

Energy Surety + Sustainability: An Information Systems Perspective

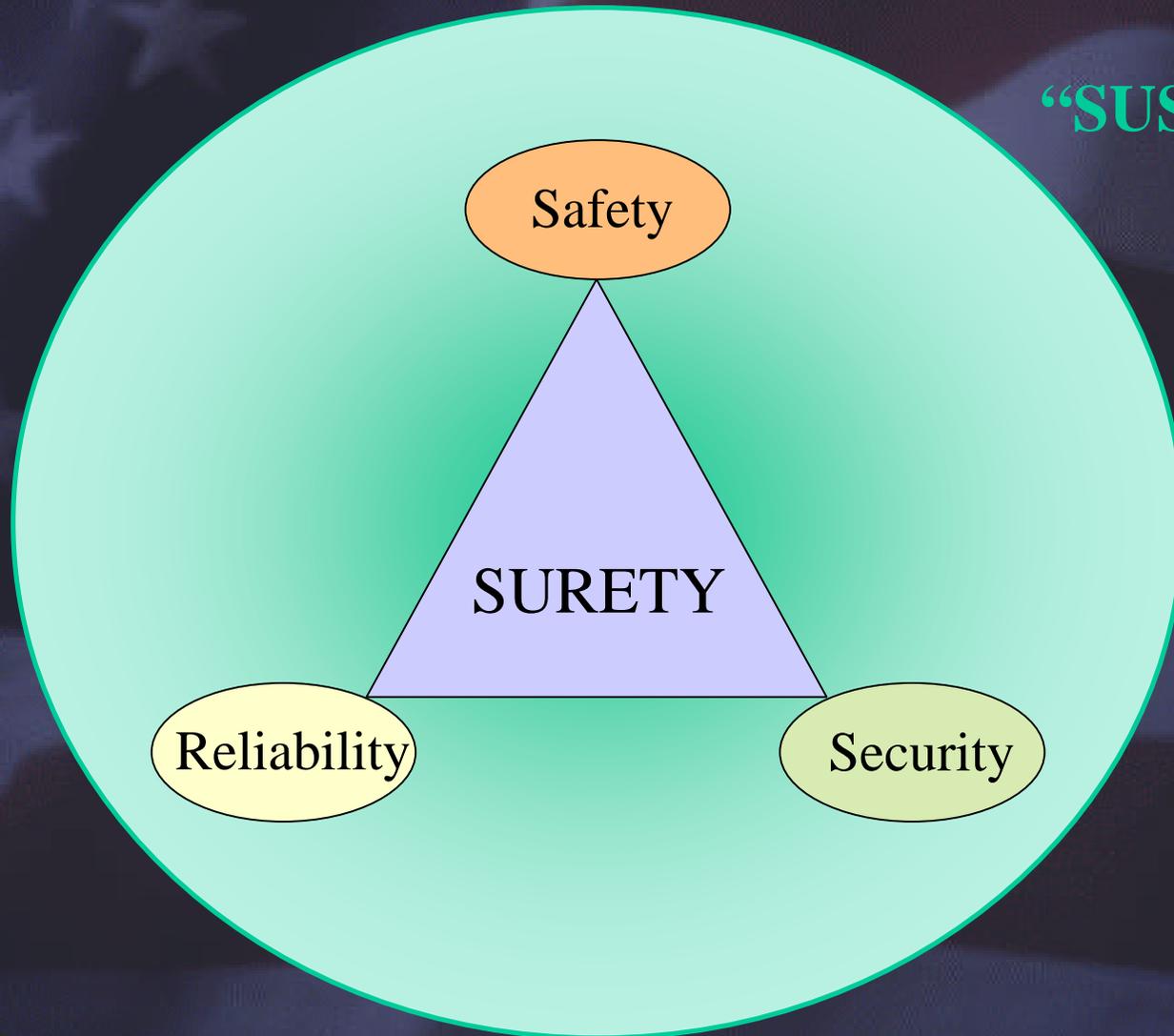
Presented to the
Energy 2003 Conference
August 18, 2003

Margie Tatro
Director,
Energy and Transportation Security Center
Sandia National Laboratories
(505) 844-3154

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy under contract DE-AC04-94AL85000.



Surety + Sustainability Provides a Framework for an Optimal Energy Infrastructure



“SUSTAINABLE”

CONTEXT

Persistent,

Clean,

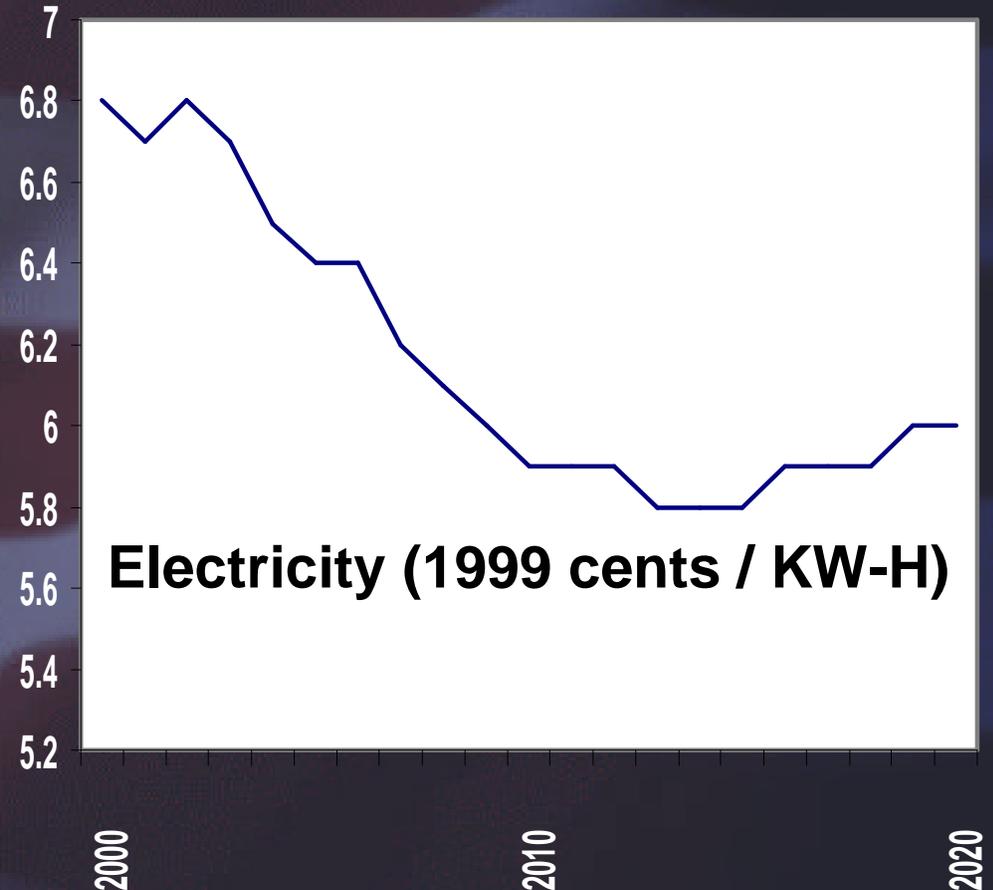
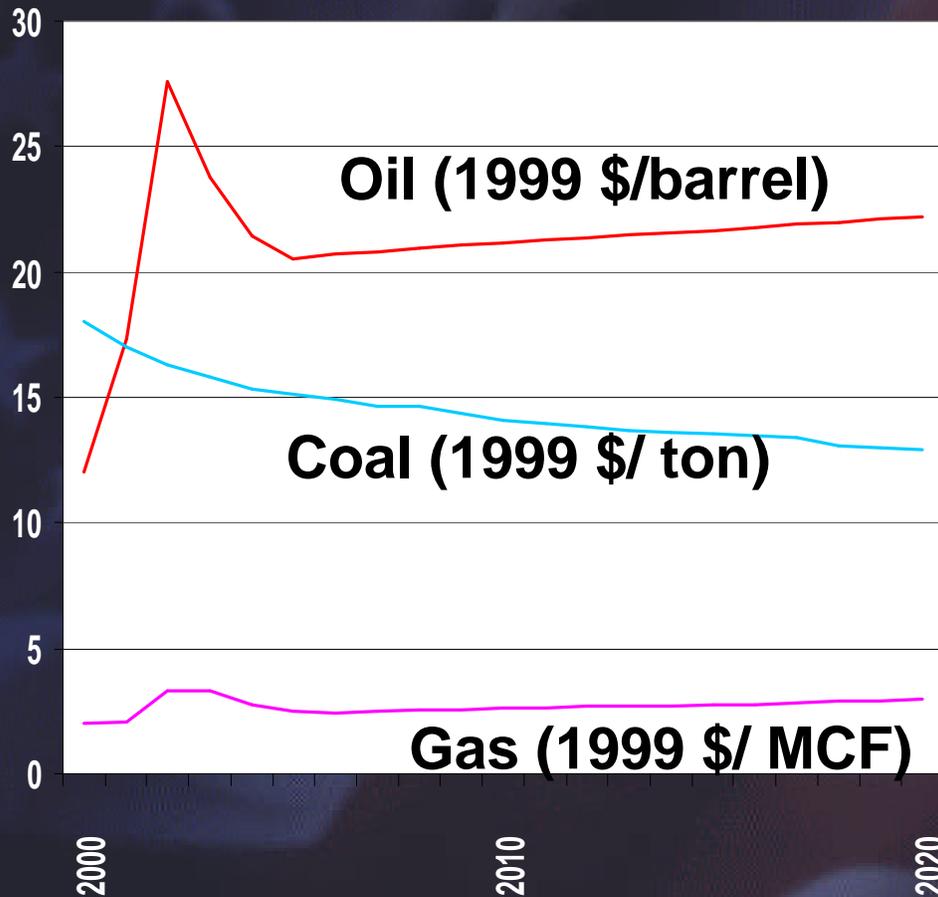
Affordable

What is Energy Security?

Energy is available **WHEN** needed
at a predictable price.

- **Measured by:**
 - Investor and consumer confidence
 - Time to restore service following a disruption and other reliability metrics
- **Secondary indicators:**
 - Energy trade deficit, imports versus domestic production, diversity of sources and delivery mechanisms, and others
- **Includes Physical and Cyber Perspectives**

Forecasted Energy Prices



How Can We Measure Energy Security?

- **Confidence** – feeling, must poll people
 - Price/earnings ratio for investors
- **Reliability** – can measure, for electricity:
 - Transmission reliability (voltage, frequency)
 - Wholesale market performance (price deltas, transmission load relief)
 - Customer outages (number of customers, unserved energy, economic impact, time to restore service)
- **Diversity of supply** – fraction from each fuel source, can measure
- **Diversity of delivery mechanisms** - options, can measure
- **Number of cyber attacks** – can measure

Critical Data Management for Electric Power Moved from Central Control to Coordination

PAST

Generation

Transmission

Distribution

Virtual Private or
Private Networks

PRESENT

Generation

Public, Private,
Virtual, Physical,
Wireless...

PX

Transmission

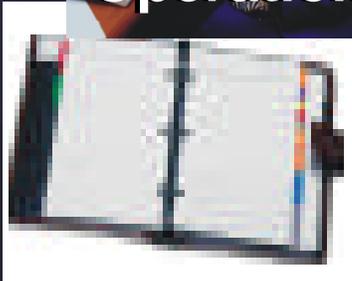
ISO/RTO

Distribution

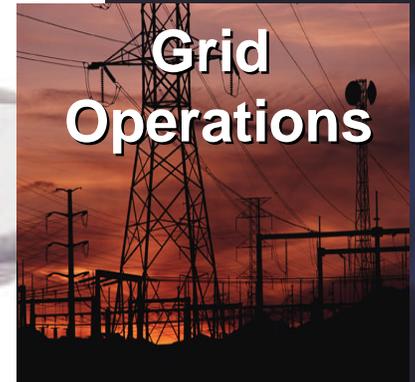
Grid Control in a New Paradigm



**Business
Operations**



**Physical and Operational
Merging of Business &
Grid Management**

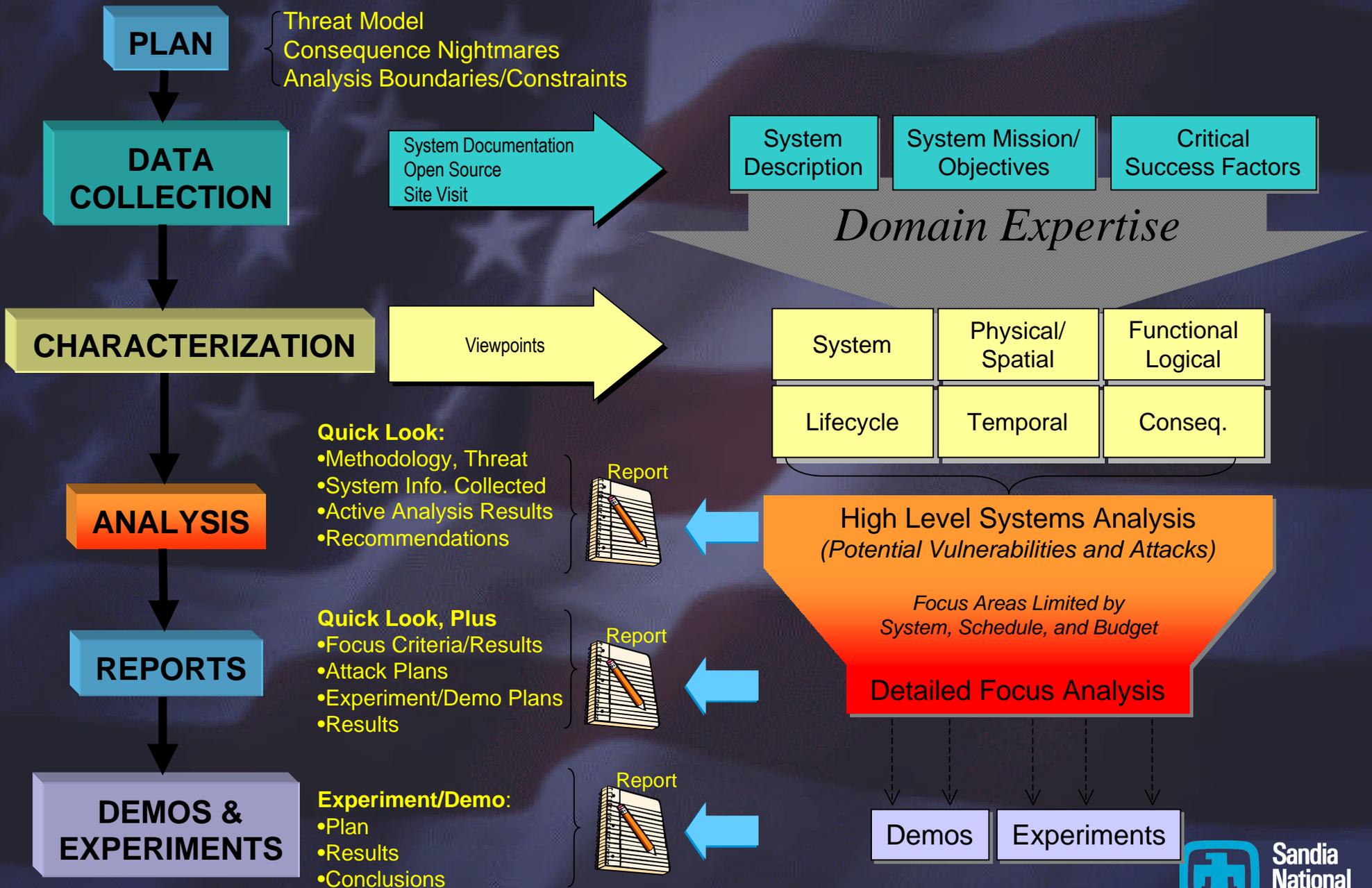


**Grid
Operations**

Challenge 1 – Protecting the Right Assets

- **Physical and Cyber**
- **Assess the Situation**
- **Evaluate Risks**
- **Mitigate Risks for Most Severe Consequences**

Red Team Analysis Can Provide Useful Insights



Estimated Resources Required to Exploit a Vulnerability

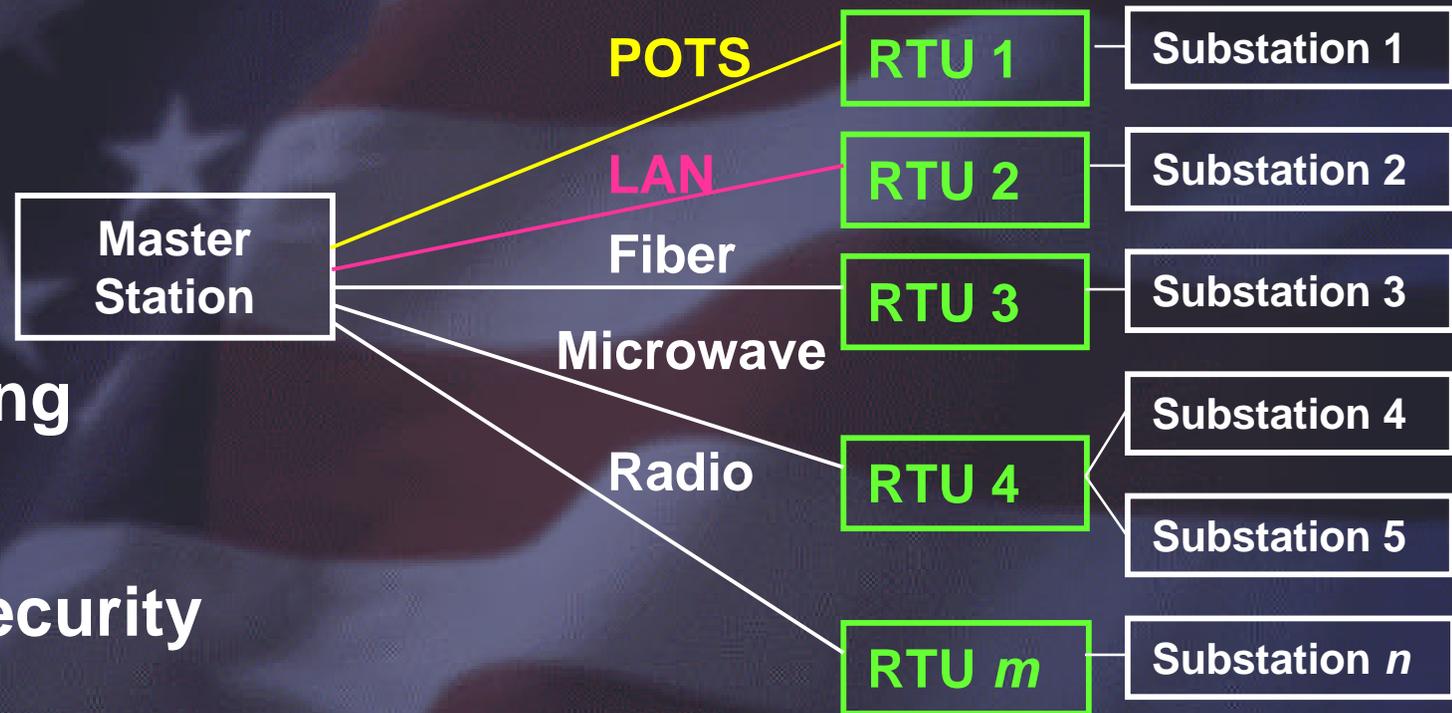
	<i>Attack #1</i>	<i>Attack #2</i>	<i>Attack #3</i>	<i>Attack #4</i>	<i>Attack #5</i>
<i>Probability of Success</i>	100%	95%	85%	80%	50%
<i>Cost to Develop</i>	\$100K	\$50K	\$50K	\$2K	\$50K
<i>Time to Develop</i>	6 months	1 month	4 months	2 days	2 months
<i>Time to Implement</i>	45 min	20 min - hr	1 hr	5 min	1 min
<i>Technology to Develop</i>	EE, Ph.D. Intuition	CS, MS	Chem, BS	Mechanical Intuition	Fiber Optics, CS, EE, Materials
<i>Technology to Implement</i>	Technician	EE, BS	Technician	Technician	Technician
<i>Equipment Required to Implement</i>	Wave Form Analyzer, Computer	Digital Scope	Hand Tools, Acids, Bases	Wooden Mallet	Digital Scope, Laser

Challenge 2 – Improve the Security of Control and Communications Systems

- Vulnerabilities are Abundant
- Research and Assessments are Reducing These
- Supporting the Expanded Use of the Internet is Critical

Legacy SCADA Architecture

- Radial
- Nonstandard Equipment
- Older Operating Systems
- Little or No Security
- No Authentication



POTS = Plain Old Telephone Systems

LAN = Local Area Network

RTU = Remote Telemetry Unit



**Procurement Application
Novell OS Platform**



SCADA



**Financial Application
NT OS Platform**



**Application
UNIX OS Platform**

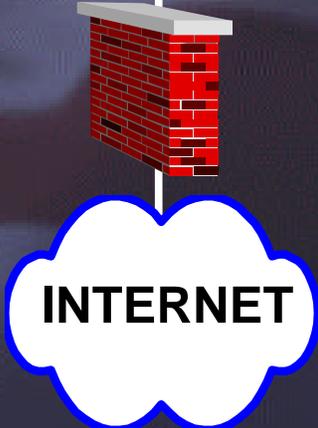
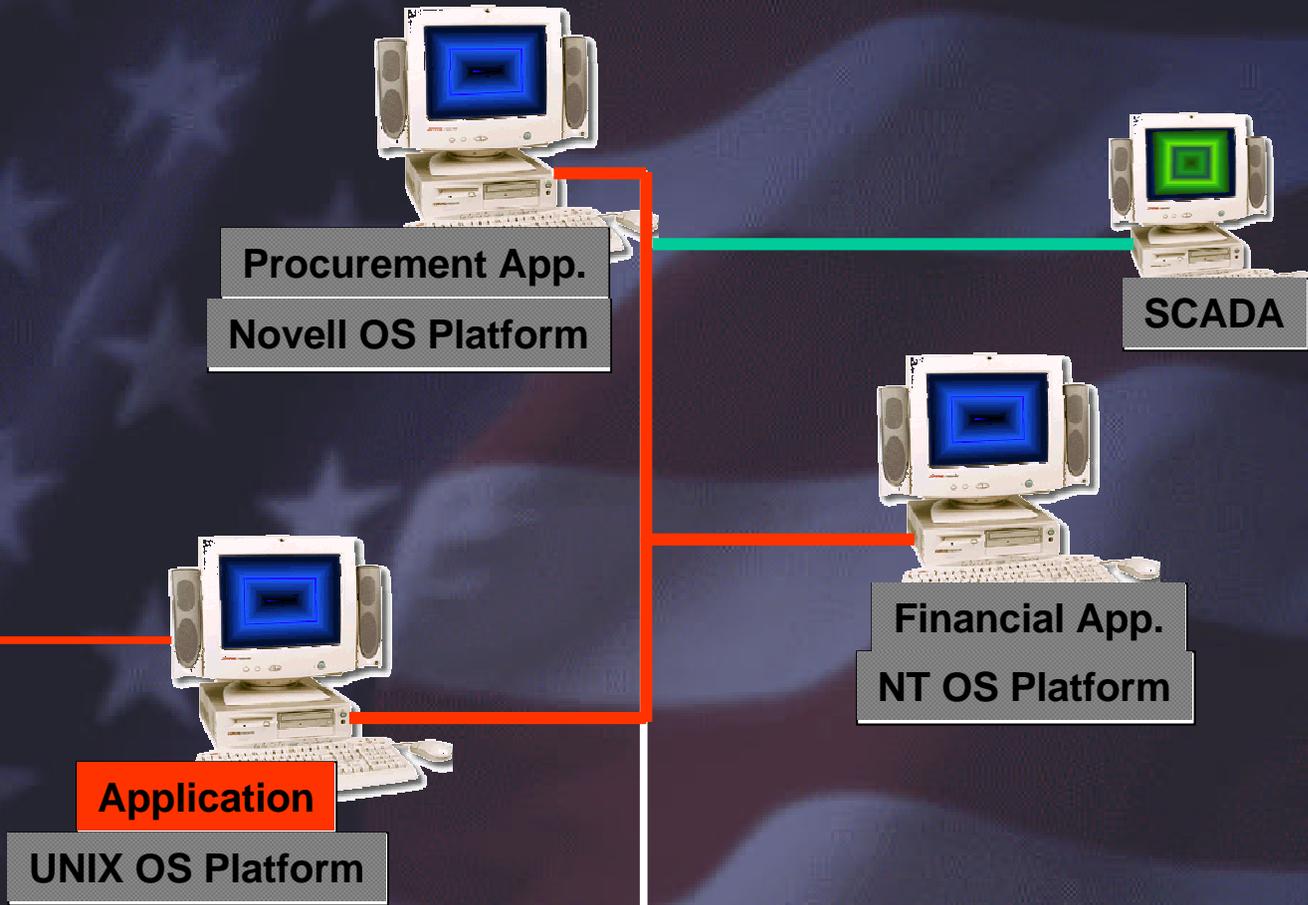
**Even with a Firewall, a
Network
May be
Vulnerable**



INTERNET

**Physical
Access**

**Password
Control**



**Remote
Access**



FTP, Telnet. . .



Application

UNIX OS Platform



**Procurement App.
Novell OS Platform**



SCADA



**Financial App.
NT OS Platform**



INTERNET

Remote Access



FTP, Telnet. . .



Application

UNIX OS Platform

Procurement App.
Novell OS Platform



SCADA



Financial App.
NT OS Platform



Other Remote Access



INTERNET

Even with a Firewall
Back Doors are
Still Open

Vulnerability of Contemporary SCADA

- **Front Doors Closed, but Not Always Locked**
 - Firewalls Sometimes Used, but Not Always Adequately Configured
 - Connections Between SCADAs and Corporate Networks Not Always Protected
- **Back Doors Usually Wide Open**
 - Connections to Contractors and Maintenance Staff
 - Connections to Partners and Other Organizations
 - Unprotected Modem Access
 - Unprotected Remote Access
 - Open Insider Access - Disgruntled Employees, Visitors, Maintenance, Custodians

More Specifically, What We've Learned

- **Examples of Vulnerabilities**
 - **Unauthenticated Dial-In Access**
 - **Unprotected Remote Access - FTP, Telnet**
 - **Open-Source Information Available to Adversaries (Web, Libraries, FERC Forms, SCADA Training Courses)**
 - **Weak Password Protection**
 - **Not Leveraging Router Security**
 - **Not Deleting Old Accounts**
 - **Data Not Categorized or Protected to Appropriate Sensitivity**
 - **Little, If Any, Intrusion Detection**

Activities Underway to Improve Security of SCADA Systems

- Vulnerability Assessments
- SCADA Research and Support of Standards Committees
- Supporting Research
 - Cryptography
 - Advanced Network Security Research
 - Distributed Energy Control
- Testbeds for system validation

Monitoring & Acquisition



Control
Equipment



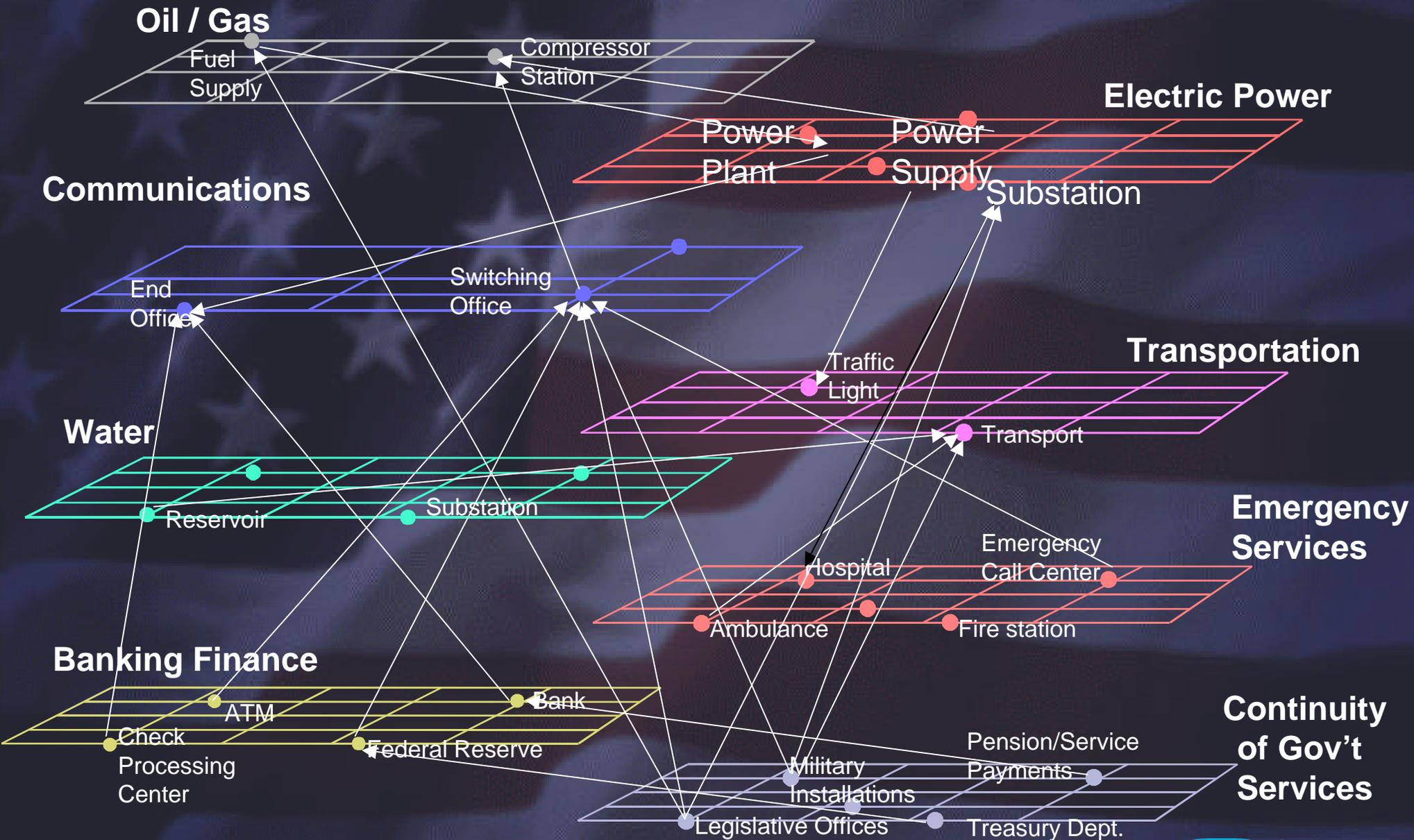
Challenge 3 – Understanding Interactions Among Infrastructures

Each Critical Infrastructure Insures Its Own Integrity

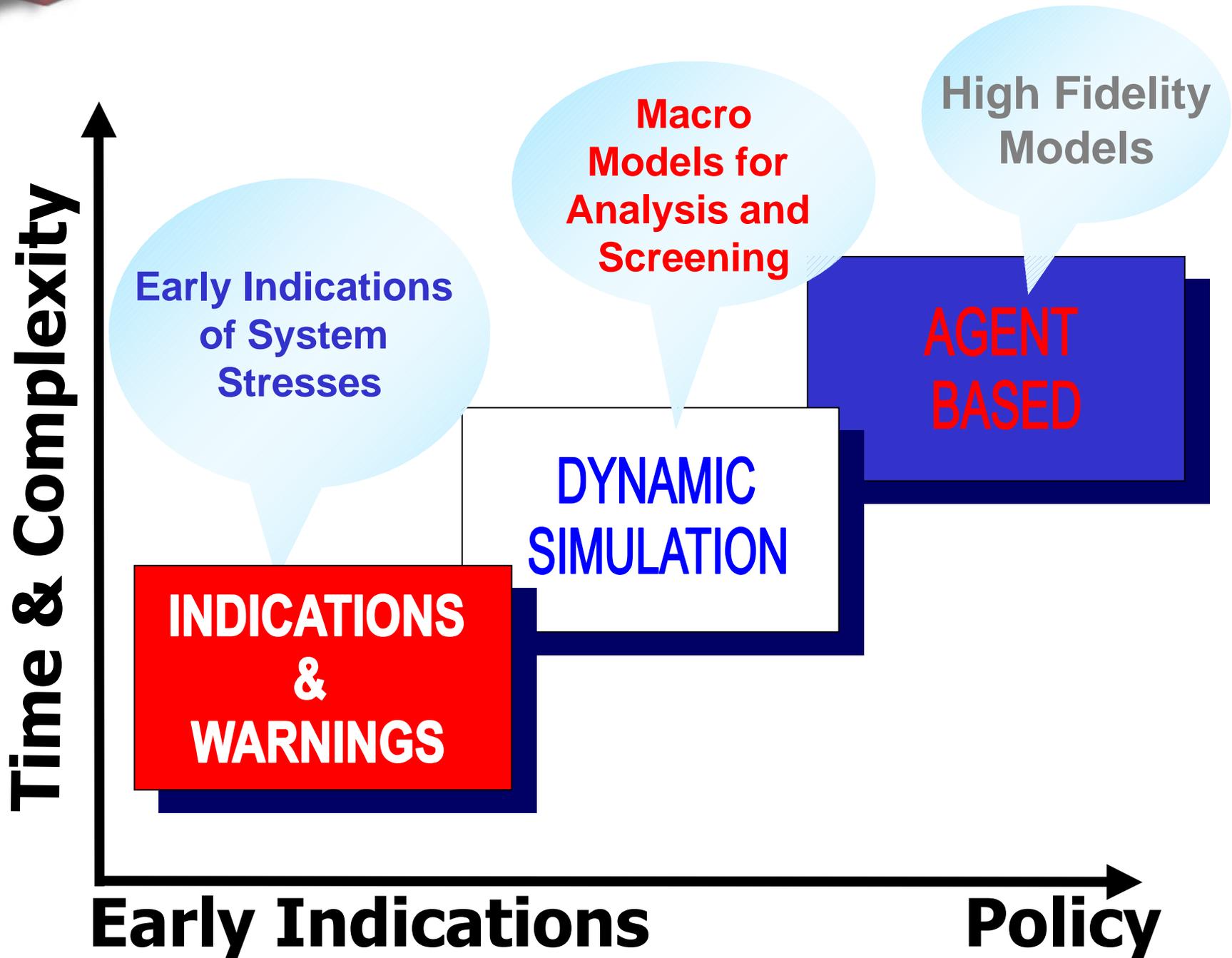


Interdependencies Between and Among Critical Infrastructures Is Key to Reliable Operation of Them All

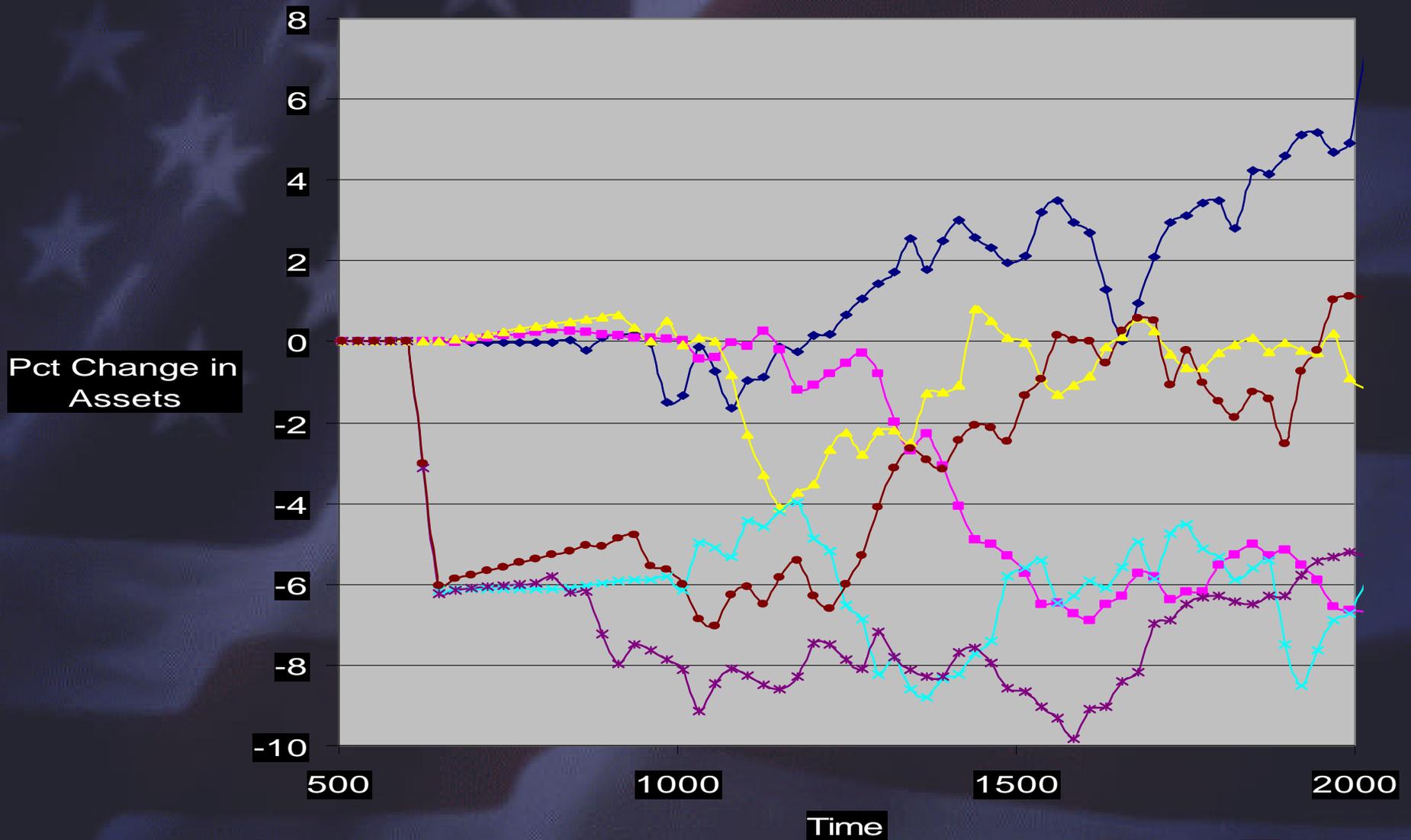
Infrastructure Protection is Complicated by Interdependencies



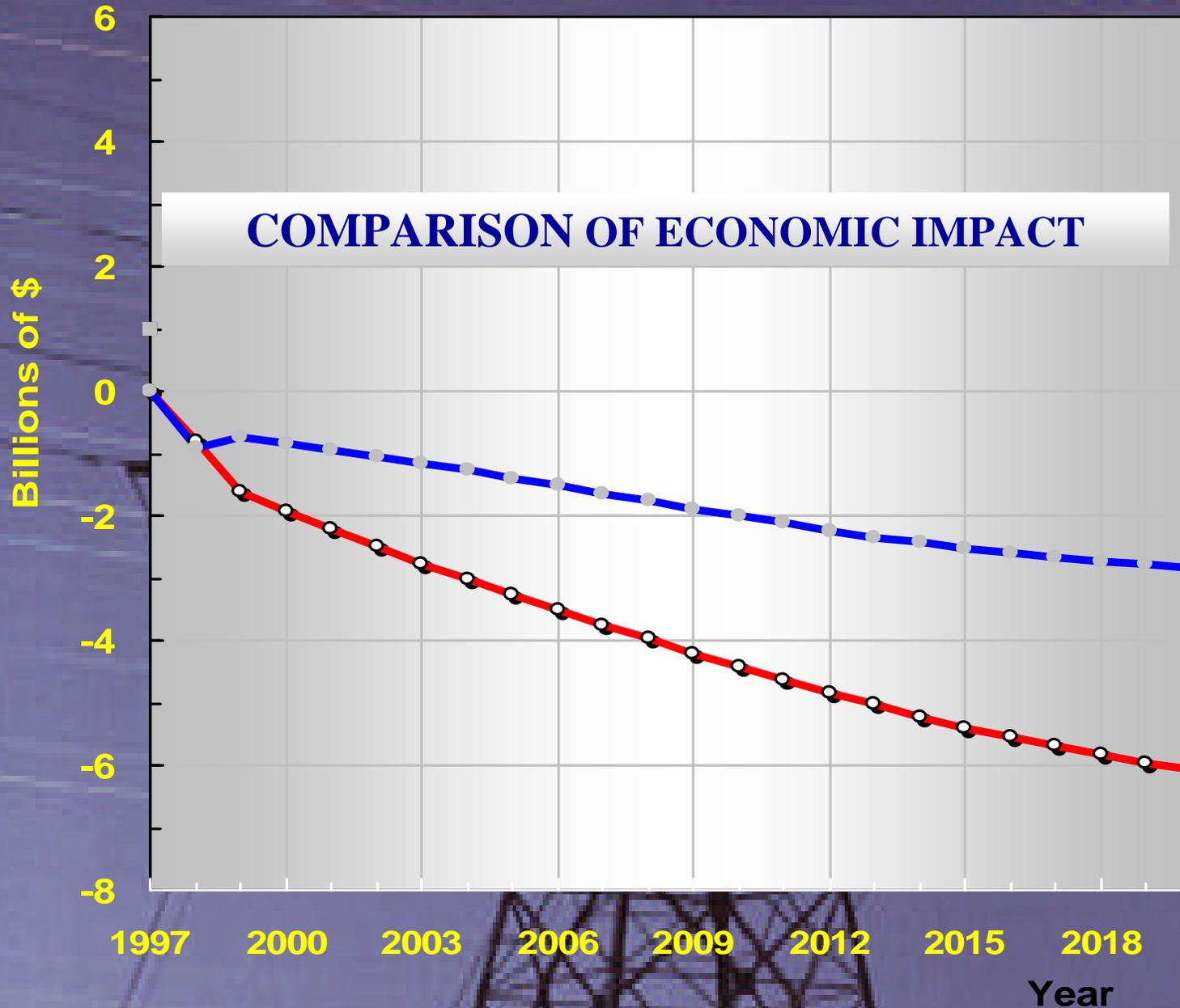
A Variety of Models is Required



Agent-based Models are Used to Study the Economic Cost of Outages



COMPARISON OF ECONOMIC IMPACT



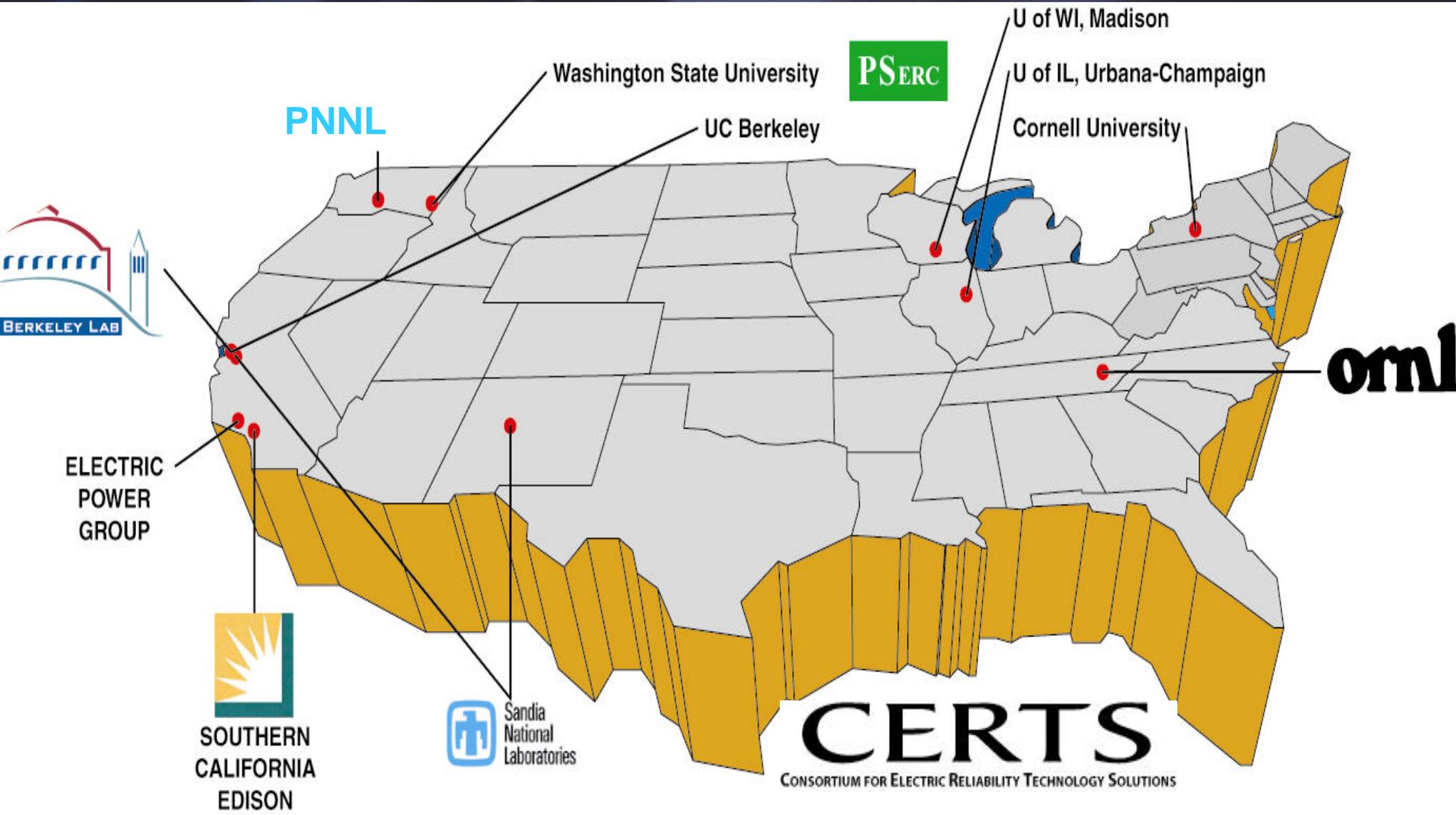
----- Houston, Scenario #1 - Series of Small Disruptions - One Month Apart/Short but Regular

----- Houston, Scenario #2 - Short-Lived but Large Disruption

Challenge 4 – Presenting Volumes of Electric Operations Data to Humans for Processing

- Electric grid operations are becoming more complex
- Large volumes of transactions
- Low reserve margins stressing grid operations
- System constraints affect use and care of the grid system
- Systems expansions and upgrades are occurring slowly, if at all

Consortium for Electric Reliability Technology Solutions



Real-Time Grid Reliability Management Roadmap

Operational Decision Support Tools and Visualization

System Security Management Tools

Advance Measurements and Controls

Development, and Demonstrate Reliability Adequacy Tools:

- VAR Management
- Ancillary Services Perform.
- Wide-Area Information Visualization
- Reliability Compliance Performance (ACE,AIE,etc)

1999-2002

Security and Congestion Assessment Tools:

- Integrated Security Analysis
- Congestion Management
- Cascading and Self Organized Criticality Utilization

2001-2003

Dispatcher and Operating Engineering Applications Using Synchronized Phasor Measurements:

- Monitoring & Post Disturbance Tool
- Enhance Stability Nomograms
- Standard, Low Cost, Reliable Phasor Technologies
- Validation of Stability Models

2000-2004

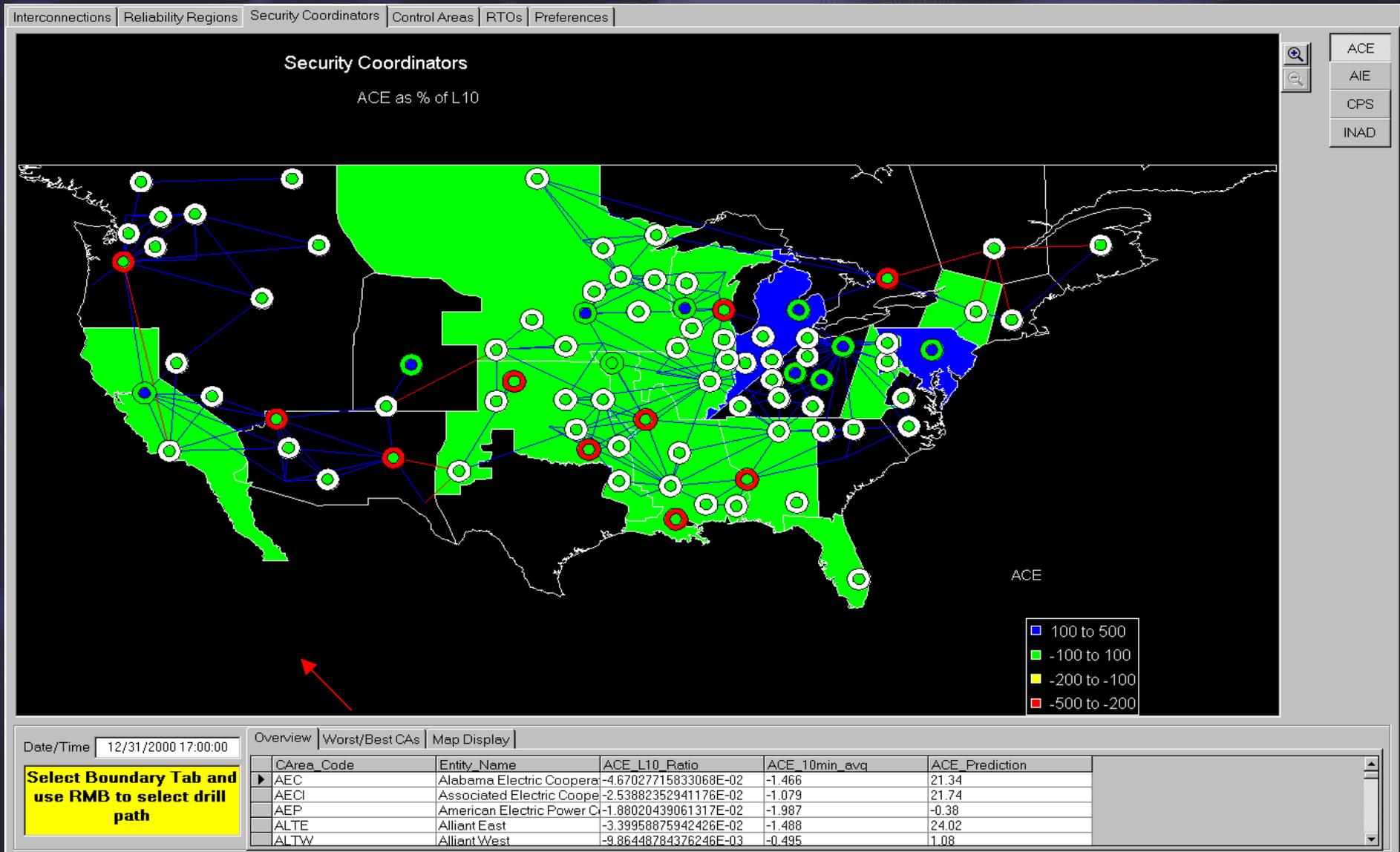
Prototype New Real Time Controls

Automated adaptive control strategies based upon real-time data monitoring

2001-2008

GOAL: AUTOMATIC SWITCHABLE NETWORK

ACE Monitoring Identifies Problems In Real-Time and Supports Corrective Action



There are Challenges Yet to be Solved

- **Assessment of vulnerabilities**
- **Security of contemporary control systems**
- **Greater understanding of infrastructure interdependencies**
- **Better ways to collect and present information for humans to process**
- **Techniques for optimizing solutions around multiple objectives**

Can We Measure Surety + Sustainability?

- **New metrics**

- **Security**

- Physical & Cyber
- Economic

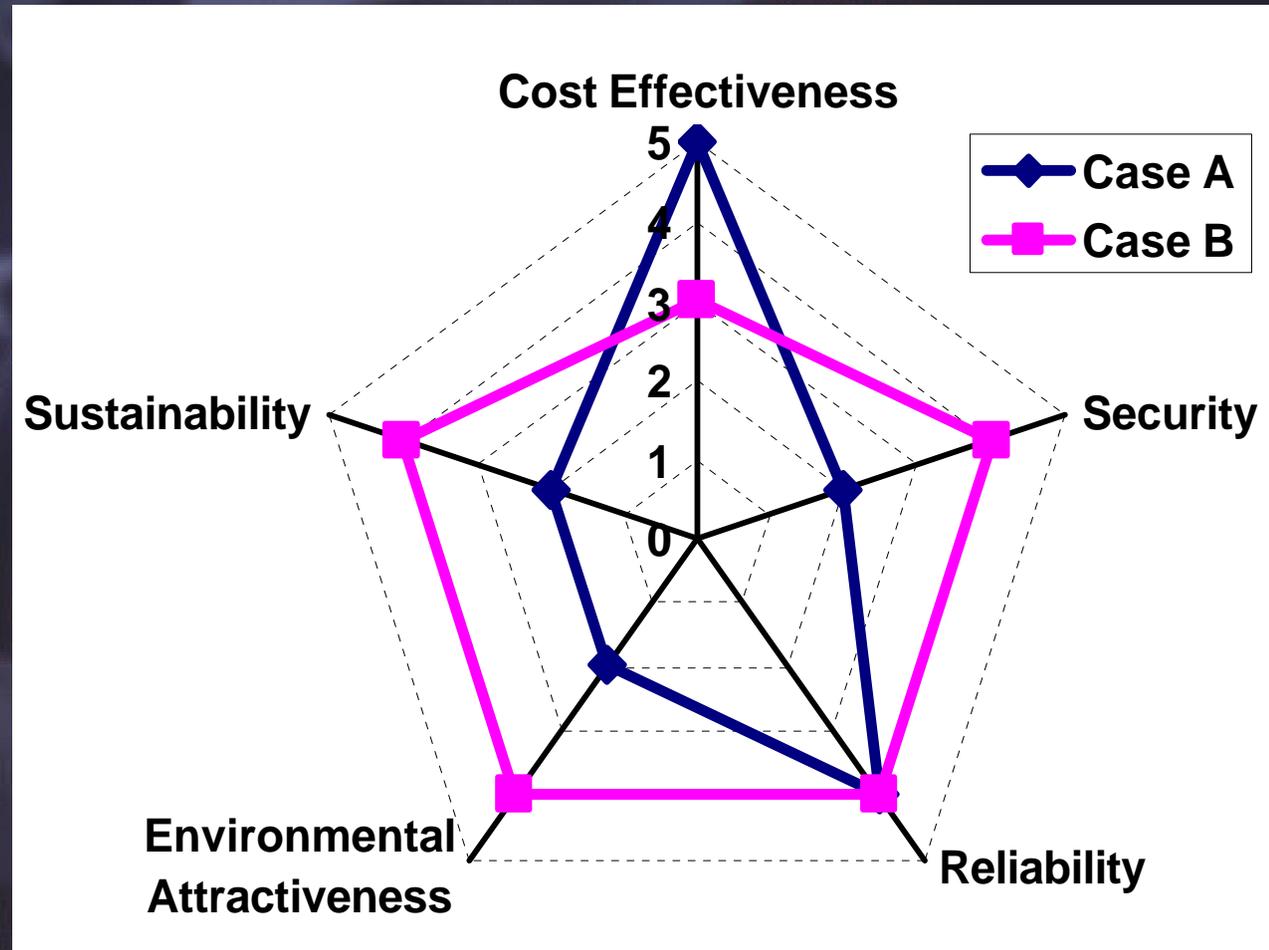
- **Reliability**

- **Sustainability**

- **Safety**

- **Resilience =**

resistance & adaptability to disruption



THANK YOU

Additional Energy 2003 Presentations by Sandia National Labs Colleagues:

- **Jerry Ginn – “Macro Benefits from a Microgrid,” Monday 10:30-12:30**
- **David Menicucci – “Affordable Heat and Power from the Sun,” Tuesday 1:30-3:3**