Critical Infrastructure Security and Protection: R&D Challenges in Infrastructure Security and Defense

S. Massoud Amin, D.Sc.
Director Technological Leadership Institute and Honeywell/HW Sweatt Chair
University Distinguished Teaching Professor
Professor of Electrical & Computer Engineering, University of Minnesota
Vice Chairman, Board of Directors, Texas Reliability Entity
Board of Directors, Midwest Reliability Organization

Keynote address at the 6th Int'l Symposium on Resilient Control Systems (ISRCS), San Francisco, CA, August 14, 2013

Material from the Electric Power Research Institute (EPRI), and support from EPRI, NSF, ORNL Honeywell and SNL for my graduate students' doctoral research is gratefully acknowledged.

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

Copyright © 2013 No part of this presentation may be reproduced in any form without prior authorization.

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?"

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Infrastructure Security

We are "Bullet Proof"

The Truth

"The Sky is Falling"

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

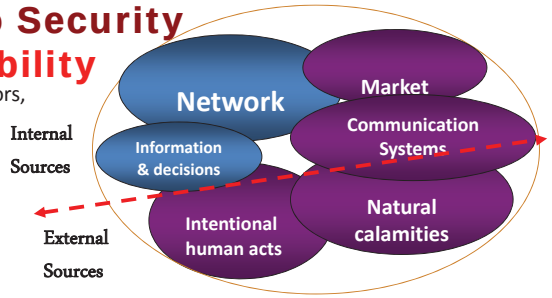
Context: Threats to Security

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 Intercon
- 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…



- EMP
- Biological contamination (real or threat)
- Over-reaction to isolated incidents
- Internet Attacks
- Over 80,000 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 … "

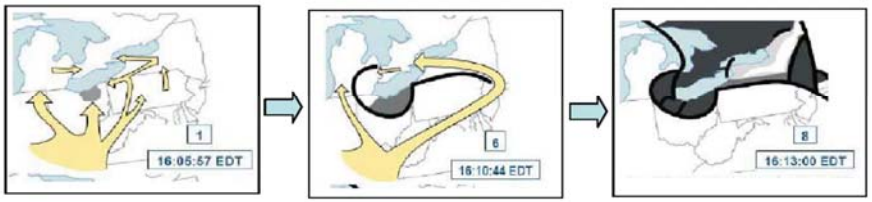
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Summary of August 14, 2003 Blackout Statistics

- Reported as affecting 50 million people
- 60-65,000 MW of load initially interrupted
  - Approximately 11% of Eastern Interconnection
- 400+ Generating units tripped
- Cascading lasted approximately 12 seconds
- Thousands of discrete events to evaluate
- Joint U.S.-Canada Task Force report published at 2 p.m. on Nov. 19, 2003

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

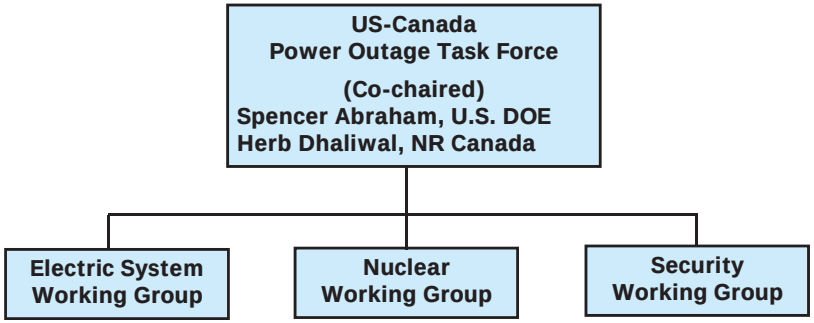
Risk of Major System Failures



- **Northeastern U.S. blackout in 2003 cost $6 – 10 billion**
- **Six major blackouts occurred within six weeks in summer '03**
  - **112 million people affected in US, UK, Denmark, Sweden, & Italy**
  - **Significant contributing factors were lack of coordination across system boundaries and slow response to emerging problems**
- **New mode of coordinated operation for real-time security assessment and control is needed**

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Joint U.S.-Canada Task Force Report

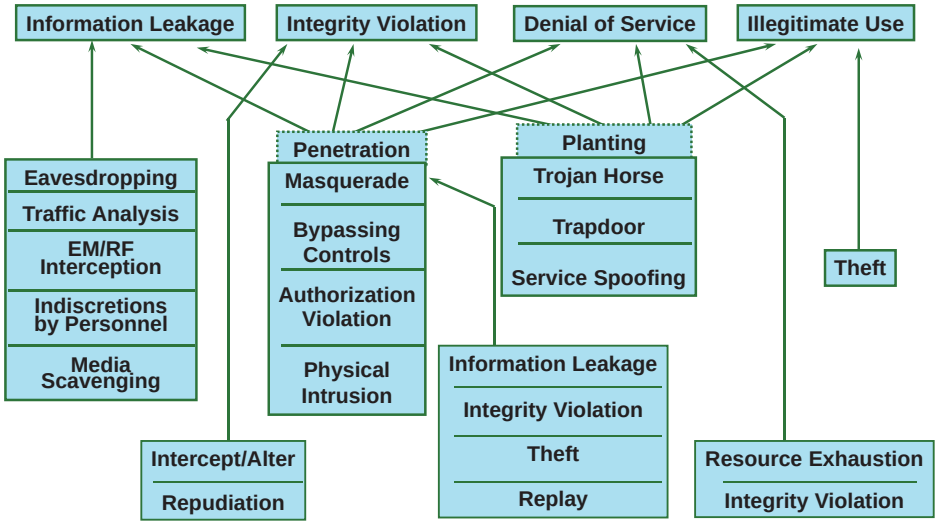


Root causes cited:

- **"Inadequate situational awareness" at First Energy Corp.**
- **Failure to adequately trim trees in its transmission right-of way**
- **Failure of reliability coordinators to promptly identify and deal with problems**

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

What Can They Do and How Can They Do It?



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

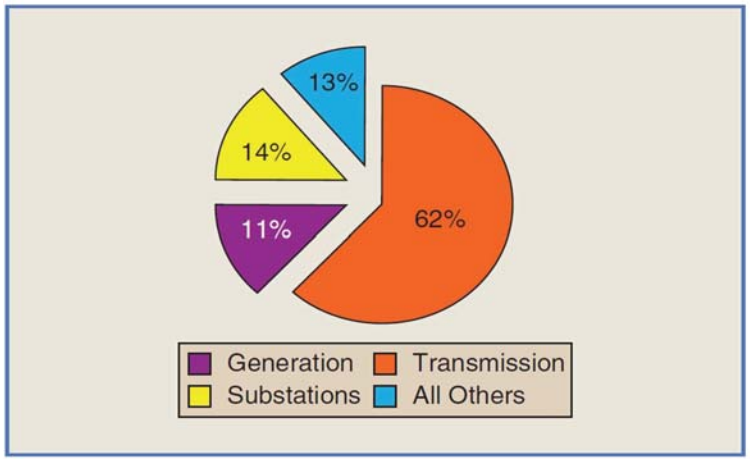
Electric Company Vulnerability Assessment

- 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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Electric Terrorism: Grid Component Targets 1994–2004

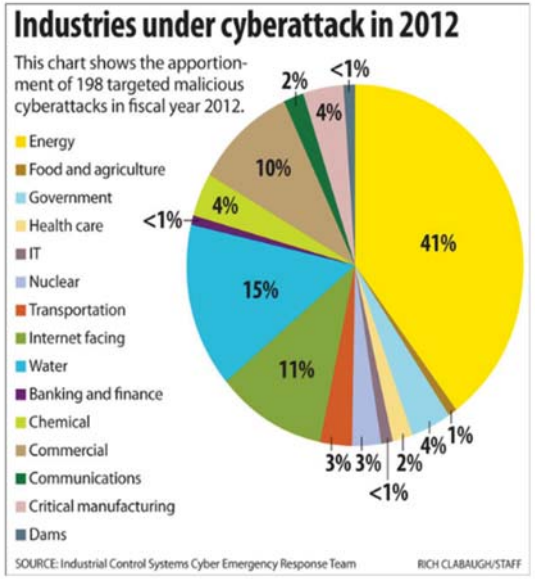


source: Journal of Energy Security

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

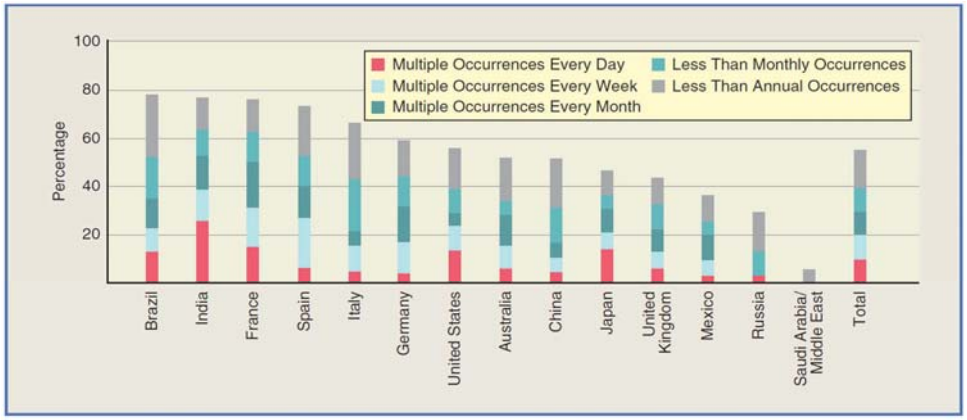
Energy Sector Vulnerability

- 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



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

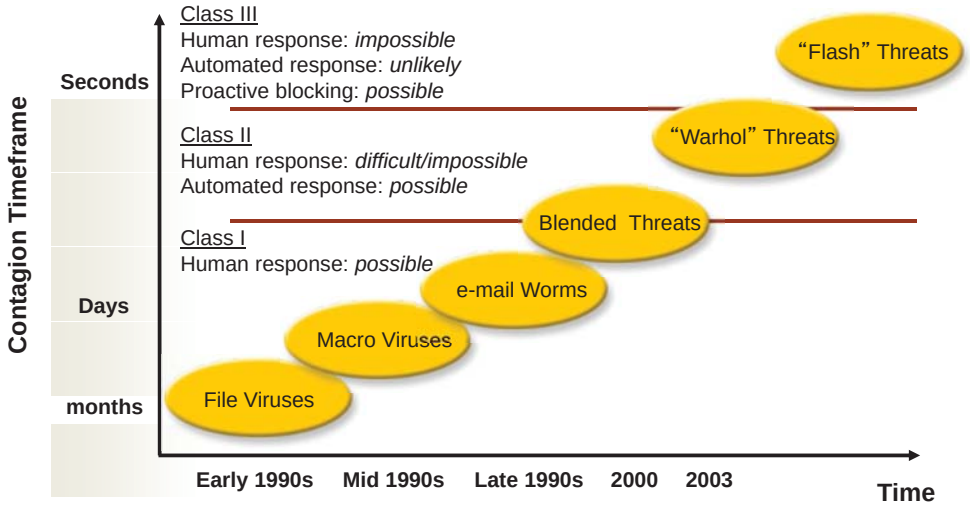
Percentage of critical infrastructure enterprise executives reporting large-scale DDoS attacks and their frequency



source: *McAfee*

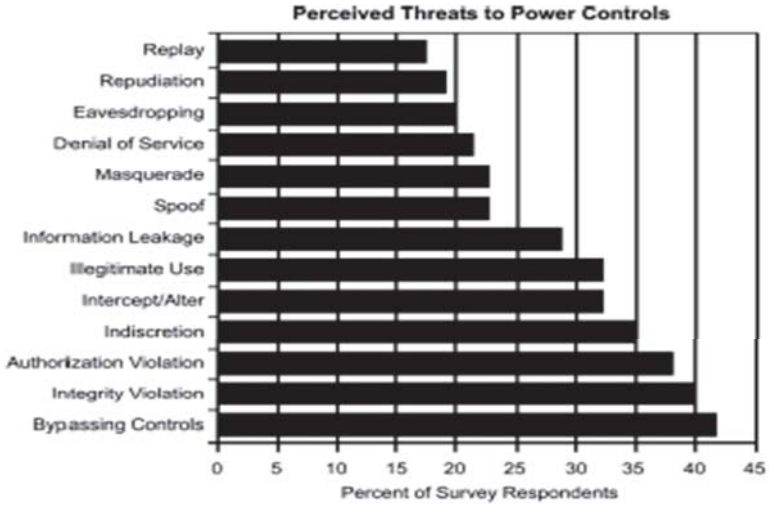
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Threat Evolution: Malicious Code



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Cyber Threats to Controls



Source: EPRI, Communication Security Assessment for the United States Electric Utility Infrastructure, EPRI, Palo Alto, CA: 2000. 1001174.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Electric Power is Critical

- **Energy and Communications are classified as the most critical of our nation's infrastructure**

Control is Critical

- **One central system with the ability to change or disrupt power flow**
- **System not designed to withstand multiple disruptions**

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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)

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

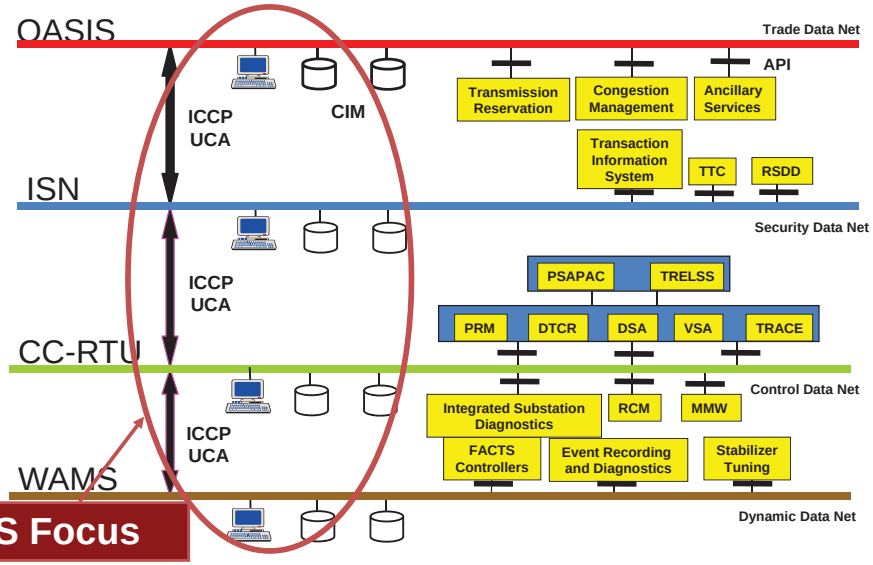
Context: Better Situational Awareness and Automation

- **Increasing Dependence on ICT, Computation 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.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Enterprise Information Security (EIS) program

Information Networks for On-Line Trade, Security & Control



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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

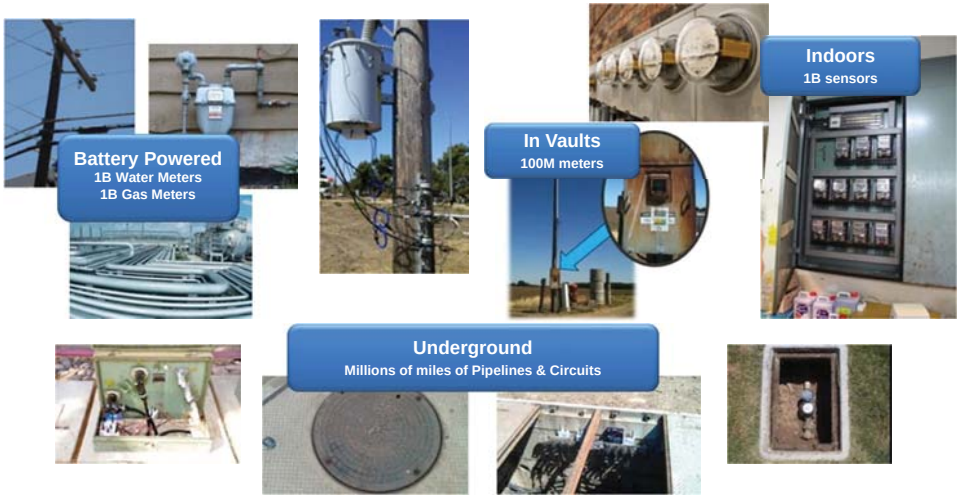
Smart Grid Protection Schemes & Communication Requirements

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**	

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

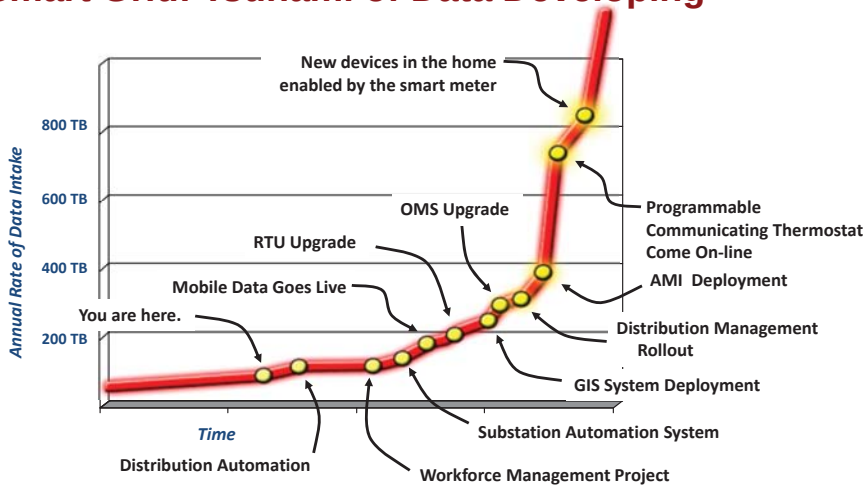
Industry Needs to Connect 50 Billion Devices by 2020

An unsolved problem costing billions per year in wasted resources requires radically improved wireless performance and lower cost



© On-Ramp Wireless, Inc. All rights reserved.
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Large utility companies need an effective, long-term strategy to mitigate the growing cyber threat facing control systems.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Approach and Methodology

Vulnerabilities

Research
- Typical control system designs and current regulations
- current and emerging cyber threats

Analyze
- Quantify the most vulnerable component and likely attacker

Solutions

Research
- Research existing and emerging cyber security solutions applicable to electric power control systems

Analyze
- Identify and prioritize solutions

Focused Recommendations

Recommend
- Provide actionable recommendations

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

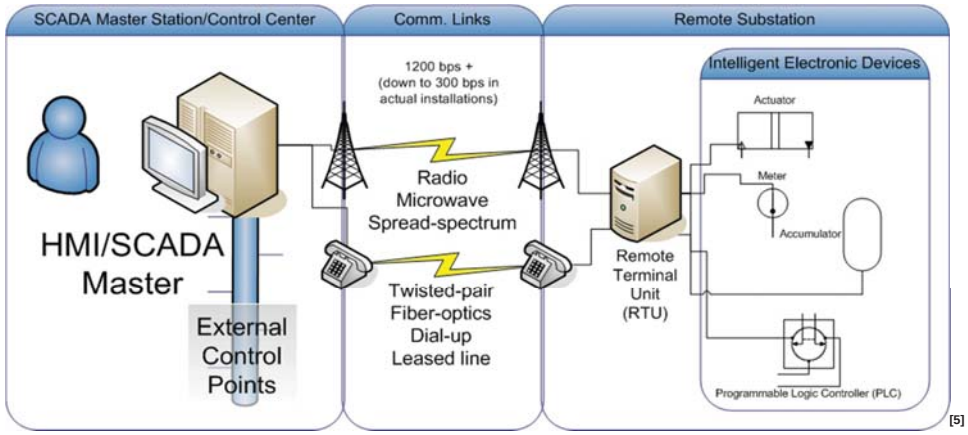
What's out there?

- 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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Control Systems Overview

Three main components

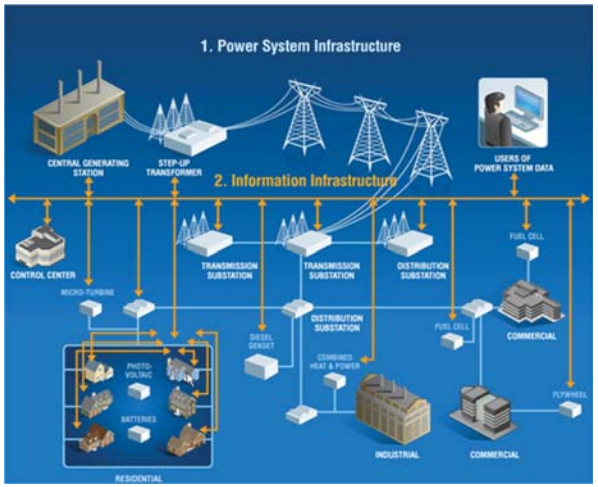


[5]

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

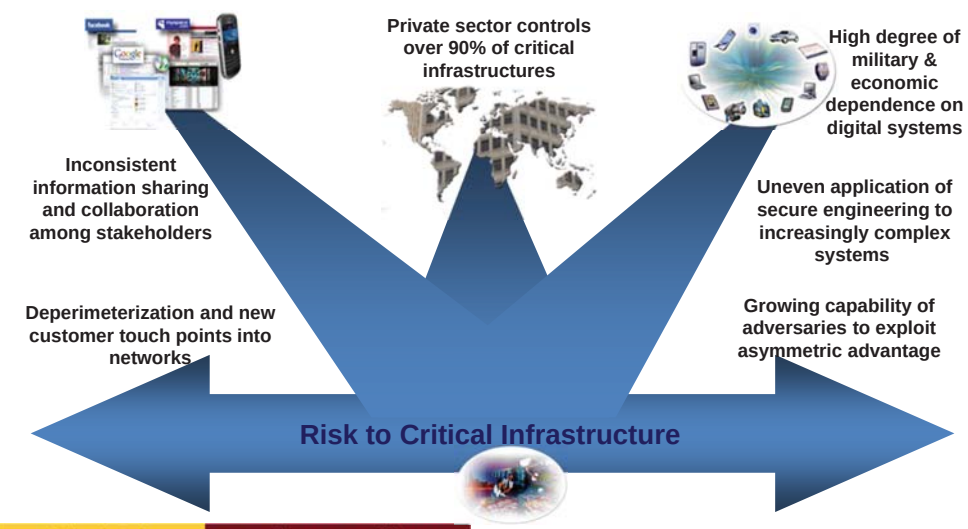
- Intense financial pressure to reduce staffing; hence more "remote" management
- Computerization and RF control common in all industries
- Project implementation excellence not always followed by outstanding security operations
- SCADA hacking can cause ' "wholesale" damage to neighborhoods and equipment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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Many Factors Shape the Degree and Nature of Communications Risks to Utilities Infrastructure



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Thus There are Multiple Scenarios to Plan For…

External Threat

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

Deliberate

Insider Threat

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Prioritization: Security Index

General

1. Corporate culture (adherence to procedures, visible promotion of better security, management security knowledge)
2. Security program (up-to-date, complete, managed, and includes vulnerability and risk assessments)
3. Employees (compliance with policies and procedures, background checks, training)
4. Emergency and threat-response capability (organized, trained, manned, drilled)

Physical

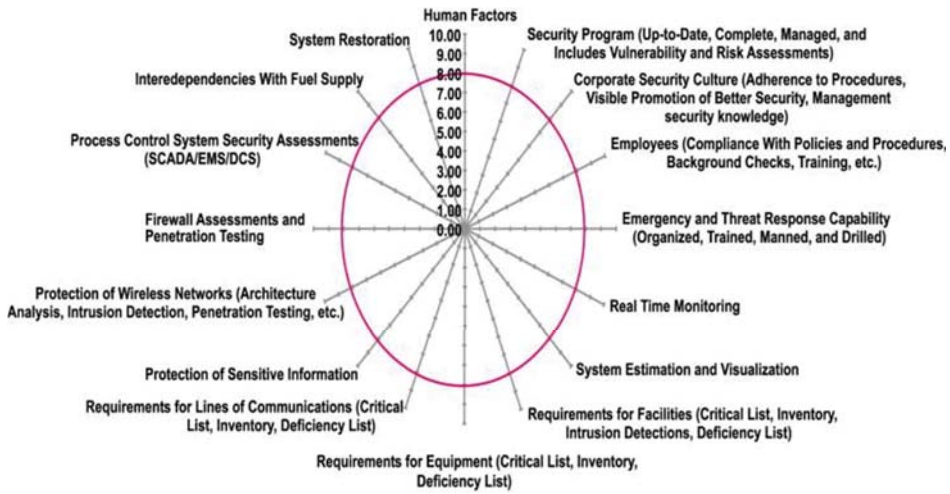
1. Requirements for facilities (critical list, inventory, intrusion detections, deficiency list)
2. Requirements for equipment (critical list, inventory, deficiency list)
3. Requirements for lines of communications (critical list, inventory, deficiency list)
4. Protection of sensitive information

Cyber and IT

1. Protection of wired networks (architecture analysis, intrusion detection)
2. Protection of wireless networks (architecture analysis, intrusion detection, penetration testing)
3. Firewall assessments
4. Process control system security assessments (SCADA, EMS, DCS)

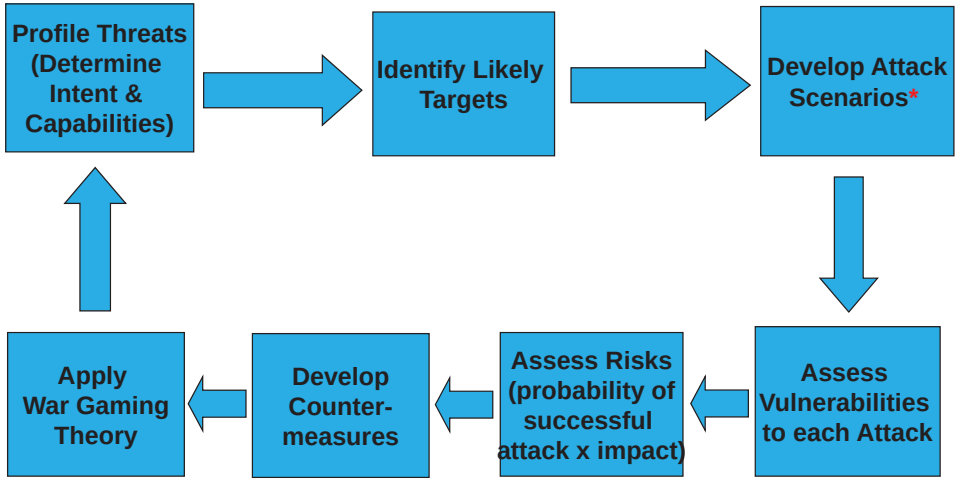
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Assessment & Prioritization: A Composite Spider Diagram to Display Security Indices



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

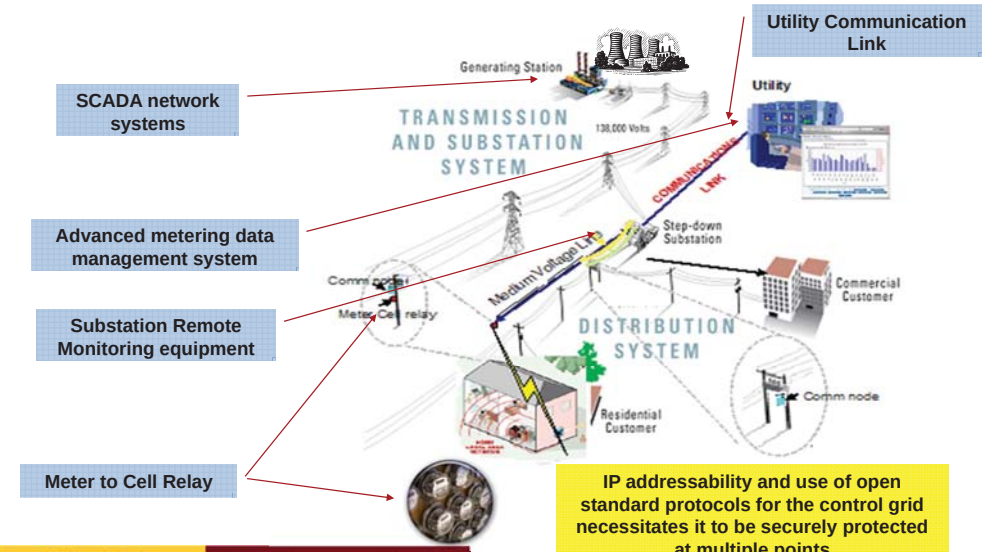
What can be Done? Vulnerability Assessment



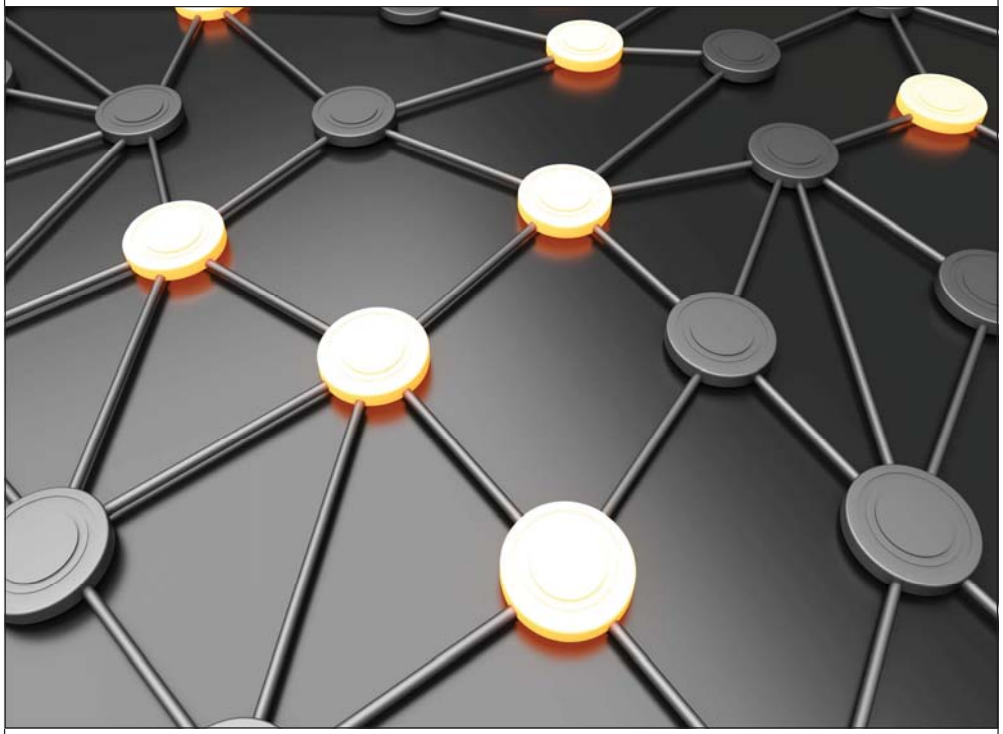
*Evolving spectra of targets and modes of attack

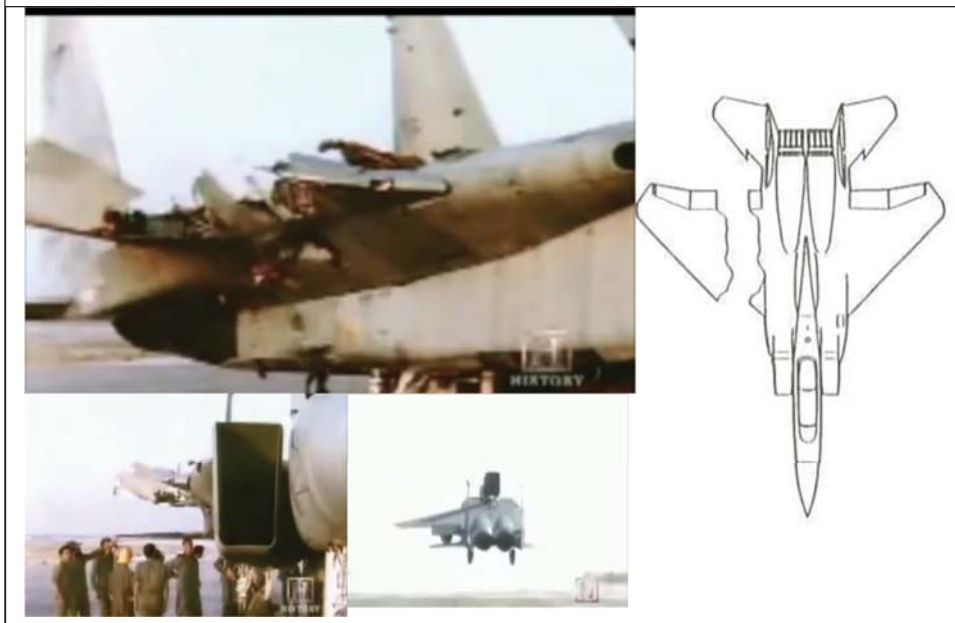
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

A Smart Grid Thus Needs Communications Security Enforcement at Multiple Points



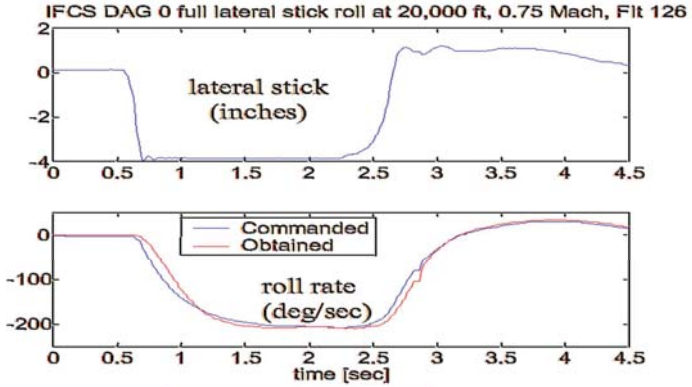
© 2013 No part of this presentation may be reproduced in any form without prior authorization.





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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.



duced in any form without prior authorization.

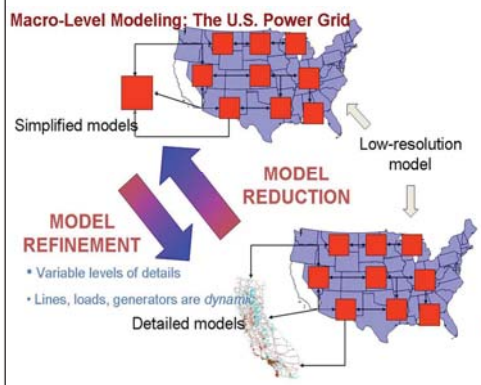
Critical System Dynamics and Resilience Capabilities

- **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

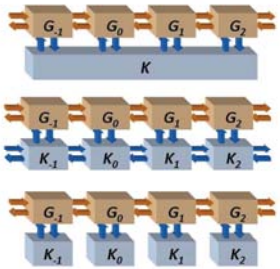
Resilience enables "Robustness": A system, organism or design may be said to be "robust" if it is capable of coping well with variations (internal or external and sometimes unpredictable) in its operating environment with minimal damage, alteration or loss of functionality.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

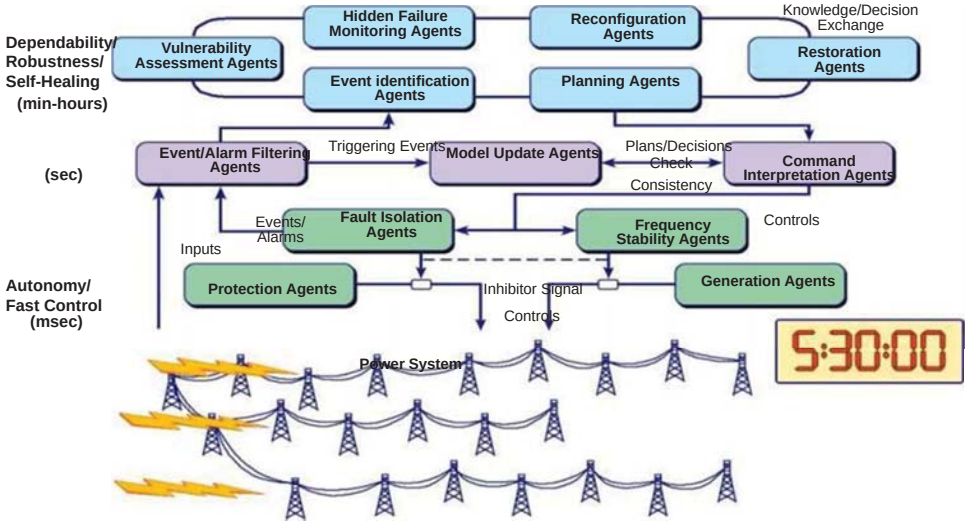


Sensing and Control Strategies

- Centralized
- Distributed
- Perfectly decentralized



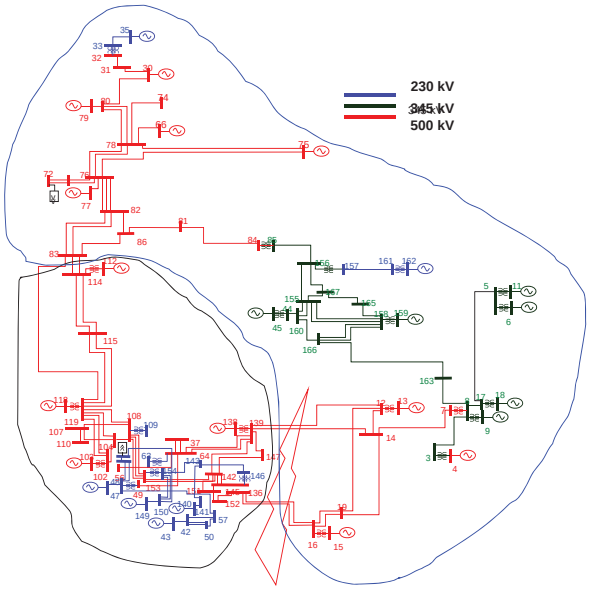
Self-Healing Grid

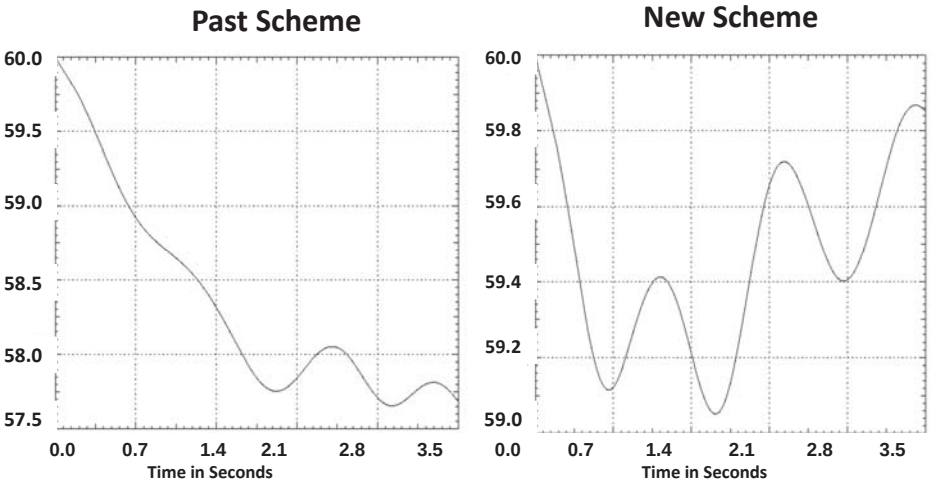


EPRI/DoD CIN/S Initiative

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

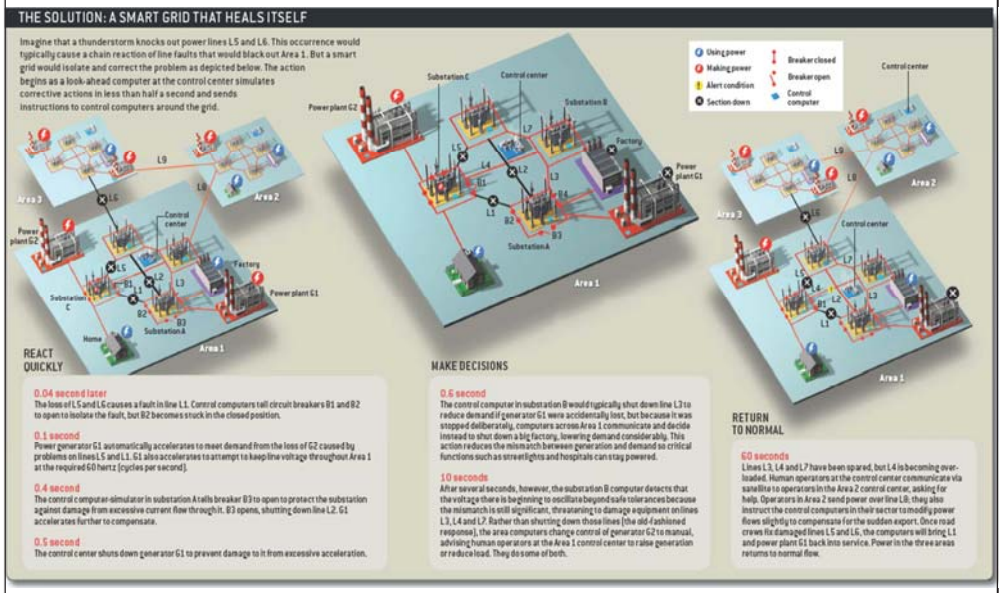
Self-Healing Grid: Intelligent Adaptive Islanding





© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Smart Self-Healing Grid



"Preventing Blackouts," Scientific American, May 2007

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

What are we working on at the U of Minnesota ?

- Integrating PHEVs into the grid
- Grid agents as smart and distributed computer
- Fast power grid simulation and risk assessment
- More Secure and Smarter Grid
- Security of cyber-physical infrastructure

University of Minnesota Center for Smart Grid Technologies (2003-present)
Dept. of Electrical & Computer Engineering
Faculty: Professors Massoud Amin and Bruce Wollenberg
PhD Candidates/Research Assistants: Anthony Giacomoni (PhD 11/11), Jesse Gantz (MS 6/12), Laurie Miller (PhD'13), and Sara Mullen (PhD 9/9)
PI: M. Amin (support from EPRI, NSF, Honeywell, SNL, ORNL, and UofM start-up research funding)

Center for Smart Grid Technologies

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Objectives

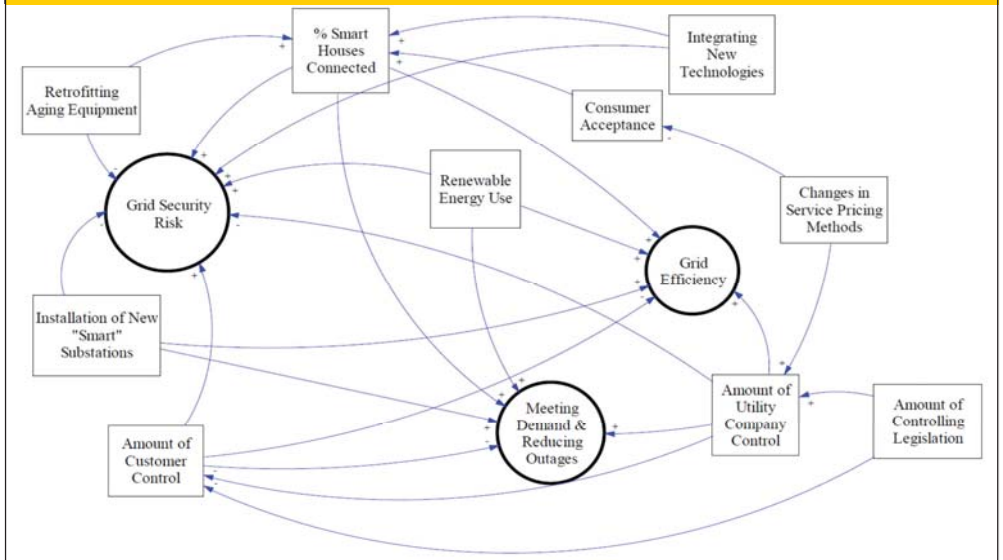
- Our *strategic goal* is to better understand the true dynamics of complex interdependent energy/communications/economic networks in order to enable stronger, greener, more secure and smarter power grids.
- The *objective of this project* is to model, design and develop reconfigurable and distributed smart energy systems supported by <u>secure sensing/wireless communication network overlay and fault-resilient real-time controls</u>.

Center for Smart Grid Technologies

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

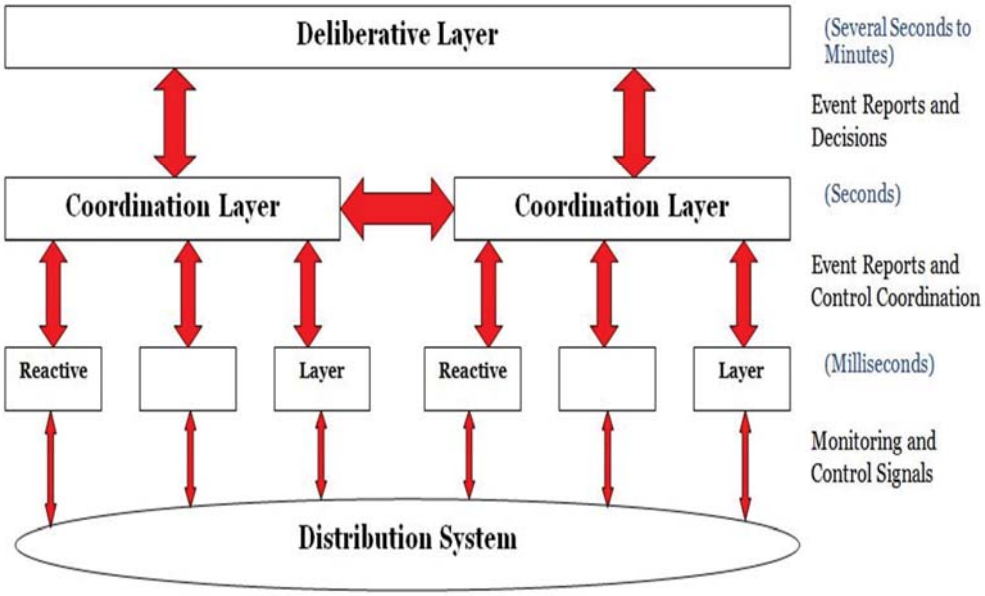
Smart Grid Interdependencies

Security, Efficiency, and Resilience

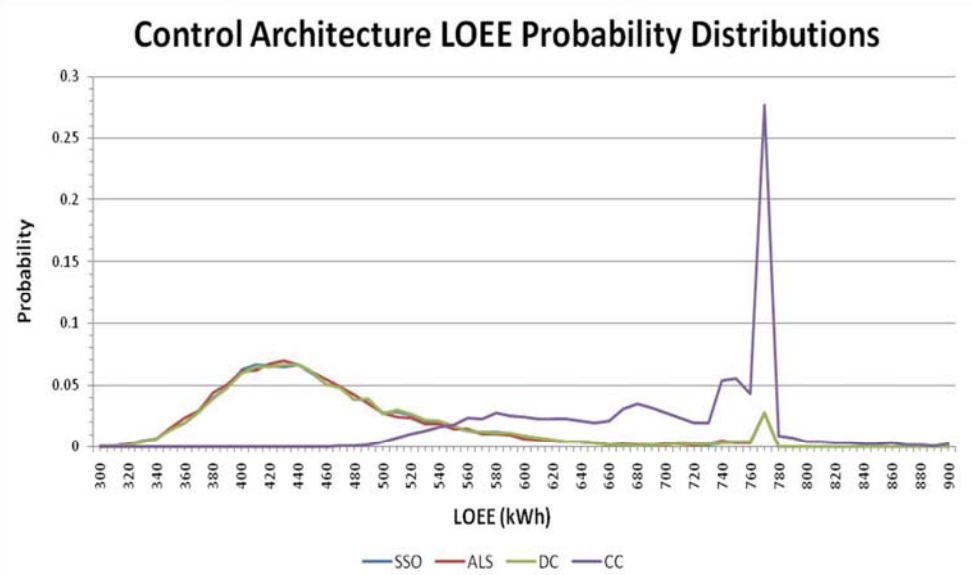


© 2013 No part of this presentation may be reproduced in any form without prior authorization.

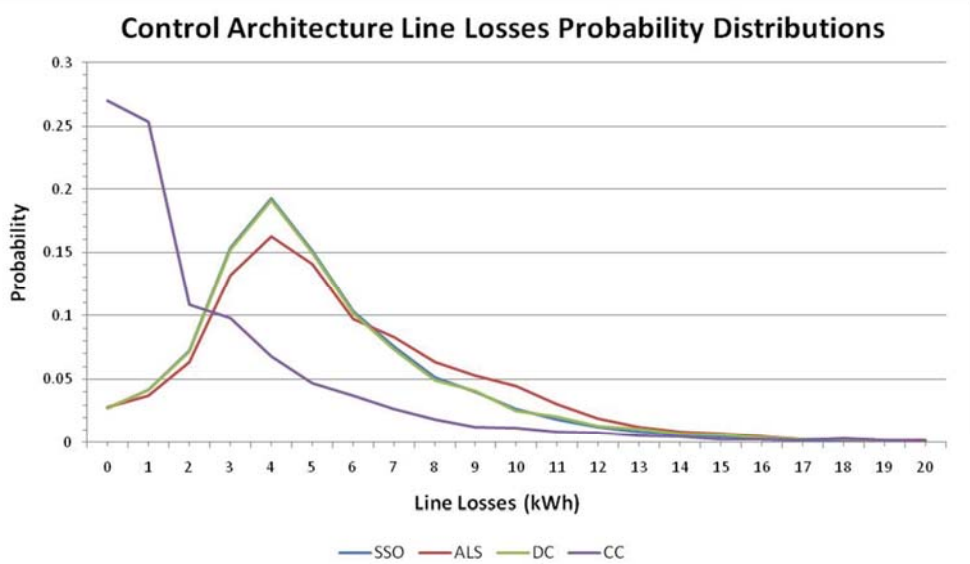
Intelligent Distributed Secure Distribution System Control Architecture



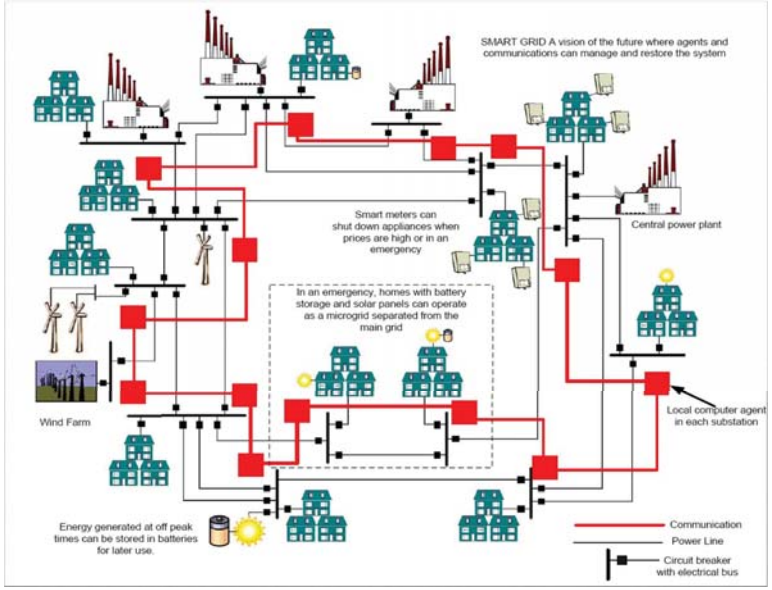
Centralized or Decentralized Control?



Centralized or Decentralized Control?



Our team's Smart Grid Research



Technological Leadership Institute

University of Minnesota Driven to Discover

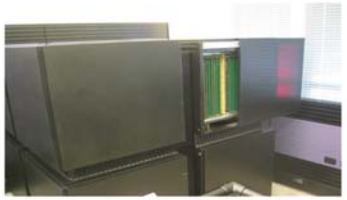
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Fast Power Systems Risk Assessment

Doctoral Dissertation: Laurie Miller (June 2005-2013)
ORNL contract, the U of MN start-up fund (2005-2008), and NSF grant (2008-2009), PI: Massoud Amin

1987 → **2010**

Connection Machine 2



$5,000,000 → **$350**

Only a dozen built → **100 million sold**

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

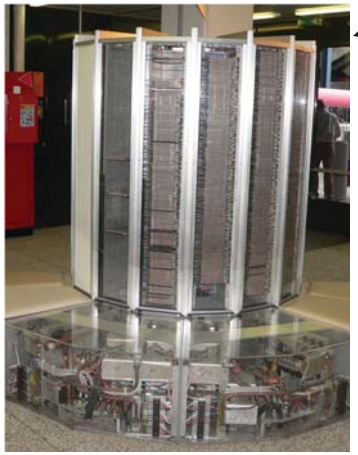
Building a super computer from many small processors

Up to 65,536 processors

- The IBM Blue Gene computer

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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)

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

A Fundamental Point

- Amdahl's Law
  - predicts a maximum theoretical speedup of an application program that can be gained by executing it in parallel

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Background

- Amdahl's Law
  - predicts a maximum theoretical speedup of an application program that can be gained by executing it in parallel
- Gustafson's Law
  - Amdahl's Law reflects how computational geeks think, now how most application users behave
  - most users of application code simply want the best results that they can get within what they have determined to be a reasonable period of time

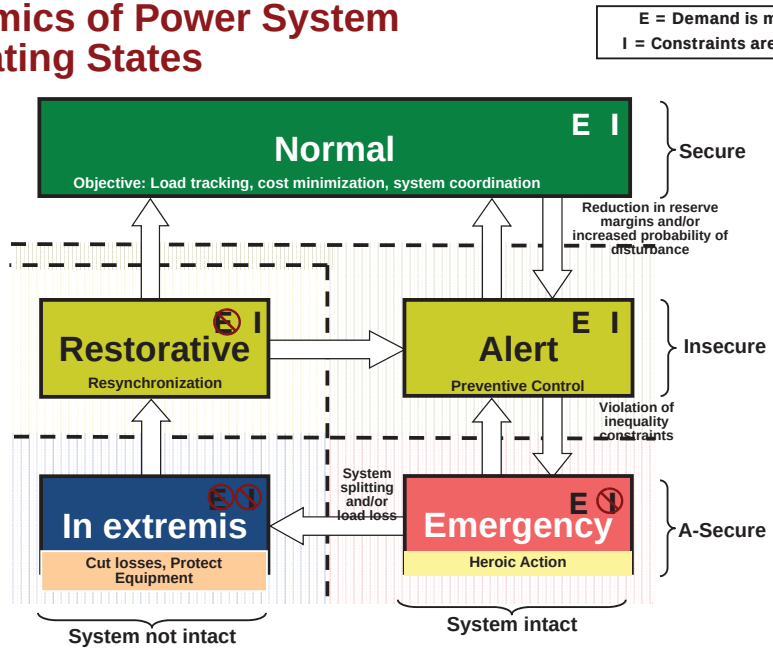
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Power Systems Security Analysis

- Set of tools used in control centers to
  - Evaluate the system state
  - Prepare against contingencies in the system
  - So that the system remains stable under potentially de-stabilizing events
- Day-ahead operational planning
  - Static system model
  - Allotted time for analysis is not a day, but a number of hours set by market closing times and other parameters
- Real-time Operations
  - Dynamic system model
  - **Time for analysis is in minutes**

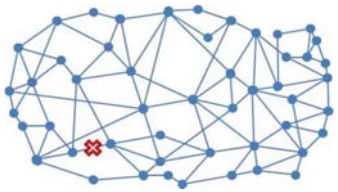
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Dynamics of Power System Operating States



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

- Mid-Continent Independent System Operator (MISO)
  - 40366 buses
  - runs a reduced list of 8300 contingencies every 4.5 minutes
- Western Interconnection
  - 17,000 to 20,000 elements
- Bonneville Power Administration (BPA): Pre-selected list of 500 contingencies every five minutes
- Hydro-Quebec
  - reduced list of 1000 contingencies every three minutes
  - requires 10 to 30 minutes to run a full list of contingencies
- Electric Reliability Council of Texas (ERCOT)
  - 3938 contingencies,
  - reduced list of 500 contingencies for full AC analysis
- NStar would have about
  - 3000 single contingencies
  - reduced list of 760 contingencies every three minutes.



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Regulatory Requirements

- In the United States and Canada, rules for maintaining the power grid in a secure state are set by the North American Electric Reliability Corporation (NERC)
- **(N-1) criterion:** The loss of any one element, such as a generator, transmission line, or transformer – will not result in a cascading blackout
- **30 Minutes:** Maximum allowable time frame after a contingency occurs to return to a normal and secure operating state, able to withstand any single contingency

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Changing nature of operational security analysis

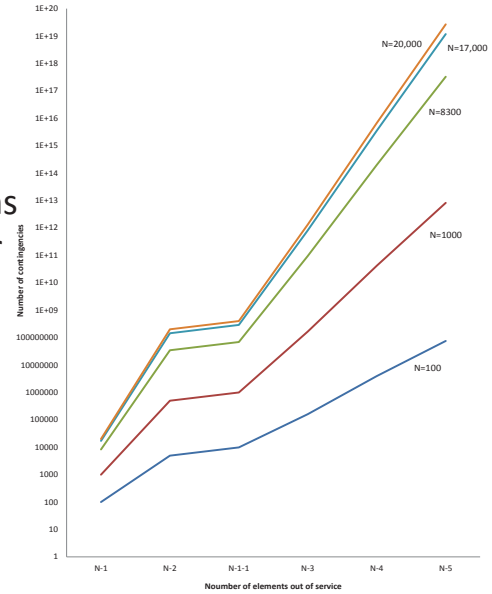
- Marketization and changing market rules
- Modern usage patterns combined with renewables
- Control area consolidation
- Increasing regulatory pressure
  - Must do more in the allotted time windows

Image from: http://www.caiso.com/about/PublishingImages/control_center.jpg

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Contingency Analysis

- Evaluation of what happens to the system when one or more elements are removed from the system
- Run a power flow calculation for each contingency, each set of elements lost



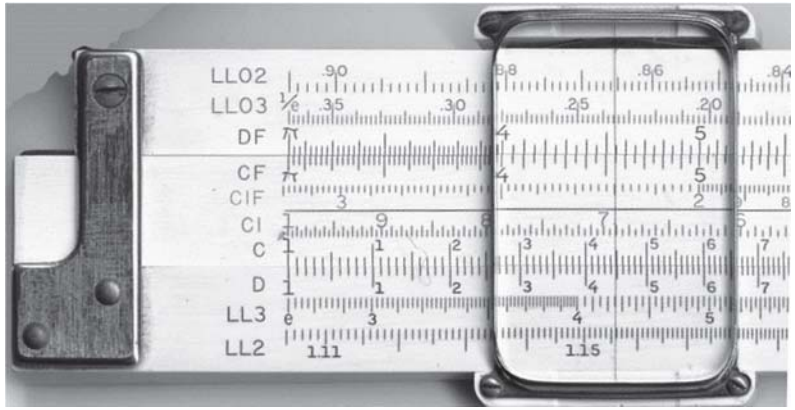
© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Some Salient GPGPU Characteristics

- Large, but slow
- Single-precision Arithmetic
- Dubious arithmetic
  - Rudimentary arithmetic, even with special-function units
  - IEEE Standard 754 compliance issues
  - Lack of atomic operations
- Rudimentary control logic
  - Penalty for divergent warps
- Lack of fully-developed toolsets, such as Linear Algebra solvers for sparse matrices

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

In Essence



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Resulting Design Choices

- Power flow algorithm: Fast Decoupled Power Flow
- Large problem size
- Balancing thread count with instructions per thread
- Vector parallelism
- Reduction and re-mapping of sparse matrix operations
- Reduced transporting of large sparse matrices
- Flexibility of implementation for different GPGPUs or combinations thereof
- Minimizing GPGPU control logic
- Simple arithmetic

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

A Novel Mathematical/Computational Method

- Revolves around setting up the computation of the set of (N-1) contingencies to slice across contingencies to create dense vector operations
- Splitting the admittance matrix:
  - Rectangular arithmetic is used for the bus current and power equations
  - The admittance matrix can thus be split into two component real matrices
- A bus current correction method
  - Allows the component admittance matrices to remain constant
  - Same matrices can be used for all (N-1) contingencies
- The FDPF is used with forms of the Matrix Inversion Lemma
  - Avoids the need to solve matrix inversions
  - Facilitate slicing computation across contingencies
  - Replace multiple lengthy series of sparse-matrix-dense-vector multiplications with the much more efficient sparse matrix multiplied by a block of dense vectors larger than the matrix itself

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Related Work in the Current Literature

- Pre-CUDA GPU contingency analysis
  - Gopal et al, 2007, 1 contingency per each of the four color channels
- Power flow or parts thereof on GPGPUs
  - Vilacha et al ran a base case of the IEEE 118 bus case on a GPGPU
    - Then ran it again thousands of times at once to see how fast it would be
    - Did not actually evaluate contingencies
  - Singh and Aruni: Good results with proprietary solvers
  - Garcia, Li et al, Guo et al, and Wigington et al accelerated parts of a single power flow by farming some calculations out to a GPGPU

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Cited Related Work

- A. Gopal, D. Niebur, and S. Venkatasubramanian, "DC power flow based contingency analysis using graphics processing units," in Power Tech, 2007 IEEE Lausanne. IEEE, Jul. 2007, pp. 731–736.
- C. Vilacha, J. C. Moreira, E. Miguez, and A. F. Otero, "Massive Jacobi power flow based on SIMD-processor," in Environment and Electrical Engineering (EEEIC), 2011 10th International Conference on. IEEE, May 2011, pp. 1–4.
- J. Singh and I. Aruni, "Accelerating Power Flow studies on Graphics Processing Unit," in India Conference (INDICON), 2010 Annual IEEE. IEEE, Dec. 2010, pp. 1–5.
- "Using jacket: Productivity platoform for gpu computing," AccelerEyes, 75 5th Street NW, Suite 204, Atlanta, GA 30308, Tech. Rep., 2010.
- N. Garcia, "Parallel power flow solutions using a biconjugate gradient algorithm and a Newton method: A GPU-based approach," in Power and Energy Society General Meeting, 2010 IEEE. IEEE, Jul. 2010, pp. 1–4.
- Z. Li, V. D. Donde, J. C. Tournier, and F. Yang, "On limitations of traditional multicore and potential of many-core processing architectures for sparse linear solvers used in large-scale power system applications," in Power and Energy Society General Meeting, 2011 IEEE. IEEE, Jul. 2011, pp. 1–8.
- C. Guo, B. Jiang, H. Yuan, Z. Yang, L. Wang, and S. Ren, "Performance Comparisons of Parallel Power Flow Solvers on GPU System," in Embedded and Real-Time Computing Systems and Applications (RTCSA), 2012 IEEE 18th International Conference on. IEEE, Aug. 2012, pp. 232–239.
- A. Wigington, L. Min, C. Li, W. Murray, and A. Narayan, "Advancing the adoption of advanced computing methods and technologies for real-time control center operations," in Power and Energy Society General Meeting, 2012 IEEE. IEEE, Jul. 2012, pp. 1–6.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

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

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

An Example: Smarter I-35W bridge

Just after 6:00 p.m. on Aug. 1, Prof. Massoud Amin was at work in his office on the University of Minnesota's West Bank, where he heard and watched the unthinkable happen—the collapse of the I-35W bridge about 100 yards away.

"As an individual, it was shocking and very painful to witness it from our offices here in Minneapolis," says Amin, director of the Center for the Development of Technological Leadership (CDTL) and the H.W. Sweatt Chair in Technological Leadership. Amin also viewed the tragedy from a broader perspective as a result of his ongoing work to advance the security and health of the nation's infrastructure.

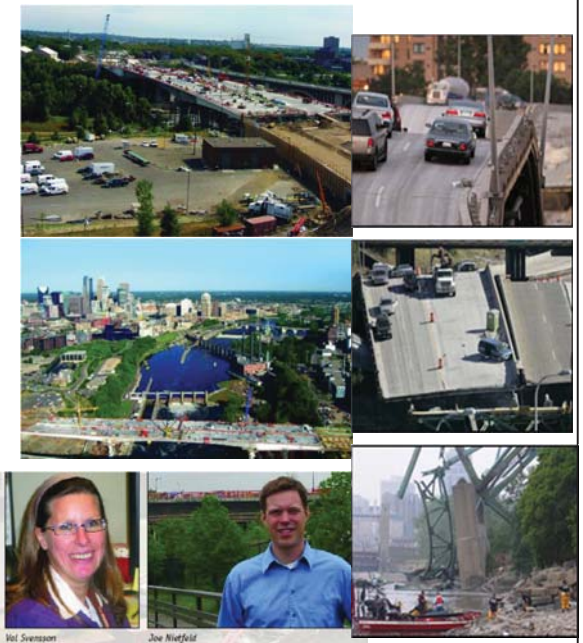
In the days and weeks that followed, he responded to media inquiries from the BBC, Reuthers, and the CBC, keeping his comments focused on the critical nature of the infrastructure. He referred reporters with questions about bridge design, conditions, and inspections to several professional colleagues, including Professors Roberto Ballarini, Ted Galambos, Vaughan Voller, and John Gulliver in the Department of Civil Engineering and the National Academy of Engineering Board on Infrastructure and Constructed Environment.

For Amin, Voller, and many others, the bridge collapse puts into focus the importance of two key issues—the tremendous value of infrastructure and infrastructure systems that help make possible indispensable activities such as transportation, waste disposal, water, telecommunications, and electricity and power, among many others, and the search for positive and innovative ways to strengthen the infrastructure.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

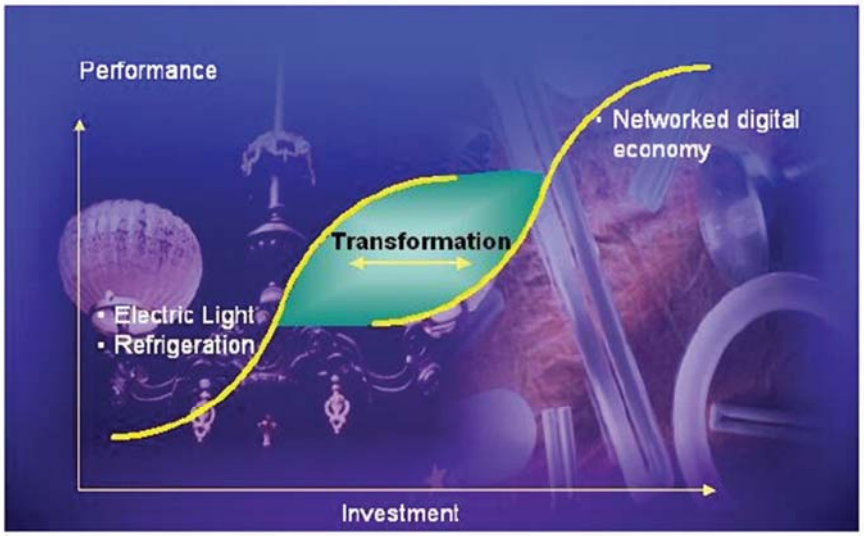
To improve the future and avoid a repetition of the past:

Sensors built in to the I-35W bridge at less than 0.5% total cost by TLI alumni



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

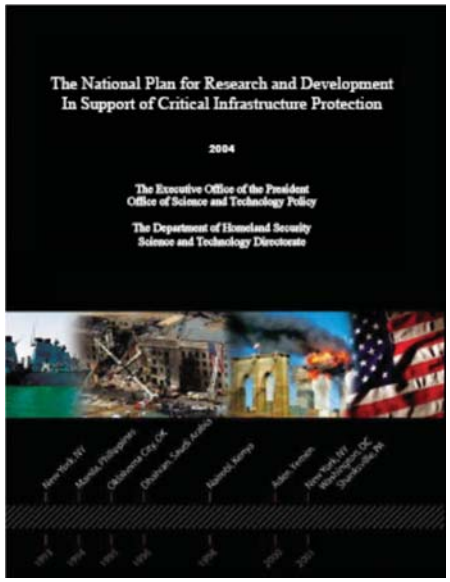
Breaking the Limits on Electricity Value



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

The National Plan for Research and Development In Support of Critical Infrastructure Protection

- The area of **self-healing infrastructure** was recommended in 2005 by the White House Office of Science and Technology Policy (OSTP) and the U.S. Department of Homeland Security (DHS) as one of three thrust areas for the National Plan for research and development in support of Critical Infrastructure Protection (CIP)



© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Smart Grid Collaboration Opportunities

- **IEEE Smart Grid Newsletter:**
  - To subscribe, free of charge, please visit: http://smartgrid.ieee.org/publications/smart-grid-newsletter
  - For details on all IEEE Smart Grid, please visit http://smartgrid.ieee.org/
- **IEEE CSS Technical Committee on Smart Grids (TC-SG)**
- **IEEE Smart Grid Vision Project for Control Systems:**
  - A long-term vision of what the smart grid will look like 20 to 30 years out what can the control systems community contribute.

© 2013 No part of this presentation may be reproduced in any form without prior authorization.

Selected References

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

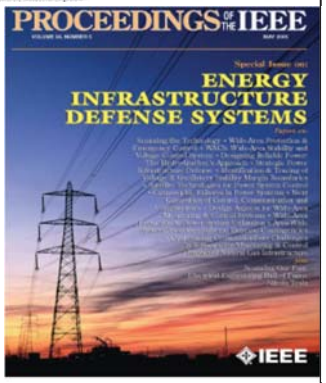
- **"Securing the Electricity Grid,"** The Bridge, quarterly publication of the U.S. National Academy of Engineering, Vol. 40, No. 1, pp. 13-20, Spring 2010
- **Special Issue of Proceedings of the IEEE on Energy Infrastructure Defense Systems**, Vol. 93, Number 5, pp. 855-1059, May 2005
- Special issues of IEEE Control Systems Magazine on **Control of Complex Networks**, Vol. 21, No. 6, Dec. 2001 and Vol. 22, No. 1, Feb. 2002
- **"Complex Interactive Networks/Systems Initiative (CIN/SI): Final Summary Report,"** Overview and Summary Final Report for Joint EPRI and U.S. Department of Defense University Research Initiative, EPRI, 155 pp., Mar. 2004
- **"New Directions in Understanding Systemic Risk,"** with NAS and FRBNY Committee, National Academy of Sciences and Federal Reserve Bank of NY, Mar. 2007

Summary of presentation by Prof. Massoud Amin and related comments from

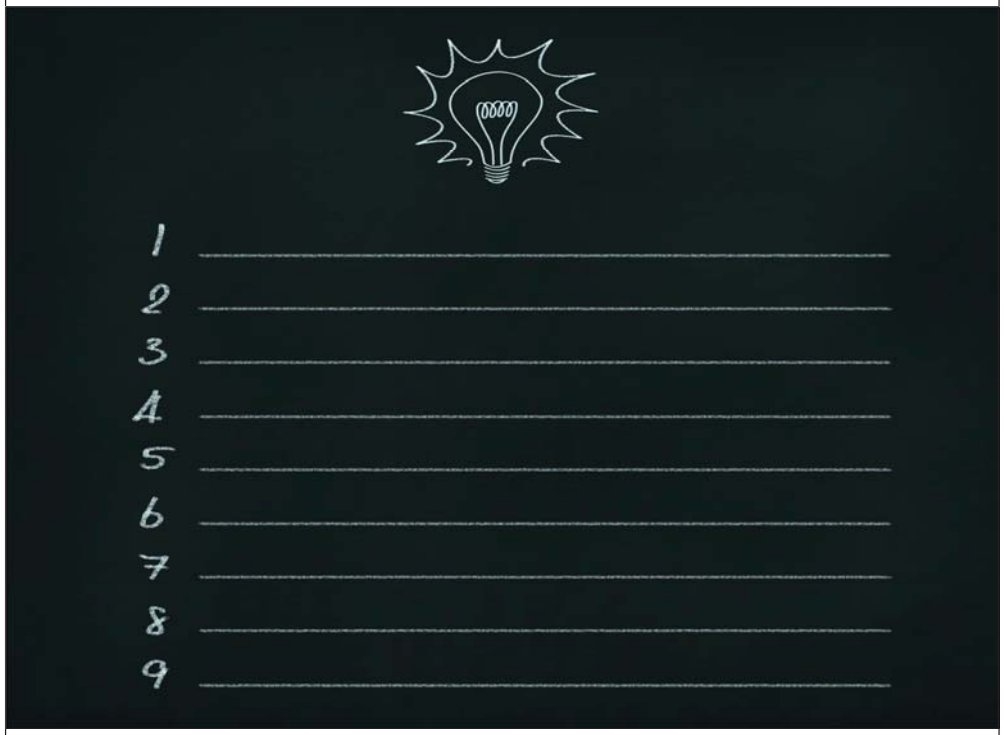
New Directions for Understanding Systemic Risk:
A report on a Conference Cosponsored by the Federal Reserve Bank of New York and the National Academy of Sciences

For the NAS book and complete FRBNY report please see:
Economic Policy Review, Federal reserve Bank of New York, Vol. 13, Number 2, Nov. 2007
New Directions for Understanding Systemic Risk, 108 pp. Nat'l Acad. Press, Washington DC, 2007

The stability of the financial system and the potential for systemic events to alter the functioning of that system have long been important topics for central banks and the related research community. Developments such as increasing industry consolidation, global networking, terrorist threats, and an increasing dependence on computer technologies underscore the importance of this area of research. Recent events, however, including the terrorist attacks of September 11th and the demise of Long Term Capital Management, suggest that existing models of systemic shocks in the financial system may no longer adequately capture the possible channels of propagation and feedback arising from major disturbances. Nor do existing models fully account for the increasing complexity of the financial system's structure, the complex range of financial and information flows, or the endogenous behavior of different agents in the system. Fresh thinking on systemic risk is, therefore, required.



Technological Leadership Institute

University of Minnesota
Driven to Discover℠

© 2013 No part of this presentation may be reproduced in any form without prior authorization.