Talk @ University of Tennessee, Knoxville, Feb. 16, 2018

Cybersecurity for the Power Grid in the face of growing challenge

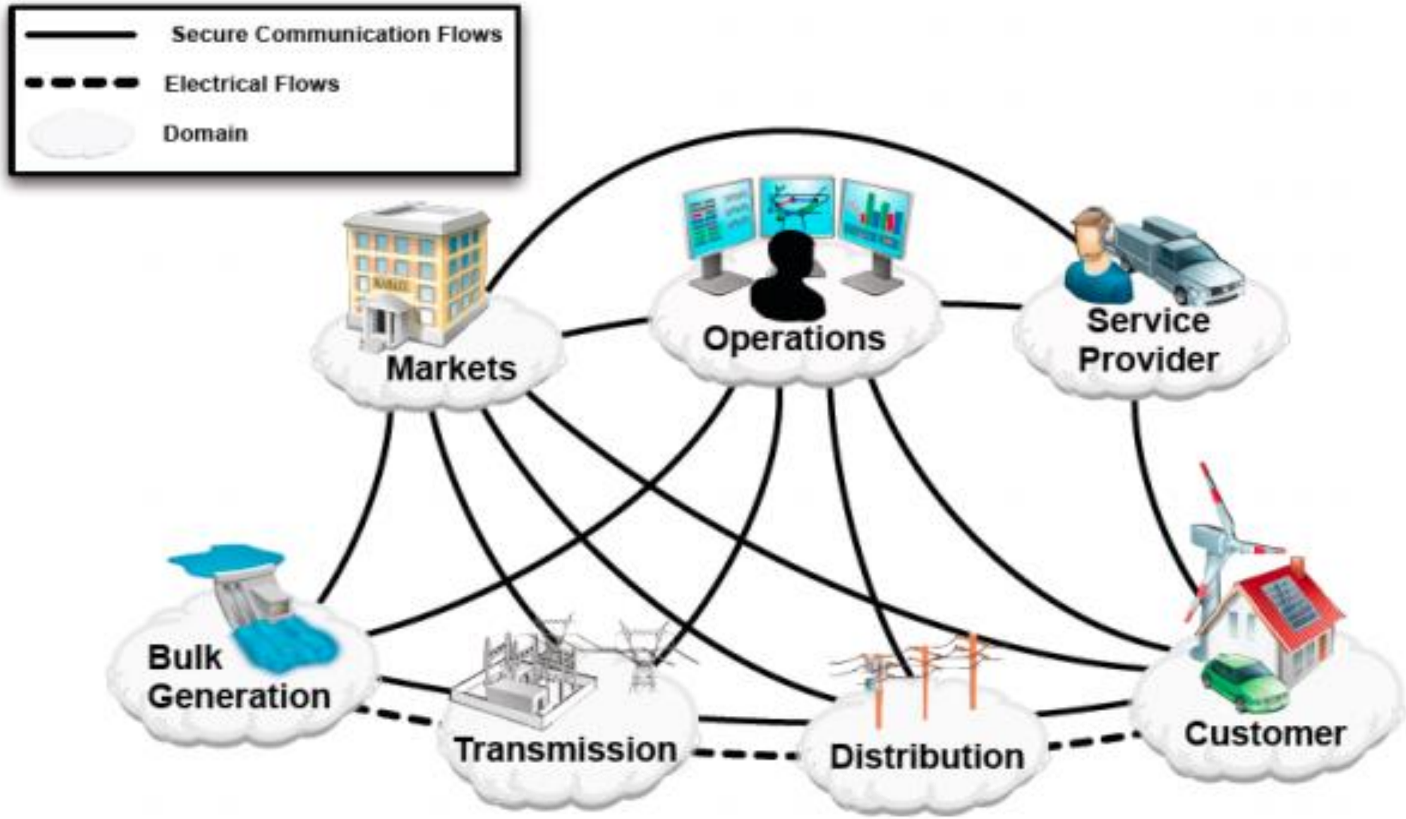
Manimaran Govindarasu

Dept. of Electrical and Computer Engineering
Iowa State University, USA
gmani@iastate.edu
http://powercyber.ece.iastate.edu

Outline of the Talk

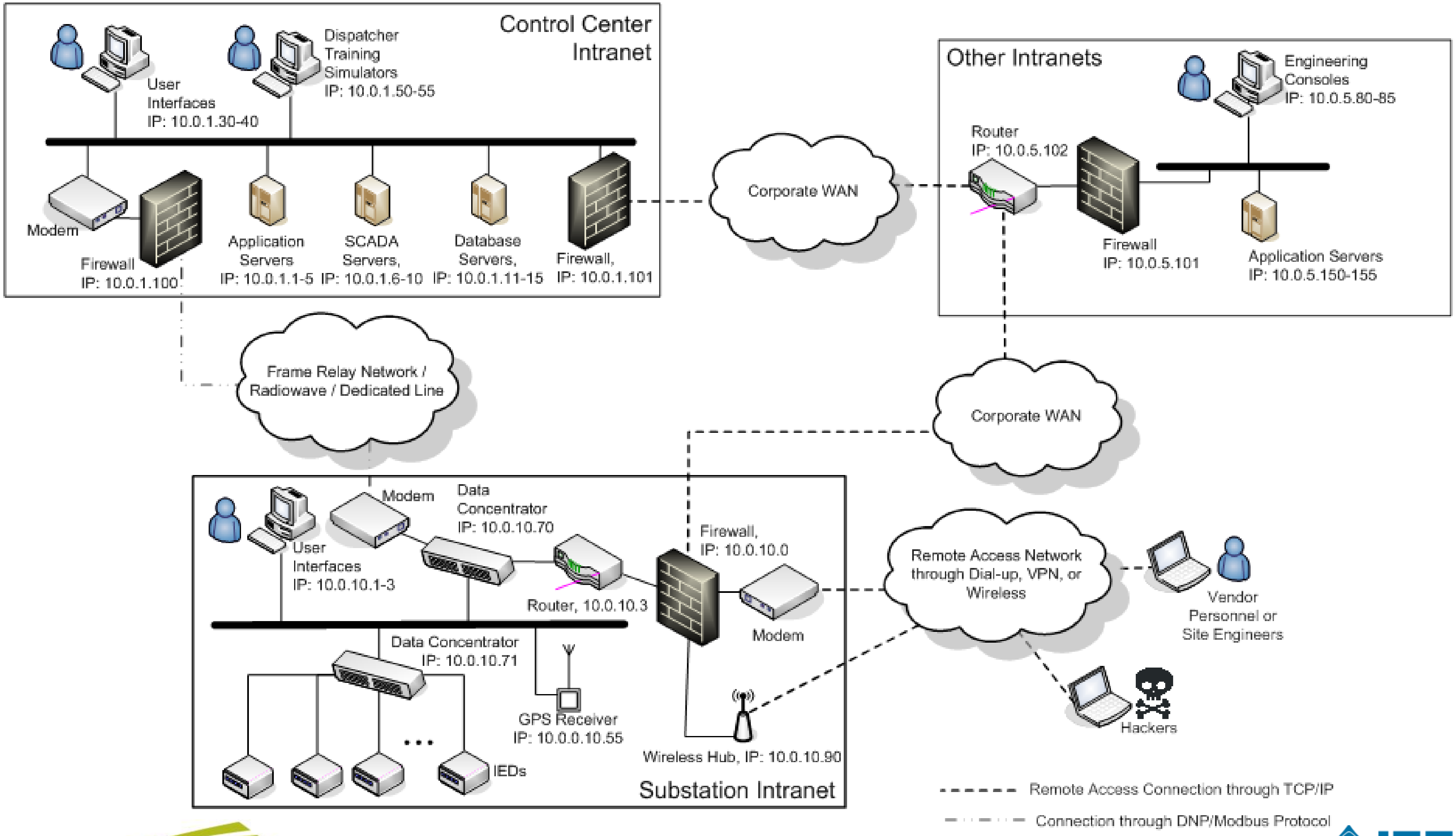
- Cyber Threat and Attacks
- Life-cycle security & Defense-in-Depth
- CPS security – case studies
- CPS security testbed
- Conclusions

Smart Grid: A Cyber-Physical System



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, February 2012

SCADA Control Network – A schematic

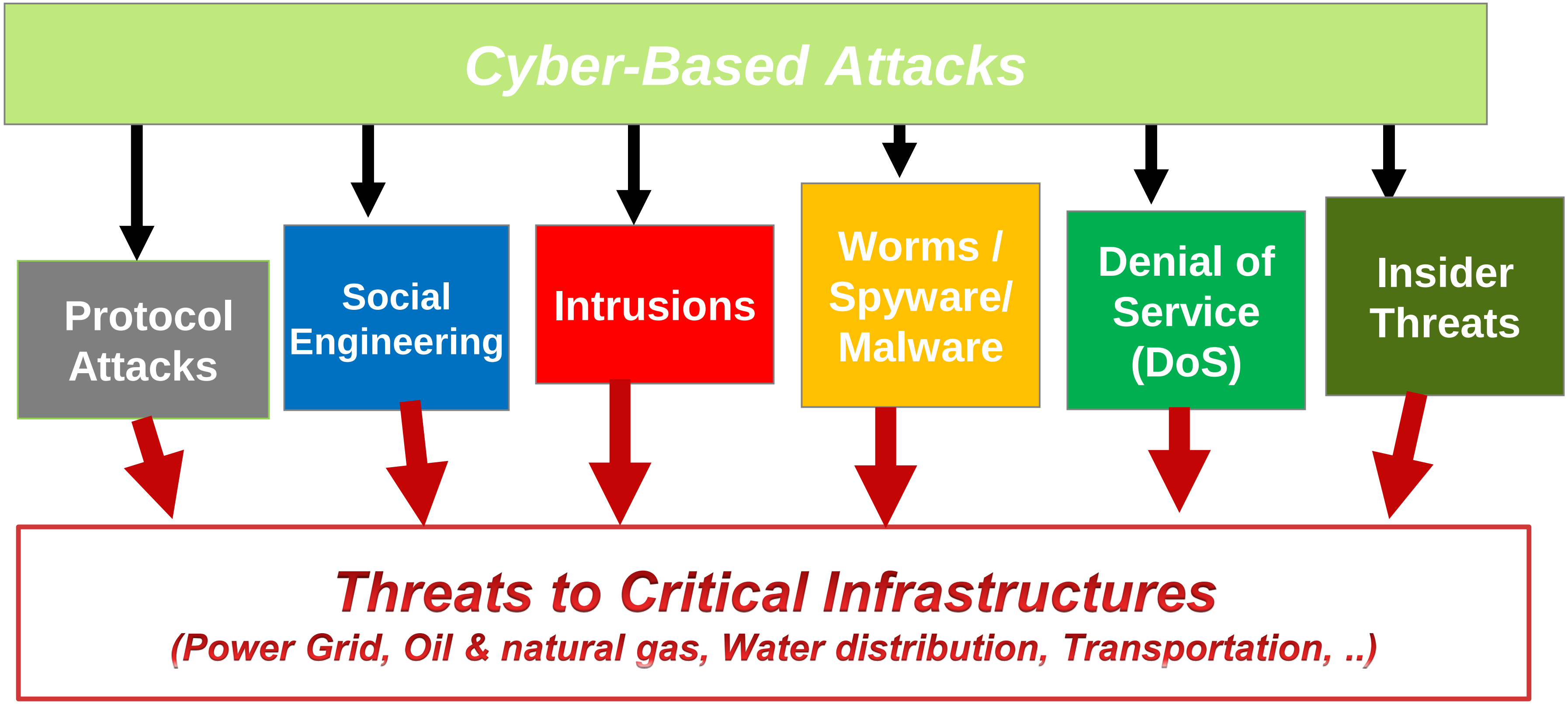


Control Center Intranet
User Interfaces IP: 10.0.1.30-40
Dispatcher Training Simulators IP: 10.0.1.50-55
Modem
Firewall IP: 10.0.1.100
Application Servers IP: 10.0.1.1-5
SCADA Servers, IP: 10.0.1.6-10
Database Servers, IP: 10.0.1.11-15
Firewall, IP: 10.0.1.101
Corporate WAN
Other Intranets
Engineering Consoles IP: 10.0.5.80-85
Router IP: 10.0.5.102
Firewall IP: 10.0.5.101
Application Servers IP: 10.0.5.150-155
Frame Relay Network / Radiowave / Dedicated Line
Corporate WAN
Modem
Data Concentrator IP: 10.0.10.70
User Interfaces IP: 10.0.10.1-3
Firewall, IP: 10.0.10.0
Router, 10.0.10.3
Modem
Data Concentrator IP: 10.0.10.71
GPS Receiver IP: 10.0.0.10.55
Wireless Hub, IP: 10.0.10.90
IEDs
Substation Intranet
Remote Access Network through Dial-up, VPN, or Wireless
Vendor Personnel or Site Engineers
Hackers
Remote Access Connection through TCP/IP
Connection through DNP/Modbus Protocol

IEEE SMARTGRID

IEEE Advancing Technology for Humanity

Cyber Threats to Critical Infrastructures



Cyber-Based Attacks

Protocol Attacks

Social Engineering

Intrusions

Worms / Spyware/ Malware

Denial of Service (DoS)

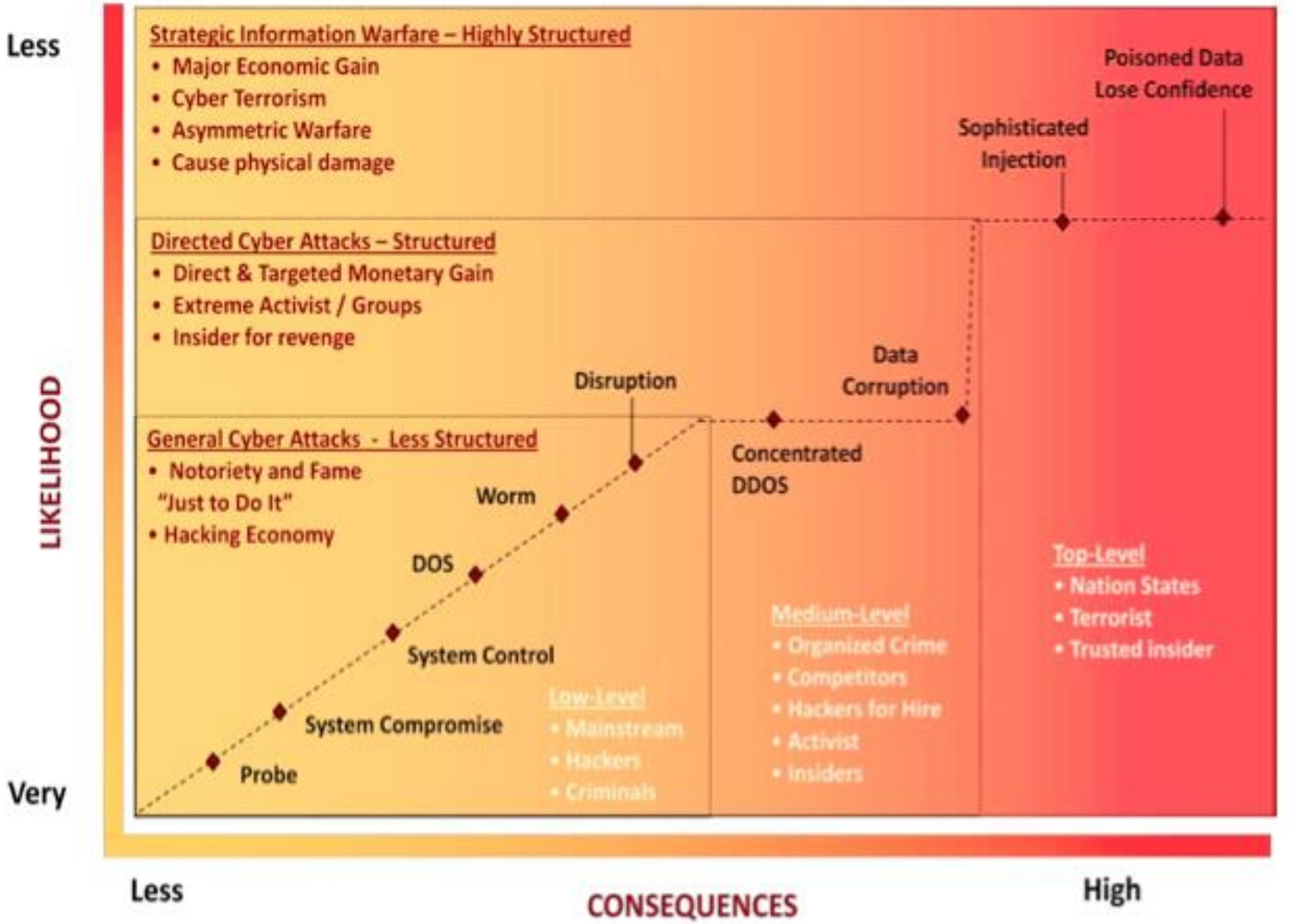
Insider Threats

Threats to Critical Infrastructures

(Power Grid, Oil & natural gas, Water distribution, Transportation, ..)

[Government Accounting Office, CIP Reports, 2004 to 2010 and beyond]; [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.*

Cyber Threats Landscape is dynamic !!! (DOE/NERC HILF Report)



Strategic Information Warfare – Highly Structured

- Major Economic Gain
- Cyber Terrorism
- Asymmetric Warfare
- Cause physical damage

Directed Cyber Attacks – Structured

- Direct & Targeted Monetary Gain
- Extreme Activist / Groups
- Insider for revenge

General Cyber Attacks - Less Structured

- Notoriety and Fame "Just to Do It"
- Hacking Economy

Low-Level

- Mainstream
- Hackers
- Criminals

Medium-Level

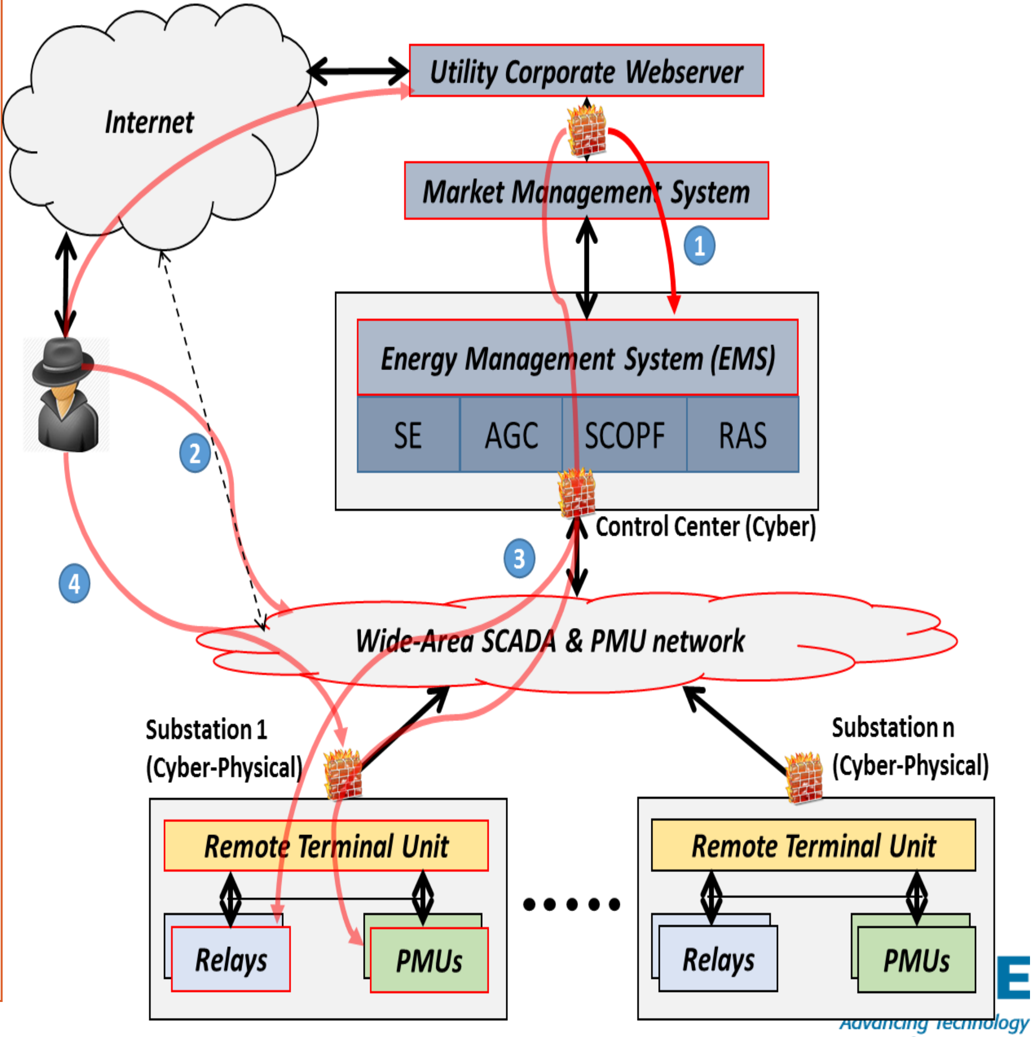
- Organized Crime
- Competitors
- Hackers for Hire
- Activist
- Insiders

Top-Level

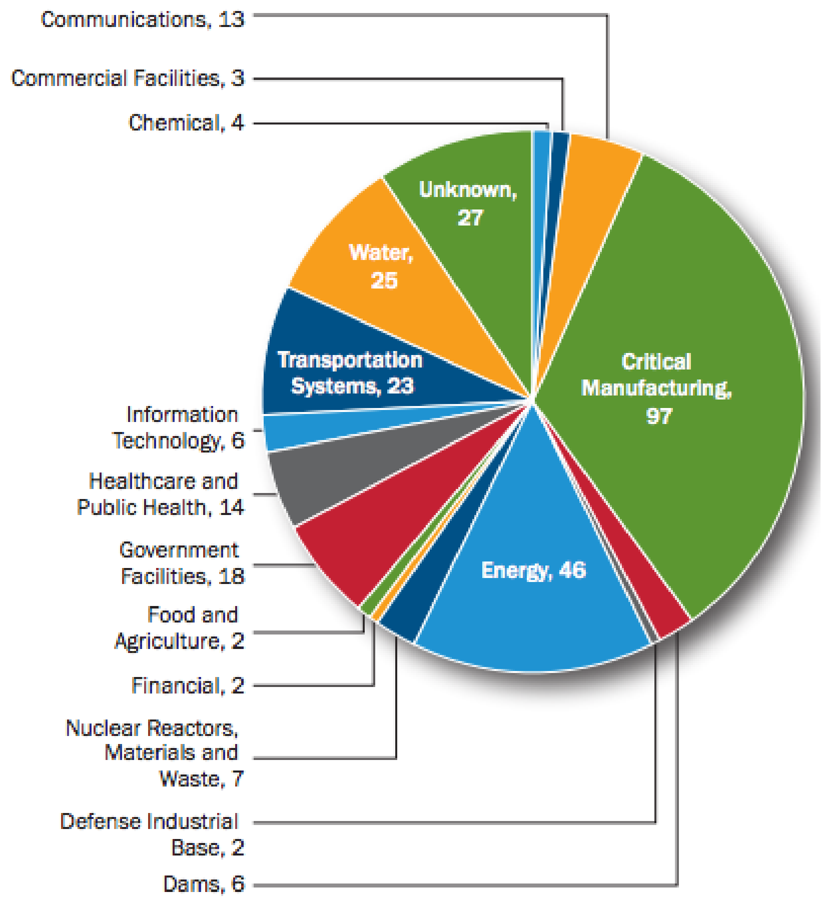
- Nation States
- Terrorist
- Trusted Insider

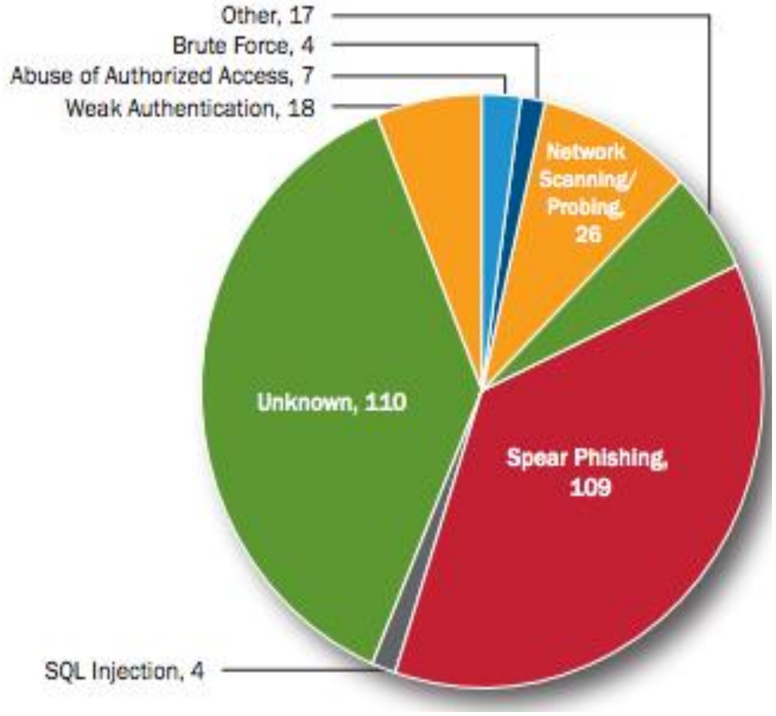
Attack Surface is increasing …

- ▣ Multiple attack paths and large attack surface
- ▣ Static configurations and network traffic → easy for reconnaisance
- ▣ Lack of clear metrics and tools to assess attack surface and reduce it
- ▣ Convergence of IT and OT lacking …
- ▣ Emergence of Internet of Things (IoT) in the grid context
- ▣ Distribution assets, smart meters, and DERs (wind, solar) are being increasingly deployed and are potentially vulnerable!



Cyber attack is growing – ICS-CERT 2015 Report





- 295 total intrusions in FY 2015
- 46 incidents in Energy Systems

Source: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

What happened in Ukraine in Dec. 2015?

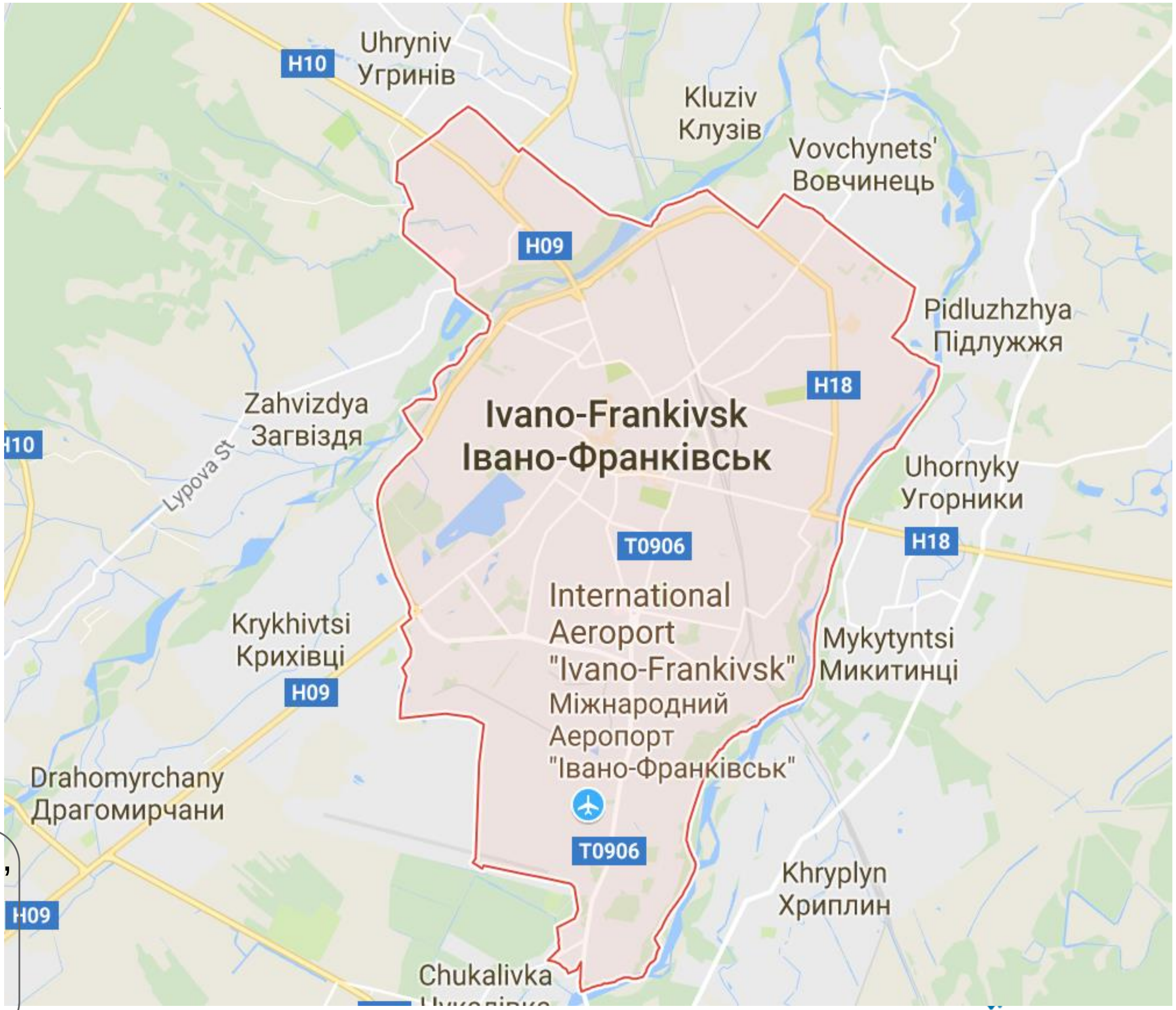
Attack-Impacts

- Coordinated cyber attack
- 3 distribution companies ~30 substations targeted
- 225k customers experienced outage

Attack path

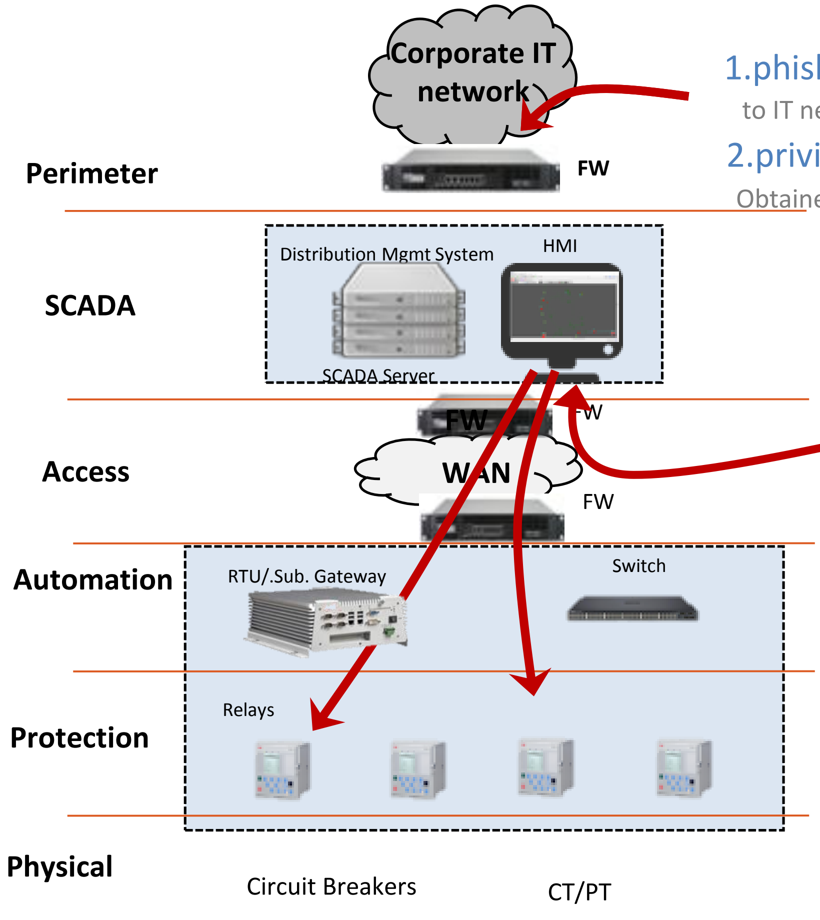
1. Spear phishing
2. Steal VPN credentials
3. VPN login
4. Open the breakers

Blackout Region: More than half of **Ivano-Frankivsk** region, some parts of **Chernivisti** region, some areas of **Kyiv** region.



Source: NERC Report on Ukraine attack

Ukraine grid's attack in Dec. 2015 ?



IT

1.phishing email

to IT network

2.privilege escalation

Obtained admin on DC

OT Pre-Impact

3.ot vpn login

Stolen credential from DC used to remotely login to vpn

4.install malware

BlackEnergy malware installed on control systems

5.remote hmi session

Created remote operators session to SCADA server

6.trip breakers

Operate key circuit breakers, 225,000 customers offline

OT Post-Impact

7.disable systems

Wipe SCADA servers, brick serial-ethernet converts and control center ups

8.telephone ddos

Telephone DDoS prevents communication about grid state

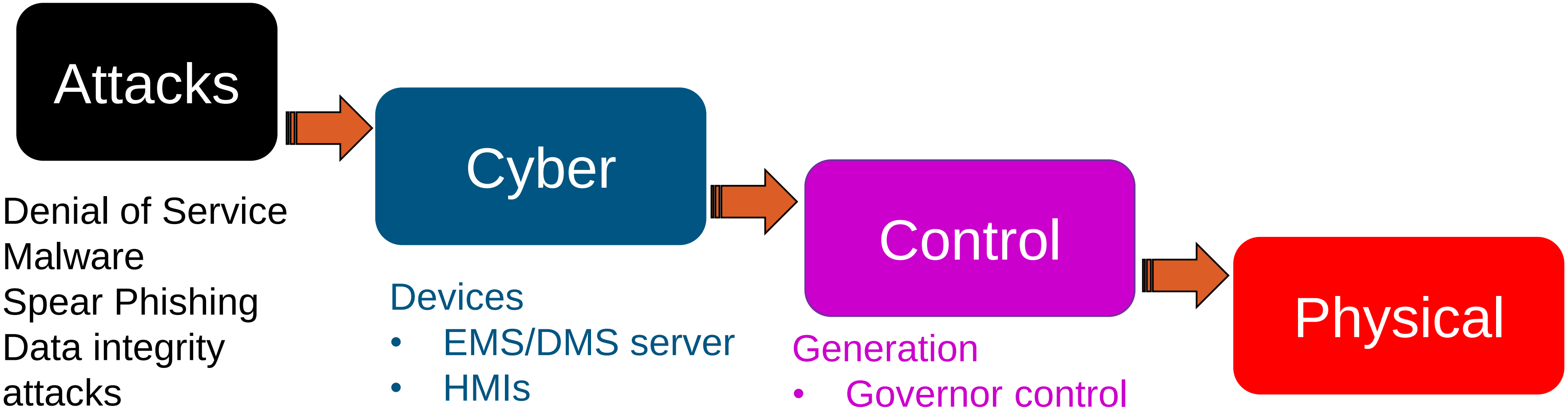
225K customers without power

Ack: Adam Hahn, Washington State University

Outline of the Talk

- Cyber Threat and Attacks
- Life-cycle security & Defense-in-Depth
- CPS security – case studies
- CPS security testbed
- Conclusions

Attacks-Cyber-Control-Physical view



Attacks

- Denial of Service
- Malware
- Spear Phishing
- Data integrity attacks
- Timing attacks
- Man-In-The-Middle attacks
- …..

Cyber

Devices

- EMS/DMS server
- HMIs
- PMUs
- Relays
- IEDs …

Networks

- Gateways
- Routers
- Protocols
- Data …

Control

Generation

- Governor control
- AGC, SCOPF
- Economic Dispatch

Transmission

- State Estimation
- Contingency analysis
- VAR compensation
- FACTS

Distribution

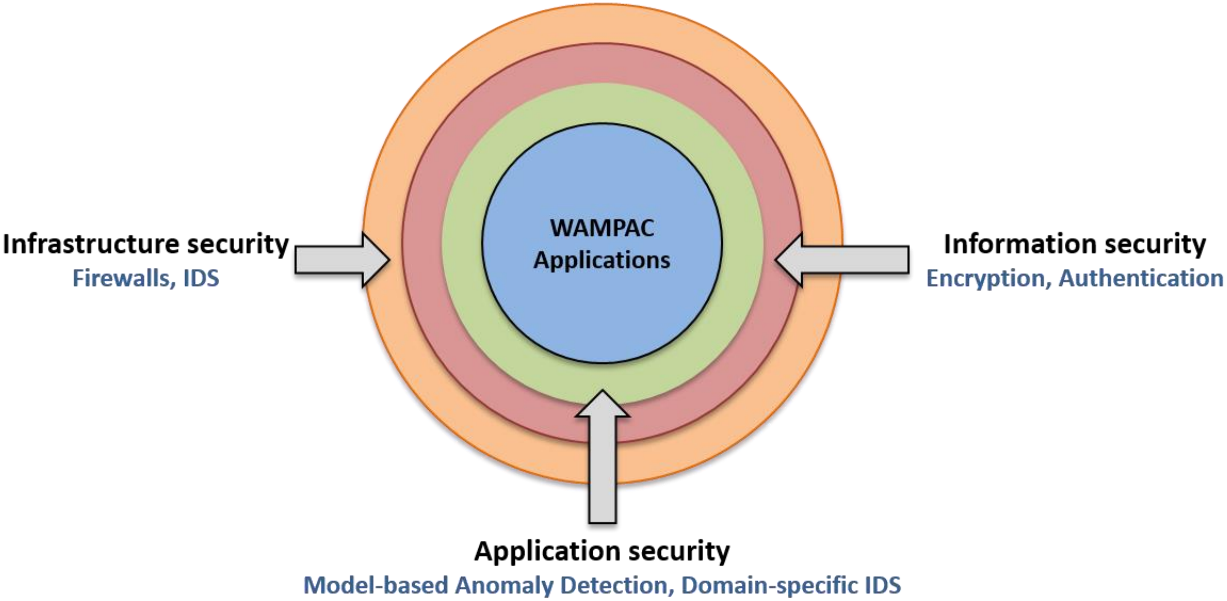
- Demand response
- Load shedding
- Storage control
- ….

Physical

- Blackout
- Stability violation
- Load rejection
- Equipment damage
- Economic impact
- …..

Cybersecurity architectural concepts:

Defense in Depth & Network segmentation



Infrastructure security

Firewalls, IDS

WAMPAC

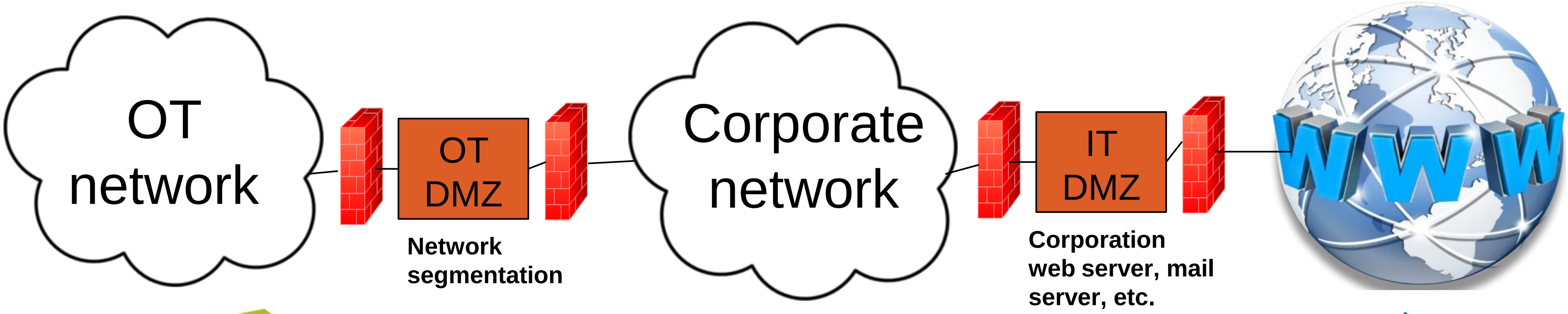
Applications

Information security

Encryption, Authentication

Application security

Model-based Anomaly Detection, Domain-specific IDS



OT network

OT DMZ

Network segmentation

Corporate network

IT DMZ

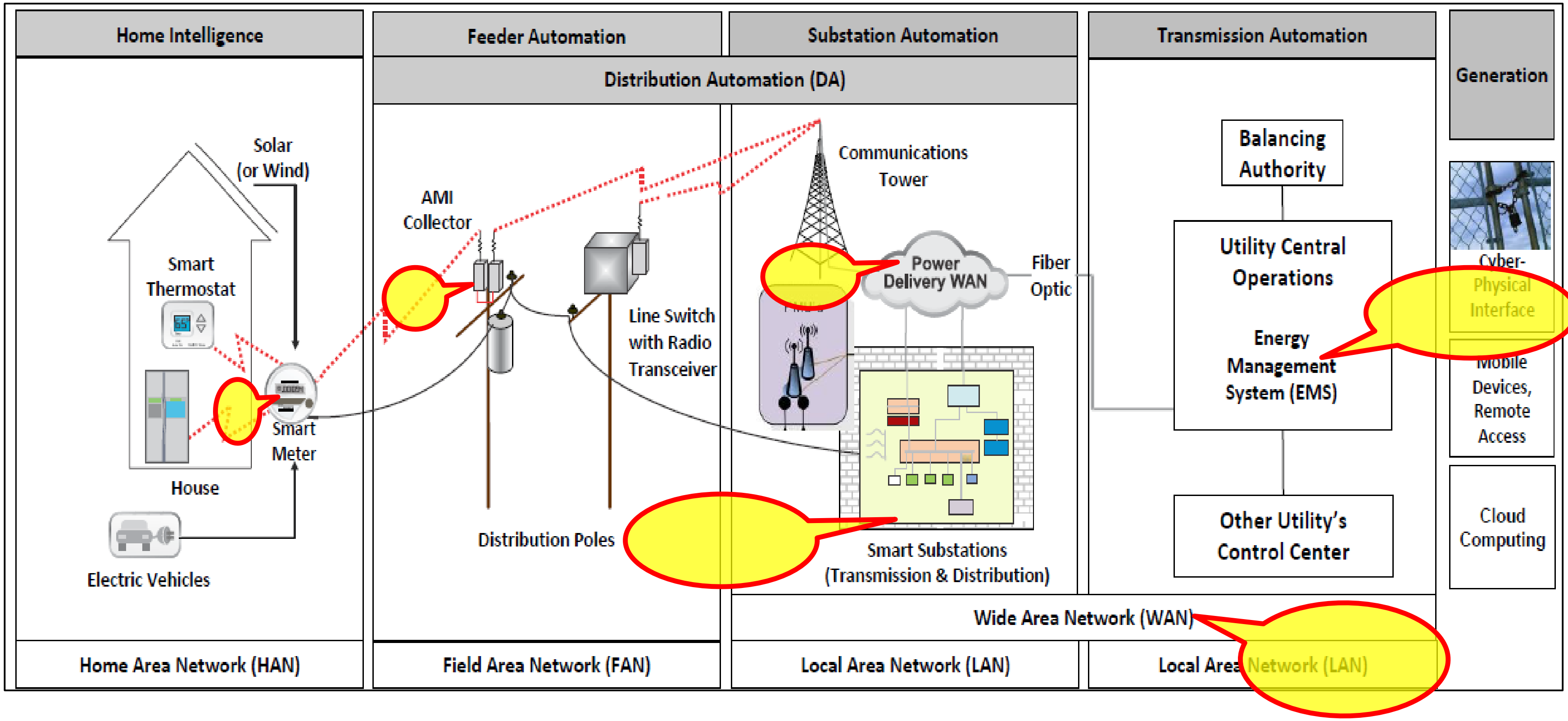
Corporation web server, mail server, etc.

Smart Security = Info + Infra + Control + Physical Security

	Information Security	Infrastructure Security	Control Systems Security	Physical Security
NEEDS	❑ Information Protection ▪ Message Confidentiality ▪ Message Integrity ▪ Message Authenticity	❑ Infrastructure protection ▪ Routers ▪ DNS servers ▪ Links ▪ Internet protocols ❑ Service availability	❑ Generation control apps. ❑ Transmission control apps. ❑ Distribution control apps. ❑ Real-Time Energy Markets	❑ Control Centers ❑ Power plants ❑ Transmission lines ❑ Substations ❑ DERs ❑ Customer devices
MEANS	❑ Encryption/Decryption ❑ Digital signature ❑ Message Auth.Codes ❑ Public Key Infrastructure	❑ Traffic Monitoring ❑ Statistical analysis ❑ Authentication Protocols ❑ Secure Protocols ❑ Secure Servers	❑ Attack-Resilient Control Algos ❑ Model-based Algorithms - Anomaly detection - Intrusion Tolerance - Bad data elimination ❑ Risk modeling and mitigation	❑ Physically secure all assets ❑ Surveillance ❑….

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

End-to-End Security & Attack Surface Reduction



Home Intelligence

Feeder Automation

Substation Automation

Transmission Automation

Generation

Distribution Automation (DA)

Solar (or Wind)

Smart Thermostat

Smart Meter

House

Electric Vehicles

AMI Collector

Line Switch with Radio Transceiver

Distribution Poles

Communications Tower

Power Delivery WAN

Fiber Optic

Smart Substations (Transmission & Distribution)

Balancing Authority

Utility Central Operations

Energy Management System (EMS)

Other Utility's Control Center

Cyber-Physical Interface

Mobile Devices, Remote Access

Cloud Computing

Wide Area Network (WAN)

Home Area Network (HAN)

Field Area Network (FAN)

Local Area Network (LAN)

Local Area Network (LAN)

Image Credit: DOE CEDS

Assess Risk	Develop and Implement New Protective Measures	Manage Incidents

Three key steps in US DOE Cybersecurity Roadmap

A Cybersecurity Lifecycle Model

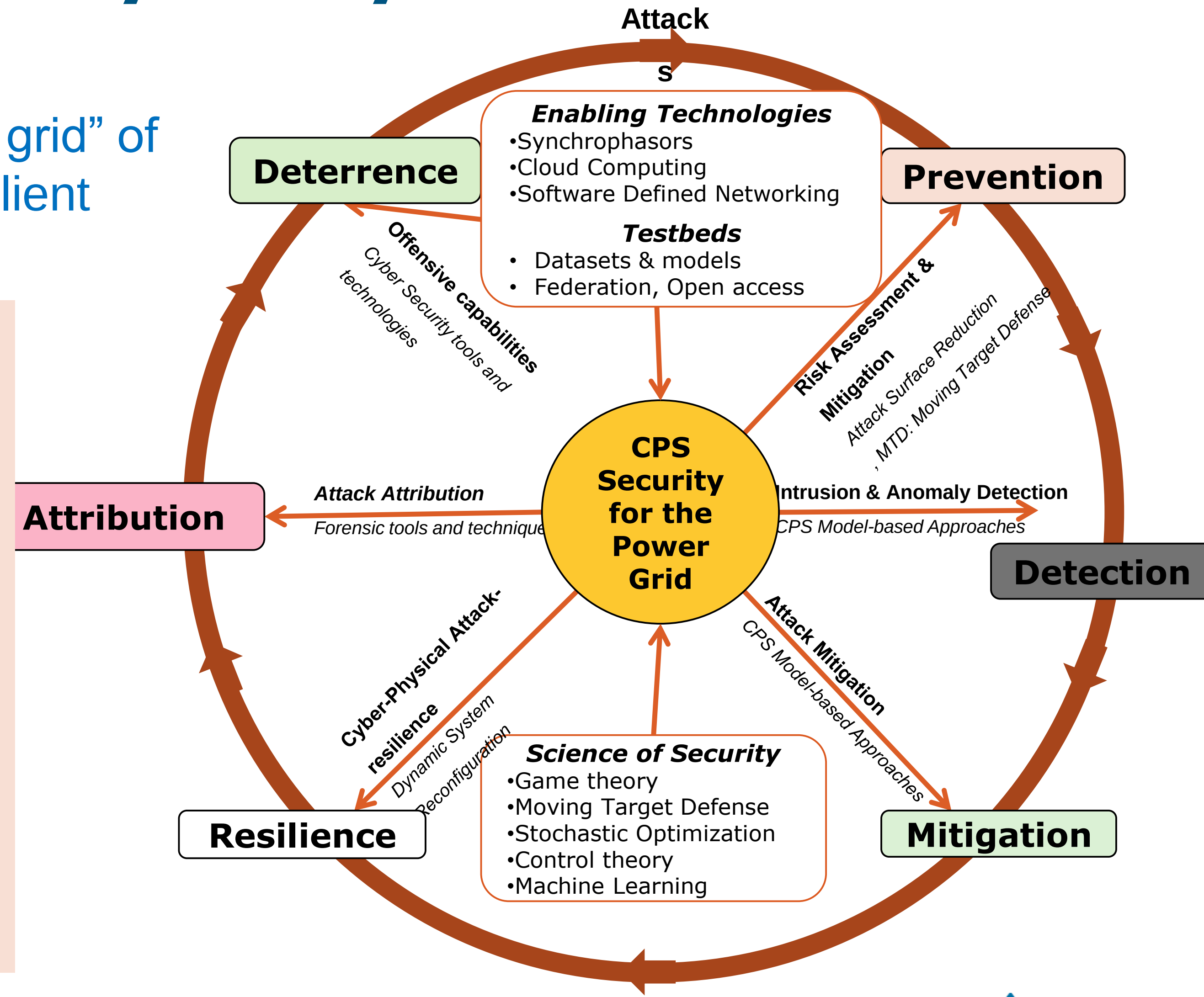
Long-term goal:

Transform “fault-resilient grid” of today into an “attack-resilient grid” of the future

- Technology
- Process
- People
- Regulation

Industry Collab.

- Problem formulation
- Testbed Experiments
- Tech Transfer
- Education & Training
- Workforce Develop.



Attacks

Deterrence

Prevention

Detection

Mitigation

Resilience

Attribution

CPS Security for the Power Grid

Enabling Technologies
- •Synchrophasors
- •Cloud Computing
- •Software Defined Networking

Testbeds
- Datasets & models
- Federation, Open access

Science of Security
- •Game theory
- •Moving Target Defense
- •Stochastic Optimization
- •Control theory
- •Machine Learning

Offensive capabilities
Cyber Security tools and technologies

Risk Assessment & Mitigation
Attack Surface Reduction
, MTD: Moving Target Defense

Intrusion & Anomaly Detection
CPS Model-based Approaches

Attack Mitigation
CPS Model-based Approaches

Cyber-Physical Attack-resilience
Dynamic System Reconfiguration

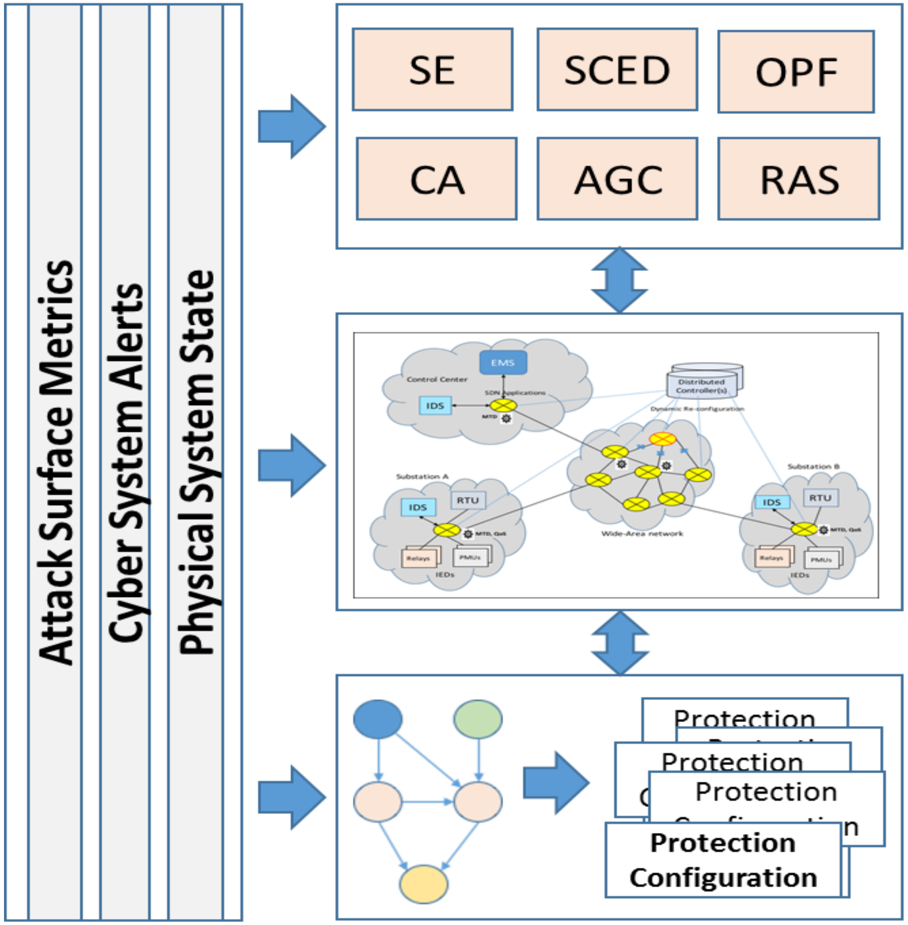
Attack Attribution
Forensic tools and technique

CPS Security for WAMPAC, Proc. of the IEEE, May 2017

Attack Surface Reduction:

Virtualization, Moving Target Defense (MTD), Anomaly Detection

- Control Center
- SCADA network
- Substations



Attack Surface Metrics

Cyber System Alerts

Physical System State

SE

SCED

OPF

CA

AGC

RAS

Protection

Protection

Protection

Protection Configuration

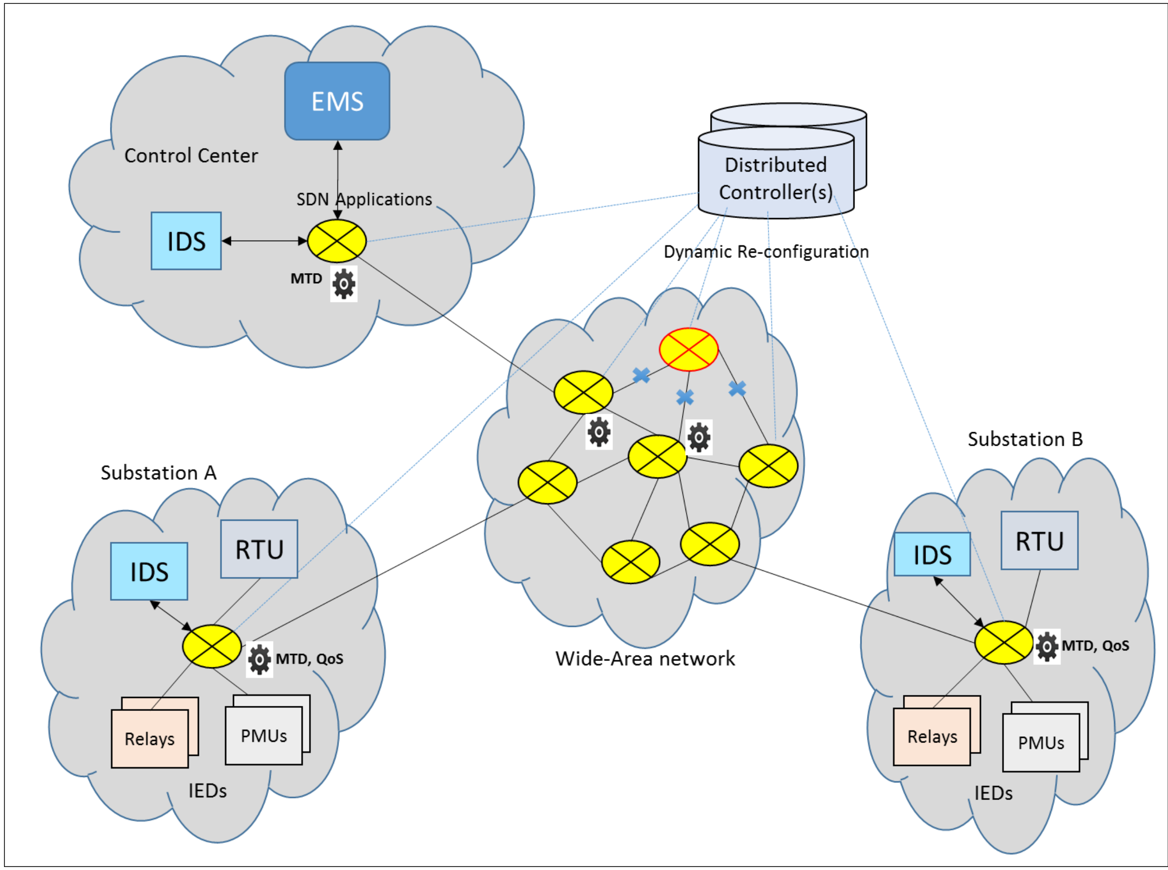
2.3.3 EMS/DMS/SCADA Application Virtualization, Isolation @ Control Center

2.3.2 Network-based MTD @ SCADA network

2.3.1 Causal Graph based CPS MTD @ Substations

Moving Target Defense (MTD)

- Introduce controlled "uncertainty" in system operation without any adverse effect → confuse the adversary



Examples:

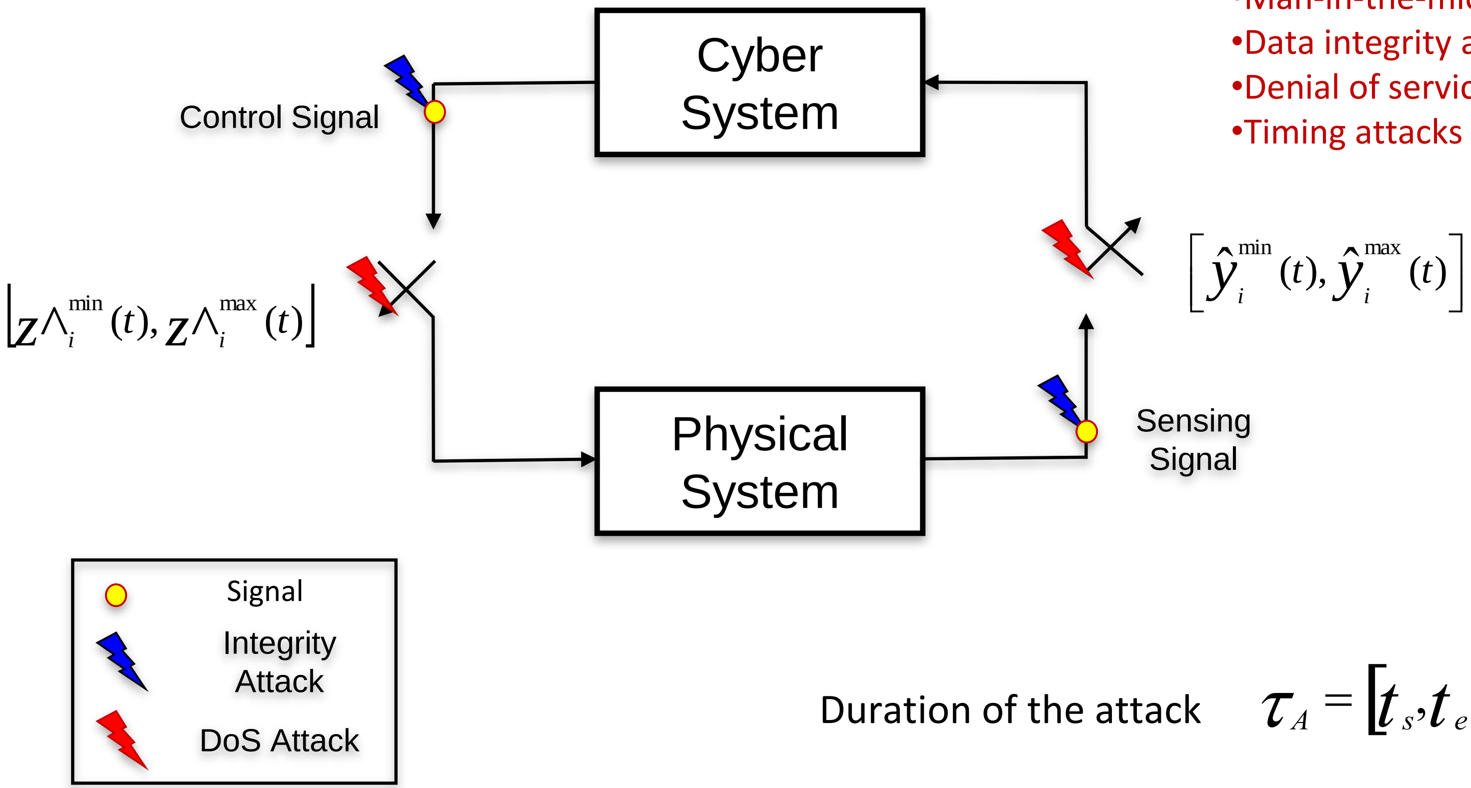
- Randomize network connectivity & addresses (IP Hopping)
- Randomize measurements & application behavior

Outline of the Talk

- Cyber Threat and Attacks
- Life-cycle security & Defense-in-Depth
- CPS security & Case studies
- CPS security testbed
- Conclusions

Cyber-Physical Control View

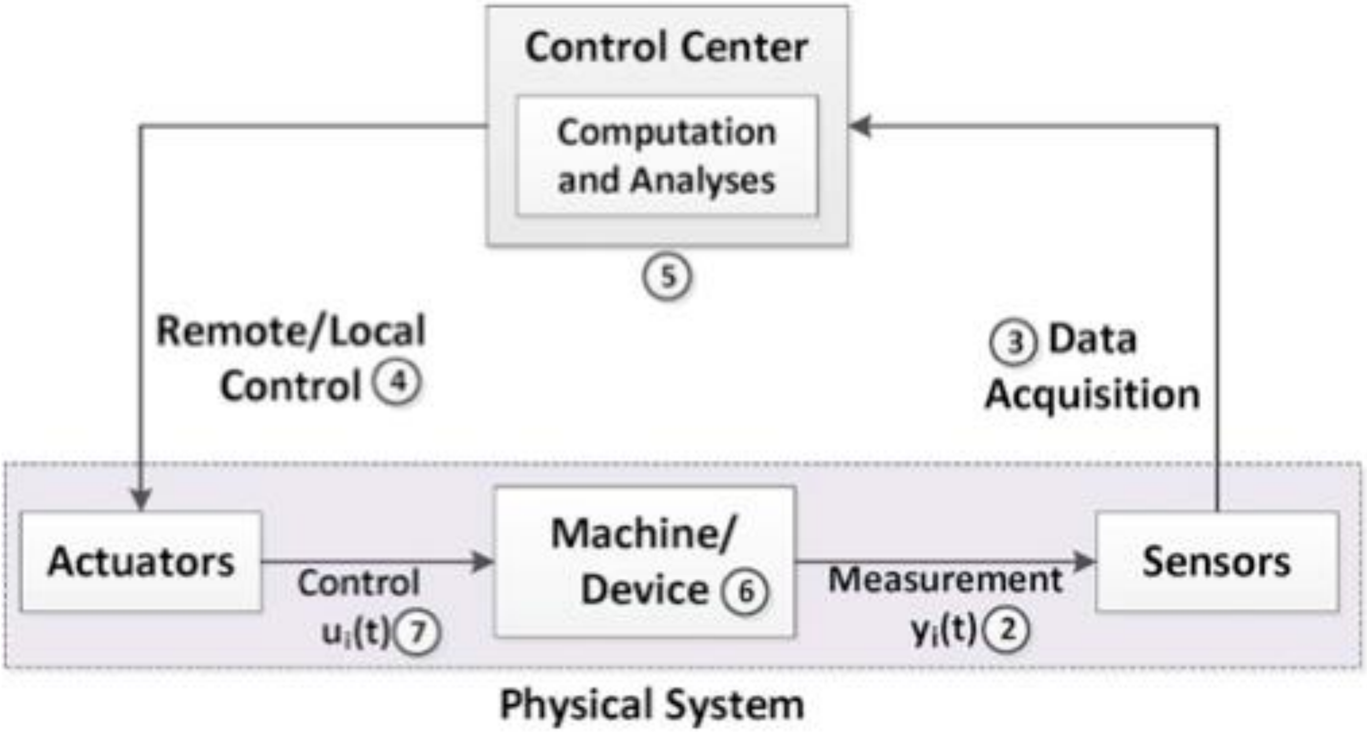
- Man-in-the-middle attacks
- Data integrity attacks
- Denial of service attacks
- Timing attacks …


Cyber System
Control Signal
Physical System
Sensing Signal
$\left[z\wedge_i^{\min}(t), z\wedge_i^{\max}(t)\right]$
$\left[\hat{y}_i^{\min}(t), \hat{y}_i^{\max}(t)\right]$
● Signal
Integrity Attack
DoS Attack

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

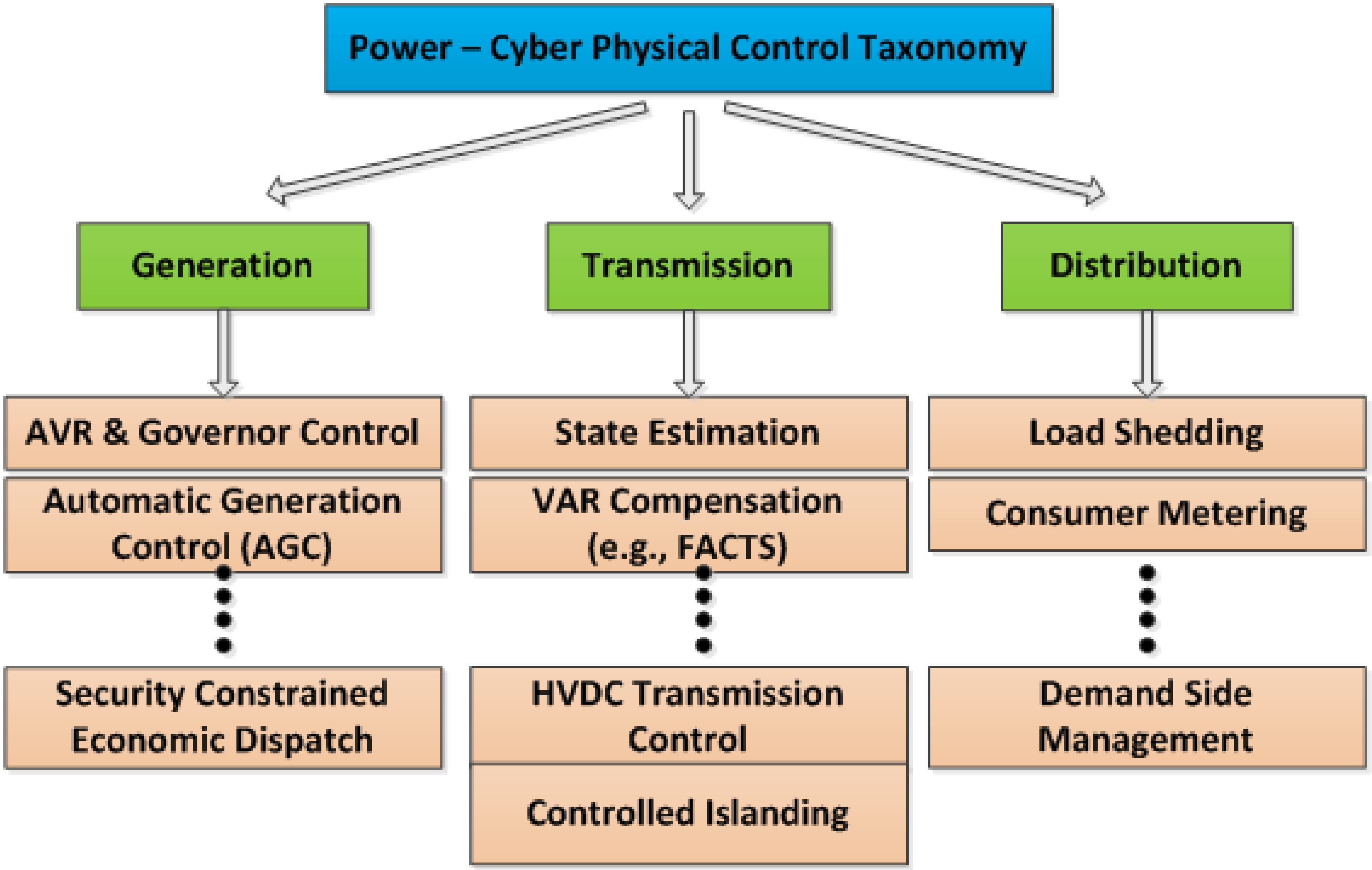
Y. Huang, A. A. Cardenas, S. Sastry, "*Understanding the Physical and Economic Consequences of Attacks on Control Systems*", Elsevier, International Journal of Critical Infrastructure Protection 2009.

Typical Power System Control loop



Siddharth Sridhar, Adam Hahn and G. Manimaran – “Cyber–Physical System Security for the Electric Power Grid” – Proceedings of the IEEE, Jan 2012

Cyber-Physical Control Taxonomy



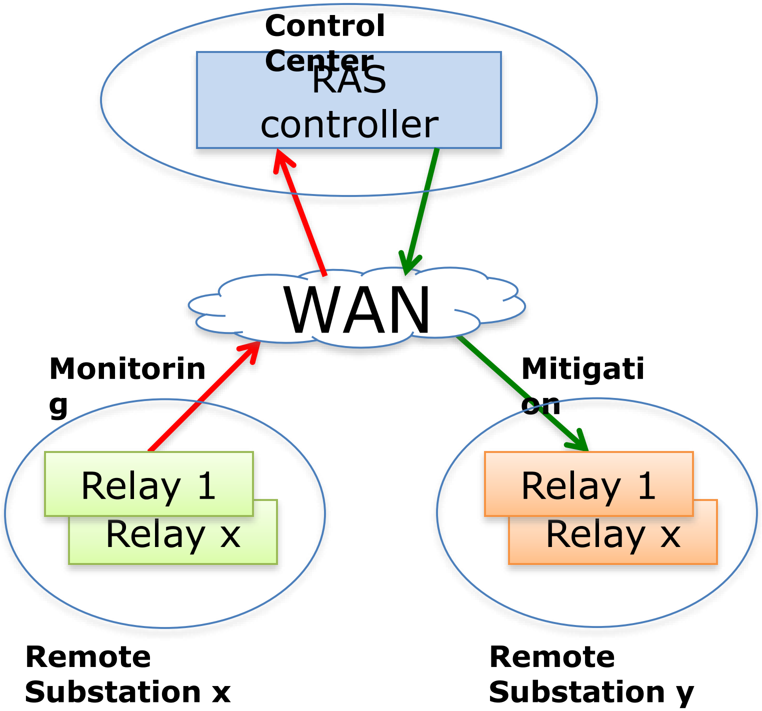
Power – Cyber Physical Control Taxonomy
Generation
Transmission
Distribution
AVR & Governor Control
Automatic Generation Control (AGC)
Security Constrained Economic Dispatch
State Estimation
VAR Compensation (e.g., FACTS)
HVDC Transmission Control
Controlled Islanding
Load Shedding
Consumer Metering
Demand Side Management

Wide-Area Protection

Remedial Action Schemes (RAS) – Automatic protection systems designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability.

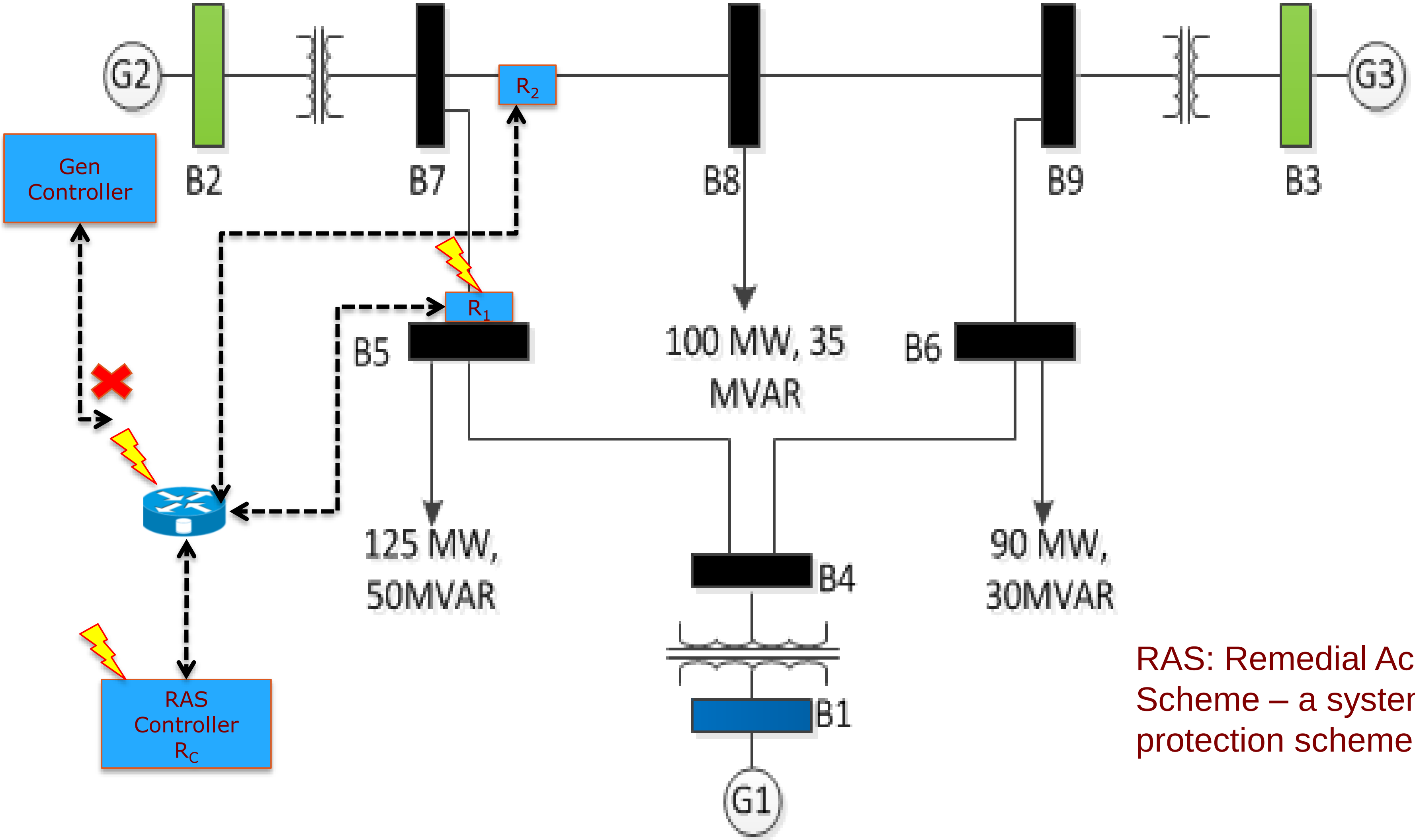
Typical RAS corrective actions are :

- Changes in load (MW)
- Changes in generation (MW and MVAR)
- Changes in system configuration to maintain system stability, acceptable voltage or power flows



Source: V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, and A. Apostolov, "Ieee psrc report on global indu experiences with system integrity protection schemes (sips)," Power Delivery, IEEE Transactions on, vol. 25, pp. 2143 –2155, oct. 2010.

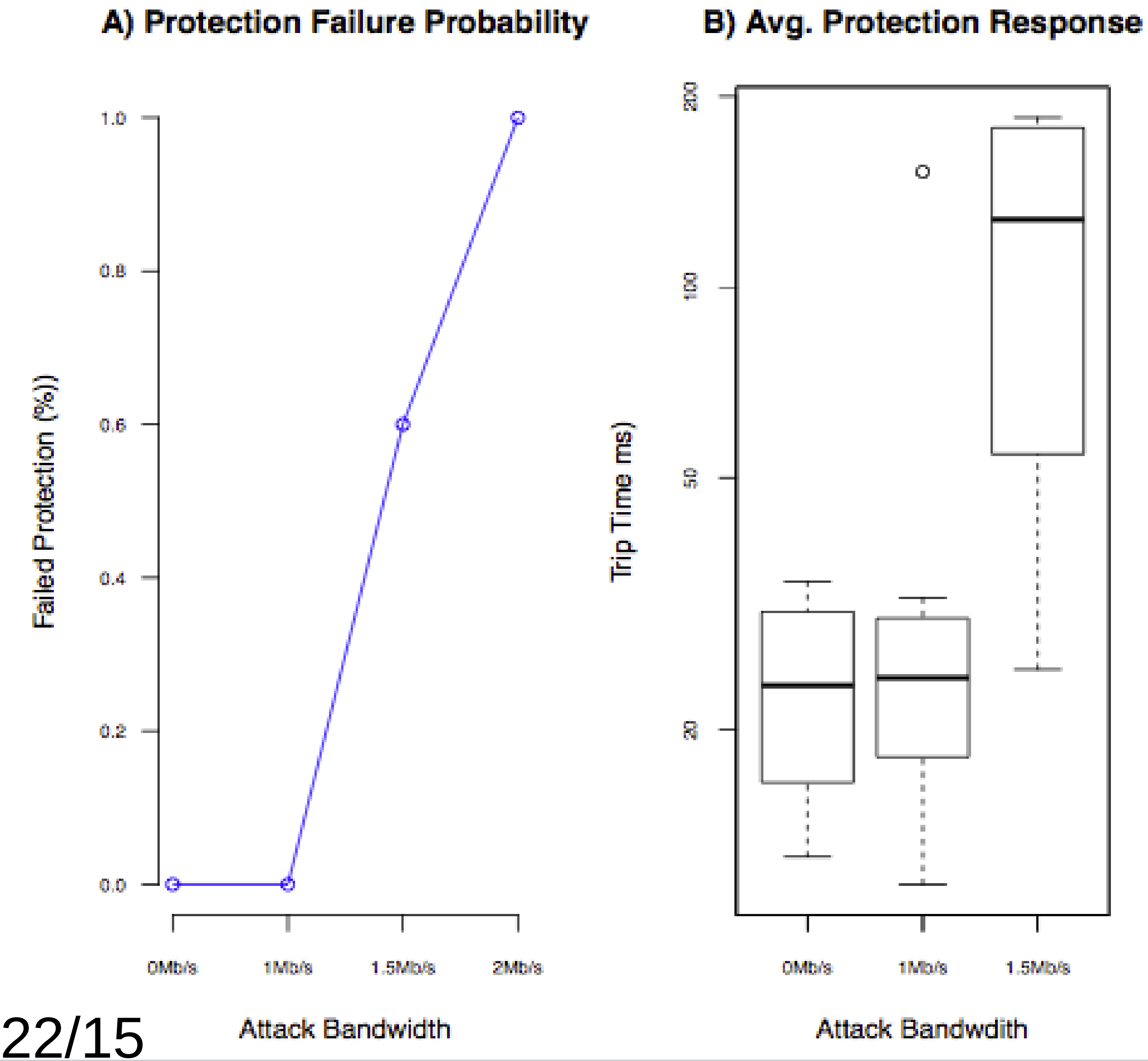
Wide-Area Protection – Attack on RAS WECC 9-bus system



RAS: Remedial Action Scheme – a system protection scheme

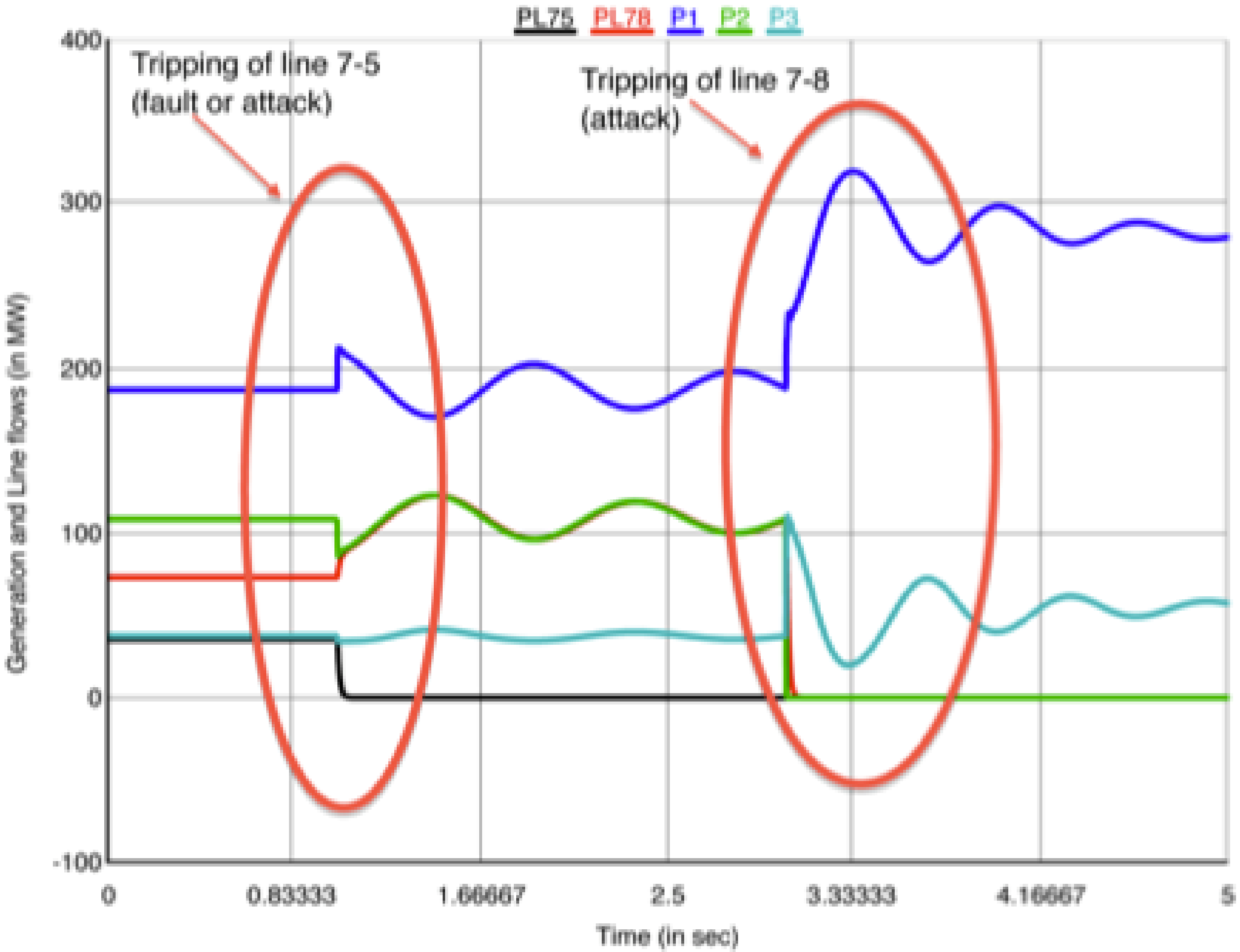
A. Hahn, A. Ashok, M. Govindarasu, “Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid”, IEEE Trans. on Smart Grid, June 2013.

DoS on RAS Controller (Relay)


A) Protection Failure Probability

B) Avg. Protection Response

Power system Impacts

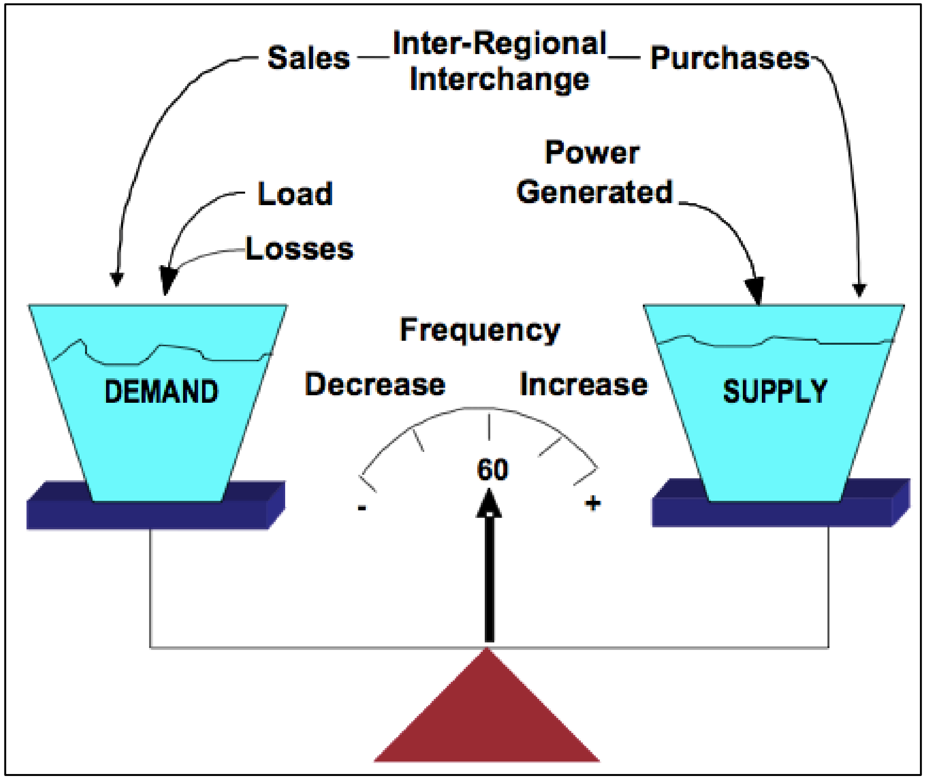


Automatic Generation Control (AGC)

AGC Features

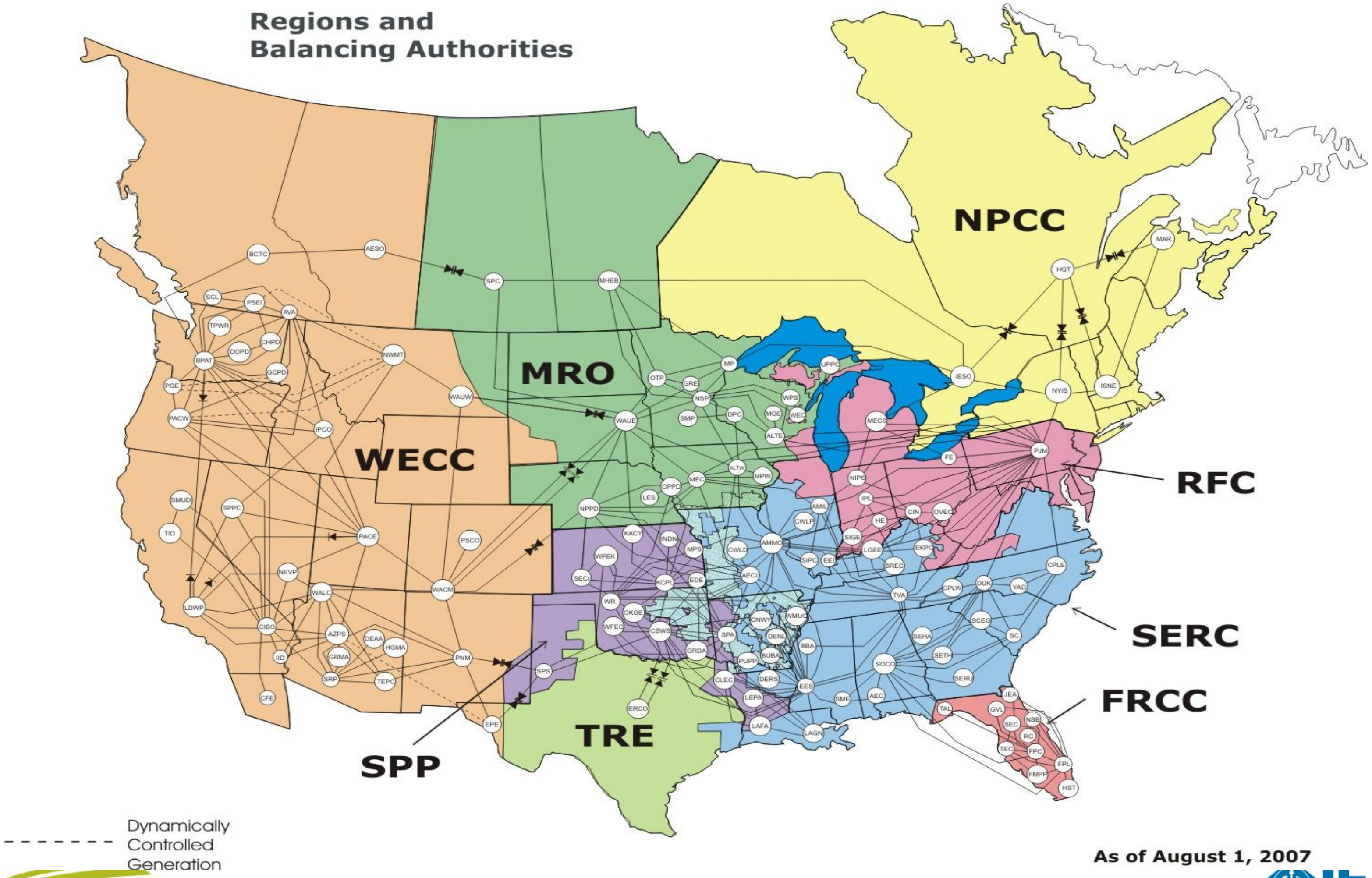
- Maintains frequency at 60 Hz
- **Supply = Demand**
- Maintain power exchange at scheduled value
- Ensures economic generation

[Figure from NERC Balancing and Frequency Control www.nerc.com]



Source: Balancing and Frequency Control – a NERC publication
http://www.nerc.com/docs/oc/rs/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf

Balancing Authorities in the U.S.



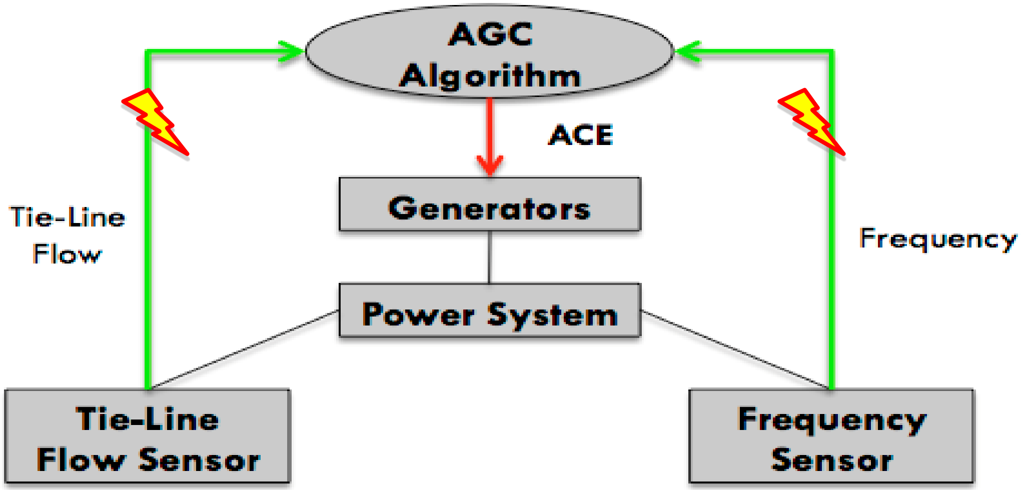
As of August 1, 2007

Source: NERC

IEEE
SMARTGRID

IEEE
Advancing Technology
for Humanity

Automatic Generation Control (AGC)



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

ΔP_{net} = Scheduled Flow – Actual Flow

Δf = 60 Hz – Measured Frequency

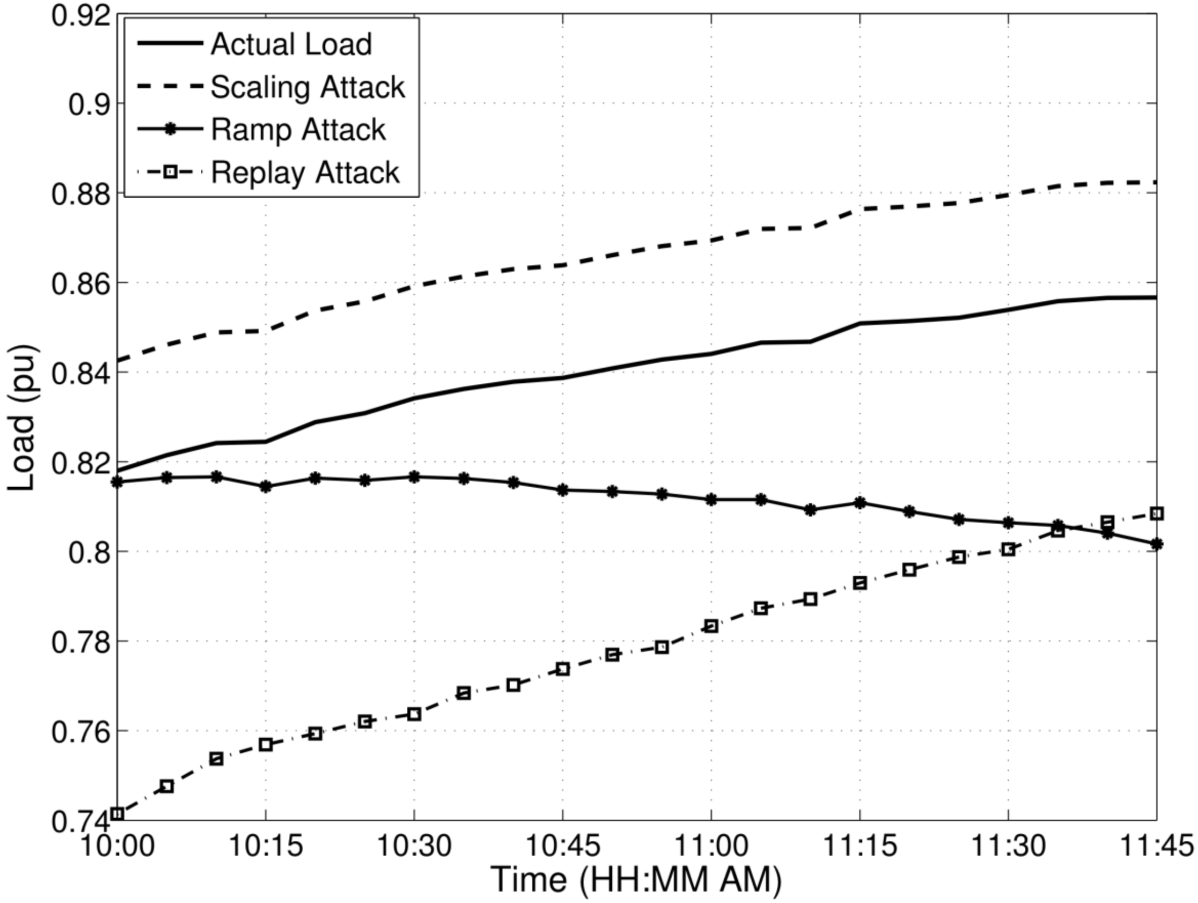
Attack: **Modify tie-line flow and frequency measurements**

Impact:
i) Abnormal operating frequency conditions
ii) Uneconomic generation

S. Sridhar and G. Manimaran – "Data Integrity Attacks and Impacts on SCADA Control System" – IEEE PES GM 2010

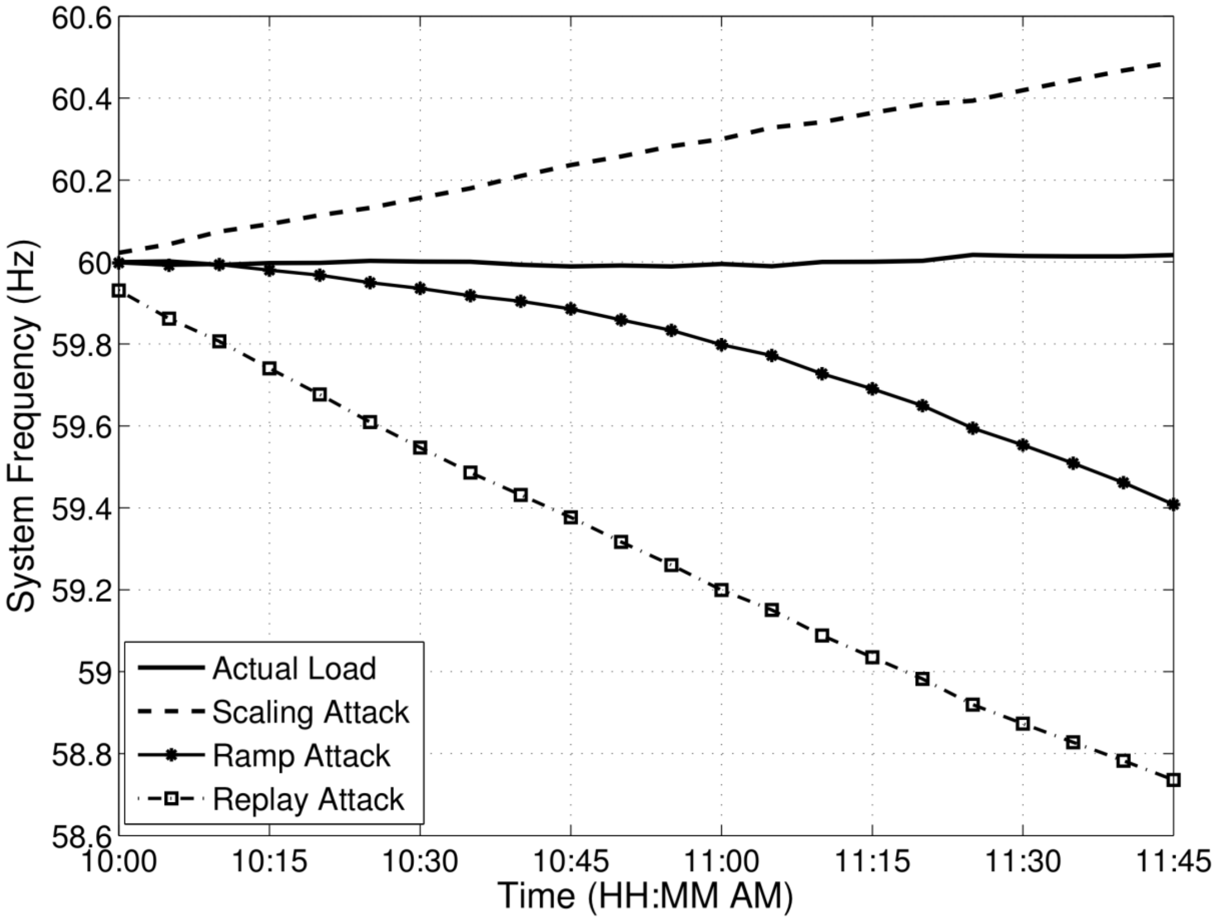
AGC – attack impacts (sample result)

Attack Impact – Perceived Load at the Control Center

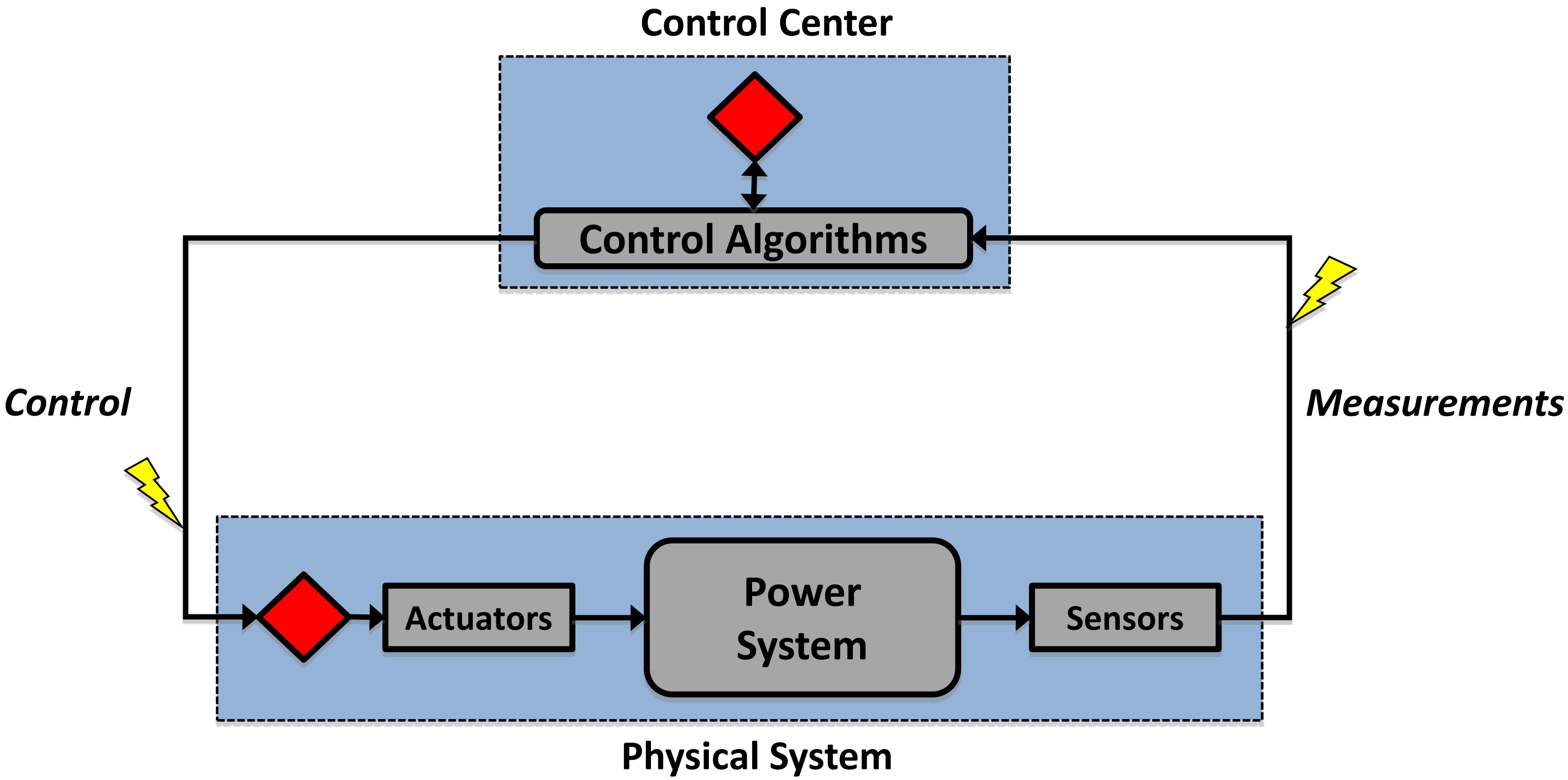


AGC – attack impacts (sample result)

Attack Impact – Resulting System Frequency

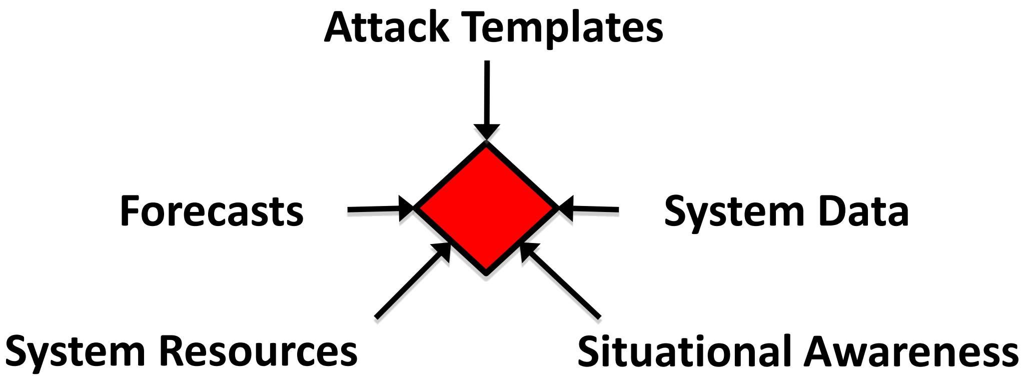


Attack Resilient Control (ARC)



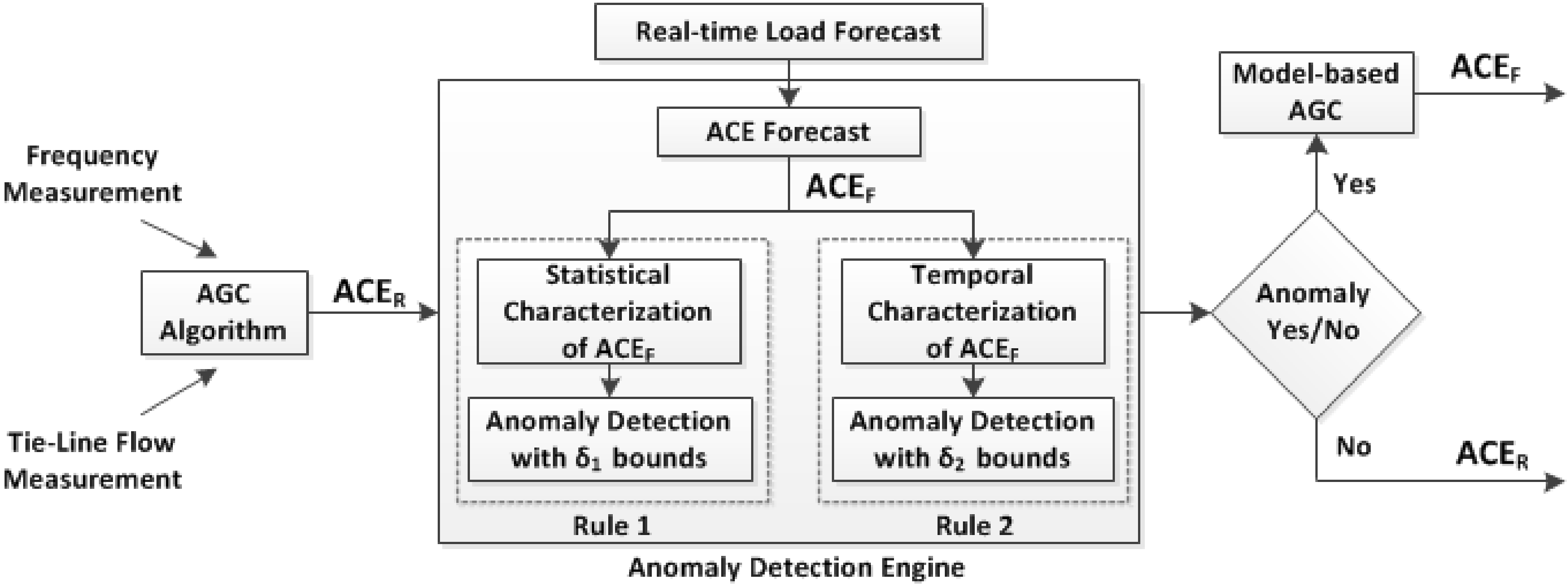
◆ → Intelligent Attack Detection and Mitigation Module

ARC – Sources of data for the model



- **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

Model-based Attack Detection & Mitigation for AGC


Real-time Load Forecast
ACE Forecast
ACE_F
Frequency Measurement
Tie-Line Flow Measurement
AGC Algorithm
ACE_R
Statistical Characterization of ACE_F
Anomaly Detection with δ_1 bounds
Rule 1
Temporal Characterization of ACE_F
Anomaly Detection with δ_2 bounds
Rule 2
Anomaly Detection Engine
Anomaly Yes/No
Yes
Model-based AGC
ACE_F
No
ACE_R

Key

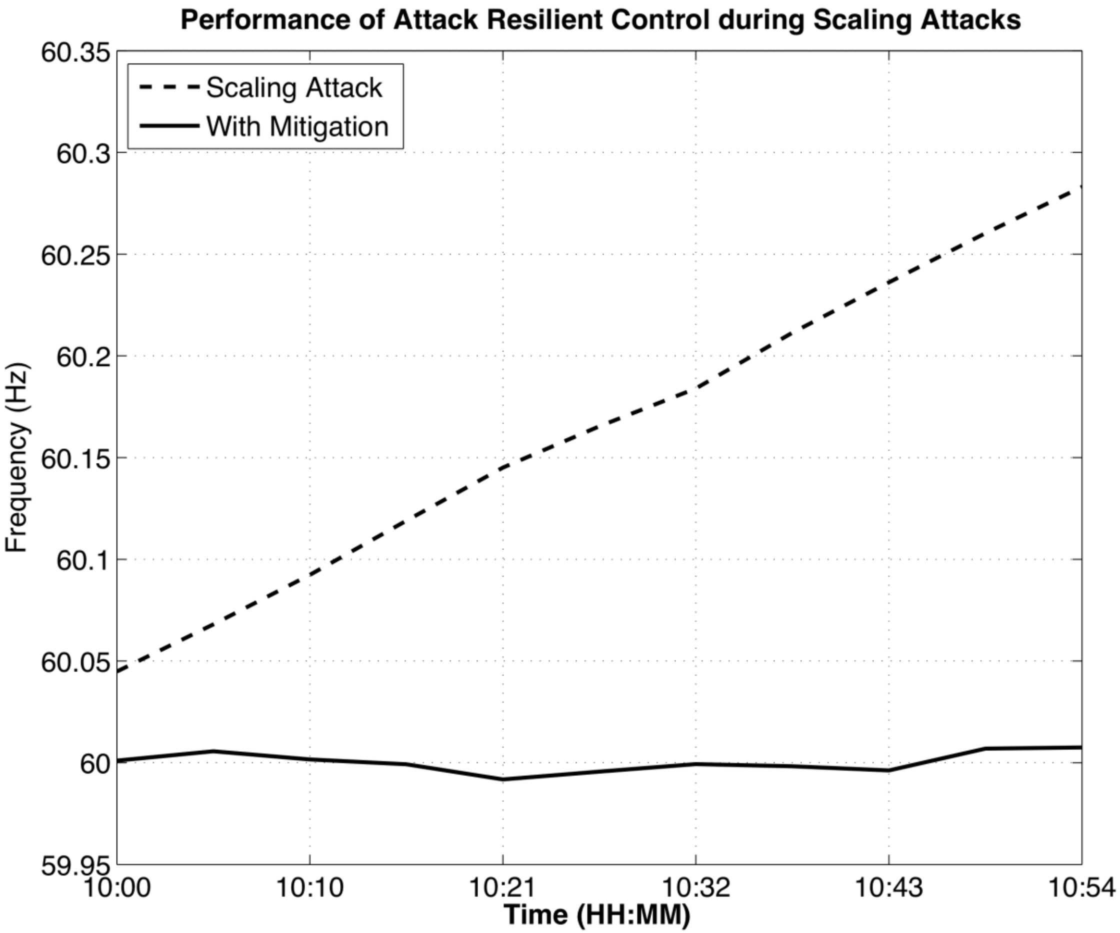
ACE_R – ACE obtained from real-time measurements

ACE_F – ACE obtained from forecast

S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for AGC”, IEEE Trans. Smart Grid, 2014

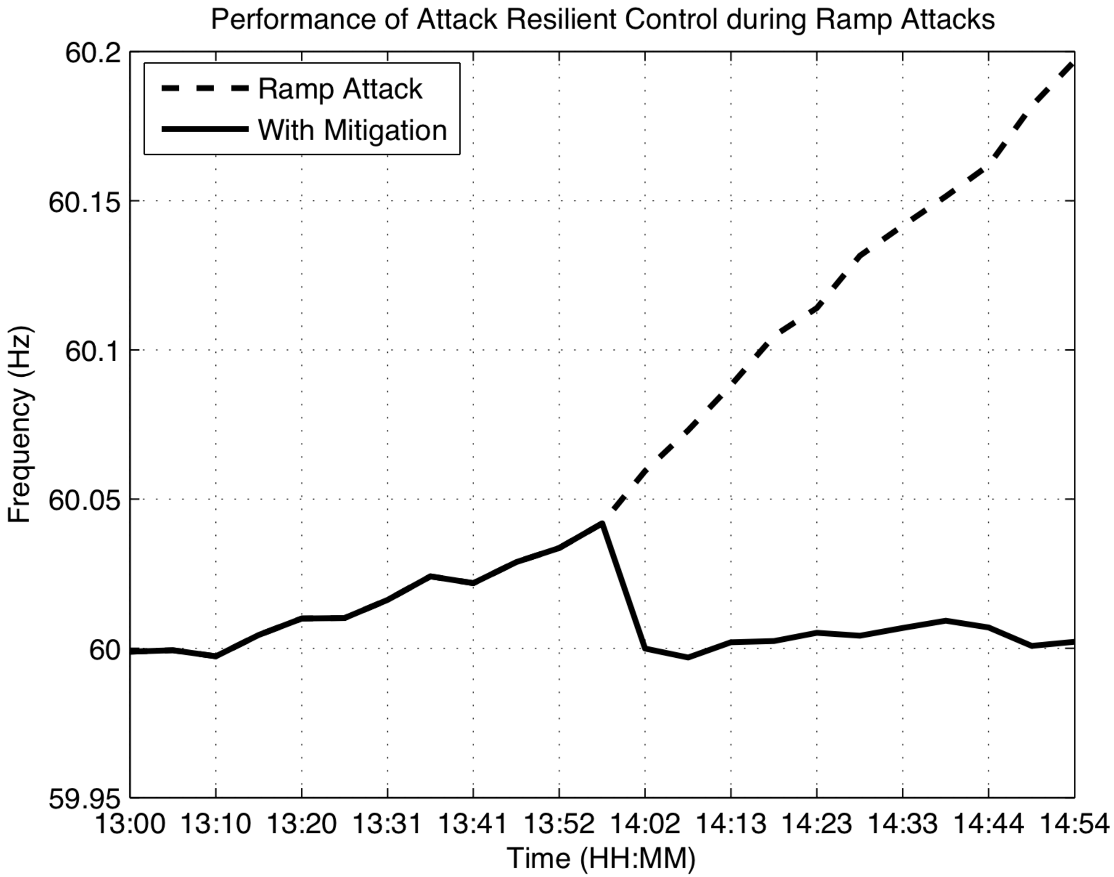
Attack Resilient Control for AGC

Result 1 – ARC during Scaling Attacks



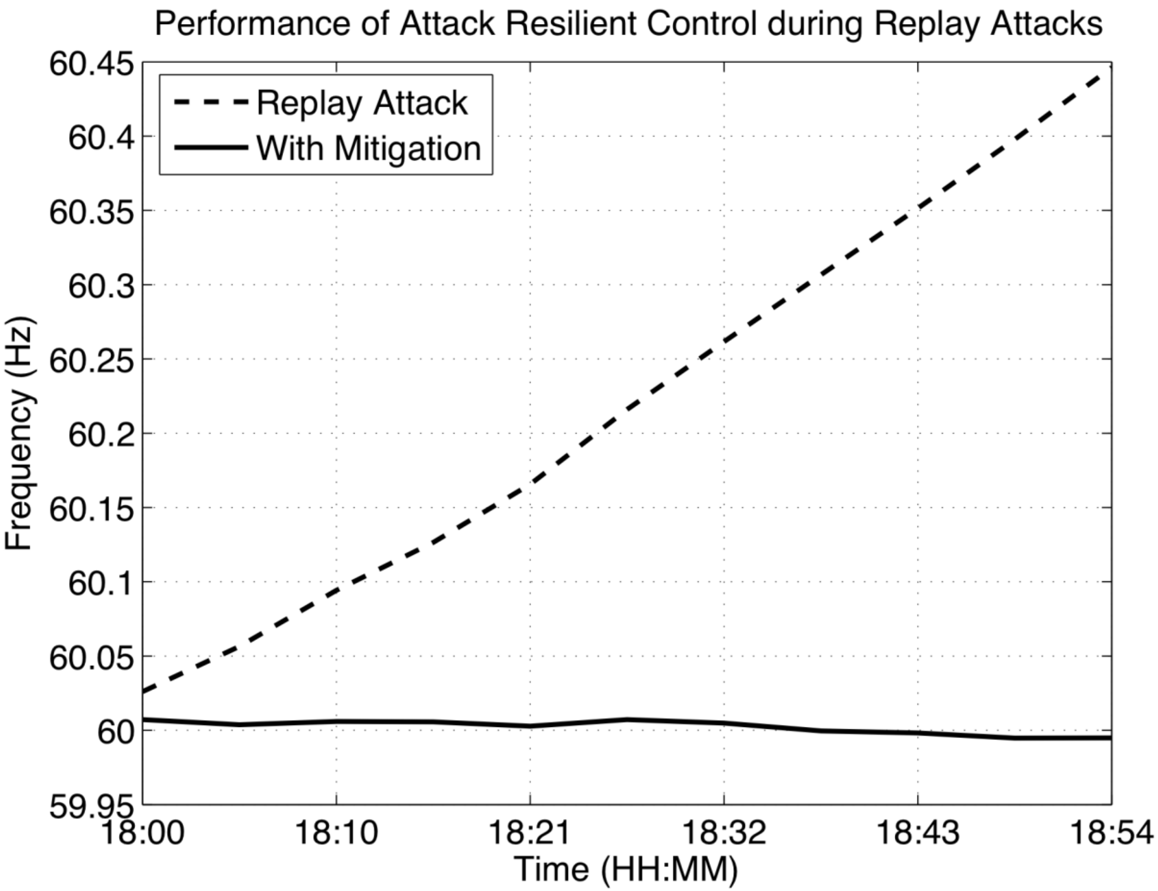
Attack Resilient Control for AGC

Result 2 – ARC during Ramp Attacks



Attack Resilient Control for AGC

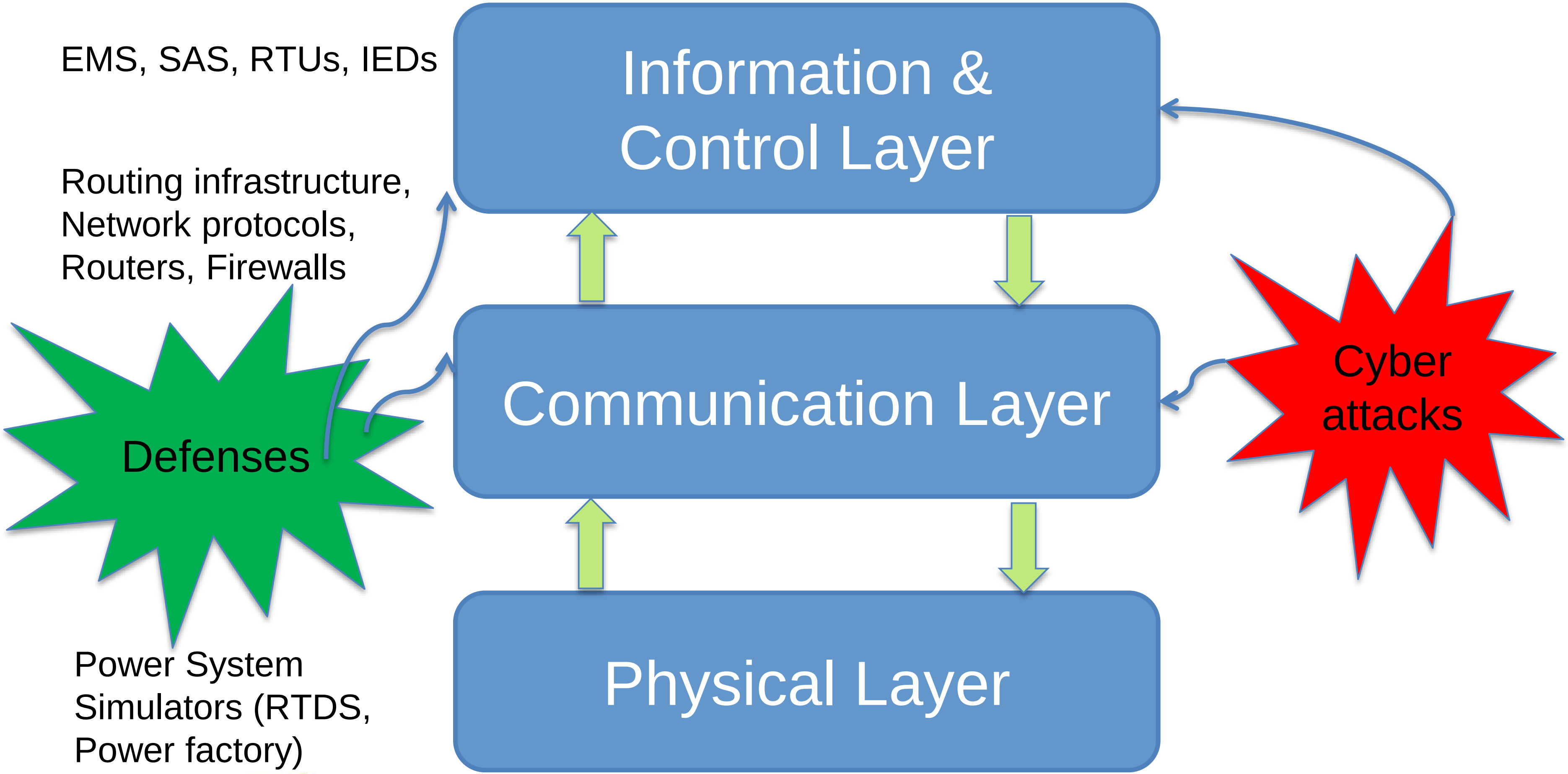
Result 3 – ARC during Replay Attacks



Outline of the Talk

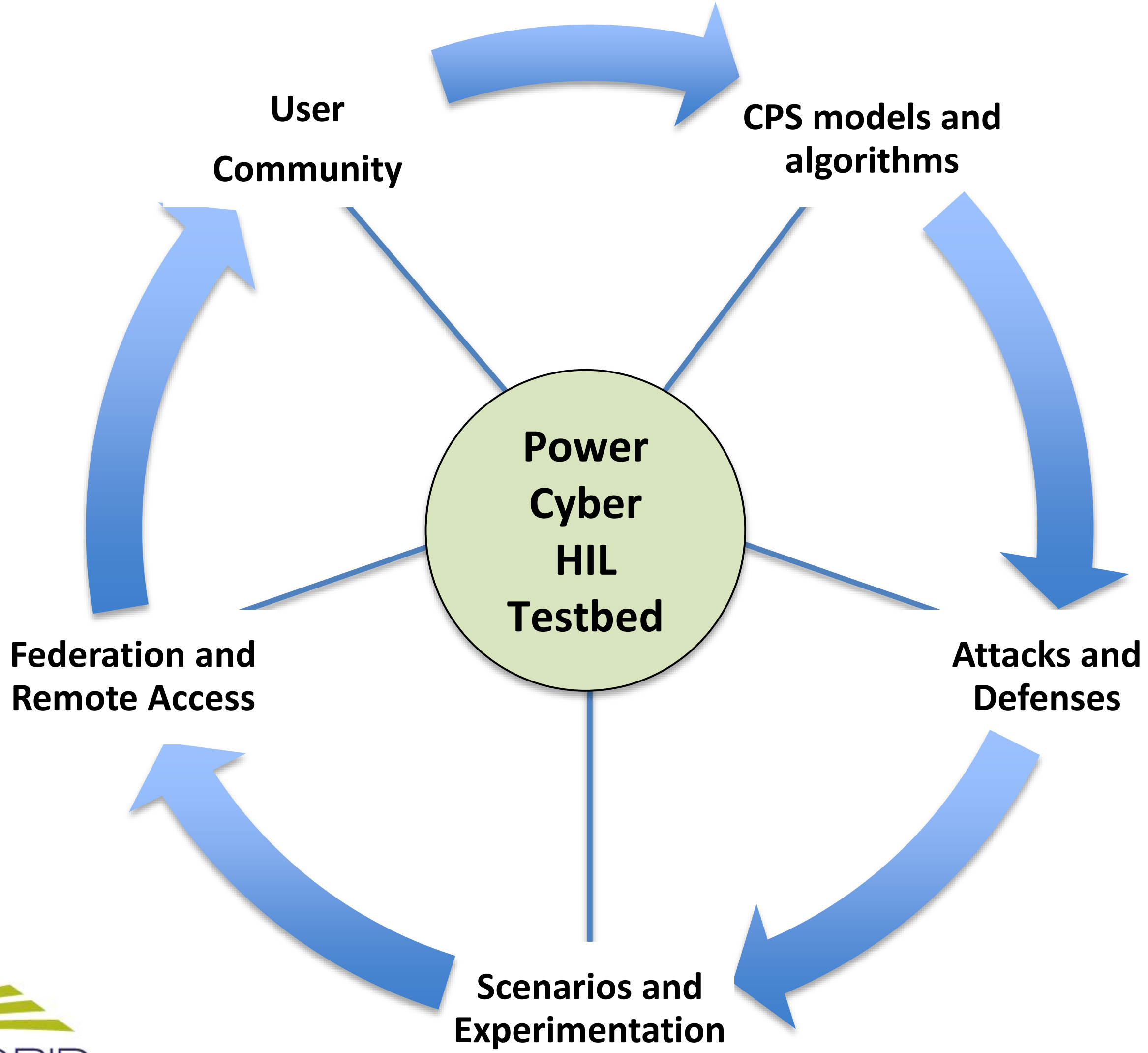
- Cyber Threat and Attacks
- Life-cycle security & Defense-in-Depth
- CPS security & Case studies
- CPS security testbed
- Conclusions

CPS Security Testbed - Abstraction



EMS, SAS, RTUs, IEDs
Information & Control Layer
Routing infrastructure, Network protocols, Routers, Firewalls
Communication Layer
Defenses
Cyber attacks
Power System Simulators (RTDS, Power factory)
Physical Layer

CPS Security Testbed R&D goals



Power Cyber HIL Testbed

User Community

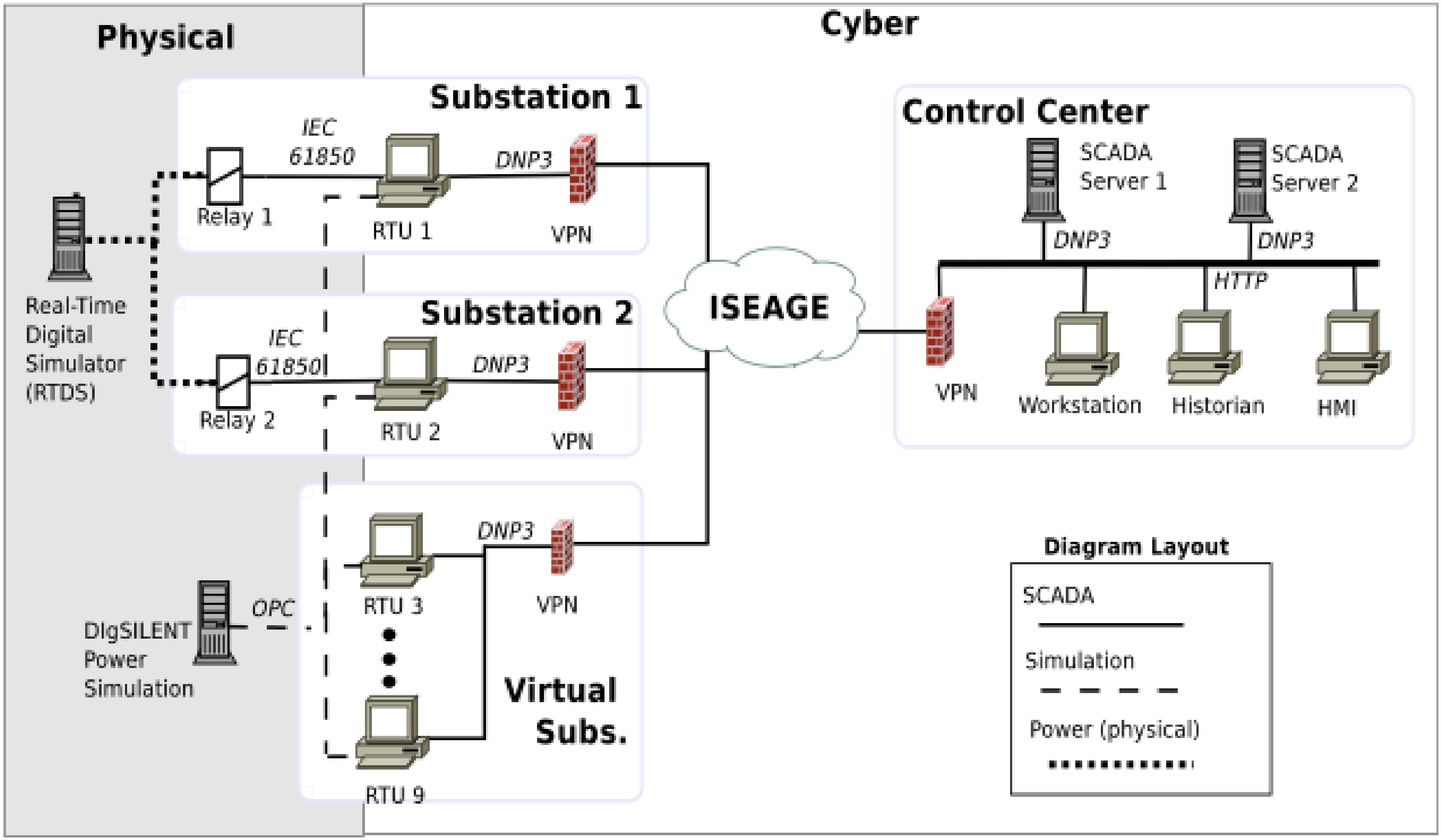
CPS models and algorithms

Attacks and Defenses

Scenarios and Experimentation

Federation and Remote Access

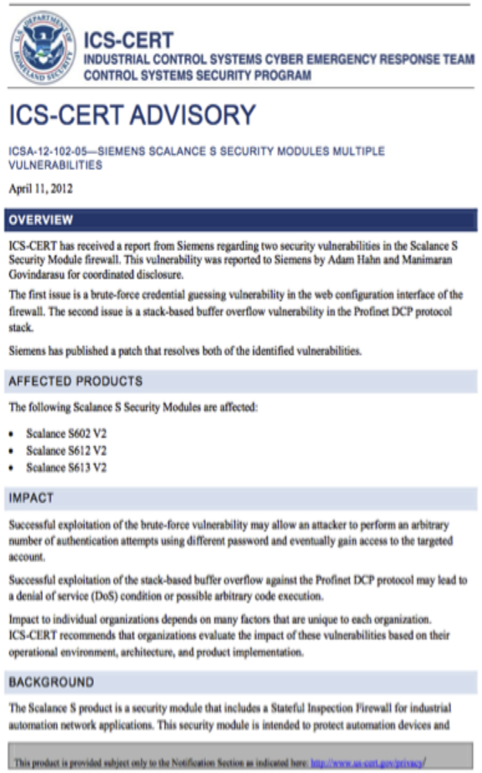
Iowa State’s PowerCyber Testbed



Adam Hahn, Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, *Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,* IEEE Transactions on Smart Grid, Vol. 4 , June 2013.

Testbed Use-Cases

Vulnerability Assessment



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-102-05—SIEMENS SCALANCE S SECURITY MODULES MULTIPLE VULNERABILITIES

April 11, 2012

OVERVIEW

ICS-CERT has received a report from Siemens regarding two security vulnerabilities in the Scalance S Security Module firewall. This vulnerability was reported to Siemens by Adam Hahn and Manimaran Govindarasu for coordinated disclosure.

The first issue is a brute-force credential guessing vulnerability in the web configuration interface of the firewall. The second issue is a stack-based buffer overflow vulnerability in the Profinet DCP protocol stack.

Siemens has published a patch that resolves both of the identified vulnerabilities.

AFFECTED PRODUCTS

The following Scalance S Security Modules are affected:

- Scalance S602 V2
- Scalance S612 V2
- Scalance S613 V2

IMPACT

Successful exploitation of the brute-force vulnerability may allow an attacker to perform an arbitrary number of authentication attempts using different password and eventually gain access to the targeted account.

Successful exploitation of the stack-based buffer overflow against the Profinet DCP protocol may lead to a denial of service (DoS) condition or possible arbitrary code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

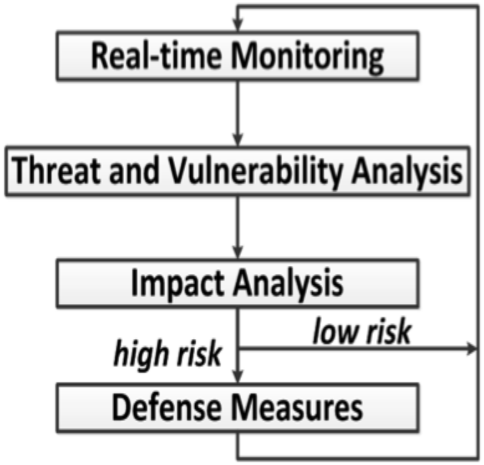
BACKGROUND

The Scalance S product is a security module that includes a Stateful Inspection Firewall for industrial automation network applications. This security module is intended to protect automation devices and

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

Risk Assessment and Mitigation

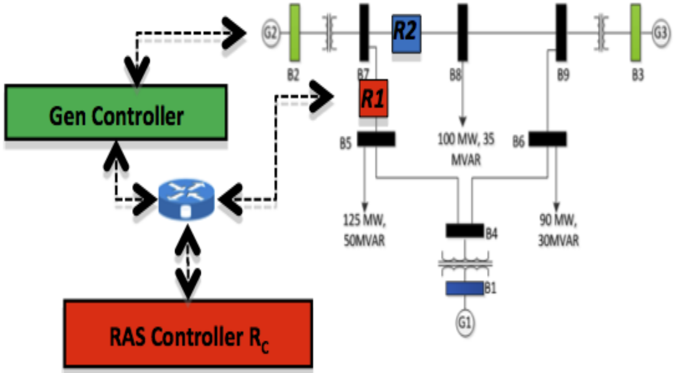
- Risk = Threat * Vulnerability * Impacts
- Security Investment Analysis
- Risk Assessment & Risk Mitigation



Attack-Defense Evaluations

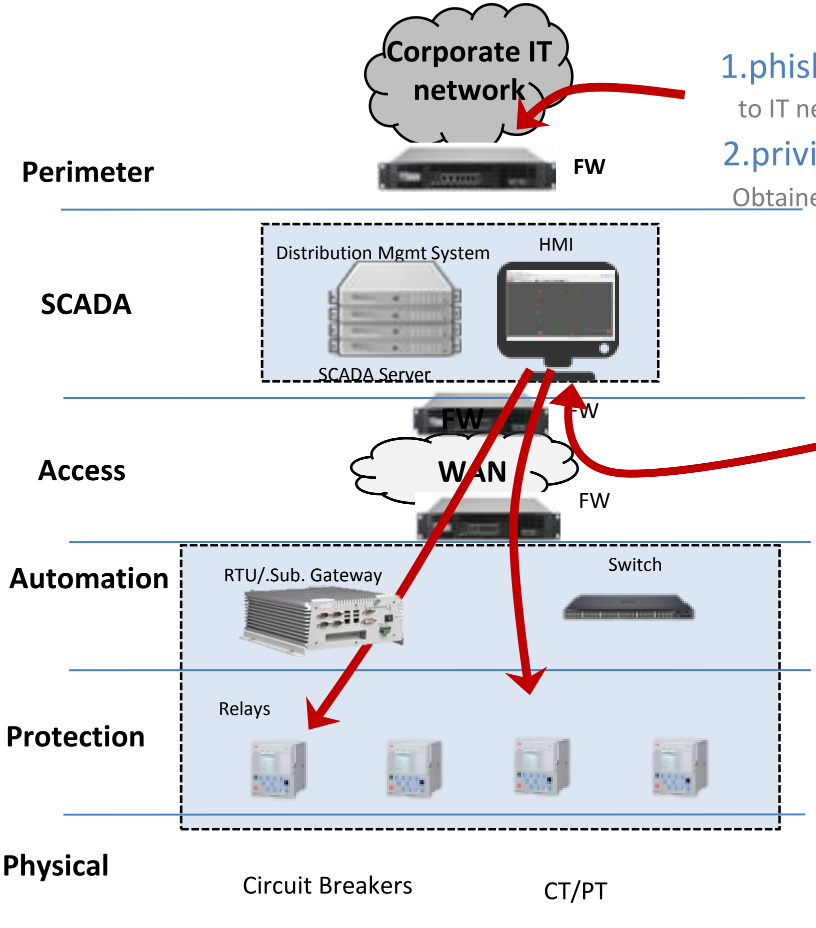
Attack on Remedial Action Scheme

WECC 9-bus System



- Data integrity attack to trip R1 + DoS on RAS controller
- R2 trips due to thermal overload; Instability; Load shedding
- Evaluating mitigation schemes

Ukraine grid's attack Dec. 2015 (revisited)



IT

1.phishing email

to IT network

2.privilege escalation

Obtained admin on DC

OT Pre-Impact

3.ot vpn login

Stolen credential from DC used to remotely login to vpn

4.install malware

BlackEnergy malware installed on control systems

5.remote hmi session

Created remote operators session to SCADA server

6.trip breakers

Operate key circuit breakers, 225,000 customers offline

OT Post-Impact

7.disable systems

Wipe SCADA servers, brick serial-ethernet converts and control center ups

8.telephone ddos

Telephone DDoS prevents communication about grid state

225K customers without power

Ack: Adam Hahn, Washington State University

Countermeasures for Ukraine 2015 attack

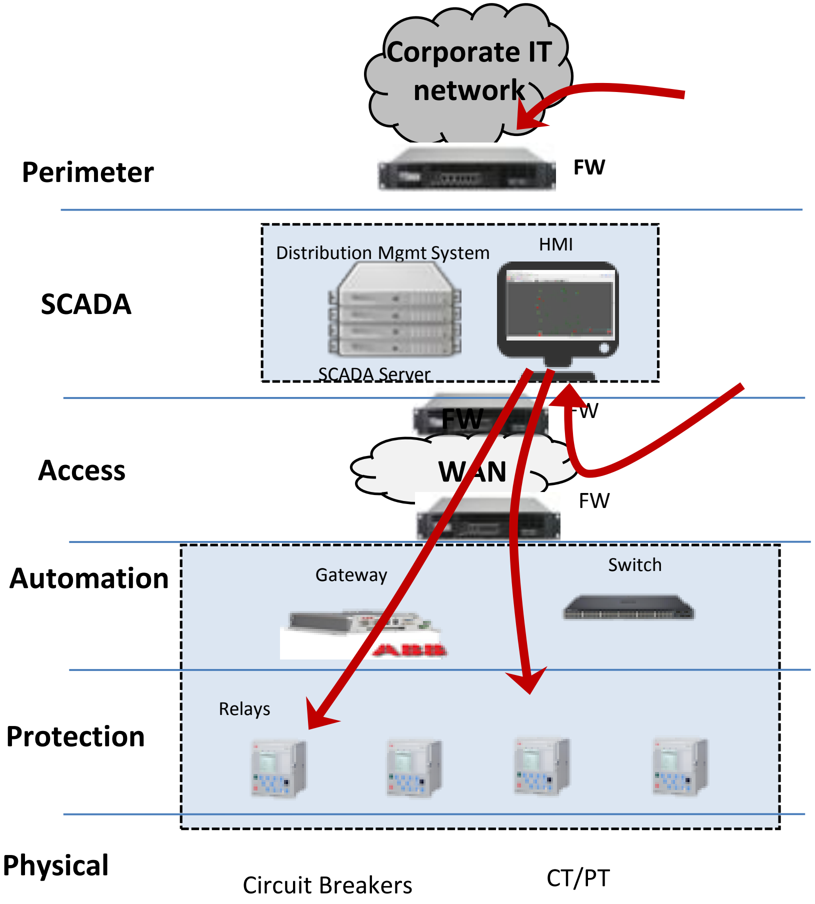
Security awareness & training

Network Monitoring – SIEM, IDS
Application Firewalls

VPN : 2-factor authentication,
time of use access

Disable remote access and
management of field devices

Prevention & Detection (NERC CIP)



NERC CIP Controls

OT Pre-Impact

CIP-005-5 R1.3
Multi-factor authentication for interactive sessions

3.ot vpn login
Stolen credential from DC used to remotely login to vpn

CIP-007-5 R3.1
Deploy methods to deter, detect, and prevent malicious code

4.install malware
BlackEnergy malware installed on control systems

5.remote hmi session
Created remote operators session to SCADA server

CIP-005-5 R1.3
Mechanisms to detect malicious communications

6.trip breakers
Operate key circuit breakers, 225,000 customers offline

Ack: Adam Hahn, Washington State University

Conclusions

- FROM Fault-Resiliency TO Attack-Resiliency
- Smart Grid Sec: Info Sec, Infra Sec, App Sec, Physical Sec
- Defense-in-Depth & End-to-End Security
- Cybersecurity Life-cycle model & CPS Security solutions
- Cybersecurity of DERs, Microgrids & Supply Chain
- CPS Security Testbeds & Experimentations
- Industry Collaboration & Tech Transfer
- Education and workforce development & Industry Training
- Synergistic collaboration: Industry-University-National Labs

THANK YOU …

- Acknowledgements:
  - U.S. National Science Foundation (NSF)
  - U.S. Department of Homeland Security (DHS)
  - U.S. Department of Energy (DOE)
  - U.S. NSF IU/CRC Power Engr. Research Center (PSERC)
  - Iowa State Univ., Electric Power Research Center (EPRC)

  Collaborators:
  - Dr. Chen-Ching Liu, Virginia Tech
  - Dr. Adam Hahn, WSU
  - Dr. C. W. Ten, Michigan Tech.
  - Dr. Aditya Ashok (PNNL)
  - Dr. Siddharth Sridhar (PNNL)
  - Dr, Venkat Ajjarapu & Dr. Doug Jacobson, Iowa State
  - Pengyuan (Bruce) Wang & Grad Students, Iowa State

- **Professional**:
  - IEEE PES AMPS CAMS Cyber Security Task Force (now Working Group)