SAND2009-3775P

Cyber Security R&D for Smart Grid Control Systems

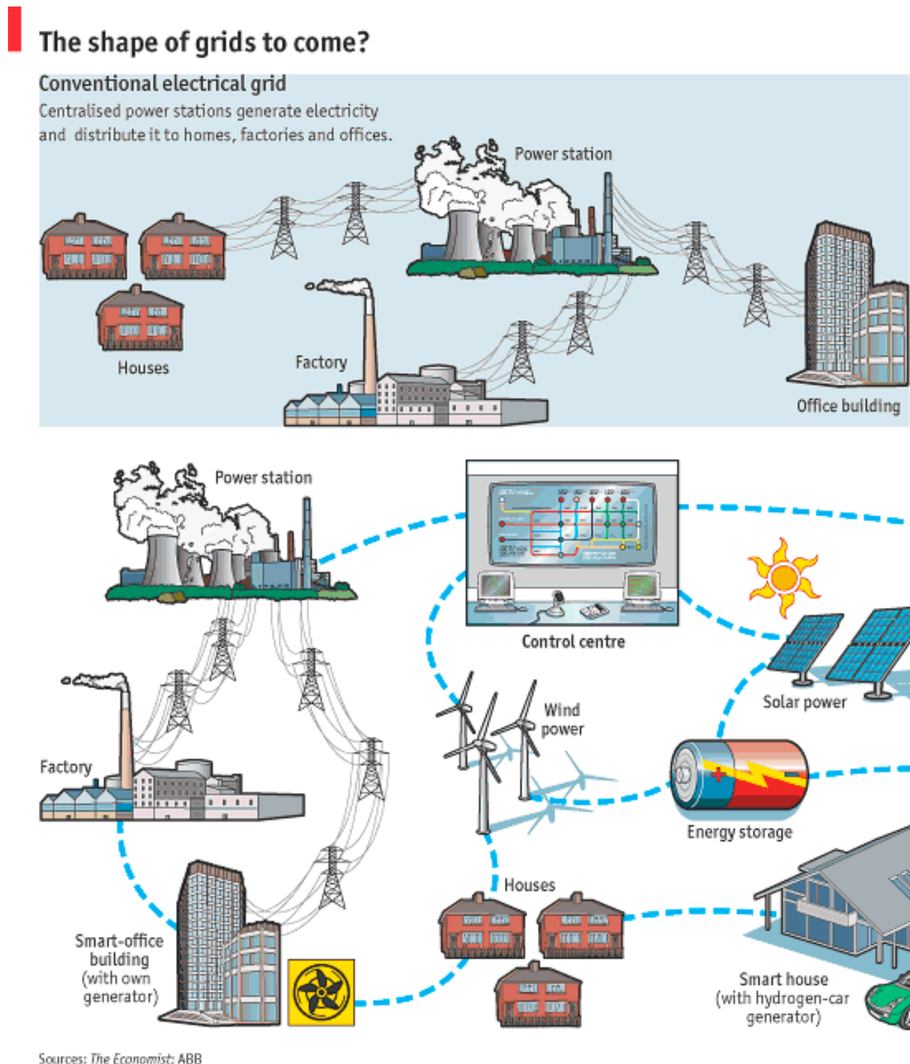
Juan Torres and Jason Stamp, Ph.D.
Energy Systems Analysis
Sandia National Laboratories

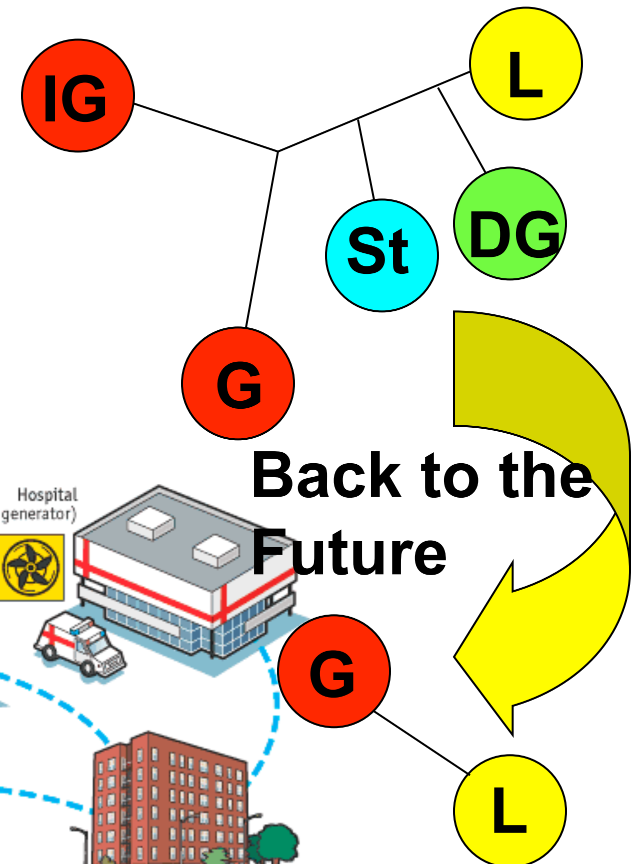
18 June 2009

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

Potential
Future Energy Grid

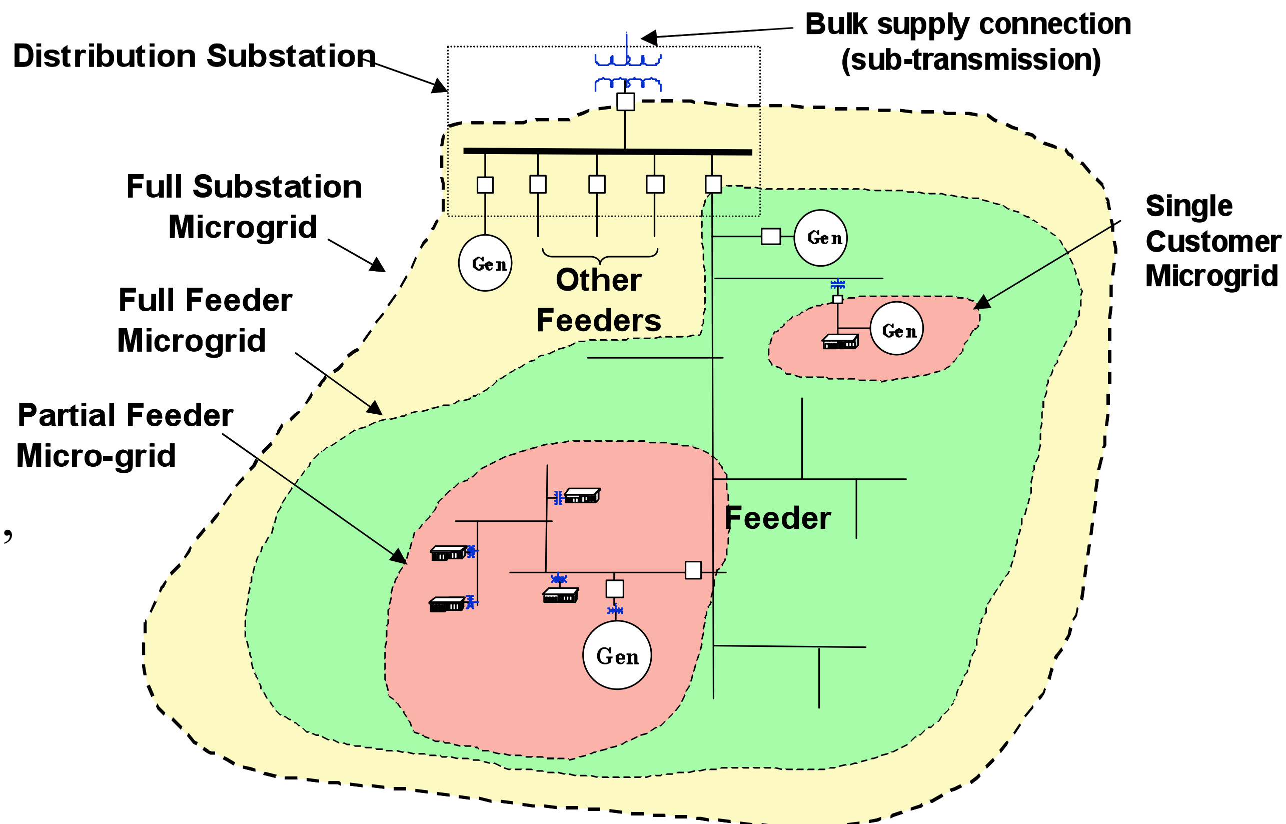




Courtesy of: California ISO

Distributed Generation And Micrograds

- Small combustion and μ-turbines
- Fuel cells
- IC engines
- Small hydro and wind
- Solar PV
- Energy storage (batteries, flywheels, …)
- Emerging plug in hybrid vehicles

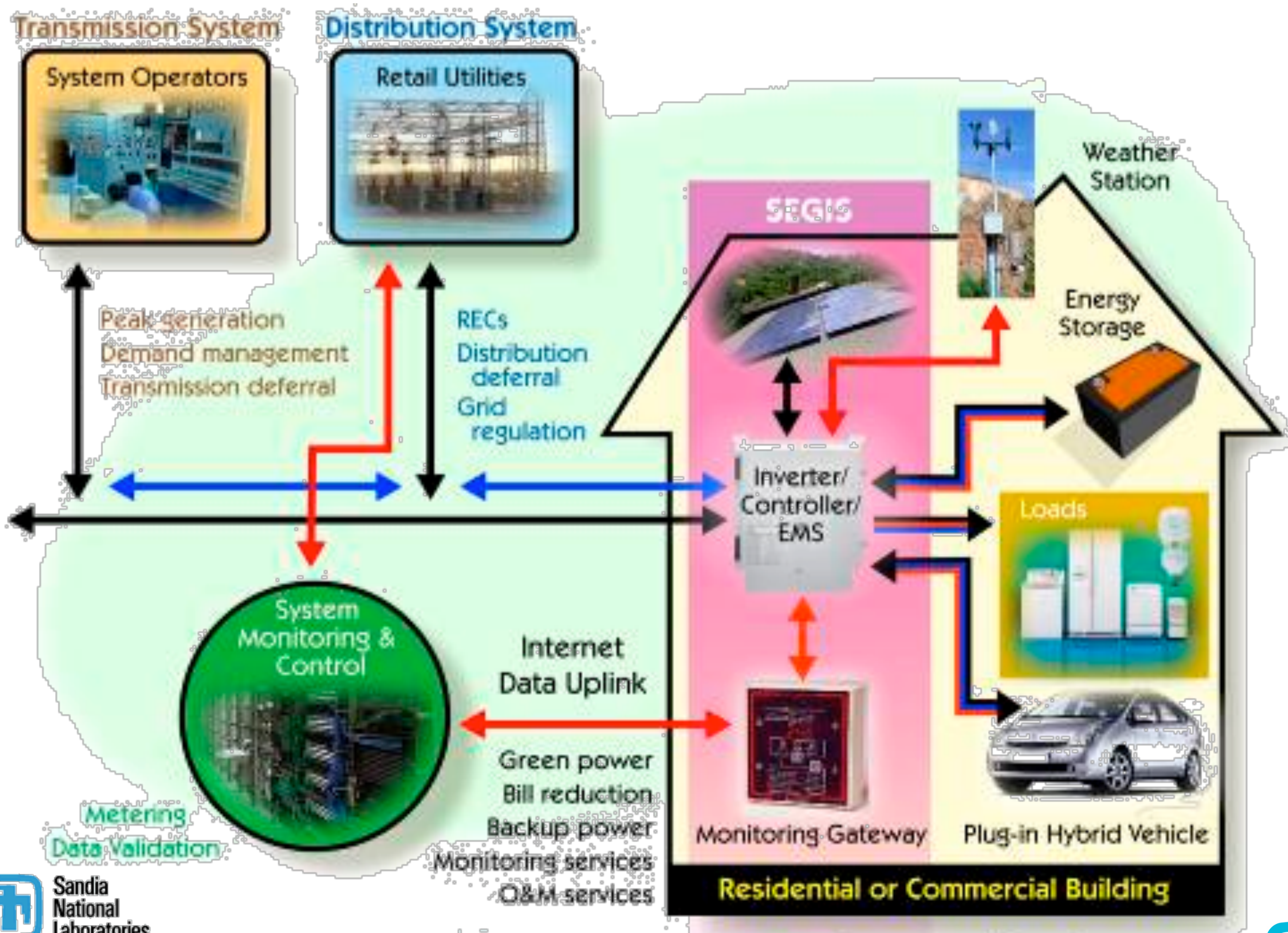


Ref. EPRI

Residential	Less than 10-kW, single-phase
Small Commercial	From 10-kW to 50-kW, typically three phase
Commercial	Greater than 50-kW up to 10MW

Sandia National Laboratories

Information Flow in The Smart Grid



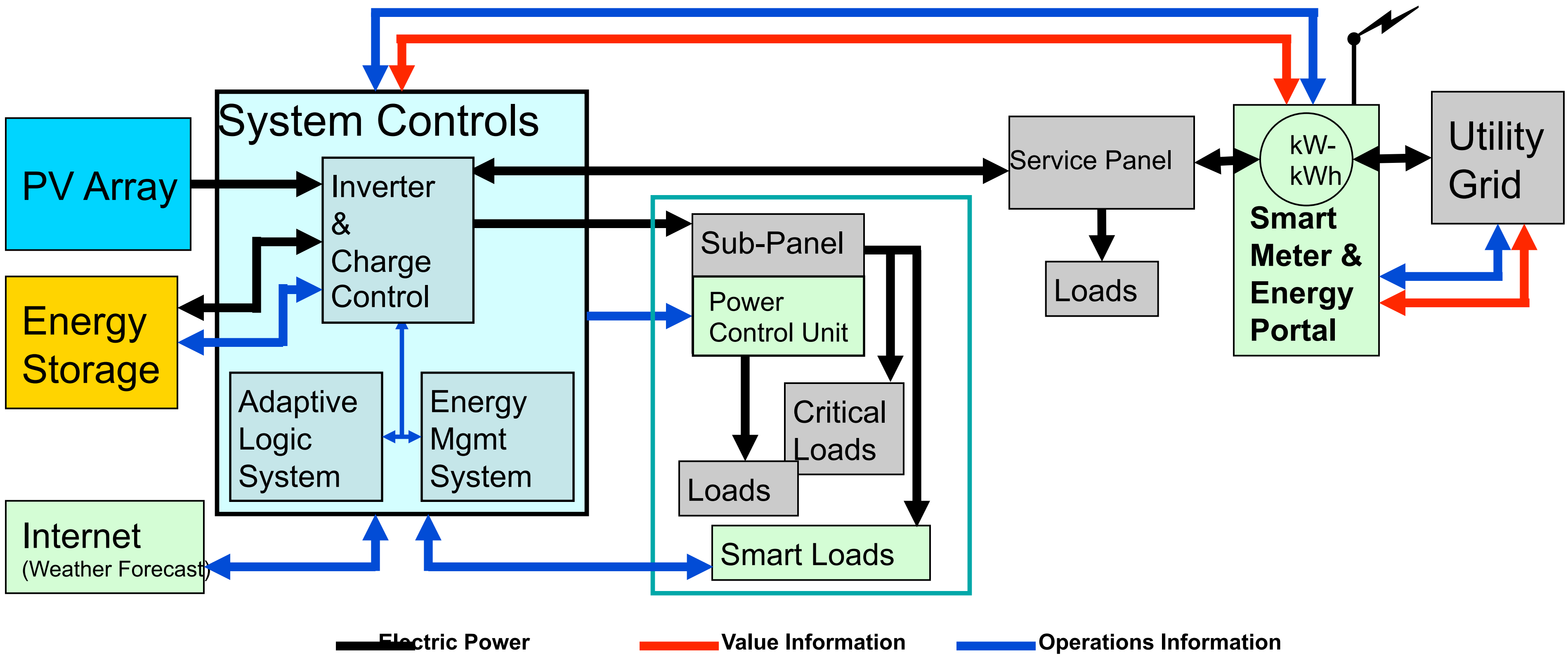
Sandia National Laboratories

NREL

Sandia National Laboratories

Smart Grid Requires Intelligence and Control

System for Supporting Advanced Distribution Infrastructure Operations



Sandia National Laboratories

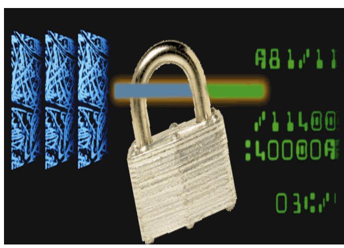
Sandia's Control Systems Laboratory Complex

IDART™
Information Design Assurance Red Team

Attack Resource Centers

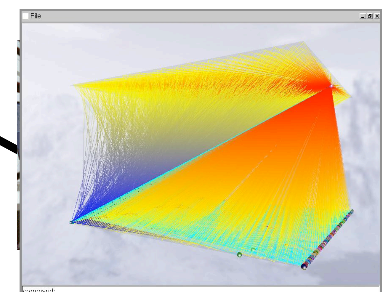
NISAC

Operational Generation & Load Assets



Cryptographic Laboratory

Network Laboratory



Center for Cyber Defenders

AISL
advanced information systems laboratory

Intelligent Infrastructure R&D

Sandia National Laboratories

Trends Impacting Control System Security

- Open Protocols
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Common Operating Systems and Technology
  - Standardized computer platforms increasingly used to support control system applications
- Interconnected to Other Systems
  - Connections with enterprise networks to obtain productivity improvements and information sharing
- Reliance on External Communications
  - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- Increased Capability of Field Equipment
  - “Smart” sensors and controls with enhanced capability and functionality

Sandia National Laboratories

US Government Cyber Security Policy Review

- Improve cybersecurity across all infrastructures
- Federal government should develop processes between all levels of government and the private sector to assist in preventing, detecting, and responding to cyber incidents
- Enhance information sharing to improve incident response capabilities
- [For] new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks

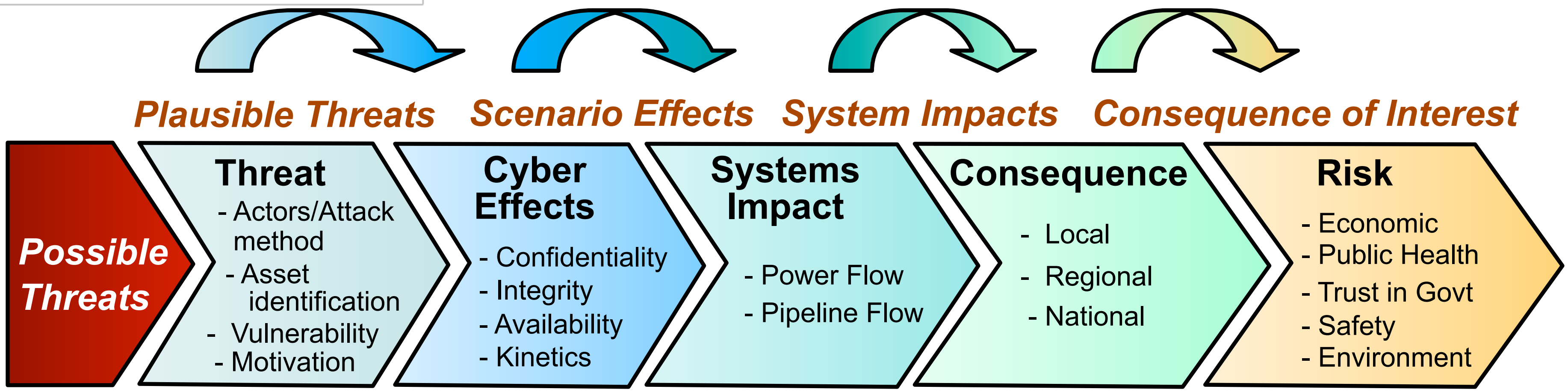
Integrated Risk Analysis: Help Reduce Risk of Energy Disruptions

- **Understand**
  - Threats, vulnerabilities, impacts, and consequences from facility to national scale
- **Assess**
  - Risk exposure through an end-to-end, threat-vulnerability-consequence analysis capability
- **Mitigate**
  - Vulnerabilities through fundamental security practices and security technologies

T * **V** * **C** = **R**

T (resource), V (weakness), C (effects)

Control System Integrated Risk Analysis



Threat-to-Consequence Risk Model

What threats are we concerned about?	Evaluate effects of cyber vulnerabili-ties	What are the physical impacts?	How do failures cascade into other CI?	Assess and quantify the Risk?

Provides a Framework for Conducting Cyber Risk Analysis

Sandia National Laboratories

Cyber Effects Analysis

Challenges/Needs

- Develop Virtual Control Systems Environment (VCSE)
- Model existing and future control system devices and communication protocols
- Design a scalable architecture to allow for Hardware/Software-in-the-Loop

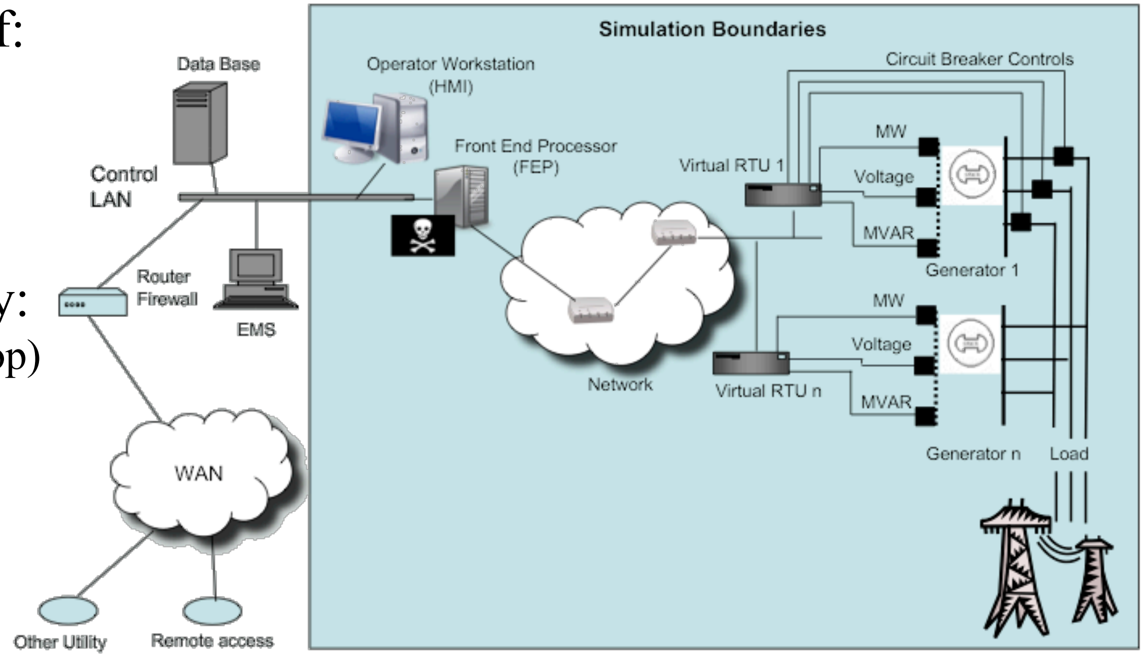
Results/Benefits

- Given a plausible threat/vulnerability - What effects can be achieved on control systems?
- Understand effects that can lead to impacts
- Reduce testing costs

Sandia National Laboratories

Cyber Effects Analysis Approach

- Analysis of the thread from command origin to the point of the effect in the infrastructure system
- Simultaneous analysis of:
  - Physical processes
  - Control systems
  - IP networks
  - Other communications
- Varying levels of fidelity:
  - Real (hardware-in-the-loop)
  - Simulated
  - Virtual (emulated)
- Launch cyber attacks in a controlled setting
- Rapid configuration and prototyping



Simulation Scenario

Sandia National Laboratories

Impact Analysis from Cyber Attack

Challenges/Needs

- Develop ability to map impacts from cyber attack to grid effects
- Incorporate outages caused by cyber attack to conventional reliability analysis approaches
- Convert hybrid grid/control system to finite state approximation for dynamic analysis
- Analyze “worst case” attacks

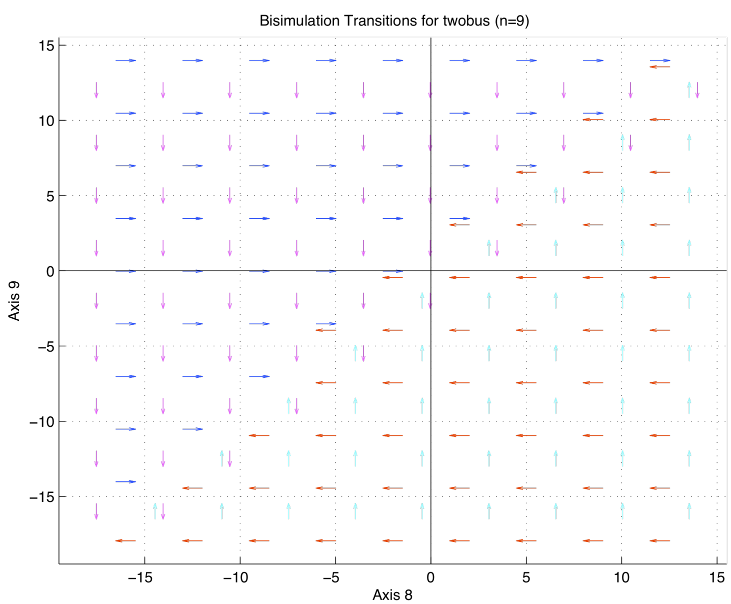
Results/Benefits

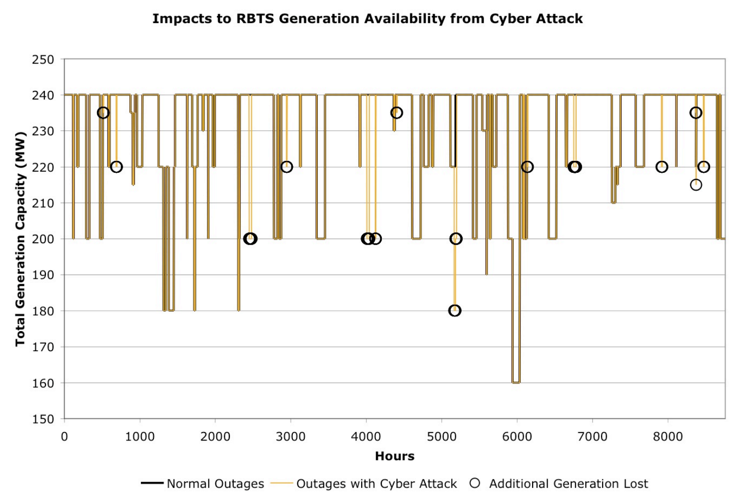
- Determine how cyber attacks translate into a physical effects failure
- Given a particular attack scenario, can a significant outage (e.g. scale and cascading) be achieved?

Sandia National Laboratories

Potential Grid Impacts For the Adversary

- Decreased system reliability (more frequent outages that last longer)
- Loss of significant or targeted power delivery capability
  - Overt approach: no electrical connectivity
  - Subtle approach: unusable delivery (low voltage, overloads, etc.)
- Leverage dynamic or static modeling for the grid
- Determination of duration for effects is crucial





Some Security Requirements

- Encryption & data authentication (key management)
- Logging & forensics support
- Intrusion detection (NIDS and HIDS) & prevention
- Firewall and network filtering
- Authentication and logging for remote access (Configuration session capture)
- Control system visualization & monitoring
- Security repository and alarm capability

Sandia National Laboratories

Sandia National Laboratories

Conclusions: Smart Grid Cyber Security

- Smart Grid depends on information flow
- Cyber security is critically important to operation and reliability
- Trends are leading toward poorer cyber security
- Integrated risk analysis is the best approach for analyzing cyber security issues and technology

Questions?