

# Cyber-Physical Systems Security of Smart Grid

**Manimaran Govindarasu**

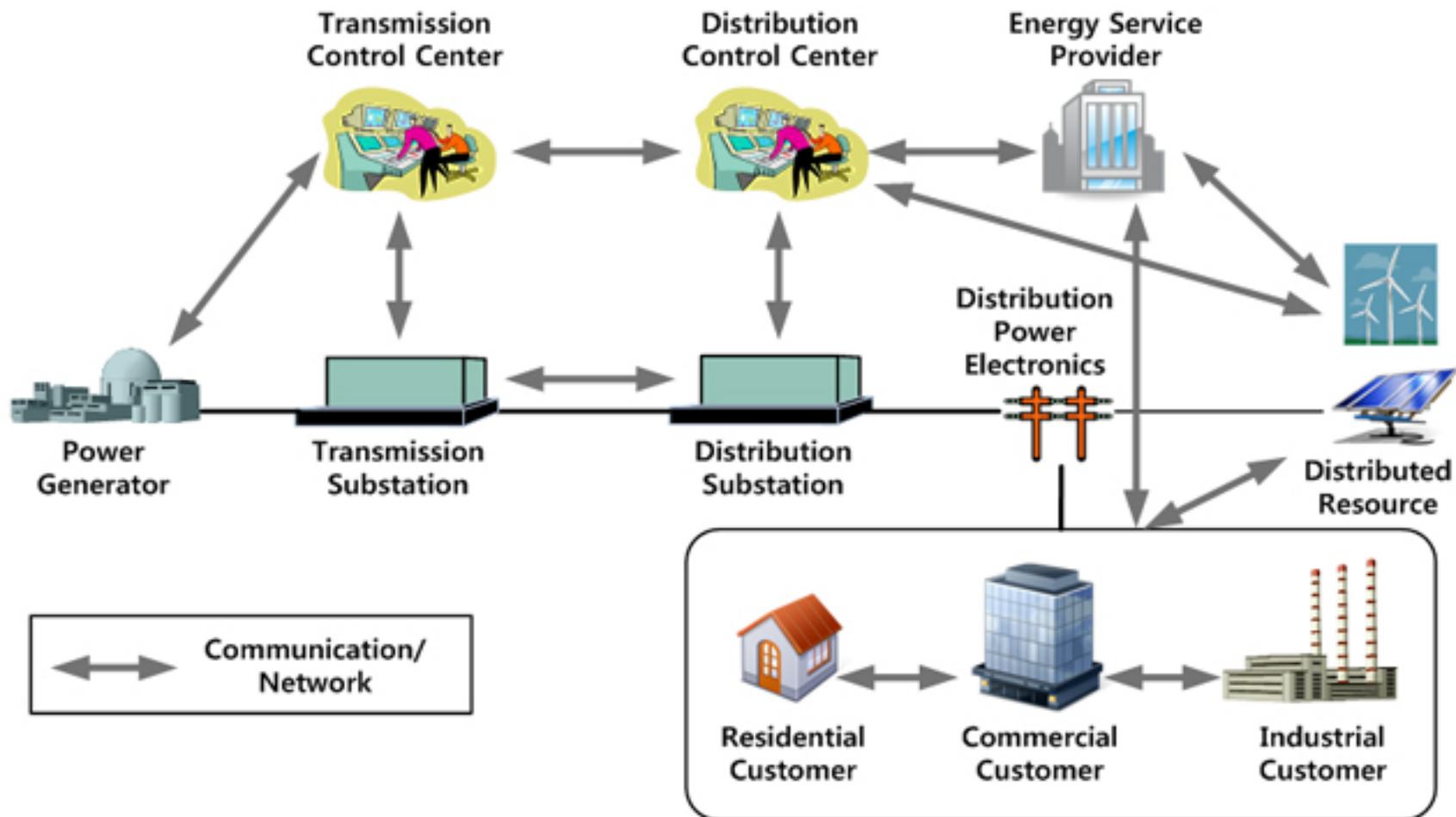
**Iowa State University**

[gmani@iastate.edu](mailto:gmani@iastate.edu)

<http://powercyber.ece.iastate.edu>

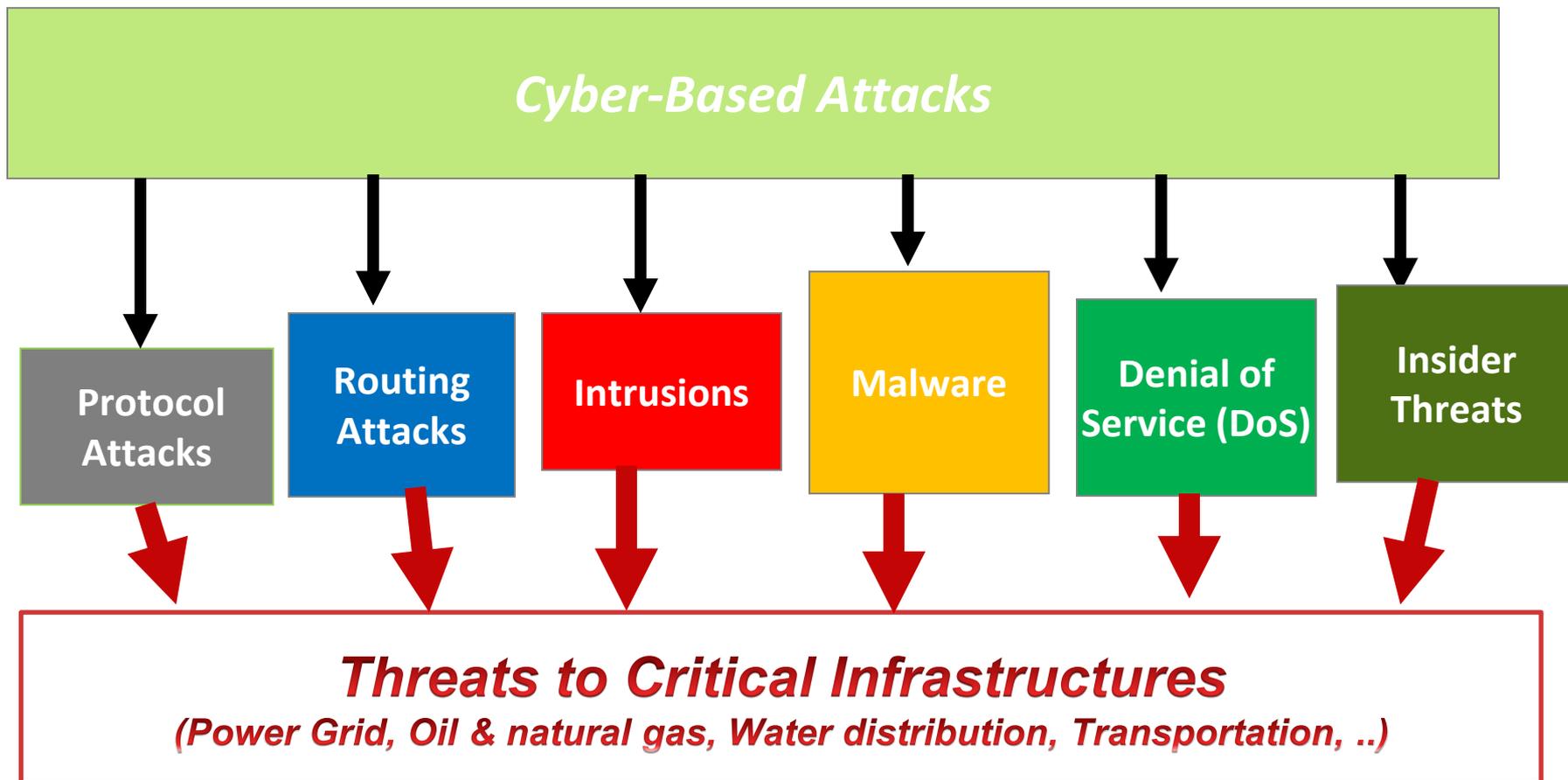
Presented at ISRCS 2012, Aug. 15, 2012

# Smart Grid: A Cyber-Physical System



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

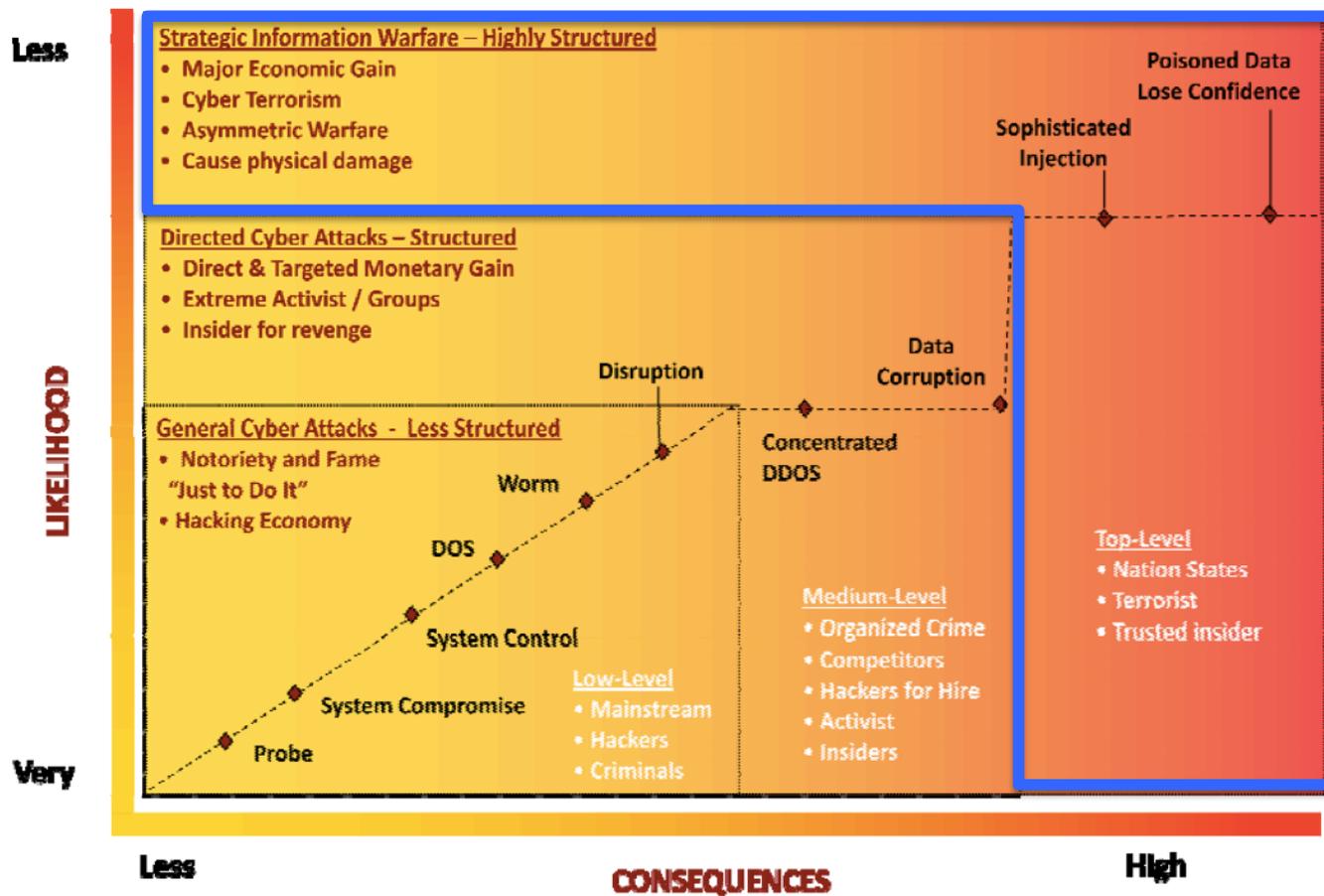
# Cyber Threats to Power Grid Infrastructure



[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.

# Consequences vs. Likelihood – High Impact Low Frequency (HILF) events



## High-level ✓

**Actors:** Nation states, Terrorists

**Attacks:** Sophisticated injection, Data poisoning

## Medium-level

**Actors:** Competitors, Insiders

**Attacks:** DDoS, Data Corruption

## Low-level

**Actors:** Hackers, Cyber criminals

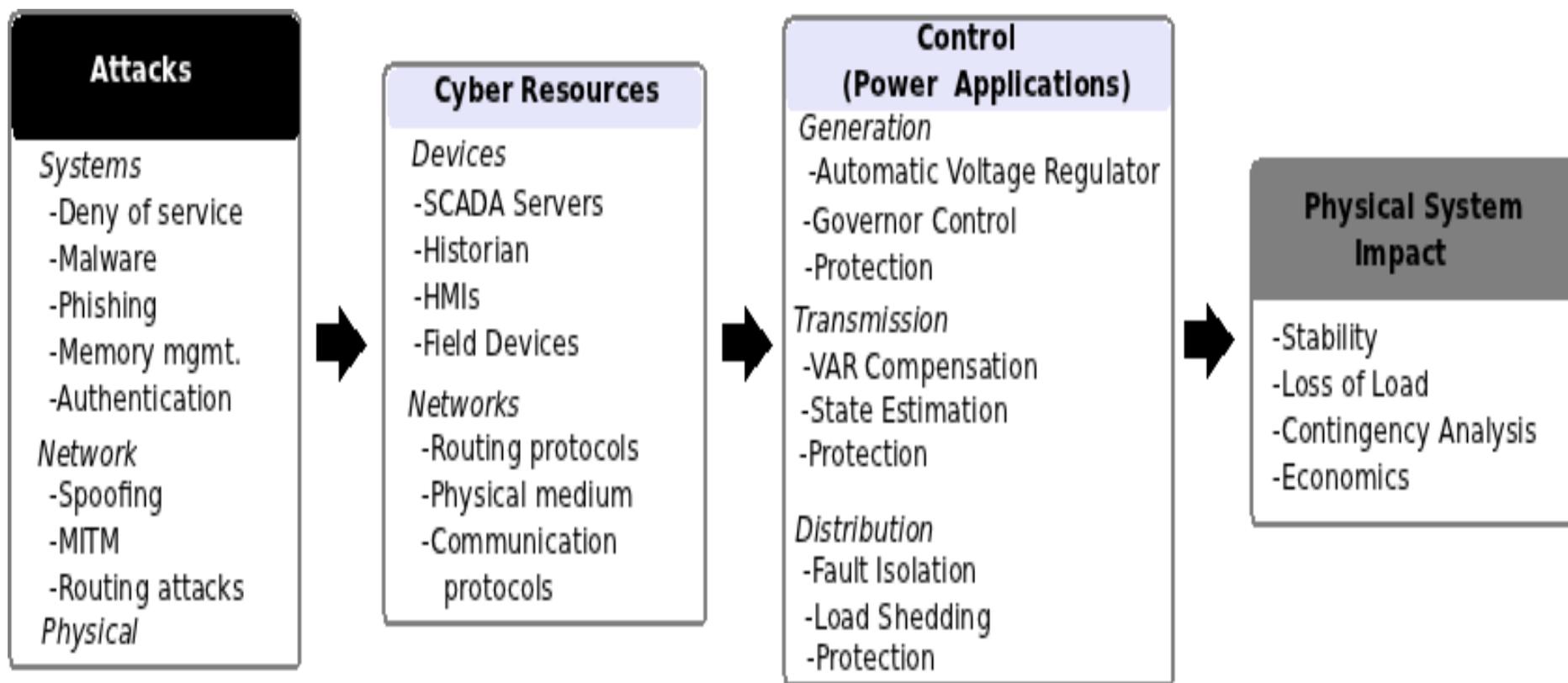
**Attacks:** DoS, System disruption

NERC Cyber Attack Task Force – High-Impact Low-Frequency Event

# Power Grid Cyber Security Roadblocks

- Legacy systems
  - Geographically disperse
  - Insecure remote connections
  - Long system deployments
  - Threats/Attacks evolve rapidly
- 
- Adoption of std. technologies with known vulnerabilities
  - Connectivity of control systems to other networks
  - No “fail-closed” security mechanisms
  - Widespread availability of technical info & tools

# Attacks-Cyber-Control-Physical



# Smart Grid Security = Info + Infra + Appln. Security

	Information Security	Infrastructure Security	Applications Security
NEEDS	<ul style="list-style-type: none"> <li>□ Information Protection               <ul style="list-style-type: none"> <li>▪ Confidentiality</li> <li>▪ Integrity</li> <li>▪ Availability</li> <li>▪ Authentication</li> <li>▪ Non-repudiation</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>□ Infrastructure protection               <ul style="list-style-type: none"> <li>▪ Routers</li> <li>▪ DNS servers</li> <li>▪ Links</li> <li>▪ Internet protocols</li> </ul> </li> <li>□ Service availability</li> </ul>	<ul style="list-style-type: none"> <li>□ Generation Control apps.</li> <li>□ Transmission Control apps.</li> <li>□ Distribution Control apps.</li> <li>□ System Monitoring functions</li> <li>□ Protection functions</li> <li>□ Real-Time Energy Markets</li> </ul>
MEANS	<ul style="list-style-type: none"> <li>□ Encryption/Decryption</li> <li>□ Digital signature</li> <li>□ Message Auth.Codes</li> <li>□ Public Key Infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>□ Firewalls</li> <li>□ IDS/IPS</li> <li>□ Authentication Protocols</li> <li>□ Secure Protocols</li> <li>□ Secure Servers</li> <li>□ IPSEC, DNSSEC</li> </ul>	<ul style="list-style-type: none"> <li>□ Attack-Resilient Control Algos</li> <li>□ Model-based Algorithms               <ul style="list-style-type: none"> <li>- Anomaly detection</li> <li>- Intrusion Tolerance</li> </ul> </li> <li>□ Risk modeling and mitigation</li> <li>□ Attack-Resilient Protection</li> </ul>

**Cyber Attacks: Deter, Prevent, Detect, Mitigate, Attribution; be Resilient**

# Research Focus

## Topic 1: Defense against Coordinated Attacks

- Risk modeling of coordinated cyber attacks
- Risk mitigation algorithms

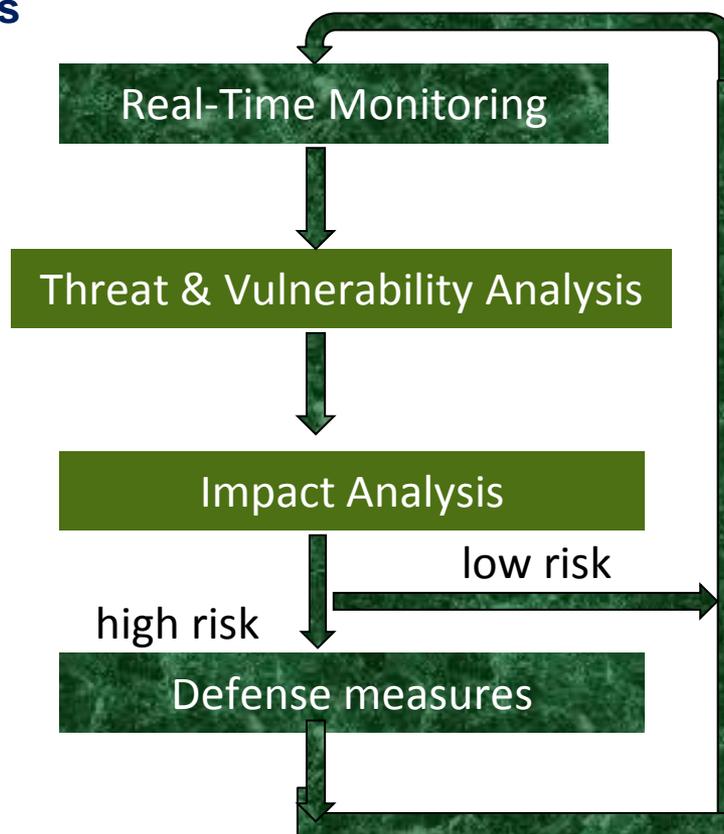
## Topic 2: Cyber Security of WAPMC

- Attack-Resilient control algorithm (AGC)
- Domain-specific Intrusion Detection/Tolerance

# Topic 1: Risk modeling coordinated attacks

Risk = Threat x Vulnerability x Impacts

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



# Risk modeling (1)

Hierarchical relationship *system*, *scenario*, and *access point* vulnerability

System  
Vulnerability

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

Scenario Vulnerability

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

Access Point Vulnerability

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

$\pi_j$  **Probability of intrusion** thro access point  $j$

$\gamma_j$  **Impact** due to compromise of substation  $j$

Hierarchical modeling

# Risk Modeling (2) – Coordinated Cyber Attacks

Attacker can control: **Space:** where to attack? **Time:** when to attack?

## Evaluating $\gamma$ – Impact Estimation

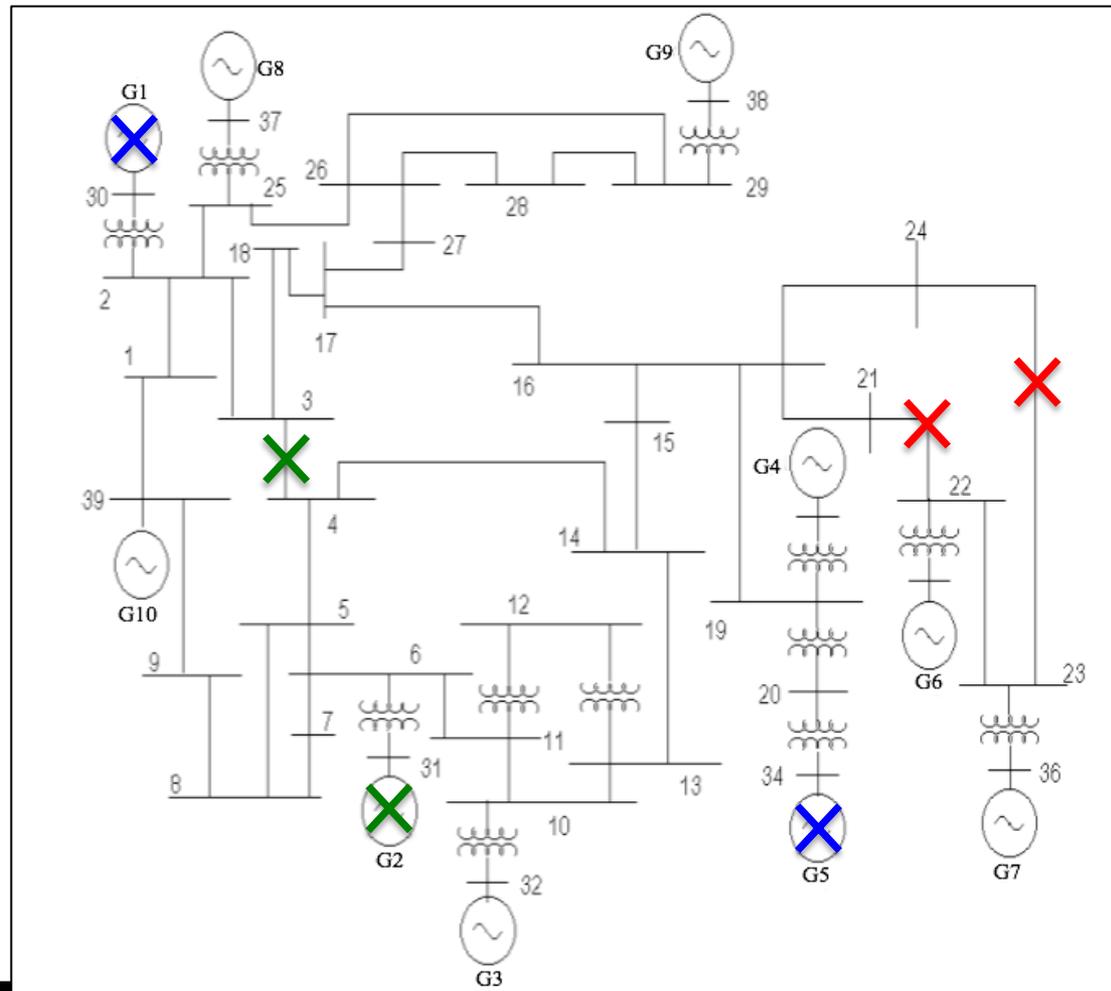
- Coordinated Attack Groups-
  - ✓ Gen + Gen
  - ✓ Gen + Trans
  - ✓ Trans + Trans
- Optimal power flow simulation
- $\gamma$  = load shedding for OPF solution

### Results

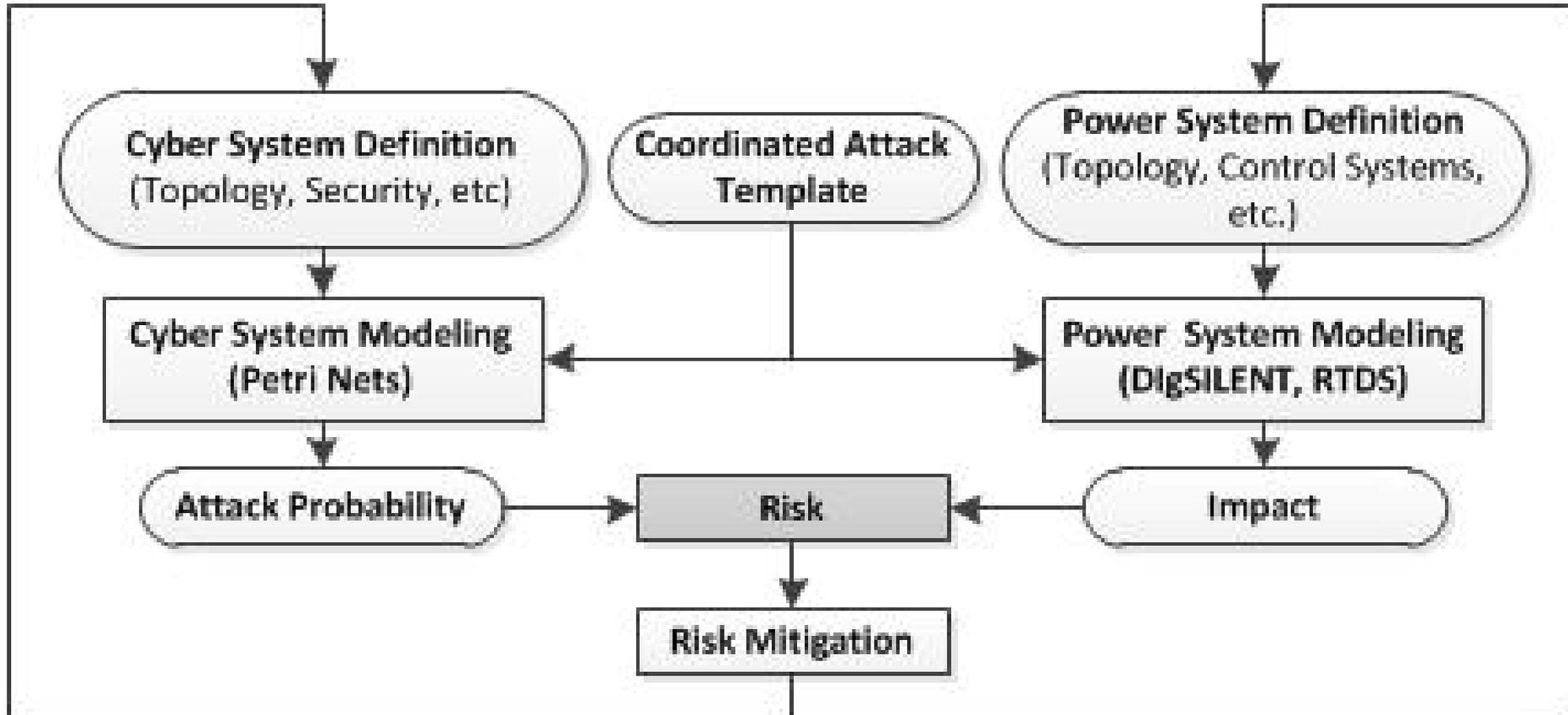
✗ →  $\gamma$  = 363 MW

✕ →  $\gamma$  = 163 MW

✗ →  $\gamma$  = 110 MW



# CPS Risk Modeling (3)

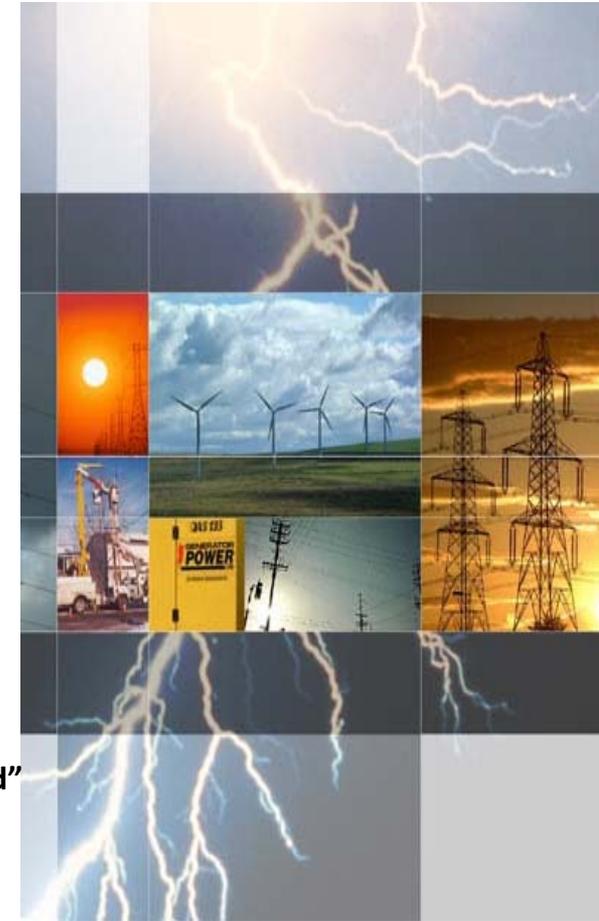


C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Trans. on Power Systems, vol. 23, no. 4, pp. 1836-1846, Nov. 2008

# TOPIC 2: Cyber Security of Wide-Area Monitoring, Protection and Control

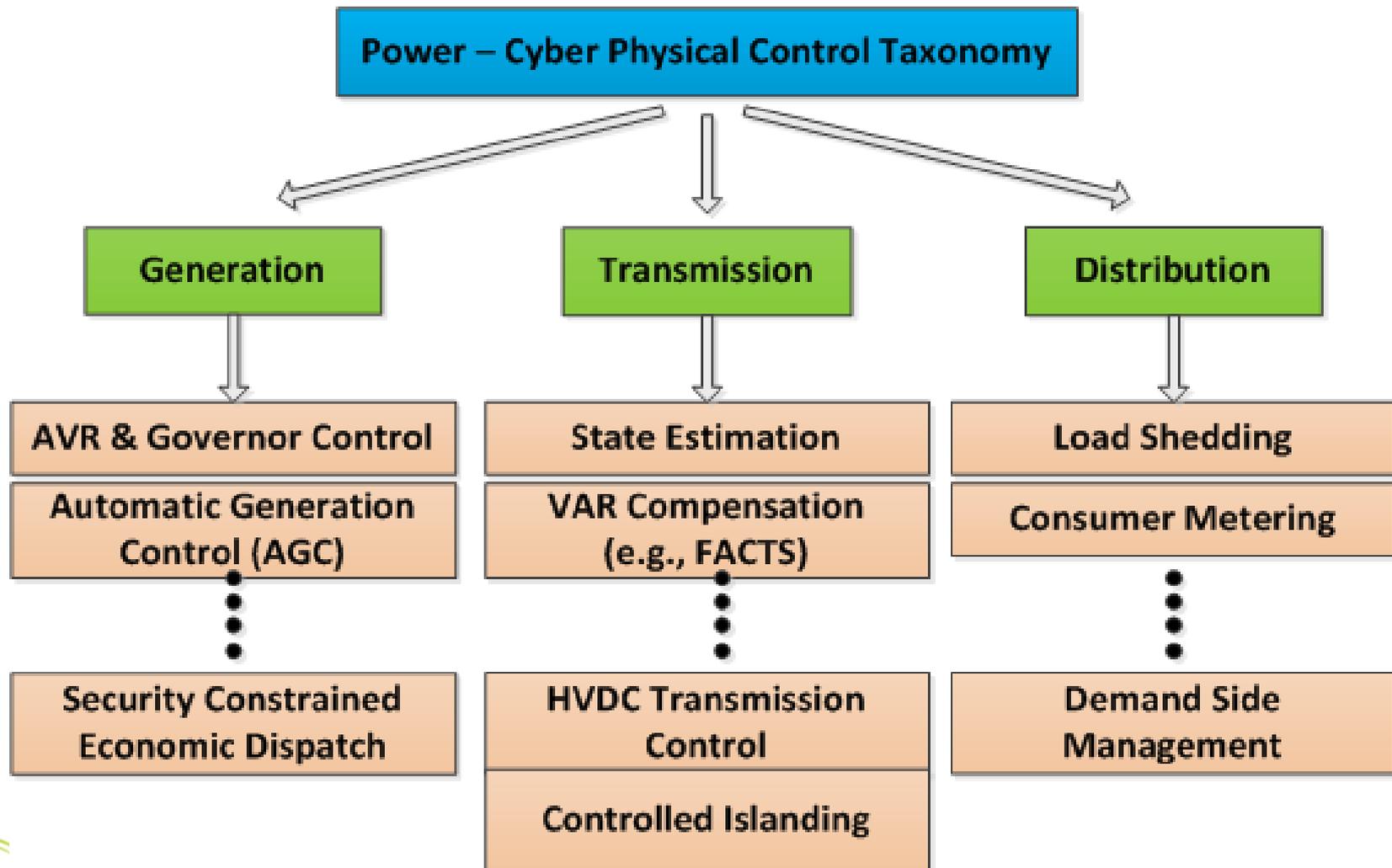
## Attack-Resilient Control Algorithms

- Man-in-the-middle attacks
- Data integrity attacks
- Denial of service attacks
- Replay attacks
- Timing attacks ...
- **Frequency control**
- **Voltage control**
- **Transient stability**

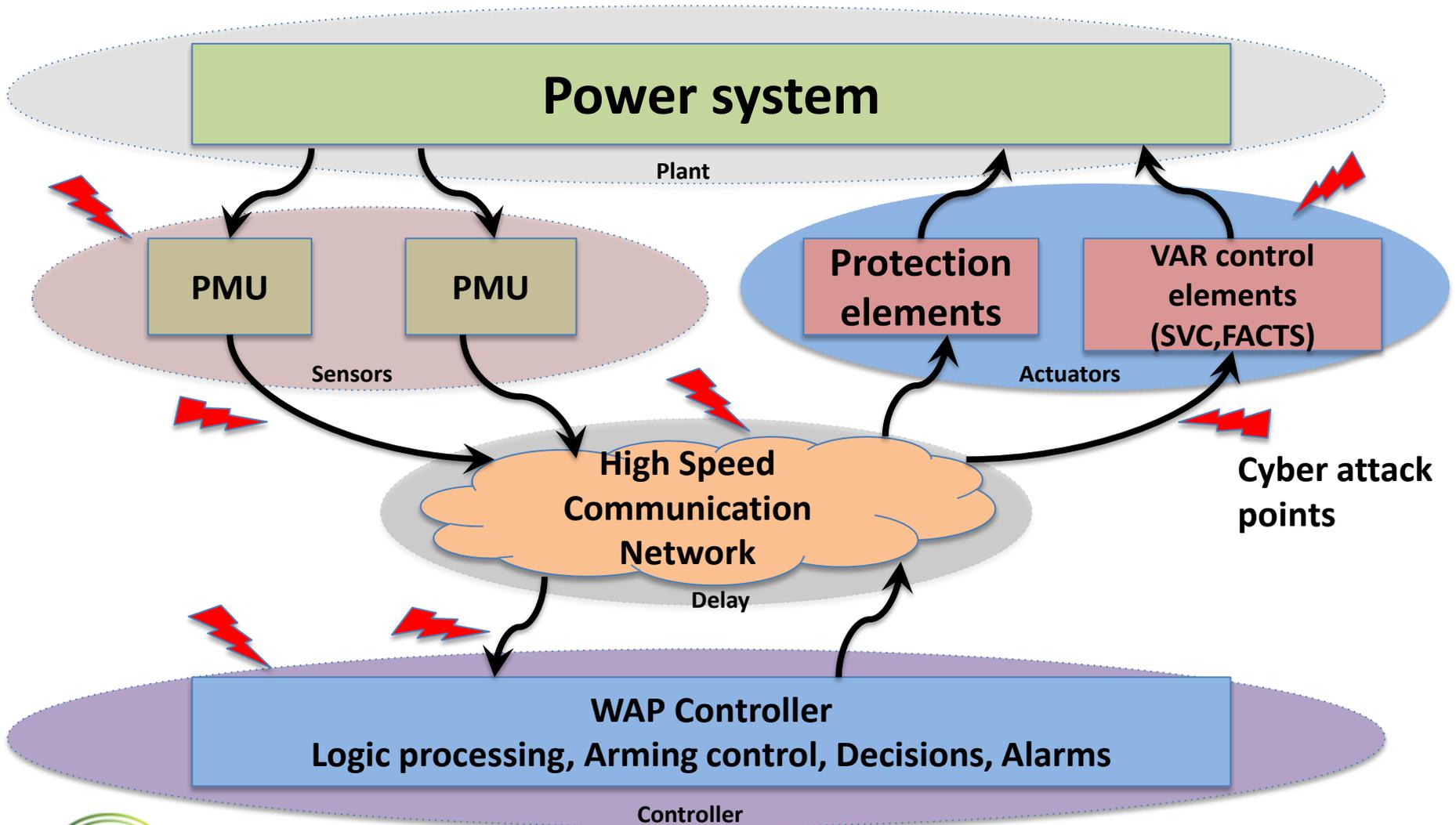


S. Siddharth, A. Hahn, and M. Govindarasu, "Cyber Physical Systems Security for Smart Grid" Special issue on Cyber-Physical Systems, Proceedings of the IEEE, Jan. 2012.

# Cyber-Physical Control in Power Grid

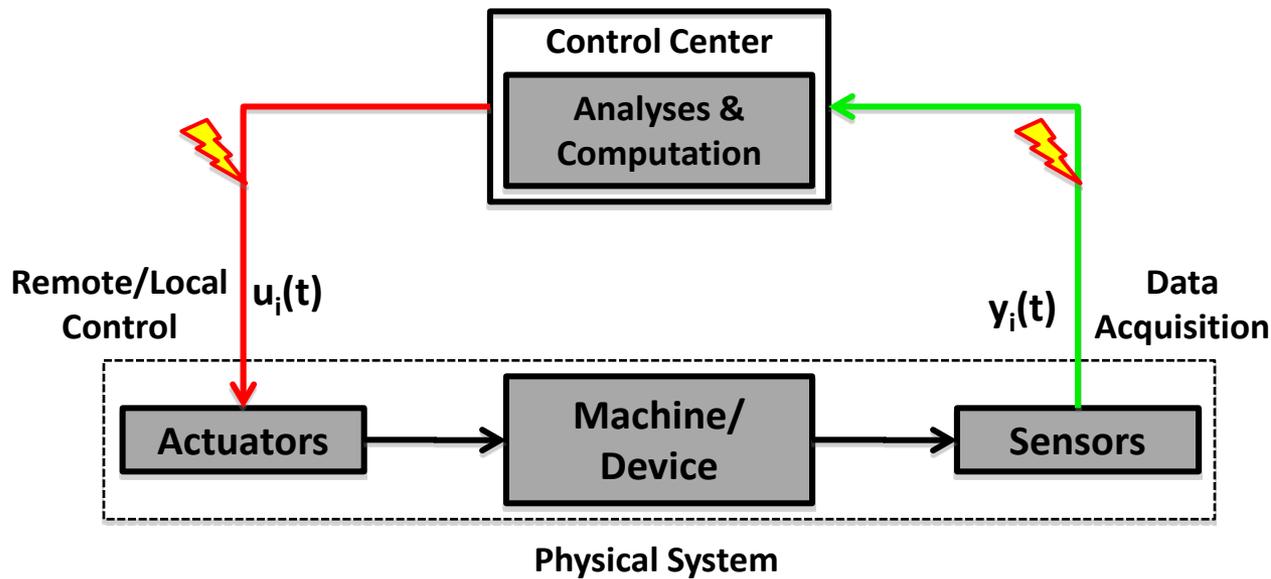


# WAMPAC architecture



# Control Systems Attack Model

## Generic Control System Model



## Types of Attacks

- Data integrity
- Replay
- Denial of service
- De-synchronization and timing-based

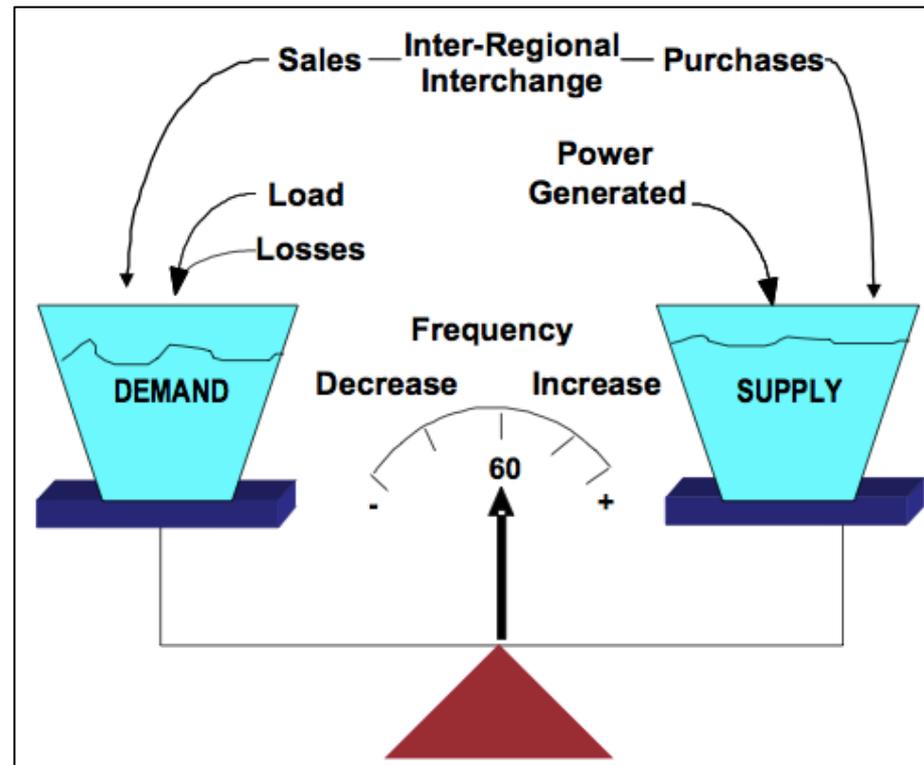
Figure adopted from - Yu-Hu. Huang, Alvaro A. Cardenas, et al, "Understanding the Physical and Economic Consequences of Attacks on Control Systems"

# Automatic Generation Control (AGC)

## AGC Features

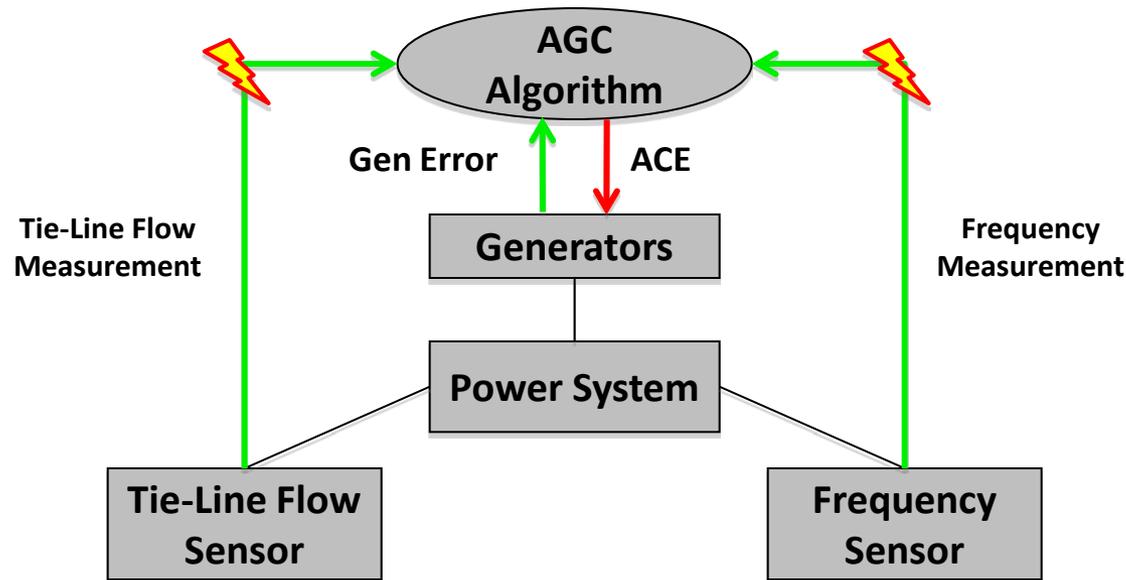
- Maintains frequency at 60 Hz
- **Supply = Demand**
- Maintain power exchange at scheduled value
- Ensures economic generation

[Figure from NERC Balancing and Frequency Control  
[www.nerc.com](http://www.nerc.com) ]



# Automatic Generation Control

## Frequency Control



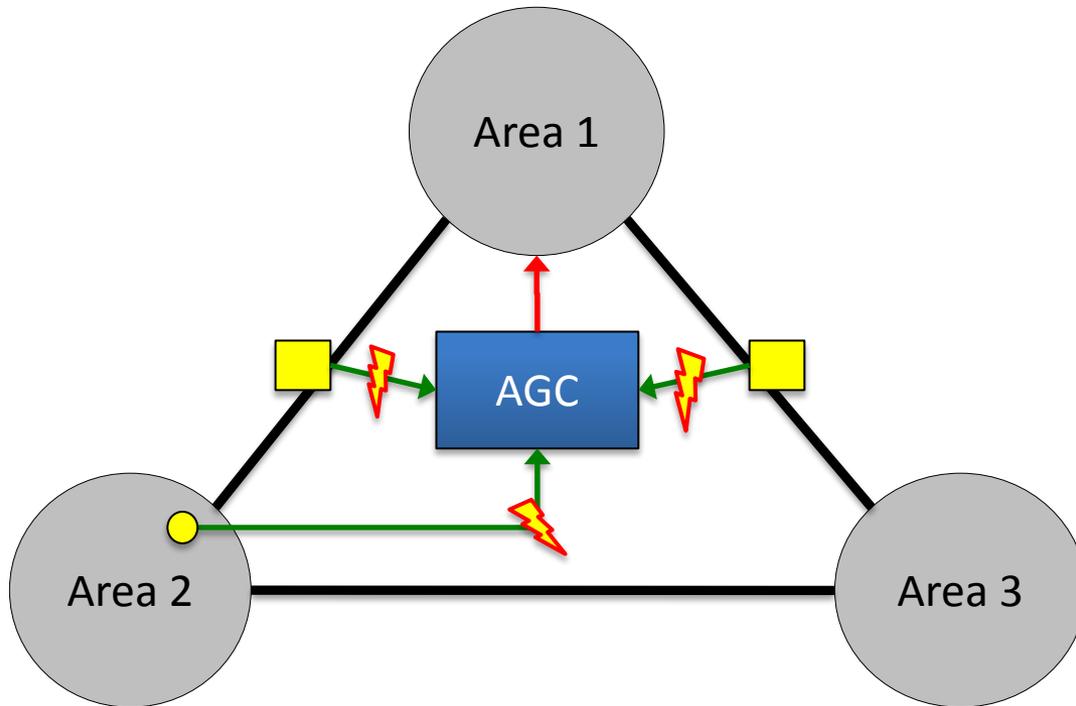
**Attack:** Modify tie-line flow and frequency measurements

**Impact:** Abnormal operating frequency conditions

Siddharth Sridhar and G. Manimaran – “Data Integrity Attacks and Impacts on SCADA Control System” – PES GM 2010



# AGC – Attack Vector



## Area Control Error

$$ACE = \Delta P_{net} + \beta \Delta f$$

$\Delta P_{net}$  = Scheduled Flow – Actual Flow

$\Delta f$  = 60 Hz – Measured Frequency

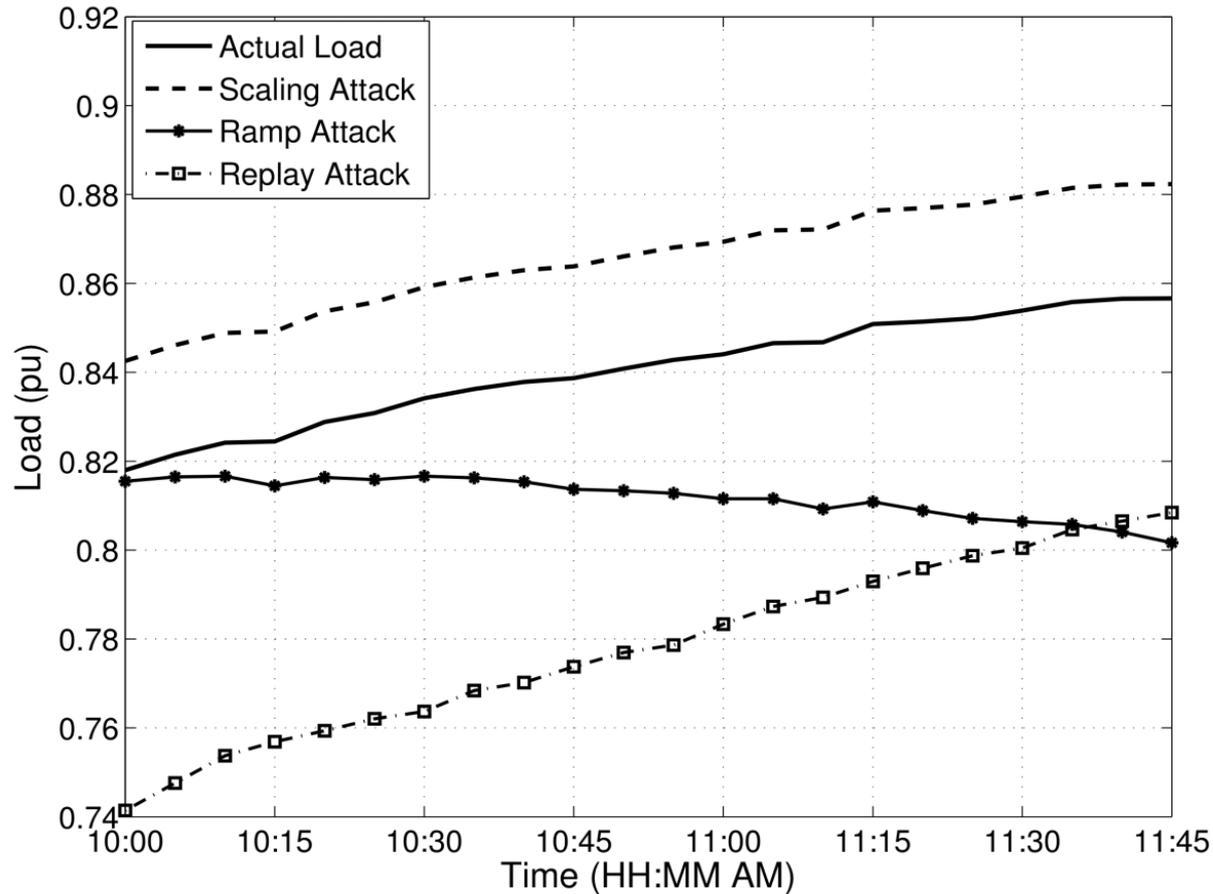
**Attack**: Modify tie-line flow and frequency measurements

**Impact**: Unhealthy operating frequency conditions

8/27/2012

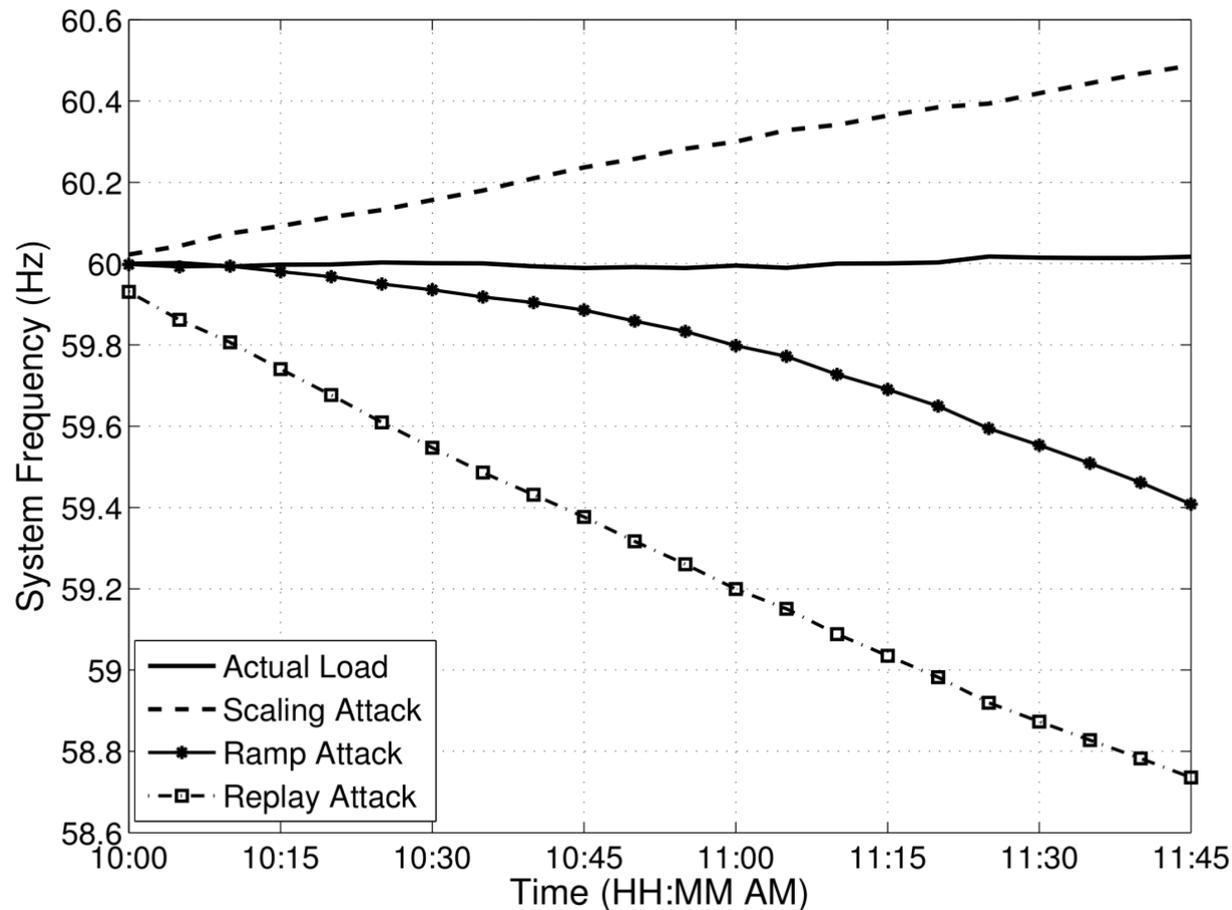
# AGC – attack impacts (sample result)

*Attack Impact – Perceived Load at the Control Center*



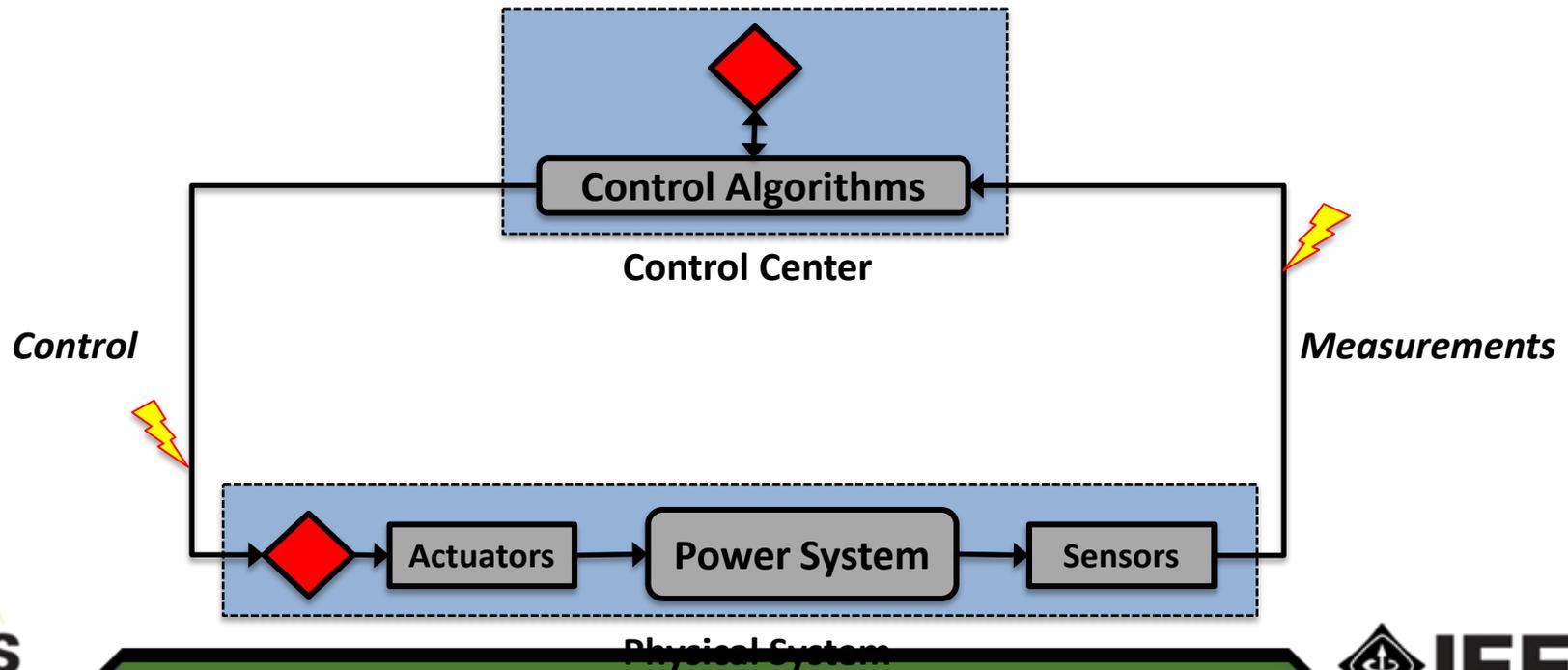
# AGC – attack impacts (sample result)

*Attack Impact – Resulting System Frequency*

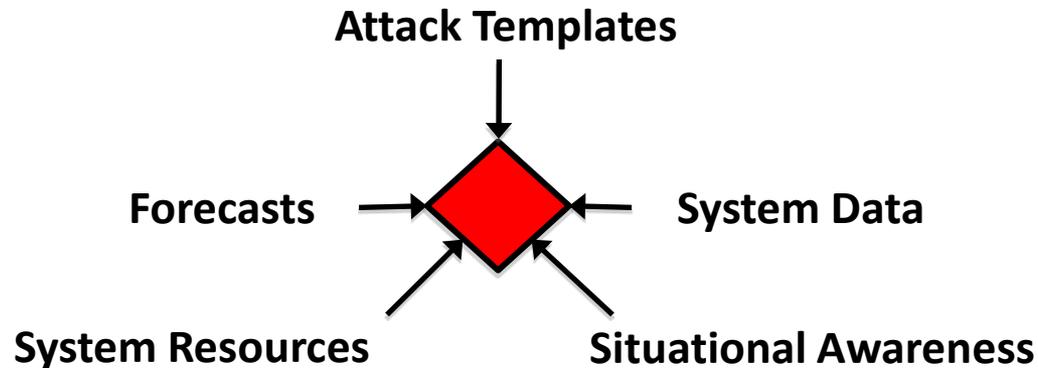


# Attack Resilient Control (ARC)

$$\text{Attack Resilient Control} = \text{Domain-specific Anomaly Detection} + \text{Model-based Mitigation}$$

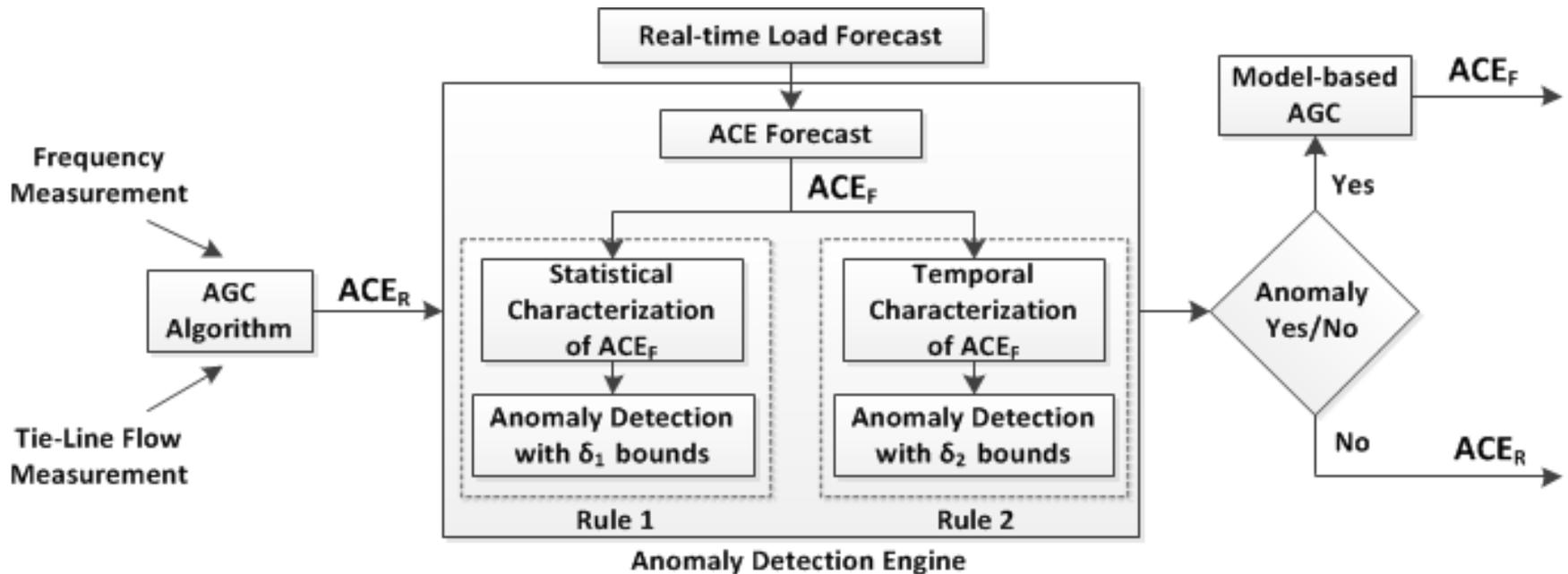


# ARC – Intelligence Sources



- **Forecasts** – Load and wind forecasts
- **Situational Awareness** – System topology, geographic location, market operation
- **Attack Templates** – Attack vectors, signatures, potential impacts
- **System Data** – Machine data, control systems
- **System Resources** – Generation reserves, VAR reserves, available transmission capacity

# ARC for AGC

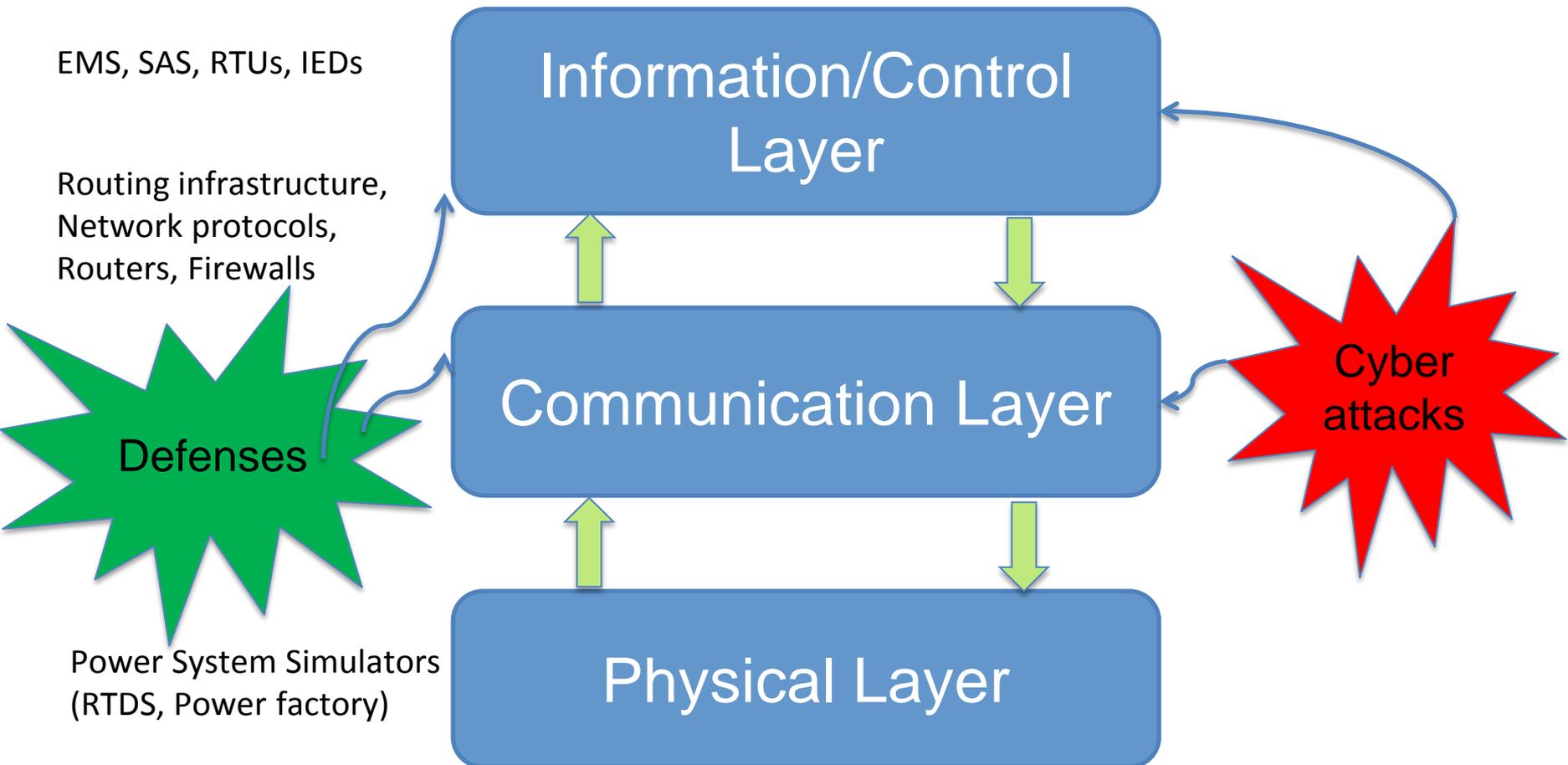


## Key

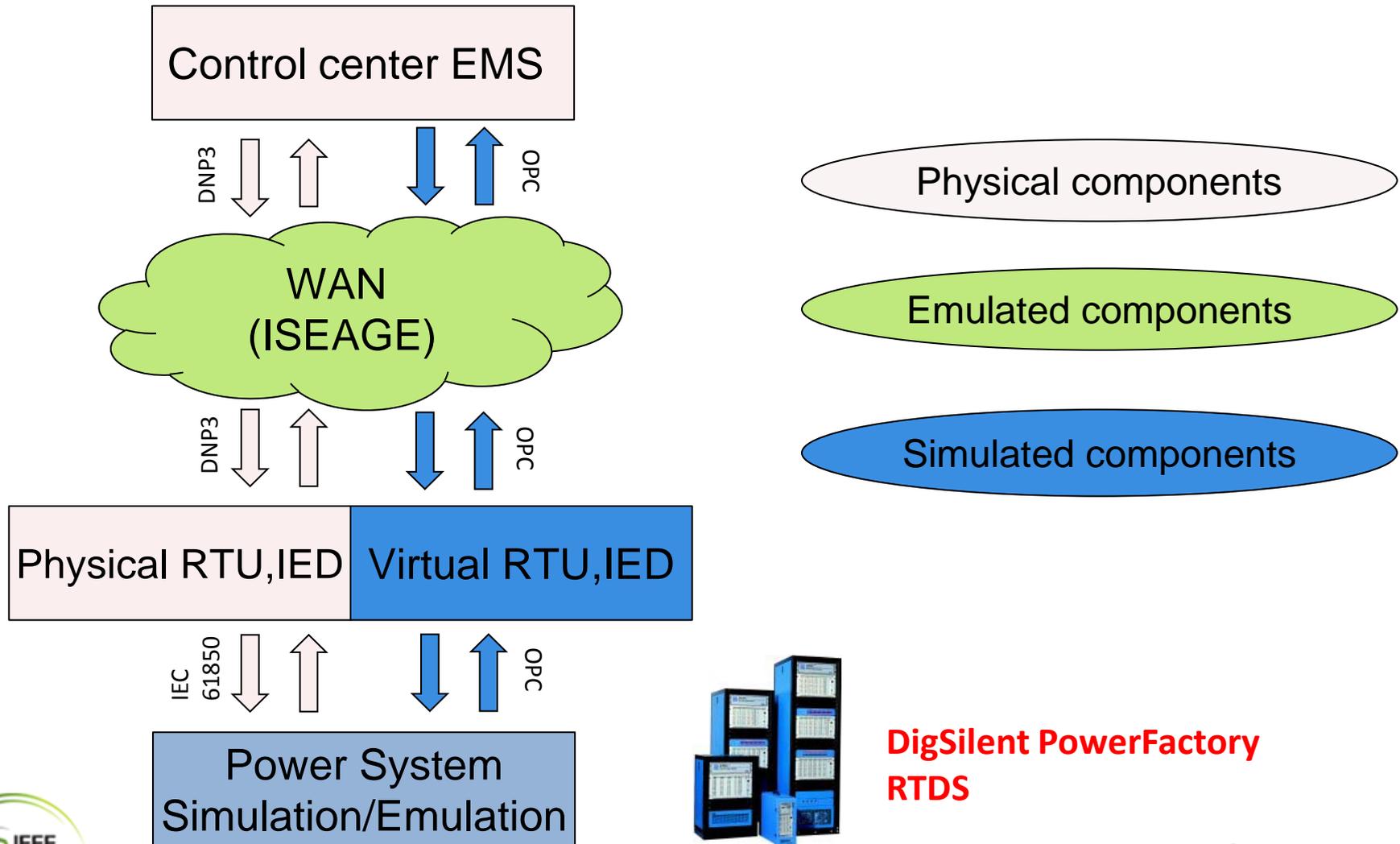
$ACE_R$  – ACE obtained from real-time measurements

$ACE_F$  – ACE obtained from forecast

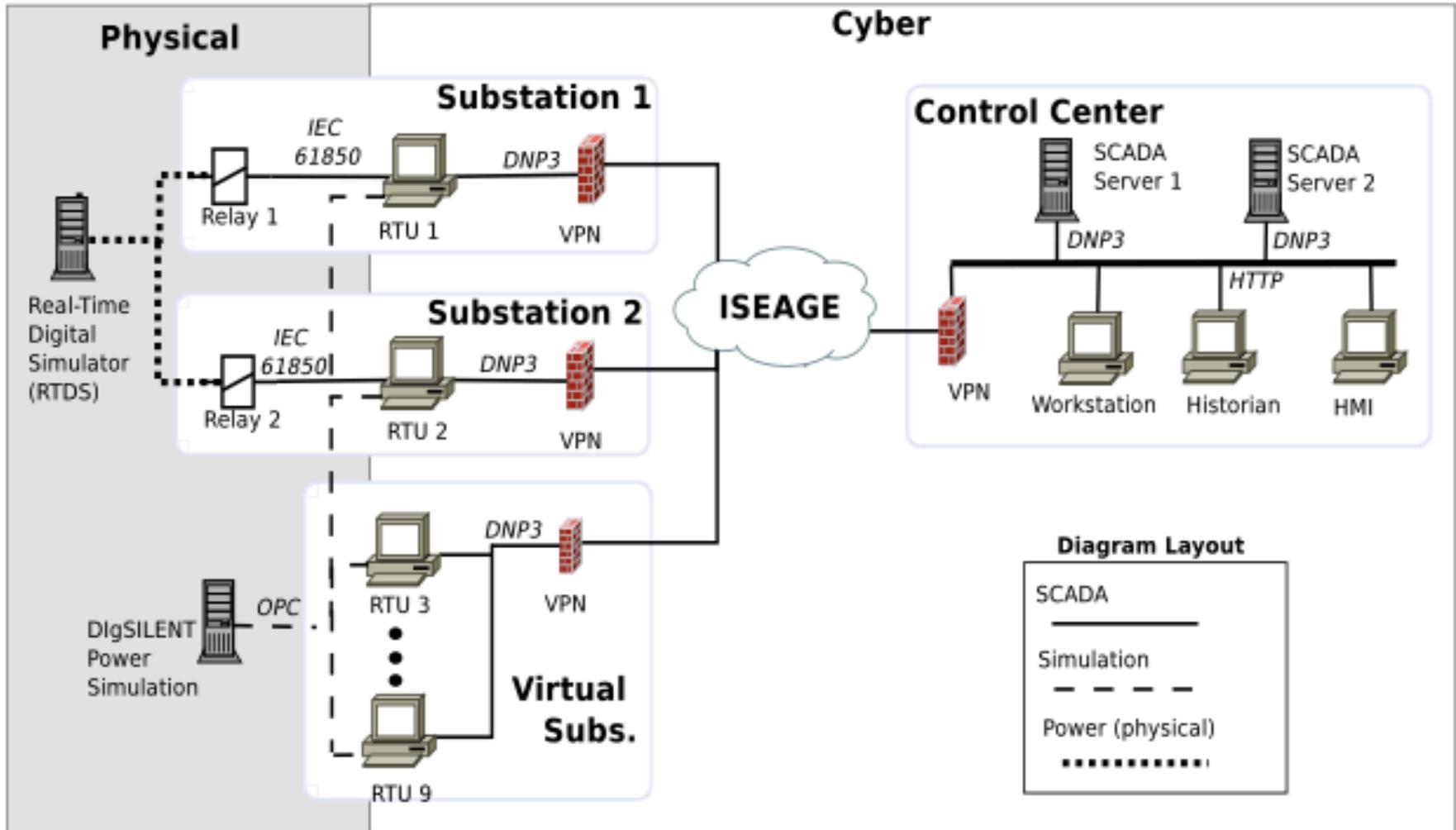
# CPS Testbed-based Evaluation



# Iowa State's *PowerCyber* Testbed



# ISU PowerCyber Testbed - Configuration



# Security Evaluations

## Vulnerability assessment

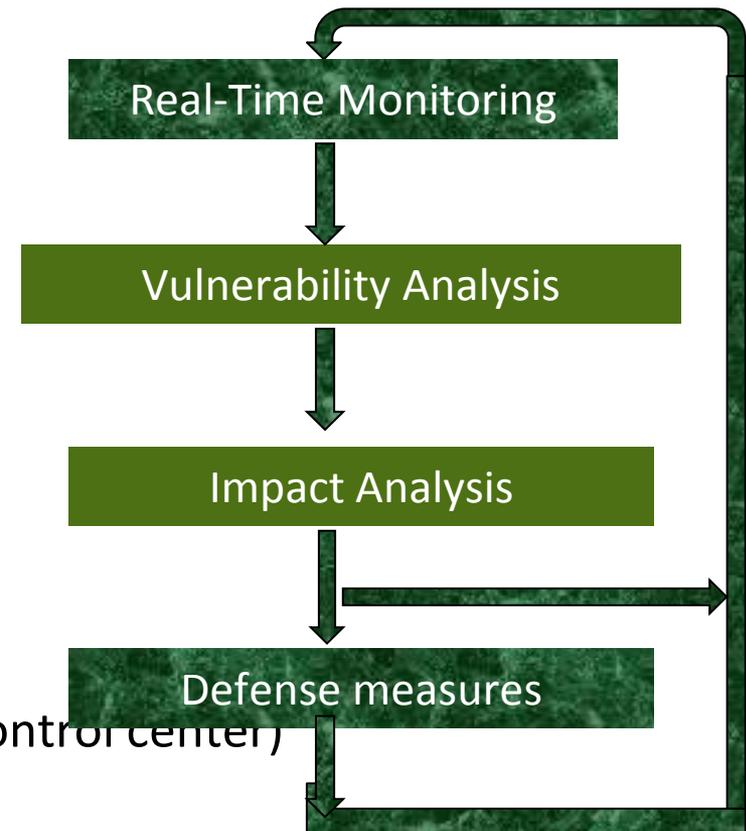
Protocol vulnerabilities  
 Firewall/VPN vulnerabilities  
 Substation automation vulnerabilities  
 Control center vulnerabilities

## Impact Analysis

System performance  
 System stability

## Attack-defense studies

Denial of Sensor measurement (Substation → Control center)  
 Denial of Control (Control center → Substation)  
 Cyber-Physical Defense Evaluation



# Conclusion

## Topic 1: Cyber Security of Wide-Area Control

- How to design Attack-Resilient algorithms?
- Domain-specific Intrusion Detection

## Topic 2: Defense against Coordinated Attacks

- How to model Risk due to **coordinated cyber attacks**
- Risk mitigation algorithms

Testbed-based Evaluation Studies

# Research Challenges

1. Cyber Physical Systems Security
2. Risk Modeling and Mitigation
3. Transform: FROM Fault-Resilient Grid of today TO Attack-Resilient Grid of tomorrow
4. Defense against HILF cyber events
5. Trust management & Attack Attribution
6. DMS and AMI Security
7. Datasets and Validations

THANK YOU