http://powercyber.ece.iastate.edu

A Cyber-Physical Security Testbed for Smart Grid: System Architecture and Studies

Manimaran Govindarasu (gmani@iastate.edu)

Aditya Ashok, Adam Hahn, Siddharth Sridhar

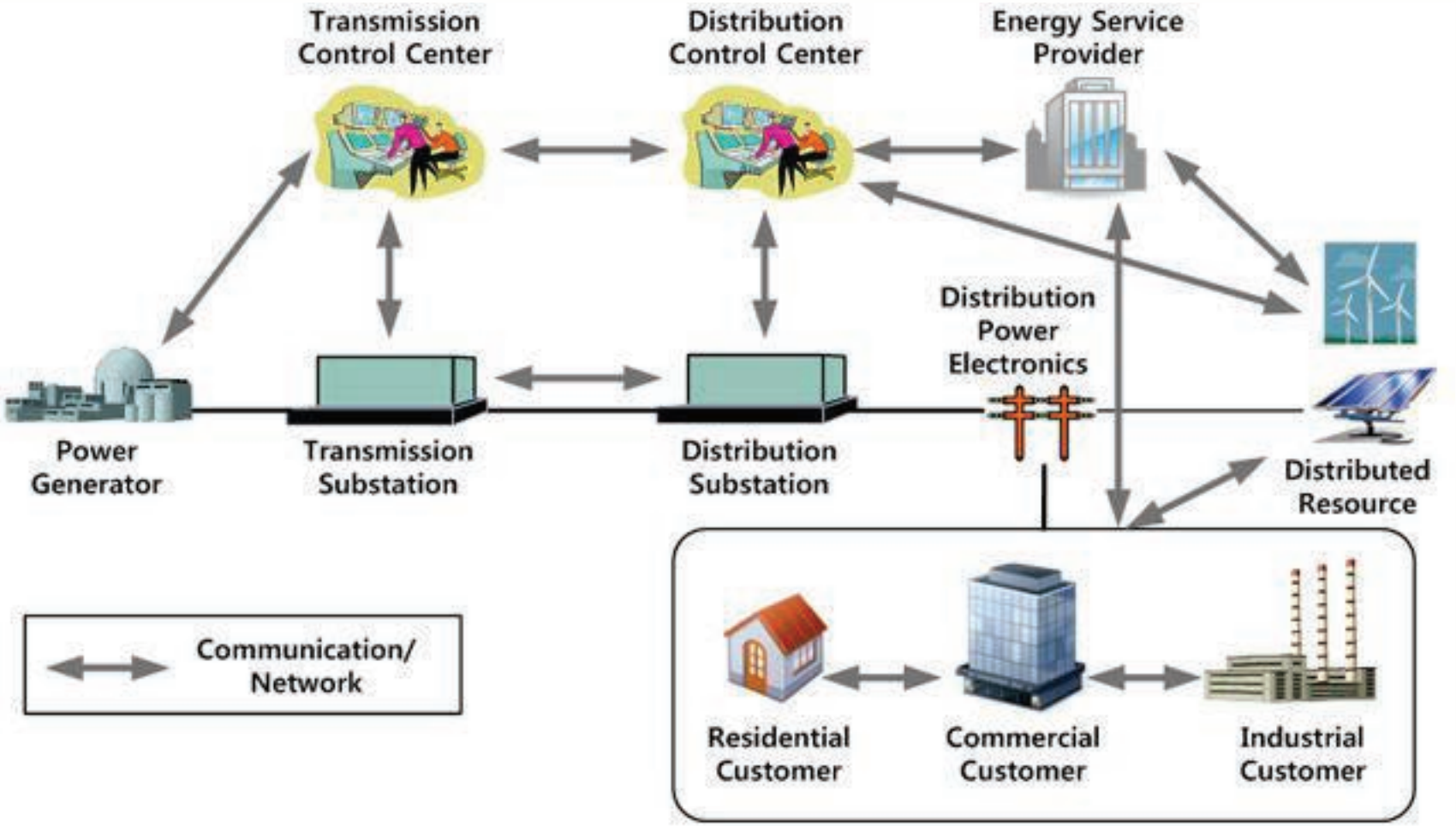
Dept. of Electrical and Computer Engineering

Iowa State University

Outline

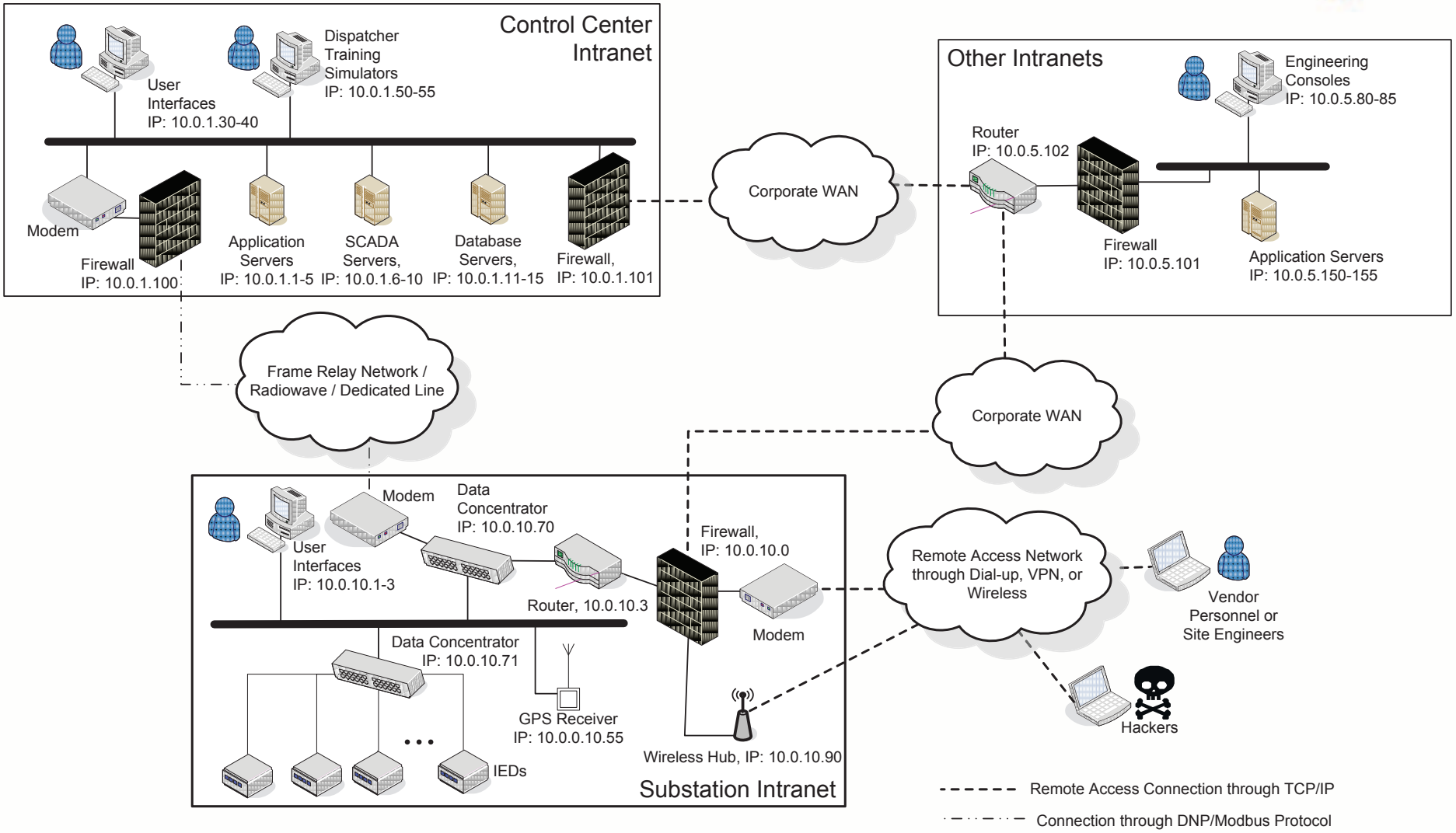
- Smart Grid – A Cyber Physical System
- Cyber Security & Testbed Research
- *PowerCyber* Testbed Architecture
- Security Evaluation Studies
- Conclusions

Electric Power Grid: A Cyber-Physical System

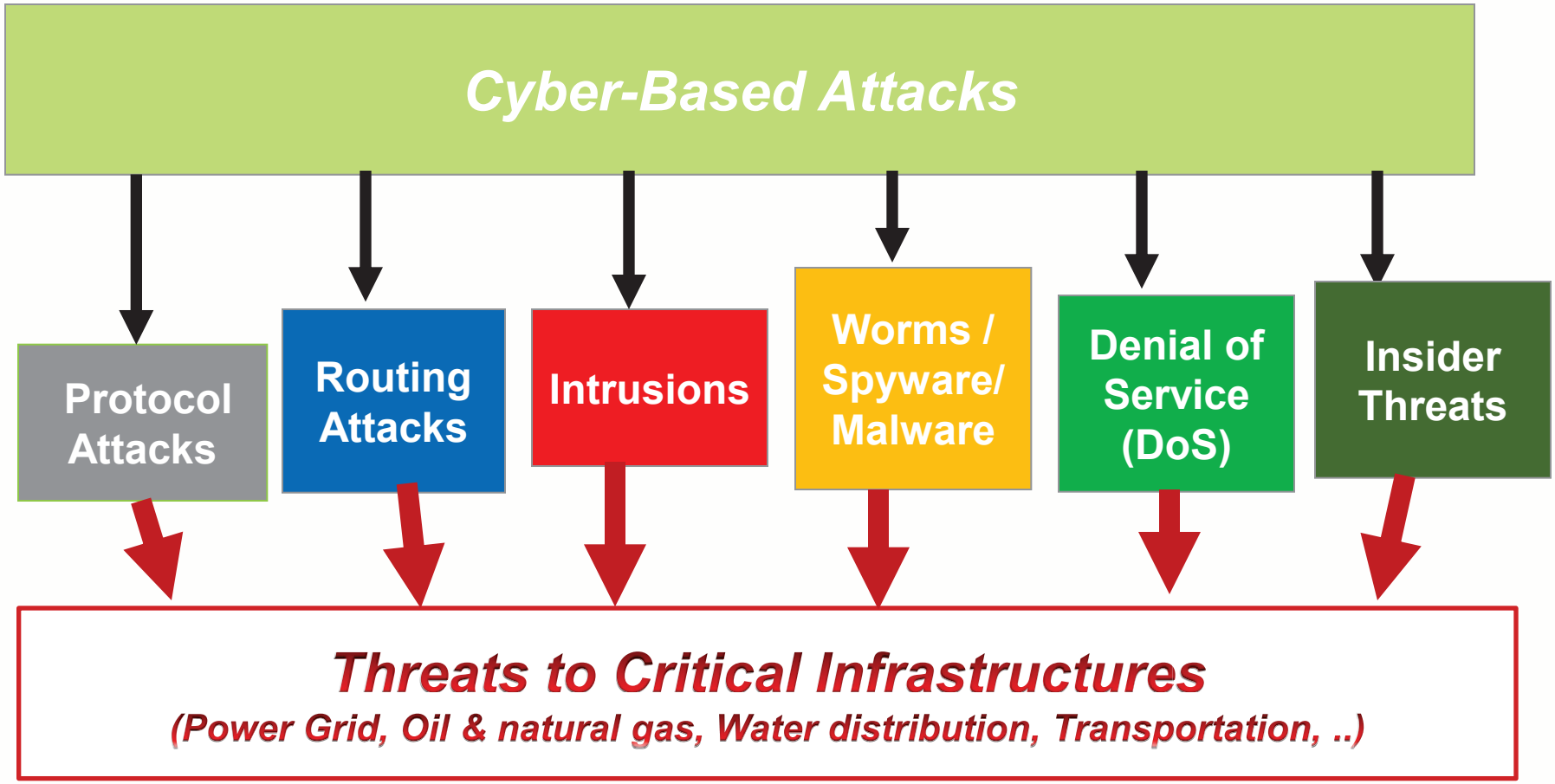


Source: http://cnslab.snu.ac.kr/twiki/bin/view/Main/Research

SCADA control network



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.

Unique challenges in Cyber-Physical system security

	Information Security	Infrastructure Security	Control Systems 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
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

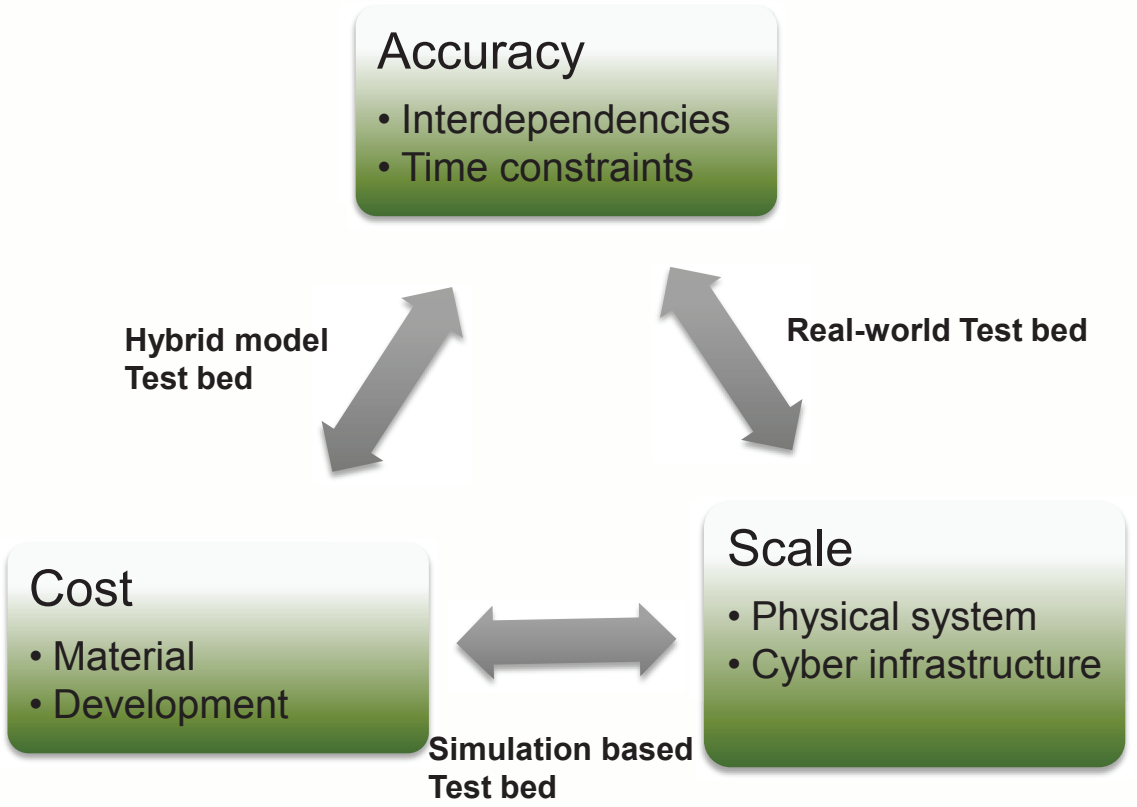
Cyber Attacks: Deter, Prevent, Detect, Mitigate, be Resilient, Attribution

Smart Grid Cyber Security

- **DoE Smart Grid vision**
  - Leverage advances in sensing, control, and communication
  - Leverage legacy network infrastructures
  - Realize emerging applications like AMI, SAS, WAMPAC

- **Cyber Security compliance and R&D**
  - NERC CIP
  - NISTIR 7628
  - DHS Control Systems Security Program
  - DoD Cyber Security Research
  - DoE National Laboratories
  - Academic Research

Testbed design tradeoffs and objectives



- Modularity
- Scalability
- Repeatability
- Re-configurability
- Interoperability

Test bed applications

- **A1:** Risk Modeling and Mitigation studies
  - Vulnerability assessment
  - Impact analysis (Adequacy and stability studies)

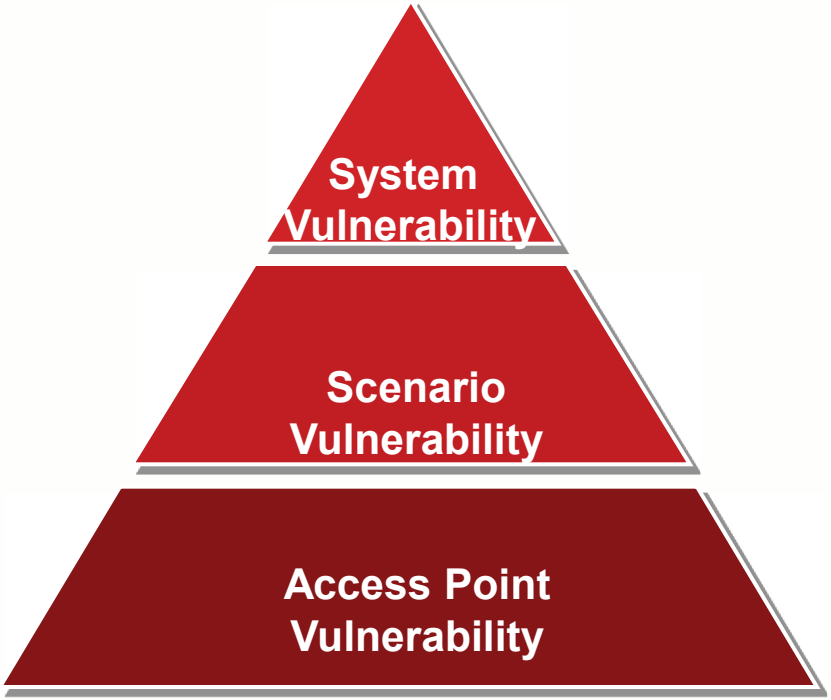
- **A2:** Cyber-Physical System studies
  - Smart attack vector formulation
  - Attack-resilient control algorithms
  - Attack-Defense exercise

- **A3:** Vendor product testing
  - Protocols, Firewalls, VPN
  - Relays, Control Software, etc.

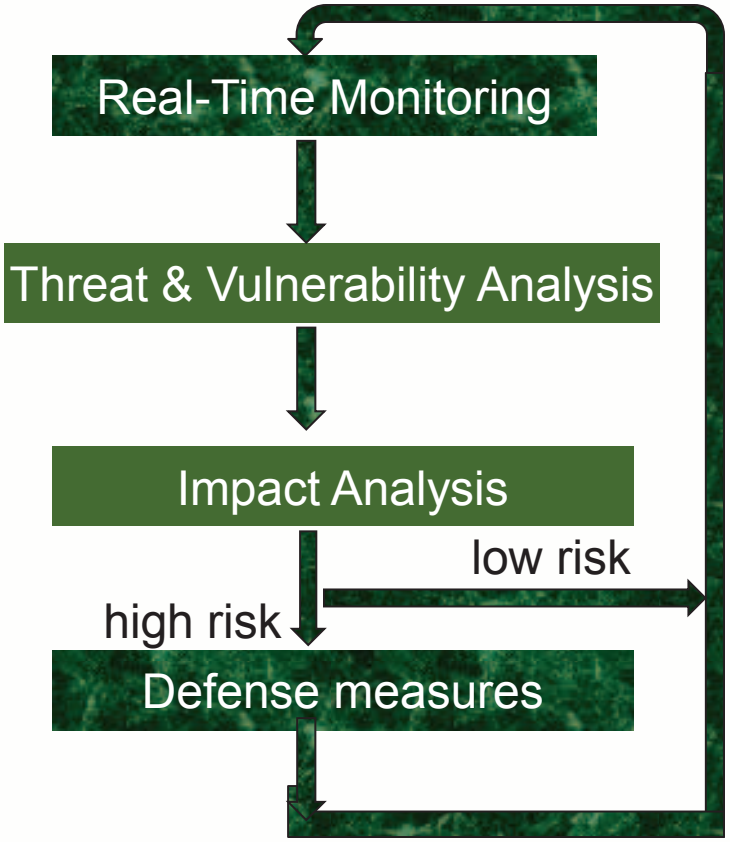
A1: Risk Modeling and Mitigation

Risk = Threat x Vulnerability x Impacts

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



Hierarchical modeling



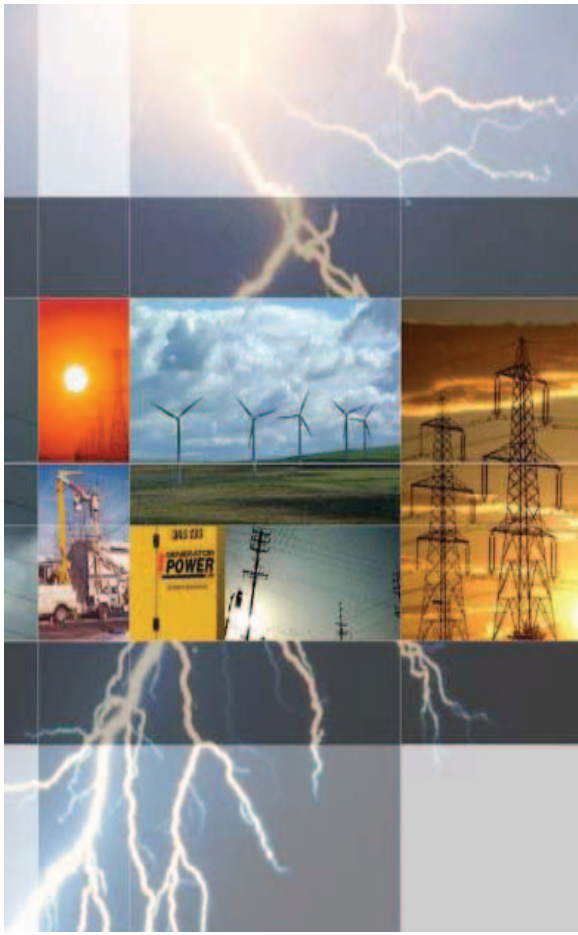
A2: Cyber-Physical System Security

Cyber Security of

Wide-Area Monitoring, Protection and Control

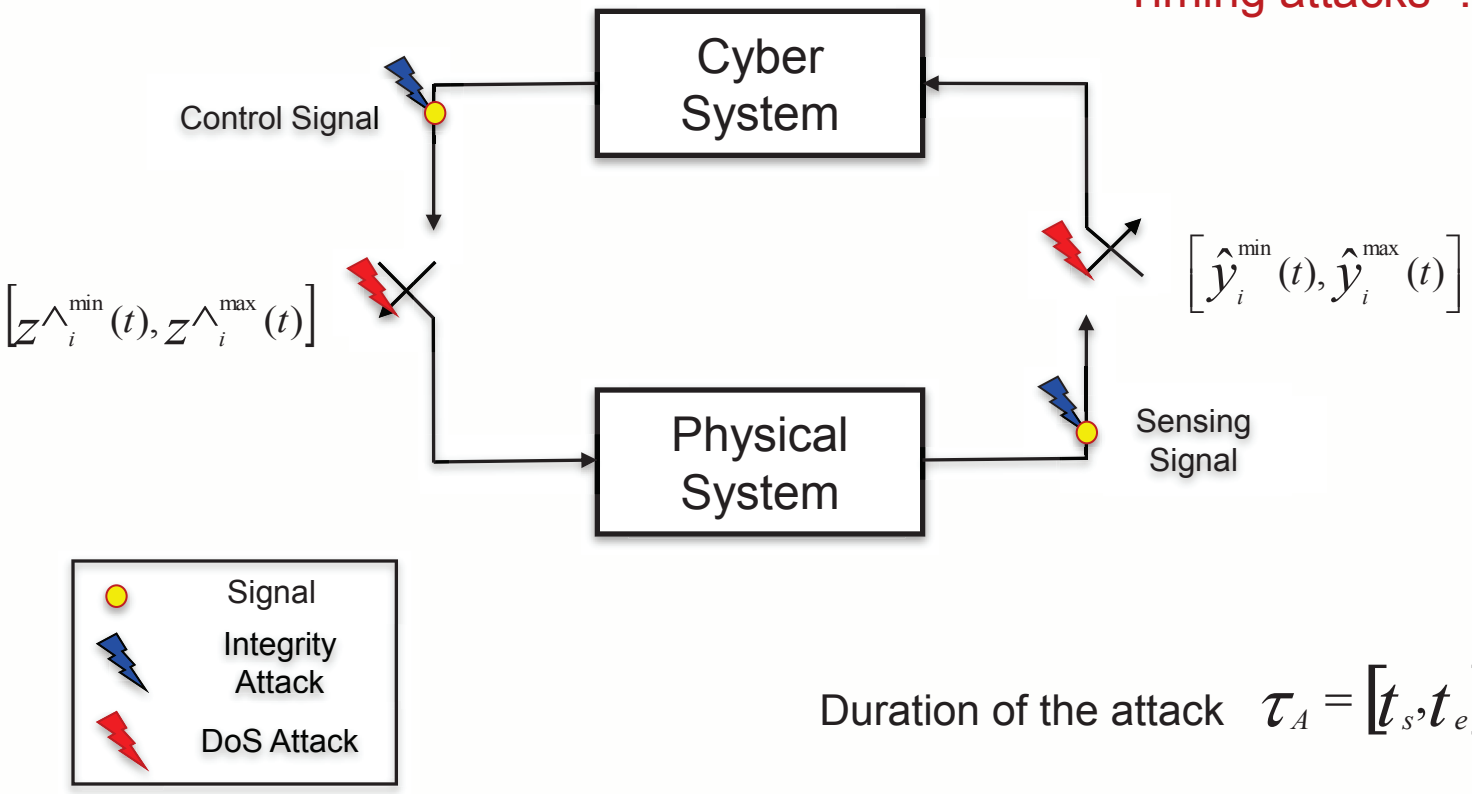
- Man-in-the-middle attacks
- Data integrity attacks
- Denial of service attacks
- Timing attacks …

- Frequency control
- Voltage control
- Stability analysis



CPS Security model

- 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.

Testbed – Related Work

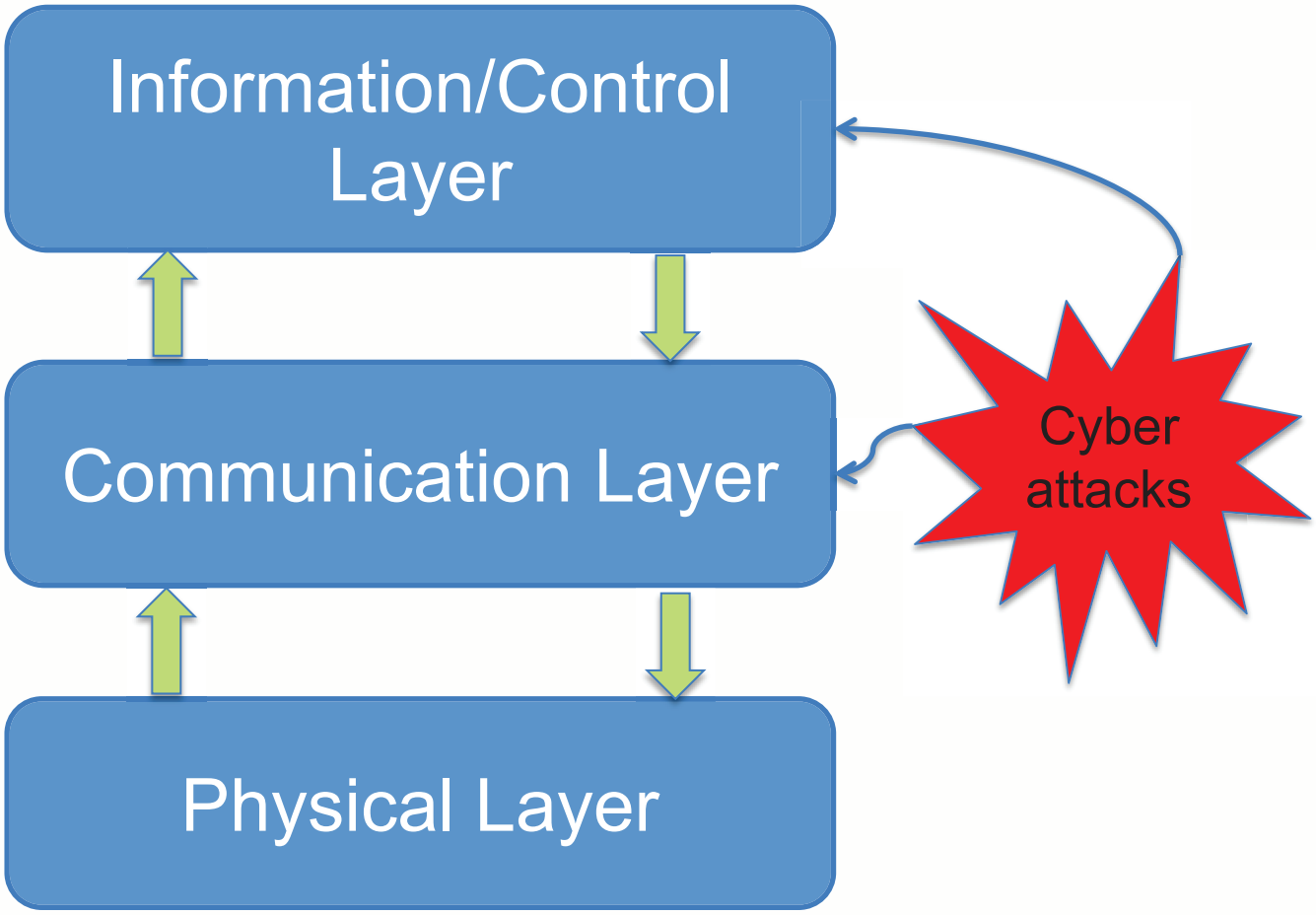
- National SCADA test bed (NSTB) @ Idaho National Laboratory
- Virtual Control System Environment @ Sandia National Laboratory
- Virtual Power System test bed (VPST) @ University of Illinois, Urbana
- SCADA Security Testbed @ University College, Dublin, Ireland
- PowerCyber Testbed @ Iowa State University

Functional Decomposition

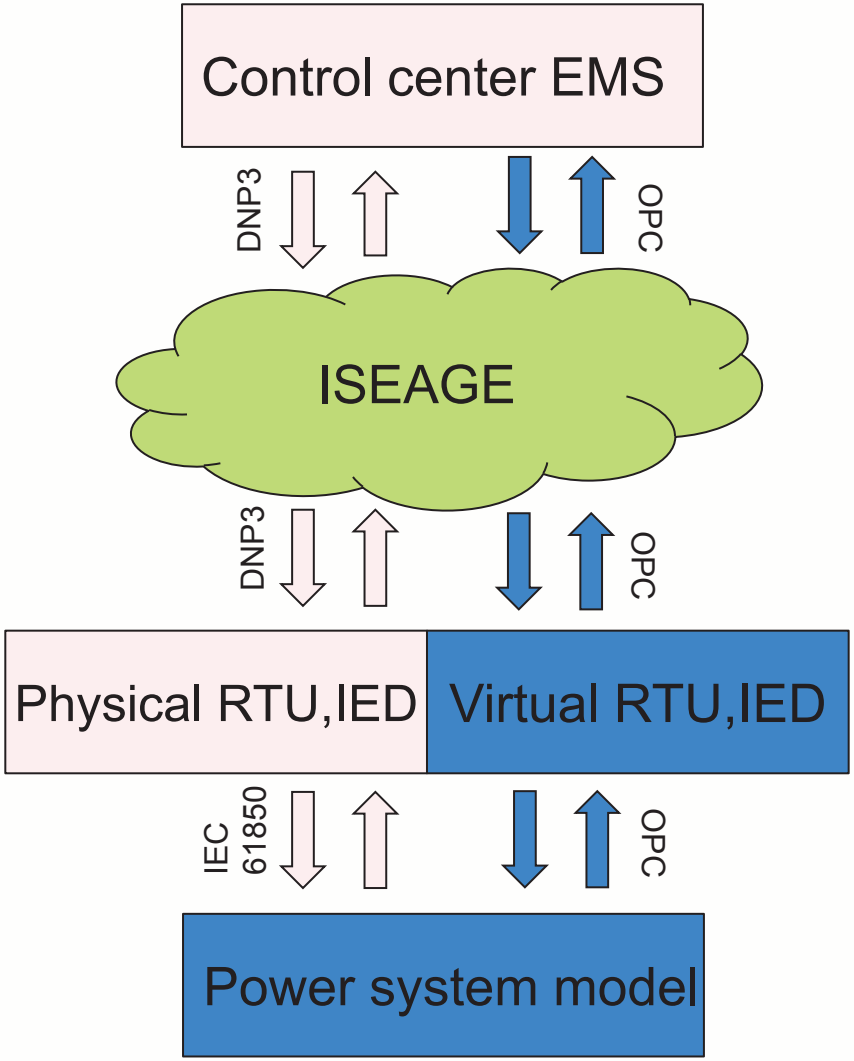
EMS, SAS, RTUs, IEDs

Routing infrastructure, Network protocols, Routers, Firewalls

Power system Simulators (RTDS, Power factory)



Components: Simulated, Emulated, Physical

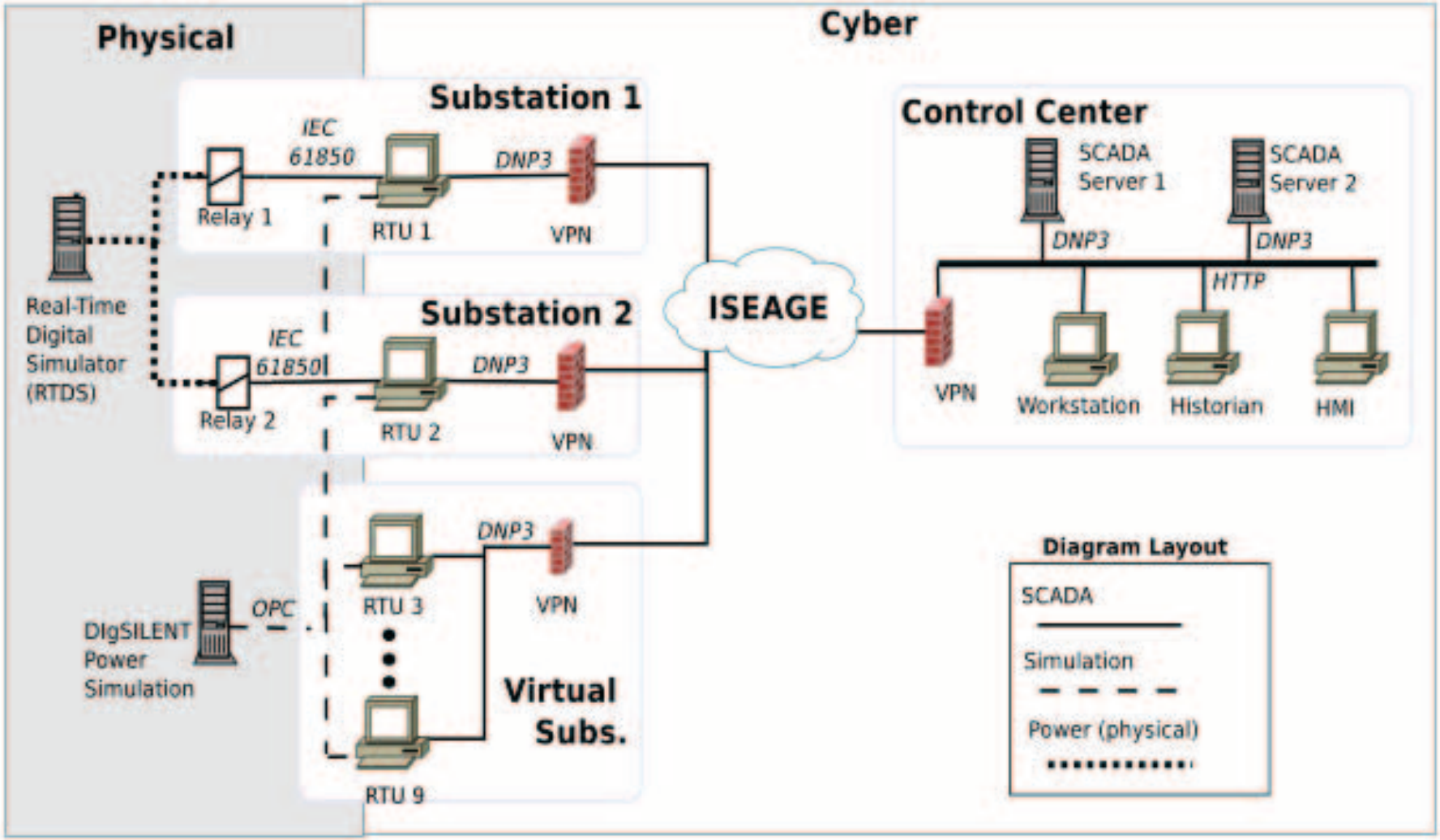


Physical components

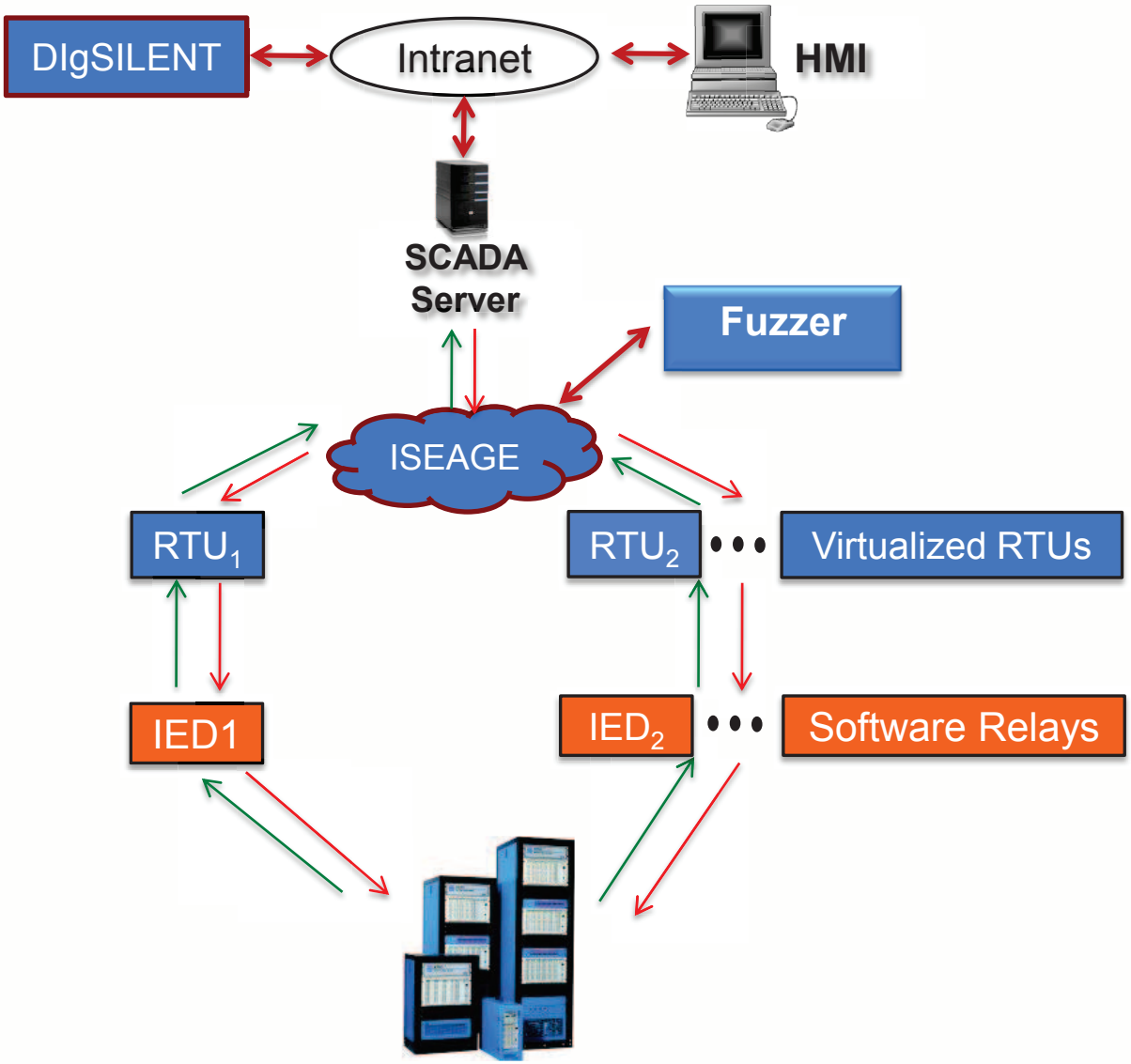
Emulated components

Simulated components

PowerCyber Testbed architecture

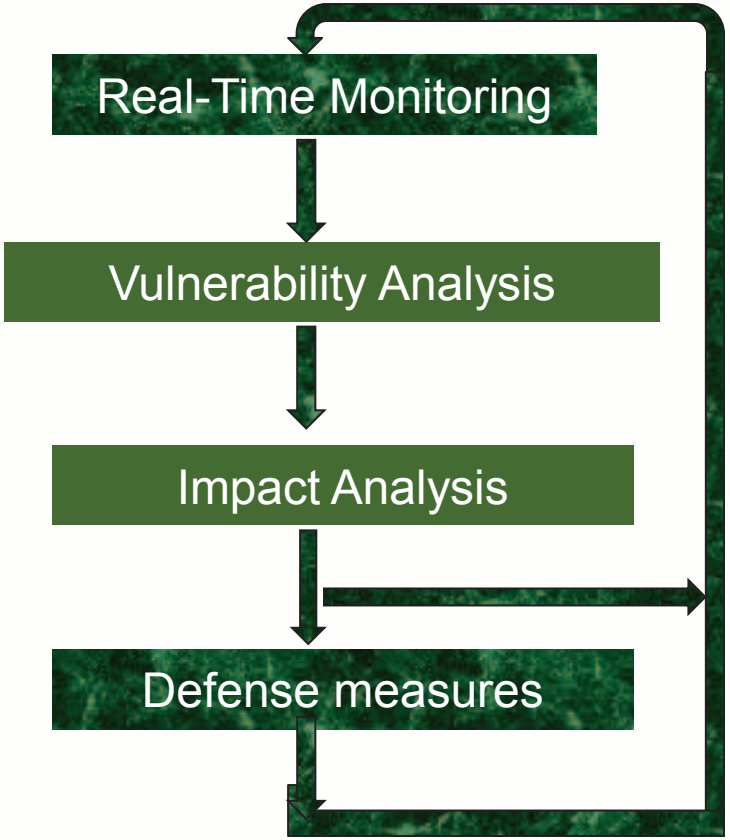


Test bed current configuration



Testbed - Security Evaluation

- Vulnerability scan
  - Port scanning
  - Communication Port
- Attack tools/actions
  - Packet capture
  - DNP 3.0 Protocol
  - Relay Open/Close request packet

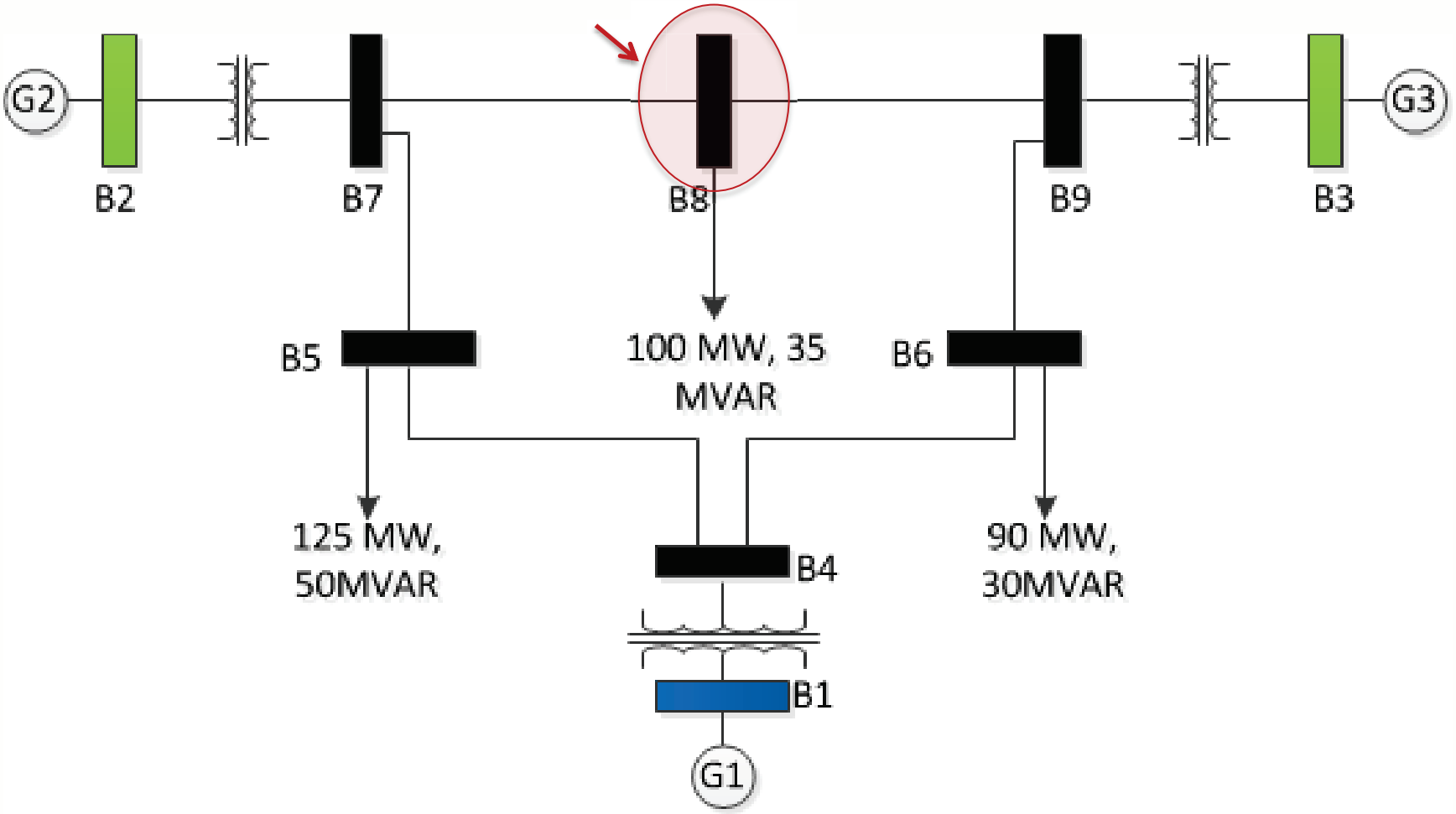


- Attack-defense studies
  - Denial of Sensor measurement (Substation → Control center)
  - Denial of Control (Control center → Substation)
  - Cyber-Physical Impact Analysis & Countermeasure evaluation

Test bed - Security Evaluation

- Vulnerability assessment
  - Review and verification of cryptographic use including protocols and key management strategies
  - Software availability requirements
  - Robustness against DoS attacks
  - Software security testing and vulnerability enumeration
  - Quantitative risk assessment based on vulnerability analysis
  - Communication network fuzz testing

Impact Analysis: Cyber attack scenario



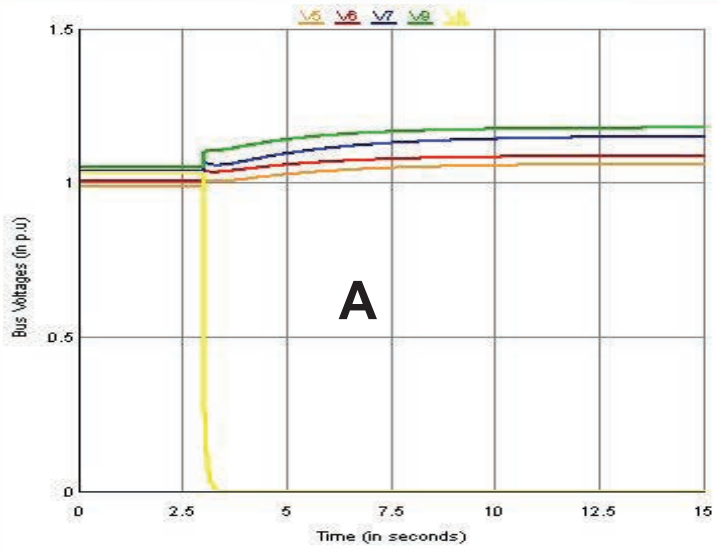
WSCC 9 bus system

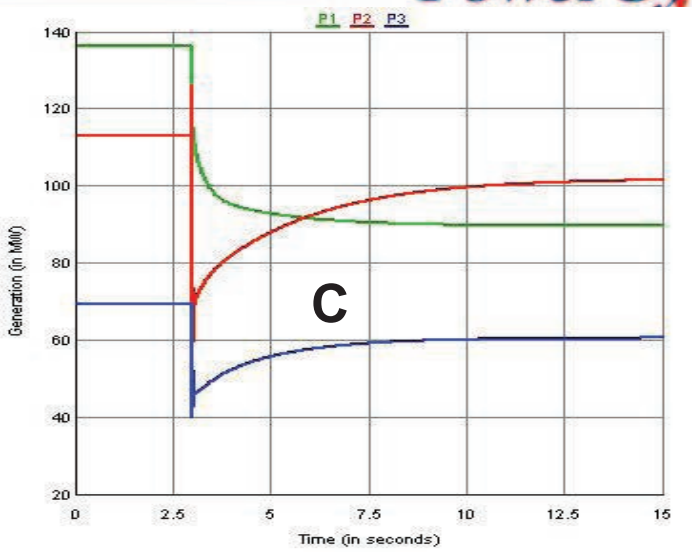
Cyber attack results

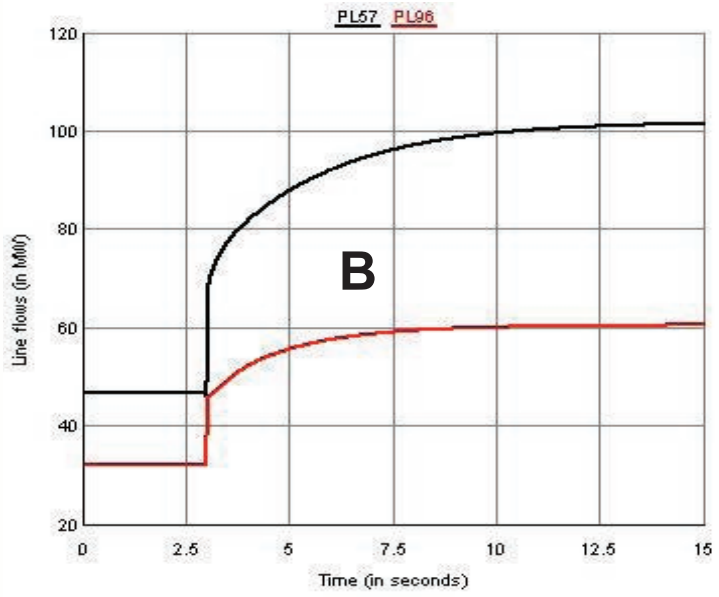
Before attack	After attack
Sum of generation= 136+113+69=318 MW Sum of loads = 123+89+100= 312 MW Flow on line 5-7= 47 MW Flow on line 6-9= 32 MW	Sum of generation= 90+101+60=251 MW Sum of loads= 142+104= 246 MW Flow on line 5-7= 102 MW Flow on line 6-9= 60 MW

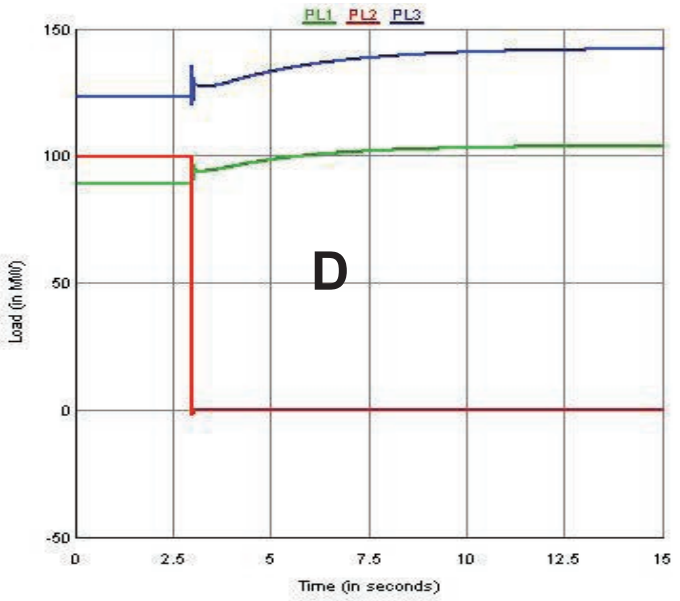
- *Key Observations:*
  - *Plot A: Increased voltages at several buses*
  - *Plot B: Some transmission lines overloaded, could lead to further tripping*
  - *Plot C: Generation is re-dispatched, results in uneconomic operation*
  - *Plot D: Loss of load due to an attack*

Real-time Simulation results of a cyber attack





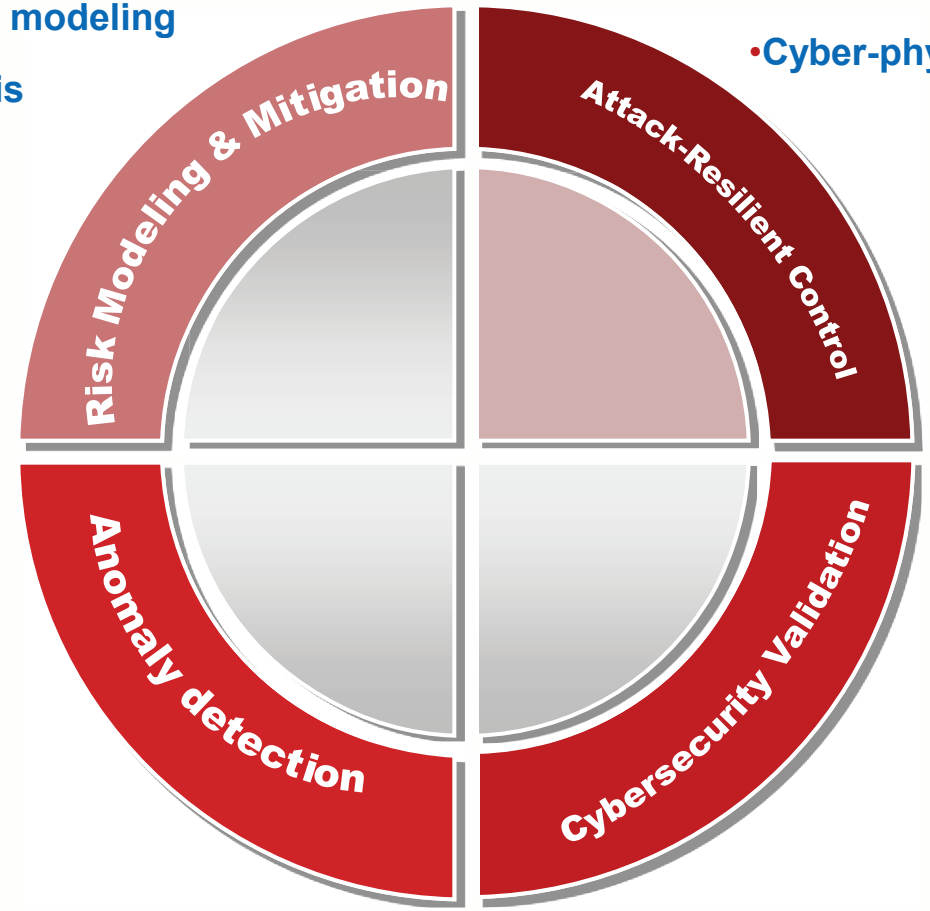




Conclusions

- Cyber-Physical system modeling
- Cyber Exposure analysis
- Mitigation Algorithms

- Model-based control
- Cyber-physical mitigation



- Model-based IDS
- Temporal and Spatial correlation of data

- Analytical
- Simulation
- Testbed

http://powercyber.ece.iastate.edu

Thank you !!!

Acknowledgements:

•National Science Foundation
•Electric Power Research Center, ISU

• Students: Aditya Ashok, Adam Hahn, Siddharth Sridhar,, Jie Yan, and several undergrad students

•Collaborator: Prof. Chen-Ching Liu, Wash. State Univ