

# Enabling a Resilient and Secure North American Electric Power Grid

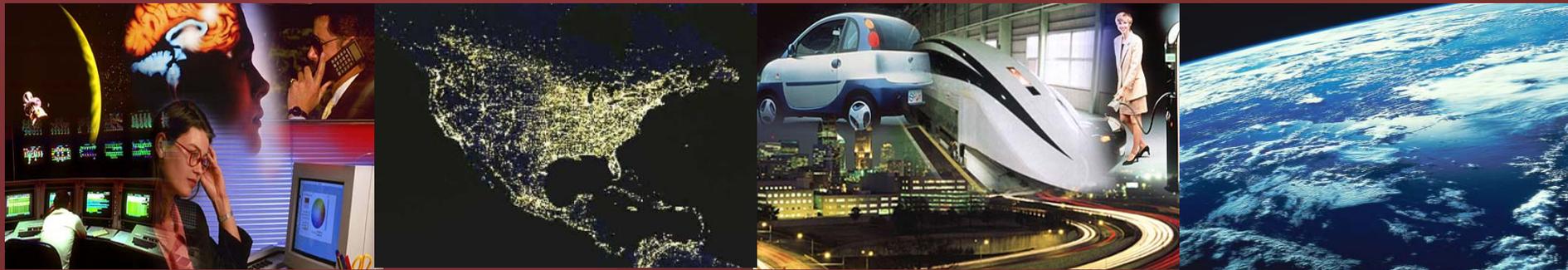
S. Massoud Amin, D.Sc.

Director, Technological Leadership Institute

Honeywell/H.W. Sweatt Chair in Technological Leadership

Professor, Electrical & Computer Engineering

University Distinguished Teaching Professor



**ISRCS 2011**

**Keynote address at the 4th International  
Symposium on Resilient Control Systems  
August 10, 2011**

**TECHNOLOGICAL  
LEADERSHIP INSTITUTE**

UNIVERSITY OF MINNESOTA

**Driven to Discover<sup>SM</sup>**

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

Copyright © 2011 No part of this presentation may be reproduced in any form without prior authorization.

# R&D Challenges

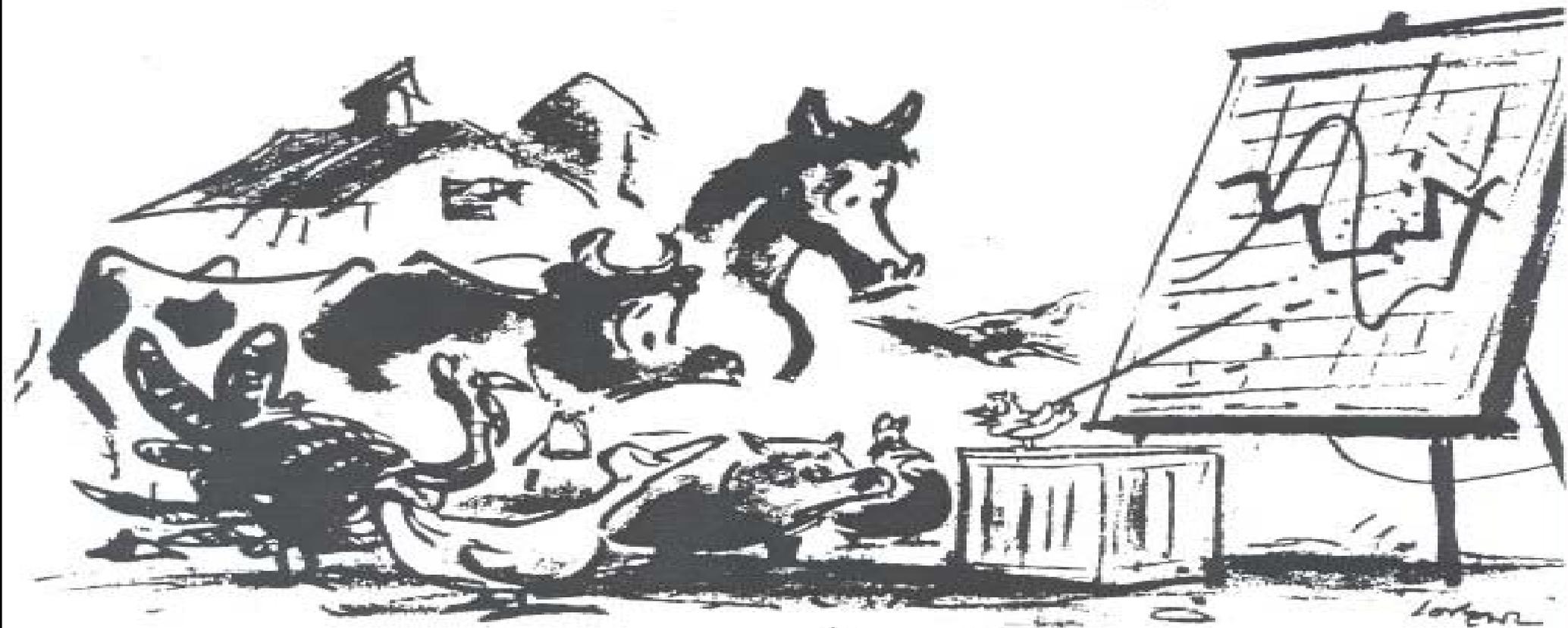
- Sensing and Communication
- Early Fault Detection and System V&V
- Systems Integration and Interoperability
- Security (from embedded... to end-to-end)



# 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?”

**“... 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

We are “Bullet  
Proof”

The Truth

“The Sky is  
Falling”



# Power Grid Vulnerabilities

- Physical:
  - Over 450,000 miles of 100kV or higher (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

# Smart Grid Vulnerabilities

- Cyber:
  - Existing control systems were designed for use with proprietary, stand-alone communications networks
  - Numerous types of equipment and protocols are used
  - More than 90% of successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices
  - Possible effects of attacks:
    - 1) Loss of load
    - 2) Loss of information
    - 3) Economic loss
    - 4) Equipment damage

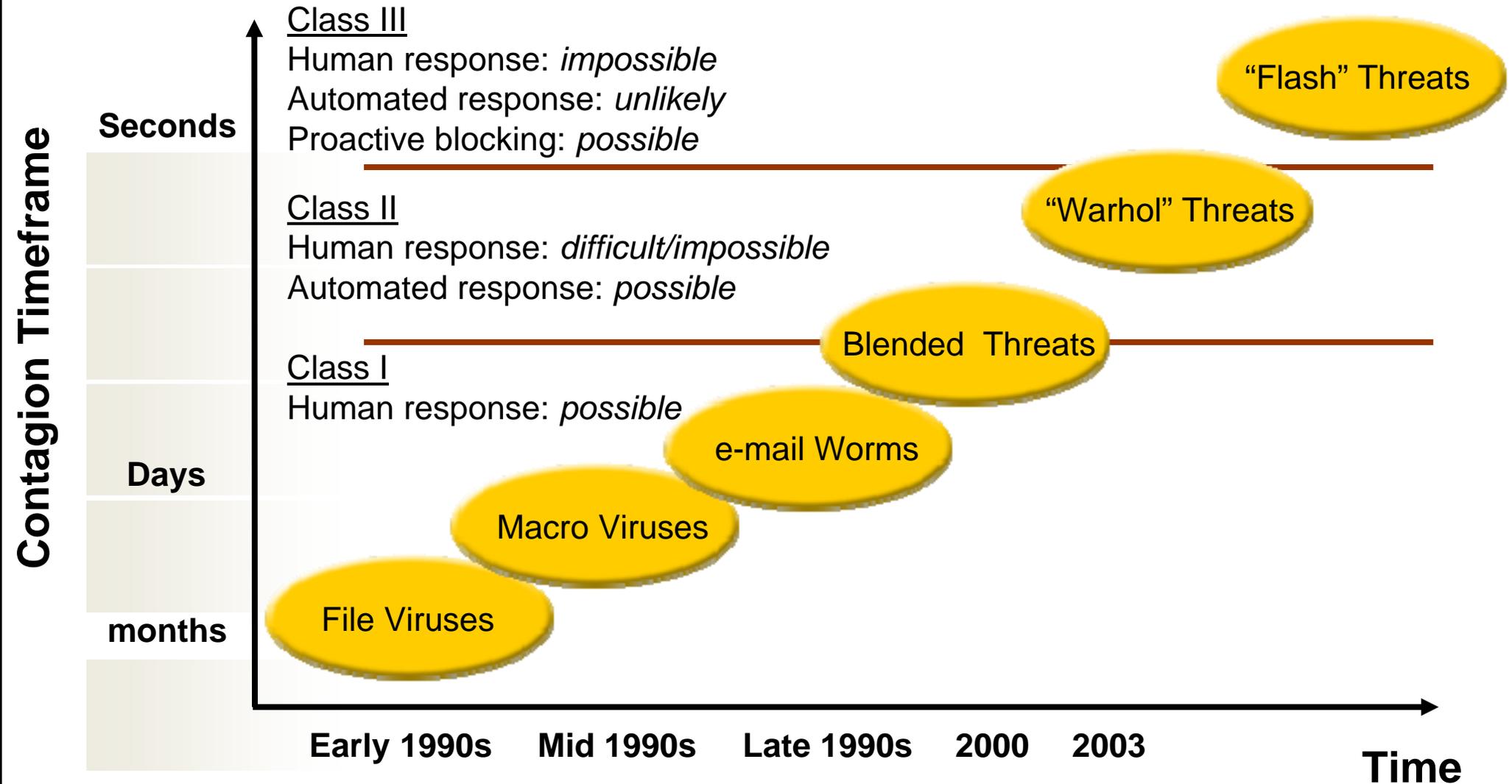
# Stuxnet & Digital Systems: SCADA, EMS, ICS

- Iran's nuclear agency trying to stop **computer worm Stuxnet worm can take over systems that control industrial plants** By NASSER KARIMI updated 9/25/2010 1:50:43 PM ET TEHRAN, Iran
- Iran's nuclear agency is trying to combat a complex computer worm that has affected industrial sites throughout the country and is **capable of taking over power plants,**
- **Stuxnet can take over systems that control the inner workings of industrial plants.** Experts in Germany discovered the worm in July, and it has since shown up in a number of attacks - primarily in Iran, Indonesia, India and the U.S.
- The ISNA report said the malware had spread throughout Iran, but did not name specific sites affected.
- The destructive **Stuxnet worm** has surprised experts because it is **the first one specifically created to take over industrial control systems,** rather than just steal or manipulate data.
- The U.S. is also tracking the worm, and the DHS has specialized teams that can respond quickly to cyber emergencies at industrial facilities across the country.

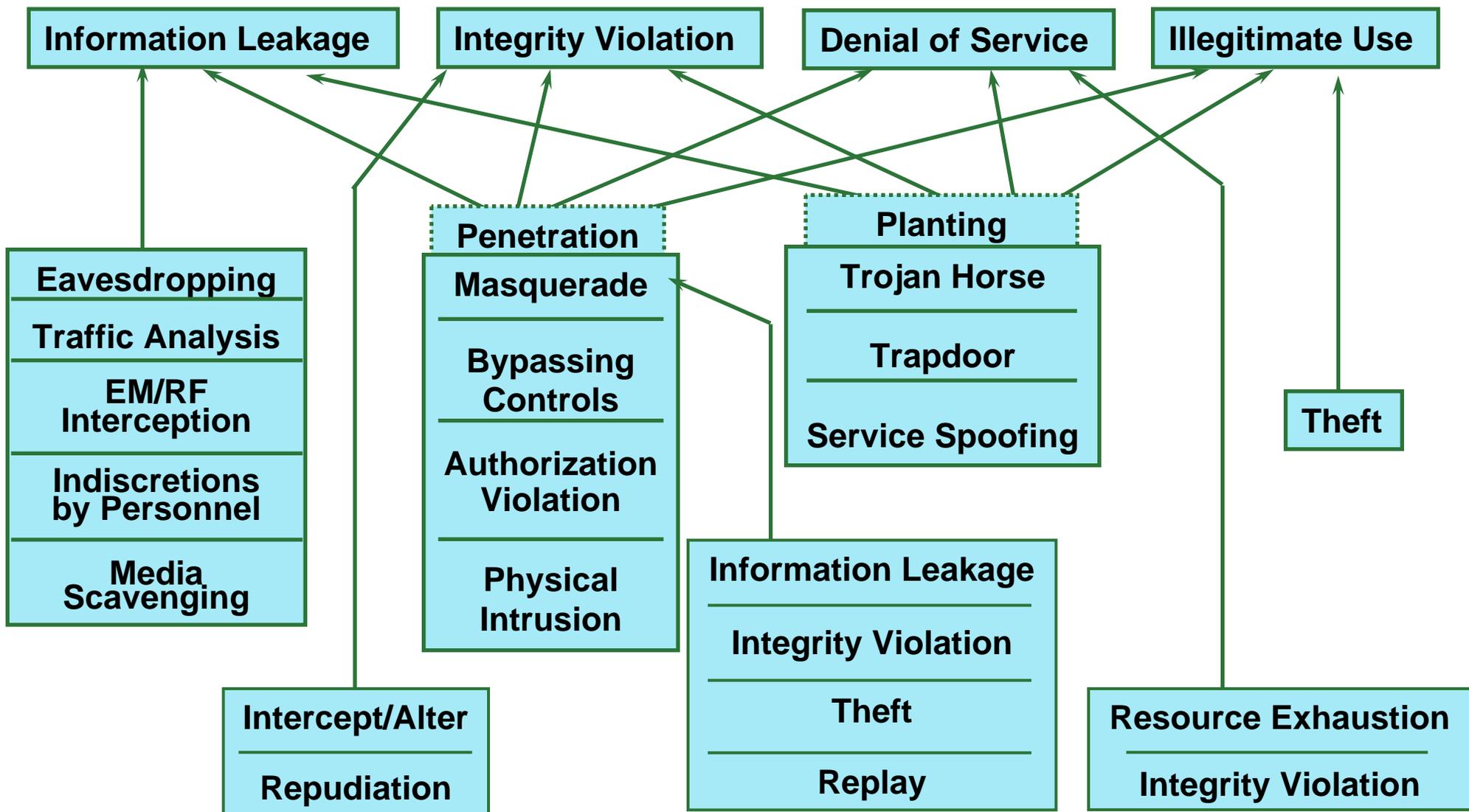
[http://www.msnbc.msn.com/id/39357629/ns/technology\\_and\\_science-tech\\_and\\_gadgets#](http://www.msnbc.msn.com/id/39357629/ns/technology_and_science-tech_and_gadgets#)



# Threat Evolution: Malicious Code



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



# Overview of focused research areas (1998-2003): Programs Initiated and Developed at EPRI

1999-2001

## EPRI/DoD Complex Interactive Networks (CIN/SI)

Underpinnings of Interdependent Critical National Infrastructures  
Tools that enable secure, robust & reliable operation of interdependent infrastructures with distributed intelligence & self-healing

Y2K2000-present

## Enterprise Information Security (EIS)

1. Information Sharing
2. Intrusion/Tamper Detection
3. Comm. Protocol Security
4. Risk Mgmt. Enhancement
5. High Speed Encryption

2002-present

## Infrastructure Security Initiative (ISI)

- Response to 9/11 Tragedies**
1. Strategic Spare Parts Inventory
  2. Vulnerability Assessments
  3. Red Teaming
  4. Secure Communications

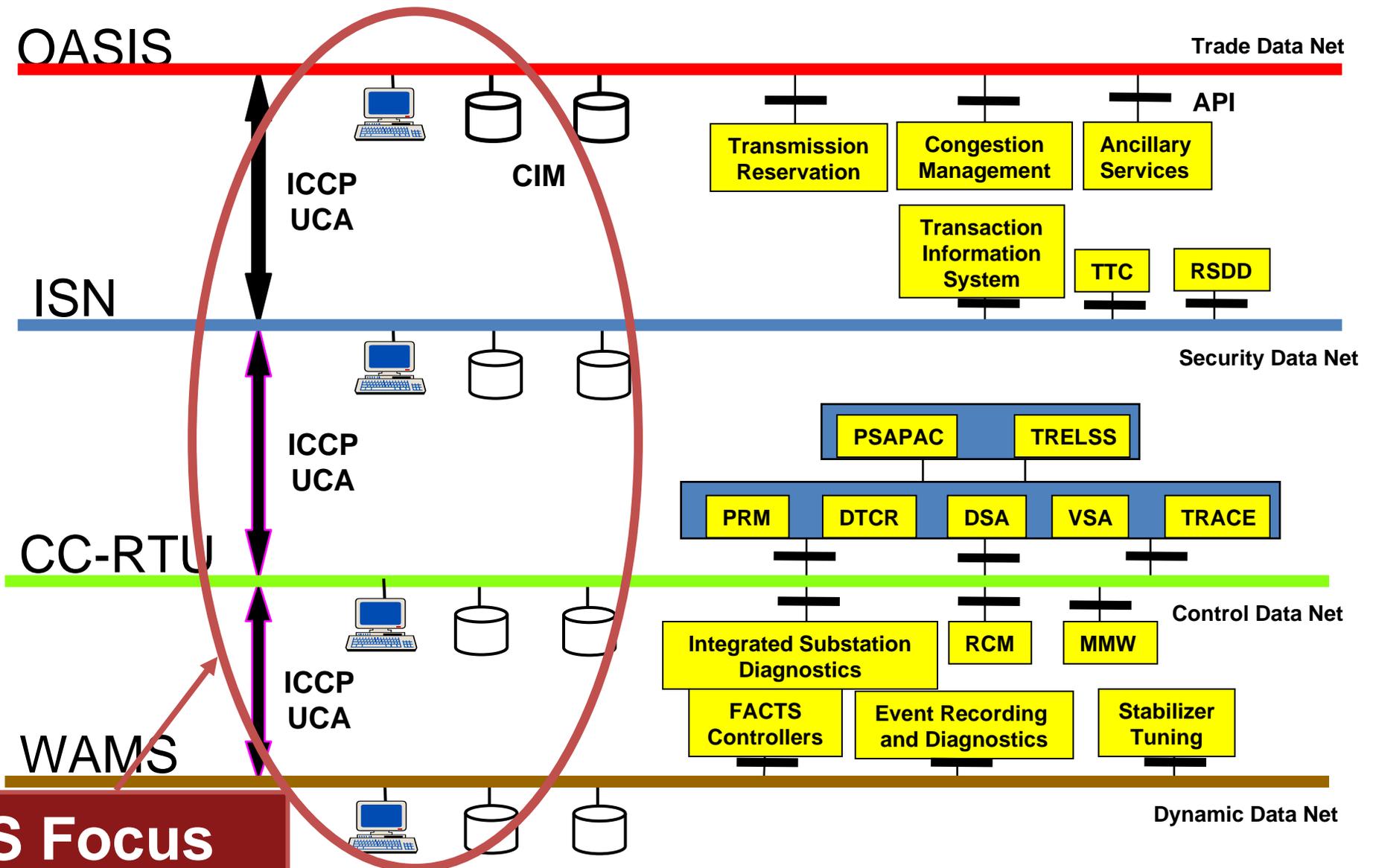
2001-present

## Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)

1. Self Healing Grid
2. IntelliGrid™
3. Integrated Electric Communications System Architecture
4. Fast Simulation and Modeling

# Enterprise Information Security (EIS) program

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



**EIS Focus**

# Lessons learned, e.g.:

## Redundancy Lowers Impact of Threats

- Two Separate Control Rooms – 500 miles apart
- Dual EMS systems at each location + Training/testing EMS
- Diversified communications networks



# 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)

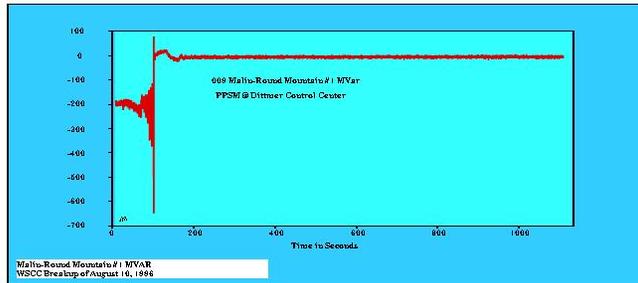
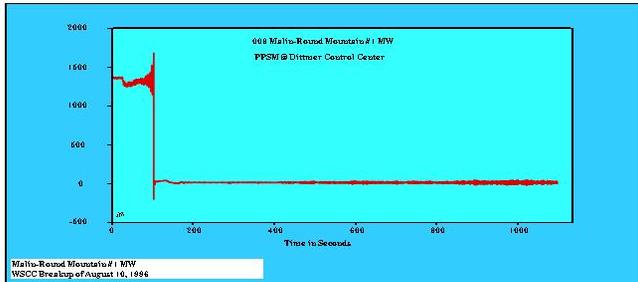
# Context: Better Situational Awareness and Automation

- **Increasing Dependence on ICT, Computation and Communications.**
- **Increasing Complexity:** System integration, increased complexity: call for new approaches to simplify the operation of complex infrastructure and make them more robust to attacks and interruptions.
- **Centralization and Decentralization of Control:** The vulnerabilities of centralized control seem to demand smaller, local system configurations. Resilience rely upon the ability to bridge top--down and bottom-up decision making in real time.



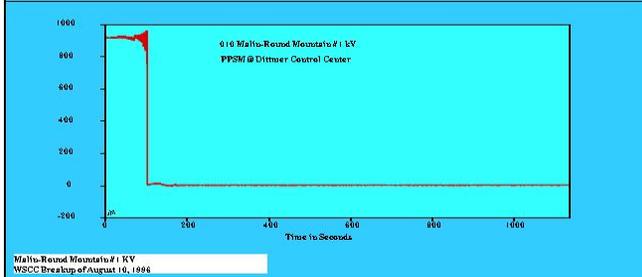
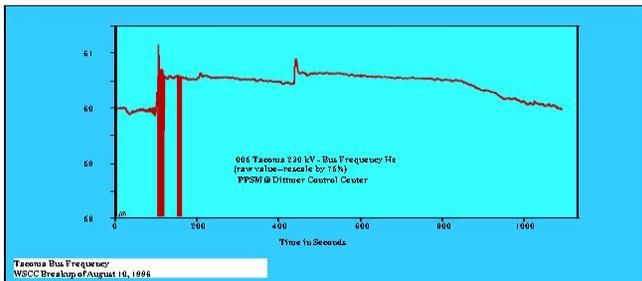
# Data and Measurements

# Disturbance records for WSCC breakup of August 10, 1996



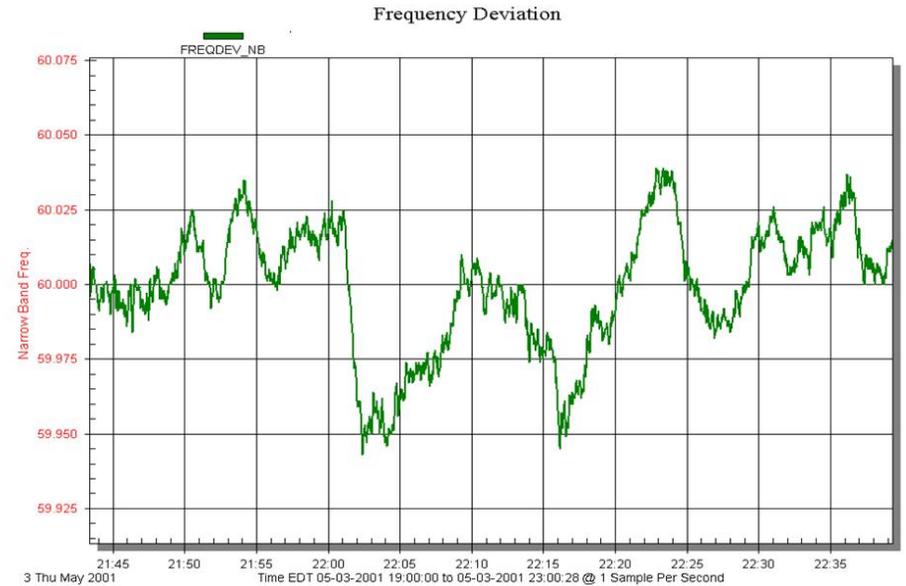
Source: DOE/EPRI WAMS project

# Disturbance records for WSCC breakup of August 10, 1996



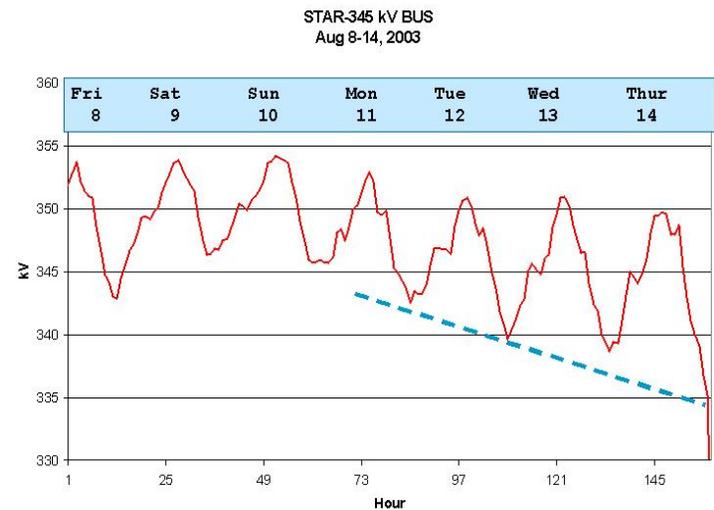
Source: DOE/EPRI WAMS project

# Last Episode of the TV series "Survivor"



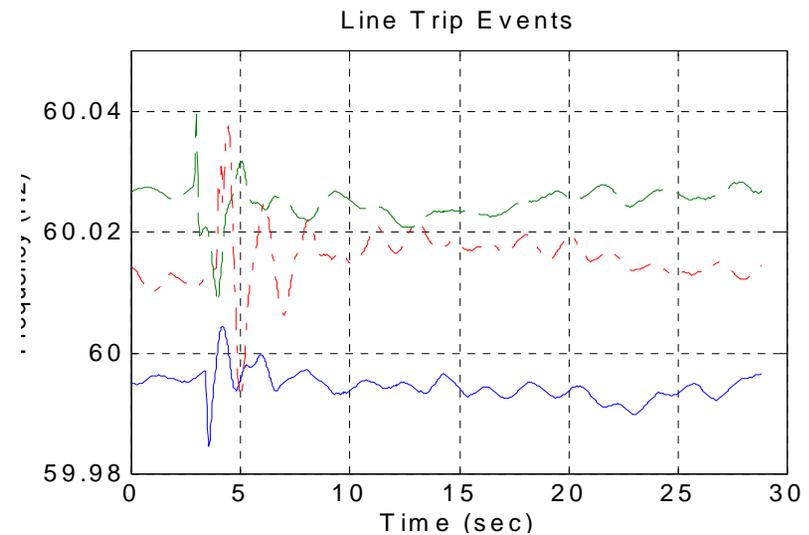
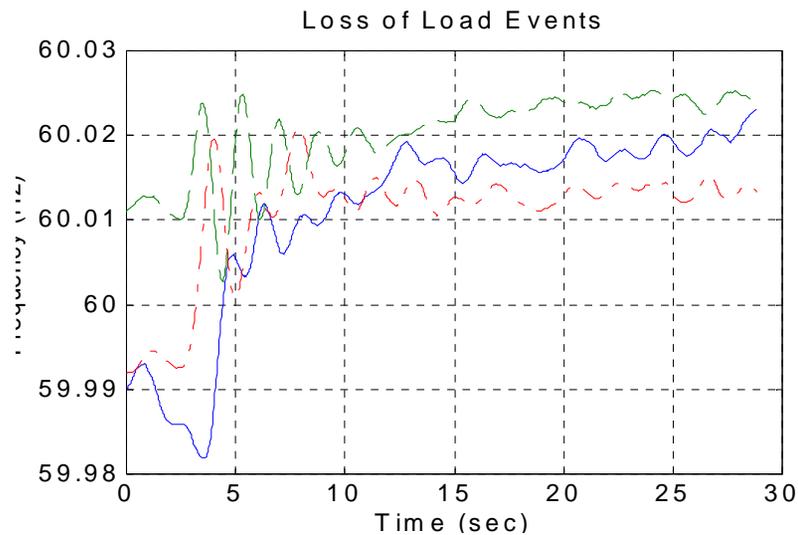
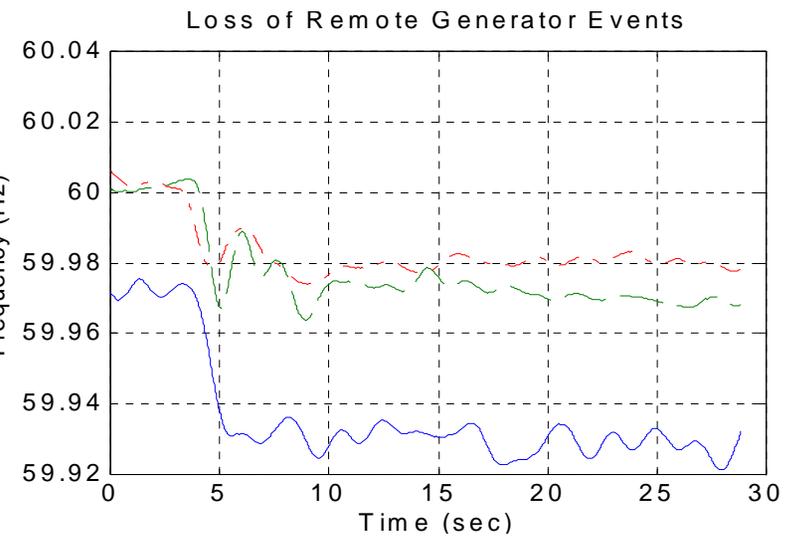
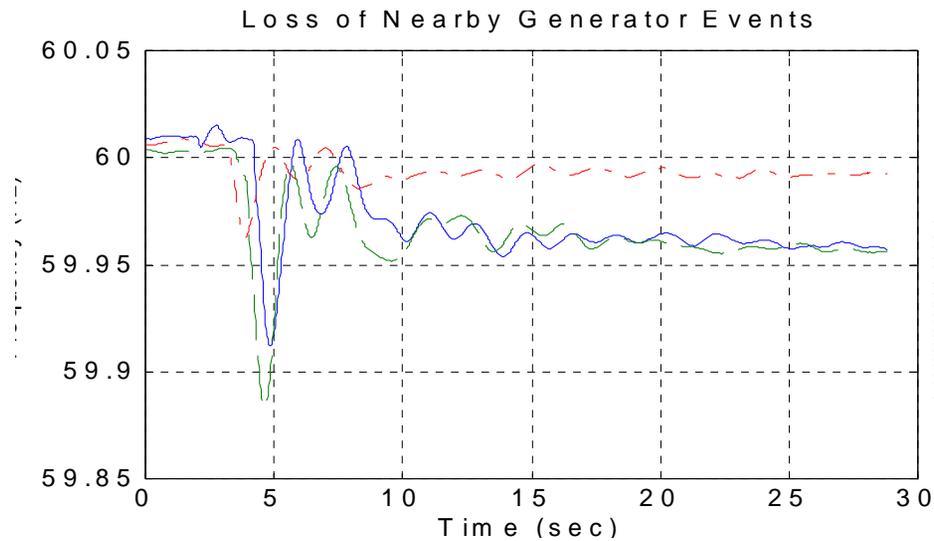
Source: Jim Ingleson (NYISO) and Joe Chow (RPI)

# Initial Conditions on August 14, 2003



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

# Detecting Precursors: Classification of fault signatures

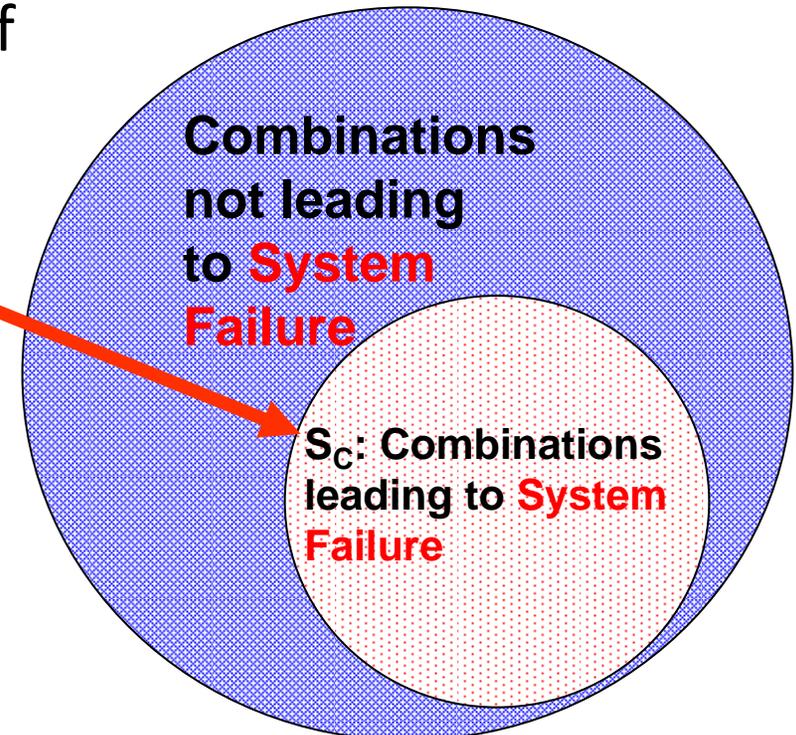


# Disturbance Feature Extraction

<b>Disturbance</b>	<b>Frequency change</b>	<b>Frequency derivative</b>	<b>Line flow change</b>
Loss of nearby generation	Negative	Steep	Large
Loss of remote generation	Negative	Moderate	Negligible
Loss of load	Positive	Moderate	Detectable
Line trip close to DRD	Negligible	Steep	Large
Oscillations	Negligible	Small	oscillations

# Precursor Detection for Situational Awareness

- Enhancing Reliability and Security of Network Operation via quantification of the system state and its “direction/speed/momentum” toward a major failure
- Making Network Availability (quick restoration) a key requirement
- Introducing Quality of Service as an additional constraint
- Ultimately, enabling operators to act more efficiently and with greater confidence in difficult (sometimes unclear, unexpected or even conflicting) circumstances



Which trajectories lead to catastrophic failures?

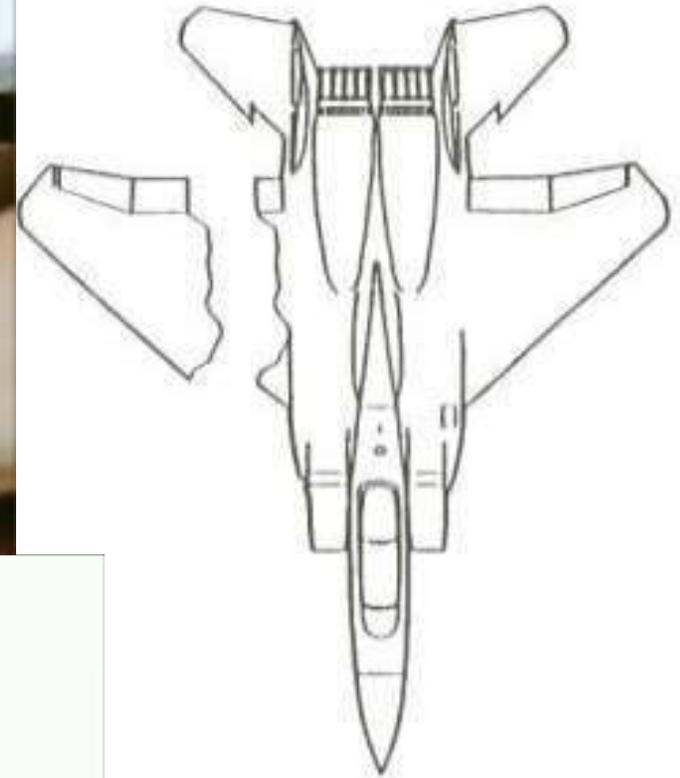
# Multi-Scale Time Hierarchy of Power Systems

ACTION / OPERATION	TIME FRAME
Wave effects (fast dynamics, lightning caused overvoltages)	Microseconds to milliseconds
Switching overvoltages	Milliseconds
Fault protection	100 milliseconds or a few cycles
Electromagnetic effects in machine windings	Milliseconds to seconds
Stability	60 cycles or 1 second
Stability Augmentation	Seconds
Electromechanical effects of oscillations in motors & generators	Milliseconds to minutes
Tie line load frequency control	1 to 10 seconds; ongoing
Economic load dispatch	10 seconds to 1 hour; ongoing
Thermodynamic changes from boiler control action (slow dynamics)	Seconds to hours
System structure monitoring (what is energized & what is not)	Steady state; on-going
System state measurement and estimation	Steady state; on-going
System security monitoring	Steady state; on-going
Load Management, load forecasting, generation scheduling	1 hour to 1 day or longer; ongoing.
Maintenance scheduling	Months to 1 year; ongoing.
Expansion planning	Years; ongoing
Power plant site selection, design, construction, environmental impact, etc.	10 years or longer

# **Precursor Detection for Situational Awareness**

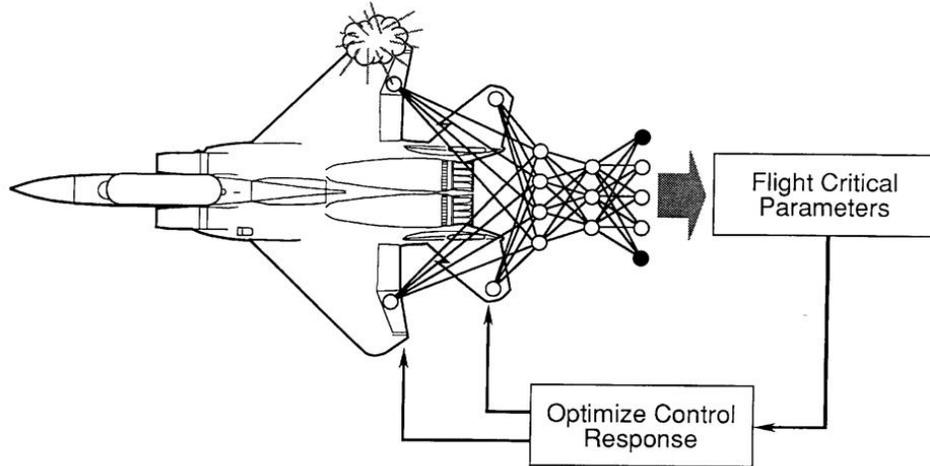
**Fast modeling high-confidence  
look-ahead simulation**

# 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



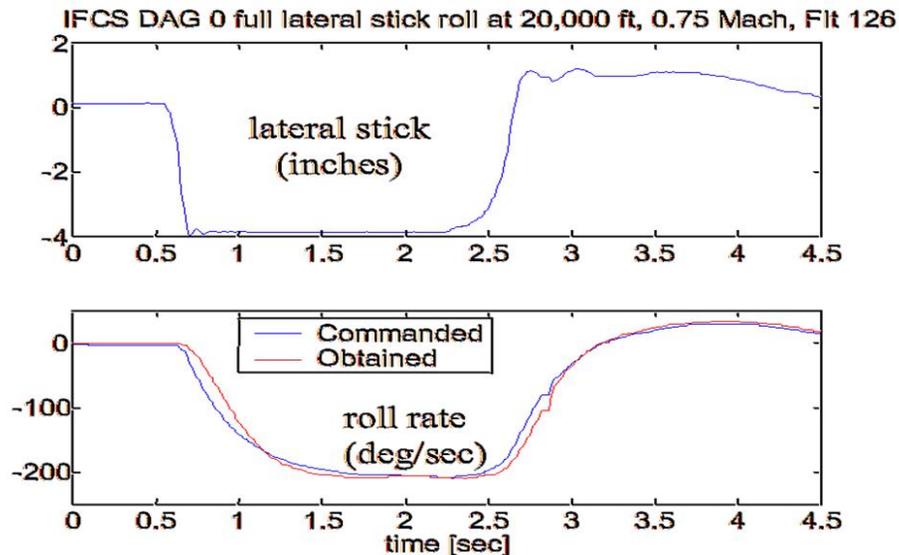
NASA/MDA/WU IFCS

## 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.

NASA/MDA/WU IFCS

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



## Self-healing Grid (1998-present)



### Building on the Foundation:

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

# Critical System Dynamics and Resilience Capabilities

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

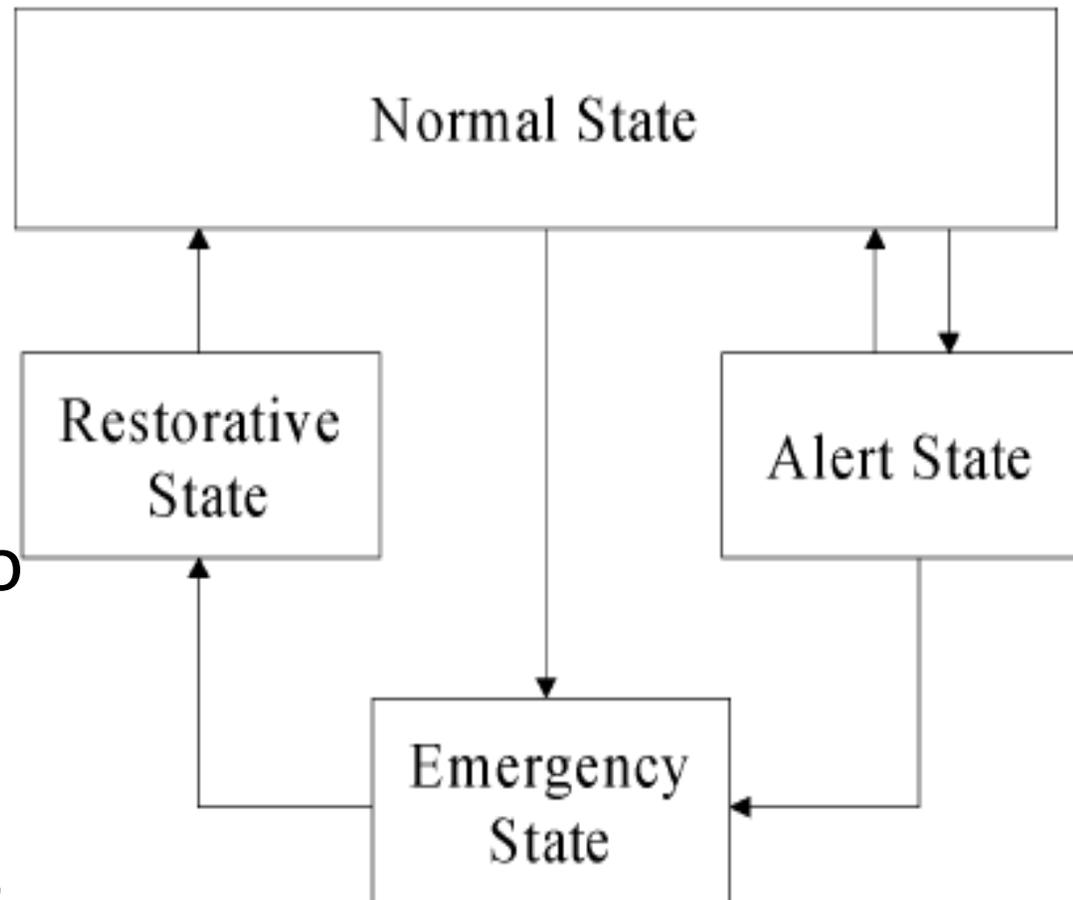
**re·sil·ience**, *noun*, 1824:  
The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress;  
An ability to recover from or adjust easily to misfortune or change

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

# Complex Dynamical Systems

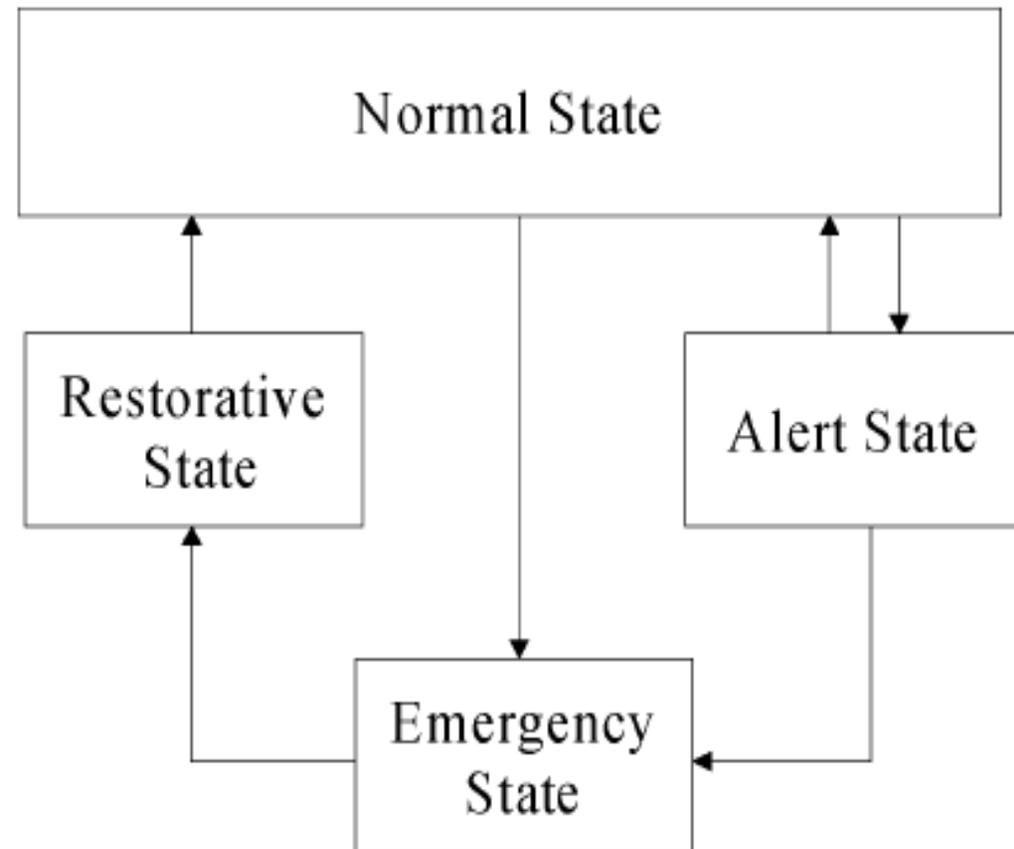
Systems have multiple “modes” during which specific operational and control actions/reactions take place

Enable complex systems to become smarter and adaptive to stressors ... detect precursors, predict, and adapt to disturbances



# Complex Dynamical 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.



# EPRI/DOD Complex Interactive Network/Systems Initiative (1998-2002) Self-healing Grid and Network-centric Objective Force

## Complex interactive networks:

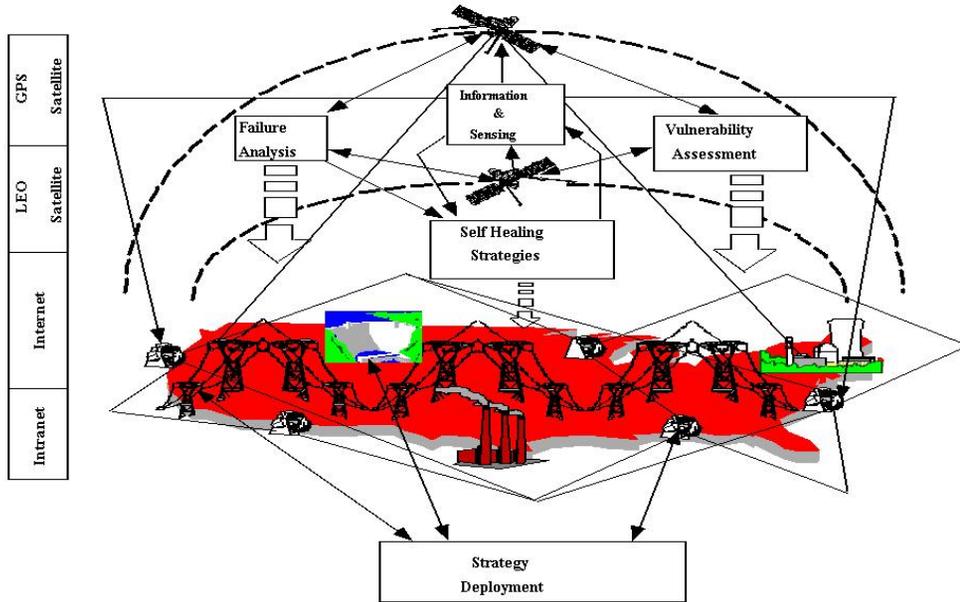
- **Energy infrastructure:** Electric power grids, water, oil and gas pipelines
- **Telecommunications:** Information, communications and satellite networks
- **Transportation and distribution networks**
- **Energy markets, banking and finance**



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

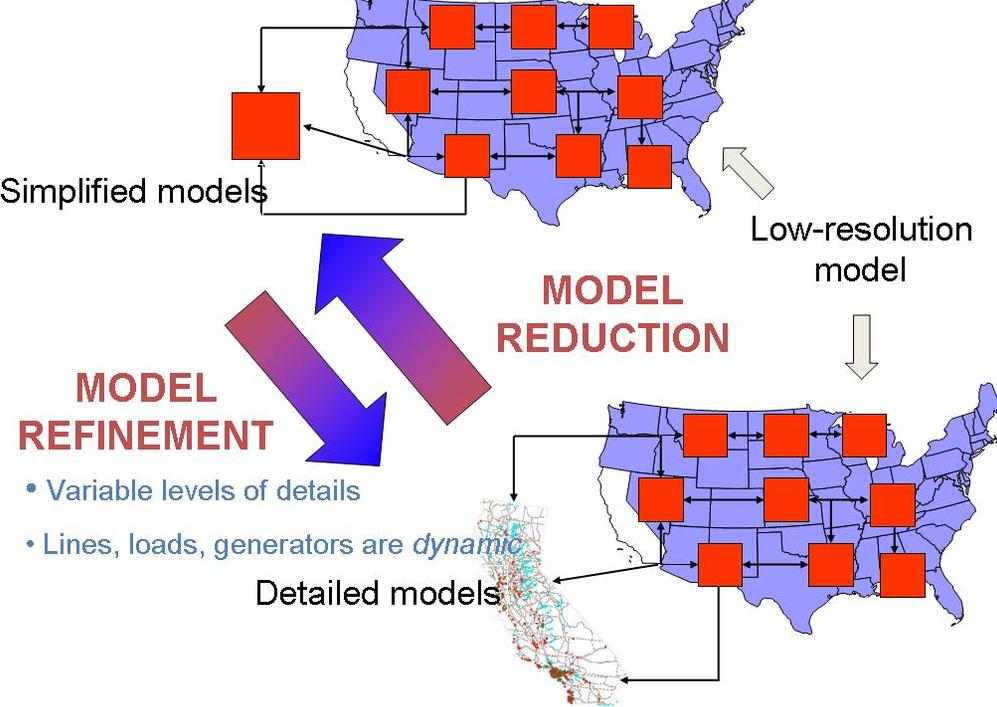


# Look-Ahead Simulation Applied to Multi-Resolution Models

- 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)

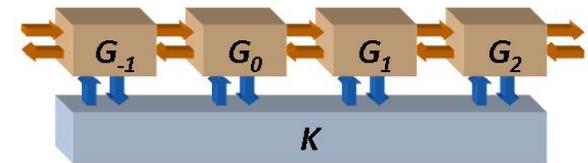


## Macro-Level Modeling: The U.S. Power Grid

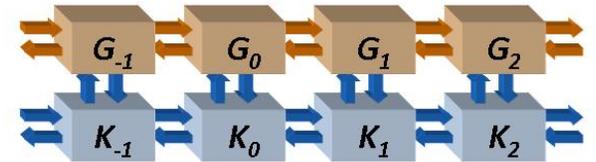


## Sensing and Control Strategies

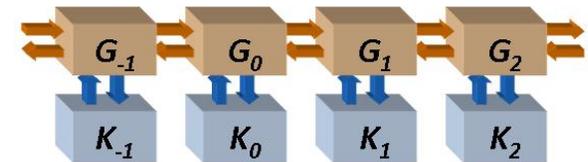
• Centralized



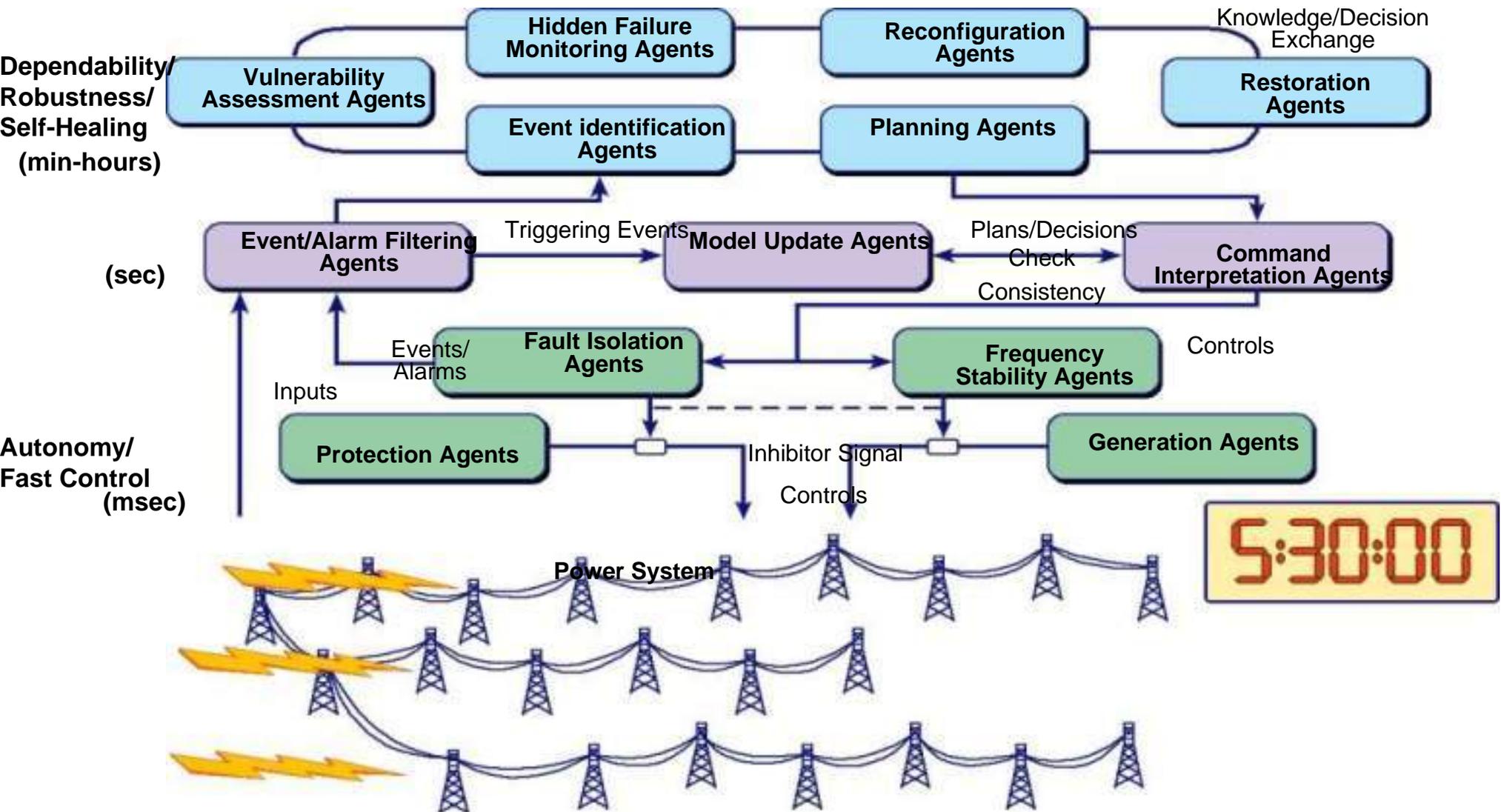
• Distributed



• Perfectly decentralized

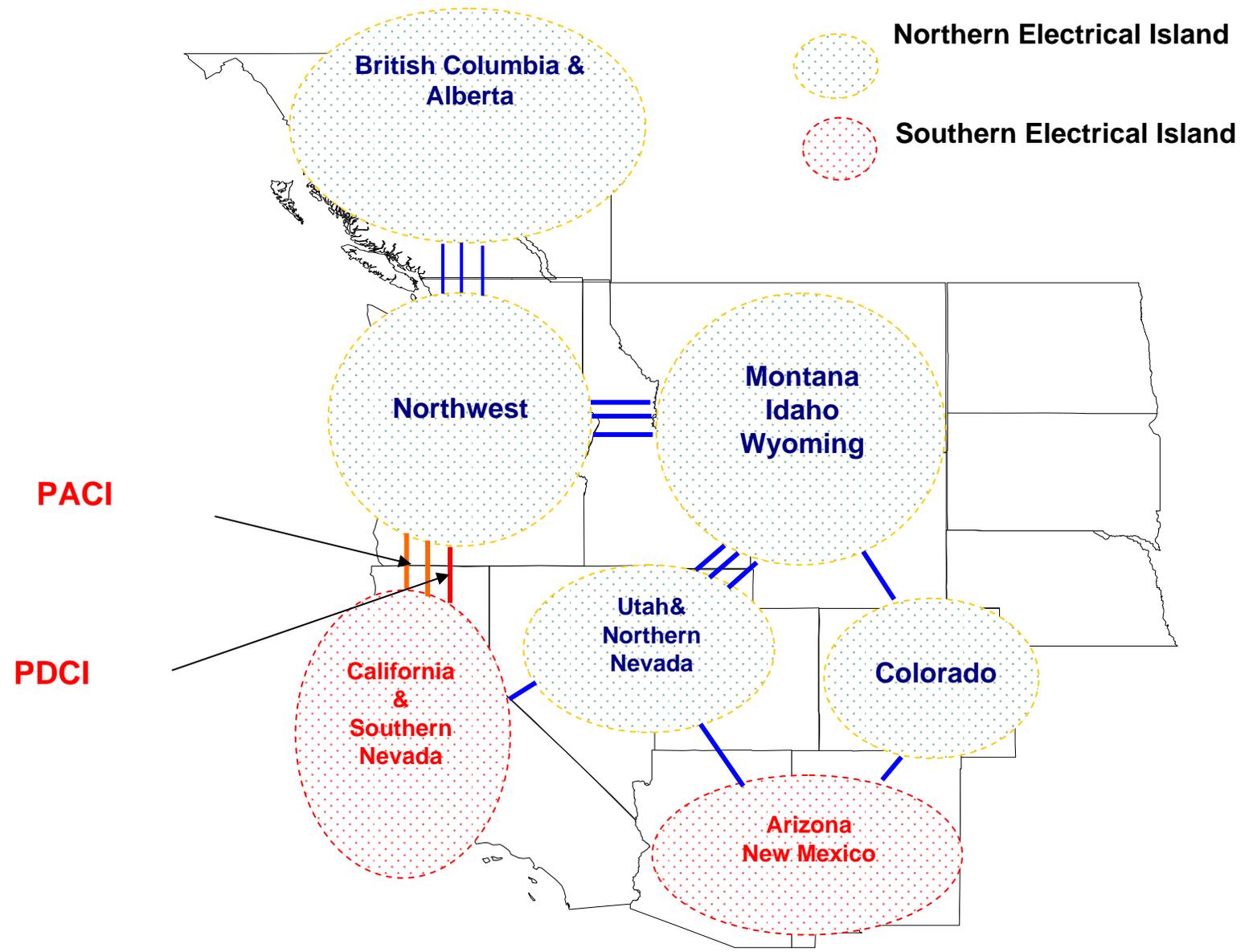


# Background: The Self-Healing Grid



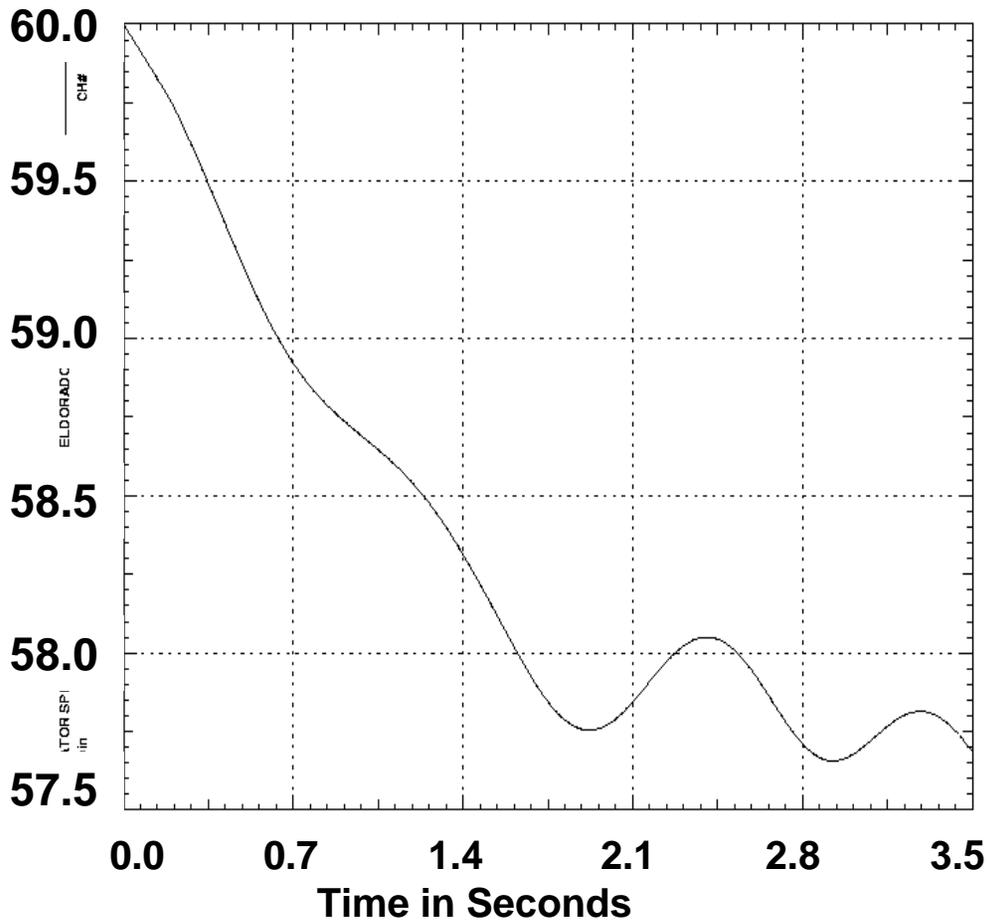
# Spectrum: Deterrence → Mitigation → Restoration

## Intelligent Adaptive Islanding: remedial action in WECC

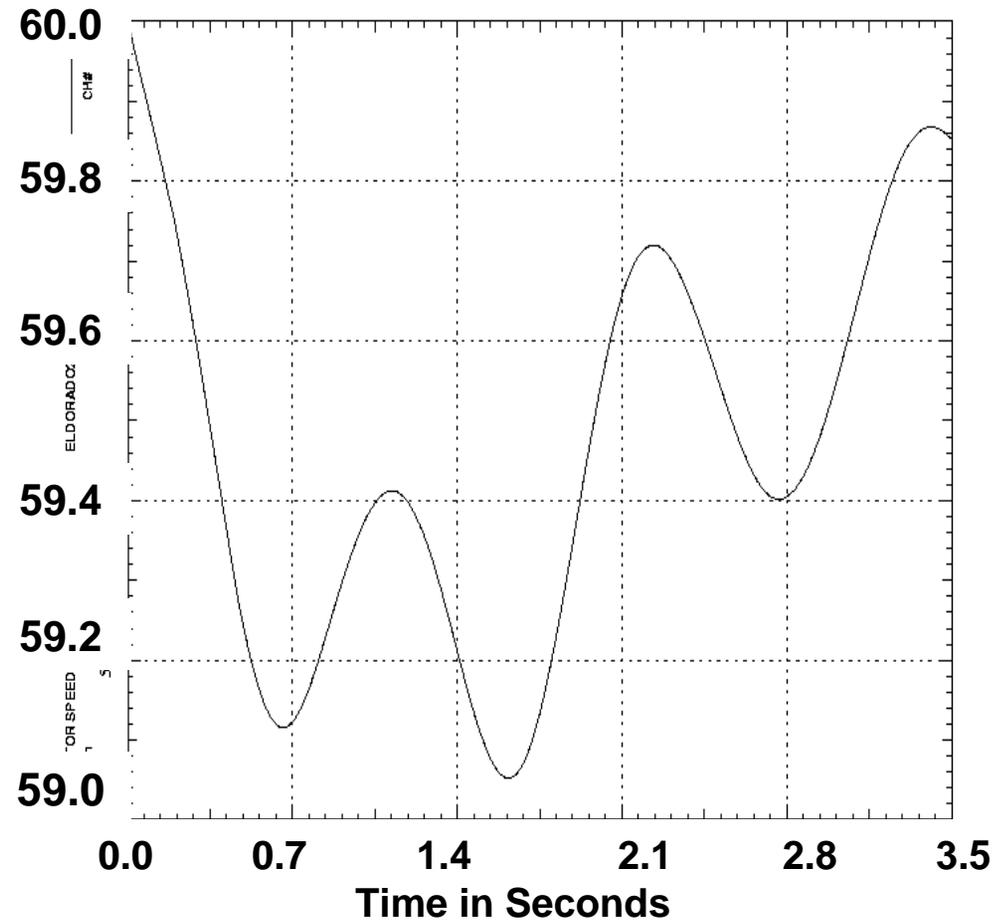




# The Self-Healing Grid



**Past Scheme**



**New Scheme**

# Critical Infrastructure Security & Protection

# 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)

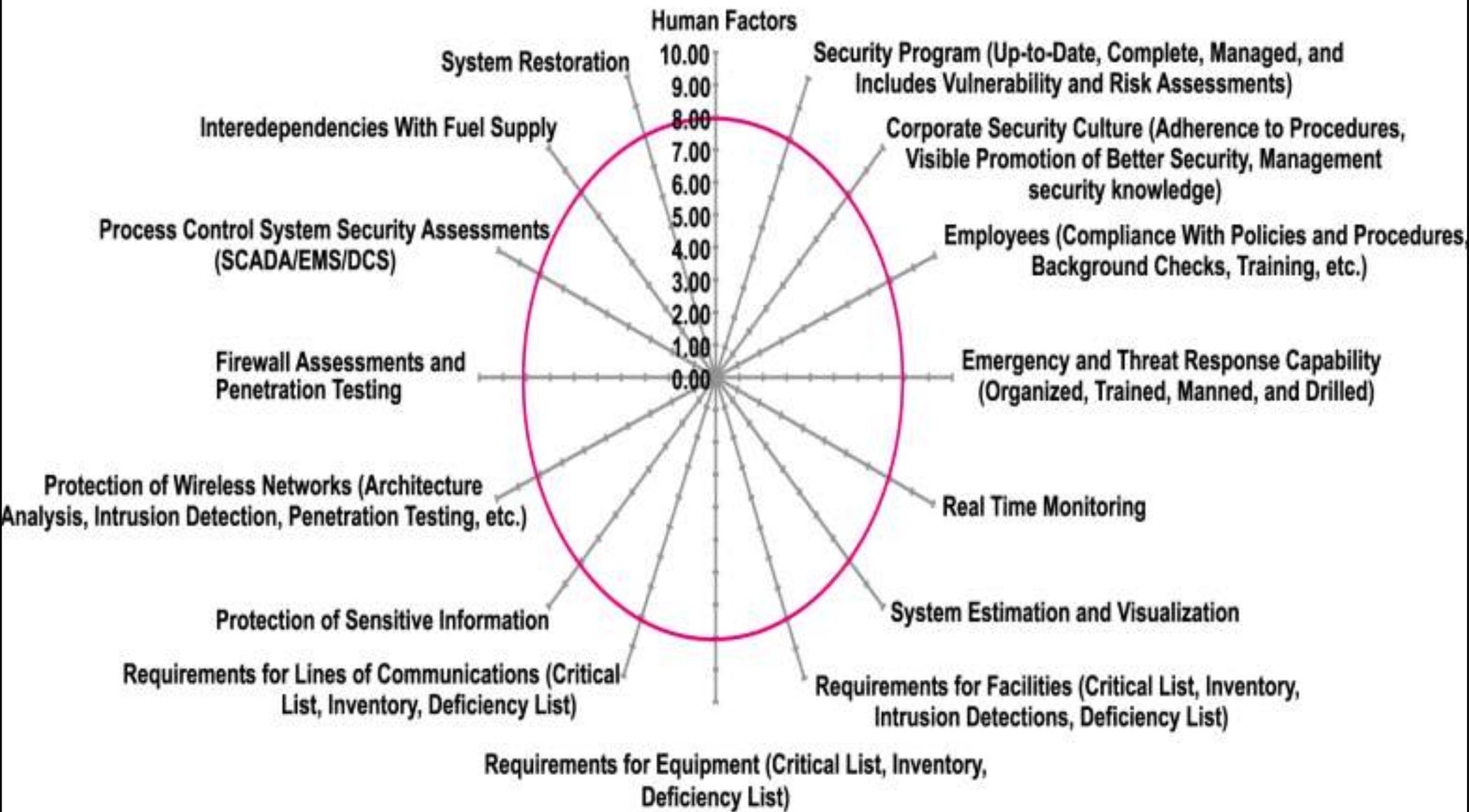
## **Physical**

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

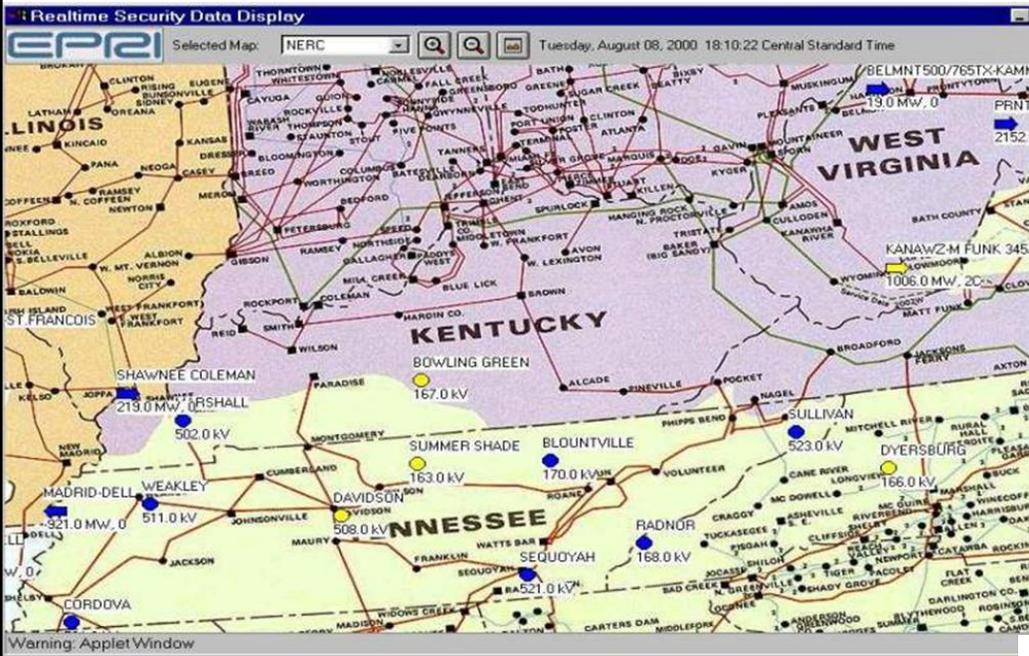
## **Cyber and IT**

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



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



# Fast Power Systems Risk Assessment

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



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



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

# Fast Power Grid Simulation



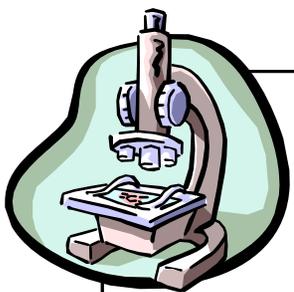
CRAY Supercomputer

Nvidia GeForce GPU card for PC

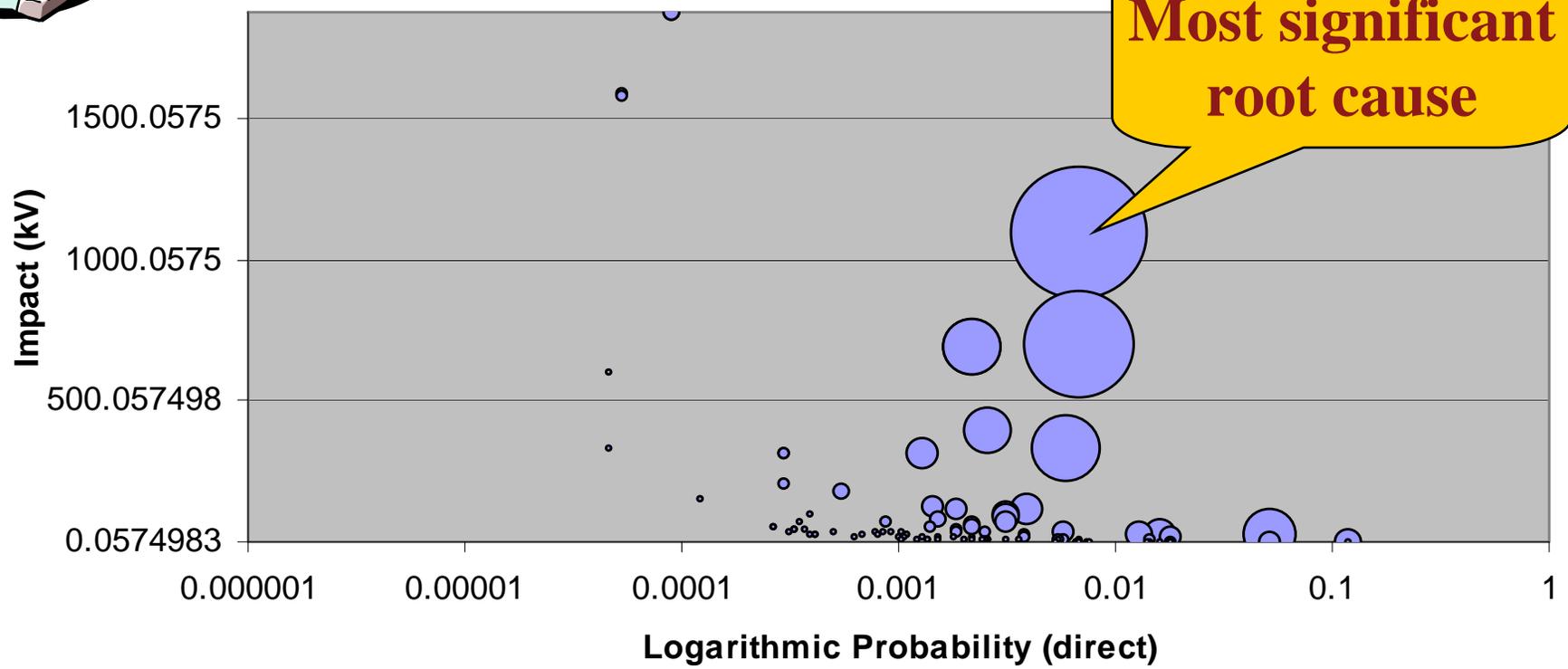


- Use Nvidia GeForce GPU card to gain 15 times faster power flow calculation on PC (Laurie Miller)

# Example of In Depth Analysis: Critical Contingency Situations

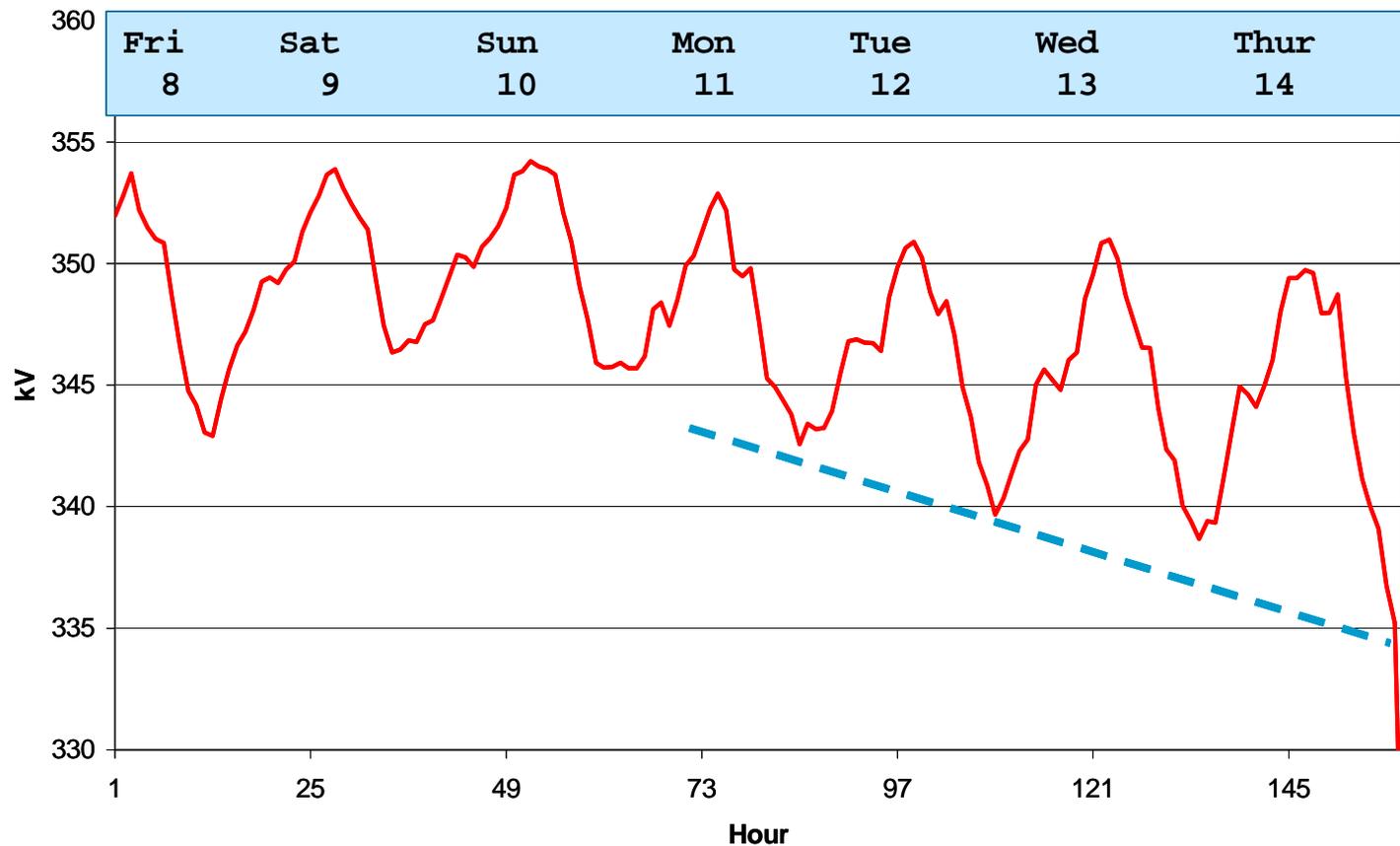


Critical Root Causes in the Proba/Voltage Impact State space (Region Cause: all, Affected Region: all)



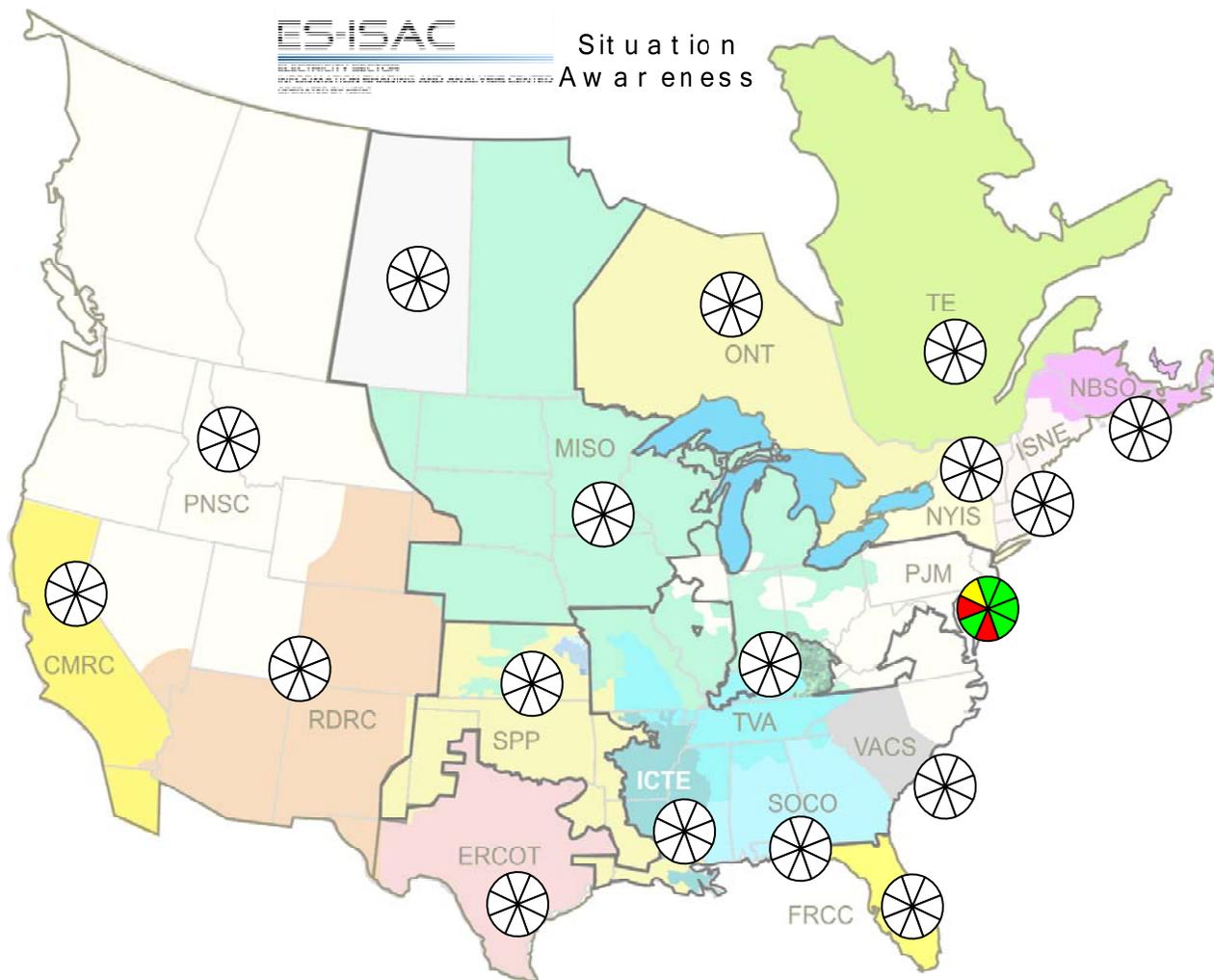
# Initial Conditions on August 14, 2003

STAR-345 kV BUS  
Aug 8-14, 2003

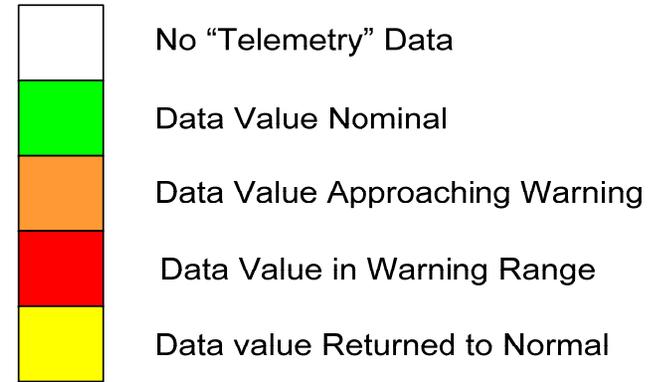
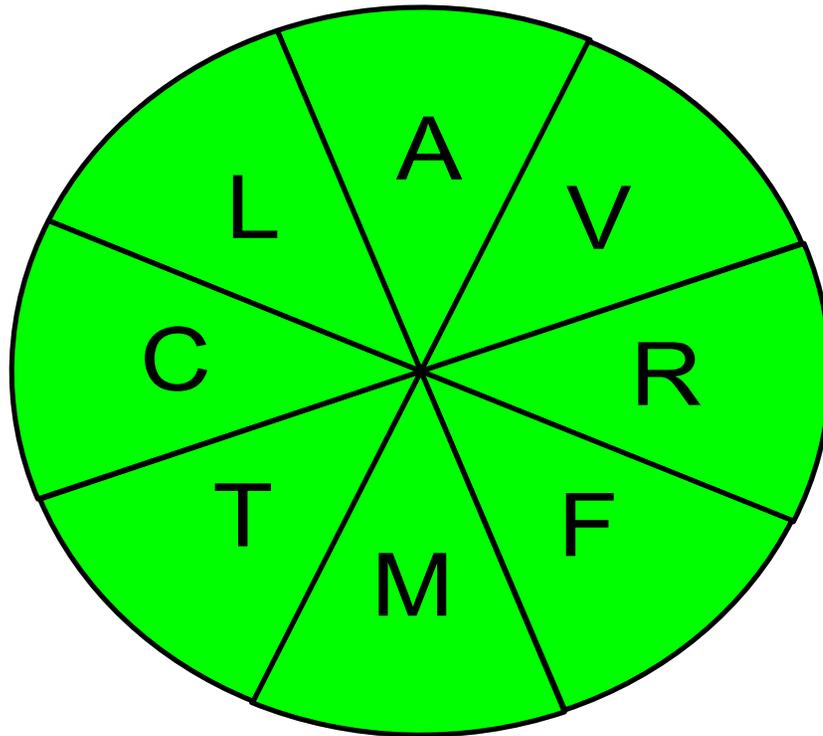


Star 345 kV Bus Voltages (Aug 8-14, 2003)

# Situation Awareness Tool (SAT)



# Situation Awareness Tool (SAT)



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

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

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

**University of Minnesota Center for Smart Grid Technologies (2003-present)**

Dept. of Electrical & Computer Engineering

Faculty: Professors Massoud Amin and Bruce Wollenberg

PhD Candidates/Research Assistants: Anthony Giacomoni, Jesse Gantz, Laurie Miller, and Sara Mullen (PhD 9/9)

PI: M. Amin (support from EPRI, NSF, Honeywell, SNL, ORNL, and UofM funding)

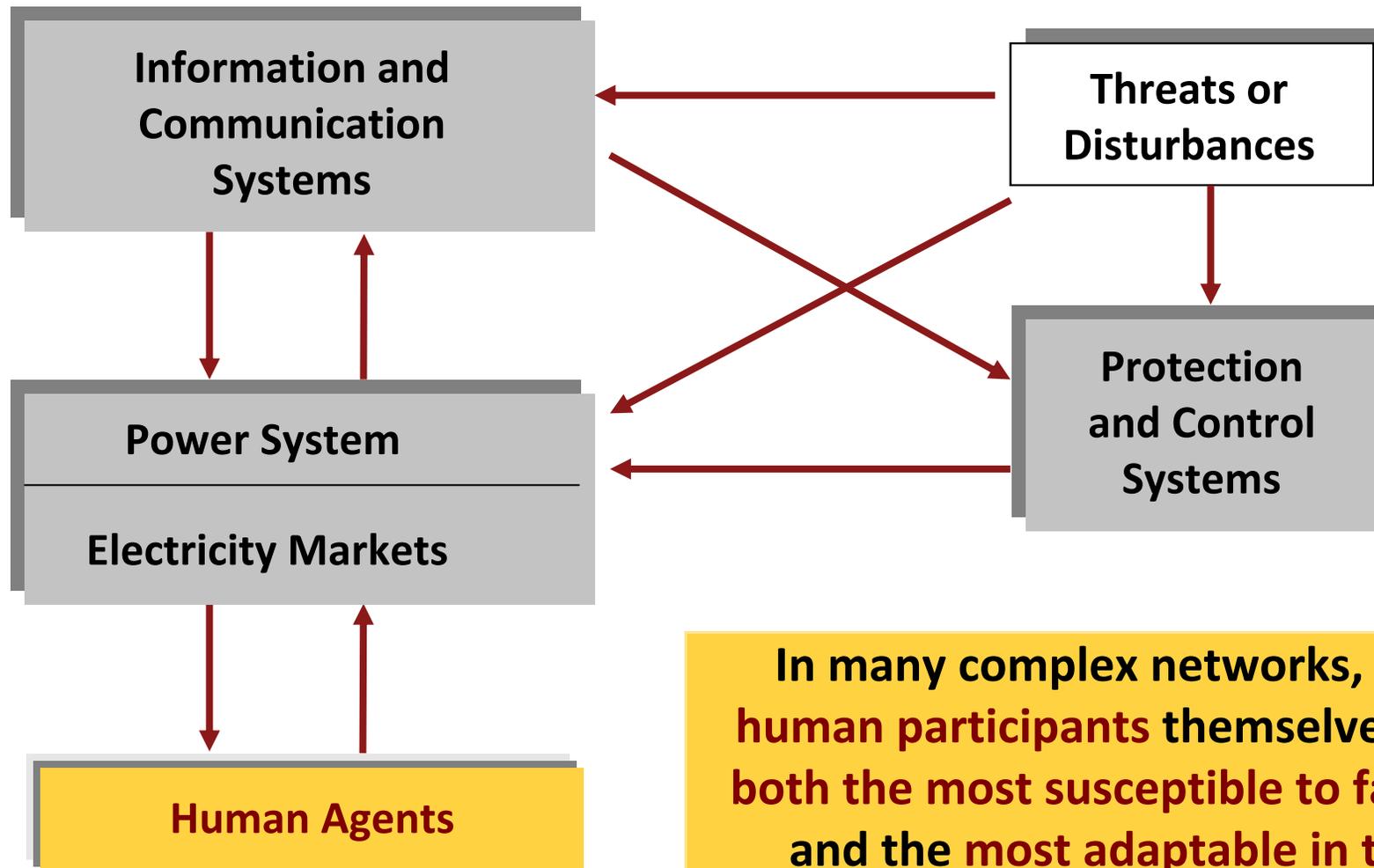


# Objectives

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



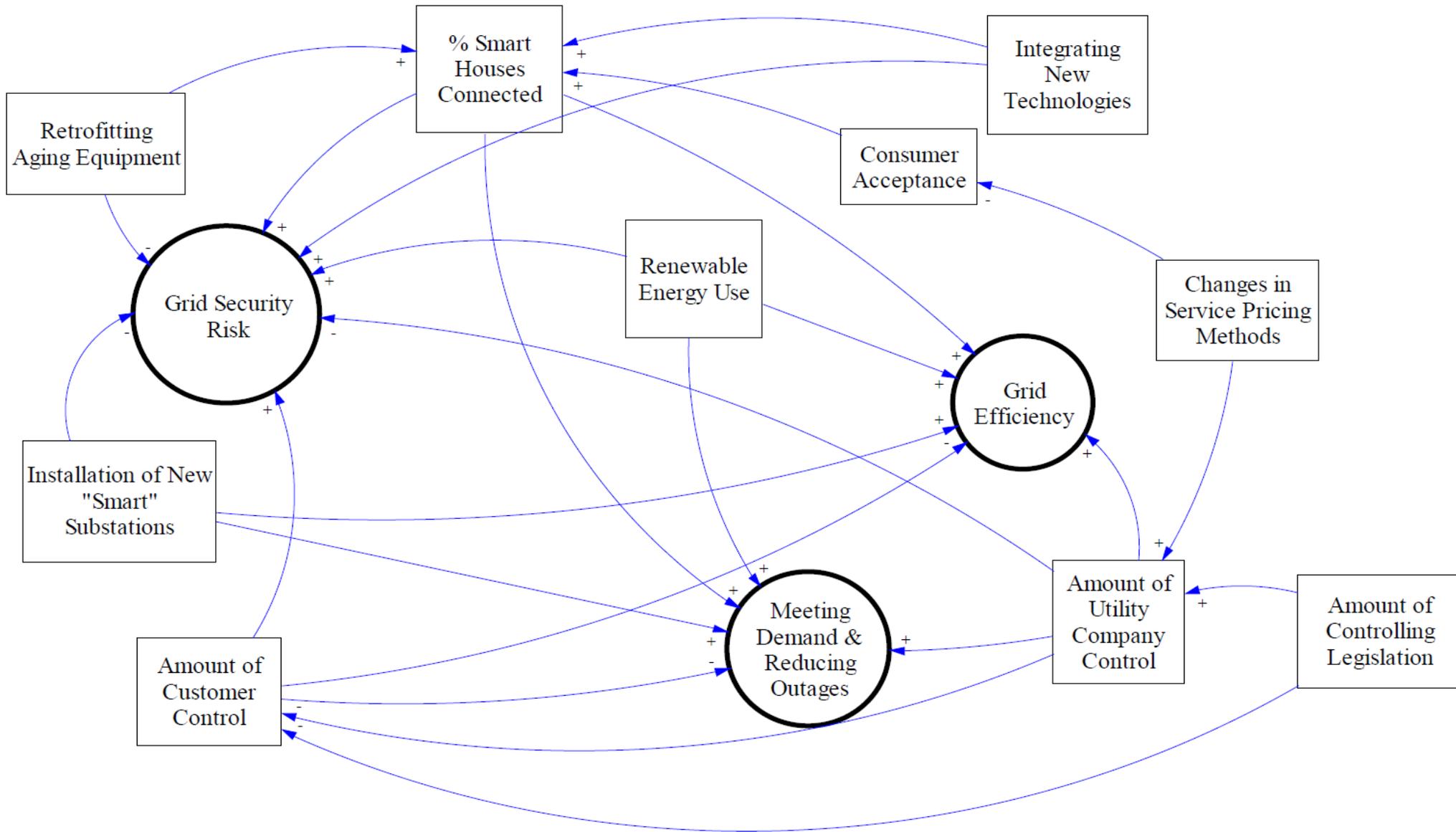
# Integrated Sensing, Protection and Control



**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 Interdependencies

## Security, Efficiency, and Resilience



# Smart Grid as a Distributed Computer

... the State Estimator



# Transmission Limits

- High dimensional problem
  - Large interconnection models (1/5 of the North American system) require ~40,000 buses & ~50,000 lines, and ~3,000 generators with ~120 control areas
  - Each line has a capacity limit
  - N-1 Contingency Criteria: The system must withstand the loss of any one line or generator (~53,000 contingencies)
    - $53,000 \times 50,000 = 2,650,000,000$  possible constraints
- Reliable operation requires an operating point that satisfy these 2.65 billion constraints!

# 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

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

$R$  = The measurement error covariance matrix

Extended to Advanced Topology Estimator:

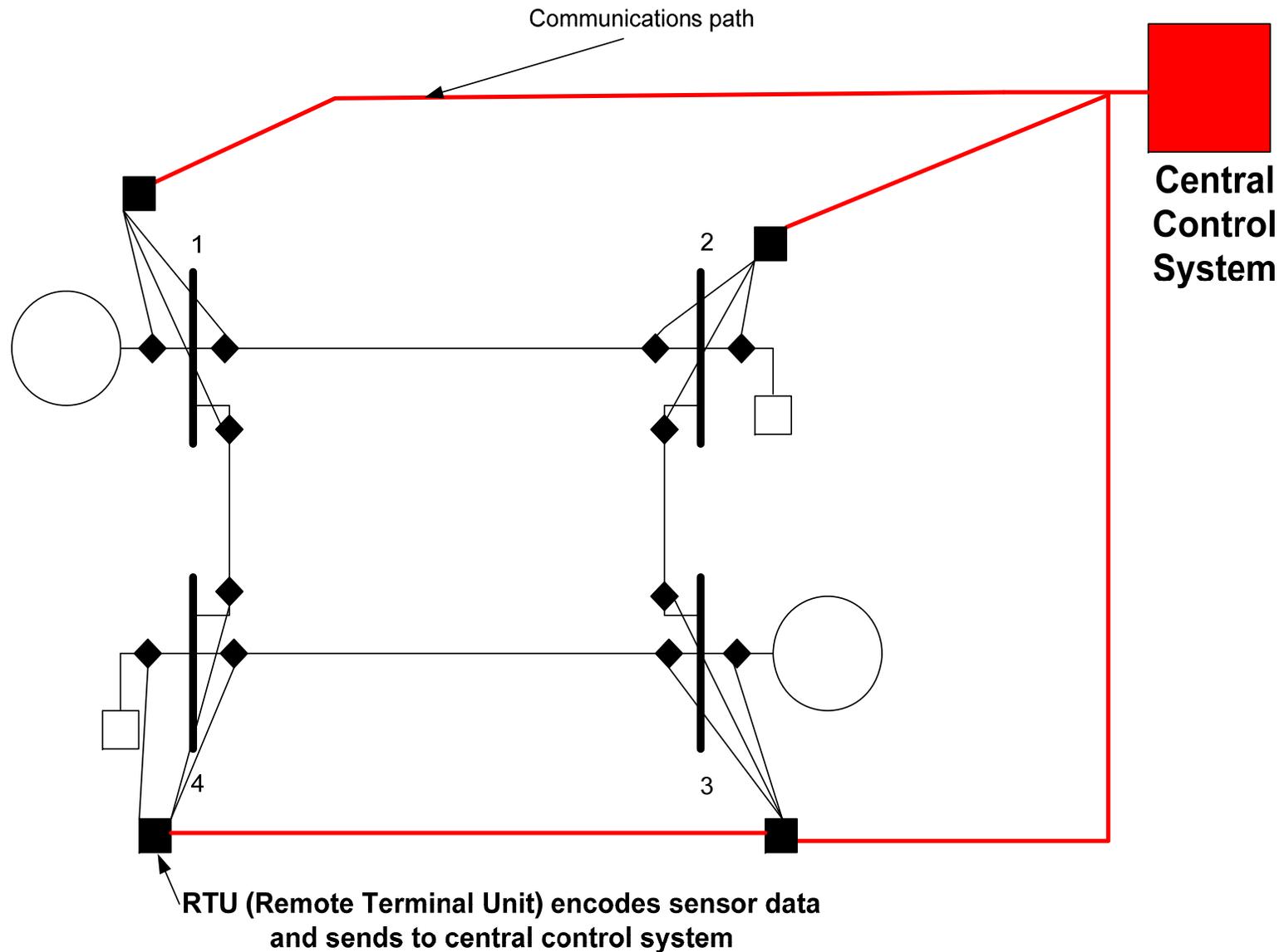
- determine unknown substation switch settings from voltages, power flows, and current measurements

# Distributed State Estimation & System Identification

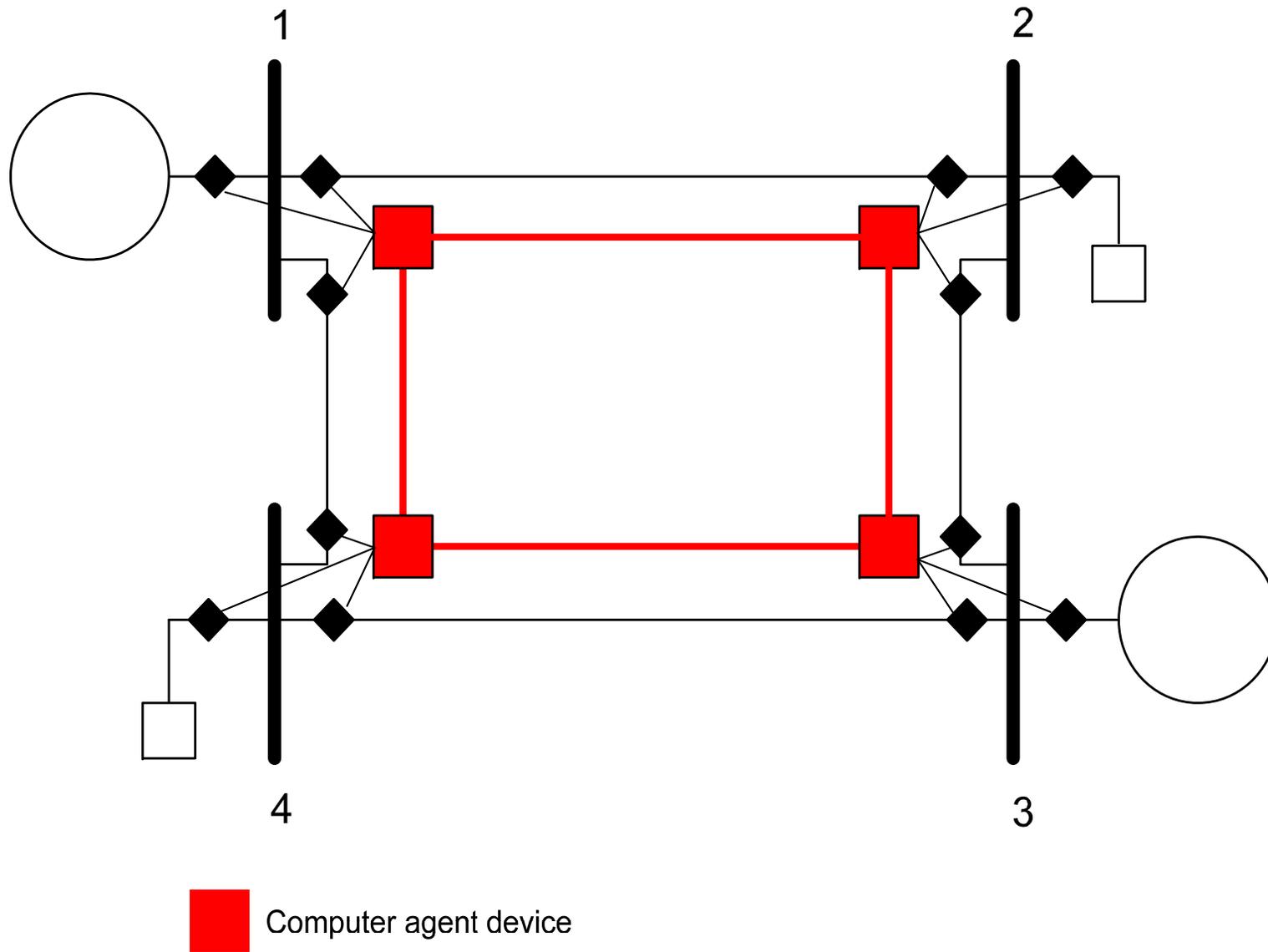
## → Look-ahead Simulation

- Process of using a set of over determined, noisy measurements to estimate the system state
  - $V$  and  $\theta$  are the state variables in our problem
  - We use measurements that are functions of  $V$  and  $\theta$  to form our estimate
- One of the first milestones in moving towards a Smart Grid is demonstrating that distributed state estimation is workable

# Central computer control system



# Using the grid agents to do power system state estimation calculation



# Relevant equations

- PQ node (typical load node):

$$P_k = V_k \sum_{m=1}^n V_m (G_{km} \cos \theta_{km} + B_{km} \sin \theta_{km})$$

$$Q_k = V_k \sum_{m=1}^n V_m (G_{km} \sin \theta_{km} + B_{km} \cos \theta_{km})$$

- PV node (typical generator node) has same P equation and trivial V equation
- Line Flow Equations

$$P_{ij} = -G_{ij} V_i^2 + V_i V_j (G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij})$$

$$Q_{ij} = -B_{ij} V_i^2 + V_i V_j (G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij}) - V_i^2 B_{capij}$$

- In our case, each bus has six measurements so we write 6 equations

# Algorithm

- 1. Choose Slack Bus
- 2. Make initial guess for voltages and phases
- 3. Determine measurement error

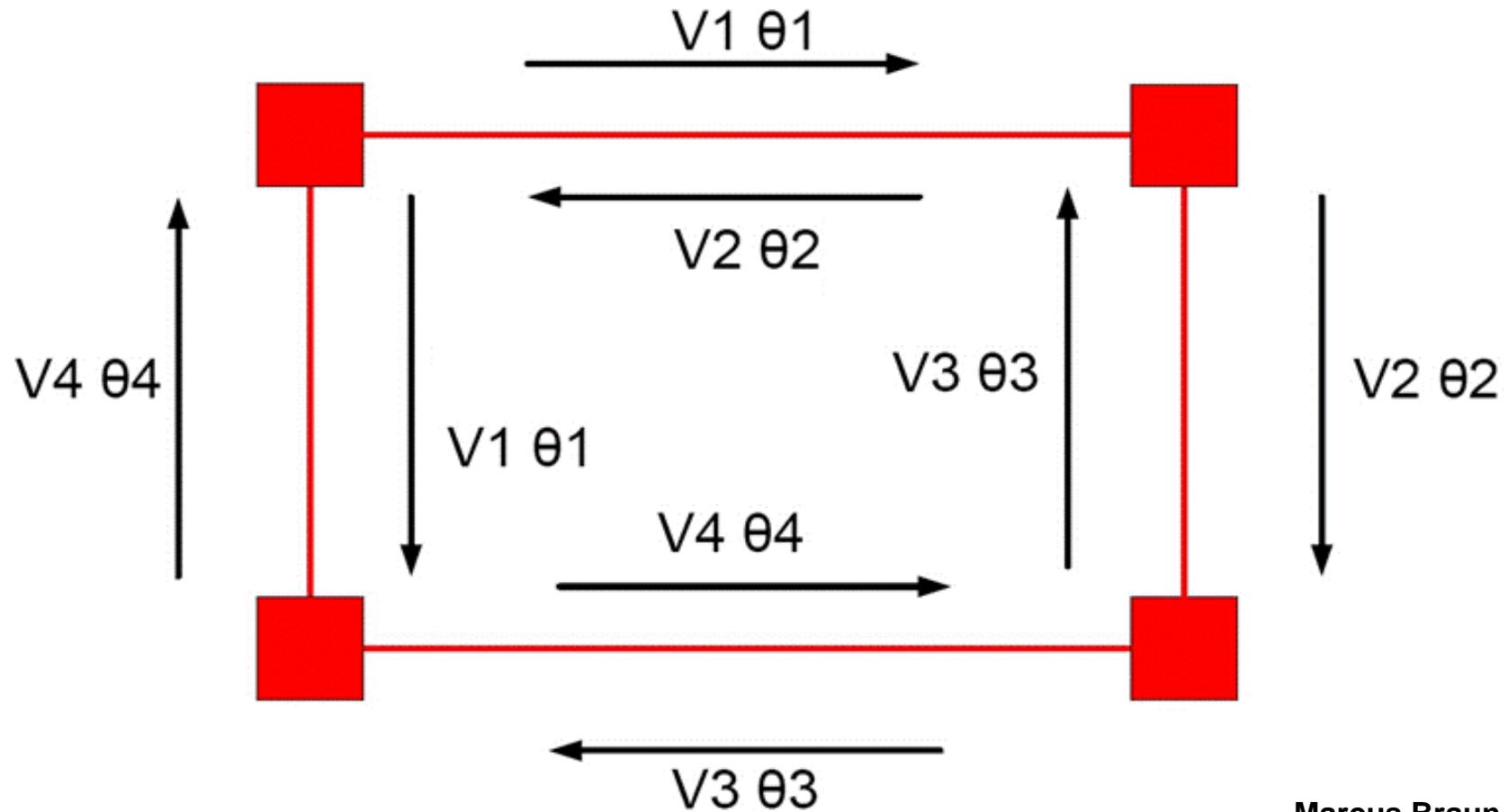
$$error = (z_{meas_i} - f_i(\vec{V}, \vec{\theta}))$$

- 4. Calculate Jacobian as a function of  $V, \theta$
- 5. Compute correction

$$\Delta \vec{x} = (J^T R^{-1} J)^{-1} J^T R^{-1} \begin{bmatrix} z_1 - f_1(\vec{V}, \vec{\theta}) \\ z_2 - f_2(\vec{V}, \vec{\theta}) \\ \vdots \end{bmatrix}$$

- 6. Determine if a component of the correction vector exceeds  $\epsilon$
- 7. If so, apply correction, repeat steps 3-6
- 8. Share state variables with adjacent nodes
- 9. Repeat

# Exchange of data



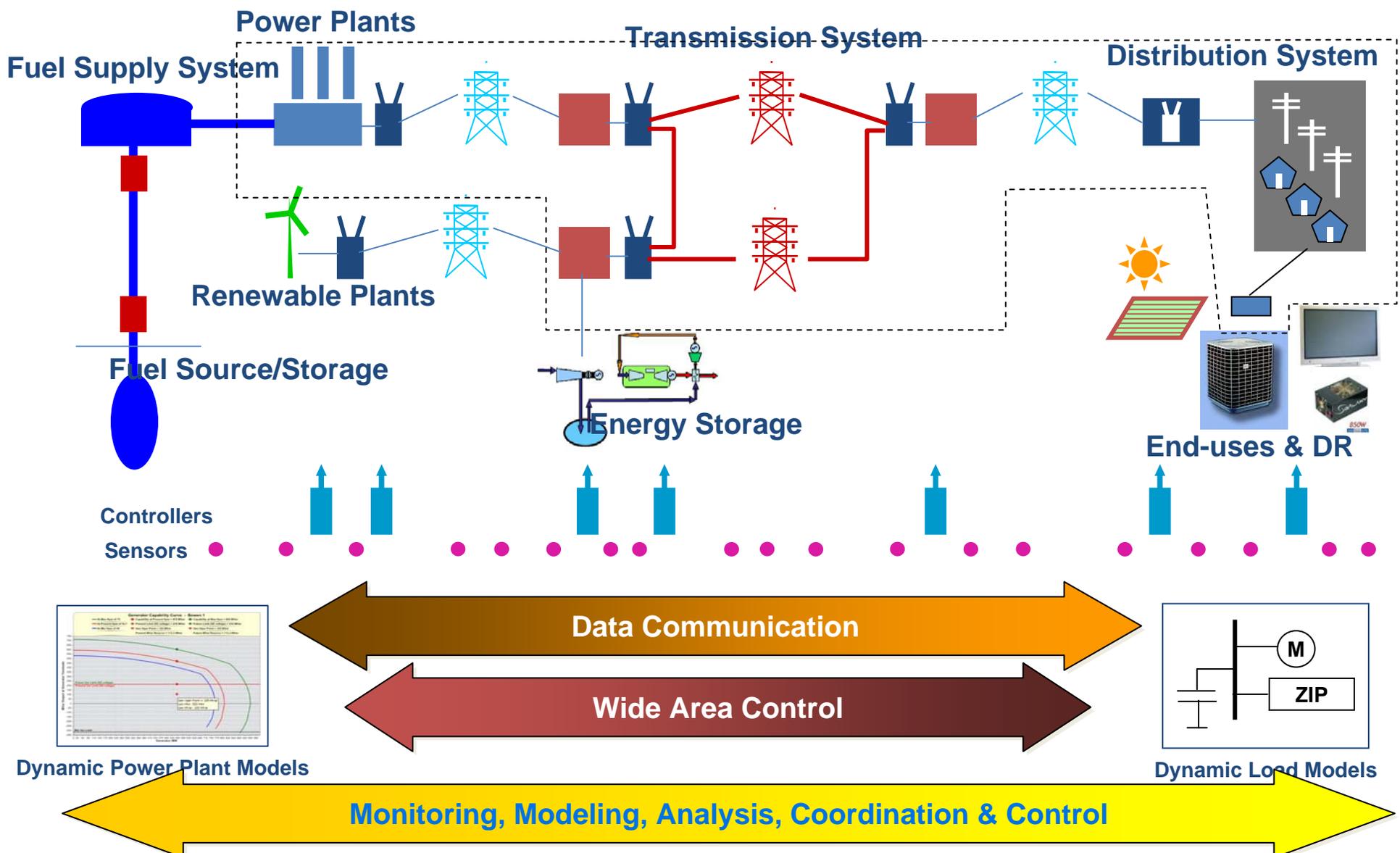
Marcus Braun

**Gives rapid reliable algorithm convergence**

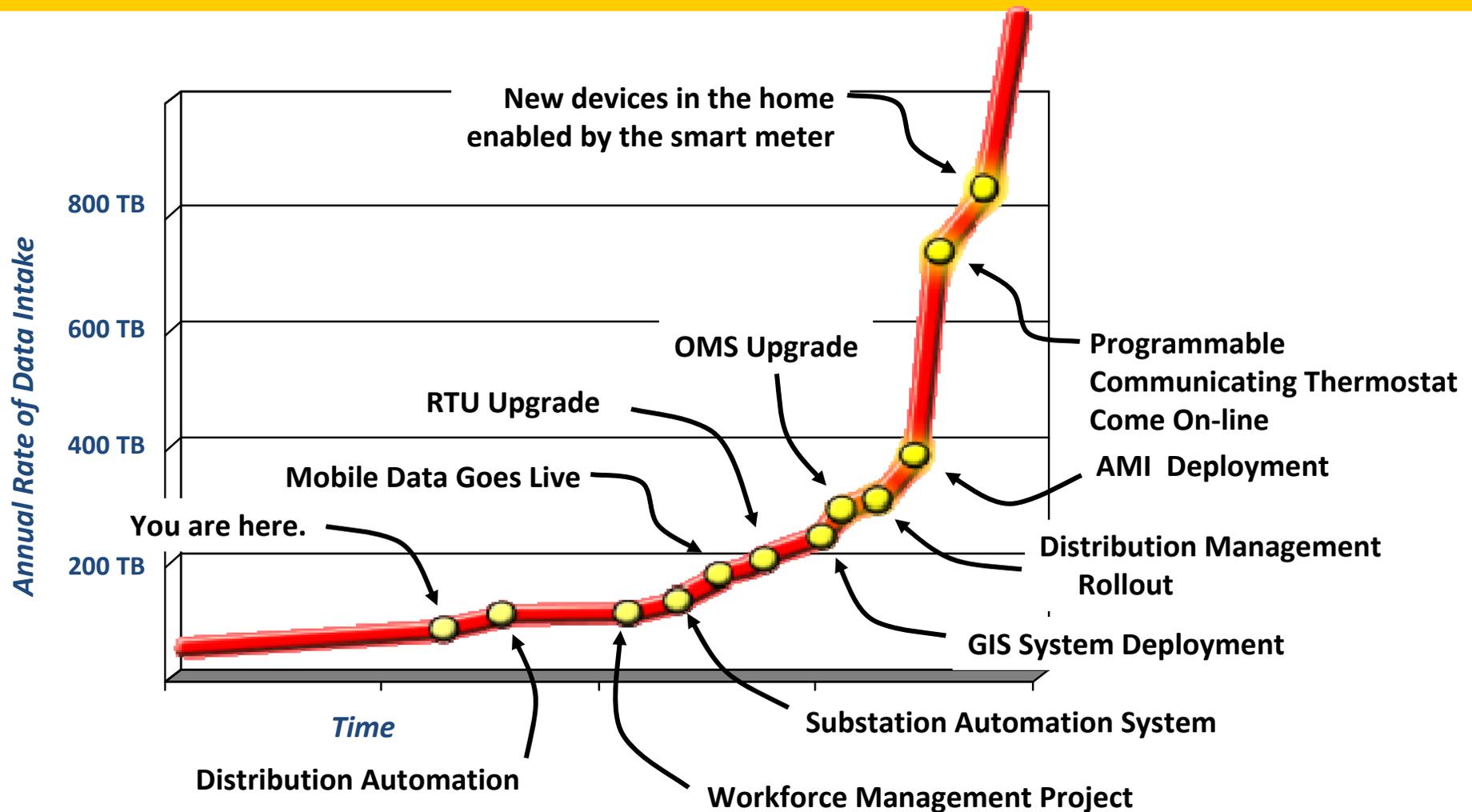
# Smart Grid Protection Schemes & Communication Requirements

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	

# End-to-End Power Delivery Operation & Planning



# 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**

# New Challenges for a Smart Grid

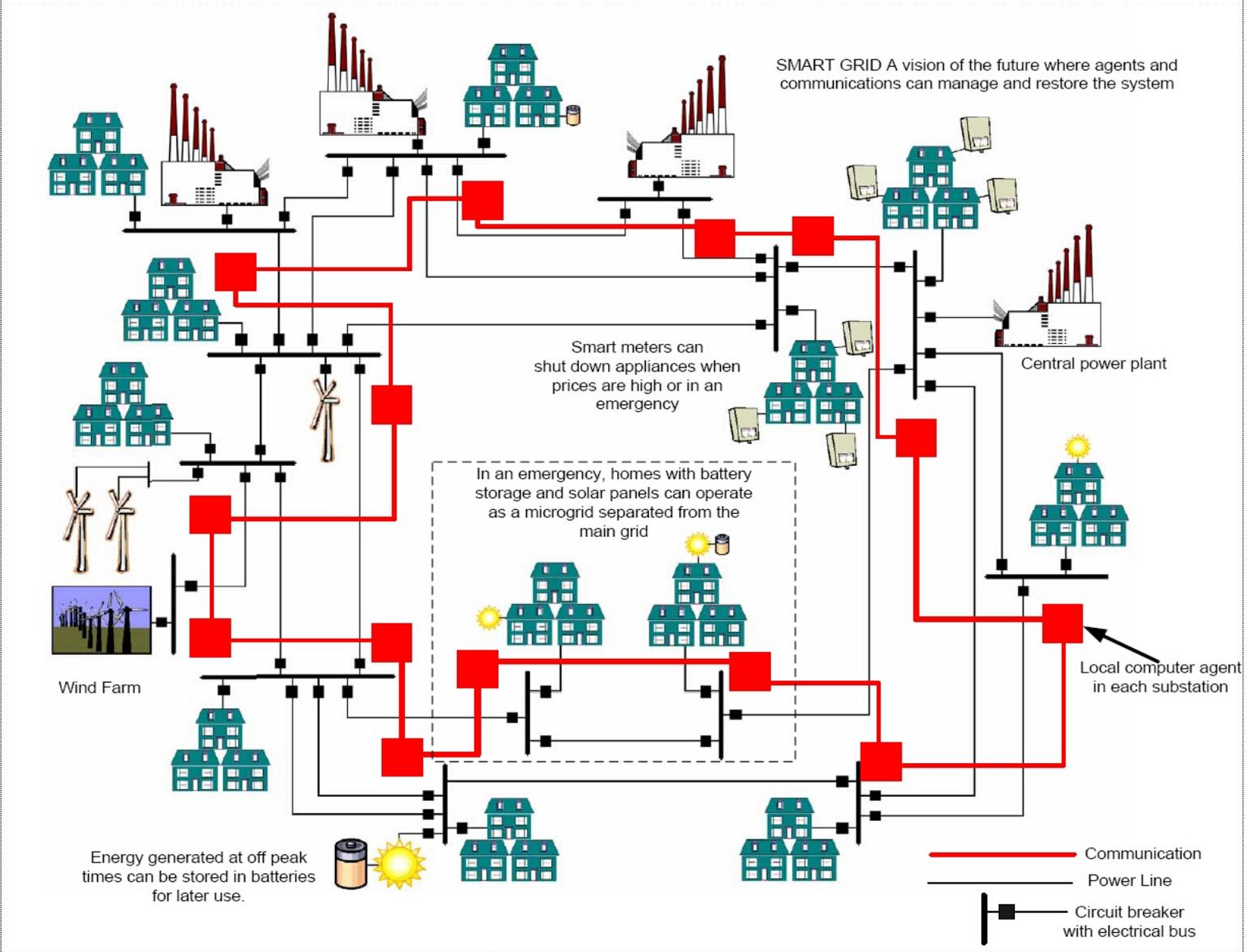
- Need to integrate:
  - Large-scale stochastic (uncertain) renewable generation
  - Electric energy storage
  - Distributed generation
  - Plug-in hybrid electric vehicles
  - Demand response (smart meters)
- Need to deploy and integrate:
  - New Synchronized measurement technologies
  - New sensors
  - New System Integrity Protection Schemes (SIPS)
- Critical Security Controls

# New Challenges for a Smart Grid

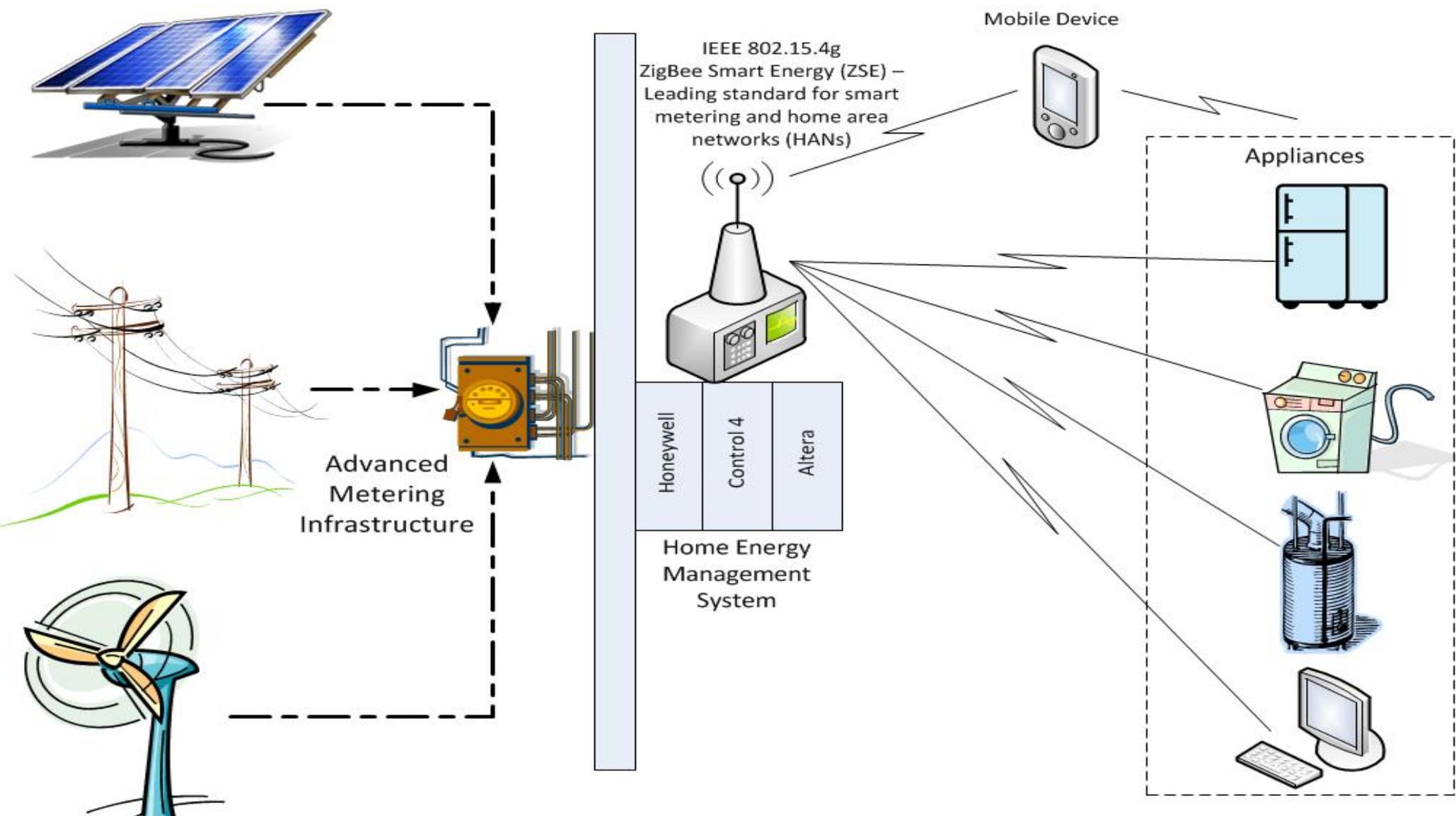
- **Cybersecurity and Interoperability**

- 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 a Smart Grid architecture; priorities for interoperability standards, including cybersecurity: **NISTIR 7628**

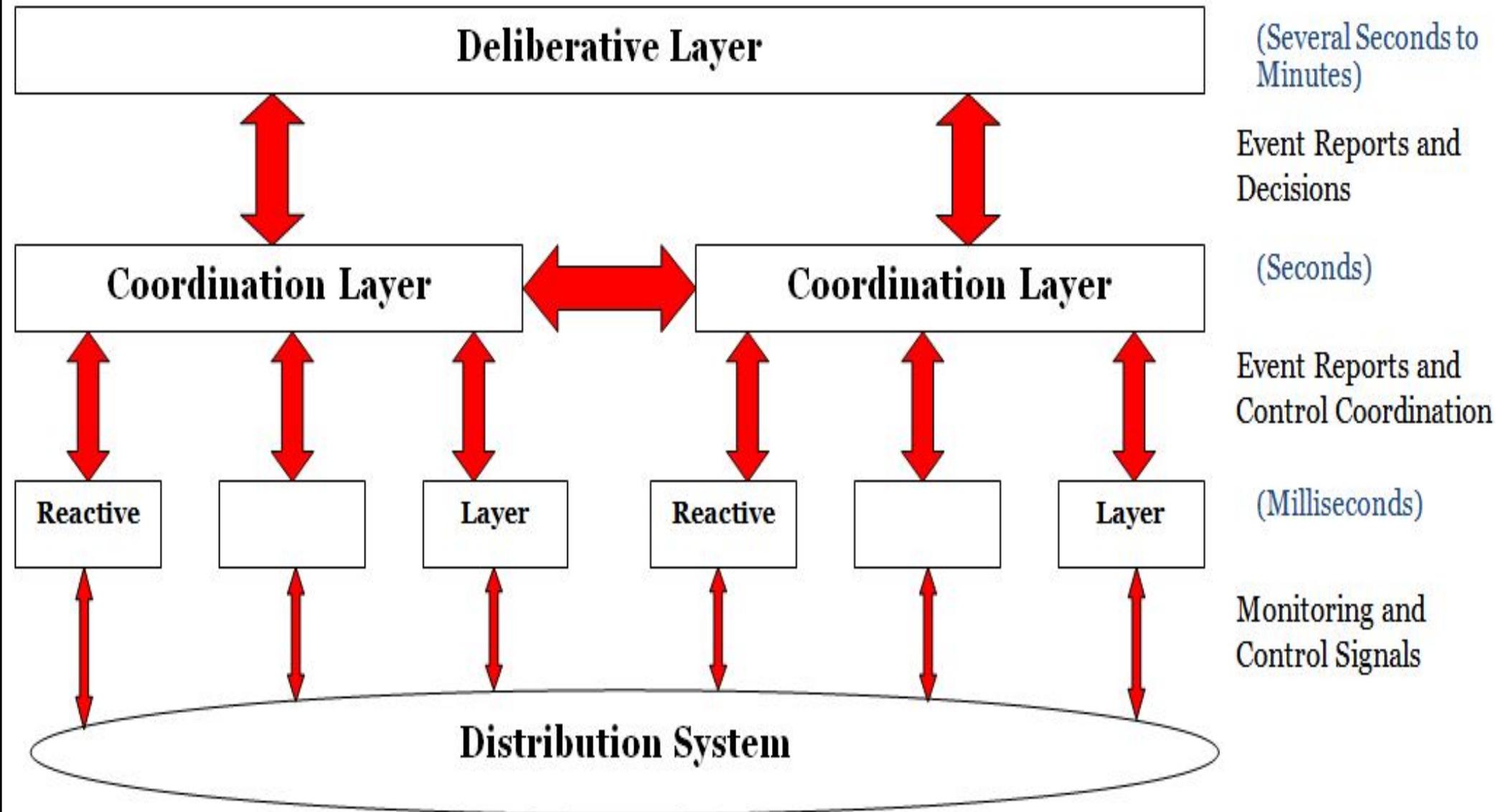
# Our team's Smart Grid Research



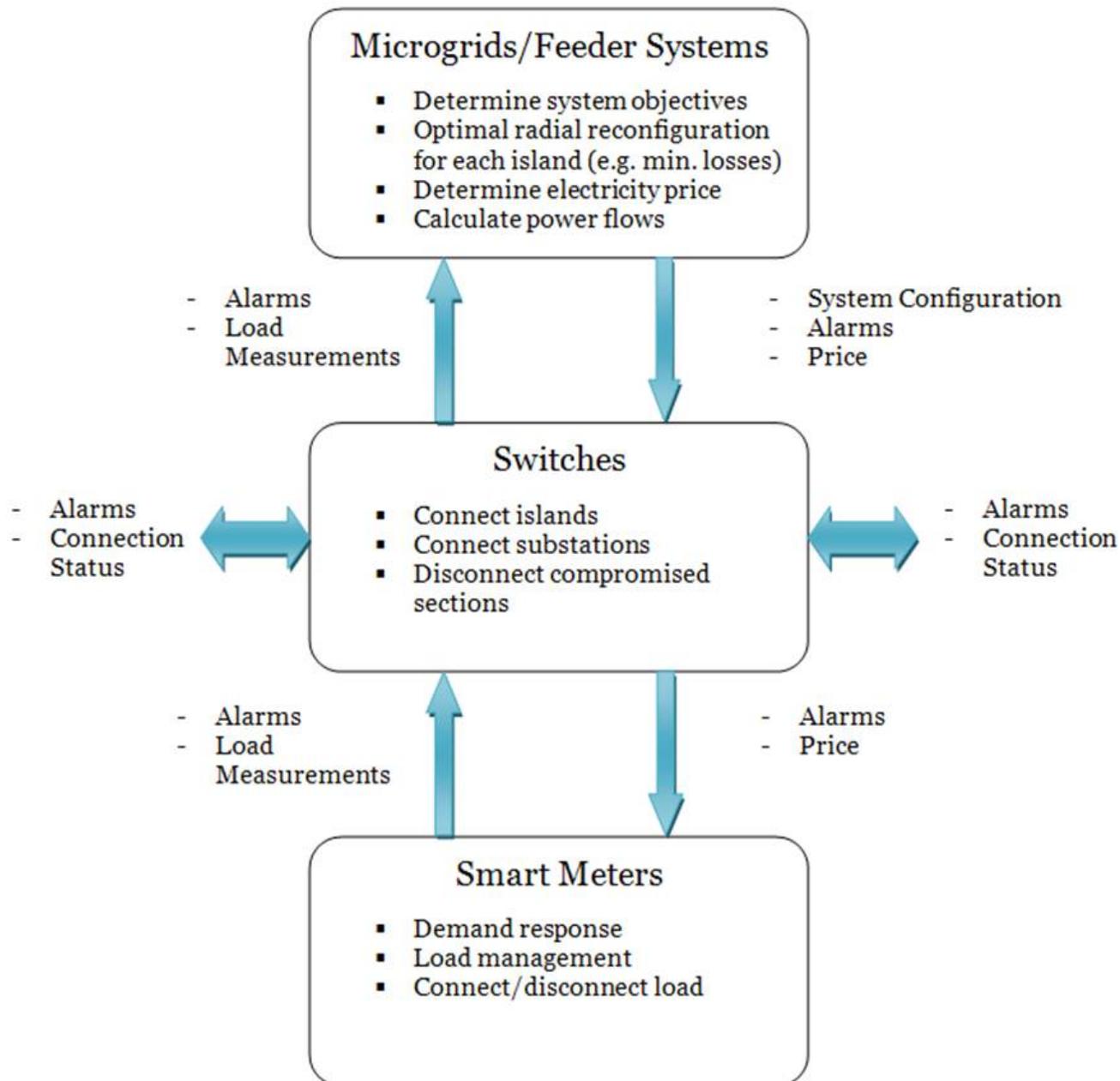
# Local System Communication Overlay



# Intelligent Distributed Secure Distribution System Control Architecture



# Distribution System Intelligent Agent Control Functions and Signals

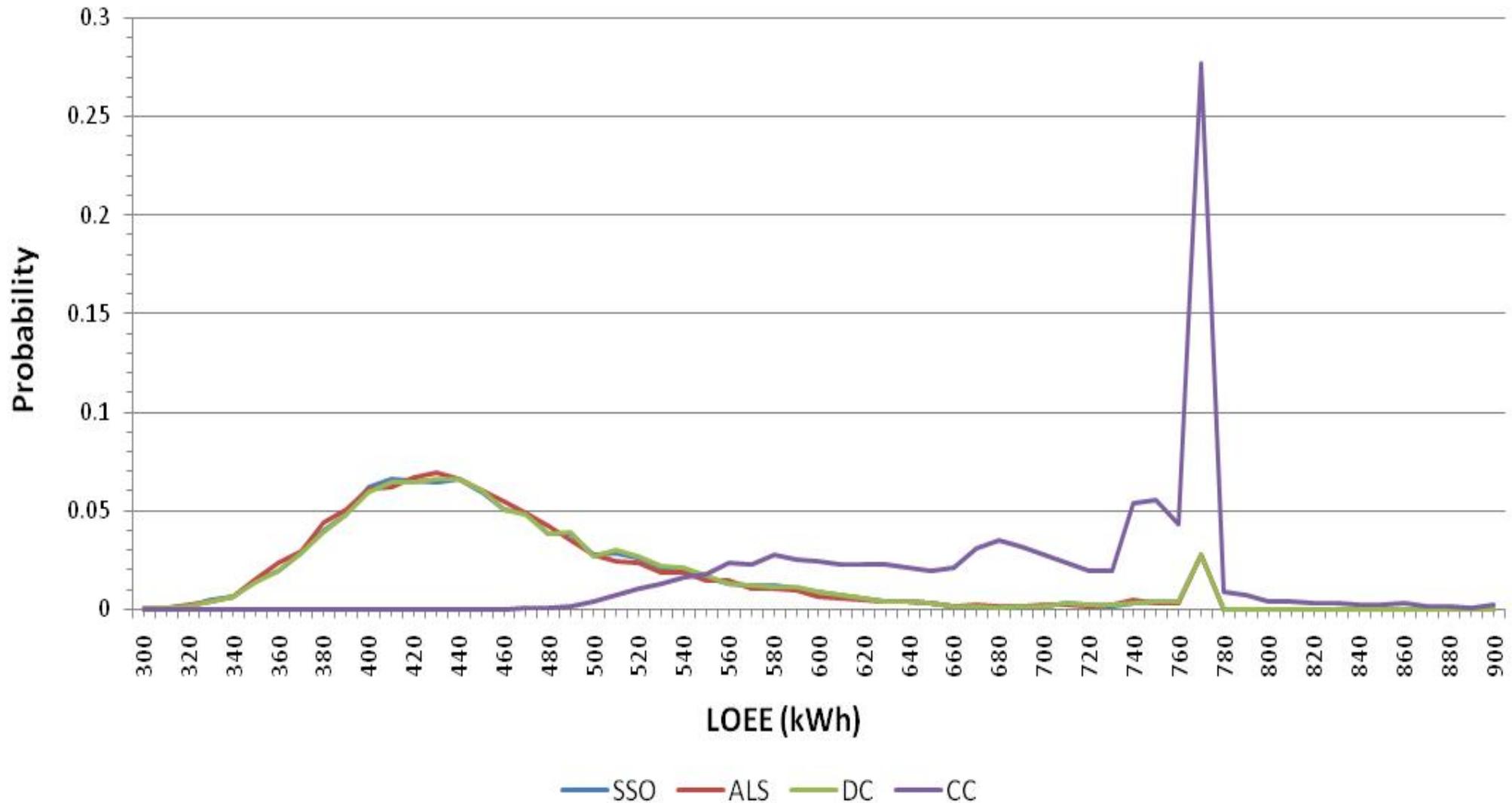


# Intelligent Agents and Functionalities

Layer	Agent Locations	Control Functions
Reactive	-Smart Meters -Substations	<ul style="list-style-type: none"> <li>- Demand response</li> <li>- Load management</li> <li>- Connect/disconnect load</li> <li>- Send alarm signals</li> </ul>
Coordination	-Switches	<ul style="list-style-type: none"> <li>- Connect islands</li> <li>- Connect substations</li> <li>- Disconnect compromised sections</li> <li>- Send alarm signals</li> </ul>
Deliberative	-Microgrids/Feeder Systems	<ul style="list-style-type: none"> <li>- Determine system objectives</li> <li>- Optimal radial reconfiguration for each island (e.g. min. losses)</li> <li>- Determine electricity price</li> <li>- Calculate power flows</li> <li>- Send alarm signals</li> </ul>

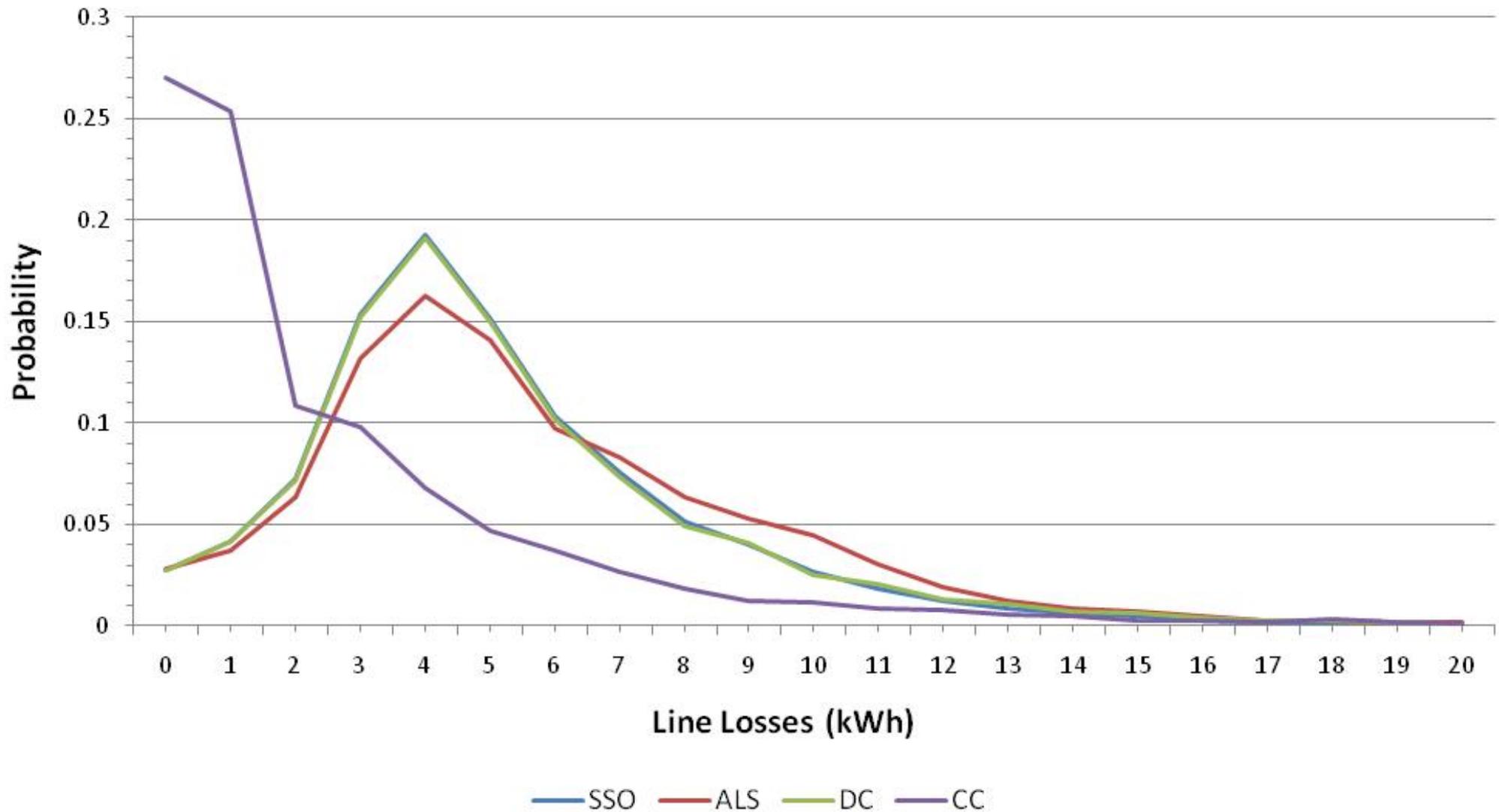
# Centralized or Decentralized Control?

## Control Architecture LOEE Probability Distributions



# Centralized or Decentralized Control?

## Control Architecture Line Losses Probability Distributions



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

Albert Einstein



# I-35W bridge

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

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

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

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



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

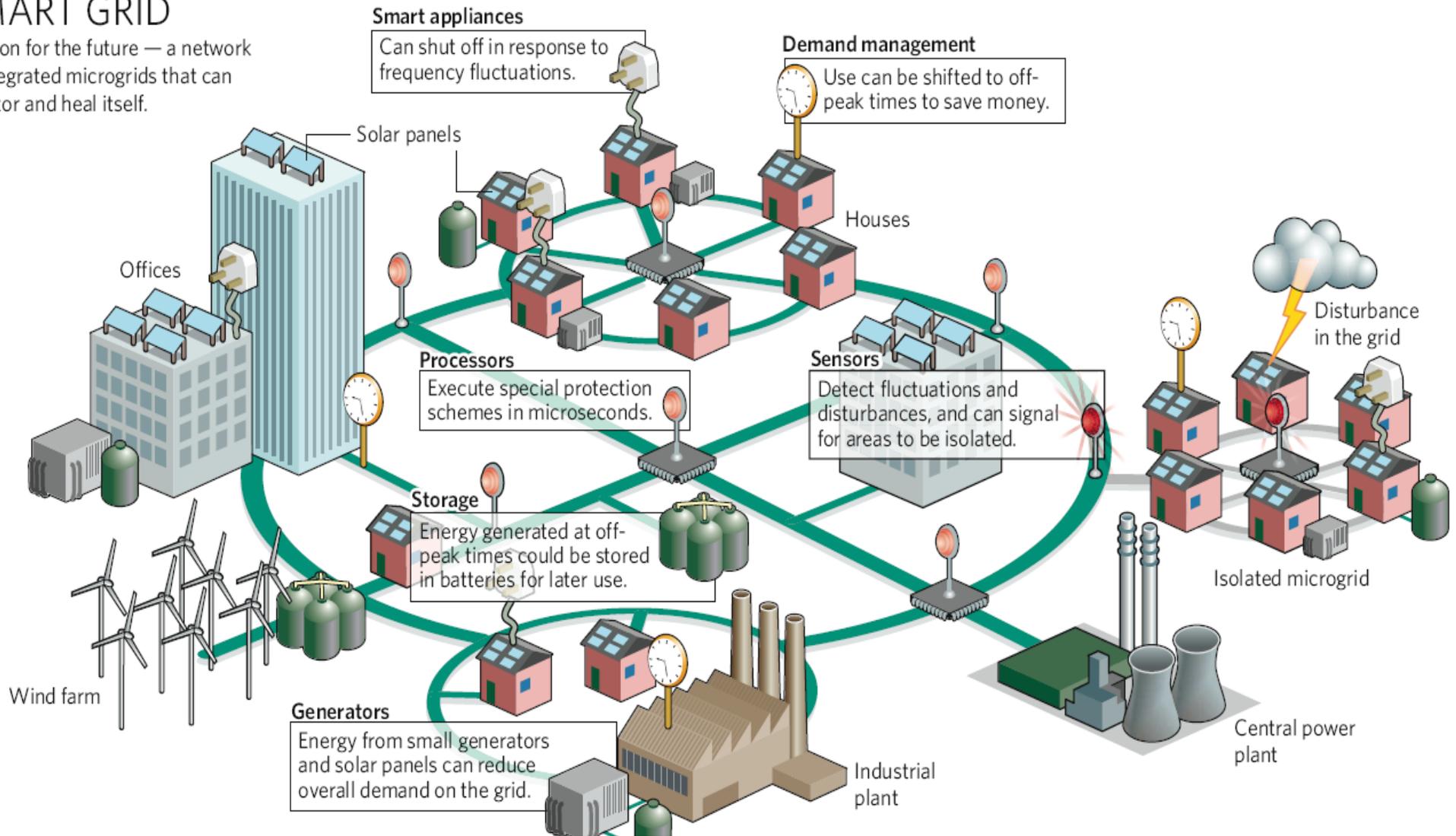


# Enabling the Future

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

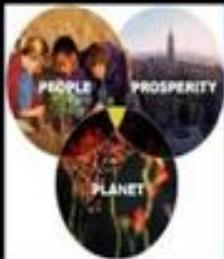
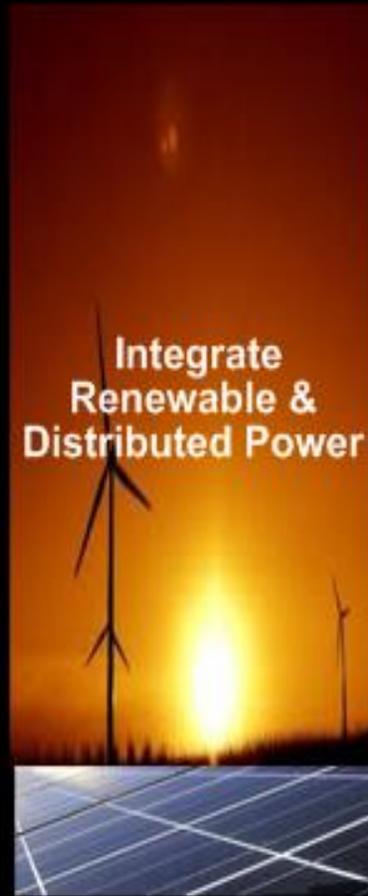
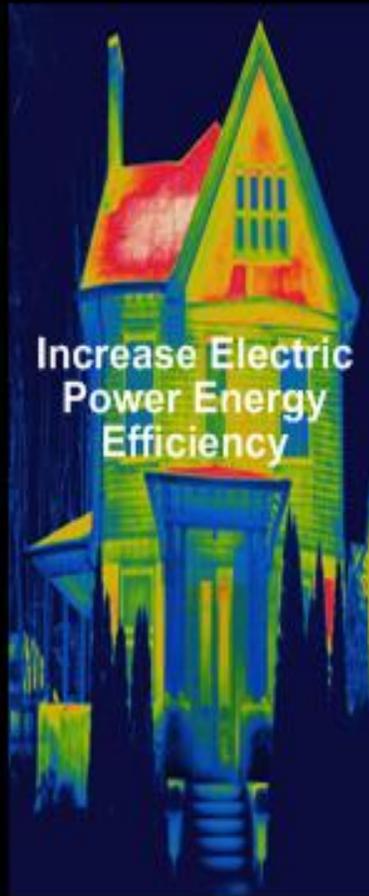
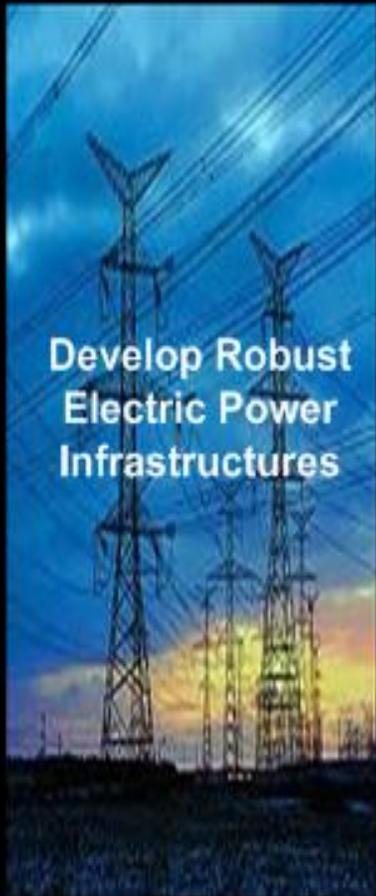
### SMART GRID

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

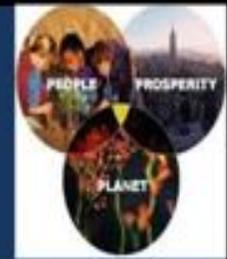


Source: Interview with Massoud Amin, "Upgrading the grid," *Nature*, vol. 454, pp. 570–573, 30 July 2008

# Smart Grid Goals



Sustainable Electrical Power



# R&D challenges

- Develop a theoretical framework, modeling and simulation tools for interdependencies and their fundamental characteristics, to provide:
  - An understanding of true dynamics and impact on coupled infrastructure robustness and reliability.
  - An understanding of emergent behaviors, and analysis of multi-scale and complexity issues and trends in the future growth and operations.
  - Real-time state estimation and visualization of infrastructures-- flexible and rapidly adaptable modeling and estimation
- 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).
  - Data mining and early signature detection
  - Infrastructure databases.

# Selected Areas in Applied Mathematics

## Dynamical Systems and Controls

- **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.

# R&D Challenges

- Sensing and Communication
- Early Fault Detection and System V&V
- Systems Integration and Interoperability
- Security (from embedded... to end-to-end)



# Strategic Goals: Enabling a Resilient, Stronger & Smarter Grid

- Isolate the network
- Fortify the network
- Reduce the attacker pool
- Assume defenses will fail
- Reduce human error
- Sensing, Communications, Controls, Security, Energy Efficiency and Demand Response if architected correctly could assist SG development:
  - Distributed Control
  - Grid Architectures
  - Cyber Security



# Selected References

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

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

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

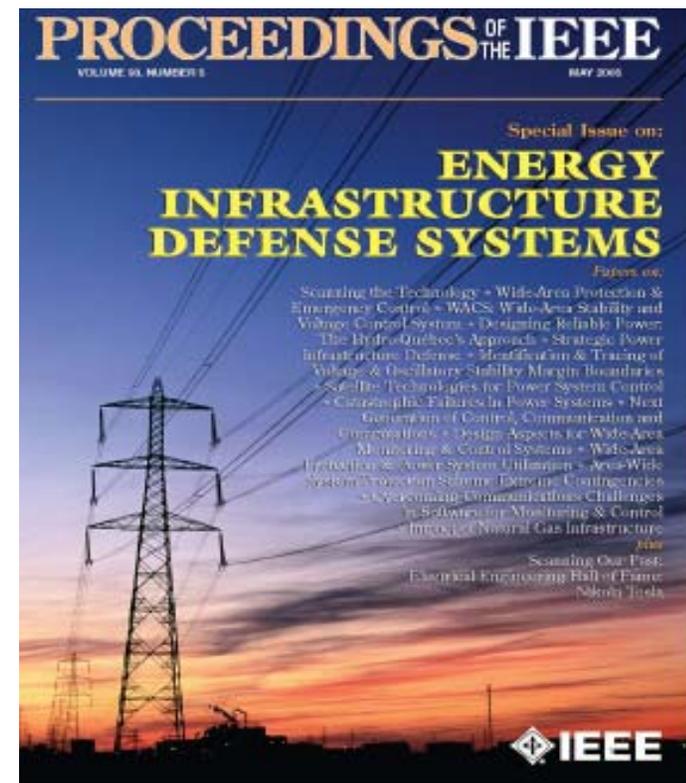
**New Directions for Understanding Systemic Risk:**

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, 100 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 11<sup>th</sup> 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.





# Selected References

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

- **“A Control and Communications Model for a Secure and Reconfigurable Distribution System,”** (Giacomini, Amin, & Wollenberg), IEEE American Control Conf., 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
- **“Toward Self-Healing Energy Infrastructure Systems,”** cover feature in IEEE Computer Applications in Power, pp. 20-28, Vol. 14, No. 1, January 2001

THANK YOU

