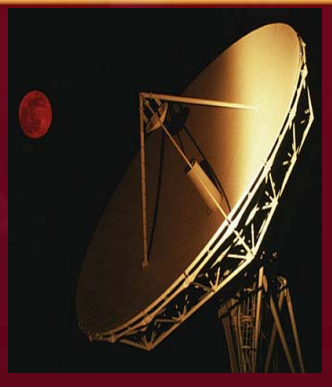
Resilience and Self-healing Challenges: Present/Possible Futures

S. Massoud Amin
Director and Honeywell/H.W. Sweatt Chair in Technological Leadership
University Distinguished Teaching Professor
Professor of Electrical & Computer Engineering

***CRITIS'08,* 3rd International Workshop on Critical Information Infrastructures Security**
October 13-15, 2008, Frascati (Rome), Italy



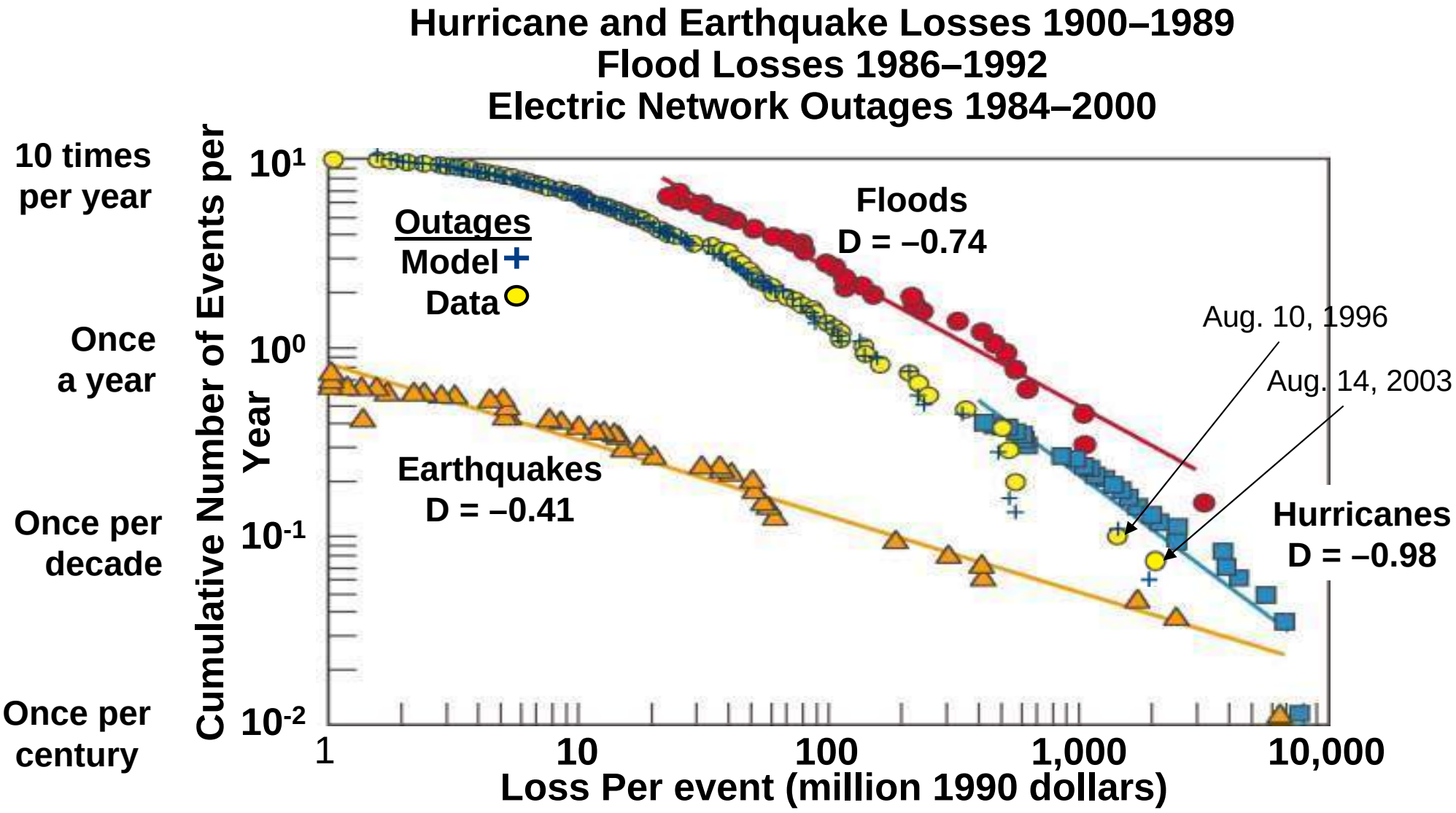




cdtl
Center for the Development of Technological Leadership

Support from the Electric Power Research Institute (EPRI}, NSF and ORNL for this work is gratefully acknowledged.

UNIVERSITY OF MINNESOTA
Driven to Discover℠

Power Law Distributions: Frequency & impacts of major disasters



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

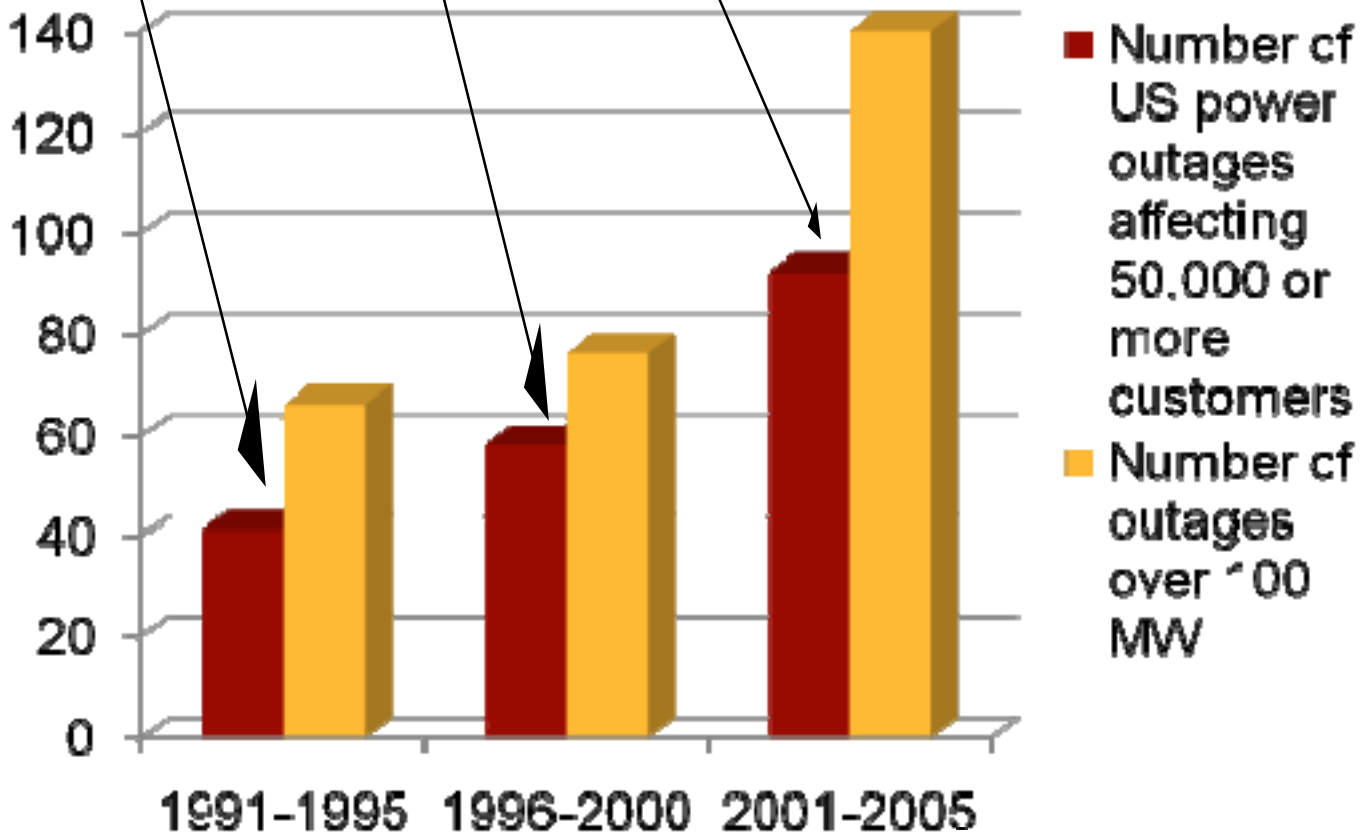
66 Occurrences over 100 MW
41 Occurrences over 50,000 Consumers

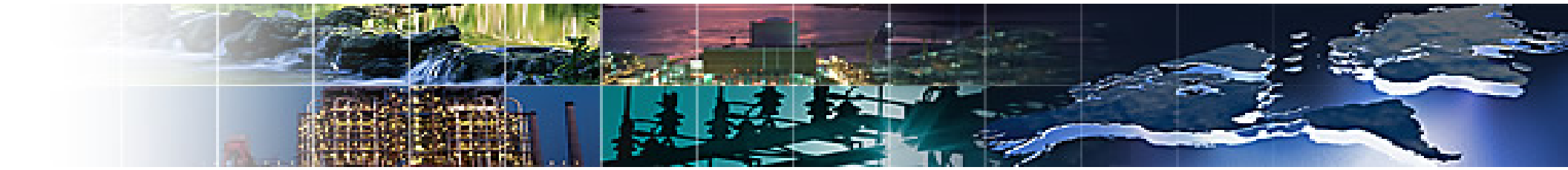
76 Occurrences over 100 MW
58 Occurrences over 50,000 Consumers

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

Result: Large blackouts are growing in number and severity

***Analyzing outages in 2006 we had:**
24 Occurrences over 100 MW
34 Occurrences over 50,000 or more Consumers
Data courtesy of NERC's Disturbance Analysis Working Group database





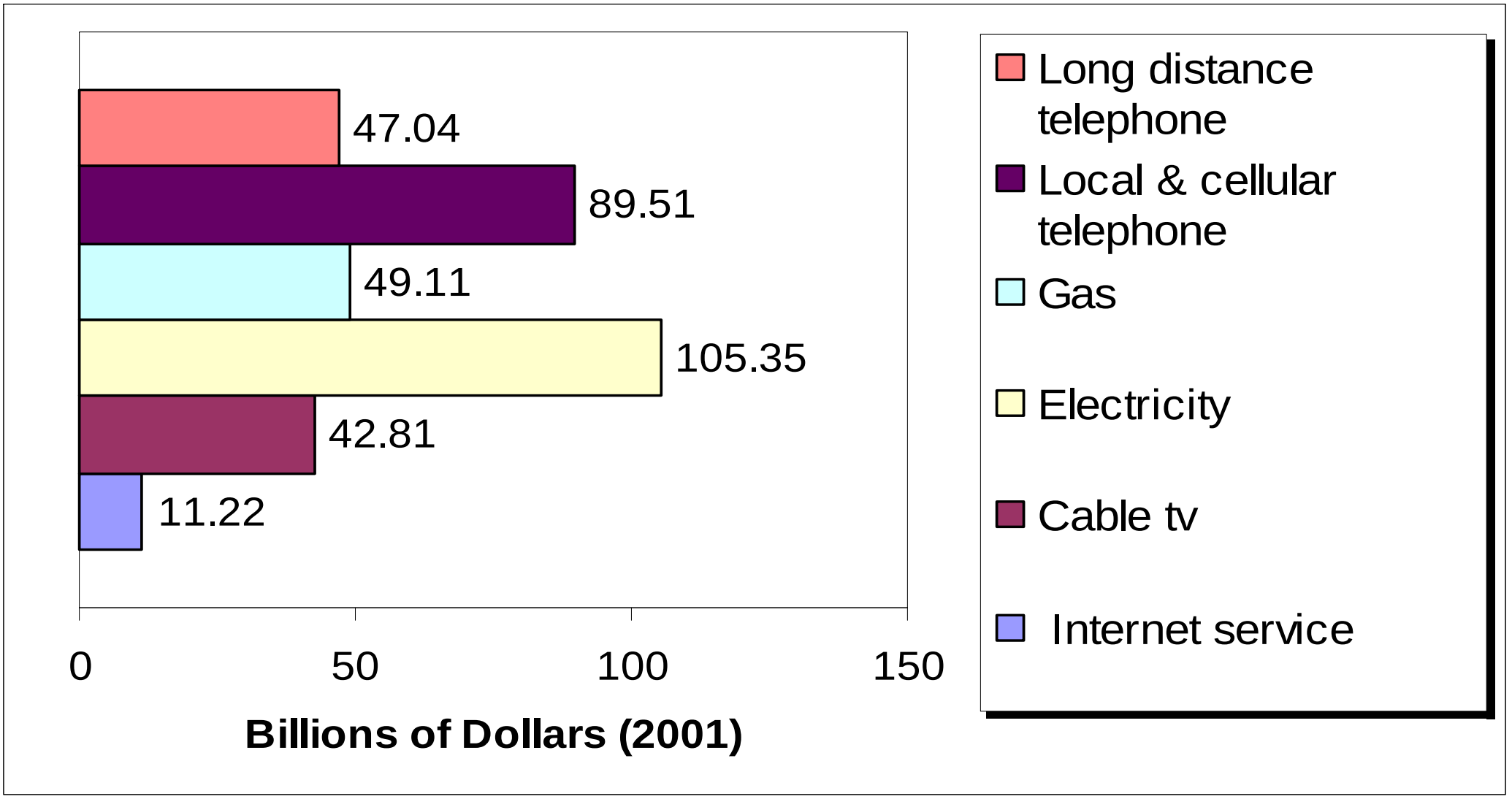
The Infrastructure Challenge

Will today's electricity supply system be left behind as an industrial relic of the 20th century, or become the critical infrastructure supporting the digital society, a smart self-healing grid?

Increasing Demand for Security & Quality

- Power, communications, and computing are all converging, making entire systems as sensitive as the most sensitive component
- Secure and reliable combined electric power, communications, fuel supply, and financial networks are essential to today's microprocessor-based economy, public health and safety, and overall quality of life
- The demands of our secure digital economy are outpacing the electricity and communication infrastructures that supports it
- $75B-$180B in annual losses to U.S. from power outages and disturbances

Personal Consumption Expenditures
(in Billions of 2001 U.S. Dollars)



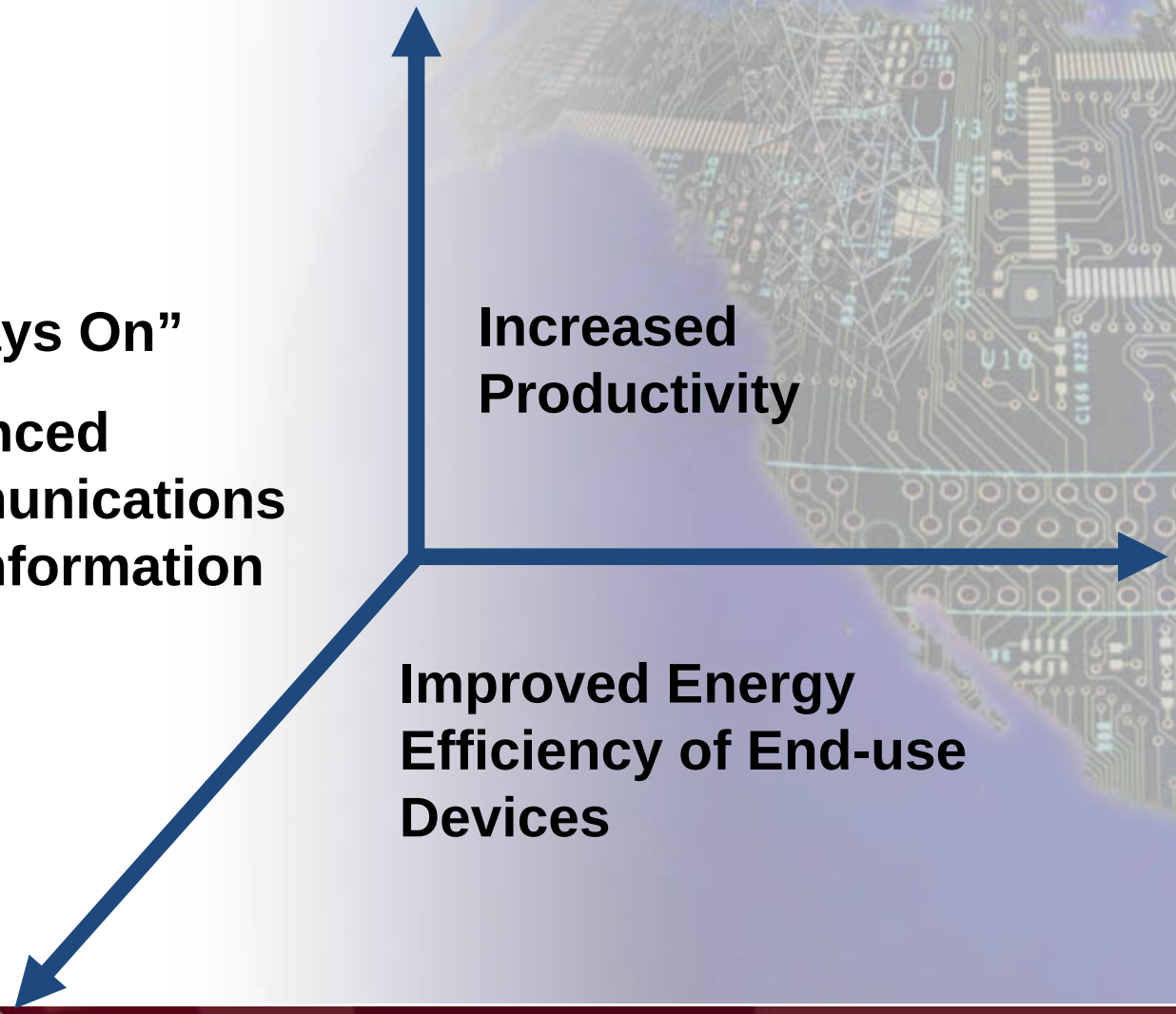
Source: US Dept of Commerce, Personal Expenditure Detail Data, File 206U, 01/03

Dimensions of the Digital Society: Benefits

Enhanced Quality of Life

Reduced Energy Demand

Increased Industrial Competitiveness



"Always On"

Enhanced communications and information

Increased Productivity

Improved Energy Efficiency of End-use Devices

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.

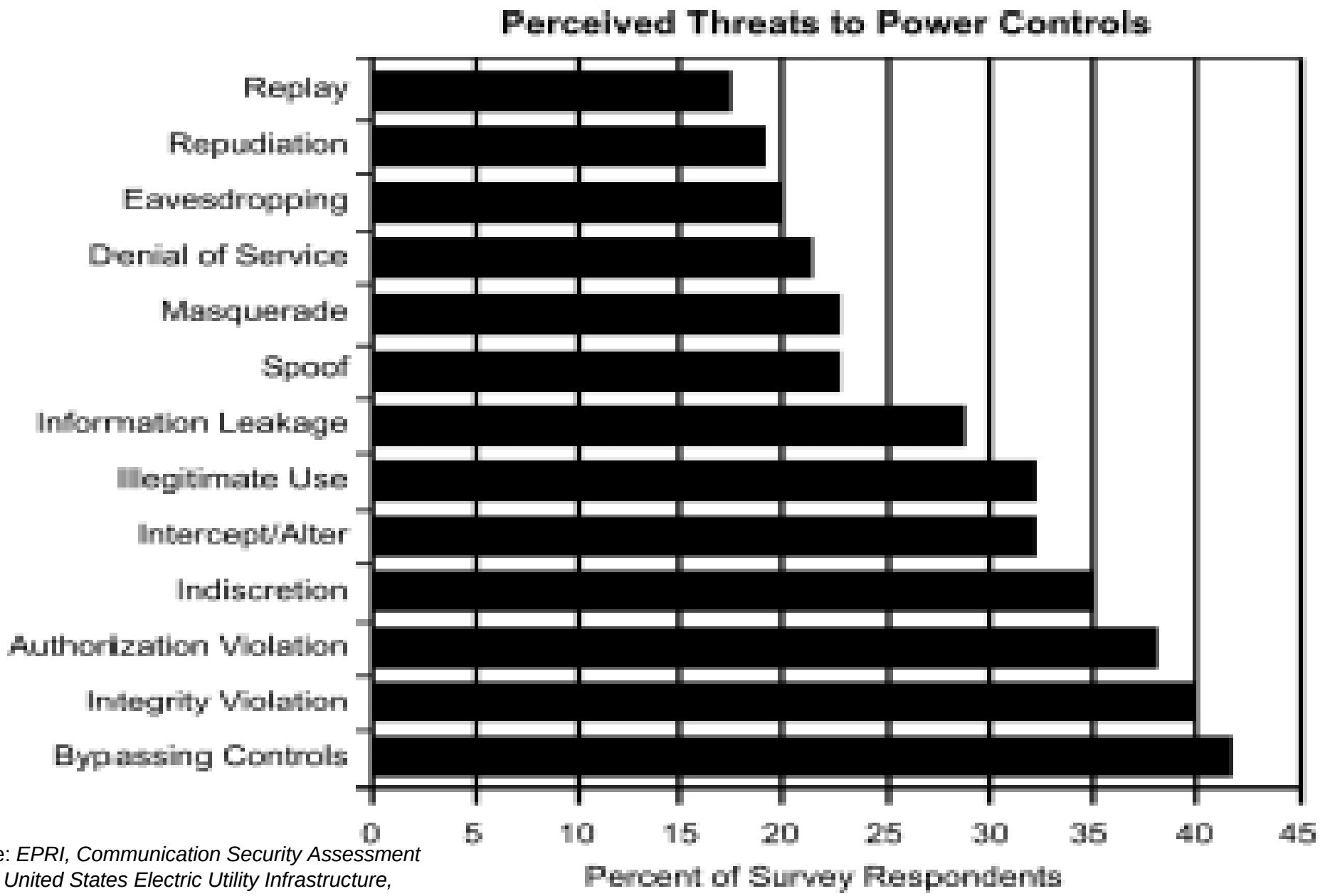
Assessing the Most Effective Security Investments: Probabilistic and dynamic assessments can offer strategic guidance on where and how to deploy security resources to greatest advantage.

Four Areas of Vulnerability

SQRA

- **Security of power delivery and market systems**
- **Quality of information and energy supplied**
- **Reliability of interdependent infrastructures**
- **Availability of affordable services**

Cyber Threats to Controls



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

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.

Definition: Resilience

- **What is “Resilience”?**
  - 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** is the property of a material to absorb energy when it is deformed elastically and then, upon unloading to have this energy recovered. In other words, it is the maximum energy per volume that can be elastically stored. It is represented by the area under the curve in the elastic region in the Stress-Strain diagram.
  - **Resilience** in psychology is the positive capacity of people to cope with stress and catastrophe. It is also used to indicate a characteristic of resistance to future negative events. In this sense "resilience" corresponds to cumulative "protective factors" and is used in opposition to cumulative "risk factors".
  - The phrase "risk and resilience“ are commonly used terms, which are essentially synonymous within psychology, are "resilience", "psychological resilience", "emotional resilience", "hardiness", and "resourcefulness".
- **What is “Robustness”?**
  - The quality of being able to withstand stresses, pressures, or changes in procedure or circumstance.
  - A system, organism or design may be said to be "robust" if it is capable of coping well with variations (sometimes unpredictable variations) in its operating environment with minimal damage, alteration or loss of functionality.

Definition: Self Healing Grid

- **What is "self healing"?**
  - A system that uses information, sensing, control and communication technologies to allow it to deal with unforeseen events and minimize their adverse impact …
- **Why is self healing concept important to the Energy Infrastructure?**
  - A secure "architected" sensing, communications, automation (control), and energy overlaid infrastructure as an integrated, reconfigurable, and electronically controlled system that will offer unprecedented flexibility and functionality, and improve system availability, security, quality, resilience and robustness.

The Challenge

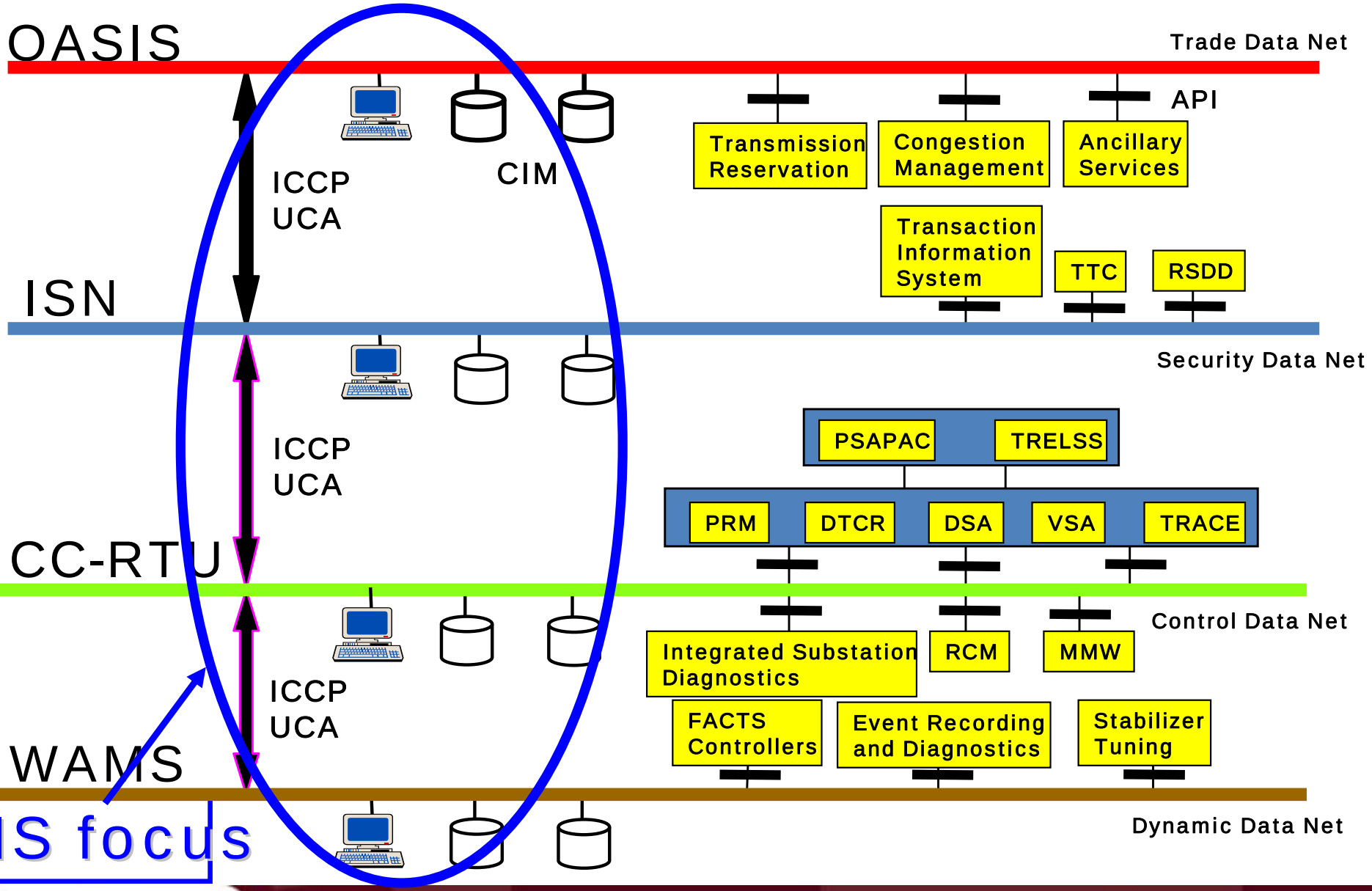
Enabling/Creating a stronger, more secure, resilient, and more stable interdependent infrastructure that is vital to support the digital society

Overview of my research areas (1998-2003):

Initiatives and Programs I developed and/or led at EPRI

1999-2001	Y2K→2000-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 intel. & self-healing	➢ Information Sharing ➢ Intrusion/Tamper Detection ➢ Comm. Protocol Security ➢ Risk Mgmt. ➢ Enhancement ➢ High Speed Encryption	Response to 9/11 Tragedies ➢ Strategic Spare Parts Inventory ➢ Vulnerability Assessments ➢ Red Teaming ➢ Secure Communications	➢ Self Healing Grid ➢ IntelliGrid™ ➢ Integrated Electric Communications System Architecture ➢ Fast Simulation and Modeling

Information Networks for On-Line Trade, Security and 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)

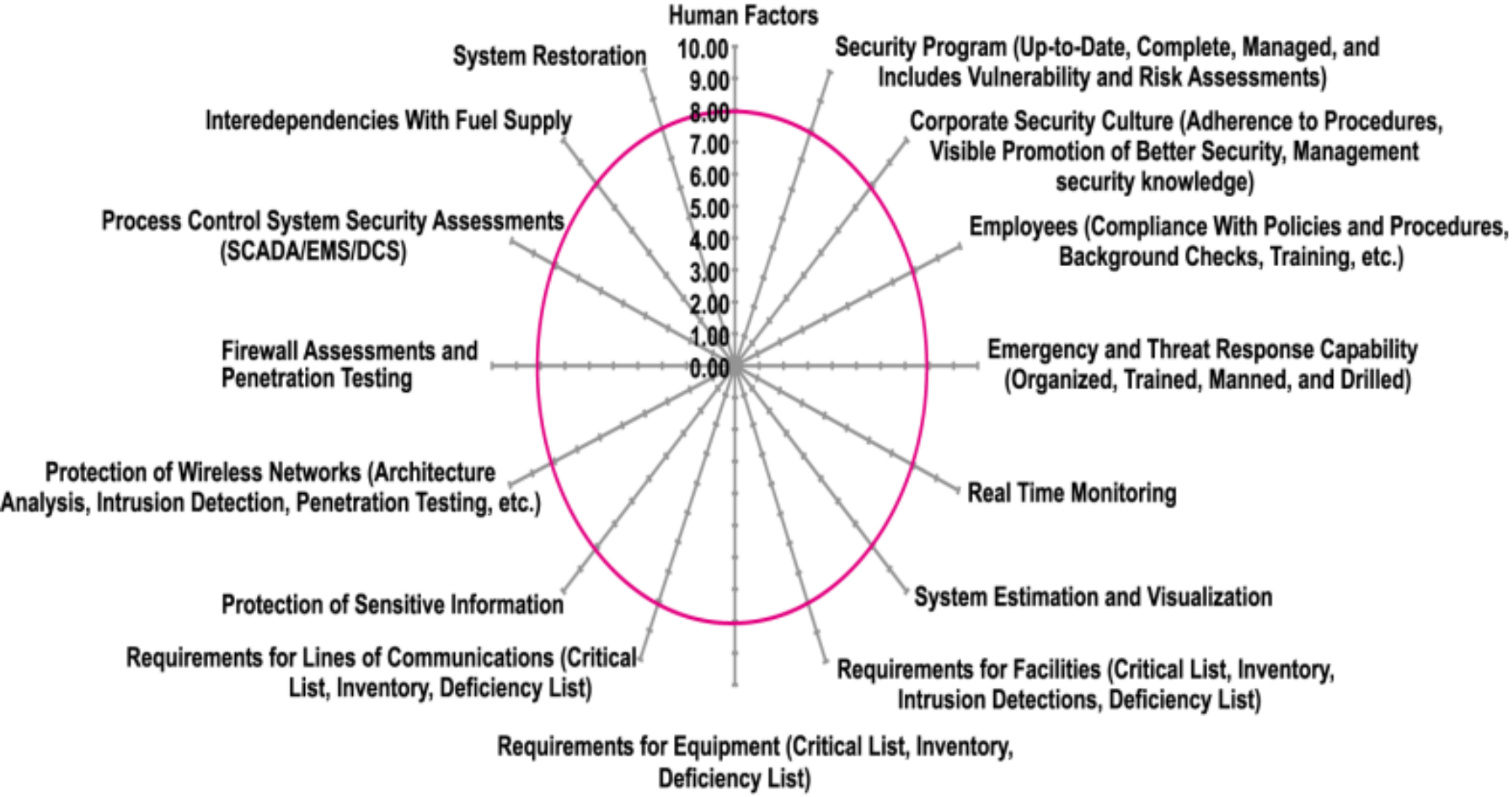
Physical

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



Foundations: EPRI/DOD Complex Interactive Network/Systems Initiative

"We are sick and tired of them and they had better change!"
Chicago Mayor Richard Daley on the August 1999 Blackout

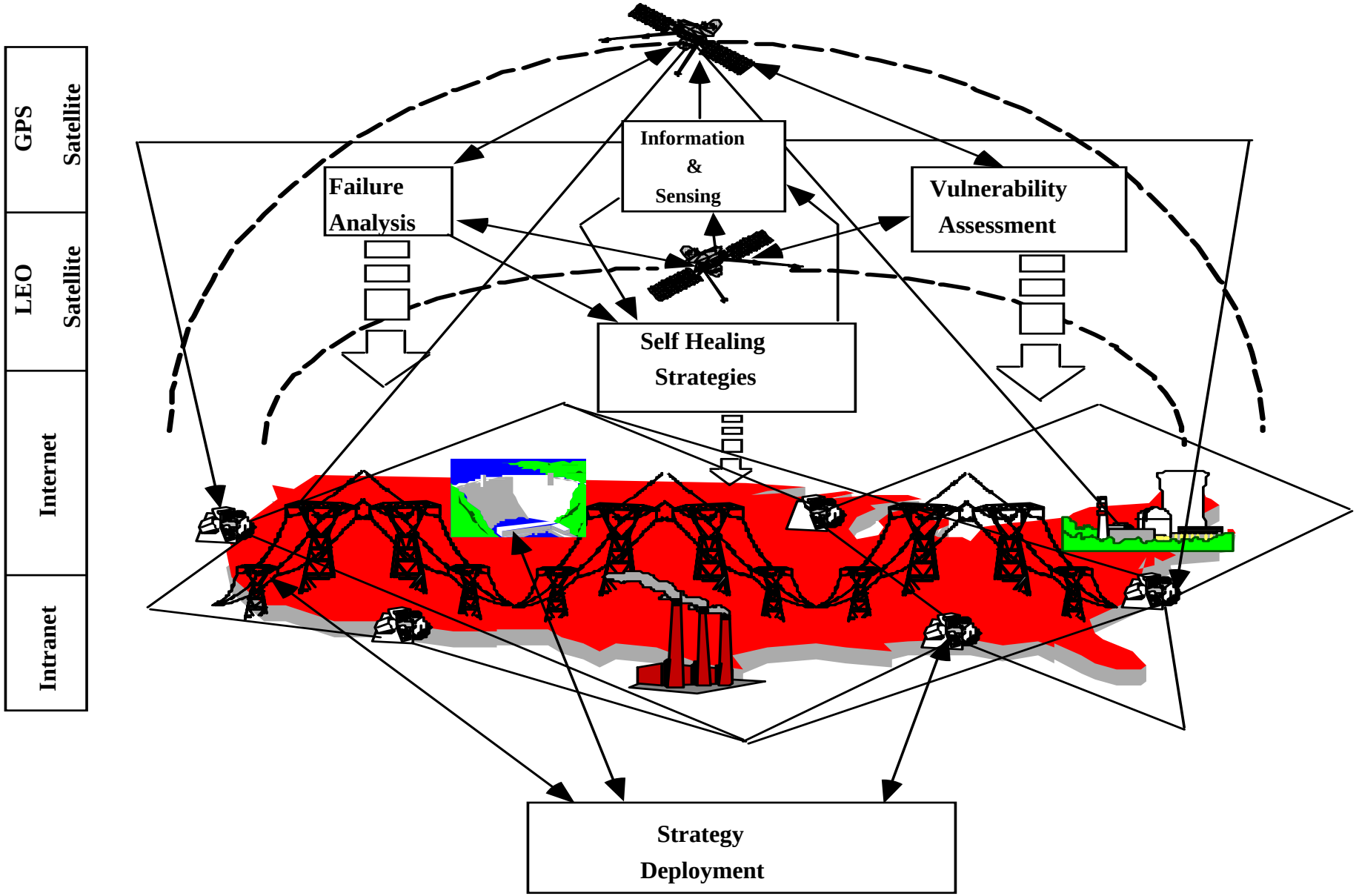
Complex interactive networks:

- *Energy infrastructure*: Electric power grids, water, oil and gas pipelines
- *Telecommunication:* Information, communications and satellite networks; sensor and measurement systems and other continuous information flow systems
- *Transportation and distribution networks*
- *Energy markets, banking and finance*

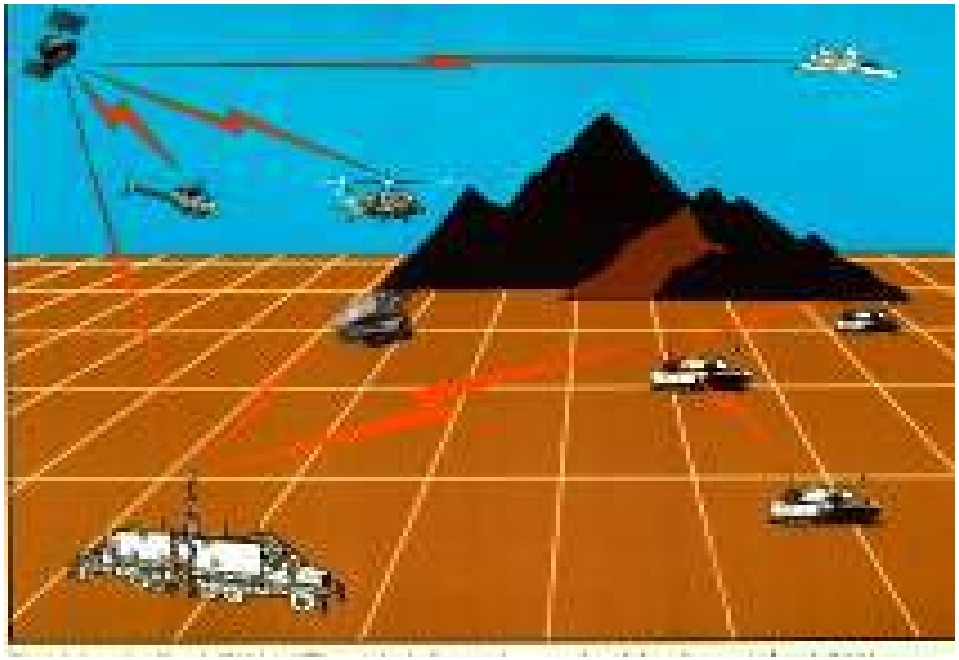
1999-2001: $5.2M / year — Equally Funded by DoD/EPRI

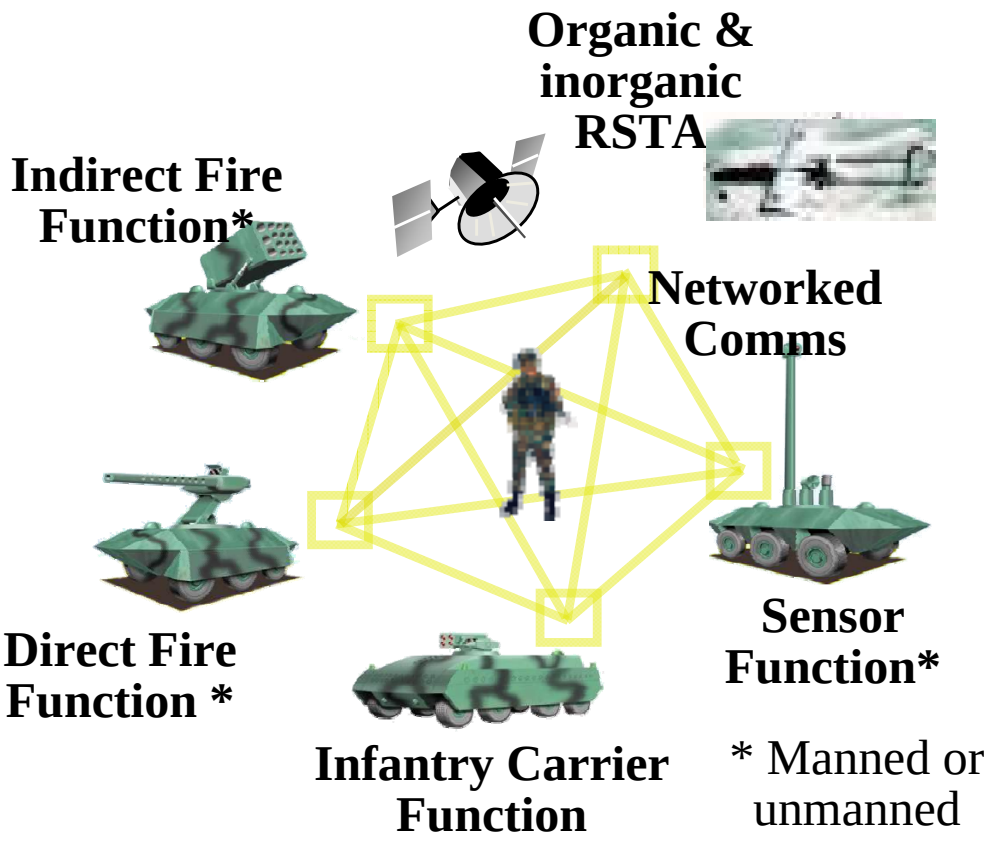
Develop tools that enable secure, robust and reliable operation of interdependent infrastructures with distributed intelligence and self-healing abilities

Complex Interactive Networks



Network Centric Objective Force





CIN/SI Funded Consortia

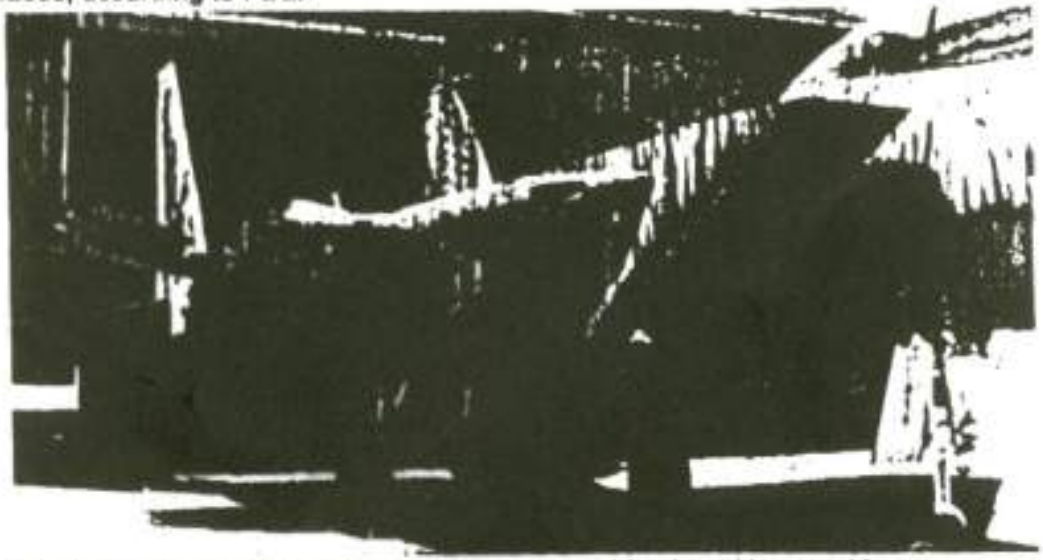
107 professors in 28 U.S. universities are funded: Over 360 publications, and 24 technologies extracted, in the 3-year initiative

- U Washington, Arizona St., Iowa St., VPI
- Purdue, U Tennessee, Fisk U, TVA, ComEd
- Harvard, UMass, Boston, MIT, Washington U.
- Cornell, UC-Berkeley, GWU, Illinois, Washington St., Wisconsin
- CMU, RPI, UTAM, Minnesota, Illinois
- Cal Tech, MIT, Illinois, UC-SB, UCLA, Stanford

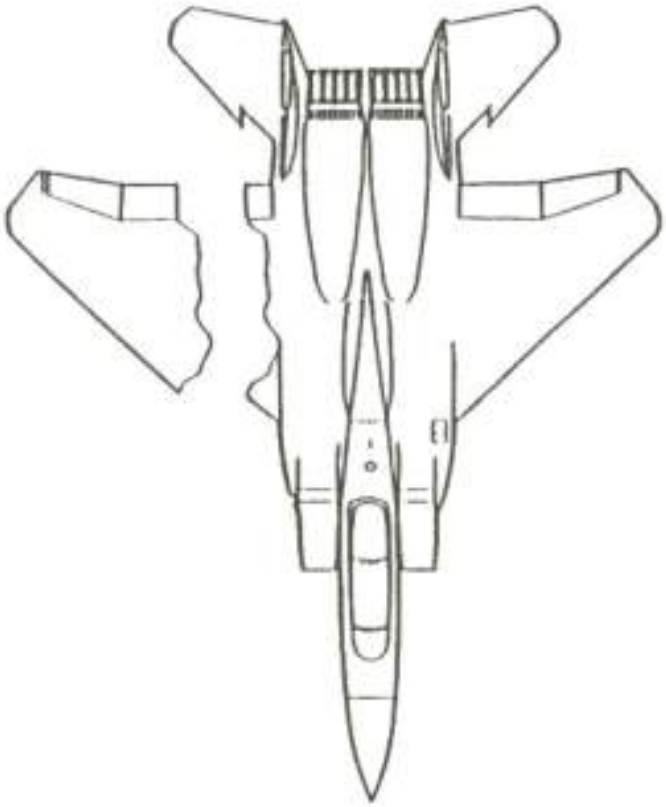
- Defense Against Catastrophic Failures, Vulnerability Assessment
- Intelligent Management of the Power Grid
- Modeling and Diagnosis Methods
- Minimizing Failures While Maintaining Efficiency / Stochastic Analysis of Network Performance
- Context Dependent Network Agents
- Mathematical Foundations: Efficiency & Robustness of Distributed Systems

Background: The Case of the Missing Wing

Believe it or not, this one made it back! This F-15, with half its wing missing, is a good example of what is currently considered an "unflyable" aircraft. However, the pilot's success in bringing it home helped to inspire a new program at Aeronautical Systems Division's Flight Dynamics Laboratory aimed at enabling future fighter pilots to fly aircraft with severely damaged control surfaces. The pilot of this F-15 configured in unusual ways the control surfaces that were still working to compensate for the damaged wing. The FDL program will make this "survivors" reaction automatic to the aircraft. Therefore, flying a damaged aircraft will be much easier on the pilot. Through a self-repairing flight control system nearing development, a computerized "brain" will automatically reconfigure such surfaces as rudders, flaperons, and allerons to compensate for grave damage to essential flying surfaces, according to FDL.

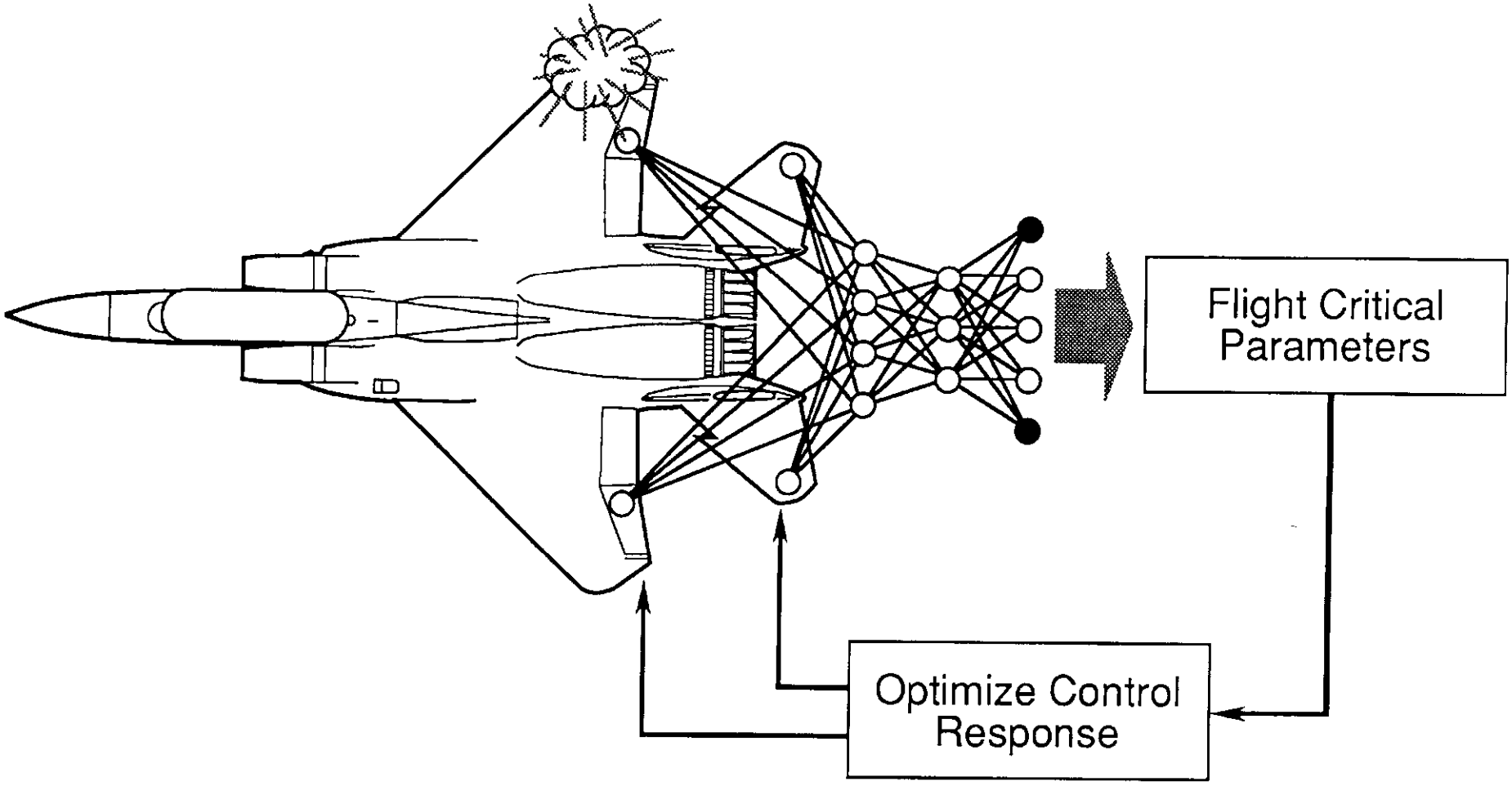


Only smart work by the pilot and the unique combination of interworking control surfaces on the F-15 brought this one back alive. With old-fashioned conventional allerons and horizontal stabilizer, it couldn't have happened.



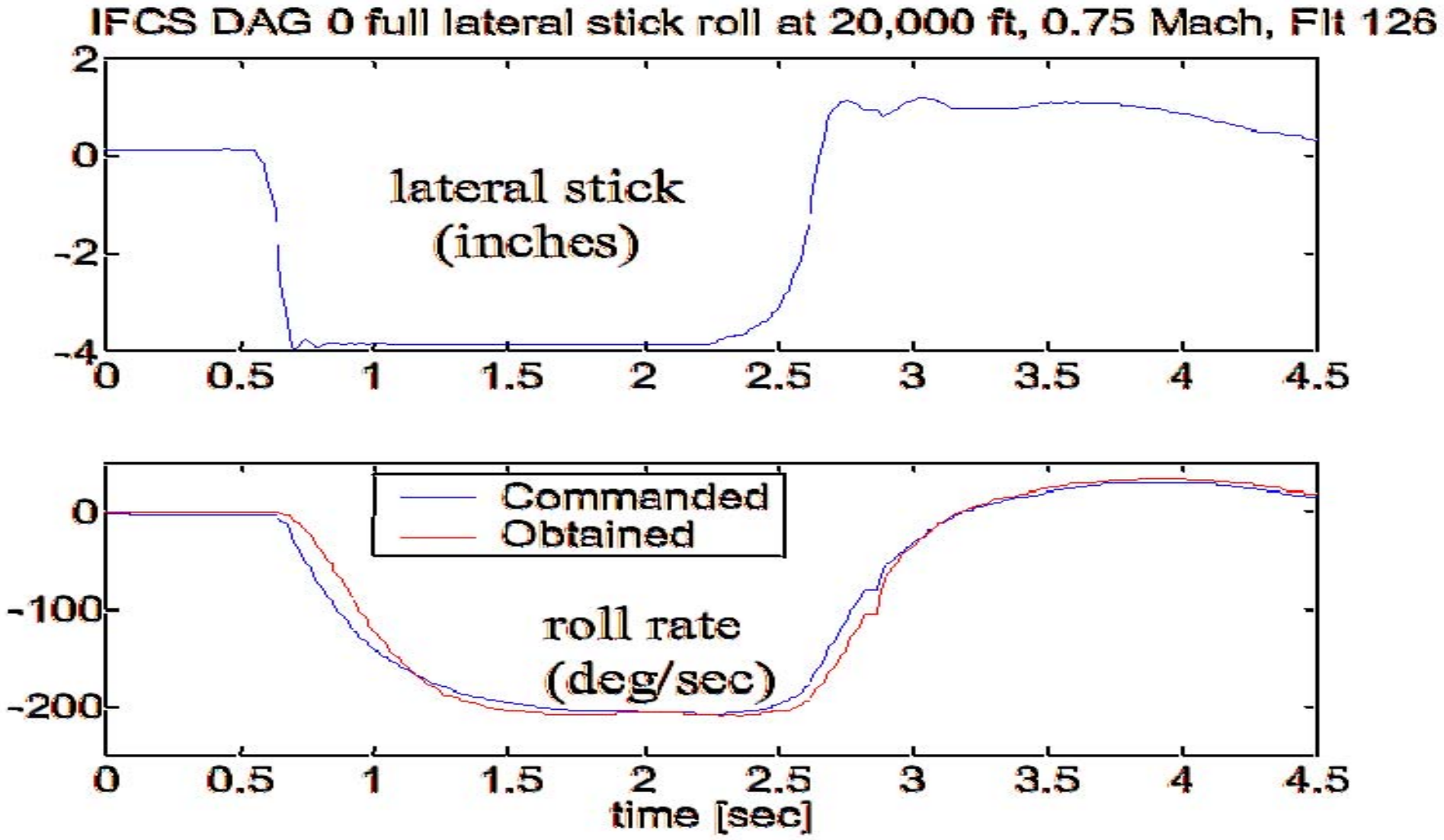
NASA/MDA/WU IFCS: NASA Ames Research Center, NASA Dryden Flight Research Center, Boeing Phantom Works, and Washington University in St. Louis.

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



NASA/MDA/WU IFCS

Roll Axis Response of the Intelligent Flight Control System



Accomplishments in the IFCS program

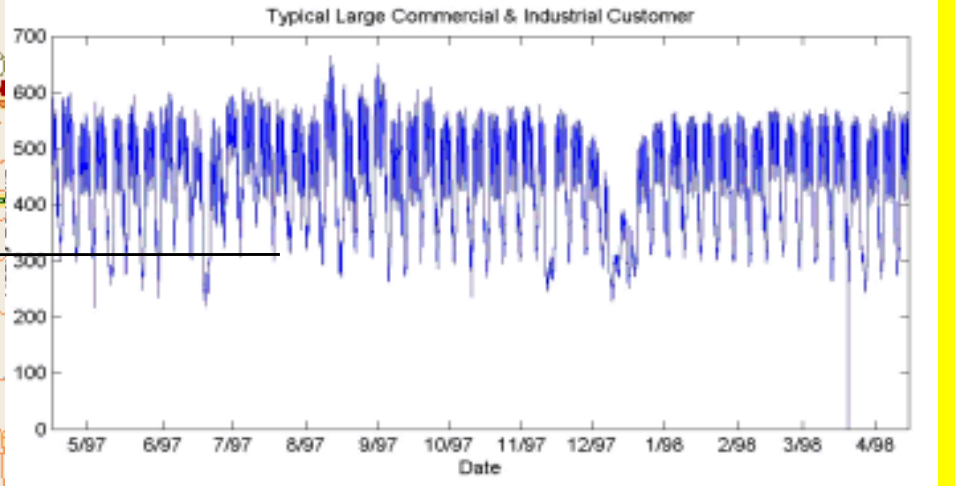
- The system was successfully test flown on a test F-15 at the NASA Dryden Flight Research Center:
  - Fifteen test flights were accomplished, including flight path control in a test flight envelope with supersonic flight conditions.
  - Maneuvers included 4g turns, split S, tracking, formation flight, 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.

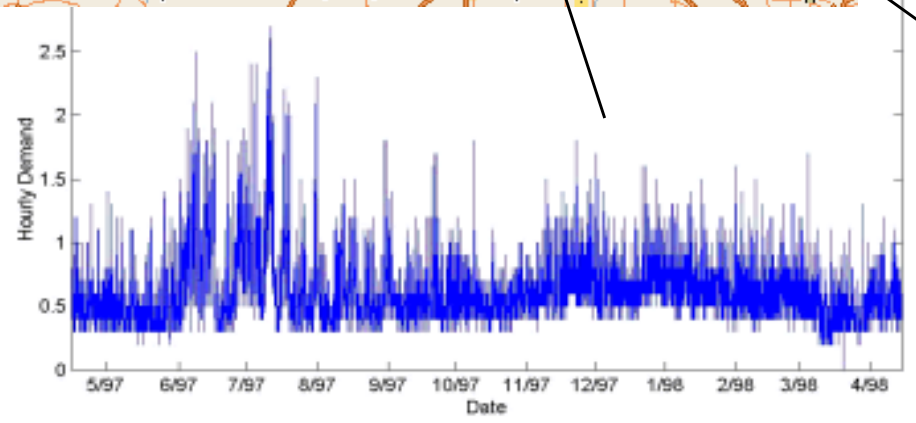
Self-healing Grid

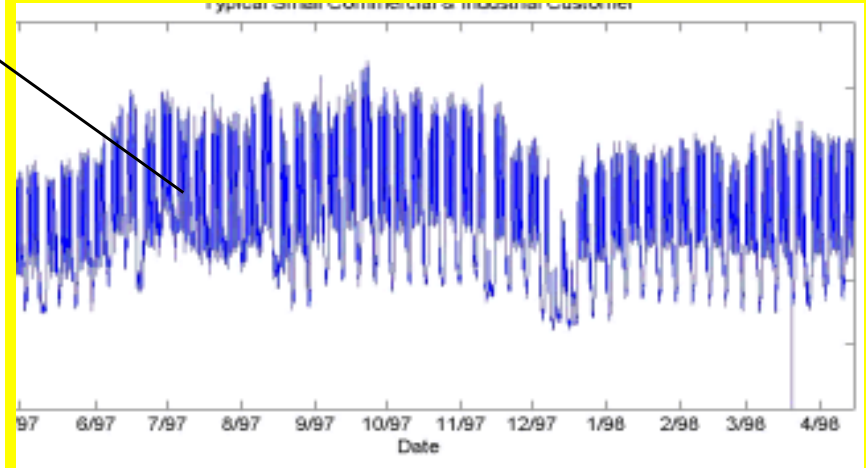
Building on the Foundation:

- Anticipation of disruptive events
- Look-ahead simulation capability
- Fast isolation and sectionalization
- Adaptive islanding

Local area grids (LAG)



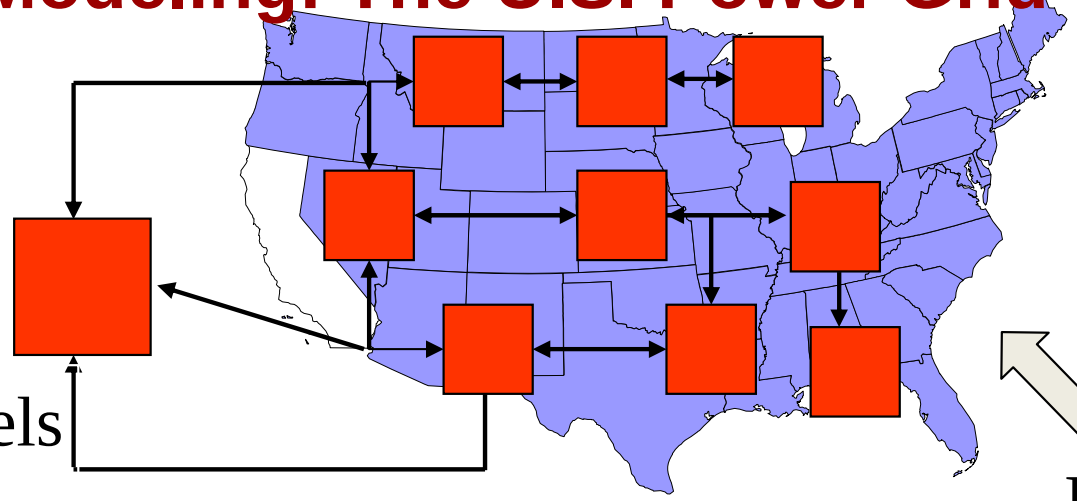




Look-Ahead Simulation Applied to Multi-Resolution Models

- 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)

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



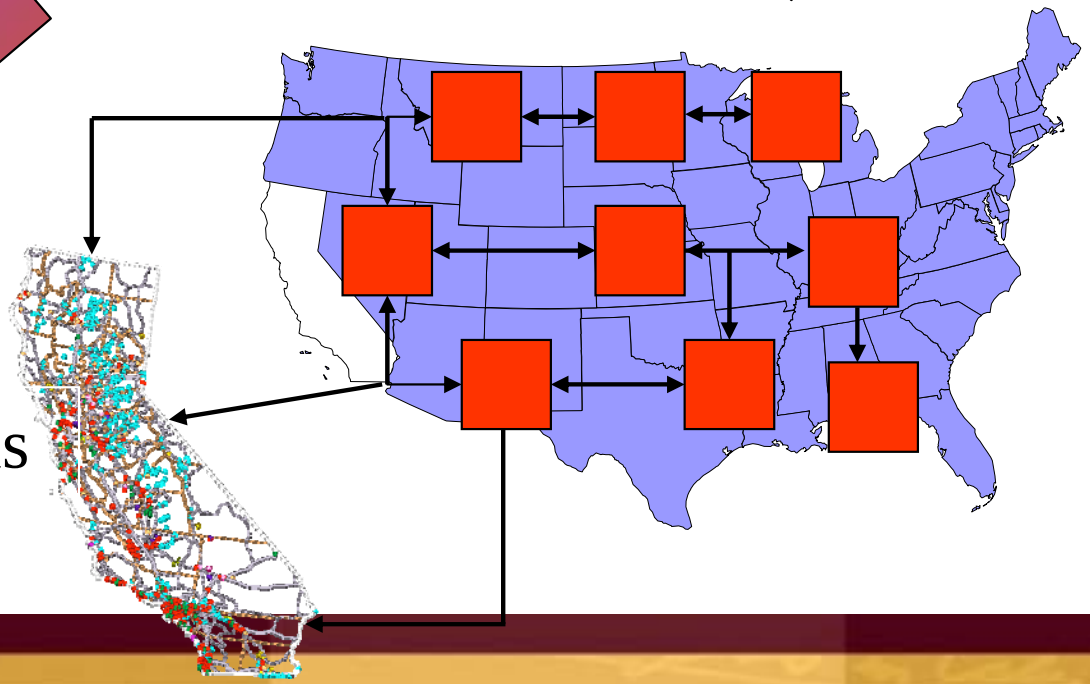
Simplified models

Low-resolution model

MODEL REDUCTION

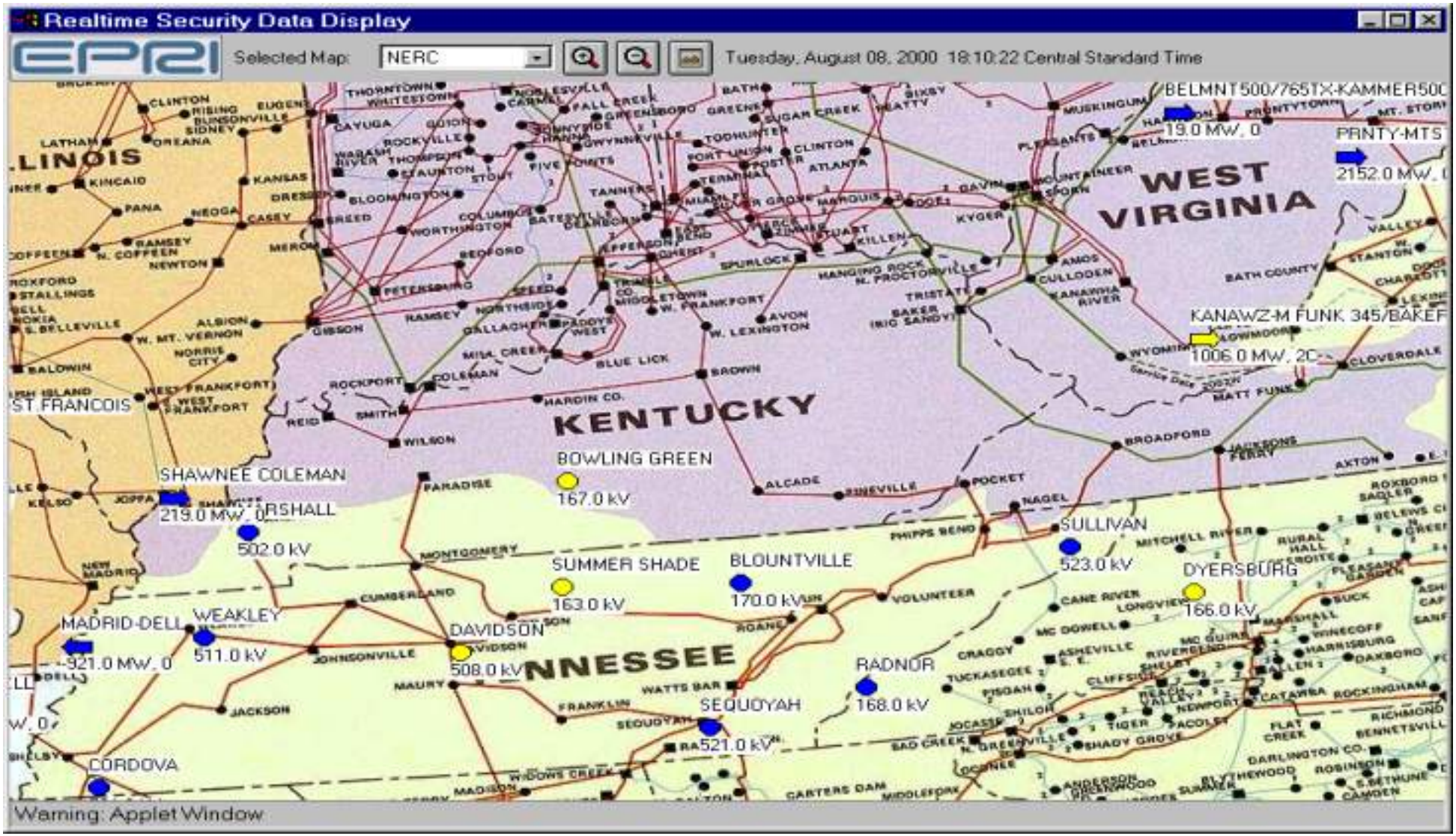
MODEL REFINEMENT

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

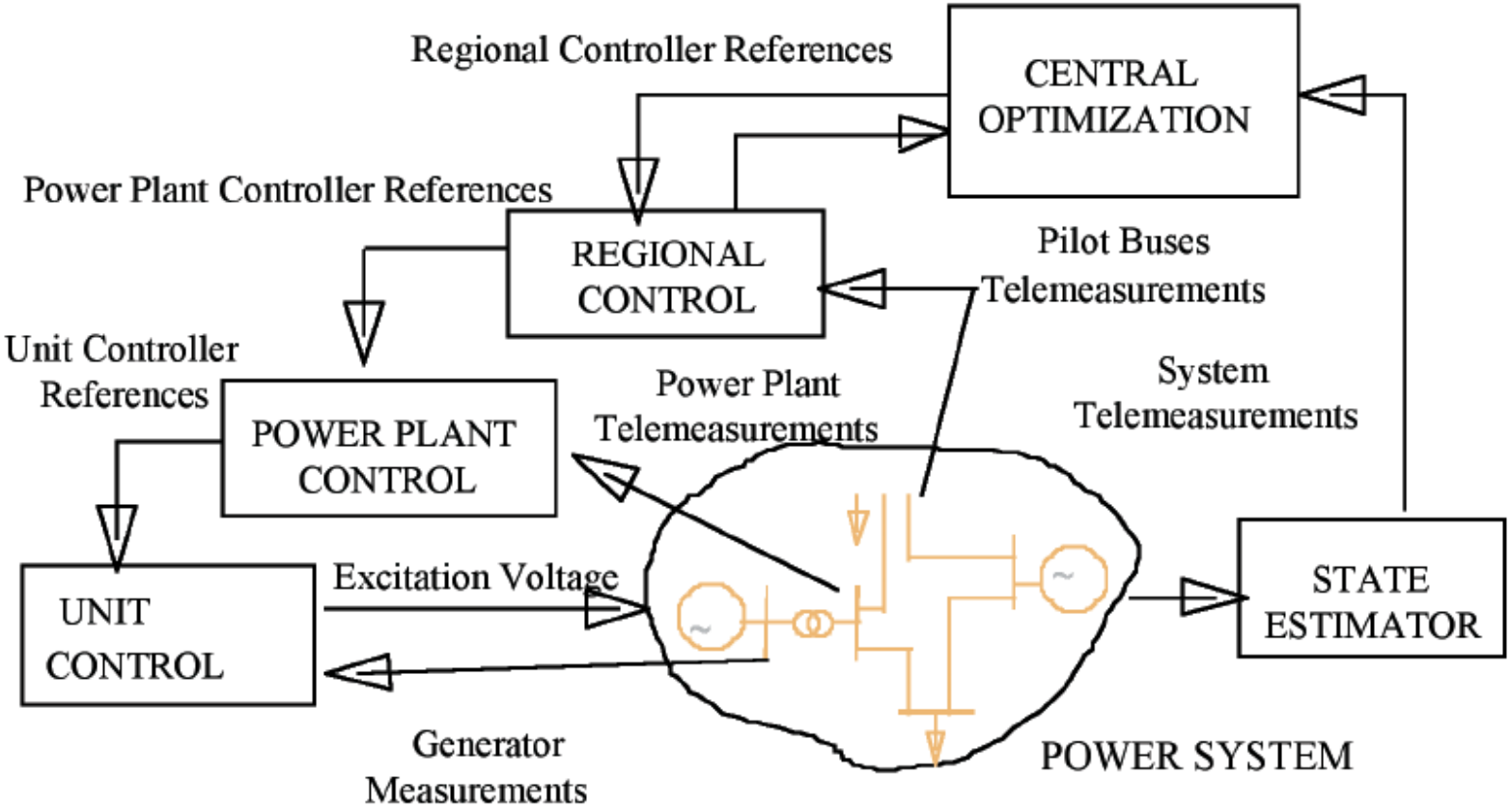


Detailed models

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



Recent related work: Coordinated voltage control in transmission networks (CIGRE TF C4.602)



Hierarchical control structure for the coordinated regulation of the transmission network voltages

- Provides an overview of the current analysis methods and practices on the coordinated transmission network voltage control, showing that its four hierarchical levels appear explicitly in the different operational practices.
- The expected performances at the different levels are specified in terms of dynamics, operation quality and system security, emphasizing aspects that seem to be technically more advanced, or original. As the automation level varies among the various existing projects (in some cases also the manual control is included), the degree of system security, reliability and quality of operation will differ accordingly.

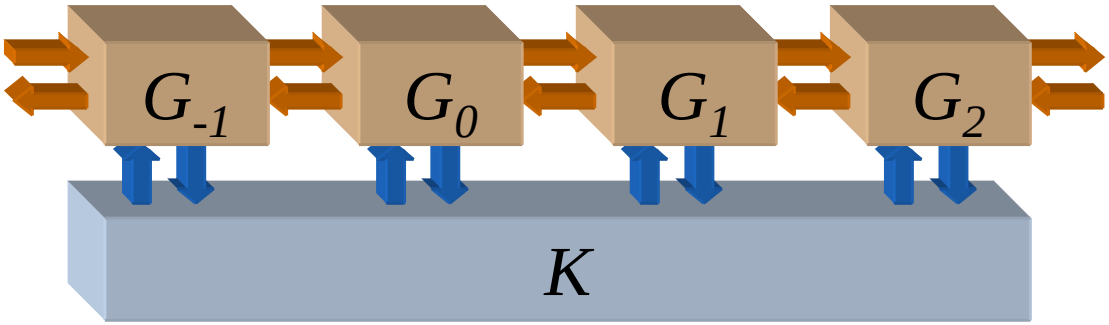
Coordinated voltage control in transmission networks (CIGRE TF C4.602):

Several area of research and advanced engineering projects, to improve the coordinated voltage control of transmission networks are described in broad lines along with the related software/hardware requirements for power system and equipment monitoring, operator support decision systems, implementation aspects of tertiary level control, link between coordinated voltage control and wide area protection, etc.

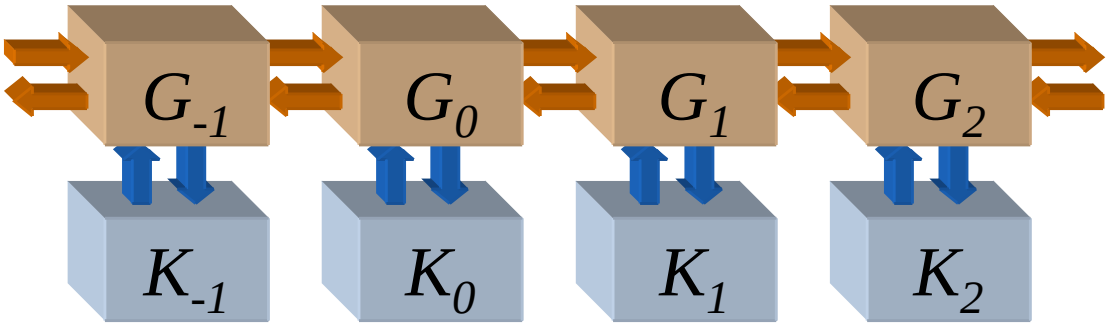
Application plan of the hierarchical Secondary Voltage Regulation in the Italian grid.

Control Strategies

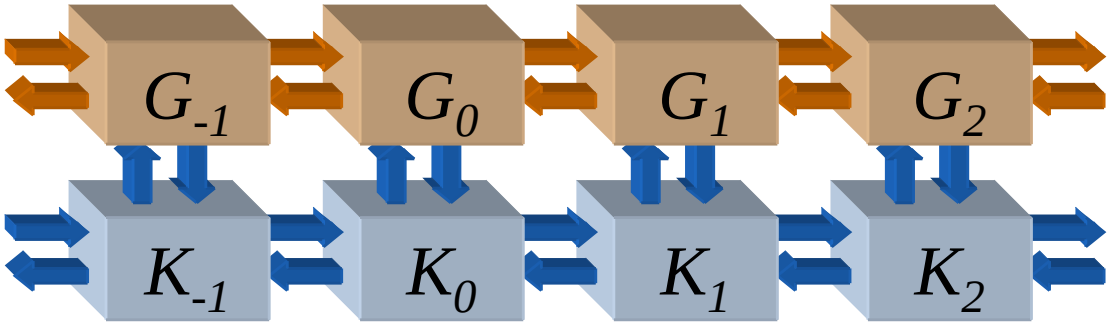
- Centralized



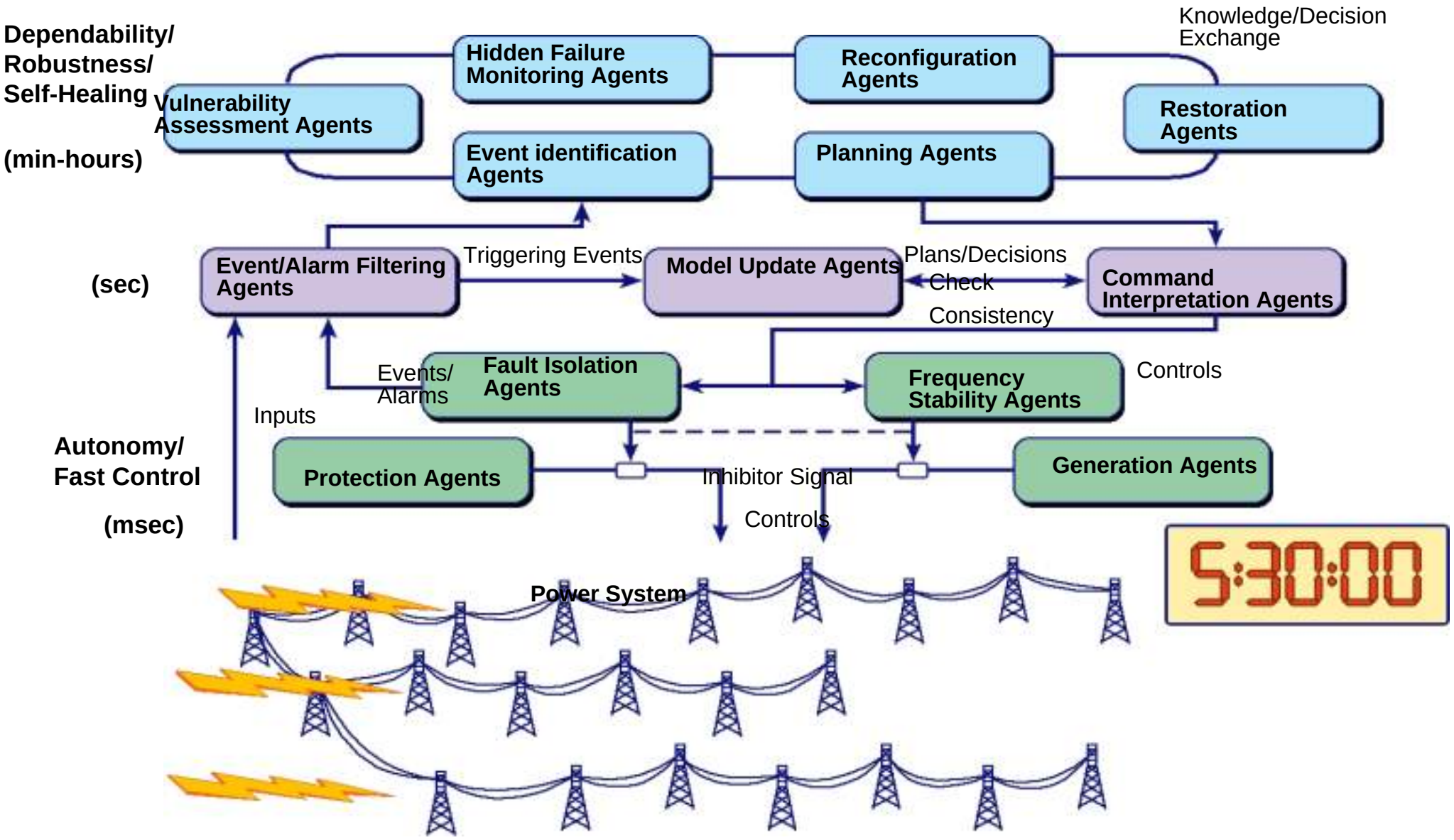
- Perfectly decentralized



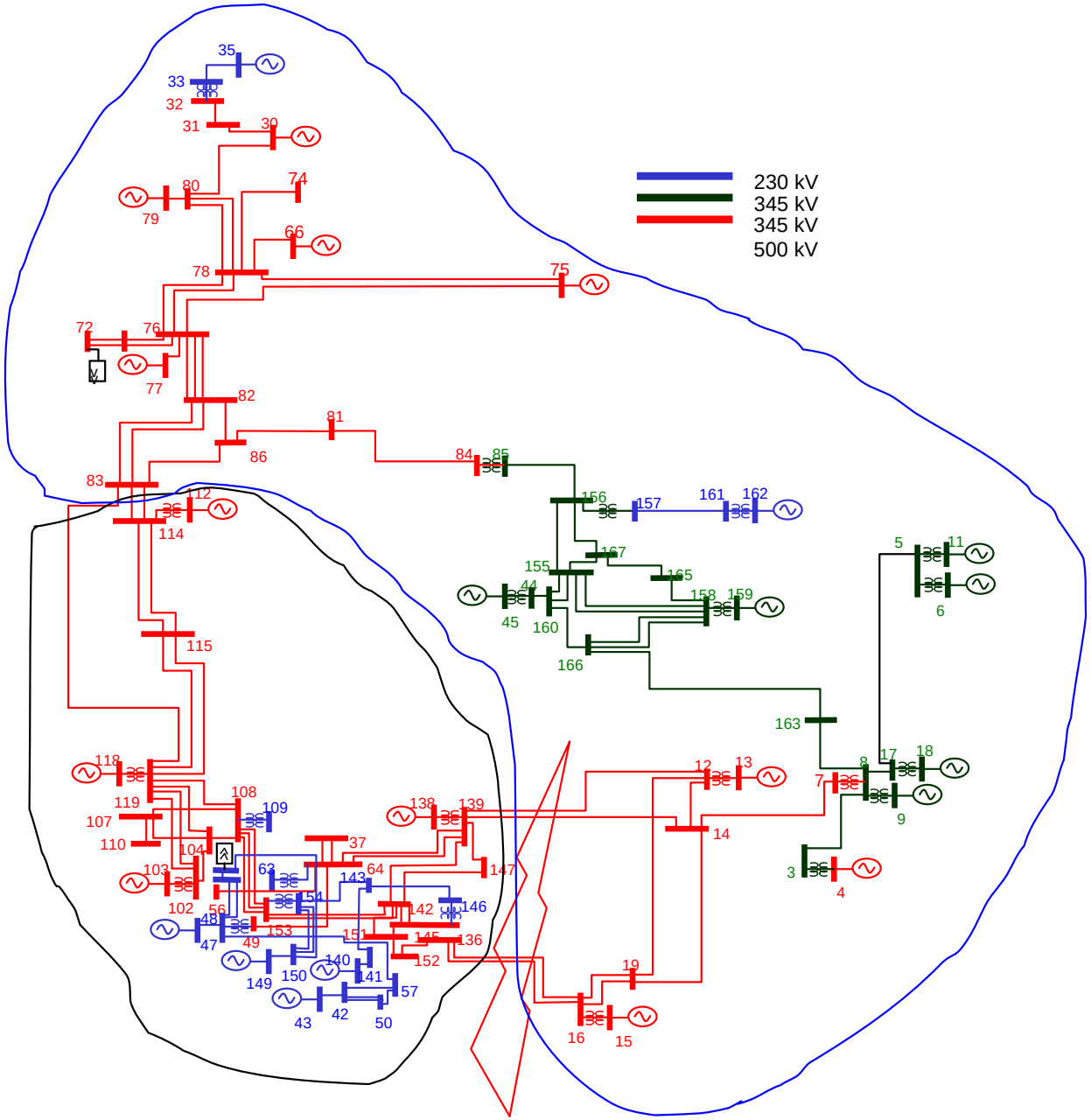
- Distributed



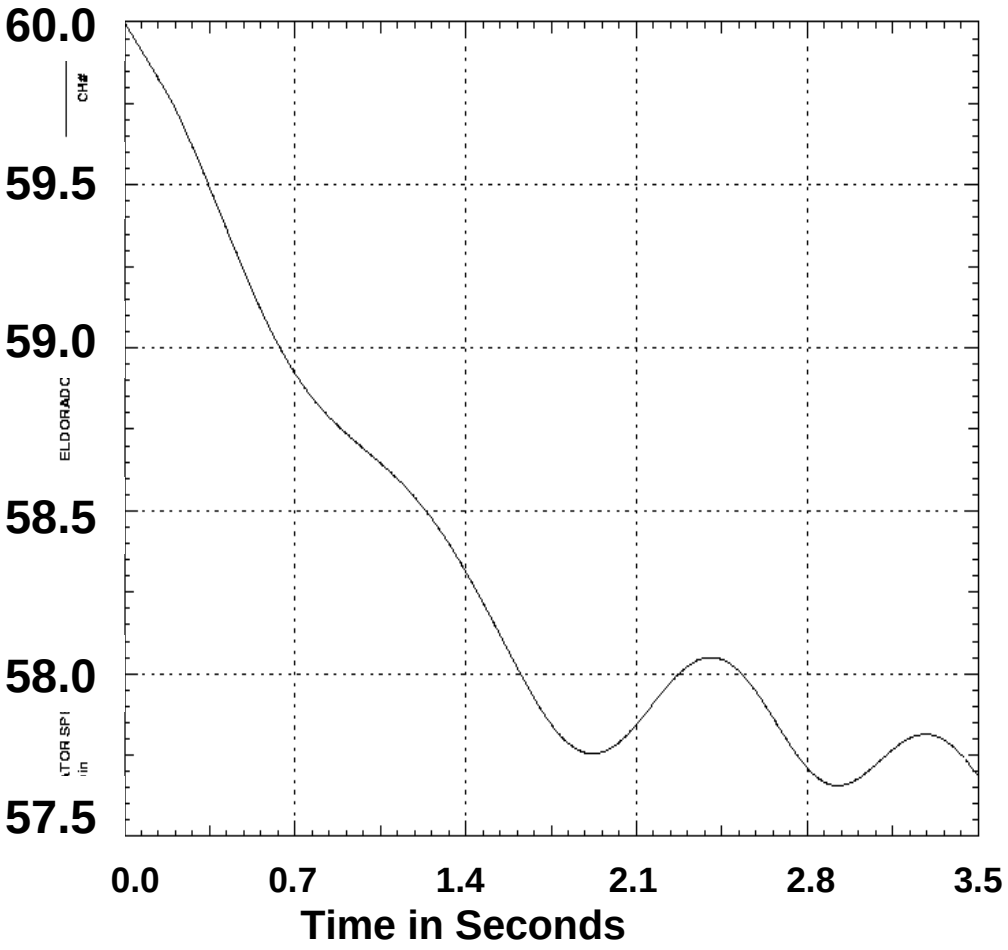
The Self-Healing Grid

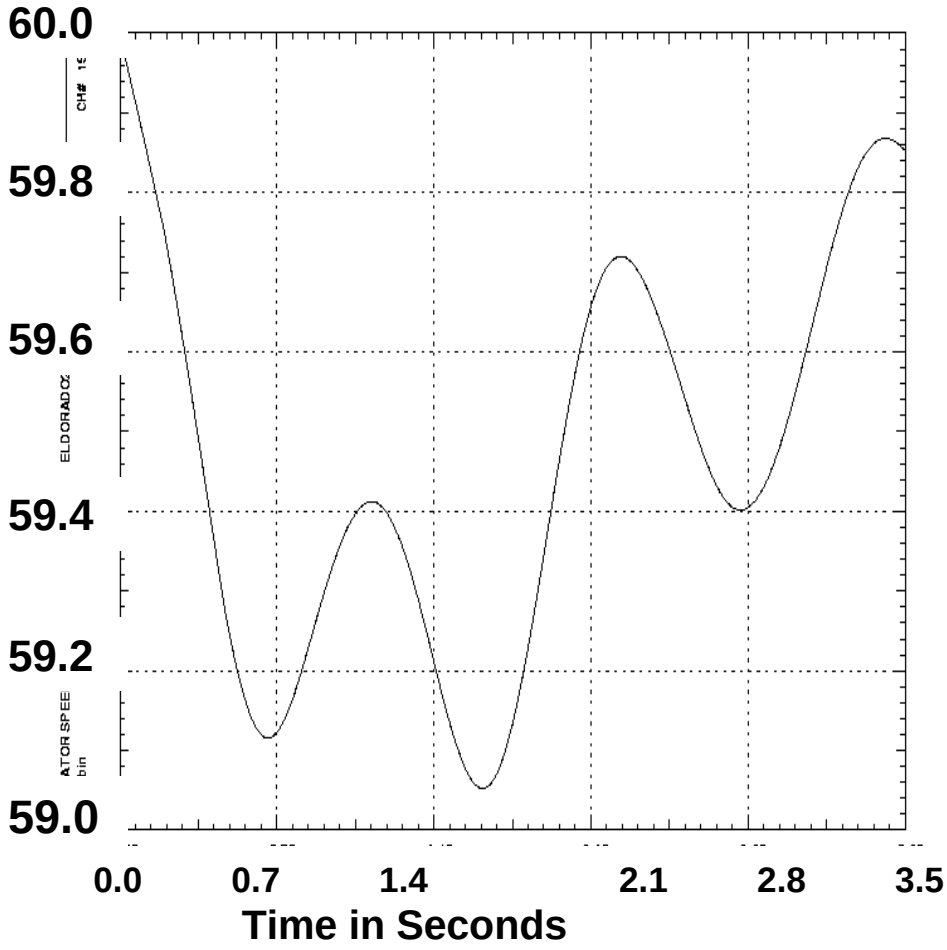


Islanding by Slow Coherency



Background: Simulation Result

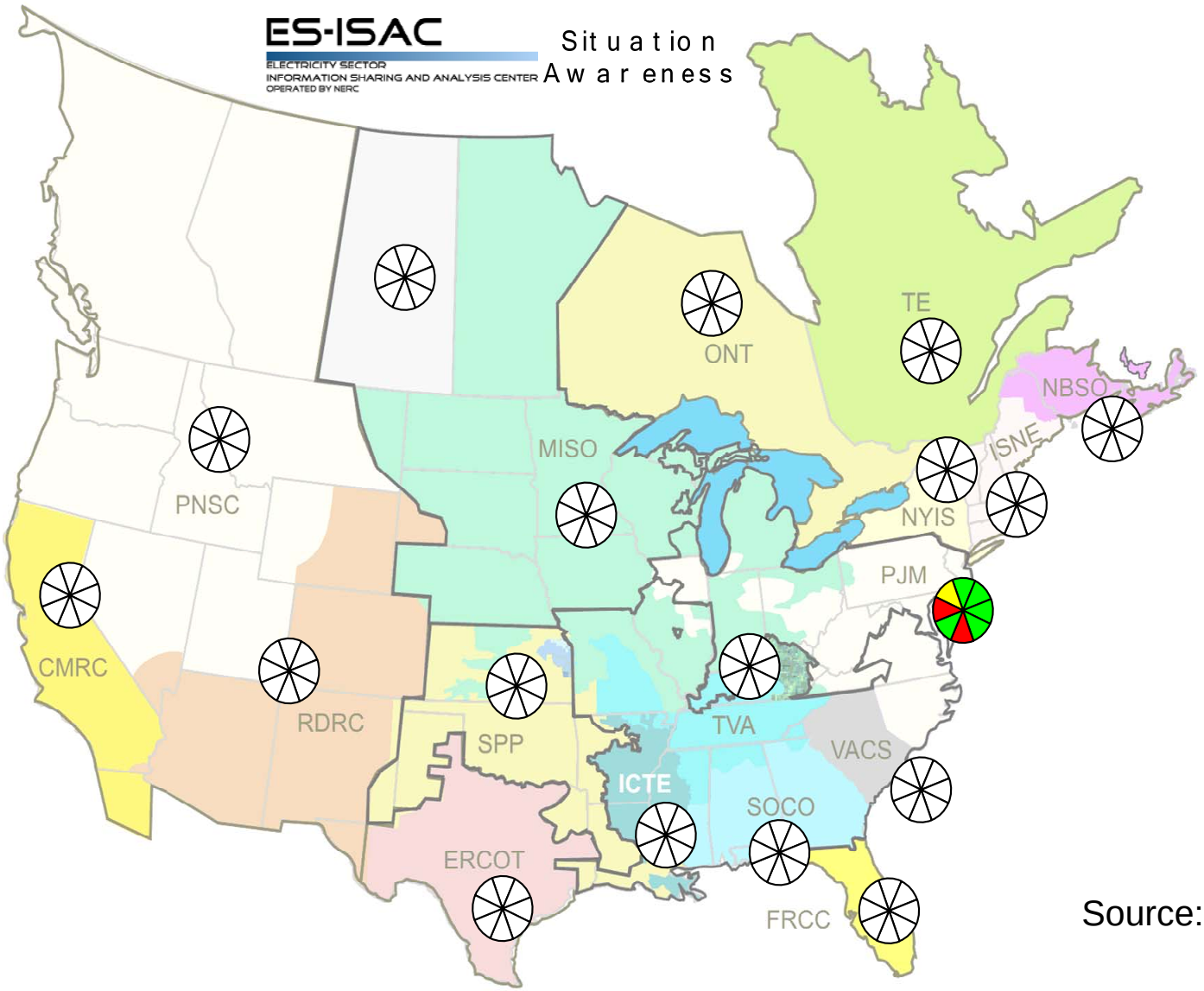




No Load Shedding Scheme

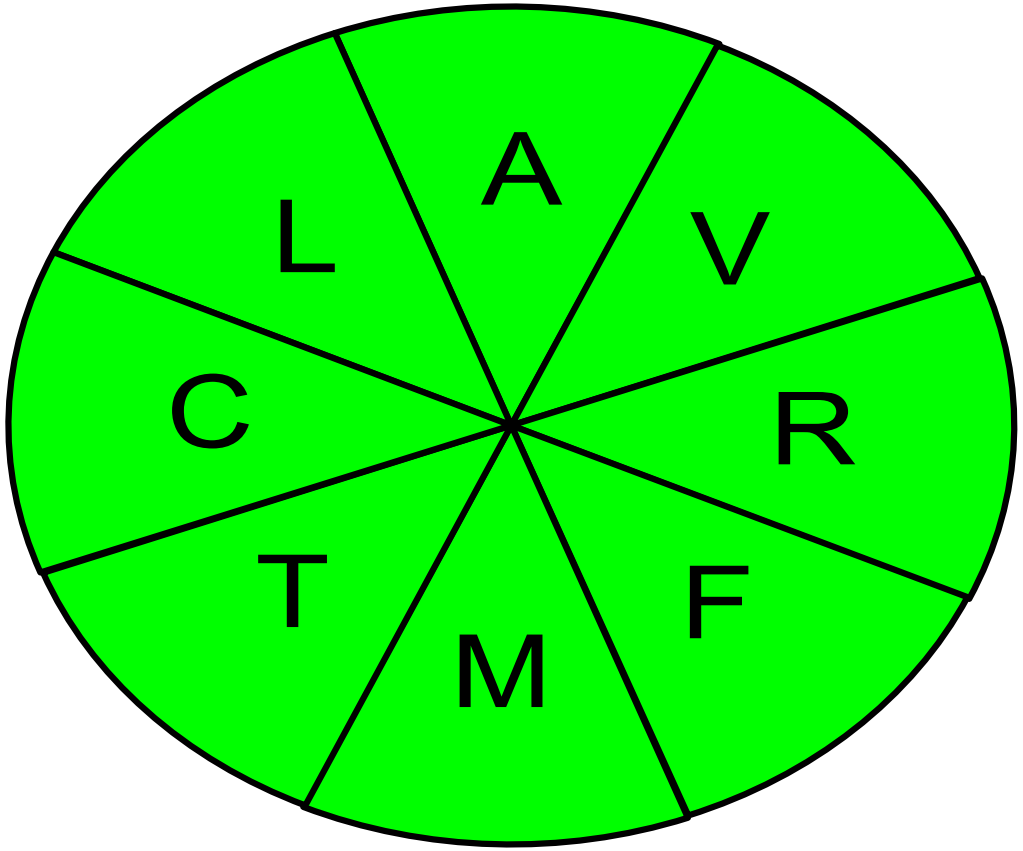
New Scheme

Situation Awareness Tool (SAT)



Source: NERC

Situation Awareness Tool (SAT)



No "Telemetry" Data

Data Value Nominal

Data Value Approaching Warning

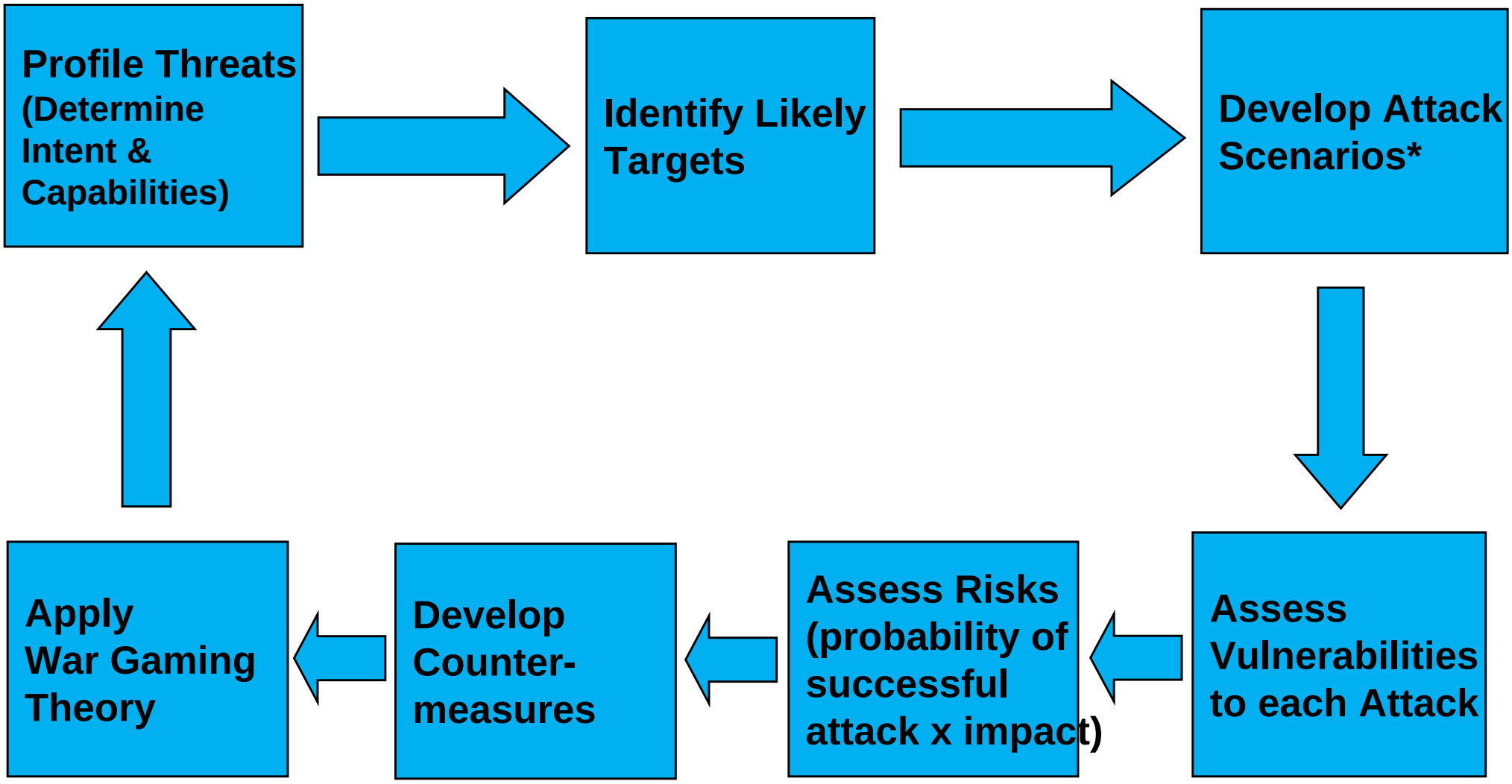
Data Value in Warning Range

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

What can be Done?
Vulnerability Assessment



*Evolving spectra of targets and modes of attack

Selected References

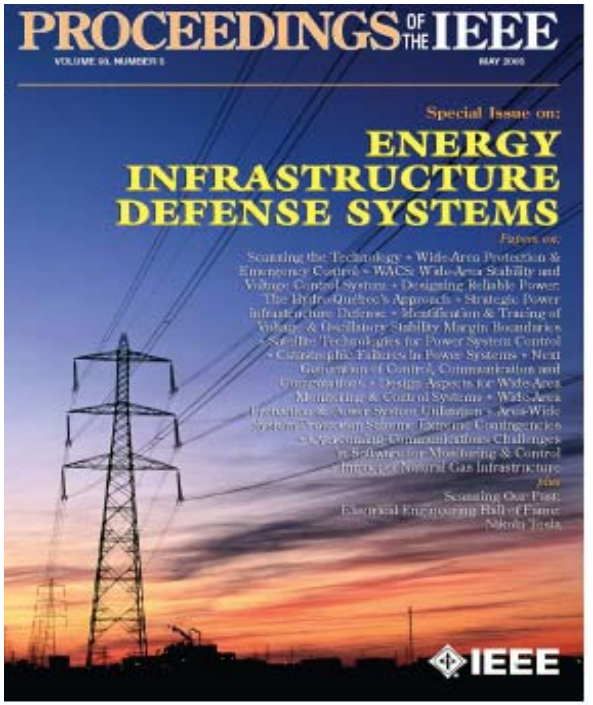
- **"New Directions in Understanding Systemic Risk",** with NAS and FRBNY Committee, National Academy of Sciences and Federal Reserve Bank of NY, Mar. 2007
- **"Complex Interactive Networks/Systems Initiative (CIN/SI): Final Summary Report",** Overview and Summary Final Report for Joint EPRI and U.S. Department of Defense University Research Initiative, EPRI, 155 pp., Mar. 2004
- **"Preventing Blackouts",** Scientific American, pp. 60-67, May 2007
- 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

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

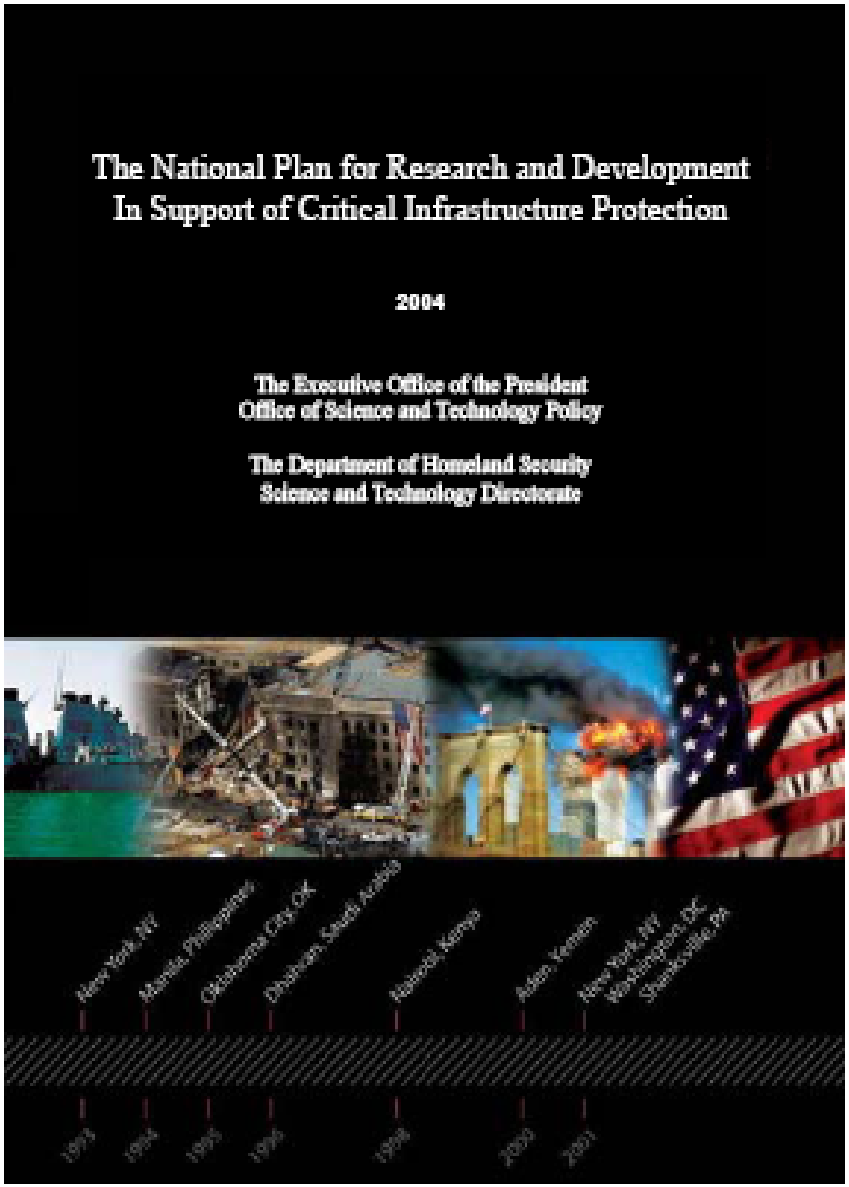
For the NAS book and complete FRBNY report please see:
Economic Policy Review, Federal reserve Bank of New York, Vol. 13, Number 2, Nov. 2007
New Directions for Understanding Systemic Risk, 108 pp, Nat'l Acad. Press, Washington DC, 2007

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 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.



THE NATIONAL PLAN FOR RESEARCH AND DEVELOPMENT IN SUPPORT OF CIP

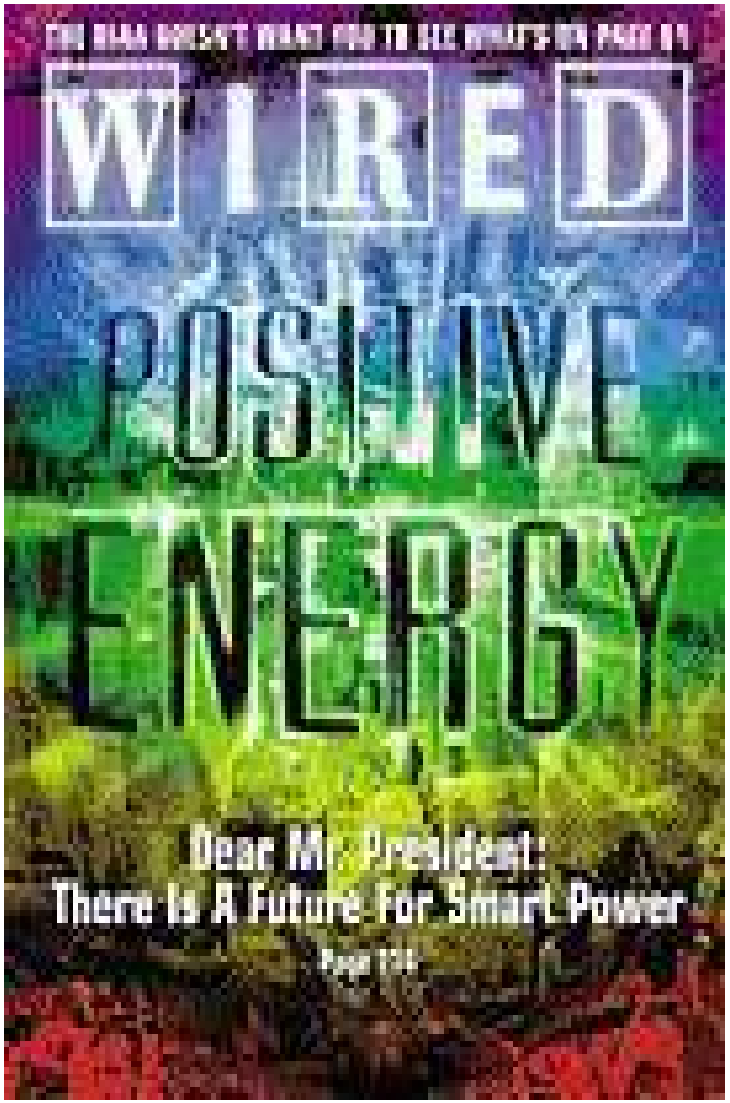
- The area of self-healing infrastructure has been recommended by the White House Office of Science and Technology Policy (OSTP) and the U.S. Department of Homeland Security (DHS) as one of three thrust areas for the National Plan for research and development in support of Critical Infrastructure Protection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



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

Smart Grid...

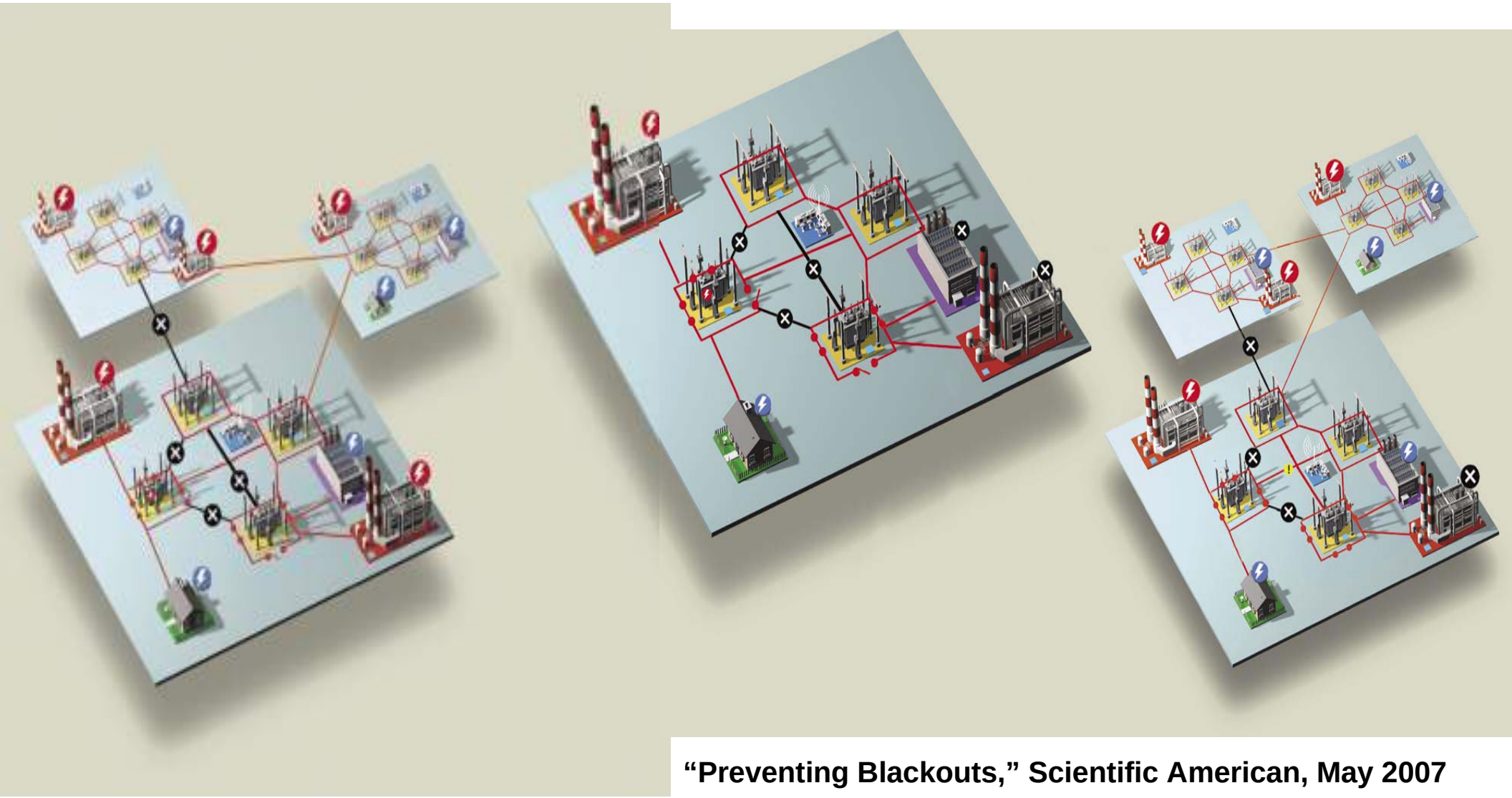
"The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming - and interconnected with everything else."



-- **The Energy Web,** Wired Magazine, July 2001

http://www.wired.com/wired/archive/9.07/juice.html

Smart Self-Healing Grid



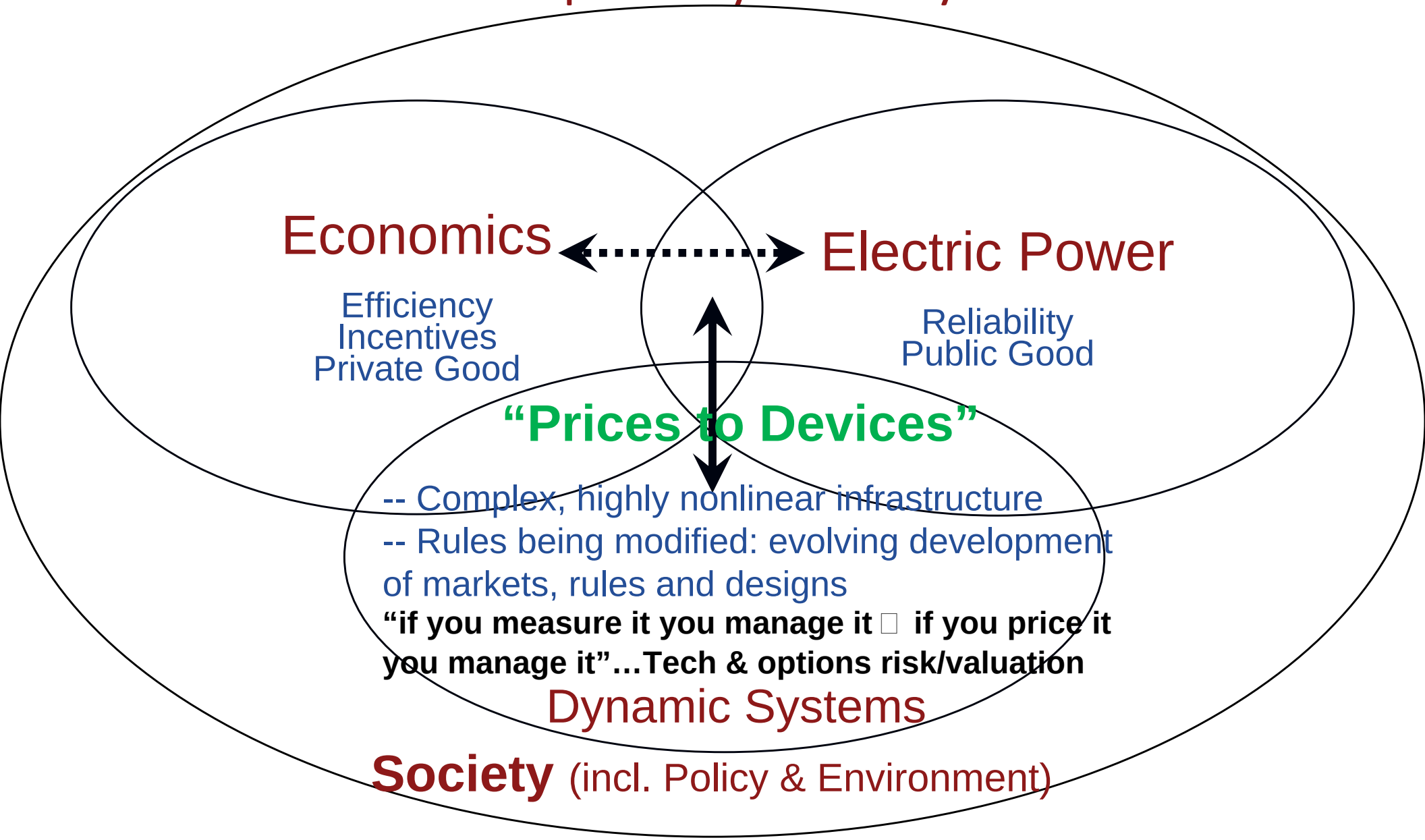
"Preventing Blackouts," Scientific American, May 2007

- "***Wind power could blow electric grid:*** Utilities and developers are poised to more than quadruple the amount of wind power in the Northwest, but a study shows the electric grid might not be able to handle it all, *The Oregonian* reported. The federal Bonneville Power Administration said in its assessment it has space on the grid to add only one-third of the planned 4,716 megawatts without additional power lines, the newspaper reported. A total of 6,000 megawatts of wind would supply about 8% of the Northwest's electricity needs, according to the BPA report. "A resource isn't very valuable unless you can deliver it," Elliot Mainzer, a transmission manager with the power agency, told *The Oregonian*. Bringing lines from the current grid to new wind farms costs up to $3 million a mile…"

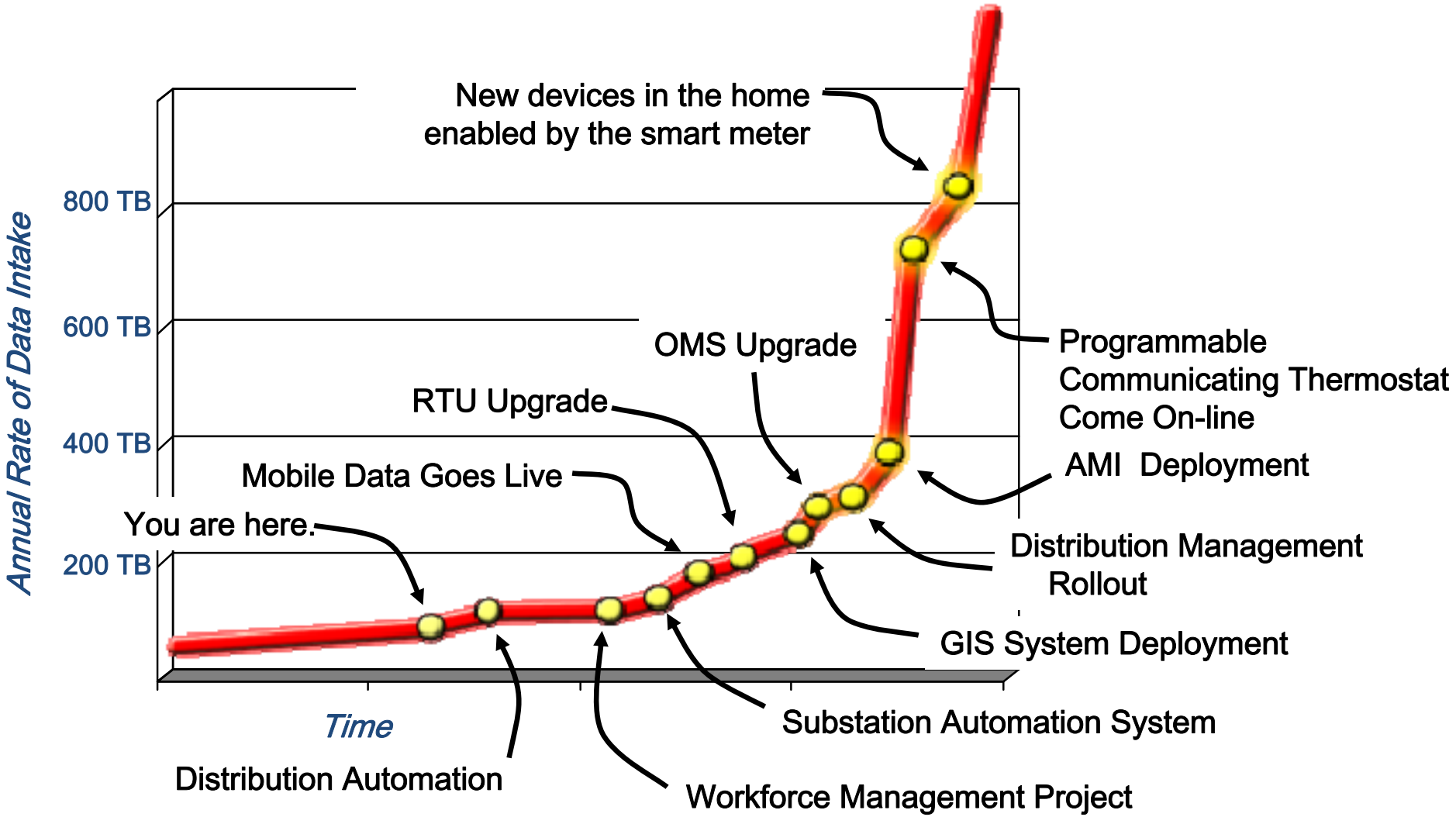
(July 22, 2008)

- ***"GM, utilities team up on electric cars:*** Partnership aims to tackle issues that will crop up when electric vehicles are rolled out… General Motors Corp. has joined with more than 30 utility companies across the U.S. to help work out electricity issues that will crop up when it rolls out new electric vehicles in a little more than two years."

Economics, Efficiency, Environment, Energy Infrastructure, Communications & Adaptive Dynamic Systems

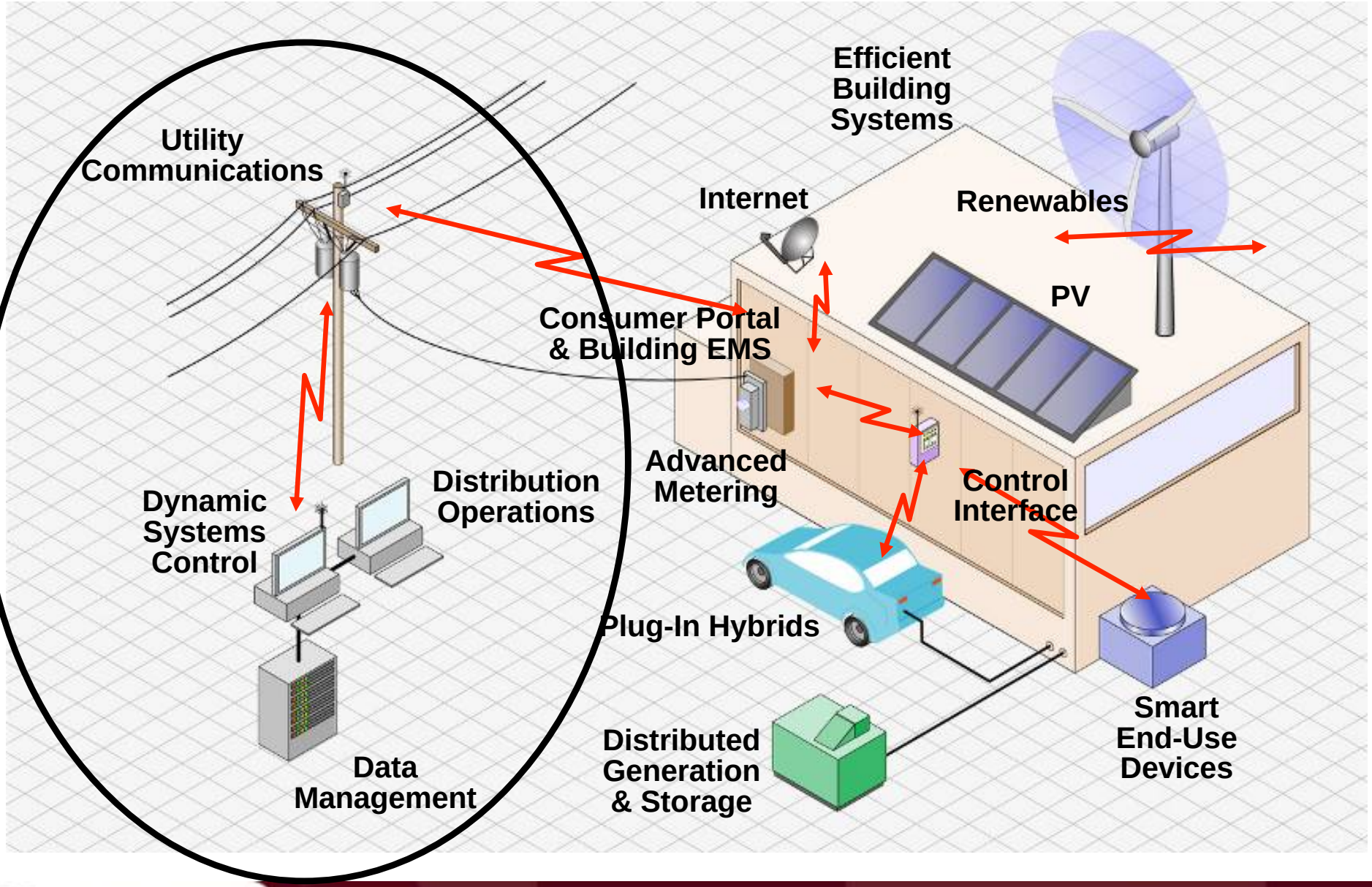


Smart Grid Field Data

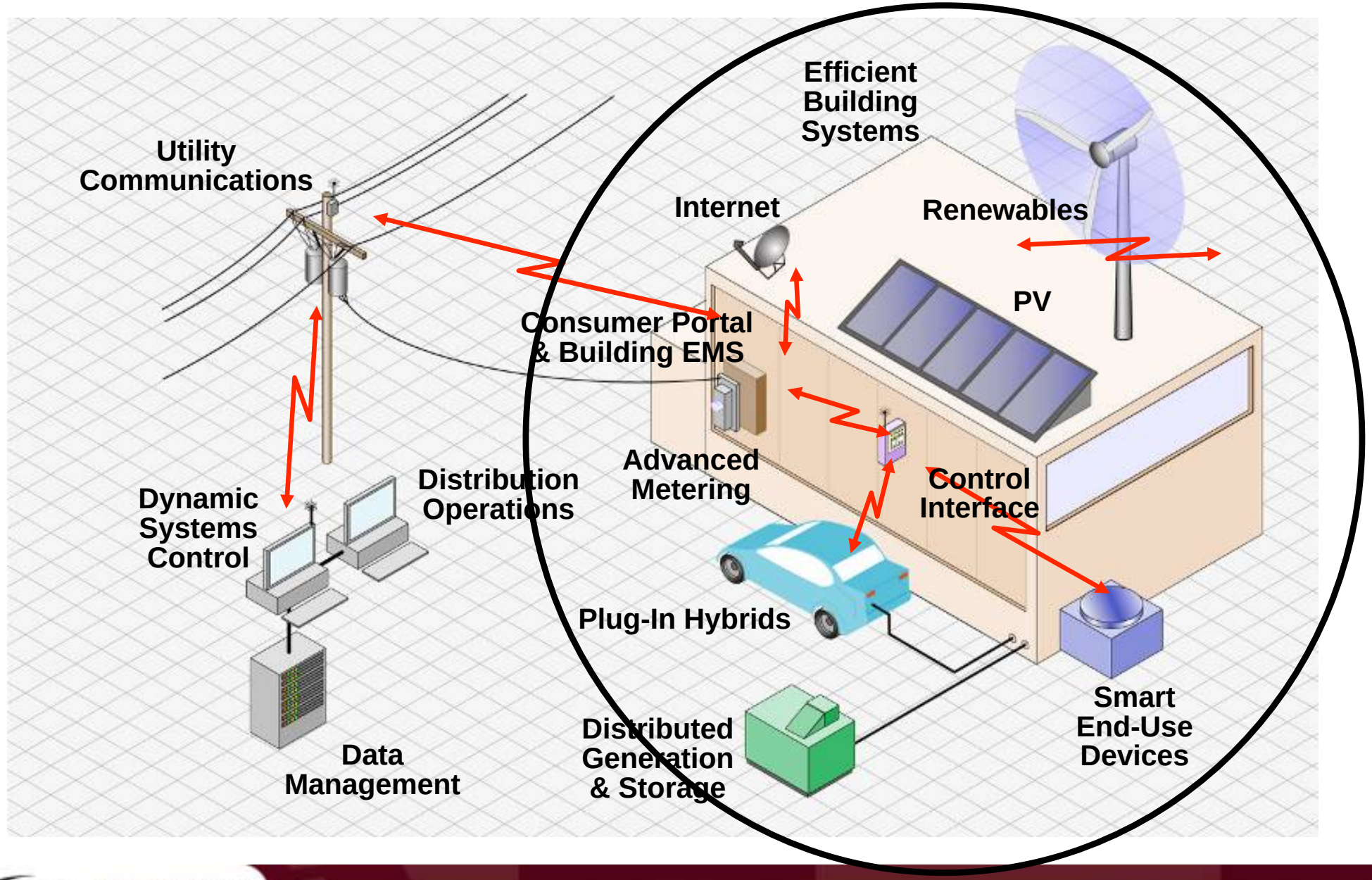


Tremendous amount of data coming from the field in the near future
- paradigm shift for how utilities operate and maintain the grid

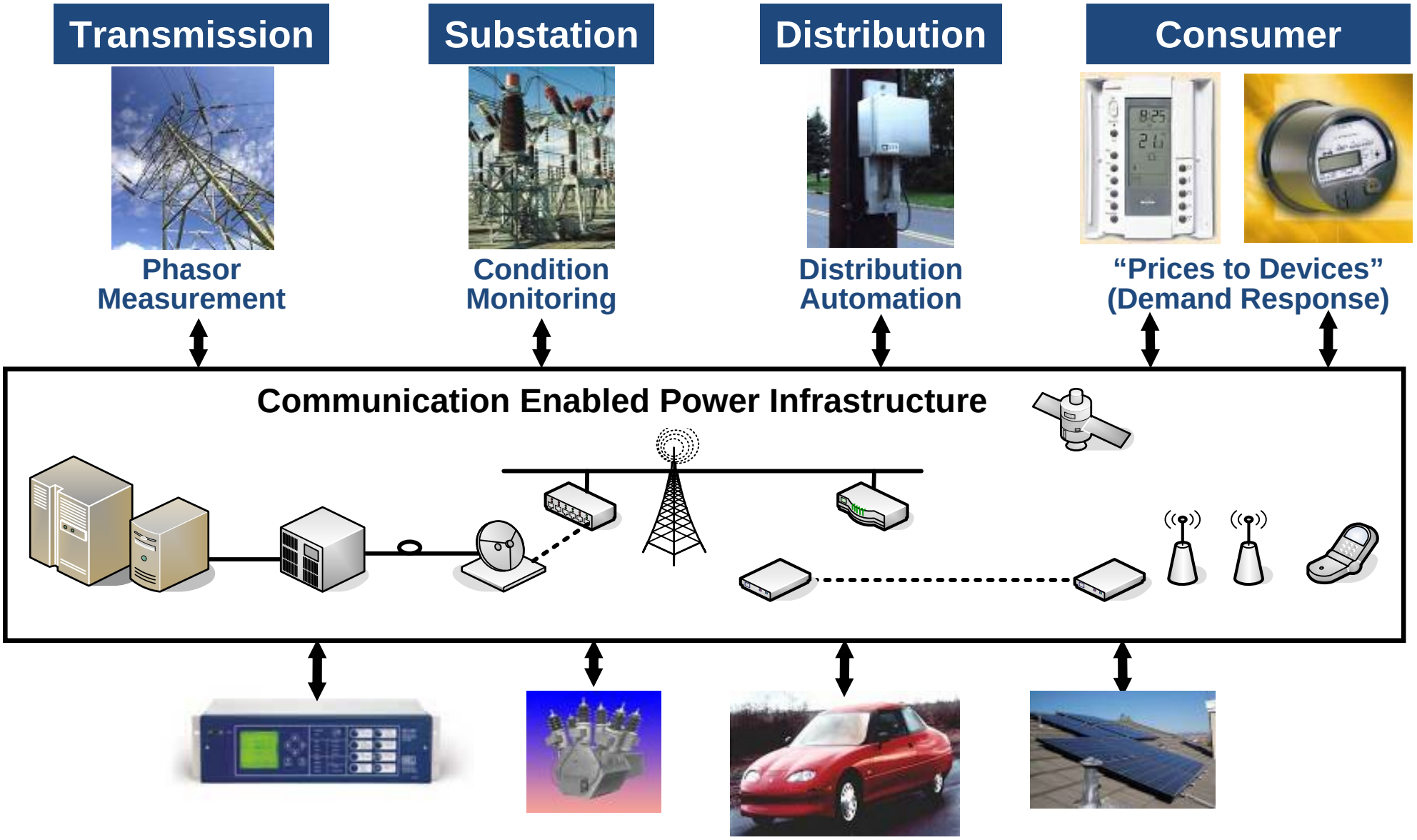
Smart Grids and Local Energy Networks



Smart Grids and Local Energy Networks

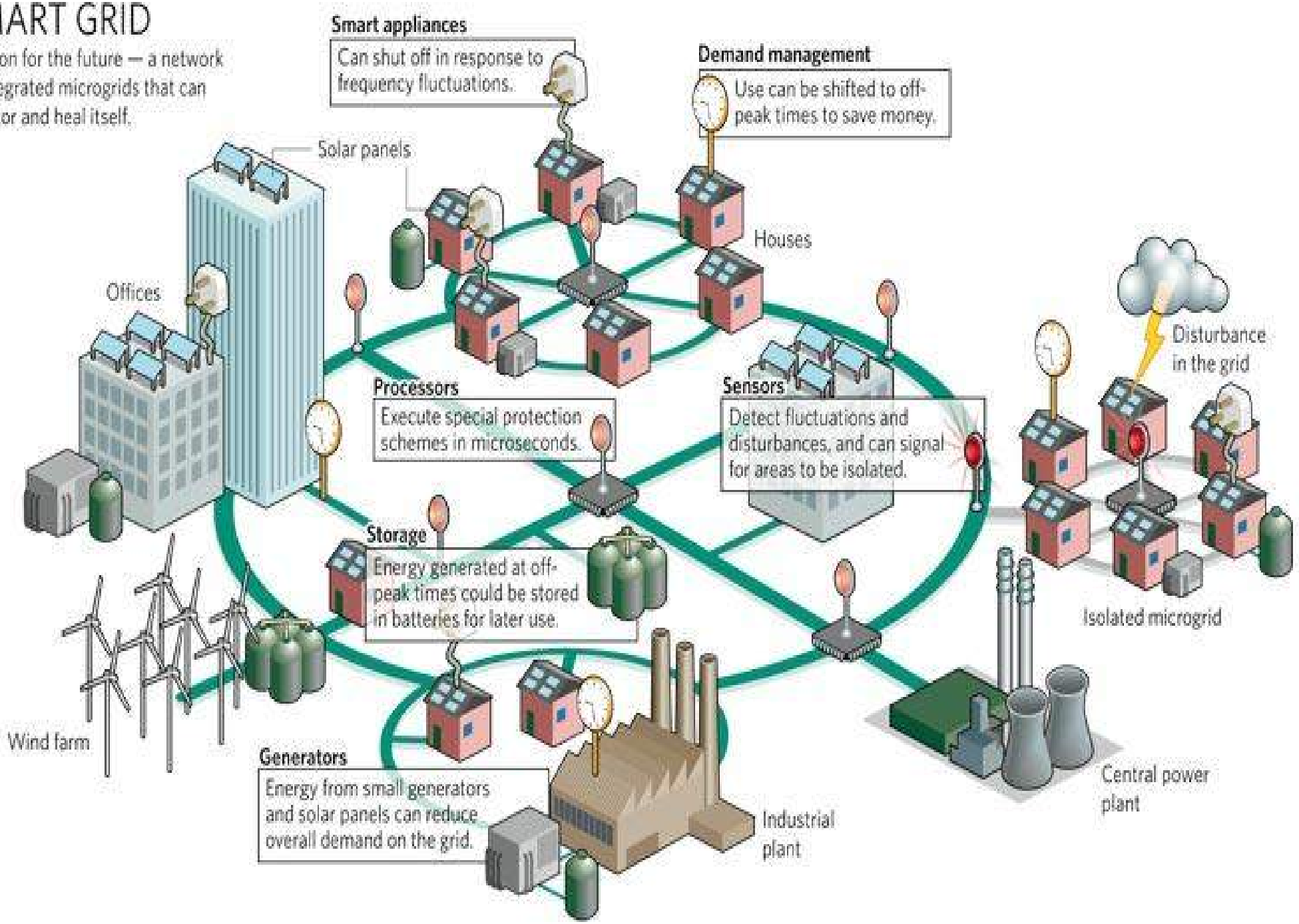


Smart Grid – Exchanging Information Seamlessly Across the Enterprise



SMART GRID

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



Related on-going R&D include

- EPRI: Intelligrid, Fast Simulation and Modeling
- Initiatives at several utilities, including Xcel, AEP, Austin Energy, ISOs, etc.)

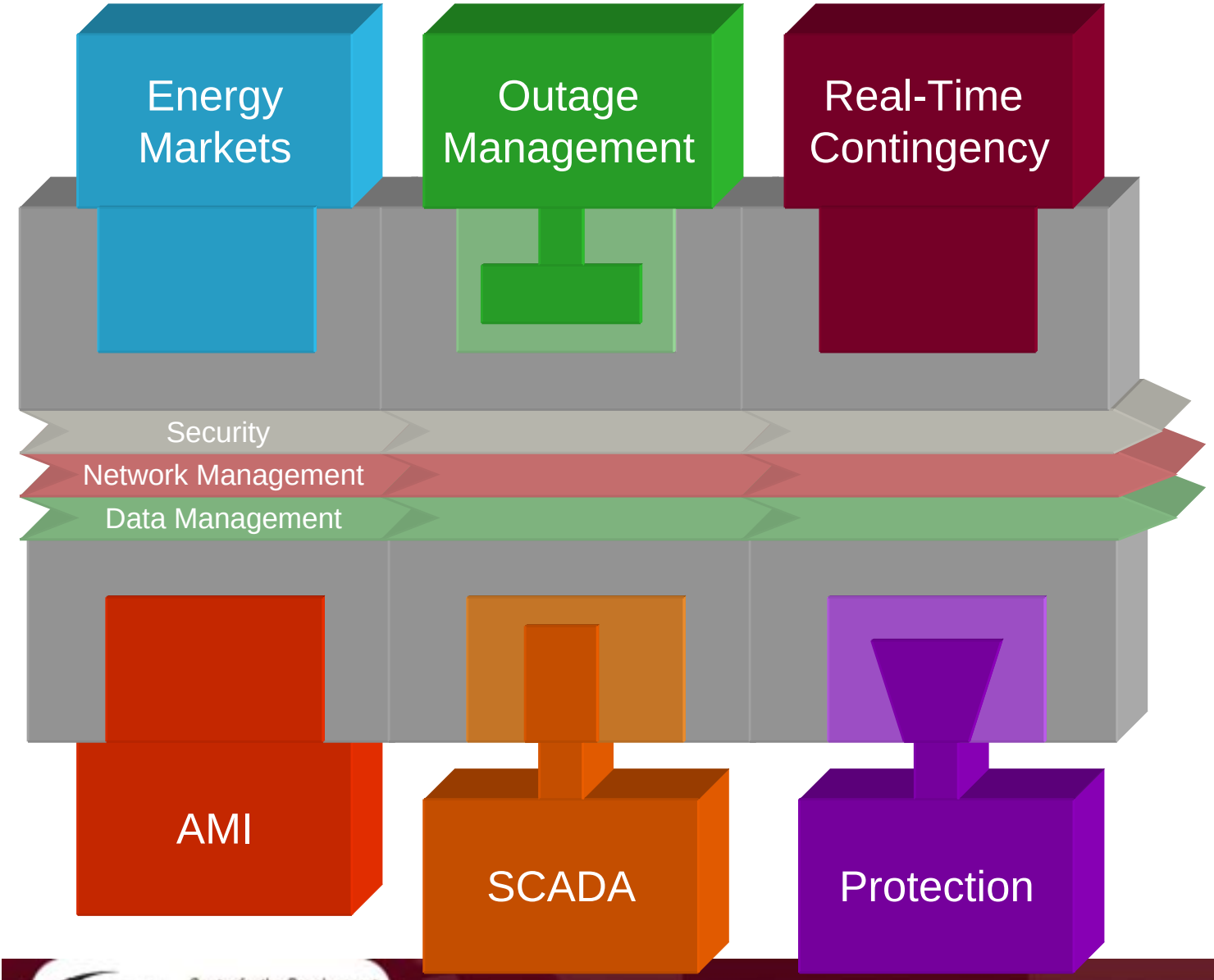
- Energy Bill passed in December 2007: Title XIII Smart Grid, Sections 1301 -1309
  - Establishes a statement of policy supporting modernization of the grid; authorizes a biennial status report and survey of barriers to modernization
- US Department of Energy: Gridwise and Modern Grid Initiatives

- University of Minnesota Center for Smart Grid Technologies

- Smart Grid Newsletter

Smart Grid: Enabling Multiple Applications

First Build the Right Foundation



Build The Right Foundation

Security

Network Management

Data Management

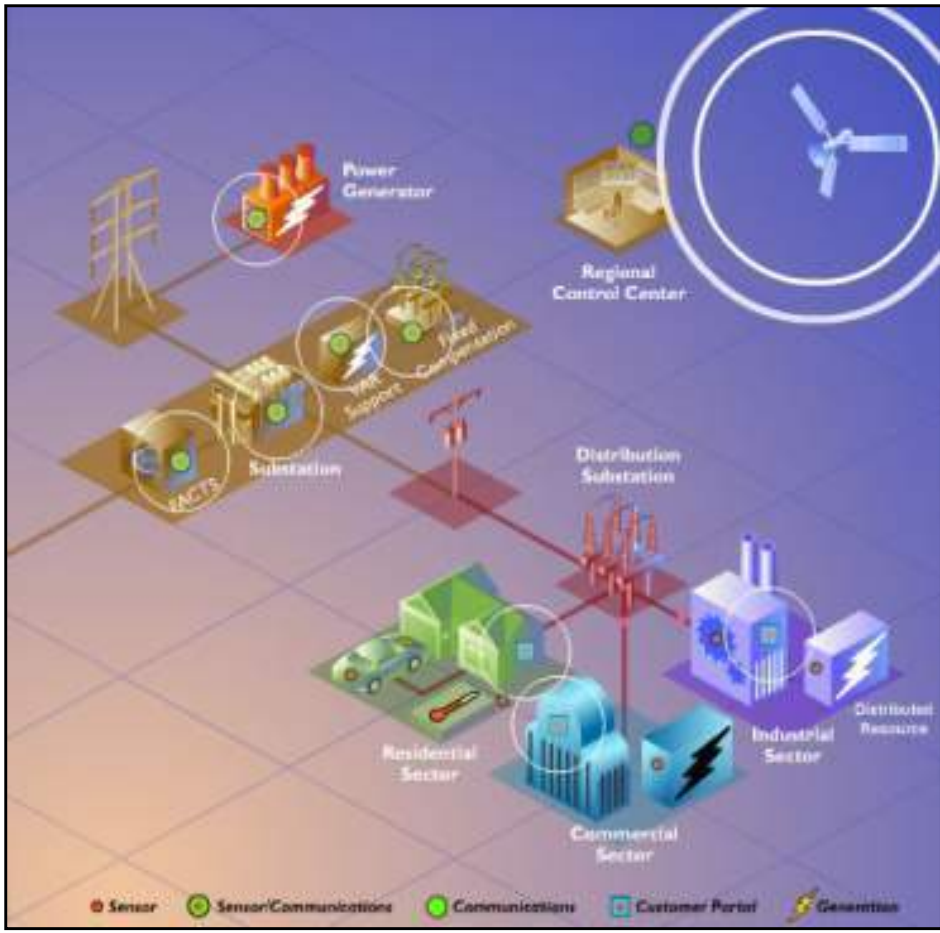
Interoperability

Key Technologies

- Communications
- Monitoring
- Embedded computing
  - Data to information, advanced operation & protection algorithms, etc.
- Advanced components
  - Superconductors, power electronics, storage, etc.
- Advanced configurations
  - Looped circuits, microgrids, DC service

Tomorrow's Grid

- **Smart**
  - with sensors
- **Flexible and Resilient**
  - an intelligent network with real-time monitoring and control
- **Self Healing and Secure**
  - capable of predicting or immediately containing outages with adaptive islanding and fast isolation or sectionalizing
- **Established Standards**
  - enabling "plug and play" distributed resources, integrated renewables, with digital appliances and devices



Strategic R&D challenges

- 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.
- Integrated 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).
  - Infrastructure databases, data mining and early signature detection

Challenges

- Management of Precursors and their Signatures (Identifying & Measuring Precursors), including DDRs, WAMS…
- Fast look-ahead simulation and modeling capability
- Adaptive and Emergency Control; 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)
  - …

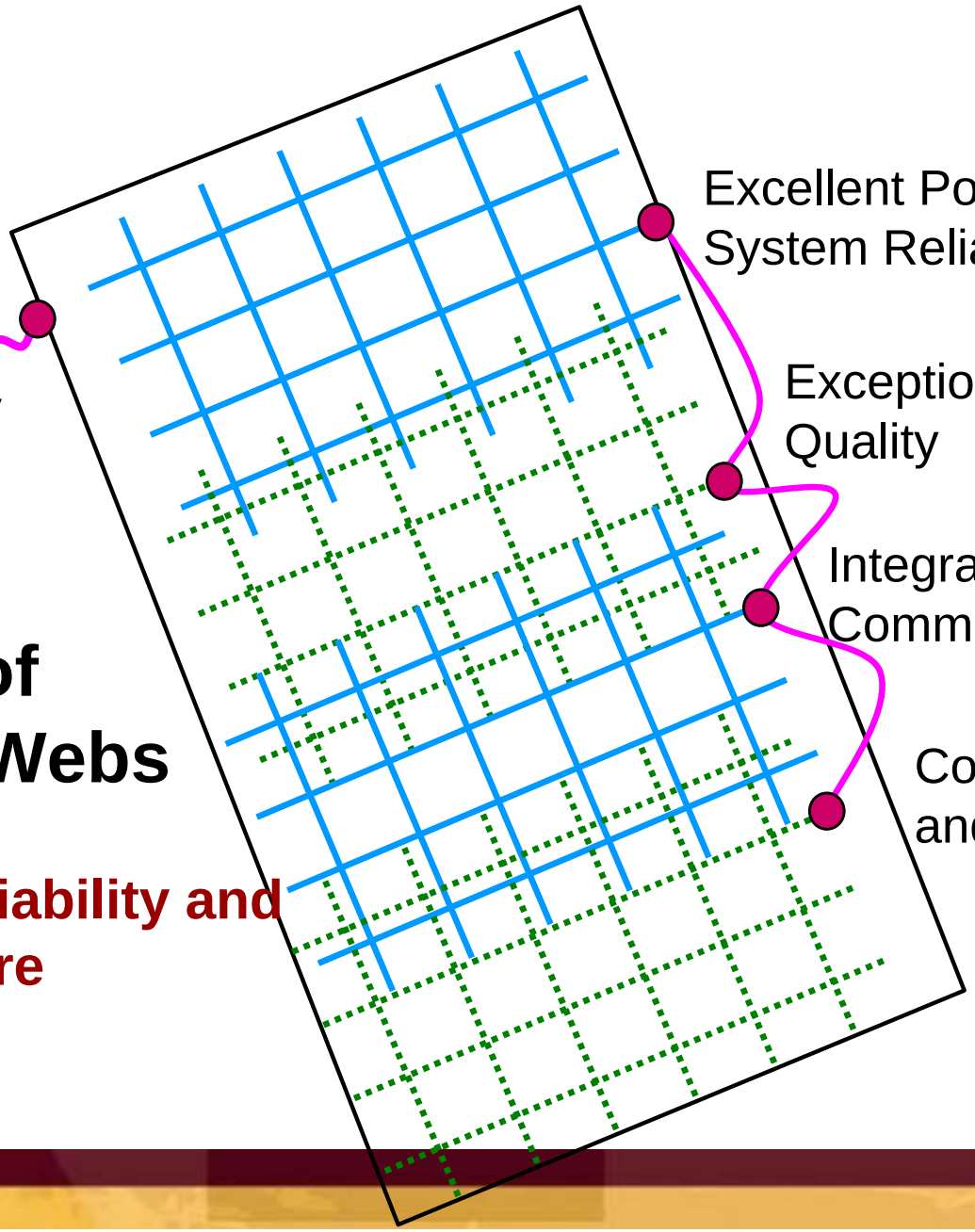
Longer term

- Near-Term: focus on the most promising technologies for testing with real data and further development; e.g.:
  - Distributed computation and sensing, including intelligent Adaptive Islanding Schemes for a larger regional system
  - Systems' approach: Provide a greater understanding of how integrating a sensor network, advanced communications and controls, power electronics, DR, and other technologies might fit into the continental grid, as well as guidance for their effective deployment and operation:
    - *In Vivo* vs. *In Silico* simulation testing of devices in the context of the whole system-- the grid, markets, communication and protection system overlays.
    - Supercomputing applications: Use parallel computation to speed up security assessment, system estimation and control of wide-area power grids: e.g. the 11 Western States (WECC), Texas (ERCOT), the Eastern Interconnection, or the North American interconnection.

Transformative Innovations

- Digital Control of the Energy Infrastructure (Reliability, Robustness, Resilience & Security)
- Integrated energy, information and communications for the user.
- Transformation of the meter into a two-way energy/information portal.
- Integration of distributed energy resource into the network.
- Robust advanced power generation portfolio.

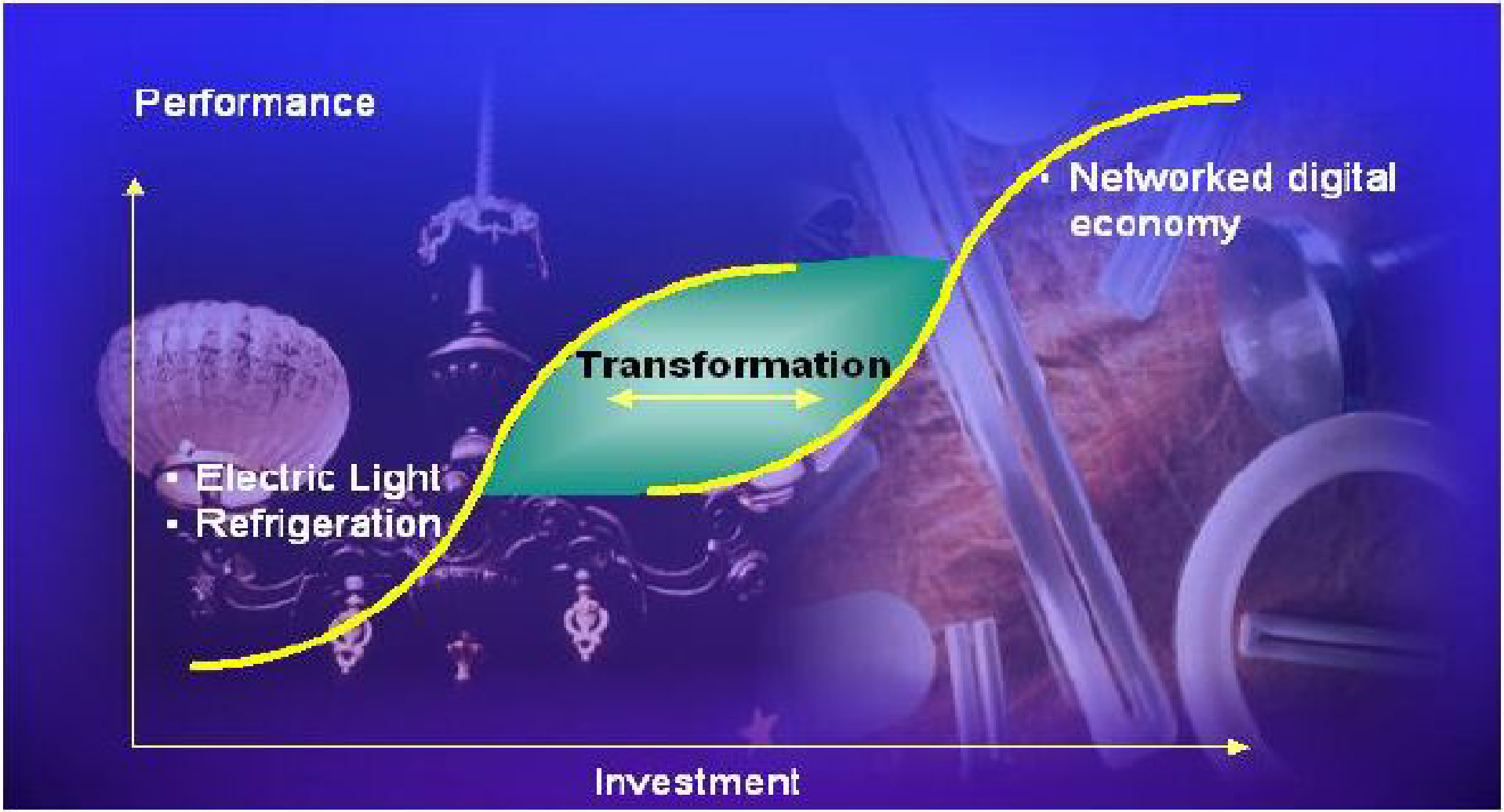
The Infrastructure for a Digital Society



A Complex Set of Interconnected Webs

Security, Quality, Reliability and Availability (SQRA) are Fundamental

Investment Required



Shaping the Future…
"Anything we can imagine, we can build"

The wealth of nations is not limited by land or minerals, it comes predominantly from "the acquired abilities of people, their education, experience, skills and health." - *Investing in people: The Economics of Population Quality, (1981)* Theodore Schultz, Economist and Nobel Laureate

- "Reversing the trend": U.S. spending in R&D accounts for 2.5% of the GDP, yet the results rippling outward from the investments in technology - and its related educational base

- University research more closely tied to the industry

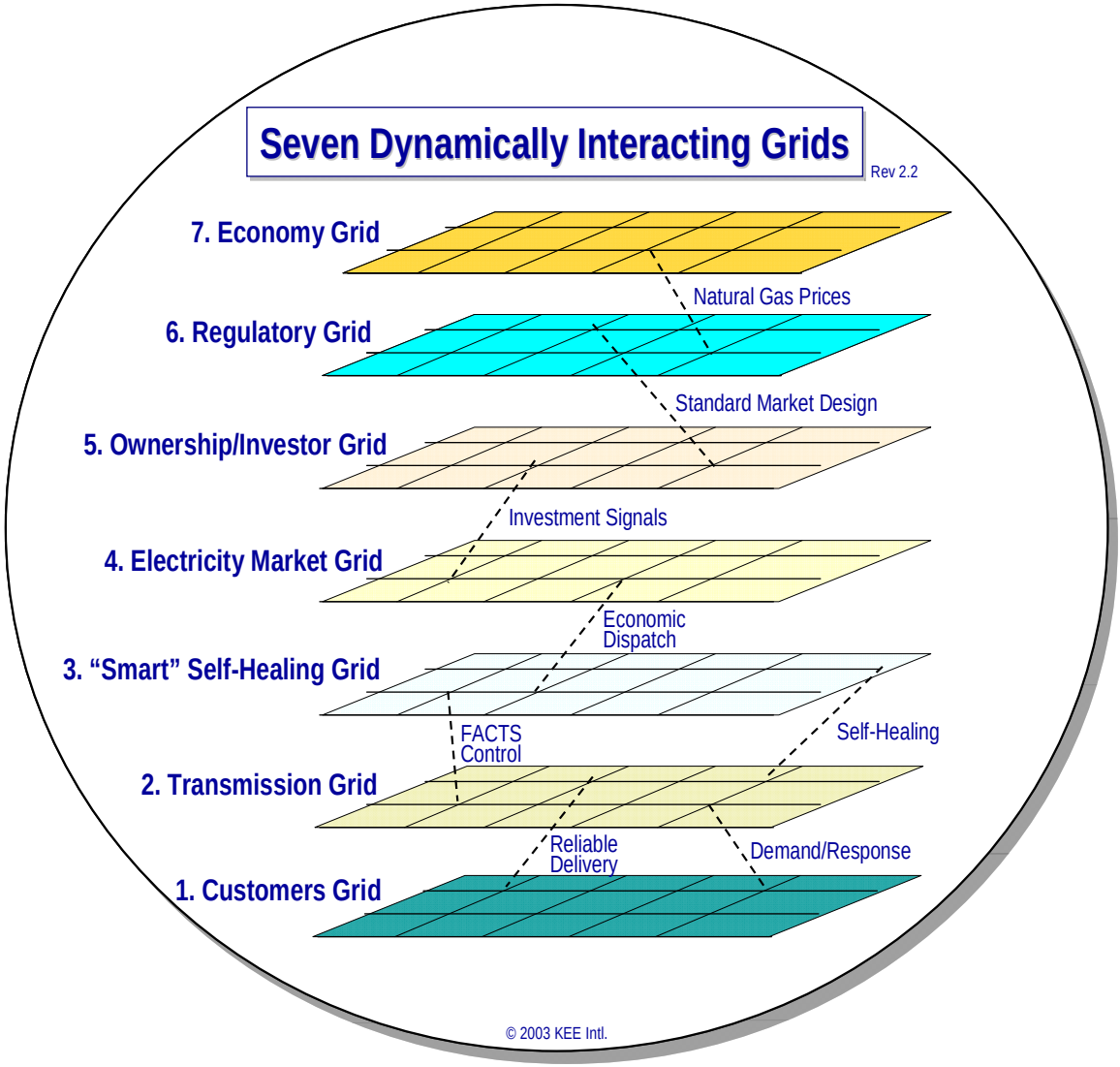
- Managing Organizational Factors and Reducing Risk

But, what do our customers really want?

And what are the societal needs?

Technology development, transition and Implementation: … the really hard part

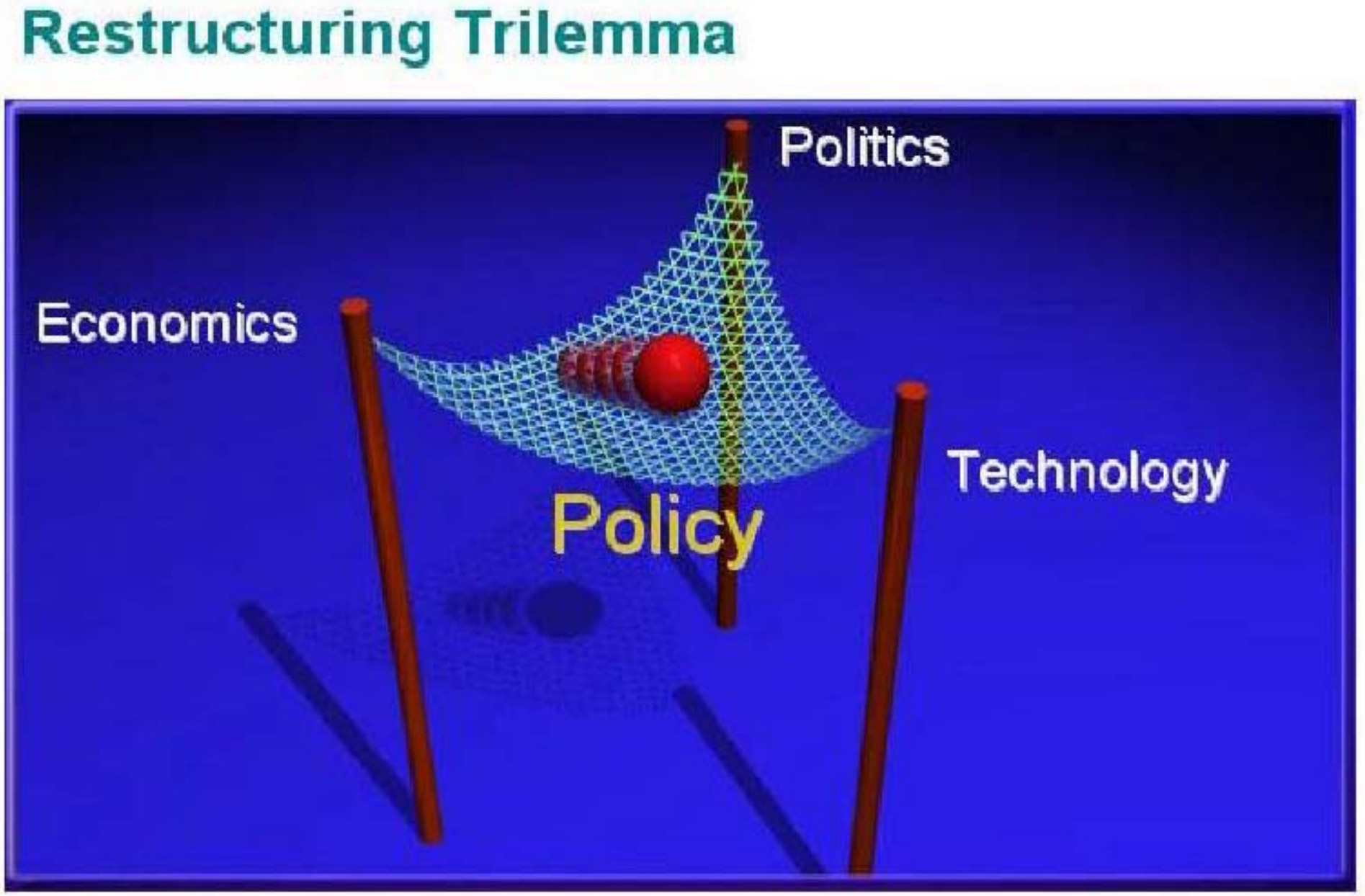
- Steps in Tech R&D and implementation
- Making the business case for the opportunity
- Have a plan …



The Challenge

Enabling/Creating a stronger, more secure, resilient, and more stable interdependent infrastructure that is vital to support the digital society

Unresolved Issues Cloud Planning for the Future



Discussion Questions

- What level of threat is the industry responsible for, and what does government need to address?
- Will market-based priorities support a strategically secure power system?
- What system architecture is most conducive to maintaining security?

Conclusions

- Utility systems are tempting targets
- Cyber attacks are very probable
- We know what we need to do to prevent & mitigate attacks
- The industry and government are working on solutions, and a lot remains to be done.
- We will be successful!


May others benefit from your lead.
Thank you

Session 3, 9:45-11:15: Increasing resilience and self-healing

- ***Selfhealing and resilient critical infrastructures***
  - **Rune Gustavsson**, Blekinge Institute of Technology (Sweden)
  - Björn Ståhl, Blekinge Institute of Technology (Sweden)
- ***Critical Infrastructures Security Modeling, Enforcement and Runtime Checking***
  - Anas Abou El Kalam, IRIT – INP (France)
  - **Yves Deswarte**, LAAS – CNRS (France)
- ***Increasing Security and Protection through Infrastructure REsilience: the INSPIREProject***
  - Salvatore D'Antonio, Consorzio Interuniversitario Nazionale per l'Informatica (Italy)
  - Abdelmajid Khelil, TU Darmstadt (Germany)
  - Luigi Romano, University of Naples "Parthenope" (Italy)
  - Neeraj Suri, TUD (Germany)
- ***Increase of power system survivability with the Decision Support Tool CRIPS based on Network Planning***
  - Christine Schwaegerl, Siemens AG (Germany)
  - Olaf Seifert, Siemens AG (Germany)
  - Robert Buschmann, IABG (Germany)
  - Hermann Dellwing, IABG (Germany)
  - **Stefan Geretshuber**, IABG (Germany)
  - Claus Leick, IABG (Germany)