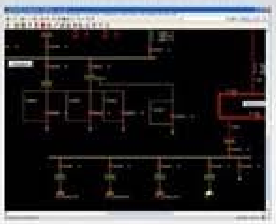
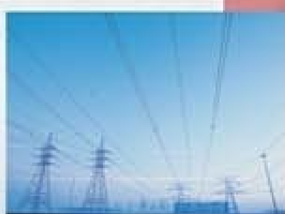
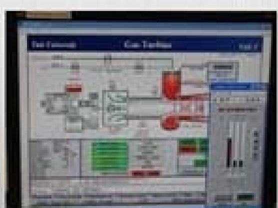






http://powercyber.ece.iastate.edu

Cyber-Physical Systems Security: Risk Modeling and Mitigation

Manimaran Govindarasu

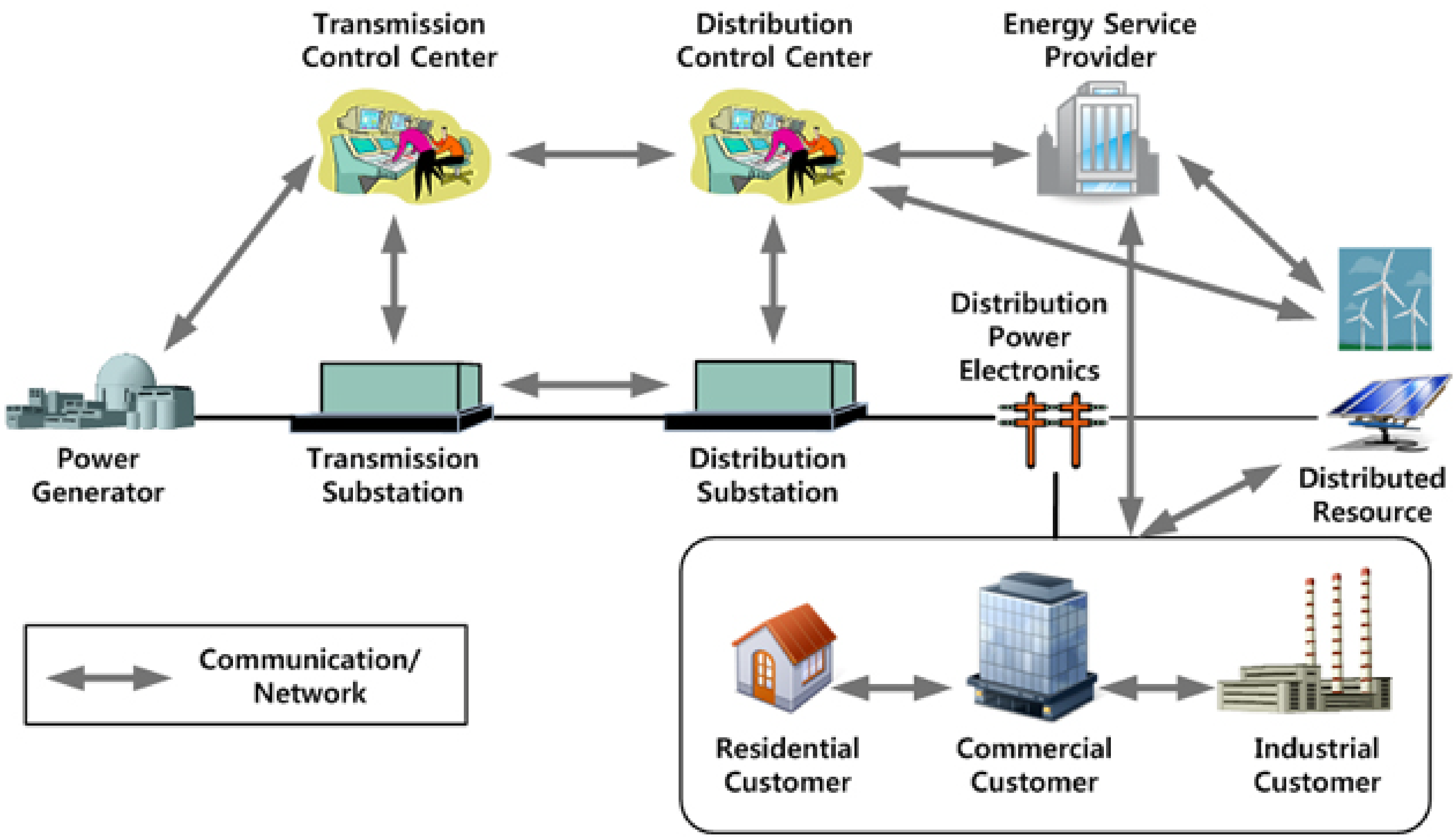
Dept. of Electrical and Computer Engineering

Iowa State University, USA

gmani@iastate.edu

Presented at Los Alamos National Laboratory, Nov. 2, 2010

Electric Power Grid: A Cyber-Physical System



Source: http://cnslab.snu.ac.kr/twiki/bin/view/Main/Research

Presentation Outline

1 Background & potential cyber attacks

2 Risk mdeling framework

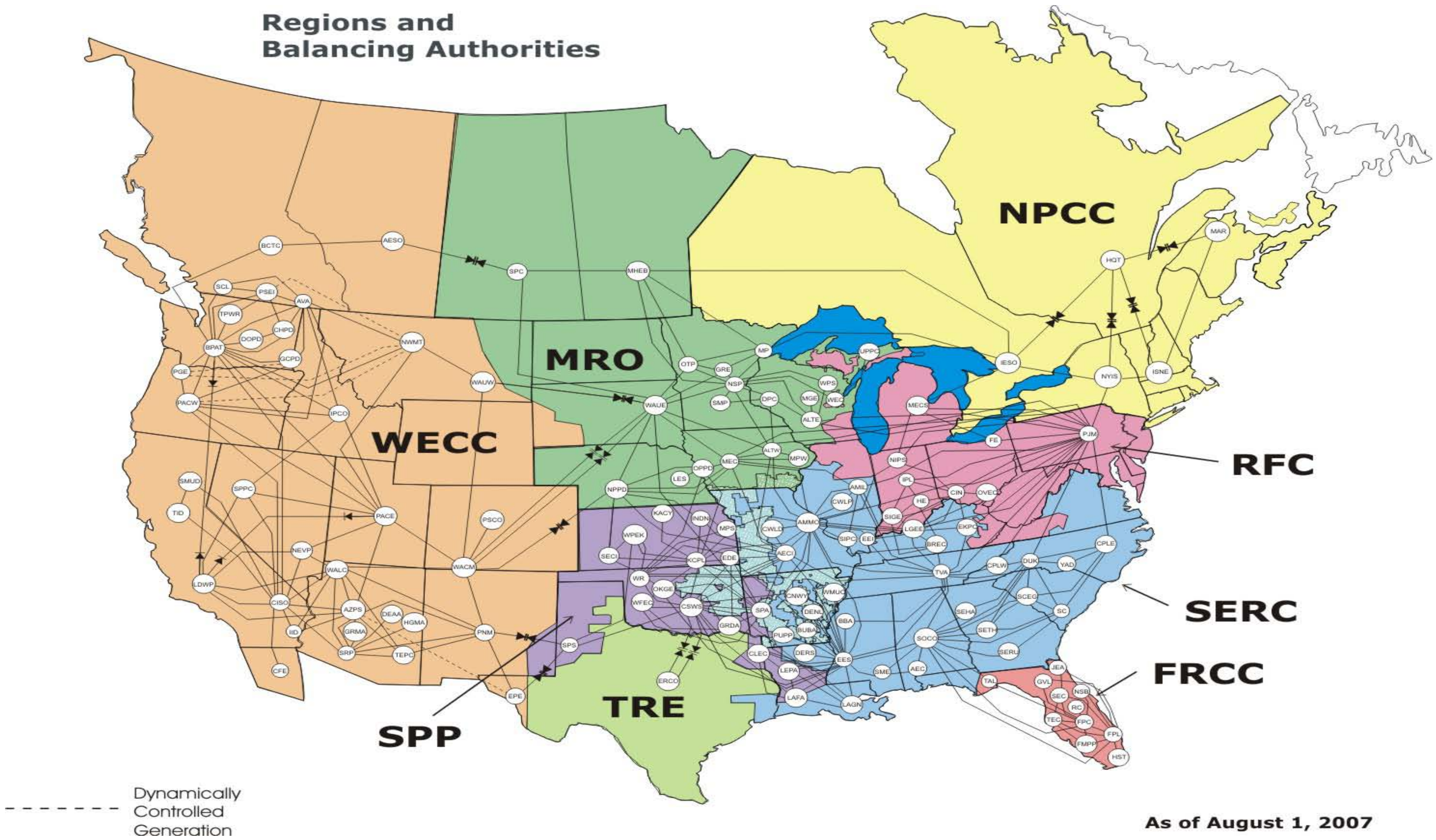
3 Case 1 - Intrusion-based attacks on substation

4 Case 2 – Data integrity attacks on wide area control

5 SCADA Security Testbed

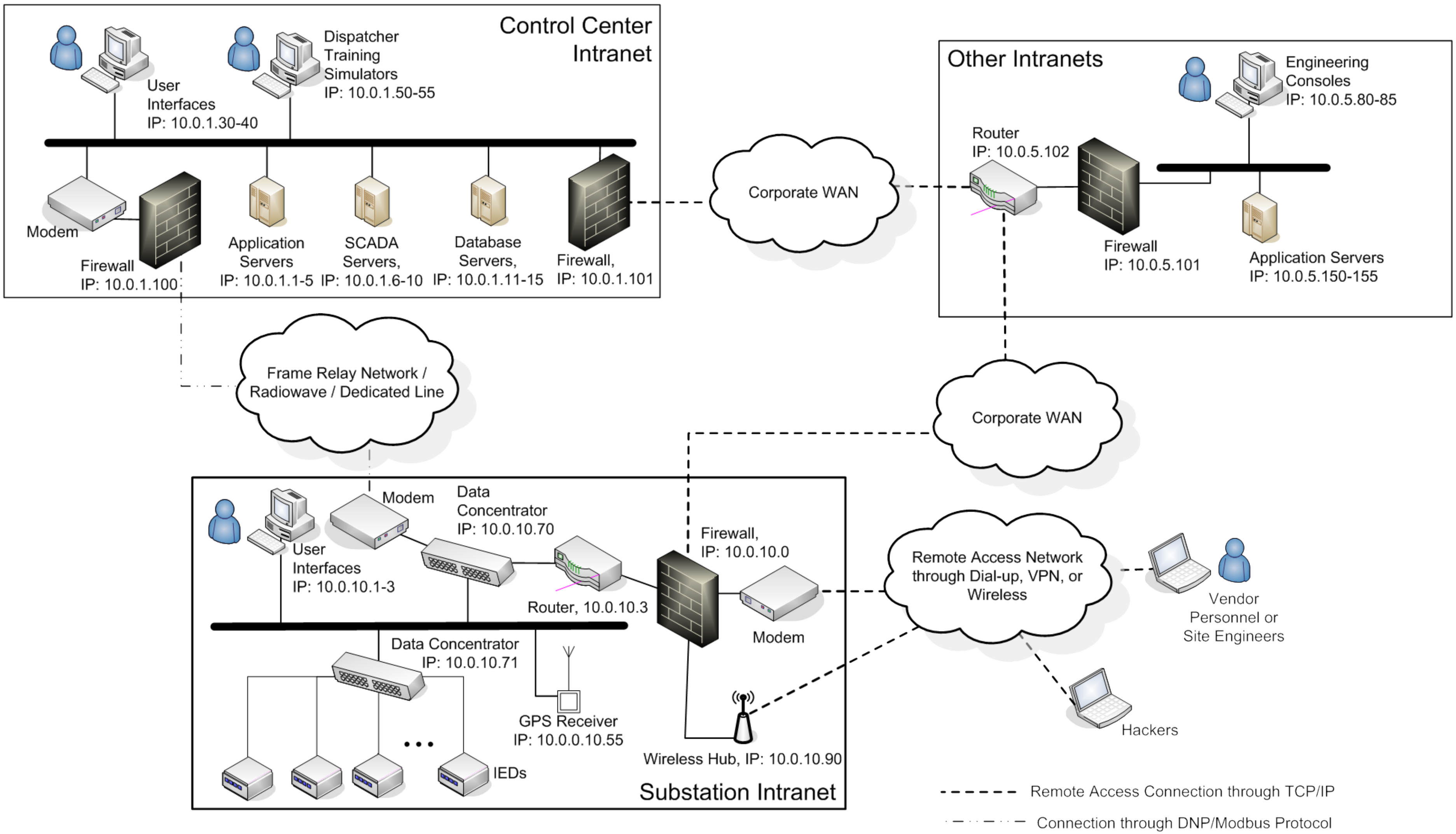
6 Conclusions

Power Grid in the U.S. – Regions & BA



Source: NERC

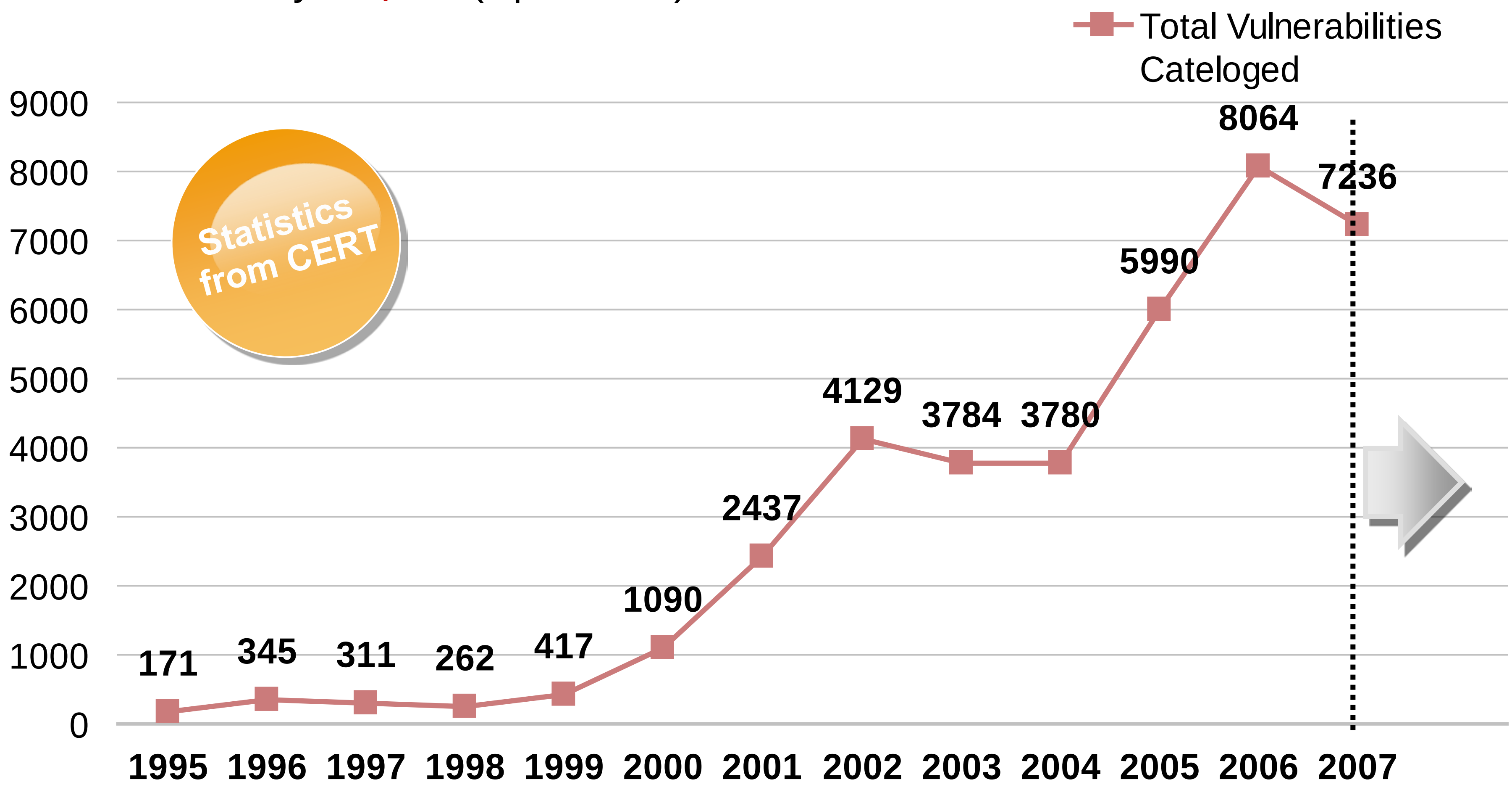
SCADA control network of power system



Statistics of Cyber Vulnerability

PowerCyber

Total vulnerability: **39,490** (Up-to-date)



Cyber threat to power grid are real …

CIP Report, General Accounting Office, March 2004

"*There has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders*"

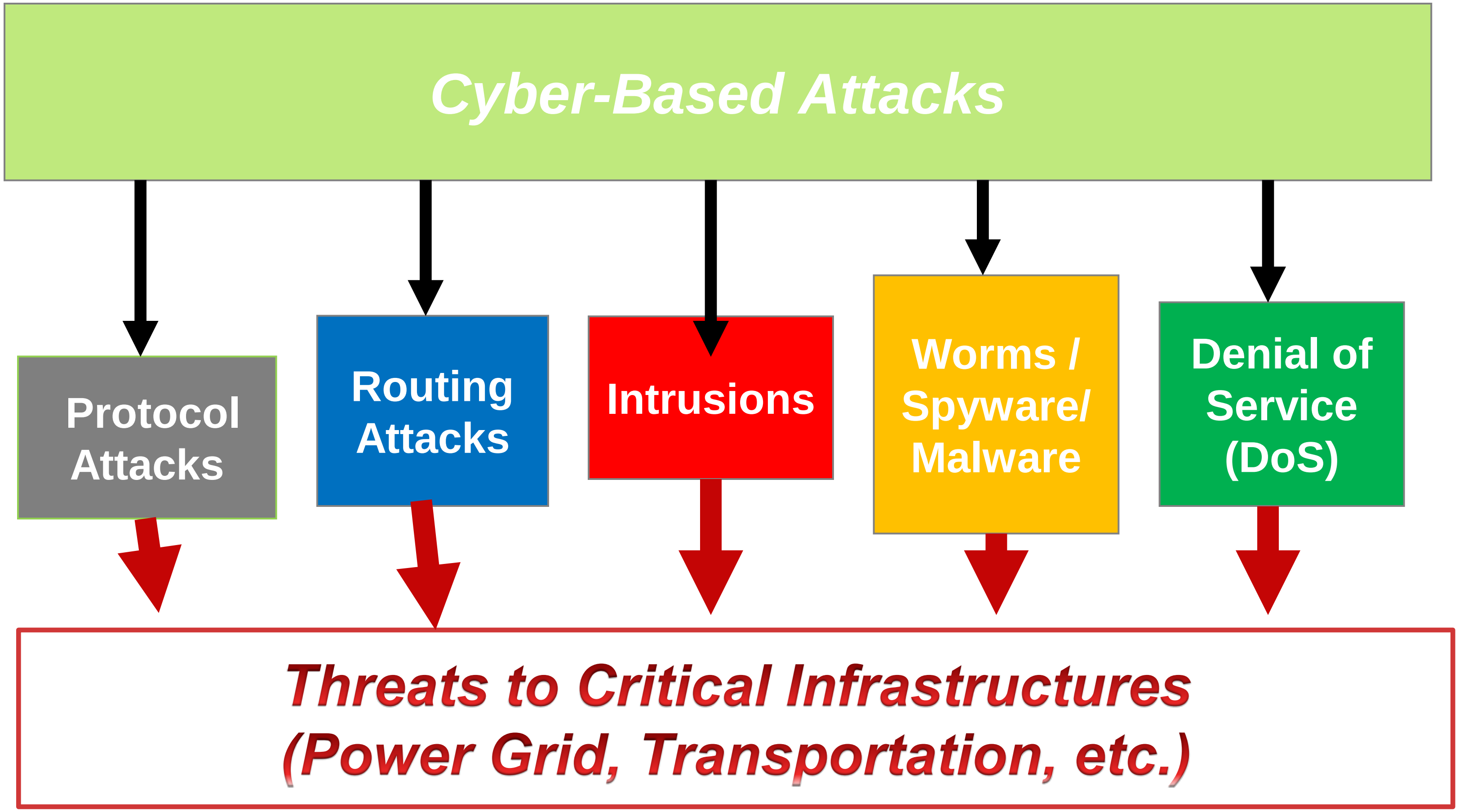
Repository for Industrial Control System (RISI) incident report, March 2010

- # industrial cyber incidents has been stable, expected to rise
- Power and utilities: 13 reported incidents in the last 5 years
  (30% increase from previous 5 years; Total: 28 incidents)

McAfee report – "In the Crossfire: Critical Infrastructure in the Age of Cyber War"

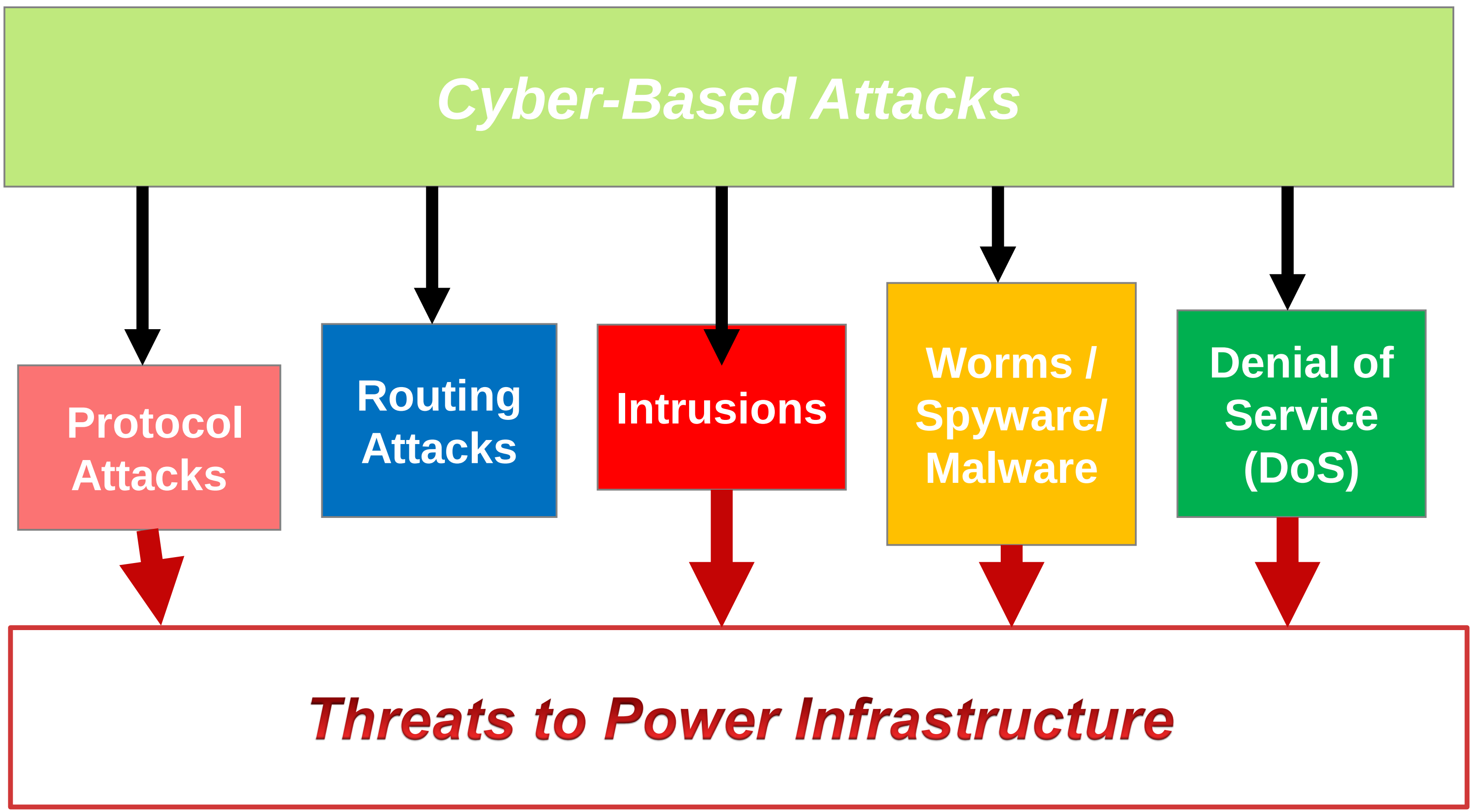
- Shows similar data and increase in cyber incidents

Cyber Threats to Critical Infrastructures

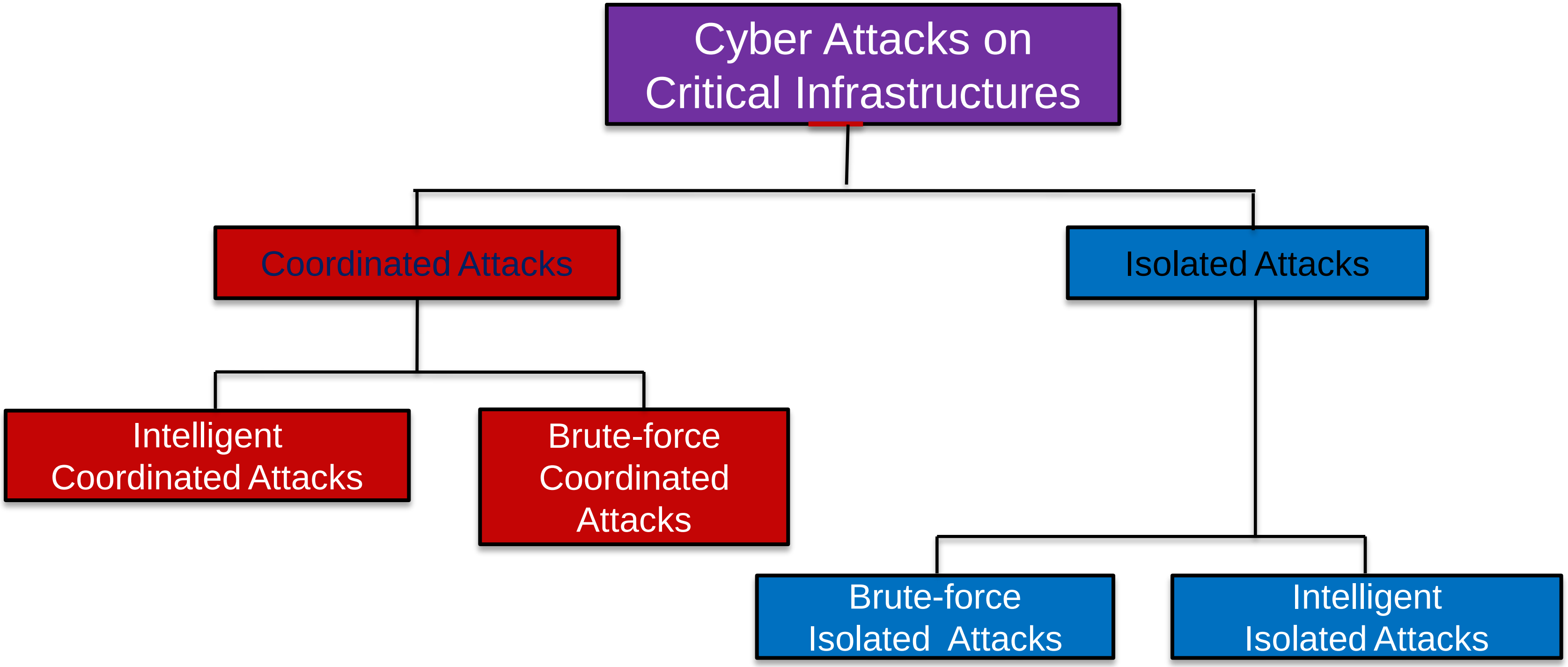


[General Accounting Office, CIP Reports, 2004 to 2010]; [NSA "Perfect Citizen", 2010]:
Recognizes that critical infrastructures are vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

Types of Cyber-Attacks on Power Systems

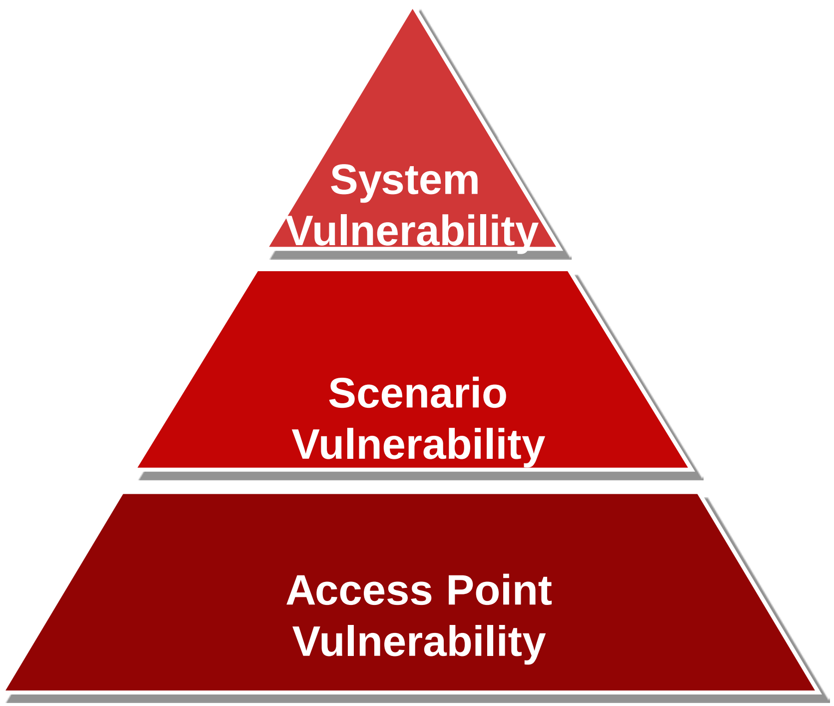


Attack Classification

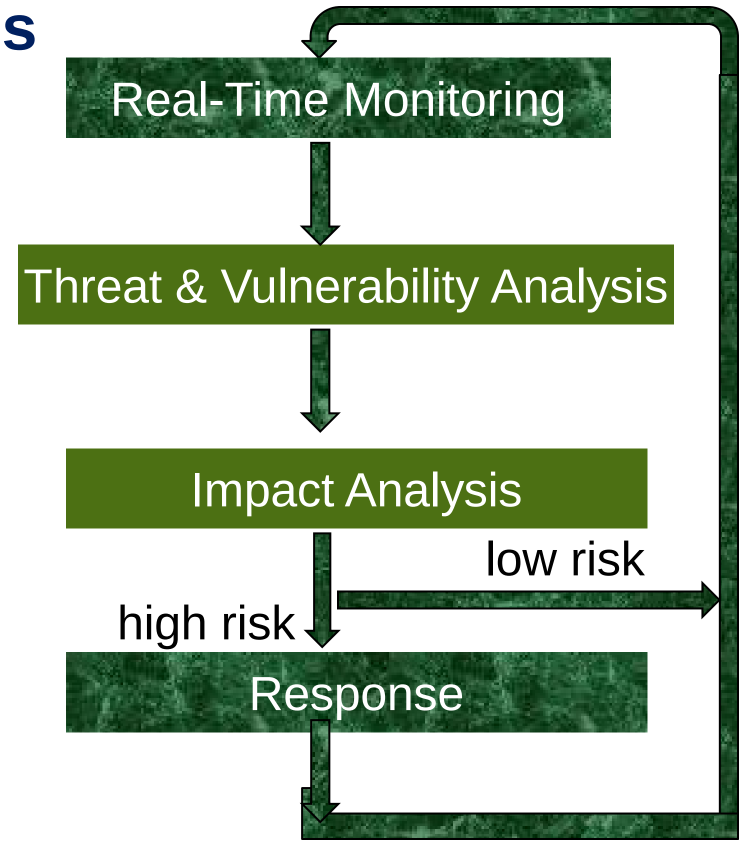


1. Cyber-Physical System Security Modeling

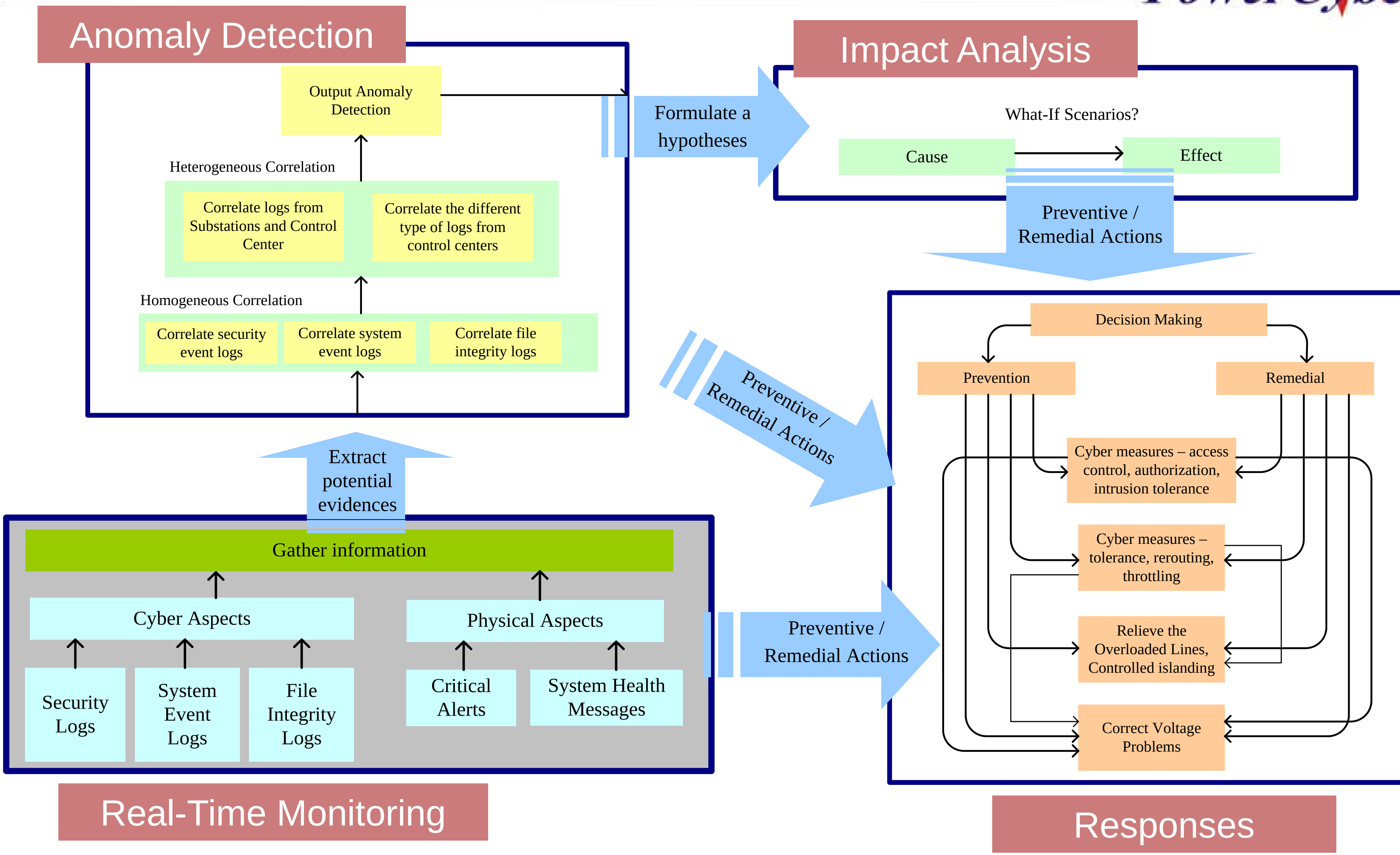
- **Risk Assessment & Risk Mitigation** (GAO CIP Report, 2010)
- **Security Investment Analysis**



Hierarchical modeling



Risk Modeling and Mitigation Framework (2)



C. Ten, G. Manimaran, C.C.Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” IEEE Trans. on SMC – Part A, July 2010

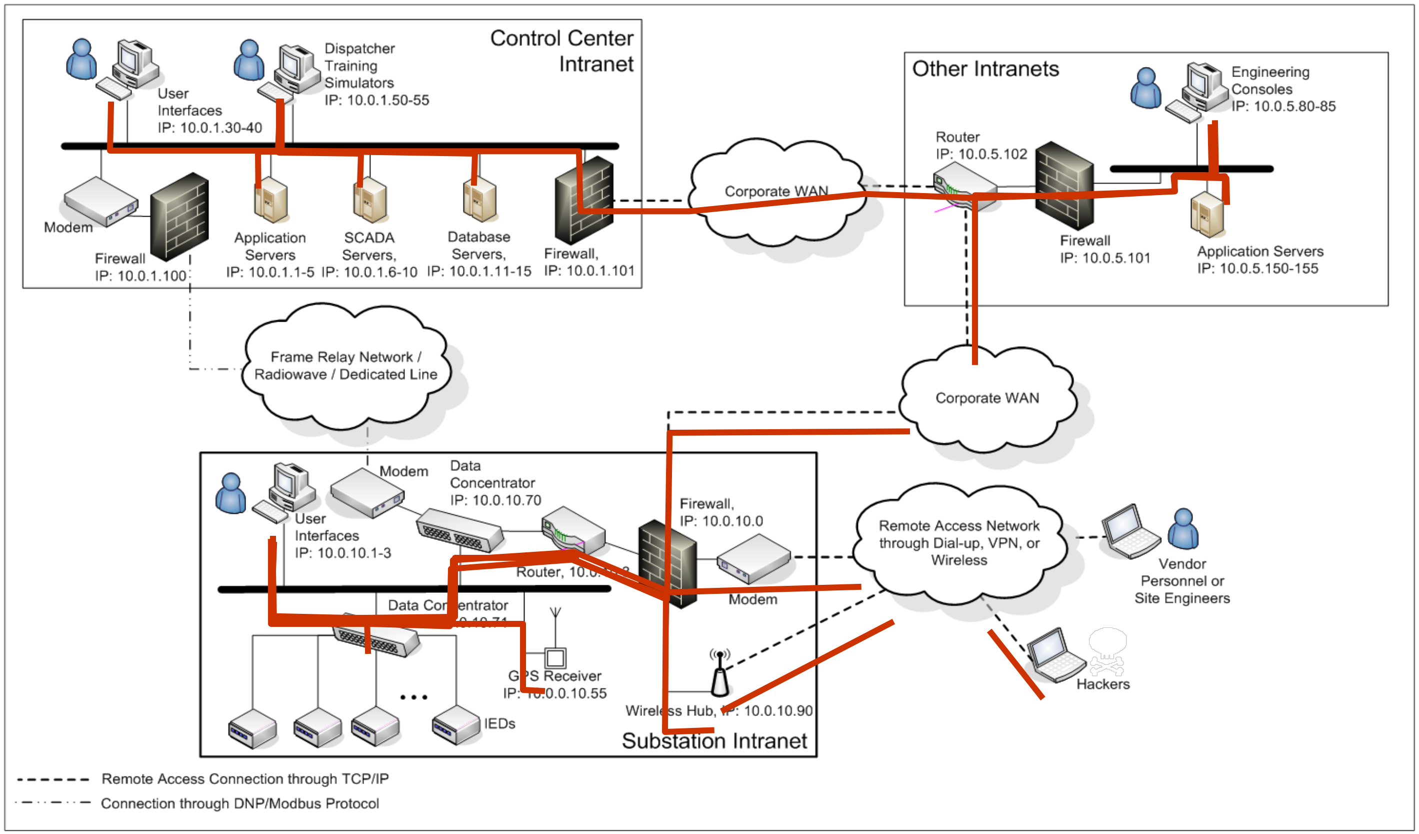
Risk Modeling Intrusion Attacks

C. Ten, C.C.Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems", IEEE Trans. Power Systems, Nov. 2008.

Intrusion Scenarios

PowerCyber

The Processes of Hacking: *Footprint*, *Scan*, *Enumerate*, and *Exploit*



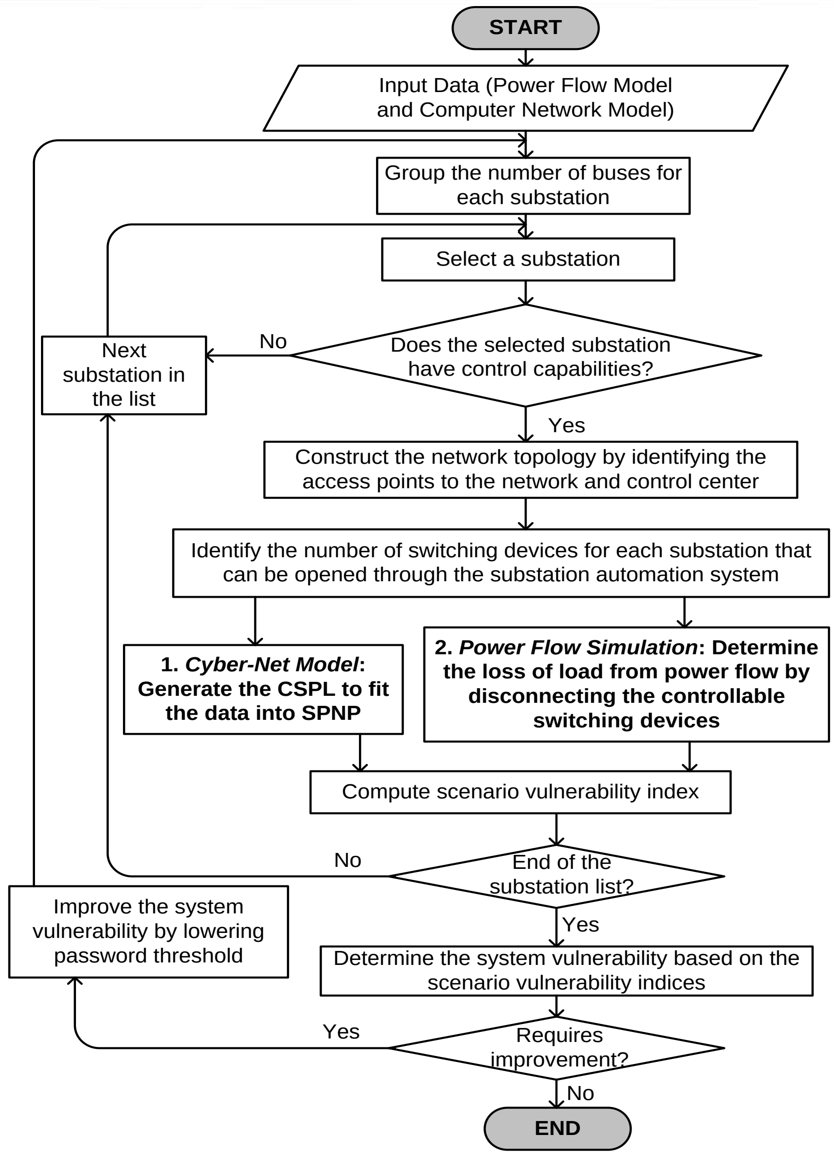
Step [illegible] Attempt [illegible] re [illegible] protected.

The Intrusion Process

Steps to penetrate into a network involve:

Footprinting	▪ **Identification of organization's security posture** ▪ locations of the substations, control centers, or generating units ▪ IP addresses and email address of the utility company
Scanning	▪ **Exhaustively identify the possibile access points** ▪ Access points: Wireless connection, LAN, VLAN, VPN, and ▪ Tools: War dialing or Traffic sniffer
Enumerating	▪ **Listing all active ports available** on a target IP address ▪ *Password guessing*: Dictionary, brute-force, or social engineering
Exploit!	▪ This is where an attacker **got lucky**! **But we do not want them to be lucky…**

Risk Analysis Framework



Key steps

1. Construct a cyber-net model

    - model the access points & associated vulnerabilities

2. Construct a GSPN: Stochastic Petri Net

    - compute steady state probabilities

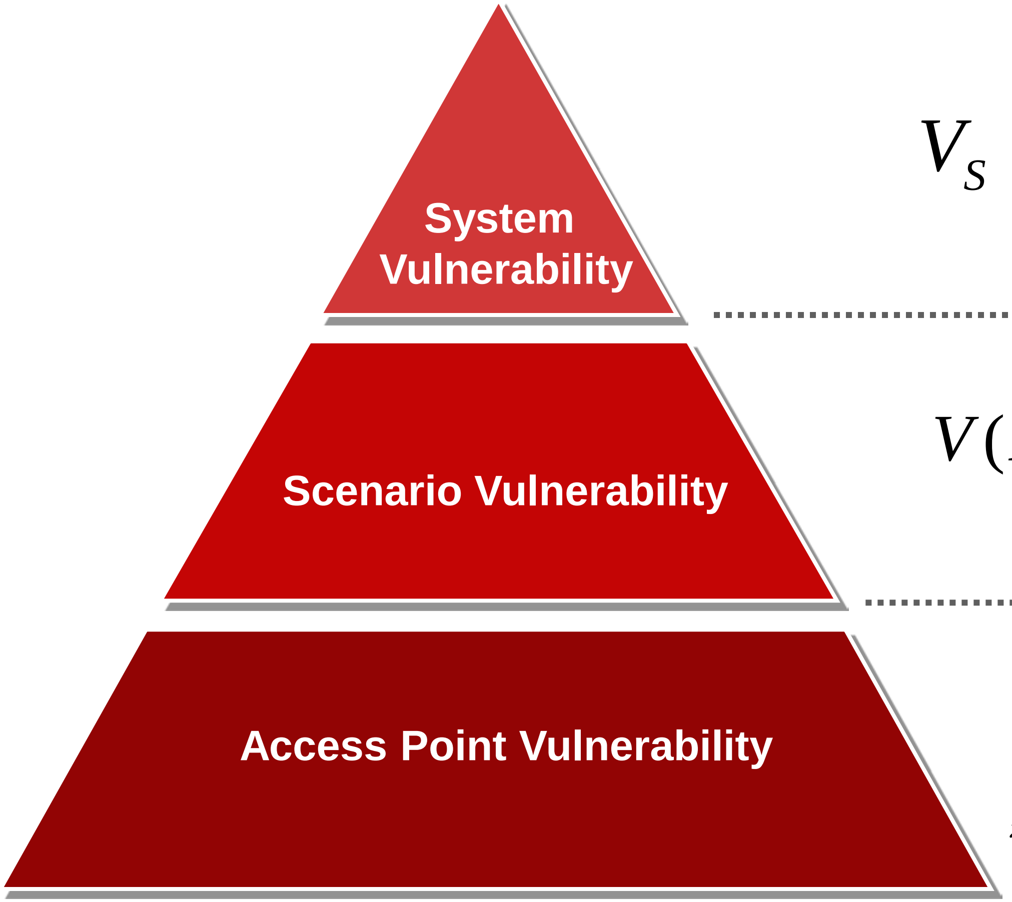
3. Perform impact analysis for the most likely scenarios

    - using Power Flow Simulation

4. Calculate Risk = Vulnerability x Impact

Risk Modeling of Intrusions …

The hierarchical relationship among ***system***, ***scenario***, and ***access point*** vulnerability



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

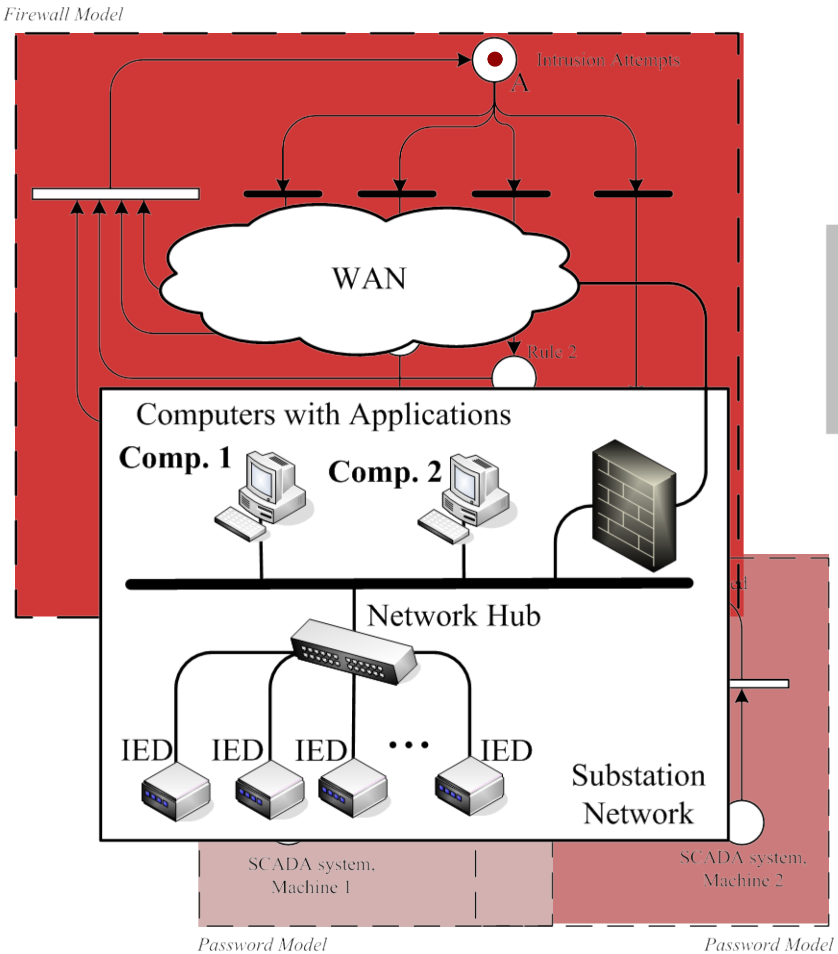
$$V(I) = \left\{V\left(i_1\right), V\left(i_2\right), \ldots, V\left(i_K\right)\right\}$$

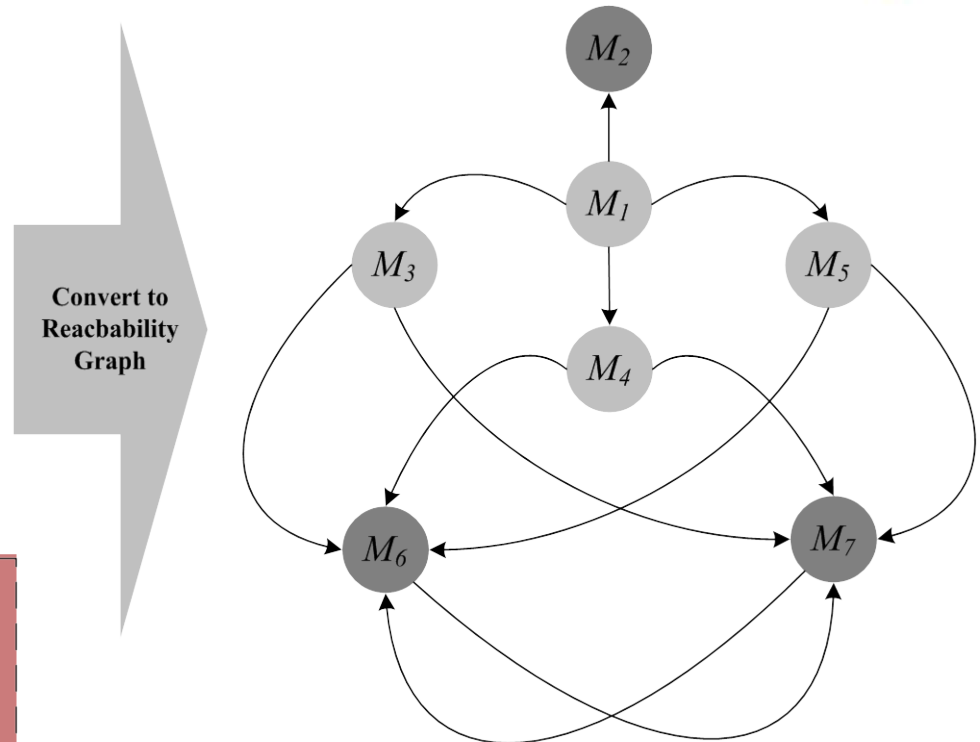
$$V(i) = \sum_{j \in S} \pi_j \times \gamma_j$$

π_j **Probability of intrusion** thro access point ***j***

γ_j **Impact** due to compromise of substation ***j***

Cyber model: 1 Firewall - 2 Machines (substation)





M_1=[1 0 0 0 0 0 0 0]

M_2=[0 1 0 0 0 0 0 0]

M_3=[0 0 1 0 0 0 0 0]

M_4=[0 0 0 1 0 0 0 0]

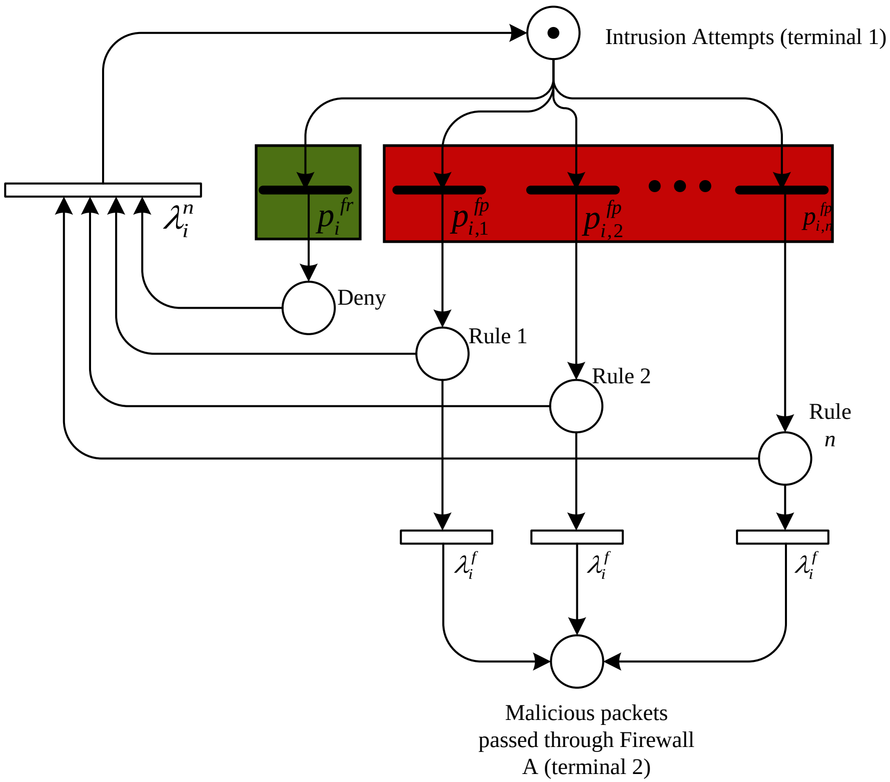
M_5=[0 0 0 0 1 0 0 0]

M_6=[0 0 0 0 0 0 1 0]

M_7=[0 0 0 0 0 0 0 1]

Firewall Model

- **model: *n* paths correspond to *n* rules**



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

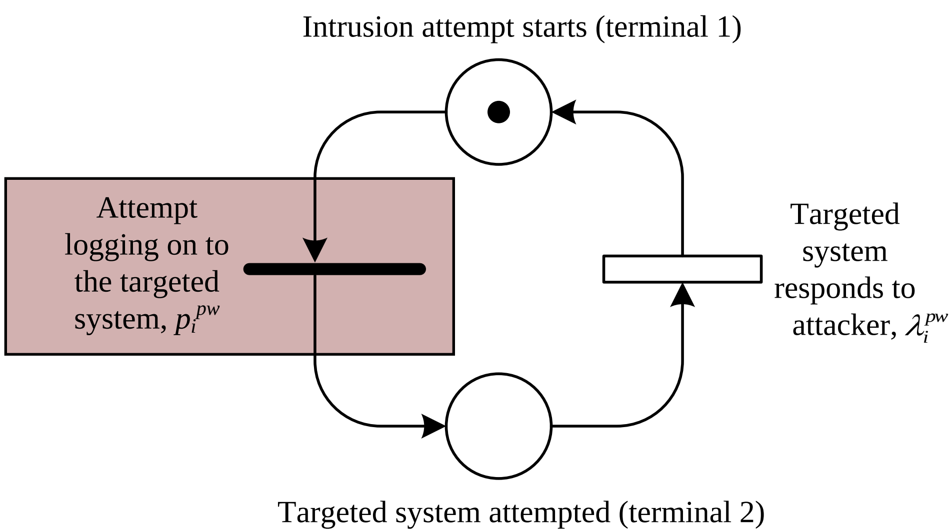
probability of the packets being *rejected*

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

denotes the total number of packets in the firewall logs

Password Model

- The **intrusion attempt to a machine** is modeled by a transition probability associated with a solid bar. An empty bar represents the *processing execution* rate that responds to each attack event
- **An account lockout feature**, with a limited number of attempts, can be simulated by initiating the ***N* tokens** (password policy threshold).



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

the intrusion attempt probability of a computer system, *i*

number of intrusion attempts

total number of observed records

Impact (factor) on power grid

Definition of Impact Factor

- Impact factor for the attack upon the power system is:

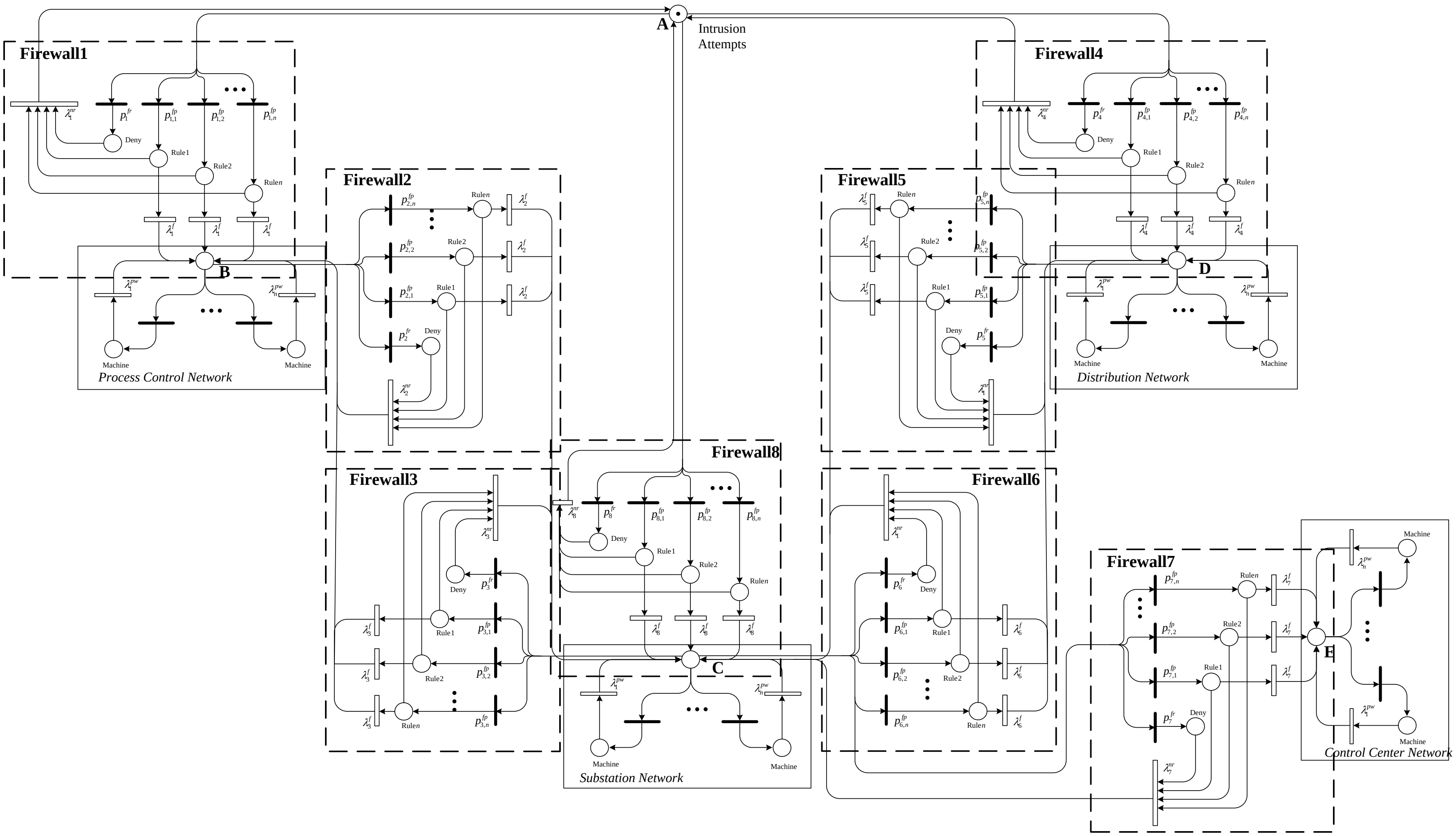
$$\gamma = \left(\frac{P_{LOL}}{P_{Total}} \right)^{L-1}$$

LOL: the loss of load for a disconnected substation

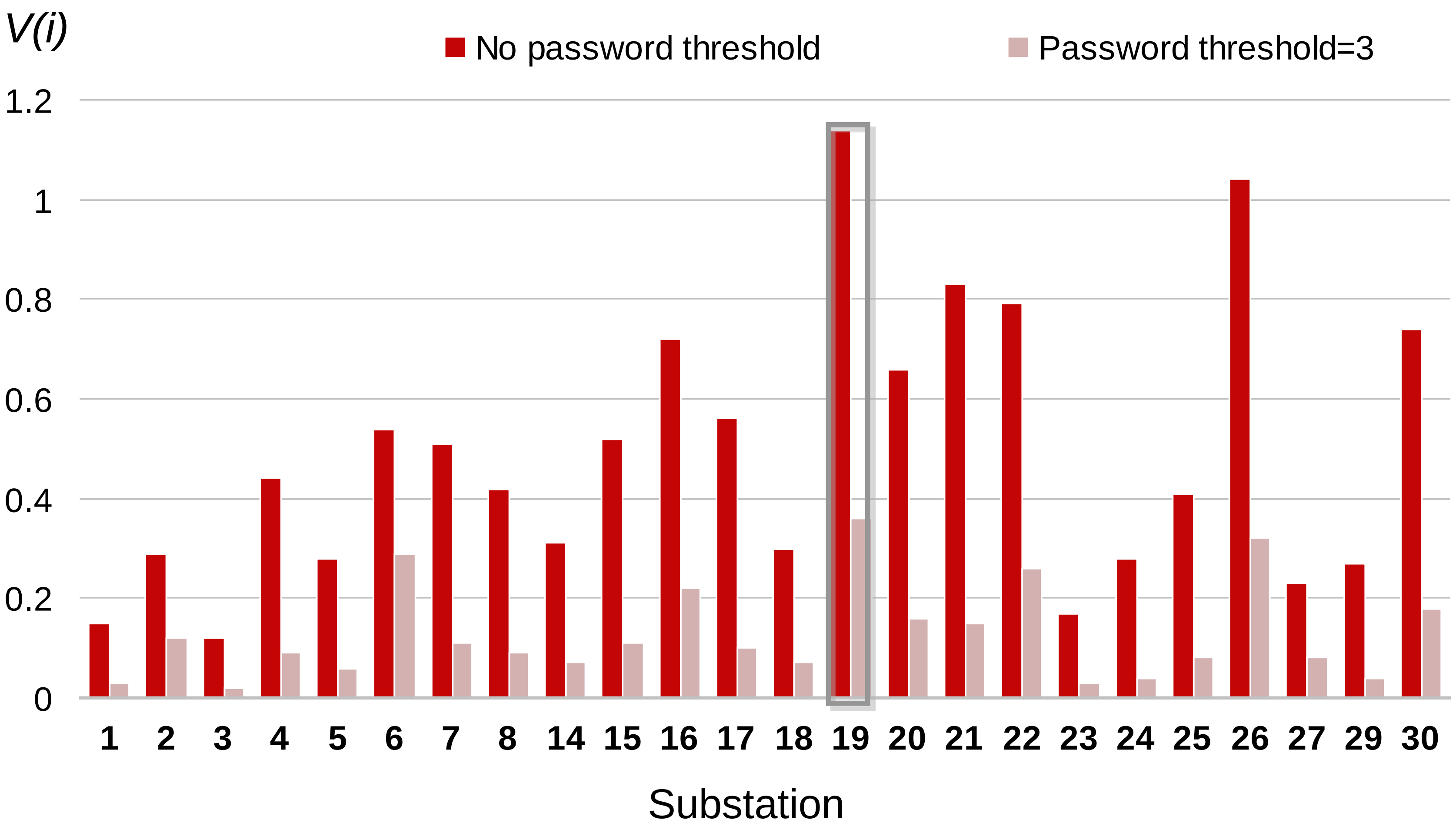
To determine the value of *L:*

- Start with the value of *L*=1 at the substation
- Gradually increases the loading level of the entire system without the substation that has been removed
- Stop when power flow diverges

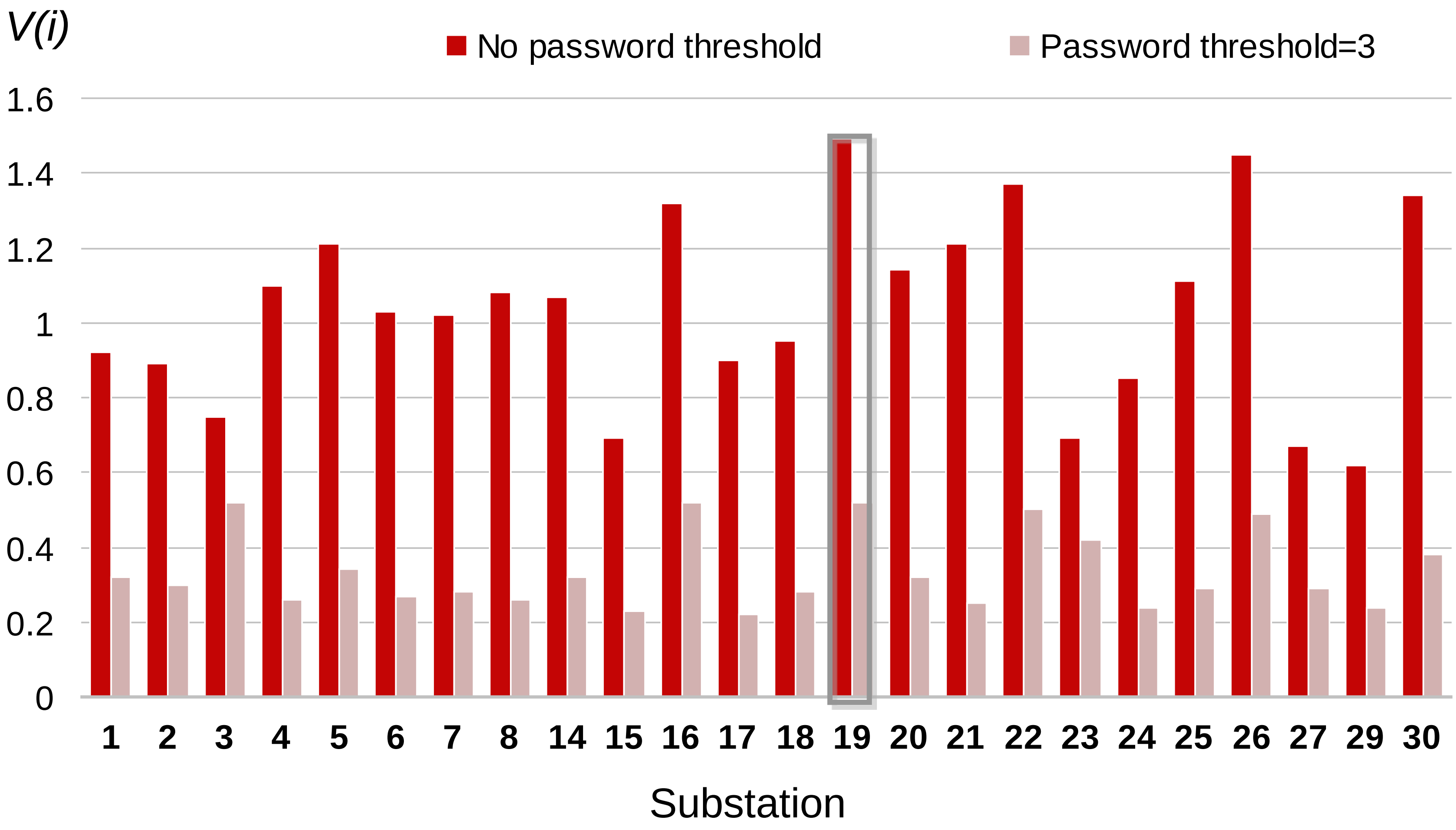
Case Study Setup (IEEE 30 Bus System)



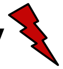
Vulnerability Evaluation - Outside Network



Vulnerability Evaluation - Within Network

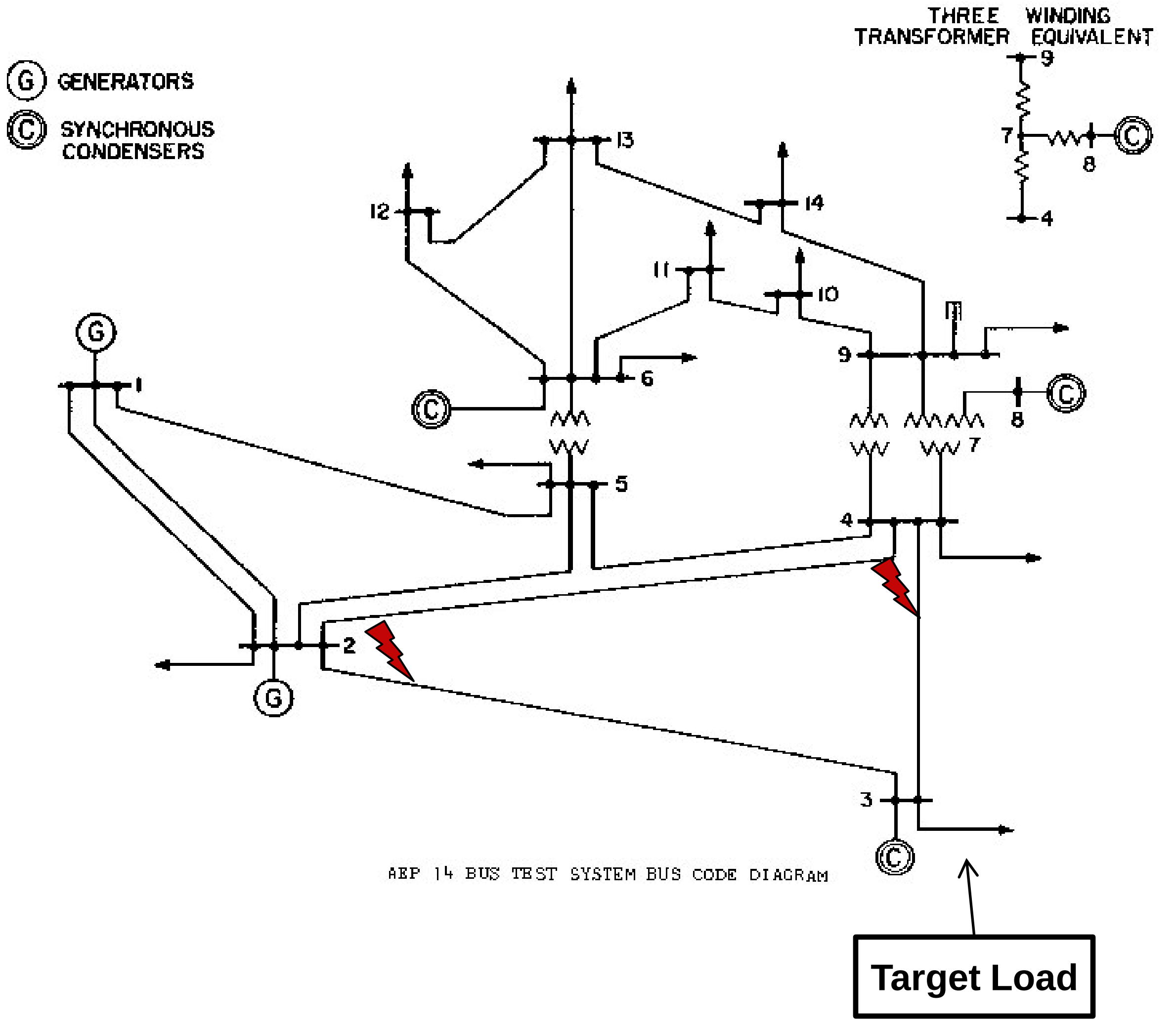


Coordinated Attacks

- **Example**
Tripping lines marked by  to ensure the load connected to bus 3 is deprived of or receives limited power supply.

- This result would be difficult to achieve with an isolated attack.

- The attack would require a good understanding of the system and operation, i.e., the control center for different components in the system.

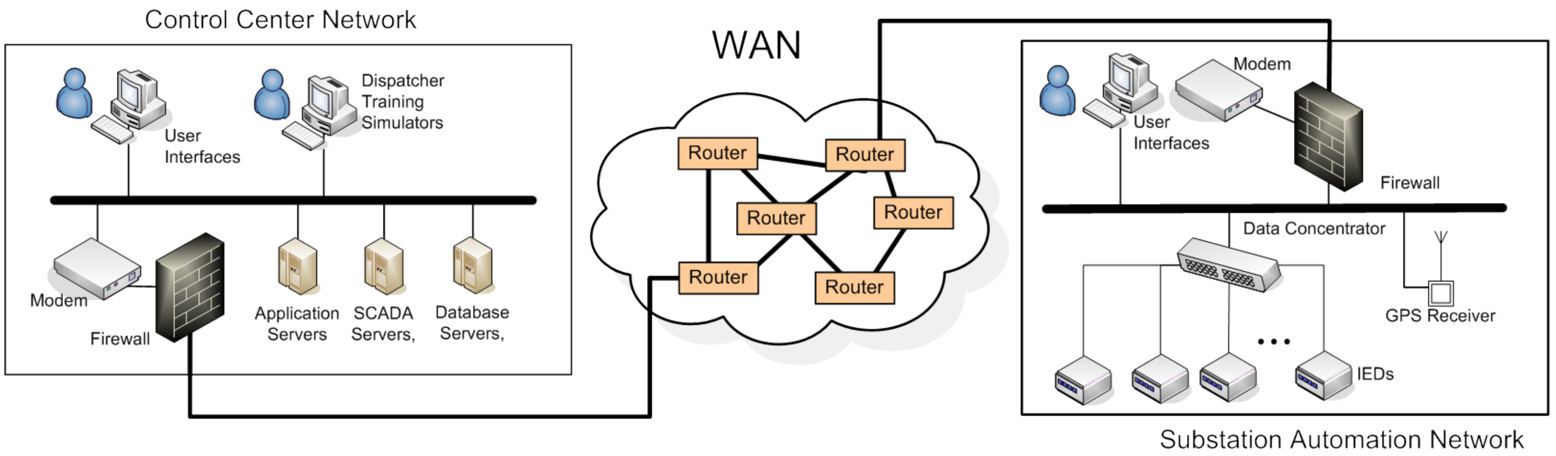


Data Integrity Attacks and Impacts on Wide Area Control

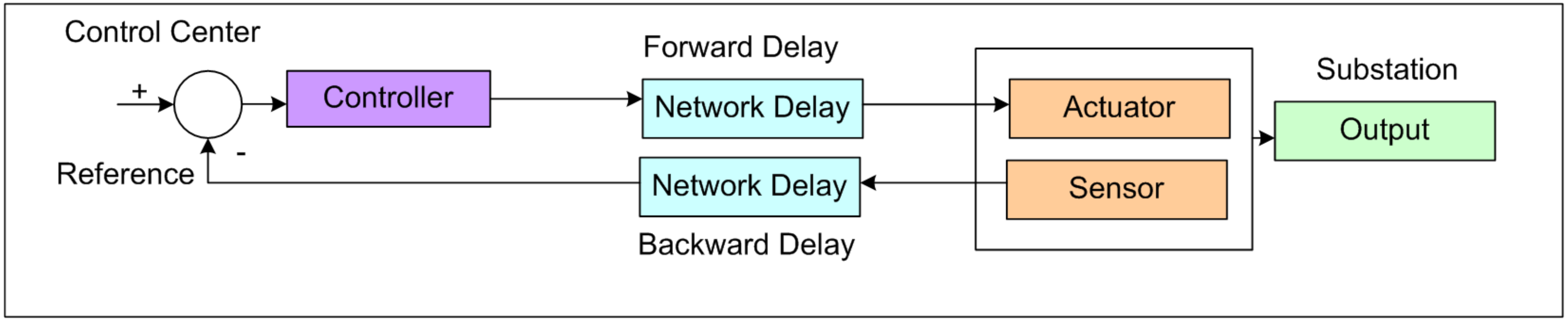
S. Siddharth and G. Manimaran, “Data integrity attacks and their impacts on SCADA control system” IEEE PES General Meeting, 2010.

The SCADA Network: Control system view

Control Center Schematic

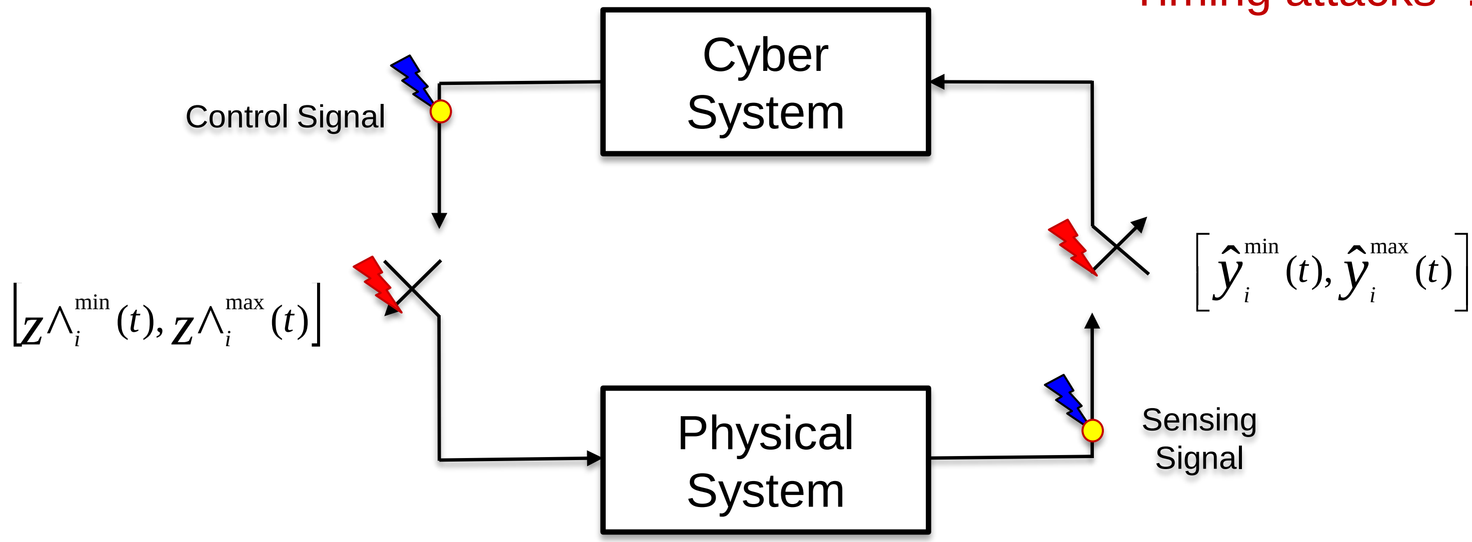


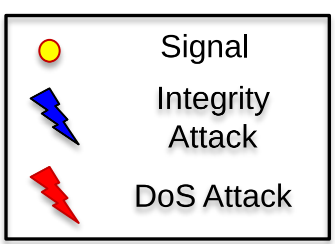
Control System Schematic



Control System – Attack Modeling

- Man-in-the-middle attacks
- Data integrity attacks
- Denial of service attacks
- Timing attacks …

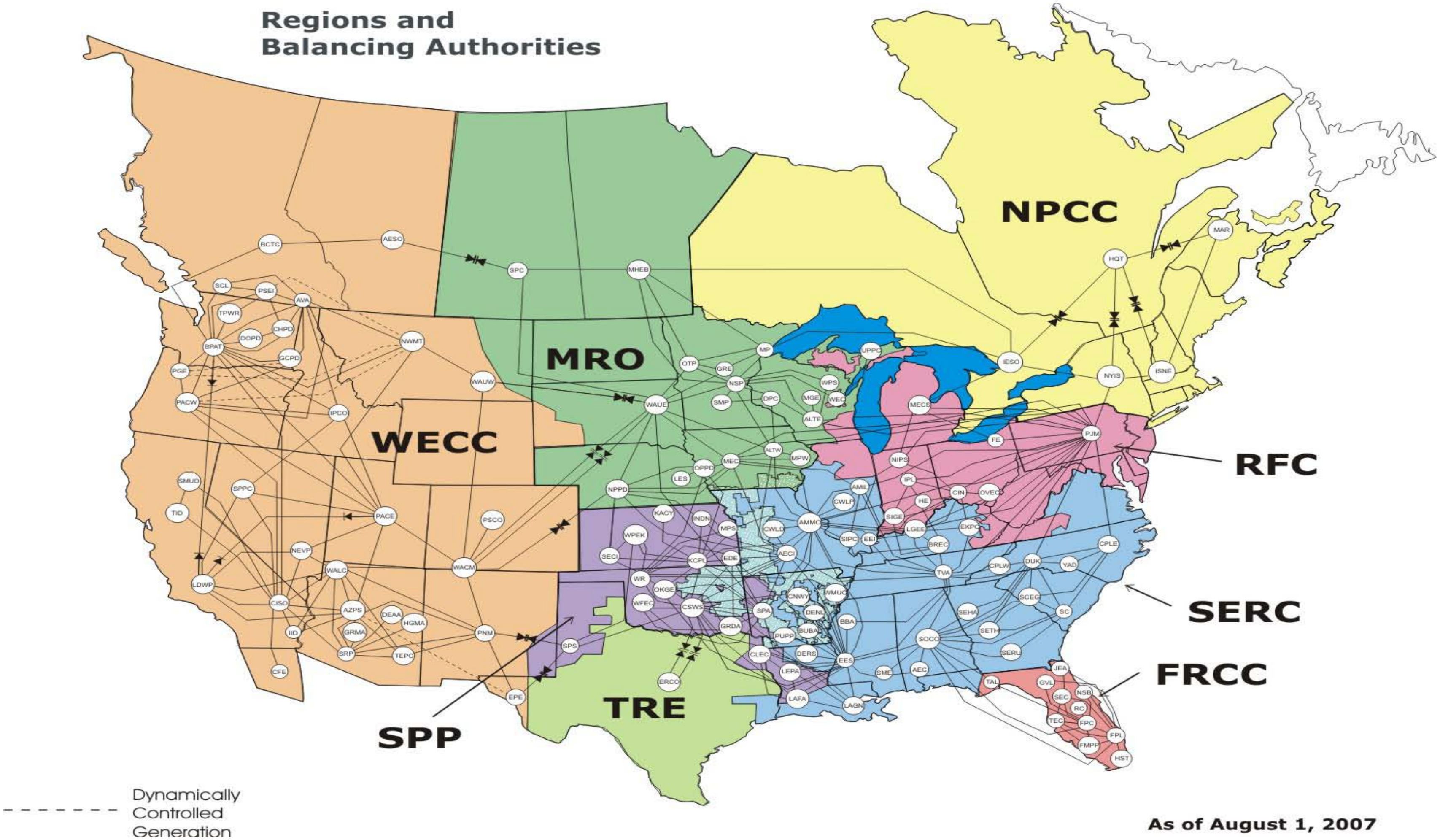




Duration of the attack $\tau_A = [t_s, t_e]$

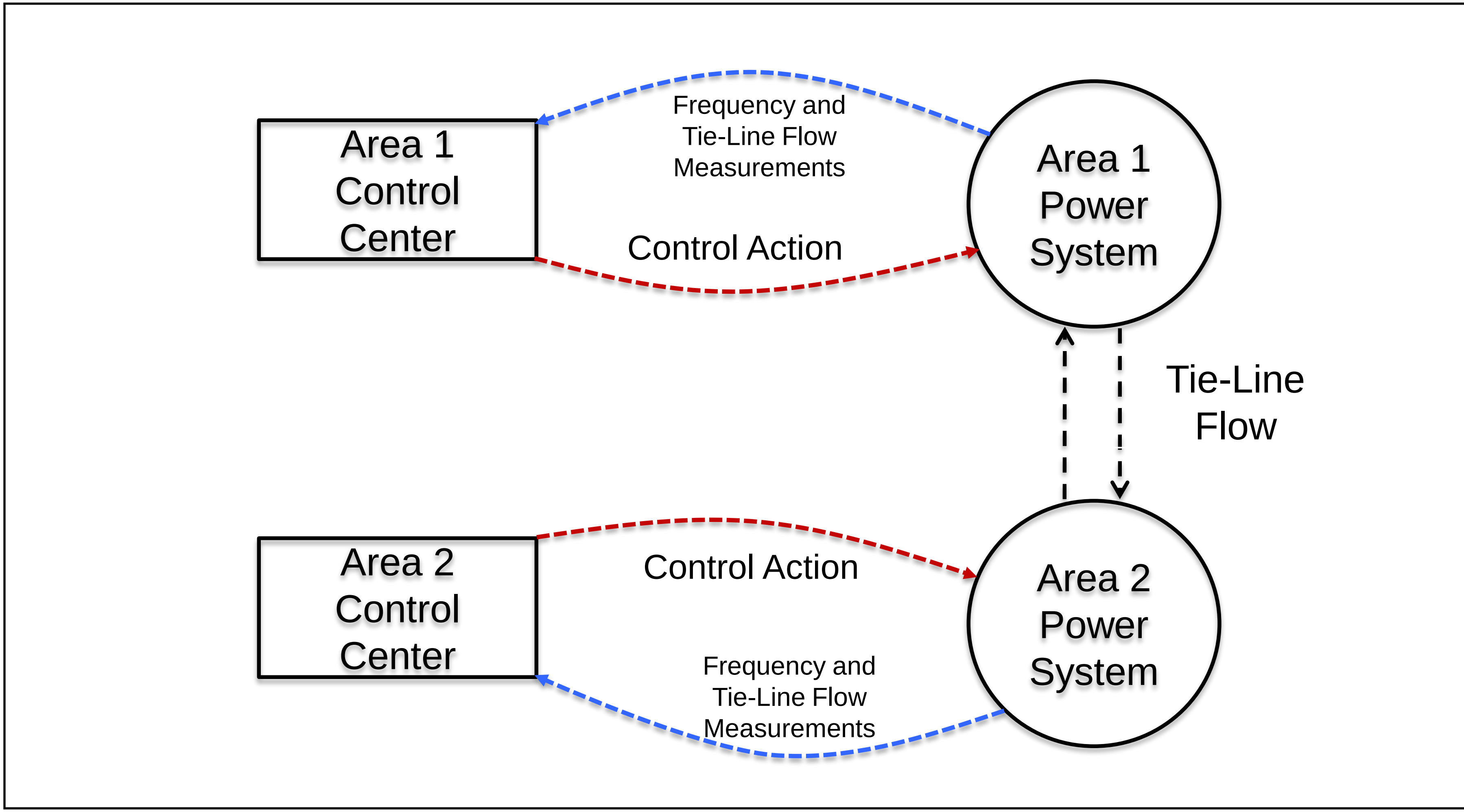
Y. Huang, A. A. Cardenas, S. Sastry, "*Understanding the Physical and Economic Consequences of Attacks on Control Systems*", Elsevier, International Journal of Critical Infrastructure Protection 2009.

Balancing Authorities in the U.S.

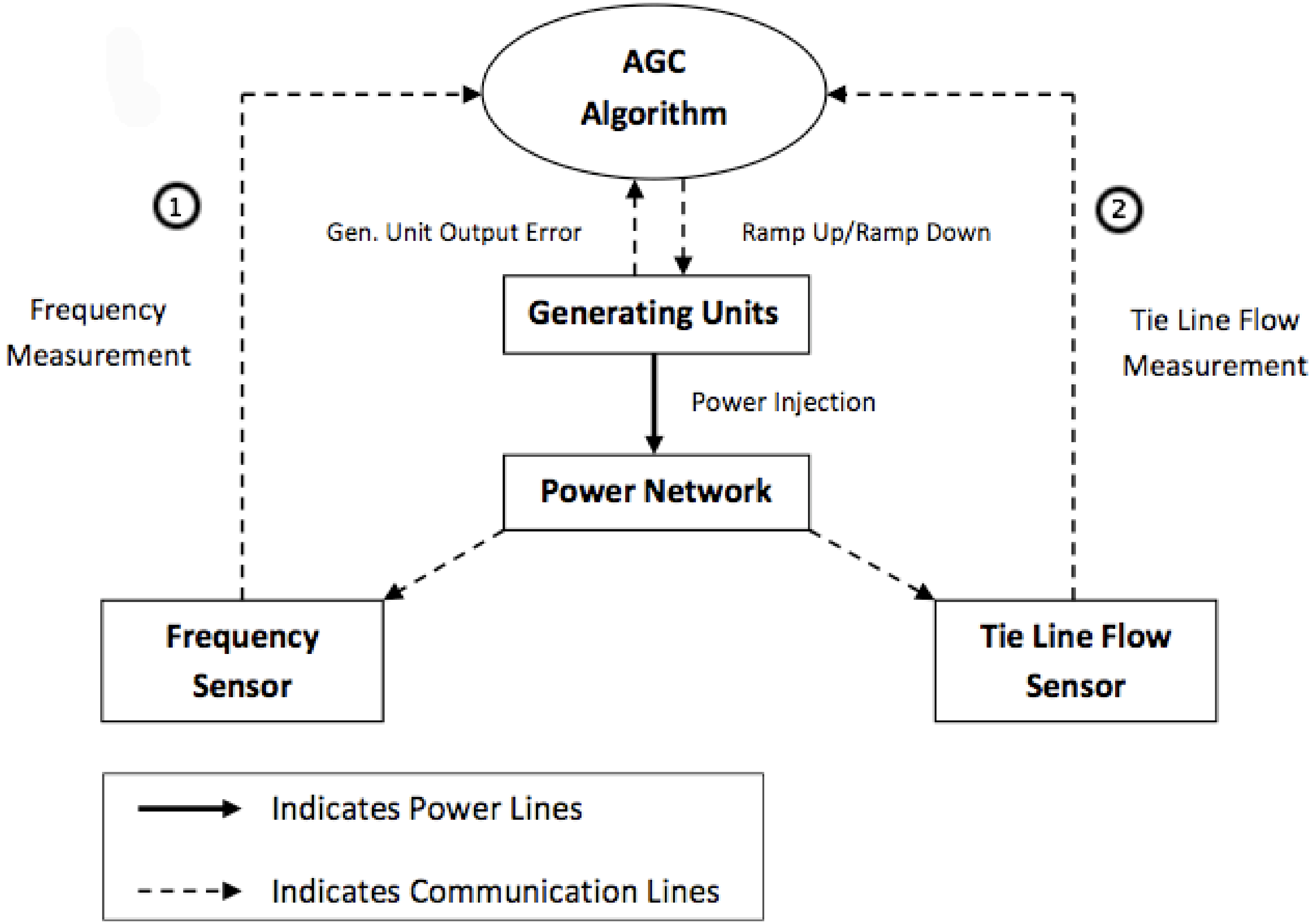


Source: NERC

Automatic Generation Control (AGC)



The AGC Algorithm



- **Inputs to AGC algorithm:** **Frequency deviation Δf , Net tie-line flow ΔP_i**

ACG: The Area Control Error

- The *Area Control Error* (ACE) represents the shift in generation required to restore frequency and net interchange
- Is a measure of the error in total generation from total desired generation
- Calculation of ACE

$$\mathbf{ACE_i = \Delta P_i + \beta_i \Delta f} \quad \textbf{(1)}$$

$$\Delta P_i = \sum (AP_i - SP_i) \quad (2)$$

$$\beta i = \frac{1}{R_i} + D_i + D_{Li} \quad (3)$$

AGC Operation (cont.)

- **In general, a load increase of ΔP_L in area 1 of an 'n' area system will result in a frequency deviation of**

$$\Delta f = \frac{-\Delta P_L}{D + \frac{1}{R_1} + \frac{1}{R_2} + ... + \frac{1}{R_N}} \qquad (4)$$

- **and a change in tie-line flow of**

$$\Delta P_{net\,\mathrm{int}_1} = \frac{(-\Delta P_L)\left(\frac{1}{R_1} + \frac{1}{R_2} + ... + \frac{1}{R_N} + D\right)}{D + \frac{1}{R_1} + \frac{1}{R_2} + ... + \frac{1}{R_N}} \qquad (5)$$

where

- R_i is the regulation constant
- D = % change in load divided by % change in frequency

AGC Operation

In a 2-area system, the following guidelines apply to AGC operation

Load Variation	Tie-Line Flow	System Frequency	Required Control Action
Load increase in Area 2	Increase in power flow to Area 2	Decrease	Increase generation in Area 2
Load increase in Area 1	Decrease in power flow to Area 2	Decrease	Increase generation in Area 1
Load decrease in Area 1	Increase in power flow to Area 2	Increase	Decrease generation in Area 1
Load decrease in Area 2	Decrease in power flow to Area 2	Increase	Decrease generation in Area 2

Simulation Studies - System Parameters

- 2-Area system with 3 generating units each.

- Generating unit 1 has a penalty factor α_i= 1.

  Therefore only unit 1 contributes to any increase in demand.

- The bias factor β= 1.9 for both areas.

- Under steady state operating conditions (before attack):

  a power of 0.4 pu flows along the tie-line from Area 1 to Area 2.

- Frequency deviation, Δf = 0.

Simulation - Attack Description

- **An intelligent attack involves manipulating the tie-line flow and frequency measurement to the following.**

$$f = 0.9974\ pu$$

$$\textit{Tie-lie flow} = 0.3951\ pu$$

- **The above malicious measurements are calculated using equations (4) and (5) to ensure that they correspond to each other.**

- **With these measurements, AGC in Area 1 would believe that there is an increased demand of 0.01 *pu* in Area 1.**

Simulation - Post-Attack System Parameters

- Generation in Area 1 would be increased by this deficit amount to maintain generation-demand stability

- This control action would disrupt the already existing generation-demand balance and cause an increase in system frequency

- The new system frequency (after control action), would be 60.156 *Hz*

- The attack could cause severe impacts if the frequency variation results in tripping of corresponding protection relays

Simulation - Results

- **Attack-impact Results**

Parameter	Before Attack	After Attack
Frequency (Hz)	60	60.156
Tie-Line Flow from Area 1 (pu)	0.4	0.4049
Unit 1 Generation change (pu)	0	0.01
Generation-Demand Imbalance (pu)	0	0.01

Mitigation: Anomaly Detection in AGC

- The rate of change of frequency (ROCOF) during a load-generation imbalance is given by

$$\frac{d\Delta f}{dt} = \frac{-\Delta P_L \cdot f}{2 \cdot \sum_i^n H_i}$$

- $\sum_{i=1}^{n} H_i$, the total system inertia, is characteristic of the system and the information is not readily available. This could be of potential use in anomaly detection.

- Example- A load increase of 0.01 pu in a test system has a ROCOF of -0.0038 Hz per second. Malicious data is injected at t+13 seconds.

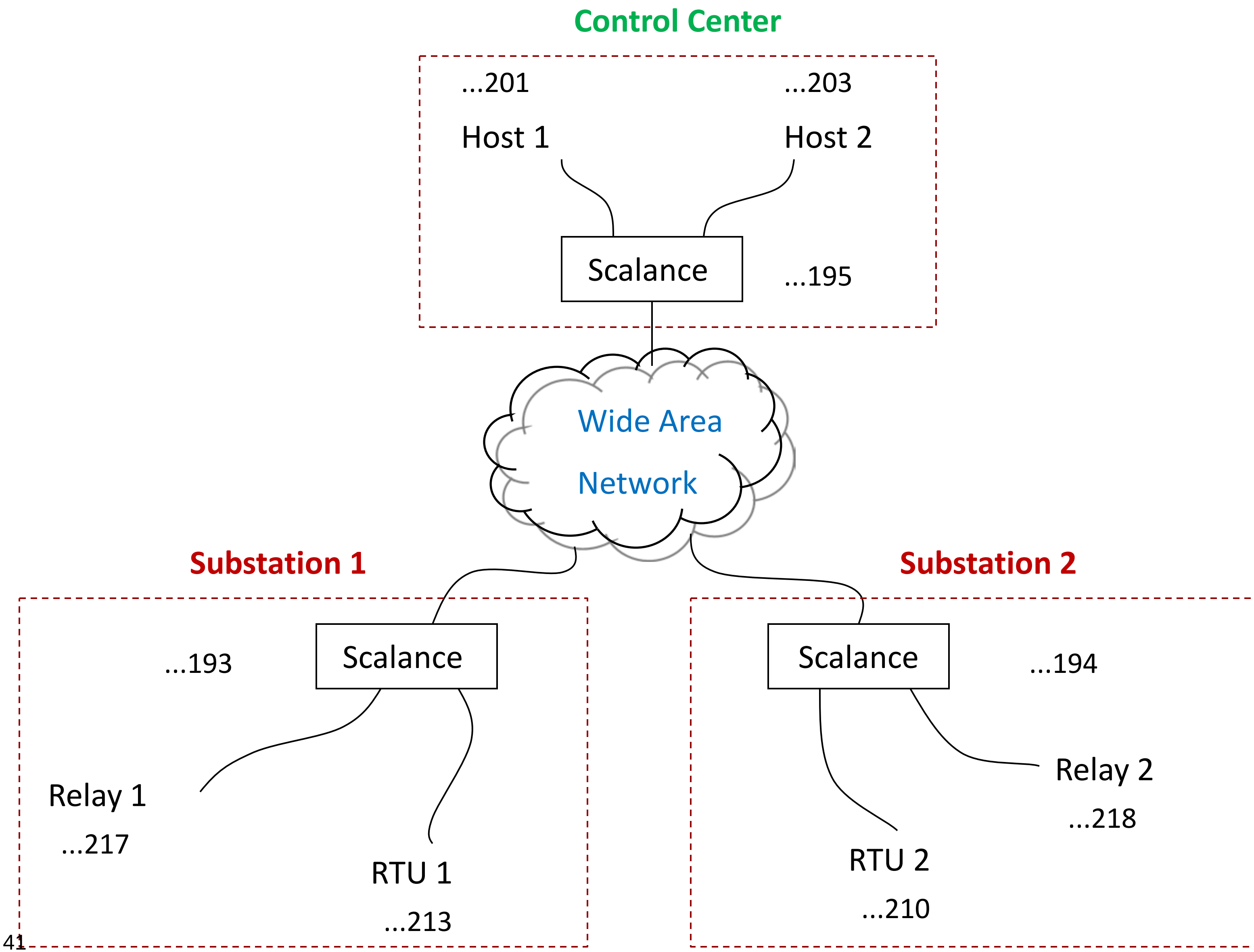
Time (seconds)	Frequency Measurement	
	Actual Change	With Anomaly Detection
t	60 Hz	60 Hz
t+6	59.9544 Hz	59.9544 Hz
t+12	59.9316 Hz	59.9316 Hz
t+18	59.9088 Hz	59.8172 Hz

Anomaly Detected

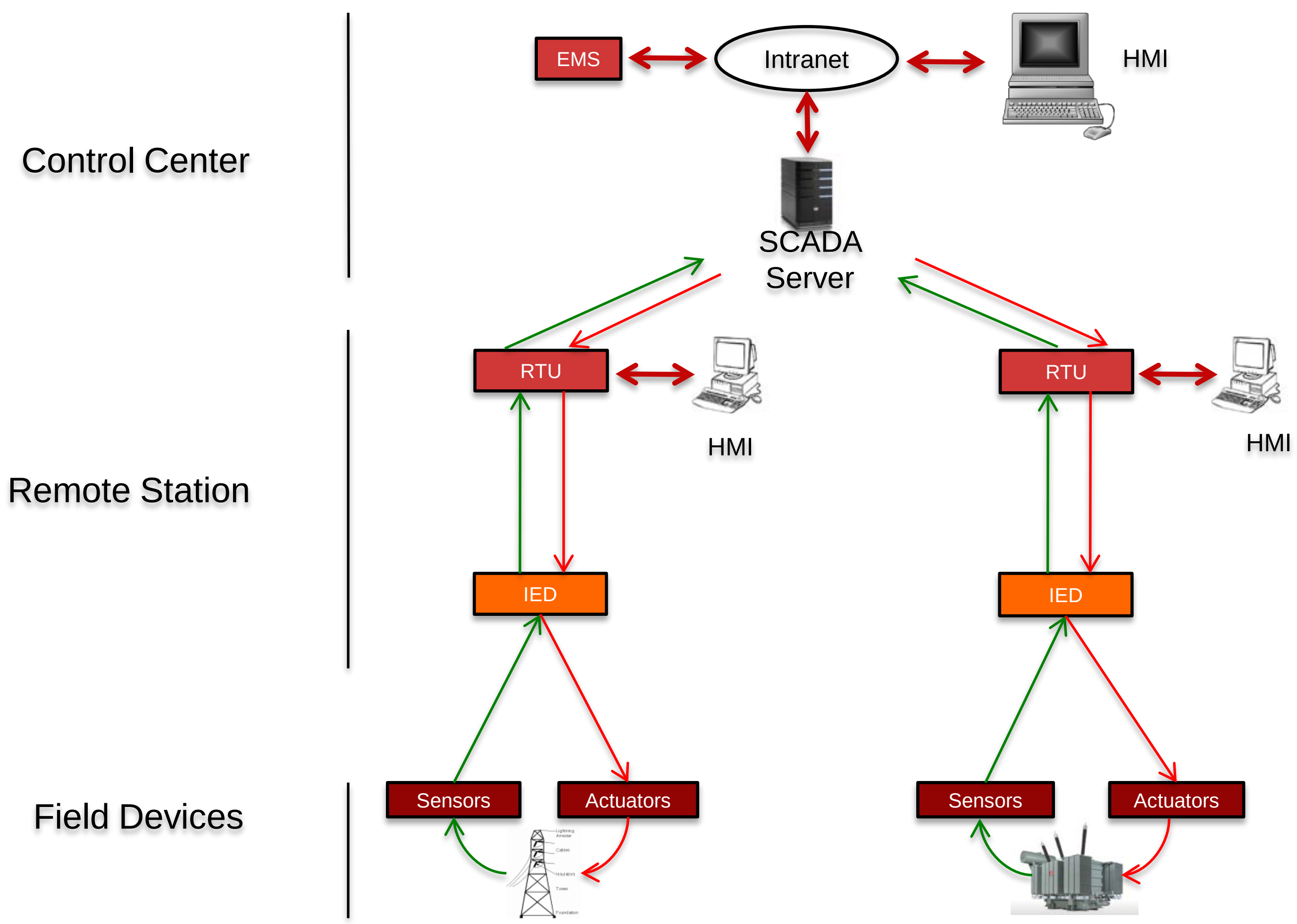
SCADA Cyber Security Testbed

A. Hahn, et. al., “Development of the PowerCyber SCADA Security Testbed”, in Cyber Security and Information Intelligence Research (CSIIR) Workshop, Oak Ridge National Laboratory, 2010.

SCADA Security Testbed

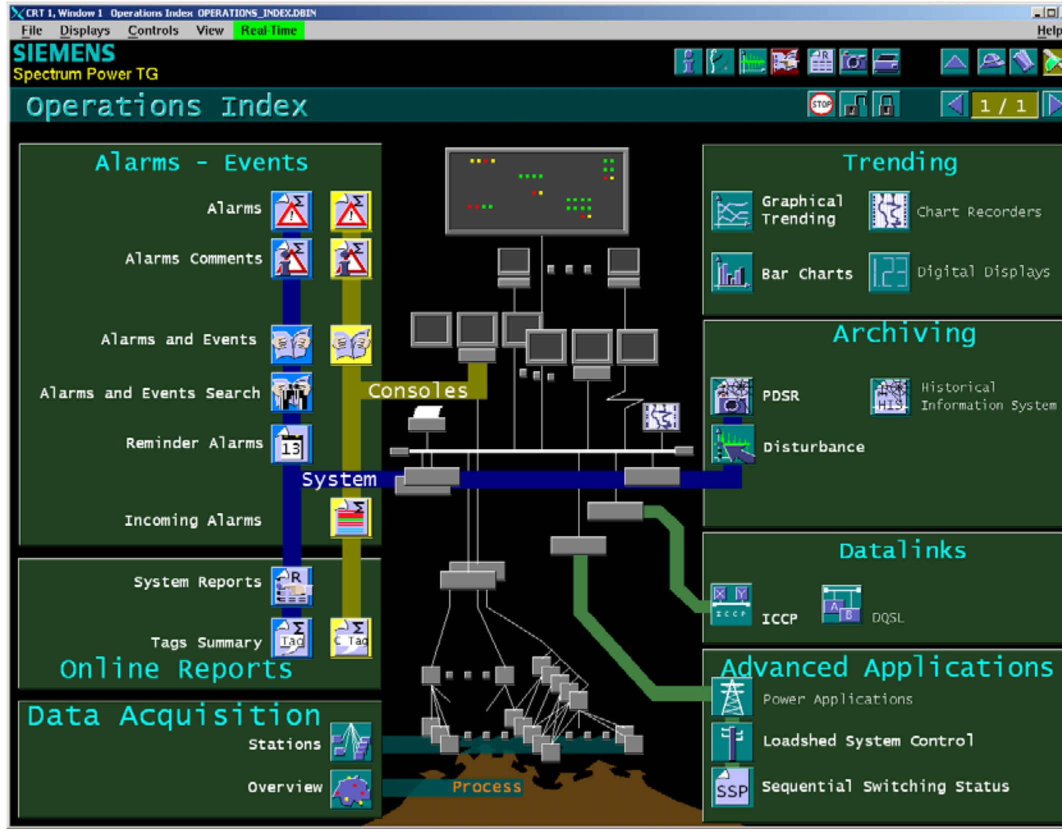


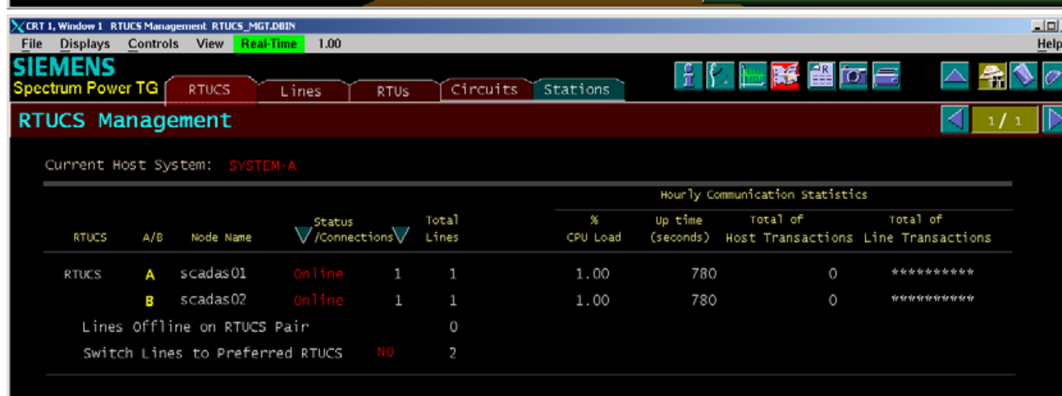
SCADA Network Configuration



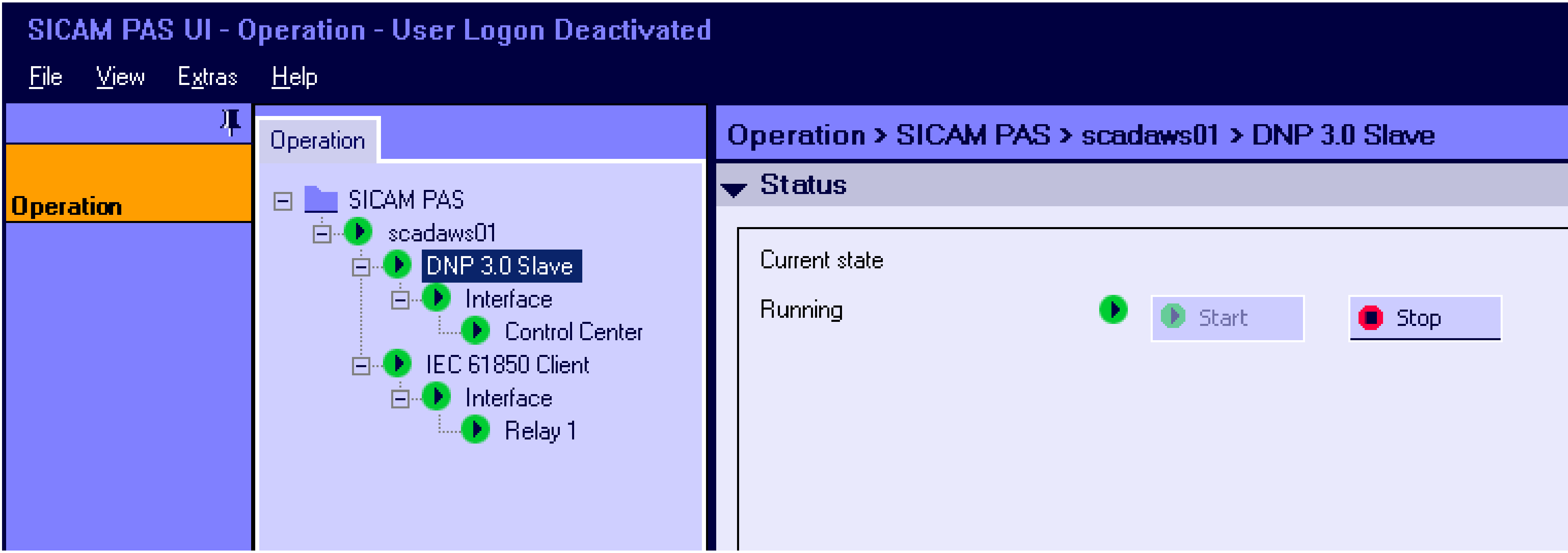
Control Center

- Spectrum Power TG
- Managing databases
- Establishing communications
- Monitoring current or voltage levels, trip breakers.
- Analog telemetry from relays
- Binary statuses for breakers





Substation: RTU, Firewall, Relay, Load



- SICAM PAS RTU
- Scalance security device
- Siemens DIGSI 4 (over current relay) with Resistive load

Testbed - Security evaluation

- **Man-in-the-middle attacks**

  - Denial of Sensor measurement (Substation → Control center)

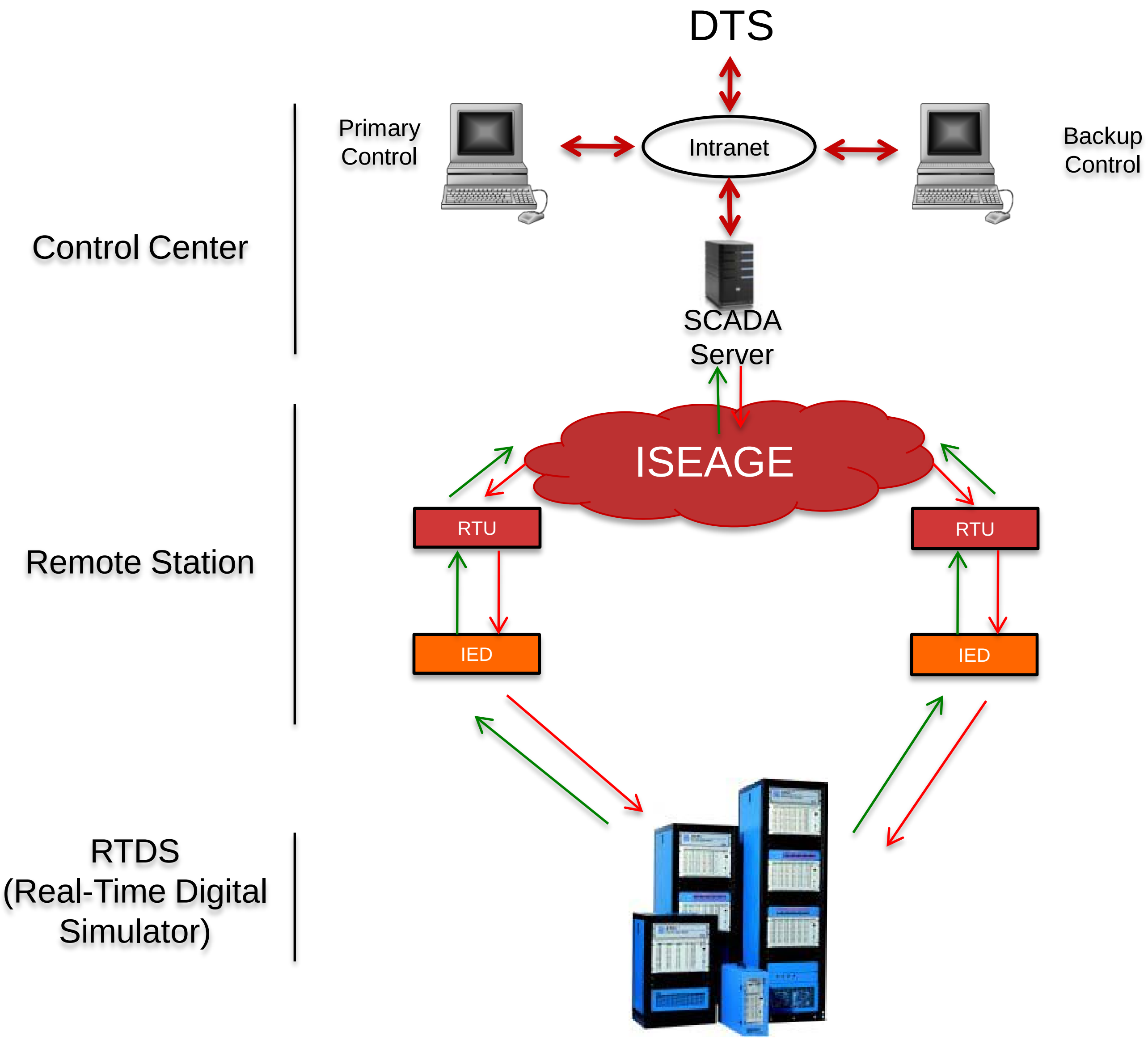
  - Denial of Control (Control center → Substation)

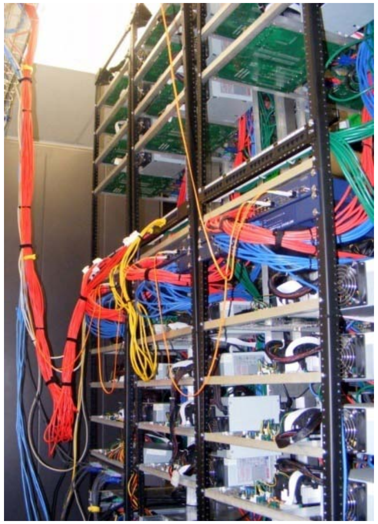
  - Disrupt operation of SCADA system

Testbed Enhancement - ongoing work

- Hardware-in-the-loop System-level Simulations
  - Realistic power system models and studies
- Integration with RTDS – Real-Time Digital Simulator
- Scaleup the testbed using virtualization technology
  - Scale the number of substations
- Wireless connectivity and studies
  - Substation-to-control center (wireless) & security attack/defense
- Advanced attack-defense studies
  - Outsider attacks
  - Coordinated attack-impact studies

Cyber-Physical Security Testbed: SCADA + ISEAGE + RTDS





ISEAGE
Internet-Scale Event and Attack Generation Environment

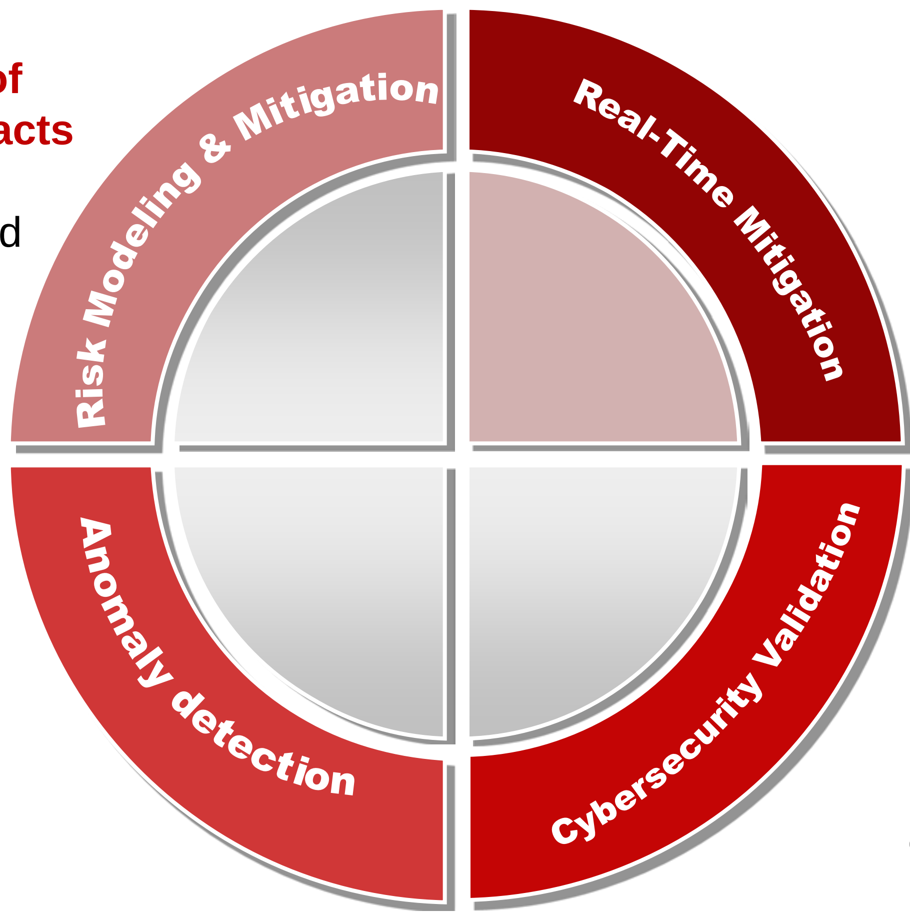
Conclusions

Research & Education at Iowa State Univ.

Integrated modeling of attacks and their impacts in terms of load loss, equipment damage, and economic loss &

Mitigation Algorithms

Real-time **temporal and spatial correlations** from substation level and control center networks



Relevant information from geographically dispersed substation network about **potential suspicious activities, intrusions, in terms of severity**

Comprehensive validation using **analytical** and **simulation**, **Testbed** evaluations for directed and intelligent attacks

Conclusions

- **Cyber security of electric power grid is of great importance**

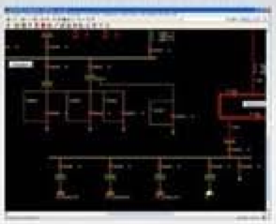
- **Smart attacks and coordinated attacks could have severe impacts to the stability, performance, and economics of the grid**
  - Data Integrity attacks, Denial of Service (e.g., Denial of Control).
  - Intrusion-based attacks, Protocol attacks, Worms/malware

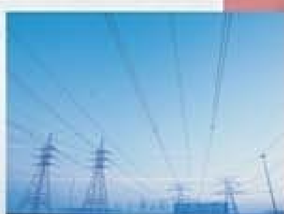
- **Cyber-Physical Systems Security is an important area of R&D**

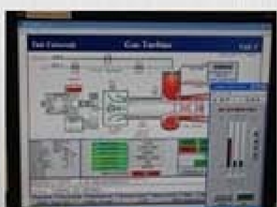
- **Development of Countermeasures:**
  - Attack prevention, detection, mitigation, and tolerance
  - Cyber + Physical countermeasures

CONCLUSIONS

- Critical infrastructure security is a national need
  - Power grid, Transportation, Water distribution, …
  - "Perfect Citizen" initiative by the US Government
- R&D is very important and requires significant effort
- Education and workforce development is a national priority
- DoE, NSF, NERC, DHS, NIST focus on this area
- Synergy between University, National Labs, Industry needed







http://powercyber.ece.iastate.edu

Thank you !!!

Acknowledgements:

- National Science Foundation
- Electric Power Research Center, Iowa State Univ.

- Dr. Chen-Ching Liu, Univ. College Dublin, Ireland
- Dr. Cheewooi Ten, Michigan Tech University
- Dr. Ajjarapu & Dr. Jacobson, Iowa State Univ.
- <u>ISU Graduate Students:</u>

Siddharth Sridhar, Adam Hahn, Aditya Ahok, Jie Yan