# Cyber and Critical Infrastructure Security:
## Toward Smarter and More Secure Power and Energy Infrastructures


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





Canada-U.S. Workshop on Smart Grid Technologies
Thursday, March 25, 2010, 8:00 am to 12:30 pm, Vancouver


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

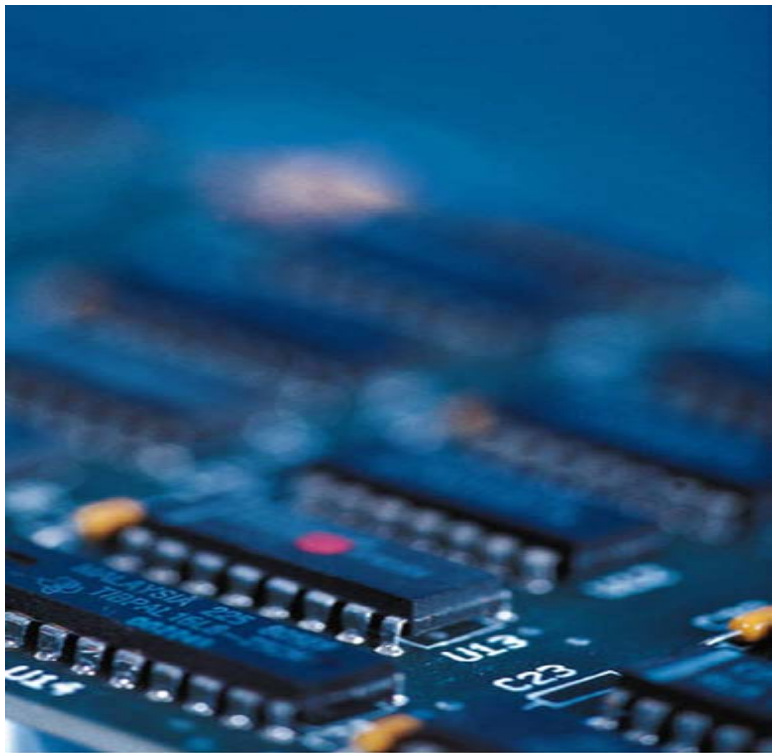




TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

# Unconventional Threats to Security

*Connectivity*



*Complexity*

# 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**

# The Threat Situation

*Continuing serious cyber attacks on information systems, large and small; targeting key federal, state, local, and private sector operations and assets…*

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with intentions of compromising federal information systems.
- Effective deployment of malicious software causing significant exfiltration of sensitive information (including intellectual property) and potential for disruption of critical information systems/services.

-- Dr. Ron Ross
NIST, *Computer Security Division*
*Information Technology Laboratory*

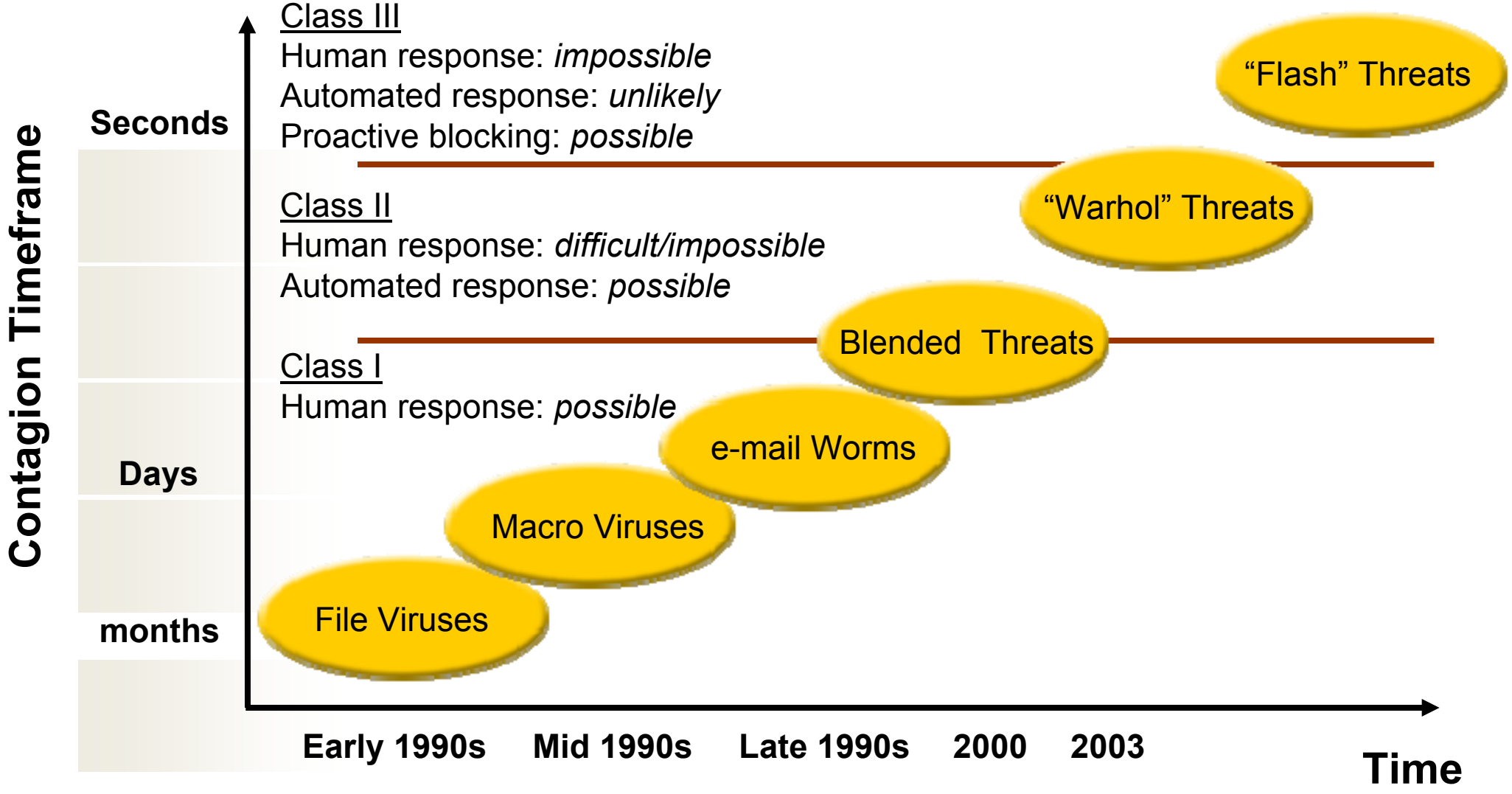
"We're the most vulnerable nation on the Earth because we're the most dependent."

- John "Mike" McConnell, former director of national intelligence, now Sr. VP at Booz Allen Hamilton, CIO Magazine, Sept. 23, 2009

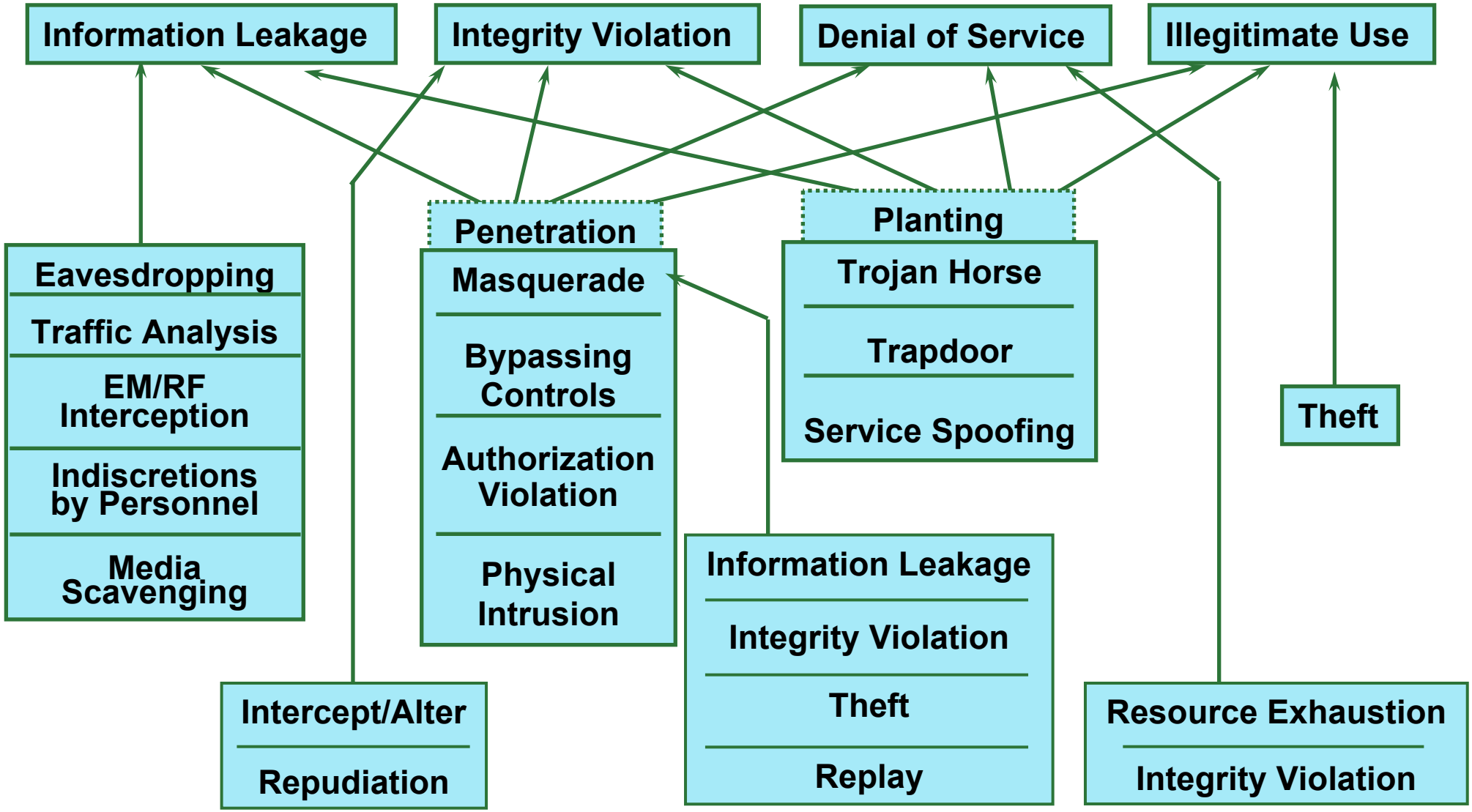
"I think we're really at a crisis point where we have no confidence in the security of our information."

- Amit Yoran, former director of the US-CERT, DHS, former CEO In-Q-Tel and CEO Net Witness, *CIO Magazine Sept. 23, 2009*

# Threat Evolution: Malicious Code



# What Can They Do and How Can They Do It?



# 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.

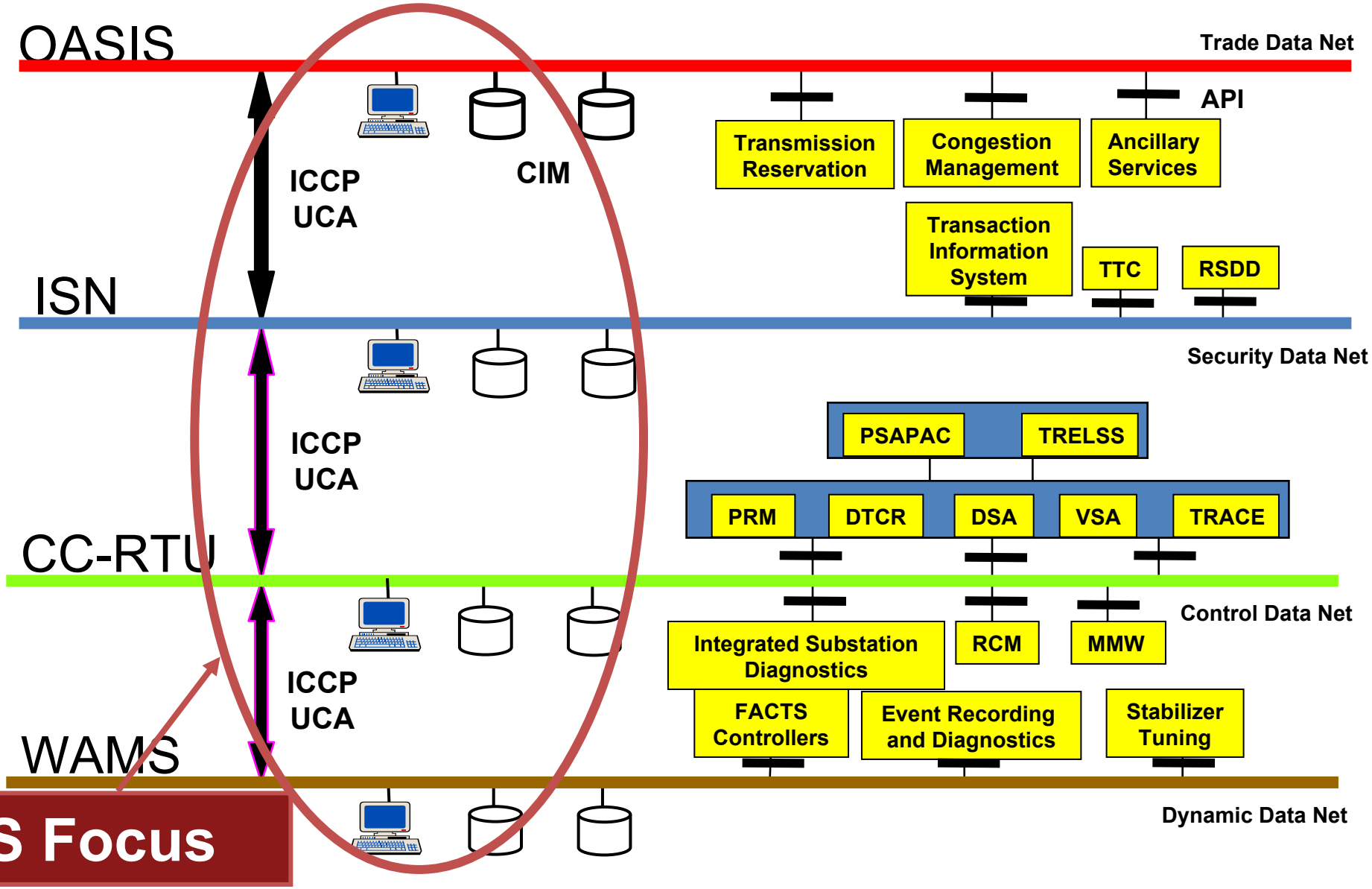
# Overview of Focused Research Areas (1998-2003):

## Programs Initiated and Developed at EPRI

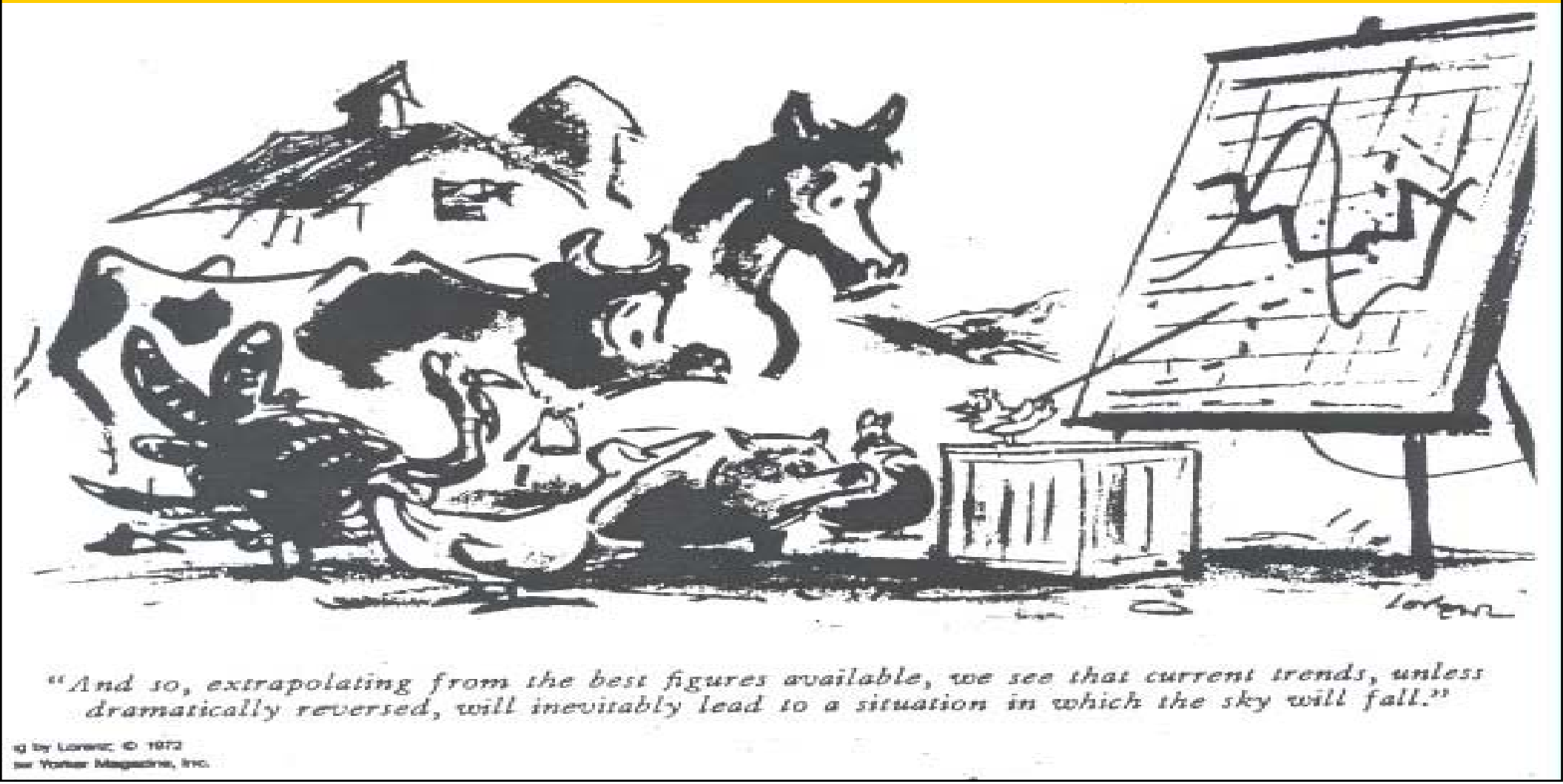
| 1999-2001 | Y2K2000-present | 2002-present | 2001-present |
|---|---|---|---|
| **EPRI/DoD Complex Interactive Networks (CIN/SI)** | **Enterprise Information Security (EIS)** | **Infrastructure Security Initiative (ISI)** | **Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)**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

# Enterprise Information Security (EIS) program

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



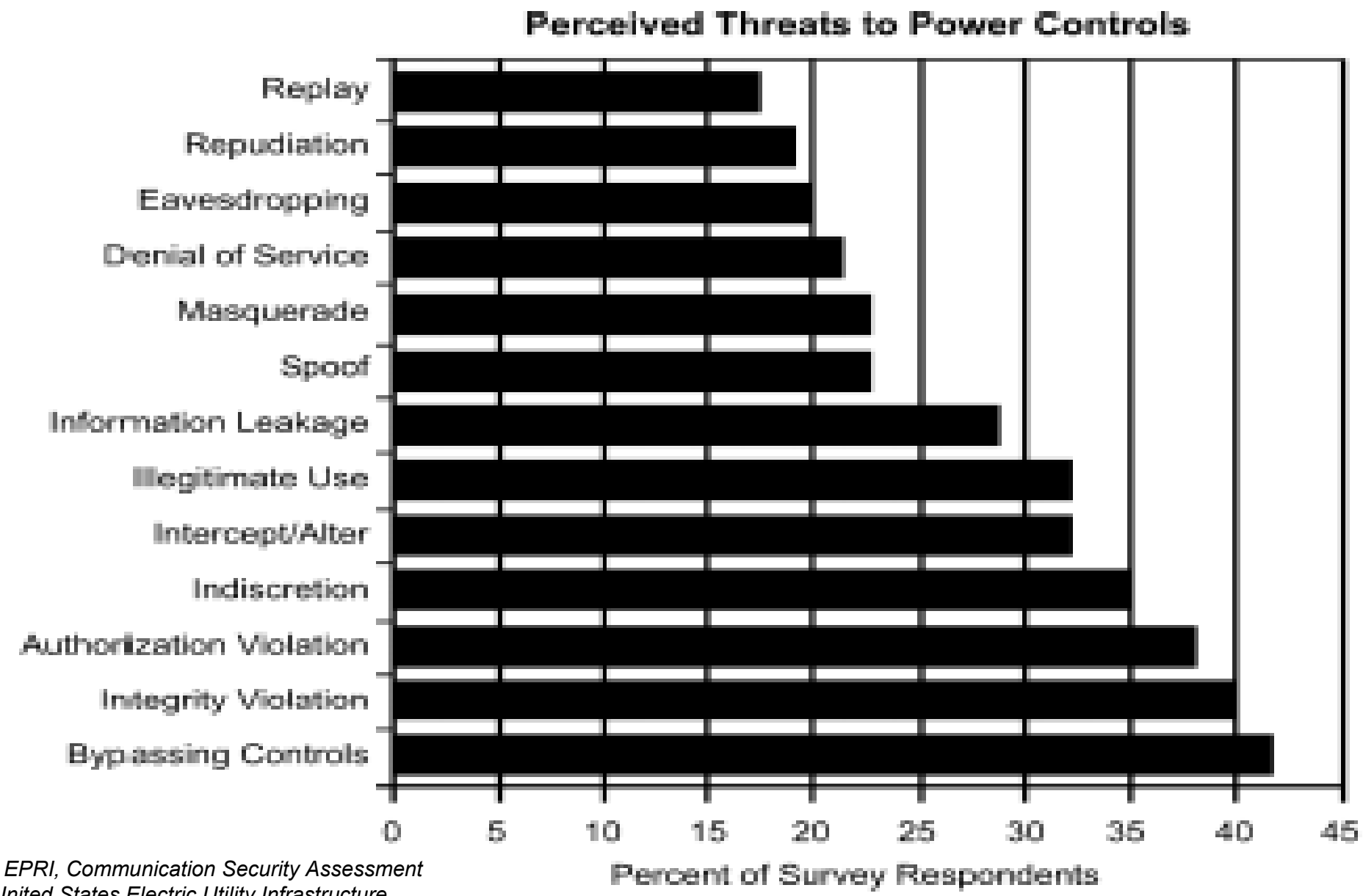
**"… And so, extrapolating from the best figures available, we see that current trends, unless dramatically reversed, will inevitably lead to a situation in which the sky will fall."**



*"And so, extrapolating from the best figures available, we see that current trends, unless dramatically reversed, will inevitably lead to a situation in which the sky will fall."*

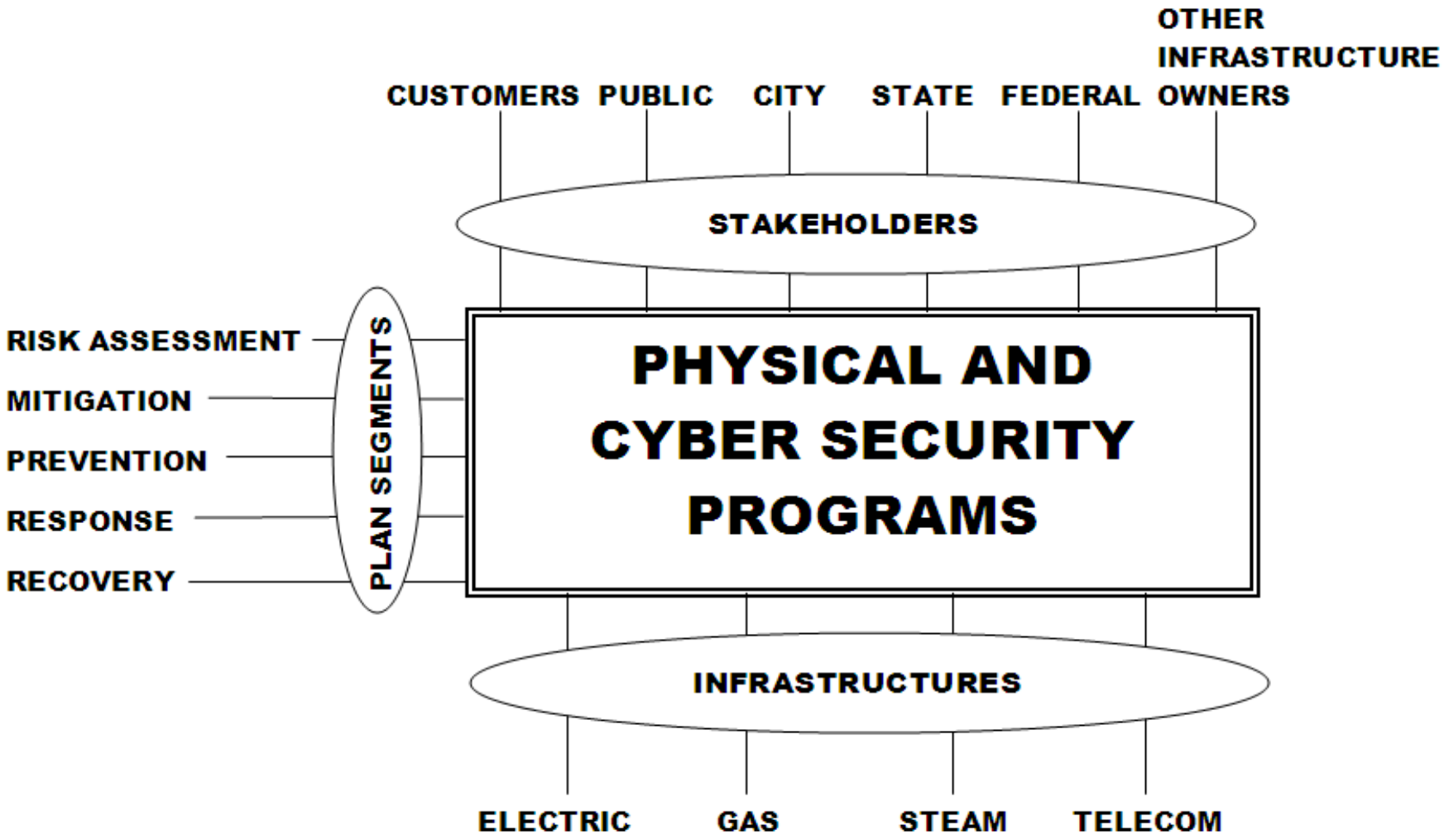
# Infrastructure Security

# Cyber Threats to Controls




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

# Example: CIP programs in the industry



# 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)

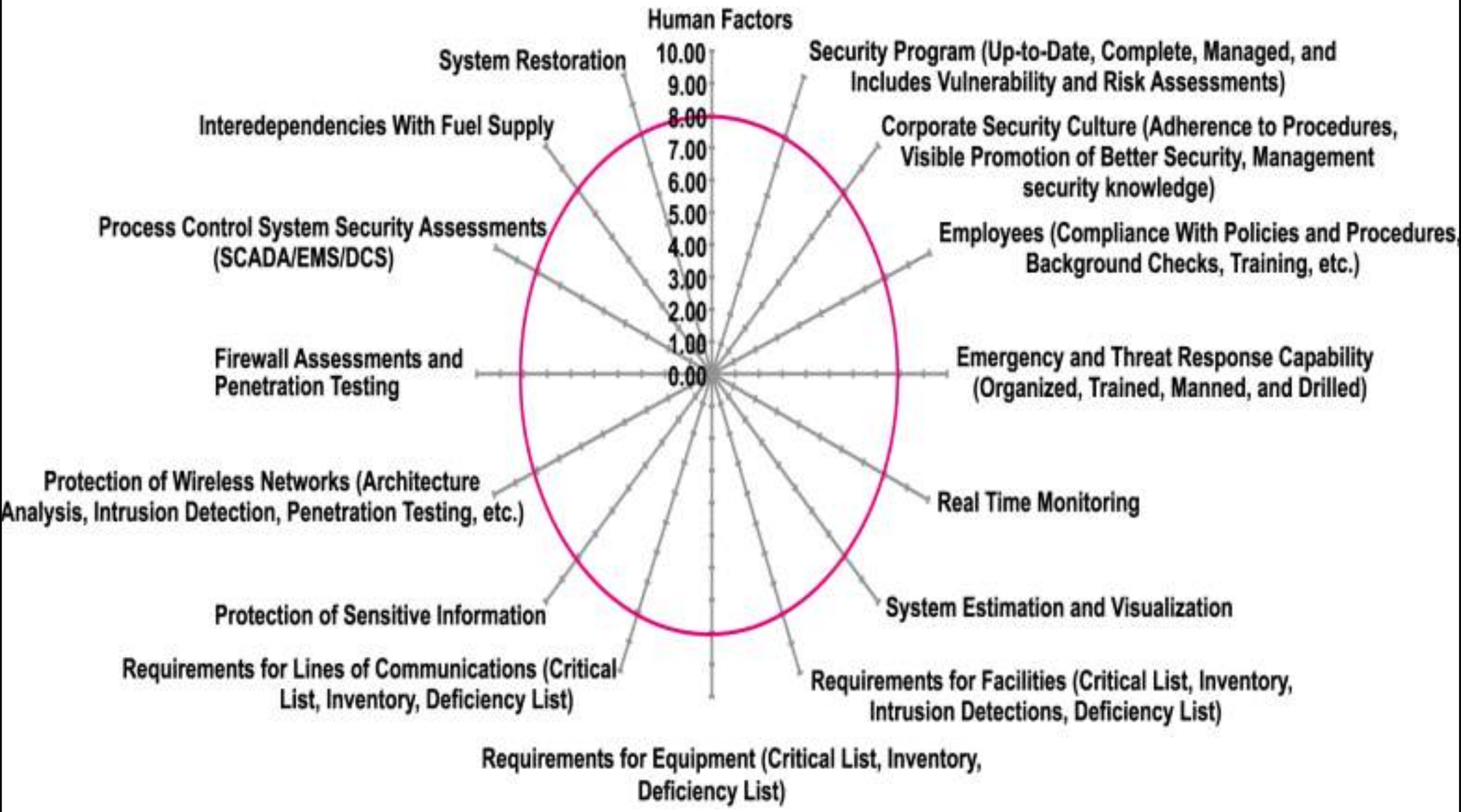
***Physical***

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

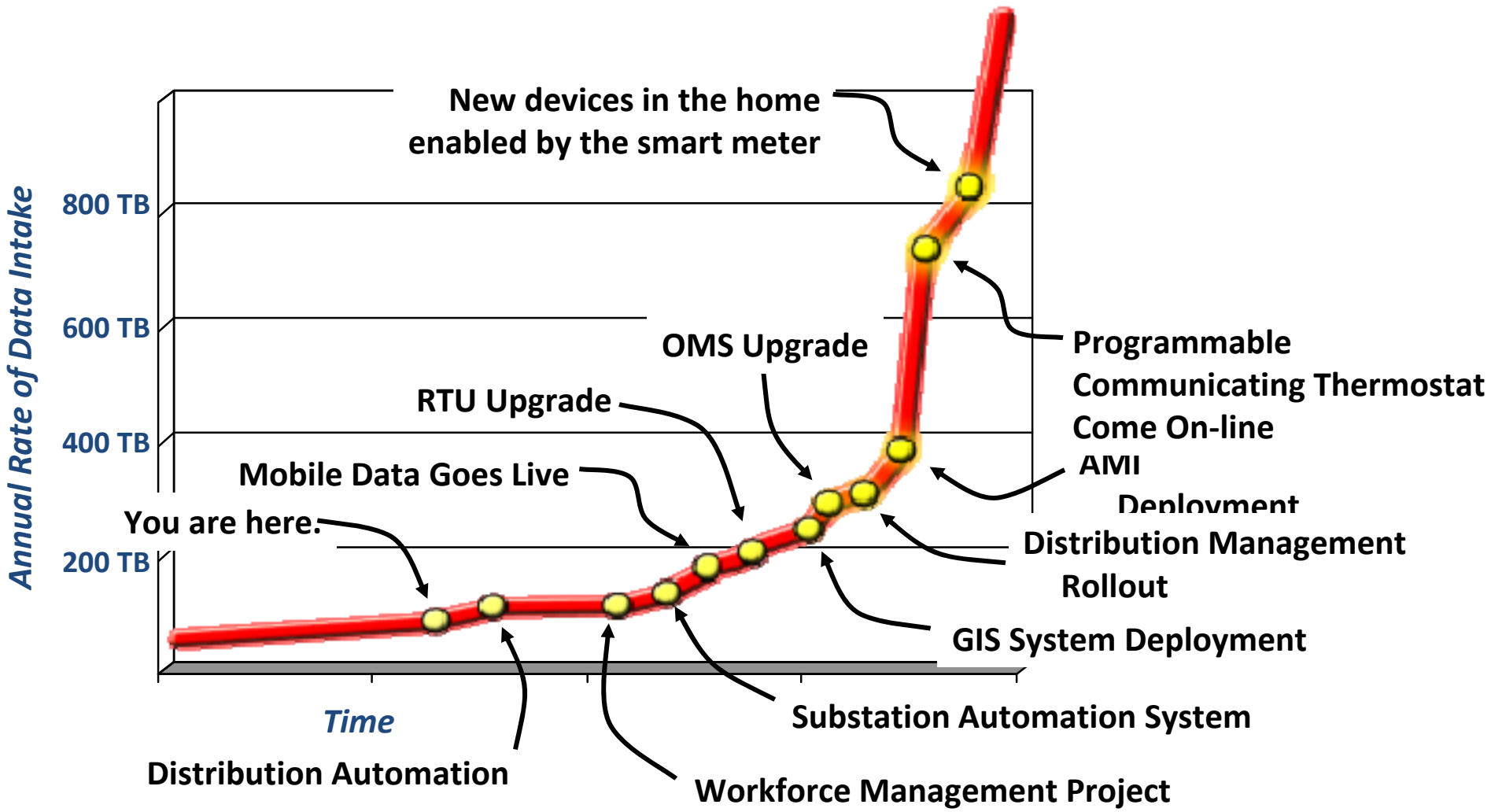
***Cyber and IT***

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

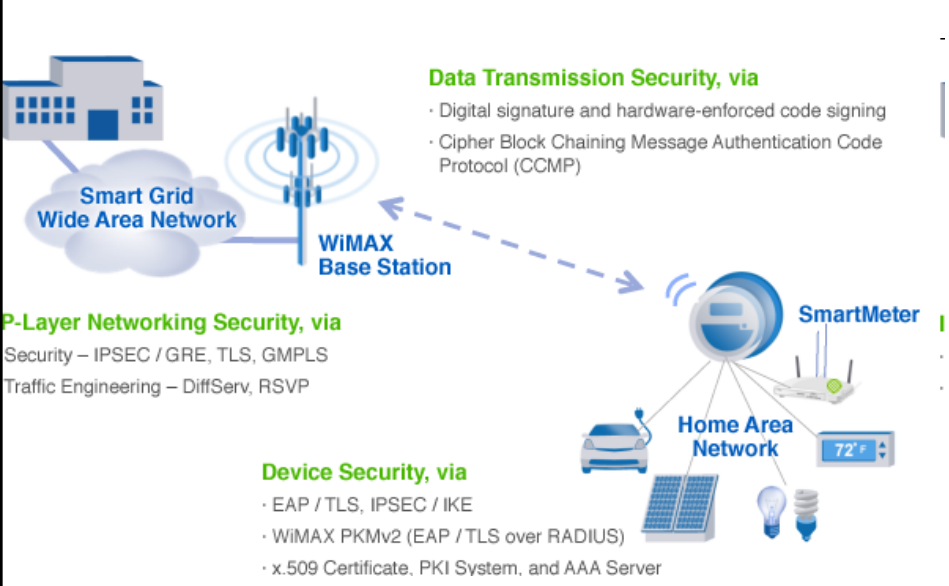


# Smart Grid: Tsunami of Data Developing




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

# “Smart Grid” Components & Devices



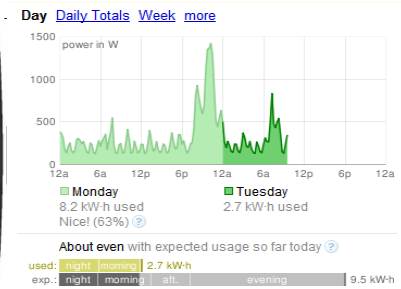


**Smart Meters**

**Secure Smart Grids are architected with standards (source: Gridnet)**

**Source: IBM Smart Grid**


**Control4’s EMS-100**




**Google Power Meter**


Technological Leadership Institute

UNIVERSITY OF MINNESOTA
Driven to Discover℠

# 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)

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

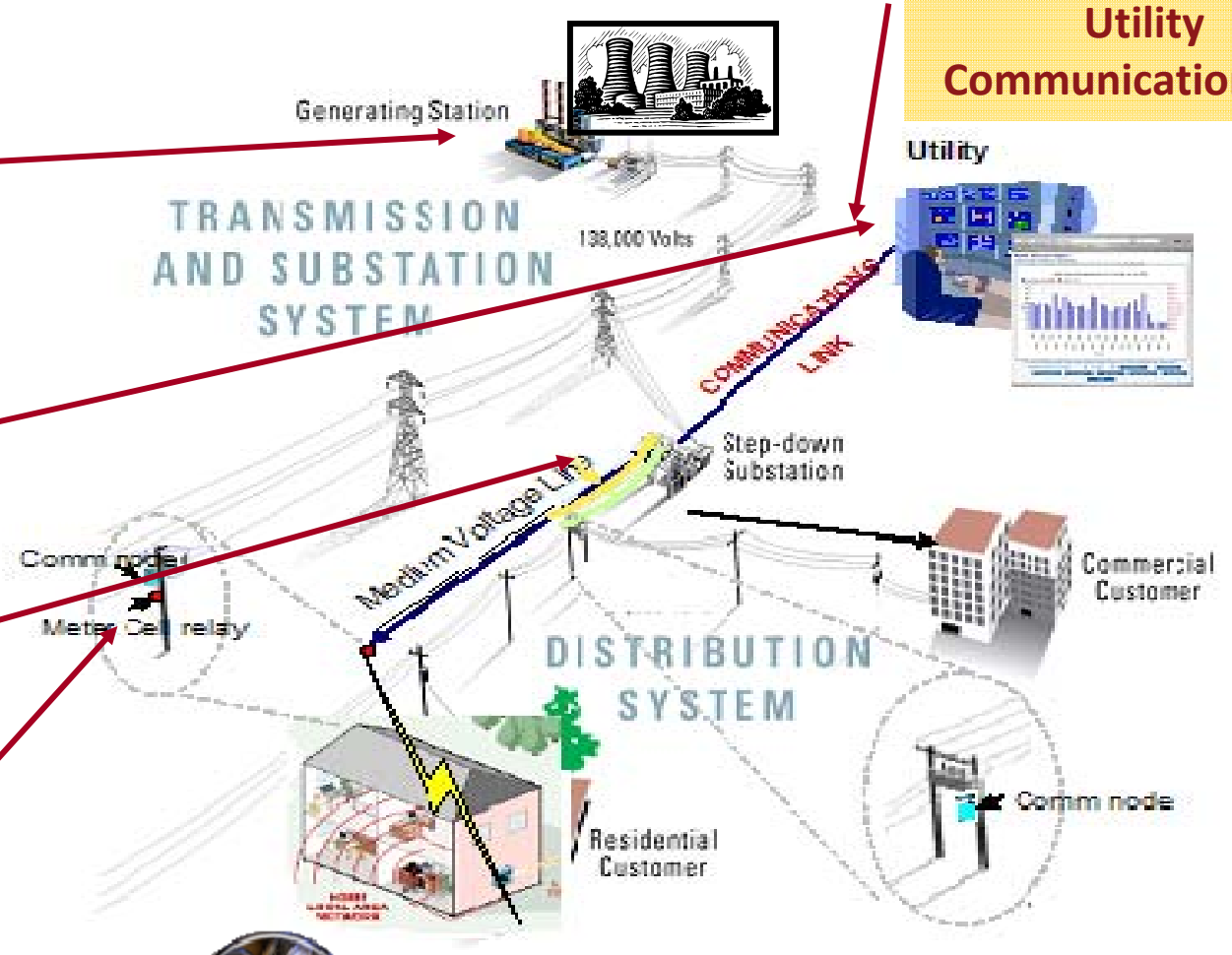
**Utility Communication Link**

**SCADA network systems**

**Advanced metering data management system**

**Substation Remote Monitoring equipment**

**Meter Communication (Meter to Cell Relay)**



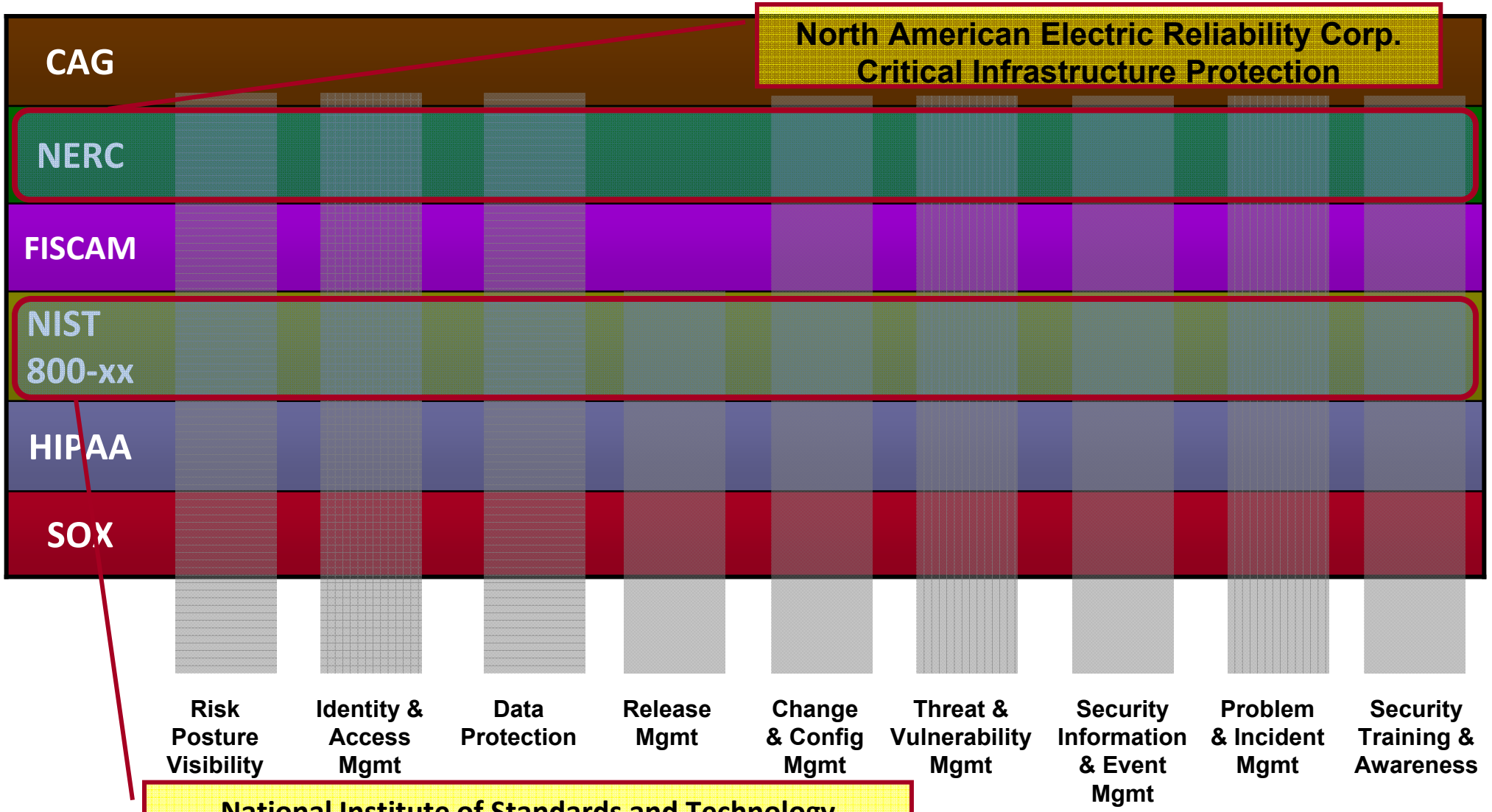

**IP addressability and use of open standard protocols for the control grid necessitates it to be securely protected at multiple points**

Source: IBM

# 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 | |

# Critical Security Controls




Source: IBM

# Issues to Watch

- **Interoperability**
  - NIST's Mandate: Energy Independence and Security Act (EISA) of 2007 ,Title XIII, Section 1305. Smart Grid Interoperability Framework
  - The Framework:
    - common architecture
    - flexible, uniform, technology-neutral
    - aligns policy, business, and technology approaches
    - includes protocols and standards for information management
    - Data exchange within the Smart Grid and between devices and technologies
  - NIST has offered an initial Smart Grid architecture; priorities for interoperability standards, including cybersecurity:
    - "Smart Grid Cyber Security Strategy and Requirements," The Smart Grid Interoperability Panel–Cyber Security Working Group, DRAFT NISTIR 7628, Feb. 2010

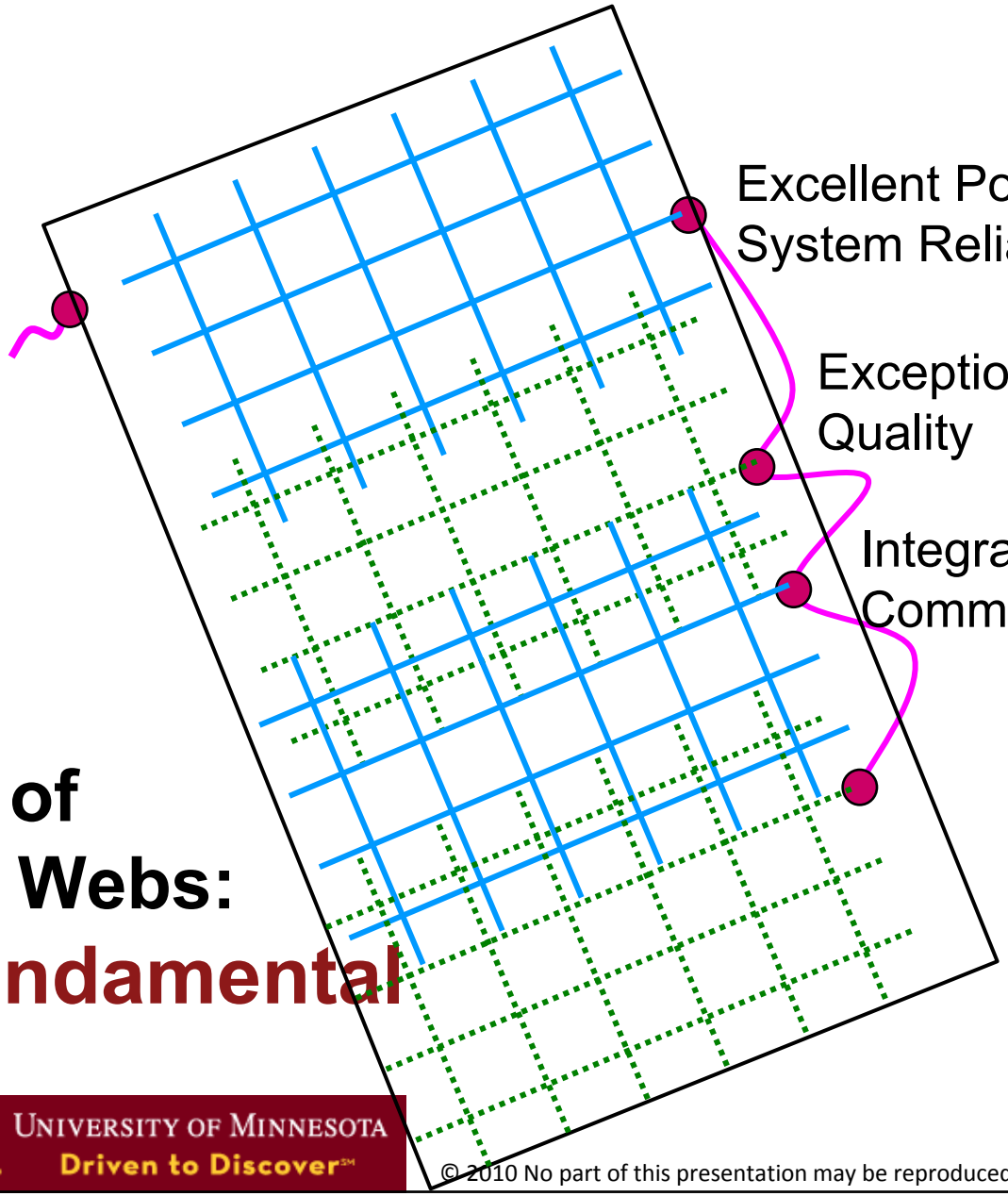
# Issues to Watch

- **Cybersecurity**
  - Bills in both House and Senate dealing with authority among FERC, DOE and NERC
  - The Commerce, Science and Transportation Committee approved the bill (S 773)

    **24 March 2010: "Cybersecurity bills easily approved by House, Senate panels"**
  - Requires the executive branch to collaborate with the private sector on developing cybersecurity standards and would mandate audits of how those standards were being met.
  - Empowers FERC to establish a cost recovery mechanism for required security measures.
  - Extends FERC's emergency authority to respond to threats to the grid from direct physical attacks, a geomagnetic storm such as a solar storm, and man-made electromagnetic pulses that could disrupt and destroy large segments of the electric grid.
  - An earlier version of the legislation would have established enforceable cybersecurity standards.
  - Legislation faces a challenging road to passage, given the crowded floor schedule, and the complexity of cybersecurity issues.
  - Major media attention to cyber-hacking may spawn more legislation

# The Smart Infrastructure for a Digital Society

A Secure Energy Infrastructure




**A Complex Set of Interconnected Webs:**

**Security is Fundamental**

# What are we working on at the University of Minnesota?

- Integrating PHEVs into the grid
- Secure Smart Meter Control
- Grid agents as distributed computer
- Security of cyber-physical infrastructure
- Fast power grid simulation and risk assessment

University of Minnesota Center for Smart Grid Technologies
Department of Electrical & Computer Engineering
Faculty: Professors Massoud Amin and Bruce Wollenberg
PhD Candidates/Research Assistants: Anthony Giacomoni, Laurie Miller, and Sara Mullen
PI: M. Amin (support from EPRI, NSF, ORNL, and University of Minnesota start-up research funding)

# 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℠

# Policy, Science and Technology Must Support This Transformation: Recommendations

- Establish the "Smart Grid" and "self-healing" interdependent infrastructure security & protection as national priorities
- Authorize increased funding for R&D and demonstrations of the "Smart Grid", and interdependency R&D, resilience/security
- Revitalize the national public/private electricity infrastructure partnership needed to fund the "Smart Grid" deployment

M. Amin's Congressional briefings on March 26 and Oct. 15, 2009

# 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

# Observations

- Tactical response is adequate, but strategic response is lacking
- There is no centralized and enforceable industry cybersecurity coordination and assurance capability
- A supportive public policy umbrella is needed
- The public doesn't appreciate the latent threat to the power system

# 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

## Threat Situation:

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

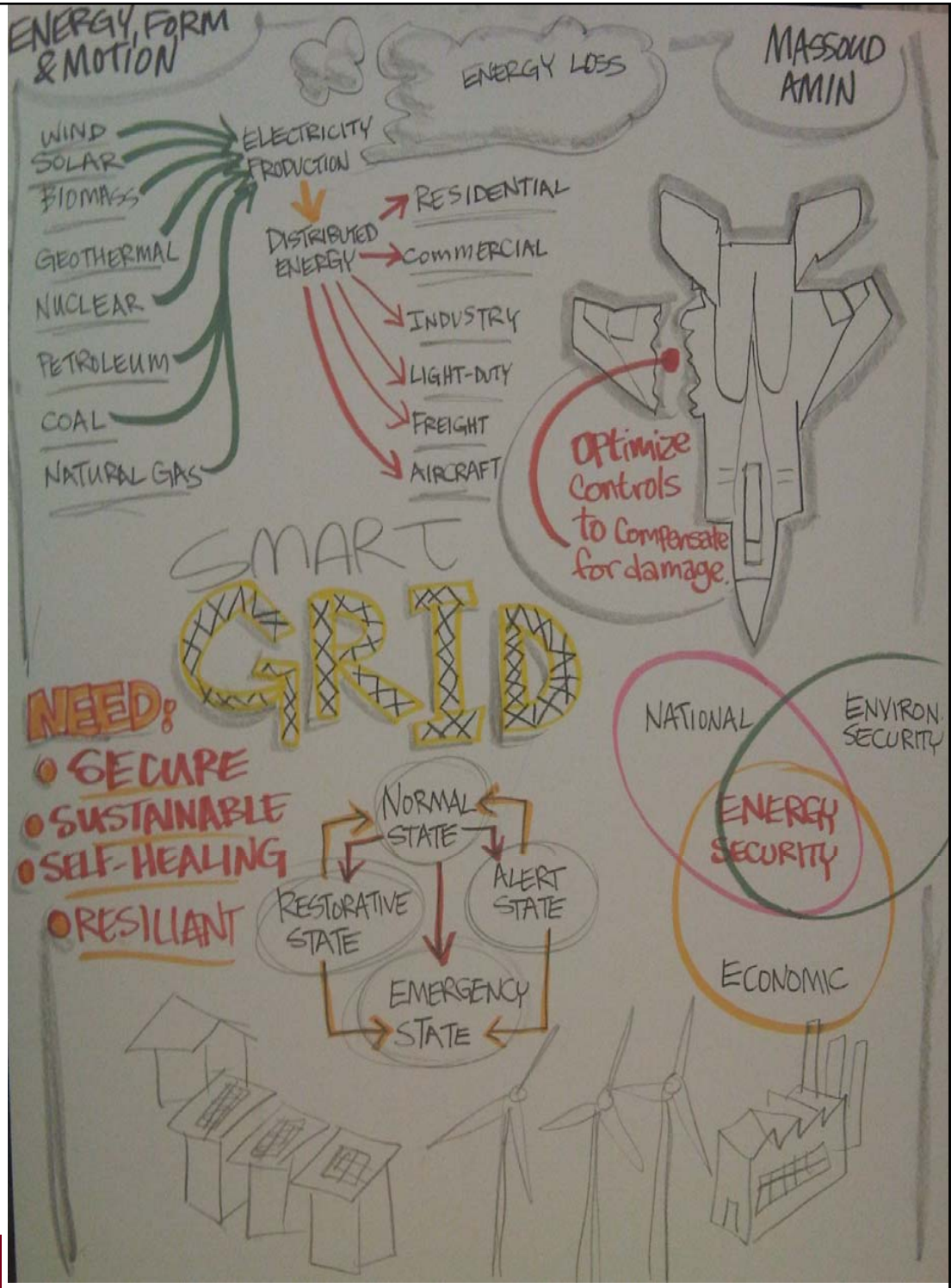
## Innovation and Policy:

- 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.

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

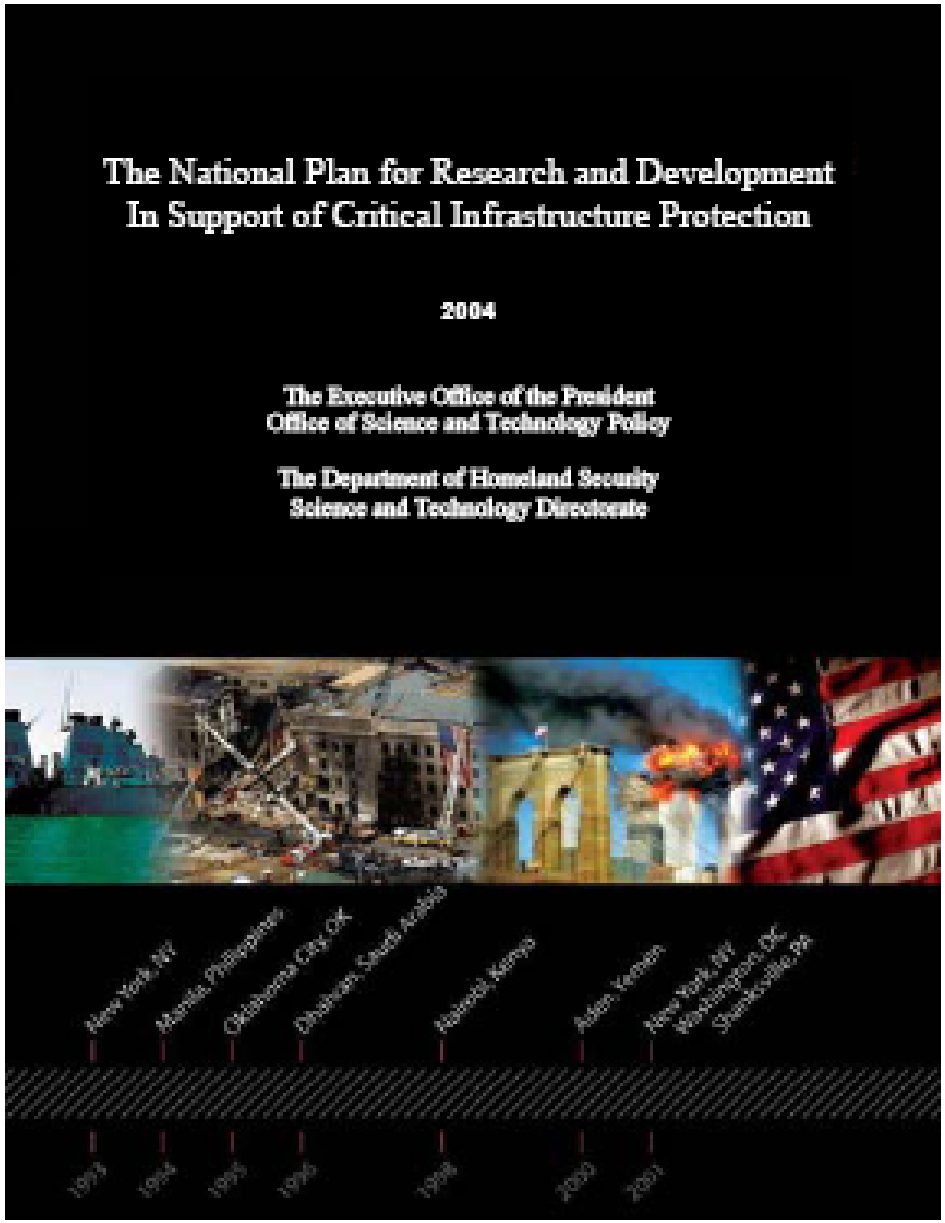
**"The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming and interconnected with everything else."**

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



# THE NATIONAL PLAN FOR RESEARCH AND DEVELOPMENT IN SUPPORT OF CRITICAL INFRASTRUCTURE PROTECTION

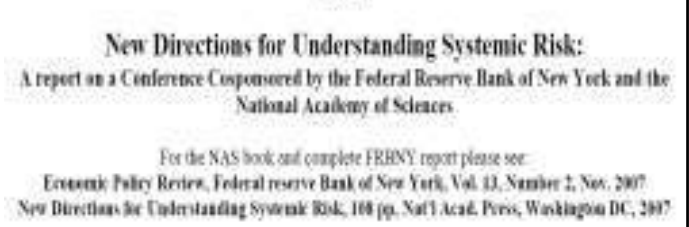
- The area of self-healing infrastructure was recommended in 2005 by the White House Office of Science and Technology Policy (OSTP) and the U.S. Department of Homeland Security (DHS) as one of three thrust areas for the National Plan for research and development in support of Critical Infrastructure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



# Selected References

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

- **"A Control and Communications Model for a Secure and Reconfigurable Distribution System,"** (Giacomoni, Amin, *&* Wollenberg), IEEE Int'l Conf. on Smart Grid Communications, Oct. 2010 - NIST
- **"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



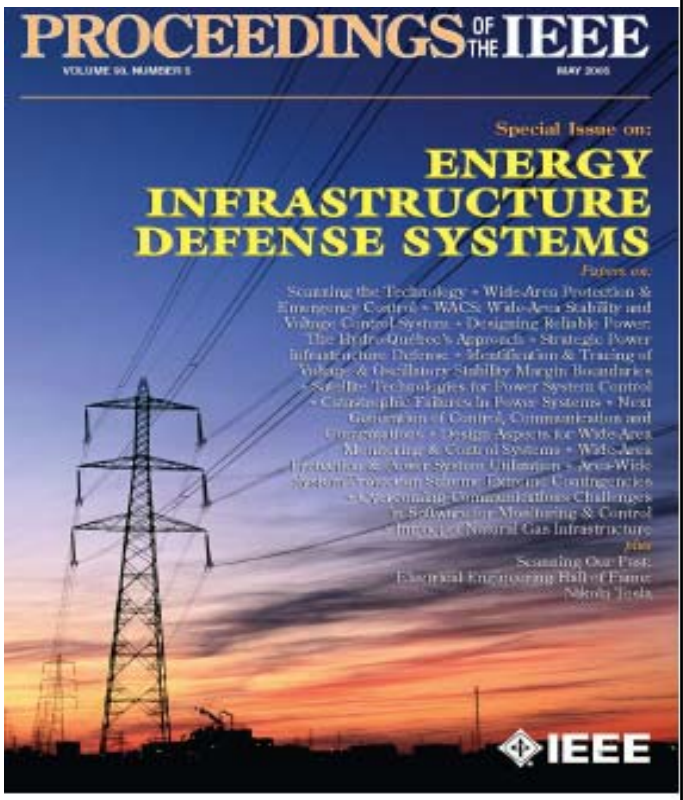
Summary of presentation by Prof. Massoud Amin and related comments from

**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 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℠