Smart Grid Research Challenges

S. Massoud Amin, D.Sc.
Director, Technological Leadership Institute
Honeywell/H.W. Sweatt Chair in Technological Leadership
Professor, Electrical & Computer Engineering
University Distinguished Teaching Professor

Keynote presentation at the DIMACS Workshop on
Algorithmic Decision Theory for the Smart Grid
DIMACS Center, Rutgers University, October 25, 2010

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

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

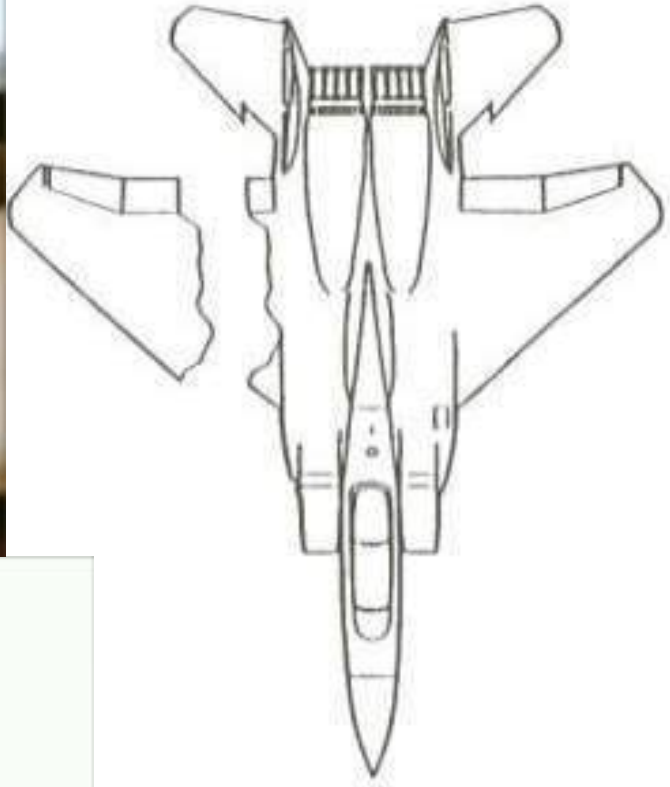
Workshop Goals:

Challenges/Opportunities for Algorithmic Decision Theory in the management and control of the electric power grid, with reference to three broad themes:

- Control
- Data and Measurements
- Security

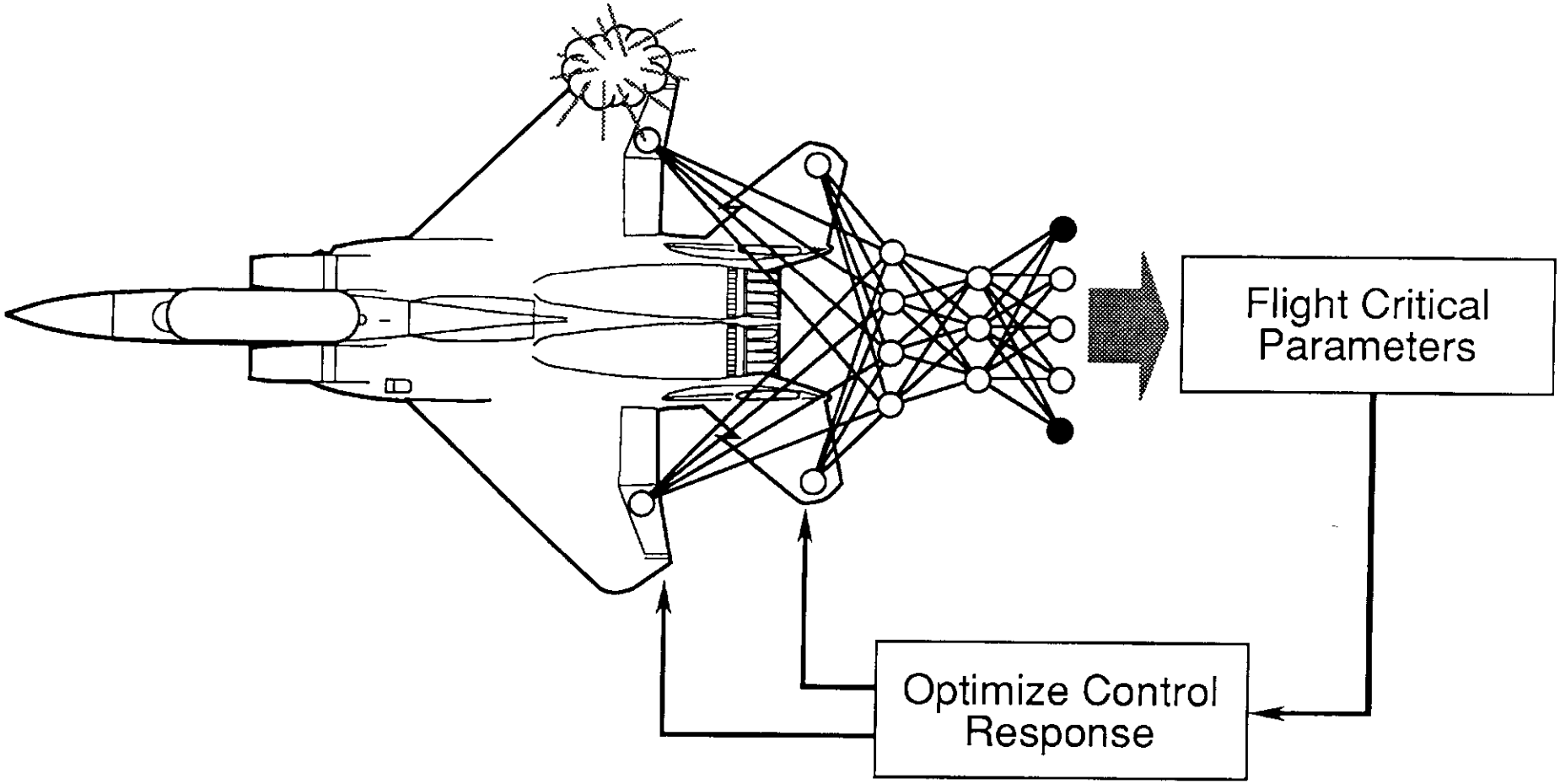
Sensing, Estimation and Control

Saving systems from collapse in Multi-hazard environments: The Case of the Missing Wing (1983-97)



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

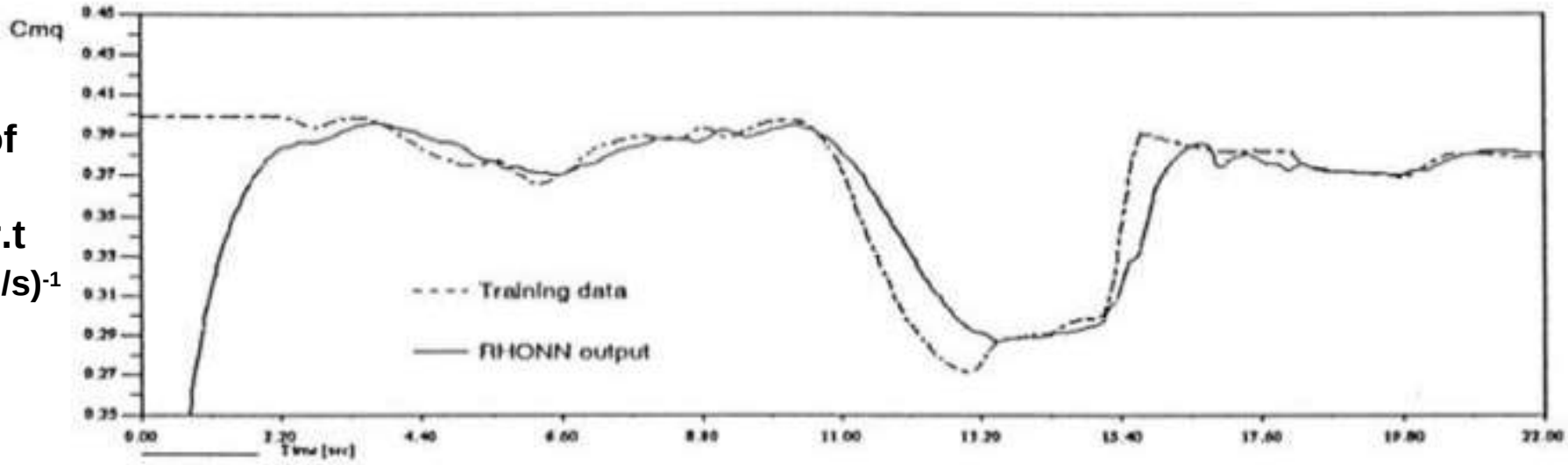
Goal: Optimize controls to compensate for damage or failure conditions of the aircraft



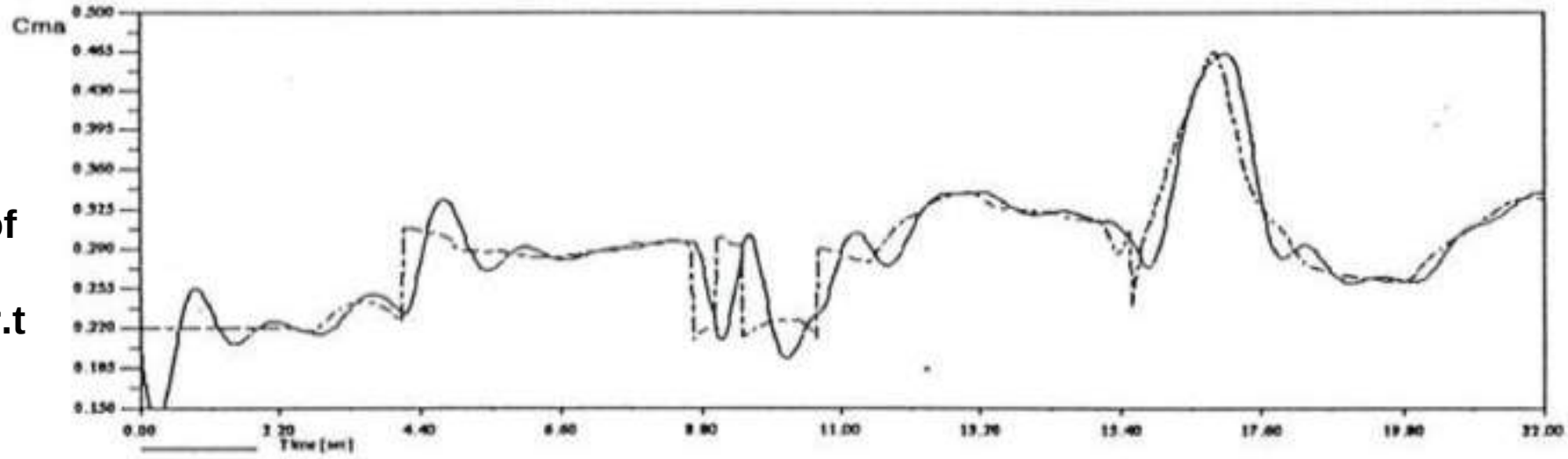
NASA/MDA/WU IFCS: NASA Ames Research Center, NASA Dryden, Boeing Phantom Works, and Washington University in St. Louis.

On-Line Learning Without Baseline Network

Partial Derivative of Pitching moment w.r.t pitch rate (d/s)$^{-1}$



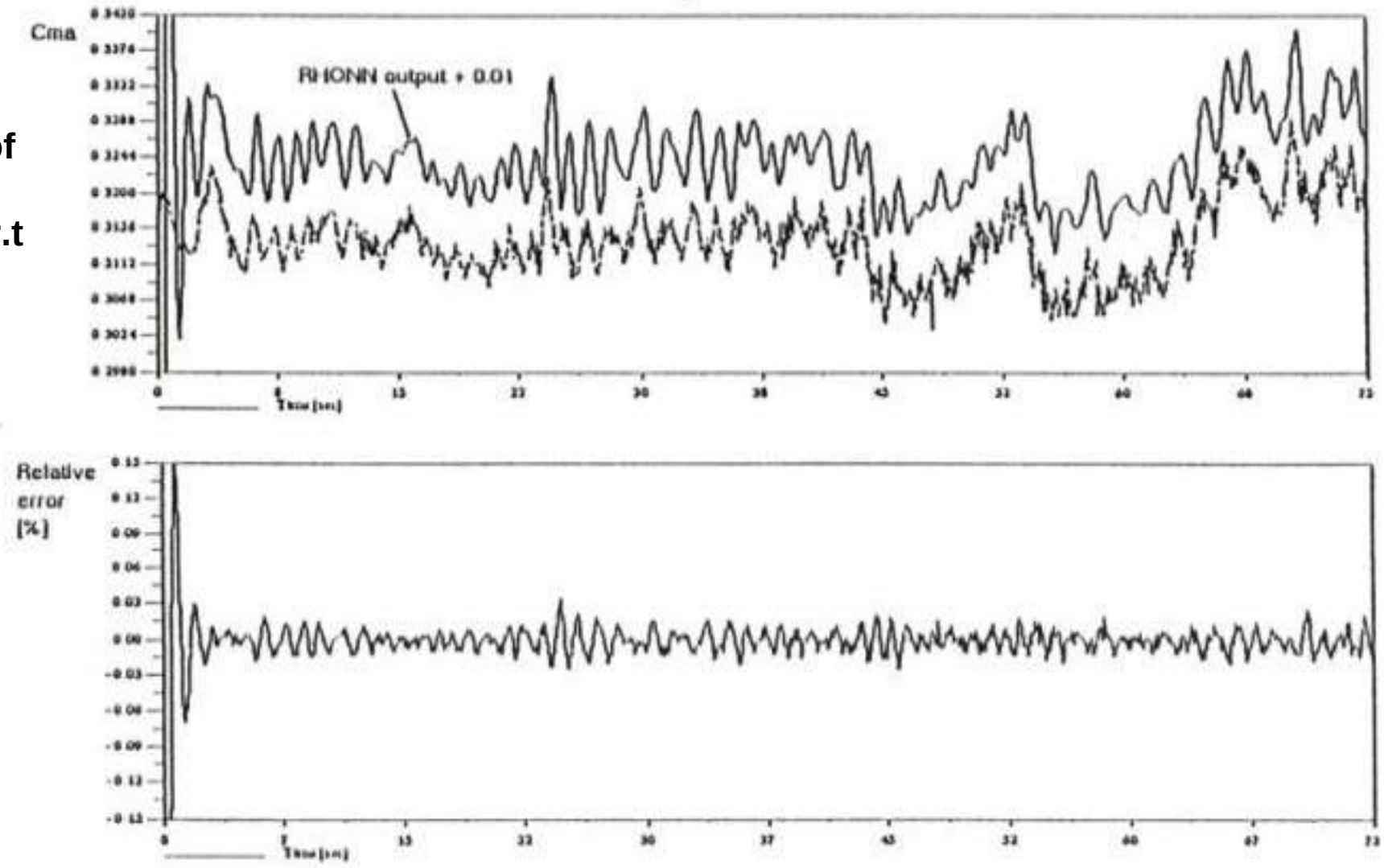
Partial Derivative of Pitching moment w.r.t AoA (d)$^{-1}$



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

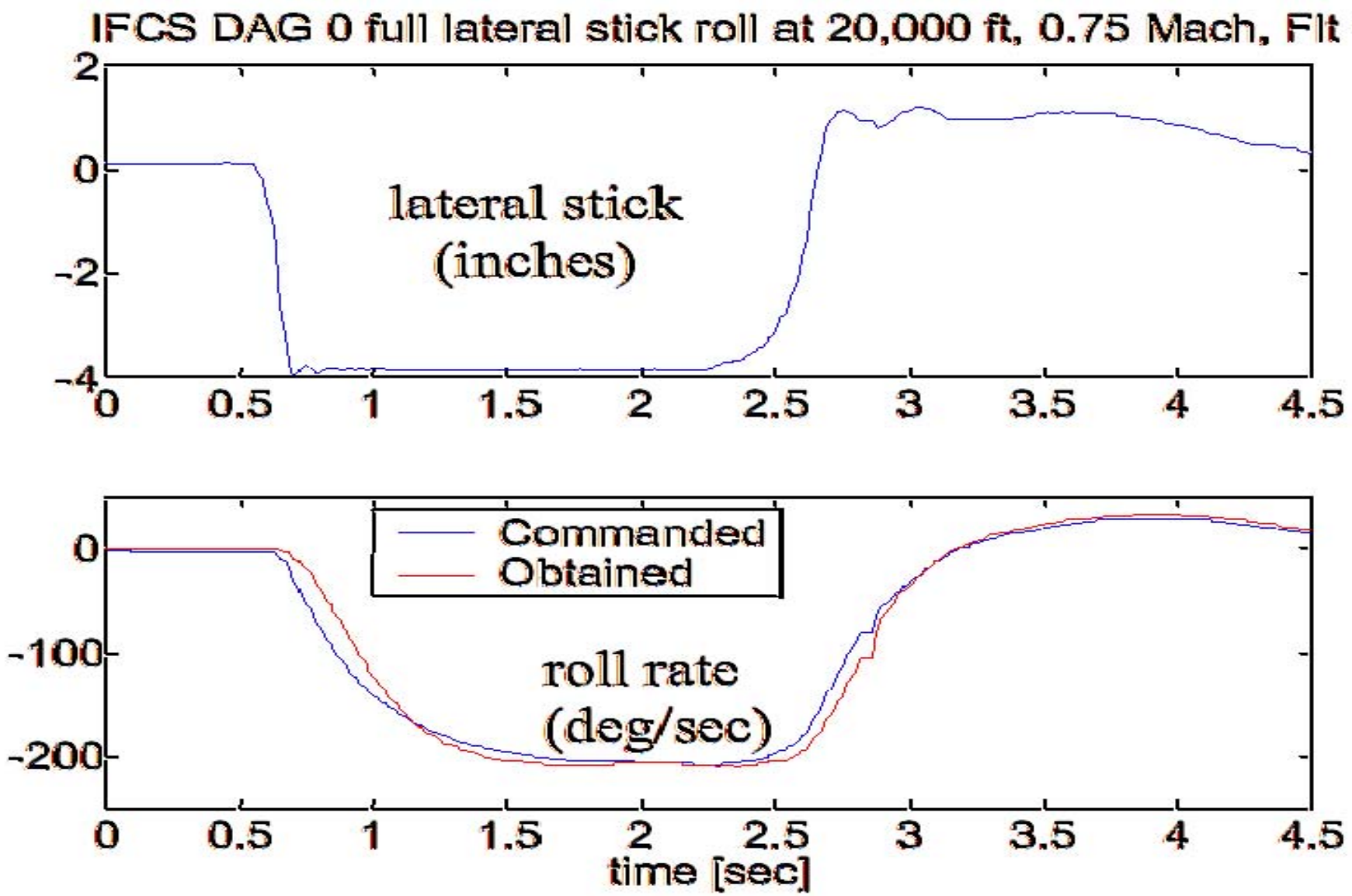
On-Line Learning Without Baseline Network

Partial Derivative of Pitching moment w.r.t AoA $(d)^{-1}$



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

Intelligent Flight Control System: Example – complete hydraulic failure (1997)



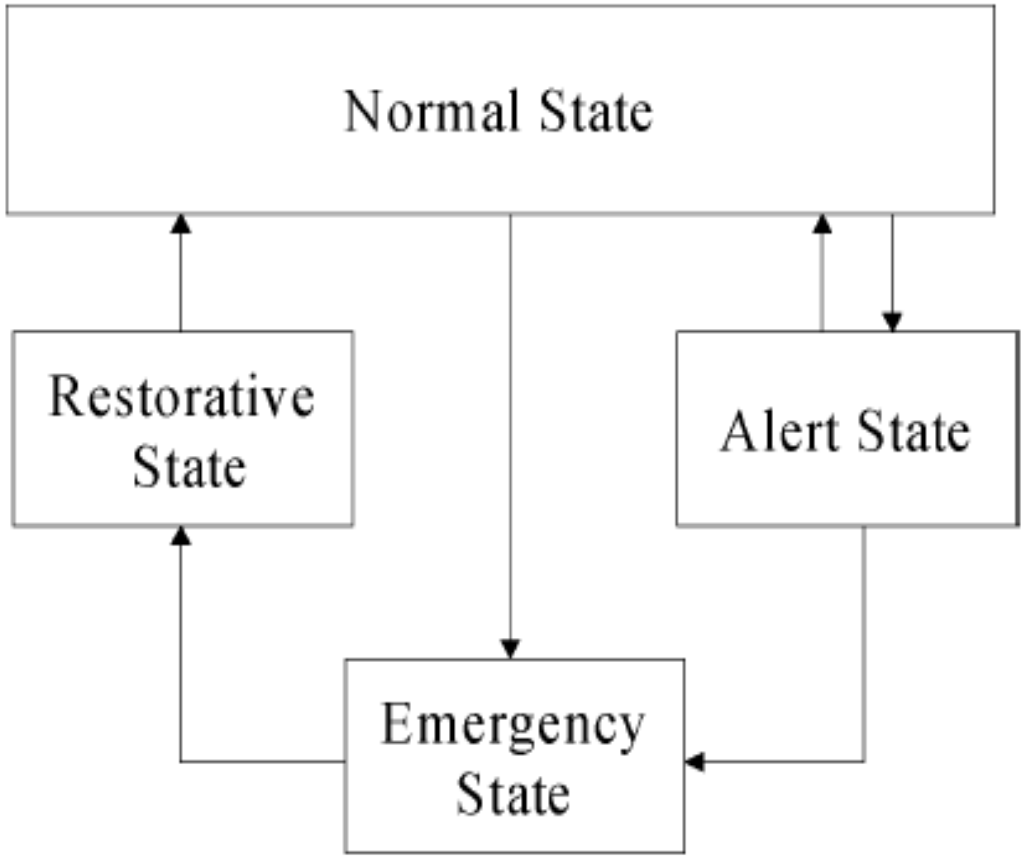
Accomplishments in the IFCS program

- The system was successfully test flown on a test F-15 at the NASA Dryden Flight Research Center:
  - Fifteen test flights were accomplished, including flight path control in a test flight envelope with supersonic flight conditions.
  - Maneuvers included 4g turns, split S, tracking, formation flight, and maximum afterburner acceleration to supersonic flight.
- Stochastic Optimal Feedforward and Feedback Technique (SOFFT) continuously optimizes controls to compensate for damage or failure conditions of the aircraft.
- Flight controller uses an on-line solution of the Riccati equation containing the neural network stability derivative data to continuously optimize feedback gains.
- Development team: NASA Ames Research Center, NASA Dryden Flight Research Center, Boeing Phantom Works, and Washington University.

Understanding Complex Dynamical Systems

Modes of Electric Power Systems:

- ***Normal mode:*** economic dispatch, load frequency control, maintenance, forecasting, etc.;
- ***Alert mode:*** red flags, precursor detection, reconfiguration and response;
- ***Emergency/Disturbance mode:*** stability, viability, and integrity -- instability, load shedding, etc.;
- ***Restorative mode:*** rescheduling, resynchronization, load restoration, etc.



Self-healing Smart Grid (1998-present)

Critical System Dynamics and 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.

The Smart Self Healing Grid

What is “self healing”?

A system that uses information, sensing, control and communication technologies to allow it to deal with unforeseen events and minimize their adverse impact

Overview of Focused Research Areas (1998-2003):
Programs Initiated and Developed at EPRI

1999-2001	Y2K2000-present	2002-present	2001-present
EPRI/DoD Complex Interactive Networks (CIN/SI)	**Enterprise Information Security (EIS)**	**Infrastructure Security Initiative (ISI)**	**Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)**
Underpinnings of Interdependent Critical National Infrastructures Tools that enable secure, robust & reliable operation of interdependent infrastructures with distributed intelligence & self-healing	1. Information Sharing 2. Intrusion/Tamper Detection 3. Comm. Protocol Security 4. Risk Mgmt. Enhancement 5. High Speed Encryption	**Response to 9/11 Tragedies** 1. Strategic Spare Parts Inventory 2. Vulnerability Assessments 3. Red Teaming 4. Secure Communications	1. Self Healing Grid 2. IntelliGrid™ 3. Integrated Electric Communications System Architecture 4. Fast Simulation and Modeling

Self-healing Lifeline Infrastructure Systems

EPRI/DOD Complex Interactive Network/Systems Initiative (1998-2002)

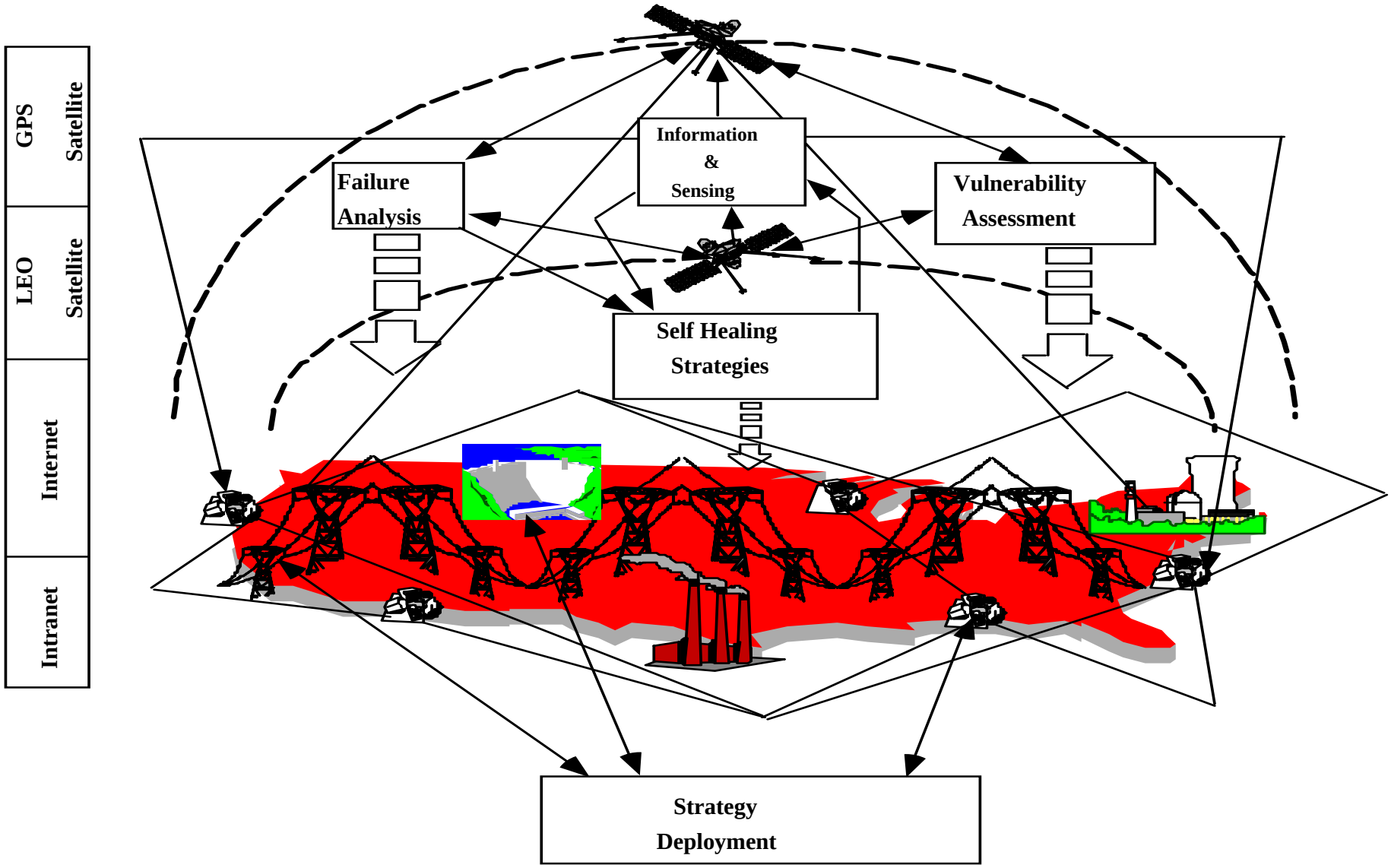
Complex interactive networks:

- **Energy infrastructure:** Electric power grids, water, oil and gas pipelines
- **Telecommunications:** Information, communications and satellite networks
- **Transportation and distribution networks**
- **Energy markets, banking and finance**

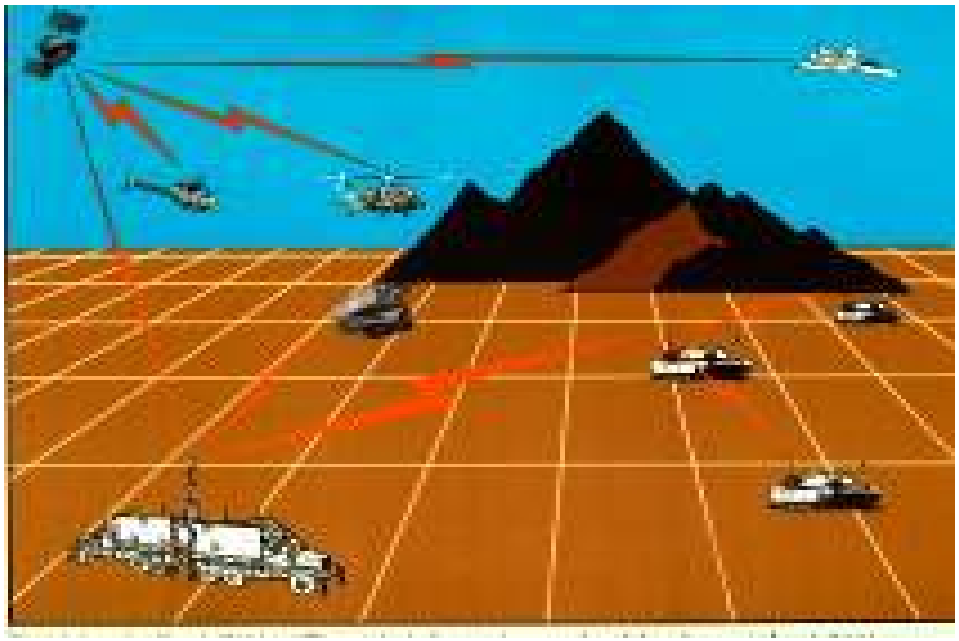
108 professors and over 240 graduate students in 28 U.S. universities were funded: Over 420 publications, and 24 technologies extracted, in the 3-year initiative

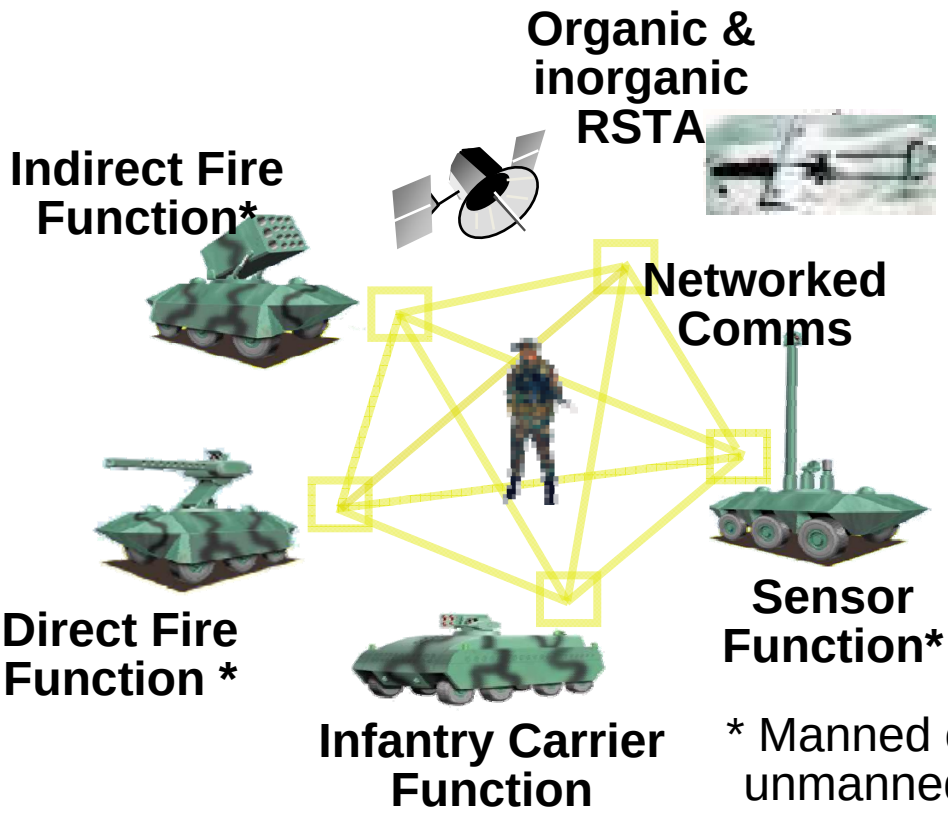
Goal: Develop tools that enable secure, robust and reliable operation of interdependent infrastructures with distributed intelligence and self-healing abilities

Complex Interactive Networks



Network Centric Objective Force





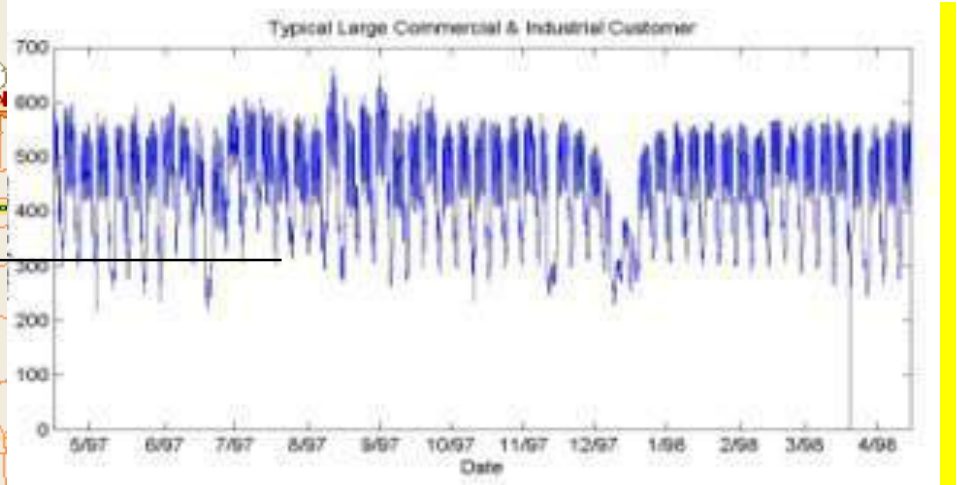
EPRI/DOD CIN/SI Funded Consortia

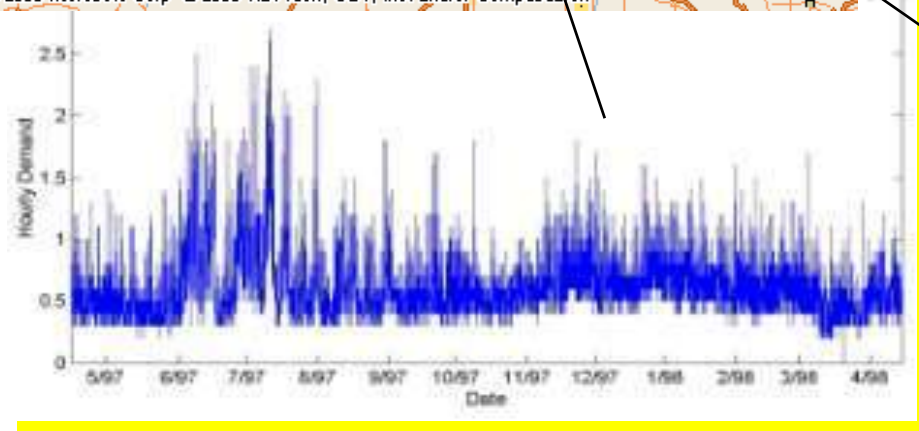
108 professors and over 240 graduate students in 28 U.S. universities were funded: Over 420 publications, and 24 technologies extracted, in the 3-year initiative (1998-2001)

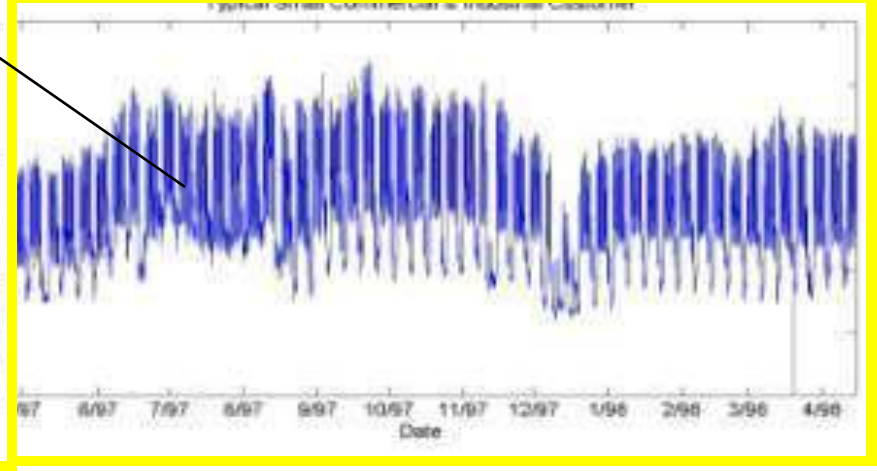
• U Washington, Arizona St., Iowa St., VPI	- Defense Against Catastrophic Failures, Vulnerability Assessment
• Purdue, U Tennessee, Fisk U, TVA, ComEd/Exelon	- Intelligent Management of the Power Grid
• Harvard, UMass, Boston, MIT, Washington U.	- Modeling and Diagnosis Methods
• Cornell, UC-Berkeley, GWU, Illinois, Washington St., Wisconsin	- Minimizing Failures While Maintaining Efficiency / Stochastic Analysis of Network Performance
• CMU, RPI, UTAM, Minnesota, Illinois	- Context Dependent Network Agents
• Cal Tech, MIT, Illinois, UC-SB, UCLA, Stanford	- Mathematical Foundations: Efficiency & Robustness of Distributed Systems

"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

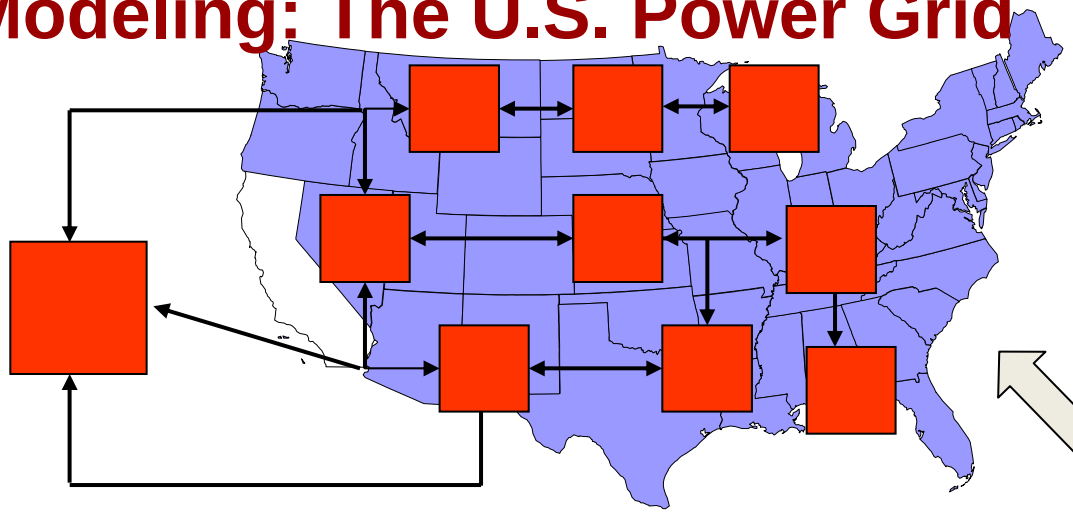
Local area grids (LAG)







Macro-Level Modeling: The U.S. Power Grid



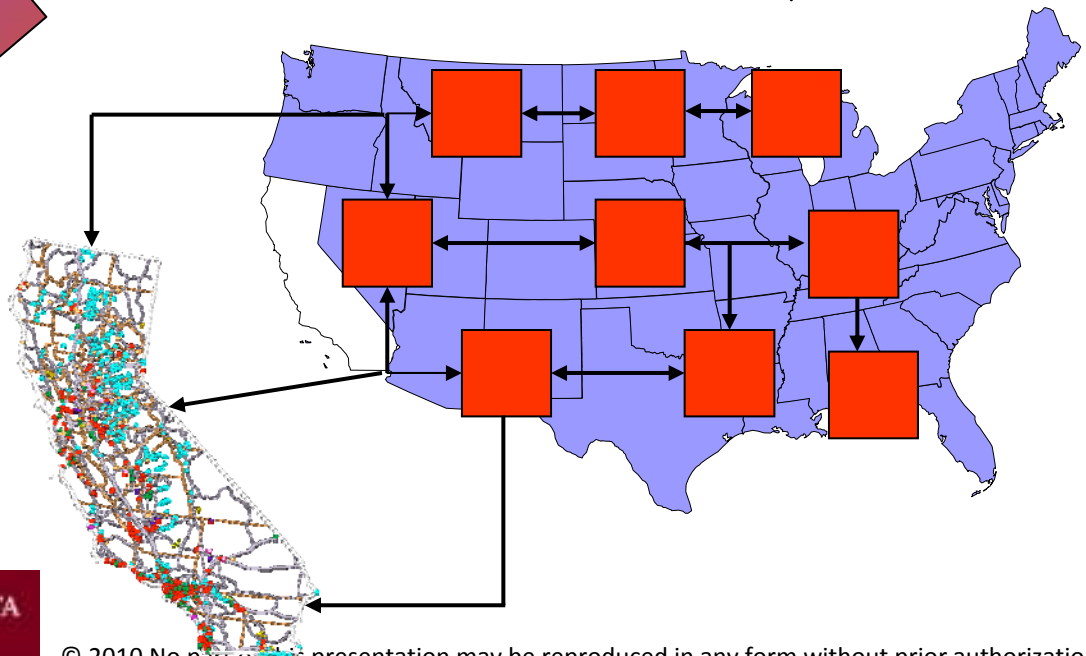
Simplified models

Low-resolution model

MODEL REDUCTION

MODEL REFINEMENT

- Variable levels of details
- Lines, loads, generators are *dynamic*



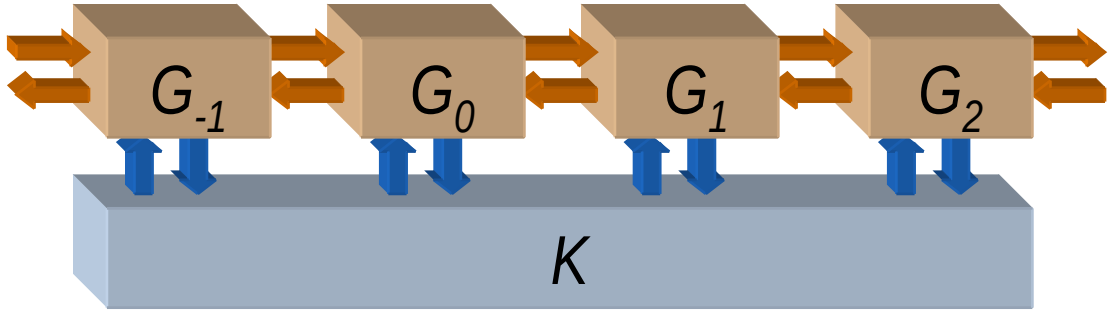
Detailed models

Look-Ahead Simulation Applied to Multi-Resolution Models

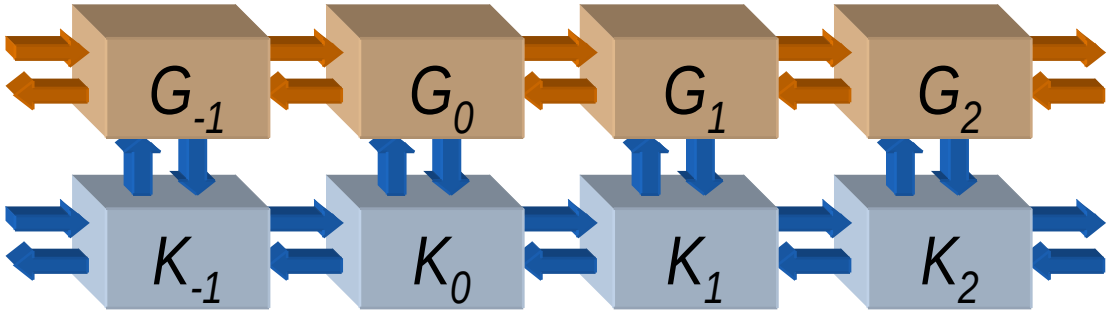
- Provides faster-than-real-time simulation
  - By drawing on approximate rules for system behavior, such as power law distribution
  - By using simplified models of a particular system
- Allows system operators to change the resolution of modeling at will
  - Macro-level (regional power systems)
  - Meso-level (individual utility)
  - Micro-level (distribution feeders/substations)

Sensing and Control Strategies

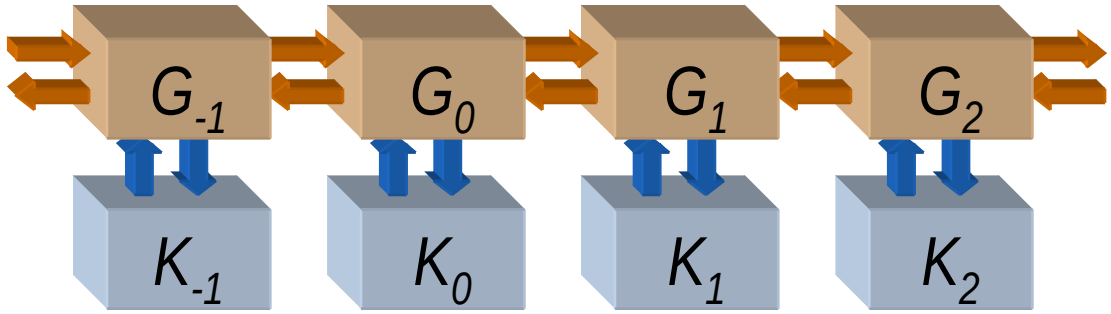
- Centralized



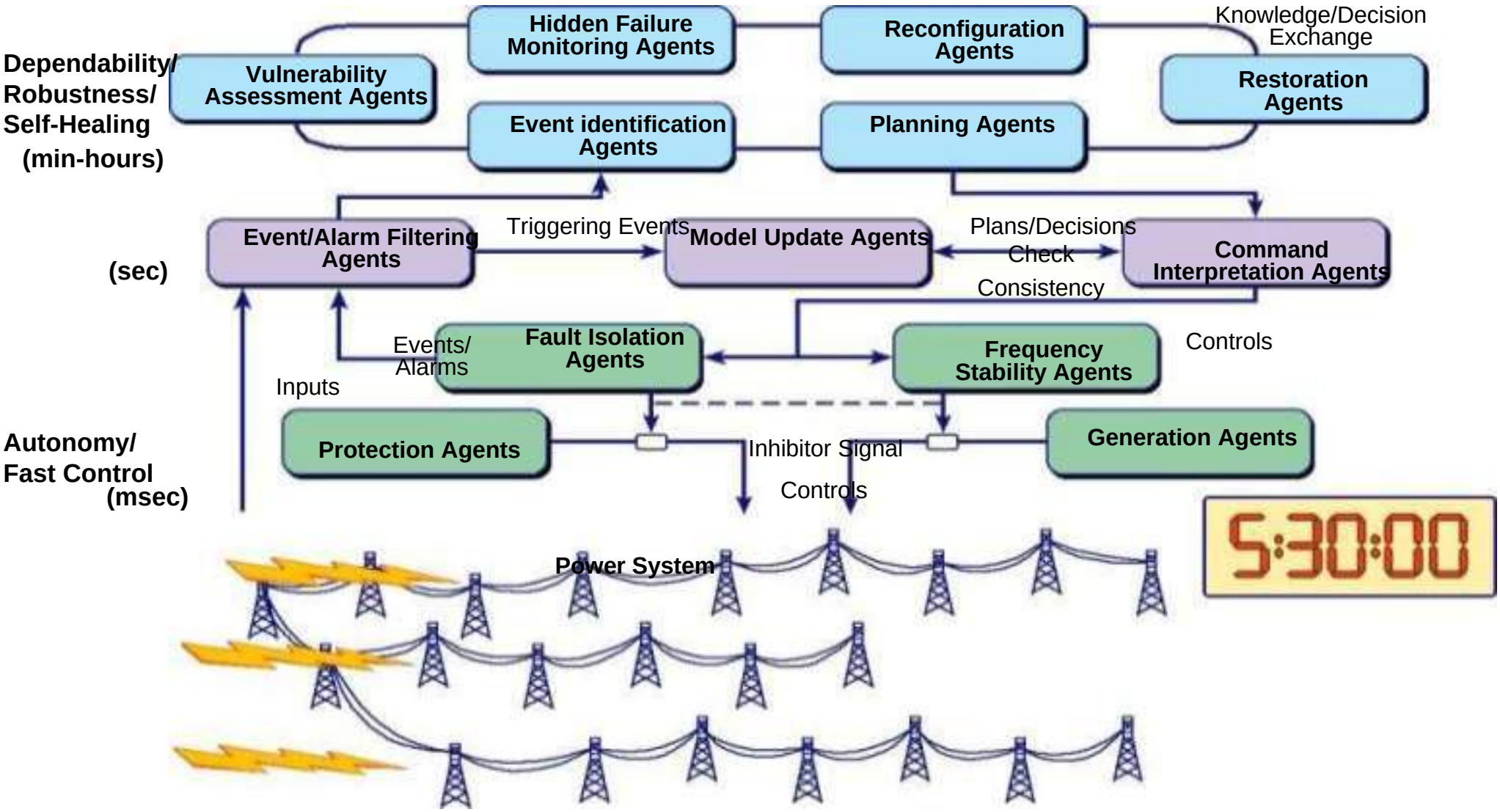
- Distributed



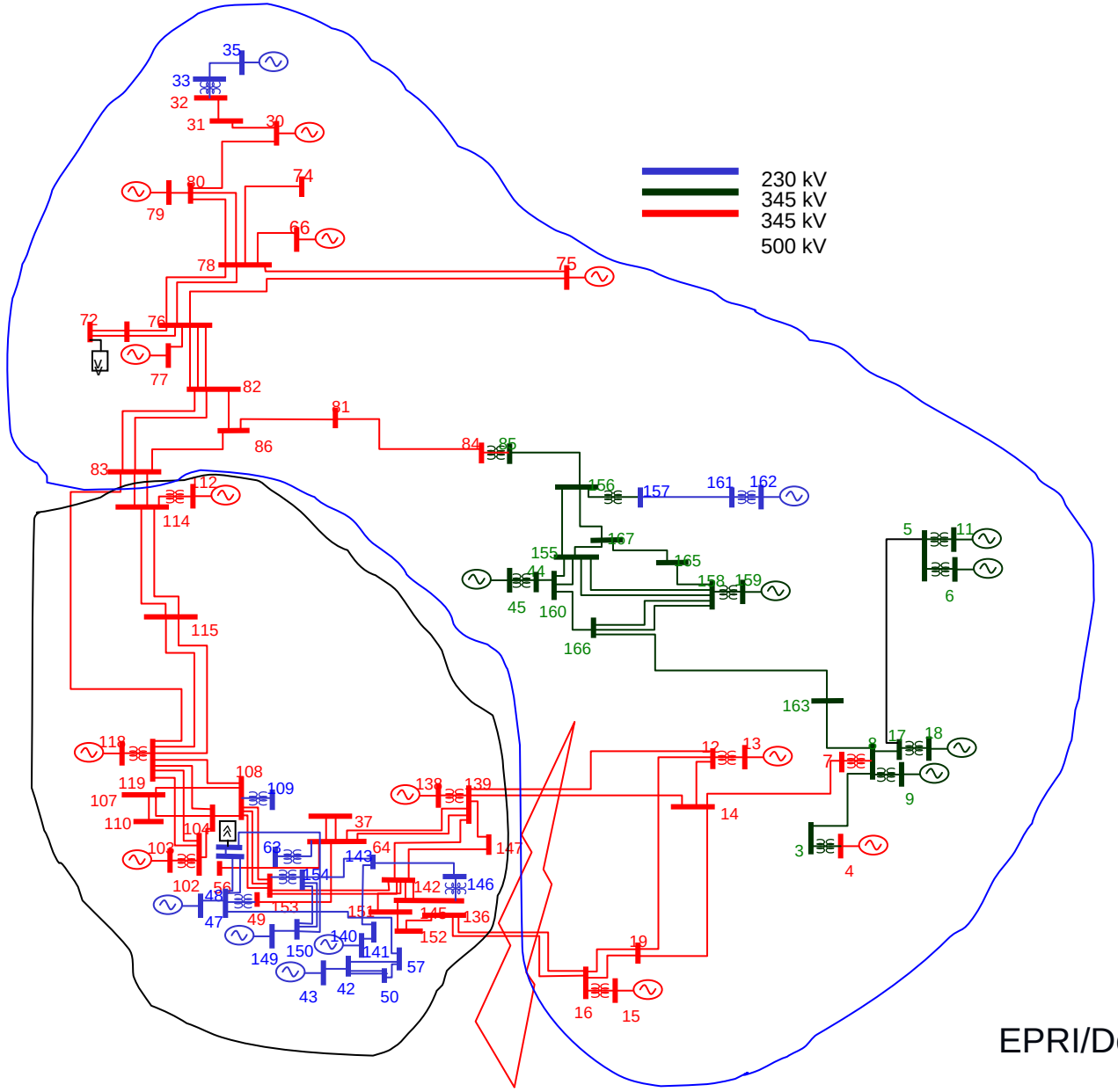
- Perfectly decentralized



Background: The Self-Healing Grid

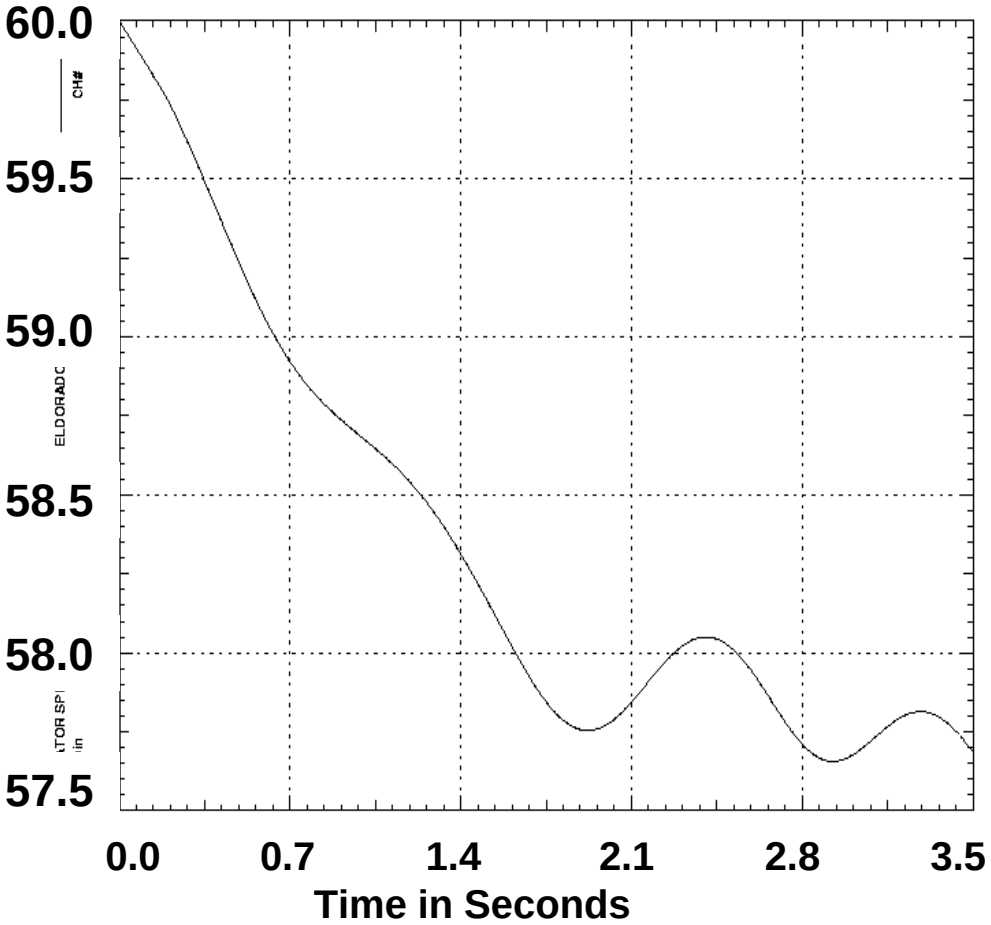


Background: The Self-Healing Grid
Intelligent Adaptive Islanding

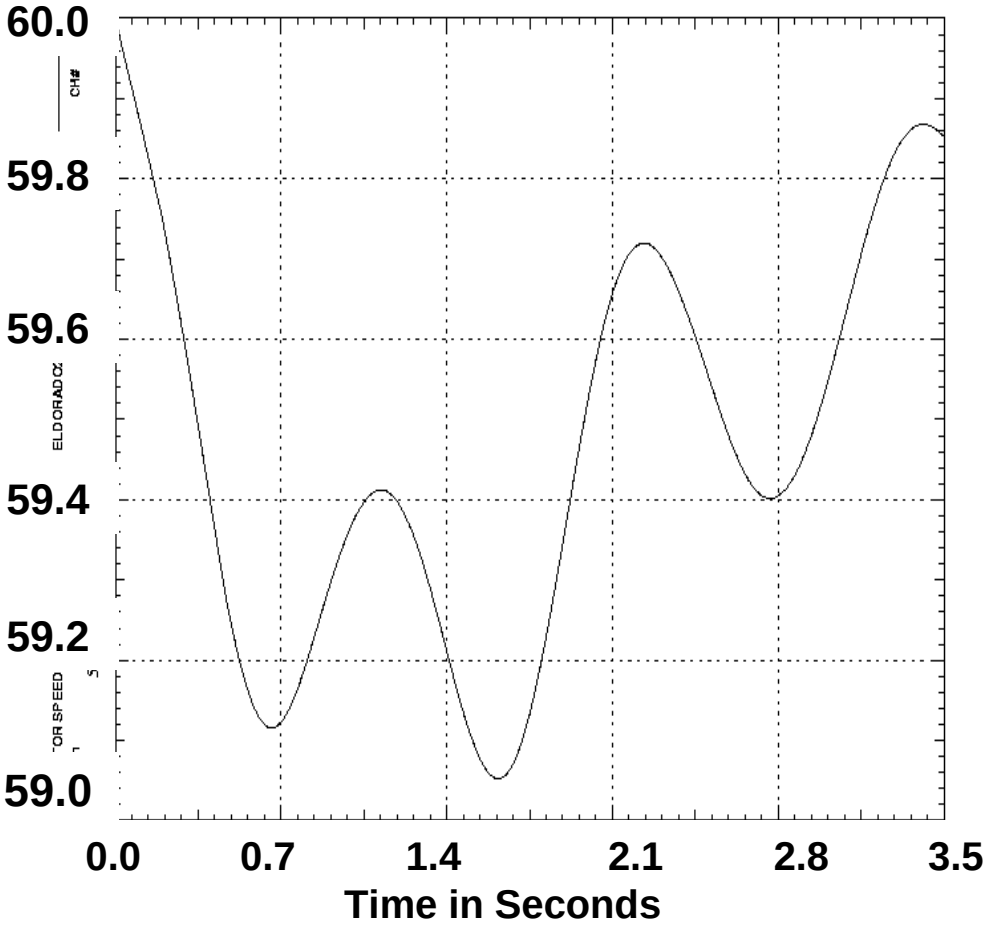


EPRI/DoD CIN/S Initiative

Background: Simulation Result

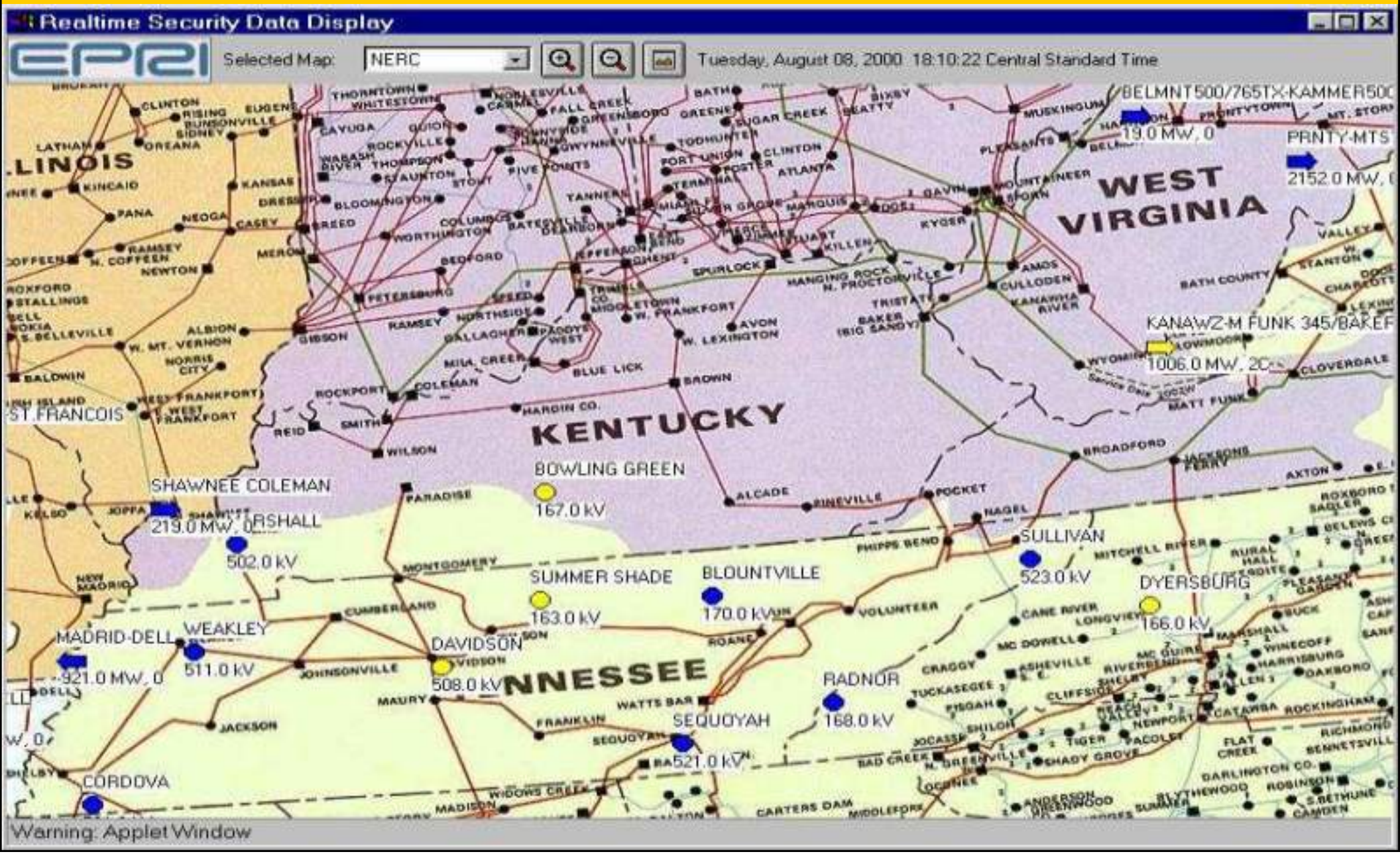


Past Scheme

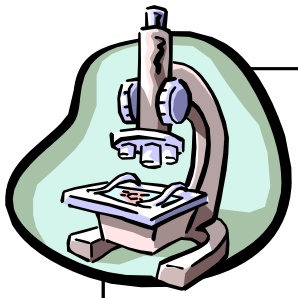


New Scheme

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



Example of In Depth Analysis: Critical Contingency Situations



Overview of Consortia Research Results:

A Canvas of R&D for Reliable and Robust Operation vs. Solution Components:

108 professors and over 240 graduate students in 28 U.S. universities funded (lead universities shown)

Challenges	Measurement & Sensing (including visualization)	Modeling & Theory	Simulation	Control System Design	Operation & Management
Efficient Operation	Harvard Purdue U. Washington	Caltech Cornell Harvard Purdue	Carn. Mellon Harvard Purdue U. Washington	Caltech Carn. Mellon Cornell Harvard U. Washington	Carn. Mellon Harvard Purdue U. Washington
Security and Robustness	Harvard Purdue U. Washington	Caltech Carn. Mellon Cornell Harvard Purdue	Caltech Carn. Mellon Harvard Purdue Washington	Caltech Carn. Mellon Cornell Harvard U. Washington	Carn. Mellon Harvard Purdue U. Washington
Cascading Failure - single infrastructure	Harvard Purdue U. Washington	Caltech Carn. Mellon Cornell Harvard Purdue U. Washington	Caltech Carn. Mellon Cornell Harvard Purdue U. Washington	Caltech Carn. Mellon Cornell Harvard U. Washington	Carn. Mellon Cornell Purdue U. Washington
Cascading Failure - multiple infrastructures	Harvard	Caltech Cornell	Caltech Cornell Harvard U. Washington	Cornell Harvard U. Washington	Cornell U. Washington

Solution Components

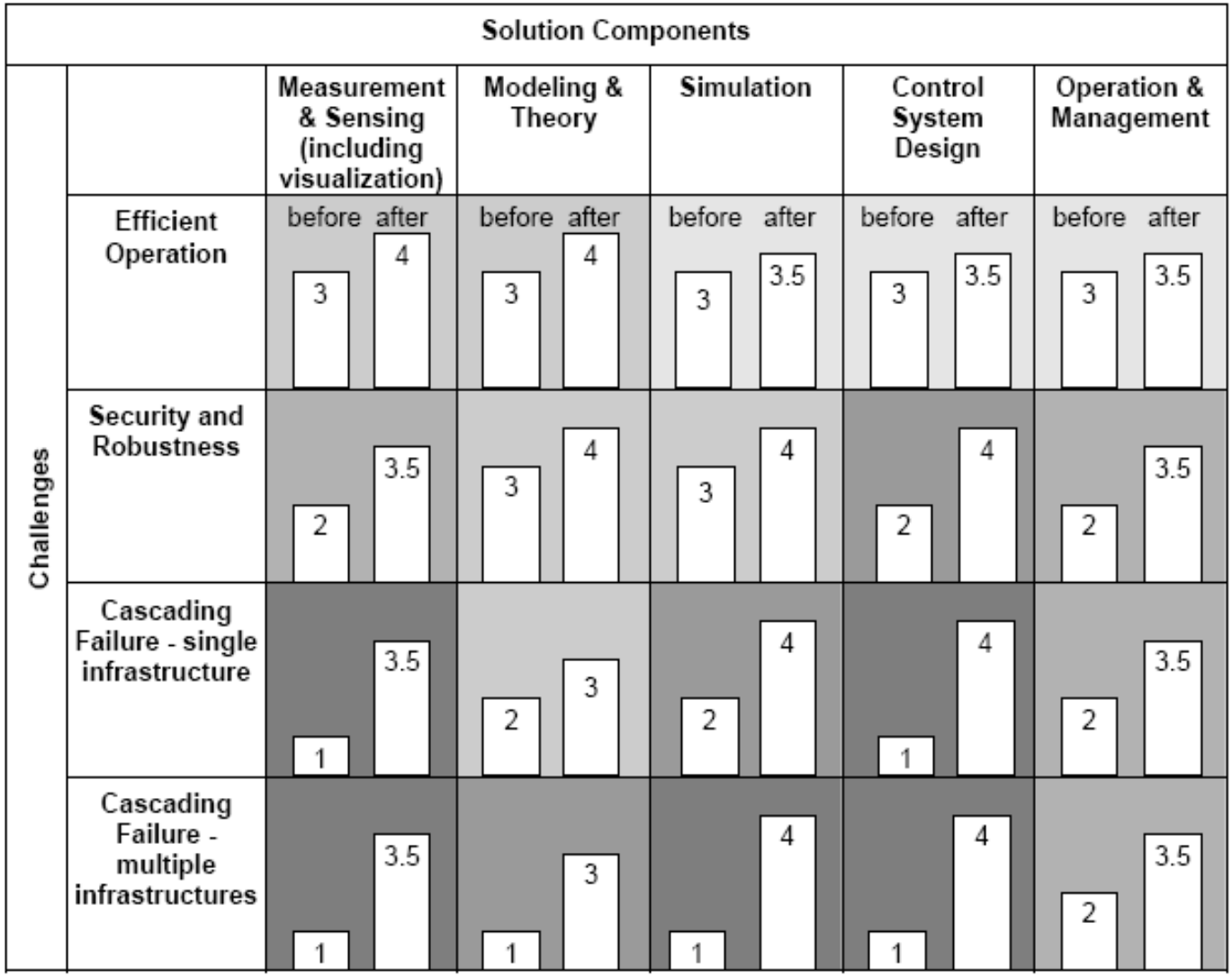
Technological Leadership Institute

UNIVERSITY OF MINNESOTA
Driven to Discover℠

State of Understanding about Complex Interactive Networks and Systems:

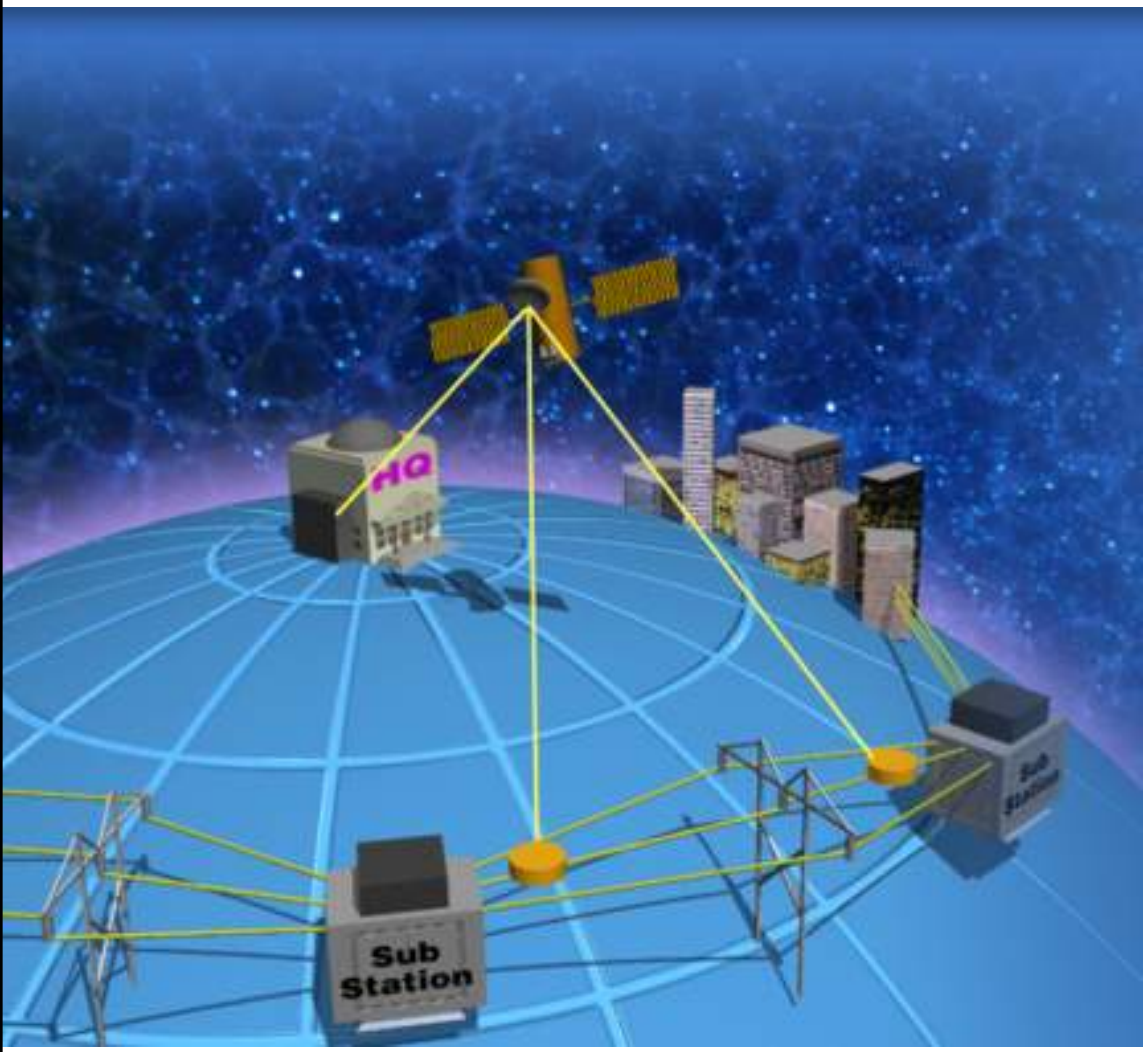
The CIN/SI represents the first systems approach to complex interactive networks, based on advancing the mathematical and theoretical foundations:

Understanding of Complex Networks in Key Challenge and Solution Component Areas before and after CIN/SI



Key:
1—minimal understanding
2—some understanding but insufficient for practical applications
3—partial understanding with some useful practical applications
4—solid understanding with many practical applications
5—complete (or near-complete) understanding and applicability
Shading indicates the degree that understanding advanced by CINSI research.

The Self-Healing, Digital Quality Smart Grid



Self-Healing Transmission Grid

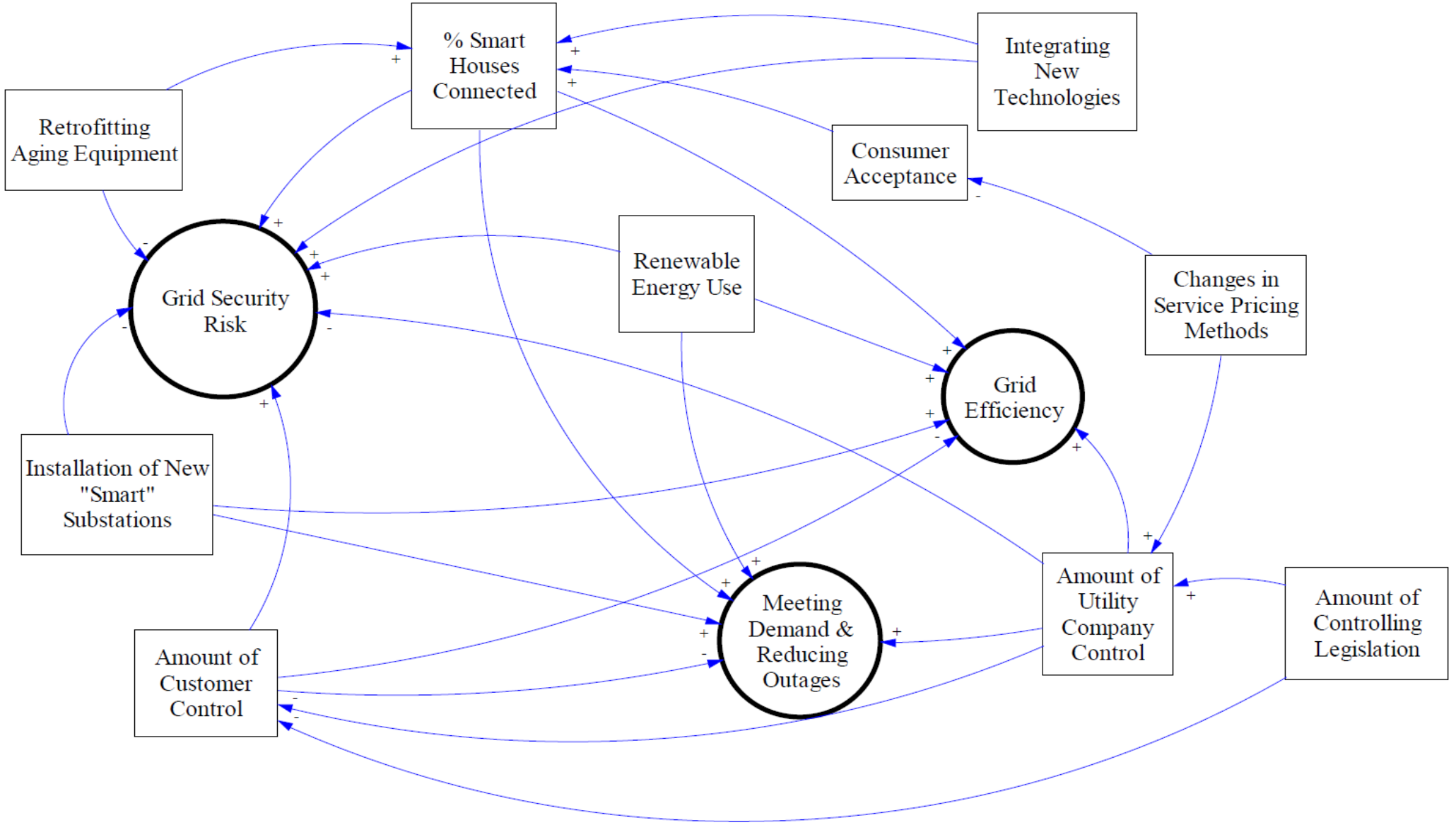
Self-Healing Distribution Network

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	

Smart Grid Interdependencies

Security, Efficiency, and Resilience



Transmission Limits

- High dimensional problem
  - Large interconnection models require ~40,000 buses & ~50,000 lines, and ~3,000 generators with ~120 control areas
  - Each line has a capacity limit
  - The system must withstand of loss of any one line or generator (~53,000 contingencies)
  - 53,000 x 50,000 = 2,650,000,000 possible constraints
- Reliable operation requires an operating point that satisfy these 2.65 billion constraints

Dynamics of Large Electric Power Systems

S = P + jQ

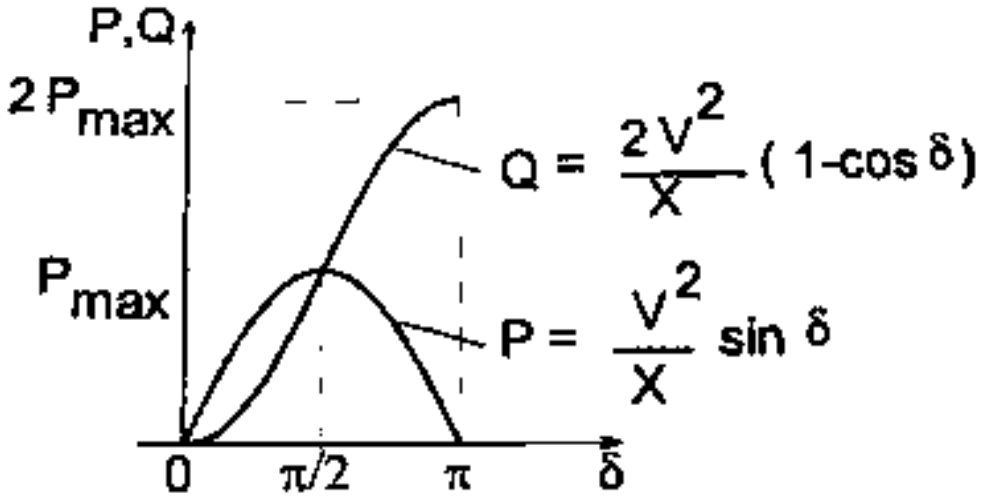
$$\sum Pi$$ = PGenerator + PLoad + PCompensation

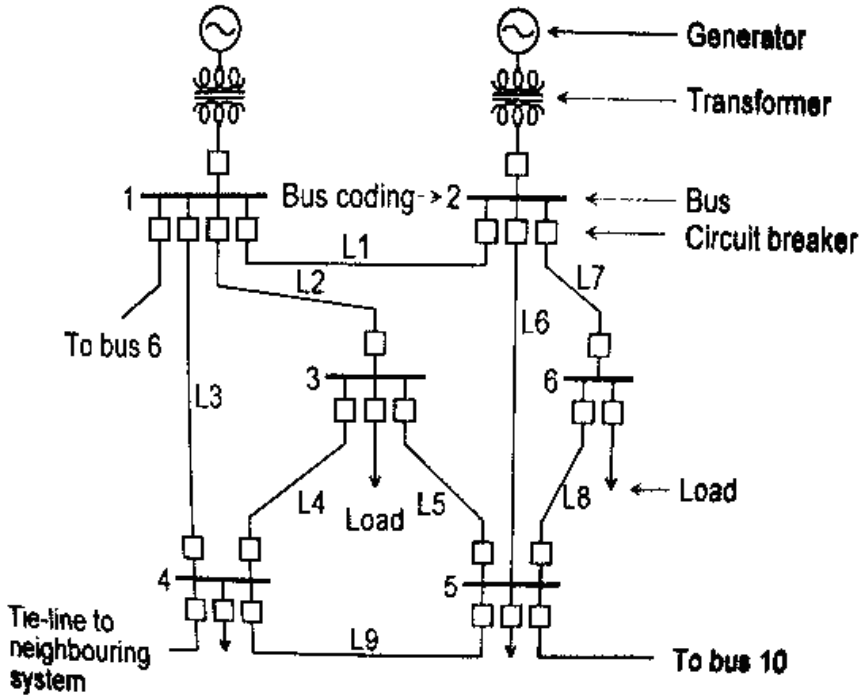
$$\sum Qi$$ = QGenerator + QLoad + QCompensation

V voltage
X reactance
δ phase angle
I current

Real Power: $$P = \frac{V^2}{X} \bullet \sin\delta$$

Reactive Power: $$Q \approx V \bullet I \bullet \sin(\delta/2) = \frac{V^2}{X} \bullet (1 - \cos\delta)$$





State Estimation:

$$Z = h(X) + V$$

where:

Z = The measurement vector

X = The state vector

V = The measurement error vector

$h(X)$ = Non-linear observation function, the set of electrical equations relating MW and MVAR values to bus voltages and angles

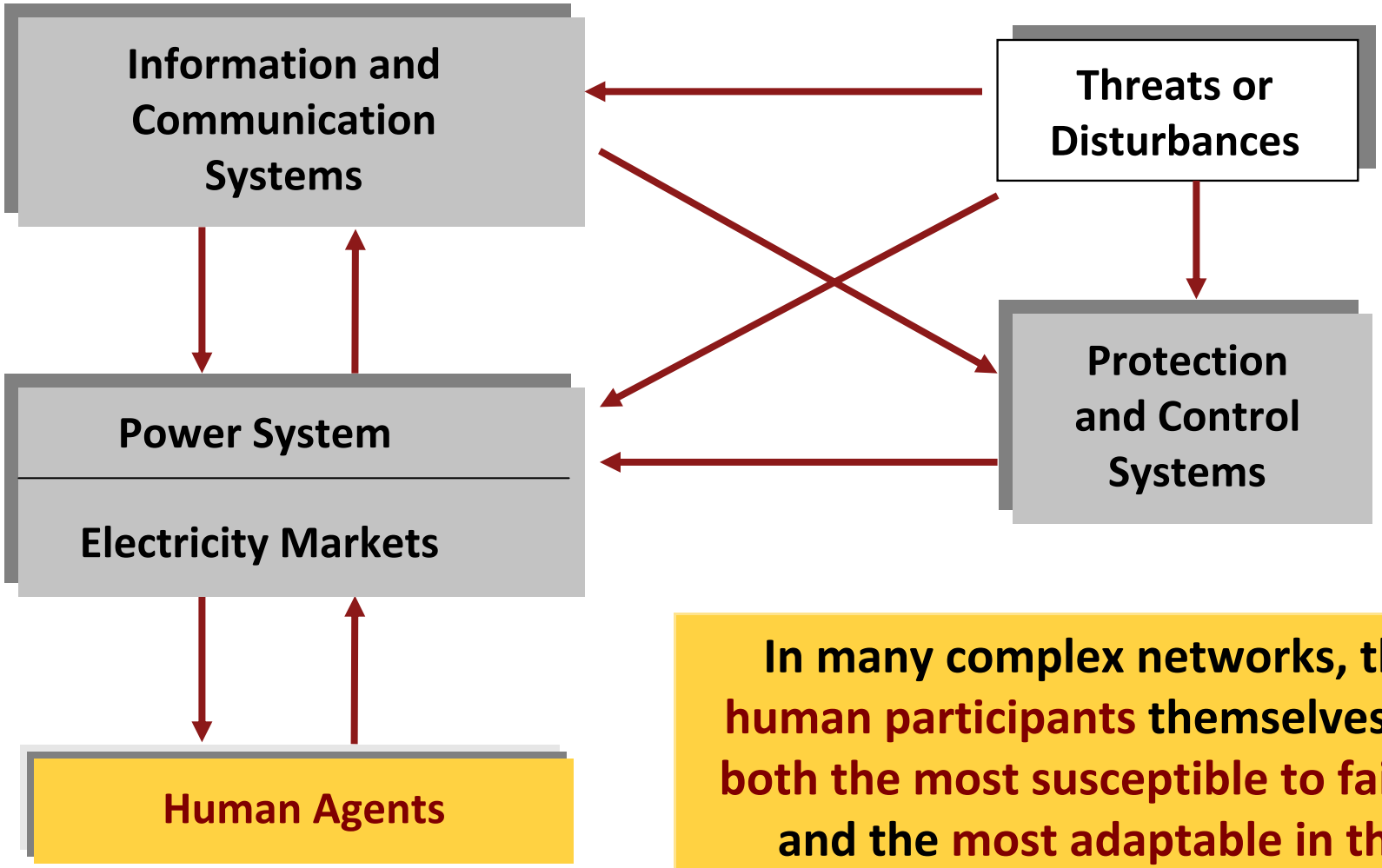
$$Min.\ J(X) = [\ Z - h(X)\ ]^T\ R^{-1}\ [\ Z - h(X)\ ]$$

R = The measurement error covariance matrix

Extended to Advanced Topology Estimator:

- Will determine unknown substation switch settings from voltages, power flows, and current measurements

Integrated Sensing, Protection and Control



In many complex networks, the human participants themselves are both the most susceptible to failure and the most adaptable in the management of recovery.

Smart Grid

The Smart Grid: 12 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: "Self-Healing" Smart Grid (1998-present, M. Amin)

- **What is a smart 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, improving security, quality, resilience, robustness, and facilitating the interconnection of new generating sources to the grid.

- **What are the power grid's emerging issues?** They include

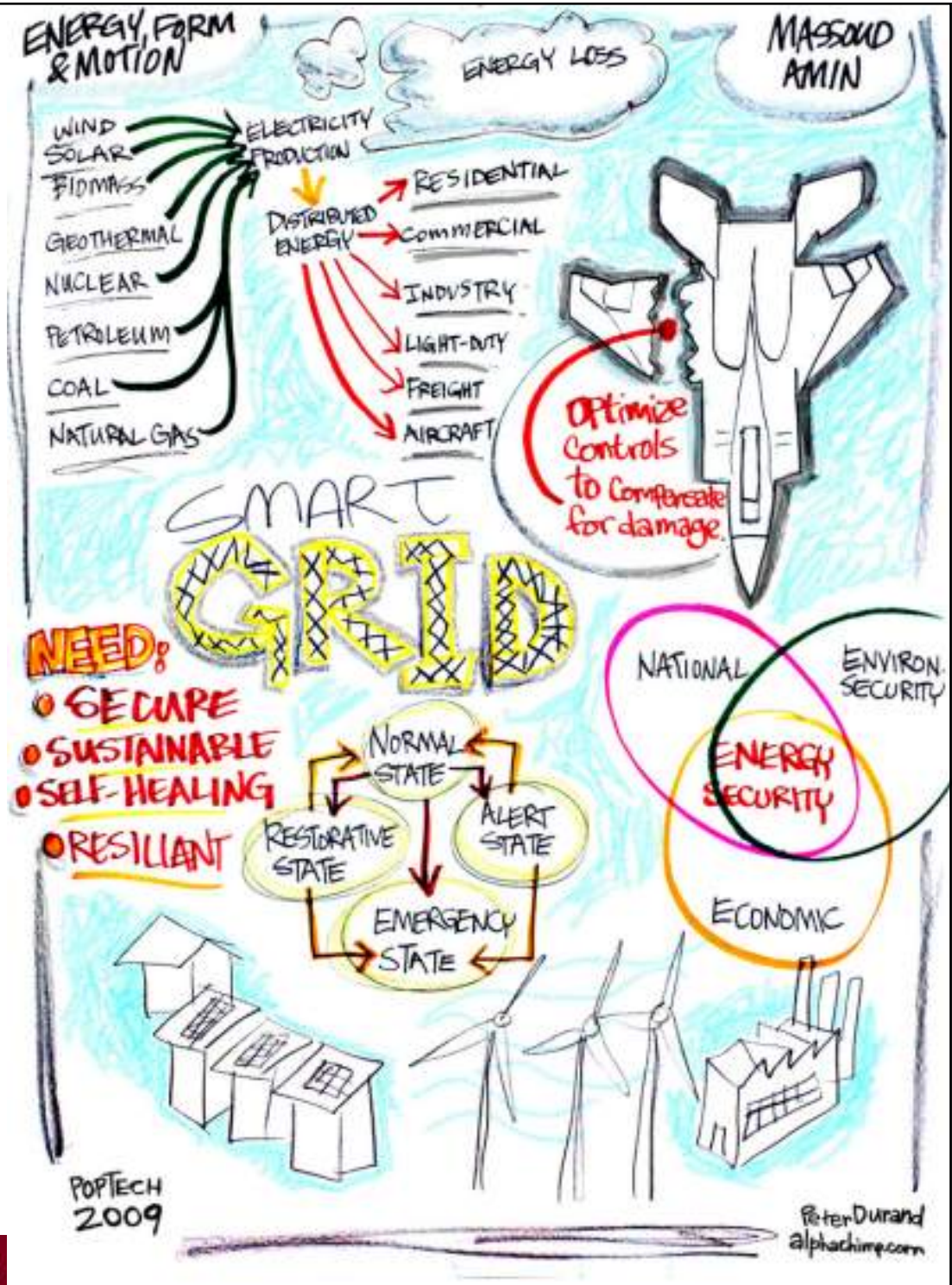
  1) integration and management of DER, renewable resources, and "microgrids";
  2) use and management of the integrated infrastructure with an overlaid sensor network, secure communications and intelligent software agents;
  3) active-control of high-voltage devices;
  4) developing new business strategies for a deregulated energy market; and
  5) ensuring system stability, reliability, robustness, security and efficiency in a competitive marketplace and carbon constrained world.

The Emerging Smart Grid or Energy Web:
A Complex Adaptive Infrastructure System

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

"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."

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



Technological Leadership Institute

UNIVERSITY OF MINNESOTA
Driven to Discover℠

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."*

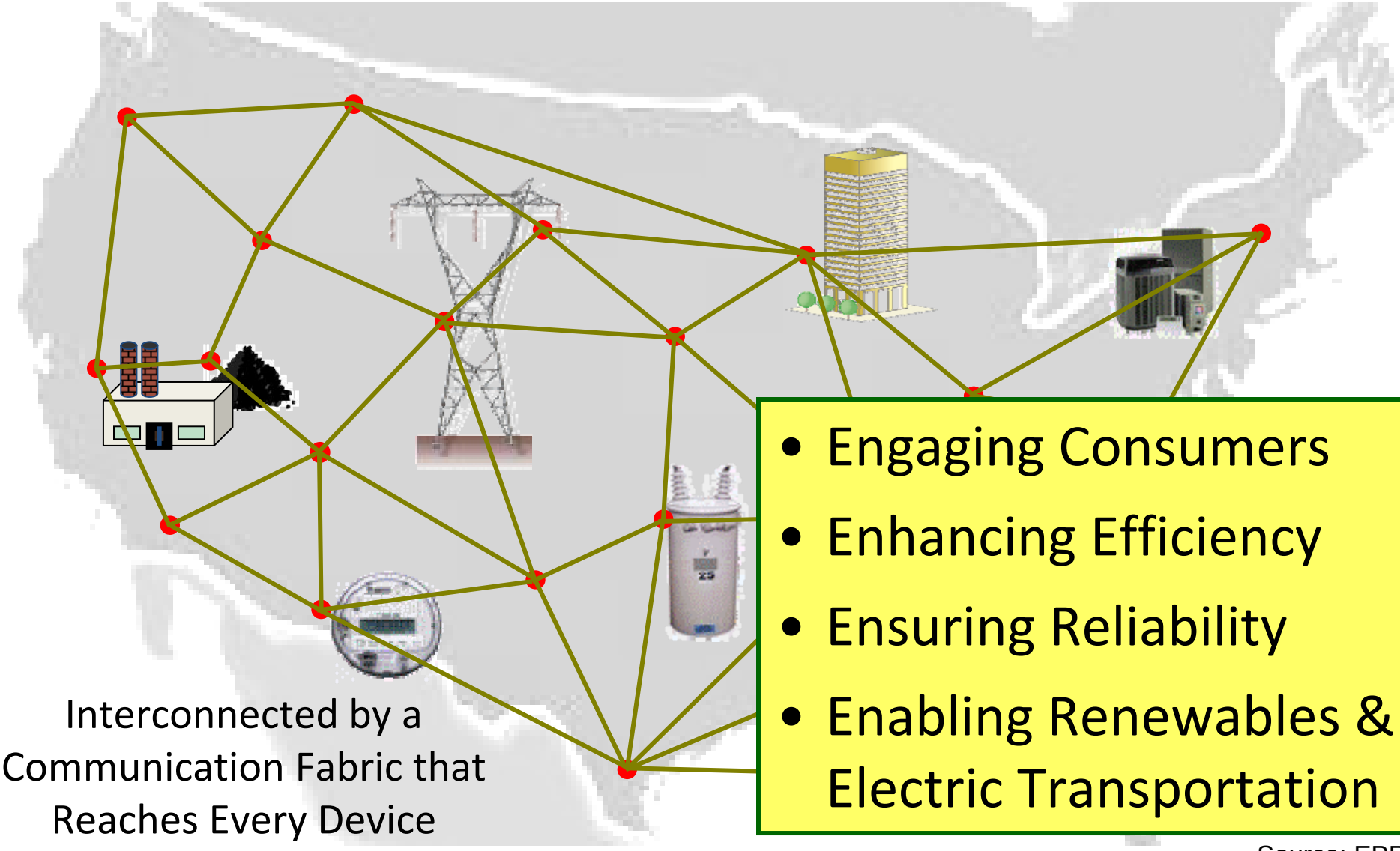
Wikipedia: *"A Smart Grid delivers electricity from suppliers to consumers using digital technology to save energy, reduce cost, and increase reliability."*

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

Visualizing the Smart Grid

Many Definitions – But One VISION

Highly Instrumented with Advanced Sensors and Computing



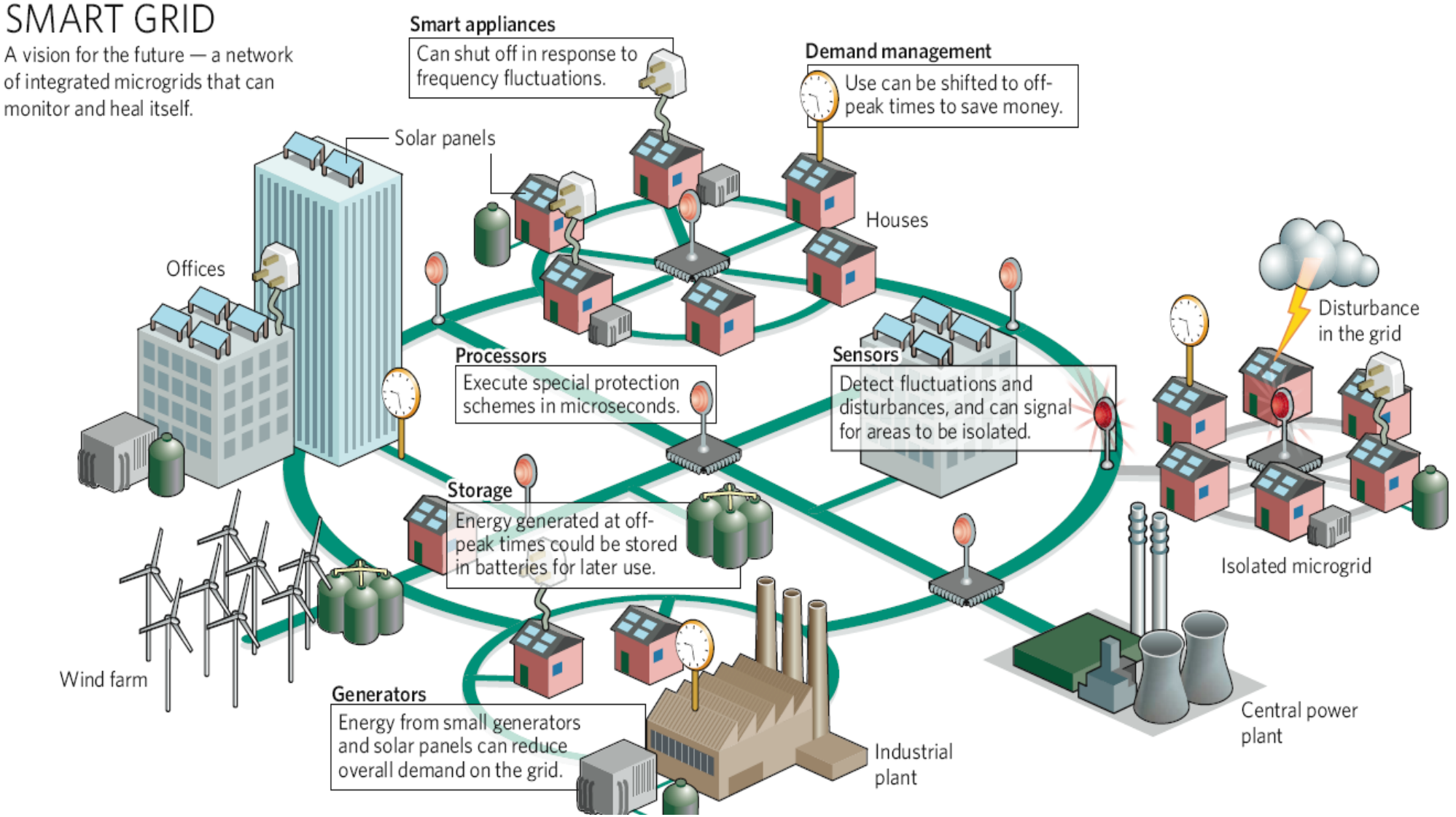
Interconnected by a Communication Fabric that Reaches Every Device

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

Source: EPRI

Enable the Future

Integrate microgrids, diverse generation and storage resources into a smart self-healing grid system



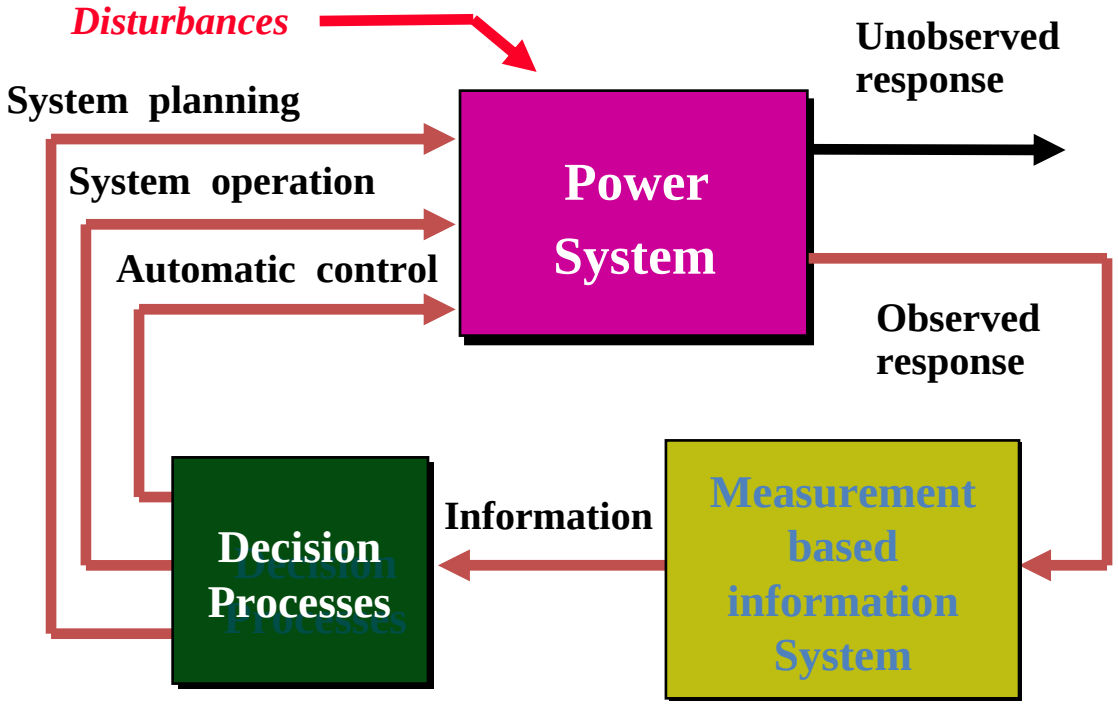
Source: Interview with Massoud Amin, "Upgrading the grid," *Nature,* vol. 454, pp. 570–573, 30 July 2008

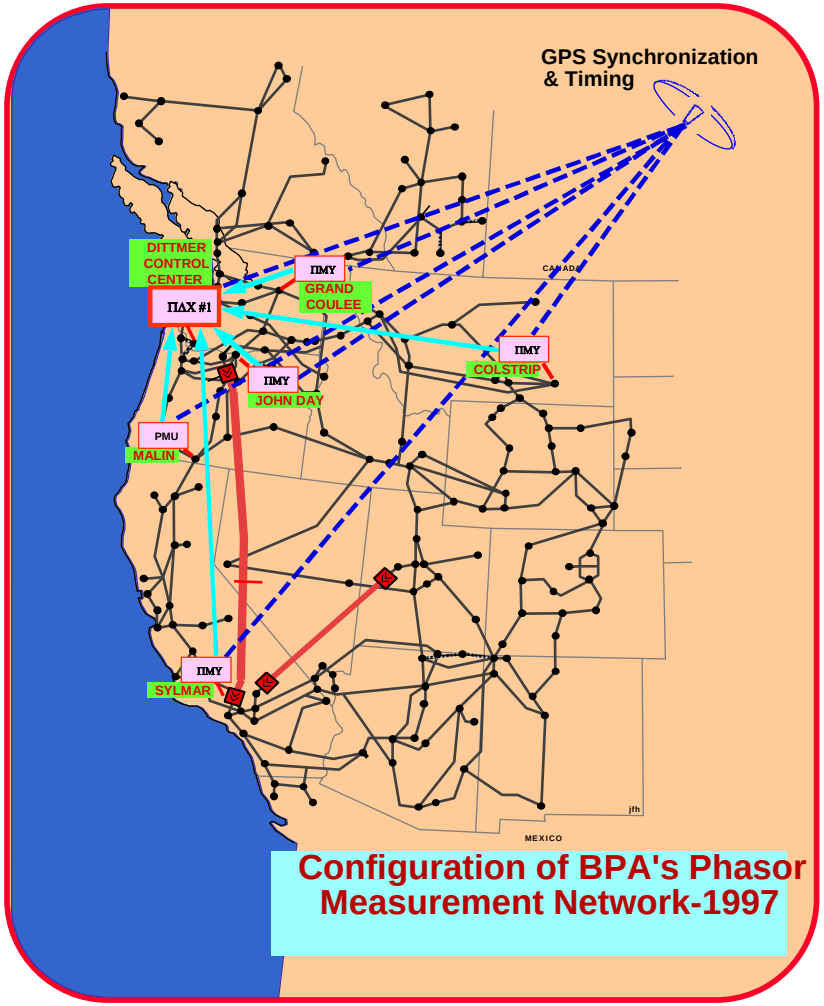
Data and Measurements

Wide-Area Measurement System (WAMS)

Integrated measurements facilitate system management

"Better information supports better - and faster - decisions."





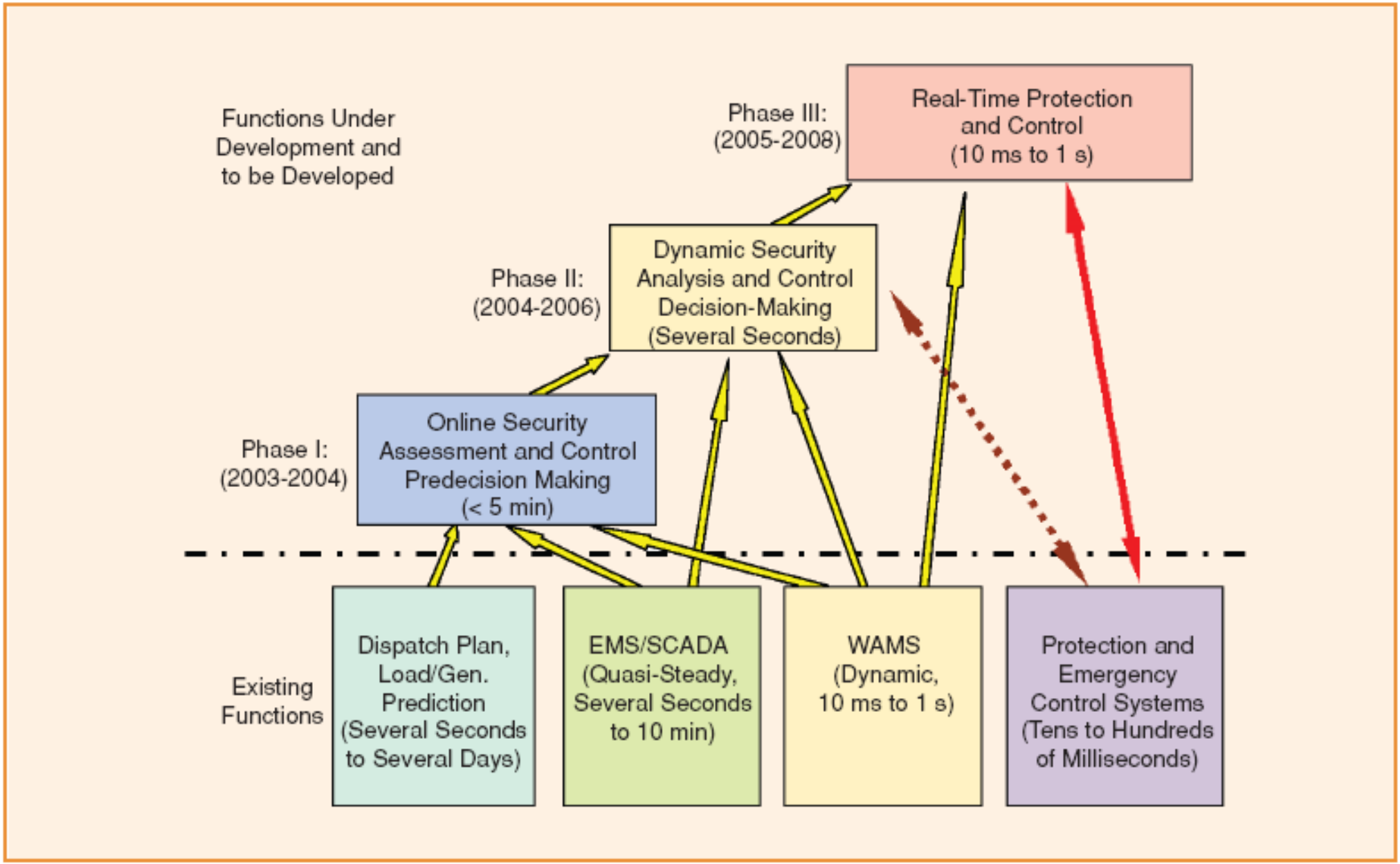
Source: DOE/EPRI WAMS project-- BPA & PNNL

Real-Time System Data

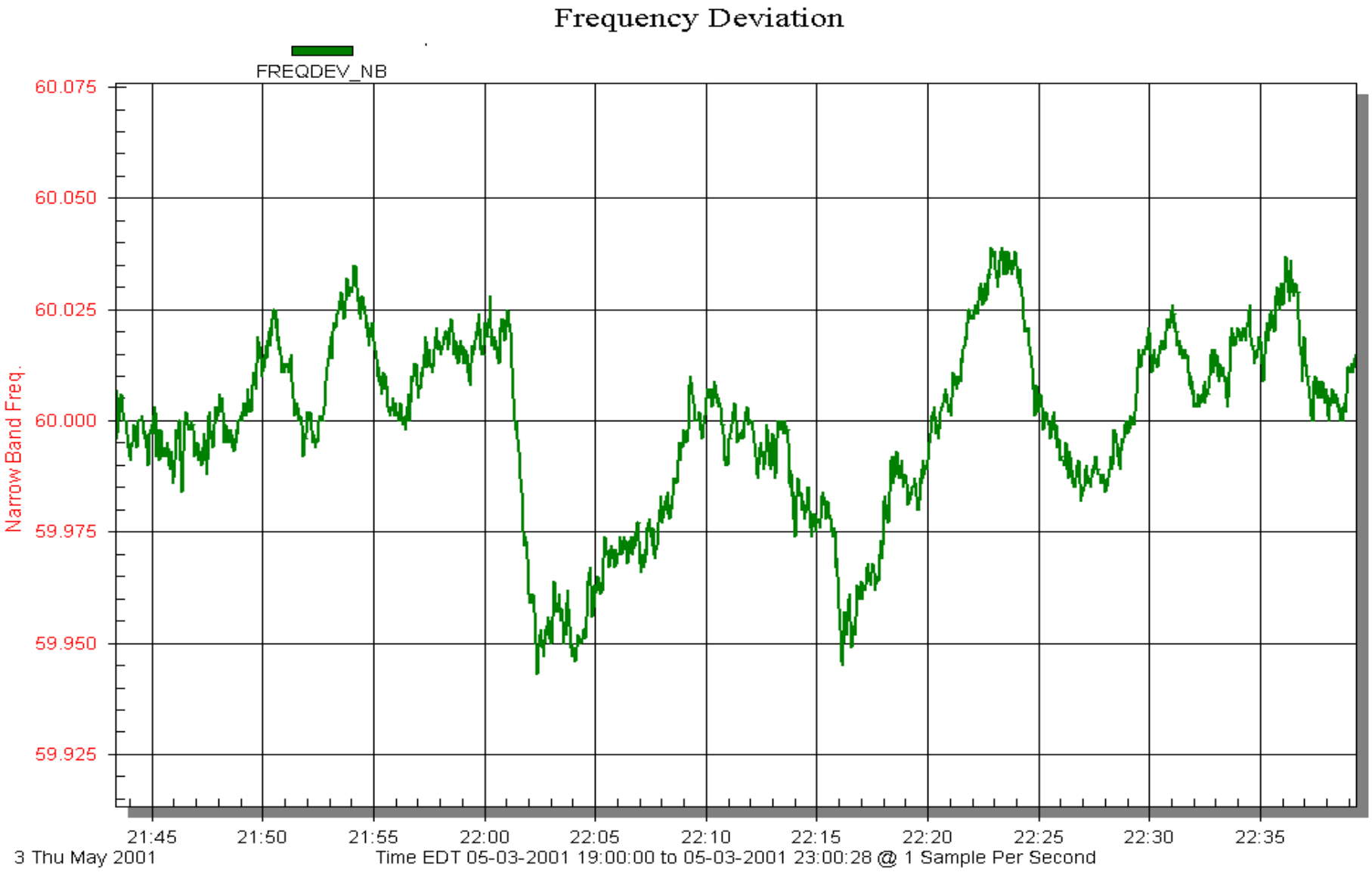
Collected from various monitors throughout the grid

Example: BPA's Phasor Data Concentrator

Three-phase WAMS application in China

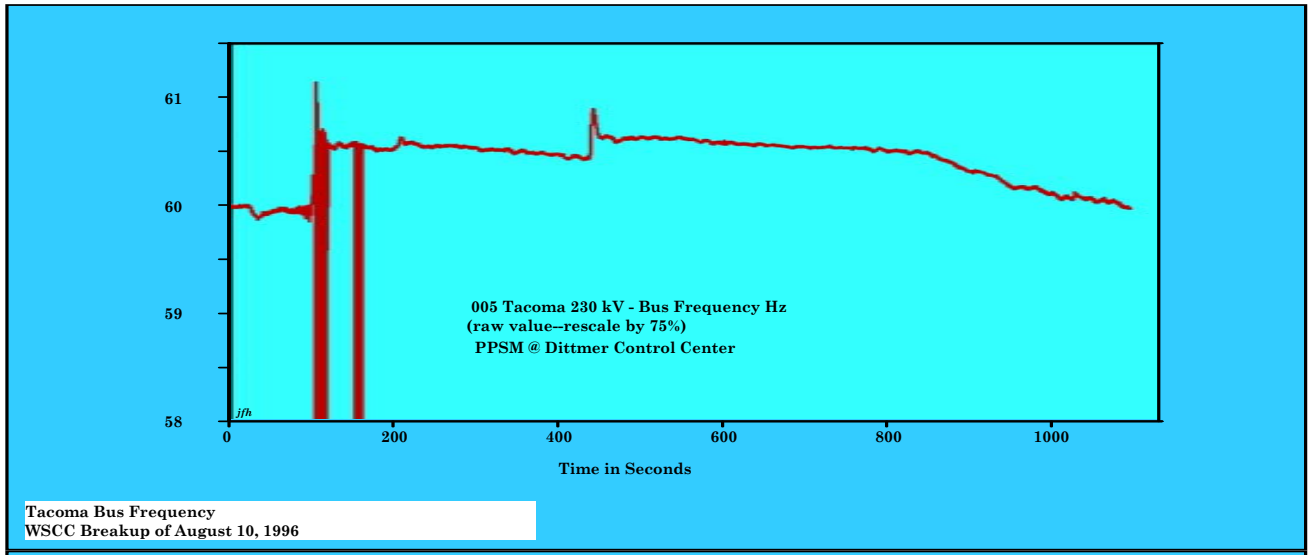


Last Episode of the TV series "Survivor"

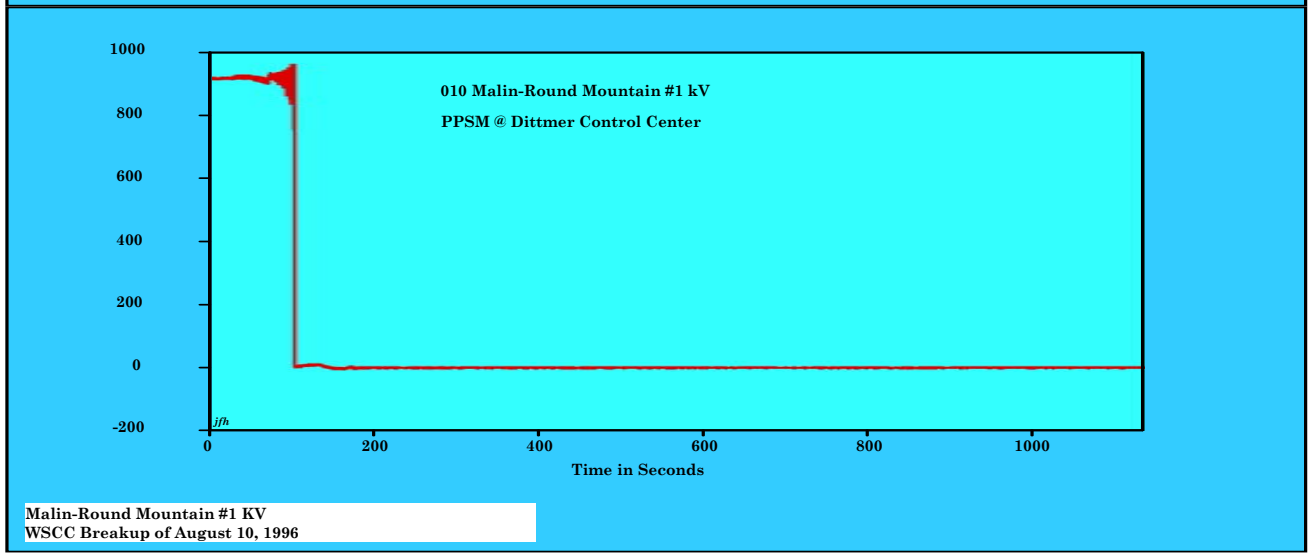


Source: Jim Ingleson (NYISO) and Joe Chow (RPI)

Disturbance records for WSCC breakup of August 10, 1996



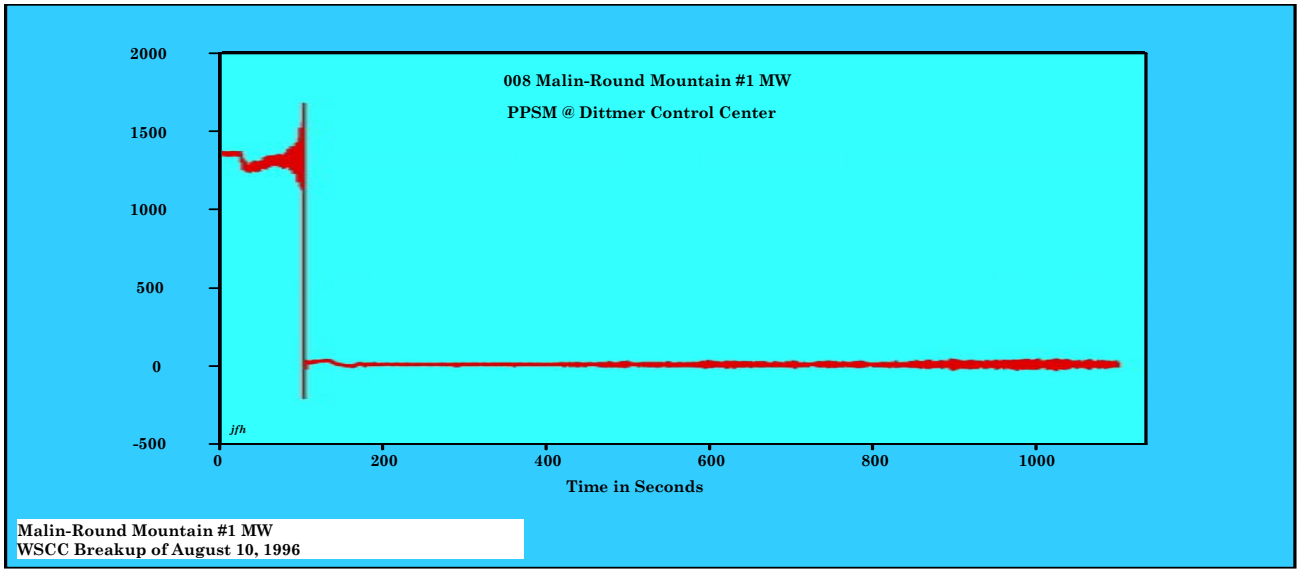
Tacoma Bus Frequency
WSCC Breakup of August 10, 1996



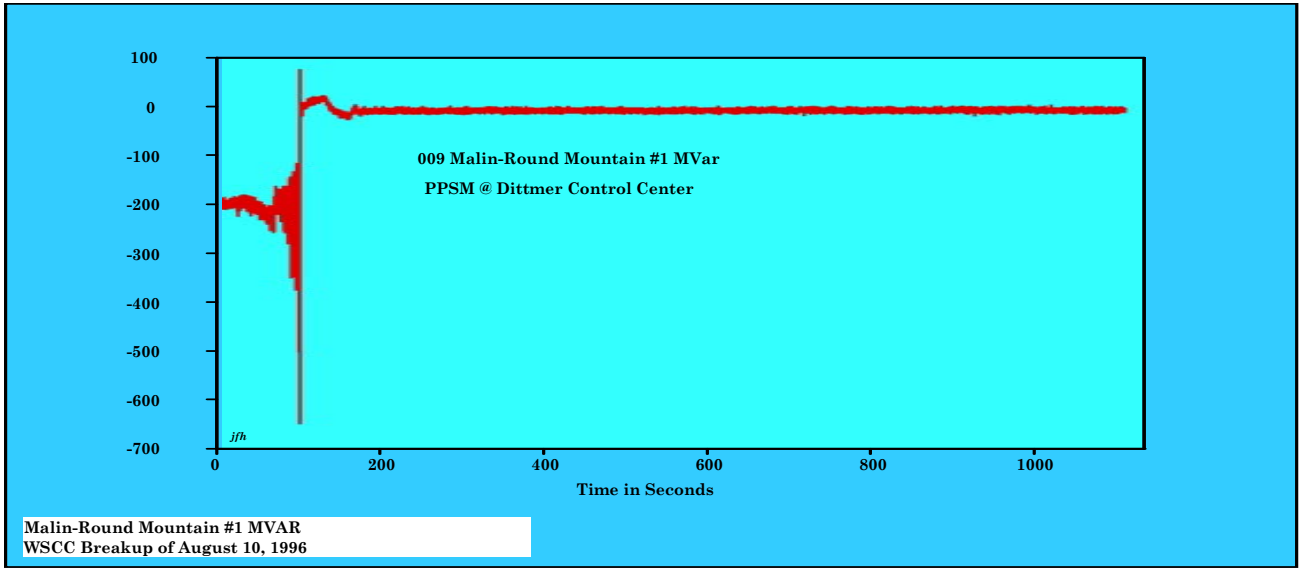
Malin-Round Mountain #1 KV
WSCC Breakup of August 10, 1996

Source: DOE/EPRI WAMS project

Disturbance records for WSCC breakup of August 10, 1996



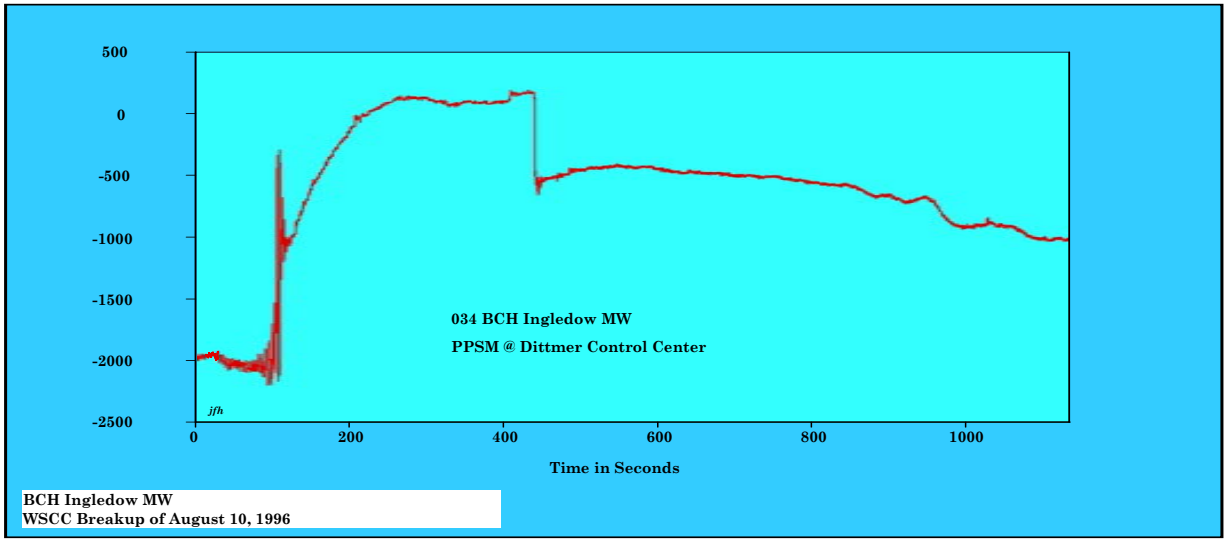
Malin-Round Mountain #1 MW
WSCC Breakup of August 10, 1996



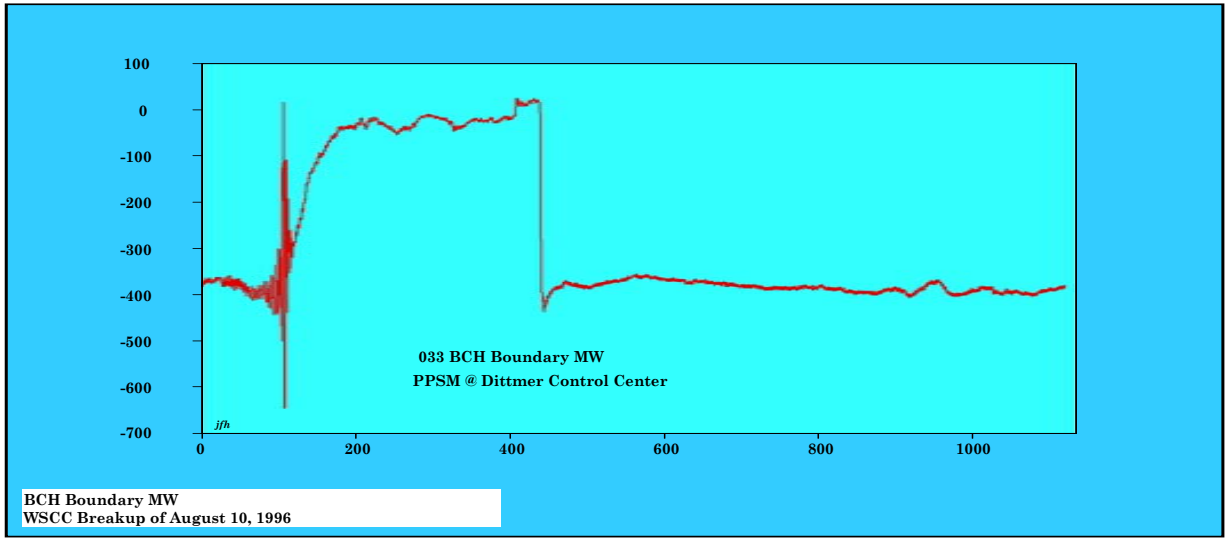
Malin-Round Mountain #1 MVAR
WSCC Breakup of August 10, 1996

Source: DOE/EPRI WAMS project

Disturbance records for WSCC breakup of August 10, 1996



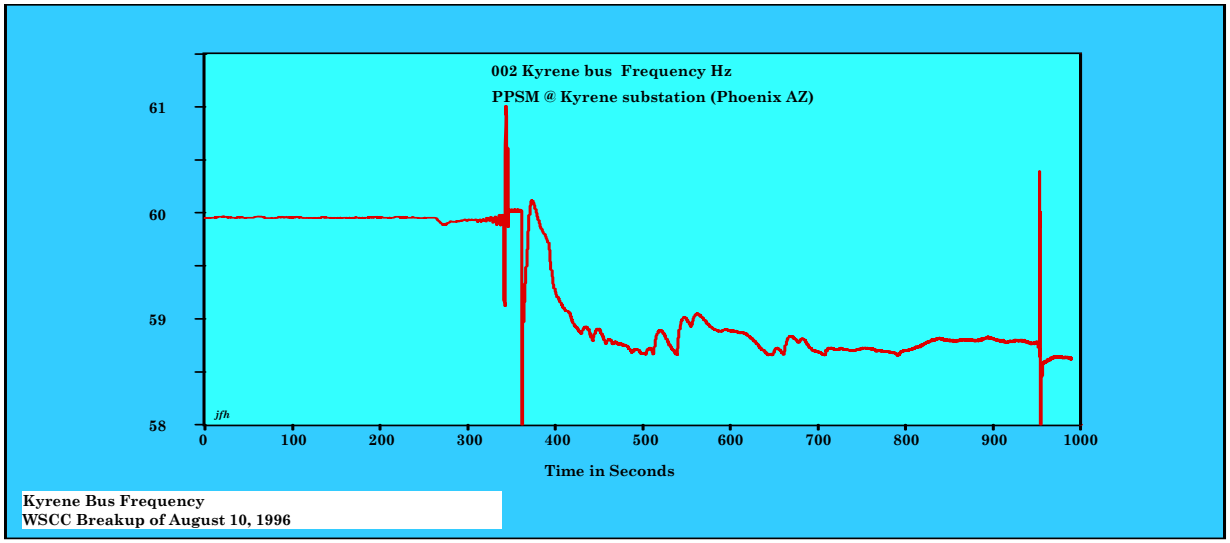
BCH Ingledow MW
WSCC Breakup of August 10, 1996



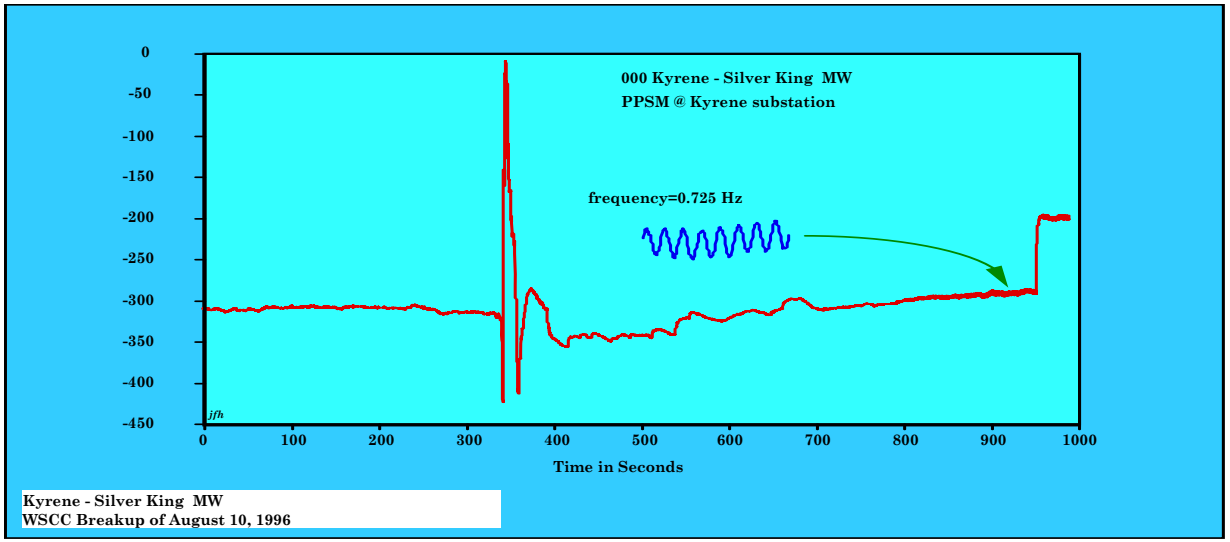
BCH Boundary MW
WSCC Breakup of August 10, 1996

Source: DOE/EPRI WAMS project

Disturbance records for WSCC breakup of August 10, 1996



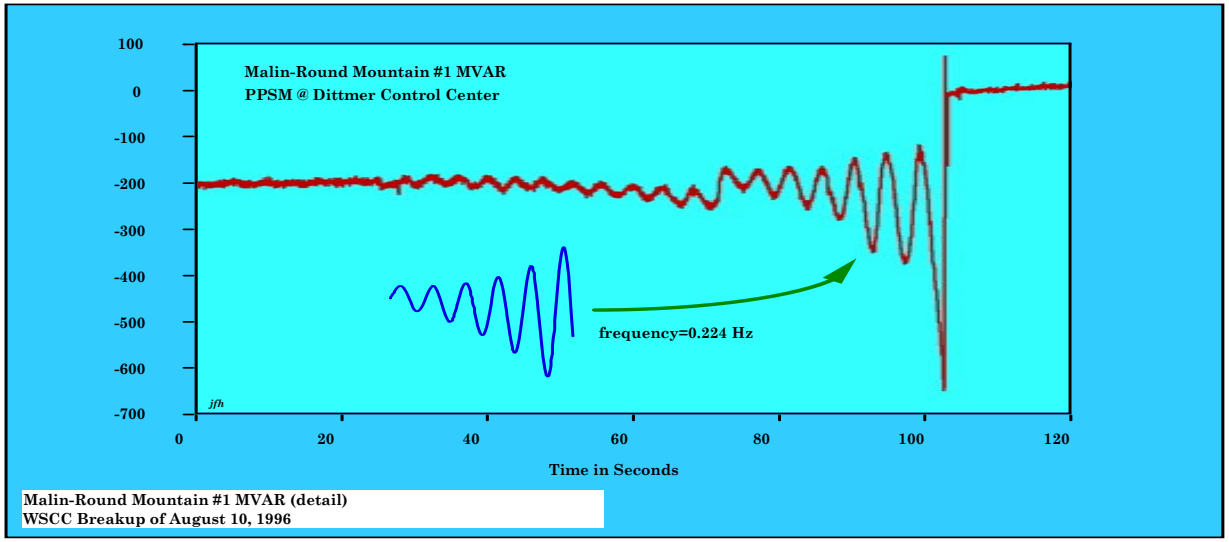
Kyrene Bus Frequency
WSCC Breakup of August 10, 1996



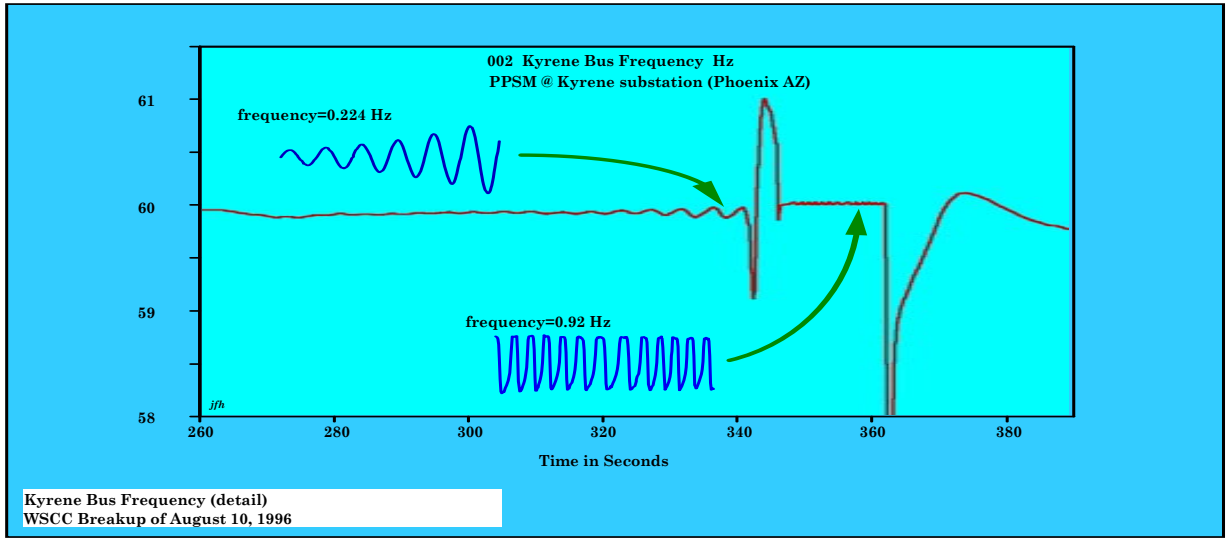
Kyrene - Silver King MW
WSCC Breakup of August 10, 1996

Source: DOE/EPRI WAMS project

Disturbance records for WSCC breakup of August 10, 1996



Malin-Round Mountain #1 MVAR (detail)
WSCC Breakup of August 10, 1996



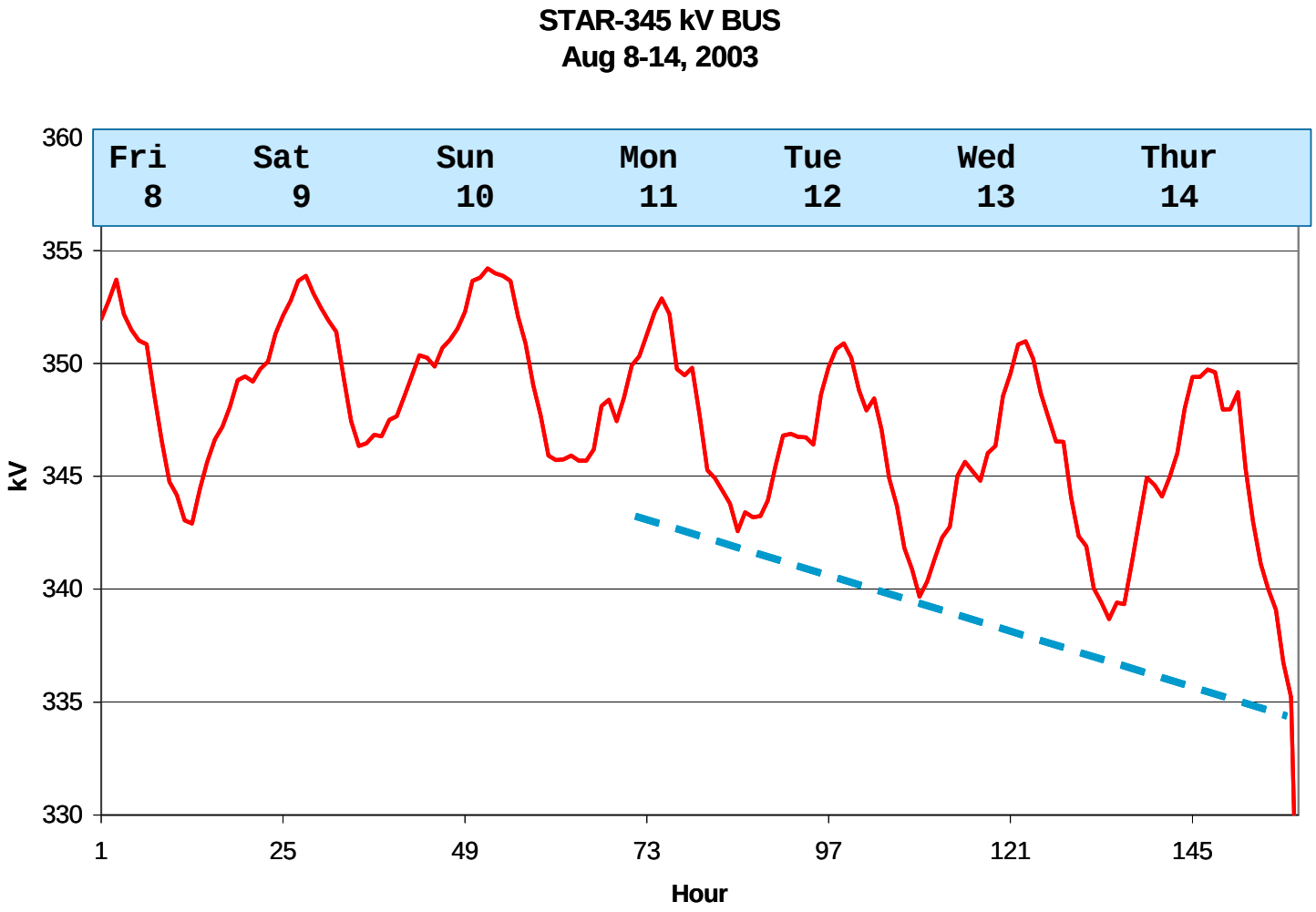
Kyrene Bus Frequency (detail)
WSCC Breakup of August 10, 1996

Technological Leadership Institute

UNIVERSITY OF MINNESOTA
Driven to Discover℠

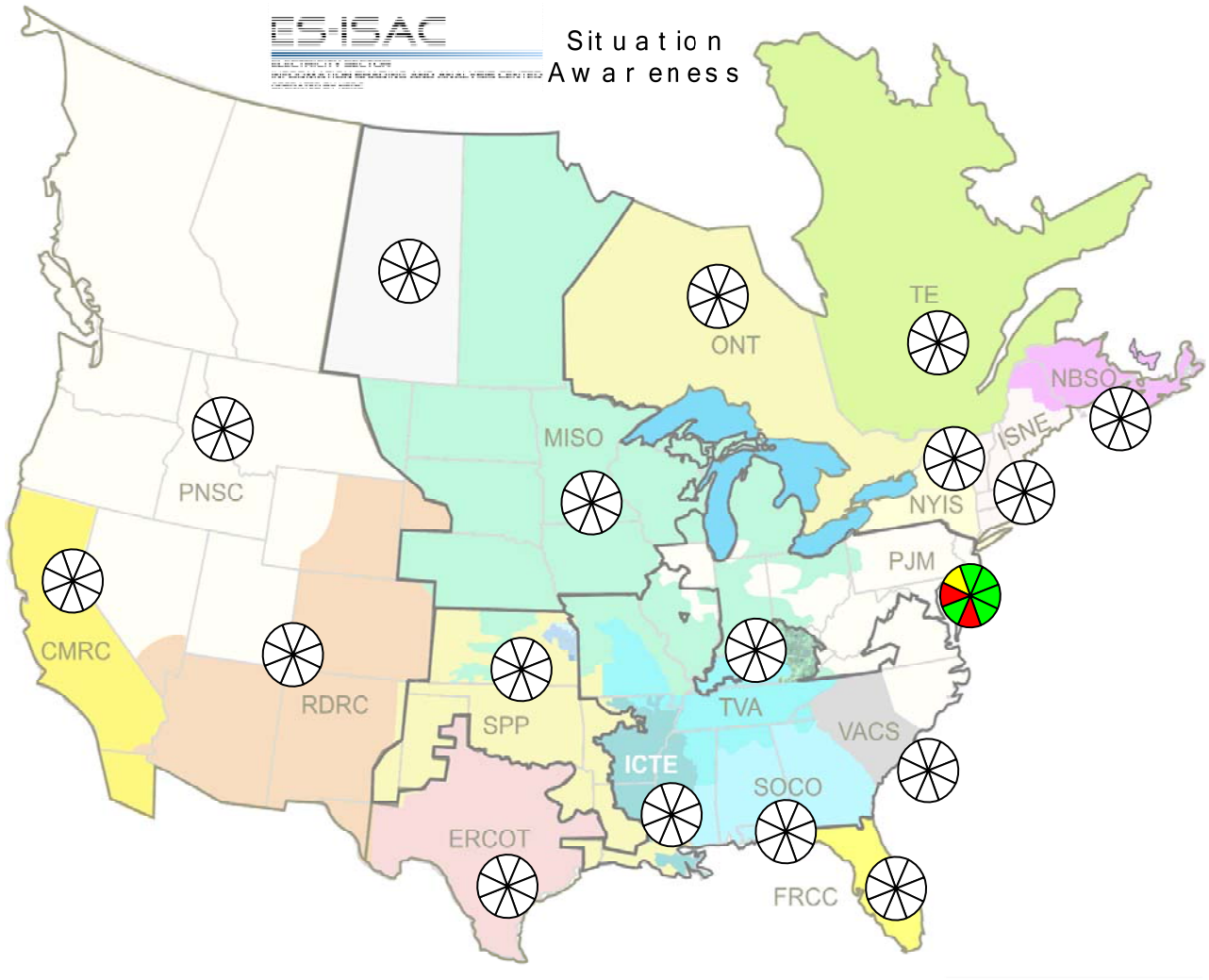
Source: DOE/EPRI WAMS project

Initial Conditions on August 14, 2003



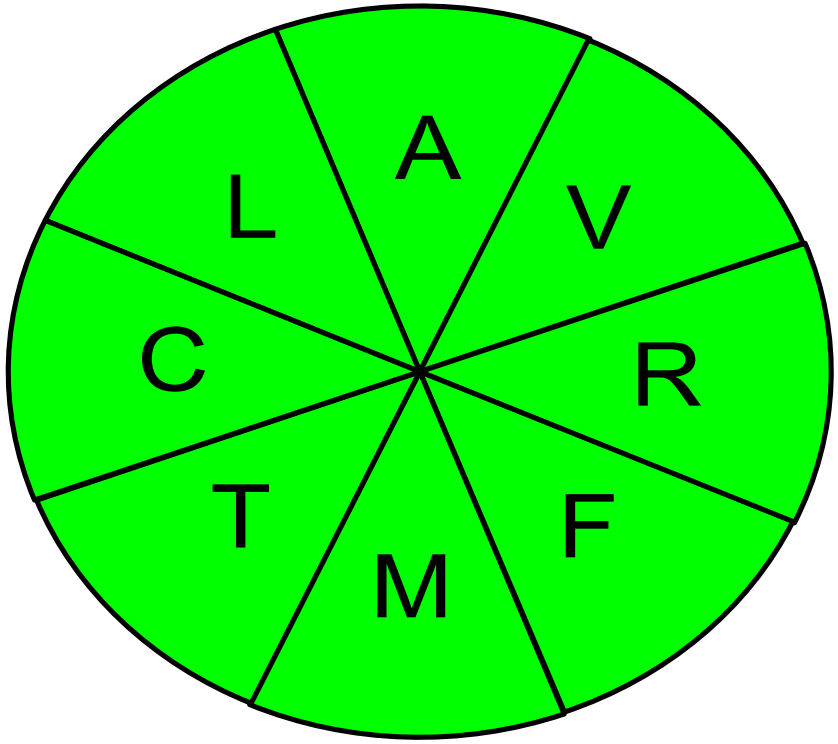
Star 345 kV Bus Voltages (Aug 8-14, 2003)

Situation Awareness Tool (SAT)



Source: NERC

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

Source: NERC

"Computers are incredibly fast, accurate, and stupid; humans are incredibly slow, inaccurate and brilliant; together they are powerful beyond imagination."

Albert Einstein

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

Terry Ward

Heidi Hamilton

Val Svensson

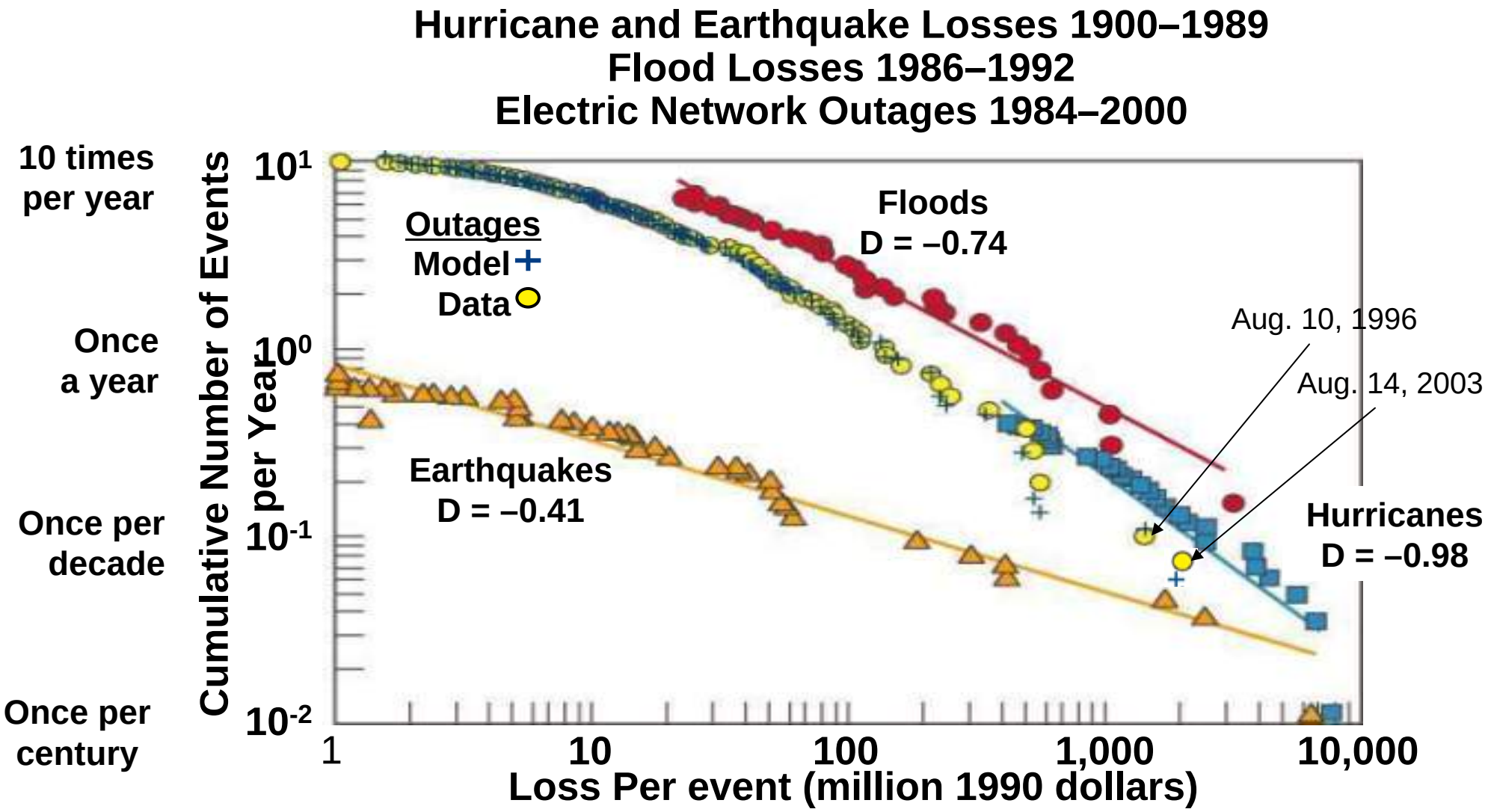
Joe Nietfeld

Technological Leadership Institute

UNIVERSITY OF MINNESOTA
Driven to Discover℠

Electric Power Grid Vulnerabilities and Security

Power Law Distributions: Frequency & impacts of major disasters



Power Grid Vulnerabilities

- Physical:
  - Over 215,000 miles of 230kV 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

Context: IT interdependencies and impact

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.

Context: The Role of Digital Control Systems in the Electric Power Industry

- Supervisory Control & Data Acquisition (SCADA) Systems & Energy Management Systems (EMS) control the power flow from generators to end users
- Distributed Control Systems (DCSs) are used to control the operation of generating plants
- Intelligent Electrical Devices (IEDs) & Programmable Logic Controllers (PLCs) are being extensively used in substations and power plants

Today, digital control systems are essential to the reliable operation of the electricity infrastructure

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)

Context: Threats to Security

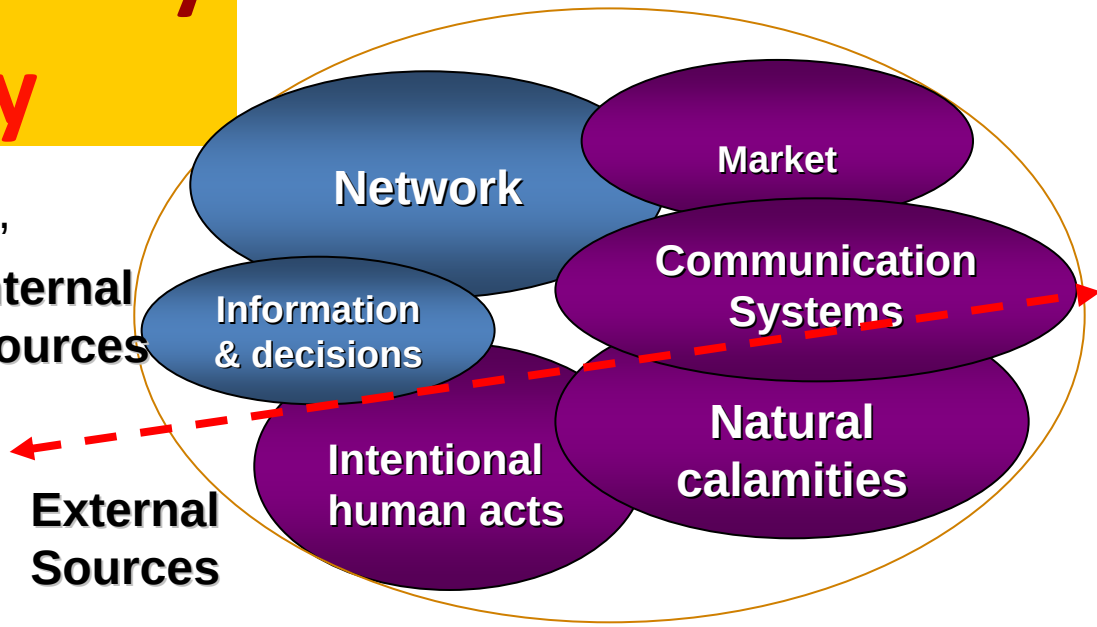
Sources of Vulnerability

- 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 … "

Historical Analysis of U.S. outages (1991-2005)

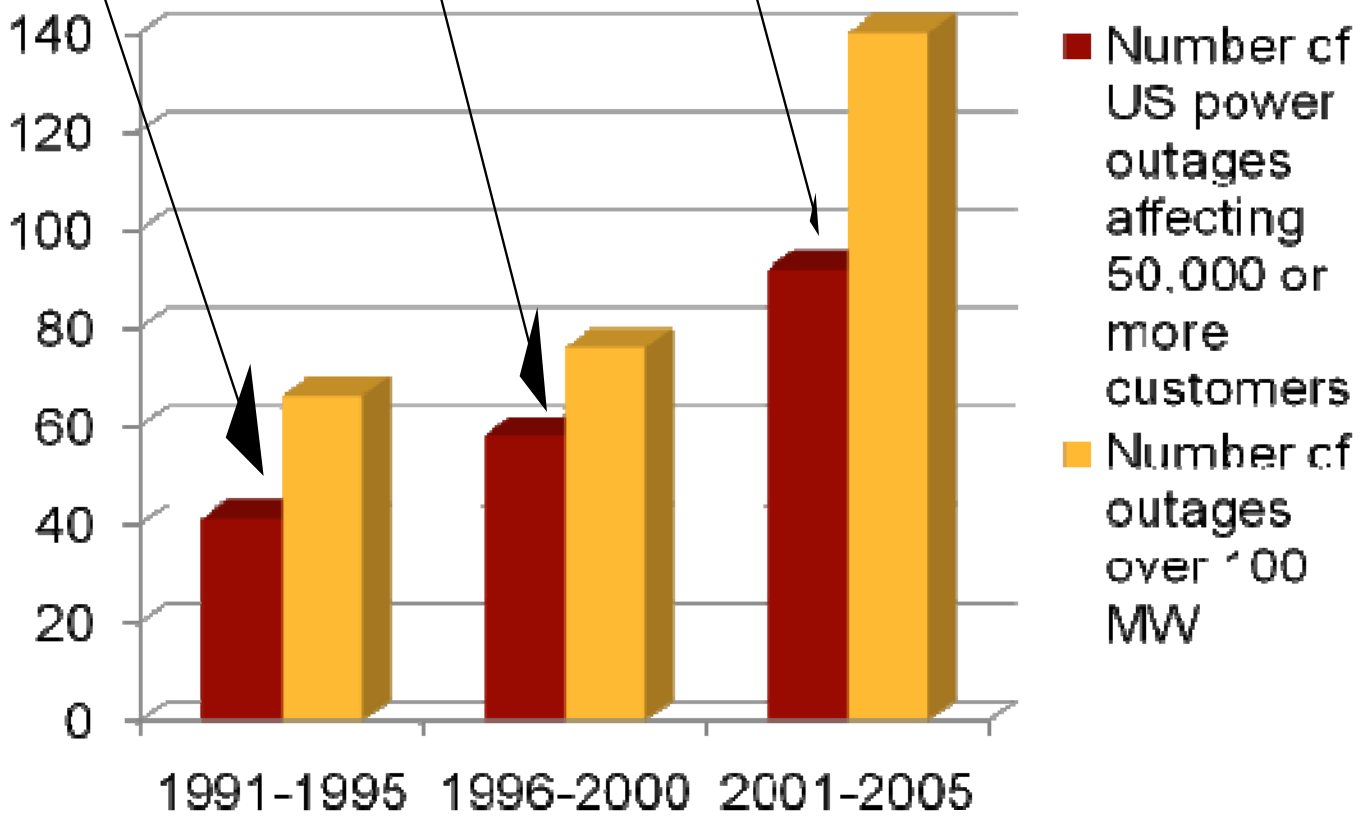
66 Occurrences over 100 MW
41 Occurrences over 50,000* Consumers

76 Occurrences over 100 MW
58 Occurrences over 50,000* Consumers

140 Occurrences over 100 MW
92 Occurrences over 50,000* Consumers

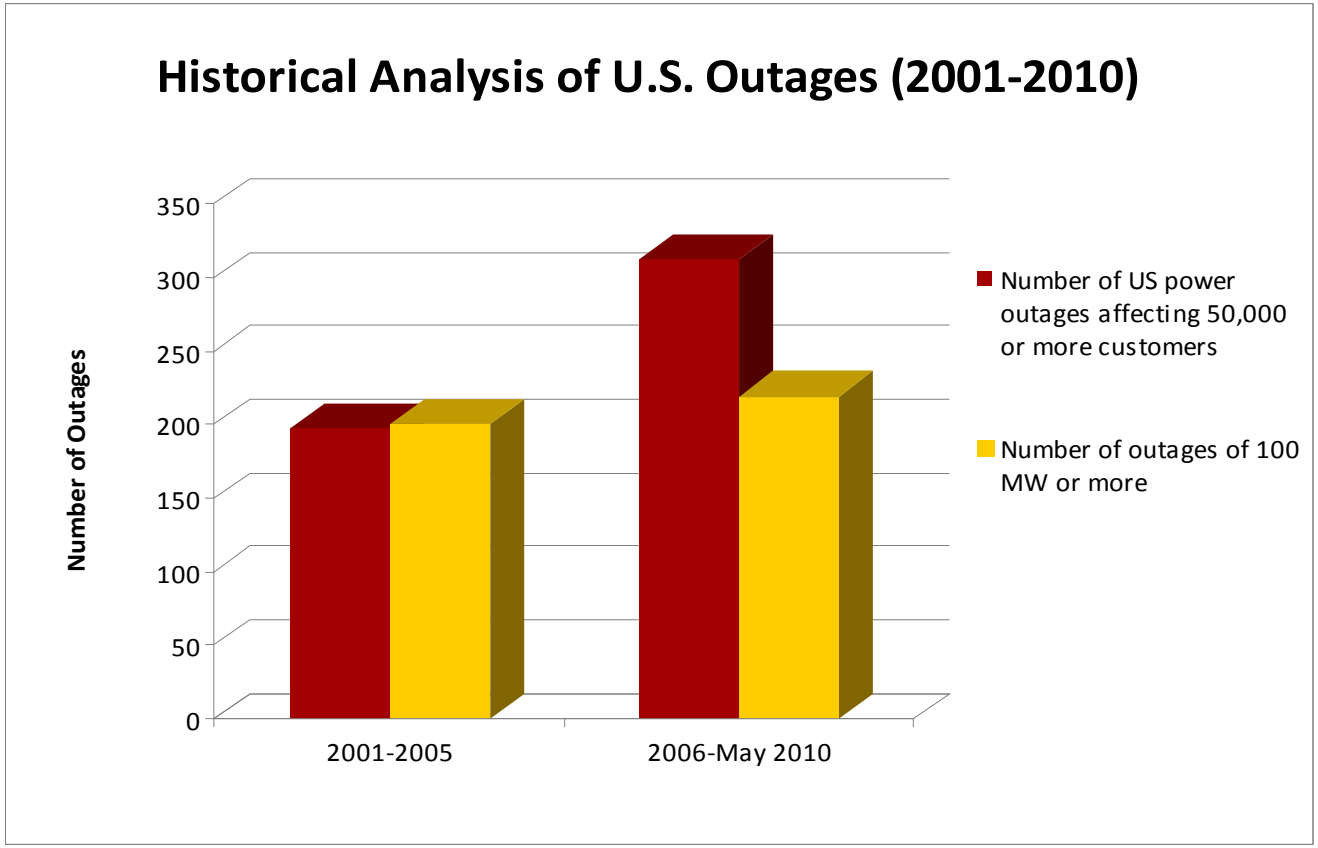
Result: Large blackouts are growing in number and severity.

*Trend persists, e.g. 2006 outages:
24 Occurrences over 100 MW
34 Occurrences over 50,000* or more Consumers
Data courtesy of NERC's Disturbance Analysis Working Group database



*Note: Annual increase in load (about 2%/year) and corresponding increase in consumers should be taken into account.

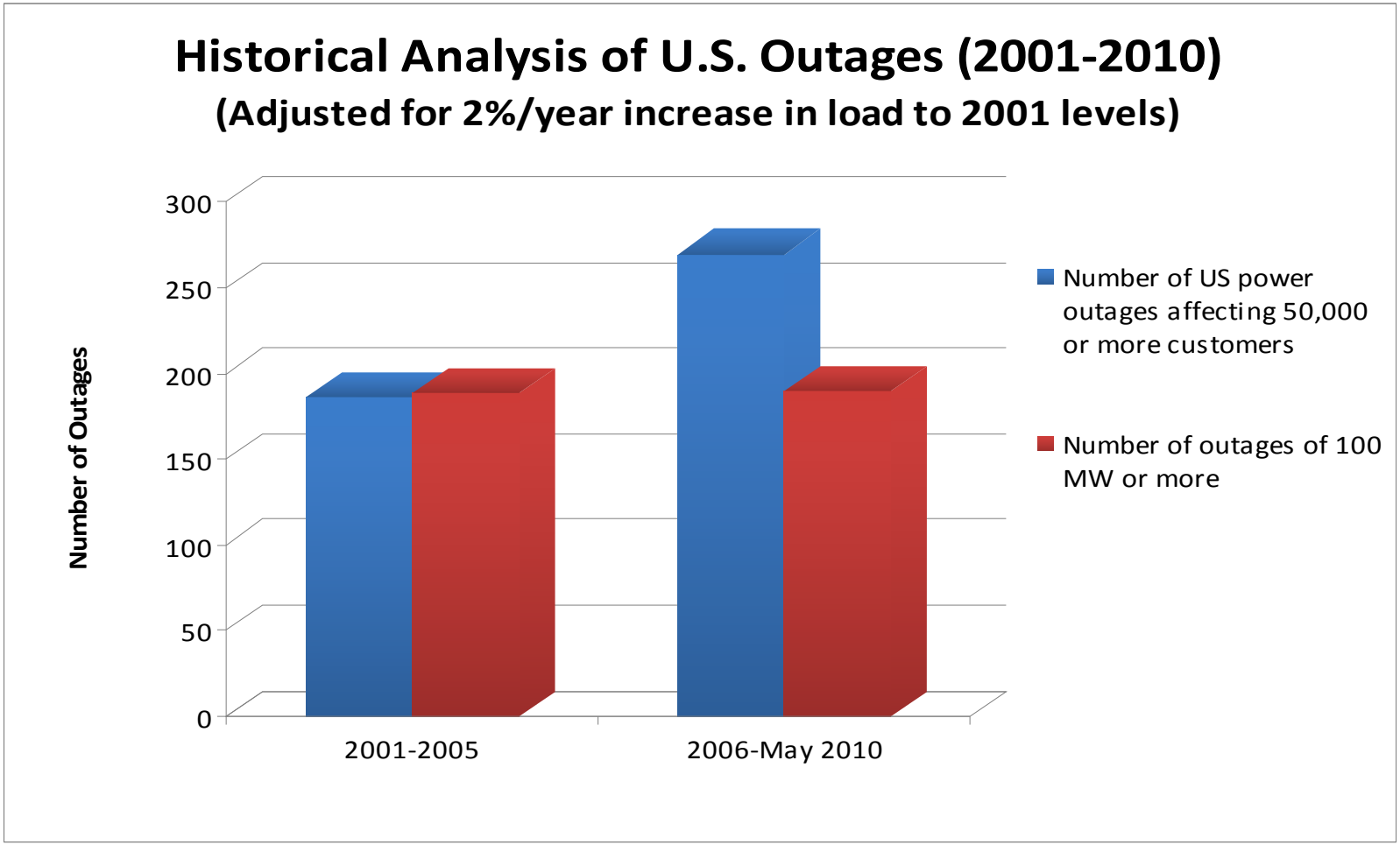
U.S. Electric Power Outages over 100MW and affecting over 50,000 Consumers (2001- May2010)



U.S. power outages during 2001- May 2010 (EIA data):

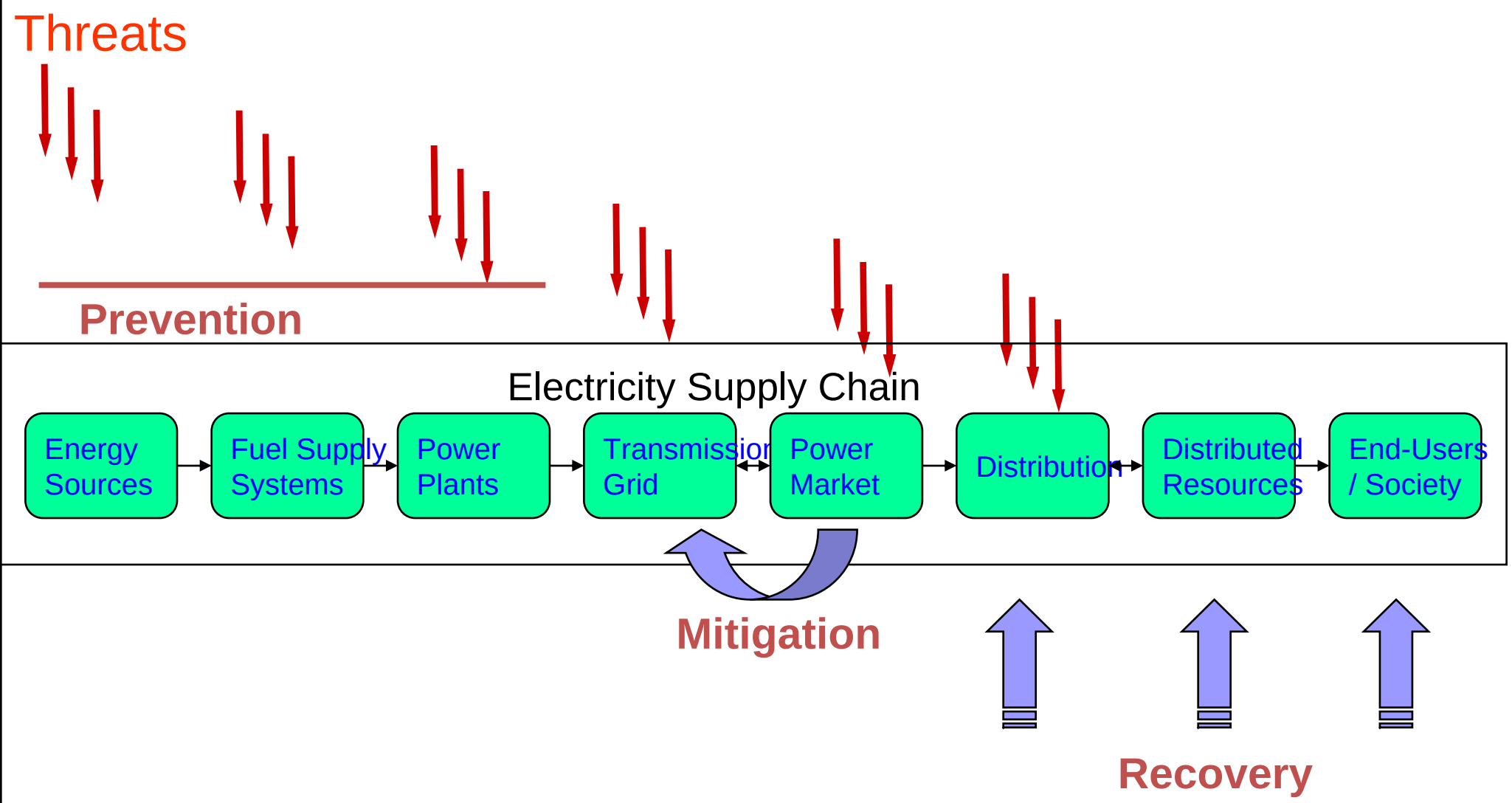
- 200 outages of 100 MW or more during 2001-2005, increased to 219 during 2006-May 2010.
- The number of outages affecting 50,000 or more consumers, increased from 197 (during 2001-2005) to 312 (during 2006-May 2010).

U.S. Electric Power Outages over 100MW and affecting over 50,000 Consumers (2001- May 2010), adj. 2% load increase/year



- 189 outages of 100 MW or more during 2001-2005, slightly increased to 190 during 2006-May 2010.
- Number of U.S. power outages affecting 50,000 or more consumers increased from 186 (during 2001-2005) to 297 (during 2006-May 2010).

End-to-End PVA Model

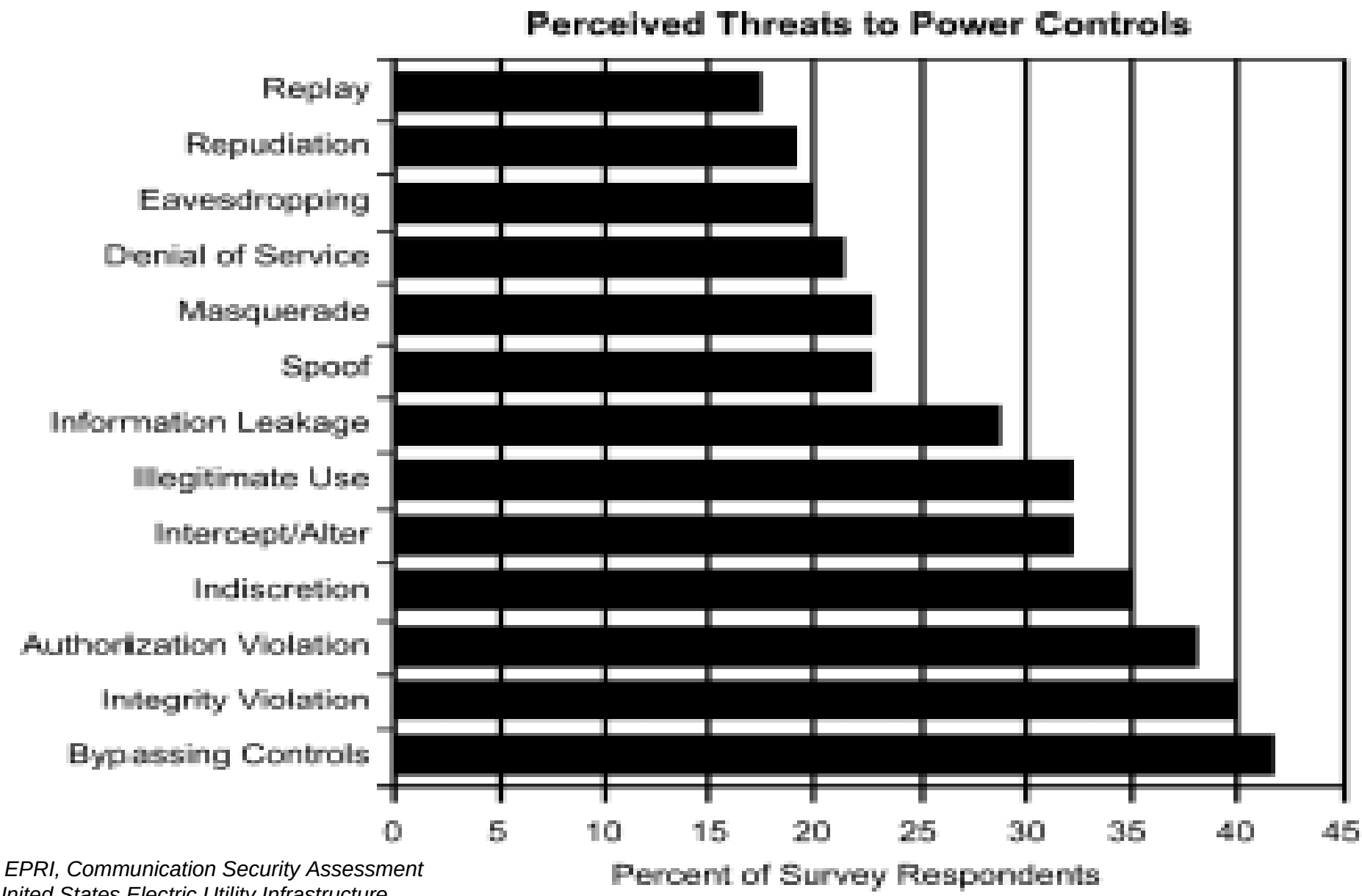


Electric Company Vulnerability Assessment

- 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.

Cyber Threats to Controls



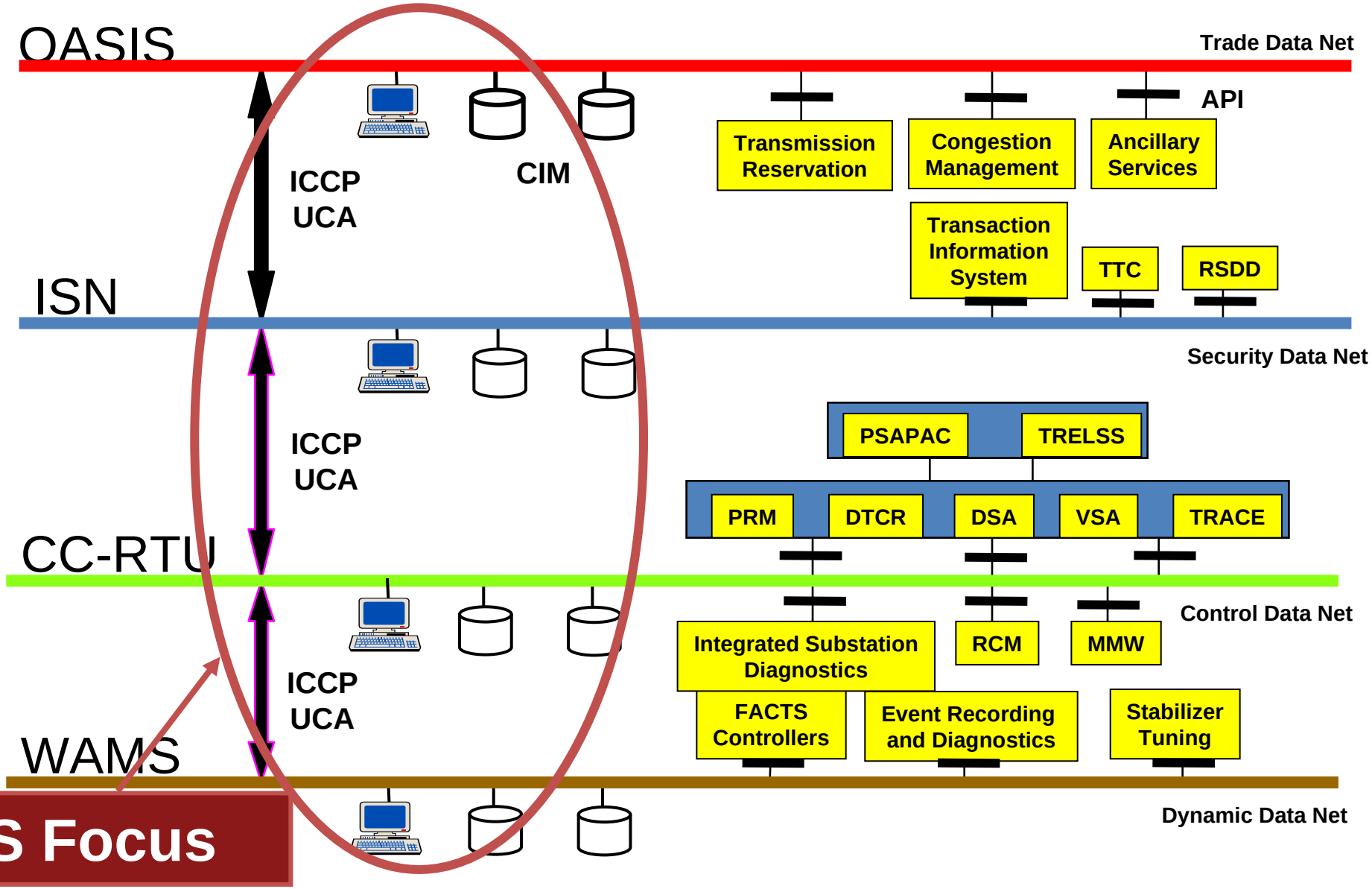
Source: *EPRI, Communication Security Assessment for the United States Electric Utility Infrastructure,* EPRI, Palo Alto, CA: 2000. 1001174.

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?"

Enterprise Information Security (EIS) program

Information Networks for On-Line Trade, Security & Control



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)

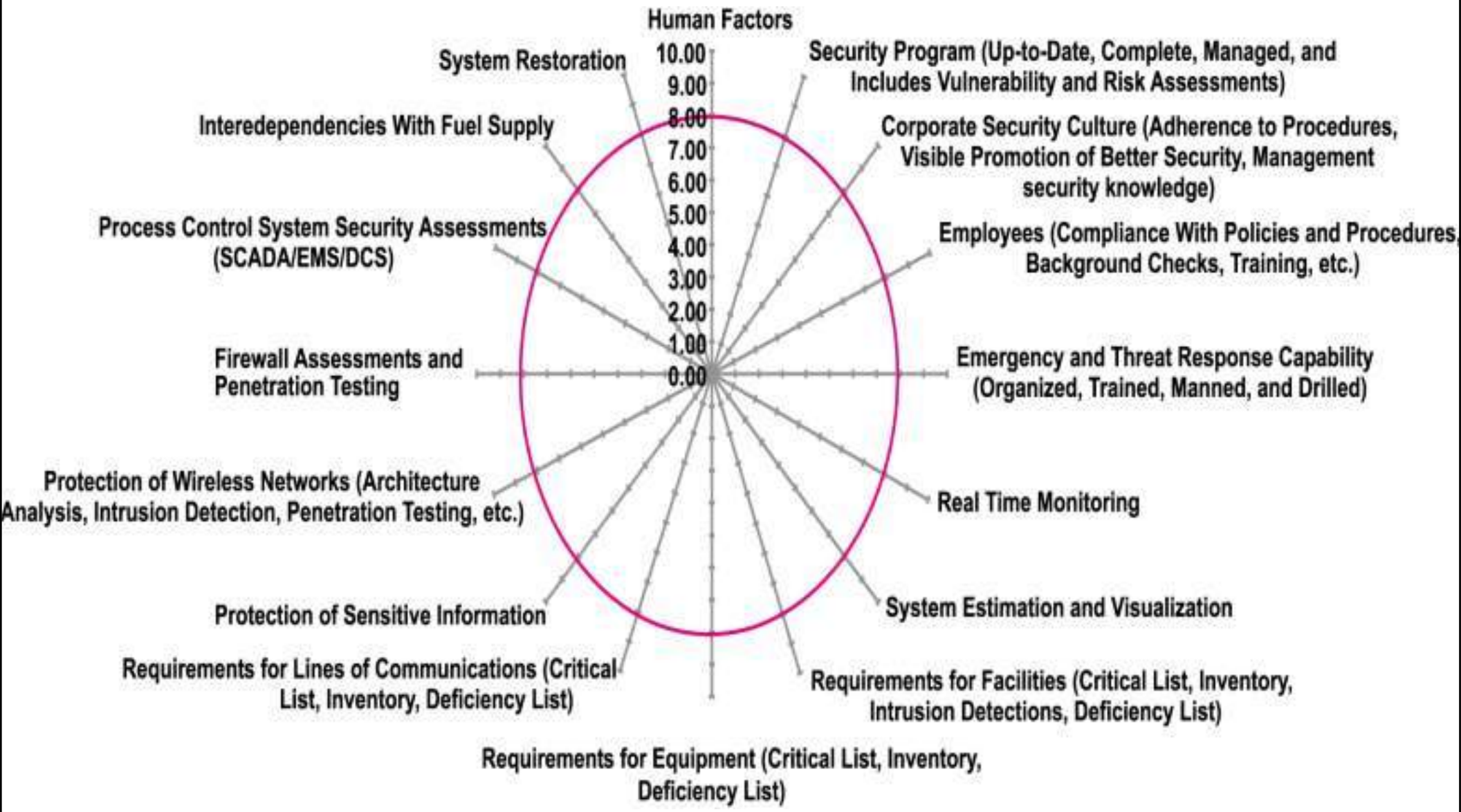
Physical

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

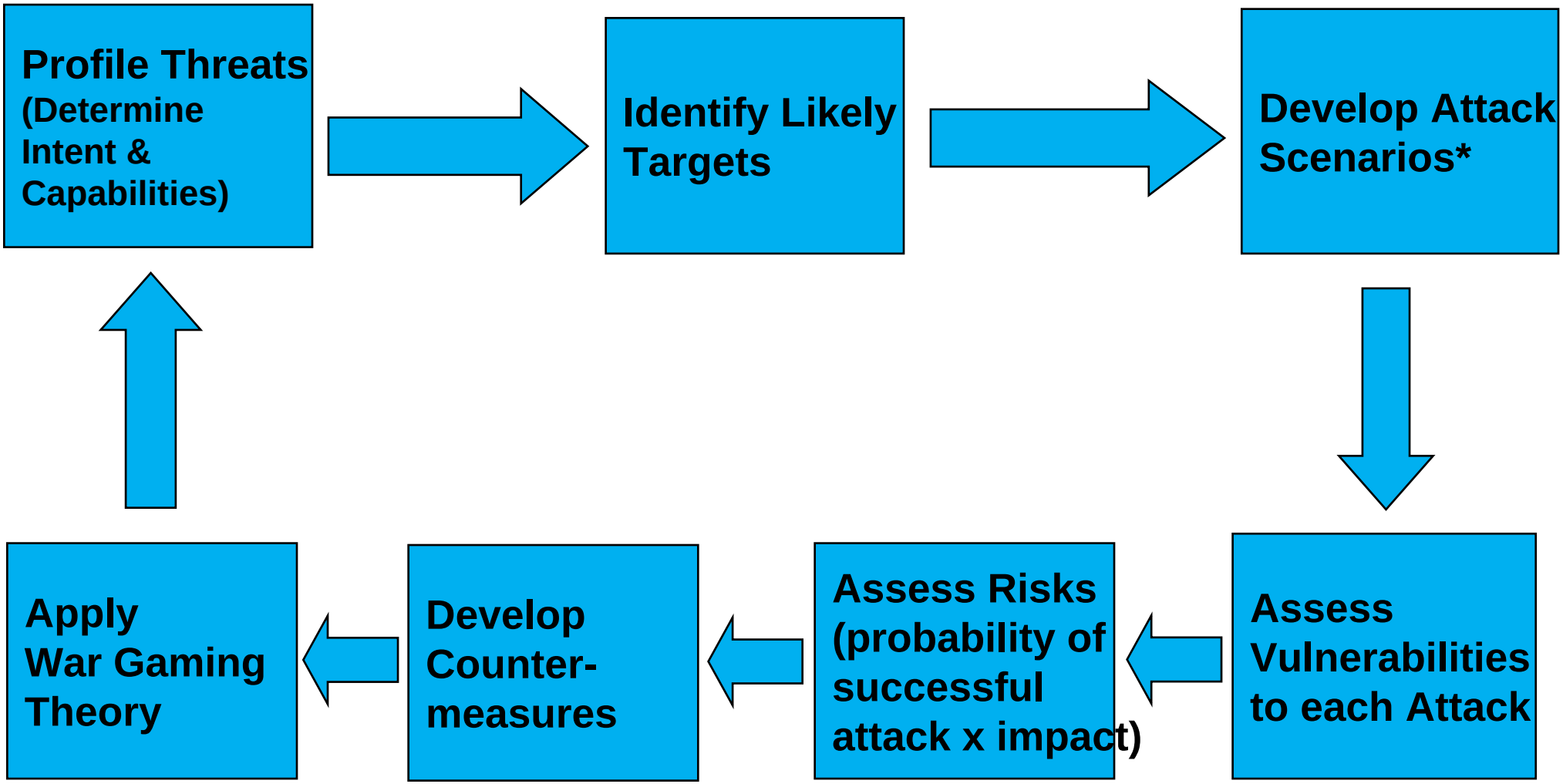
1. Protection of wired networks (architecture analysis, intrusion detection)
2. Protection of wireless networks (architecture analysis, intrusion detection, penetration testing)
3. Firewall assessments
4. Process control system security assessments (SCADA, EMS, DCS)

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



What can be Done?

Vulnerability Assessment and Layered Defense in Depth



*Evolving spectra of targets and modes of attack

Smart Grid Security

Smart Grid Vulnerabilities (cont.)

- 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

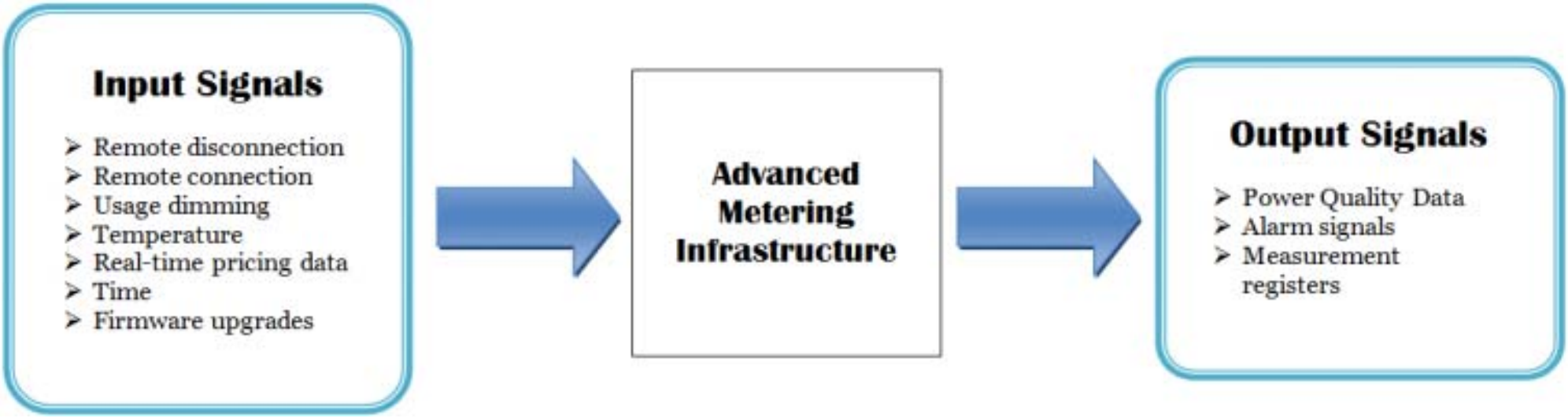
Focus on Distribution Systems

- Nearly 90% of all power outages and disturbances have their roots in the distribution network
- Of the $3.4 billion awarded by the American Recovery and Reinvestment Act (ARRA) Smart Grid Investment Grants (SGIGs) (October 2009) only $148 million went to transmission related projects
- Other countries are taking different approaches

Advanced Metering Infrastructure (AMI)

- Provide two-way communication
- Italy, The Netherlands, Denmark, Sweden, and the United States have already installed automated meter reading (AMR) systems
- Provide numerous capabilities

AMI Input and Output Signals



AMI Vulnerabilities

- Very little work done to identify the security needs for such devices
- Extremely attractive targets for exploitation since vulnerabilities can be easily monetized
- Privacy concerns due to the immense amount of energy use information stored at the meter

Current Grid Control Architecture

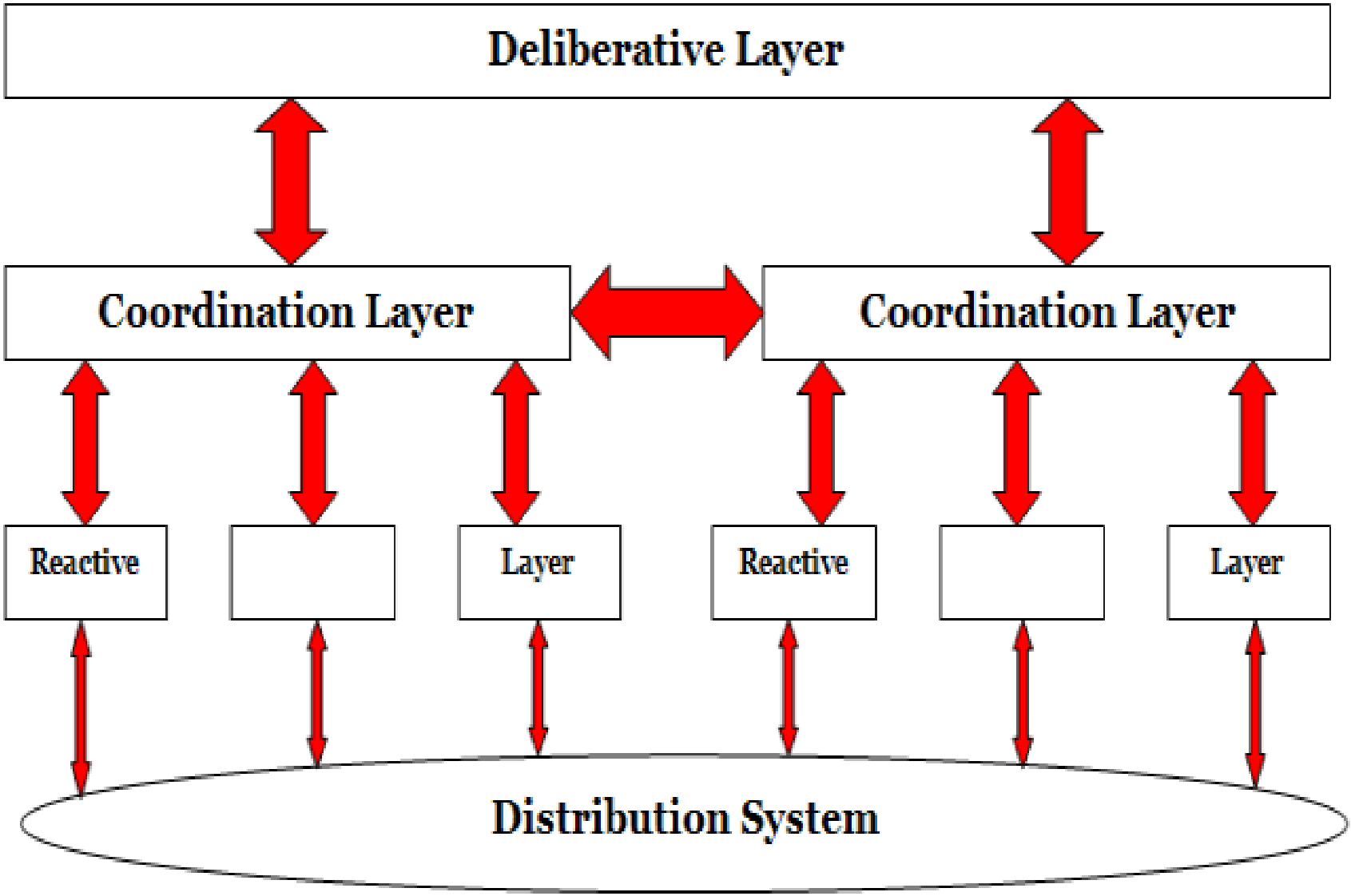
Five premises:

1. Components are predominantly dumb conductors and are not controllable
2. If they are controllable, they cannot react quickly enough
3. No energy storage; an interruption on the grid means an interruption of service
4. Customer demands are not controllable, and the grid can only react passively to changes in demand with centralized control
5. Grid can only react to changes in demand by continuously balancing the output of the central power plants in order to remain in a dynamic equilibrium.

DAS Control

- Centralized vs. Decentralized:
  - Centralized control, all computing and control functions are based in one centralized location
    - Easier to implement but is unable to respond quickly to adverse events
  - Decentralized control, computing and control functions may be dispersed in many different locations
    - Able to respond quicker to adverse events, but the lack of information exchange may lead to unreliable or biased decision making

Intelligent Distributed Secure Distribution System Control Architecture



(Several Seconds to Minutes)

Event Reports and Decisions

(Seconds)

Event Reports and Control Coordination

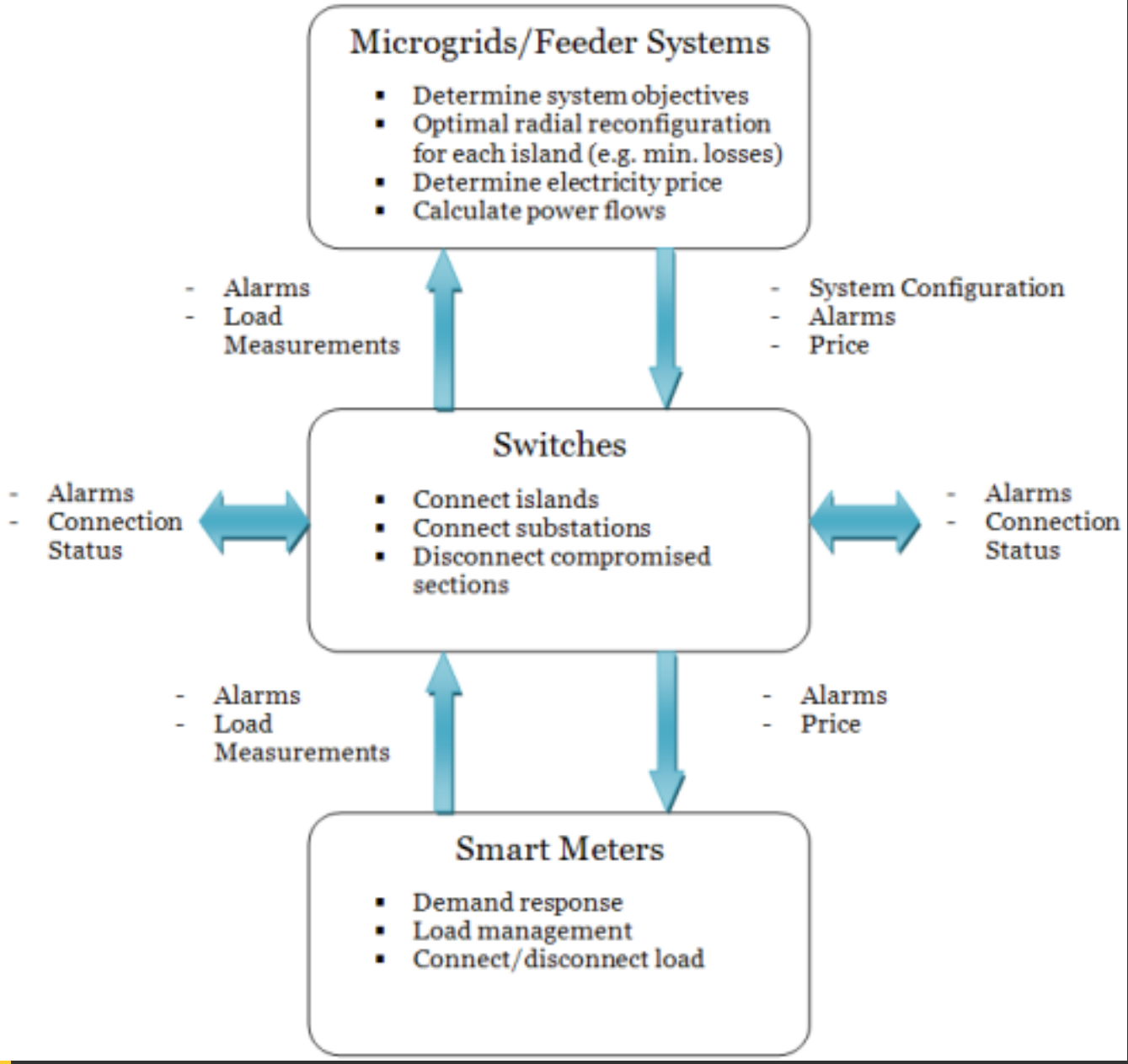
(Milliseconds)

Monitoring and Control Signals

Intelligent Agents and Functionalities

Layer	Agent Locations	Control Functions
Reactive	-Smart Meters -Substations	- Demand response - Load management - Connect/disconnect load - Send alarm signals
Coordination	-Switches	- Connect islands - Connect substations - Disconnect compromised sections - Send alarm signals
Deliberative	-Microgrids/Feeder Systems	- Determine system objectives - Optimal radial reconfiguration for each island (e.g. min. losses) - Determine electricity price - Calculate power flows - Send alarm signals

Distribution System Intelligent Agent Control Functions and Signals



Need for a Layered Security and Defense for Smart Grids: Security Enforcement at Multiple Points

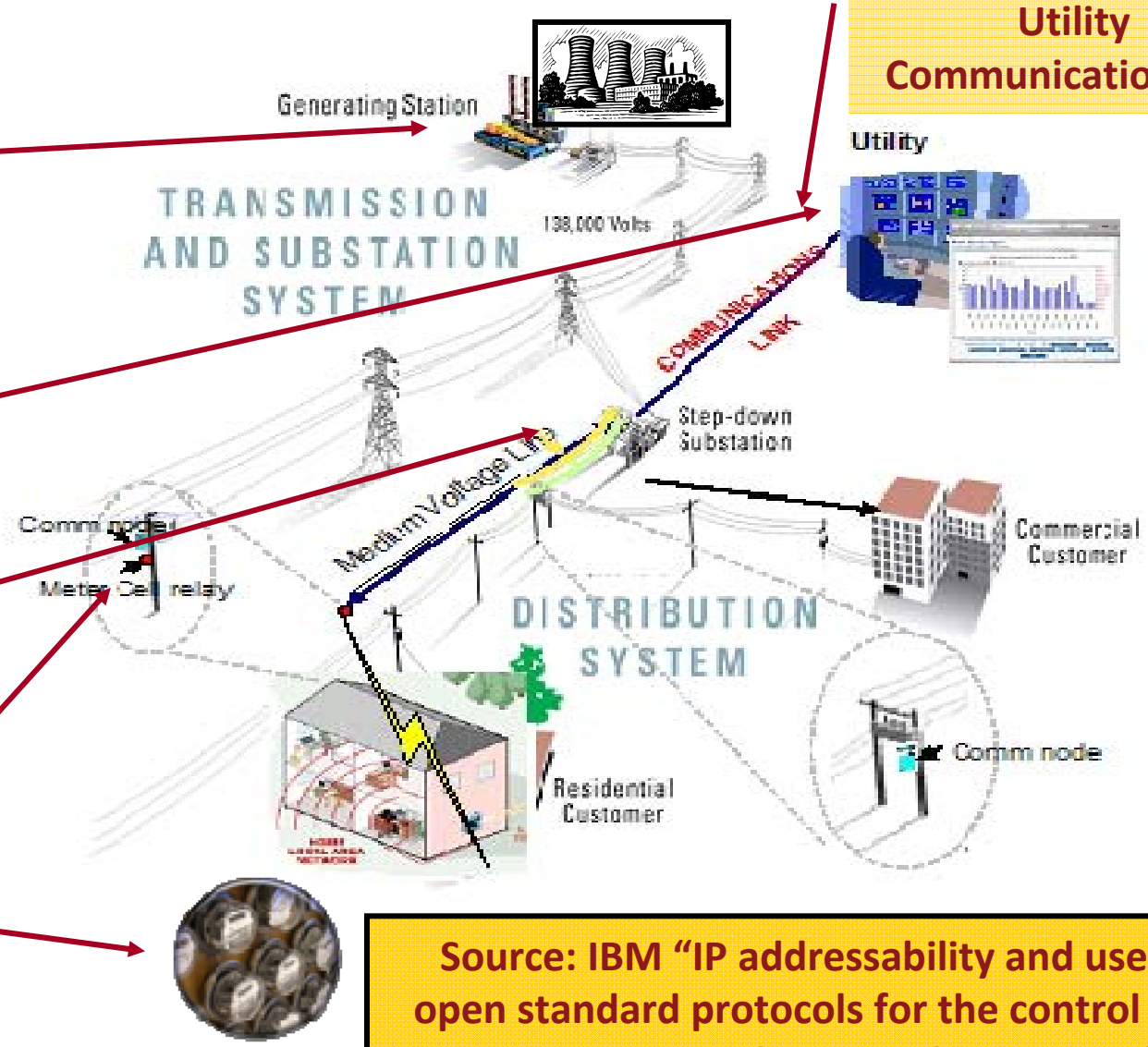
SCADA network systems

Advanced metering data management system

Substation Remote Monitoring equipment

Meter Communication (Meter to Cell Relay)

Utility Communication Link



Source: IBM "IP addressability and use of open standard protocols for the control grid necessitates it to be securely protected at multiple points"

Research Areas

Research Challenges

Sensing/Measurement → Analysis/Visualization → Automation/Self-healing Systems

- **Complex Dynamical Systems: Systems Science and Applied Mathematics**
  - **Modeling:** Idealized models, consisting of static graph-theoretic models, and interactive dynamic models, such as interconnected differential-algebraic systems; Hybrid Models.
  - **Robust Control:** Design of self-healing systems requires the extension of the theory of robust control in several ways beyond its present focus on the relatively narrow problem of feedback control.
  - **Complex Systems:** Theoretical underpinnings of complex interactive systems.
  - **Dynamic Interaction in Interdependent Layered Networks:** Characterization of uncertainty in large distributed networks: Multi-resolutional techniques where various levels of aggregation can co-exist.
  - **Disturbance Propagation in Networks:** Prediction and detection of the onset of failures both in local and global network levels.
  - **Forecasting, Handling Uncertainty and Risk:** Characterizing Uncertainties and Managing Risk**;** Hierarchical and multi-resolutional modeling and identification; Stochastic analysis of network performance; Handling Rare Events.
- **Mathematical/Theoretical Foundation is Fragmented:** Computational complexity, information theory, dynamical systems and control science… need for a new science of interdependent complex networks and infrastructure security.

Strategic R&D Challenges

Sensing/Measurement → Analysis/Visualization → Automation/Self-healing Systems

- **Planning: Develop a theoretical framework, modeling and simulation tools for infrastructure couplings and fundamental characteristics, to provide:**
  - An understanding of true dynamics and impact on infrastructure reliability, robustness and resilience
  - Real-time state estimation and visualization of infrastructures-- flexible and rapidly adaptable modeling and estimation
  - An understanding of emergent behaviors, and analysis of multi-scale and complexity issues and trends in the future growth and operations.

- **Security: Integrated systems assessment, monitoring, and early warning:**
  - Vulnerability assessment, risk analysis and management
  - Underlying causes, distributions, and dynamics of and necessary/sufficient conditions for cascading breakdowns (metrics)
  - Impact: "if you measure it you manage it, if you price it you manage it even better"
  - Infrastructure databases, data mining and early signature detection

Strategic R&D Challenges

Sensing/Measurement → Analysis/Visualization → Automation/Self-healing Systems

- Management of Precursors and their Signatures
- Fast look-ahead simulation and modeling capability
- Adaptive and Emergency Control and Rapid Restoration
- Impact of all pertinent dynamic interactive layers including:
  - Fuel supply (Oil & Gas), Information, Communication and Protection layers
  - Electricity Markets and Policy/Regulatory layers
  - Ownership and investor layer (investment signals)
  - Customers layer (demand response, smart meters, reliability/quality)
  - …

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)

Sensors

- Phasor measurement units (PMUs) providing time-stamped magnitude and phase of fundamental voltage/current, frequency, harmonics, …
- Other sensors (temperature, sag)? e.g. to monitor key components and permit dynamic rating (transient overloads)
- New sensors?
- “Sensors” for market data

Issues and Problems in Wide-Area Sensing

- What mix of sensors?
- Where to deploy them?
- Economic and performance justifications
- Communication
- Data management

Communication & Data Management

- Flexible and robust communication architectures (wireless to optical backbone? wireline schemes?), protocols
- Dealing with latency, variable time delay
- Data management, calibration & validation (bad or missing or malicious data), sharing and distribution, archiving, hierarchical aggregation
- Dynamic, distributed databases
- Appropriate computer network architectures

Improved State Estimation, Monitoring and Simulation

- Use sensed variables to improve quality and speed of state (and topology and parameter) estimation
- System-wide monitoring, disturbance signatures
- Situational awareness
- Post-disturbance analysis
- Dynamic determination of ATC
- Voltage instability prediction
- Use as corrective inputs to (near/faster than) real-time simulators (observers) for wide-area dynamics? --- multiresolution models.
- Impact on market transactions?

Improved Protection and Discrete-Event Control

- Use sensed variables as inputs to adaptive and coordinated (system-wide) protection, discrete-event (switched) control, islanding, restoration
- Coordinated relaying
- Feedforward (one-shot, event-driven) control (generator tripping, var compensation switching,…)
- Control of network topology
- Controlled load shedding, islanding, restoration

Wide-Area Control

- Working closer to margins
- “Fail-safe” control, defense in depth
- More effective use of controllers, backup controllers (1 PSS with distant inputs rather than 2 with local inputs, …)
- Bridging the gap between dynamic on-line security assessment and wide-area control
- Accounting for variable delays and uncertainty in feedback signals
- Intelligent substations
- Distributed control, distributed ownership of control, quantifying value of control

Enabling Technologies

Sensing/Measurement → Analysis/Visualization → Automation/Self-healing Systems

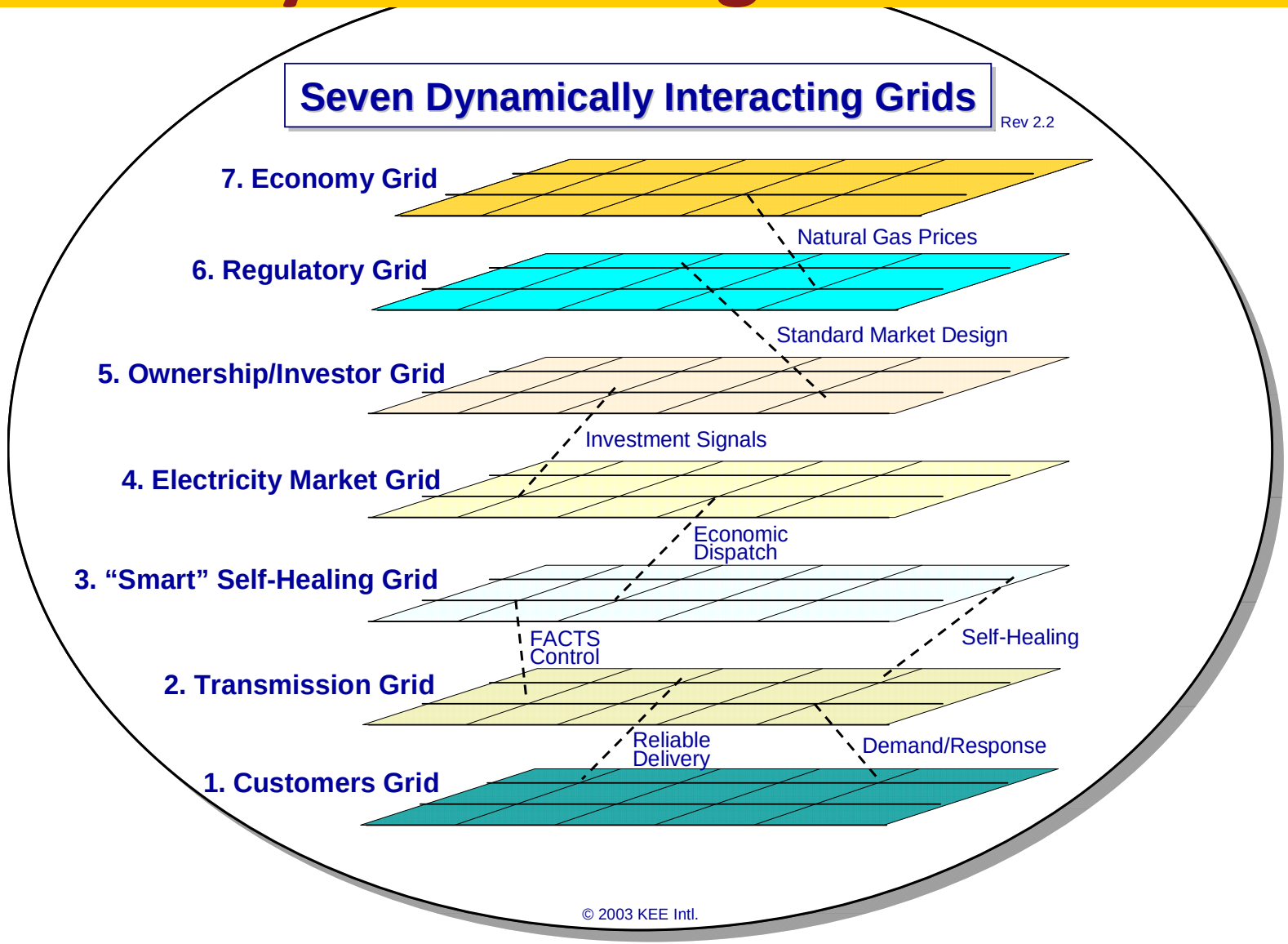
- **Sensing, Communication and Data Management**
  - Intelligent sensors as elements in real-time data base; seek appropriate high level query tools for such a database? sensor interface to multi-resolutional (micro to macro levels of details) models? Metrics?
  - Increased dependence on information systems and software Effect of market structures, distributed generation, other new features on above issues; economic evaluations
- **Monitoring and Analysis:** Seeing/understanding what is going on and dynamic risk assessment
- **Automation/Control:** Active-control of high-voltage devices… Ensuring system stability, reliability, robustness, security and efficiency in a competitive marketplace and carbon-constrained world
- **Materials science:** High-temperature superconducting cables, advanced silicon devices and wide-bandgap semiconductors for power electronics
- **Power Electronics** to enable integration of intermittent sources, connection to smart grid, and increased controllability
- **Maximize Utilization via Superconducting Cables**
  - 2 to 5 times the current; Can be used to retrofit existing ducts and pipes
  - Need to reduce cost, improve reliability of cryogenic system and gain more operating experience
- **Distributed Energy Resources (DER)** such as renewables, "microgrids," storage, solid oxide and other fuel cells, photovoltaics, superconducting magnetic energy storage (SMES), transportable battery energy storage systems (TBESS), etc. with integration and management of resources, and developing new business strategies for a deregulated energy markets

Enabling a Stronger and Smarter Grid

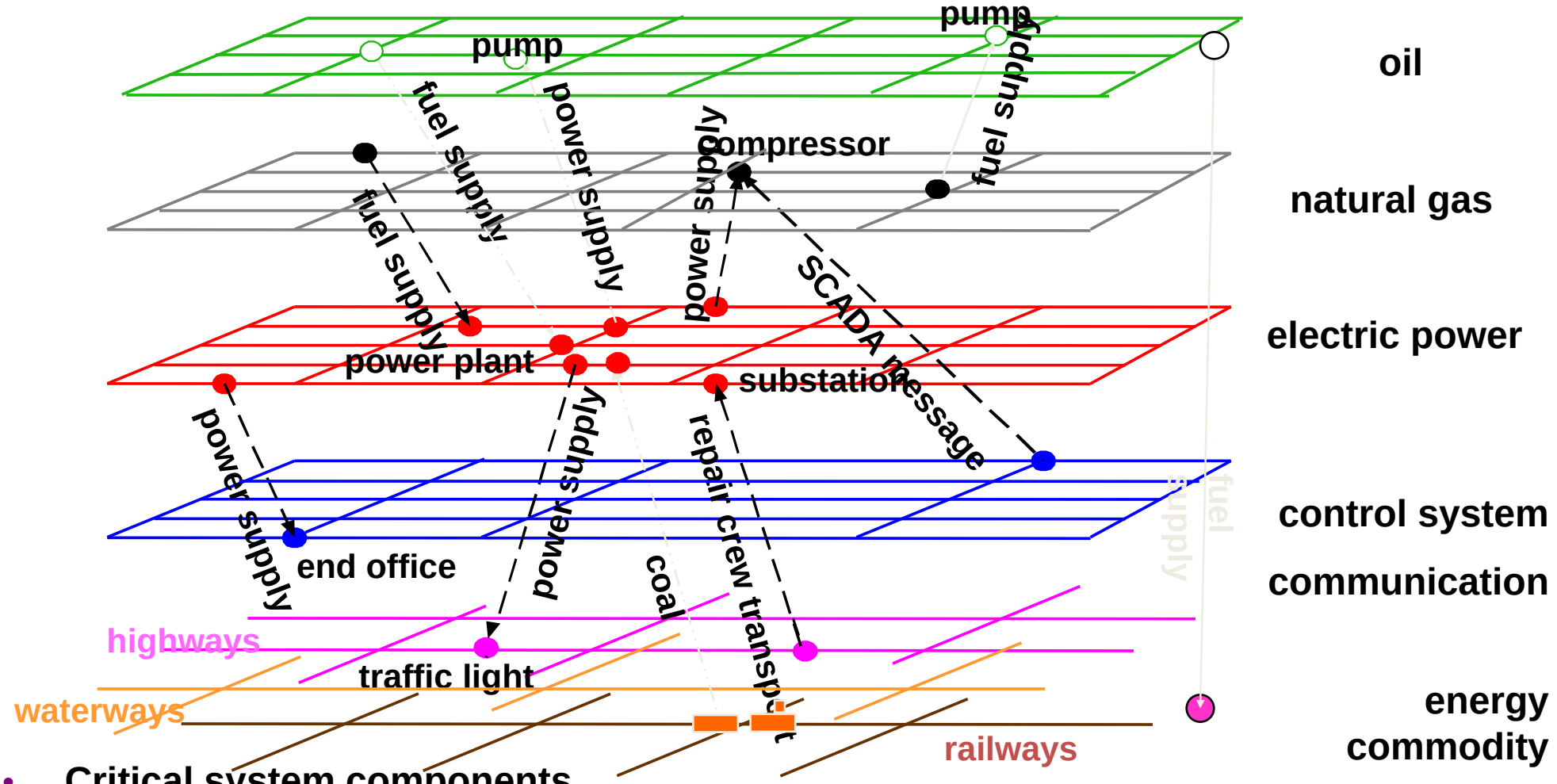
- **Smart Grid Challenges/Opportunities:**
  - Infrastructure for Generation/Transmission/Distribution Systems
  - Infrastructure for Smart Customer Interface
  - Distribution Automation
  - Smart metering improves load models and profiles
  - Distributed Sensing and Control
  - Device monitoring and self-healing diagnostics
  - Communication infrastructure provides opportunities for monitoring and diagnostics
  - Fault detection, sensor networks, etc. for smart grid
  - Alternative Smart Grid Architectures
  - Infrastructure Security: Controls, Communications and Cyber Security
  - Markets and Policy
  - Distributed generation and storage adds complexity

Modeling, Measuring/Sensing & Controlling Interdependent Complex Systems

Interdependencies: Dynamically Interacting Grids



Systems science, modeling and simulation: Infrastructure Interdependencies



- Critical system components
- Interdependent propagation pathways and degrees of coupling
- Benefits of mitigation plans

Source: SNL and ANL

Global Transition Dynamics

Globally Interlocked Dynamics:
Understanding the Full Impacts of Decision Pathways

- To unfold the full potential of social progress requires an integrated understanding of the many dimensions of social development, their underpinnings, and the role of science and technology.
- Goal: To target our constrained development resources to maximize benefit and minimize unintended consequences

Background: Sensing, modeling, simulation and control of complex systems in multi-hazard environments

EPRI: Jan. 1998 – February 2003

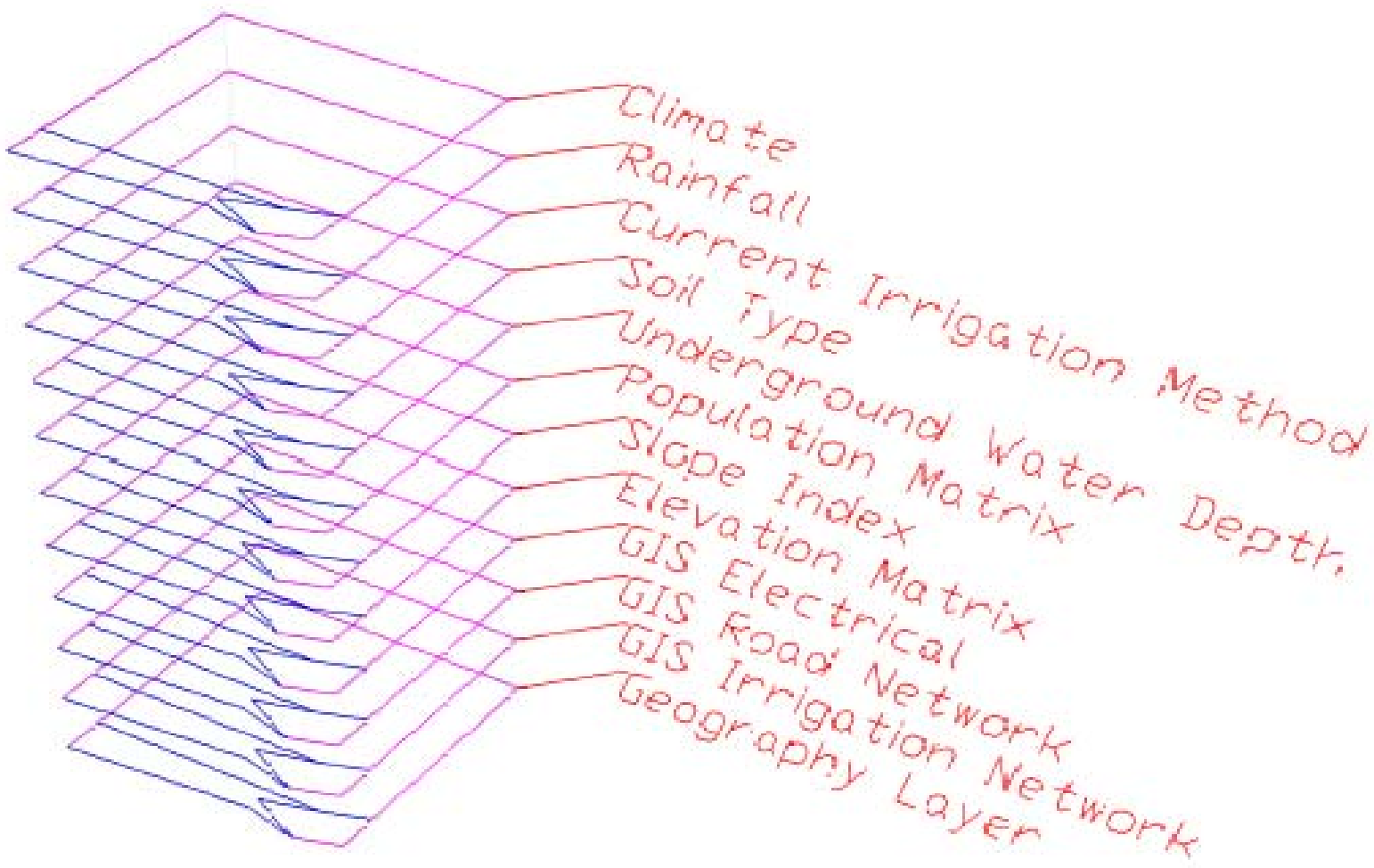
- EPRI/DoD Complex Interactive Networks Initiative: To address secure operations & management of our national critical infrastructures (1998-2001)
  - Systems-based R&D toward the smart self-healing electric power grid and the development of more than 24 advanced technologies to enhance the security of our national critical infrastructures.
  - Led strategic research in modeling, simulation, optimization, and adaptive control of national infrastructures for energy, telecommunication, transportation, and finance.
- Directed R&D in Infrastructure Security, Grid Operations and Planning, Risk and Policy Assessment and Energy Markets (Oct 2001-Feb 2003)

UofM: March 2003 – present

- Global Transition Dynamics to enhance resilience, security and efficiency of complex dynamic systems. These systems include national critical infrastructures for interdependent energy, computer networks, communications, transportation and economic systems. →

- Technology scanning, mapping, and valuation to identify new science and technology-based opportunities that meet the needs and aspirations of today's consumers, companies and the broader society. This thrust builds coherence between short- and longer-term R&D opportunities and their potential impact.

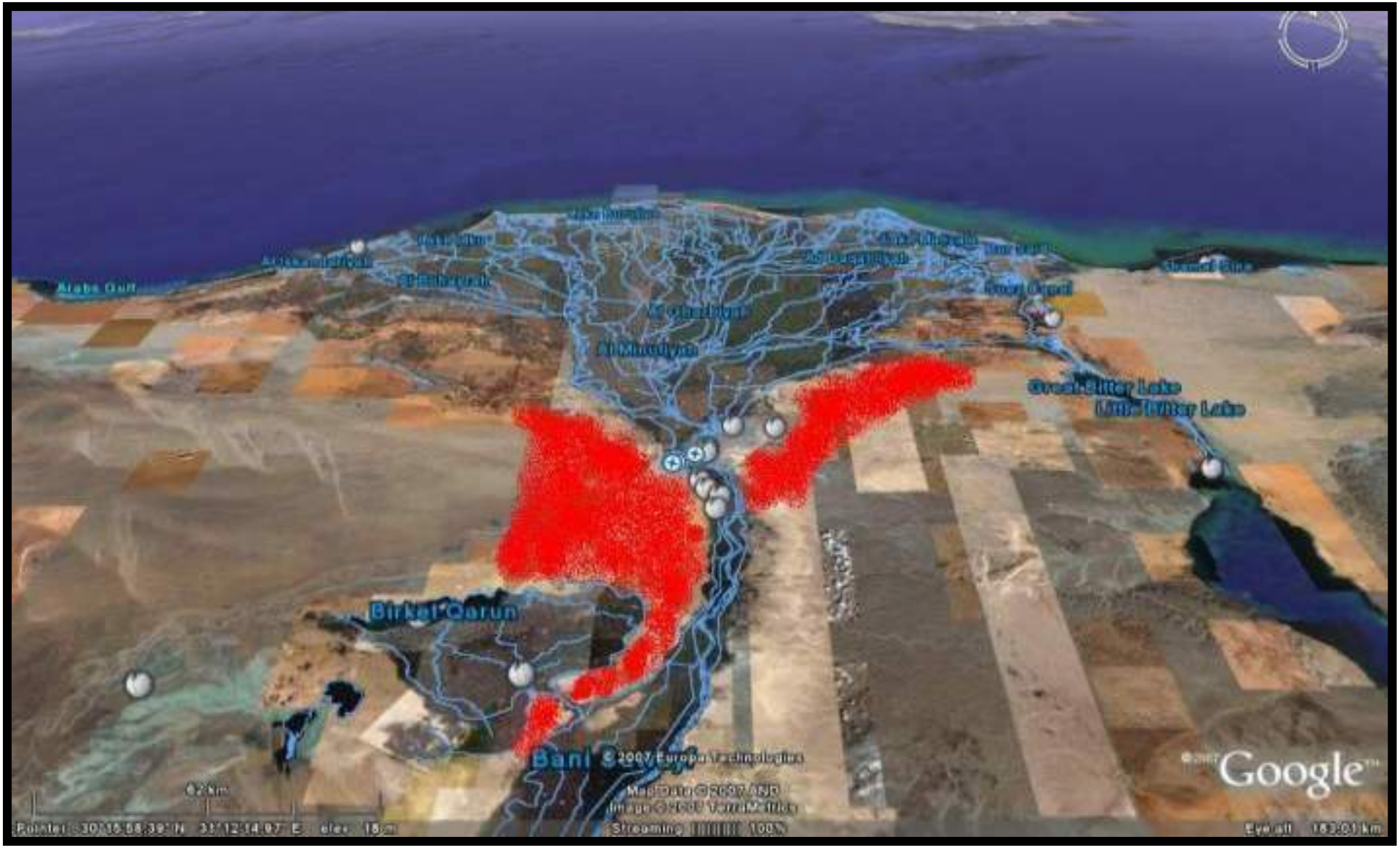
Example: EGYPT
Analysis-- Factors Affecting Agriculture



Data Collection: Water Source Locations

- Locations have been estimated along the river Nile and its laterals
- Water source elevations were estimated using Google earth

Decision Real Life Picture



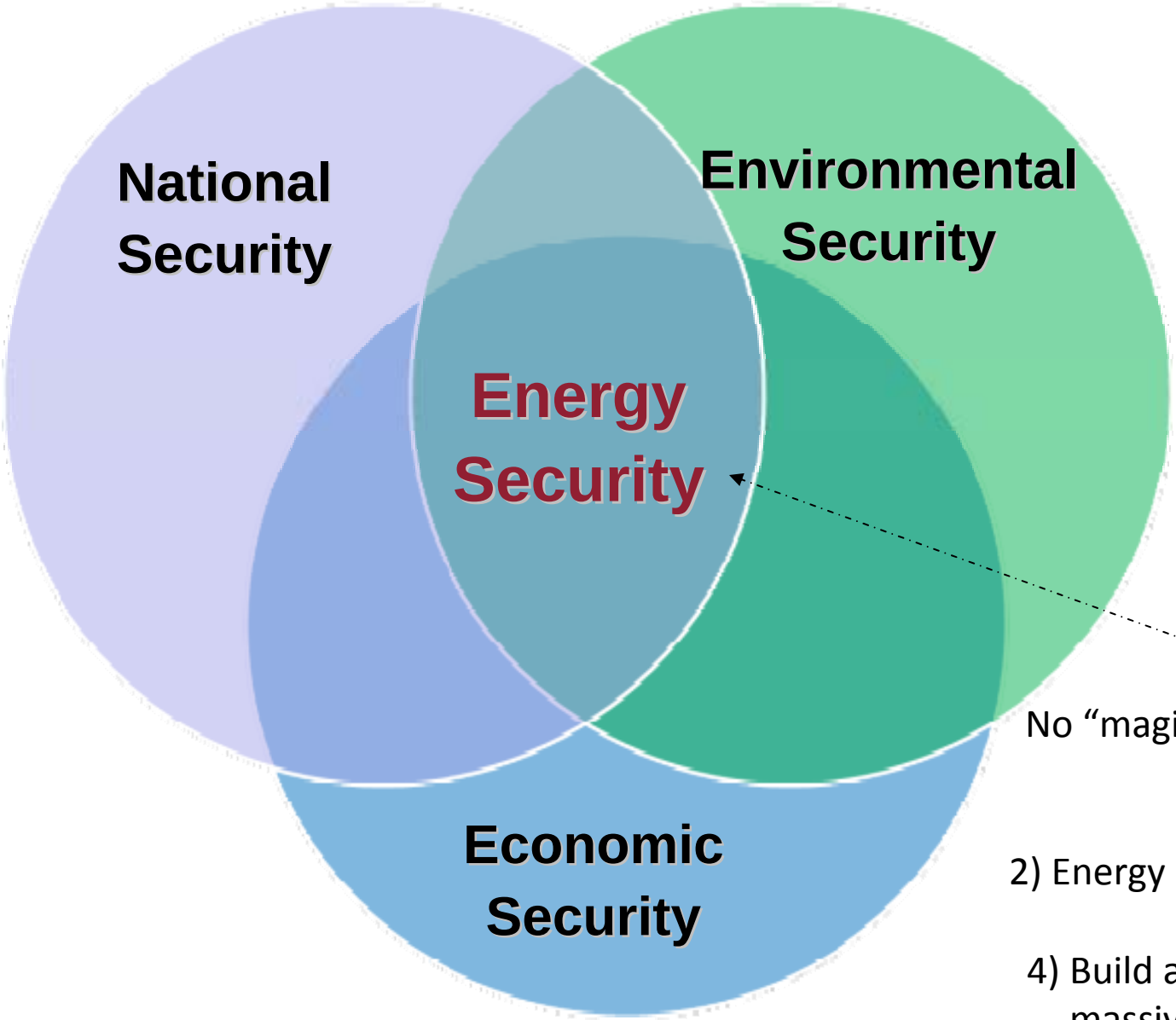
Bigger Picture: Challenges…

- Development of advanced Computers, Communications, & Control networks overlay the power network
- Knowing what is happening- Satellite-based WAMS
- Understanding what constitutes a problem- Dynamic Stability Analysis, visualization tools
- Understanding the “true” dynamics soon enough to do something about it- Faster analysis, look-ahead simulation,...
- Determining what actions could solve the problem- Contingency plans, and risk management
- Implementing the solution- Control devices/systems; alternate path options

… Require Basic Research

- Intelligent sensors as elements in real-time data base; sensor interface to multi-resolutional models? Metrics?
- Increased dependence on information systems (e.g., software as the glue among various subsystems/tasks)
- Dependability/robustness is the key; V&V remains a big challenge
- Effect of market structures, distributed generation, other new features on above issues
- Designing/Evolving a robust system - Complexity, distributed sensing, control and adaptation

The Energy Crises Taught Us Interdependency



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.

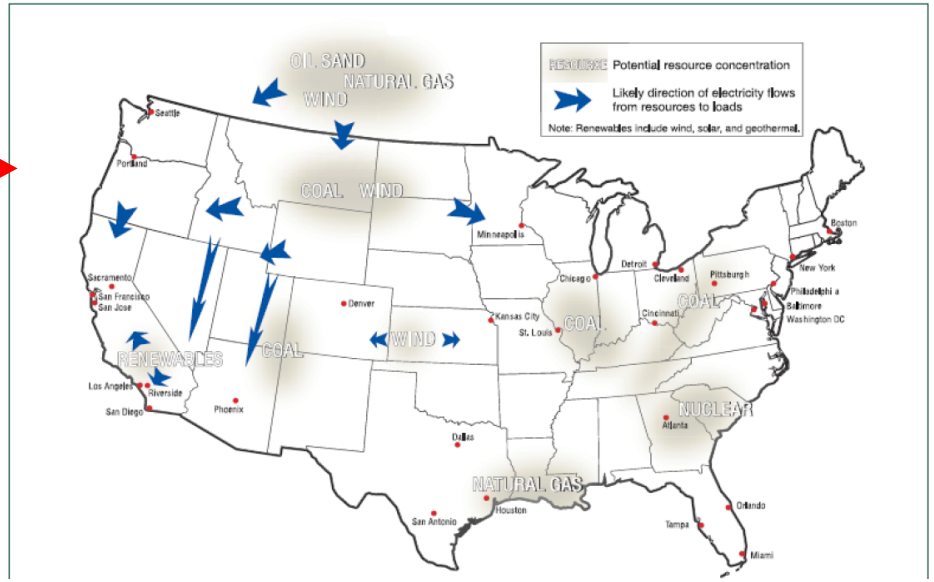
Smart Grid: Integrate Dispersed Energy Sources into a Modern Grid to Provide Energy to Centers of Demand

Recommendations for moving to energy systems to meet demand of tomorrow

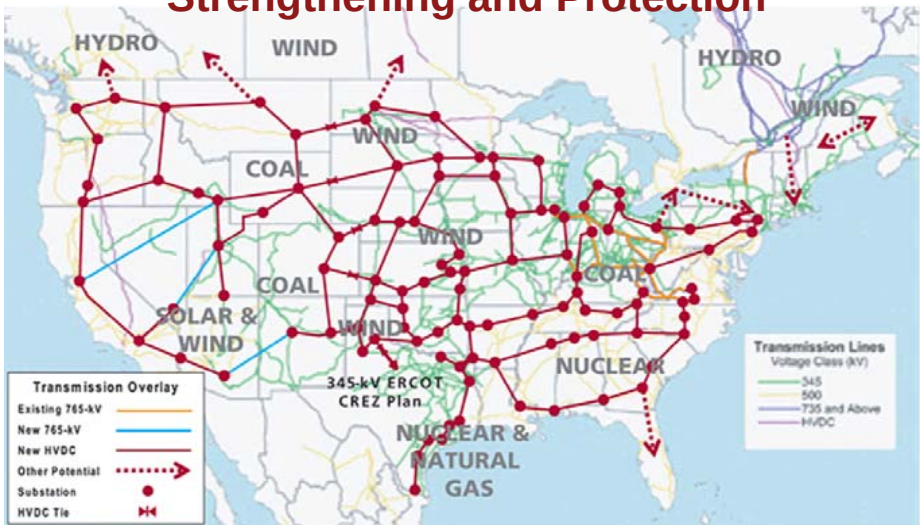
- **Build a stronger and smarter electrical energy infrastructure**
  - – Transform the Network into a Smart Grid
  - – Develop an Expanded Transmission System
  - – Develop Massive Electricity Storage Systems
- **Break our addiction to oil by transforming transportation**
  - – Electrify Transportation: Plug-In Hybrid Electric Vehicles
  - – 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**

Source: Massoud Amin's Congressional briefings on March 26 and Oct. 15, 2009

Emerging Supply and Demand Patterns



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

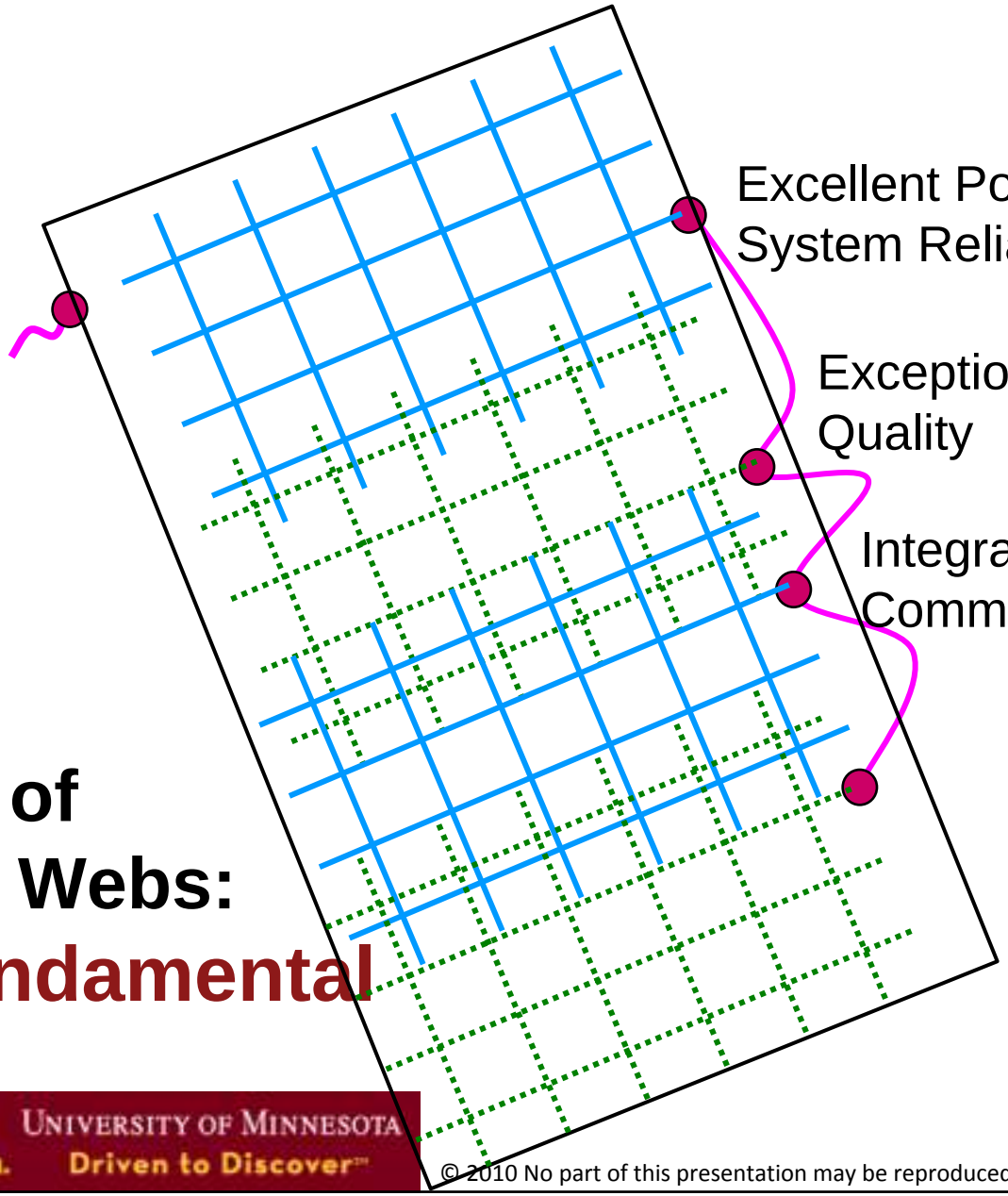


Technological Leadership Institute

University of Minnesota Driven to Discover℠

The Smart Infrastructure for a Digital Society

A Secure Energy Infrastructure



A Complex Set of Interconnected Webs:

Security is Fundamental

Observations

Threat Situation:

- Cyber has “weakest link” issues
- Cyber threats are dynamic, evolving quickly and often combined with lack of training and awareness.

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.

Enabling a Stronger and Smarter Grid:

- Broad range of R&D including end-use and system efficiency, electrification of transportation, stronger and smarter grid with massive storage

- Sensing, Communications, Controls, Security, Energy Efficiency and Demand Response *if architected correctly* could assist the development of a smart grid

- Smart Grid Challenge/Opportunity areas include:
  - Distributed Control
  - Grid Architectures
  - Cyber Security

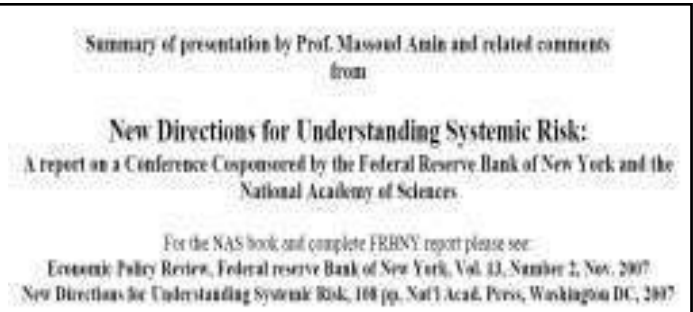
Source: Massoud Amin, Congressional briefings, March 26 and October 15, 2009


THANK YOU
MINNESOTA

Selected References

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

- **"A Control and Communications Model for a Secure and Reconfigurable Distribution System,"** (Giacomoni, Amin, *&* Wollenberg), IEEE ACC, June 2011
- **"Securing the Electricity Grid,"** (Amin), *The Bridge,* the quarterly publication of the National Academy of Engineering, Volume 40, Number 1, Spring 2010
- **"Preventing Blackouts,"** (Amin and Schewe), Scientific American, pp. 60-67, May 2007
  "New Directions in Understanding Systemic Risk", with NAS and FRBNY Committee, National Academy of Sciences and Federal Reserve Bank of NY, Mar. 2007
- **"Powering the 21st Century: We can -and must- modernize the grid,"** IEEE Power & Energy Magazine, pp. 93-95, March/April 2005
- Special Issue of Proceedings of the IEEE on **Energy Infrastructure Defense Systems**, Vol. 93, Number 5, pp. 855-1059, May 2005
- **"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
- **"North American Electricity Infrastructure: Are We Ready for More Perfect Storms? ,"** IEEE Security and Privacy, Vol. 1, no. 5, pp. 19-25, Sept./Oct. 2003



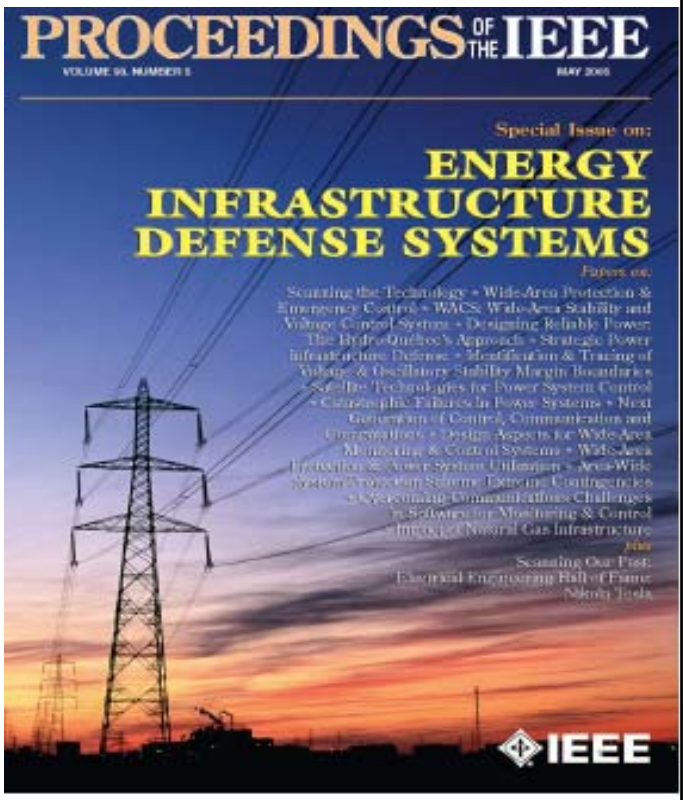
Summary of presentation by Prof. Masoud Amin and related comments from

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 pg. 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 complete 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℠