



- August 15-18, 2010 • Dallas, Texas •
- Dallas Convention Center •



Grid Modernization and the Smart Grid

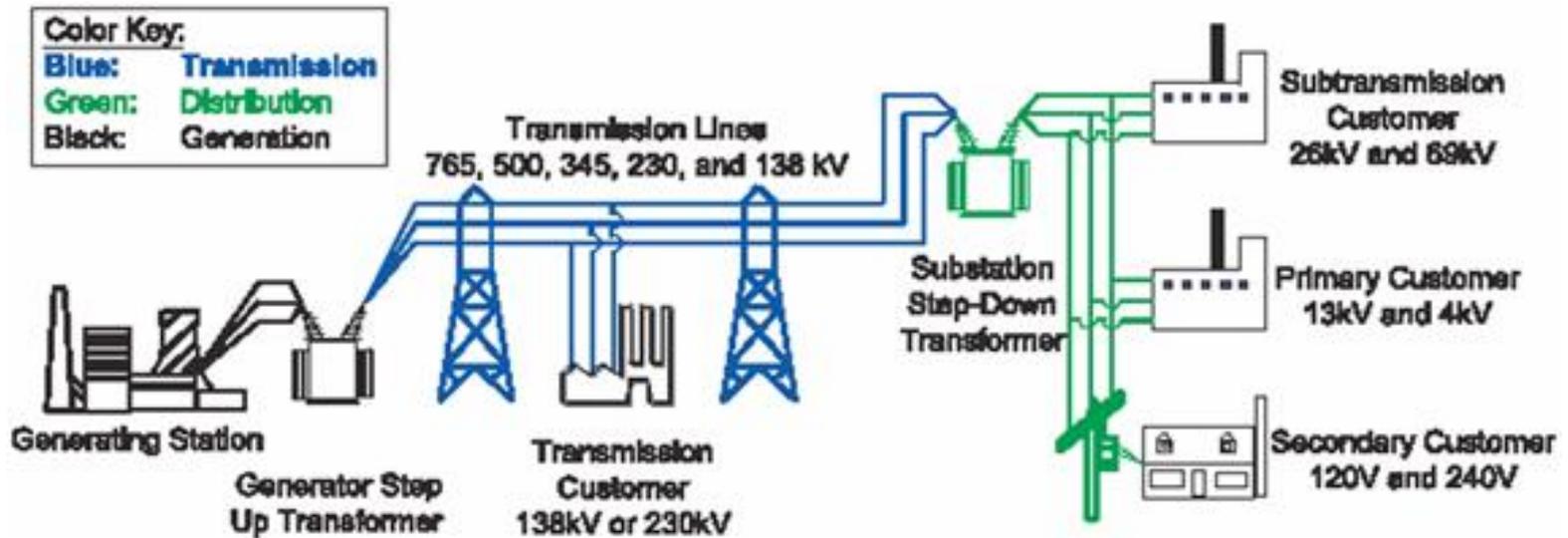
Hank Kenchington

Deputy Assistant Secretary R&D

Office of Electricity Delivery and Energy Reliability

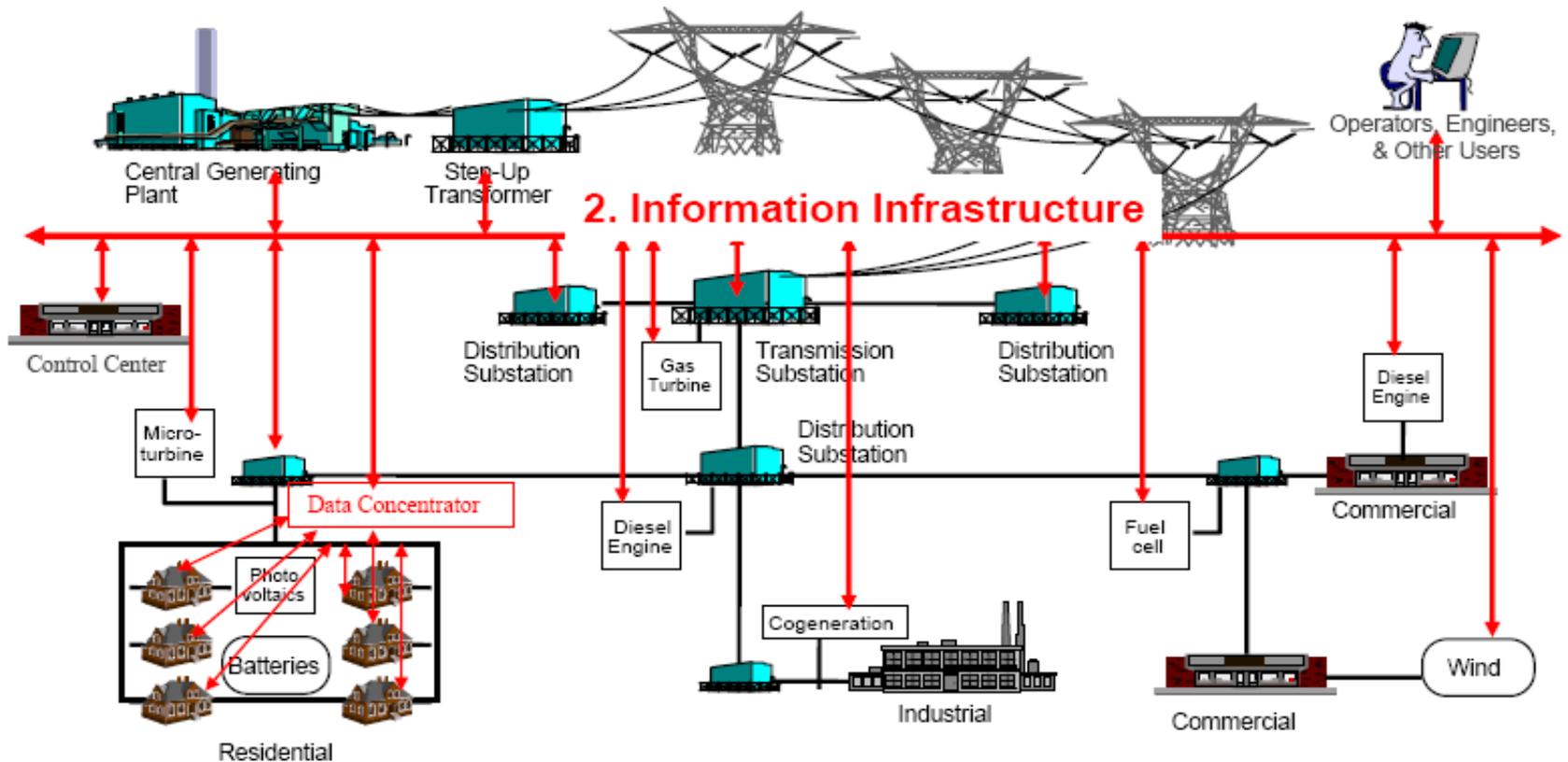
U.S. Department of Energy

Traditional Electricity Delivery System



Electric Grid – Electricity + Information

1. Power System Infrastructure

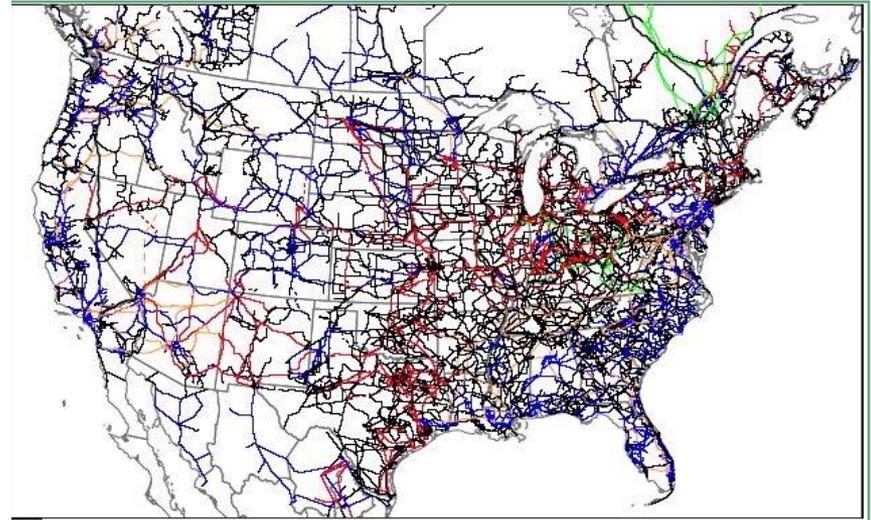


Source: Electric Power Resource Institute (EPRI)

The Electric Grid - A Complex System

Physically

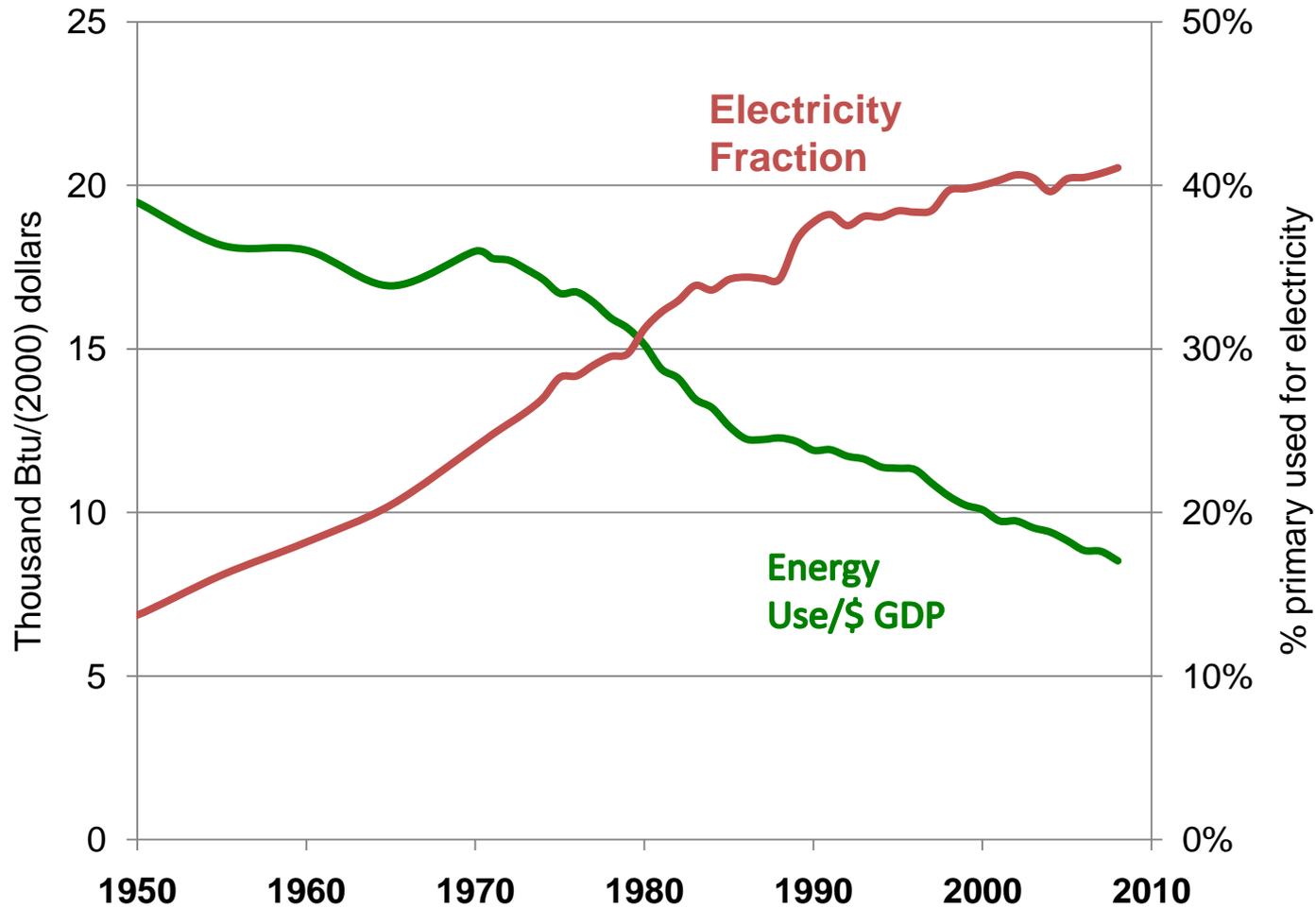
- **Not holistically designed, evolved incrementally in response to local load growth. Today:**
 - 30,000 Transmission paths; + 180,000 miles of transmission line
 - 14,000 Transmission substations
 - Distribution grid connects these substations with over 100 million loads - residential, industrial, and commercial customers
- **Diverse industry**
 - 3,170 traditional electric utilities
 - 239 investor-owned, 2,009 publicly owned, 912 consumer-owned rural cooperatives, and 10 Federal electric utilities



Technically

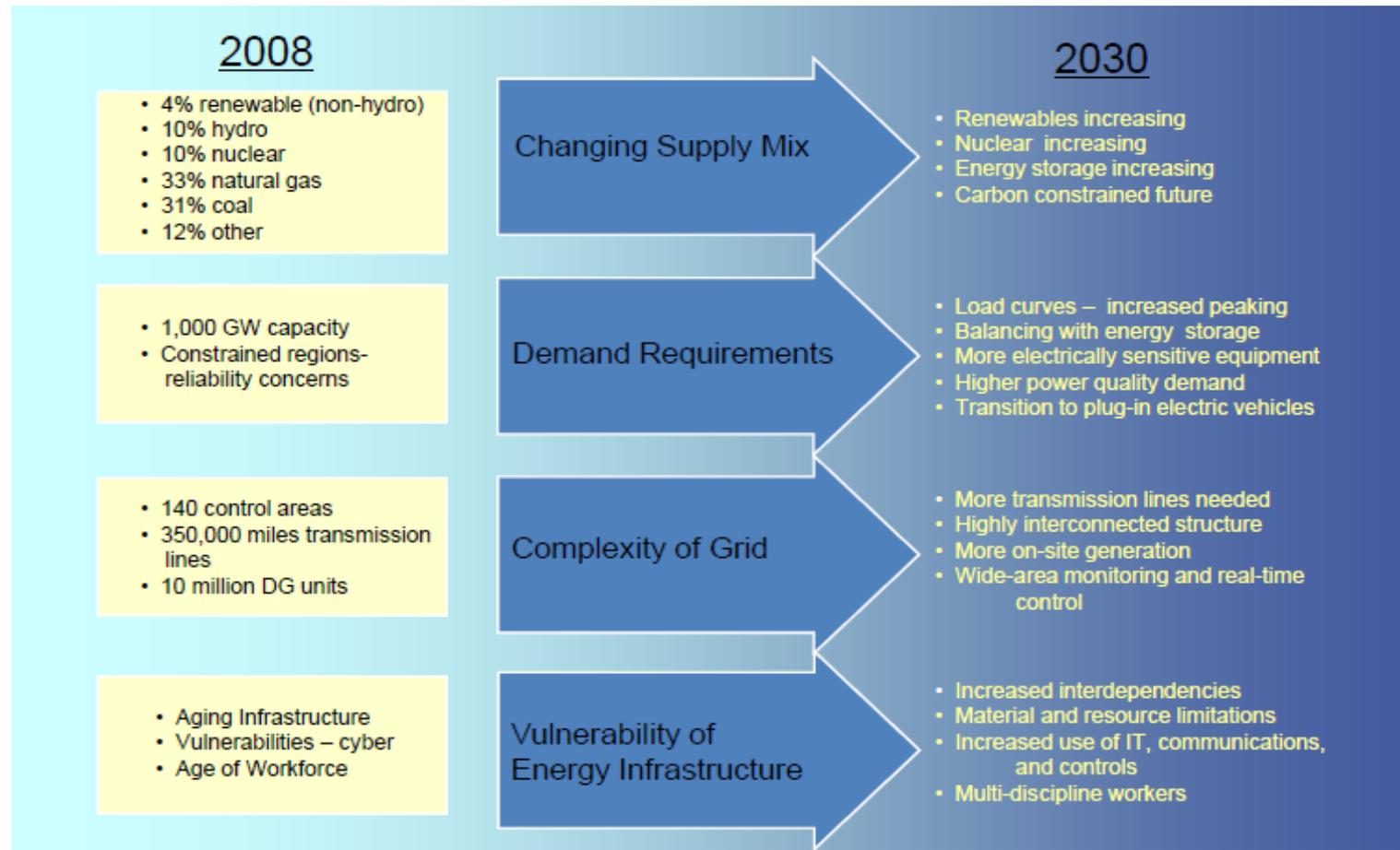
- **Electricity flows within three major interconnections** along paths of lowest impedance (at the speed of light); yet grid is **operated in a decentralized manner** by over 140 control areas
- **Demand is semi-uncontrolled** – smart grid technologies provide opportunity for dynamic, real-time balancing of demand and supply (demand response)
- Ultimate “**just-in-time**” production process

US highly dependent on electricity – and growing

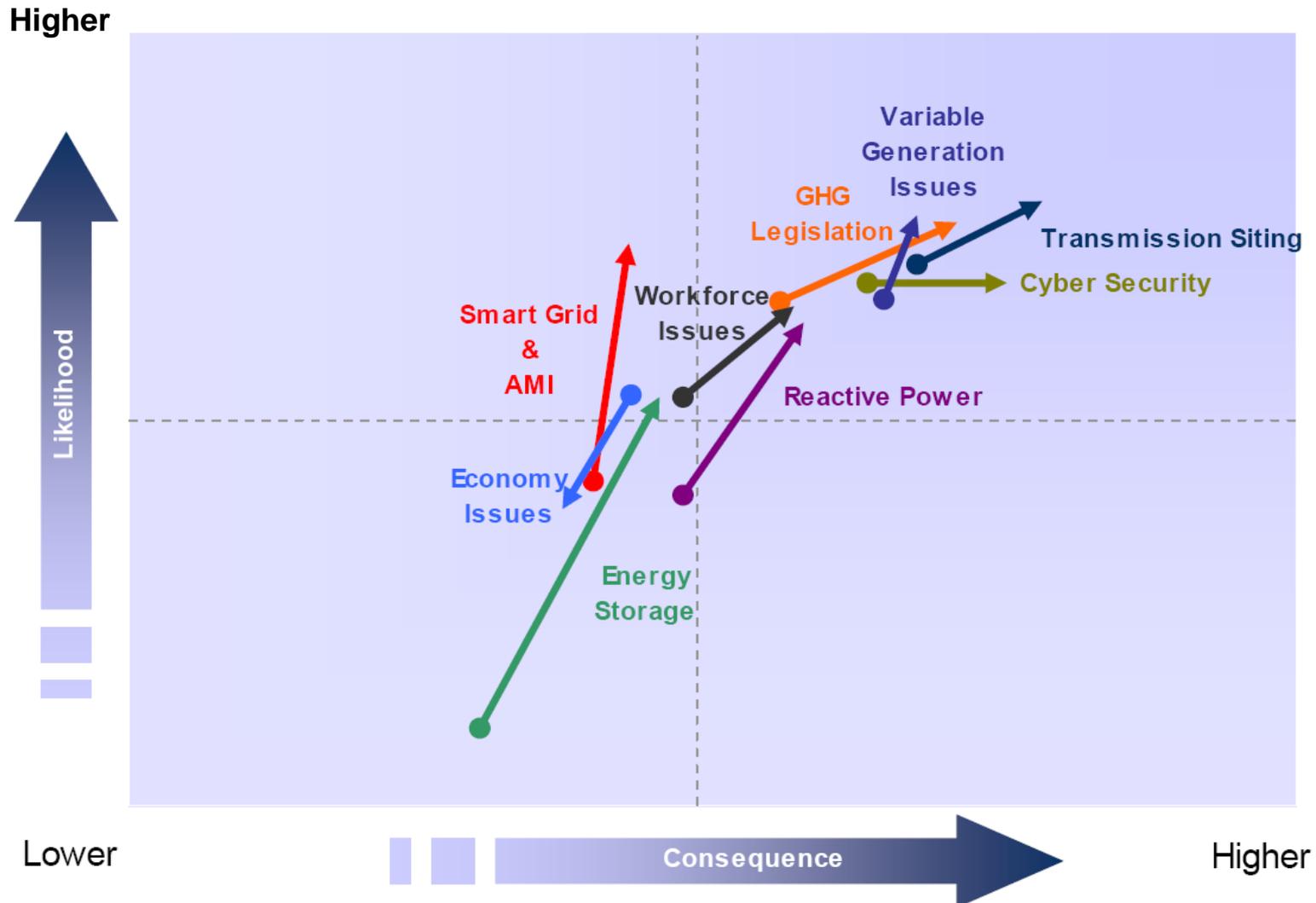


Source: DOE/EIA Annual Energy Review 2008

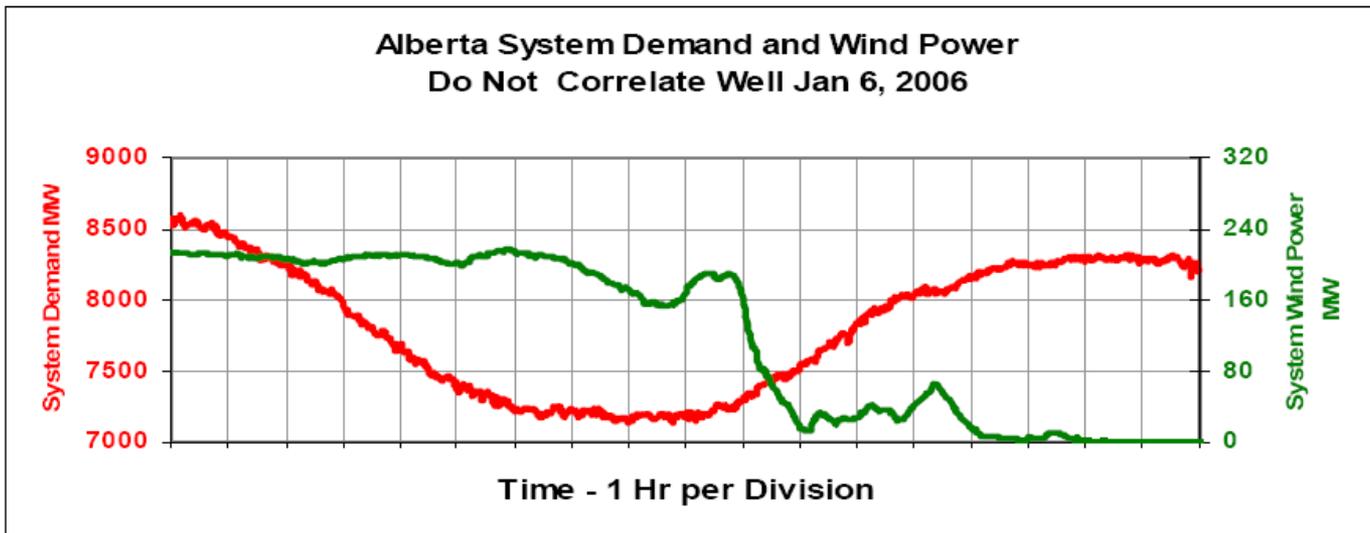
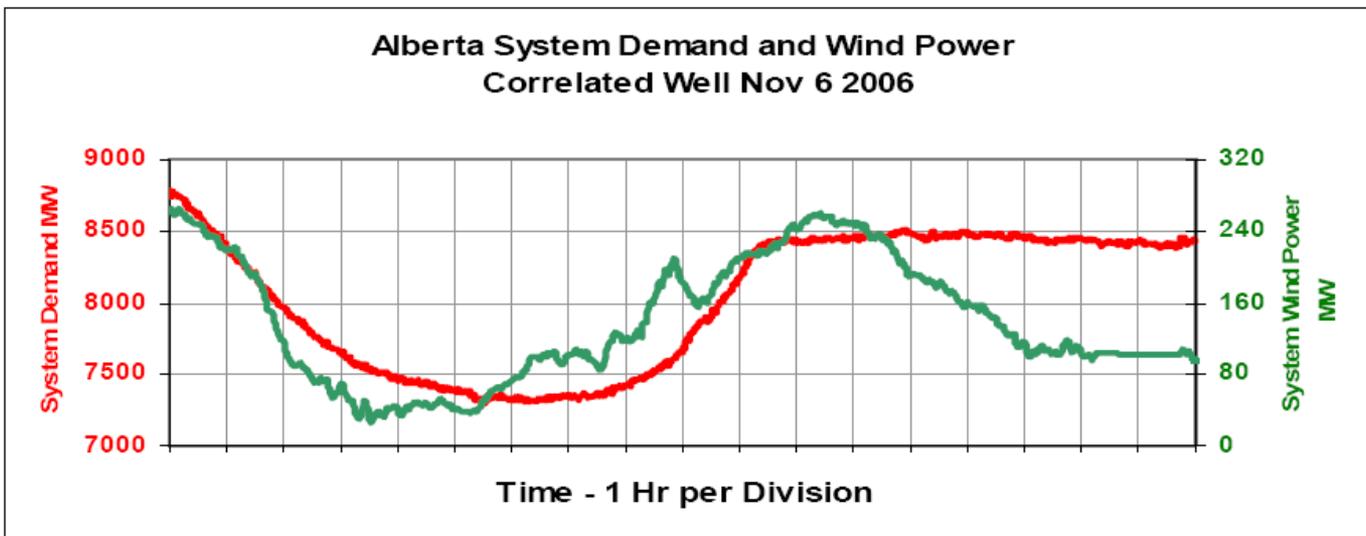
Demands of a 21st century economy will significantly affect nature of 2030 electric grid



Grid Reliability Risk Trends

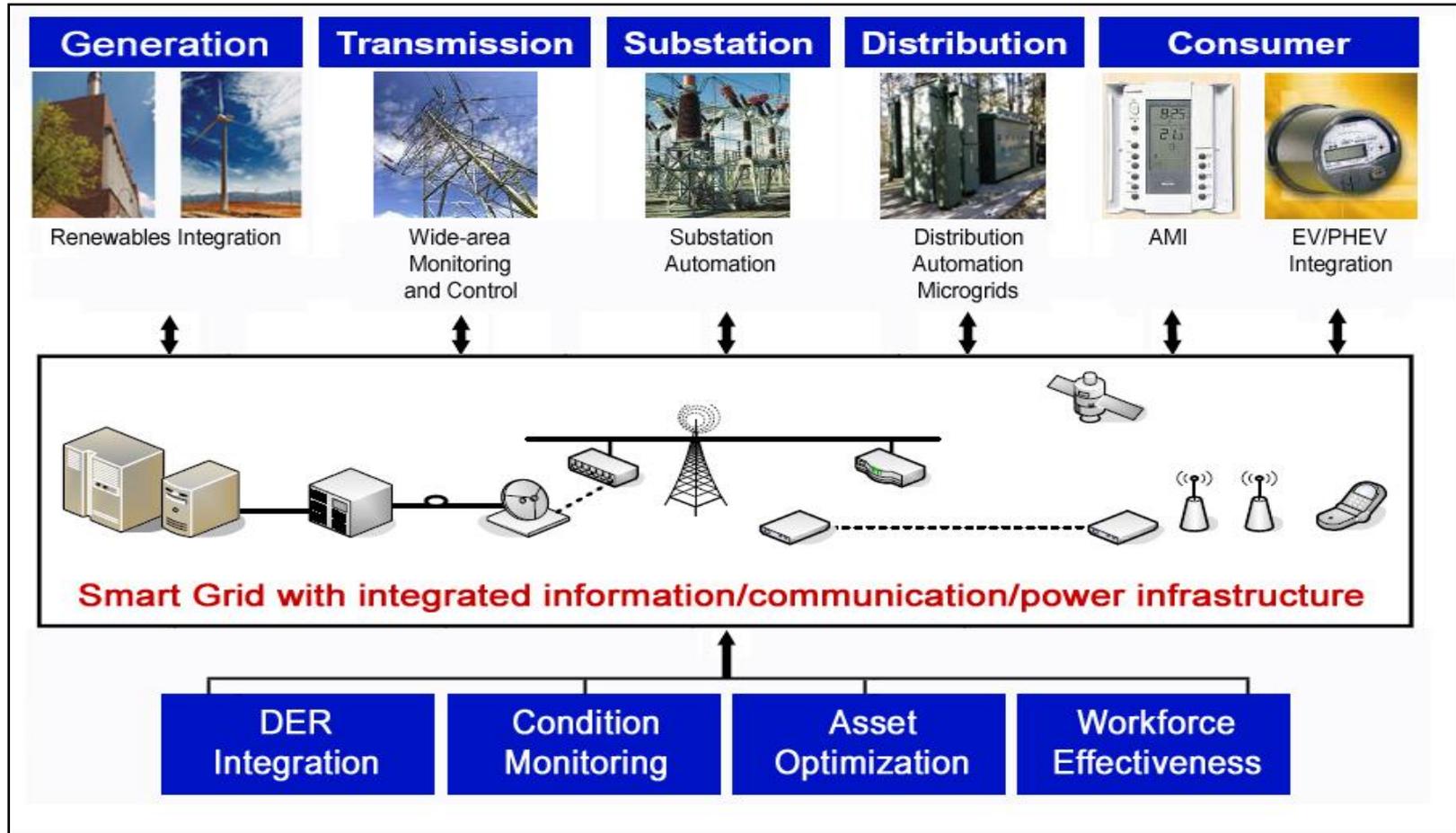


Variable generation resources can create challenges for reliable grid operations



Smart Grid

Integration of Electric Power Delivery with Digital Information, Communications, and Control Technologies



2009 American Recovery and Reinvestment Act provides \$4.5 Billion to *Jumpstart* Smart Grid

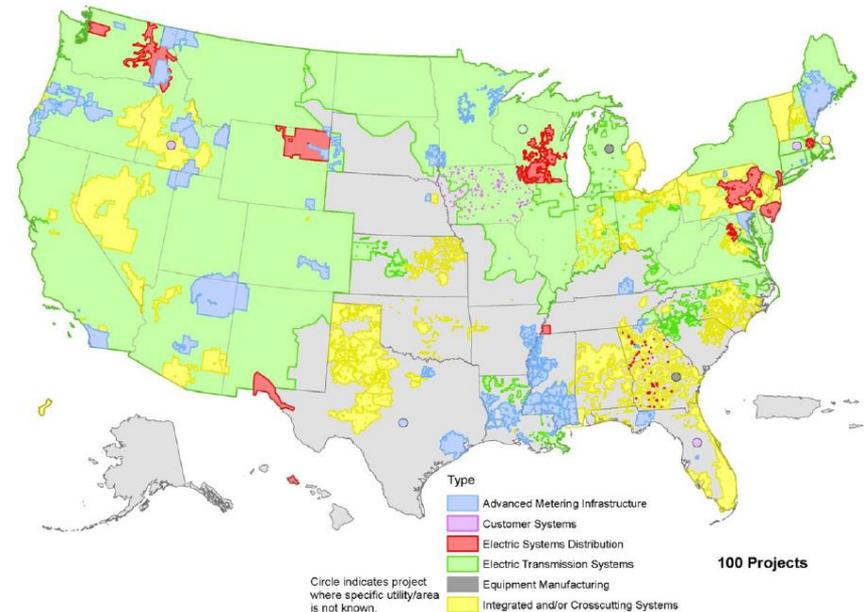
Office of Electricity Delivery and Energy Reliability	\$ Millions
Smart Grid Investment Grant Program; ≤3 years	\$3,400
Smart Grid Demonstrations; 3-5 years	\$615
Interoperability Framework Development by NIST	\$10
Resource Assessment and Interconnection-Level Transmission Analysis and Planning	\$80
State Electricity Regulators Assistance	\$50
Enhancing State Government Energy Assurance Capabilities and Planning for Smart Grid Resiliency	\$55
Workforce Development	\$100

100 Smart Grid Investment Grants

Category	\$ Million
Integrated/Crosscutting	2,150
AMI	818
Distribution	254
Transmission	148
Customer Systems	32
Manufacturing	26
Total	3,429

18 million	smart meters
1.2 million	in-home display units
206,000	smart transformers
177,000	load control devices
170,000	smart thermostats
877	networked phasor measurement units
671	automated substations
100	PEV charging stations

COVERAGE AREA FOR SMART GRID PROJECTS



www.smartgrid.gov

GovEnergy 2010

Cybersecurity - *Critical to Smart Grid Success*

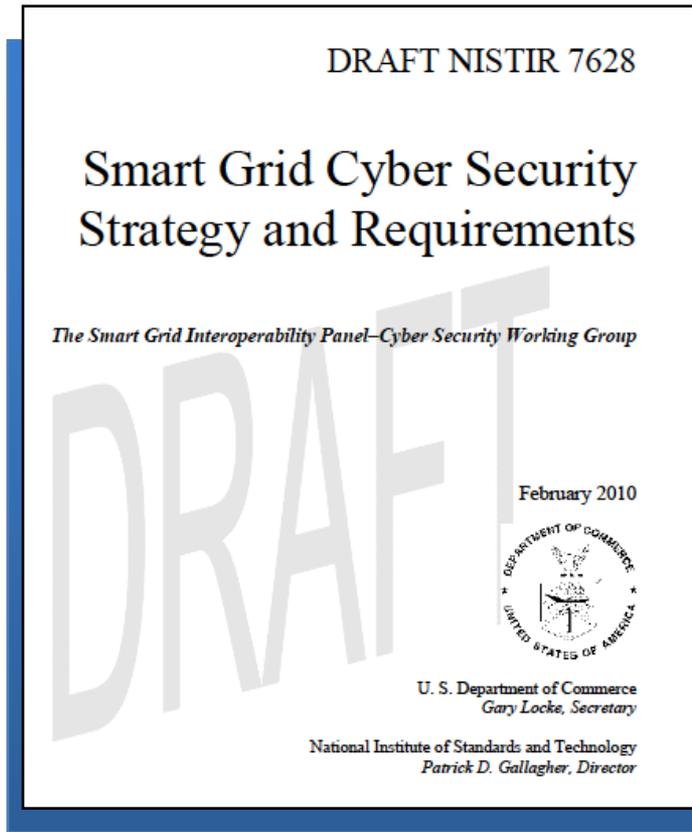
- Organized interagency group (DOE, NIST, FERC, DHS, CIA) to develop cyber security requirements for RFP
- Cyber security plans - major factor in Technical Merit Review
- Utilized technical merit review team and cybersecurity SME team to provide independent reviews
- DOE will work with grantees to ensure cyber security plans are adequate

ARRA Cyber Security Website
www.ARRAsmartgridcyber.net



The screenshot displays the ARRA Cyber Security Website interface. At the top left is the American Recovery & Reinvestment Act logo with the text "RECOVERY.GOV". To the right is a banner image of power lines in a field. Below the banner is a navigation menu with links: "Program Overview", "Register", "Reset Password", and "Security & Privacy". The main content area is divided into two columns. The left column, titled "Training Sections", lists "SMART GRID CYBER TOPICS" (Operational Resilience, Interoperability, Information Sharing) and "CYBER PROGRAM ELEMENTS" (Roles & Responsibilities, Cyber Risk Management & Assessment, Defensive Strategy, Security Controls). The right column, titled "Program Overview", shows a page navigation bar (1-8) and an "Introduction" section. The introduction includes the heading "THE SMART GRID CYBER MISSION" and a bulleted list of core capabilities: "Maintain the capability for timely detection and response", "Mitigate the consequences of a cyber event", "Correct exploited vulnerabilities", and "Restore affected systems, networks and equipment". A small image of a circuit board is shown next to the text. Below the list, a paragraph states: "These core cyber security capabilities will provide assurances that enable resilient next generation Smart Grid capabilities necessary for significant improvements in reliability and efficiency of the bulk power generation and distribution systems allowing a stronger more agile delivery of energy throughout our Nation's critical energy infrastructure."

Guidelines for Smart Grid Cybersecurity

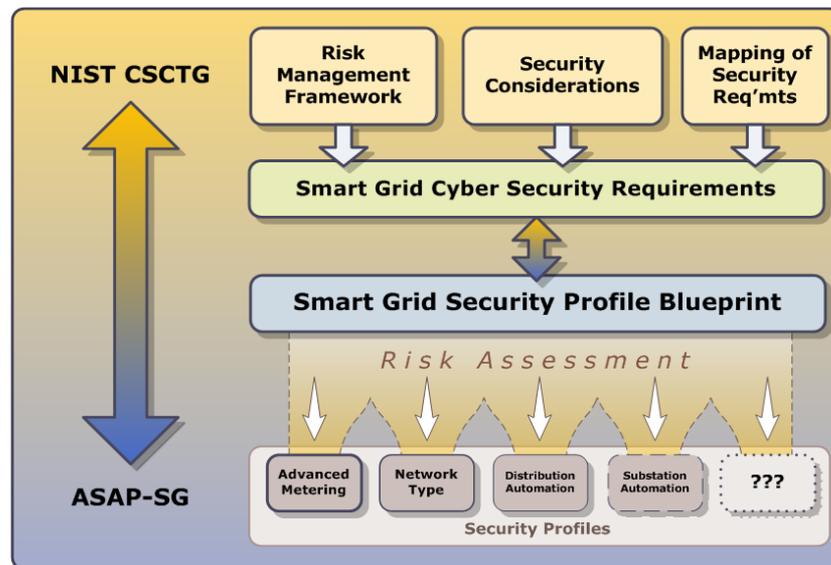


- Final Draft of NIST Interagency Report 7628 v1.0 posted July 2010
- Tool to support research, design, development, and implementation of cybersecurity measures for Smart Grid technologies
- May be used as a guideline to evaluate the overall cyber risks to a Smart Grid system
- Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid.
- Does NOT prescribe particular solutions
- NOT mandatory

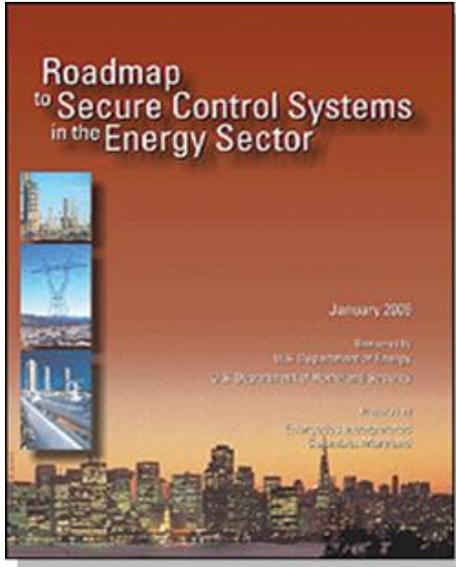
ASAP-SG

Advanced Security Acceleration Project - Smart Grid

- Industry-government collaboration (50/50 cost share) to accelerate security standards development for Smart Grid (May 2009 – till finished)
- Completed *"Security Profile for Advanced Metering Infrastructure, v 1.0"* - major contribution to NISTIR 7628
- Security Profile drafts for 3rd Party Data Access and Distribution Automation completed, HAN getting started
- DOE funding Software Engineering Institute and Oak Ridge National Laboratory working with Enernex
- Industry sponsors
 - American Electric Power
 - Con Edison
 - Consumers Energy
 - Florida Power & Light
 - Southern California Edison
 - Oncor
 - BC Hydro



Roadmap - Energy Sector's Plan for a Resilient Energy Infrastructure



- Energy Sector's synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
 - align activities to a common goal
 - coordinate public and private programs
 - stimulate investments in control systems security
- **2010 Roadmap Update** – address changing technological, operational, and threat environment (e.g., smart grid)

Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to **survive an intentional cyber assault with no loss of critical function.**

DOE Cybersecurity for Energy Delivery Systems Program

(aka National SCADA Test Bed – NSTB)

Key Activities

(designed to achieve Roadmap vision for a Resilient Power Grid)

Next Generation
Control Systems

- Trustworthy Cyber Infrastructure for the Power Grid
- Precompetitive Technologies Development
- Industry-led Technology Development

System Vulnerability
Assessments

- Smart Grid Test and Evaluation Capability
- Cyber Assessments for Next-Generation Control Systems

Integrated Risk
Analysis

- Modeling and Simulation
- Scenario Analysis
- Operational Analysis

Partnership and
Outreach

- Outreach
- Information Sharing
- Advanced Red/Blue Training

DOE National SCADA Test Bed (NSTB) System Vulnerability Assessments - SCADA/EMS

- Created world-class cybersecurity research capabilities, including 6 DOE National Laboratories
- Capability to test and evaluate full-scale SCADA/EMS systems
- Completed assessments of the majority of systems currently being offered in electric sector
- 12 hardened systems developed, 49 now deployed in market



imagination at work

SIEMENS



TELVENT



GovEnergy 2010

Red Team/Blue Team Advanced Training for Energy Sector

- Intensive, hands-on training to **attack** or **defend** a simulated control center
- Realistic control center environment
- Demonstrates control system network exploits
- Teaches how control system attacks are launched, why they work, and potential mitigation
- Uncovers blind spots
- Over 200 energy asset owners and operators have participated



Cybersecurity R&D solutions are being commercialized

- **Hallmark Cryptographic Serial Communication**—a cryptographic card and link module integrating the Secure SCADA Communications Protocol to provide secure serial communications for existing and new energy control systems (*commercialized by SEL, Inc. in 2010*)
- **Lemnos Interoperable Security**—a capability based on open-source specifications—demonstrated in a vendor product—that enables secured interoperability among energy control systems devices (*commercialized by SEL, Inc. in 2010*)
- **Cyber Security Audit and Attack Detection Toolkit**—Bandolier Audit Files for optimizing security configurations and the Portledge event detection capability for energy control systems (*Files now available via open source by Digital Bond, Inc.*)
- **ANTFARM** —Advanced Network Toolkit for Assessments and Remote Mapping, a free, open source tool to map and visualize control systems networks, a critical step in meeting the NERC CIP standards. Developed by Sandia National Laboratories.

Game-changing R&D Needed to Make *Survivable* Systems a Reality

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

Vision: Architecture for End-to-End Resilient, Trustworthy & Real-time Cyber Infrastructure for the Power Grid

Recent Papers

Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

Katherine M. Rogers, Student Member
Member, IEEE

Abstract—At the residential level, devices which now and expected in the future have the ability reactive power support. Inverters which connect generation such as solar panels and pluggable by vehicles (PHEVs) to the grid are an example. Such not currently utilized by the power system. We in integration of these end-user reactive-power-capable provide voltage support to the grid via a secure can infrastructure. We show how to determine effective the transmission system and how to control resources at those locations. We also discuss how reactive support groups which parallel the regions communications architecture that is presented. Our goal is to present how the Smart Grid can allow the available end-user devices as a resource to mitigate problems such as voltage collapse.

Index Terms—reactive power resources, cv voltage control, real-time sensitivity analysis

I. INTRODUCTION

Power system operation is currently constrained, and often by low-voltage voltage contingency is a "what if" scenario that utilize the operational reliability of the power system regularly run a series of contingencies in a process contingency analysis. Under normal conditions, it operated so that it can withstand the loss of any [1] or one credible contingency. The ability of withstand a list of "credible" disturbances or cont defined to be operational reliability, but was previ security [2]. This means that for any single cont steady-state analysis converges to a solution th result in any limit violations in the post contin state. However, as power systems become m loaded, they are pushed closer to their operating this can result in an increase in the number of lit and unsolvable contingencies. In the case of a contingency, the effects of the real-world outag modeled by the steady-state power flow equations.

The authors would like to acknowledge the support of the supp through its grant CNS-0524695, the Power System Engineering Center (PSEERC), and the Grainger Foundation. The authors we thank U.S. Congressman Bill Foster who motivated the idea b paper. The authors are with the University of Illinois Urbana-Champa 61801 (e-mail: kmg@uiuc.edu, kmg@pseerc.uiuc.edu, kmg@uiuc.edu, kmg@uiuc.edu, kmg@uiuc.edu).

Smart-Grid Security Issues

The North American electric power grid is a highly interconnected system, considered by many as one of the 20th century's greatest engineering feats. Still, changing power supply and demand are motivating changes in this system; this ongoing

modernization is often called the "smart grid." This process has many drivers, such as reliability and efficiency, and many potential benefits—for example, minimizing climate impact by making it easier to incorporate renewable energy sources such as geothermal and wind power, and increased consumer participation. However, these improvements will incur increased risk. Some risk will be tied to tighter incorporation of the digital-communications and computer infrastructure with the existing physical infrastructure, with all the inherent vulnerabilities. Other risk comes from changes in how power companies and consumers interact. Here we describe some looming changes and highlight security issues related to the infrastructure's digital element.

However, these improvements will incur increased risk. Some risk will be tied to tighter incorporation of the digital-communications and computer infrastructure with the existing physical infrastructure, with all the inherent vulnerabilities. Other risk comes from changes in how power companies and consumers interact. Here we describe some looming changes and highlight security issues related to the infrastructure's digital element.

A Look at Smart Grids

The smart grid (see Figure 1) uses intelligent transmission and distribution networks to deliver electricity. This approach aims to improve the electric system's reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning.



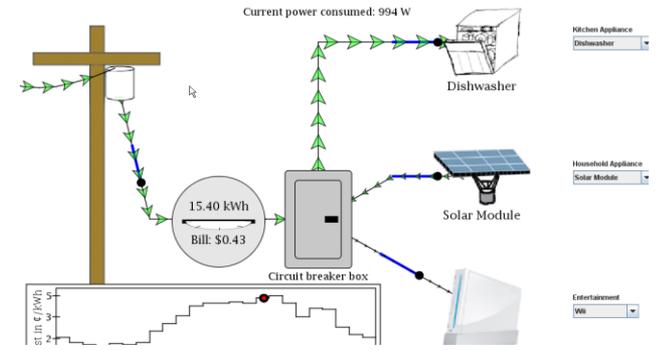
Building Security In
Editors: John Stevens, jstevens@uiuc.edu
Gusmar Peterson, gusmar@arcetgroup.net
Deborah A. Finnick, deborah.finnick@ipf.uiuc.edu

HANANBU KHURANA, University of Illinois at Urbana-Champaign

MARK HADLEY, NING LI, AND DIJIBOYA A. FERDINAND Pacific Northwest National Laboratory

facilitate many resources and applications, including smart meters, standards, and protocols. The smart grid is poised to transform a centralized, producer-controlled network to a decentralized, consumer-interactive network that is supported by fine-grained monitoring. For example, consumers react to price signals (that is, supply) with the help of smart meters to achieve active load management. On the monitoring side, old metering data recorded hourly or monthly is replaced by a smart meter that collects data every minute. Similarly, current supervisory control and data acquisition (SCADA) systems collect one data point every 1 to 2 seconds, whereas phase measurement units (PMUs) collect 30 to 60 data points per second.

Applets for Schools



NetAPT Network Access Policy Tool (adopted by utility in Spring 2010)

Policy Name	Constraint Name	Description
PCS Services accessible from the outside	SQL Service on PCS Historian accessible f	SQL Service on PCS Historian accessible f
	SQL Service on PCS Historian accessible f	SQL Service on PCS Historian accessible f
	Honeywell PHD Historian	



University of Illinois • Dartmouth College
University of California at Davis • Washington State University

GovEnergy 2010

Path Forward - No Silver Bullet!



Source:



Sandia
National
Laboratories

THANK YOU!