Cyber Security of Power Grids

Chen-Ching Liu
Boeing Distinguished Professor
Director, Energy Systems Innovation Center
Washington State University

In Collaboration with M. Govindarasu,
Iowa State University

This research is sponsored by U.S. National Science Foundation, and NSF/Department of Energy through CURENT ERC.

WASHINGTON STATE UNIVERSITY
World Class. Face to Face.

Research framework

Intrusion detection

Preventive / remedial actions

Before Intrusion → Intrusion → After Intrusion

Before Intrusion

- Real-time monitoring
- Security rules
- Data and information logs

Intrusion

- Intrusion detection using detection algorithms
- Find same type of attacks
- Impact analysis (what-if scenario)
- Find more vulnerable point

After Intrusion

- Mitigation actions
- Preventive and remedial action
- Reconfigure firewall rules

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

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

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.

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

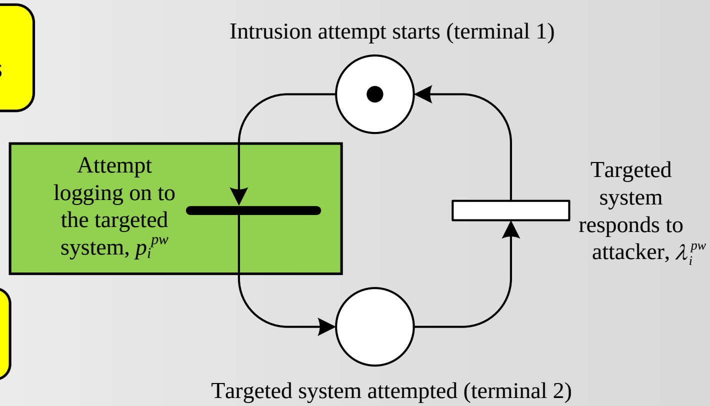
where π_j is the steady state probability that a SCADA system is attacked through a specific access point *j*, which is linked to the SCADA system. The damage factor, γ_j , represents the level of damage on a power system when a substation is removed

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).

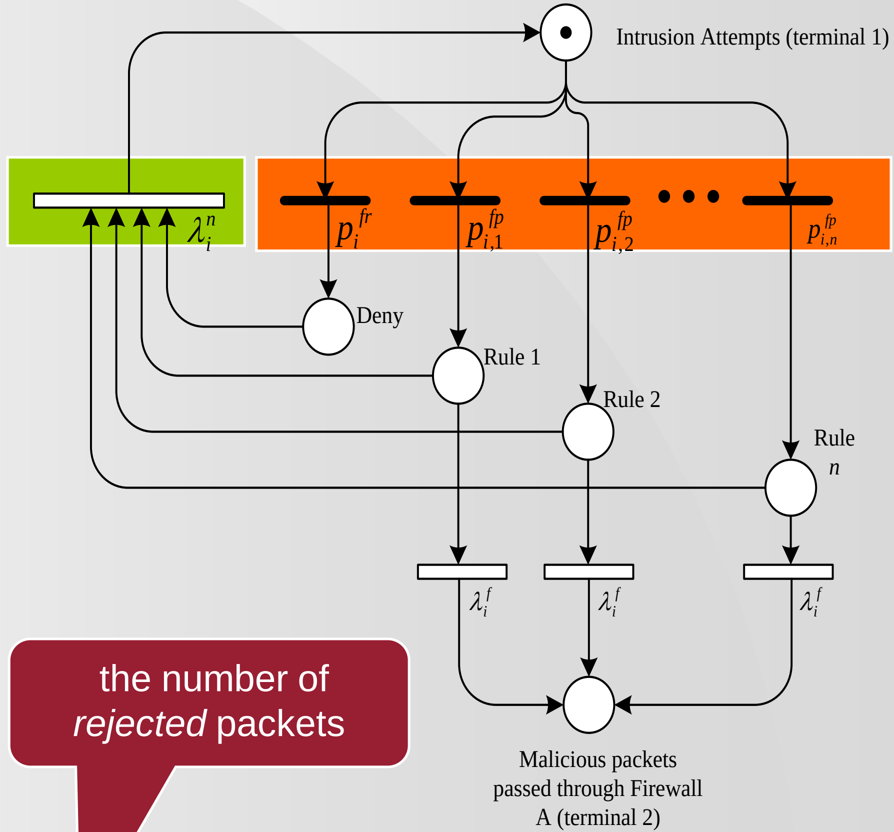
$$p_i^{pw} = \frac{f_i^{pw}}{N_i^{pw}}$$

- p_i^{pw}: the intrusion attempt probability of a computer system, i
- f_i^{pw}: number of intrusion attempts
- N_i^{pw}: total number of observed records



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

Impact Factor Evaluation

- Impact factor for the attack upon a SCADA system is

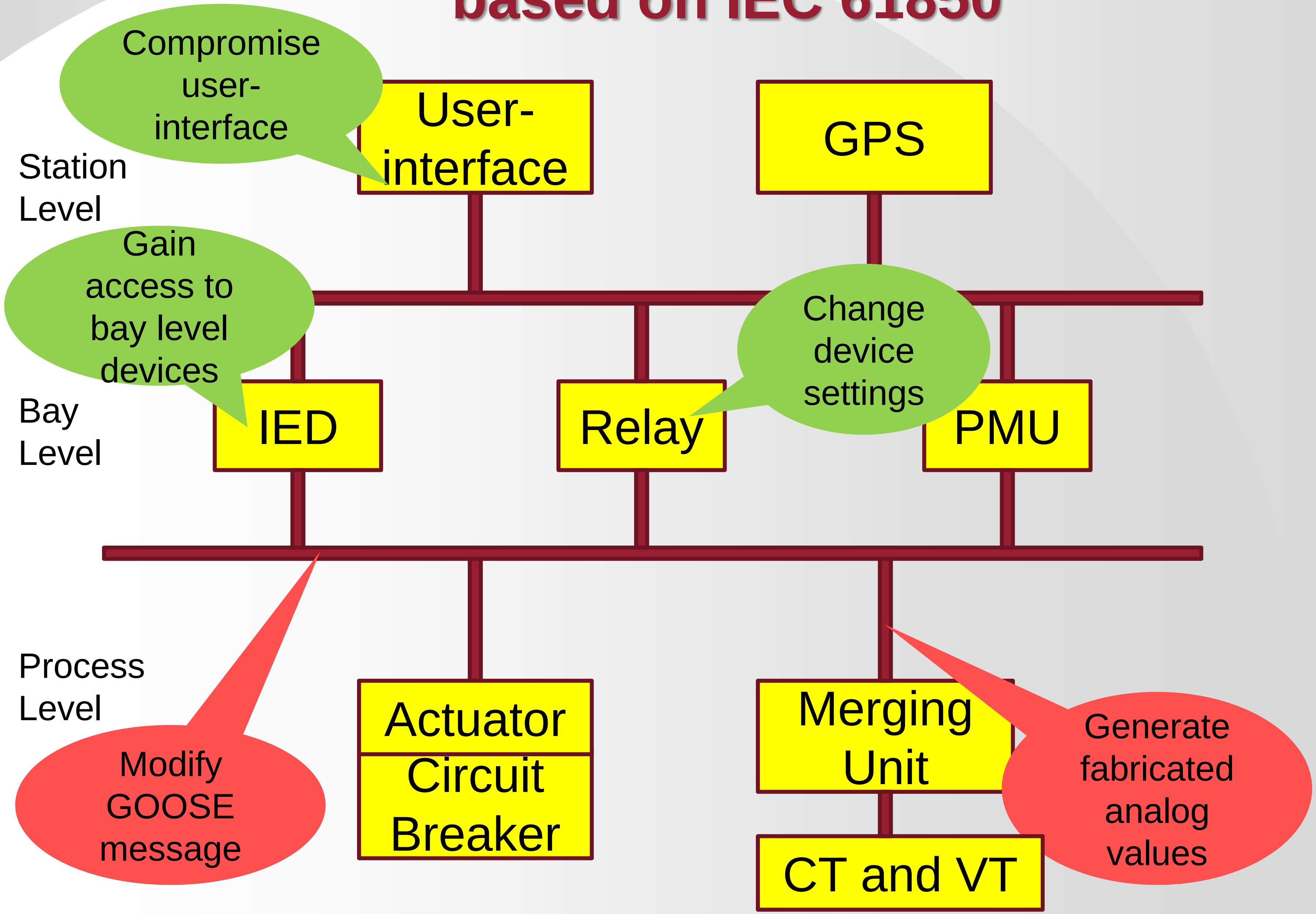
$$\gamma = \left(\frac{P_{LOL}}{P_{Total}} \right)^{L-1}$$

- 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

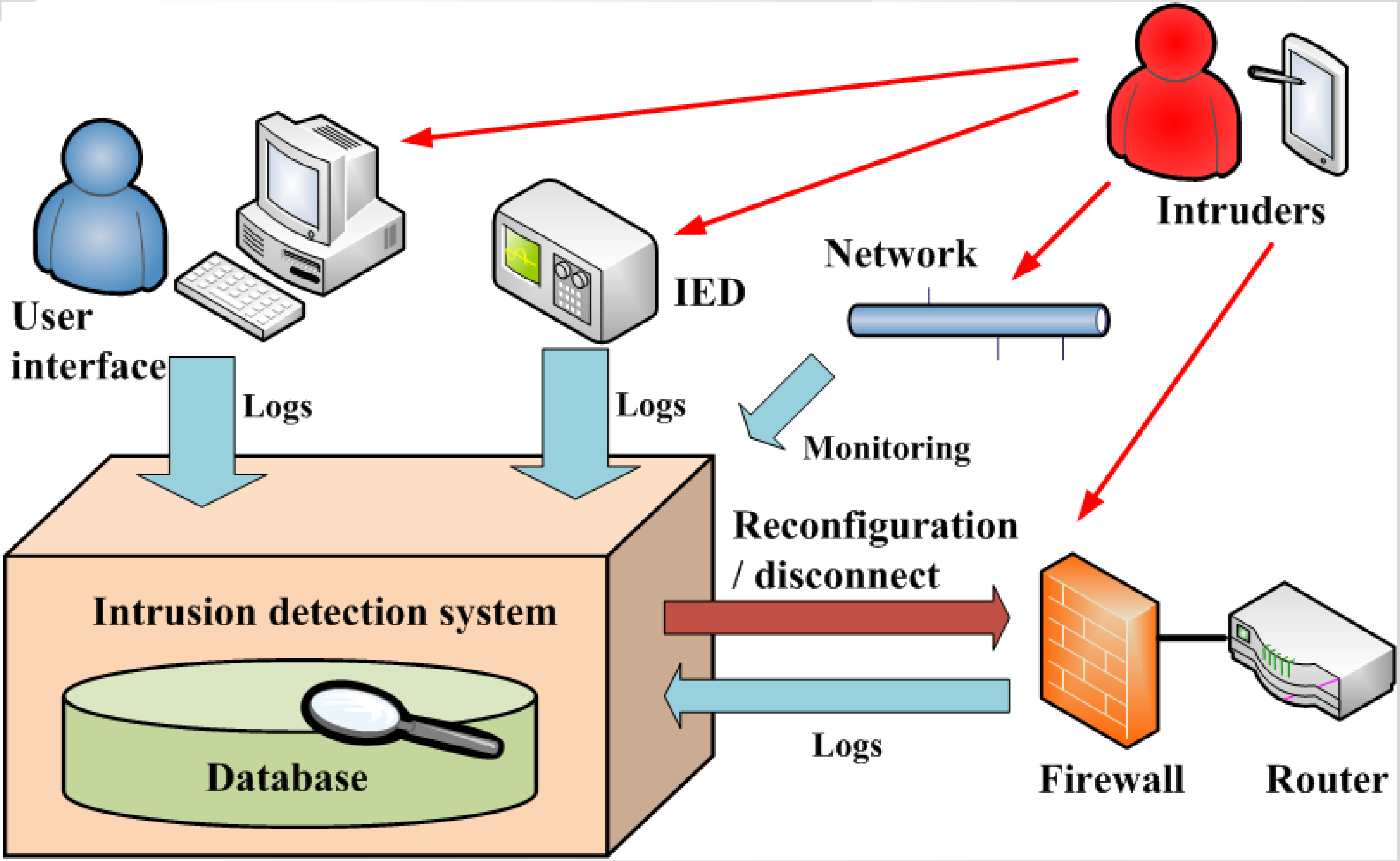
Vulnerabilities of substations

- 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



Host-based anomaly detection

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

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

- 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

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

Attack similarity

- The simultaneous anomaly detection is achieved in 3 steps, i.e.,
- 1) Find the total number of types of attacks
- 2) Find the same attack groups, and
- 3) Calculate the similarity between attacks in the same group

$$Attack\ Similarity = 1 - \frac{\sum_{i=1}^{x}\sum_{j=1}^{y}\left|\boldsymbol{\Omega}_{(i,j)} - \boldsymbol{\Omega}'_{(i,j)}\right|}{x \cdot y},$$

- Attack similarity value of 0 indicates no overlap and a value 1 indicates a complete overlap

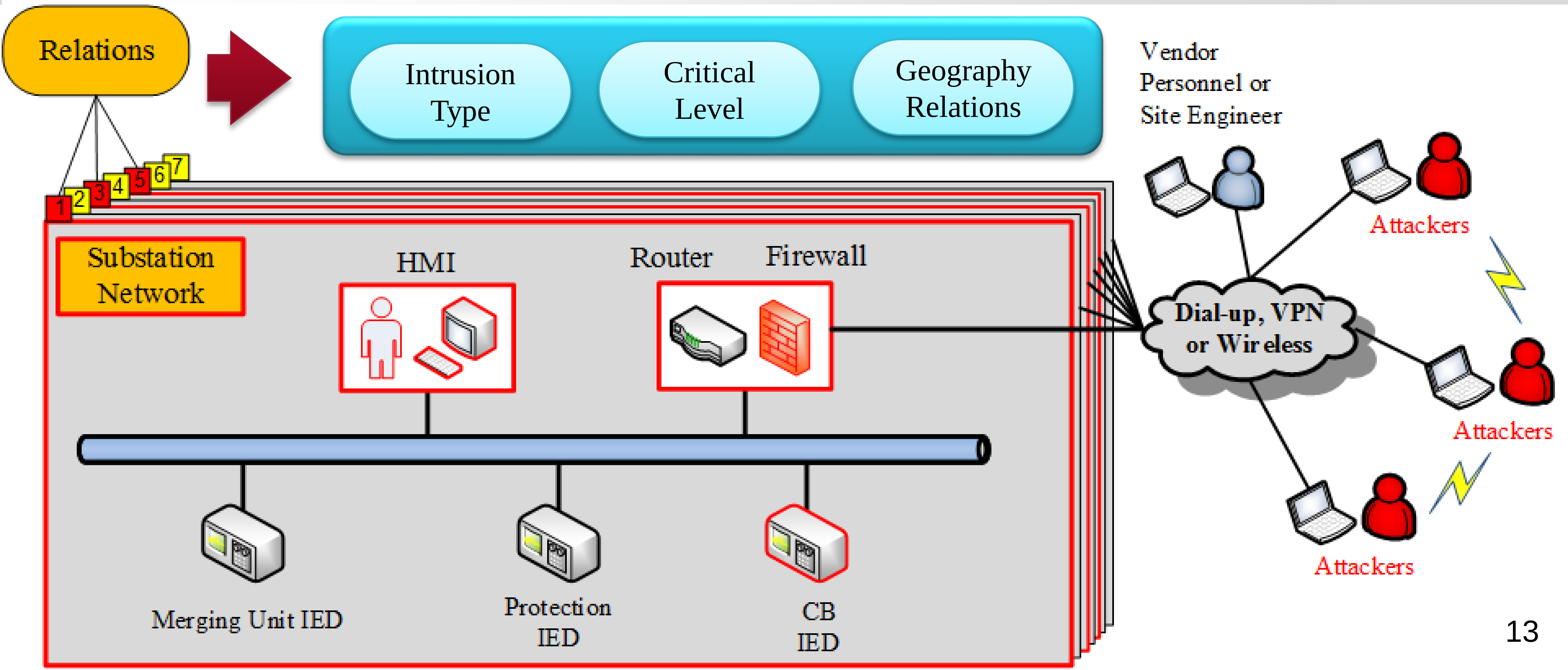
Substation A	Substation B
$\boldsymbol{\Omega} = \begin{matrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{matrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$	$\boldsymbol{\Omega}'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

similarity index = 0.9643

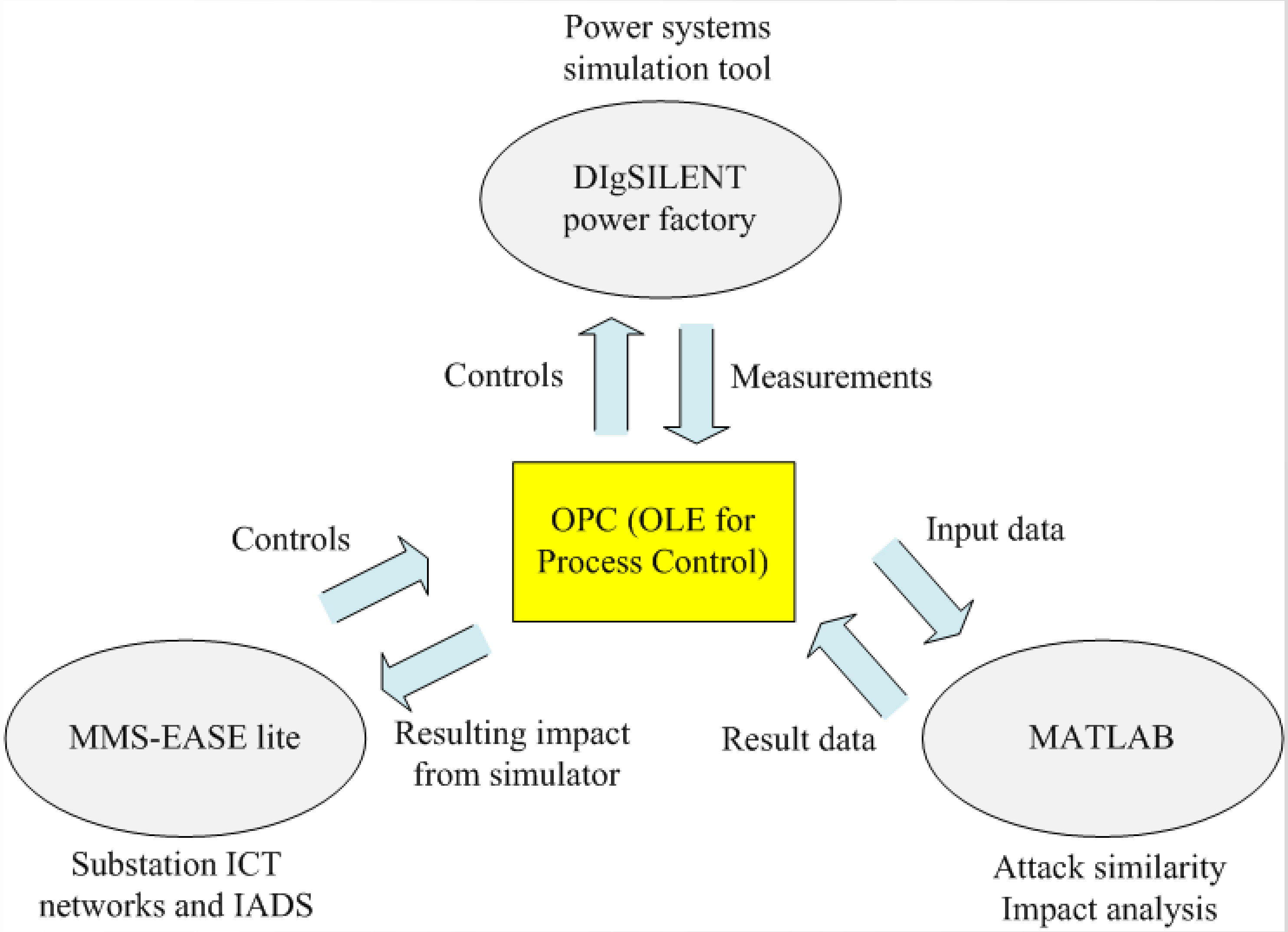
Coordinated cyber attack

- Coordinated cyber attacks cause a greater impact

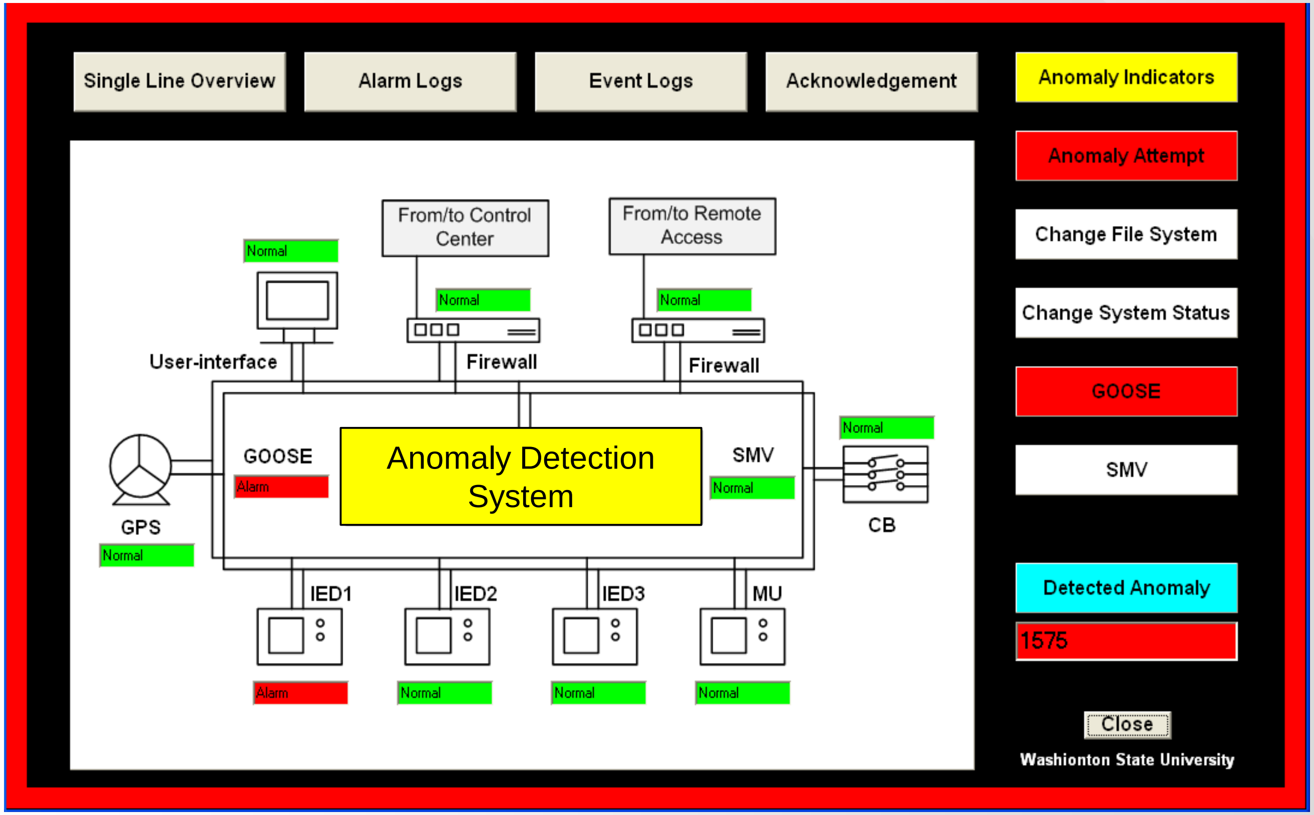
- In coordinated cyber attacks, attack steps are associated with each other. Identifying "relations" helps system operators detect a coordinated cyber attack.



System Integration



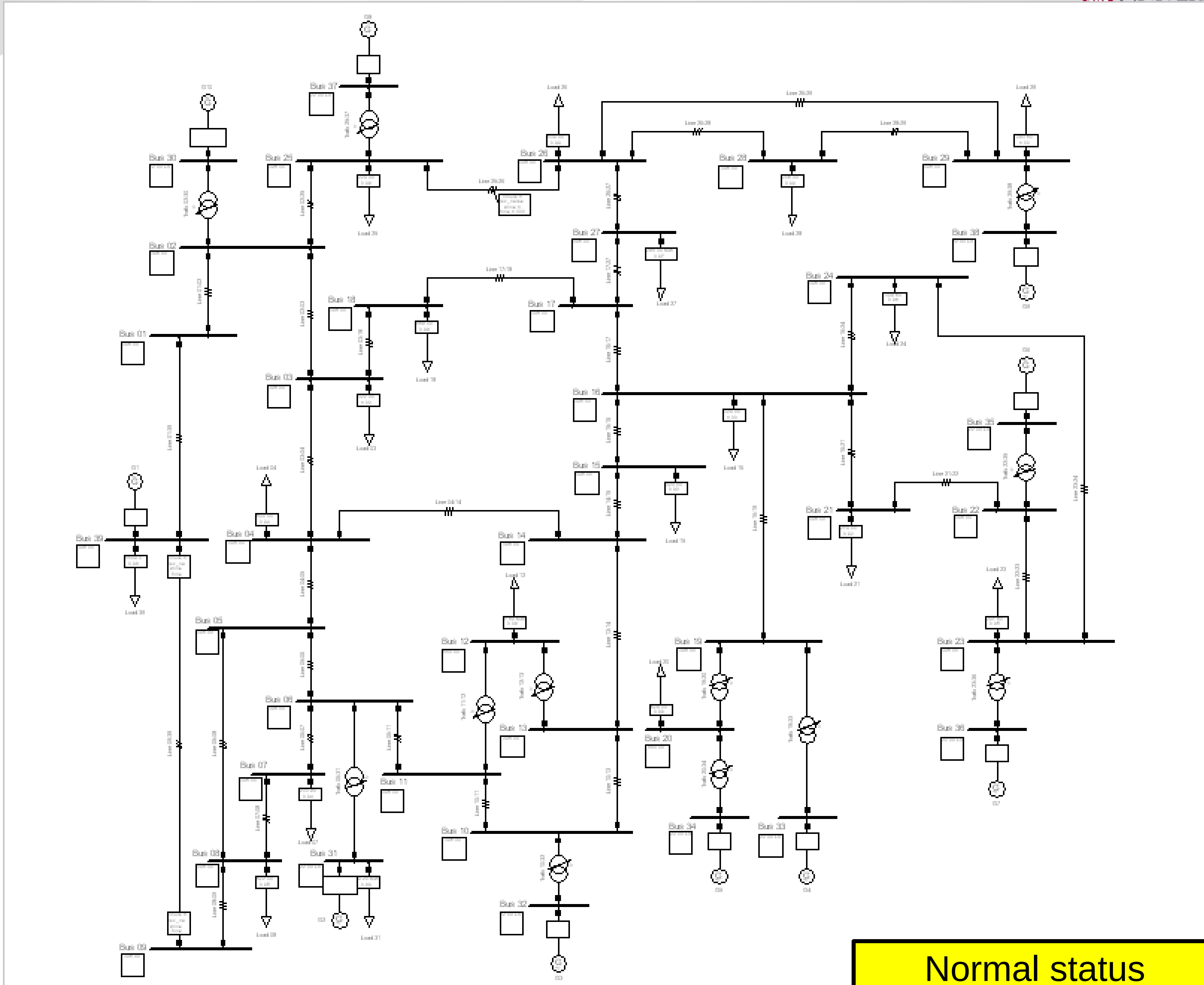
HMI



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
Normal
Normal
User-interface
Firewall
Firewall
GOOSE
Alarm
Anomaly Detection System
SMV
Normal
Normal
CB
GPS
Normal
IED1
IED2
IED3
MU
Alarm
Normal
Normal
Normal

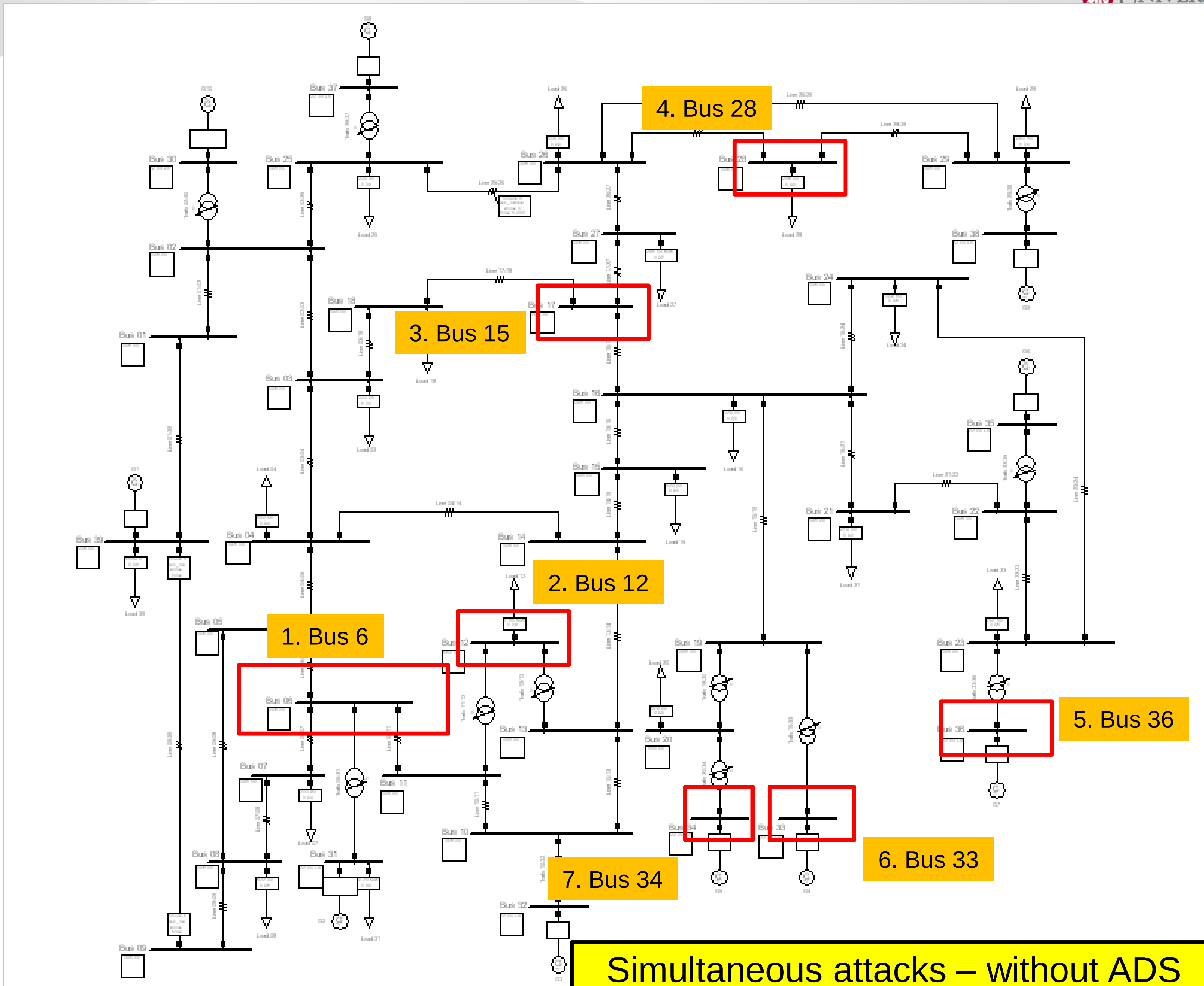
IEEE 39 bus system (DIgSILENT)

WASHINGTON STATE UNIVERSITY



Normal status

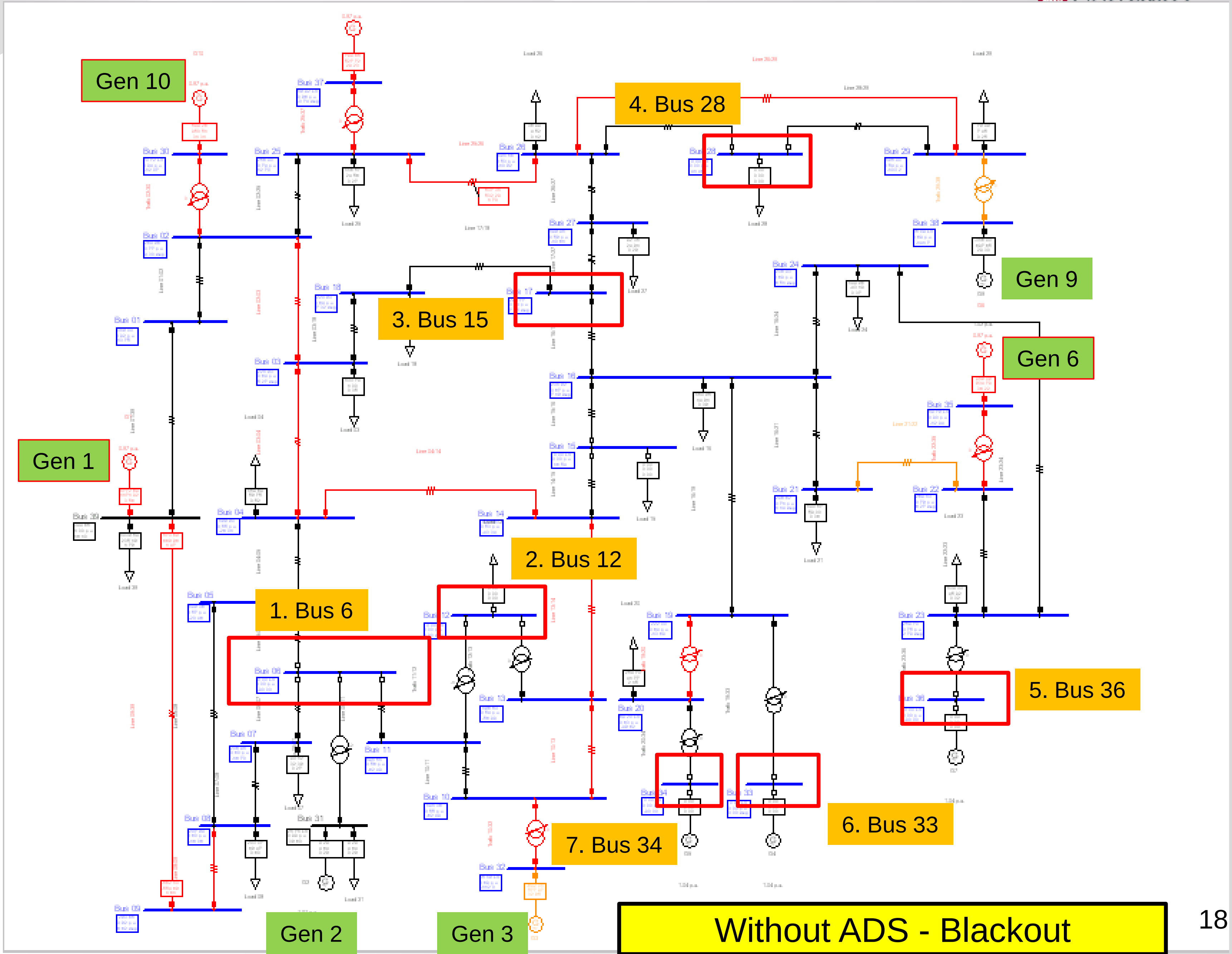
IEEE 39 bus system (DIgSILENT)



Simultaneous attacks – without ADS

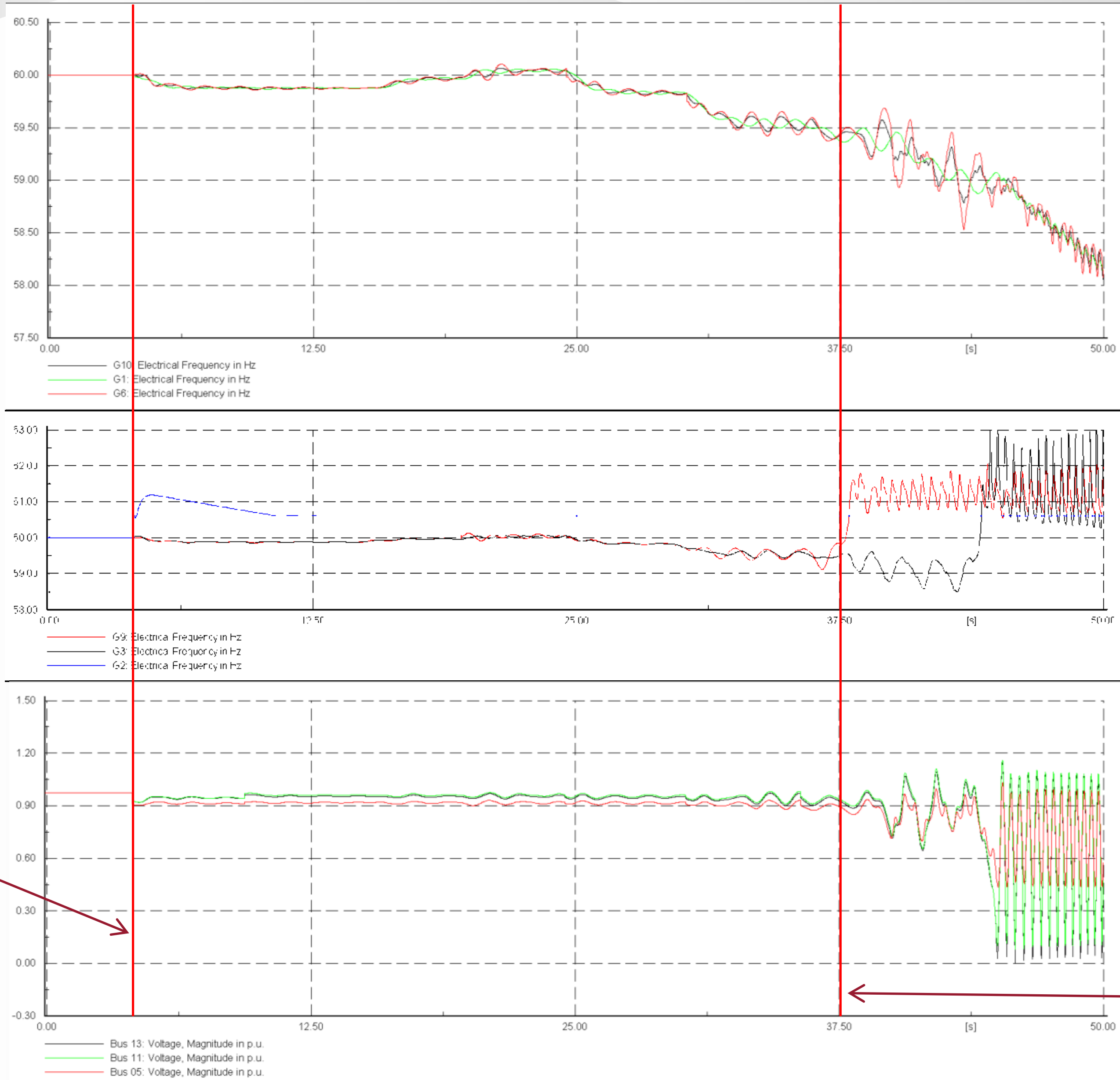
IEEE 39 bus system (DIgSILENT)

Washington State University



Without ADS - Blackout

IEEE 39 bus system (DIgSILENT)

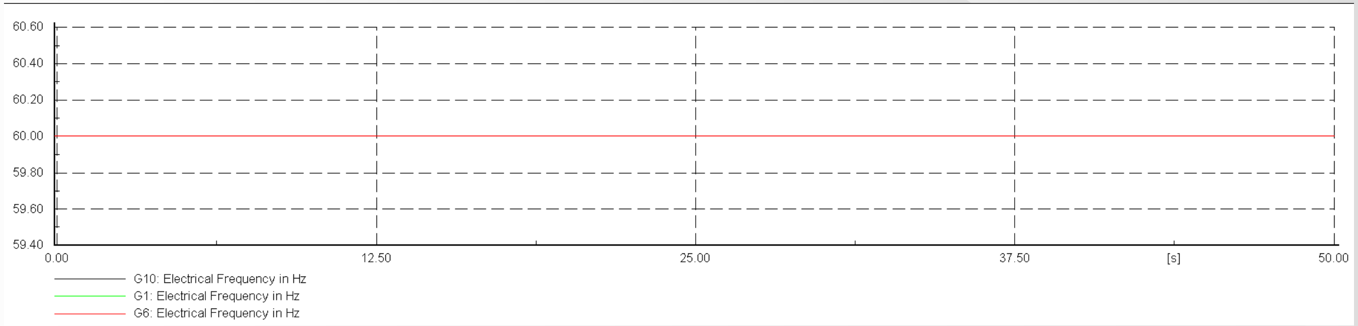


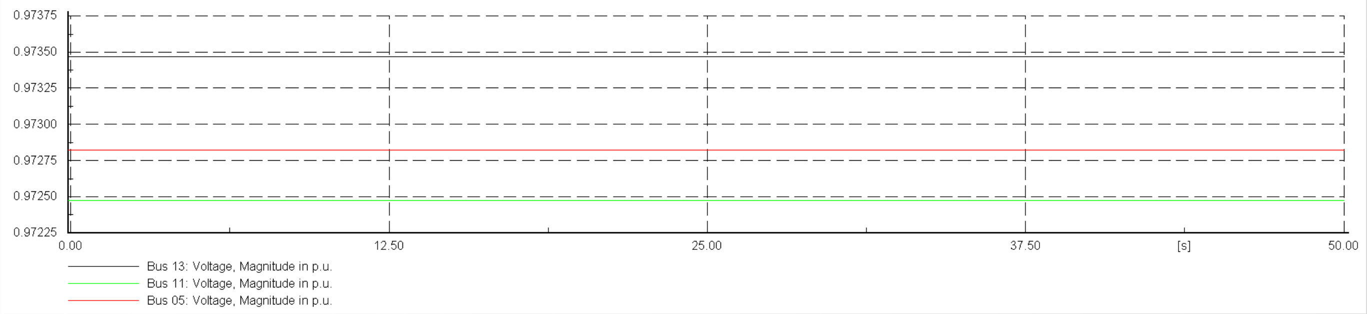
Attack Start

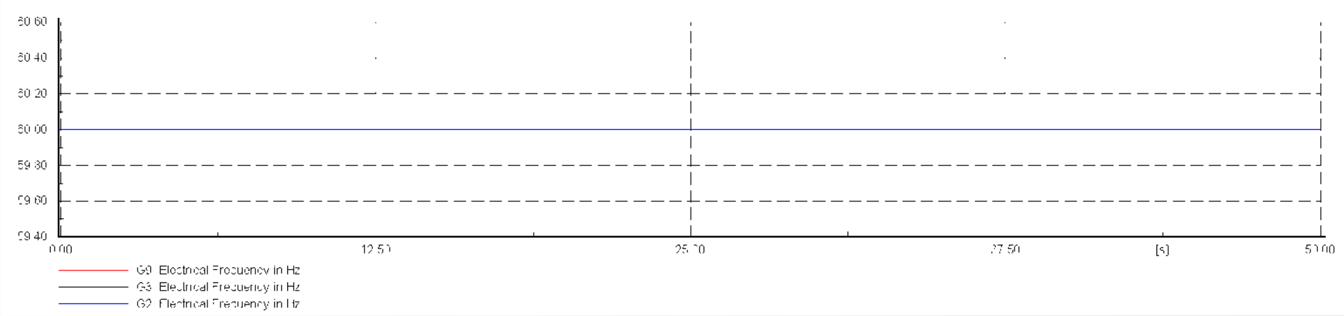
Attack End

Without ADS - Blackout

IEEE 39 bus system (DIgSILENT)

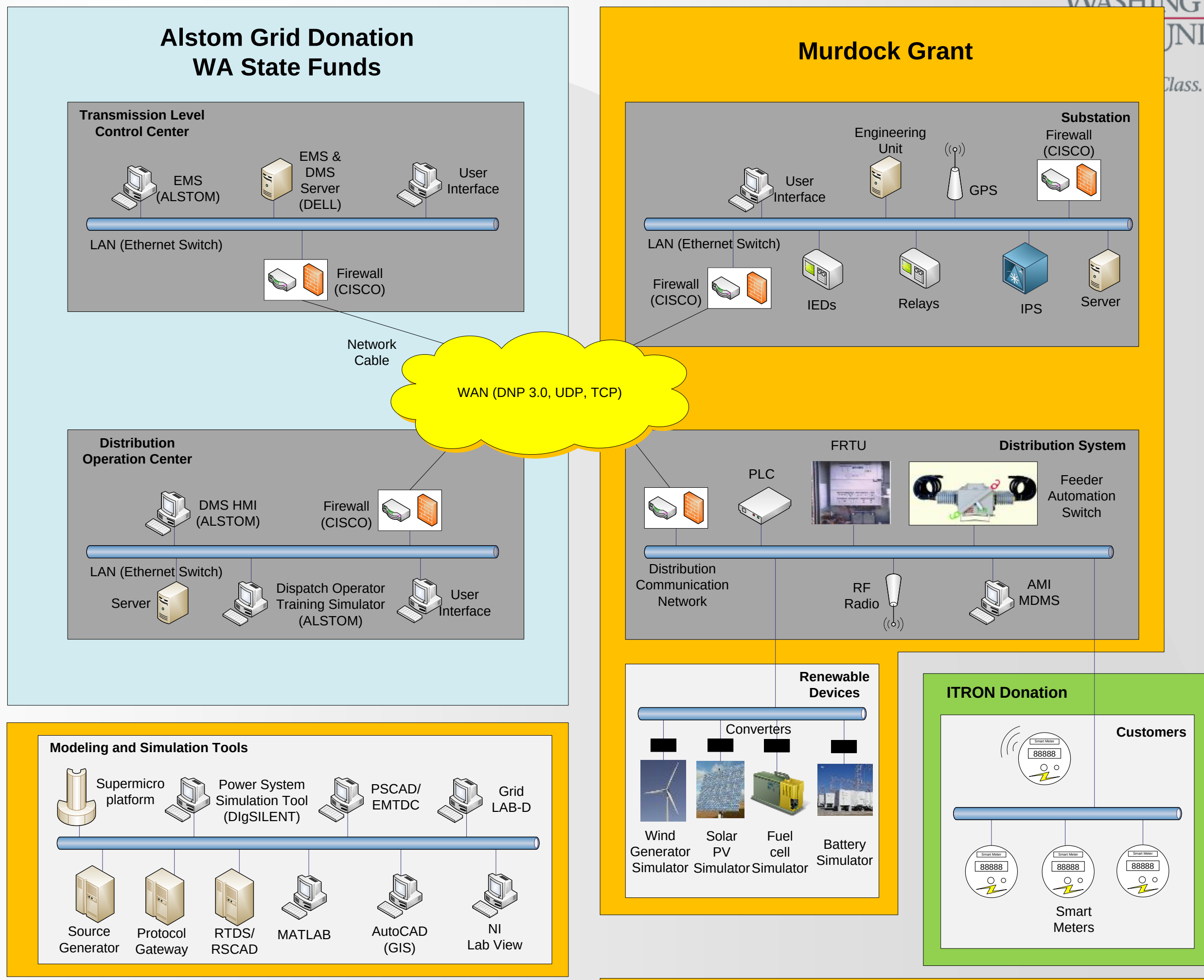




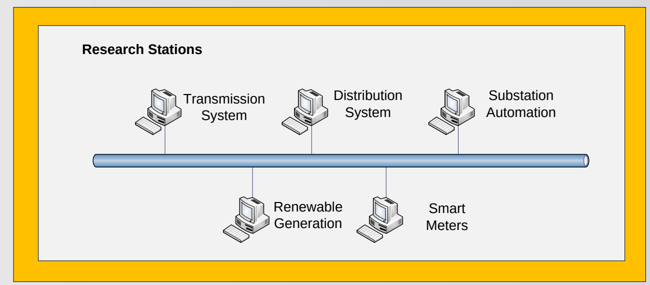


With ADS - Normal

WSU Smart City Testbed



HMI: Human Machine Interface
EMS: Energy Management System
DMS: Distribution Management System
LAN: Local Area Network
WAN: Wide Area Network
RTDS: Real Time Data Simulator
IED: Intelligent Electronic Device
AMI: Advanced Metering Infrastructure
MDMS: Meter Data Management System
PLC: Power Line Communication
FRTU: Feeder Remote Terminal Unit
ICCP: Inter Control Center Communication Protocol
IPS: Intrusion Prevention System



Conclusions and future work

- Substation cyber security enhancement
- Anomaly detection using proposed Integrated IDS
- Attack similarity and Impact factor analysis
- Vulnerability assessment by cyber-physical testbed
- More protocols and more anomaly indicators
- Cyber-physical vulnerability analysis
- Coordinated simultaneous cyber attack detection
- Smart city testbed