Smart Grids: Toward a More Resilient, Secure, and Modern Infrastructure

S. Massoud Amin, D.Sc.
Director, & Endowed Chair, Technological Leadership Institute
Professor of Electrical & Computer Engineering
University Distinguished Teaching Professor
University of Minnesota

Chairman, IEEE Smart Grid
Chairman, Board of Directors, Texas Reliability Entity (TRE)
Director, Board of Directors, Midwest Reliability Organization (MRO)

Keynote address at the 47th Annual Frontiers of Power Conference
Stillwater, OK, Monday, October 27, 2014

* Support from EPRI, NSF, ORNL, Honeywell and SNL is gratefully acknowledged.

Context: US Energy Supply Since 1850

Energy Security: System of Systems
The Energy Crises Taught Us Interdependency

S. Massoud Amin's Congressional briefing's on March 26 and Oct. 15, 2009, and November 2013

Transforming Society

The vast networks of electrification are the greatest engineering achievement of the 20th century
– U.S. National Academy of Engineering

© 2014 No part of this presentation may be reproduced in any form without prior authorization.
Smart Grid: Integrate Dispersed Energy Sources into a Modern Grid to Provide Energy to Centers of Demand

Recommendations for moving to energy systems to meet demand of tomorrow

- **Build a stronger and smarter electrical energy infrastructure**
  - Transform the Network into a Smart Grid
  - Develop an Expanded Transmission System
  - Develop Massive Electricity Storage Systems

- **Break our addiction to oil by transforming transportation**
  - Electrify Transportation: PHEVs and EVs
  - Develop and Use Alternative Transportation Fuels

- **Green the electric power supply**
  - Expand the Use of Renewable Electric Generation
  - Expand Nuclear Power Generation
  - Capture Carbon Emissions from Fossil Power Plants

- **Increase energy efficiency**

- **With full cyber and physical security**

---

Evolution of Smart Grid Programs at DOE and EPRI

- **EPRI Common Information Model (CIM) for Energy Management Systems (EMS)**
- **EPRI Utility Communication Architecture (UCA) for Substation Automation**
- **EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI), including Self-healing Smart Grid**
- **EPRI Intelligrid Architecture**
- **Smart Grid Demonstration Projects**

---

The Smart Grid: 15 Years in the Making

    - 52 utilities and ISO (including TVA, ComEd/Exelon, CA-ISO, ISO-NE, etc..) provided feedback; 24 resultant technologies extracted.

- **Intelligrid (2001-present): EPRI trademarked**
- **Smart Grid: Final name adopted at EPRI and DOE**

---

Definition: Smart Self-Healing Grid


- **What is a Smart Self-healing grid?**
  The term “smart grid” refers to the use of computer, communication, sensing and control technology which operates in parallel with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, and facilitating the interconnection of new generating sources to the grid.

- **What are the power grid’s emerging issues? They include**
  1) integration and management of DER, renewable resources, and “microgrids”;
  2) use and management of the integrated infrastructure with an overlaid sensor network, secure communications and intelligent software agents;
  3) active-control of high-voltage devices;
  4) developing new business strategies for a deregulated energy market; and
  5) ensuring system stability, reliability, robustness, security and efficiency in a competitive marketplace and carbon constrained world.
Definition: Smart Self-Healing Grid

- What is “self healing”?  
  - A system that uses information, sensing, control and communication technologies to allow it to deal with unforeseen events and minimize their adverse impact

- Why is self healing concept important to the Electric Power Grid and Energy Infrastructure?  
  - A secure “architected” sensing, communications, automation (control), and energy overlaid infrastructure as an integrated, reconfigurable, and electronically controlled system that will offer unprecedented flexibility and functionality, and improve system availability, security, quality, resilience and robustness.

Smart Grid... “The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming - and interconnected with everything else.”

Energy Independence and Security Act


- “It is the policy of the United States to support the modernization of the Nation’s electricity transmission and distribution system … that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:
  1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
  2. Dynamic optimization of grid operations and resources, with full cyber-security…”

Smart Grid Definitions

<table>
<thead>
<tr>
<th>FERC</th>
<th>“Grid advancements will apply digital technologies to the grid and enable real-time coordination of information from both generating plants and demand-side resources.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOE</td>
<td>“A smarter grid applies technologies, tools, and techniques available now to bring knowledge to power – knowledge capable of making the grid work far more efficiently…”</td>
</tr>
<tr>
<td>GE</td>
<td>“The Smart Grid is in essence the marriage of information technology and process-automation technology with our existing electrical networks.”</td>
</tr>
<tr>
<td>IEEE</td>
<td>“The term ‘Smart Grid’ represents a vision for a digital upgrade of distribution and transmission grids both to optimize current operations and to open up new markets for alternative energy production.”</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>“A Smart Grid delivers electricity from suppliers to consumers using digital technology to save energy, reduce cost, and increase reliability.”</td>
</tr>
</tbody>
</table>

- Functionality
  - Common themes:
    - Technology
      - Two-way communication
      - Advanced sensors
      - Distributed computing
    - Reliability
      - Interconnectivity
      - Renewable integration
      - Distributed generation
    - Efficiency
      - Demand response
      - Consumer savings
      - Reduced emissions
**Smart Self-Healing Grid**

**THE SOLUTION: A SMART GRID THAT HEALS ITSELF**

Enabling the Future - Infrastructure integration of microgrids, diverse generation and storage resources into a secure system of a smart self-healing grid.

- **Smart appliances**
  - Can shut off in response to frequency fluctuations.

- **Demand management**
  - Use can be shifted to off-peak times to save money.

- **Storage**
  - Energy generated at off-peak times can be stored in batteries for later use.

**Smart Grid**

Highly Instrumented with Advanced Sensors and Computing

- Engaging Consumers
- Enhancing Efficiency
- Ensuring Reliability
- Enabling Renewables & Electric Transportation

Interconnected by a Communication Fabric that Reaches Every Device

Enabling the Future - A vision for the future — a network of integrated microgrids that can monitor and heal itself.


© 2014 No part of this presentation may be reproduced in any form without prior authorization.
Dynamics of Power System Operating States

- **Normal:**
  - Objective: Load tracking, cost minimization, system coordination
  - Secure

- **Restorative:**
  - Resynchronization
  - Insecure

- **Alert:**
  - Preventive Control
  - Secure

- **Emergency:**
  - Heroic Action
  - A-Secure

**System not intact**

**System intact**

---

Critical System Dynamics and Resilience Capabilities

- **Anticipation of disruptive events**

- **Look-ahead simulation capability**

- **Fast isolation and sectionalization**

- **Adaptive islanding**

- **Self-healing and restoration**

Re-sil-i-ence, noun, 1824: The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress; An ability to recover from or adjust easily to misfortune or change.

Resilience enables "Robustness": A system, organism or design may be said to be "robust" if it is capable of coping well with variations (internal or external and sometimes unpredictable) in its operating environment with minimal damage, alteration or loss of functionality.
Sensing and Control Strategies

- Centralized
- Distributed
- Perfectly decentralized

Self-Healing Grid

- Dependability/Robustness
- Self-Healing
- (min-hours)
- Vulnerability Assessment Agents
- Reconfiguration Agents
- Planning Agents
- Restoration Agents

Autonomy/Fast Control (msec)

- Event/Alarm Filtering Agents
- Fault Isolation Agents
- Protection Agents
- Inhibitor Signal Controls
- Generation Agents

EPR/DoD CIN/S Initiative

Past Scheme vs. New Scheme
Context: IT interdependencies and impact
Source: Massoud Amin, “Toward a Secure and Smart Self-Healing Grid,” presentation to the Strategic Science & Technology EPRI Research Advisory Committee (RAC), Tuesday, January 27, 1998

Dependence on IT: Today’s systems require a tightly knit information and communications capability. Because of the vulnerability of Internet communications, protecting the system will require new technology to enhance security of power system command, control, and communications.

Increasing Complexity: System integration, increased complexity: call for new approaches to simplify the operation of complex infrastructure and make them more robust to attacks and interruptions.

Centralization and Decentralization of Control: The vulnerabilities of centralized control seem to demand smaller, local system configurations. Resilience rely upon the ability to bridge top-down and bottom-up decision making in real time.

Assessing the Most Effective Security Investments: Probabilistic assessments can offer strategic guidance on where and how to deploy security resources to greatest advantage.
**Smart Grid: Tsunami of Data Developing**

- New devices in the home enabled by the smart meter
- Programmable Communicating Thermostat Come On-line
- AMI Deployment
- Distribution Management Rollout
- GIS System Deployment
- OMS Upgrade
- Mobile Data Goes Live
- Substation Automation System
- Workforce Management Project

---

**Tremendous amount of data coming from the field in the near future**

- paradigm shift for how utilities operate and maintain the grid

---

**Smart Grid Protection Schemes & Communication Requirements**

<table>
<thead>
<tr>
<th>Type of relay</th>
<th>Data Volume (kb/s)</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Present Future</td>
<td>Primary (ms) Secondary (s)</td>
</tr>
<tr>
<td>Over current protection</td>
<td>160 2500</td>
<td>4-8  0.3-1</td>
</tr>
<tr>
<td>Differential protection</td>
<td>70  1100</td>
<td>4-8  0.3-1</td>
</tr>
<tr>
<td>Distance protection</td>
<td>140  2200</td>
<td>4-8  0.3-1</td>
</tr>
<tr>
<td>Load shedding</td>
<td>370  4400</td>
<td>0.06-0.1 (s)</td>
</tr>
<tr>
<td>Adaptive multi terminal</td>
<td>200  3300</td>
<td>4-8  0.3-1</td>
</tr>
<tr>
<td>Adaptive out of step</td>
<td>1100 13000</td>
<td>Depends on the disturbance</td>
</tr>
</tbody>
</table>

---

**Trends: Resilience and Asset Investments***

- **Achieving Electric System Resilience**
  - Energy Sector is uniquely critical infrastructure as it provides an “enabling function”
    - Aging Infrastructure **Investment**
    - Reliability/Hardening **Investment** – Outage cost of $125B/y (DOE), with weather-related ~ ($18B - $33B)/y
    - Natural Gas, Renewable Microgrids, Electric Vehicles, Storage, and Demand response **Investment**
    - Electrical – Natural Gas Interdependency

- **Source:** IEEE QER Report, Chap. 4, October 2014

---

**Many challenges facing the energy and power infrastructure**

- Aging assets
- Severe weather events
- Physical and cyber attacks
- Dependencies and inter-relationships with other infrastructures (gas, telecommunications, etc)
- Market and policy including recovery of investments
**Holistic Asset Management**

**Asset management: Predictability of Cost & Reliability**

- As system ages, operating cost increases and reliability decrease – limited resources for wholesale replacements
- How to manage Smart Grid assets?
- Need for sound strategy for controlling the symptoms of aging within the utility’s overall business plan – maintain accepted levels of performance

**Overview**

- Microgrids
  - U of M - Morris campus project
  - UMore Park Project
  - Controller architecture
  - Resiliency
  - Dollars and watts – Prices to devices
  - Storage and Renewables integration
  - Autonomous Microgrids
  - Big Data

- Smart Grid U™
- MN Smart Grid Coalition (2008-11) /Governor’s Summit ‘14
- IEEE Smart Grid
- Discussion

**Smart Grids: What are we working on at the University of Minnesota?**

- Integration and optimization of storage devices and PHEVs with the electric power grid
- Grid agents as distributed computer
- Fast power grid simulation and risk assessment
- Security of cyber-physical infrastructure: A Resilient Real-Time System for a Secure & Reconfigurable Grid
- Security Analyses of Autonomous Microgrids: Analysis, Modeling, and Simulation of Failure Scenarios, and Development of Attack-Resistant Architectures

*University of Minnesota Center for Smart Grid Technologies (2003-present)*
Faculty: Professors Massoud Amin and Bruce Wollenberg
PhD Candidates/RA and Postdocs: Anthony Giacomoni (PhD'11), Jesse Gantz (MS'12), Laurie Miller (PhD'13), Vamsi Parachuri (part-time PhD candidate, full-time at Siemens), Sara Mullen (PhD'09)
PI: Massoud Amin, Support from EPRI, NSF, ORNL, Honeywell and SNL

**Our team’s Smart Grid Research**
Smart Grid Interdependencies
Security, Efficiency, and Resilience

Building a super computer from many small processors
- The IBM Blue Gene computer

Up to 65,536 processors

Fast Power Systems Risk Assessment
Doctoral Dissertation: Laurie Miller (June 2005-present)
ORNL contract, the U of MN start-up fund (2005-2008), and NSF grant (2008-2009), PI: Massoud Amin

Connection Machine 2: $5 million in 1987, only a few dozen made
NVIDIA Tesla C870: $1300 in 2009, over 5 million sold

Fast Power Grid Simulation
- Use Nvidia GeForce GPU card to gain 15 times faster power flow calculation on PC (Laurie Miller)
Example of In Depth Analysis: Critical Contingency Situations

Critical Root Causes in the Proba/Voltage Impact State space (Region Cause: all, Affected Region: all)

Most significant root cause

Cybersecurity
Changing Risks

Cyberspace  Cyber Activism

Cyber Insurance  Cyber War  Cyberattack

Cyber-Alert  Cyber Bullying

Cyber-ethics  Cyber crime  Cyber FININT

Cyberpower  Cyber Espionage

Cyber-Commerce  Cyber Law

Cybersecurity  Cyber Communication
Bulk Electric System (BES) Reliability Oversight Is a Shared Responsibility

- FERC has regulatory jurisdiction over transmission tariffs, wholesale market rules and BES reliability standards
  - State regulators are engaged and very influential but do not have direct authority over the Bulk Electric System
  - Interstate Commerce per US Supreme Court
  - States have authority for siting of transmission lines
- NERC develops and enforces FERC approved mandatory reliability standards
- RTOs and all “users, owners and operators of the bulk power system” are bound by FERC/NERC standards and regulations

Utilities and Market Participants

NERC
North American Electric Reliability Corporation

FERC
Federal Energy Regulatory Commission

RTOs
(Regional Transmission Organizations)
(PJM, MISO, ISO-NE, etc)

October 2013-2014: A Year in Review

- December 19th→ Target Corp. announces cyber breach
disclosed to the public
- February 12th→ NIST announces industry voluntary standards for cybersecurity entitled “Framework for Improving Critical Infrastructure Cybersecurity”
- March 19th→ eBay announces cyber intrusion, urges customers to change passwords
- April 7th→ Heartbleed bug

As of 9/2/2014, there have been:

- 521 Total breaches (across all sectors)
- 17,829,689 (over 17 million) exposed records
- Government/Military experienced 10.6% of total breaches
- Medical/Healthcare category experienced 42.6% of total breaches
- Business category experienced 35.3% of total breaches


Energy Sector Vulnerability

- 41% of reported cyber security incidents between Oct 2011 and Sept 2012 were in the energy sector (DHS report)
- An attack on a Saudi Arabian oil company last summer wiped data from 30,000 computers.
- Two generators recently reported to have suffered cyber attacks; one knocked the plant out for three weeks.
- DOD engaging in 5-fold expansion of cyber security
  - Offensive and defensive postures
- Canadian Government doubling cyber expenditures

Source: Industrial Control Systems Cyber Emergency Response Team
Electric Terrorism: Grid Component Targets 1994–2004

What to look forward to today

- The Evolving Threat Landscape
- What the Cyber Security Crisis Means for American Business
- Year of the Large Scale Breach “Crimeware as a Service”
- Liability
- Cyber Security: A Team Effort

Infrastructure Security

A “Sanitized” Example: Lack of awareness and inadvertent connection to the Internet

- Power plant: 2-250MW, gas fired turbine, combined cycle, 5 years old, 2 operators, and typical multi-screen layout:
  - A: do you worry about cyber threats?
  - Operator: No, we are completely disconnected from the net.
  - A: That’s great! This is a peaking unit, how do you know how much power to make?
  - Operator: The office receives an order from the ISO, then sends it over to us. We get the message here on this screen.
  - A: Is that message coming in over the internet?
  - Operator: Yes, we can see all the ISO to company traffic. Oh, that’s not good, is it?”
September 11, 2001 Tragedies

Electric industry may lead pack in disaster safeguards

By David Wagman
dwagman@iefenergy.com

Massoud Amin, a mathematician with EPRI, was attending a disaster risk management workshop outside Washington, D.C., Sept. 11 when pagers and cell phones began going off in the room.

The workshop, whose attendees included White House and Department of Defense (DOD) officials, quickly ended with word of the World Trade Center and Pentagon attacks.

"It was indeed ironic that we were engaged at the very moment of the attack in a conference attempting to find realistic technical ways to mitigate disaster," said Amin.

What is even more ironic is that the DOD late last year opted to stop funding its $80 million, five-year project Amin is leading on behalf of EPRI to design a "self-healing" electric transmission network. The DOD money ran out Friday at the end of the current federal fiscal year.

SCADA Systems are Vulnerable

- Past failures
- Increasing threats
- Little security in place

Large Utility Challenges

- Large upfront cost
- Long implementation times
- Greater complexity of systems

Evolution of Electrical Utility Threats

<table>
<thead>
<tr>
<th>PAST</th>
<th>HARD-WIRED CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Most controls are “hard wired” AND require manual intervention</td>
</tr>
<tr>
<td></td>
<td>Lesser public availability of “hacking” devices</td>
</tr>
<tr>
<td></td>
<td>Little capability for damage to, or financial benefit from, attacks</td>
</tr>
<tr>
<td></td>
<td>Cost-plus utility charging – “If we need it, we’ll do it! If we can’t do it, we’ll buy it!”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRESENT</th>
<th>SCADA / RF ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intense financial pressure to reduce staffing; hence more “remote” management</td>
<td></td>
</tr>
<tr>
<td>Computerization and RF control common in all industries</td>
<td></td>
</tr>
<tr>
<td>Project implementation excellence not always followed by outstanding security operations</td>
<td></td>
</tr>
<tr>
<td>SCADA hacking can cause “wholesale” damage to neighborhoods and equipment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NEAR FUTURE</th>
<th>SMART GRID / RF PERVERSIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control inside-the-home of all appliances</td>
<td></td>
</tr>
<tr>
<td>Wide use of 802.x, ZigBee, X10 methodologies</td>
<td></td>
</tr>
<tr>
<td>Uncertain Software Provenance, Packaged Code and Offshore Development Zero-Day Attacks</td>
<td></td>
</tr>
<tr>
<td>Increased organized crime/terrorist focus</td>
<td></td>
</tr>
<tr>
<td>Potential for damage to, and “net” theft by, every customer</td>
<td></td>
</tr>
<tr>
<td>Revenue/Risk Asymmetry for each customer</td>
<td></td>
</tr>
<tr>
<td>Transition to IP and Windows “Monoculture” for RF devices</td>
<td></td>
</tr>
</tbody>
</table>

What’s out there?

- Google News
- Google Scholar
- IEEE Xplore
- IEEE Standards
- University of Minnesota Library
- Electric Power Research Institute (EPRI)
- National Academies Press
- North American Electric Reliability Corporation (NERC)
- Federal Energy Regulatory Commission (FERC)
- Executive Orders and Presidential Directives Department of Homeland Security
- National Institute of Standards and Technology (NIST)
- SANS Institute
- Minnesota Public Utilities Commission
- Recent dissertation submissions
- Various vendor sources
- Discussions with subject matter experts

Evolution of Electrical Utility Threats
Thus There are Multiple Scenarios to Plan For...

- **External Threat**
  - Power failures
  - Natural disasters
  - Economic upheaval
  - Malware
  - Denial of service
  - Sophisticated, organized attacks

- **Inadvertent**
  - Unpatched systems
  - Code vulnerability
  - Lack of change control
  - Human error or carelessness

- **Deliberate**
  - Developer-created back door
  - Information theft
  - Insider fraud

**Insider Threat**

- **Power failures**
- **Natural disasters**
- **Economic upheaval**
- **Malware**
- **Denial of service**
- **Sophisticated, organized attacks**

CIP programs in the industry

Real world solutions may be elusive

- **Functionality and Mission Objectives**
- **Multiple Hazard Spectrum**
- **Life Safety Issues**
- **Business Contingency Planning**
- **Cost**

Prioritization: Security Index

<table>
<thead>
<tr>
<th>Category</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>Corporate culture, Security Program, Employees, Emergency and threat response capability</td>
</tr>
<tr>
<td><strong>Physical</strong></td>
<td>Requirements for facilities, equipment and lines of communication, Protection of sensitive information</td>
</tr>
<tr>
<td><strong>Cyber and IT</strong></td>
<td>Protection of wired and wireless networks, Firewall assessments, Process control system security assessments</td>
</tr>
</tbody>
</table>
Assessment & Prioritization:
A Composite Spider Diagram to Display Security Indices

Importance of Control Systems and Technology

- Control and telecommunications systems are an integral part of the grid
  - Outage notification and analysis
  - Work scheduling
  - Scenario modeling
  - Automated switching
  - Control of new technologies like PEVs and distributed generation

Power Grid Vulnerabilities

- Physical:
  - Over 450,000 miles of 100kV or higher transmission lines, and many more thousands of miles of lower-voltage lines
  - Natural disasters or a well-organized group of terrorists can take out portions of the grid as they have done in the U.S., Colombia, and other countries
  - Effects typically confined to the local region.

- Open-Source Information:
  - Analysts have estimated that public sources could be used to gain at least 80% of information needed to plot an attack

Utility Telecommunications

- Electric power utilities usually own and operate at least parts of their own telecommunications systems
- Consist of backbone fiber optic or microwave connecting major substations, with spurs to smaller sites

- Media:
  - Fiber optic cables
  - Digital microwave
  - Analog microwave
  - Multiple Address Radio (MAS)
  - Spread Spectrum Radio
  - VSAT satellite
  - Power Line Carrier
  - Copper Cable
  - Leased Lines and/or Facilities
  - Trunked Mobile Radio
  - Cellular Digital Packet Data (CDPD)
  - Special systems (Itron, CellNet)
Threat Evolution: Malicious Code

- **Class III**
  - Human response: impossible
  - Automated response: possible
  - "Flash" Threats

- **Class II**
  - Human response: difficult/impossible
  - Automated response: possible
  - "Warhol" Threats

- **Class I**
  - Human response: possible

Blended Threats

- File Viruses
- Macro Viruses
- e-mail Worms

Contagion Timeframe
- Seconds
- Days
- Months
- Early 1990s, Mid 1990s, Late 1990s, 2000, 2003

Context: Threats to Security Sources of Vulnerability

- Transformer, line reactors, series capacitors, transmission lines...
- Protection of ALL the widely diverse and dispersed assets is impractical
  - over 215,000 miles of HV lines (230 kV and above)
  - 6,644 transformers in Eastern Interconnection
- Control Centers
- Interdependence: Gas pipelines, compressor stations, etc.; Dams; Rail lines; Telecom – monitoring & control of system
- Combinations of the above and more using a variety of weapons:
  - Truck bombs; Small airplanes; Gun shots
  - line insulators, transformers; more sophisticated modes of attack...

Smart Grid Vulnerabilities

- **Cyber:**
  - Existing control systems were designed for use with proprietary, stand-alone communications networks
  - Numerous types of equipment and protocols are used
  - More than 90% of successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices
  - Possible effects of attacks:
    1) Loss of load
    2) Loss of information
    3) Economic loss
    4) Equipment damage

New Challenges for a Smart Grid

- **Need to integrate:**
  - Large-scale stochastic (uncertain) renewable generation
  - Electric energy storage
  - Distributed generation
  - Plug-in hybrid electric vehicles
  - Demand response (smart meters)

- **Need to deploy and integrate:**
  - New Synchronized measurement technologies
  - New sensors
  - New System Integrity Protection Schemes (SIPS)

- **Critical Security Controls**
Control Systems Overview

Three main components

- SCADA Master Station/Control Center
- Comm. Links
- Remote Substation

- HMI/SCADA Master
- External Control Points

- Radio Microwave Spread-spectrum
- Twisted-pair Fiber-optics
- Dial-up Leased line

- Remote Terminal Unit (RTU)
- Intelligent Electronic Devices

- Actuator
- Meter
- Accumulator
- Programmable Logic Controller (PLC)

Power and Control Systems

The energy industry uses "Supervisory Control and Data Acquisition (SCADA)" networks. SCADA systems are complex event driven systems with centralized monitoring of thousands of remotely managed points of process control equipment.

This information infrastructure forms a grid of its own - a control grid.

Control Grids are rapidly adopting IP addressable solutions to promote corporate connectivity for remote access of equipment.

Smart Grid implies overhauling both the Power system infrastructure and the Information/Controls.
Technical Threats are Already Widespread

- SCADA (Supervisory Control And Data Access) systems already control most “bulk” electrical distribution
- These often have used poorly-secured cellphone and radio links for various readings and controls
- Both SCADA and AMI have occasioned numerous lurid security stories in the press

http://www.breitbart.com/article.php?id=D97EJPBG1&show_article=1
http://www.hstoday.us/content/view/4951/92/
http://www.scmagazineus.com/Power-surge-SCADA-industry-must-prep-for-attacks/article/120416/
http://www.foxnews.com/story/0,2933,511648,00.html

Cyber Threats to Power Grid Infrastructure

- Protocol Attacks
- Coordinated Attacks
- Intrusions
- Malware
- Denial of Service (DoS)

Cyber-Based Attacks

- Protocol Attacks
- Coordinated Attacks
- Intrusions
- Malware
- Denial of Service (DoS)

Threats to Critical Infrastructures
(Power Grid, Oil & natural gas, Water distribution, Transportation, ..)

[General Accounting Office, CIP Reports, 2004 -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.

What Can They Do and How Can They Do It?

- Information Leakage
- Integrity Violation
- Denial of Service
- Illegitimate Use

Eavesdropping
Traffic Analysis
EM/RF interception
Indiscretions by Personnel
Media Scavenging

Penetration
Masquerade
Bypassing Controls
Authorization Violation
Physical Intrusion

Planting
Trojan Horse
Trapdoor
Service Spoofing

Information Leakage
Integrity Violation
Theft
Replay

Resource Exhaustion
Integrity Violation

Electric Company Vulnerability Assessment

- Conducted by 4 National Labs and consultant
- Able to assemble detailed map of perimeter
- Demonstrated internal and end-to-end vulnerabilities
- Intrusion detection systems did not consistently detect intrusions
- X-Windows used in unsecured manner
- Unknown to IT, critical systems connected to internet
- Modem access obtained using simple passwords

Much of the above determined from over 1200 miles away
The world of cybersecurity

<table>
<thead>
<tr>
<th>Threats</th>
<th>Targets</th>
<th>Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity theft</td>
<td>Government (Federal, State, and Local); e.g.,</td>
<td>Cyber workforce</td>
</tr>
<tr>
<td>Information manipulation</td>
<td>- E-Government</td>
<td>Advanced network and</td>
</tr>
<tr>
<td>(e.g., Malware)</td>
<td>- E-Commerce</td>
<td>resilience controls</td>
</tr>
<tr>
<td>Cyber Assaults/Bullying</td>
<td>Industry; e.g.,</td>
<td>Outbound traffic monitoring</td>
</tr>
<tr>
<td>Advanced Persistent Threats (APTs)</td>
<td>- Aerospace &amp; Defense</td>
<td>Dynamic situational</td>
</tr>
<tr>
<td>Information theft</td>
<td>- Banking &amp; finance</td>
<td>awareness</td>
</tr>
<tr>
<td>Crime (e.g., Credit card fraud)</td>
<td>- Health care</td>
<td>Open source Information</td>
</tr>
<tr>
<td>Insider</td>
<td>- Insurance</td>
<td>Risk intelligence &amp;</td>
</tr>
<tr>
<td>Espionage</td>
<td>- Manufacturing</td>
<td>management</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>- Oil &amp; Gas</td>
<td>- Forensic analysis</td>
</tr>
<tr>
<td>Transnational</td>
<td>- Power Grid</td>
<td>- Data analytics</td>
</tr>
<tr>
<td>Attack of software</td>
<td>- Retail</td>
<td>Financial intelligence</td>
</tr>
<tr>
<td>“boomerangs”</td>
<td>- Telecommunications</td>
<td>(FININT)</td>
</tr>
<tr>
<td>Terrorism</td>
<td>- Utilities</td>
<td>- Tighter laws &amp; enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--------------------------</td>
</tr>
<tr>
<td>You should assume that your information network has been or will be compromised.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What global experts are thinking about cybersecurity…

- 54% doubt their organization is capable of defending itself against a sophisticated cyber attack
- 61% anticipate the impact of losing global connectivity for an extended period of time to be catastrophic with irreversible consequences
- 66% think home users need to take more responsibility for cybersecurity
- 66% view their government’s maturity as low regarding international cooperation
- 66% a “treaty on cyber warfare” is needed or is overdue
- 69% doubt their country could defend against a sophisticated cyber attack
- 70% believe that international policies and regulations are far behind technology advances

Security needs

- Physical Security
  - Transmission Equipment
  - System Security: Preventing system impact and Protecting critical substations
  - Standards
- Cyber Security

Security: What should we be trying to protect

- Fuel Supply and Generation Assets
- Transmission and Distribution
- Controls and Communications
- Other Assets
Security: What issues impede Protection

- Inability to share information
- Increased cost of security
- Widely dispersed assets
- Widely dispersed owners and operators
- Finding training and empowering security personnel
- Commercial off-the-shelf (COTS) controls and communications
- Siting constraints
- Long lead-time equipment
- Availability of restoration funds
- R&D focused on vulnerabilities

Executive Order -- Improving Critical Infrastructure Cybersecurity; Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (2/12/2013)

The new E.O. changes the definition of “critical infrastructure”

The new E.O. defines “critical infrastructure at greatest risk,” as infrastructure where “a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”
Executive Order – Improving Critical Infrastructure Cybersecurity

“We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cyber security information sharing and collaboratively develop and implement risk-based standards.”

- **Critical Infrastructure**: systems and assets, physical or virtual
- **Cybersecurity Information Sharing**: Increase sharing of cyber threat information with private sector
  - Unclassified reports
  - Process and system to be established for dissemination
  - Expand Enhanced Cybersecurity Services program to all CI sectors
  - Expedite security clearance process
  - Leverage industry SMEs regarding content, structure and types of information most useful to CI owners/operators
  - Engagement model includes CI Partnership Advisory Council, Sector Coordinating Councils, CI owners/operators, Sector Specific Agencies (SSAs), regulatory agencies, SLTT, universities, experts and others
  - Ensure privacy and civil liberties protection

Critical Infrastructure Cybersecurity - Executive Order (EO) and Presidential Policy Directive (PPD-21)

**State/local government impact**

1. Federal Department of Homeland Security and a few federal agencies are responsible for most of the direct actions resulting from the EO and Presidential Policy Directive
   - State homeland security agencies are likely to play a pivotal information sharing role for government and commercial sector
2. State/local government agencies coming under the critical infrastructure definition will look for funding opportunities from the federal government to implement the Cybersecurity Framework
   - Transportation (mass transit, highways, bridges, airports)
   - Health (disease management, health information exchanges),
   - Public safety (emergency management, law enforcement), and
   - Utilities (nuclear/power/chemical plants)
3. Most states have not adopted or implemented a security framework and the EO will be a catalyst for them to consider embracing the Cybersecurity Framework
4. Unrelated to the EO/PPD, NGA has formed a “National Policy council for State Cybersecurity”. Deloitte is a participant and will help shape policy recommendations for state governors on Cybersecurity

Key milestones of the Executive Order (EO)

<table>
<thead>
<tr>
<th>Private Sector</th>
<th>Public Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Near-term</strong></td>
<td><strong>Mid-term</strong></td>
</tr>
<tr>
<td>&lt; 150 days</td>
<td>150 days to 1 year</td>
</tr>
</tbody>
</table>

- **Private Sector**
  - Partner to shape development of a cybersecurity framework
  - Dialogue on information sharing
  - Expand Cybersecurity Services (120 days)
  - Establish voluntary program to support Framework adoption (120 days)

- **Public Sector**
  - Broaden information-sharing process, assess privacy risks, analyze incentives (120 days)
  - Review and comment on Cybersecurity Framework
  - Develop a preliminary Framework (240 days)

- **Cybersecurity Framework**
  - Identify critical infrastructure at greatest risk
  - Review, update CI list (annually)
  - Review, update CI list (annually)
  - Expand Enhanced Cybersecurity Services program to all CI sectors

- **Unclassified reports**
  - Issue final Framework (1 year)
  - Report on CI impacts (2 years)

- **Engagement model**
  - Leverage industry SMEs regarding content, structure and types of information most useful to CI owners/operators

- **Dialogue on information sharing**
  - Identify Cybersecurity Framework
  - Report program participation and opportunities to implement Cybersecurity Framework

- **Private Sector**
  - Executive Order – Improving Critical Infrastructure Cybersecurity
  - Presidential Policy Directive (PPD-21)

- **Public Sector**
  - Critical Infrastructure Cybersecurity - Executive Order (EO) and Presidential Policy Directive (PPD-21)

- **State/local government impact**
  - Federal Department of Homeland Security and a few federal agencies are responsible for most of the direct actions resulting from the EO and Presidential Policy Directive
  - State homeland security agencies are likely to play a pivotal information sharing role for government and commercial sector

- **Critical Infrastructure**
  - Systems and assets, physical or virtual

- **Cybersecurity Information Sharing**
  - Increase sharing of cyber threat information with private sector

- **Partnership**
  - With owners and operators of critical infrastructure to improve cyber security information sharing and collaboratively develop and implement risk-based standards.

- **Private Sector**
  - Partner to shape development of a cybersecurity framework
  - Dialogue on information sharing
  - Expand Cybersecurity Services (120 days)
  - Establish voluntary program to support Framework adoption (120 days)

- **Public Sector**
  - Broaden information-sharing process, assess privacy risks, analyze incentives (120 days)
  - Review and comment on Cybersecurity Framework
  - Develop a preliminary Framework (240 days)

- **Unclassified reports**
  - Issue final Framework (1 year)
  - Report on CI impacts (2 years)

- **Engagement model**
  - Leverage industry SMEs regarding content, structure and types of information most useful to CI owners/operators

- **Dialogue on information sharing**
  - Identify Cybersecurity Framework
  - Report program participation and opportunities to implement Cybersecurity Framework

- **Private Sector**
  - Executive Order – Improving Critical Infrastructure Cybersecurity
  - Presidential Policy Directive (PPD-21)

- **Public Sector**
  - Critical Infrastructure Cybersecurity - Executive Order (EO) and Presidential Policy Directive (PPD-21)

- **State/local government impact**
  - Federal Department of Homeland Security and a few federal agencies are responsible for most of the direct actions resulting from the EO and Presidential Policy Directive
  - State homeland security agencies are likely to play a pivotal information sharing role for government and commercial sector

- **Critical Infrastructure**
  - Systems and assets, physical or virtual

- **Cybersecurity Information Sharing**
  - Increase sharing of cyber threat information with private sector

- **Partnership**
  - With owners and operators of critical infrastructure to improve cyber security information sharing and collaboratively develop and implement risk-based standards.

- **Private Sector**
  - Partner to shape development of a cybersecurity framework
  - Dialogue on information sharing
  - Expand Cybersecurity Services (120 days)
  - Establish voluntary program to support Framework adoption (120 days)

- **Public Sector**
  - Broaden information-sharing process, assess privacy risks, analyze incentives (120 days)
  - Review and comment on Cybersecurity Framework
  - Develop a preliminary Framework (240 days)

- **Unclassified reports**
  - Issue final Framework (1 year)
  - Report on CI impacts (2 years)

- **Engagement model**
  - Leverage industry SMEs regarding content, structure and types of information most useful to CI owners/operators

- **Dialogue on information sharing**
  - Identify Cybersecurity Framework
  - Report program participation and opportunities to implement Cybersecurity Framework

- **Private Sector**
  - Executive Order – Improving Critical Infrastructure Cybersecurity
  - Presidential Policy Directive (PPD-21)

- **Public Sector**
  - Critical Infrastructure Cybersecurity - Executive Order (EO) and Presidential Policy Directive (PPD-21)

- **State/local government impact**
  - Federal Department of Homeland Security and a few federal agencies are responsible for most of the direct actions resulting from the EO and Presidential Policy Directive
  - State homeland security agencies are likely to play a pivotal information sharing role for government and commercial sector

- **Critical Infrastructure**
  - Systems and assets, physical or virtual

- **Cybersecurity Information Sharing**
  - Increase sharing of cyber threat information with private sector

- **Partnership**
  - With owners and operators of critical infrastructure to improve cyber security information sharing and collaboratively develop and implement risk-based standards.

- **Private Sector**
  - Partner to shape development of a cybersecurity framework
  - Dialogue on information sharing
  - Expand Cybersecurity Services (120 days)
  - Establish voluntary program to support Framework adoption (120 days)

- **Public Sector**
  - Broaden information-sharing process, assess privacy risks, analyze incentives (120 days)
  - Review and comment on Cybersecurity Framework
  - Develop a preliminary Framework (240 days)

- **Unclassified reports**
  - Issue final Framework (1 year)
  - Report on CI impacts (2 years)

- **Engagement model**
  - Leverage industry SMEs regarding content, structure and types of information most useful to CI owners/operators

- **Dialogue on information sharing**
  - Identify Cybersecurity Framework
  - Report program participation and opportunities to implement Cybersecurity Framework
**Approach**

- Vulnerability mapping
- Scenario analysis
  - The green movement
    - Resilience requirement for new suppliers
  - Middle East embargo
    - New projects require improved delivery
  - Non-renewable energy abundance
    - Supplier and product distribution will provide snapshot of product portfolio health

**Observations**

**Threat Situation is Changing:**
- Cyber has “weakest link” issues
- Cyber threats are dynamic, evolving quickly and often combined with lack of training and awareness.
- All hazard, including aging infrastructure, natural disasters and intentional attacks

**Innovation and Policy:**
- The green movement
- Resilience requirement for new suppliers
- No amount of technology will make up for the lack of the 3 Ps (Policy, Process, and Procedures).
- Installing modern communications and control equipment (elements of the smart grid) can help, but security must be designed in from the start.
- Build in secure sensing, “defense in depth,” fast reconfiguration and self-healing into the infrastructure.
- Security by default – certify vendor products for cyber readiness
- Security as a curriculum requirement.
- Increased investment in the grid and in R&D is essential.

**Recommendations**

- Facilitate, encourage, or mandate that secure sensing, “defense in depth,” fast reconfiguration and self-healing be built into the infrastructure.
- Wireless and the public Internet increase vulnerability and thus should be avoided.
- Bridge the jurisdictional gap between Federal/NERC and the state commissions on cyber security.
- Electric generation, transmission, distribution, and consumption need to be safe, reliable, and economical in their own right. Asset owners should be required to practice due diligence in securing their infrastructure as a cost of doing business.
- Develop coordinated hierarchical threat coordination centers – at local, regional, and national levels – that proactively assess precursors and counter cyber attacks.
- Speed up the development and enforcement of cyber security standards, compliance requirements and their adoption. Facilitate and encourage design of security in from the start and include it in standards.
- Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security).
- Develop methods, such as self-organizing micro-grids, to facilitate grid segmentation that limits the effects of cyber and physical attacks.

Currently, there are 16 industry sectors defined as critical infrastructure

85% of critical infrastructure is in private sector hands\(^1\)

Trends exposing industry to increased risk
- Interconnectedness of sectors
- Proliferation of exposure points
- Concentration of assets

<table>
<thead>
<tr>
<th>Critical infrastructure sectors</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture and Food</td>
<td>Dams</td>
<td>Information Technology</td>
</tr>
<tr>
<td>Banking and Financial Services</td>
<td>Defense Industrial Base</td>
<td>Nuclear Reactors, Materials and Waste</td>
</tr>
<tr>
<td>Chemical</td>
<td>Emergency Services</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td>Commercial Facilities</td>
<td>Energy</td>
<td>Water and Wastewater Systems</td>
</tr>
<tr>
<td>Communications</td>
<td>Government Facilities</td>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td>Healthcare and Public Health</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enabling secure, reliable and resilient systems

Enabling **secure, reliable and resilient** systems requires people and organizations that can:

- Anticipate
- Plan
- Implement
- Adapt and Improvise

Risk-managed Architectures and Layered Defense

- Resilience: ability to recover quickly
- Robustness: failure-resistant through design and/or construction
- Redundancy: duplicative capacity for service delivery

Critical Features of Survivable Systems: Lessons from September 11

- Resilience: ability to recover quickly
- Robustness: failure-resistant through design and/or construction
- Redundancy: duplicative capacity for service delivery

Verizon, AT&T, ConEd, and MTA (among others) possessed all these attributes in equipment and people

Verizon, AT&T, ConEd, and MTA (among others) possessed all these attributes in equipment and people

Markov Closed-Form Solution: State Transition Diagram for Each Microgrid

Markov Closed-Form Solution: State Transition Diagram for Each Microgrid
State Transition Diagram for Three Interconnected Microgrids

Monte Carlo Simulation Test Case

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microgrids in Assembly</td>
<td>3</td>
</tr>
<tr>
<td>Loads per Microgrid</td>
<td>3</td>
</tr>
<tr>
<td>Load Real Power (kW)</td>
<td>100</td>
</tr>
<tr>
<td>Load Reactive Power (kVAR)</td>
<td>50</td>
</tr>
<tr>
<td>Generators per Microgrid</td>
<td>3</td>
</tr>
<tr>
<td>Generator Real Power max. (kW)</td>
<td>130</td>
</tr>
<tr>
<td>Generator Real Power min. (kW)</td>
<td>25</td>
</tr>
<tr>
<td>Generator Reactive Power max. (kVAR)</td>
<td>100</td>
</tr>
<tr>
<td>Generator Reactive Power min. (kVAR)</td>
<td>-100</td>
</tr>
<tr>
<td>Storage Units per Microgrid</td>
<td>3</td>
</tr>
<tr>
<td>Storage Unit Capacity (MWh)</td>
<td>1</td>
</tr>
<tr>
<td>Voltage Magnitude max. (pu)</td>
<td>1.07</td>
</tr>
<tr>
<td>Voltage Magnitude min. (pu)</td>
<td>0.95</td>
</tr>
<tr>
<td>Line Rating (kW)</td>
<td>200</td>
</tr>
<tr>
<td>Switch Rating (kW)</td>
<td>100</td>
</tr>
<tr>
<td>Base Voltage (kV)</td>
<td>4.16</td>
</tr>
<tr>
<td>Base Complex Power (MVA)</td>
<td>10</td>
</tr>
</tbody>
</table>

Transition Rates

<table>
<thead>
<tr>
<th>Availability</th>
<th>$\lambda$ (failures/year)</th>
<th>$\mu$ (repairs/year)</th>
<th>$MTTF$ (h)</th>
<th>$MTTR$ (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformer</td>
<td>0.99</td>
<td>3.69</td>
<td>365</td>
<td>2374</td>
</tr>
<tr>
<td>Busbar</td>
<td>0.99</td>
<td>3.69</td>
<td>365</td>
<td>2374</td>
</tr>
<tr>
<td>Generator</td>
<td>0.9</td>
<td>8.11</td>
<td>73</td>
<td>1080</td>
</tr>
<tr>
<td>Storage Unit</td>
<td>0.85</td>
<td>32.21</td>
<td>182.5</td>
<td>272</td>
</tr>
<tr>
<td>Line</td>
<td>0.95</td>
<td>9.61</td>
<td>182.5</td>
<td>912</td>
</tr>
<tr>
<td>Switch</td>
<td>0.95</td>
<td>9.61</td>
<td>182.5</td>
<td>912</td>
</tr>
<tr>
<td>Agent</td>
<td>0.97</td>
<td>20</td>
<td>780</td>
<td>438</td>
</tr>
</tbody>
</table>

Three Interconnected Microgrid Simulation Results

Loss of Energy Expectation

Loss of Load Expectation
Interim Conclusions

Analytical Models vs. Simulations: We need both to analyze system performance

Analytical Models
- Pros:
  - Can be solved very fast
  - Easy to perform sensitivity analyses, trade-off studies, etc.
- Cons:
  - Difficult to model
  - Abstract

Simulations
- Pros:
  - Can be very detailed
- Cons:
  - May take long time to run
  - Need multiple runs to search simulation space

Centralized or Decentralized Control?

Centralized or Decentralized Control?

Intelligent Distributed Secure Distribution System Control Architecture

Control Architecture LOEE Probability Distributions

Control Architecture Line Losses Probability Distributions
Smart Grid Interdependencies
Security, Efficiency, and Resilience

Multi-Objective Optimization Model

Objective 1: Minimize aggregate customer outage cost
Objective 2: Minimize capital cost of storage systems

Prioritizing Emergency Backup Service

Feeder Reconfiguration/Intentional Islanding

Outline
• System divided into sub-networks joined by controllable switches
• The fault is isolated for a given outage situation
• Non-faulted sub-networks are intentionally islanded to supply back-up service to local loads

Simulation
• Perform Sequential Monte-Carlo simulation to simulate outages
• Determine optimal locations to place storage elements

<table>
<thead>
<tr>
<th>SYSTEM CHARACTERISTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage (kV)</td>
</tr>
<tr>
<td>Number of Loads</td>
</tr>
<tr>
<td>Peak Load</td>
</tr>
<tr>
<td>Number of Customers</td>
</tr>
<tr>
<td>Large C&amp;I Customers</td>
</tr>
<tr>
<td>Medium C&amp;I Customers</td>
</tr>
<tr>
<td>Residential Customers</td>
</tr>
</tbody>
</table>

Simulated Outage
• 120 minute outage on bulk power system
• 1500 kWh backup storage a distribution substation (node 150)
• Loads selectively served for outage ride-through

<table>
<thead>
<tr>
<th>LOADS SERVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small C&amp;I | Large C&amp;I</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customer Outage Costs (2008$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large C&amp;I</td>
</tr>
<tr>
<td>No Storage</td>
</tr>
<tr>
<td>With Storage - All Loads</td>
</tr>
<tr>
<td>With Storage - Selective Service</td>
</tr>
</tbody>
</table>
Energy Storage for C&I Applications

<table>
<thead>
<tr>
<th>Technology</th>
<th>Maturity</th>
<th>Capacity (kWh)</th>
<th>Power (kW)</th>
<th>Duration (hrs)</th>
<th>Efficiency (%)</th>
<th>Cycle Life (cycles)</th>
<th>Total Cost ($/kW)</th>
<th>Cost ($/kWh)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Lead-Acid 1</td>
<td>Demo-Commercial</td>
<td>5000</td>
<td>1000</td>
<td>5</td>
<td>85</td>
<td>4500</td>
<td>3000</td>
<td>600</td>
</tr>
<tr>
<td>Advanced Lead-Acid 2</td>
<td>Demo-Commercial</td>
<td>1000</td>
<td>2000</td>
<td>5</td>
<td>80</td>
<td>4500</td>
<td>3600</td>
<td>720</td>
</tr>
<tr>
<td>NaS</td>
<td>Commercial</td>
<td>7200</td>
<td>1000</td>
<td>7.2</td>
<td>75</td>
<td>4500</td>
<td>3600</td>
<td>500</td>
</tr>
<tr>
<td>Zn/Br Flow 1</td>
<td>Demo</td>
<td>625</td>
<td>125</td>
<td>5</td>
<td>62</td>
<td>&gt;10000</td>
<td>2420</td>
<td>485</td>
</tr>
<tr>
<td>Zn/Br Flow 2</td>
<td>Demo</td>
<td>2500</td>
<td>500</td>
<td>5</td>
<td>62</td>
<td>&gt;10000</td>
<td>2200</td>
<td>440</td>
</tr>
<tr>
<td>Vanadium Flow</td>
<td>Demo</td>
<td>1000</td>
<td>285</td>
<td>3.5</td>
<td>67</td>
<td>&gt;10000</td>
<td>3800</td>
<td>1085</td>
</tr>
<tr>
<td>Li-Ion</td>
<td>Demo</td>
<td>625</td>
<td>175</td>
<td>3.5</td>
<td>87</td>
<td>4500</td>
<td>3800</td>
<td>1085</td>
</tr>
</tbody>
</table>


Single Customer Multi-Objective Optimization Model

Objective 1: Minimize Outage Costs

minimize \[ \sum_{n=1}^{N_{outage}} \left( t_o - P_{load,n} \right) \sum_{j=1}^{N_{BESS}} X_j \]

Objective 2: Minimize Energy Costs

minimize \[ \sum_{j=1}^{N_{BESS}} \left( P_{load,t} - P_{gen,t} + P_{BESS,t} \right) C_{CJ} \Delta t \]

Objective 3: Minimize Demand Costs

minimize \[ \sum_{j=1}^{N_{BESS}} \left( \max \left( P_{load,t} - P_{gen,t} + P_{BESS,t} \right) \right) C_{CJ} \]

Objective 4: Minimize Capital Costs

minimize \[ \sum_{j=1}^{N_{BESS}} C_{CJ} X_j \]

Voltage Profiles

Normal Operation: 1.04 – 0.98pu voltages

Priority Ride-Through: 1.04 – 0.99pu voltages

Multi-Application Energy Storage

Approach: Partition energy storage capacity according to application

Remaining kWh

Emergency Backup

Power Factor Management

Energy Management

BESS Total kWh capacity
Distribution Reliability Analysis

- **Failure rate**, \( \lambda \): expected # of failures per year for network component
- **Repair time**, \( r \): average number of hours to repair network component
- **\( N_s \)**: Number of customers at load point \( s \)

**System Average Interruption Frequency Index (SAIFI)**

\[
SAIFI = \frac{\sum N_s \Delta t}{\sum N_s} = \text{Average number of interruptions per customer served}
\]

**System Average Interruption Duration Index (SAIDI)**

\[
SAIDI = \frac{\sum N_s \Delta t^2}{\sum N_s} = \text{System wide average interruption duration}
\]

**Customer Average Interruption Duration Index (CAIDI)**

\[
CAIDI = \frac{\sum N_s \Delta t^2}{\sum N_s} = \text{Average outage duration experienced by a customer}
\]

Feeder Main Reliability Analysis

Optimal Mix and Placement

<table>
<thead>
<tr>
<th>No. Units Selected</th>
<th>BESS Selected</th>
<th>Location</th>
<th>Capital Cost</th>
<th>Added Savings</th>
<th>Annual Outage Costs</th>
<th>Payback Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>--</td>
<td>$0</td>
<td>--</td>
<td>$1,435,814</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>Zinc Bromine 1</td>
<td>M4</td>
<td>$303,125</td>
<td>$285,776</td>
<td>$1,150,038</td>
<td>1.06 years</td>
</tr>
<tr>
<td>2</td>
<td>Zinc Bromine 1</td>
<td>M4</td>
<td>$606,250</td>
<td>$207,749</td>
<td>$942,289</td>
<td>1.23 years</td>
</tr>
<tr>
<td>3</td>
<td>Zinc Bromine 1</td>
<td>M4</td>
<td>$909,375</td>
<td>$224,758</td>
<td>$717,531</td>
<td>1.27 years</td>
</tr>
<tr>
<td>4</td>
<td>Zinc Bromine 1</td>
<td>M4</td>
<td>$1,212,500</td>
<td>$225,395</td>
<td>$492,136</td>
<td>1.29 years</td>
</tr>
<tr>
<td>5</td>
<td>Zinc Bromine 1</td>
<td>M3</td>
<td>$1,515,625</td>
<td>$103,449</td>
<td>$388,687</td>
<td>1.45 years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>M1</th>
<th>M2</th>
<th>M3</th>
<th>M4</th>
<th>M5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cost:</td>
<td>200</td>
<td>85</td>
<td>44</td>
<td>72</td>
<td>112</td>
</tr>
<tr>
<td>Cust. Served</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>35</td>
<td>0</td>
</tr>
<tr>
<td><strong>SAIDI</strong>: 3.93 (down 0.44)</td>
<td><strong>SAIFI</strong>: 5.90 (down 0.66)</td>
<td><strong>CAIDI</strong>: 1.5 (same)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Smart Grid U™

- **Goal**: Transform the University of Minnesota’s Twin Cities’ campus into a *SmartGridU*.
  - Develop system models, algorithms and tools for successfully integrating the components (generation, storage and loads) within a microgrid on the University of Minnesota campus.
  - Conduct “wind-tunnel” data-driven simulation testing of smart grid designs, alternative architectures, and technology assessments, utilizing the University as a living laboratory.
  - Roadmap to achieve a “net zero smart grid” at the large-scale community level — i.e., a self contained, intelligent electricity infrastructure able to match renewable energy supply to the electricity demand.
Smart Grid U™

- Control algorithms and interfaces for turning individual energy components (storage, generation and loads) into an integrated, optimized energy system.
  - E.g., demand surface plots of raw data for demands, emissions, & efficiency

Next steps: demonstrate ability to integrate renewables/storage, cogeneration and achieve NZE status.

UM-Morris Potential Smart Grid projects

- Location: Morris, MN
- Size: 1,800 student residential campus
- Energy Sources:
  - Biomass gasification plant
  - Solar thermal panels
  - Solar photovoltaic system
  - Two 1.65MW wind turbines (provides ~70% of campus’ electricity needs)
- Load 300,000-750,000 kWh/month

Going Carbon Negative…

UM Morris Net Energy Balance

[Graph showing net energy balance over years]

Minnesota’s Wind Resource by Wind Speed at 80 Meters

[Map showing wind speed distribution across Minnesota]

[Legend for wind speed categories]
University of Minnesota - Morris

CURRENT SYSTEM
P_{\text{OYPC}} = P_{\text{load}} - P_{\text{gen}}
Otter Tail Power Company

PROPOSED SYSTEM
P_{\text{OYPC}} = P_{\text{load}} - P_{\text{gen}} + P_{\text{BESS}}
Otter Tail Power Company

P_{\text{gen}} = 2 \times 1.65 \text{ MW Wind Turbines}
P_{\text{load}} = 1.5 \text{ MW Peak}

UMMorris – Typical Week in 2011

DR: Total Cost Savings

Cost Savings From Energy Conservation, Time of Day Pricing, and Load Management

\[ y = 0.3769x + 12.969 \]
\[ y = 0.2542x + 12.969 \]

Load Managed (%) | Savings ($) | Savings (%)
--- | --- | ---
10 | 51,398 | 15.5
20 | 59,823 | 18.1
30 | 68,247 | 20.6
40 | 76,671 | 23.1
50 | 85,096 | 25.7

Load Shifted to Lowest Price Period

Load Managed (%) | Savings ($) | Savings (%)
--- | --- | ---
10 | 55,463 | 16.7
20 | 67,952 | 20.5
30 | 80,442 | 24.3
40 | 92,931 | 28.0
50 | 105,420 | 31.8
Can the application of smart grid technologies, and more broadly, smart systems provide a better method and designs for managing the energy needs of the community?

Massoud Amin and his team of graduate MOT assistants, Eric Bohnert, Andrew Fraser, Hope Johnson and Shanna Leeland

UMore Park: Smart Grid Technologies for Homes

- Photovoltaic inverters
- Smart meters, in-home displays
- Grid-ready appliances
- Electric vehicle power charging station
- Battery storage backup
- Estimated costs: $10,670 to $27,190 per home
- About 4-5% of total cost

Estimated Prices for Energy-Efficient, Smart Grid Ready Homes in UMore Park

<table>
<thead>
<tr>
<th>Lot Size</th>
<th>Price Ranges</th>
<th>Cost Over Traditional Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Lot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>$225,000</td>
<td>$19,920</td>
</tr>
<tr>
<td>High</td>
<td>$300,000</td>
<td>$29,920</td>
</tr>
<tr>
<td>Average</td>
<td>$262,500</td>
<td>$24,920</td>
</tr>
<tr>
<td>Traditional</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>$225,000</td>
<td>$19,920</td>
</tr>
<tr>
<td>High</td>
<td>$410,000</td>
<td>$34,920</td>
</tr>
<tr>
<td>Average</td>
<td>$267,500</td>
<td>$27,920</td>
</tr>
<tr>
<td>Large Lot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>$450,000</td>
<td>$37,920</td>
</tr>
<tr>
<td>High</td>
<td>$725,000</td>
<td>$58,920</td>
</tr>
<tr>
<td>Average</td>
<td>$587,500</td>
<td>$48,920</td>
</tr>
</tbody>
</table>

Average prices are within range of the low-high estimated home prices for UMore Park.
UMore Park: District Energy and Smart Grid Options

Smart Grid U™

- Lessons learned and key messages:
  - Consider all parts together (Holistic Systems approach)
  - Focus on Benefits to Cost Payback
  - Remove deficiencies in foundations
  - The University as a Living laboratory
  - Education and Research → Implement new solutions

- Consumer engagement critical to successful policy implementation to enable end-to-end system modernization

- If the transformation to smart grid is to produce real strategic value for our nation and all its citizens, our goals must include:
  - Enable every building and every node to become an efficient and smart energy node.

Selected References

Downloadable at: http://umn.edu/~amin


- “Securing the Electricity Grid,” (Amin), The Bridge, the quarterly publication of the National Academy of Engineering, Volume 40, Number 1, Spring 2010


- “Powering the 21st Century: We can -and must- modernize the grid,” IEEE Power & Energy Magazine, pp. 93-95, March/April 2005
