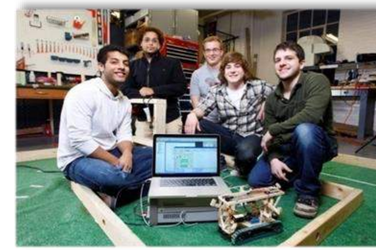
# *Cyber-Physical System Security of the Power Grid*

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

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

# Bradley Dept. of Electrical & Computer Engineering

- Tenured/tenure-track faculty: 79
- Students: 1,400 BS; 210 MS; 350 PhD
- Graduates: 54 PhDs; 130 MS/MEng; 267 BS awarded past academic year
- Ranked 10th for research expenditures by NSF
- Fellows: IEEE 31; other societies 9
- National Academy of Engineering (NAE): 4
- NSF CAREER Awards: 20; DoD YIP Awards: 6; Sloan Research Fellow: 1
- US News & World Report rankings
  - Graduate programs (2018): EE 18th ; CPE 17th
  - Undergraduate programs (2017): EE 13th ; CPE 15th



# ECE Locations

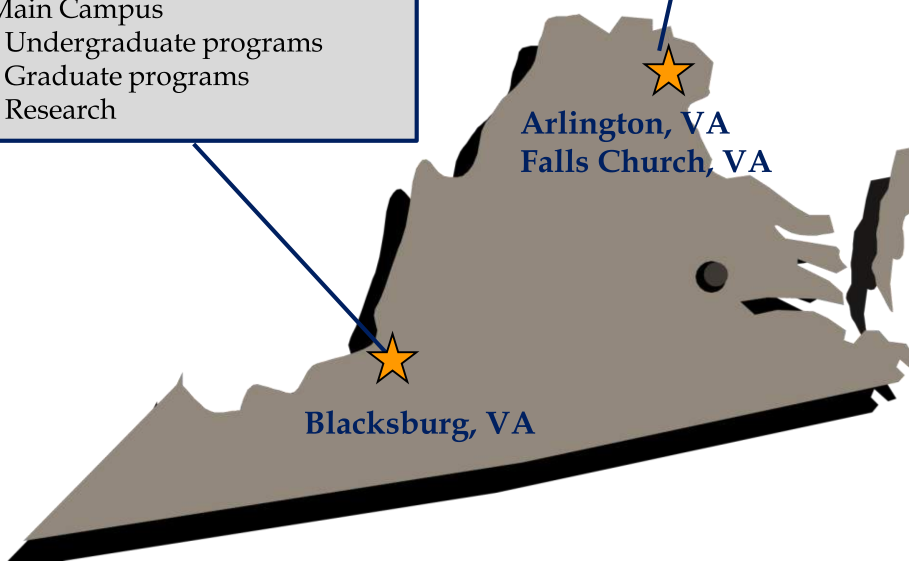
Whittemore Hall

Durham Hall

Torgersen Hall

Main Campus
- Undergraduate programs
- Graduate programs
- Research

12 faculty at National Capital Region
- Primarily graduate programs
- Research




VT Research Center (Arlington)

Northern Virginia Center (Falls Church)

# 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

# CPE Core Faculty

**Chen-Ching Liu**
Director & AEP Professor
- Distribution systems, cyber security of the grid
- Industry software for system restoration: EPRI (T), PNNL (D)

**Jaime De La Ree**
Associate Professor &
Assistant Dept. Head

**Lamine M. Mili**
Professor (NVC)

**Mona Ghassemi**
Assistant Professor

**Robert Broadwater**
Professor

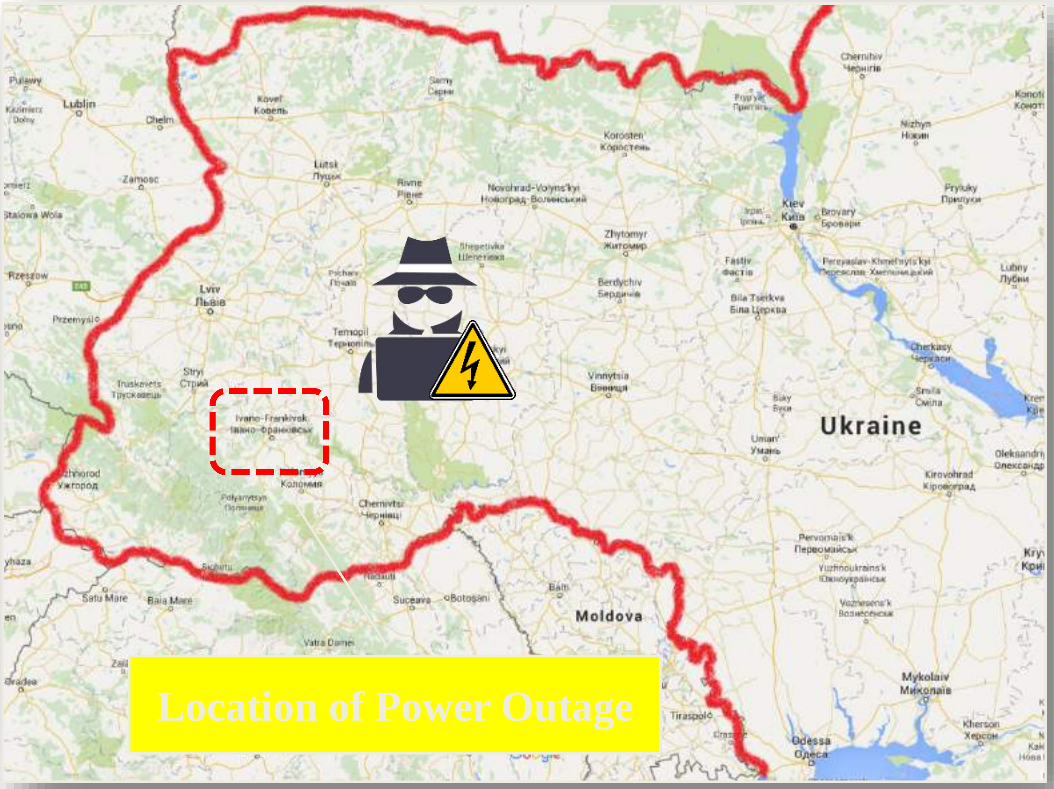
**Saifur Rahman**
Joseph Loring Professor (VT-ARC)
- Energy efficiency and sensor integration
- DoE BEMOSS Platform; President of IEEE PES

**Vassilis Kekatos**
Assistant Professor
- *Optimization and learning of smart grids*

**Virgilio A. Centeno**
Associate Professor

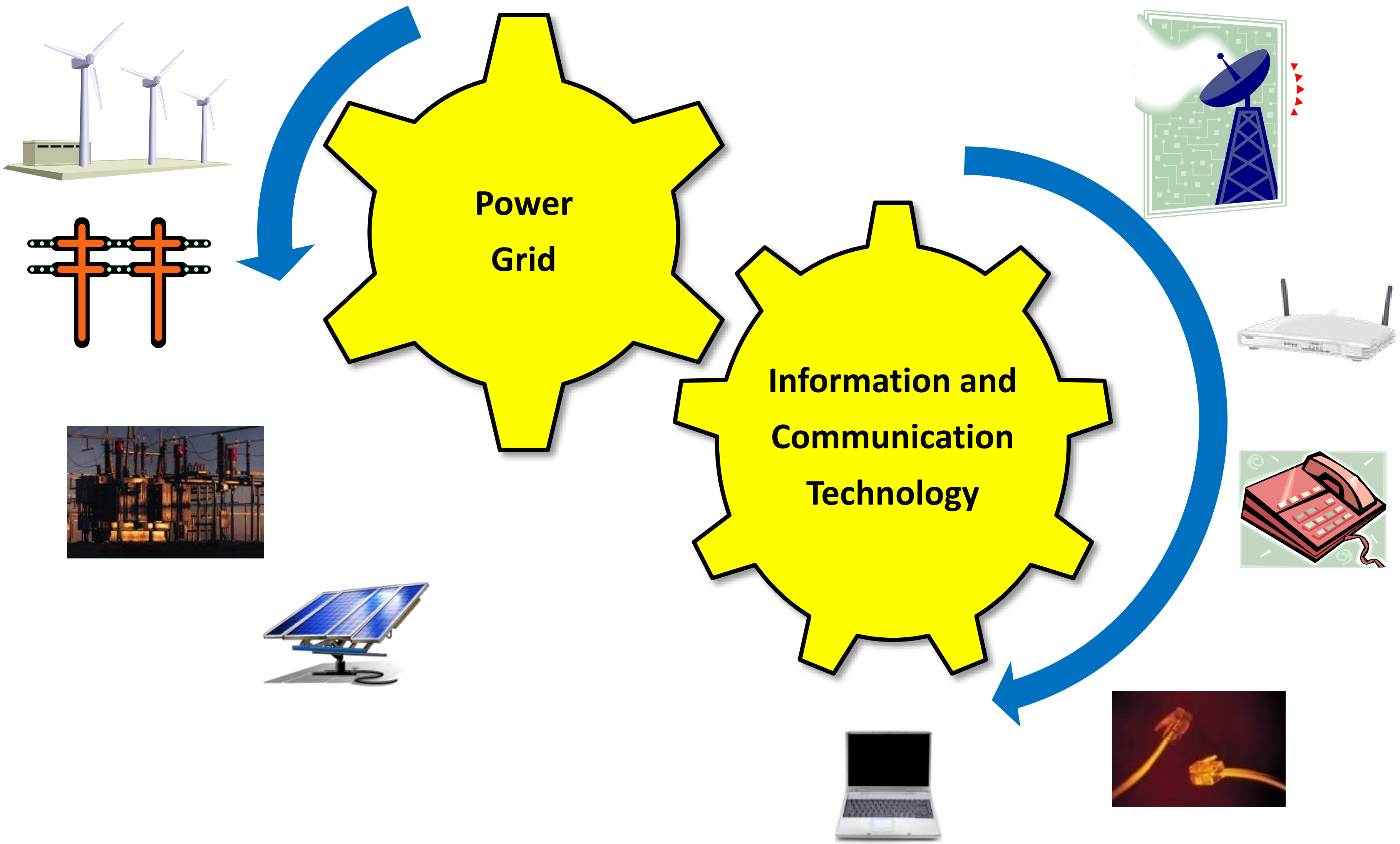
# Cyber Attack in Ukraine’s Power System

- **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

# Power Grid with ICT



# 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

# Access Points in Control Networks

- Virtual Private Network (VPN)
- Dial-up Networks
- Wireless Networks
- Any Remote Logon Programs
- Backdoor Access - Trojan Horse

# Intrusion Tools

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

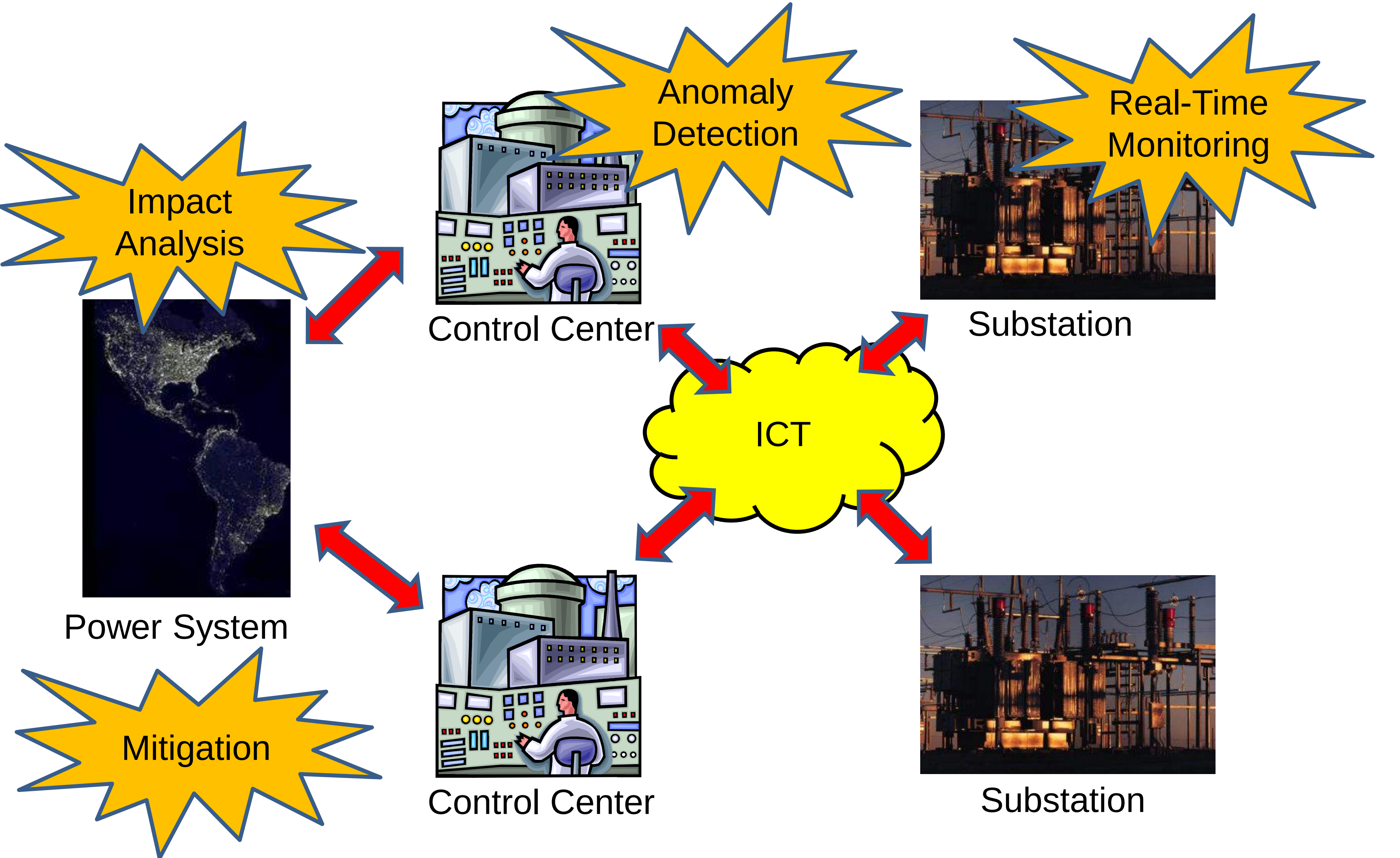
# Supervisory Control And Data Acquisition (SCADA)

| | 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 |

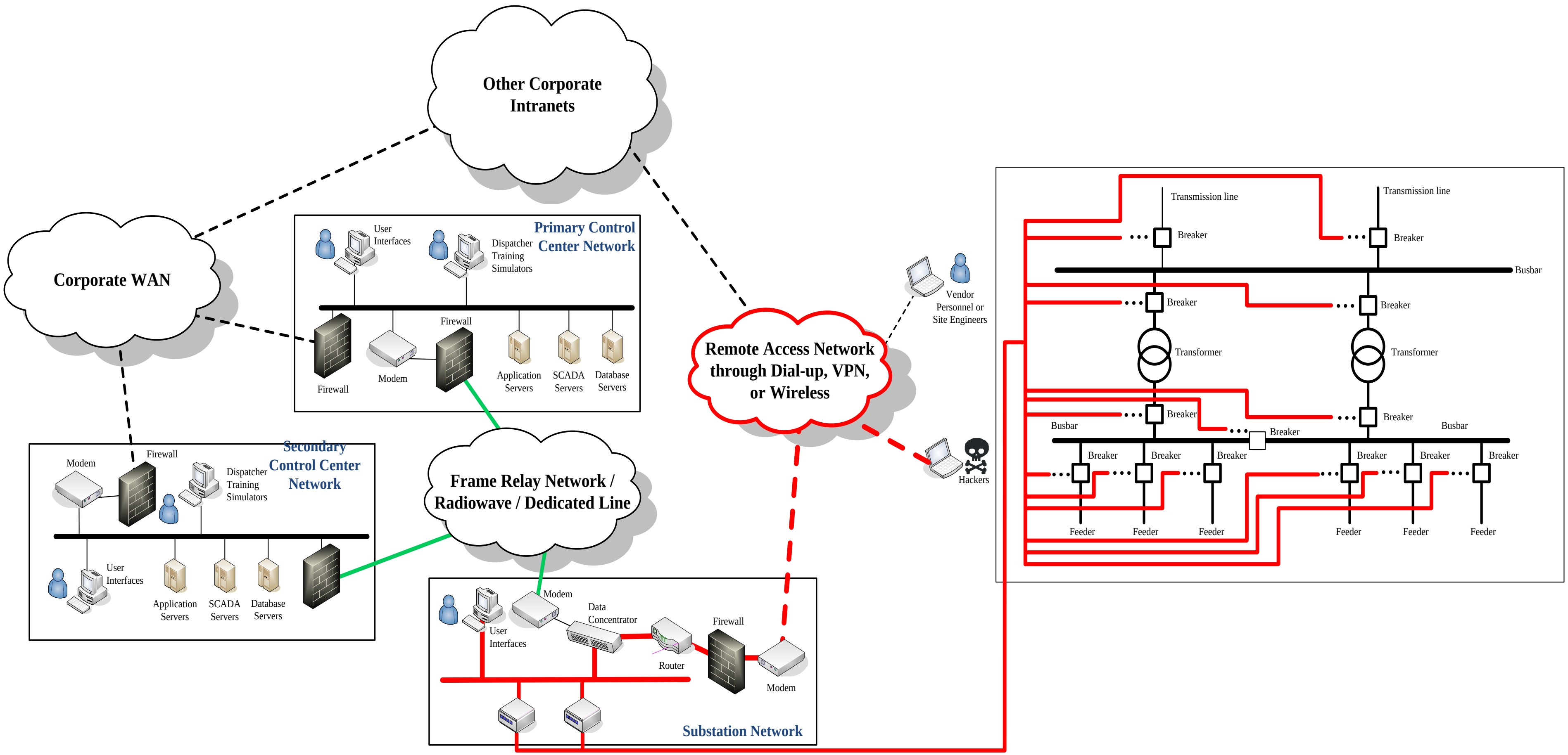
# Cyber Security Standards NERC CIP 002-009

- 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)

# Cyber Security Monitoring



# 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

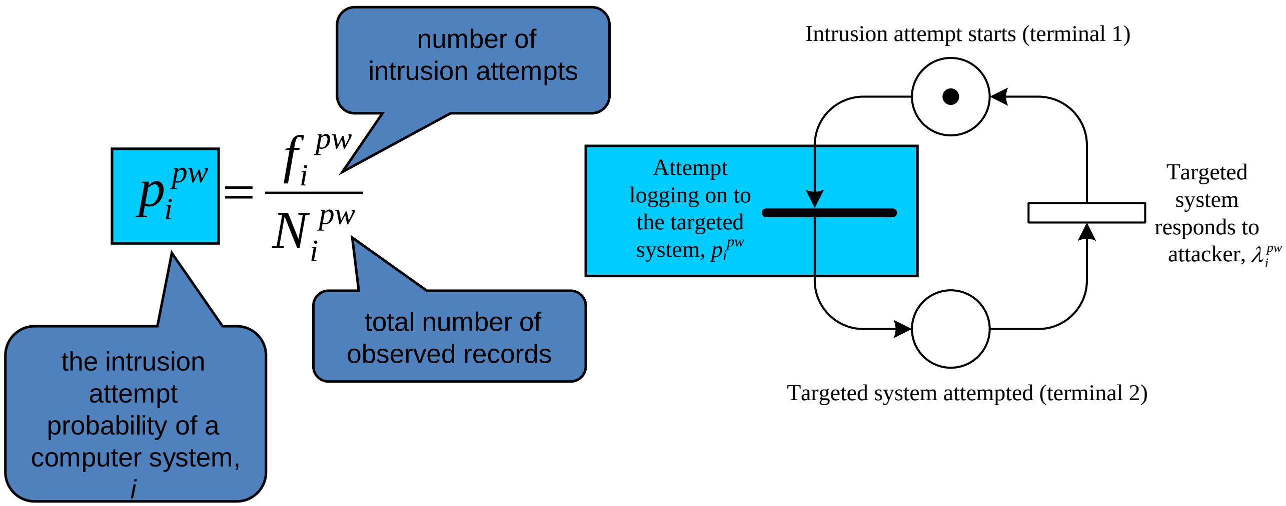
- Access point provides the port services to establish a connection for an intruder to penetrate SCADA computer systems
- Vulnerability of a scenario i, V(i), through an access point is evaluated to determine its potential damage
- Scenario vulnerability - weighted sum of the potential damages over the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

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

where $\pi_j$ 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

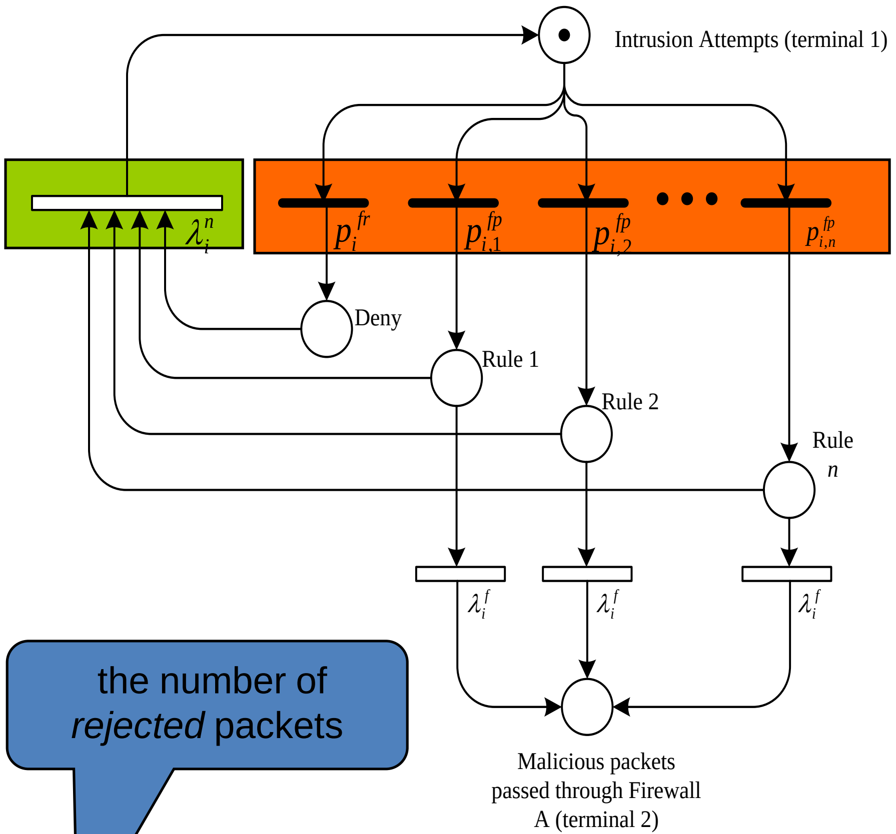
# Password Model

- Intrusion attempt to a machine
  - A solid bar - transition probability
  - An empty bar - processing execution rate that responds to the attacker
- Account lockout feature, with a limited number of attempts, can be simulated by initiating the N tokens (password policy threshold).



# 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.



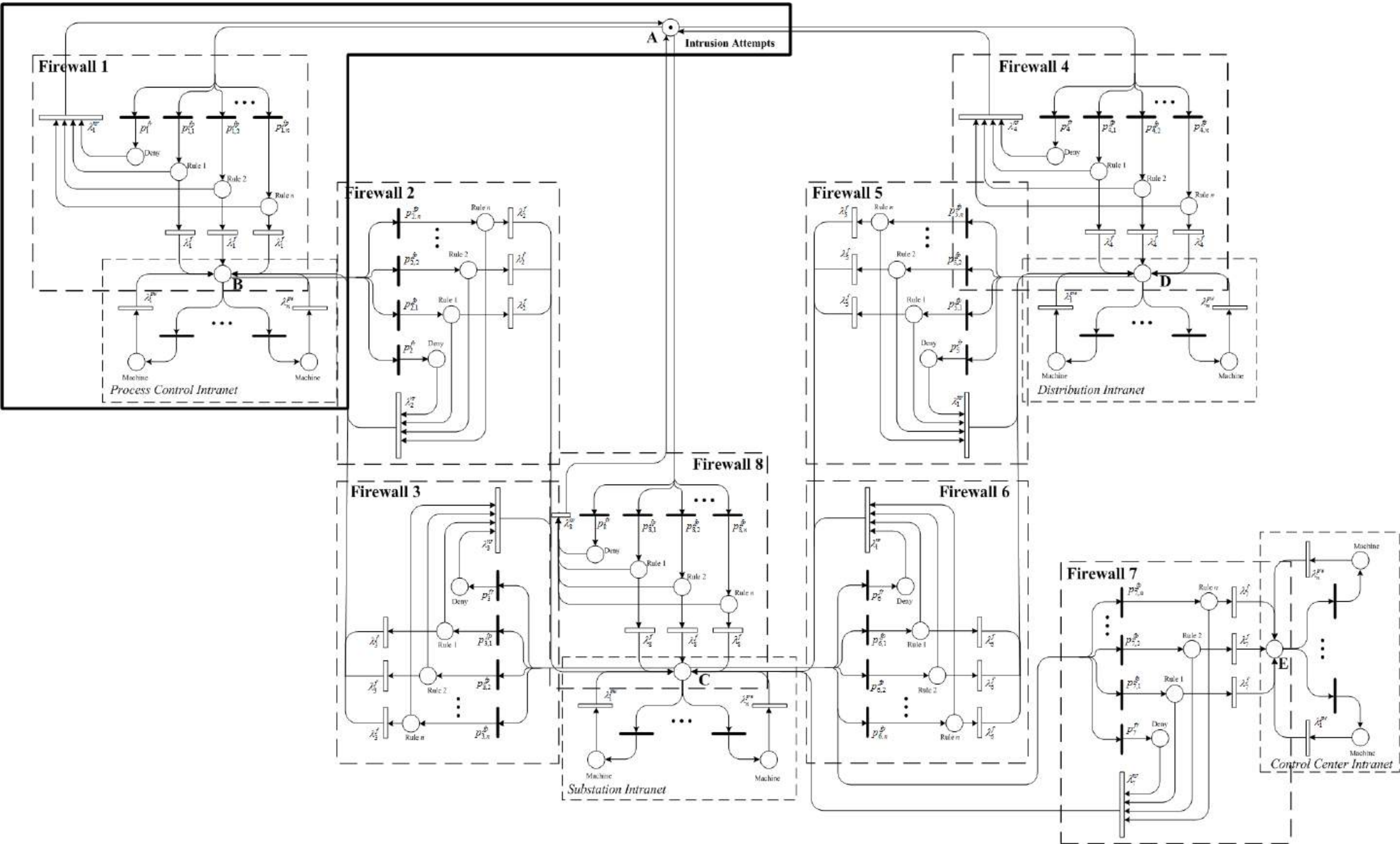

$$p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}$$

- $p_{i,j}^{fp}$: probability of malicious packets traveling through a firewall rule
- $f_{i,j}^{fp}$: denotes the frequency of malicious packets through the firewall rule
- $N_{i,j}^{fp}$: total record of firewall rule *j*.

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

- $p_i^{fr}$: probability of the packets being *rejected*
- $f_i^{fr}$: the number of *rejected* packets
- $N_i^{fr}$: 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

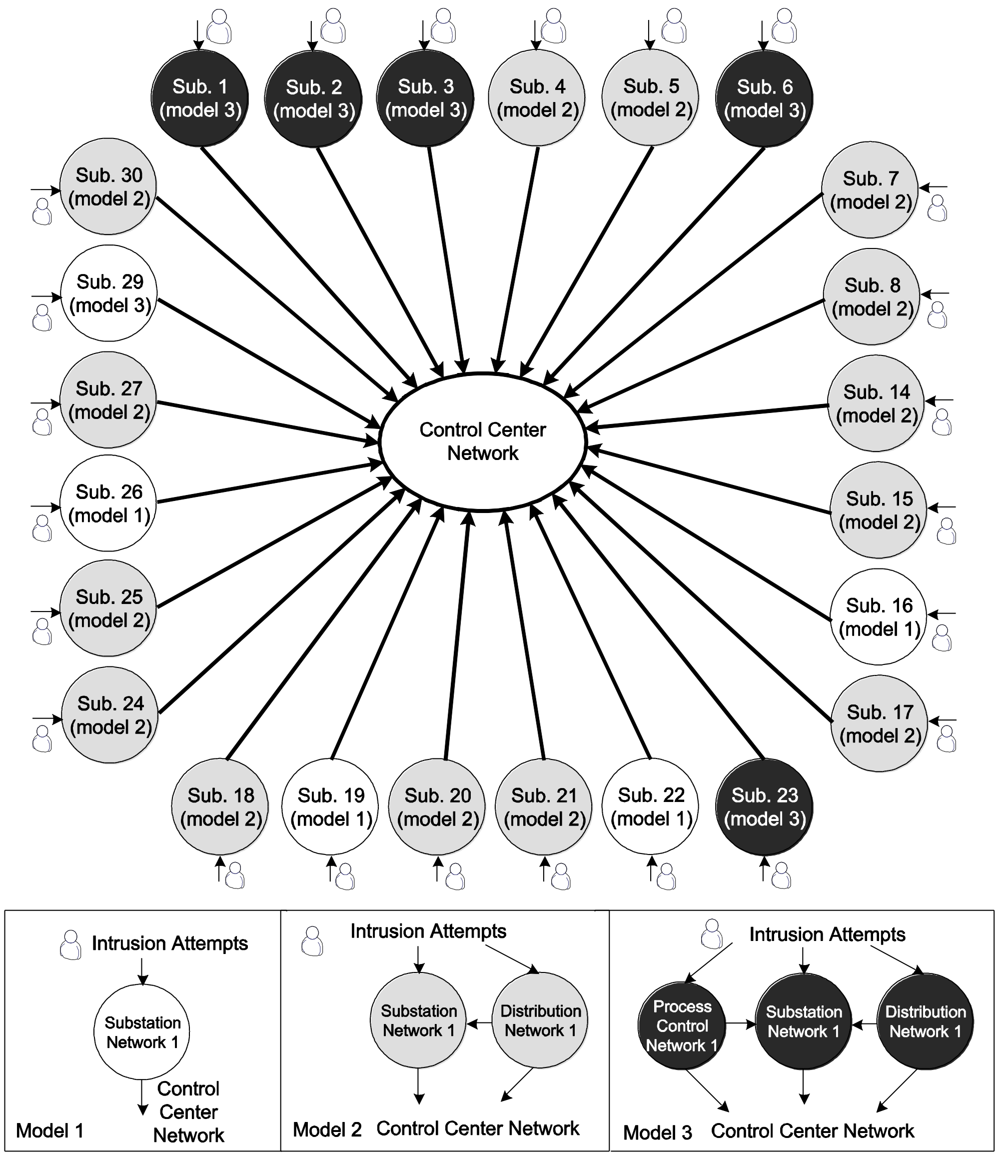
$$\gamma = \left( \frac{P_{LOL}}{P_{Total}} \right)^{L-1}$$

- 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)

# Impact Factor Evaluation for IEEE 30-Bus System

Impact Factor for Each Substation

| Sub. | Associated Buses | LOL(MW) | L | $\gamma$ |
|---|---|---|---|---|
| 1 | 1 | .3 | 2.5 | .0016 |
| 2 | 2 | 21.7 | 1.8 | .1769 |
| 3 | 3 | 2.4 | 2.5 | .0014 |
| 4 | 4, 12, 13 | 18.8 | 1.4 | .3971 |
| 5 | 5 | 0 | 2.5 | 0 |
| 6 | 6, 9, 10, 11 | 5.8 | 1 | 1 |
| 7 | 7 | 22.8 | 2.8 | .0222 |
| 8 | 8 | 30 | 3.6 | .0083 |
| 9 | 14 | 6.2 | 2.9 | .0015 |
| 10 | 15 | 8.2 | 3 | .0019 |
| 11 | 16 | 3.5 | 2.6 | .0017 |
| 12 | 17 | 9 | 2.9 | .0031 |
| 13 | 18 | 3.2 | 3.1 | .0002 |
| 14 | 19 | 9.5 | 2.9 | .0034 |
| 15 | 20 | 2.2 | 2.9 | .0002 |
| 16 | 21 | 17.5 | 2.6 | .0222 |
| 17 | 22 | 0 | 2.2 | 0 |
| 18 | 23 | 3.2 | 2.7 | .0010 |
| 19 | 24 | 8.7 | 2.9 | .0029 |
| 20 | 25 | 0 | 2.8 | 0 |
| 21 | 26 | 3.5 | 2.8 | .0008 |
| 22 | 27, 28 | 0 | 1 | 1 |
| 23 | 29 | 2.4 | 2.8 | .0004 |
| 24 | 30 | 10.6 | 2.8 | .0056 |



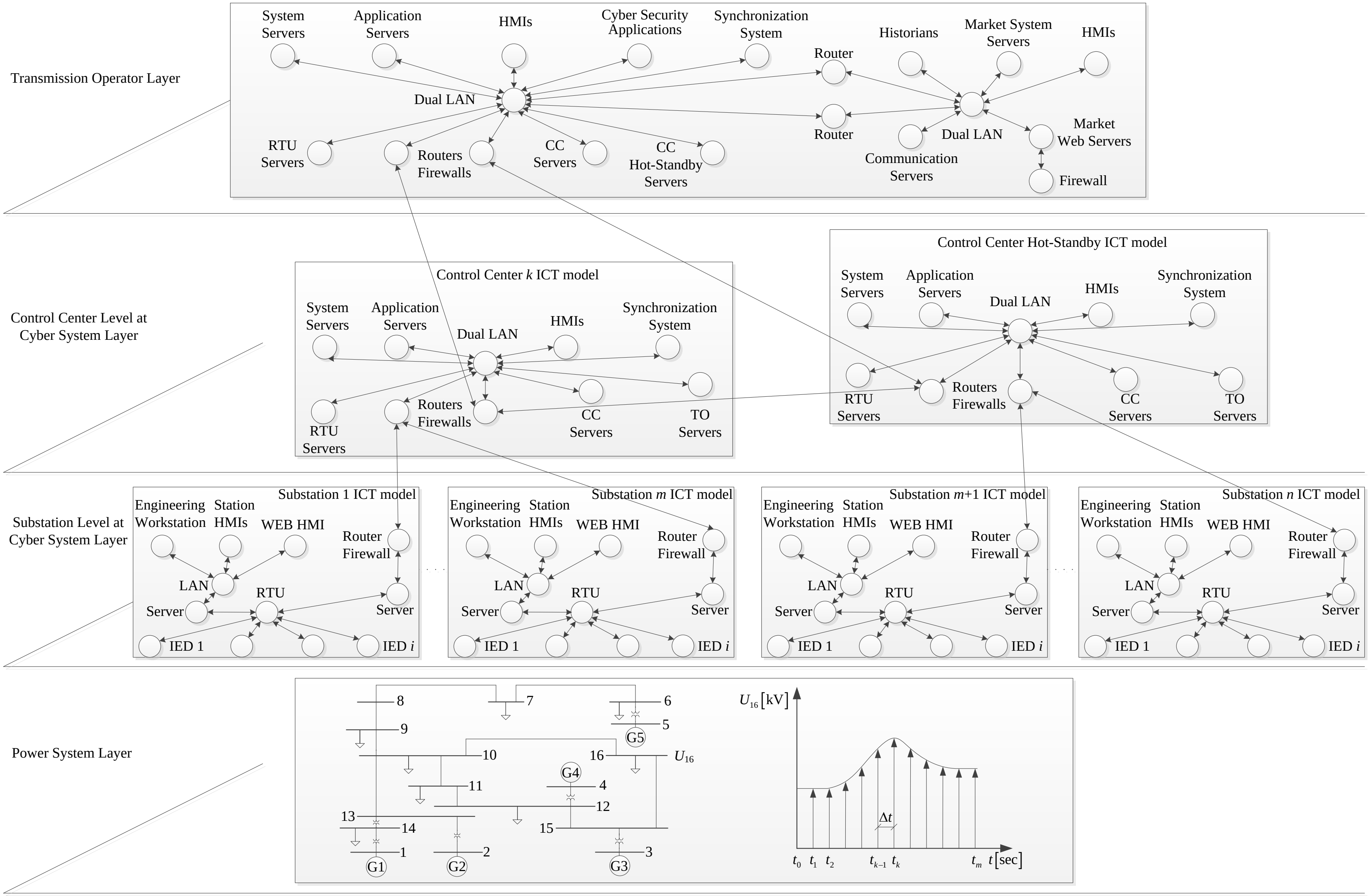
# Modeling Integrated Cyber-Power System

- **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

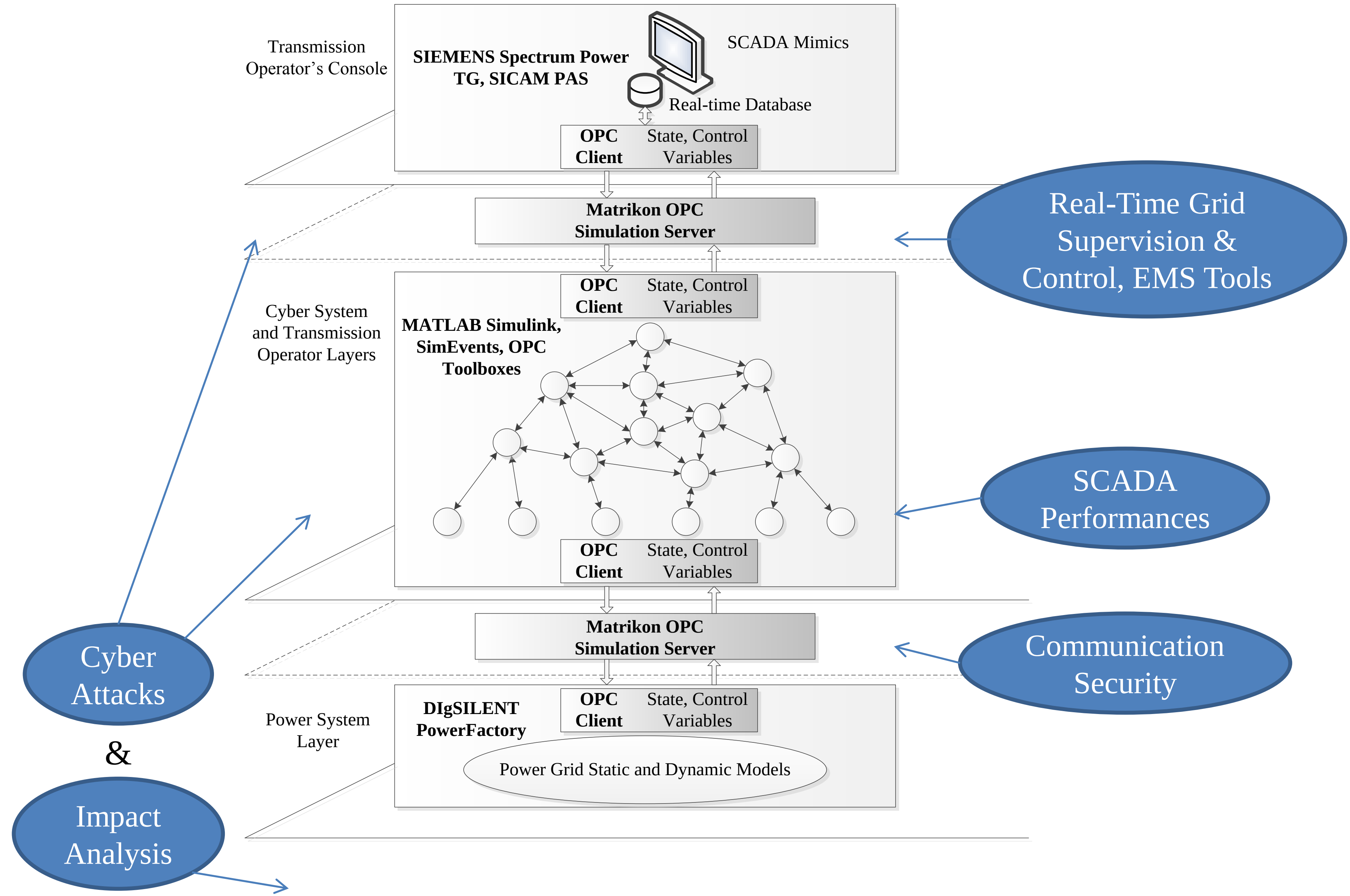
- **CPS tool used for assessment of SCADA communication performance**
  - Plan SCADA and ICT systems for power grids

- **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

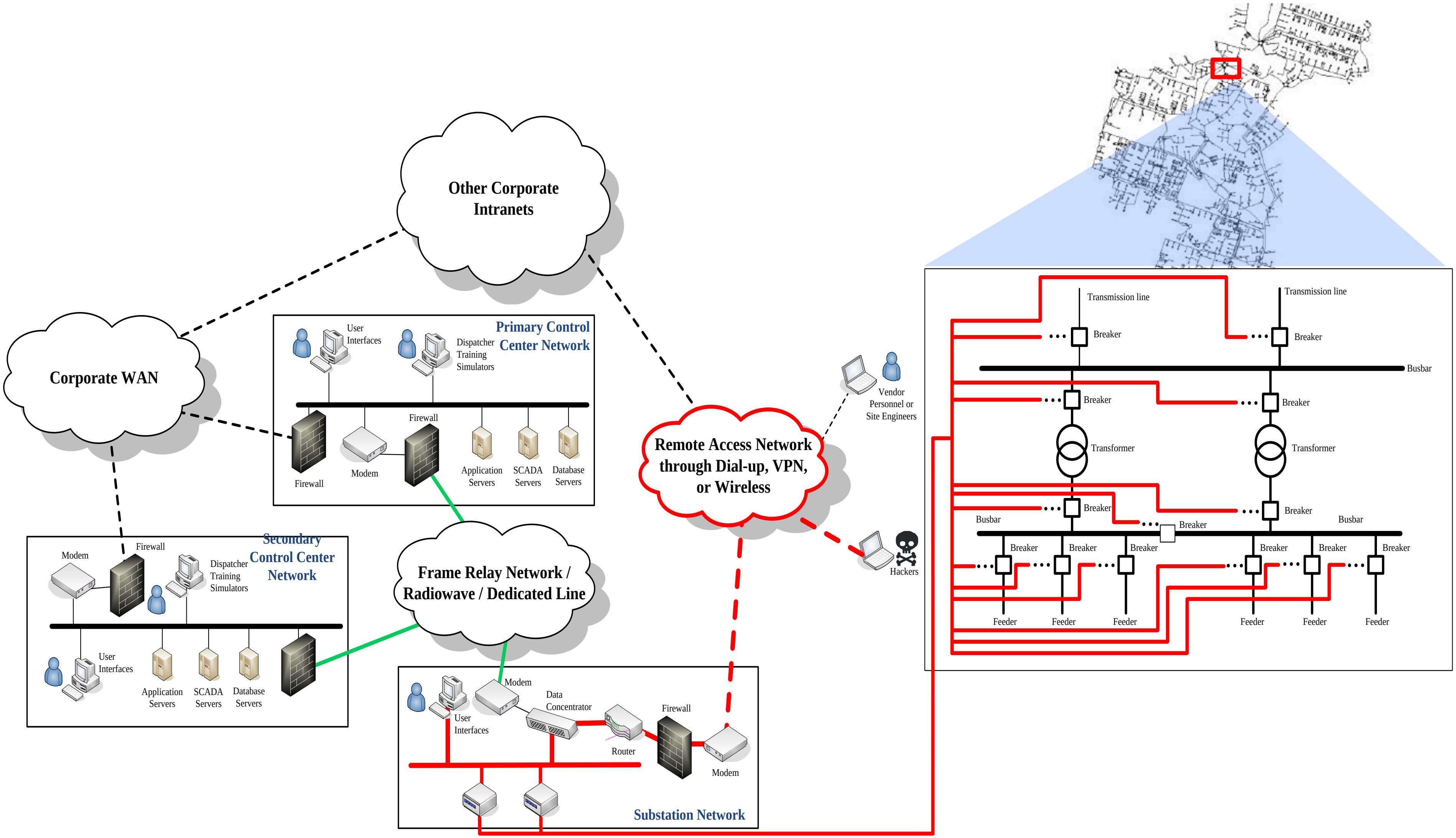
# Cyber-Physical System Model



# Cyber-Physical System Tool



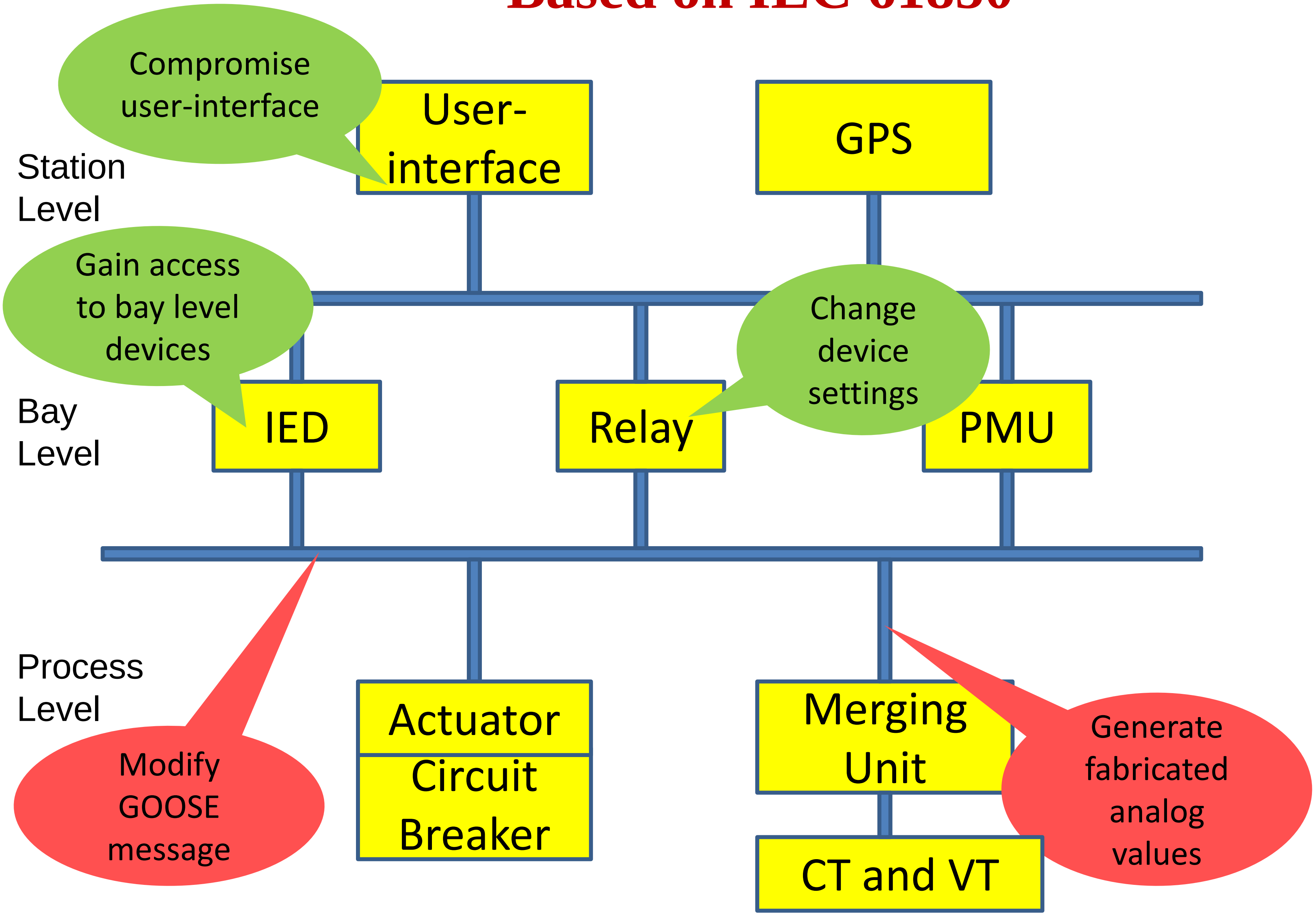
# Intrusion into a Substation Network



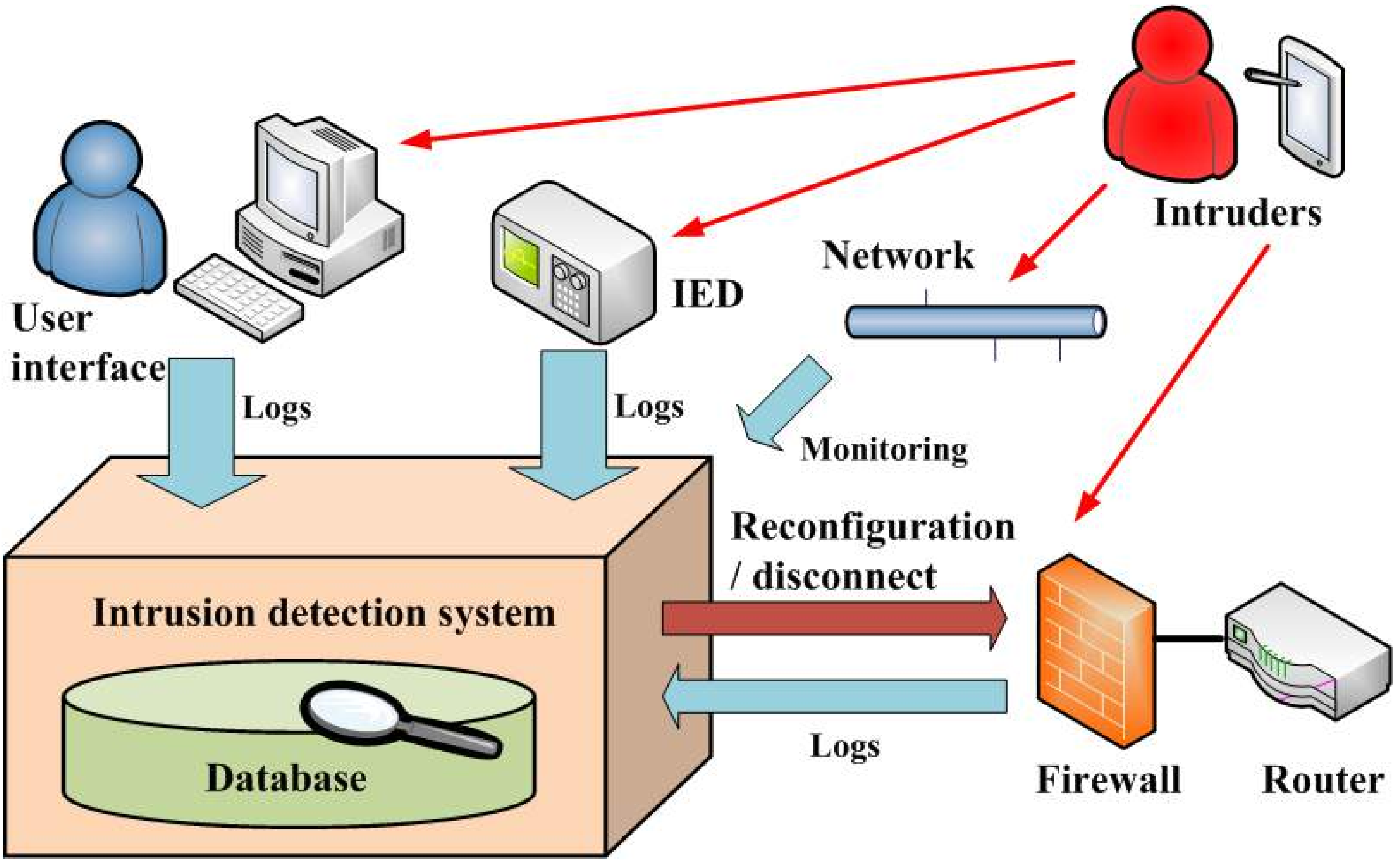
# Vulnerabilities of Substations

- Control centers rely on substations and communications to make decisions
- Substations are a critical infrastructure in the power grid (relays, IEDs, PMUs)
- Remote access to substation user interface or IEDs for maintenance purposes
- Unsecured standard protocol, remote controllable IED and unauthorized remote access
- Some IED and user-interface have available web servers and it may provide a remote access for configuration and control with default passwords
- Well coordinated cyber attacks can compromise more than one substation – it may become a multiple, cascaded sequence of events

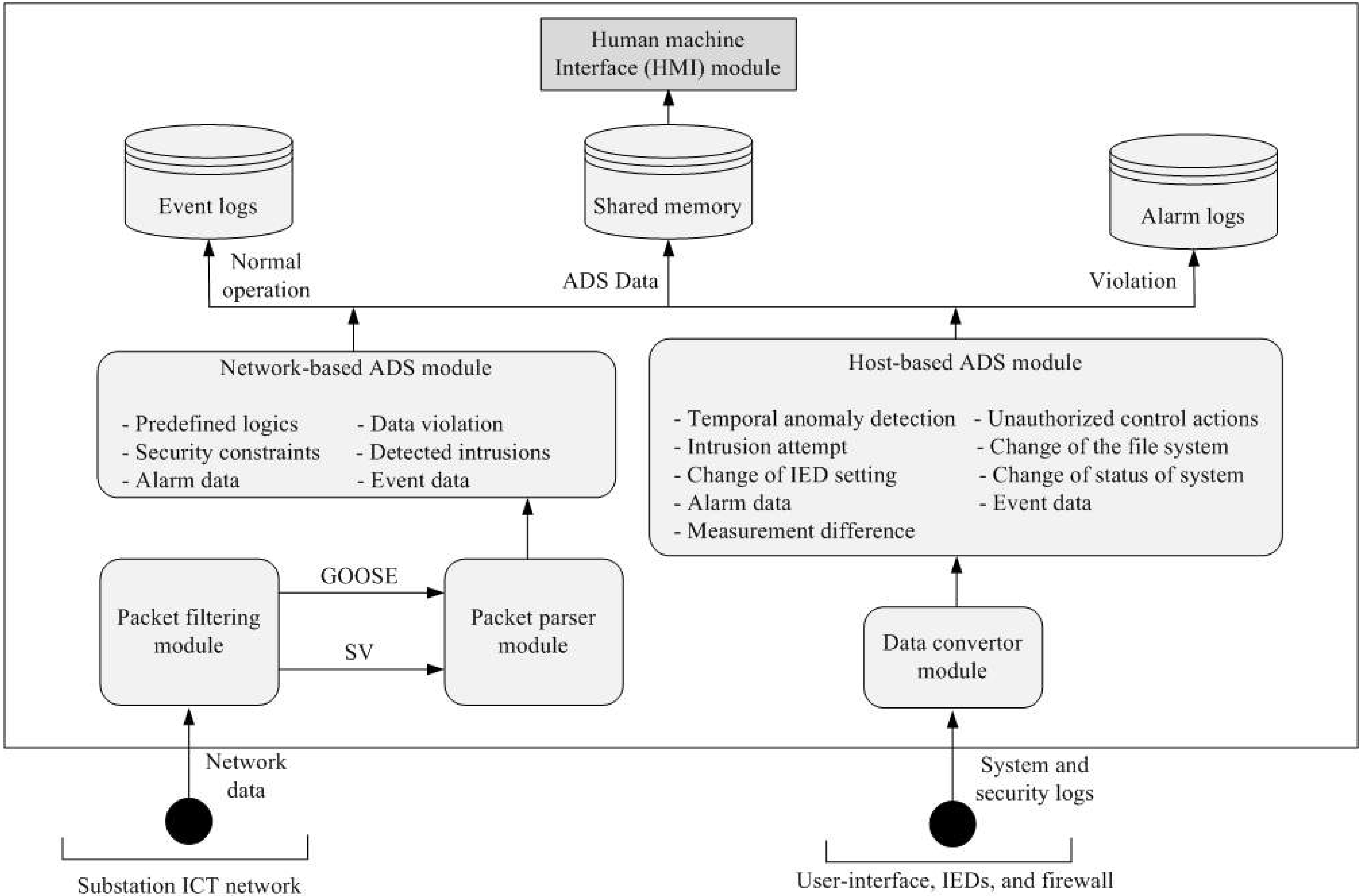
# Potential Threats in a Substation Based on IEC 61850



# 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

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

# Host-Based Anomaly Detection

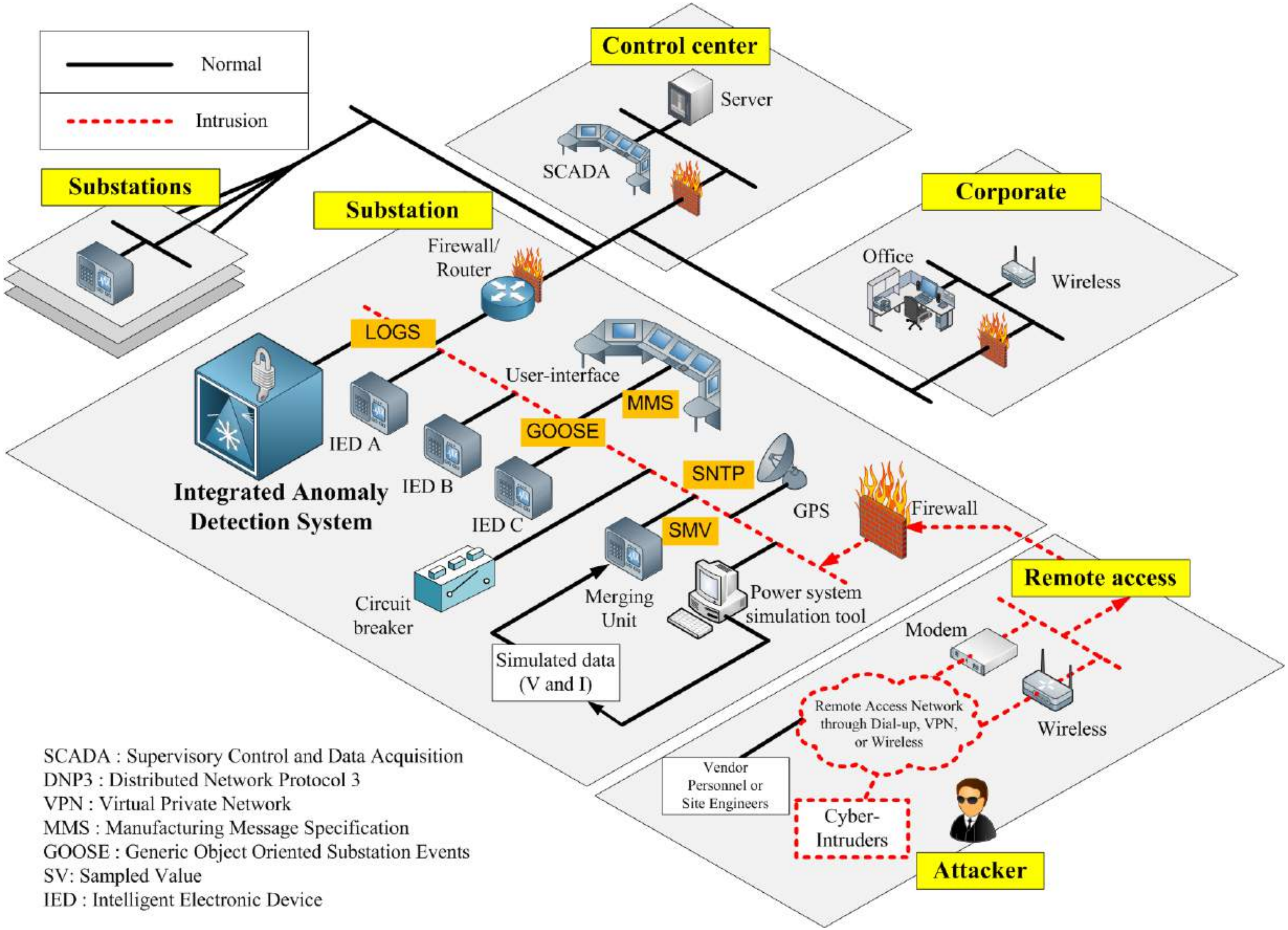
| Substation A | | | | |
|---|---|---|---|---|
| **o.** | **Date** | **Time** | **Contents** | **Issue** |
| 45 | 15.09.2013 | 10:28:33,560 | IED 1 | Wrong password attempt |
| 46 | 15.09.2013 | 10:35:43,159 | User-interface | Unauthorized file change |
| 47 | 15.09.2013 | 11:02:04,368 | IED 2 | Unauthorized setting change |
| 48 | 15.09.2013 | 11:03:14,270 | Transformer 1 | Unauthorized tap change |

Substation A

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

- At 10:20:000, there is no anomaly so t_1 is [0 0 0 0 0].
- At 10:30:000, ADS detects a wrong password attempt to IED 1 so t_2 is [1 0 0 0 0].
- At 10:40:000, ADS detects an unauthorized file change to the user-interface so t_3 is [1 1 0 0 0].
- At 10:50:000, there is no change so t_4 is [1 1 0 0 0].
- At 11:00:000, there is no change so t_5 is [1 1 0 0 0].
- At 11:10:000, ADS detects two anomalies, unauthorized setting change to IED 2 and unauthorized tap change to transformer 1 so t_6 is [1 1 1 1 0].
- At 11:20:000, there is no change so t_7 is [1 1 1 1 0].

# Substation Cyber Security Testbed



# Consequence of GOOSE Based Attack

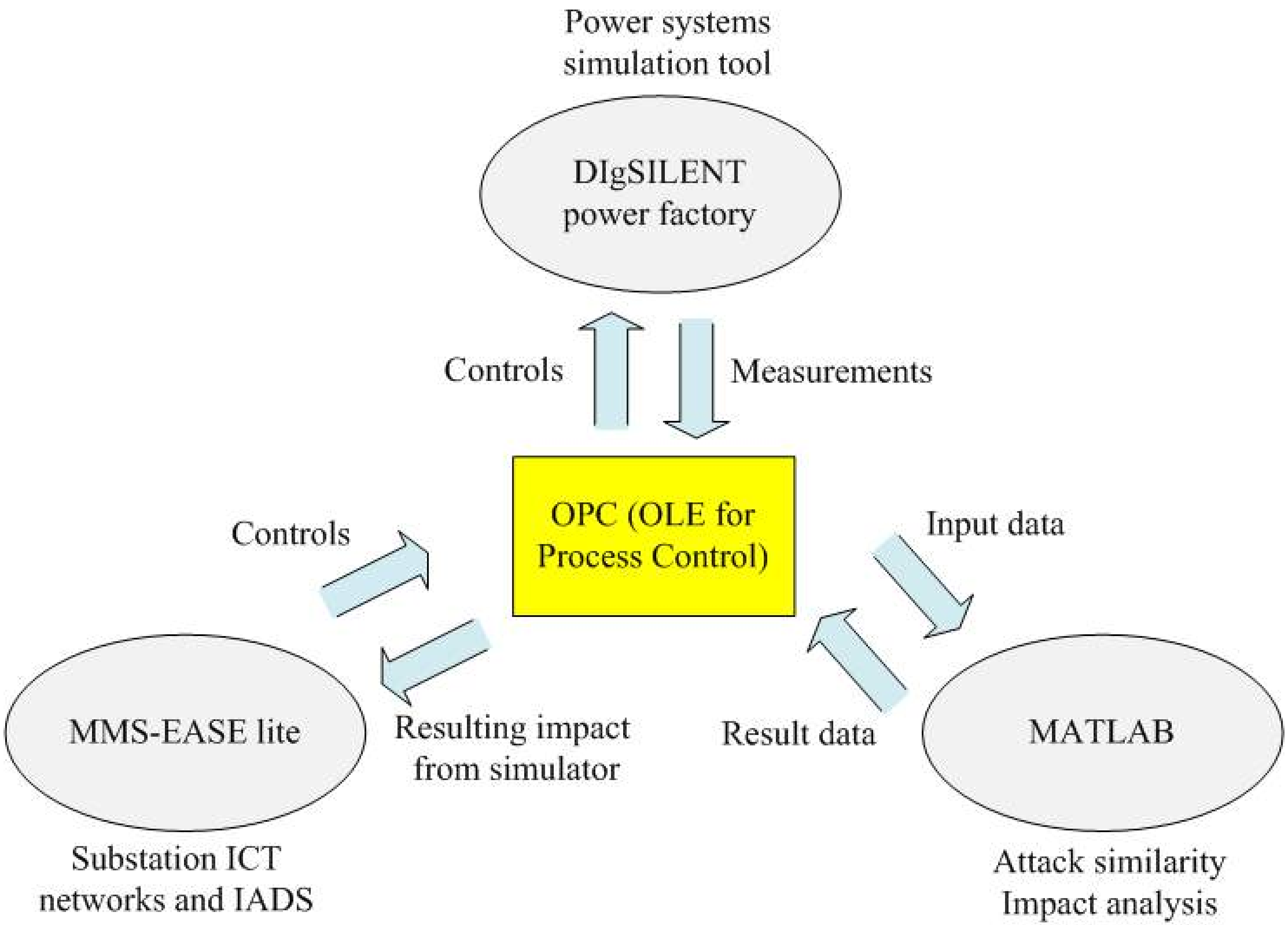
| Action | Result |
|---|---|
| Disconnect Ethernet cable from IED | Lost availability of IED |
| Send normal control | Open CB |
| Replay attack | Open CB |
| Modify sequence & state number | Warning occurred at CB |
| Modify transferred time | Warning occurred at CB |
| Modify GOOSE control data |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

# Consequence of SV Based Attack

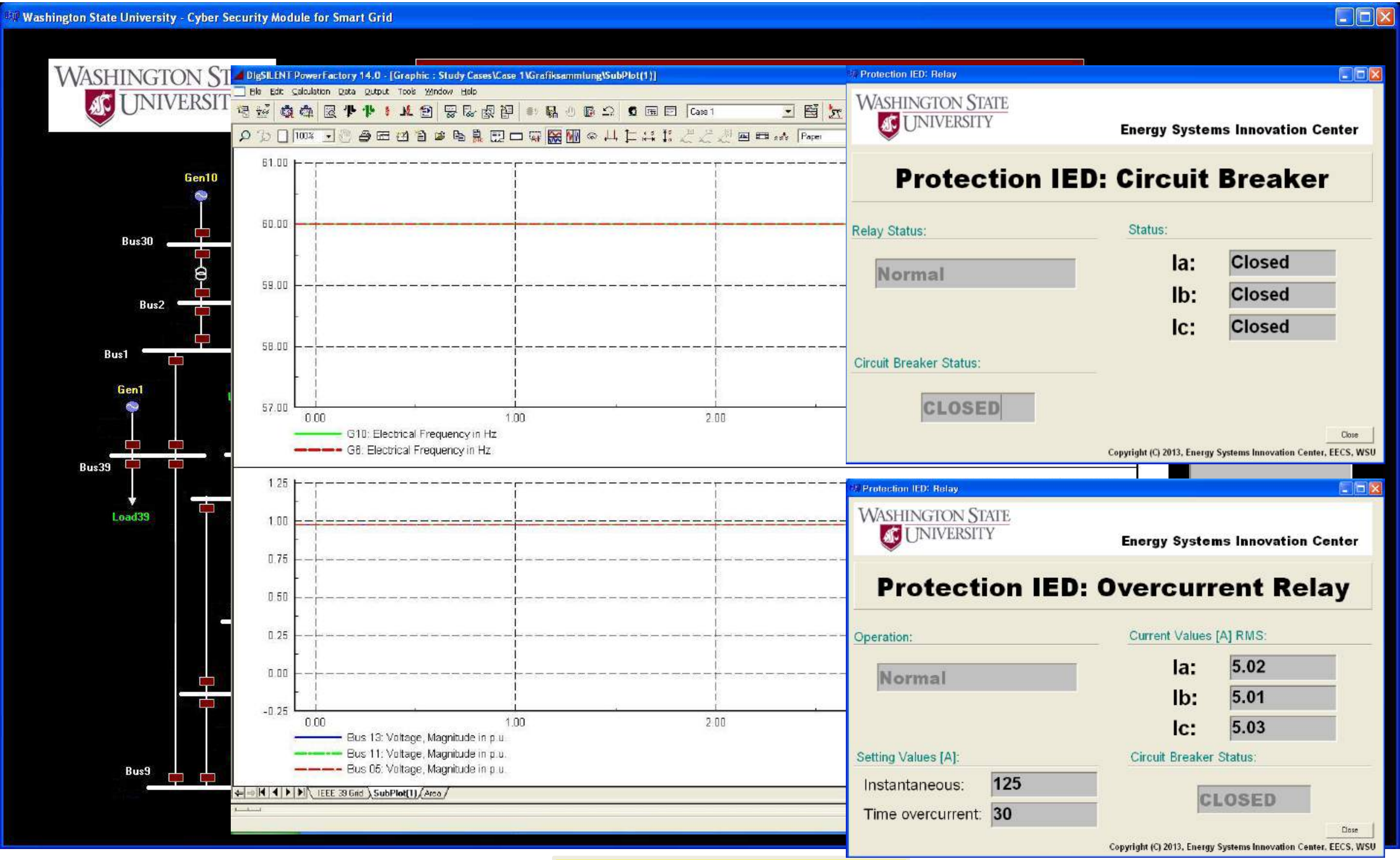
| Action | Result |
|---|---|
| Disconnect Ethernet cable from MU | Lost availability of MU |
| Increase measured values | Open CB |
| Replay attack | Open CB |
| Modify counter number | Warning occurred at IED |
| Modify SMV dataset | Warning occurred at IED |
| Denial of Service attack | Lost availability of IED |
| Generate SMV data | Open CB |

# *WSU Smart City Testbed*

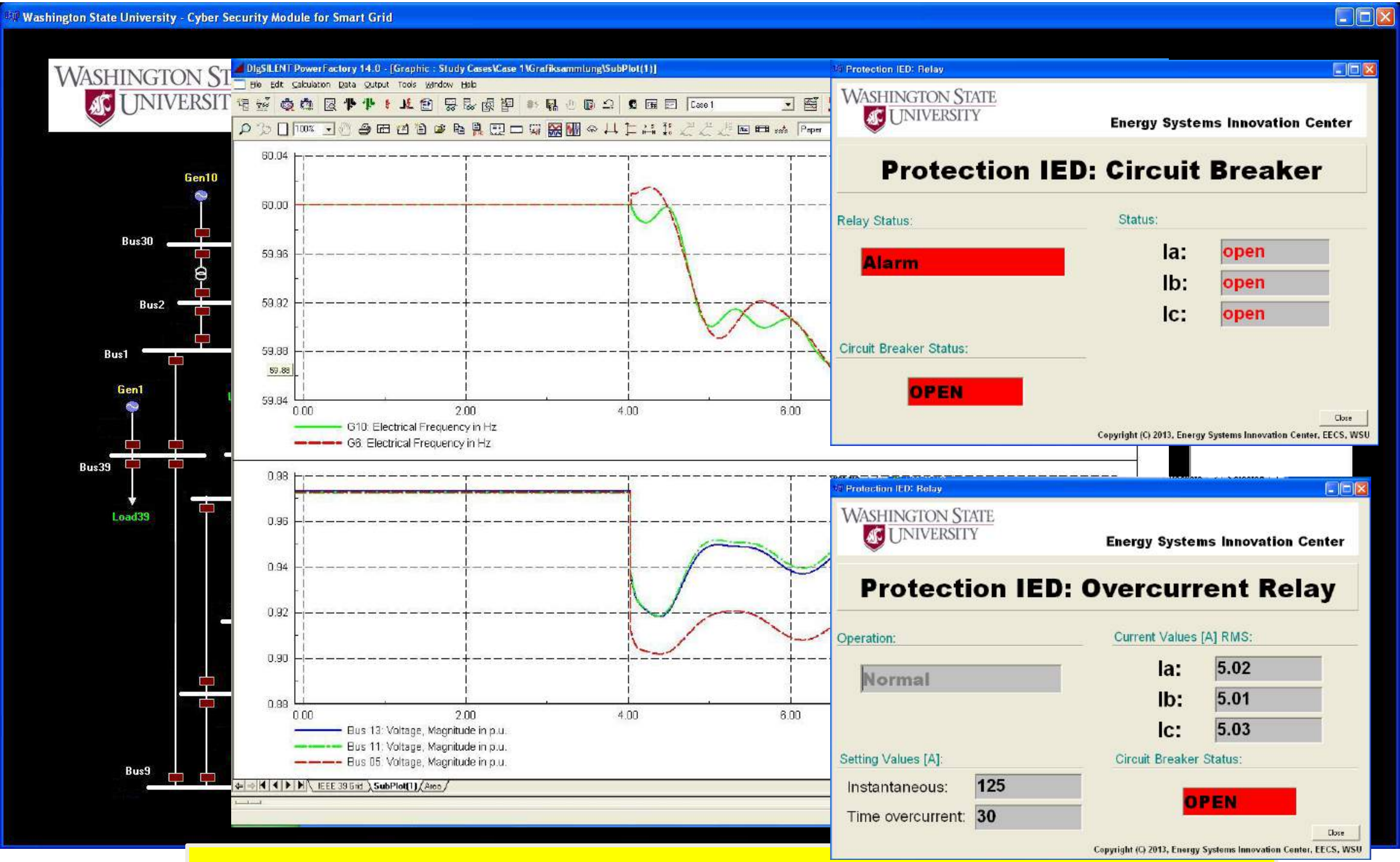
# System Integration



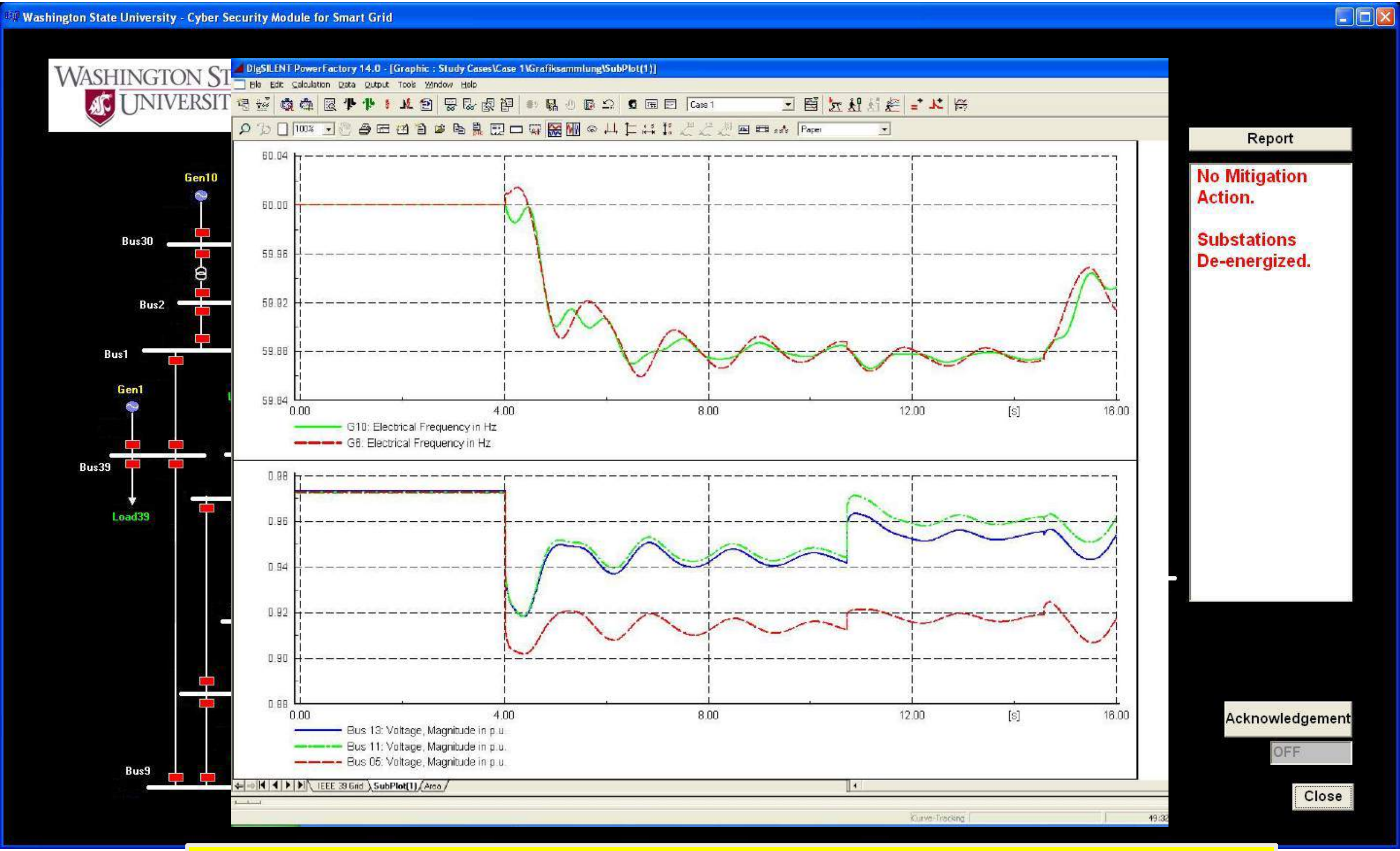
# IEEE 39 Bus System



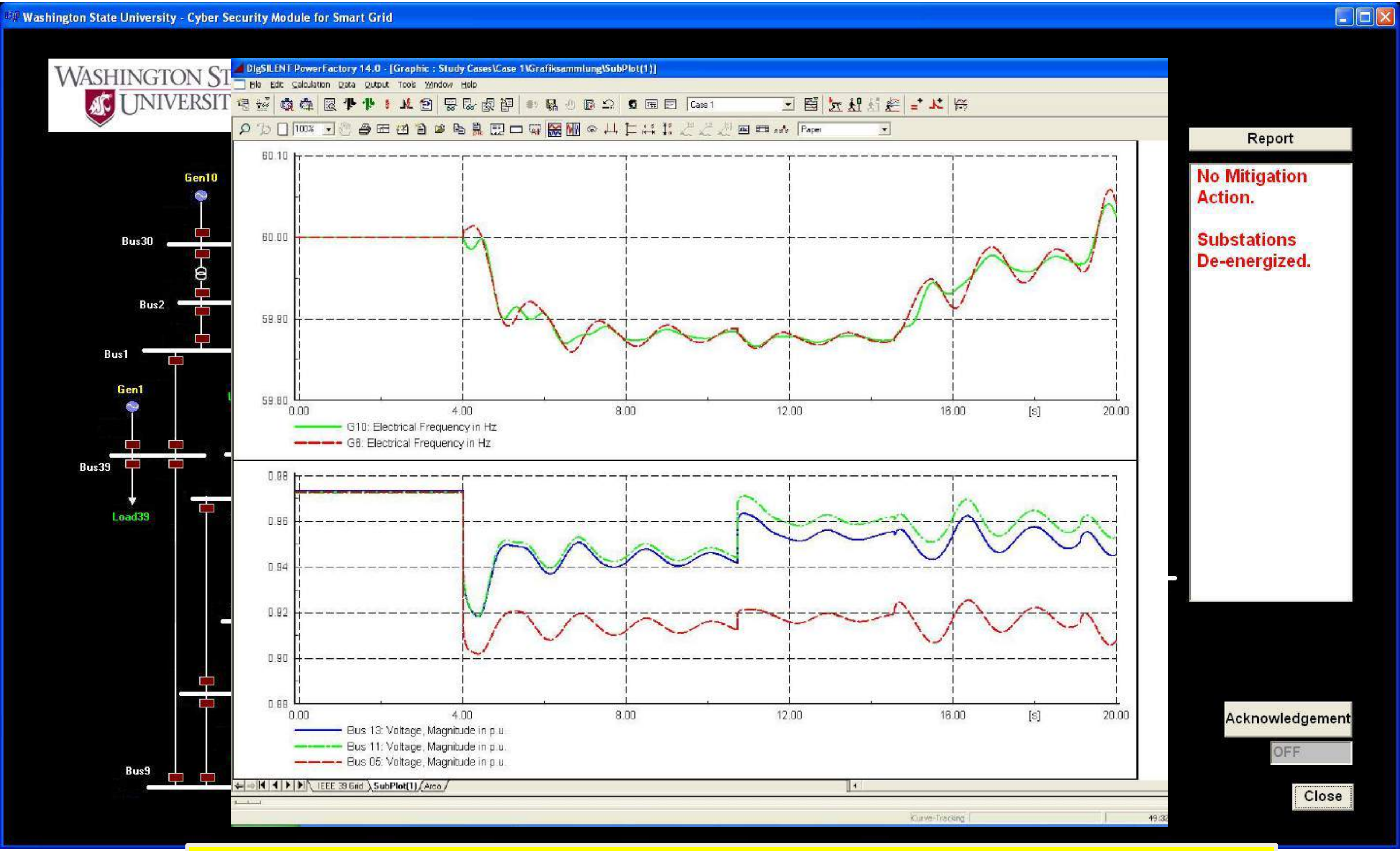

Normal status



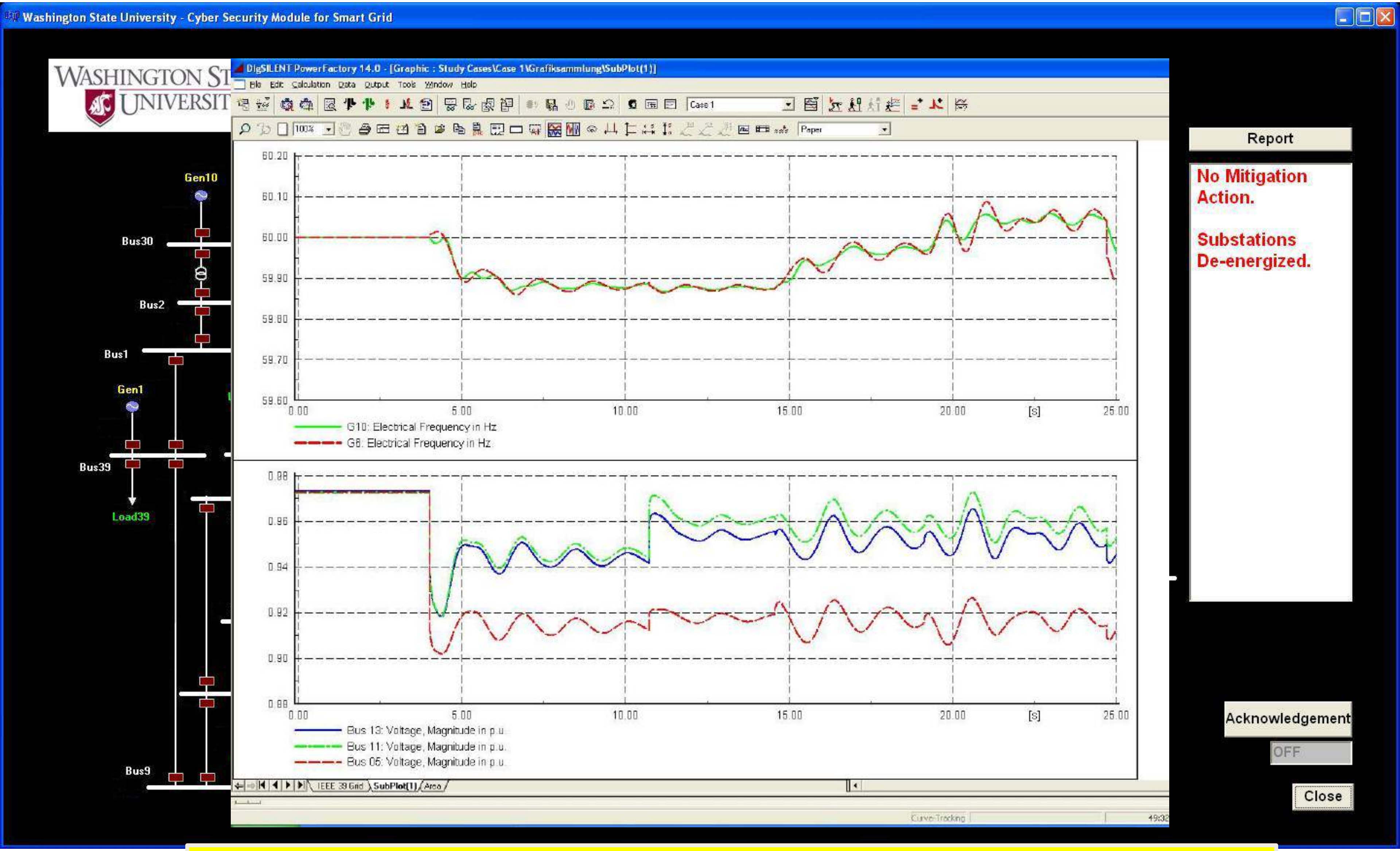

Sequential attacks – Sub # **6** → 12 → 15 → 28 → 36 → 33 → 34



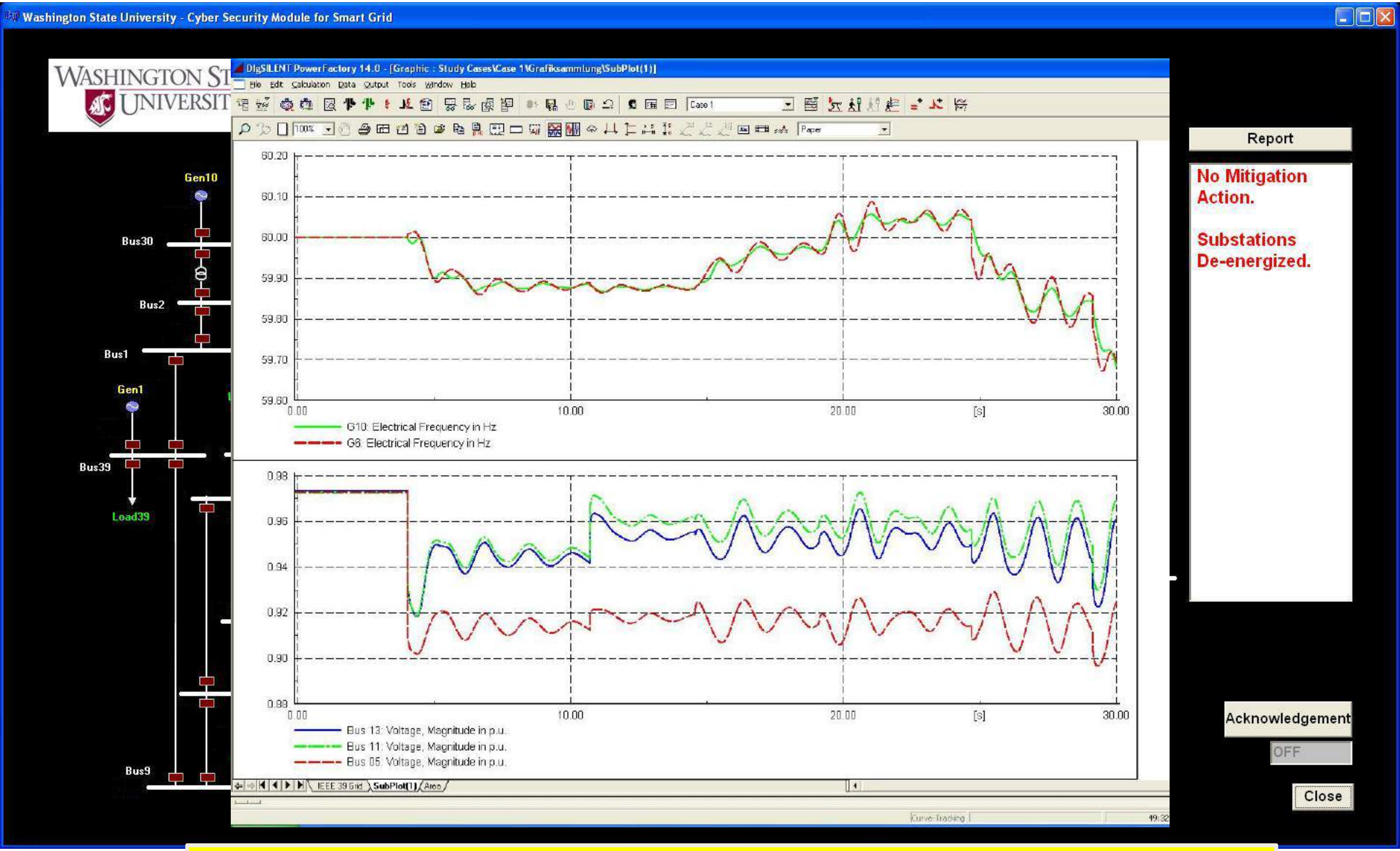

Sequential attacks – Sub # 6 → **12** → 15 → 28 → 36 → 33 → 34



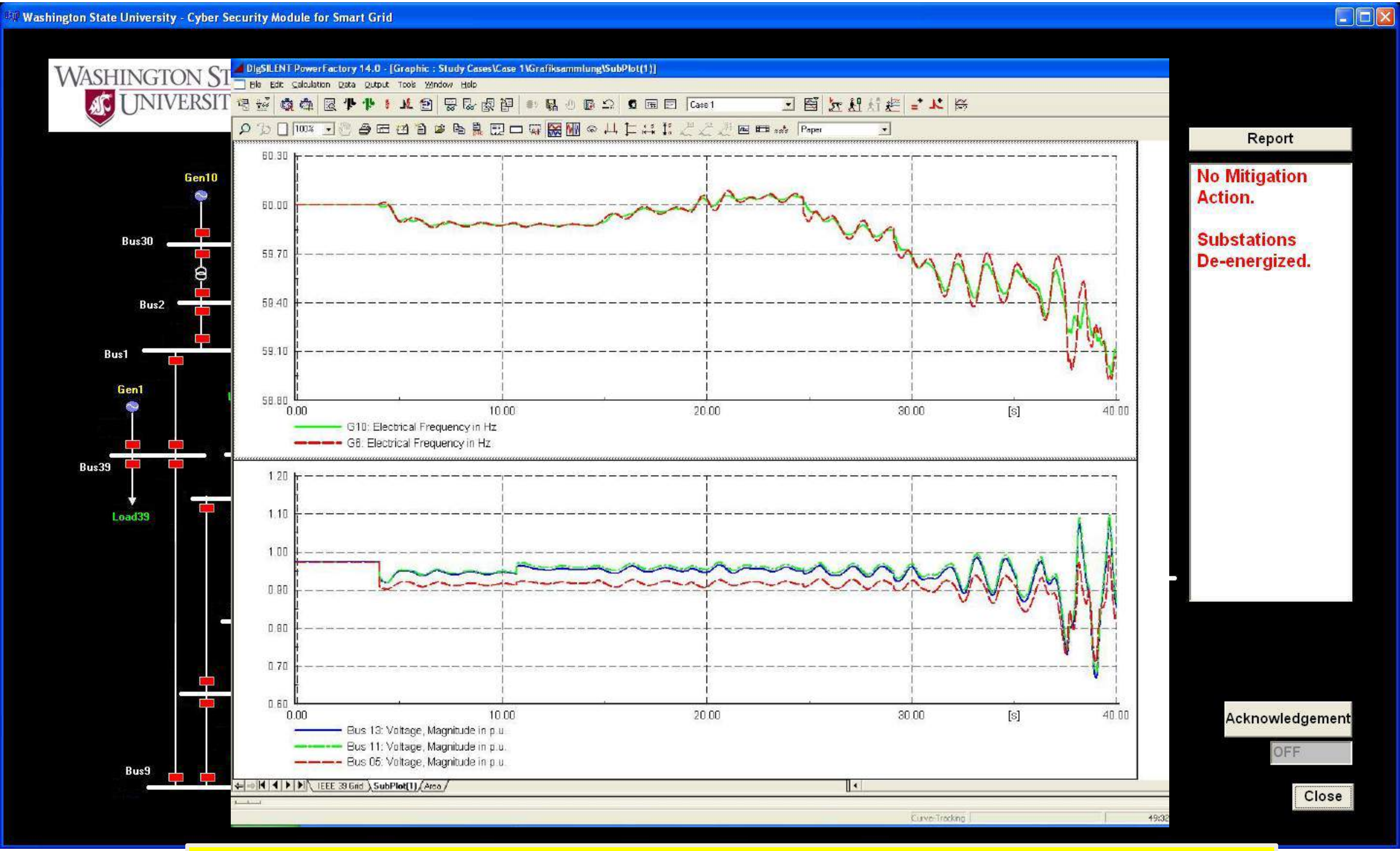

Sequential attacks – Sub # 6 → 12 → **15** → 28 → 36 → 33 → 34



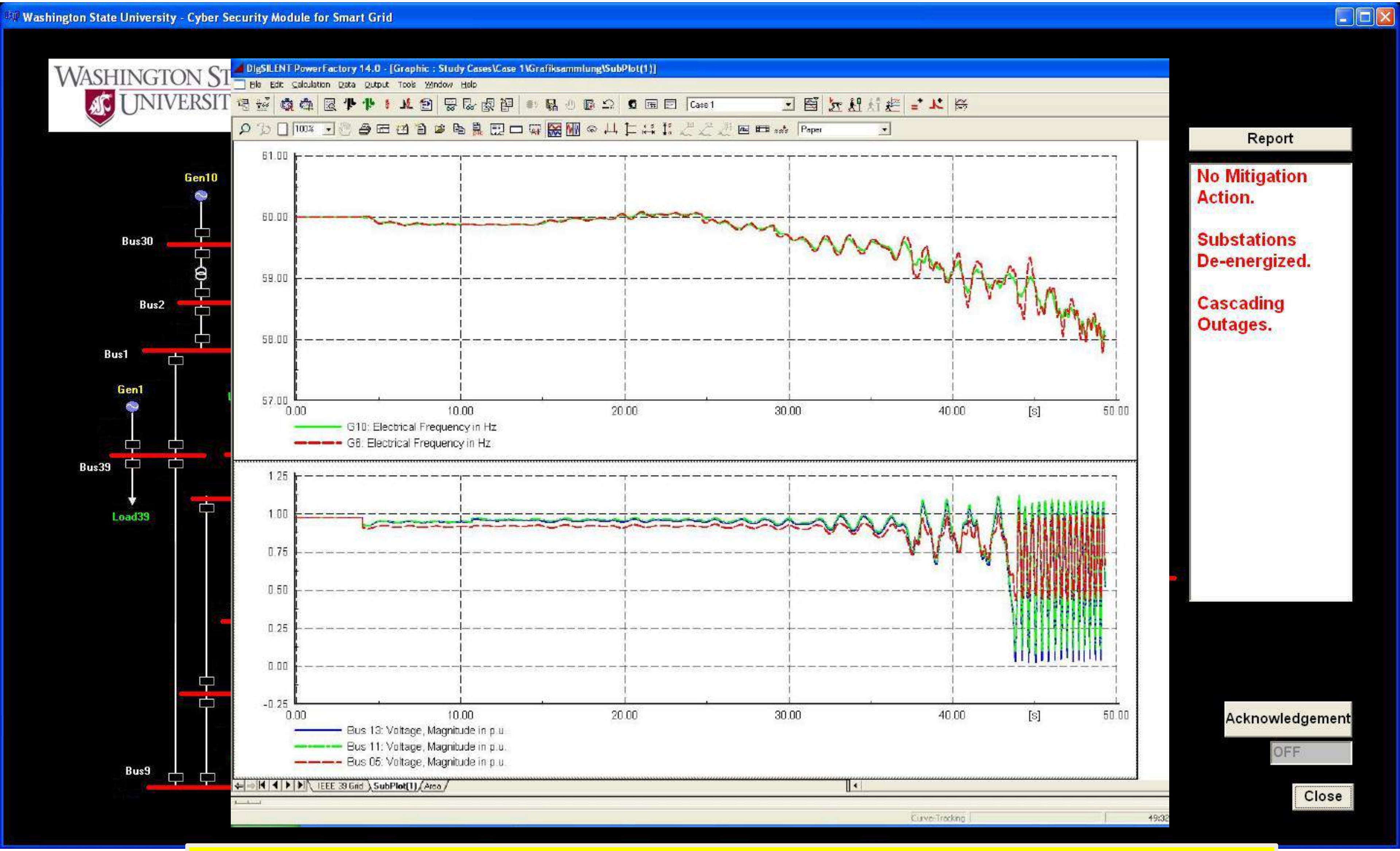

Sequential attacks – Sub # 6 → 12 → 15 → **28** → 36 → 33 → 34




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

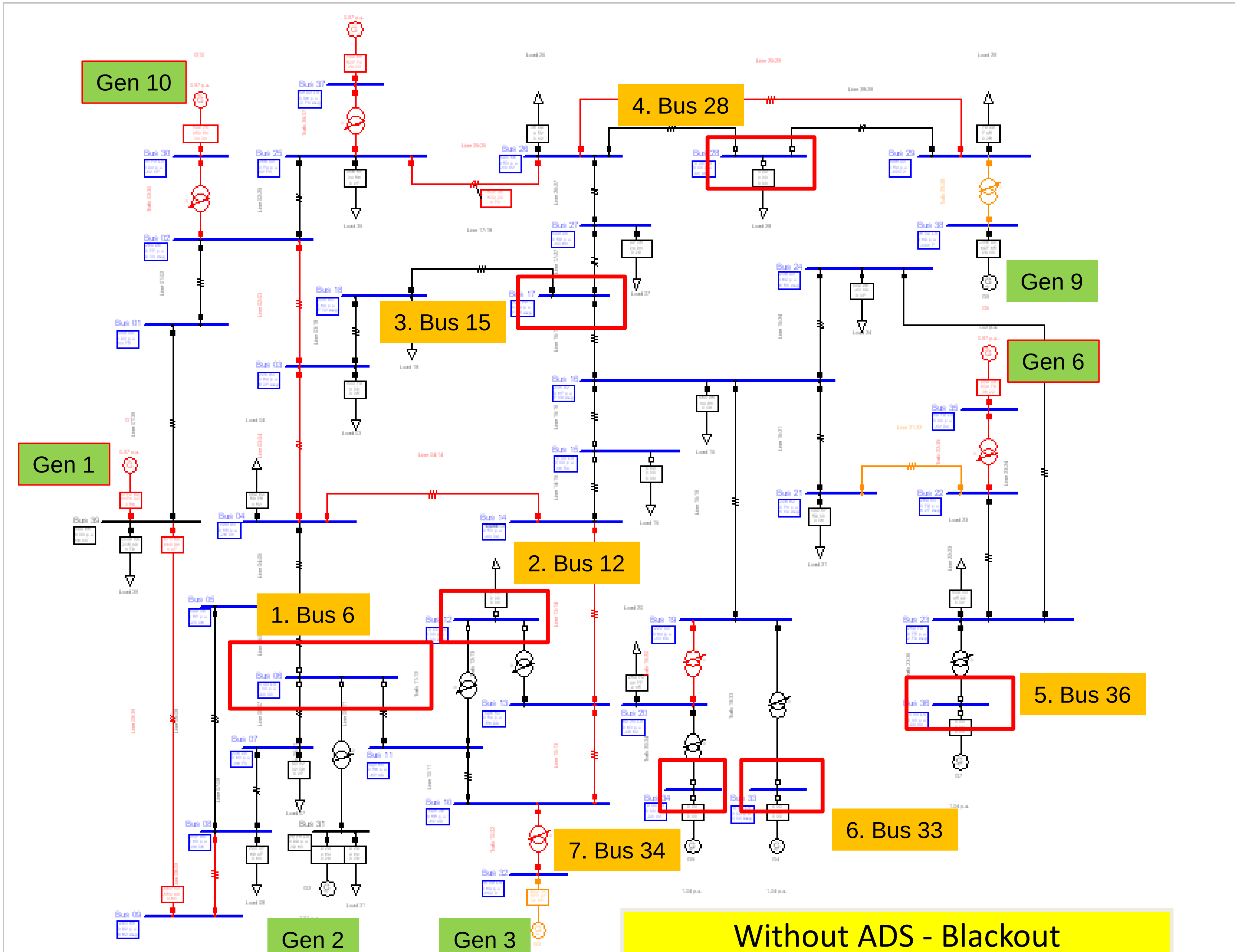


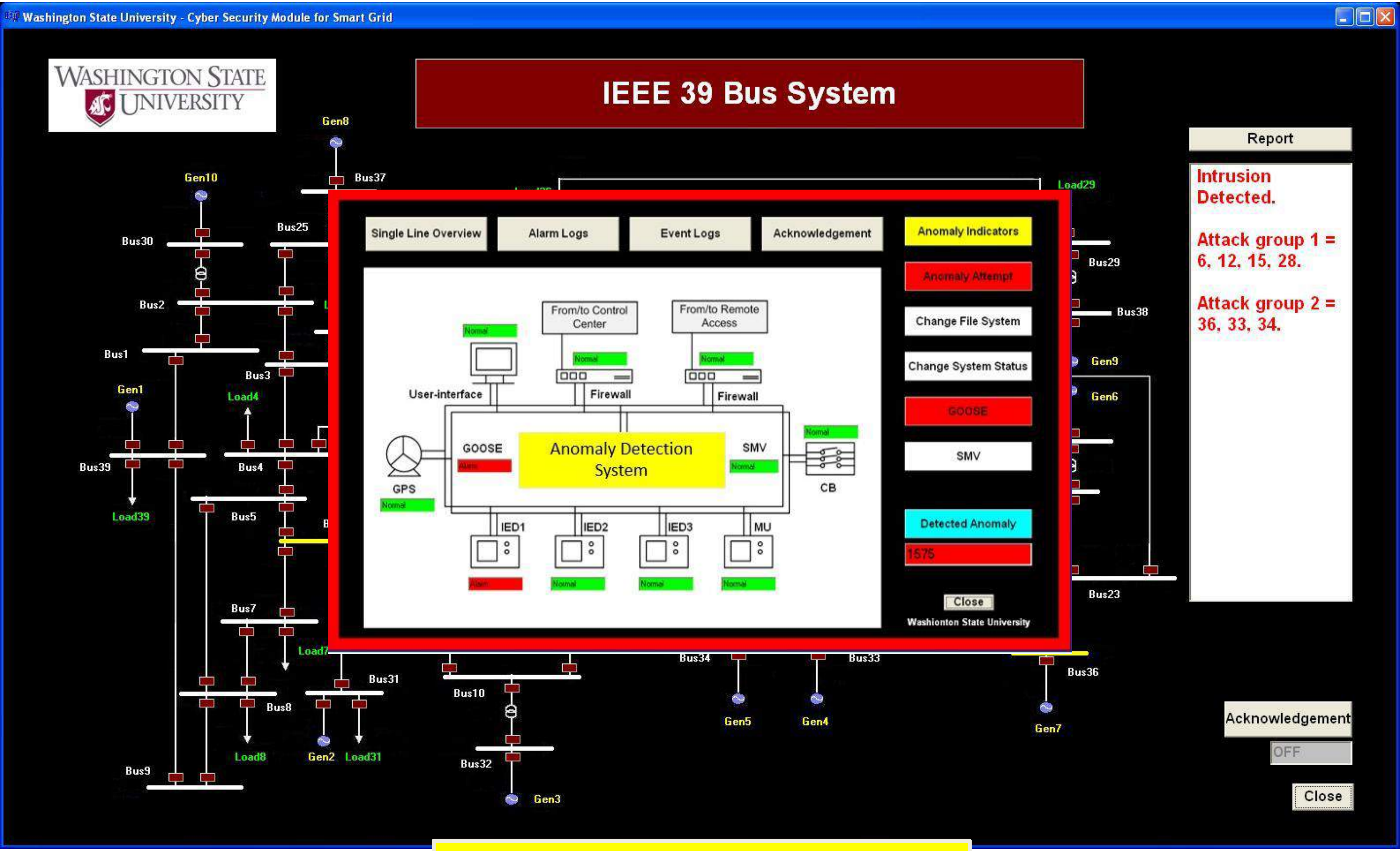

Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → **33** → 34




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

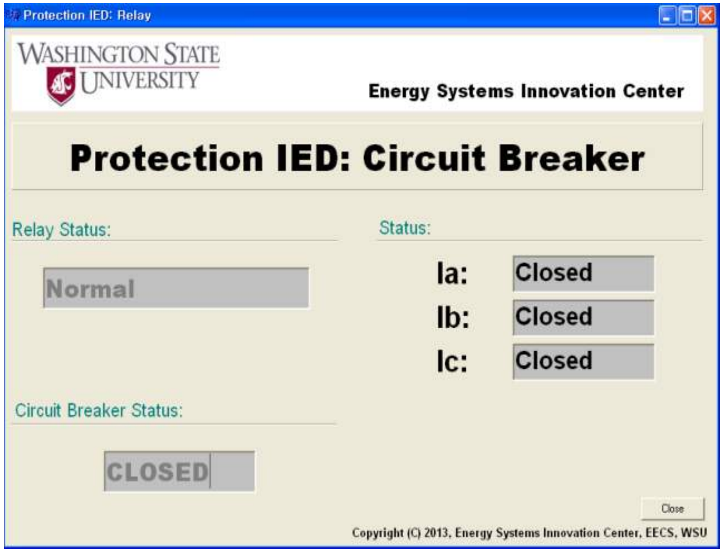
# IEEE 39 Bus System (DIgSILENT)

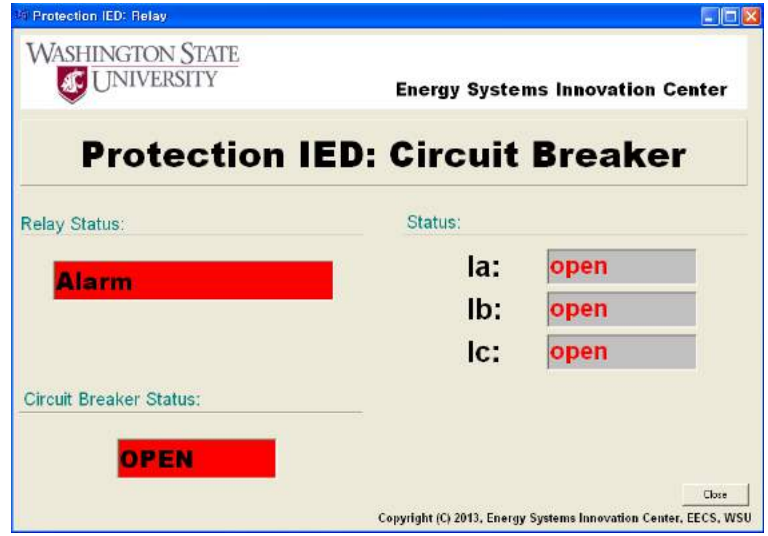


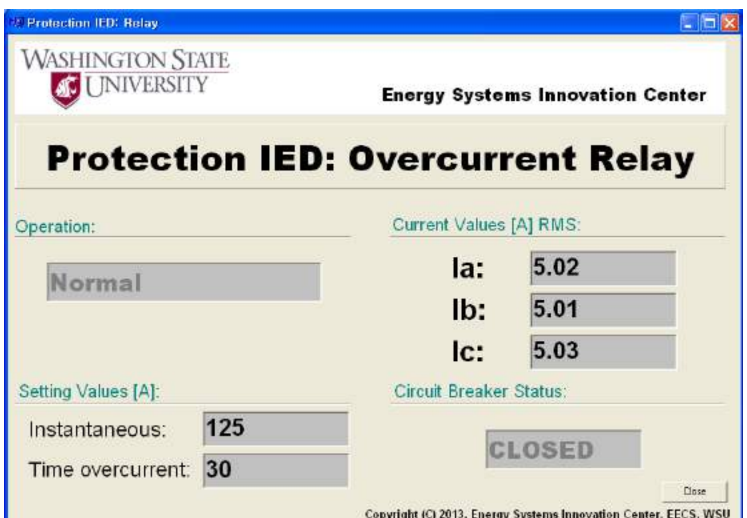


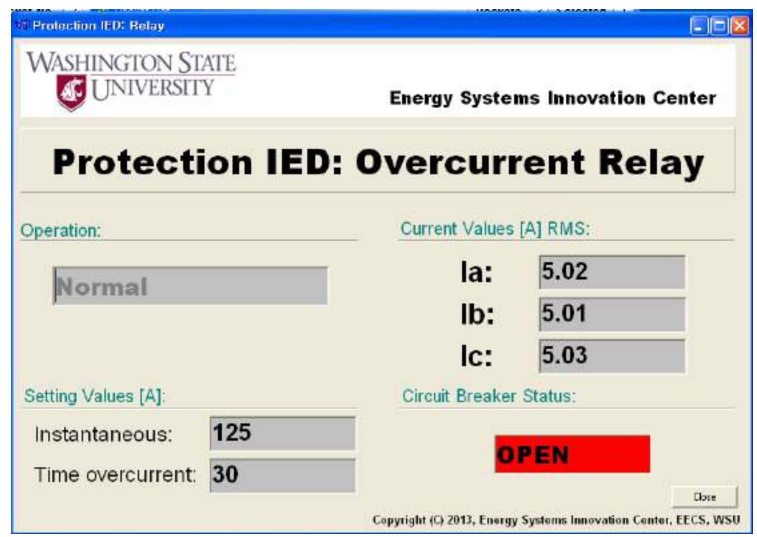

Sequential attacks with ADS

# HMI

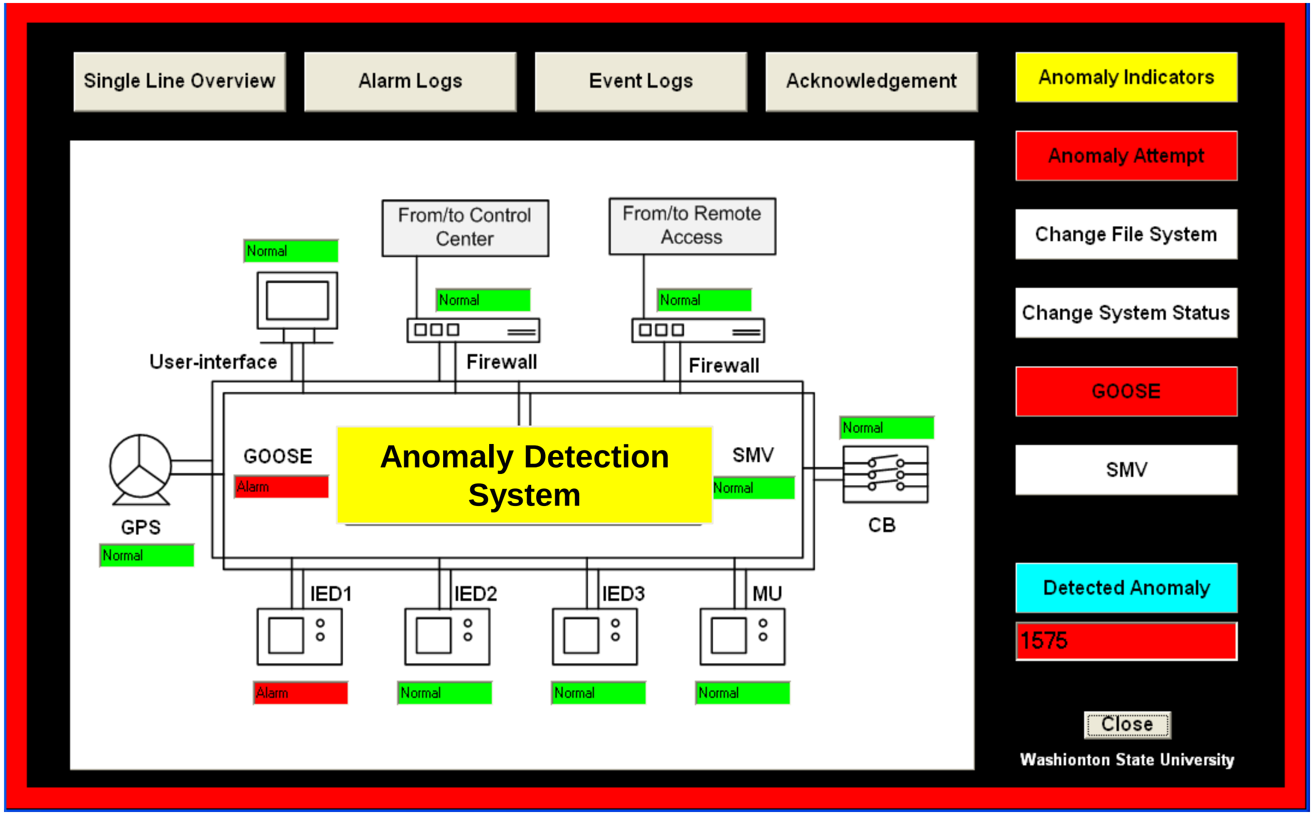

Protection IED: Relay
WASHINGTON STATE UNIVERSITY
Energy Systems Innovation Center
Protection IED: Circuit Breaker
Relay Status:
Normal
Status:
Ia: Closed
Ib: Closed
Ic: Closed
Circuit Breaker Status:
CLOSED
Close
Copyright (C) 2013, Energy Systems Innovation Center, EECS, WSU


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

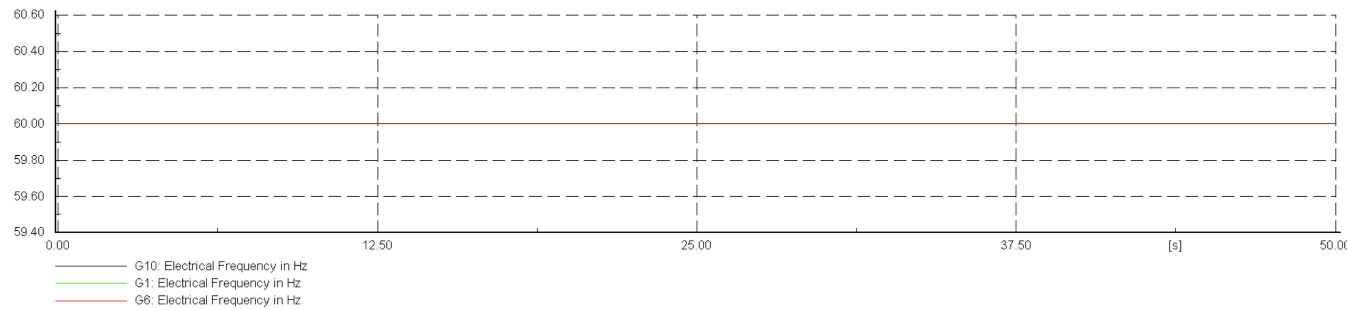

Protection IED: Relay
WASHINGTON STATE UNIVERSITY
Energy Systems Innovation Center
Protection IED: Overcurrent Relay
Operation:
Normal
Current Values [A] RMS:
Ia: 5.02
Ib: 5.01
Ic: 5.03
Setting Values [A]:
Instantaneous: 125
Time overcurrent: 30
Circuit Breaker Status:
OPEN
Close
Copyright (C) 2013,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

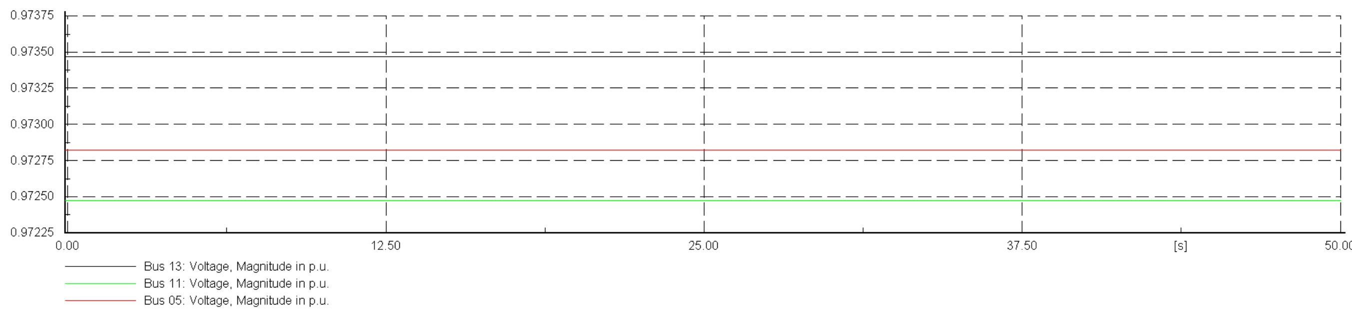
# HMI

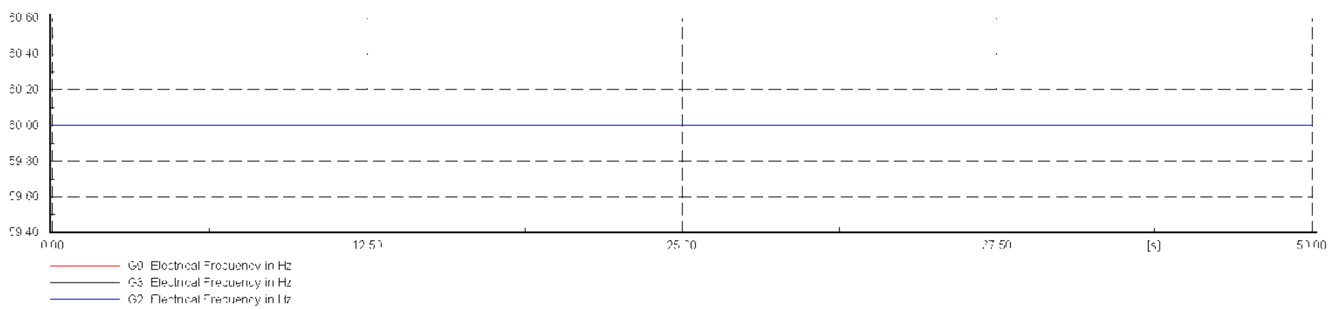


Single Line Overview
Alarm Logs
Event Logs
Acknowledgement
Anomaly Indicators
Anomaly Attempt
Change File System
Change System Status
GOOSE
SMV
Detected Anomaly
1575
Close
Washionton State University
From/to Control Center
From/to Remote Access
Normal
User-interface
Firewall
Firewall
GOOSE
Alarm
Anomaly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

# IEEE 39 Bus System (DIgSILENT)

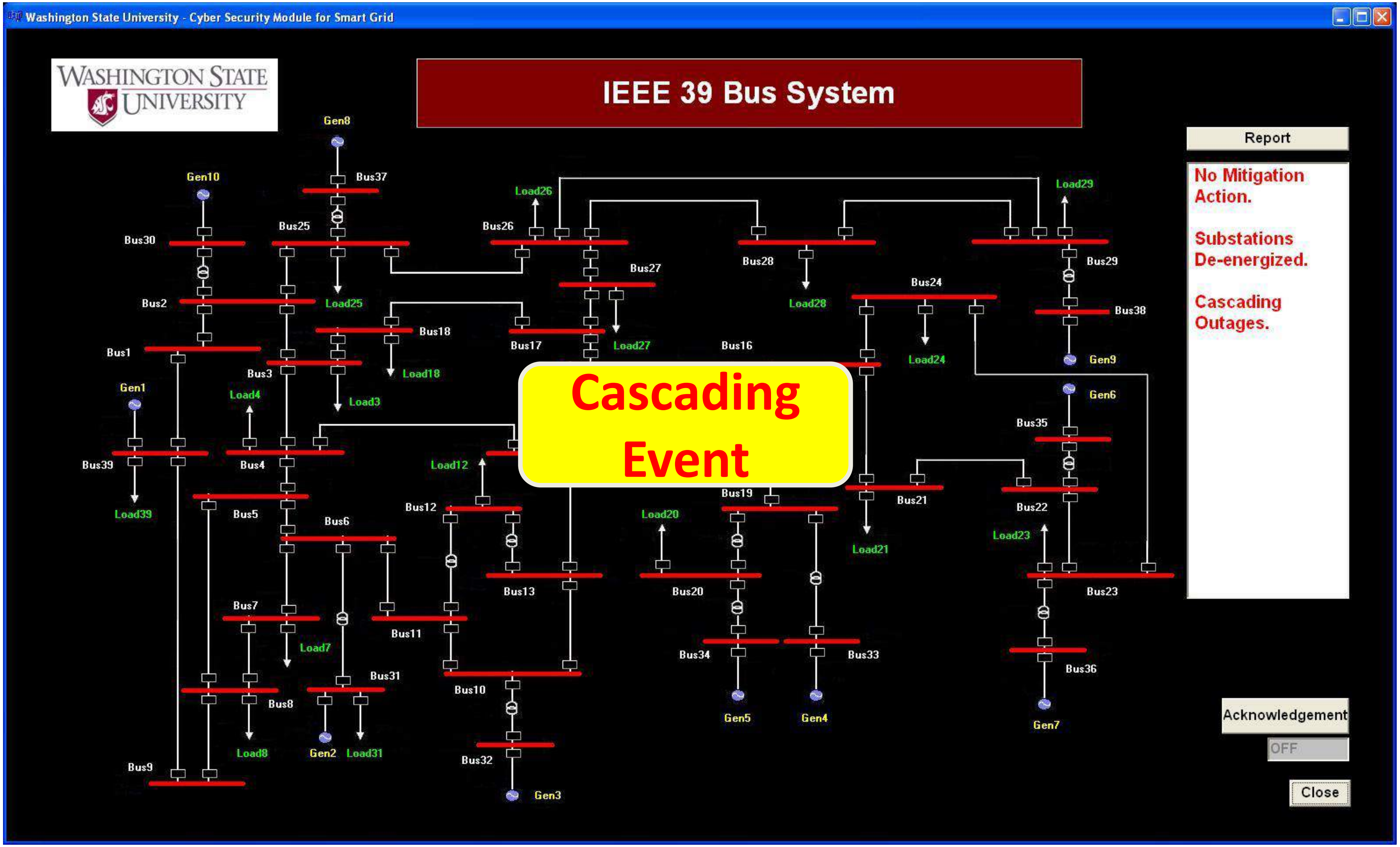


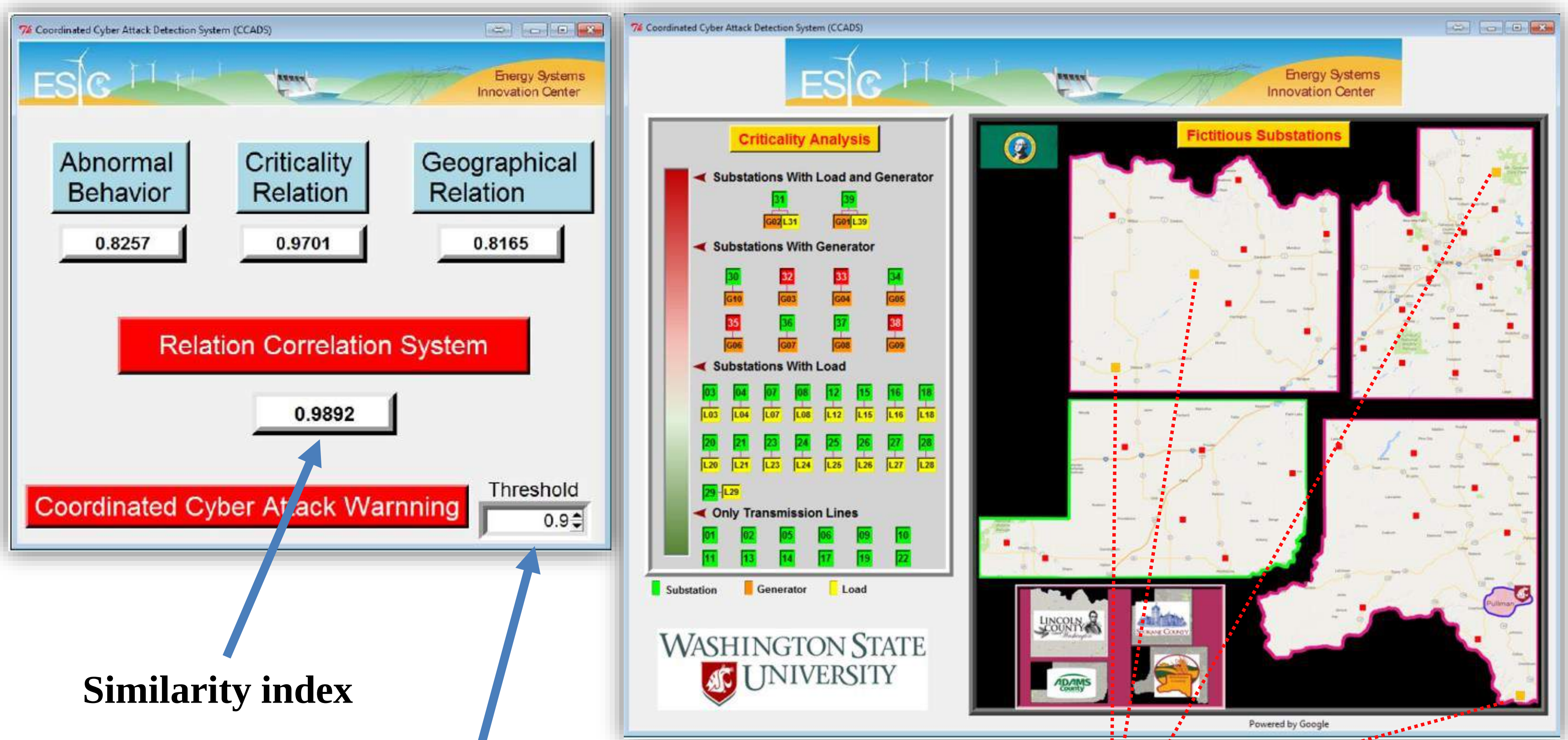




With ADS - Normal

# Coordinated Cyber Attack



# GUI of CCADS

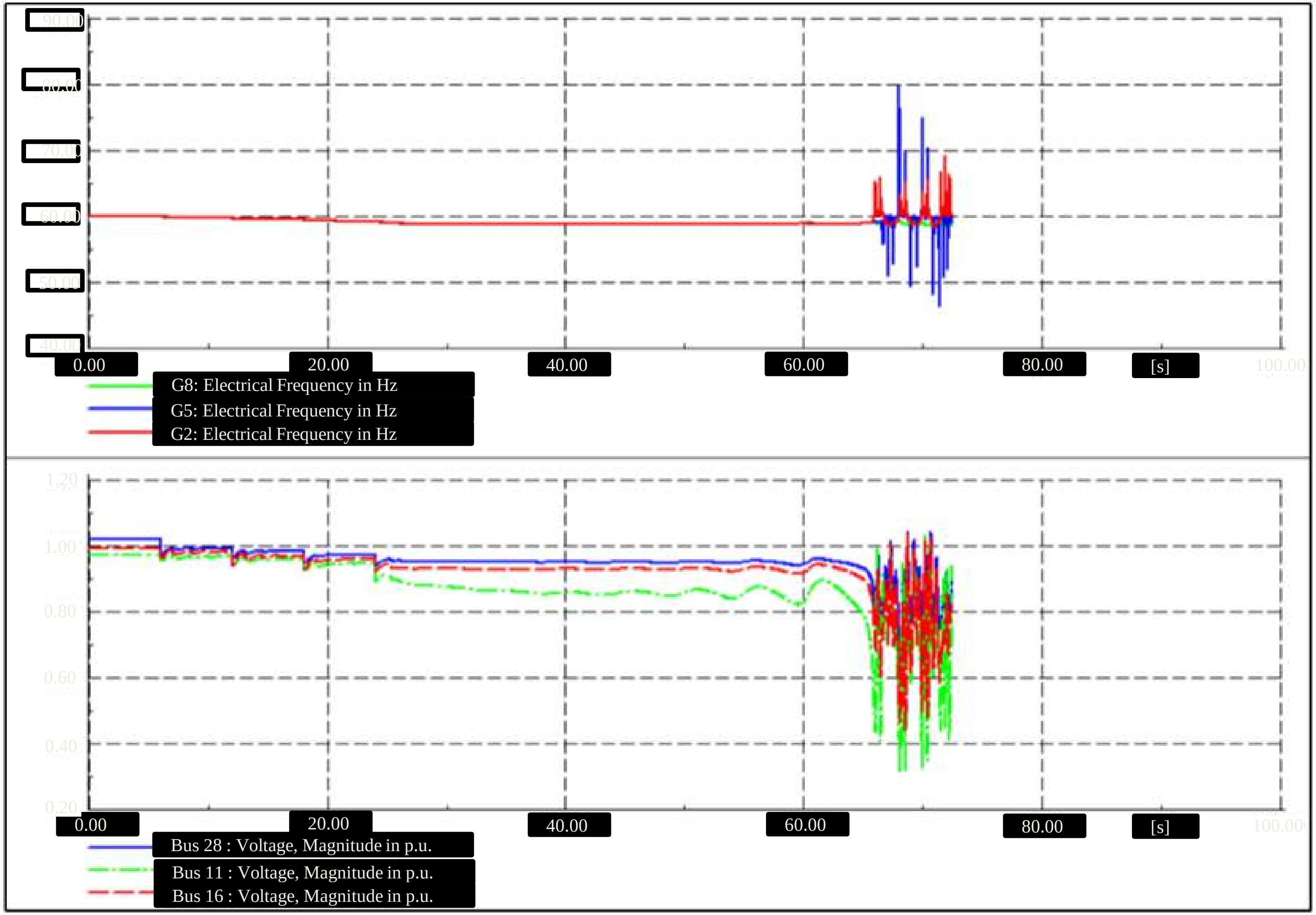



Similarity index

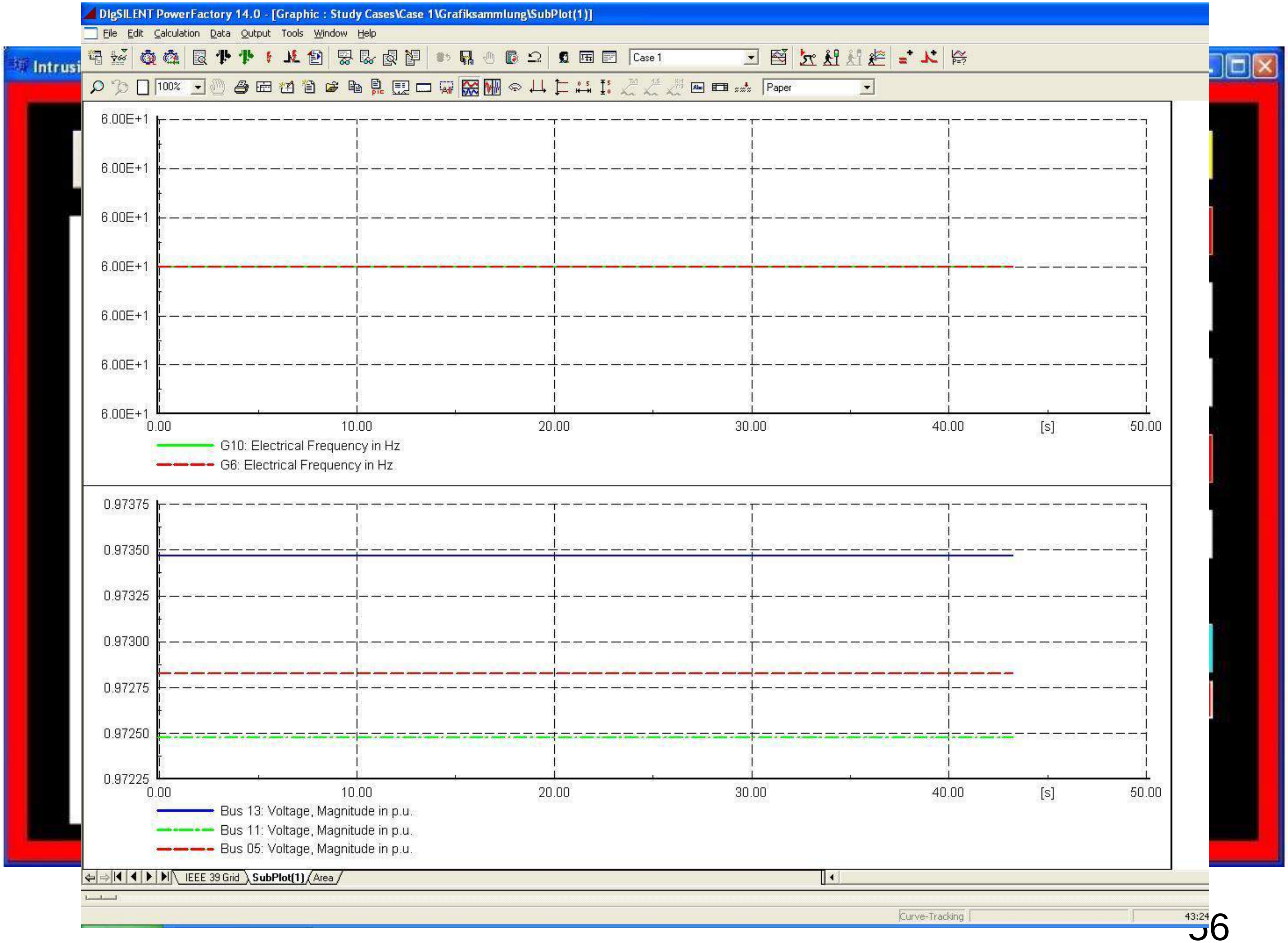
User defined threshold value

Compromised substations

# Simulation of Power System



# Intrusion Detection System



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

[2] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, “Intruders in the Grid,” *IEEE Power and Energy Magazine*, Jan/Feb 2012, pp. 58-66.

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

[4] 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, pp. 498-519.

[5] 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, pp. 1148–1170.

[6] J. Xie, A. Stefanov, and 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

[7] C. C. Sun, C. C. Liu, and Jing Xie, "Cyber-Physical System Security of a Power Grid: State-of-the-Art," *Electronics*, 2016, DOI: 10.3390/electronics5030040.

[8] 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*, DOI 10.1109/TSG.2016.2614603.

[9] J. Hong and C. C. Liu, "Intelligent Electronic Devices with Collaborative Intrusion Detection Systems," Accepted for publication in *IEEE Trans. Smart Grid.*

# Further Information (Conti)


[10] C. C. Liu, A. Stefanov, J. Hong, "Cyber Vulnerability and Mitigation Studies Using a SCADA Testbed," *IEEE Power and Energy Magazine,* Jan. 2012.

[11] S. K. Khaitan, J. D. McCalley, and C. C. Liu (Co-Editors), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Springer, 2015.