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)

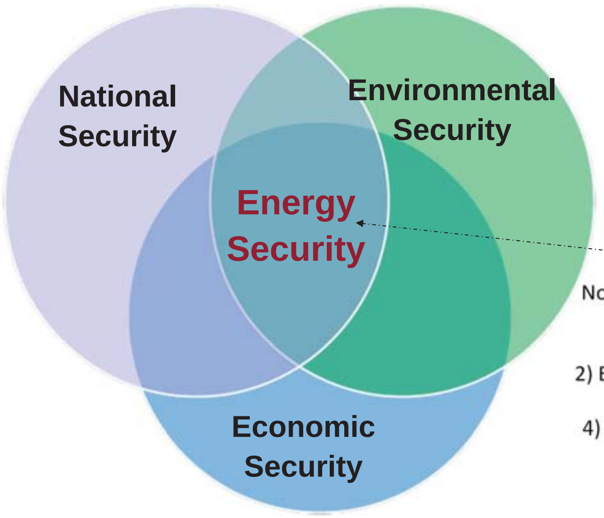
Keynote address at the 47th Annual Frontiers of Power Conference
Stillwater, OK, Monday, October 27, 2014

TECHNOLOGICAL
LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

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

Energy Security: System of Systems

The Energy Crises Taught Us Interdependency



National Security

Environmental Security

Energy Security

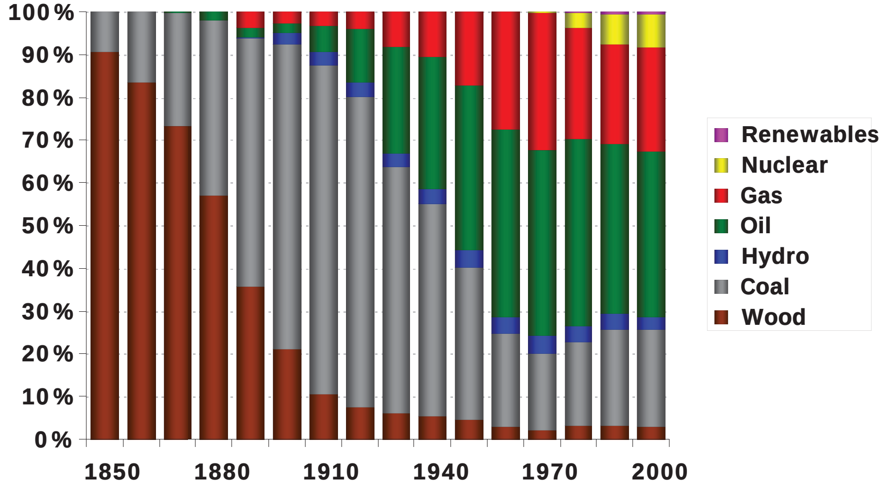
Economic Security

System of Systems:
No “magic bullets” but there are many innovative bullets, including:

1) Green the power supply,
2) Energy systems & end-use efficiency,
3) Electrify transportation,
4) Build a stronger & smarter grid with massive storage integrating greener electrical energy,
5) With full cyber security.

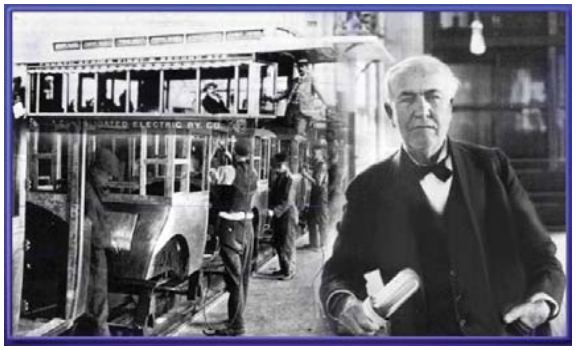
Source: Massoud Amin’s Congressional briefing s on March 26 and Oct. 15, 2009, and November 2013

Context: US Energy Supply Since 1850



Author: Koonin Source: EIA

Transforming Society



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

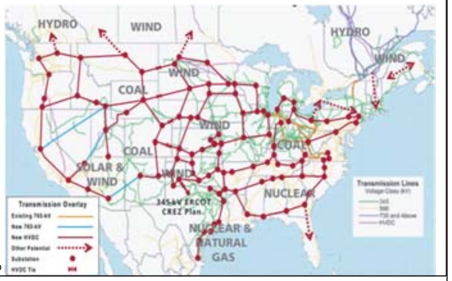
Smart Grid: Integrate Dispersed Energy Sources into a Modern Grid to Provide Energy to Centers of Demand

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**

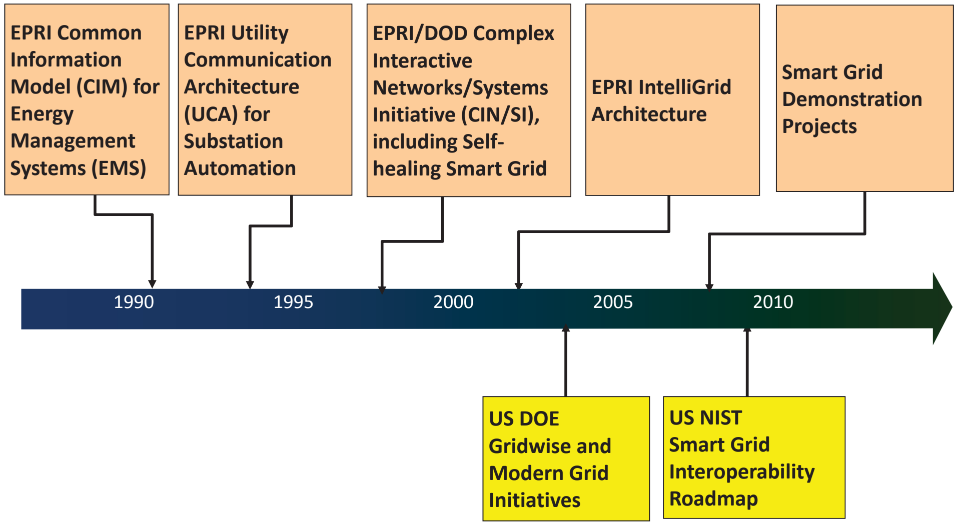
Emerging Supply and Demand Patterns

A Multi-layer Grid System in need of Strengthening and Protection



Source: Massoud Amin's Congressional briefings , March & Oct 2009, & Nov 2013

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

1990 1995 2000 2005 2010

US DOE Gridwise and Modern Grid Initiatives

US NIST Smart Grid Interoperability Roadmap

The Smart Grid: 15 Years in the Making

- Self-Healing Grid (May 1998- Dec. 2002)
  – 1998-2002: EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI):
  – 108 professors and over 240 graduate students in 28 U.S. universities funded, including Carnegie Mellon, Minnesota, Illinois, Arizona St., Iowa St., Purdue, Harvard, MIT, Cornell, UC-Berkeley, Wisconsin, RPI, UTAM, Cal Tech, UCLA, and Stanford.
  – 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

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 page 5 at http://massoud-amin.umn.edu/presentations/CINSI_01-27-1998_RAC.pdf

- 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

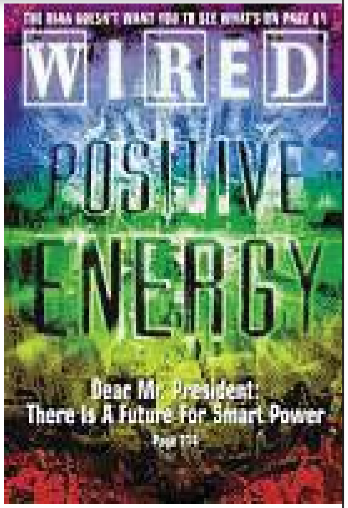
Source: Massoud Amin, "Toward a Secure and Smart Self-Healing Grid," presentation to the Strategic Science & Technology EPRI Research Advisory Committee (RAC), Tuesday, January 27, 1998 page 6 at http://massoud-amin.umn.edu/presentations/CINSI_01-27-1998_RAC.pdf

- 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.

"… not to sell light bulbs, but to create a network of technologies and services that provide illumination…"

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."*

-- **The Energy Web,** Wired Magazine, July 2001
http://www.wired.com/wired/archive/9.07/juice.html



Energy Independence and Security Act

- Passed by U.S. Congress in 2007.
- "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

FERC: "Grid advancements will apply digital technologies to the grid and enable real-time coordination of information from both generating plants and demand-side resources."

DOE: "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…"

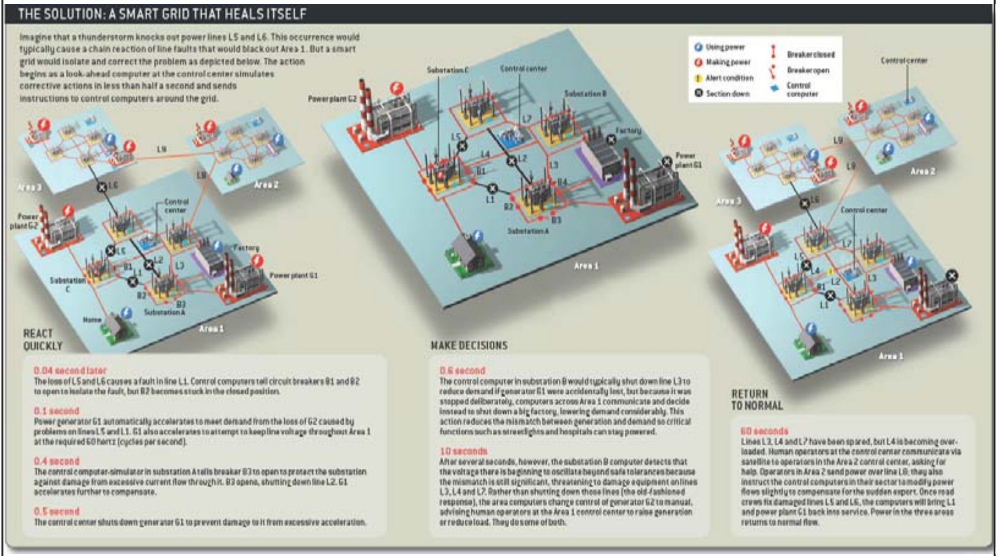
GE: "The Smart Grid is in essence the marriage of information technology and process-automation technology with our existing electrical networks."

IEEE: "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."

Wikipedia: "A Smart Grid delivers electricity from suppliers to consumers using digital technology to save energy, reduce cost, and increase reliability."

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

Smart Self-Healing Grid



THE SOLUTION: A SMART GRID THAT HEALS ITSELF

Imagine that a thunderstorm knocks out power lines L5 and L6. This occurrence would typically cause a chain reaction of line faults that would black out Area 1. But a smart grid would isolate and correct the problem as depicted below. The action begins as a look-ahead computer at the control center simulates corrective actions in less than half a second and sends instructions to control computers around the grid.

REACT QUICKLY

0.04 second later
The loss of L5 and L6 causes a fault in line L1. Control computers tell circuit breakers B1 and B2 to open to isolate the fault, but B2 becomes stuck in the closed position.

0.1 second
Power generator G1 automatically accelerates to meet demand from the loss of G2 caused by problems on lines L5 and L1. G1 also accelerates to attempt to keep line voltage throughout Area 1 at the required 60 hertz (cycles per second).

0.4 second
The control computer-simulator in substation A tells breaker B3 to open to protect the substation against damage from excessive current flow through it. B3 opens, shutting down line L2. G1 accelerates further to compensate.

0.5 second
The control center shuts down generator G1 to prevent damage to it from excessive acceleration.

MAKE DECISIONS

0.6 second
The control computer in substation B would typically shut down line L3 to reduce demand if generator G1 were accidentally lost, but because it was stopped deliberately, computers across Area 1 communicate and decide instead to shut down a big factory, lowering demand considerably. This action reduces the mismatch between generation and demand so critical functions such as streetlights and hospitals can stay powered.

10 seconds
After several seconds, however, the substation B computer detects that the voltage there is beginning to oscillate beyond safe tolerances because the mismatch is still significant, threatening to damage equipment on lines L3, L4 and L7. Rather than shutting down these lines (the old-fashioned response), the area computers change control of generator G2 to manual, advising human operators at the Area 1 control center to raise generation or reduce load. They do some of both.

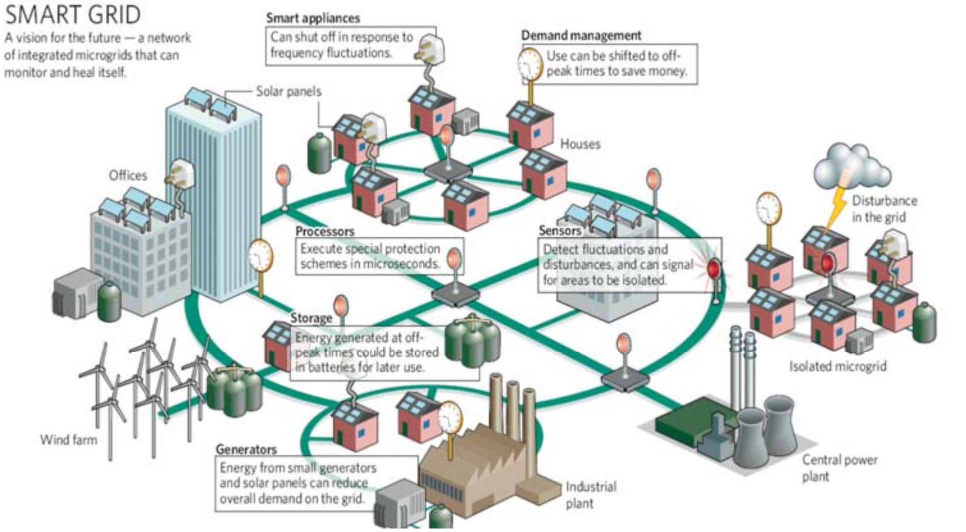
RETURN TO NORMAL

60 seconds
Lines L3, L4 and L7 have been spared, but L4 is becoming overloaded. Human operators at the control center communicate via satellite to operators in the Area 2 control center, asking for help. Operators in Area 2 send power over line L8; they also instruct the control computers in their sector to modify power flows slightly to compensate for the sudden export. Once road crews fix damaged lines L5 and L6, the computers will bring L1 and power plant G1 back into service. Power in the three areas returns to normal flow.

M. Amin and P. Schewe, "Preventing Blackouts," Scientific American, May 2007

Enabling the Future

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



SMART GRID

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

Smart appliances
Can shut off in response to frequency fluctuations.

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

Processors
Execute special protection schemes in microseconds.

Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.

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

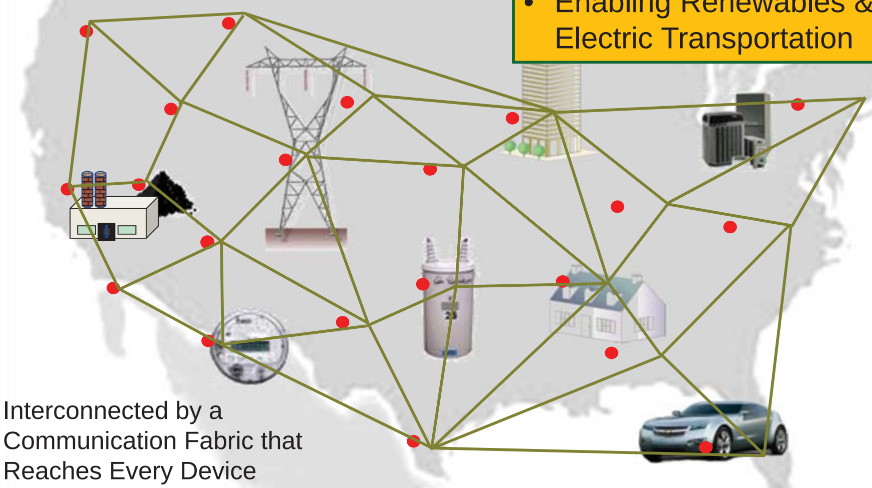
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.

Source: Interview with Massoud Amin, "Upgrading the grid," *Nature*, vol. 454, pp. 570–573, 30 July 2008

Smart Grid

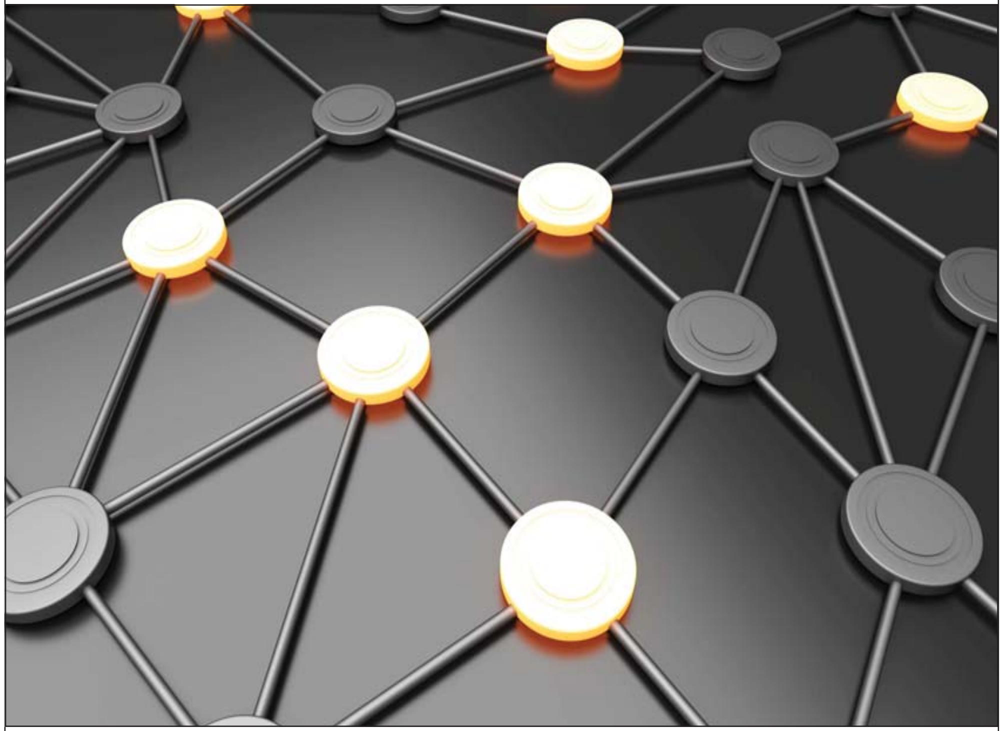
- Engaging Consumers
- Enhancing Efficiency
- Ensuring Reliability
- Enabling Renewables & Electric Transportation

Highly Instrumented with Advanced Sensors and Computing



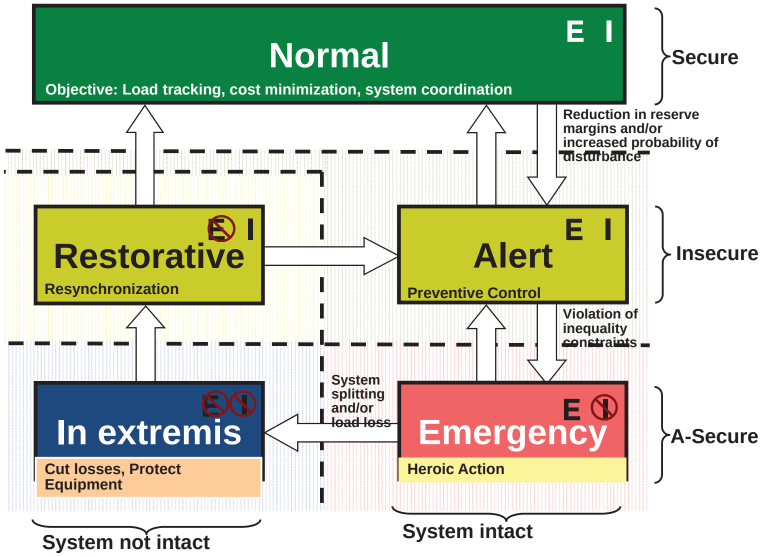
Interconnected by a Communication Fabric that Reaches Every Device

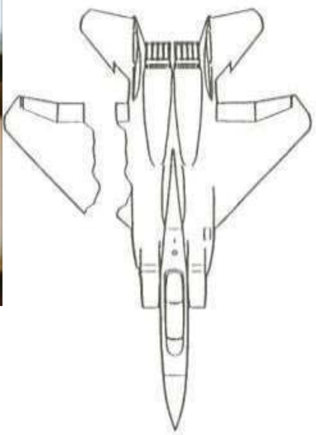
---



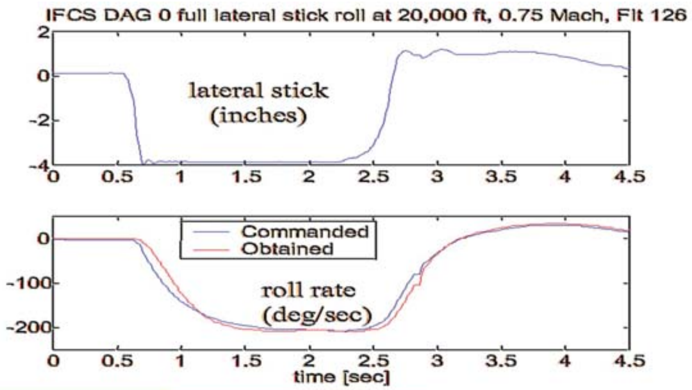
Dynamics of Power System Operating States

E = Demand is met
I = Constraints are met





NASA/MDA/WU IFCS: NASA Ames Research Center, NASA Dryden, Boeing Phantom Works, and Washington University in St. Louis.

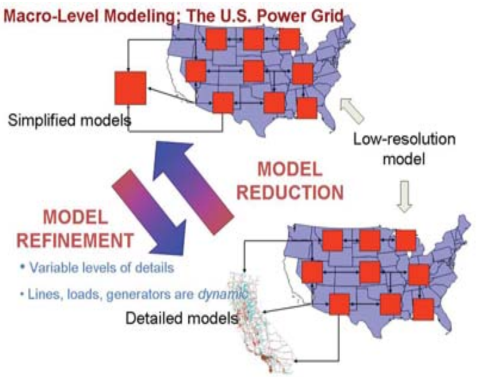


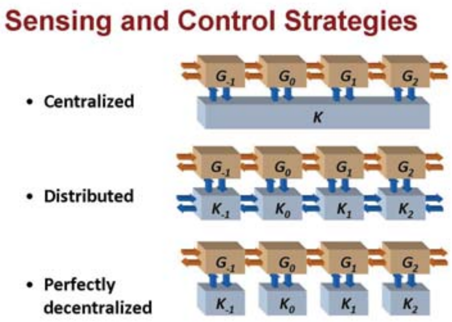
Critical System Dynamics and Resilience Capabilities

- **Anticipation of disruptive events**
- **Look-ahead simulation capability**
- **Fast isolation and sectionalization**
- **Adaptive islanding**
- **Self-healing and restoration**

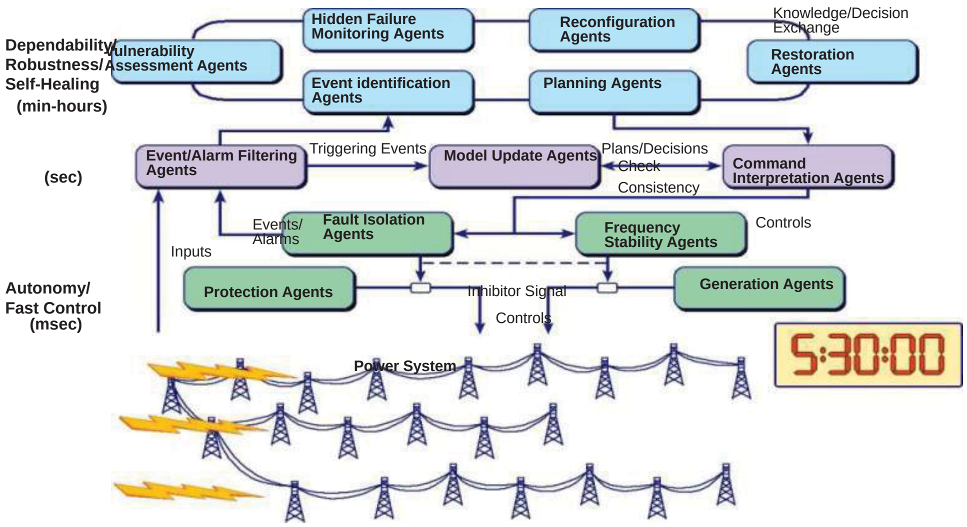
re·sil·ience, *noun*, 1824: The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress; An ability to recover from or adjust easily to misfortune or change

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.





Self-Healing Grid



Dependability/ Robustness/ Self-Healing (min-hours)

Vulnerability Assessment Agents

Hidden Failure Monitoring Agents

Event identification Agents

Reconfiguration Agents

Planning Agents

Knowledge/Decision Exchange

Restoration Agents

(sec)

Event/Alarm Filtering Agents

Triggering Events

Model Update Agents

Plans/Decisions Check Consistency

Command Interpretation Agents

Inputs

Events/ Alarms

Fault Isolation Agents

Frequency Stability Agents

Controls

Autonomy/ Fast Control (msec)

Protection Agents

Inhibitor Signal

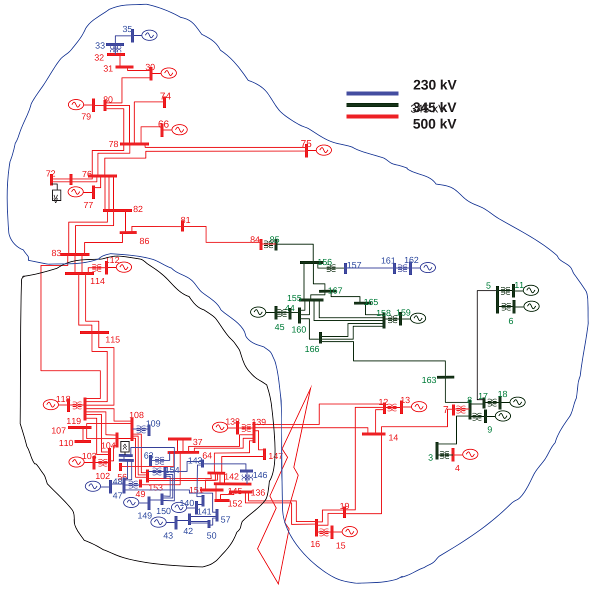
Controls

Generation Agents

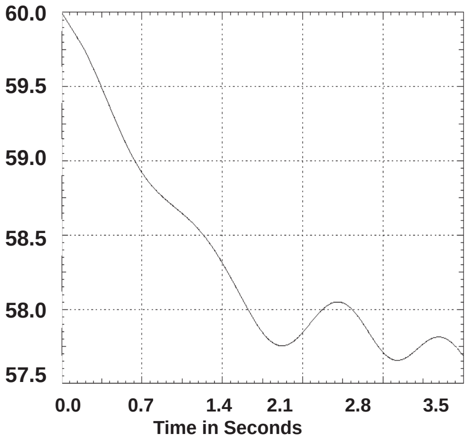
Power System

EPRI/DoD CIN/S Initiative

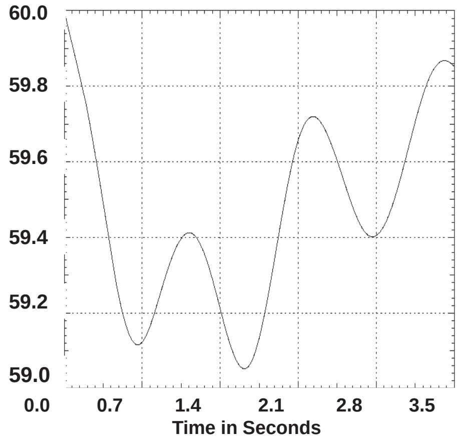
Self-Healing Grid: Intelligent Adaptive Islanding



Past Scheme



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 page 7 at http://massoud-amin.umn.edu/presentations/CINSI_01-27-1998_RAC.pdf

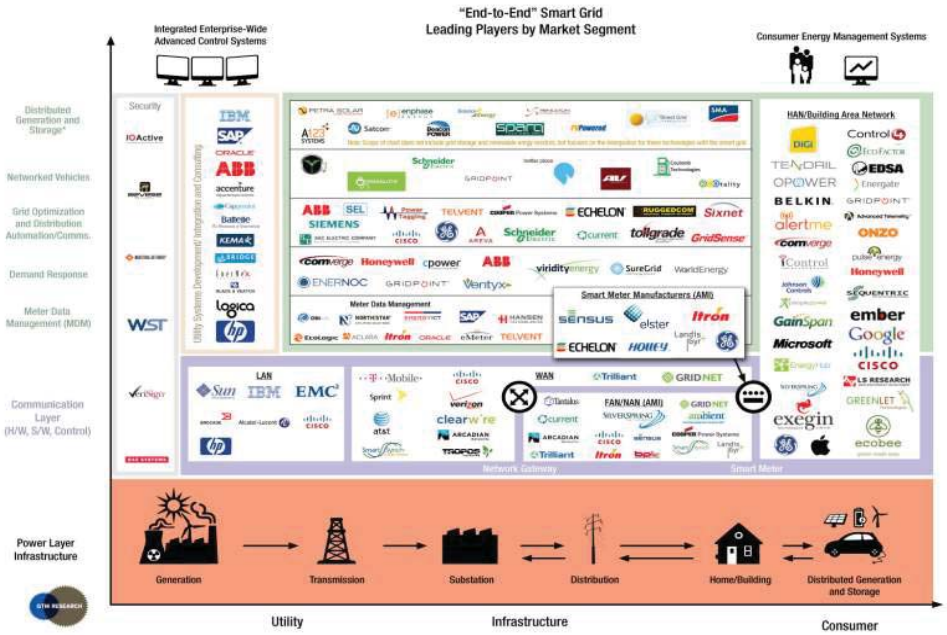
Dependence on IT: Today's systems require a tightly knit information and communications capability. Because of the vulnerability of Internet communications, protecting the system will require new technology to enhance security of power system command, control, and communications.

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.

End-to-End Smart Grid Players/Opportunities



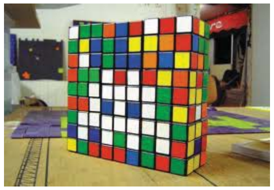
Examples of SG Technologies & Systems

Electric Transmission Systems	Electric Distribution Systems	Advanced Metering Infrastructure	Customer Systems
			
• Synchrophaser technologies • Communications infrastructure • Wide area monitoring and visualization • Line monitors	• Automated switches • Equipment monitoring • Automated capacitors • Communications infrastructure • Distribution management systems	• Smart meters • Communications infrastructure • Data management systems • Back-office integration	• In-home displays • Programmable communicating thermostats • Home area networks • Web portals • Direct load controls • Smart appliances

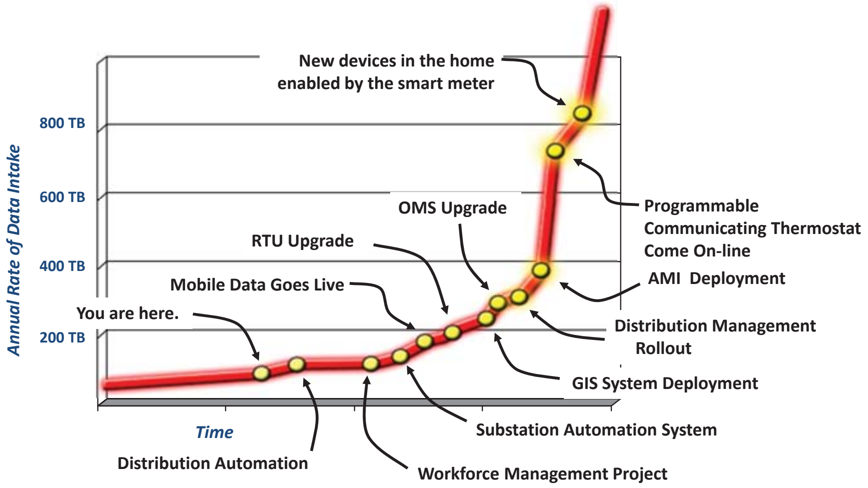
---

Paradigm Shift – Data at MN Valley Coop

- Before smart meters
  - Monthly read
  - 480,000 data points per year
- After smart meters
  - 15-60 minute kWh
  - Peak demand
  - Voltage
  - Power interruptions
  - 480,000,000 data points per year



Smart Grid: Tsunami of Data Developing



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

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

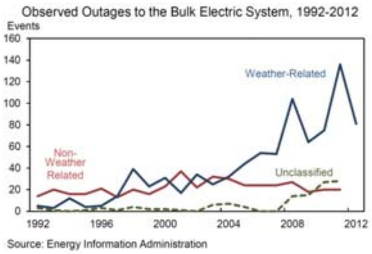
Trends: Resilience and Asset Investments*

Complex grid structures require “Smart Grid” solutions

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



Observed Outages to the Bulk Electric System, 1992-2012

Source: Energy Information Administration

*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

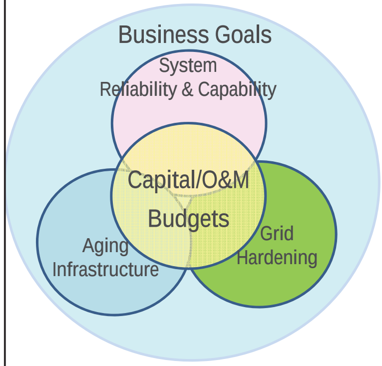
Holistic Asset Management

Asset management:
Predictability of Cost
& Reliability

Average systems 40 to 60 years old

25% of electric infrastructure is of an age and situation where condition is a concern

Demand for maintenance double over the next 10-20 y



- 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

- Micrograms
  - 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)

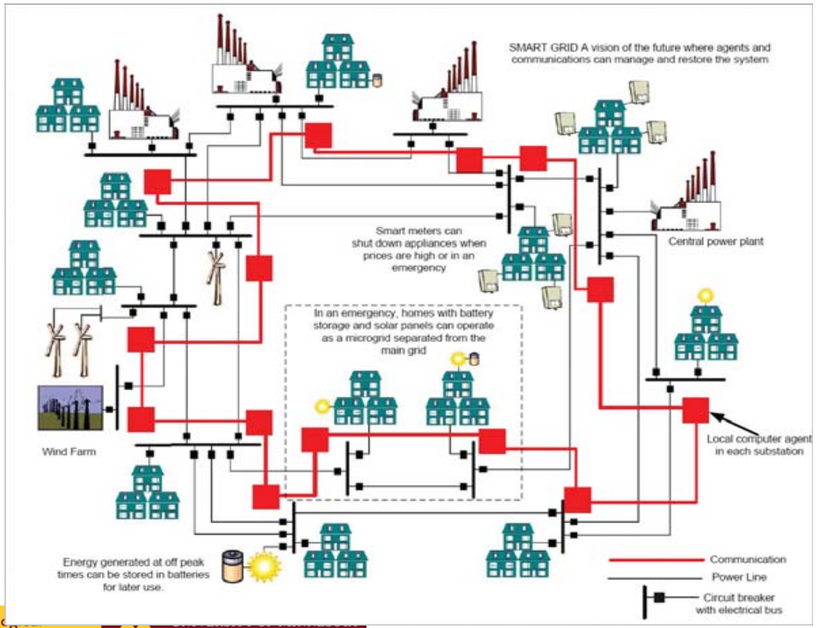
Faculty: Professors Massoud Amin and Bruce Wollenberg

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

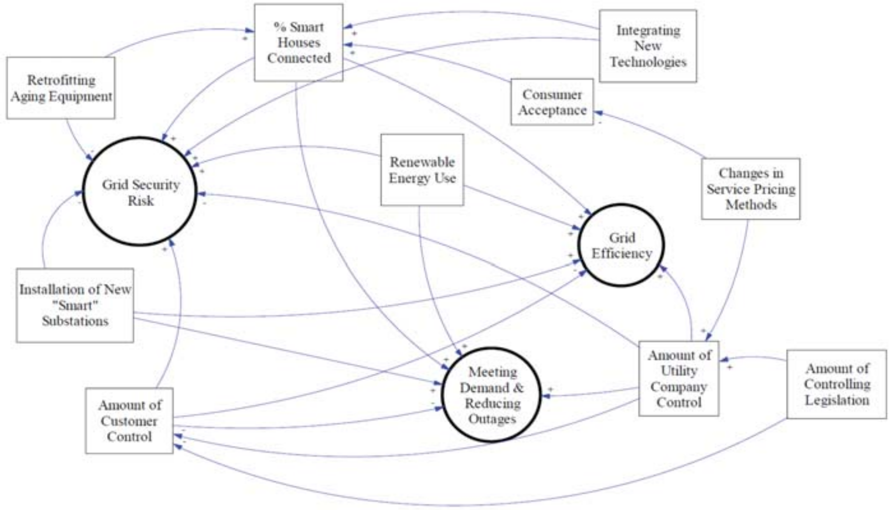
Center for Smart Grid Technologies

Our team’s Smart Grid Research



Smart Grid Interdependencies

Security, Efficiency, and Resilience



% Smart Houses Connected

Integrating New Technologies

Retrofitting Aging Equipment

Consumer Acceptance

Renewable Energy Use

Grid Security Risk

Changes in Service Pricing Methods

Grid Efficiency

Installation of New "Smart" Substations

Amount of Utility Company Control

Amount of Controlling Legislation

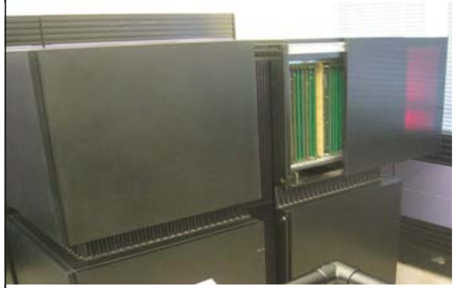
Meeting Demand & Reducing Outages

Amount of Customer Control

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

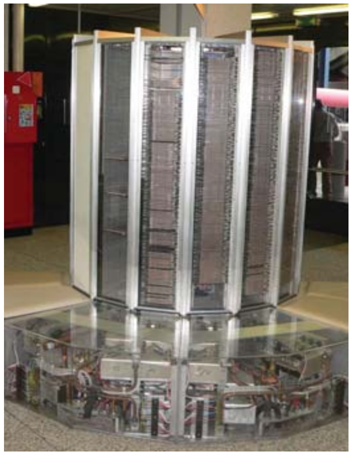
NVIDIA Tesla C870: $1300 in 2009, over 5 million sold

Building a super computer from many small processors

Up to 65,536 processors

- The IBM Blue Gene computer

Fast Power Grid Simulation



CRAY Supercomputer

Nvidia GeForce GPU card for PC

- Use Nvidia GeForce GPU card to gain 15 times faster power flow calculation on PC (Laurie Miller)

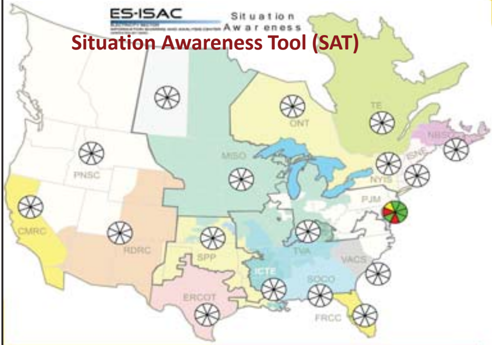
EPRI's Reliability Initiative-- Sample Screen of Real-time Security Data Display (RSDD)

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

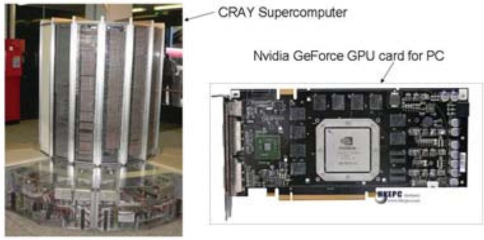
Connection Machine 2: $5 million in 1987, only a few dozen made

NVIDIA Tesla C870: $1300 in 2009, over 5 million sold



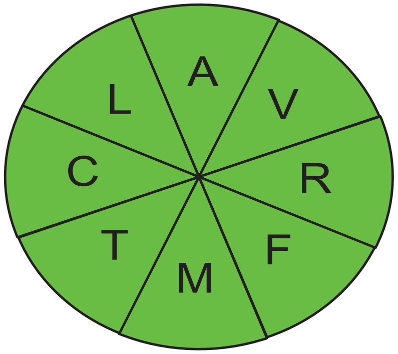
Situation Awareness Tool (SAT)

Fast Power Grid Simulation



- Use Nvidia GeForce GPU card to gain 15 times faster power flow calculation on PC (Laurie Miller)

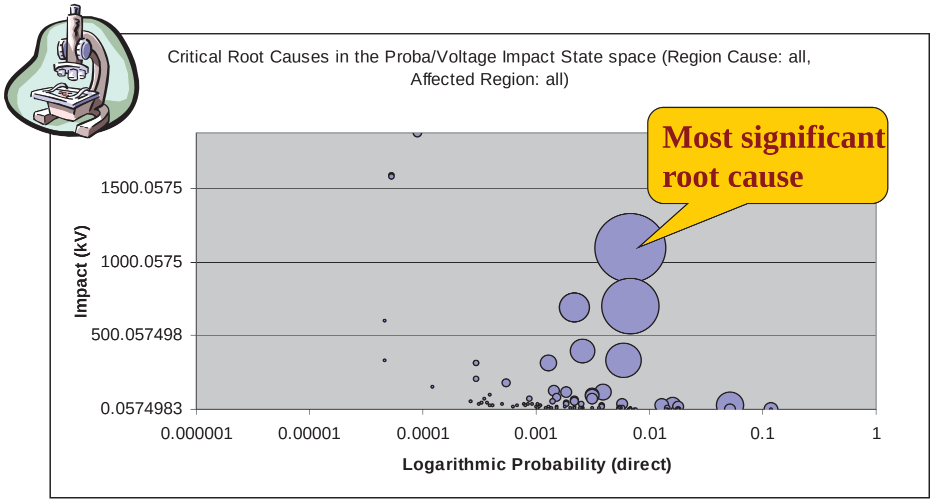
Situation Awareness Tool (SAT)



☐	No "Telemetry" Data
🟩	Data Value Nominal
🟧	Data Value Approaching Warning
🟥	Data Value in Warning Range
🟨	Data value Returned to Normal

A – ACE
L – Deviation from Forecasted Load
C – Reserve Real-power Capacity
V – Voltage Deviation from Normal
R – Reserve Reactive-power Capacity
M – Text Message
T – Transmission Constraint
F – Frequency

Example of In Depth Analysis: Critical Contingency Situations

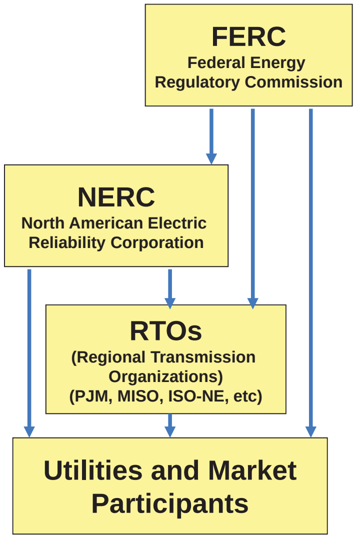


Cybersecurity

Changing Risks

Cyberspace
Cyber Activism
Cyber Insurance
Cyber War
Cyberattack
Cyber-Alert
Cyber Bullying
Cyber-ethics
Cyber crime
Cyber FININT
Cyberpower
Cybersecurity
Cyber-Commerce
Cyber Espionage
Cyber Law
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

---

October 2013-2014: A Year in Review

- December 19th→ Target Corp. announces cyber breach
- 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 disclosed to the public
- May 8th→ Ron Ross announces NIST Special Publication 800-160: Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems
- August 31st→ iCloud services hacked: Private celebrity photographs leaked

---

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

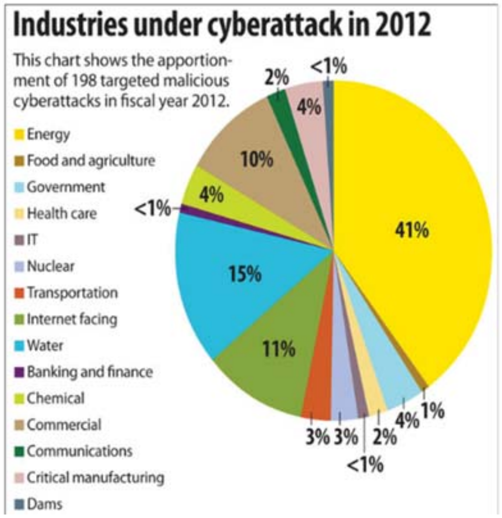
- 521 Total breaches (across all sectors)
- 17,829,689 (over 17 million) exposed records
- Government/Military experienced 10.6% of total breaches
- Medical/Healthcare category experienced 42.6% of total breaches
- Business category experienced 35.3% of total breaches

Source: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

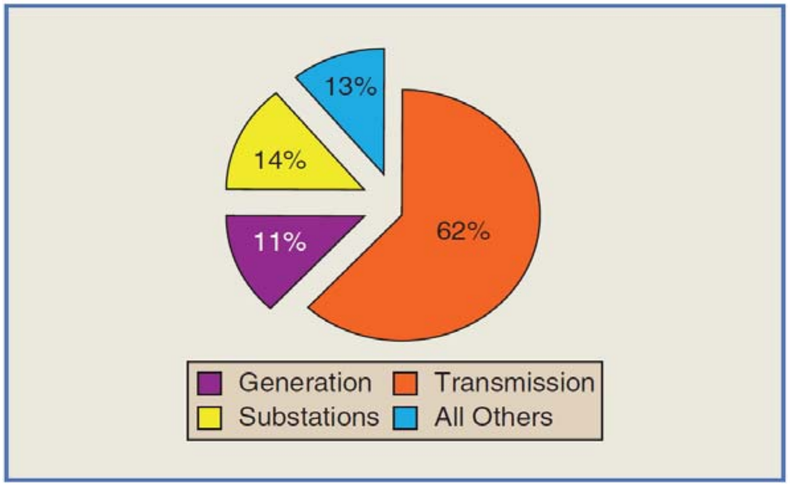
---

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



Electric Terrorism: Grid Component Targets 1994–2004

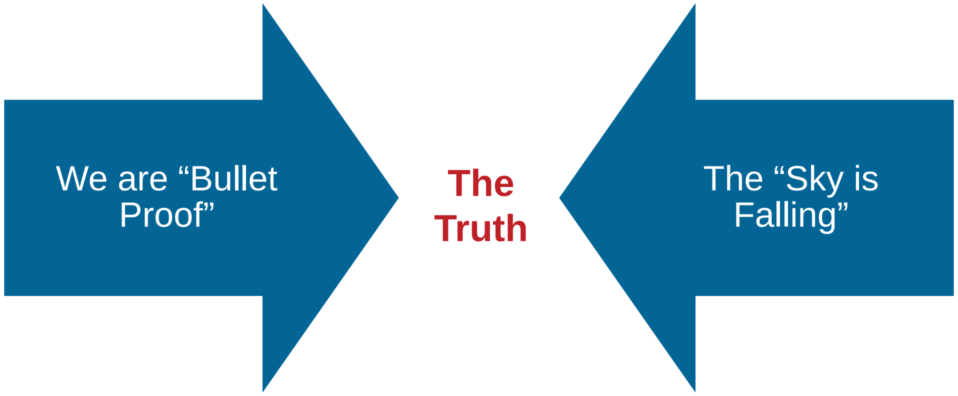


source: *Journal of Energy Security*

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



We are "Bullet Proof"

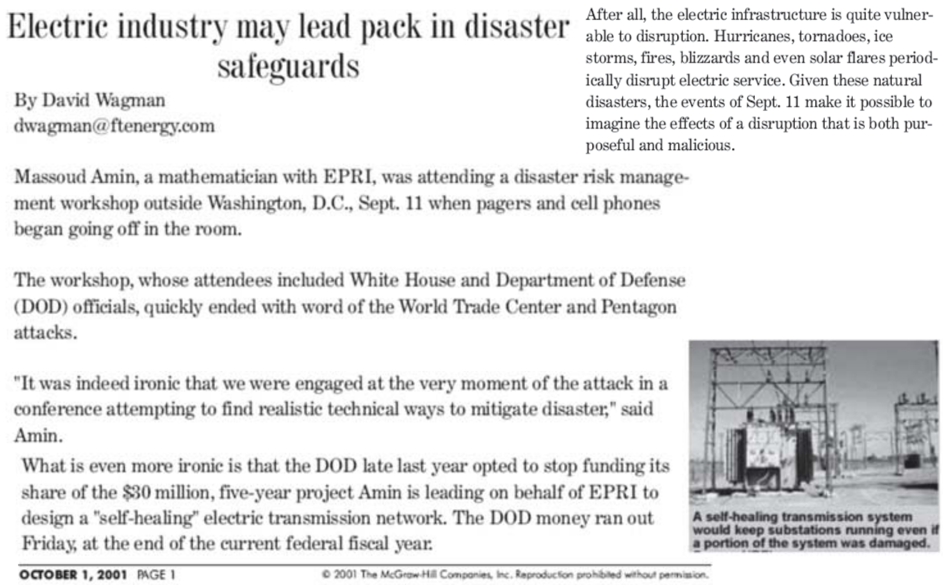
The Truth

The "Sky is Falling"

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@ftenergy.com

After all, the electric infrastructure is quite vulnerable to disruption. Hurricanes, tornadoes, ice storms, fires, blizzards and even solar flares periodically disrupt electric service. Given these natural disasters, the events of Sept. 11 make it possible to imagine the effects of a disruption that is both purposeful and malicious.

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 share of the $30 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.

A self-healing transmission system would keep substations running even if a portion of the system was damaged.

OCTOBER 1, 2001 PAGE 1

© 2001 The McGraw-Hill Companies, Inc. Reproduction prohibited without permission.

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**

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

PAST
HARD-WIRED CONTROL

- Most controls are "hard wired" AND require manual intervention
- Lesser public availability of "hacking" devices
- Little capability for damage to, or financial benefit from,attacks
- Cost-plus utility charging – "If we need it, we'll do it! If we can't do it, we'll buy it!"
- Clear regulatory and financial landscape

PRESENT
SCADA / RF ENABLED

- Intense financial pressure to reduce staffing; hence more "remote" management
- Computerization and RF control common in all industries
- Project implementation excellence not always followed by outstanding security operations
- SCADA hacking can cause ' "wholesale" damage to neighborhoods and equipment
- Uncertain regulatory, audit, and liability landscape
- Increased public and regulatory Scrutiny

NEAR FUTURE
SMART GRID / RF PERVASIVE

- Control inside-the-home of all appliances
- Wide use of 802.x, ZigBee, X10 methodologies
- Uncertain Software Provenance, Packaged Code and Offshore Development Zero-Day Attacks
- Increased organized crime/ terrorist focus
- Potential for damage to, and "net" theft by, every customer
- Revenue/Risk Asymmetry for each customer
- Transition to IP and Windows "Monoculture" for RF devices

Thus There are Multiple Scenarios to Plan For…

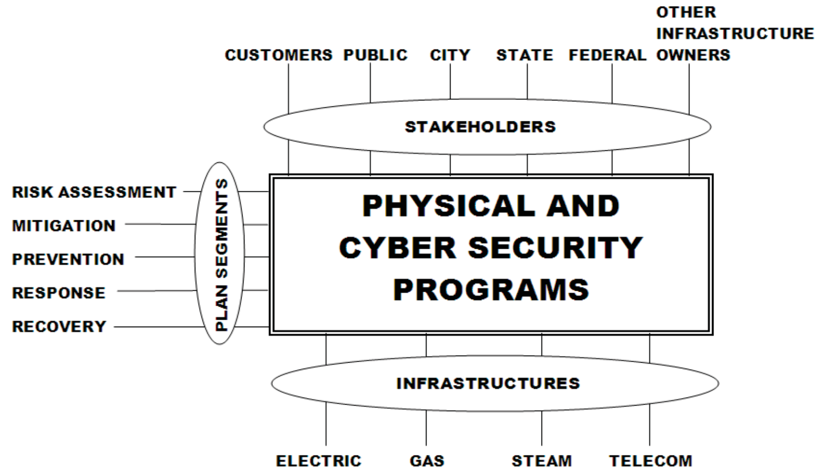
External Threat

- Power failures

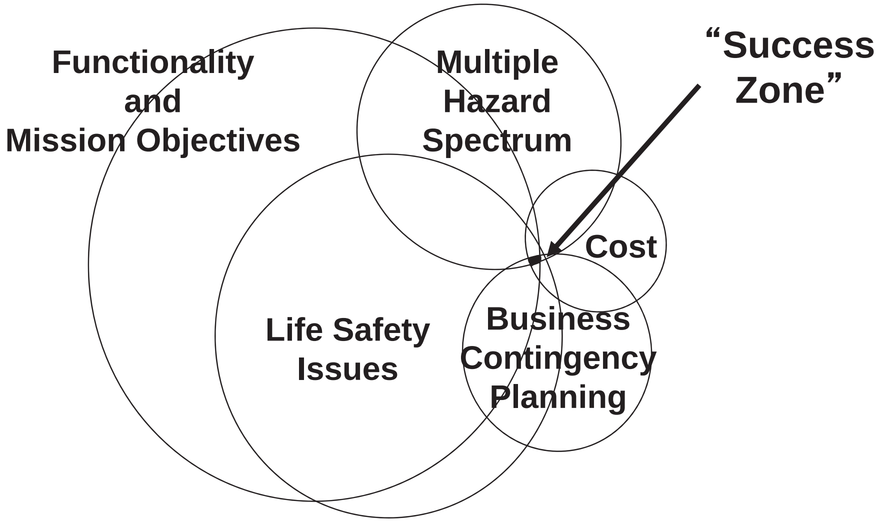
	Inadvertent	*Deliberate*
External Threat	Natural disasters Economic upheaval	Malware Denial of service Sophisticated, organized attacks
Insider Threat	Unpatched systems Code vulnerability Lack of change control Human error or carelessness	Developer-created back door Information theft Insider fraud

Insider Threat

CIP programs in the industry



Real world solutions may be elusive

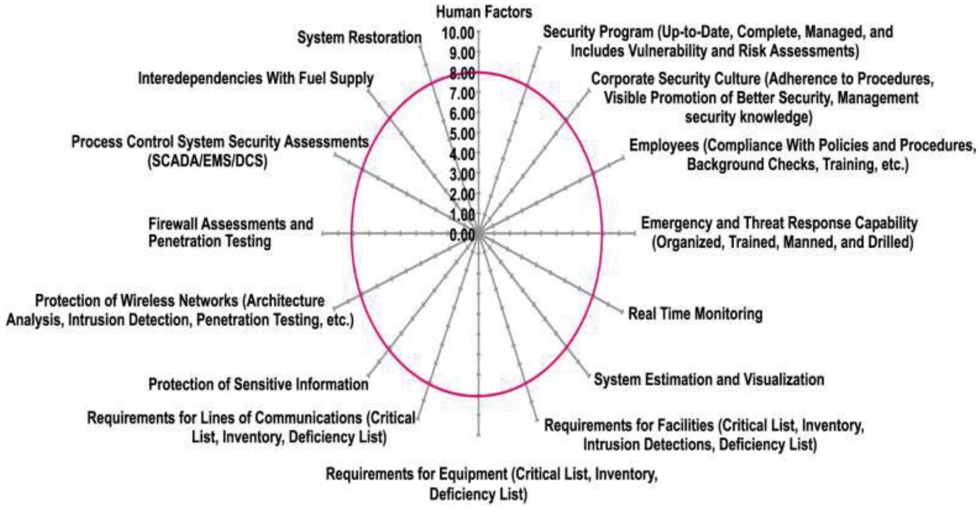


Prioritization: Security Index

General	Corporate culture
	Security Program
	Employees
	Emergency and threat response capability
Physical	Requirements for facilities, equipment and lines of communication
	Protection of sensitive information
Cyber and IT	Protection of wired and wireless networks
	Firewall assessments
	Process control system security assessments

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

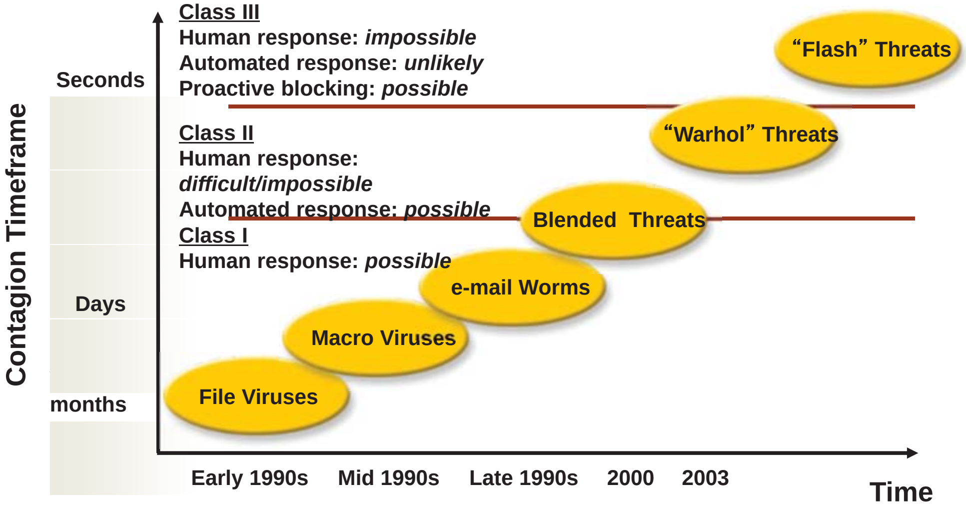
---

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



Contagion Timeframe

Seconds

Days

months

Class III
Human response: *impossible*
Automated response: *unlikely*
Proactive blocking: *possible*

Class II
Human response: *difficult/impossible*
Automated response: *possible*

Class I
Human response: *possible*

"Flash" Threats

"Warhol" Threats

Blended Threats

e-mail Worms

Macro Viruses

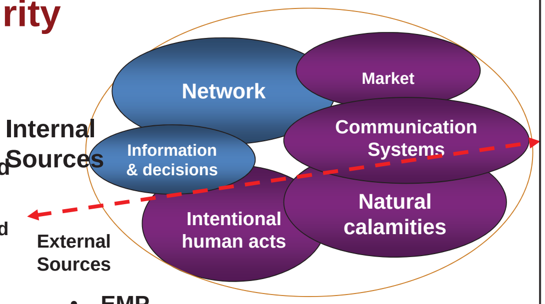
File Viruses

Early 1990s Mid 1990s Late 1990s 2000 2003

Time

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…



Internal Sources

External Sources

Network

Market

Information & decisions

Communication Systems

Intentional human acts

Natural calamities

- EMP
- Biological contamination (real or threat)
- Over-reaction to isolated incidents
- Internet Attacks
- Over 130,000 hits/day at an ISO
- Hijacking of control
- Storms, Earthquakes, Forest fires & grass, land fires… Loss of major equipment – especially transformers…

"… for want of a horseshoe nail …"

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

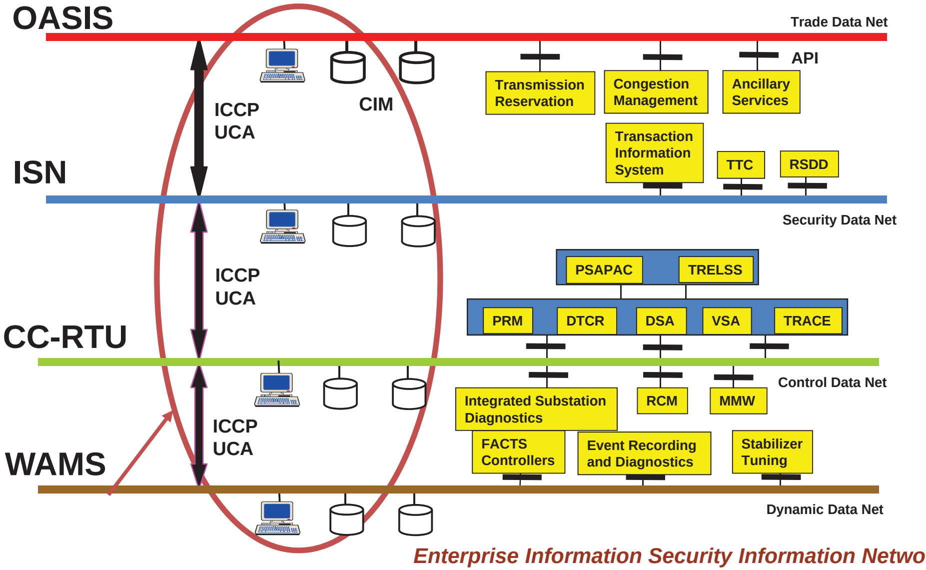
New Challenges for a Smart Grid

- 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

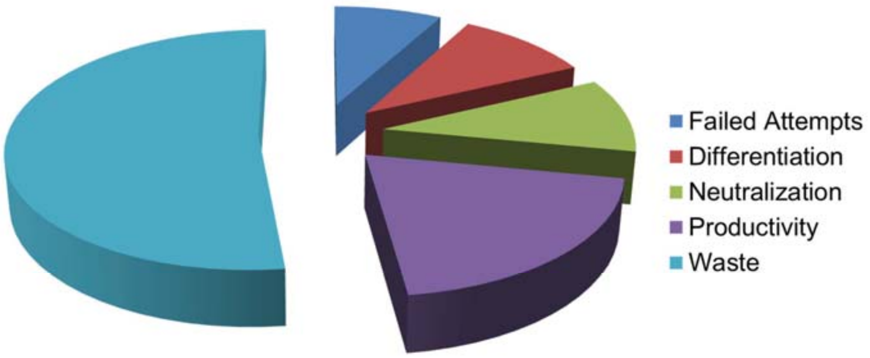
Is the Threat Real?



Enterprise Information Security Information Networks for On-Line Trade, Security & Control

---

Return on IT Innovation

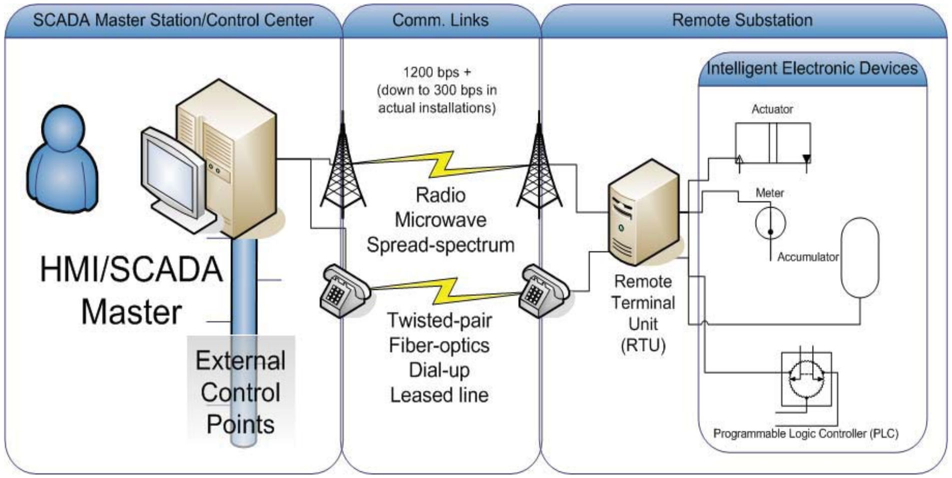


Sources of Waste:

- Differentiation projects that don't go far enough
- Neutralization projects that go beyond good enough
- Unaligned innovation efforts that cancel each other out

Control Systems Overview

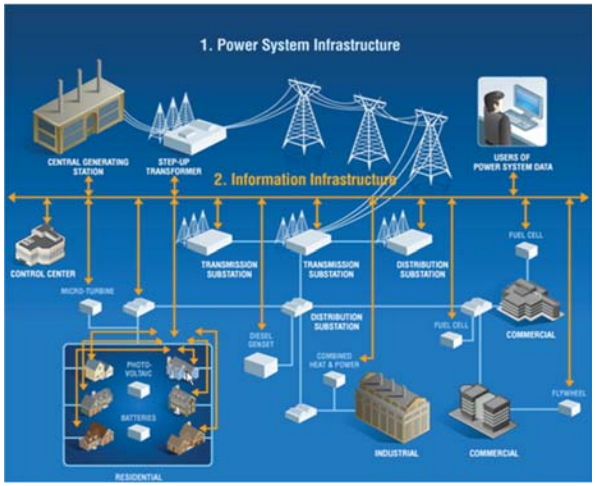
Three main components



[5] http://upload.wikimedia.org/wikipedia/en/c/ca/DNP-overview.png

---

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

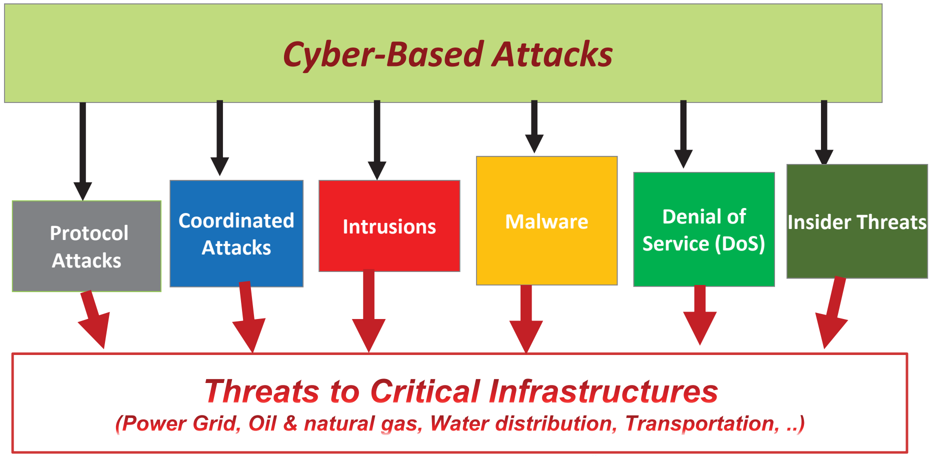
Smart Grid implies overhauling both the Power system infrastructure and the Information/Controls

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.wired.com/threatlevel/2009/11/brazil/
http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/
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



Cyber-Based Attacks

Protocol Attacks

Coordinated Attacks

Intrusions

Malware

Denial of Service (DoS)

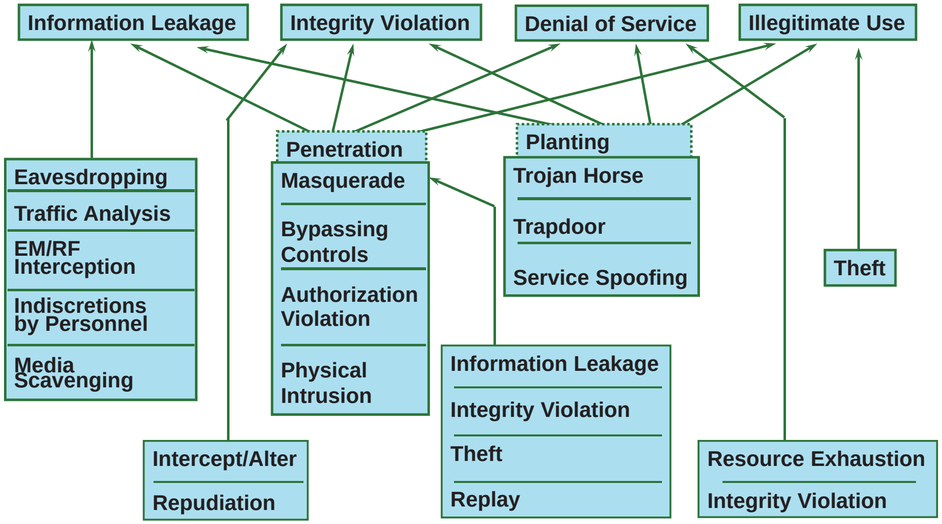
Insider Threats

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

Theft

Intercept/Alter
Repudiation

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

Threats

- Identity theft
- Information manipulation (e.g. Malware)
- Cyber Assaults/Bullying
- Advanced Persistent Threats (APTs)
- Information theft
- Crime (e.g., Credit card fraud)
- Insider
- Espionage
- Cyber attack
- Transnational
- Attack of software "boomerangs"
- Terrorism

Targets

- Government (Federal, State, and Local); e.g.,
  - E-Government
  - E-Commerce
- Industry; e.g.,
  - Aerospace & Defense
  - Banking & finance
  - Health care
  - Insurance
  - Manufacturing
  - Oil & Gas
  - Power Grid
  - Retail
  - Telecommunications
  - Utilities
- Universities/Colleges
- Individuals

Counters

- Cyber workforce
- Advanced network and resilience controls
- Outbound traffic monitoring
- Dynamic situational awareness
- Open source Information
- Risk intelligence & management
  - Forensic analysis
  - Data analytics
- Financial intelligence (FININT)
- Tighter laws & enforcement
- Expanded diplomacy
- Legislation?

You should assume that your information network has been or will be compromised.

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

"Protecting the Digital Economy", East West Institute Report from the First Worldwide Cybersecurity Summit , May 2010

70% believe that international policies and regulations are far behind technology advances

"Mobilizing for International Action", EastWest Institute Report from the Second Worldwide Cybersecurity Summit, June 2011

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)

http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

---

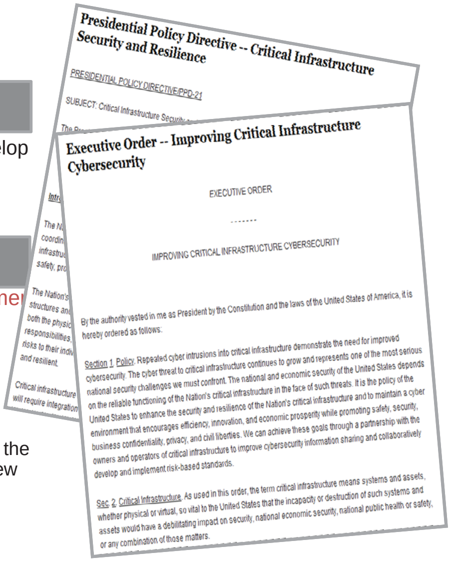
President Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity" & PPD-21 (February 12, 2013)

Goal

- Improve cybersecurity information sharing and develop and implement risk-based critical infrastructure standards through a public-private partnership.

Key Takeaways

  - Increase information sharing from governme to private sector
  - Develop Standards
- NIST leading public-private collaboration to build Cybersecurity Framework
  - Identify Critical Infrastructure
- Uses a lower threshold for critical infrastructure than the standard definition (catastrophic regional/national view versus the standard "debilitating impact")



Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

\- - - - - - -

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

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, Section 9

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

Key milestones of the Executive Order (EO)

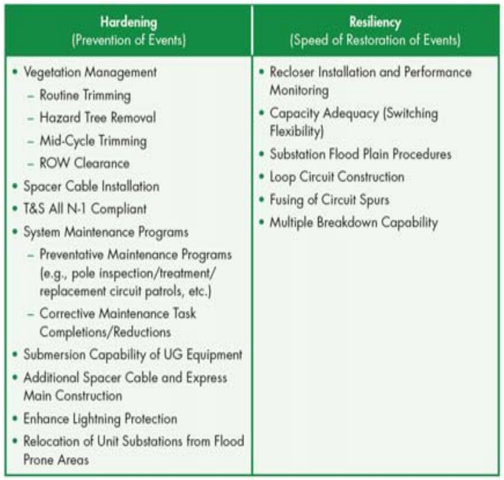
	Near-term	Mid-term	Long-term
	< 150 days	150 days to 1 year	1+ years
Private Sector	• Partner to shape development of a cybersecurity framework • Dialogue on information sharing	• New companies identified as "critical infrastructure" • Identify Cybersecurity Framework leader	• Adopt the Cybersecurity Framework • Report on impact of requirements (2 years)
Public Sector	• Broaden information-sharing process, assess privacy risks, analyze incentives (120 days) • Expand on enhanced Cybersecurity Services (120 days) • Establish voluntary program to support Framework adoption (120 days)	• Identify critical infrastructure at greatest risk • Review and comment on Cybersecurity Framework • Develop a preliminary Framework (240 days) • Look for funding and budget opportunities to implement Cybersecurity Framework	• Issue final Framework (1 year) • Report program participation and privacy risks (annually) • Review, update CI list (annually) • Report *if* current regulatory requirements are insufficient • Report on CI impacts (2 years)

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

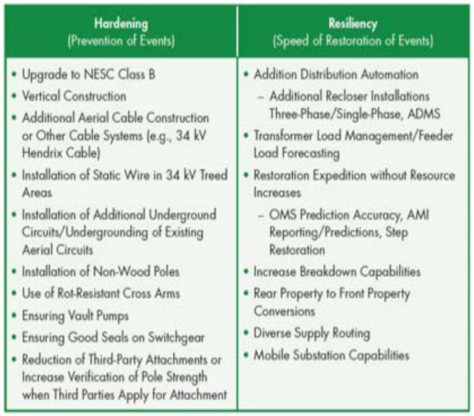
State/local government impact

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*

Storm Hardening and Grid Resiliency



Hardening (Prevention of Events)	Resiliency (Speed of Restoration of Events)
• Vegetation Management – Routine Trimming – Hazard Tree Removal – Mid-Cycle Trimming – ROW Clearance • Spacer Cable Installation • T&S All N-1 Compliant • System Maintenance Programs – Preventative Maintenance Programs (e.g., pole inspection/treatment/replacement circuit patrols, etc.) – Corrective Maintenance Task Completions/Reductions • Submersion Capability of UG Equipment • Additional Spacer Cable and Express Main Construction • Enhance Lightning Protection • Relocation of Unit Substations from Flood Prone Areas	• Recloser Installation and Performance Monitoring • Capacity Adequacy (Switching Flexibility) • Substation Flood Plain Procedures • Loop Circuit Construction • Fusing of Circuit Spurs • Multiple Breakdown Capability



Hardening (Prevention of Events)	Resiliency (Speed of Restoration of Events)
• Upgrade to NESC Class B • Vertical Construction • Additional Aerial Cable Construction or Other Cable Systems (e.g., 34 kV Hendrix Cable) • Installation of Static Wire in 34 kV Treed Areas • Installation of Additional Underground Circuits/Undergrounding of Existing Aerial Circuits • Installation of Non-Wood Poles • Use of Rot-Resistant Cross Arms • Ensuring Vault Pumps • Ensuring Good Seals on Switchgear • Reduction of Third-Party Attachments or Increase Verification of Pole Strength when Third Parties Apply for Attachment	• Addition Distribution Automation – Additional Recloser Installations Three-Phase/Single-Phase, ADMS • Transformer Load Management/Feeder Load Forecasting • Restoration Expedition without Resource Increases – OMS Prediction Accuracy, AMI Reporting/Predictions, Step Restoration • Increase Breakdown Capabilities • Rear Property to Front Property Conversions • Diverse Supply Routing • Mobile Substation Capabilities

Source: EPRI 2013, Craig Adams, PECO, EPRI RAC member
Industry Considerations for Hardening/Resiliency

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:

- Protect the user from the network, and protect the network from the user: Develop tools and methods to reduce complexity for deploying and enforcing security policy.
- 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
- Mandate security for the Advanced Metering Infrastructure, providing protection against Personal Profiling, guarantee consumer Data Privacy, Real-time Remote Surveillance, Identity Theft and Home Invasions, Activity Censorship, and Decisions Based on Inaccurate Data
- 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

Critical infrastructure sectors		
Agriculture and Food	Dams	Information Technology
Banking and Financial Services	Defense Industrial Base	Nuclear Reactors, Materials and Waste
Chemical	Emergency Services	Transportation Systems
Commercial Facilities	Energy	Water and Wastewater Systems
Communications	Government Facilities	Critical Manufacturing
	Healthcare and Public Health	

---

[1] GAO Report, Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. July 2007, http://www.gao.gov/assets/100/95010.pdf

Enabling secure, reliable and resilient systems

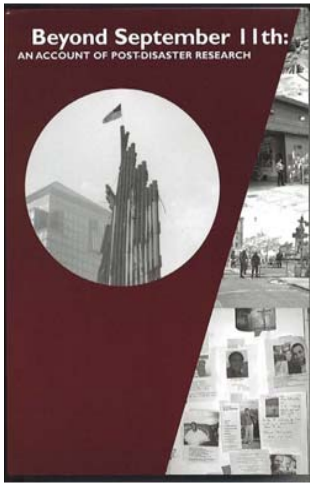
Enabling secure, reliable and resilient systems requires people and organizations that can….

- 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



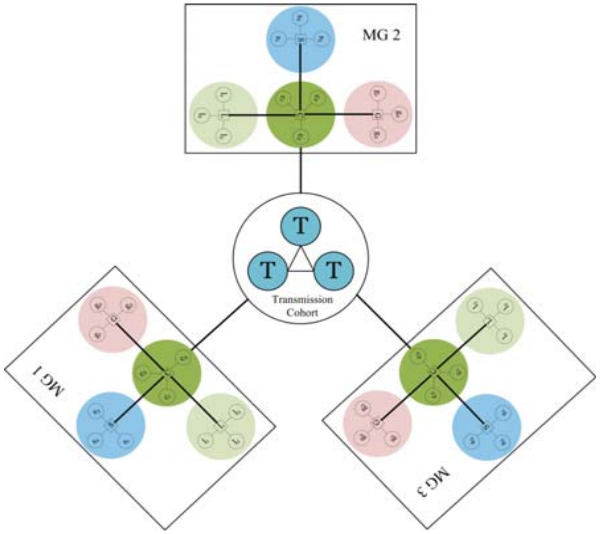
Beyond September 11th:
AN ACCOUNT OF POST-DISASTER RESEARCH

⌘	resilience:	ability to recover quickly
⌘	robustness:	failure-resistant through design and/or construction
⌘	redundancy:	duplicative capacity for service delivery

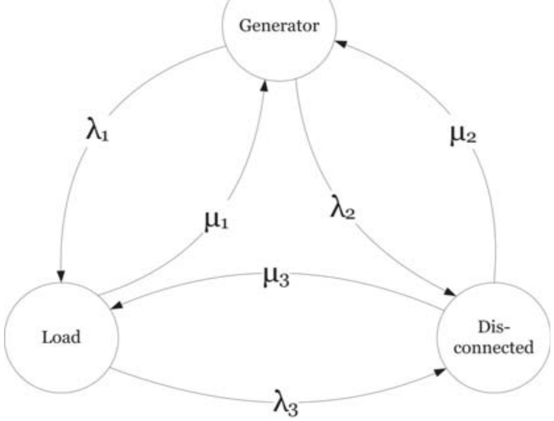
Verizon, AT&T, ConEd, and MTA (among others) possessed all these attributes in equipment and people

Natural Hazards Research and Applications Information Center

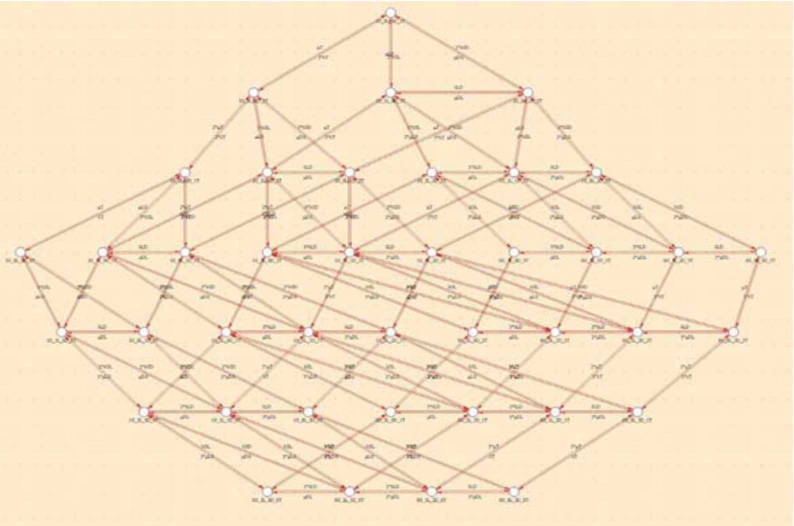
An Example:
Three Interconnected Multi-Agent Microgrids



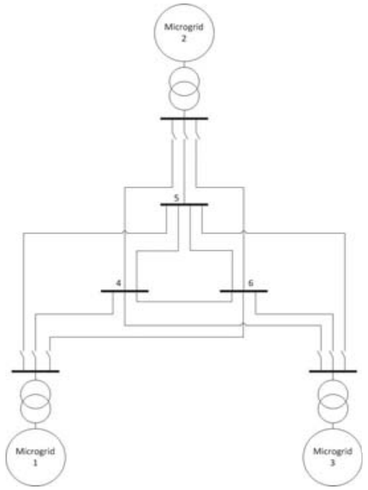
Markov Closed-Form Solution: State Transition Diagram for Each Microgrid



State Transition Diagram for Three Interconnected Microgrids



Monte Carlo Simulation Test Case



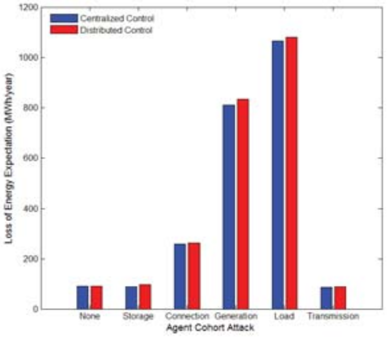
Parameter	Value
Microgrids in Assembly	3
Loads per Microgrid	3
Load Real Power (kW)	100
Load Reactive Power $(kVAR)$	50
Generators per Microgrid	3
Generator Real Power max. (kW)	130
Generator Real Power min. (kW)	25
Generator Reactive Power max. $(kVAR)$	100
Generator Reactive Power min. $(kVAR)$	-100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

Transition Rates

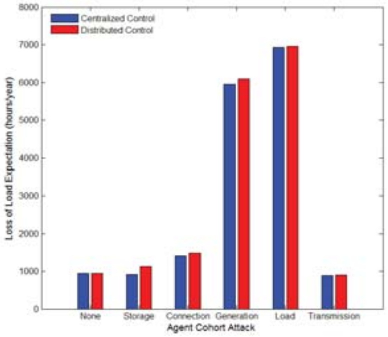
	Availability	λ (failures/year)	μ (repairs/year)	$MTTF$ (h)	$MTTR$ (h)
Transformer	0.99	3.69	365	2374	24
Busbar	0.99	3.69	365	2374	24
Generator	0.9	8.11	73	1080	120
Storage Unit	0.85	32.21	182.5	272	48
Line	0.95	9.61	182.5	912	48
Switch	0.95	9.61	182.5	912	48
Agent	0.97	20	730	438	12

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

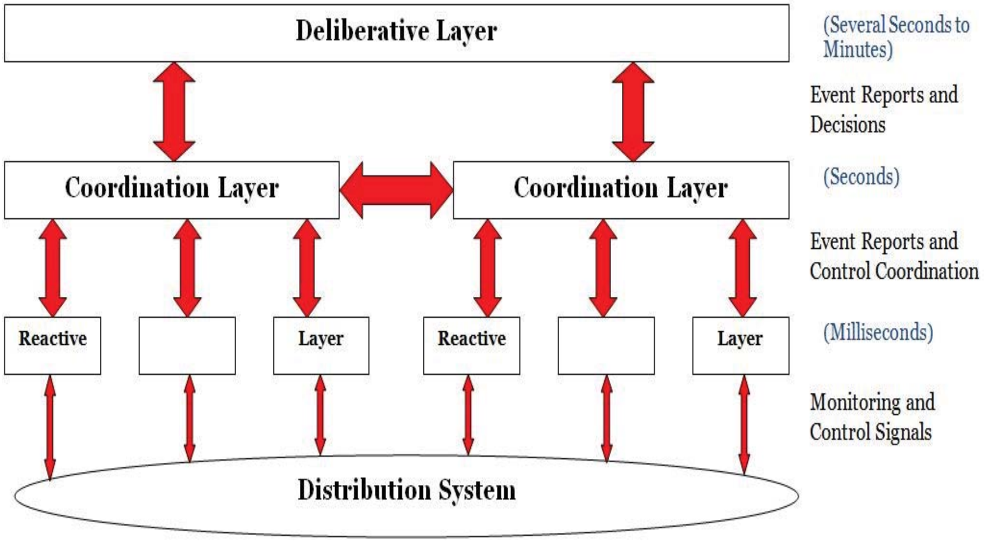
Analytical Models

- 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

Intelligent Distributed Secure Distribution System Control Architecture



(Several Seconds to Minutes)

Event Reports and Decisions

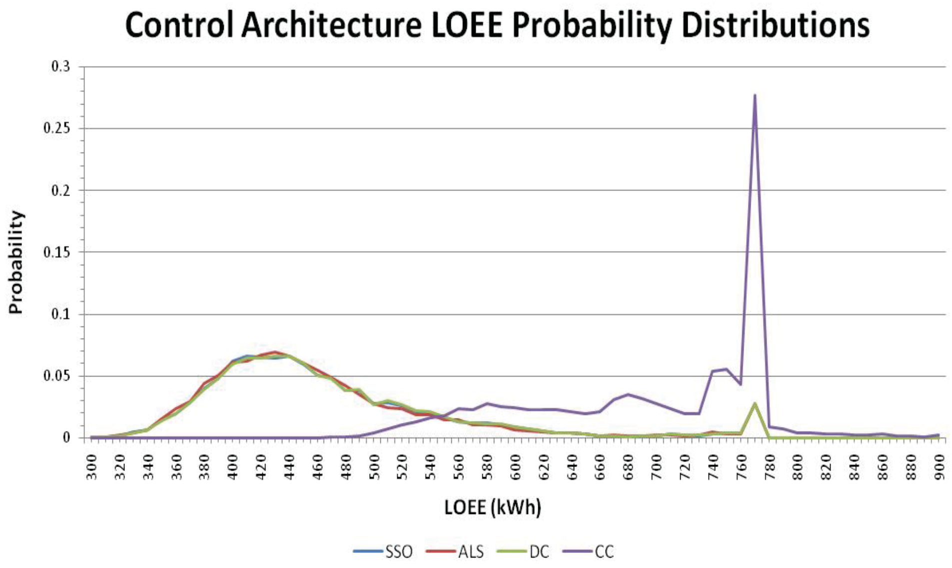
(Seconds)

Event Reports and Control Coordination

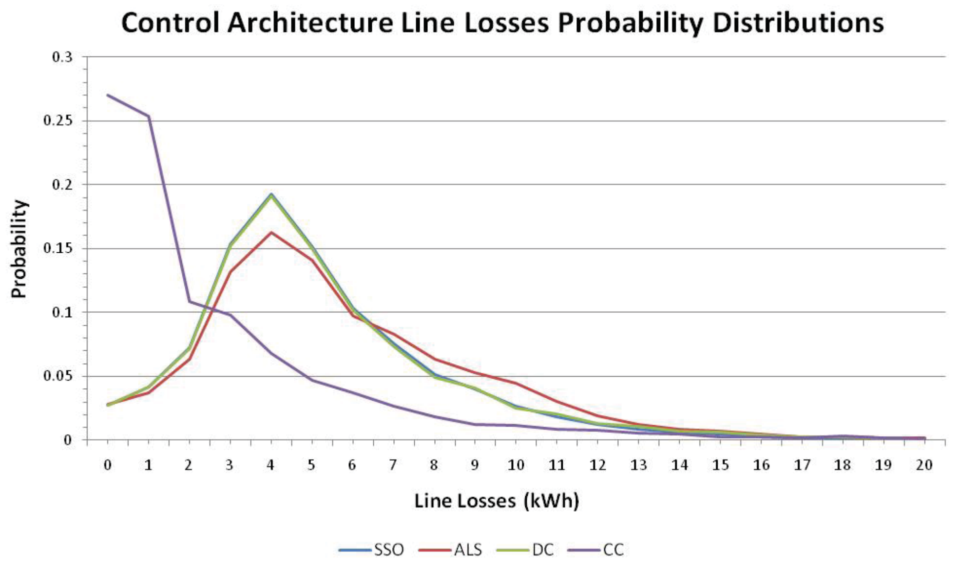
(Milliseconds)

Monitoring and Control Signals

Centralized or Decentralized Control?

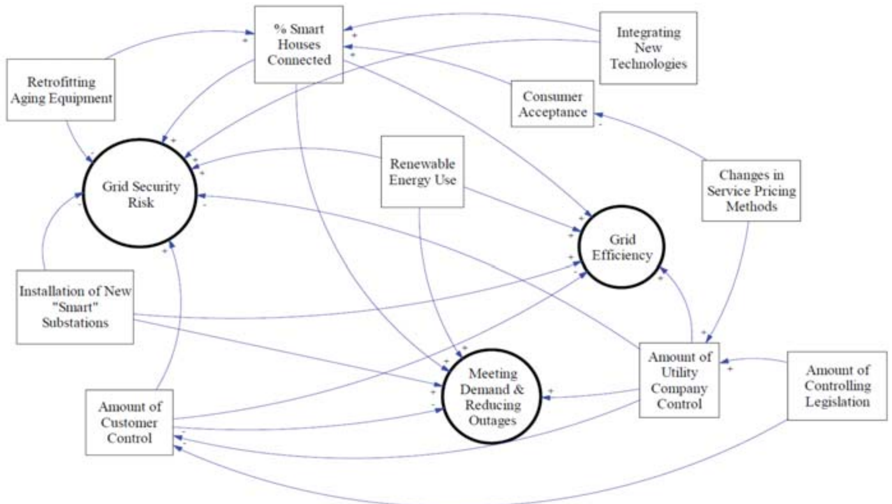


Centralized or Decentralized Control?



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

$$\underset{X,Y}{\text{minimize}} \quad \alpha \sum_{i=1}^{n} N_i * CDF_i\,(t_o - Y_i t_s) + (1-\alpha) \sum_{j=1}^{t} C_j X_j \qquad s.t.$$

(1) $t_s = \dfrac{\sum_{j=1}^{t} X_j S_j}{\sum_{i=1}^{n} Y_i D_i}$

(2) $X_j \in \mathbb{Z}_n \forall\, j$

(3) $Y_i \in \{0,1\} \forall\, i$

(4) *Power System Operating Constraints*

Where,
i: Load index $\epsilon \{1 \ldots . n\}$
j: Storage type index $\epsilon \{j \ldots . s\}$
Y_i : Emergency service indicator variable for load i
X_j : Number of storage systems of type j selected
N_i: Number of customers of given type at load i
$CDF_i(*)$: Non-linear customer damage function
t_o: Duration of system outage (min)
t_s: Duration storage to serve emergency loads
S_{cap}: kWh capacity of storage facility
D_i: kW demand of load i
Cj: Capital cost of storage unit type j

Prioritizing Emergency Backup Service

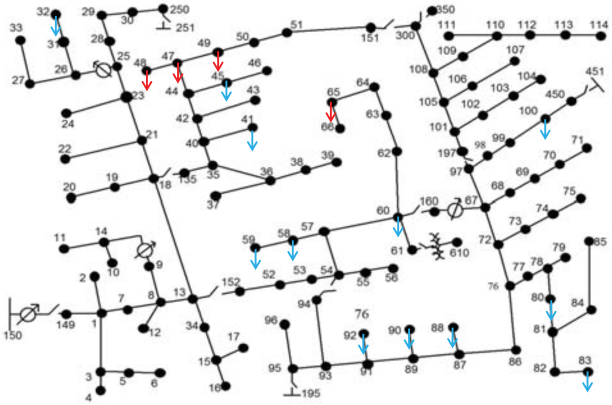
SYSTEM CHARACTERISTICS	
Voltage (kV)	4.16
Number of Loads	85
Peak Load	3490 kW at 0.88 PF
Number of Customers	513
Large C&I Customers	10
Medium C&I Customers	62
Residential Customers	441

Simulated Outage

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

LOADS SERVED
- **Small C&I** ↓
- **Large C&I** ↓

123 IEEE Test Feeder Model



Customer Outage Costs (2008$)	Large C&I	Med C&I	Res.	Total	Loads Served
No Storage	95,900	98,260	3,550	197,710	0
With Storage - All Loads	88,610	91,400	3,390	183,450	All 85
With Storage - Selective Service	35,900	84,980	3,550	124,430	19

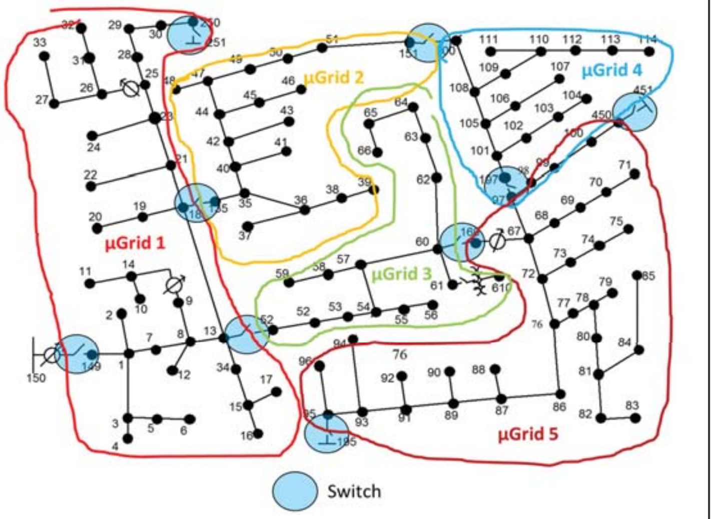
Feeder Reconfiguration/Intentional Islanding

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



Energy Storage for C&I Applications

Energy Storage for Commercial and Industrial Applications	Maturity	Capacity (kWh)	Power (kW)	Duration (hrs)	Efficiency (%)	Cycle Life (cycles)	Total Cost ($/kW)	Cost ($/kW-h)
Advanced Lead-Acid 1	Demo-Commercial	5000	1000	5	85	4500	3000	600
Advanced Lead-Acid 2	Demo-Commercial	1000	200	5	80	4500	3600	720
NaS	Commercial	7200	1000	7.2	75	4500	3600	500
Zn/Br Flow 1	Demo	625	125	5	62	>10000	2420	485
Zn/Br Flow 2	Demo	2500	500	5	62	>10000	2200	440
Vanadium Flow	Demo	1000	285	3.5	67	>10000	3800	1085
Li-Ion	Demo	625	175	3.5	87	4500	3800	1085

* Rastler D., "Electricity Energy Storage Technology Options – A White Paper Primer on Applications, Costs and Benefits", EPRI, 2010

Single Customer Multi-Objective Optimization Model

Objective 1: Minimize Outage Costs

$$\underset{Y}{\text{minimize}} \sum_{n=1}^{N_{outage}} CDF\,(t_o - P_{load,n} \sum_{j=1}^{J_{types}} \frac{X_j}{S_{BESS,j}})$$

Objective 2: Minimize Energy Costs

$$\underset{SOC}{\text{minimize}} \sum_{t=1}^{T} (P_{load,t} - P_{gen,t} + P_{BESS,t}) C_{e,t} \Delta t$$

Objective 3: Minimize Demand Costs

$$\underset{SOC}{\text{minimize}} \sum_{p=1}^{P} \left(max\left(P_{load,t} - P_{gen,t} + P_{BESS,t}\right)_p + PF_p \right) C_{d,p}$$

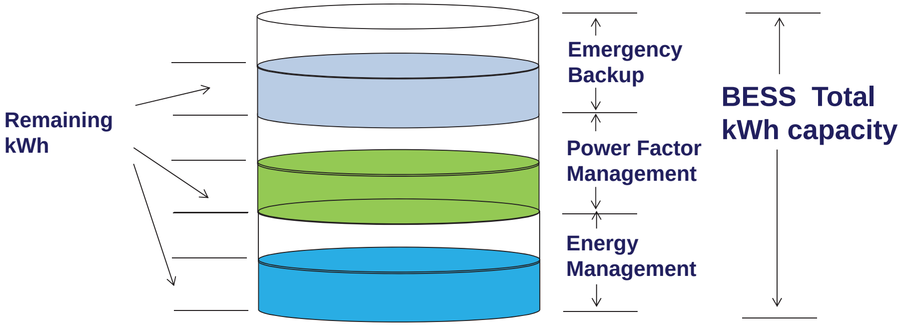
Objective 4: Minimize Capital Costs

$$\underset{X}{\text{minimize}} \sum_{j=1}^{t} C_j X_j$$

Where,
n: Outage index $\epsilon \{1 \dots . N_{outage}\}$
$CDF_i(*)$: Customer damage function
t_o: Duration of outage (min)
j: Storage type index $\epsilon \{j \dots . s\}$
X_j : Number of storage systems of type j selected
$P_{load,n}$: Ave. load during outage, n
$S_{BESS,j}$: kWh storage capacity
S_{cap}: kWh capacity of storage facility
Cj: Capital cost of storage unit type j

Multi-Application Energy Storage

Approach: Partition energy storage capacity according to application



Remaining kWh

Emergency Backup

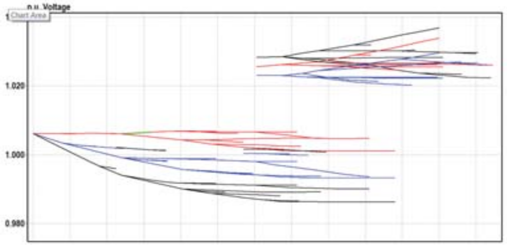
Power Factor Management

Energy Management

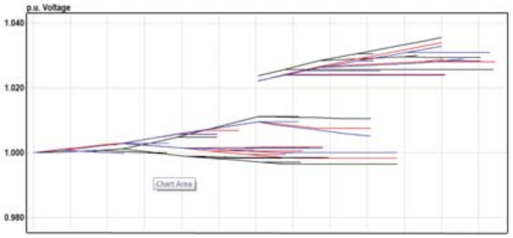
BESS Total kWh capacity

Voltage Profiles

Normal Operation:
1.04 – 0.98pu voltages



Priority Ride-Through:
1.04 – 0.99pu voltages

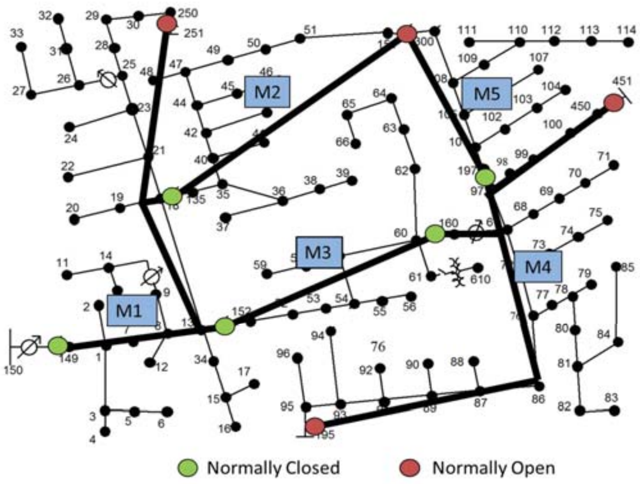


Distribution Reliability Analysis

- **Failure rate, λ**: 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)**
- $SAIFI = \frac{\sum N_s \lambda_s}{\sum N_s} = Average\ number\ of\ interruptions\ per\ customer\ served$
- **System Average Interruption Duration Index (SAIDI)**
- $SAIDI = \frac{\sum N_s \lambda_s r_s}{\sum N_s} = System\ wide\ average\ interruption\ duration$
- **Customer Average Interruption Duration Index (CAIDI)**
- $CAIDI = \frac{\sum N_s \lambda_s r_s}{\sum N_s \lambda_s} = Average\ outage\ duration\ experienced\ by\ a\ customer$

Feeder Main Reliability Analysis



Optimal Mix and Placement

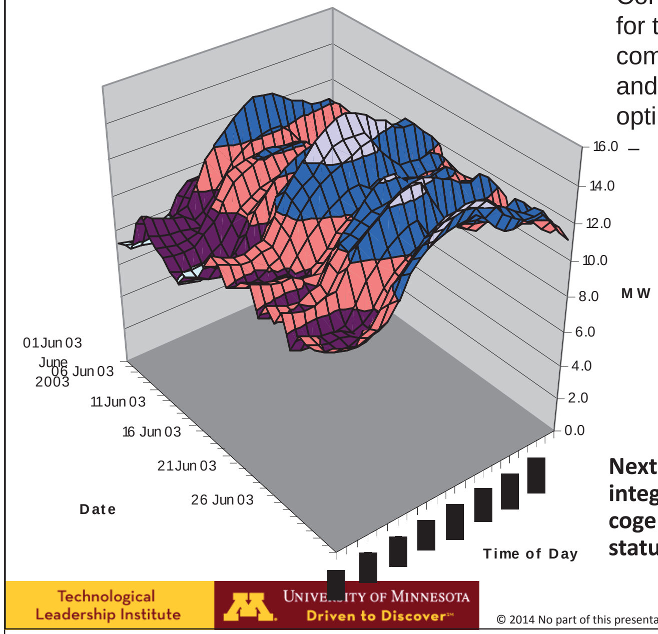
No. Units Selected	BESS Selected	Location	Capital Cost	Added Savings	Annual Outage Costs	Payback Period
0	None	--	$ 0	--	$ 1,435,814	---
1	Zinc Bromine 1	M4	$ 303,125	$ 285,776	$ 1,150,038	*1.06 years*
2	Zinc Bromine 1	M4	$ 606,250	$ 207,749	$ 942,289	*1.23 years*
3	Zinc Bromine 1	M4	$ 909,375	$ 224,758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

Index	M1	M2	M3	M4	M5
Total Cust.	200	85	44	72	112
Cust. Served	0	0	4	35	0
SAIDI: 3.93 (down 0.44)		*SAIFI: 5.90 (down 0.66)*		*CAIDI: 1.5 (same)*	

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.

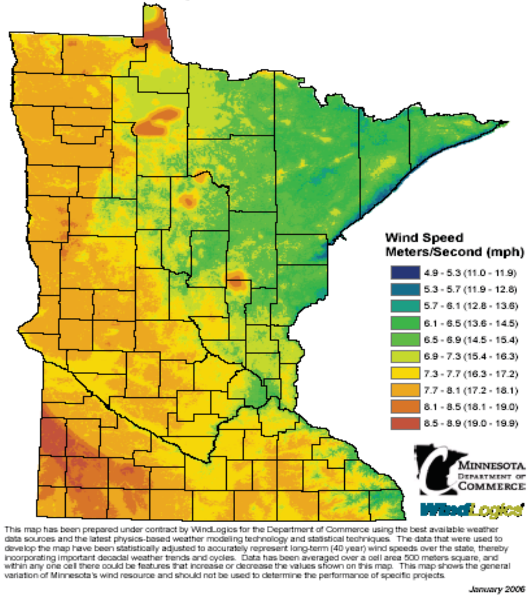
Smart Grid U™



- 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.

Minnesota's Wind Resource by Wind Speed at 80 Meters



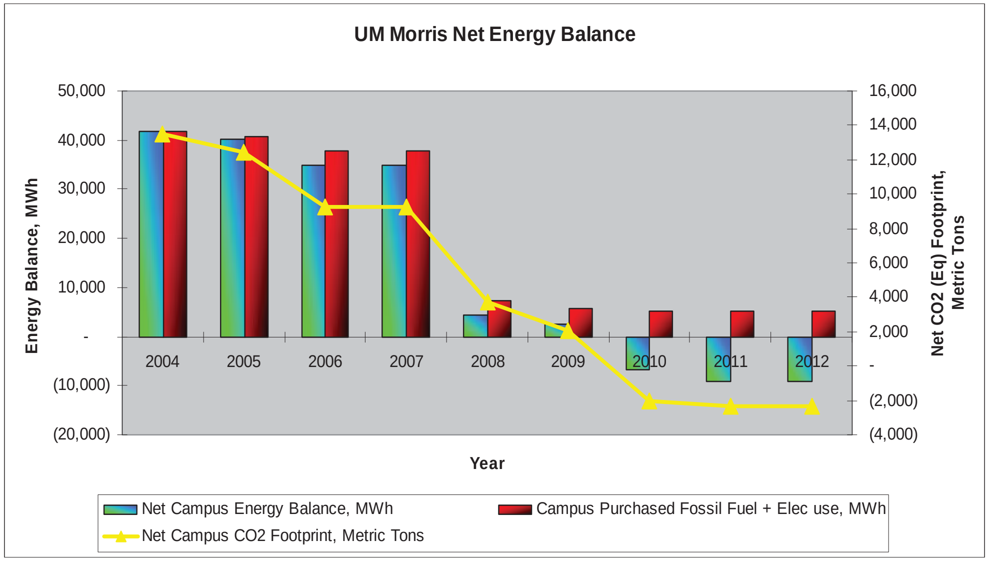
This map has been prepared under contract by WindLogics for the Department of Commerce using the best available weather data sources and the latest physics-based weather modeling technology and statistical techniques. The data that were used to develop the map have been statistically adjusted to accurately represent long-term (40 year) wind speeds over the state, thereby incorporating important decadal weather trends and cycles. Data has been averaged over a cell area 500 meters square, and within any one cell there could be features that increase or decrease the values shown on this map. This map shows the general variation of Minnesota's wind resource and should not be used to determine the performance of specific projects.

January 2006

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’s electricity needs)
- Load 300,000-750,000 kWh/month

Going Carbon Negative…

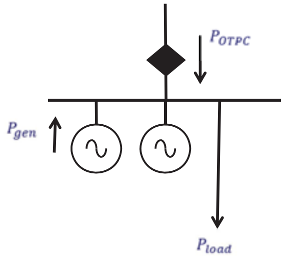


University of Minnesota - Morris

CURRENT SYSTEM

$P_{OTPC} = P_{load} - P_{gen}$

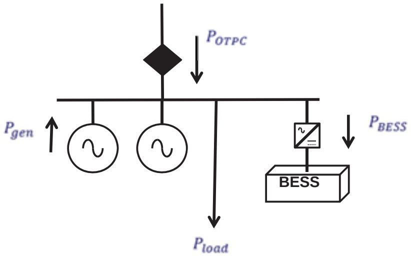
Otter Tail Power Company



PROPOSED SYSTEM

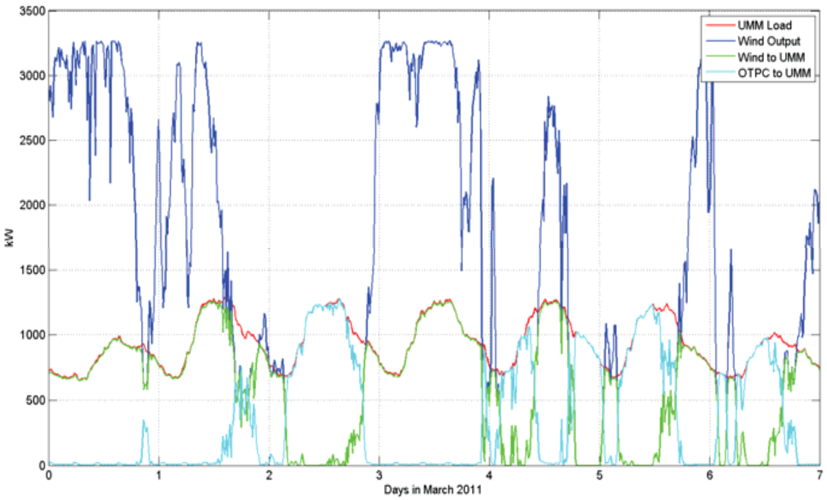
$P_{OTPC} = P_{load} - P_{gen} + P_{BESS}$

Otter Tail Power Company

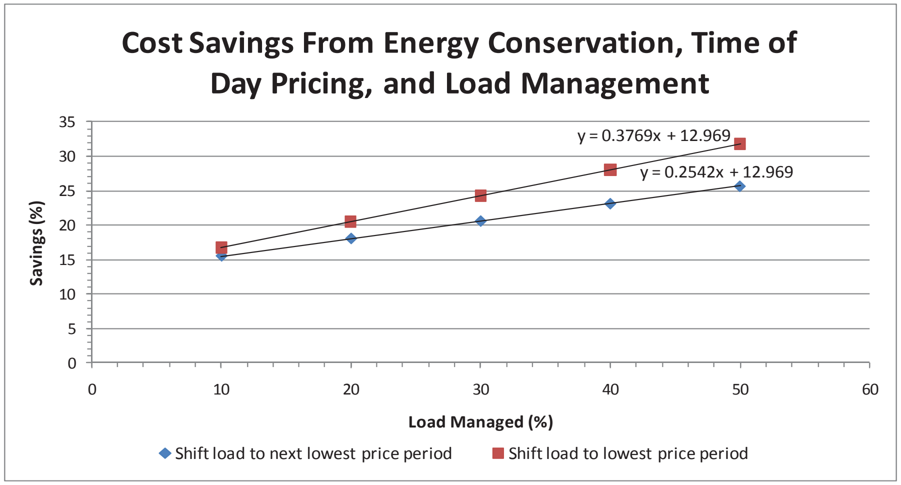


Pgen = 2 x 1.65 MW Wind Turbines
Pload = 1.5 MW Peak

UMMorris – Typical Week in 2011



DR: Total Cost Savings


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

---

DR: Total Cost Savings (cont.)

Load Managed (%)	Savings ($)	Savings (%)
Load Shifted to Next Lowest Price Period		
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		
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

Smart Grid Assessment for UMore Park

Smart Grid assessment for UMore Park

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

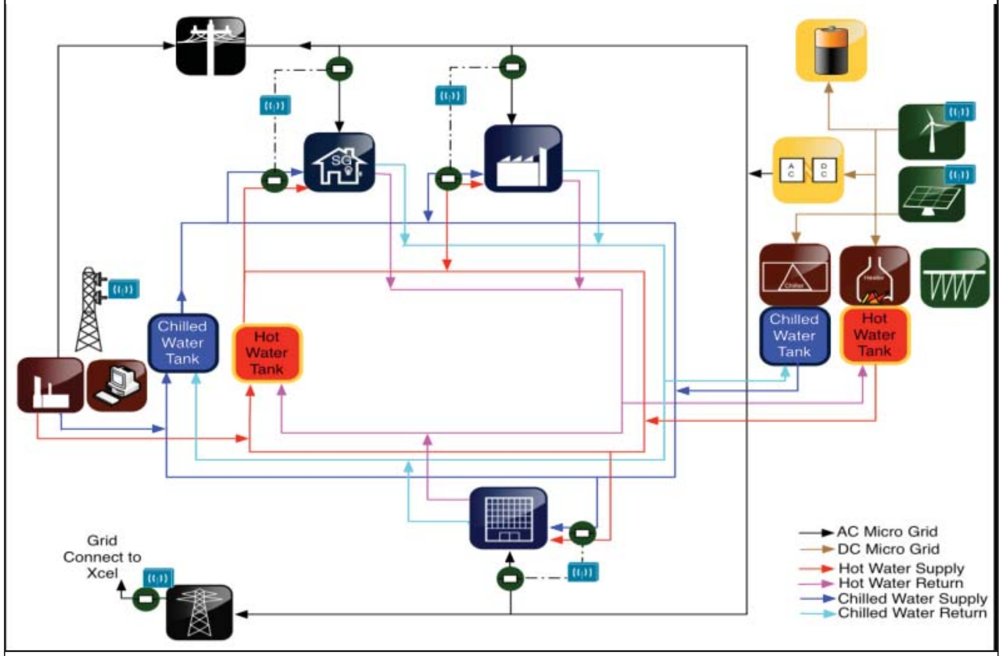
Estimated Prices for Energy-Efficient, Smart Grid Ready Homes in UMore Park

	Square Foot Range			Estimated Home Pricing		
	Low	High	Average	Low	High	Average
Small Lot	1,600	2,500	2,050	$225,000	$350,000	$287,500
Traditional	1,800	2,800	2,300	$225,000	$410,000	$317,500
Large Lot						

	Price Ranges			Cost Over Traditional Home		
	Low	High	Average	Low	High	Average
Small Lot	$244,920	$379,920	$312,420	$19,920	$29,920	$24,920
Traditional	$244,920	$444,720	$344,820	$19,920	$34,720	$27,320
Large Lot	$487,920	$784,920	$636,420	$37,920	$59,920	$48,920

Average prices are within range of the low-high estimated home prices for UMore Park

UMore Park: District Energy and Smart Grid Options

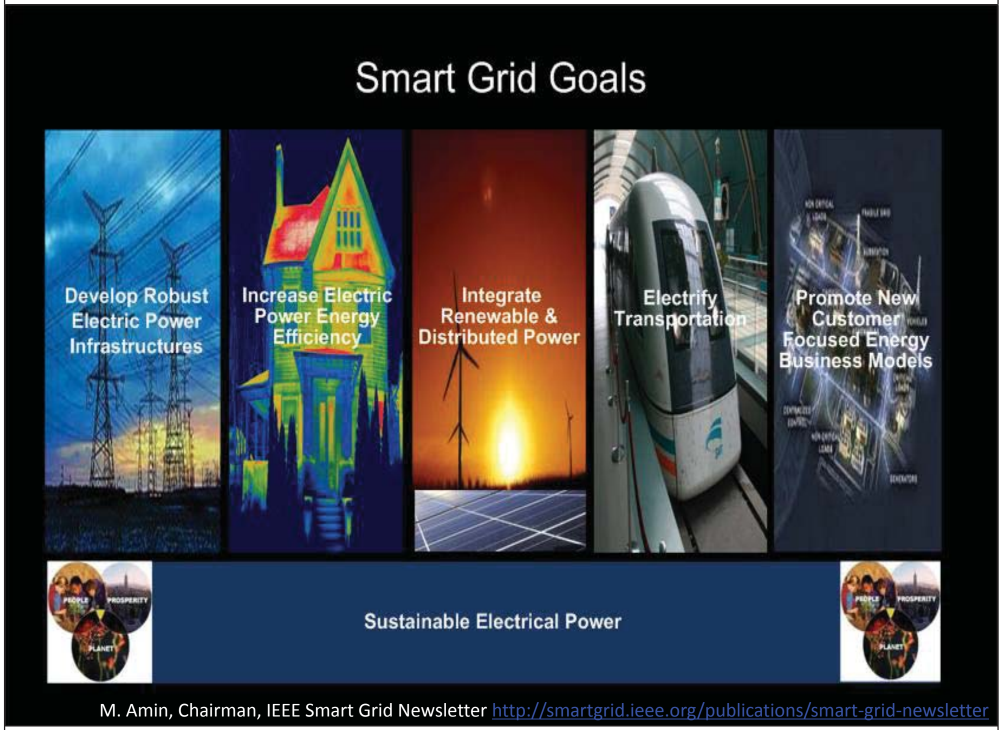


Smart Grid U™

- 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.**

Technological Leadership Institute

University of Minnesota
Driven to Discover℠



Smart Grid Goals

M. Amin, Chairman, IEEE Smart Grid Newsletter http://smartgrid.ieee.org/publications/smart-grid-newsletter

---

Selected References

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

- **“Smart Grids,”** (Amin and Giacomoni) in *Climate Change: An Encyclopedia of Science and History*, B. C. Black et al., Eds. Santa Barbara: ABC-CLIO, LLC, 2013, pp. 1243-1255.
- **"Analysis, modeling, and simulation of autonomous microgrids with a high penetration of renewables,"** (Giacomoni, Goldsmith, Amin and Wollenberg), *IEEE Power and Energy Society General Meeting*, San Diego, CA, July 2012
- **“Securing the Electricity Grid,”** (Amin), *The Bridge,* the quarterly publication of the National Academy of Engineering, Volume 40, Number 1, Spring 2010
- **"For the Good of the Grid: Toward Increased Efficiencies and Integration of Renewable Resources for Future Electric Power Networks,"** (Amin), *IEEE Power & Energy Magazine*, Vol. 6, Number 6, pp. 48-59, November/December 2008
- **“Preventing Blackouts,"** (Amin and Schewe), Scientific American, pp. 60-67, May 2007
- **“Electricity Infrastructure Security,”** (Amin) Chapter 9 in The CRC *Handbook of Energy Conservation and Renewable Energy* Y.D. Goswami, and F. Kreith (editors), 24 pp., CRC Press, 2006
- **“Powering the 21st Century: We can -and must- modernize the grid,"** IEEE Power & Energy Magazine, pp. 93-95, March/April 2005
- **"Toward Self-Healing Energy Infrastructure Systems,“** cover feature in IEEE Computer Applications in Power, pp. 20-28, Vol. 14, No. 1, January 2001

Technological Leadership Institute

University of Minnesota
Driven to Discover℠

Dr. S. Massoud Amin

TECHNOLOGICAL
LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

http://tli.umn.edu
Email: amin@umn.edu
http://massoud-amin.umn.edu/
http://www.LinkedIn.com/in/massoudamin

@Massoud_Amin

smartgrid.ieee.org

1 ______
2 ______
3 ______
4 ______
5 ______
6 ______
7 ______
8 ______
9 ______