Cyber Physical Security for Smart Grid

Broad Analysis: Information Hierarchy for the Future Grid

Manimaran Govindarasu & Adam Hahn
Iowa State University
gmani@iastate.edu adamhahn@iastate.edu

Pete Sauer
University of Illinois at Urbana-Champaign
psauer@illinois.edu

Talk Outline

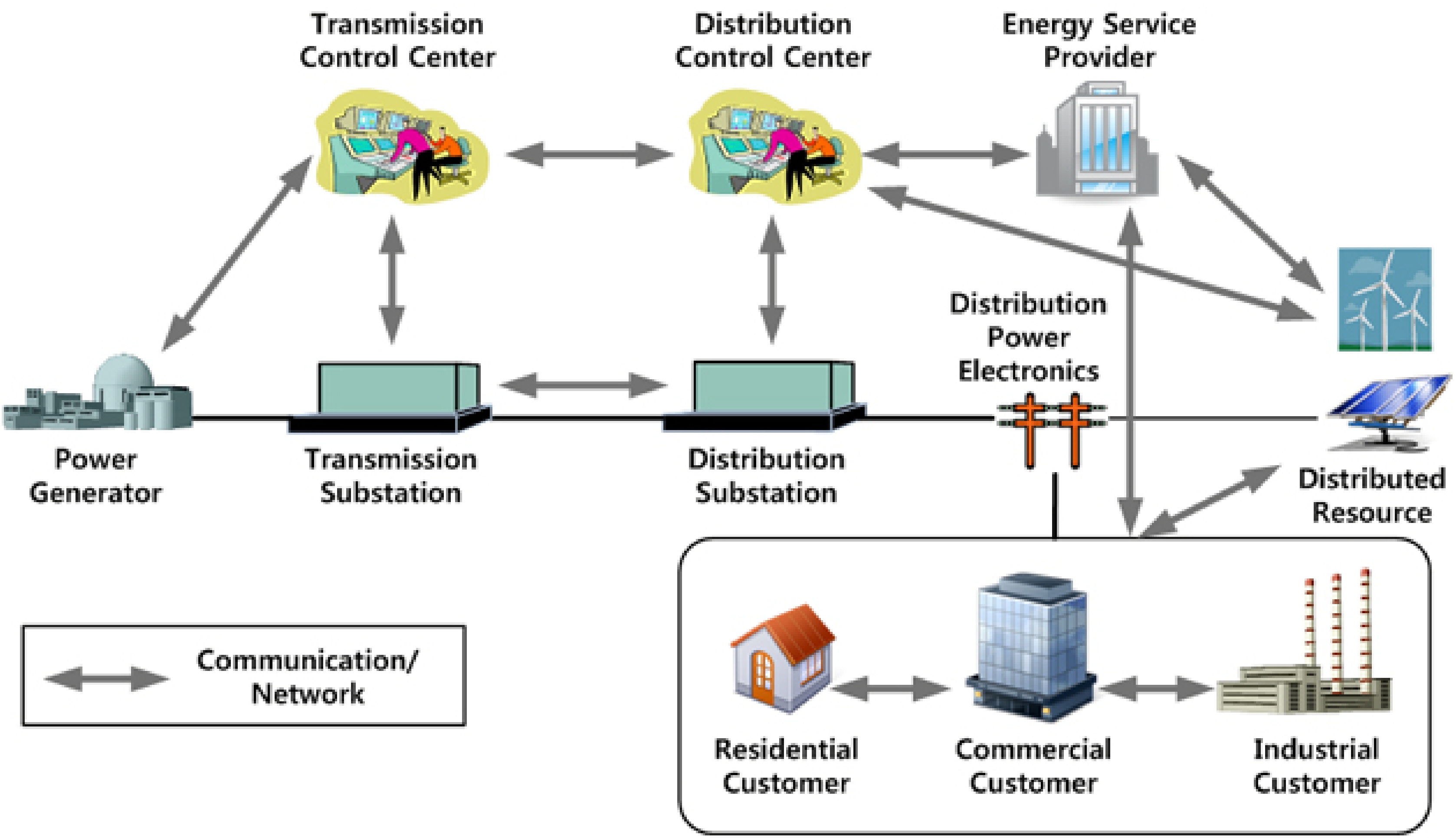
- Cyber Physical Power Grid
- Cyber Threats & Impacts
- Research Challenges
  1. Cyber-Physical System Security
  2. Risk modeling and mitigation
  3. Security of WAM, WAP, WAC
  4. DMS & AMI Security
  5. Defense against coordinated attacks
  6. Trust management & attack attribution
  7. Data sets, models, validation studies

Covered in detail (items 1–3)

Covered briefly (items 4–7)

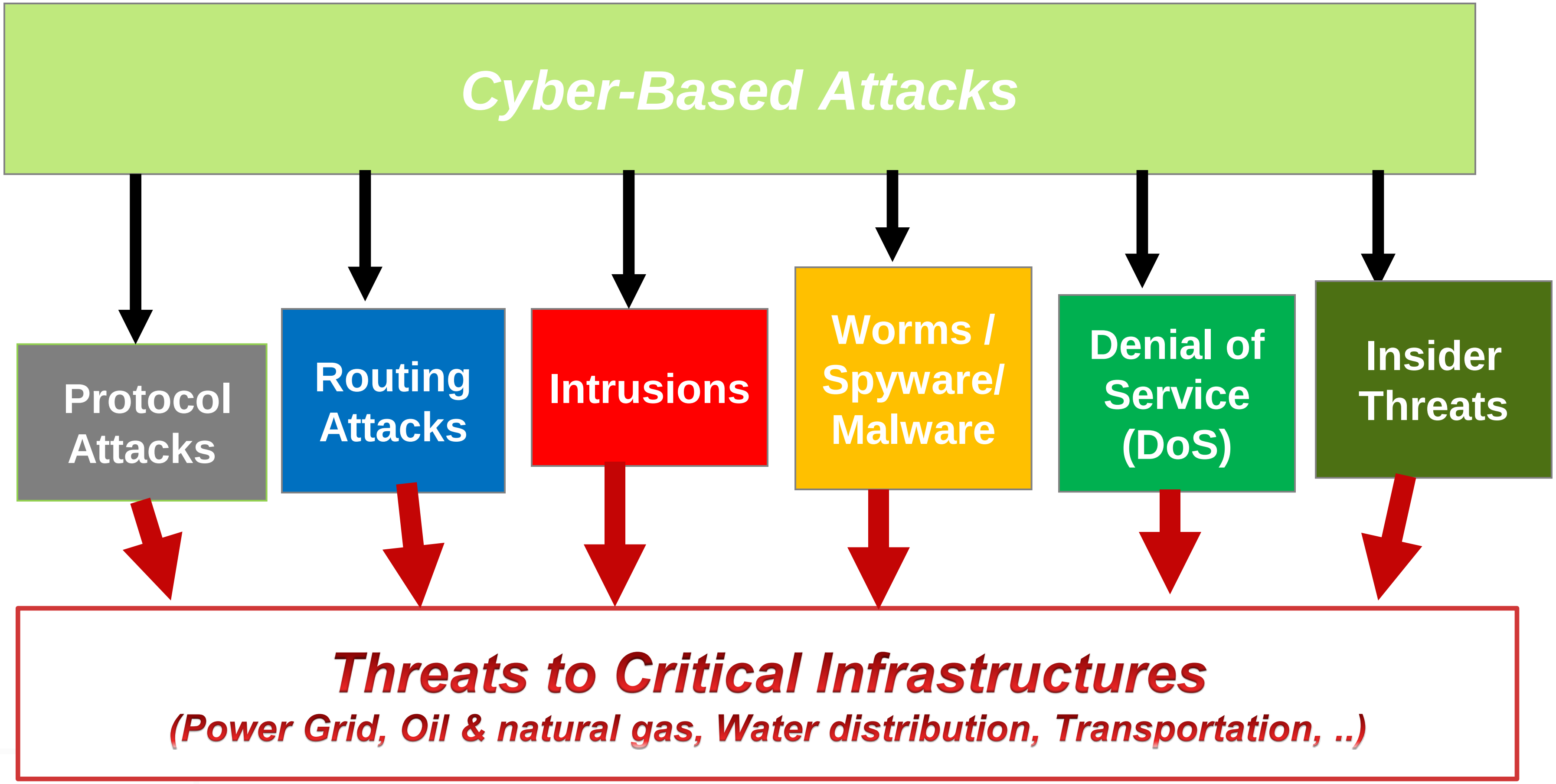
- Conclusions

Smart Grid: A Cyber-Physical System



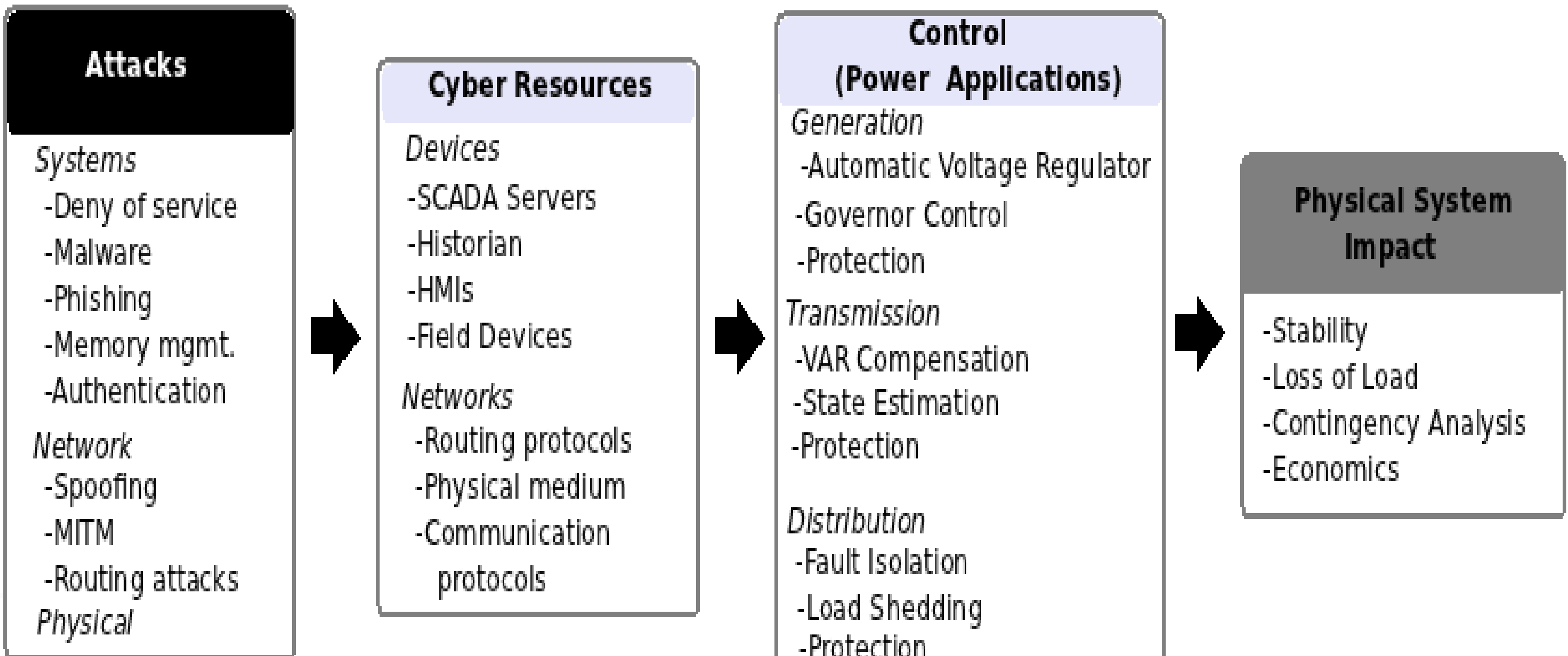
Source: http://cnslab.snu.ac.kr/twiki/bin/view/Main/Research

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.

Attacks-Cyber-Control-Physical



Security systems is difficult …

- **Open and interoperable protocols**
- **Security vs. performance tradeoff**
- **Security vs. usability tradeoff**
- **Security is expensive**
- **Attackers enjoy breaking into system**
- **Security had been not a design criteria**
- Securing legacy systems even harder

Power Grid Cyber Security Roadblocks

- Legacy systems
- Geographically disperse
- Insecure remote connections
- Long system deployments
- Limited physical protections

- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- No “fail-closed” security mechanisms
- Widespread availability of technical info

Documented Concerns

Policies/Reports	
DoE Roadmap to Achieve Energy Delivery System Cybersecurity, 2011	**NERC-DoE HILF:** High-Impact, Low-Frequency (HILF) Event Risk to the North American Bulk Power System
NISTIR 7628, “Guidelines for Smart Grid Cyber Security”	**NERC CIP** (Critical Infrastructure Protection)
NIST 800-82, “Guide to Industrial Control Systems (ICS) Security”	**DHS** Common Cyber Security Vulnerabilities in Industrial Control Systems
GAO-11-117: Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed	**MIT Report**: The Future of the Electric Grid, 2011

Smart Grid Vision

Smart Grid vision

- Economic Benefits
- Reliability Benefits
- Environmental Benefits

Enabling Technologies

- Advanced sensing, communication, control
- Built-in Security
- Renewable Energy
- Emerging apps: WAMS, WAMPAC, DMS, SAS, AMI

Smart Grid Security = Info + Infra + Appln. Security

	Information Security	Infrastructure Security	Applications Security
NEEDS	❑ Information Protection ▪ Confidentiality ▪ Integrity ▪ Availability ▪ Authentication ▪ Non-repudiation	❑ Infrastructure protection ▪ Routers ▪ DNS servers ▪ Links ▪ Internet protocols ❑ Service availability	❑ Generation Control apps. ❑ Transmission Control apps. ❑ Distribution Control apps. ❑ System Monitoring functions ❑ Protection functions ❑ Real-Time Energy Markets
MEANS	❑ Encryption/Decryption ❑ Digital signature ❑ Message Auth.Codes ❑ Public Key Infrastructure	❑ Firewalls ❑ IDS/IPS ❑ Authentication Protocols ❑ Secure Protocols ❑ Secure Servers ❑ IPSEC, DNSSEC	❑ Attack-Resilient Control Algos ❑ Model-based Algorithms - Anomaly detection - Intrusion Tolerance ❑ Risk modeling and mitigation ❑ Attack-Resilient Monitoring & Protection

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

Smart Grid Cyber Security requirements

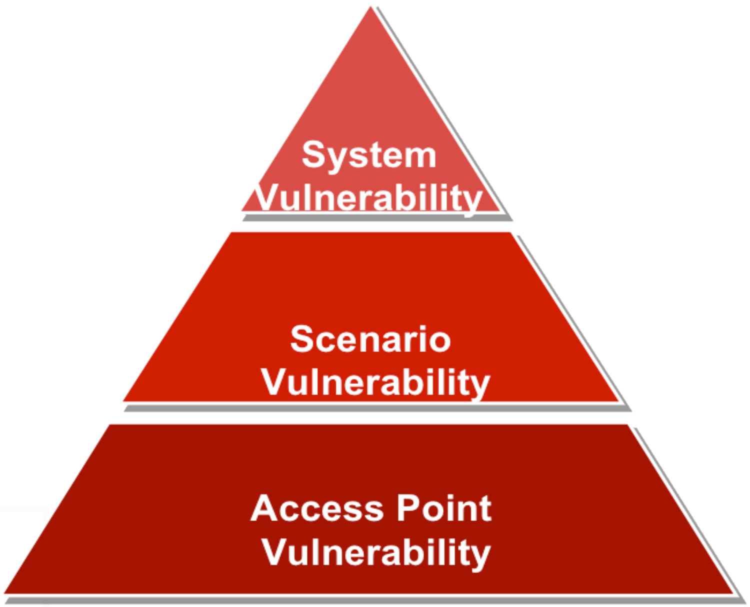
- Confidentiality (C), Integrity (I), Availability (A),
- Authentication (AT), Non-repudiation (N)

Smart Grid Application	Information & Infrastructure Security	Application Security
AMI	I, AT, C	I, N
DMS	I, A, AT	I, AT
EMS	I, A, AT	I, AT
WAMPAC	I, A, AT, C	I, A
Power Markets	I, A, AT, C	I, N

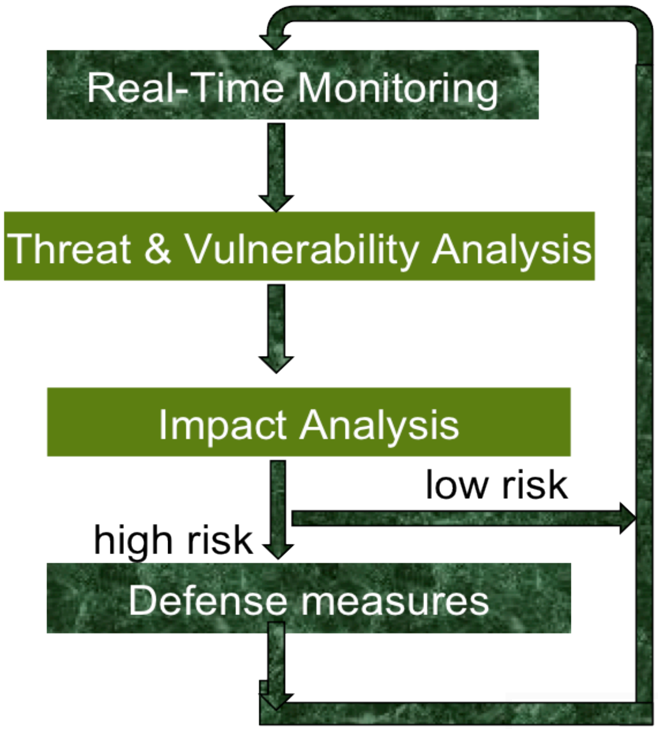
Risk modeling & Mitigation

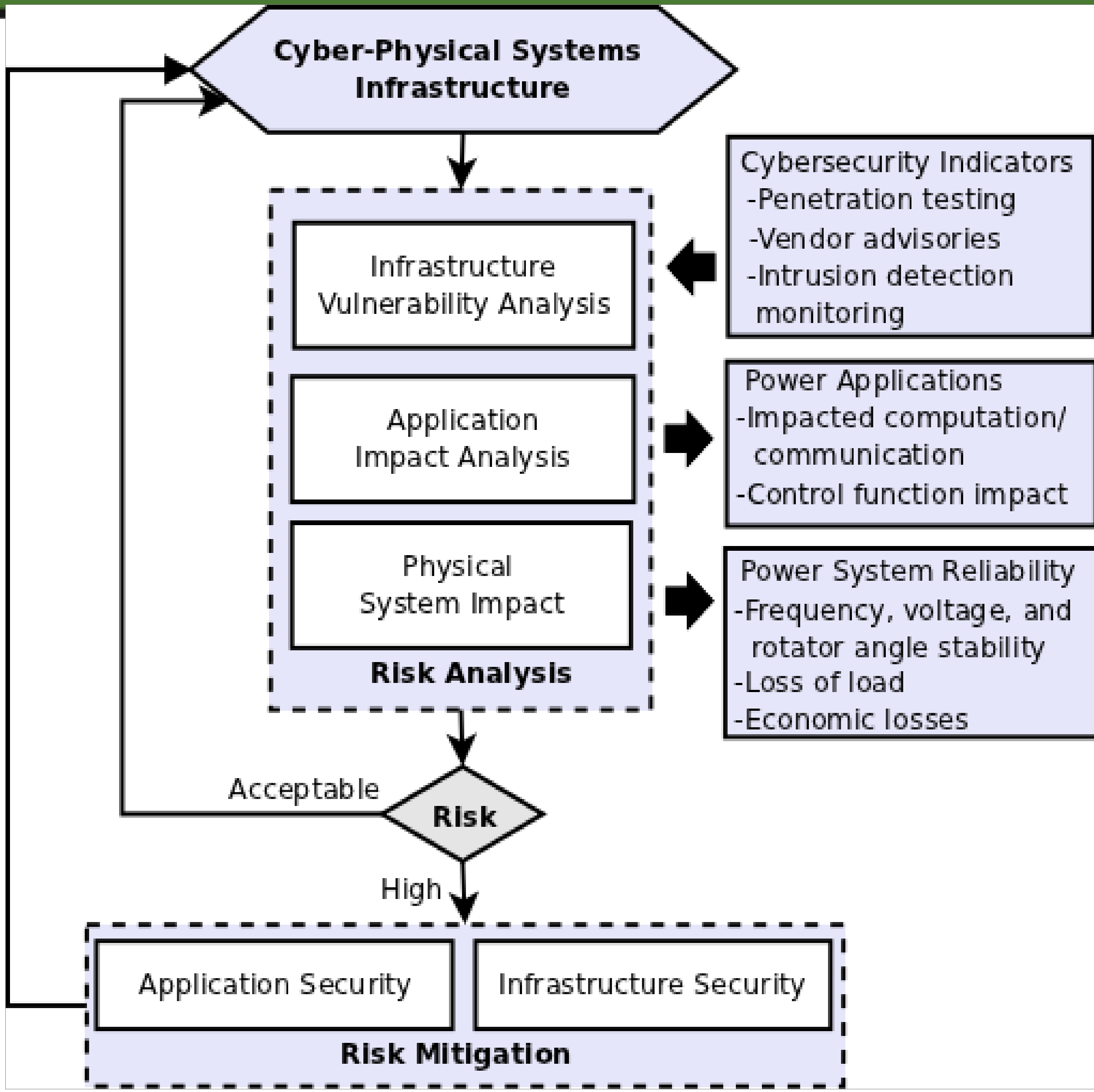
Risk = Threat x Vulnerability x Impacts

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



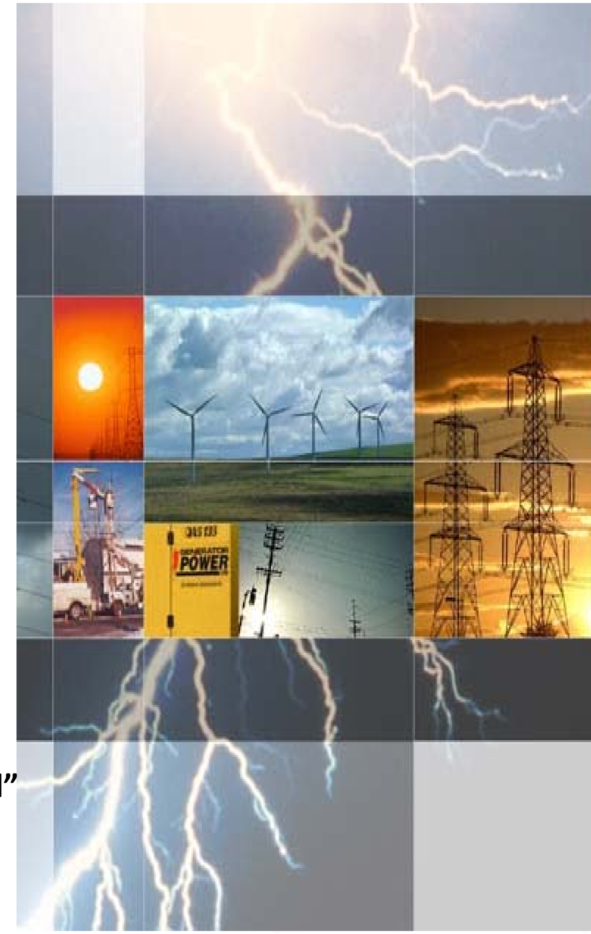
Hierarchical modeling





Cyber-Physical Systems Infrastructure
Infrastructure Vulnerability Analysis
Application Impact Analysis
Physical System Impact
Risk Analysis
Cybersecurity Indicators
-Penetration testing
-Vendor advisories
-Intrusion detection monitoring
Power Applications
-Impacted computation/ communication
-Control function impact
Power System Reliability
-Frequency, voltage, and rotator angle stability
-Loss of load
-Economic losses
Acceptable
Risk
High
Application Security
Infrastructure Security
Risk Mitigation

Cyber Security of
Wide-Area Monitoring, Protection and Control



Attack-Resilient Monitoring, Protection Control Algorithms

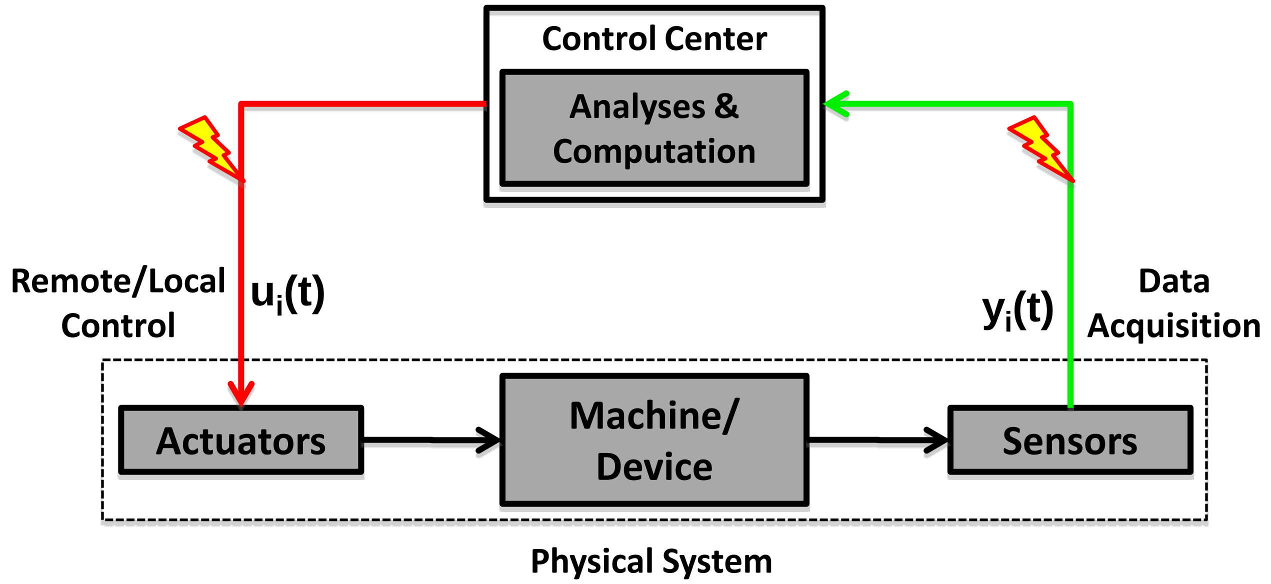
- Man-in-the-middle attacks
- Data integrity attacks
- Denial of service attacks
- Replay attacks
- Timing attacks …

- 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.

Control Systems Attack Model

Generic Control System Model

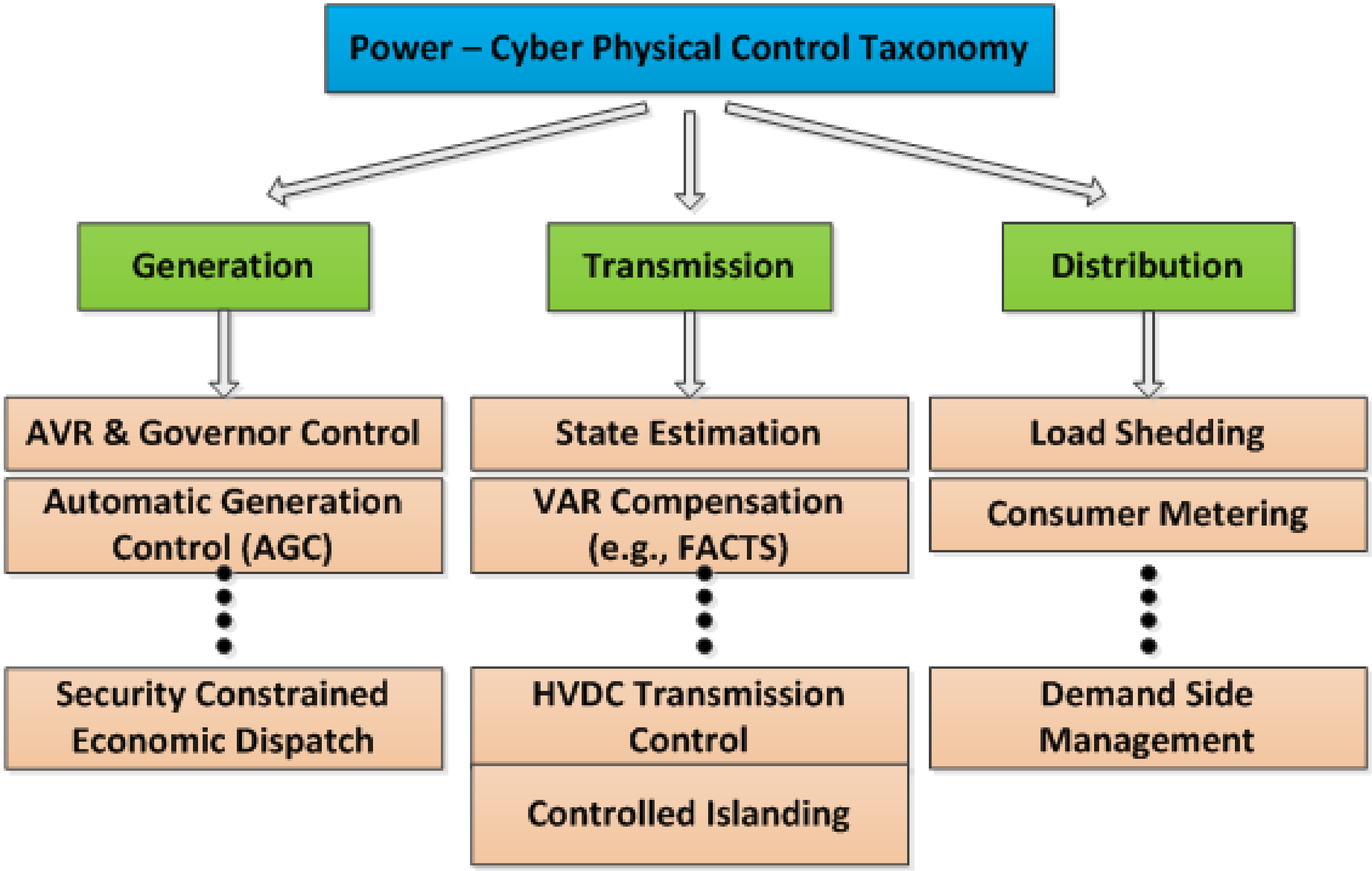


Types of Attacks

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

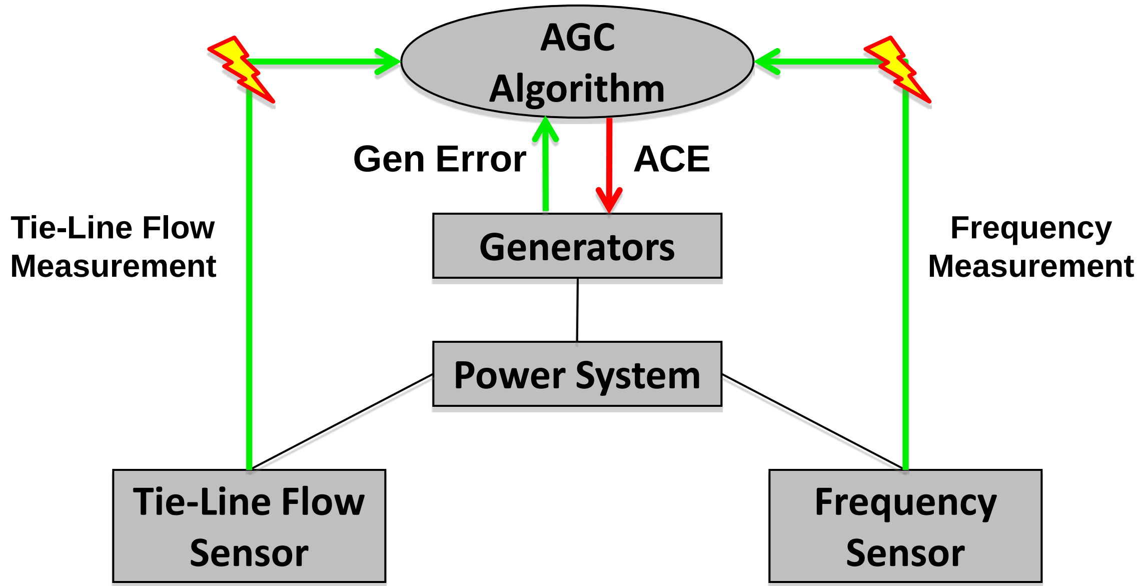
Figure adopted from - Yu-Hu. Huang, Alvaro A. Cardenas, et al, "*Understanding the Physical and Economic Consequences of Attacks on Control Systems*"

Power System Control Loops



Automatic Generation Control

Frequency Control

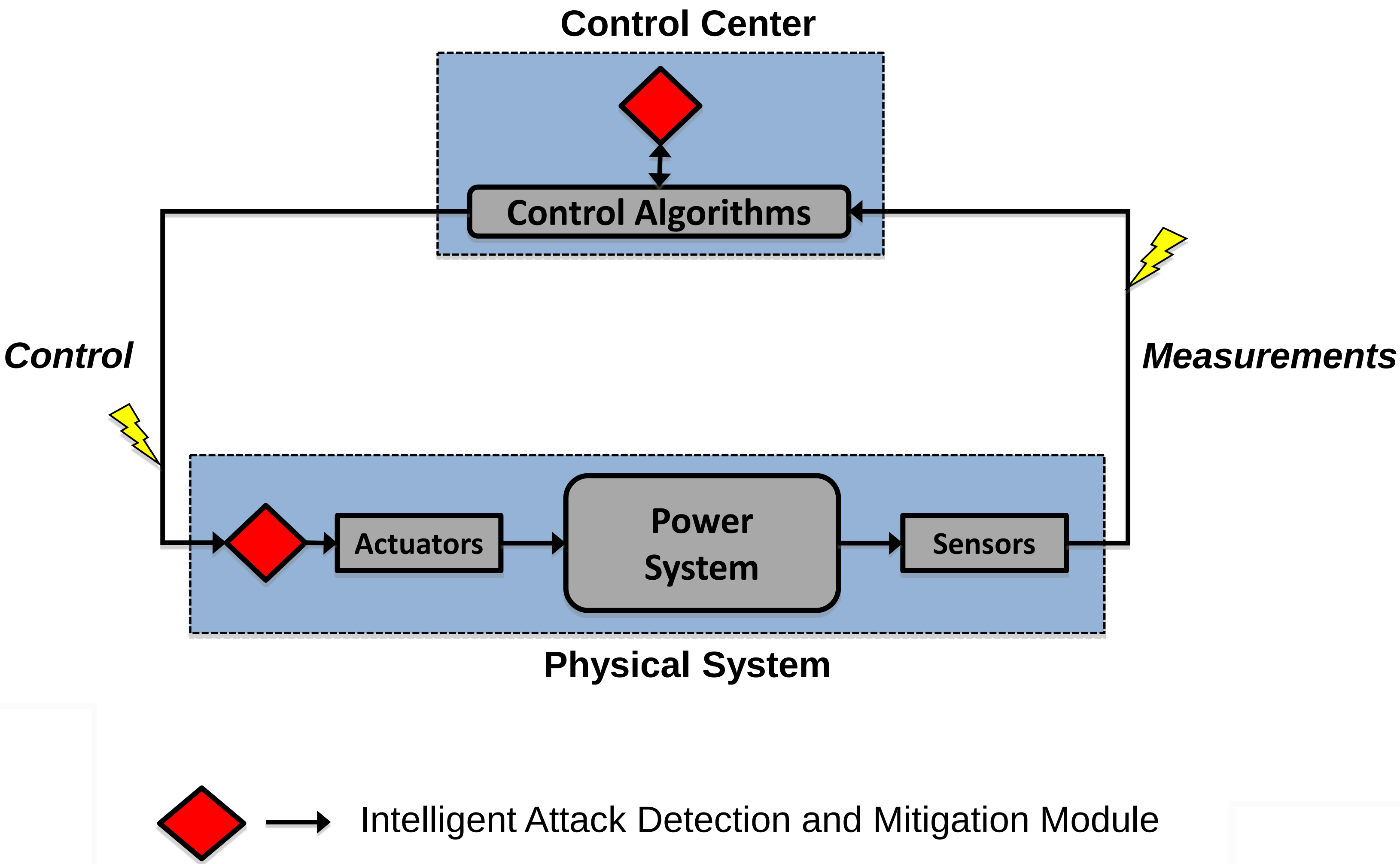


Attack: **Modify tie-line flow and frequency measurements**

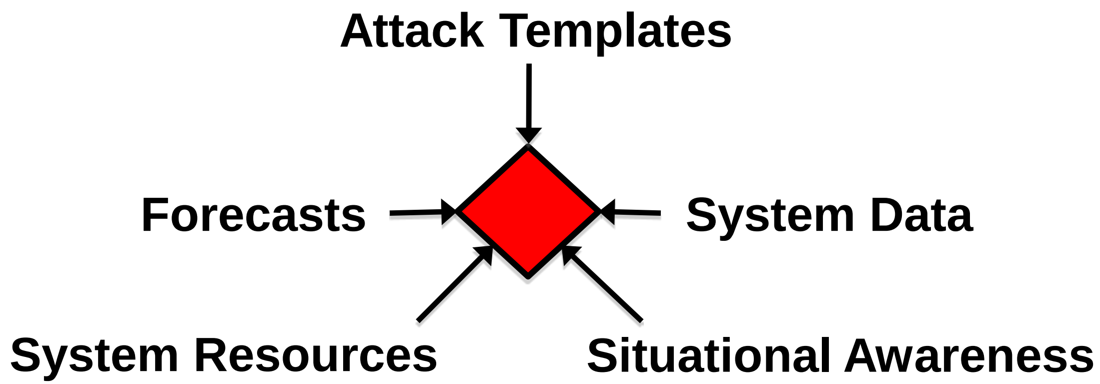
Impact: **Abnormal operating frequency conditions**

Siddharth Sridhar and G. Manimaran – "Data Integrity Attacks and Impacts on SCADA Control System" – PES GM 2011

Attack Resilient Control (ARC)

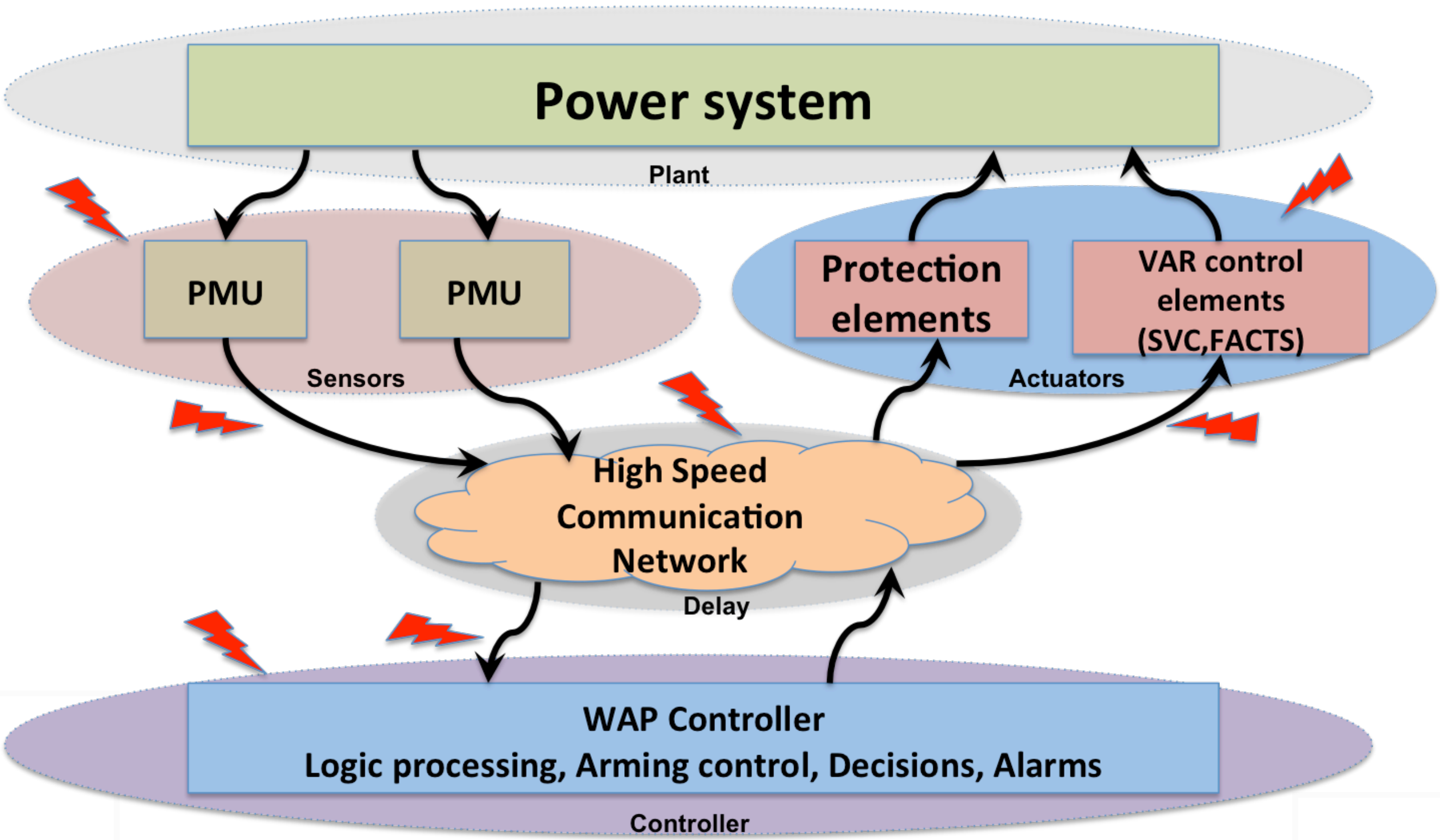


ARC – Intelligence Sources

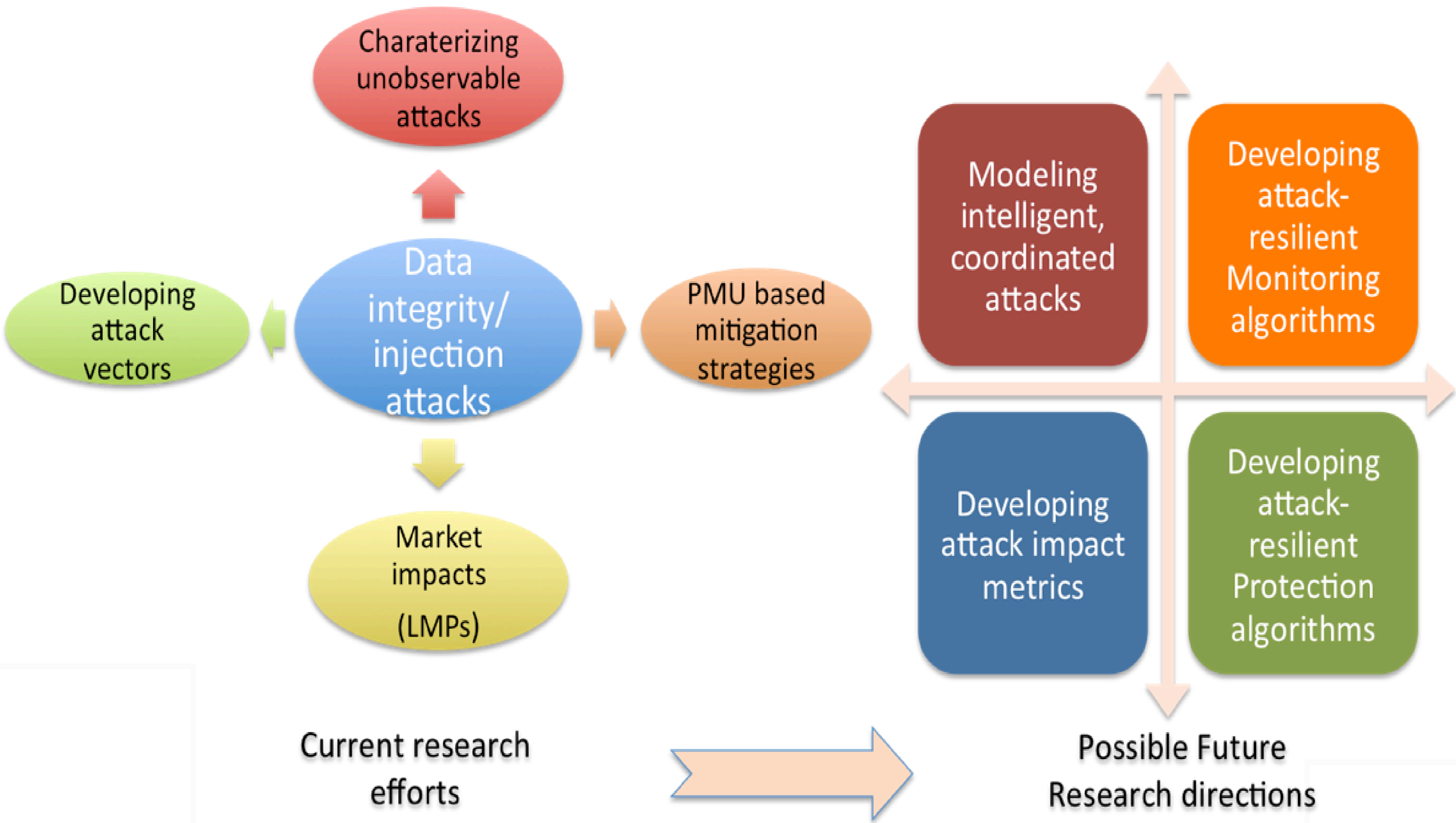


- **Forecasts –** Load and wind forecasts
- **Situational Awareness –** System topology, geographic location, market operation
- **Attack Templates –** Attack vectors, signatures, potential impacts
- **System Data –** Machine data, control systems
- **System Resources –** Generation reserves, VAR reserves,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

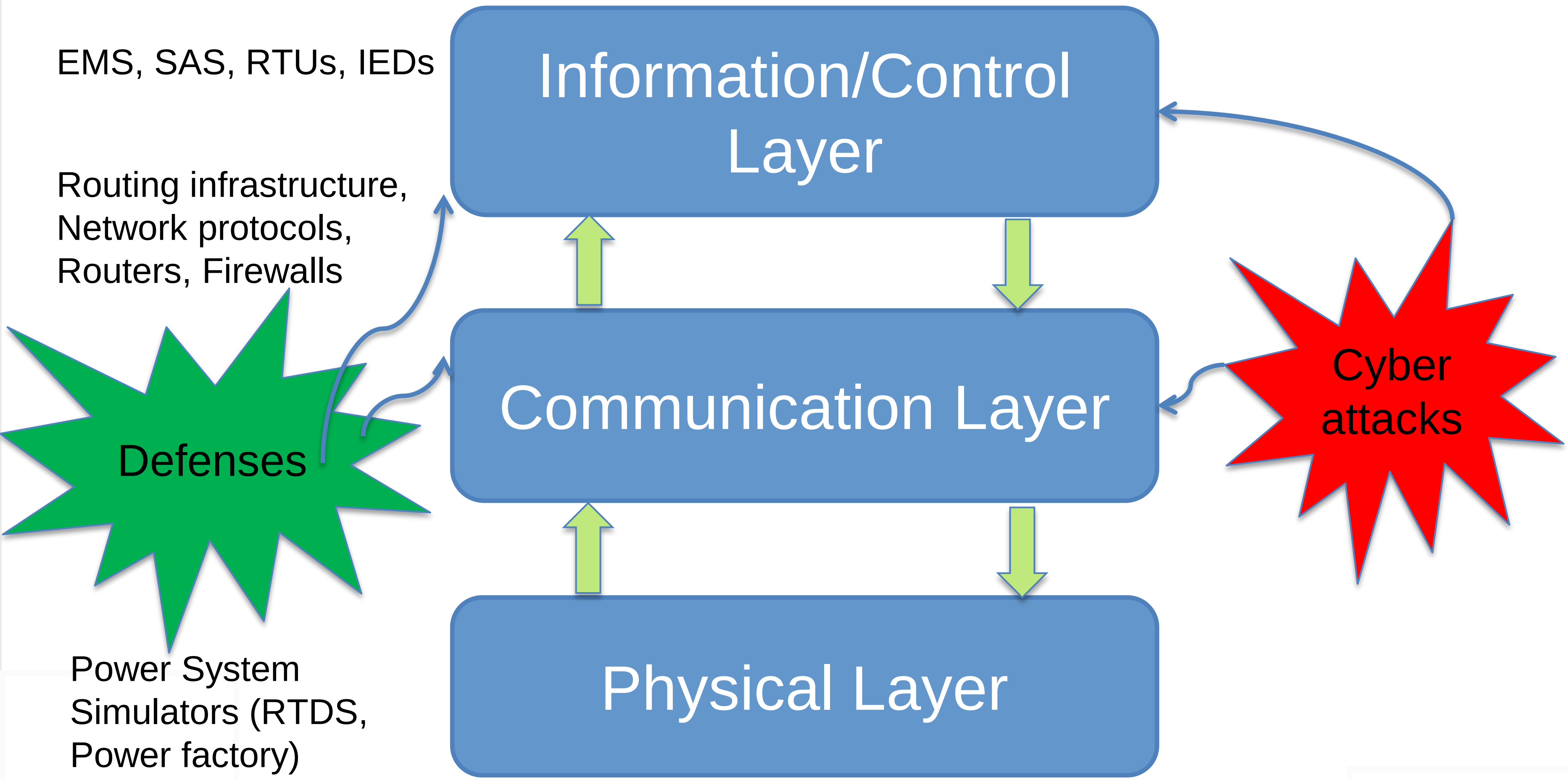
Wide-Area Monitoring & Protection



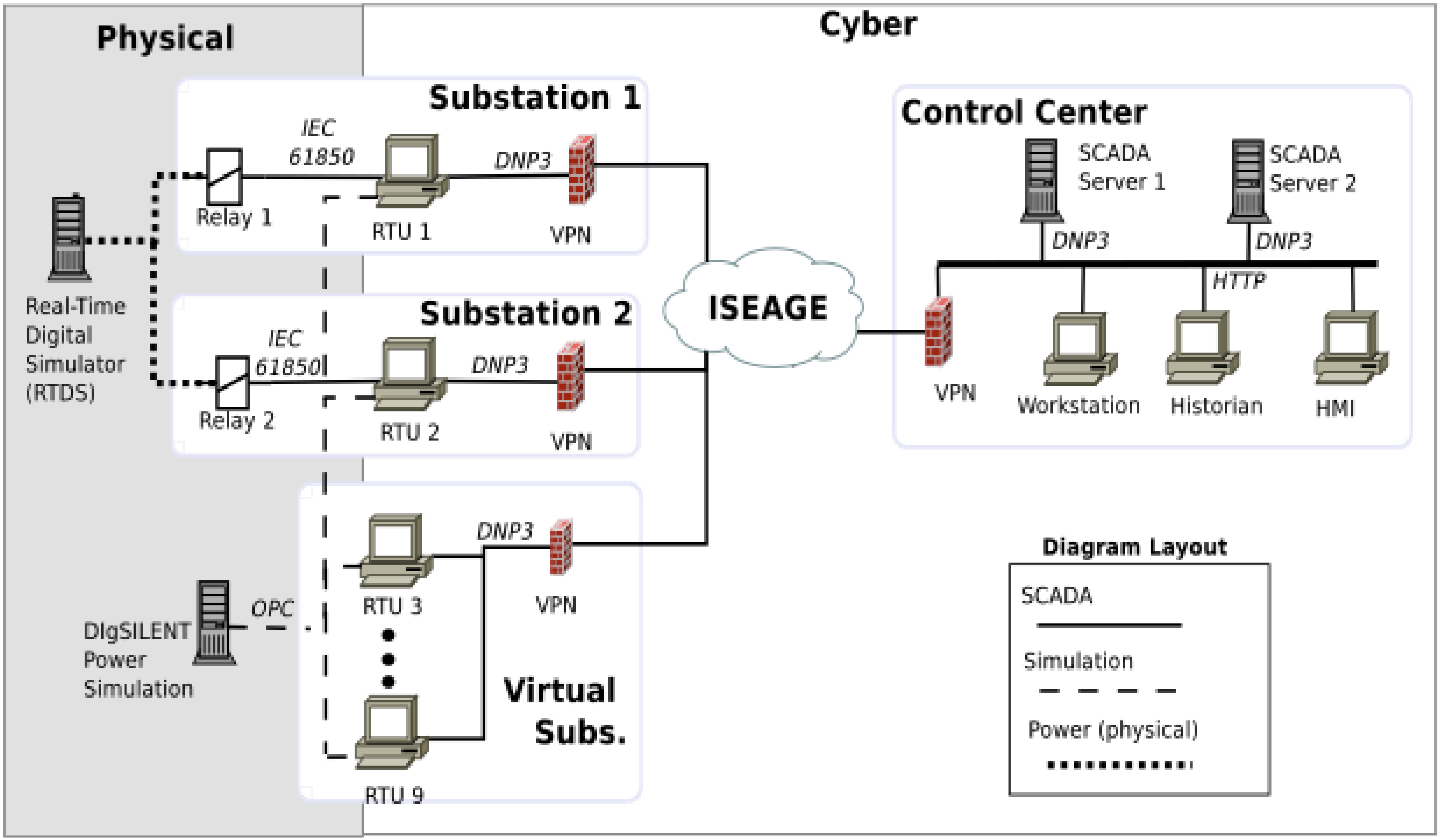
Secure WAMS &Protection (& NASPInet)



CPS Testbed – A Layered View



PowerCyber Testbed @ Iowa State



Research Challenges

1. Cyber Physical Systems Security

- Information Hierarchy
- Communication, Control Architectures
- Cyber-Control- Physical Mapping:

Threats → Attacks → Cyber → Control → Impacts

Research Challenges

2. Risk Modeling and Mitigation

- Vulnerability Assessment
- Impact Analysis
- Novel metrics
  - Load loss, Stability, Reliability, Economic factors
- Hierarchical risk modeling framework
- Synergistic Cyber-Physical mitigation

Research Challenges

3. Attack Resilient WAMPAC Algorithms

- Attack Resilient Wide-Area Measurement
  - Security of PMU networks and data (NASPInet)
- Attack Resilient Wide-Area Control
  - Secure Automatic Generation Control (AGC)
- Attack Resilient Wide-Area Protection
  - Adaptive, Intelligent Remedial Action Scheme
- Secure Energy Management System (EMS)

Research Challenges

4. Defense against Coordinated Attacks

- Risk modeling of coordinated attacks
- Beyond N-1 contingency
  - Scope, planning, system design
- Cyber-physical mitigation

Research Challenges

5. DMS & AMI Security

- Remote attestation of AMI components
- Model-based anomaly detection methods
- Secure Distribution Management Systems (DMS)
- Security vs. Privacy tradeoffs

Research Challenges

6. Trust Management & Attack Attribution

- Dynamic trust
  - Models, protocols, and validation
- Insider threats
  - Models, metrics, mitigation
- Attack attribution
  - Scalable architectures and algorithms

Research Challenges

7. Datasets and Validation

- Data sets and models for:
  - SCADA networks, AMI, WAMPAC, CIM
- Realistic attack models and traces
- Testbed Development
- Realistic Attack-Defense studies

Conclusions

- Cyber security of smart grid is a national security issue
- Smart Grid Security = Info Sec + Infra Sec + Application Security
- Defense against Smart Coordinated Cyber Attacks
- Risk Modeling & Mitigation Algorithms
- Attack-Resilient Monitoring, Protection, and Control algorithms
- Trust management, Attack Attribution, AMI & DMS Security
- Data sets, models, and Validation studies
- Cyber-Physical Systems Security is an important area of R&D
- Standards development and Industry adoption are critical

Thank you !!!

- Reviewers:
  - Scott Backhaus, Las Alamos National Laboratory
  - Jianhui Wang, Argonne National Laboratory

Acknowledgements:

- Department of Energy
- National Science Foundation
- Power Engineering Research Center (PSERC)

•Grad Students: Aditya Ashok, Siddharth Sridhar @ Iowa State University