessed by monitoring the dynamic behavior:
  - frequency
  - bus voltage magnitudes
  - current levels on network elements
  - loss of loads

$$\beta_j = \beta_{f,j} + \beta_{P_{L,j}} + \beta_{U,j} + \beta_{L,j}$$
$$= \gamma_f \frac{|\Delta f|}{\Delta f_{rated}} + \gamma_P \sum_{i=1}^{n_{Loads}} \frac{\Delta P_{L,i}}{P_{initial,i}} + \gamma_U \sum_{i=1}^{n_{bus}} \frac{|\Delta U_i|}{\Delta U_{rated}} + \gamma_I \sum_{i=1}^{n_{branch}} \frac{I_i}{I_{rated,i}}$$

- It shows how much the operation has moved from the secure condition:
  - Secure state
  - Insecure state
  - Emergency state
- The most critical attack path is identified based on the attack's efficiency

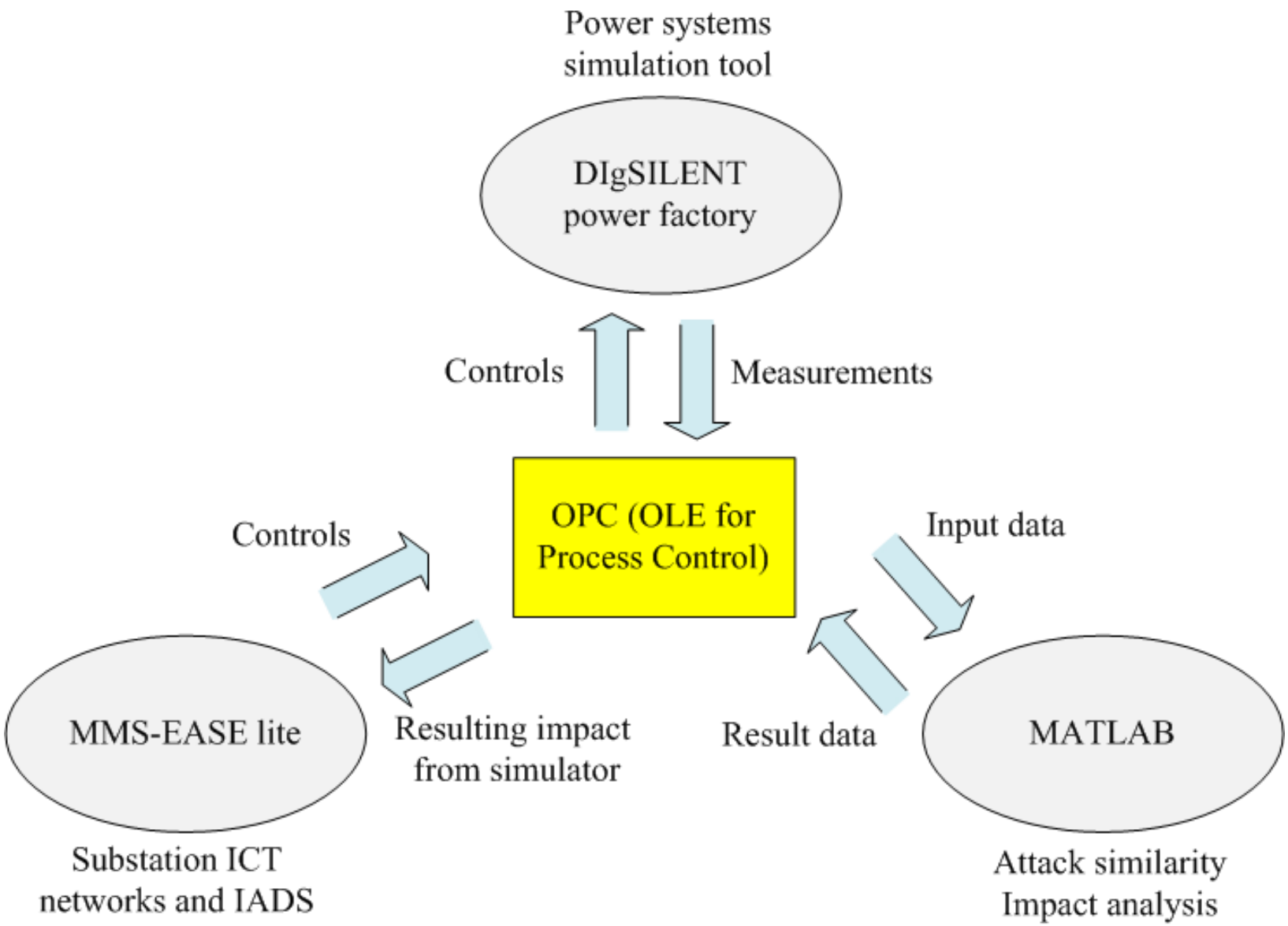
# Potential Threats in a Substation Based on IEC 61850



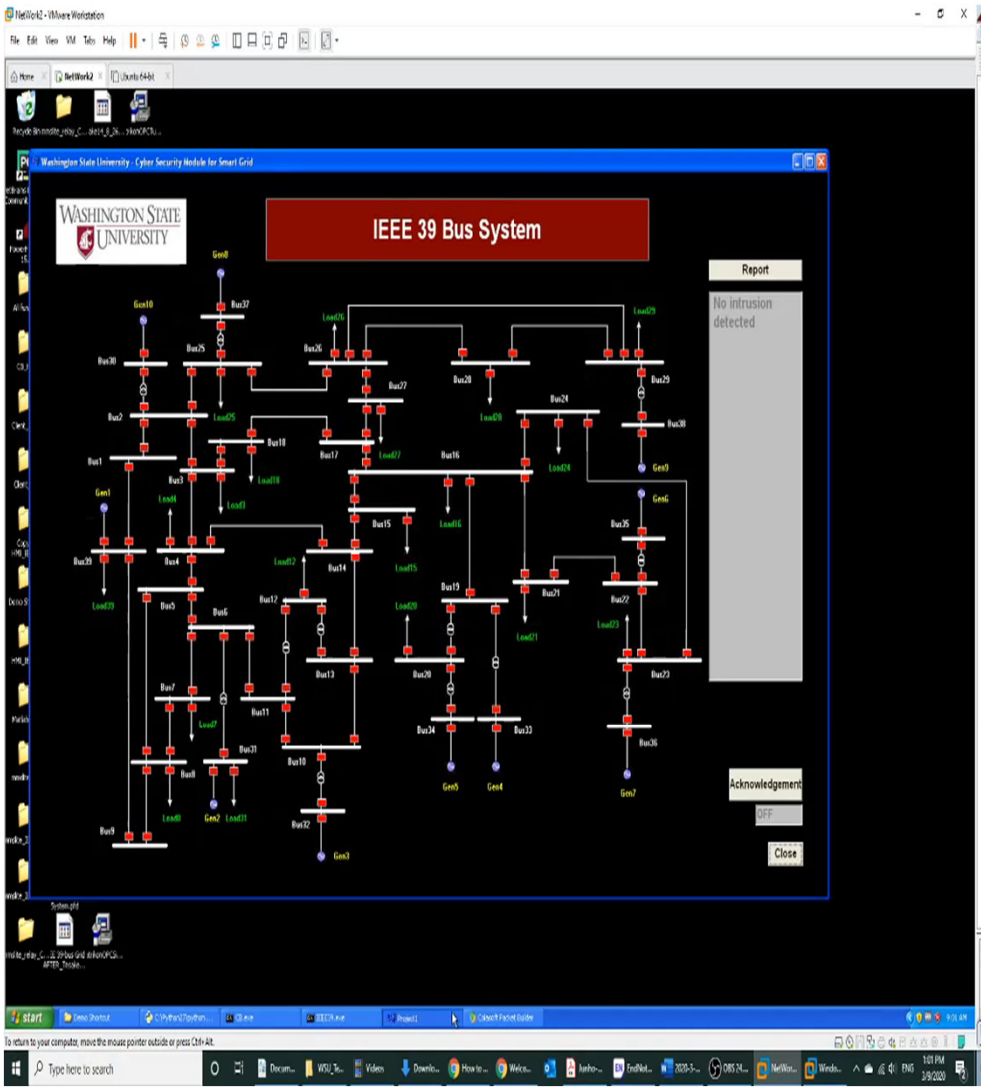
# Generic Object-Oriented Substation Events (GOOSE) Based Attack

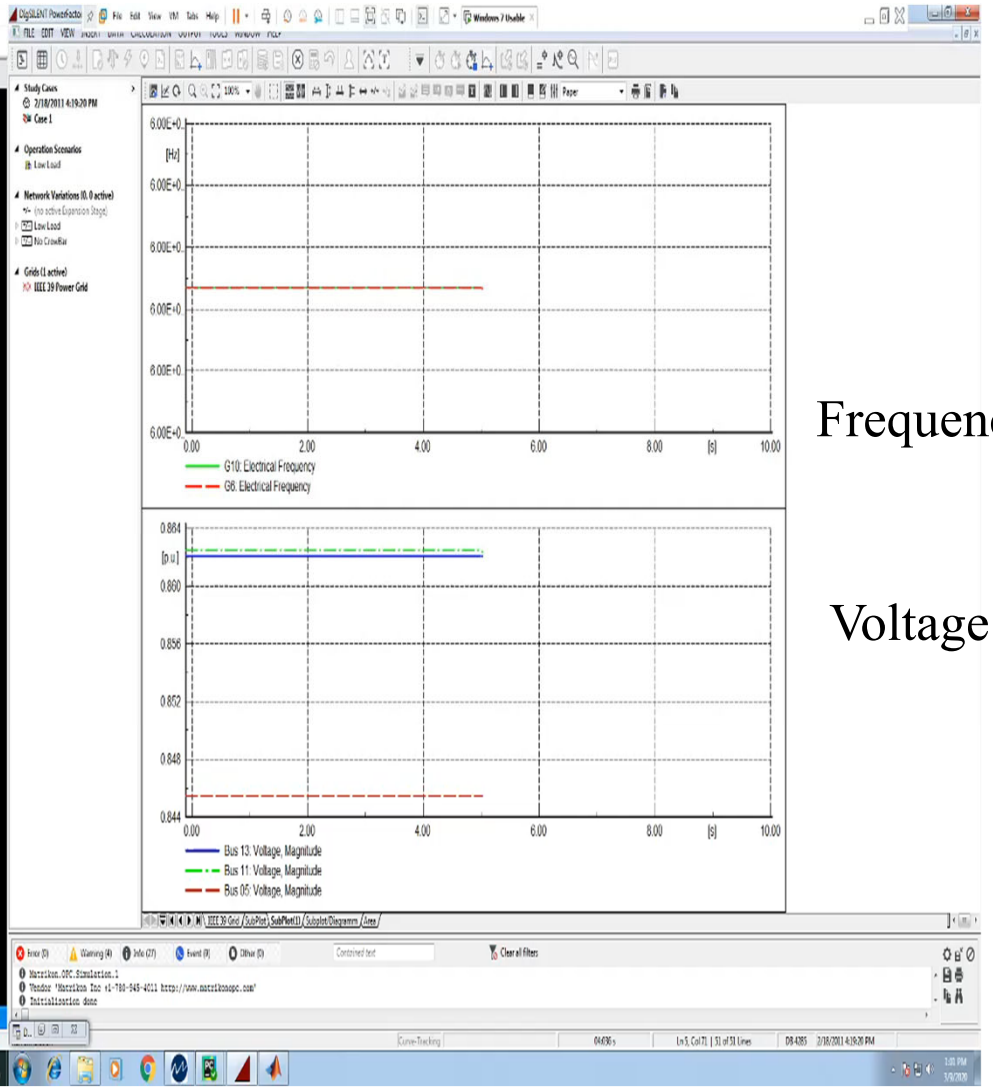
| Action | Result |
|---|---|
| Disconnect Ethernet cable from IED | Lost availability of IED |
| Send normal control | Open CB |
| Replay attack | Open CB |
| Modify sequence & state number | Warning occurred at CB |
| Modify transferred time | Warning occurred at CB |
| Modify GOOSE control data | Open CB |
| Denial of Service attack | Lost availability of CB |
| Generate GOOSE control data | Open CB |

# Integration of Cyber-Power System Tools



# Vulnerabilities: Cyber Attacks on SCADA/Substations

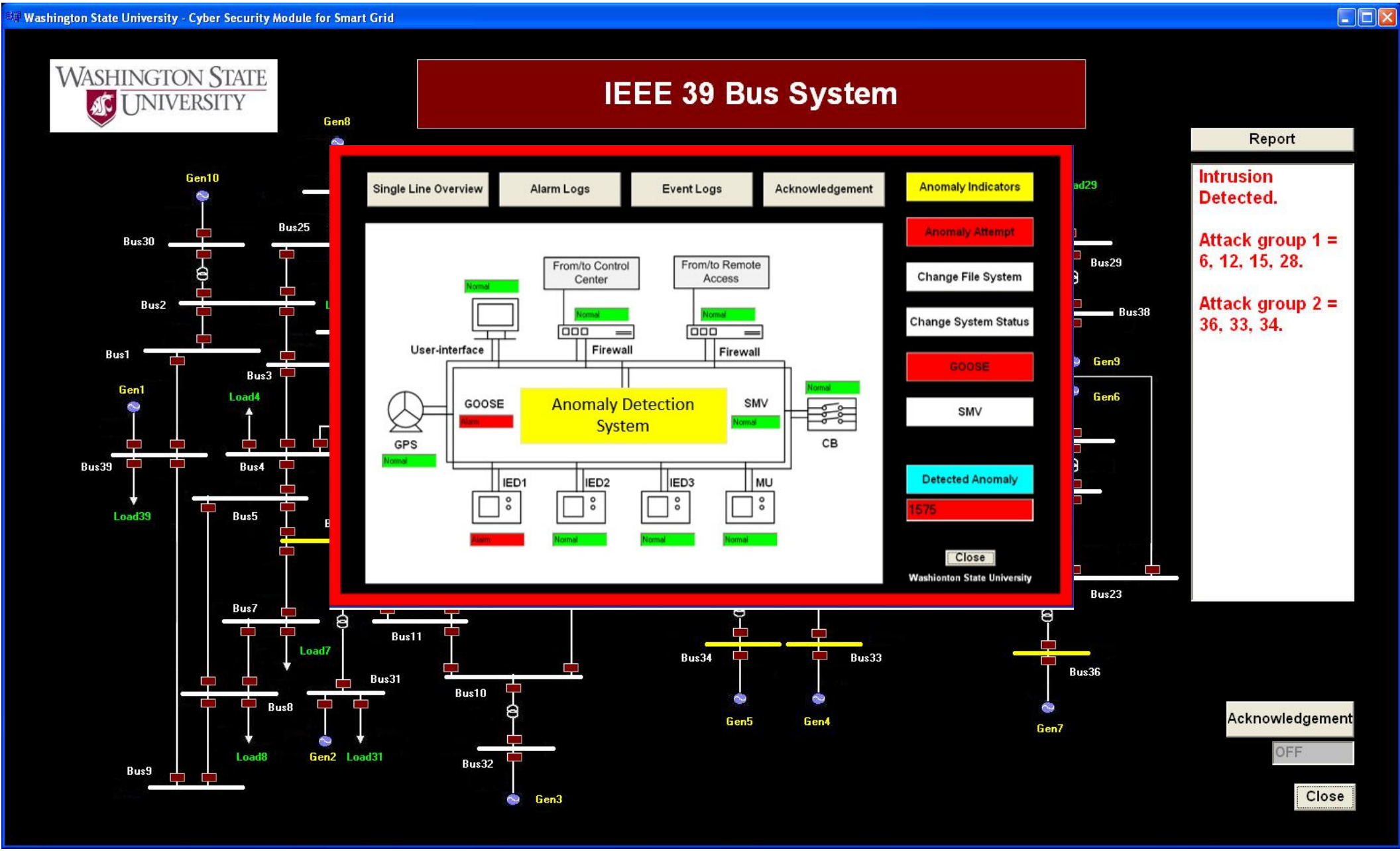



Frequency

Voltage

## Integrated Cyber-Power System Model




# Anomaly Detection System (ADS) at Substations

- J. Hong, C. C. Liu, M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," *IEEE Trans. Smart Grid*, July 2014, pp. 1643-1653.

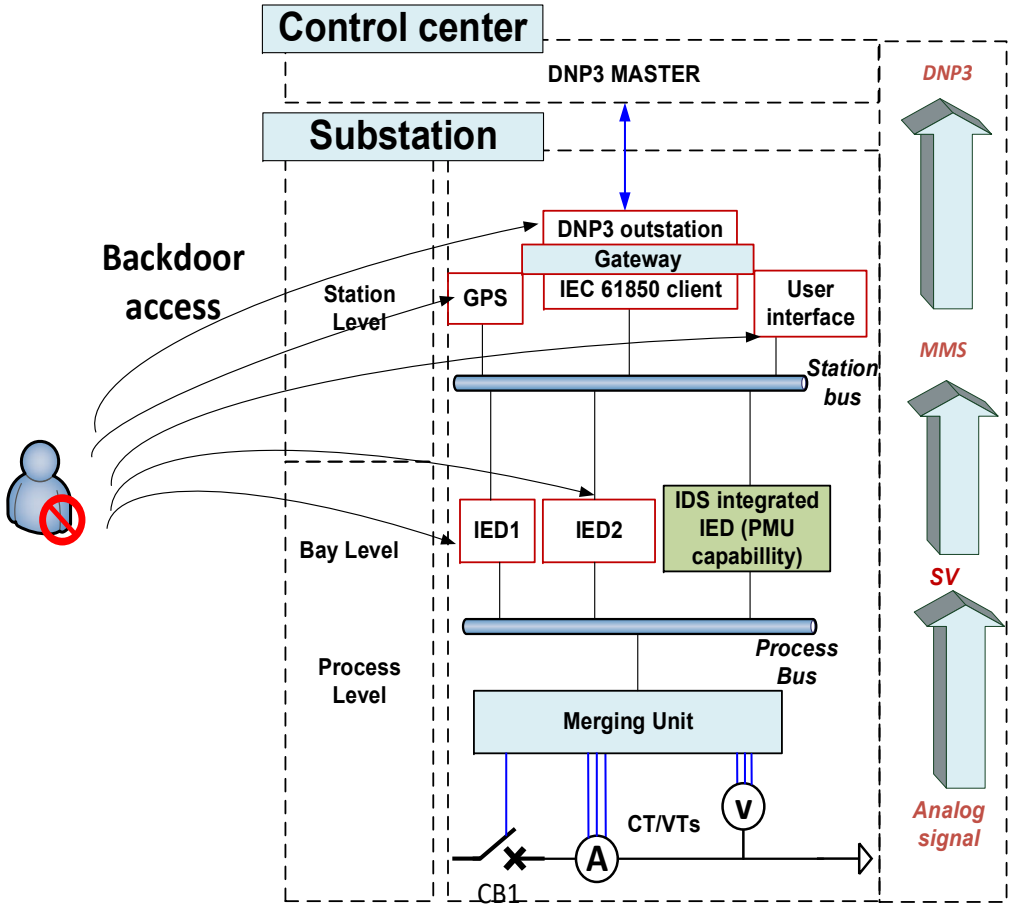
# *Measurement-Based Attacks*
# IEC 61850 Substations

Stage 1: From vendors' network
- Malicious code injected into source code of firmware or updates

Stage 2: From substation
- Malicious firmware/updates are downloaded
- Backdoors are installed at the devices (red boxes in the figure)

Stage 3: From remote access
- Steal signing keys/certifications
- Attempt to access IEDs through backdoor

Stage 4: Attack act
- Steal sensitive information
- Falsify the configuration of IEDs
- Inject **malicious measurements** from substation level



# Measurement Attacks at Substations

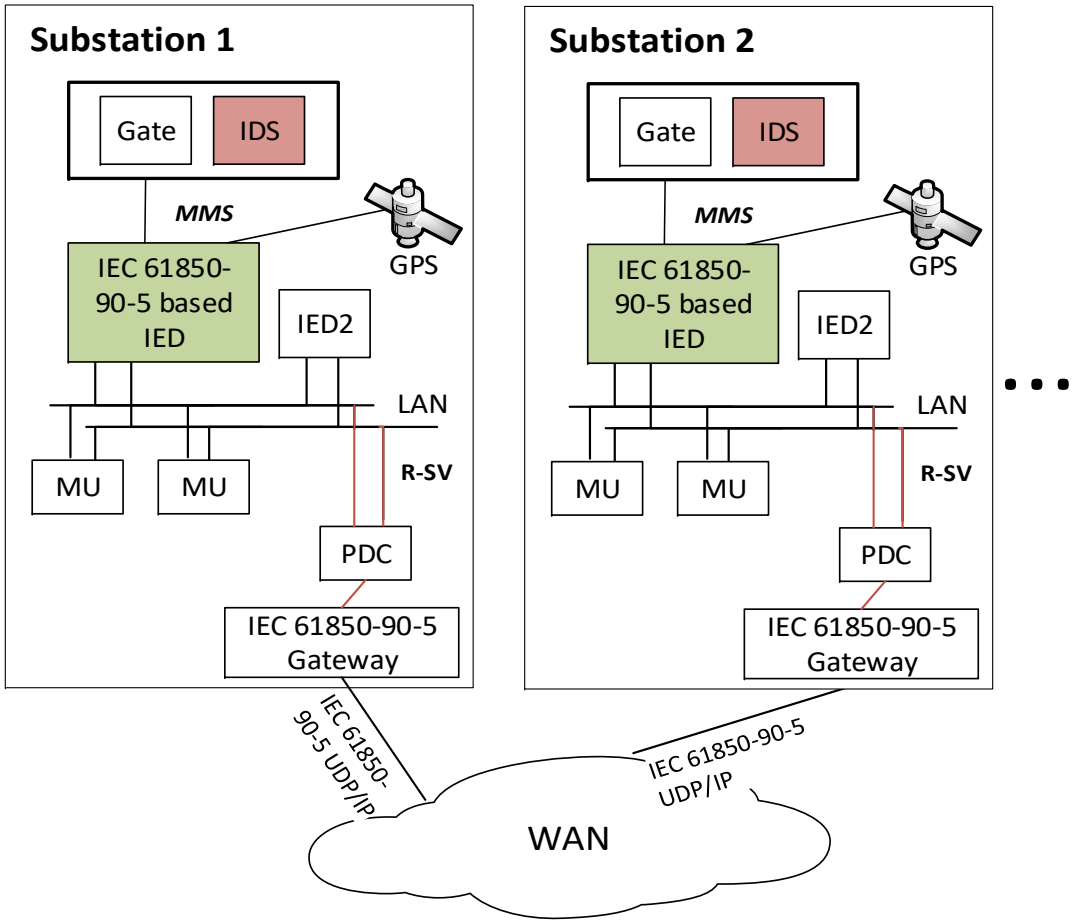
- Falsified measurements from substations may mislead system operators
- Control center IDS cannot detect measurement-based attacks before it compromises state estimation
- Specification-based IDS cannot detect falsified measurements in payload of the packets

# Electric Circuit Laws for IDS

| Measurements | IDS rules |
|---|---|
| Current | Kirchhoff`s Current Law (KCL): $\left\lvert\sum i_{exit} - \sum i_{enter}\right\rvert \leq k_{cer1}\lvert i_1\rvert + \cdots + k_{cern}\lvert i_n\rvert$ |
| Voltage | Kirchhoff`s Voltage Law (KVL): $\lvert v_1 + \cdots + v_n\rvert \leq k_{ver1}\lvert v_1\rvert + \cdots + k_{vern}\lvert v_n\rvert$ |
| Voltage and Current | Ohm`s Law: $\left\lvert v_j - v_k - i_{jk}Z_{line}\right\rvert \leq \mathrm{MAX}\left\{k_{verj}\lvert v_j\rvert, k_{verk}\lvert v_k\rvert, k_{cerjk}\lvert i_{jk}\right.$ |

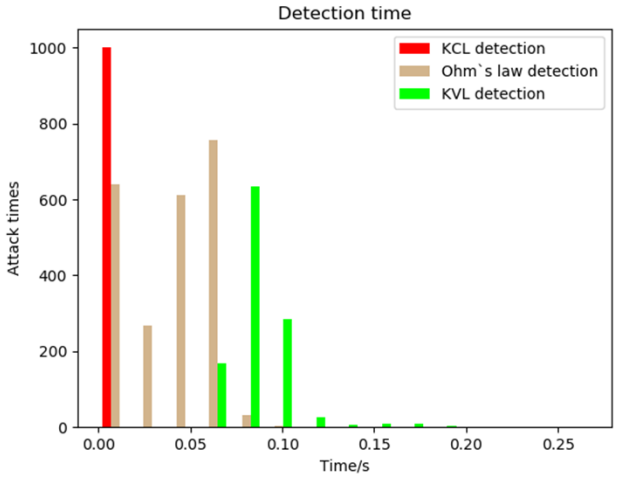
Measurement errors from CT/VT and merging units are included. $k_{ceri}, k_{veri}$ are the coefficients in the accuracy class for $\mathrm{CT_i}, VT_i$.

# Distributed Architecture of IDS

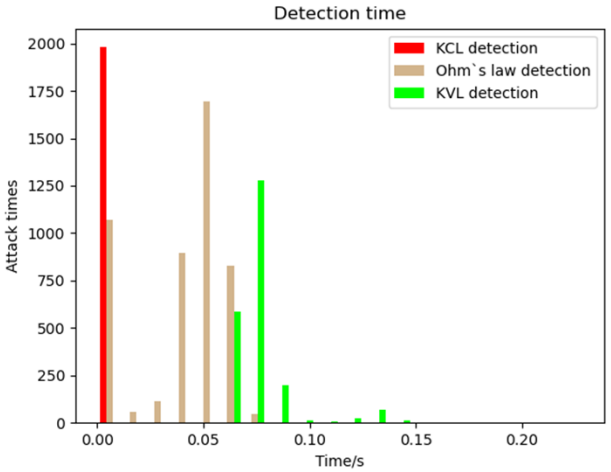



- Communication between substations for measurement cross check
- Proposed distributed IDS uses IDSIEC/TR 61850-90-5 for **secure transmission** of synchrophasor data between different LANs
- Each distributed IDS analyzes the measurements based on time stamps of the packets

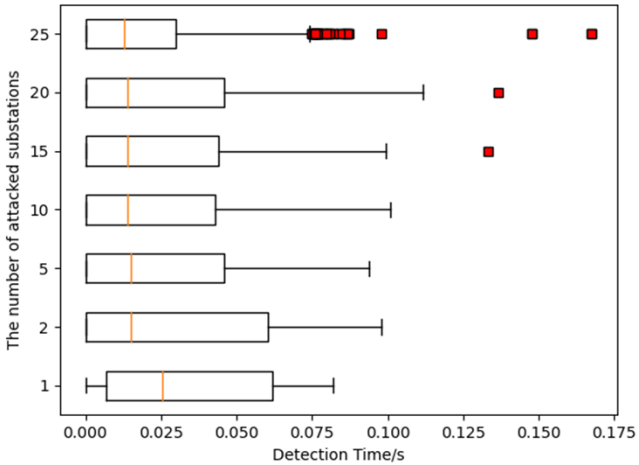
# Simulation Results: Detection Time (DT)




Single-bus attacks executed 1000 times



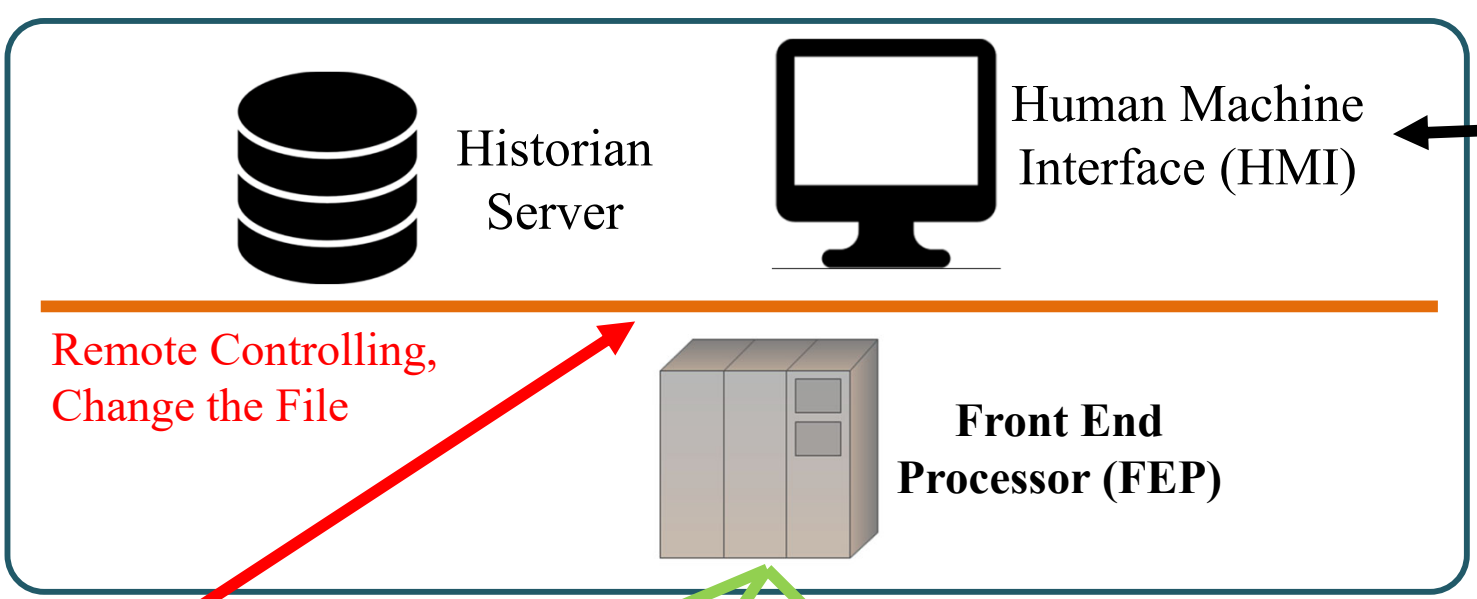

Two-bus attacks executed 1000 times



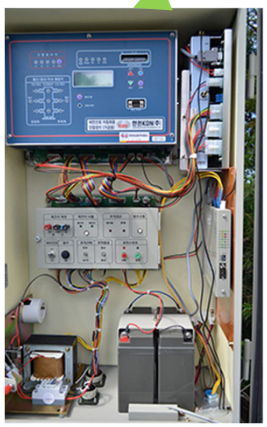

Distribution of detection time for attacks targeting multiple substations

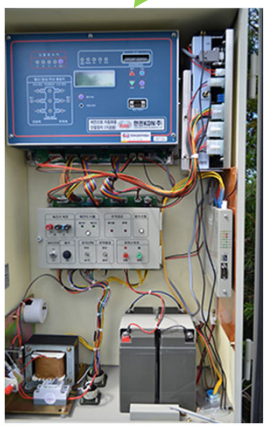
- DT distribution of single-bus attacks is close to that of two-bus attacks: the proposed IDS checks the consistency of measurements in a *distributed* manner
- For a broad range of attacks, the median DT falls under 0.025s.

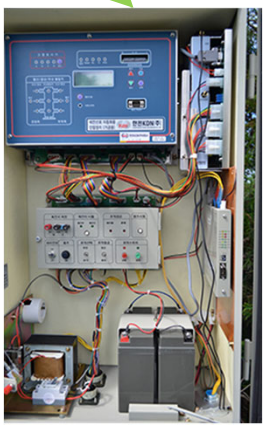
# Potential Attacks on Remote Controlled Switches




Hacker



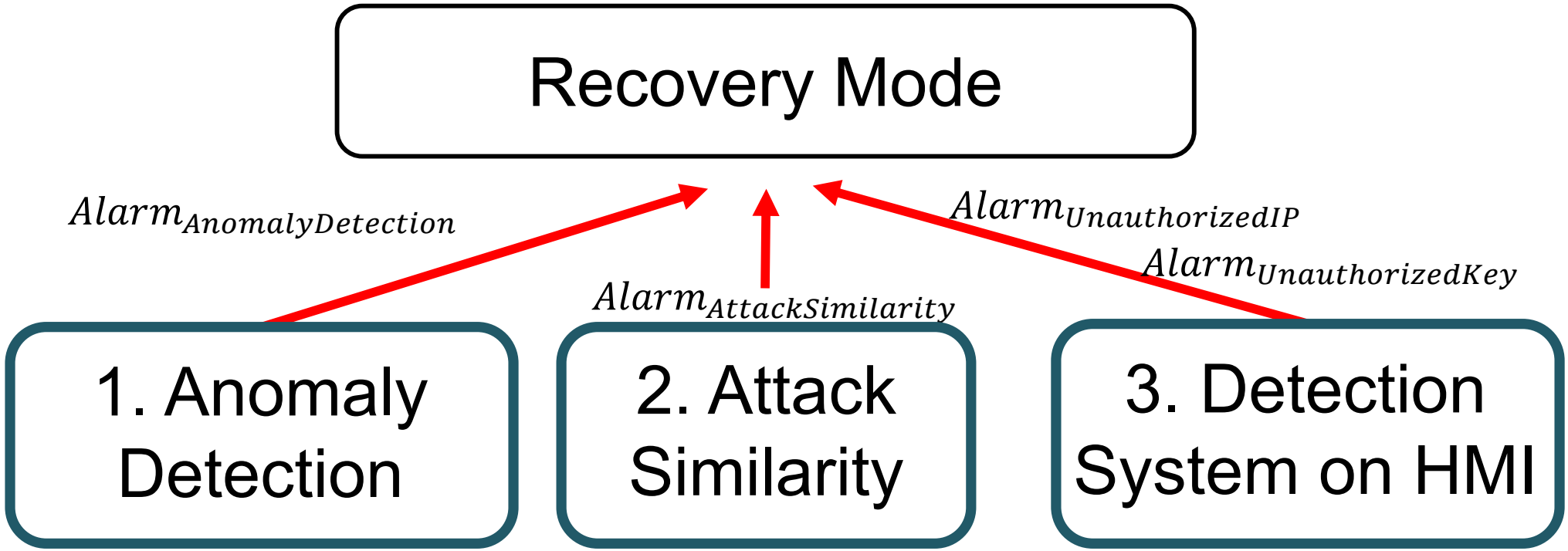




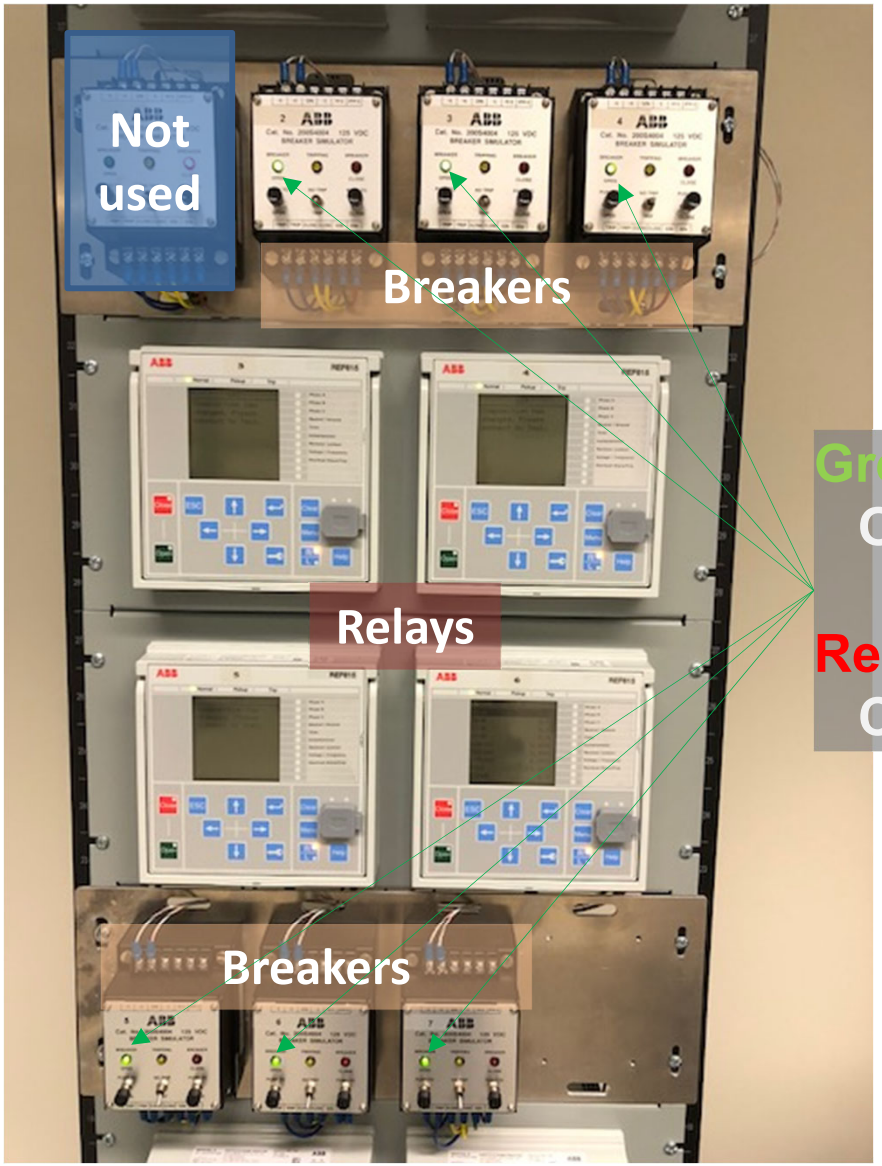
**F**eeder **R**emote **T**erminal **U**nits (FRTU)

- Substation sends command data to field devices and stores log data.
- Field devices receive data from substation and act.
- Two vulnerabilities in this example:
  - On substation
  - Communication with field devices

# Defense Algorithm

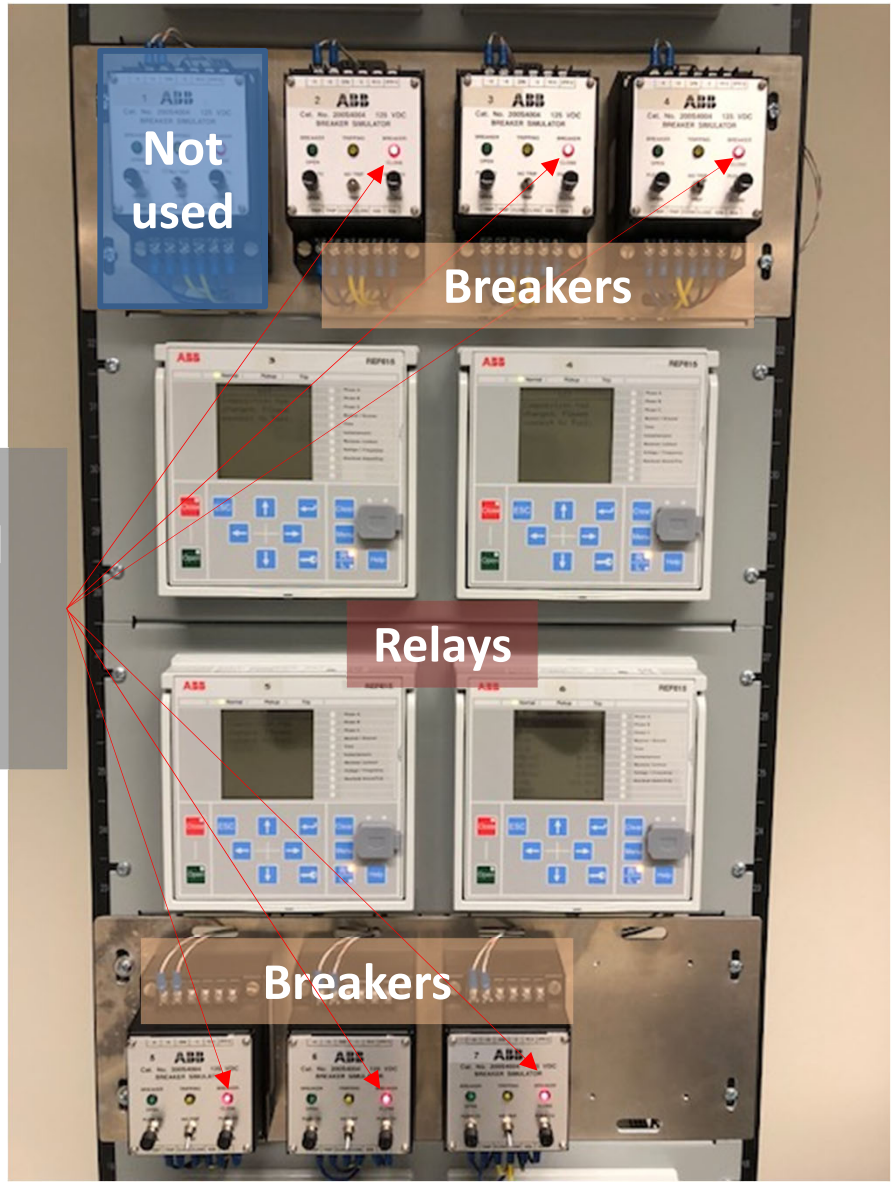


# Implementation on the Testbed at WSU




Green:
Opened

Red:
Closed

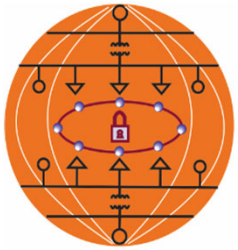



Tripping the breaker (No defense)

Successful defense

# Remarks

- Supply chain attacks in the context of substations and potential attack vectors.
- A comprehensive ***cyber*** system restoration strategy should be studied so that it can recover the cyber system of substations, control center, and SCADA communication network from cyber attacks.
- A distributed intelligence environment enabled by a Distributed Information System (DIS) in the distribution systems.



PEC

Power and Energy Center

VIRGINIA TECH™

# Further Information


[1] *Cyber Physical Systems Approach to Smart Electric Power Grid*, Eds. S. Khaitan, J. D. McCalley, C. C. Liu, Springer 2015.

[2] C. W. Ten, C. C. Liu, M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Trans. Power Systems*, Nov. 2008, pp. 1836-1846.

[3] S. Pudar, M. Govindarasu, C. C. Liu, "PENET: A Practical Method and Tool for Integrated Modeling of Security Attacks and Countermeasures," *Computers and Security*, Elsevier, 28, Nov. 2009, pp. 754-771.

[4] C. W. Ten, M. Govindarasu, C. C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Trans. Systems, Man, and Cybernetics*, Vol. 40, No. 4, July 2010, pp. 853-865.

[5] C. W. Ten, J. Hong, C. C. Liu, "Anomaly Detection for Cybersecurity of the Substations," *IEEE Trans. Smart Grid*, Dec 2011, pp. 865-873.

[6] J. Hong, C. C. Liu, M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," *IEEE Trans. Smart Grid*, July 2014, pp. 1643-1653.

[7] A. Stefanov, C. C. Liu, M. Govindarasu, "Modeling and Vulnerability Assessment of Integrated Cyber-Power Systems," *Int. Transactions on Electrical Energy Systems*, Vol. 25, No. 3, March 2015, pp. 498-519.

[8] J. Xie, A. Stefanov, C. C. Liu, "Physical and Cyber Security in a Smart Grid Environment," *Wiley Interdisciplinary Reviews Energy and Environment*, *WIREs Energy Environ* 2016. DOI: 10.1002/wene.202

[9] Y. Chen, J. Hong, C. C. Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations," *IEEE Trans. Smart Grid*, July 2018, pp. 2541-2552.

[10] C. C. Sun, A. Hahn, C. C. Liu, "Cyber Security of a Power Grid," *Int. J. Electrical Power and Energy Systems*, Jan 2018, pp. 45-56.

[11] J. Hong and C. C. Liu, "Intelligent Electronic Devices with Collaborative Intrusion Detection Systems," *IEEE Trans. Smart Grid.* Jan 2019, pp. 271-281.

[12] J. Appiah-Kubi and C. C. Liu, "Decentralized Intrusion Prevention (DIP) against Coordinated Cyberattacks on Distribution Systems," *IEEE Open Access Journal of Power and Energy,* 2020.

[13] R. Zhu, C.C. Liu, J. Hong, J. Wang, "Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations," *IEEE Access*, vol. 9, pp. 1240-1249, 2021