IEEE PES Bid Data Webinar Series, July 2019

VIRGINIA TECH

Cyber-Physical System Security of the Power Grid

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

Research Professor
Washington State University

Sponsored by U.S. National Science Foundation and
Science Foundation Ireland, Murdock Charitable Trust, ESIC
Washington State University, State of Washington

Center for Power & Energy (CPE)

- Founded by A. Phadke in 1986
- **Original members:** A. Phadke; L. Mili; R. Broadwater; S. Rahman; K. Tam; Y. Liu; and J. DeLaRee

- 1988: First Phasor Measurement Unit (PMU)
- 2002: Frequency Monitoring Network (FNET)
- 2008: A. Phadke and J. Thorp awarded Benjamin Franklin Medal in EE
- 2013: PMU-only three-phase state estimator in Dominion Virginia Power

PEC Core Faculty

Chen-Ching Liu

- Distribution systems, cyber security of the grid
- Industry software for system restoration: EPRI (Trans.), PNNL (Distr.)

Jaime De La Ree

Associate Professor &
Assistant Dept. Head

- Protection
- Machines

Lamine M. Mili

- Static and dynamic state estimation
- Robust power system parameter and dynamic state estimation w/ PMUs

Mona Ghassemi

Assistant Professor

- High voltage and high field engineering
- High voltage phenomena modeling: GE, Eversource, Hydro-Quebec, SaskPower, Manitoba H

Virgilio A. Centeno

Associate Professor

- PMU
- Instrumentation

Saifur Rahman

VT-ARC)

- Energy efficiency and sensor integration
- DoE BEMOSS Platform; President IEEE PES

Vassilis Kekatos

Assistant Professor

- *Optimization and learning of smart grids*

Ali Mehrizi-Sani

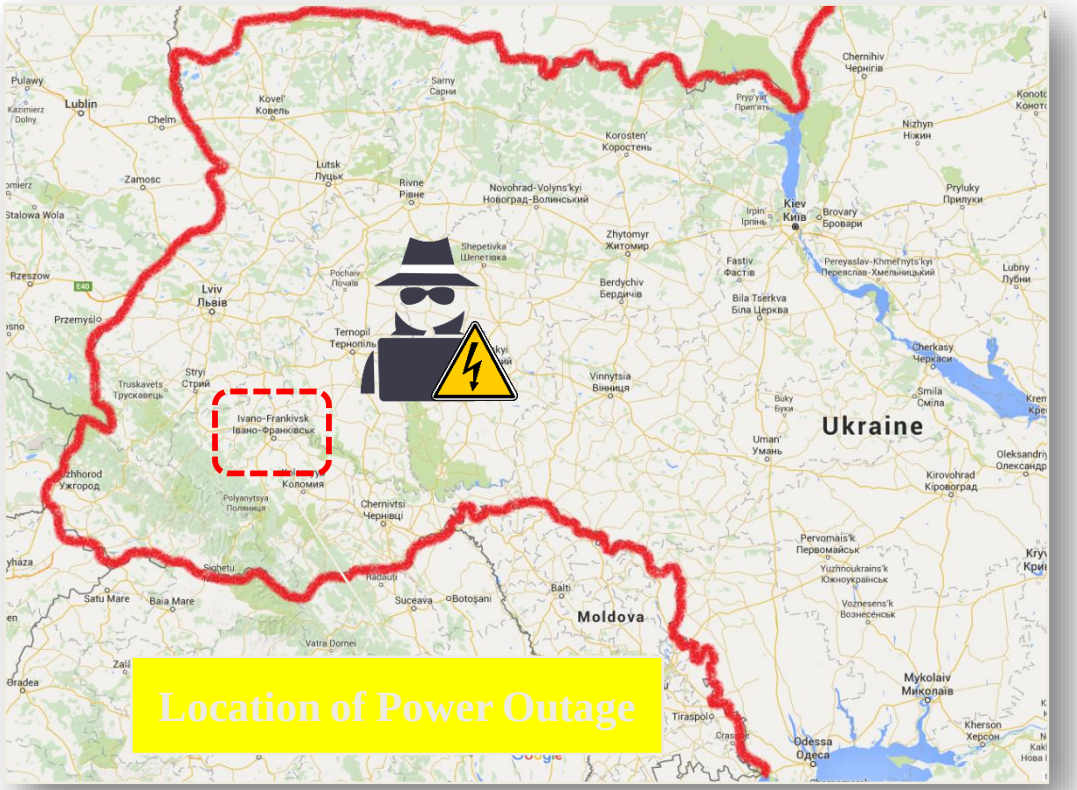
Associate Professor

- Microgrid control
- Power converters
- Integration of renewables
- Cyber security

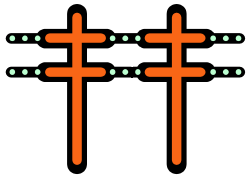
To join Aug 2019

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.



Power Grid with ICT



Power Grid

Information and Communication Technology

Critical Cyber Assets

- Critical Cyber Assets in Power infrastructure
  - Energy Management System (EMS) in Control Center
  - Distribution Management System (DMS)
  - Process Control System (Power Plants)
  - Substation Automation System (SAS)

Evolution of SCADA Systems

Evolved through generations

- Monolithic
- Distributed
- Networked

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

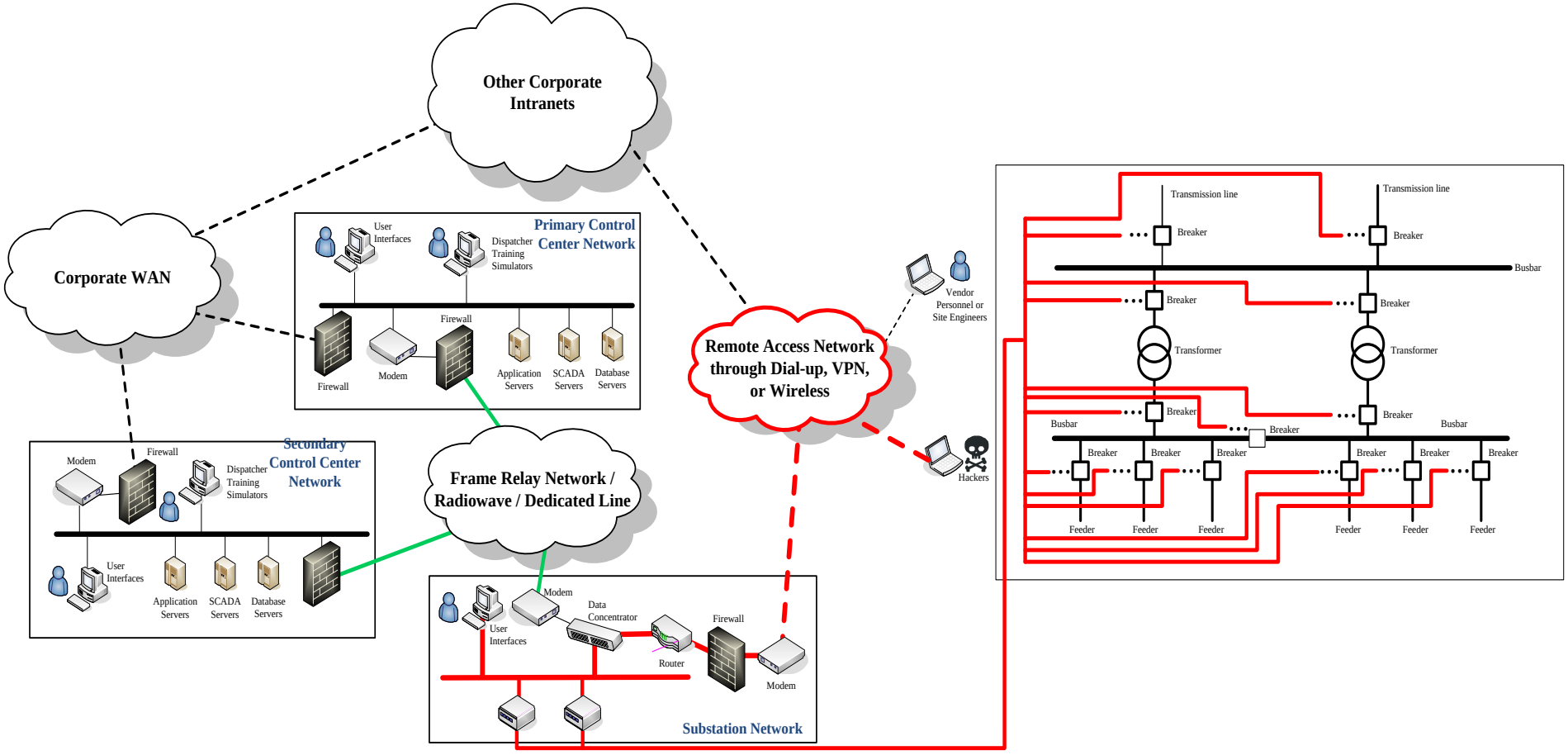
Intrusion Tools

- War Dialing
- Scanning
- Traffic Sniffing
- Password Cracking
- Stuxnet
- Ukraine

Supervisory Control And Data Acquisition (SCADA)

	Electric Power	Natural Gas Pipelines, Process Control Systems	Transportation
Sectors	Transmission, Distribution, Substation Network Monitoring) Wind Farms	Gas Pipeline, Chemical, Oil and Gas, Power Plants	Roadway, Rail System, Space and Air Traffic
Example Protocols	ICCP / DNP3i / Modbus over TCP/IP / IEC870-5-101/104 / IEC 61850	Fieldbus or Profibus	Cellular Digital Packet Data Network and Global Positioning System
Framework	Data Polling Acquisition & Control / Automation Are Configured for Interlocking and Protection Scheme	Automation by Programmable Logic Controller (PLC)	Ensuring Associated Tasks with Given Function, Satisfying System Performance in Centre
Input Variables	Voltage, Current, Frequency, Time, Active Power, Reactive Power, Apparent Power	Temperature, Pressure, Time, etc.	Traffic and Roadway Sensors, Visual Closed Circuit Television Sensors, Voice Communication, Probe Vehicle and Database Services, Global Positioning System
Control Variables	Switching Devices	Valve, Pump	Controls of Roadway Access and Intersection Devices
Application	Energy Management System () / Distribution Management System (DMS) / Substation Automation System (SAS)	Generation Management System (GMS), Resource Planning System (ERP)	Adaptive Traffic Control System, Incident Detection and Location System, and Predictive Traffic Modelling System

Cyber Systems in Power Infrastructure



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

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

Scenario Vulnerability

- An intrusion scenario consists of the steps taken by an attempted attack from a substation-level network

- Substation-level networks in a power system
  - substation automation systems
  - power plant control systems
  - distribution operating centers

- Scenario vulnerability is defined by

$$V(I) = \{V(i_1), V(i_2), \ldots, V(i_K)\}$$

where *K* is the number of intrusion scenarios to be evaluated

Access Point Vulnerability

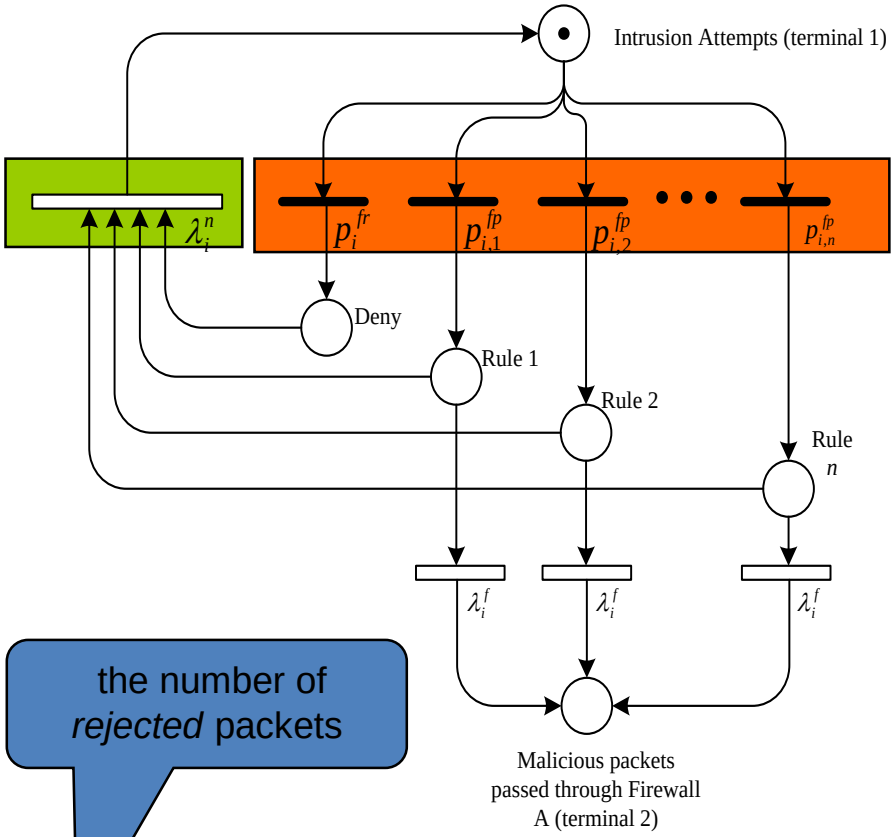
- Access point provides the port services to establish a connection for an intruder to penetrate SCADA computer systems
- Vulnerability of a scenario i, V(i), through an access point is evaluated to determine its potential damage
- Scenario vulnerability - weighted sum of the potential damages over the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

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

where π_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, γ_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*.

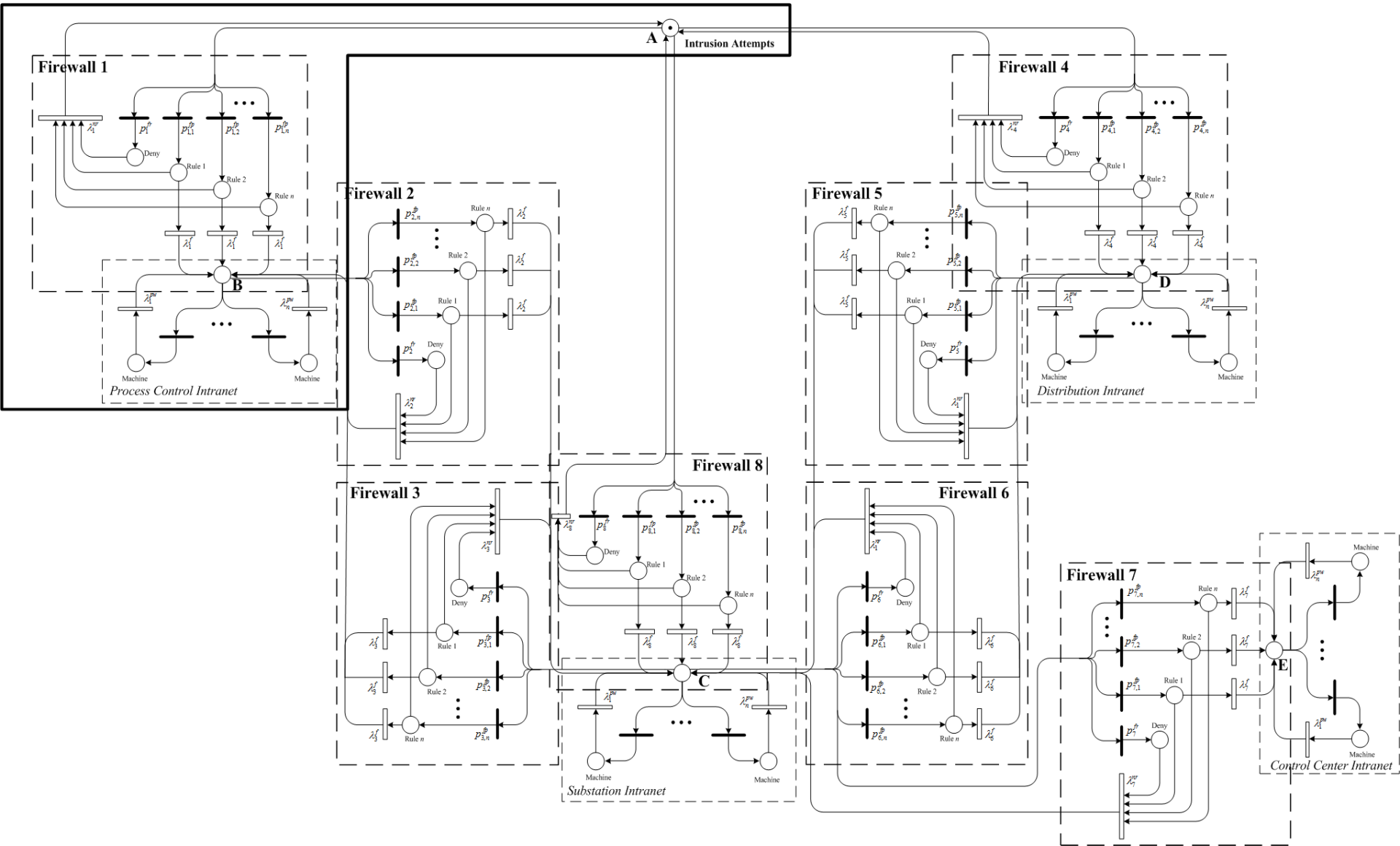
the number of *rejected* packets

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

Construction of Cyber-Net Based on Substation with Load and Generator



Impact Factor Evaluation

- Impact factor for the attack upon a SCADA system is

$$\gamma = \left(\frac{P_{LOL}}{P_{Total}} \right)^{L-1}$$

- Loss of load (LOL) is quantified for a disconnected substation

- To determine the value of L, one starts with the value of L=1 at the substation and gradually increases the loading level of the entire system without the substation that has been attacked.

- Stop when power flow fails to converge (System is considered unstable)

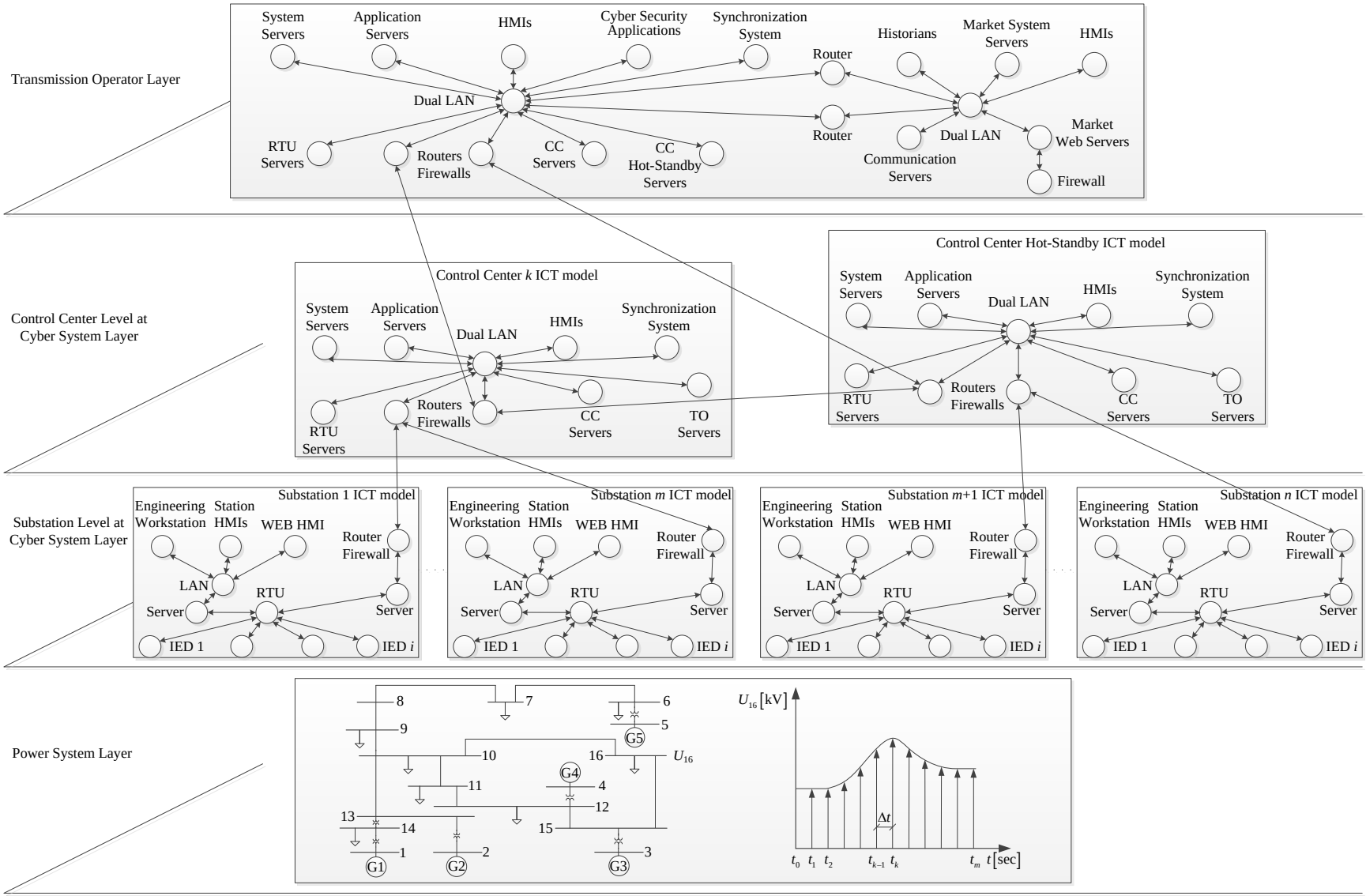
Modeling Integrated Cyber-Power System

- **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

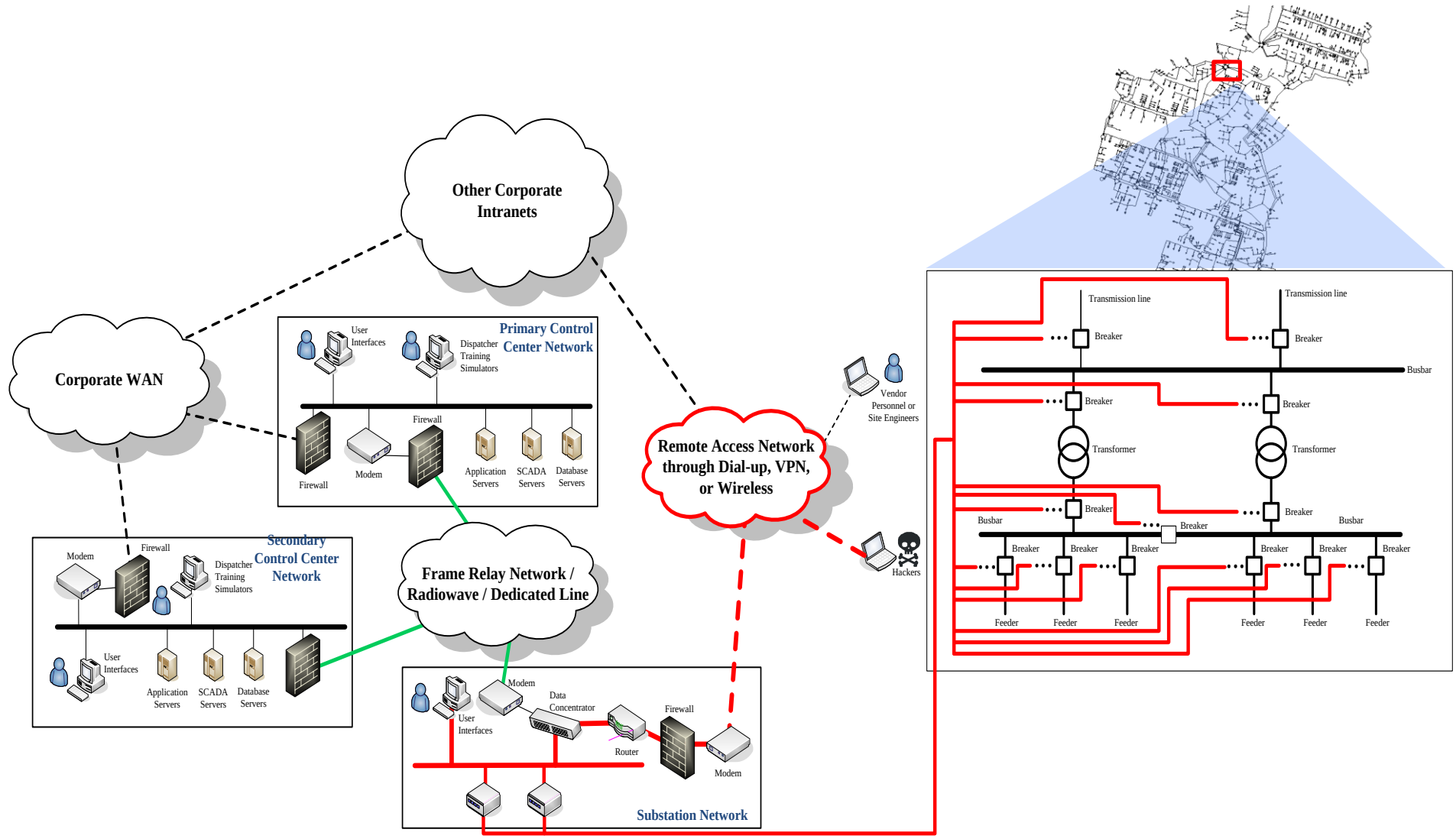
- **CPS tool used for assessment of SCADA communication performance**
  - Plan SCADA and ICT systems for power grids

- **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

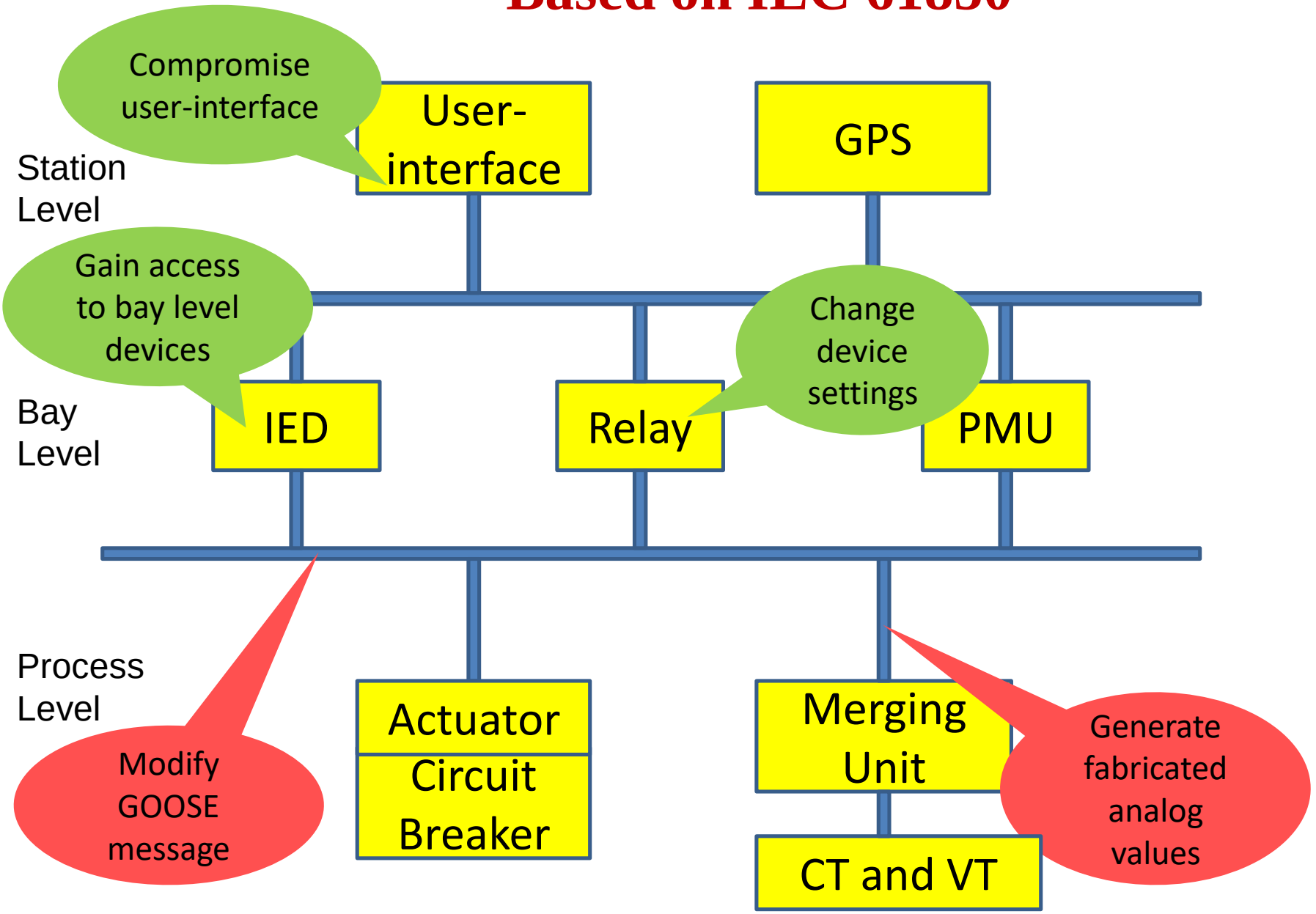
Cyber-Physical System Model



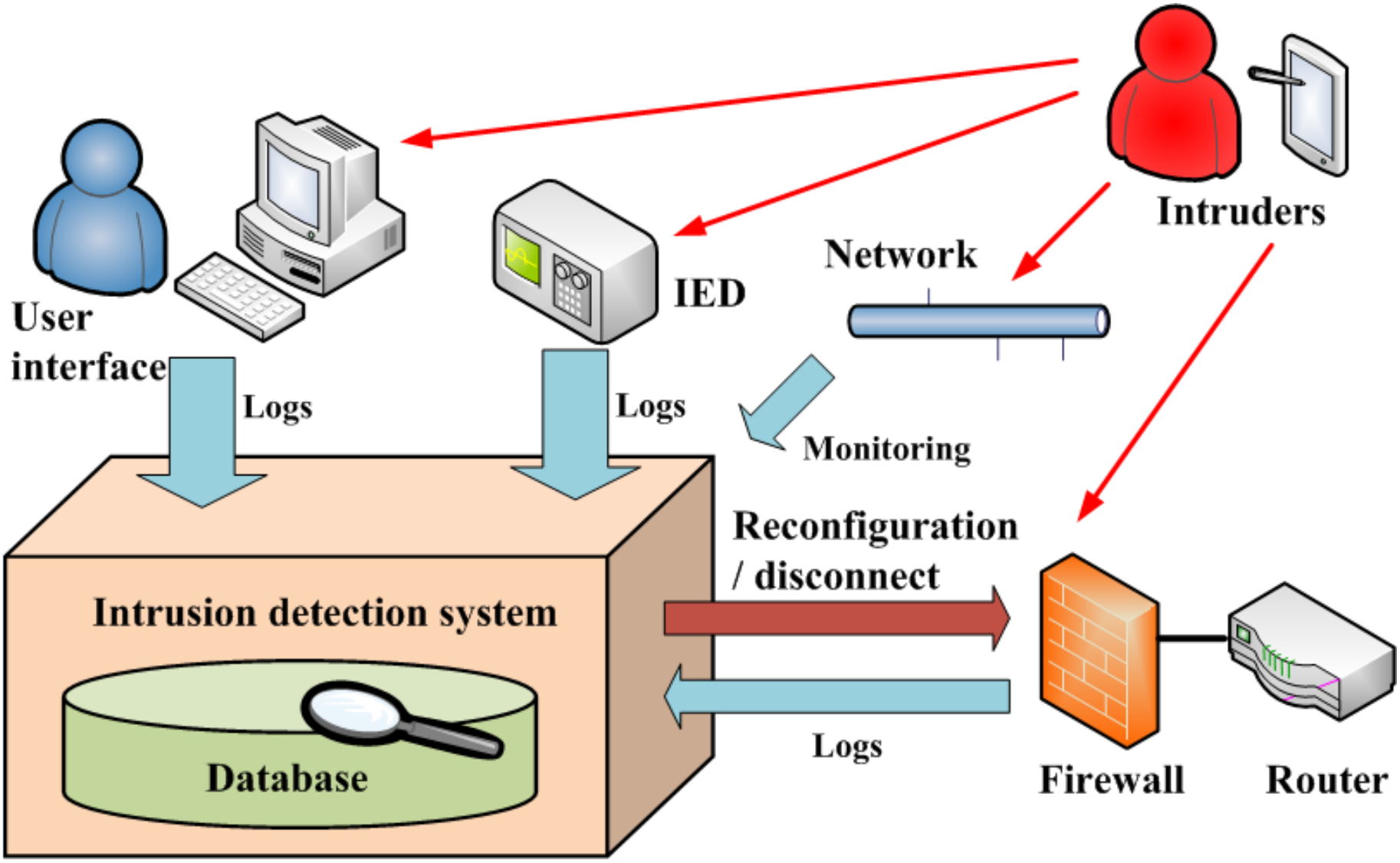
Intrusion into a Substation Network



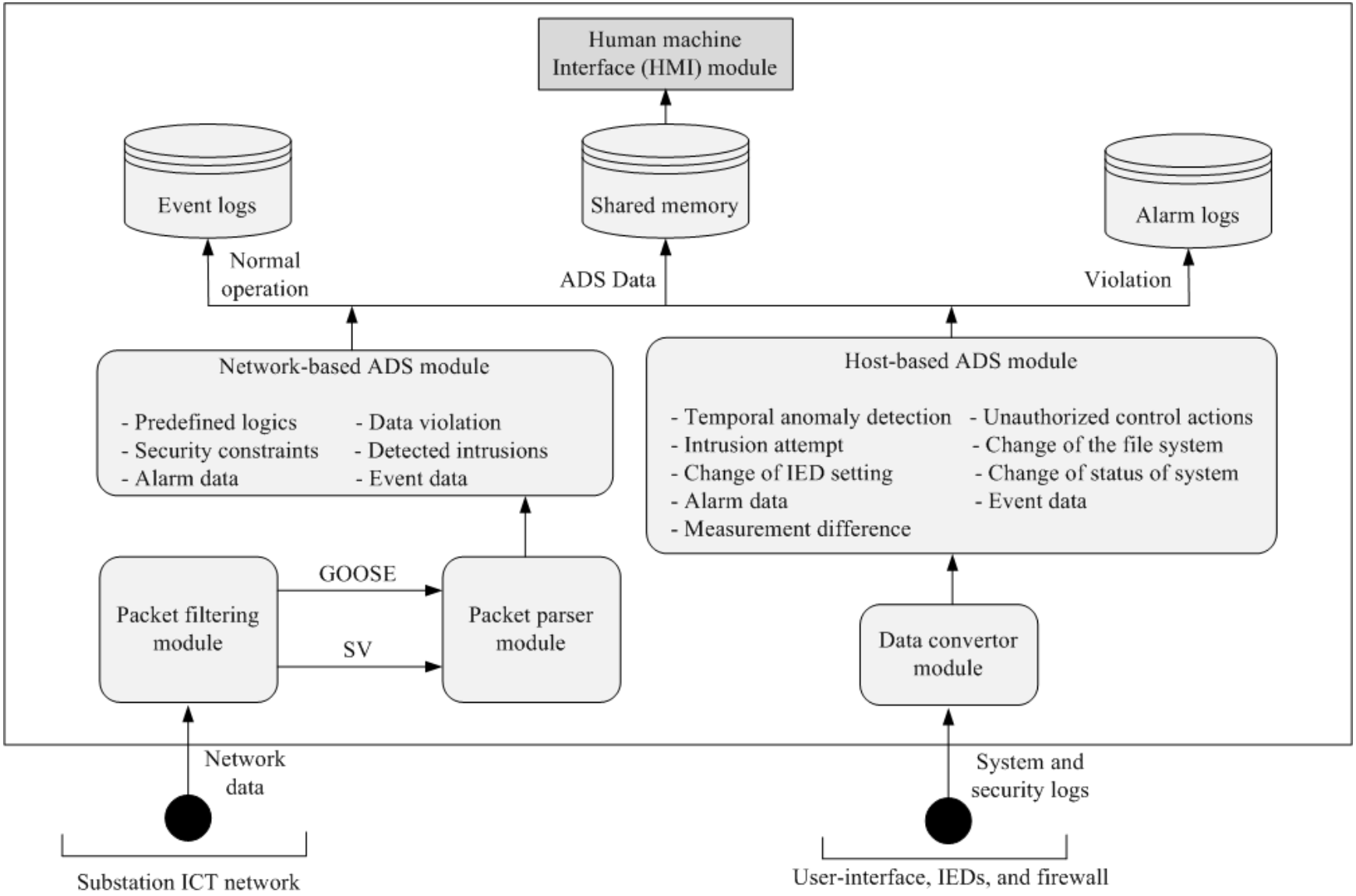
Potential Threats in a Substation Based on IEC 61850



Anomaly Detection at Substations



Integrated Anomaly Detection System



Host-Based Anomaly Detection

- Detection of temporal anomalies is performed by comparing consecutive row vectors representing a sequence of time instants

$$V_{h(i)}^{\boldsymbol{\Omega}} = \frac{\sum_{j=1}^{n} \left| \boldsymbol{\Omega}_{(i,j)} - \boldsymbol{\Omega}_{(i+1,j)} \right|}{n}, \; i = 1, \ldots, 6,$$

- If a discrepancy exists between two different periods (rows, 10 seconds), the anomaly index is a number between 0 and 1

- A value of 0 implies no discrepancy whereas 1 indicates the maximal discrepancy

Host-based anomaly indicators

- ψ^a (intrusion attempt on user interface or IED)
- ψ^cf (change of the file system)
- ψ^cs (change of IED critical settings)
- ψ^o (change of status of breakers or transformer taps)
- ψ^m (measurement difference)

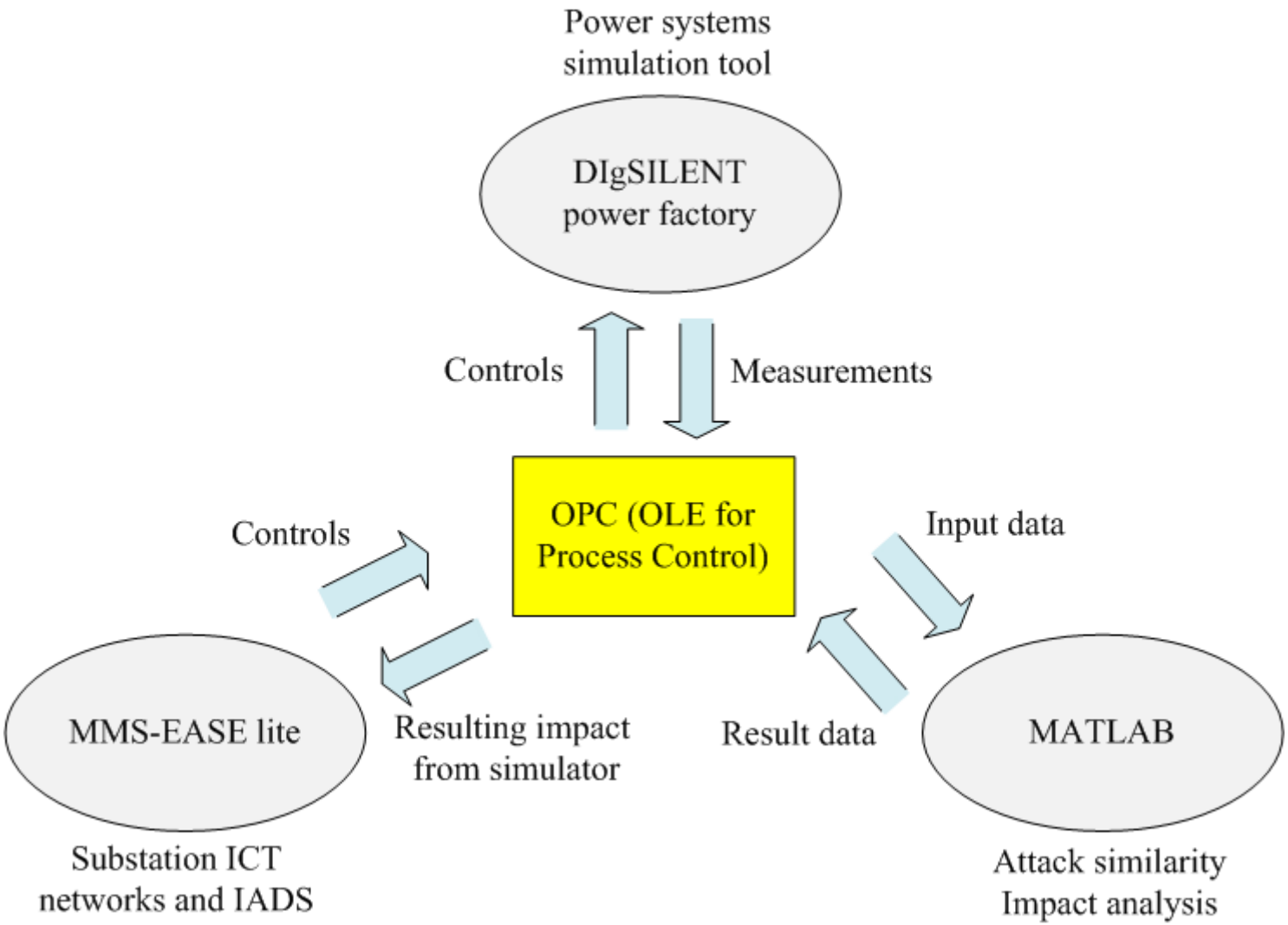
Substation A

$$\boldsymbol{\Omega} = \begin{array}{c} \\ t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{array} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

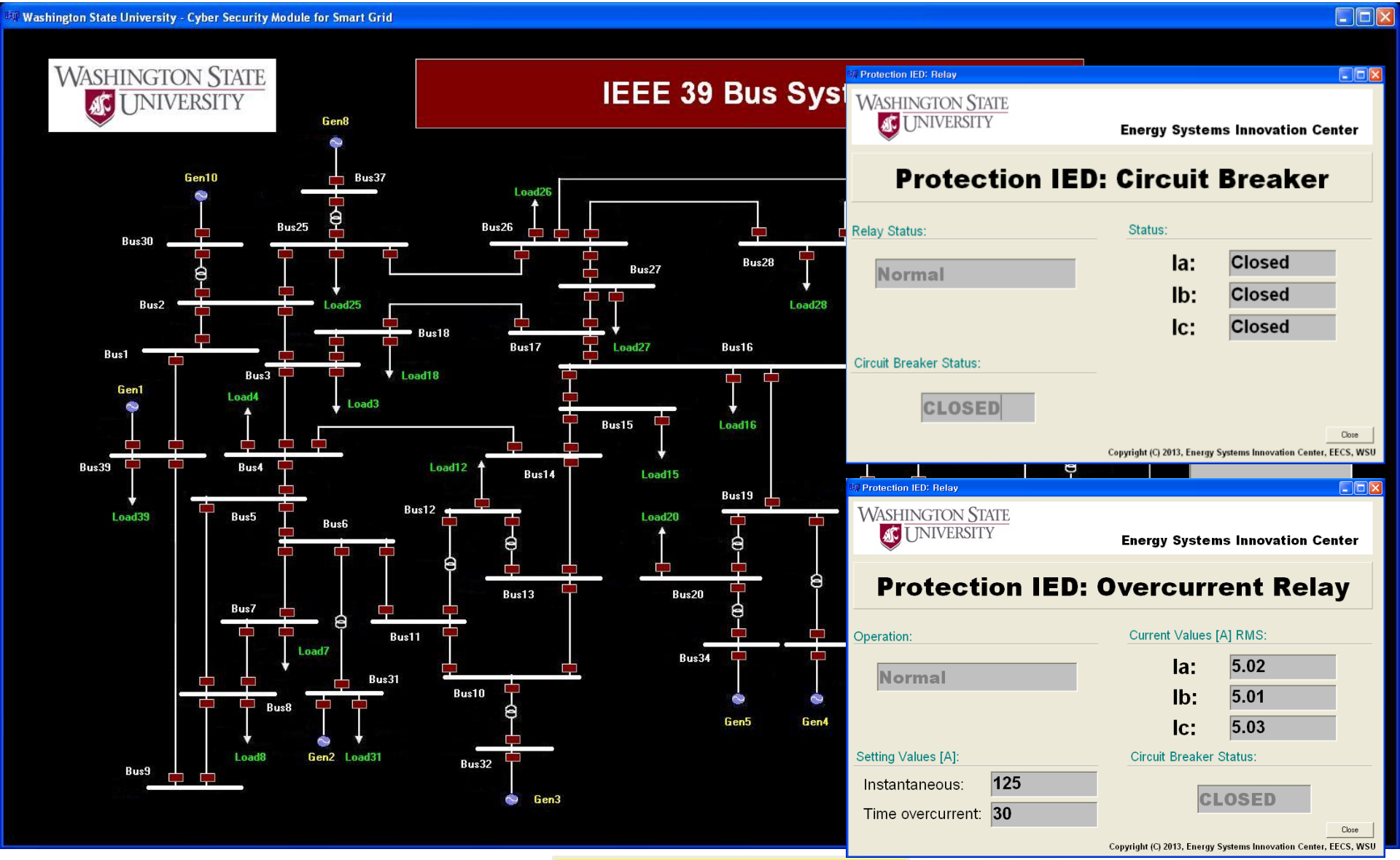
Consequence of GOOSE Based Attack

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

System Integration

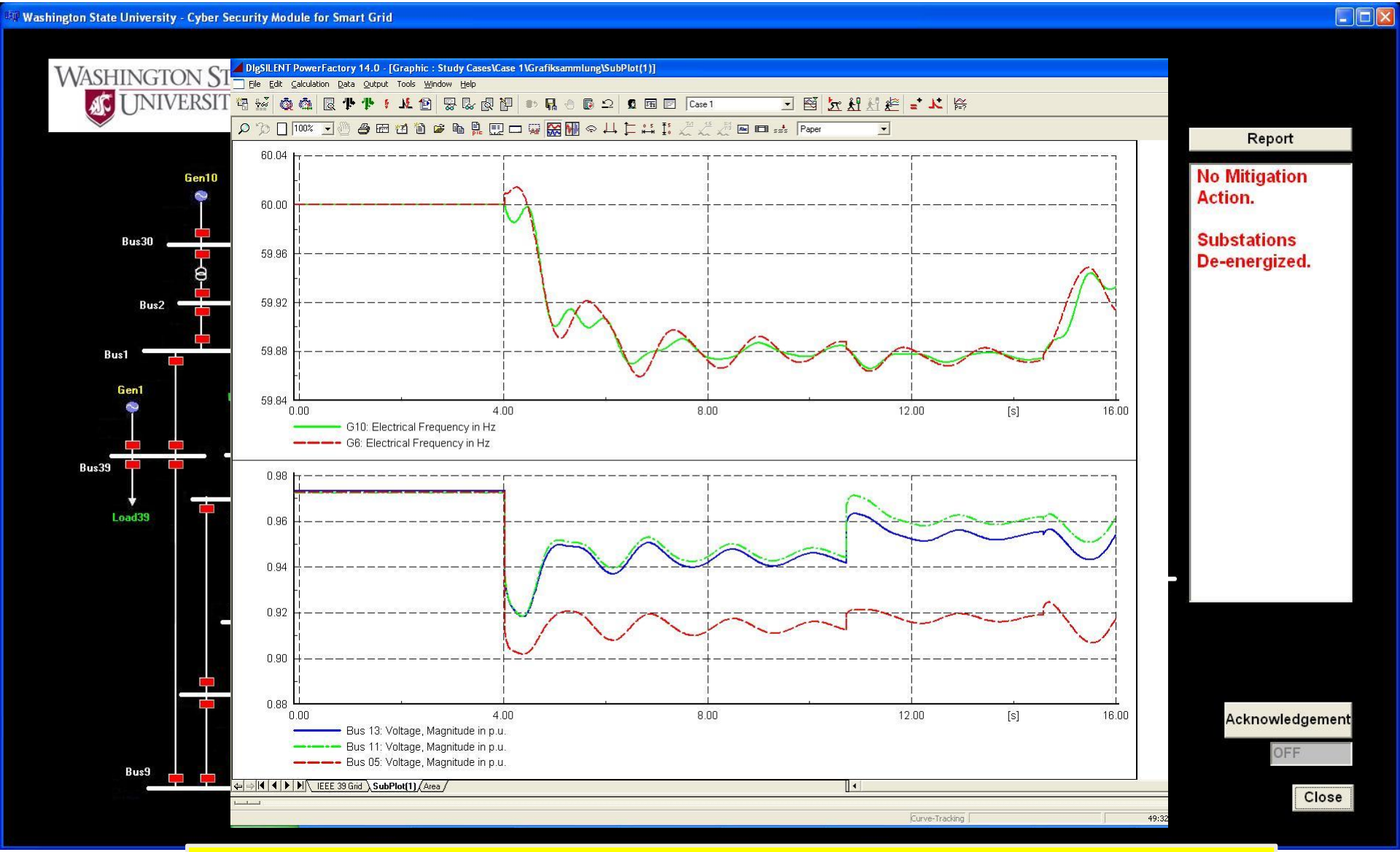


IEEE 39 Bus System

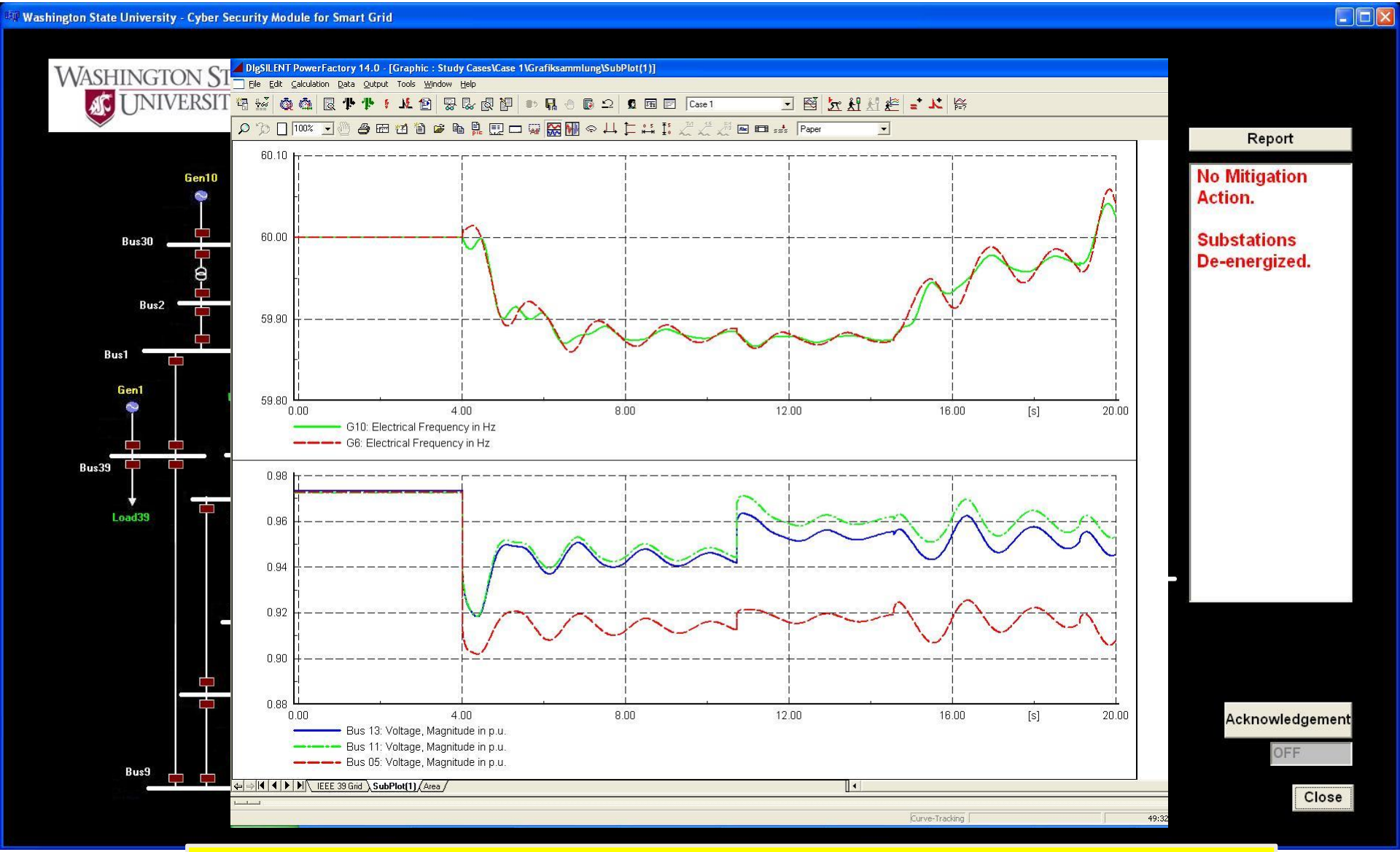


Normal status

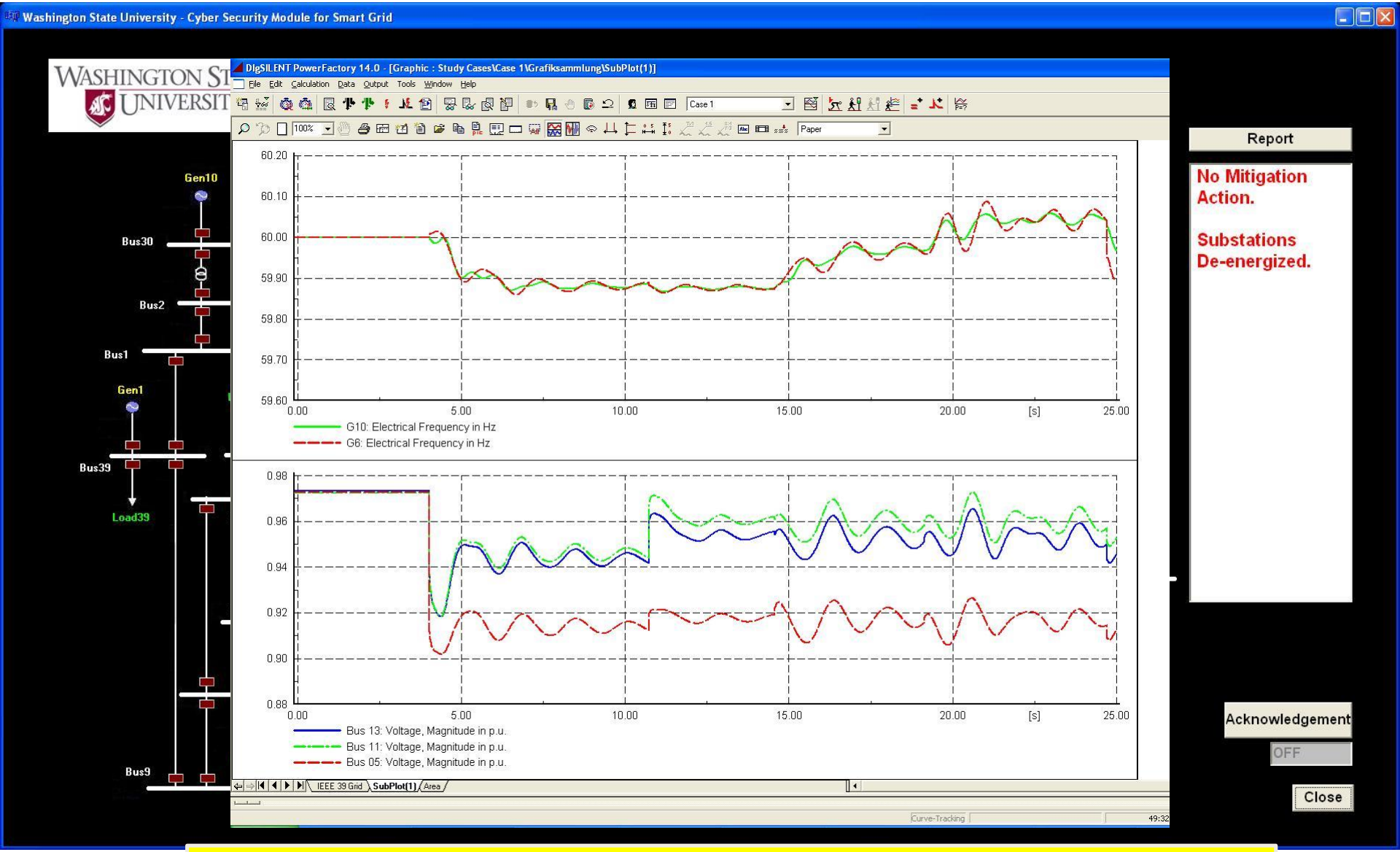
Sequential attacks – Sub # **6** → 12 → 15 → 28 → 36 → 33 → 34



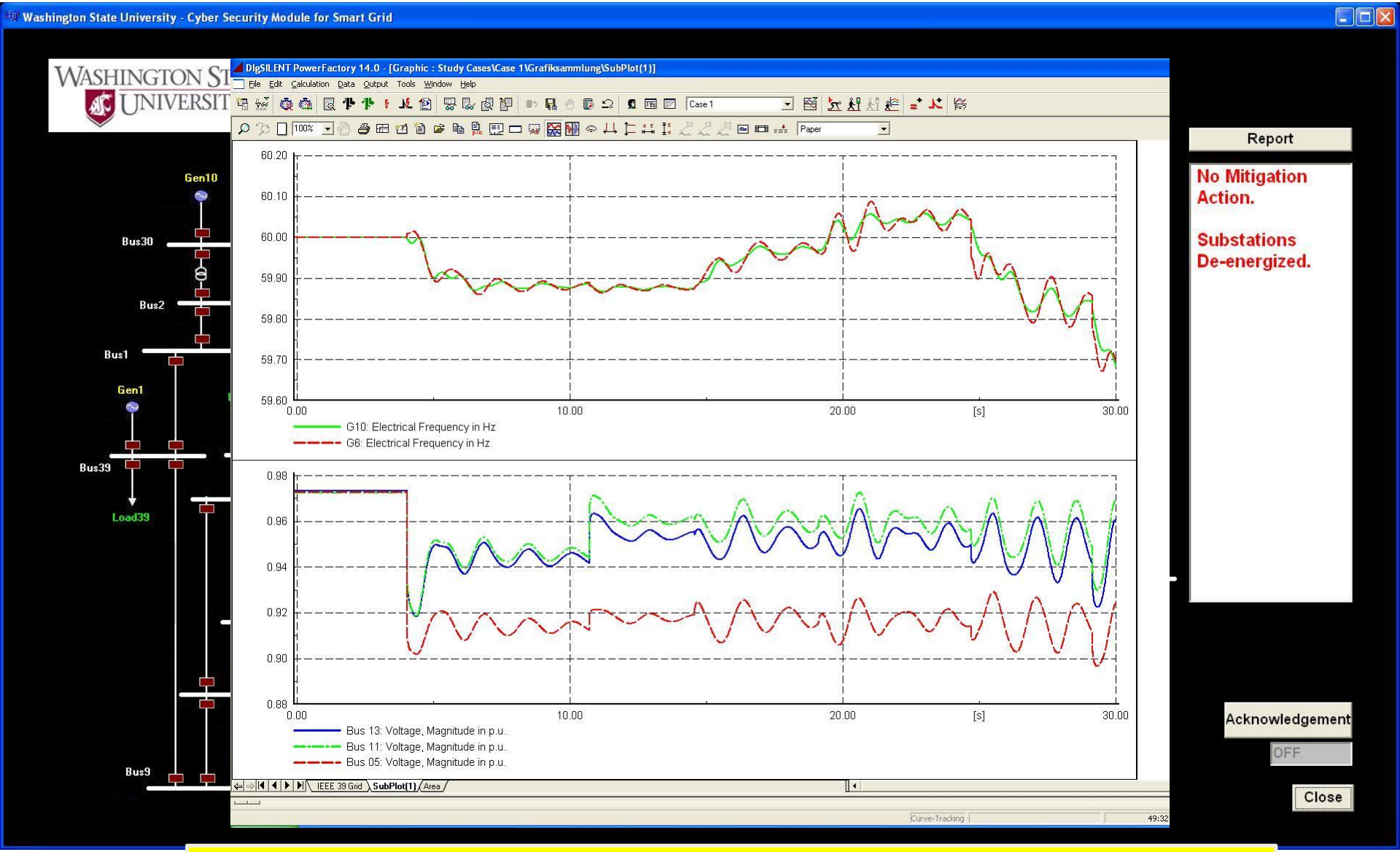
Sequential attacks – Sub # 6 → **12** → 15 → 28 → 36 → 33 → 34



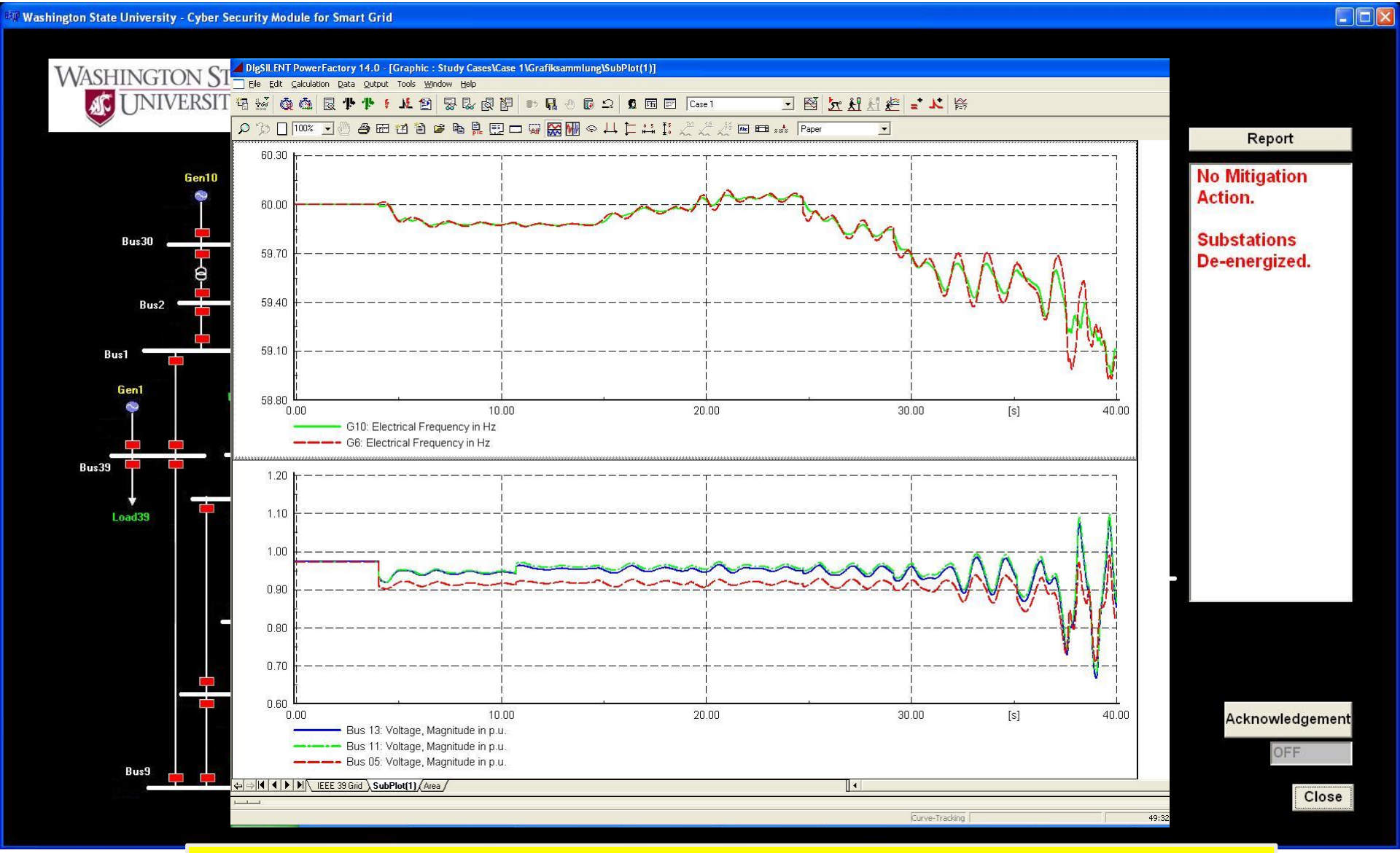
Sequential attacks – Sub # 6 → 12 → **15** → 28 → 36 → 33 → 34



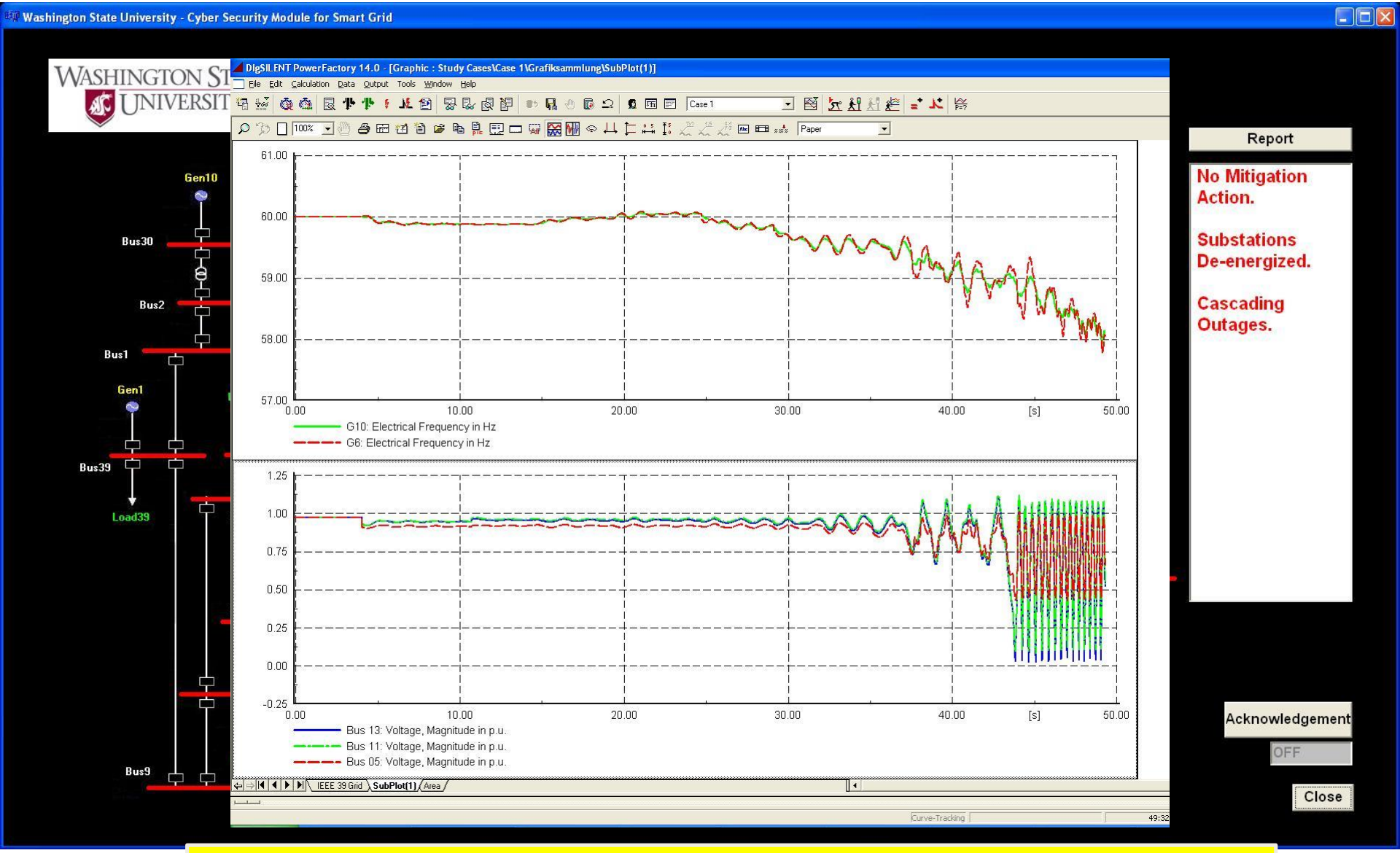
Sequential attacks – Sub # 6 → 12 → 15 → **28** → 36 → 33 → 34



Sequential attacks – Sub # 6 → 12 → 15 → 28 → **36** → 33 → 34

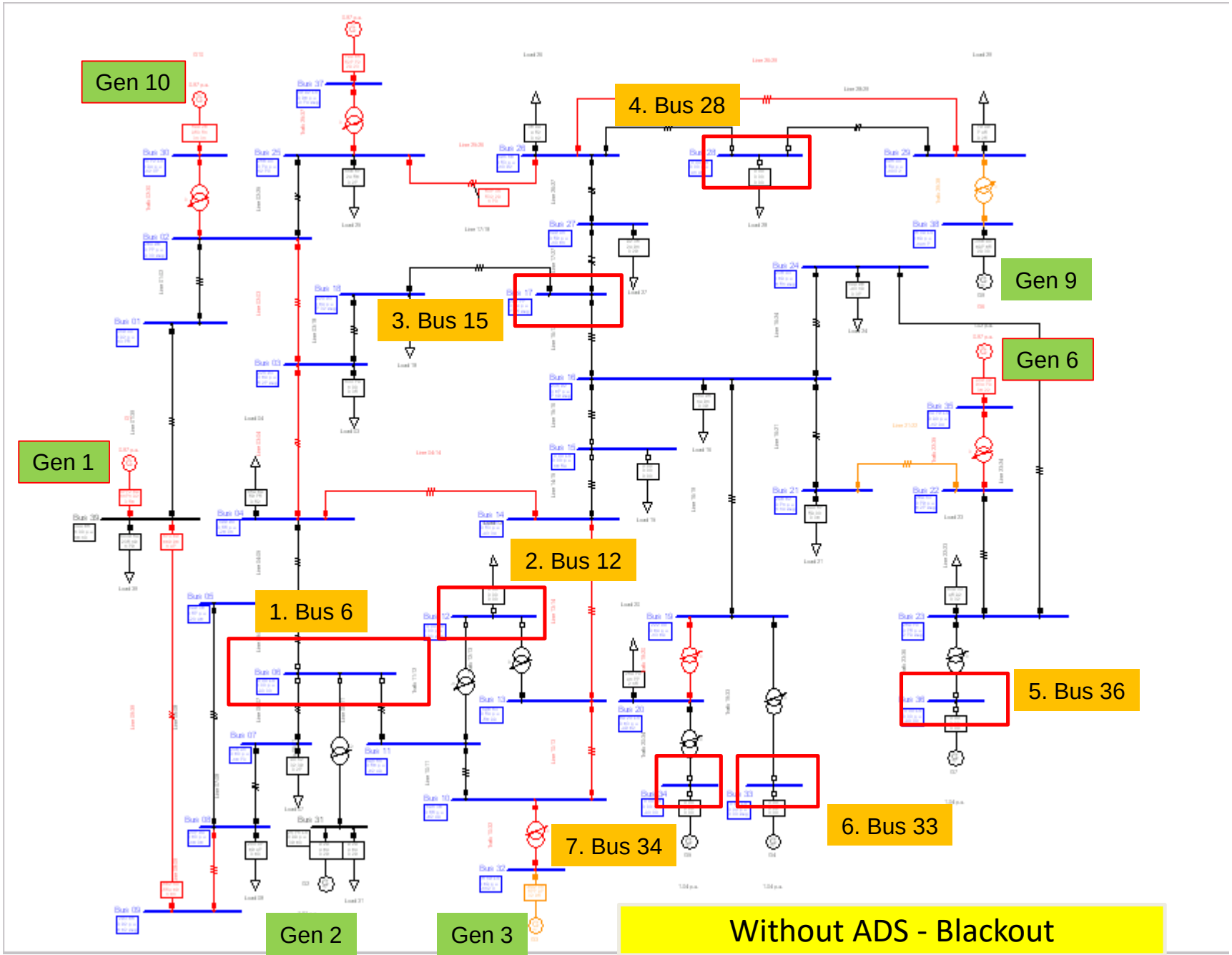


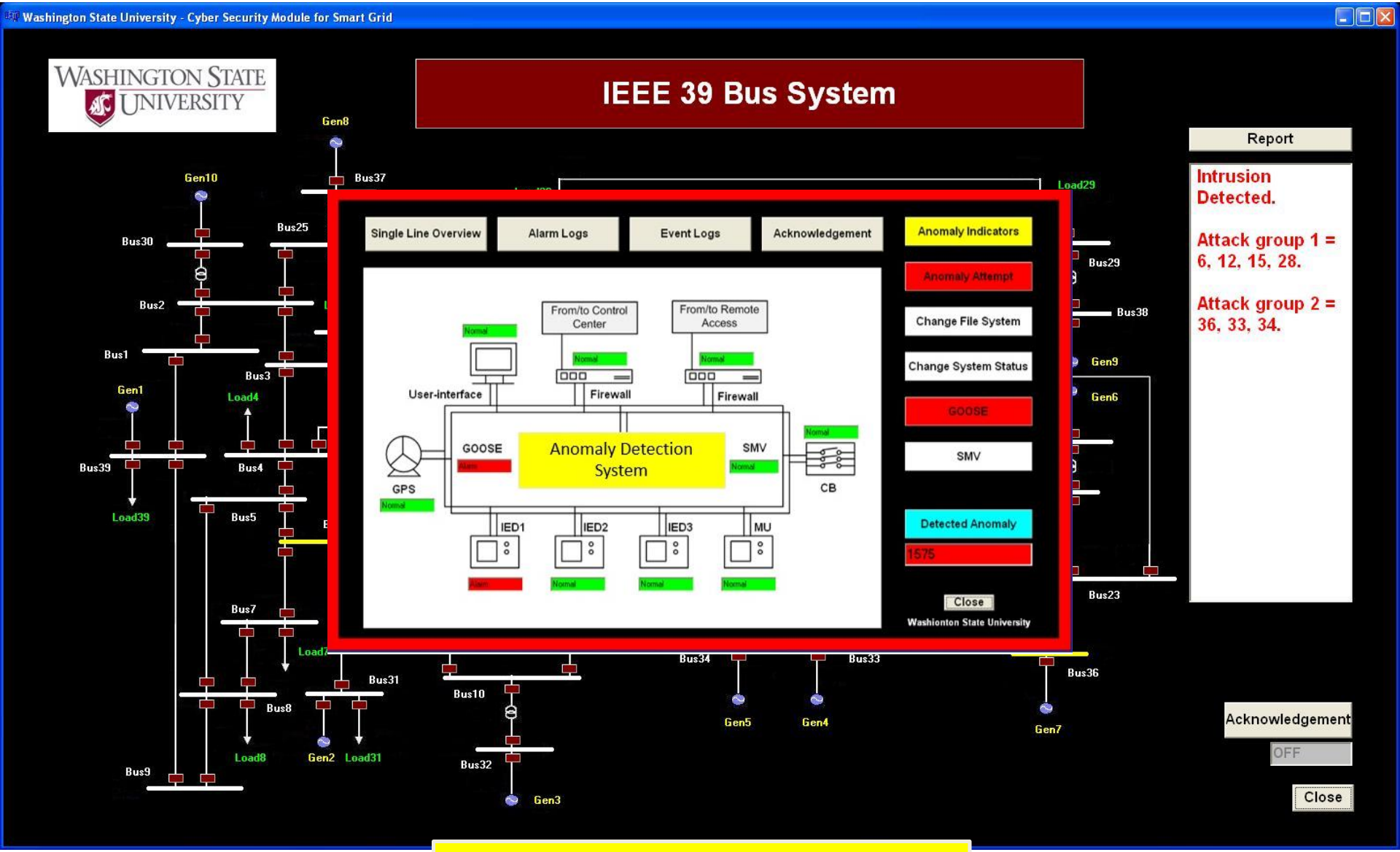
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → **33** → 34



Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → **34**

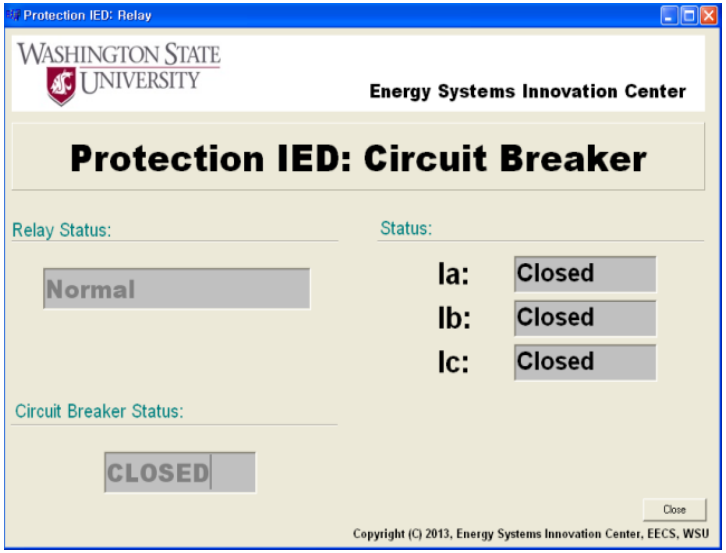
IEEE 39 Bus System (DIgSILENT)

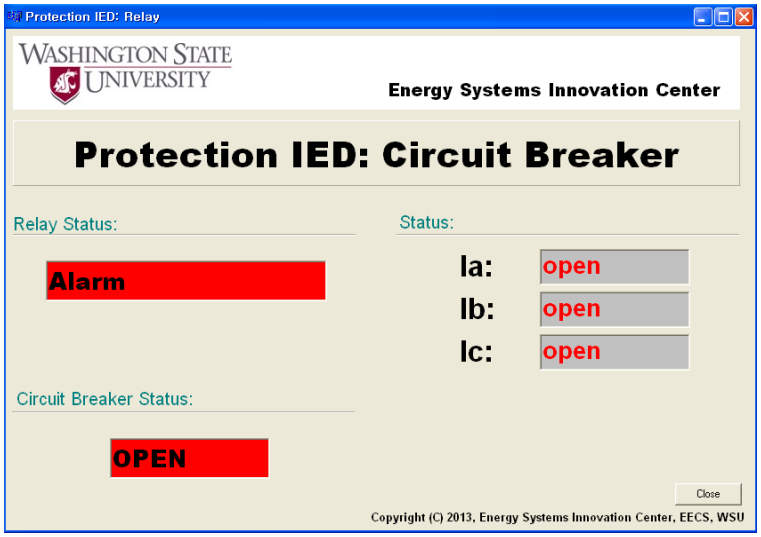


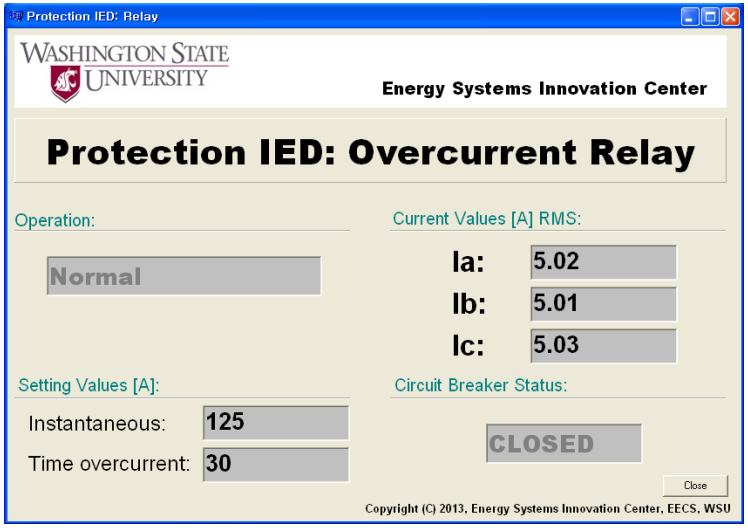


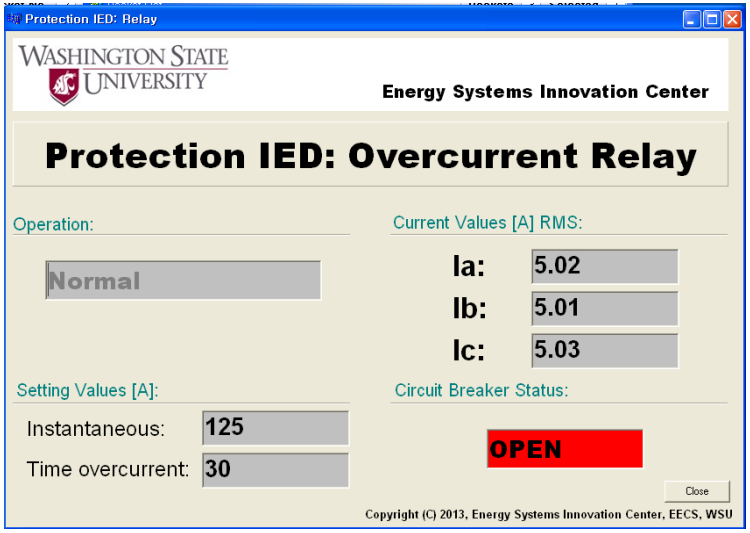
Sequential attacks with ADS

HMI

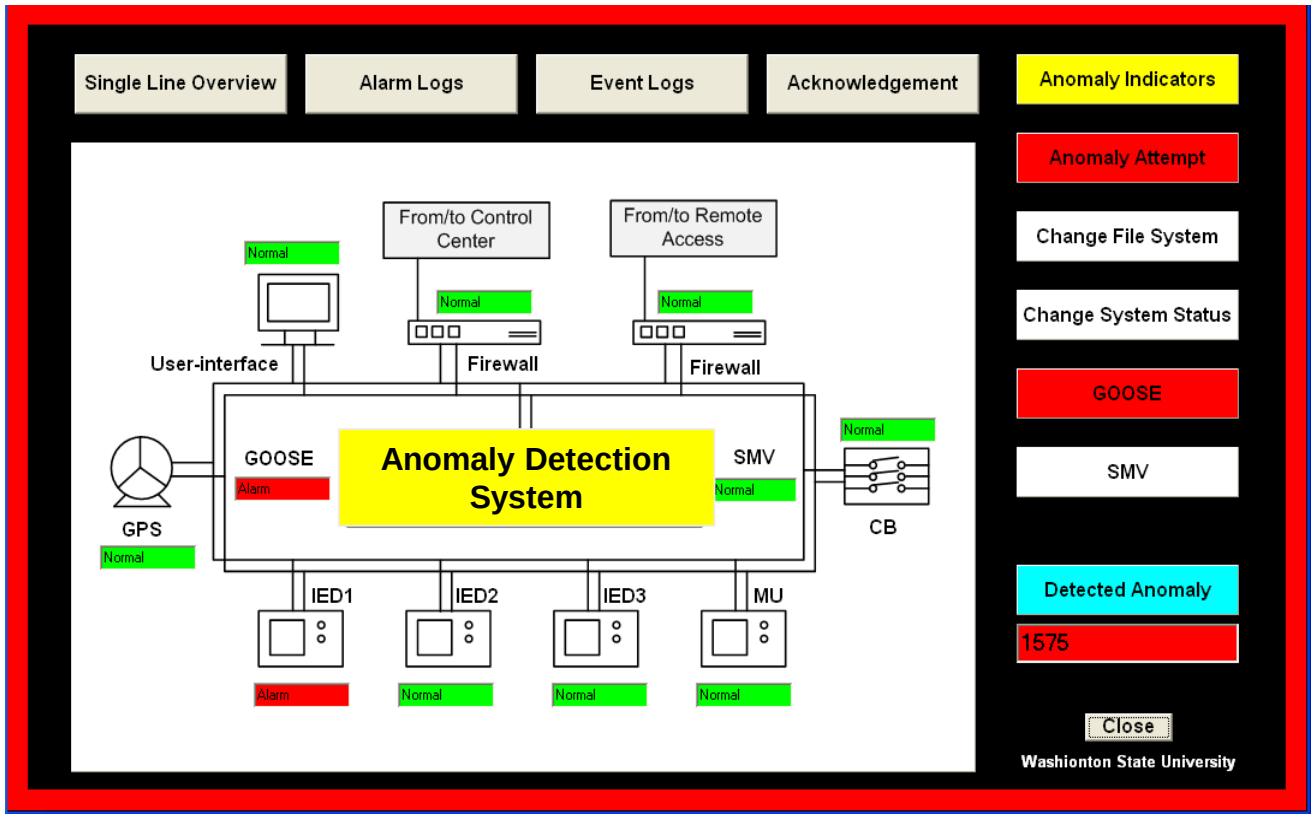

Protection IED: Relay
WASHINGTON STATE UNIVERSITY
Energy Systems Innovation Center
Protection IED: Circuit Breaker
Relay Status:
Normal
Status:
Ia: Closed
Ib: Closed
Ic: Closed
Circuit Breaker Status:
CLOSED
Close
Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU


Protection IED: Relay
WASHINGTON STATE UNIVERSITY
Energy Systems Innovation Center
Protection IED: Circuit Breaker
Relay Status:
Alarm
Status:
Ia: open
Ib: open
Ic: open
Circuit Breaker Status:
OPEN
Close
Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU

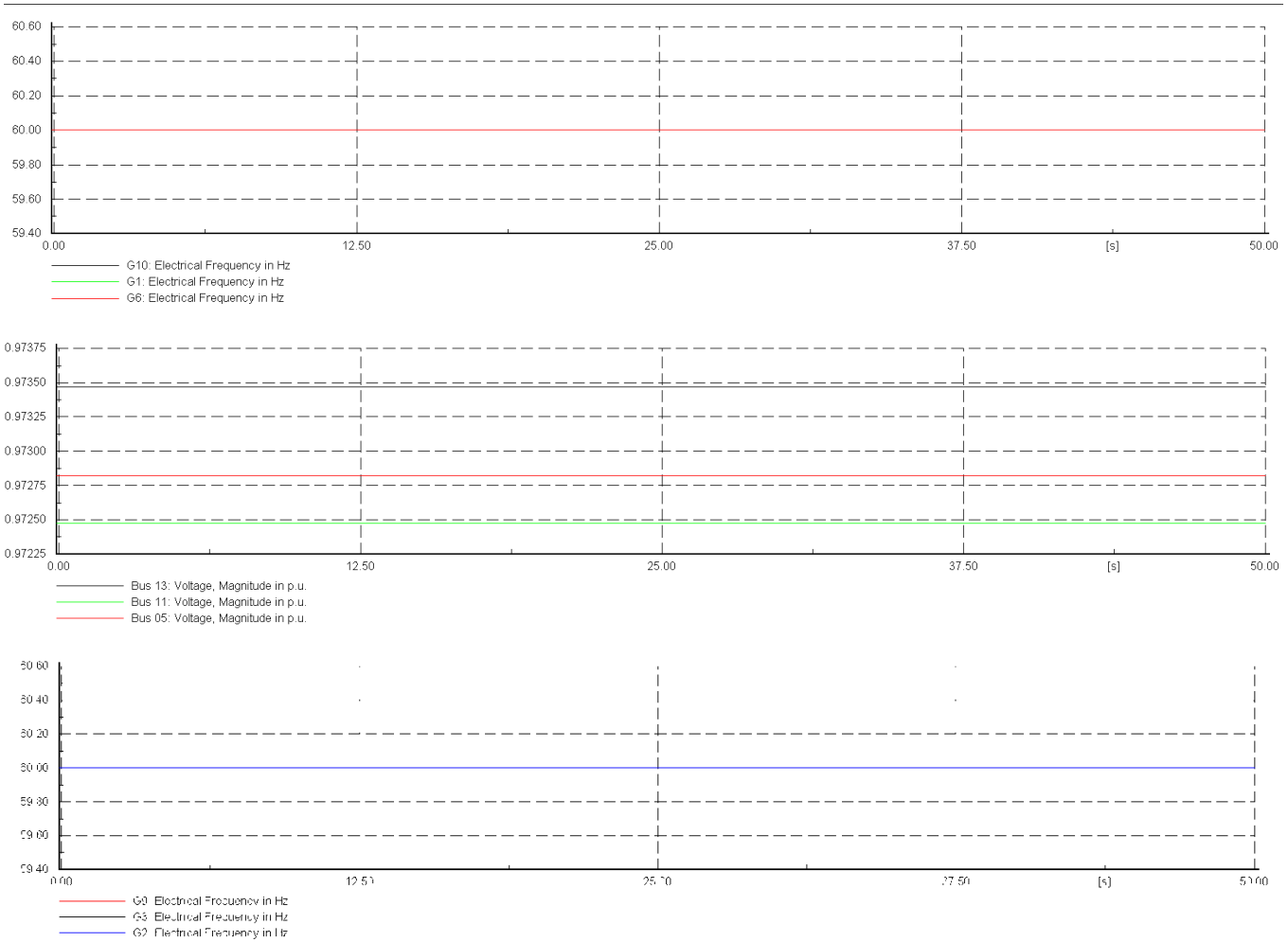

Protection IED: Relay
WASHINGTON STATE UNIVERSITY
Energy Systems Innovation Center
Protection IED: Overcurrent Relay
Operation:
Normal
Current Values [A] RMS:
Ia: 5.02
Ib: 5.01
Ic: 5.03
Setting Values [A]:
Instantaneous: 125
Time overcurrent: 30
Circuit Breaker Status:
CLOSED
Close
Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU


Protection IED: Relay
WASHINGTON STATE UNIVERSITY
Energy Systems Innovation Center
Protection IED: Overcurrent Relay
Operation:
Normal
Current Values [A] RMS:
Ia: 5.02
Ib: 5.01
Ic: 5.03
Setting Values [A]:
Instantaneous: 125
Time overcurrent: 30
Circuit Breaker Status:
OPEN
Close
Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU

HMI

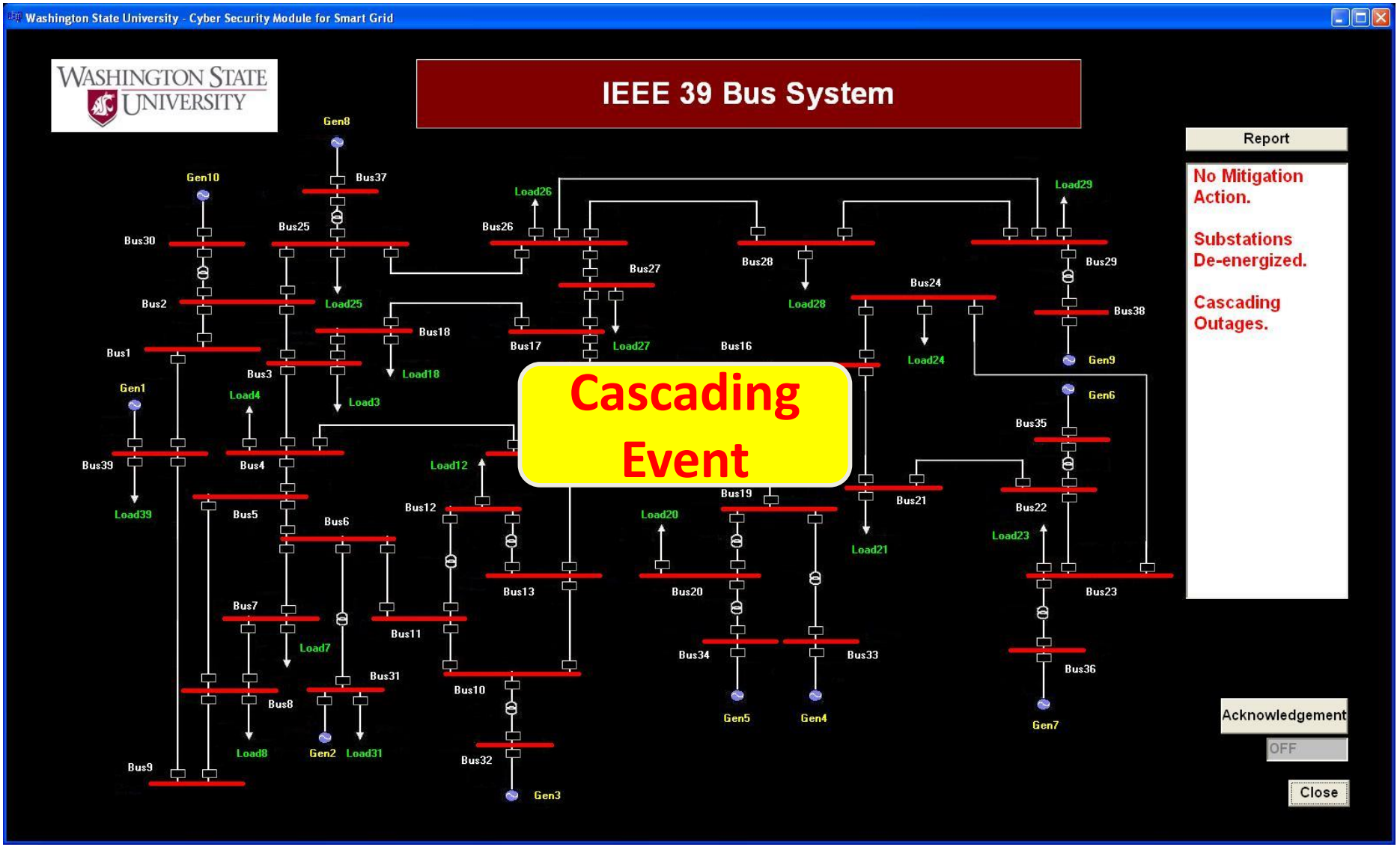

Single Line Overview
Alarm Logs
Event Logs
Acknowledgement
Anomaly Indicators
Anomaly Attempt
Change File System
Change System Status
GOOSE
SMV
From/to Control Center
From/to Remote Access
Normal
Normal
Normal
User-interface
Firewall
Firewall
Normal
GOOSE
Alarm
Anomaly Detection System
SMV
Normal
GPS
Normal
CB
IED1
IED2
IED3
MU
Alarm
Normal
Normal
Normal
Detected Anomaly
1575
Close
Washionton State University

IEEE 39 Bus System (DIgSILENT)

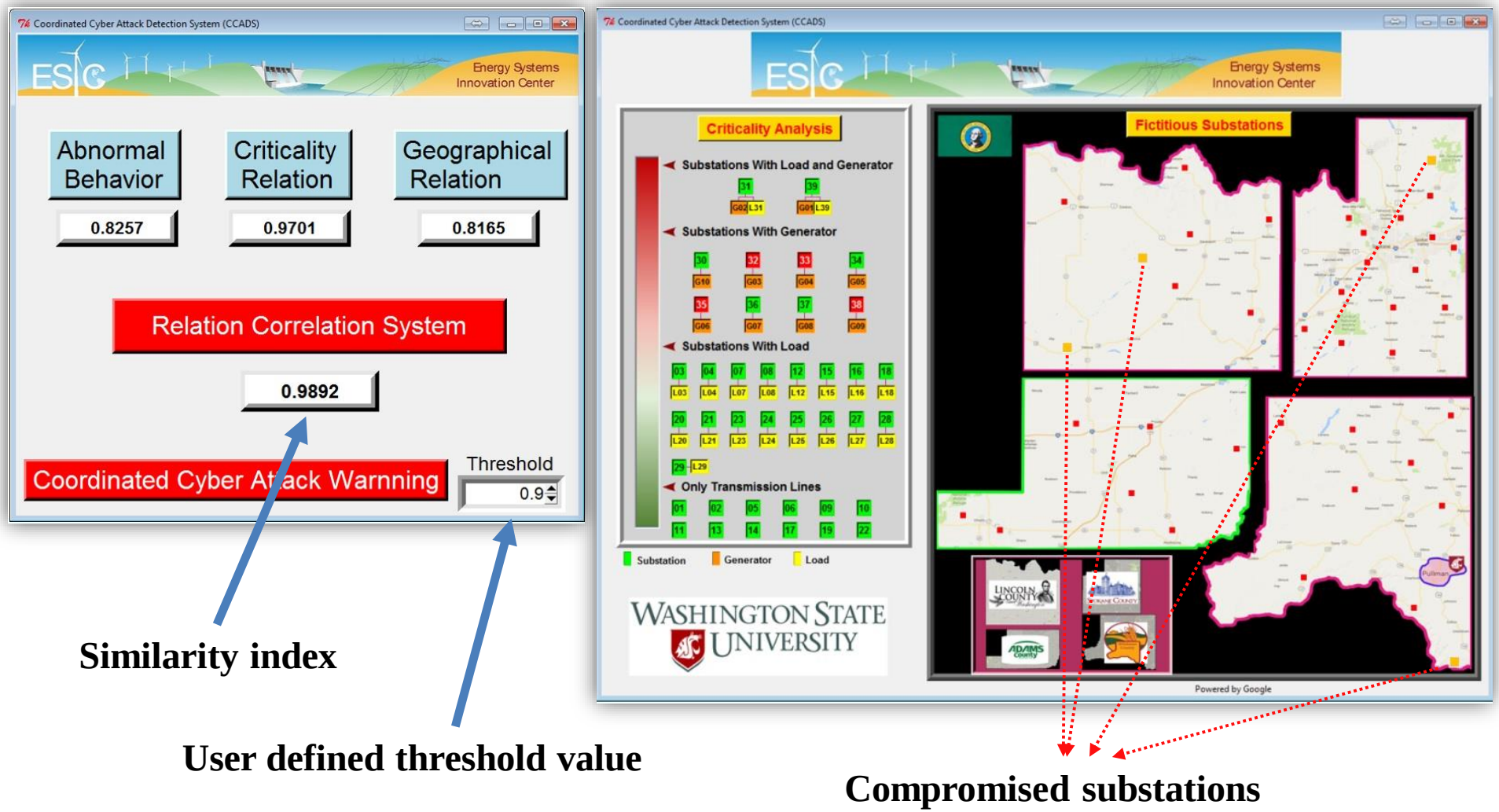


With ADS - Normal

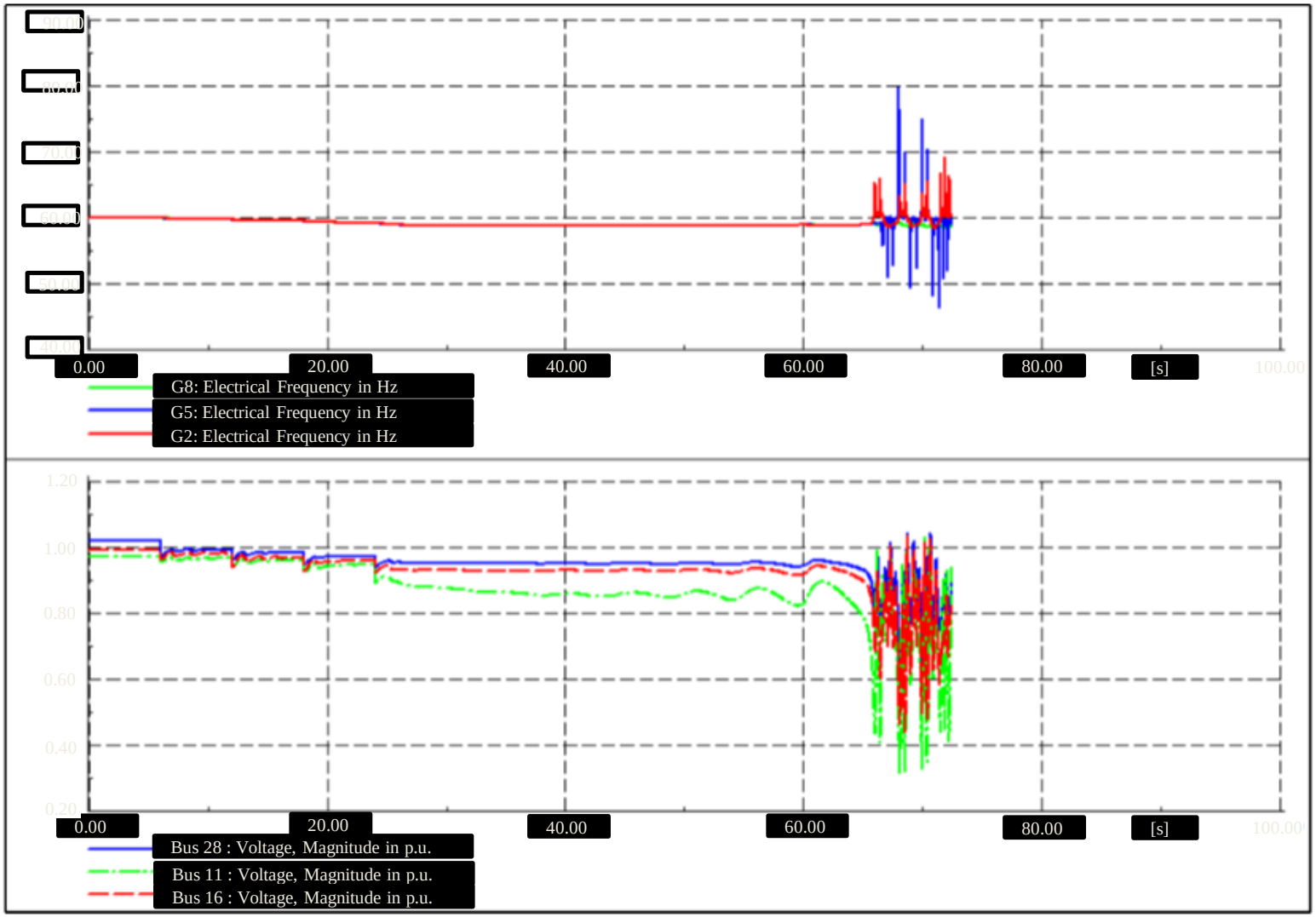
Coordinated Cyber Attack



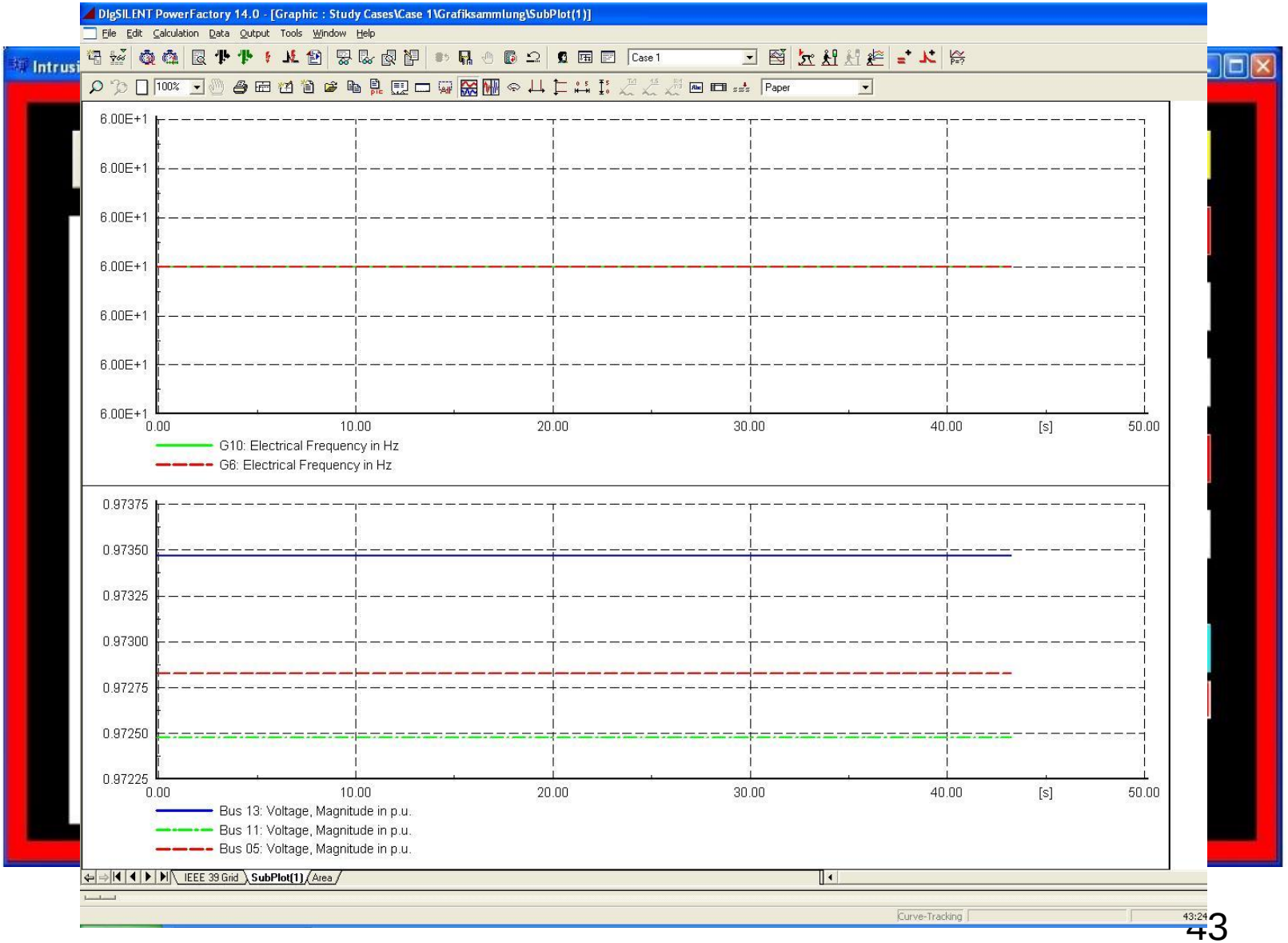
GUI of CCADS


Coordinated Cyber Attack Detection System (CCADS)
Energy Systems Innovation Center
Abnormal Behavior
Criticality Relation
Geographical Relation
0.8257
0.9701
0.8165
Relation Correlation System
0.9892
Coordinated Cyber Attack Warnning
Threshold
0.9
Criticality Analysis
Substations With Load and Generator
Substations With Generator
Substations With Load
Only Transmission Lines
Substation
Generator
Load
WASHINGTON STATE UNIVERSITY
Fictitious Substations
Powered by Google
Similarity index
User defined threshold value
Compromised substations

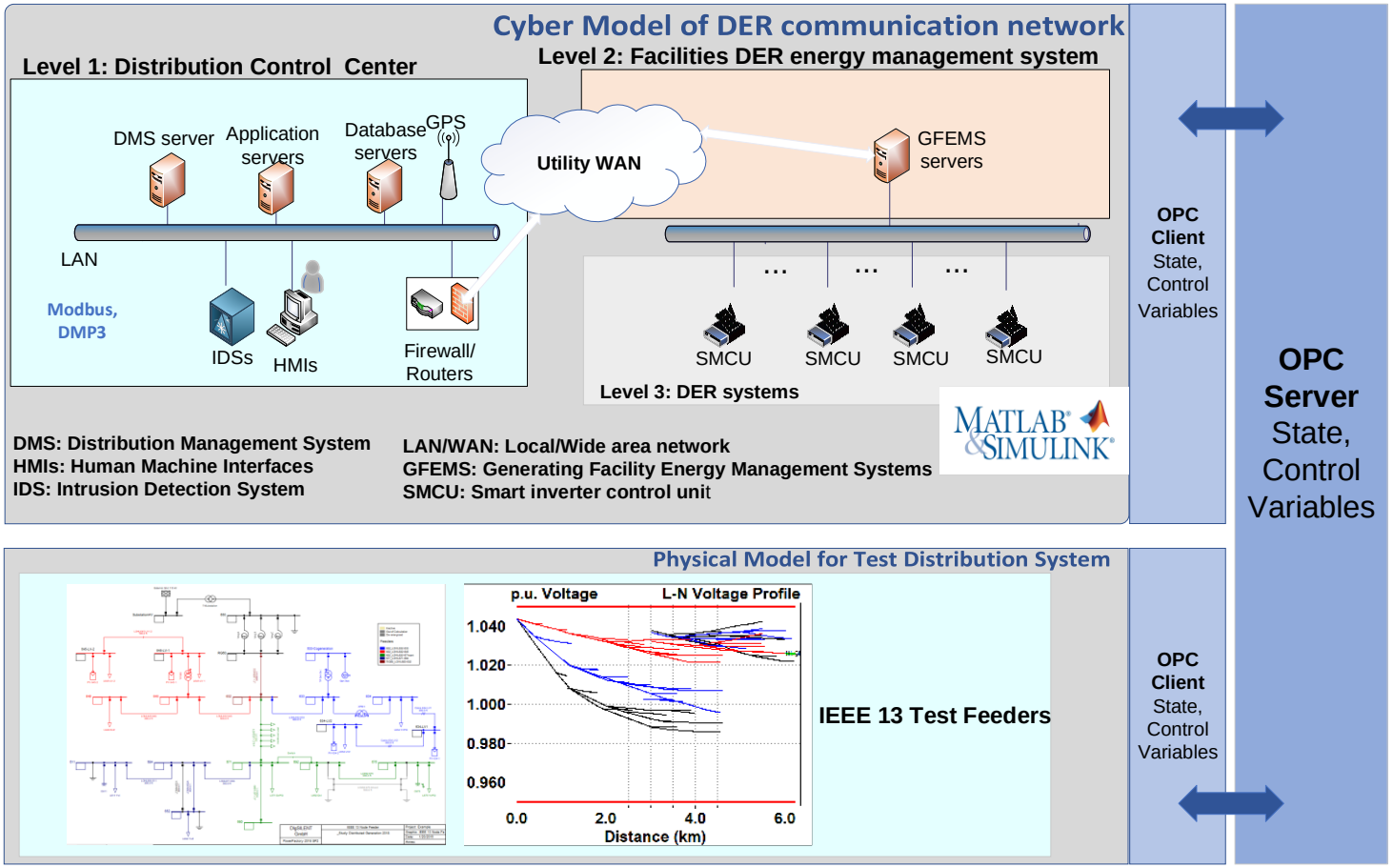
Simulation of Power System



Intrusion Detection System



PV Smart Inverter Cyber Physical System Simulation Environment



Cyber system: DER communication network

Queue based cyber system model is developed by using MATLAB Simulink

Physical system: IEEE 13 Test Feeders

DIgSILENT PowerFactory real time power system simulator

Connection:

OPC server with embedded OPC clients in both physical system and cyber system

Flooding Attack
Targeting on Smart Inverters on IEEE 13-Node Feeder

Unknown Connection

Multiple Connections /Reconnections

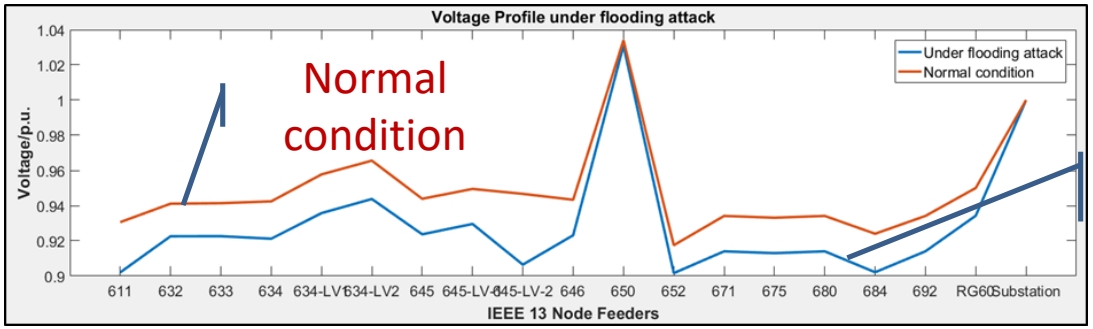
Flooding attack with dummy packets

Heavy network traffic

Inaccessibility of smart inverters

Disconnection between distribution control center and SMCU

Under voltage event: synchronized machine connected to feeder 633 is tripped



Under flooding attack

Anomaly Events Sequence	Attack route sets from Dictionary	Edit Manipulations of Anomaly Event Sequence	ED_{min}	ATS_{ind}
a→b→c→d→e→f	P_{1a}: a→b→d→e→f P_{1b}: a→c→d→e→f	Delete "c" Delete "b"	1 (min) 1 (min)	0.833>0.7 (threshold V_{th})

Flooding attack is detected by IDS!

Further Information

[1] C. W. Ten, C. C. Liu, and M. Govindarasu, “Vulnerability Assessment of Cybersecurity for SCADA Systems,” *IEEE Trans. Power Systems*, Nov. 2008, pp. 1836-1846.
[2] C. W. Ten, J. Hong, and C. C. Liu, “Anomaly Detection for Cybersecurity of the Substations,” *IEEE Trans. Smart Grid*, Dec 2011.
[3] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, “Intruders in the Grid,” *IEEE Power and Energy Magazine*, Jan/Feb 2012.
[4] C. C. Liu, A. Stefanov, J. Hong, "Cyber Vulnerability and Mitigation Studies Using a SCADA Testbed,“ *IEEE Power and Energy Magazine,* Jan. 2012.
[5] J. Hong, C. C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," *IEEE Trans. Smart Grid*, July 2014.
[6] A. Stefanov, C. C. Liu, and M. Govindarasu, "Modeling and Vulnerability Assessment of Integrated Cyber-Power Systems," *Int. Transactions on Electrical Energy Systems*, Vol. 25, No. 3, March 2015.
[7] J. Xie, C. C. Liu, M. Sforna, M. Bilek, and R. Hamza, "On Line Physical Security Monitoring of Power Substations, *Int. Trans. Electrical Energy Systems*, June 2016.
[8] C. C. Sun, A. Hahn, and C. C. Liu, “Cyber Security of a Power Grid: State-of-the-Art,” *Int. J. Electrical and Power and Energy Systems*, pp. 45-56, 2018.
[9] Y. Chen, J. Hong, and C. C. Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations," *IEEE Trans. Smart Grid*, July 2018.
[10] J. Hong and C. C. Liu, "Intelligent Electronic Devices with Collaborative Intrusion Detection Systems," *IEEE Trans. Smart Grid,* Jan 2019.
[11] C. C. Sun, R. Zhu, and C. C. Liu, “Cyber Attack and Defense for Smart Inverters in a Distribution System,” CIGRE Symposium, Study Committee D2, Helsinki, Finland, June 2019.
[12] S. K. Khaitan, J. D. McCalley, and C. C. Liu (Co-Editors), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Springer, 2015.