

# **A Methodology to Support Dependable Survivable Cyber- Secure Infrastructures**

**HICSS-38 January 3-6, 2005**

Frederick Sheldon, Mallikarjun Shankar,  
Stephen Batsell

Oak Ridge National Laboratory / CSE

---

Stacy Prowell and Michael Langston  
University of Tennessee / CS

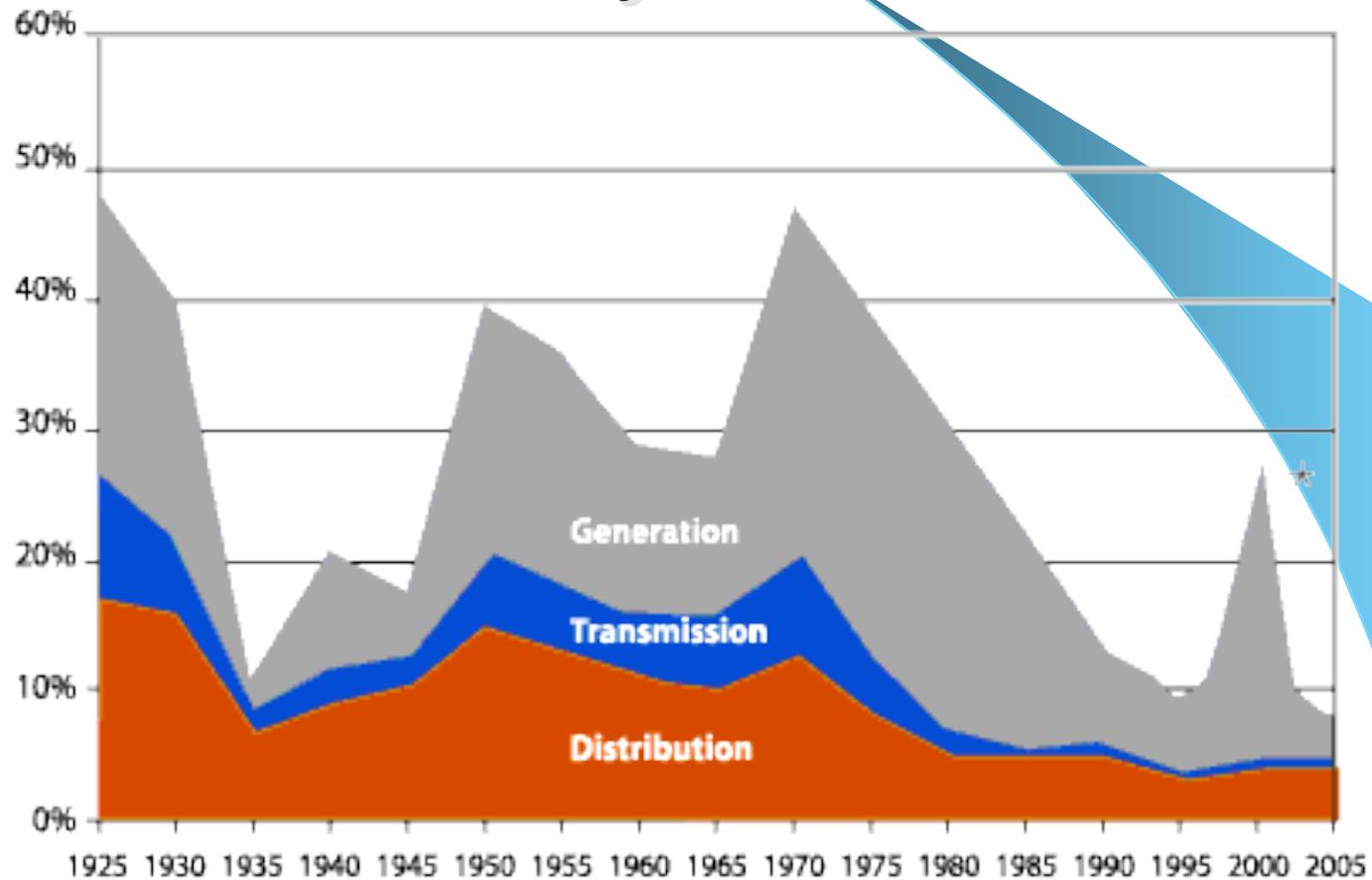
# Outline

- Reflections of Critical Infrastructure (CI) survivability
- Advanced techniques available/ employable for CI Protection (CIP)
- Network Vulnerabilities
- Autonomic Framework
- Software Agents
- Summary/ Recommendations

# Reflections on CIP/ Survivability

- Information systems now form the backbone of nearly every government and private system. Increasingly these systems are networked together allowing for distributed operations, sharing of databases, and redundant capability
- *Ensuring these networks are secure, robust, and reliable is critical for the strategic and economic well being of the Nation.*

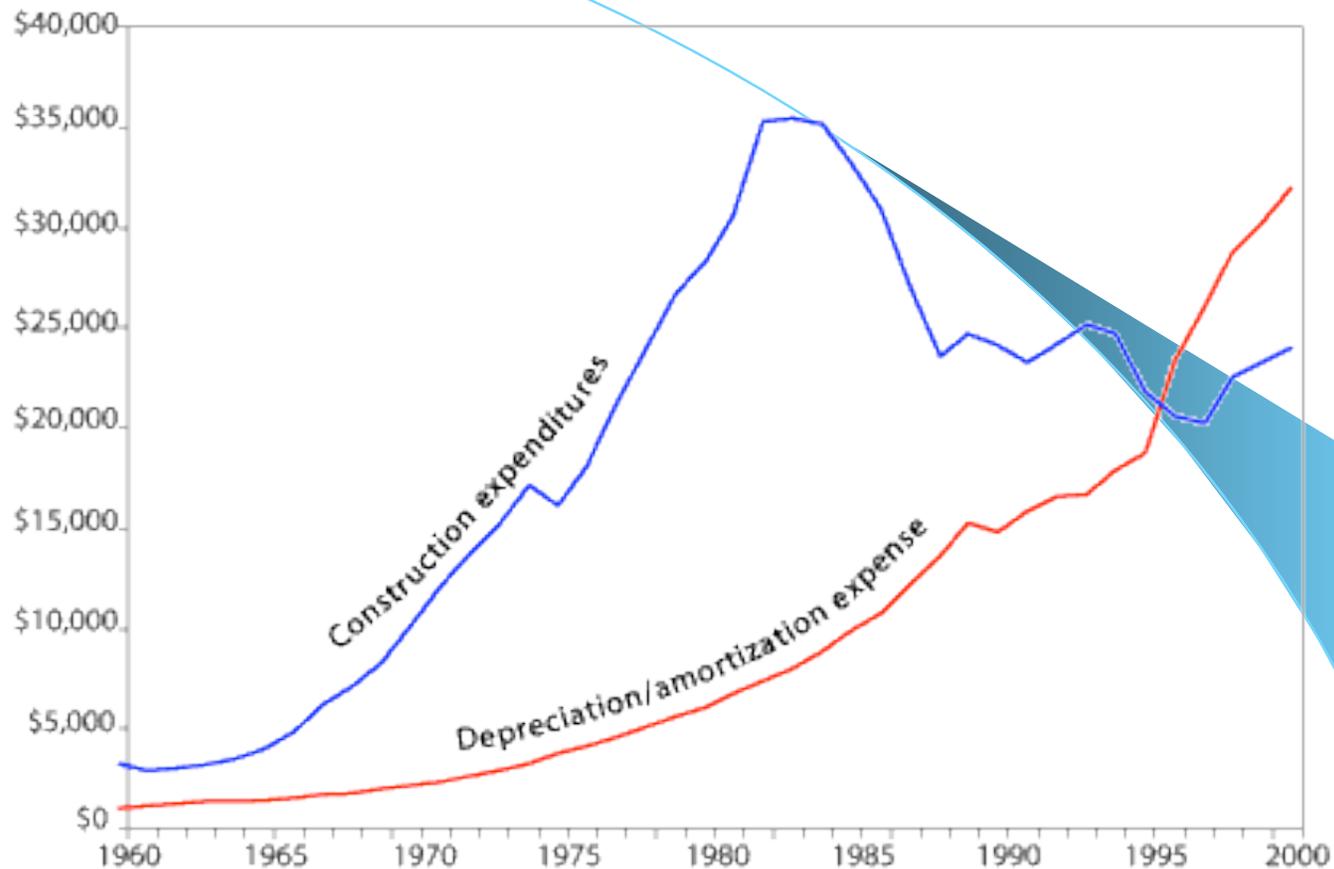
# Capital Invested as % of Electricity Revenue



Sources: Electric Utility Industry Statistics, and 2001 Financial Review, Edison Electric Institute

**Capital invested as % of electricity revenues**

# Utility Construction Expenditures



## Utility construction expenditures and depreciation/amortization expense

In recent years, the investor-owned utility industry's annual depreciation expenses have exceeded construction expenditures. The industry is now generally in a "harvest the assets" mode rather than an "invest in the future of the business" mode.

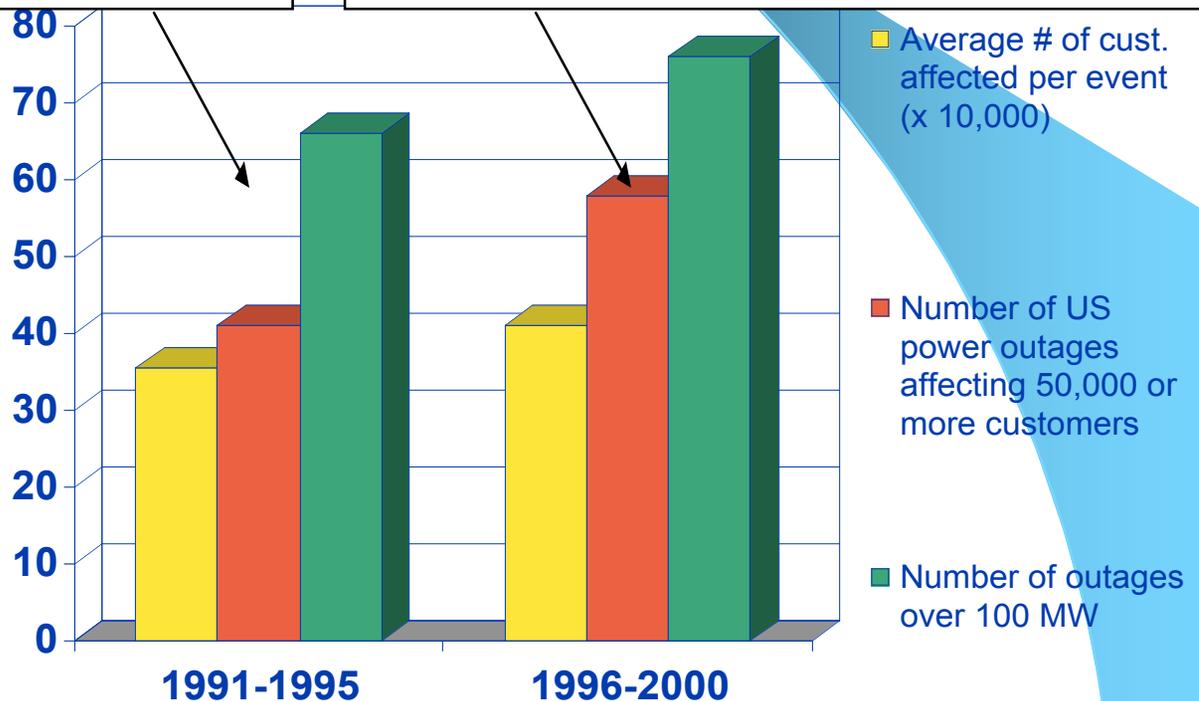
Source: "Historical Statistics of the Electric Utility Industry" and "EEI Statistical Yearbook" - EEI  
Copyright © 2003 Electric Power Research Institute, Inc. All rights reserved.

# Historical Analysis of U.S. outages (1991-2000)

66 Occurrences over 100 MW  
798 Average MW Lost  
41 Occurrences over 50,000 Consumers  
355,204 Average Consumers Dropped

76 Occurrences over 100 MW  
1,067 Average MW Lost  
58 Occurrences over 50,000 Consumers  
409,854 Average Consumers Dropped

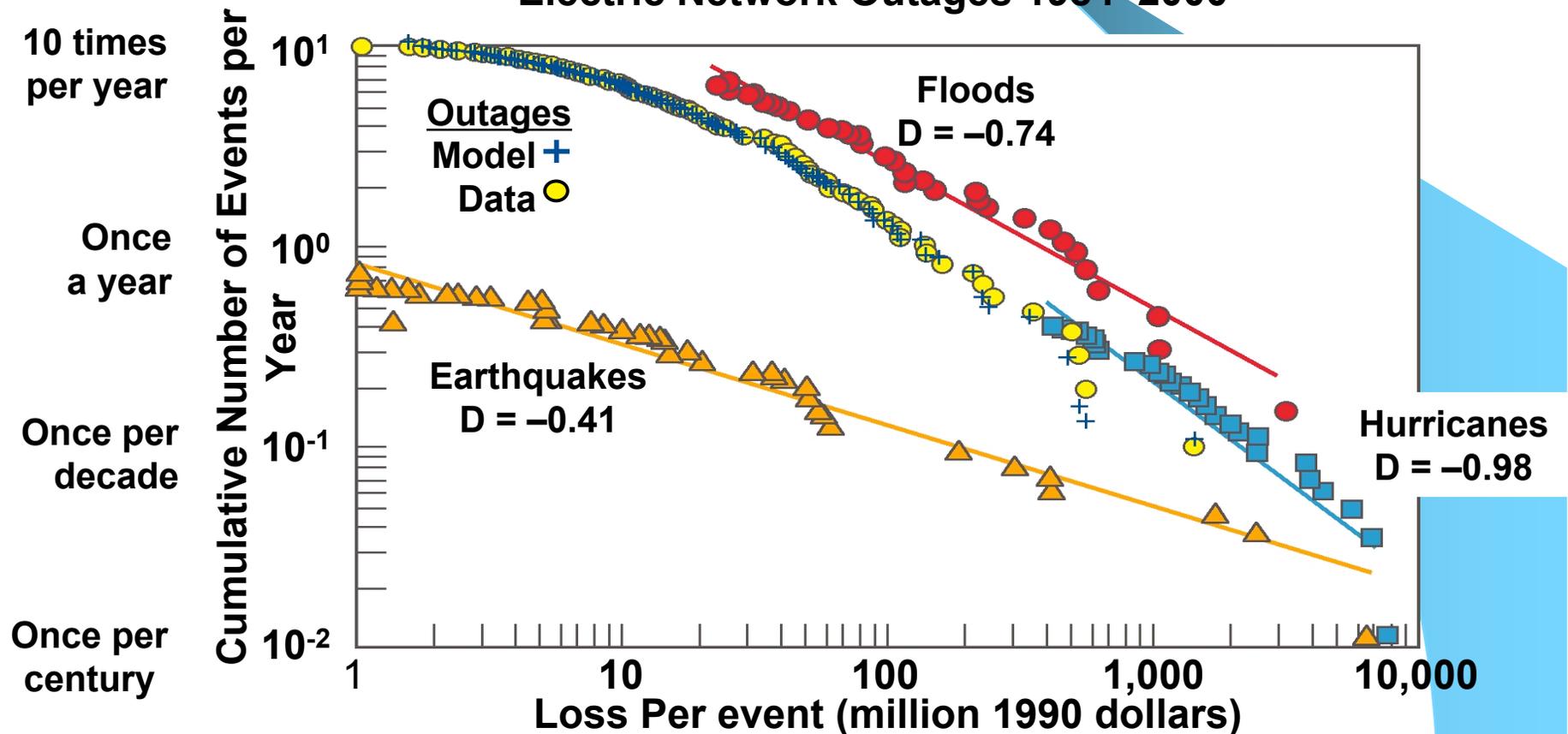
Increasing frequency and size of US power outages 100 MW or more (1991-1995 versus 1996-2000), affecting 50,000 or more consumers per event.



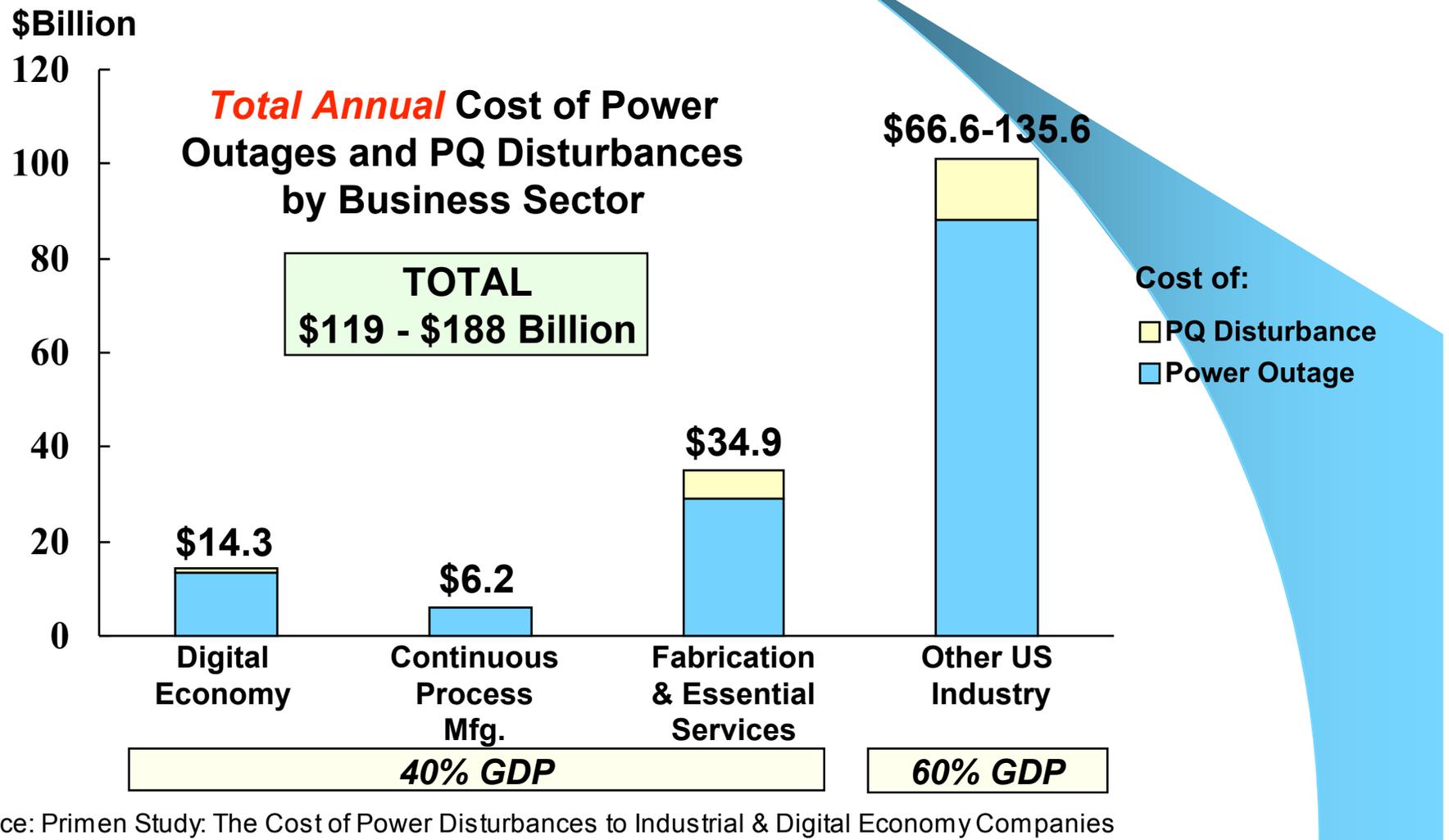
Data courtesy of NERC's  
Disturbance Analysis Working  
Group database

# Frequency & impacts of Major disasters

Hurricane and Earthquake Losses 1900–1989  
Flood Losses 1986–1992  
Electric Network Outages 1984–2000

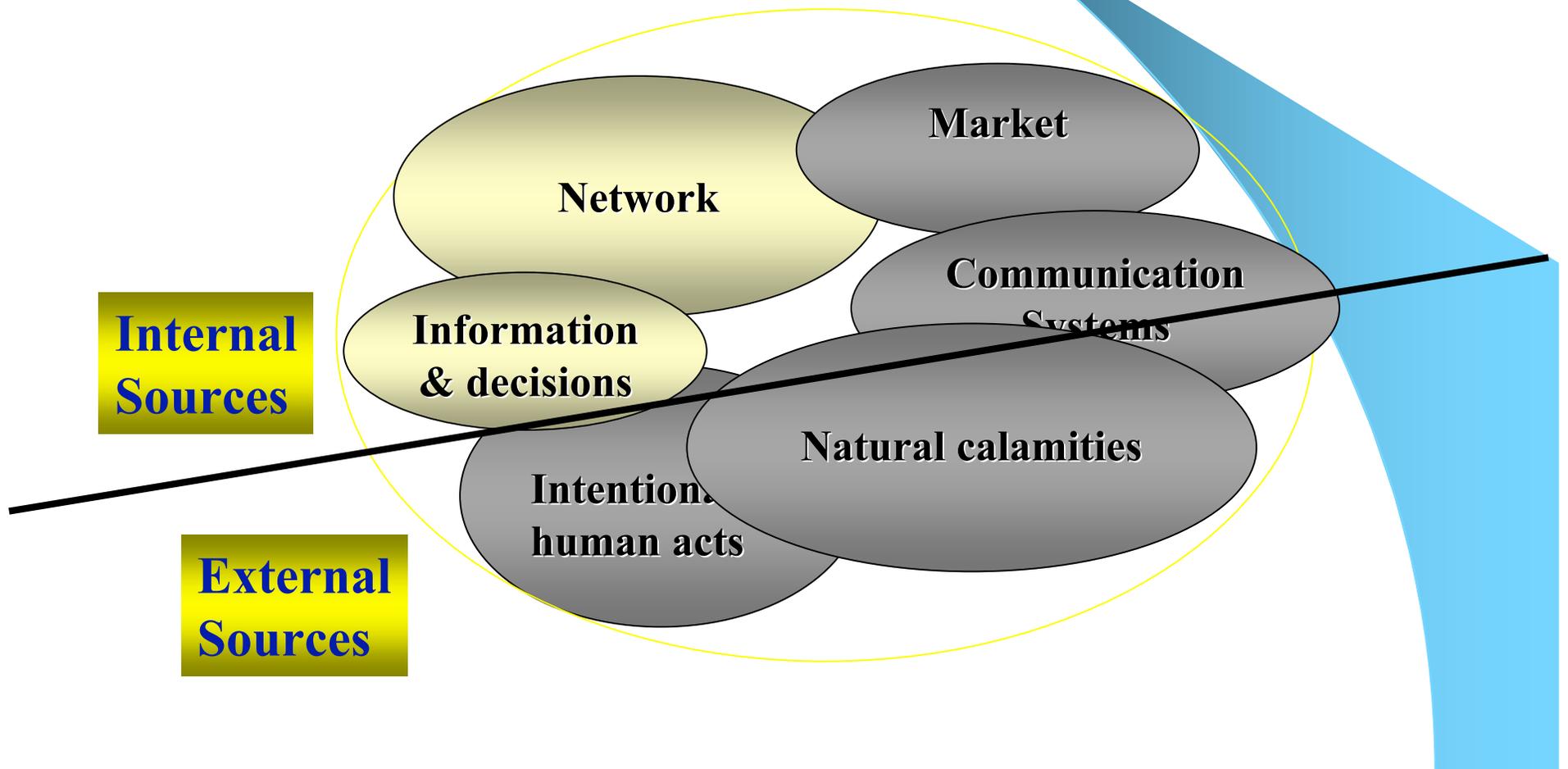


# A Toll Felt Throughout the U.S. Economy: Over \$100B per year



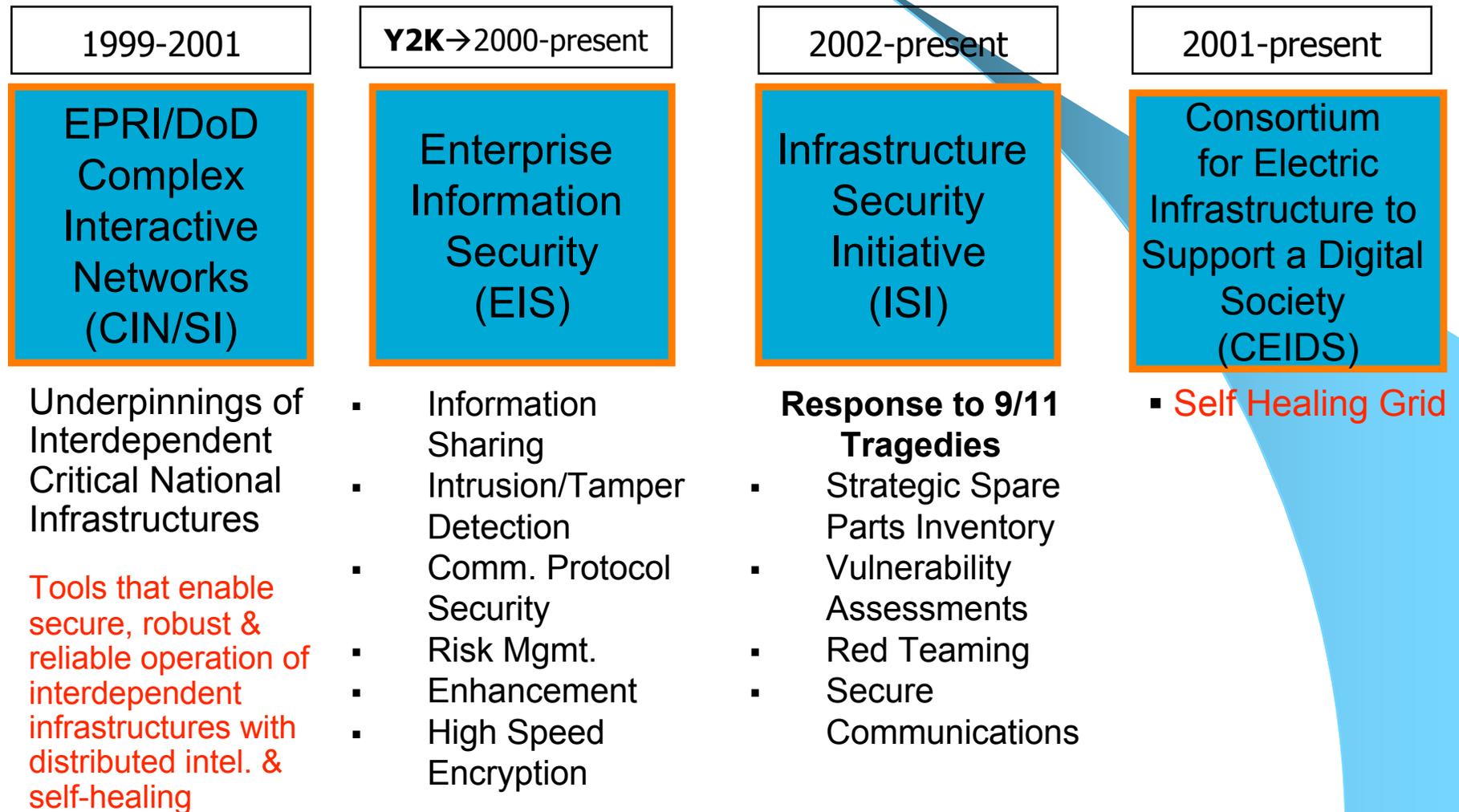
Source: Primen Study: The Cost of Power Disturbances to Industrial & Digital Economy Companies

# Sources of Threat/ Vulnerability

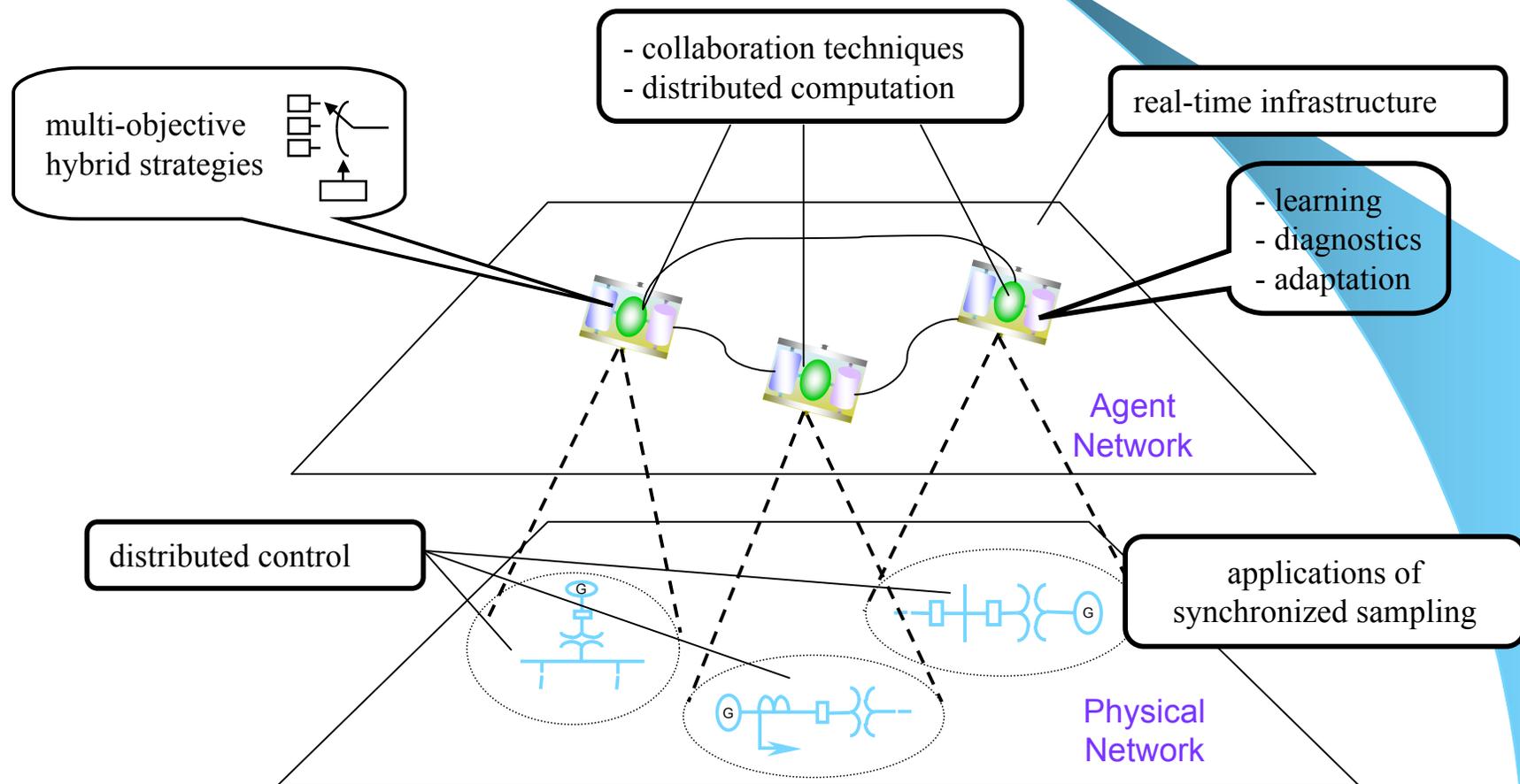


# So what are we doing about it?

## Selected Recent Security & Reliability Related Programs in EPRI



# Context Dependand Network Agents

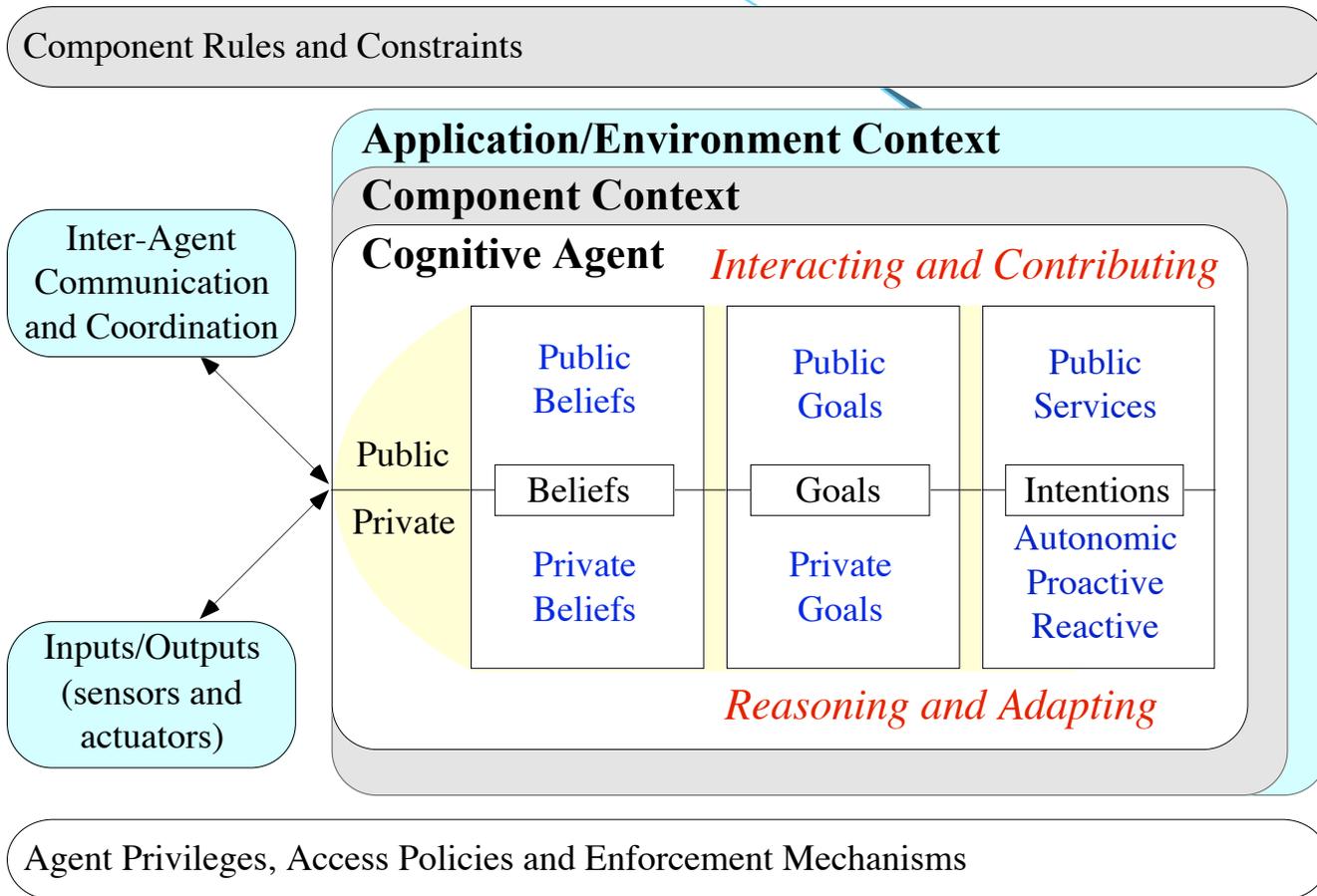


# Advancing the State-of-the-Art for Critical Infrastructures

- The next generation of high performance dynamic and adaptive nonlinear networks, of which *power systems* are an application, will be designed and upgraded with interdisciplinary knowledge for achieving improved
  - survivability,
  - security,
  - reliability,
  - reconfigurability and
  - efficiency
- Using *cognitive immunity* and *self-healing*

# Cognitive Immunity

Conceptualization: cognitive agents, components & application.

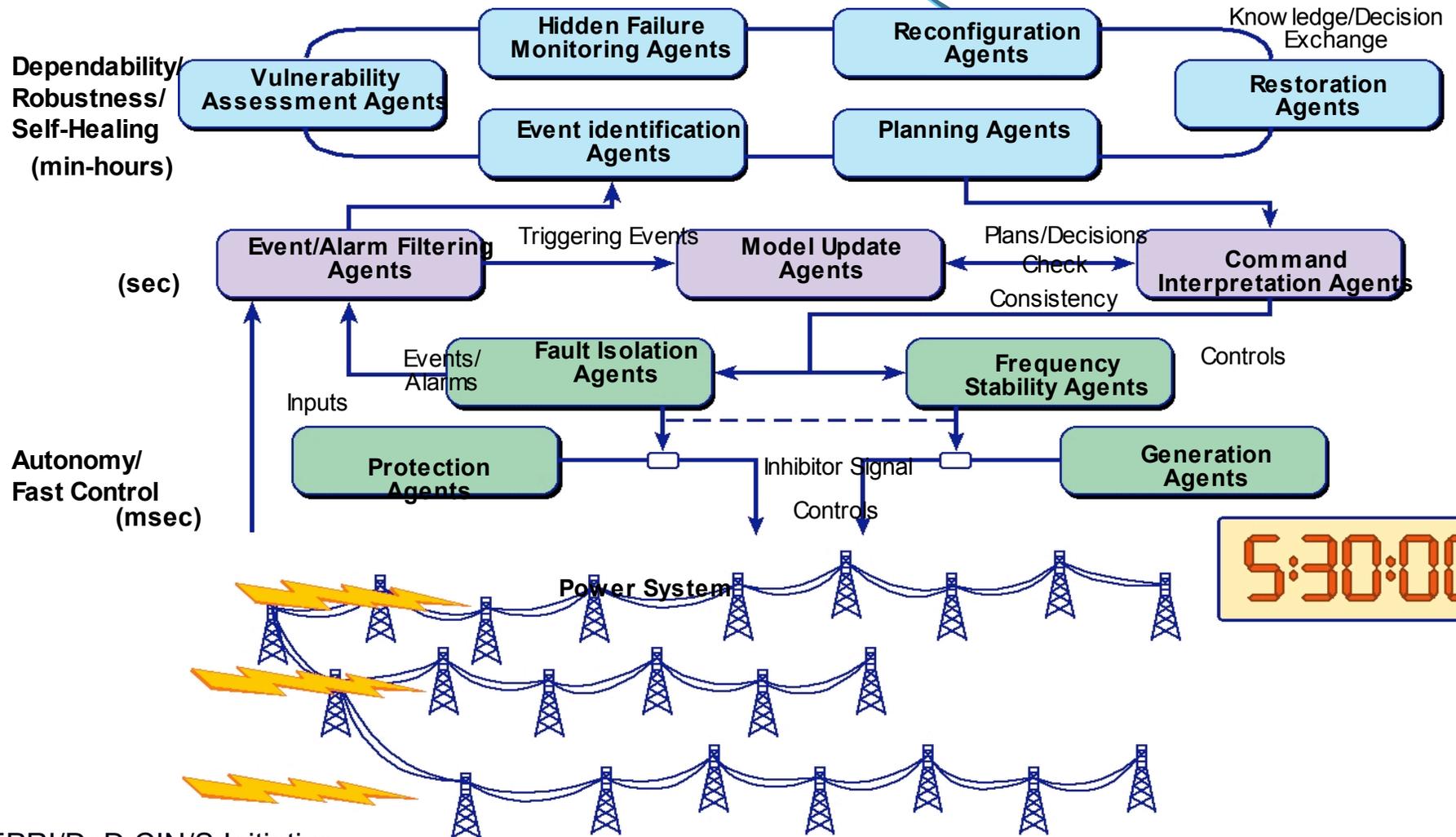


Cognitive systems may comprise 3 types of processes: a) *reactive*, timely response to external stimuli, b) *deliberative*, learning and reasoning, c) *reflective*, continuously monitor/adapt based on introspection

# Based on the BDI Model

- ***Beliefs*** of an agent can consist of private and public beliefs.
  - Private beliefs represent local agent state information, which form the main basis for reasoning and reactive behavior.
  - Public beliefs include (distributed) information about the context/environment and are the basis for reflective processes.
- The ***Desires*** are goals, where private goals govern the deliberative activities while the public goals direct the reflective processes as they describe the overall cognitive system goals.
- ***Intentions*** (services) consist of reactive, proactive, autonomic and public plans.

# Self-Healing (Adaptive) Grid



# Autonomic Framework

- *Self-configuration* – Automated configuration of components and systems follows high-level policies while the rest of system adjusts automatically and seamlessly
- *Self-optimization* – Components and systems continually seek opportunities to improve their own performance and efficiency
- *Self-healing* – System automatically detects, diagnoses, and repairs localized software and hardware problems. *Self-protection* – System automatically defends against malicious attacks or cascading failures and uses early warning to anticipate and prevent system wide failures.

# Challenge: Long Term Stability

- The requirements of reliability, flexibility (adaptability), and efficiency are often in conflict in large distributed control systems (e.g., SCADA systems) because the infrastructure is built and tuned independently to meet those individual requirements.
- Reliability requirements translate to an ability to tolerate and recover from failures and to give *a priori* assurances of a certain level of long-term stability.

# Prospects: Large Complex System Control

- To realize a “*self-healing ability*,” the system must be flexible enough to dynamically adapt through reconfiguration.
- However, the capacity to be flexible could make the system prone to design or runtime errors and the overhead of flexibility may take away from the performance efficiency of both the control and data planes.
- To address these conflicting requirements, our approach coordinates the creation and distributed layout of control software in the form of autonomous software components or agents to meet these service quality level needs for large complex system control.

# Three Phased Approach

- Our approach is *three-phased* and resolves conflicts in the different control loop performance requirements toward developing more survivable SCADA distributed control architectures.
- *First*, by specifying a distributed layout of autonomous agents we can programmatically describe the end-to-end control structures at the time of system design to enable a *compile-for-service-performance* approach to the control plane.

# *Compile-for-service-performance*

- To accomplish this, we will use a narrowly specified grammar for the control framework building upon available specification methodologies such as Petri-nets and derivatives of original distributed programming/ specification languages (e.g., Z, CSP, Statecharts) will create a capability to specify a verifiable control scheme toward gaining ultra high dependability.

# Formal models for distributed computation have had qualified success

- While formal models for distributed computation have had qualified success...
- The novelty in this approach lies in translating the formalism to a network of cooperating agents.
- Furthermore, this step describes both the requirements and system specifications in concrete terms to enable rigorous analysis and design for provisioning and resource management, enabling close-to-optimal performance and future adaptation.

# Graph Theoretic Mapping

- Graph theoretic algorithms will be used to decide how to optimally structure our approach:
  - (1) reduce/abstract the size/scale of the National Power Grid problem to realistically manage the problem of reliability validation/assessment, and ...
  - (2) make structural/architectural decisions (e.g., identify vulnerabilities/weaknesses and containment zones, as well as map agents to the grid hierarchy).

# Second Phase

- Second, given that analytical modeling is not sufficient to accurately represent complex power grid systems, we rely on large-scale leadership class *simulation and modeling at scale* approaches to evaluate the deployed agent-based control scenarios.
- Particularly challenging at this level of complexity is the problem of faults, which originate from different sources such as hardware malfunctions and software inadequacies.

# Systematic Fault Coverage

- Faults must be minimized at the design stage and a strategy be put in place to quickly diagnose and manage dynamic faults generated during the deployments.
- A testing methodology that performs *systematic fault coverage* is lacking in the area of distributed control using agents.
- This is particularly true in large-scale deployments such as the power grid, and furthermore the existing methods, when effective, are not particularly optimized for the power grid

# Anticipatory Diagnosis

- Simulations will run in real-time along with the controlled system to allow dynamic tuning of the simulation parameters, and create opportunities, when feasible, for *anticipatory diagnosis* of system failures.
- A grand challenge problem in the context of high-performance simulation, we will show in specific contexts how *early signs of an instability can be simulated faster than real-time to predict future failures*.
- Offering the opportunity for preemptive removal of weaknesses in the control system.

# Third Phase

## Autonomous SW Agents (SAs)

- Finally (third), monitoring/control and run-time self-healing will be facilitated using *autonomous* agents. SAs have the advantage that they can respond locally to abnormal stimuli derived from operational sensor data.
- An overlay network will be created via communicating agents to gather and present *situational data* to the control agents.
  - The data is collected by sensors, stored at caching agents, and forwarded to decision centers that are distributed across the network.

# Situational Data

## Activating the Healing Process

- These data sets are then correlated and fused at the centers and presented to the decision makers, either human or automated programs.
- By constantly monitoring the system using strategically deployed agents, problems can be quickly detected and diagnosed to activate the healing process.
- Self-healing networks require autonomous actuation of the network based on the dynamic sensor data to apply protective and reparative enhancements

# SCI: Hierarchical Evaluation

- Bottom-up two step approach:
  - Individual components of the infrastructure are evaluated in isolation to derive individual component survivability (CS). The process identifies feasible *mitigation* mechanisms on a per component basis.
  - 2nd step, CS is composed into the system-at-large (i.e., system-of-systems).
  - This approach leverages individual CS models to create hierarchical structures with increased system survivability (e.g., against failures due to the complexity of engaging unanticipated component interactions)

# Consequently,...

- Response policies and actuation techniques are driven by rule-engines at different points in the network hierarchy.
- These rule engines are control-system specific and communicate with the agent-infrastructure over well-defined interfaces.

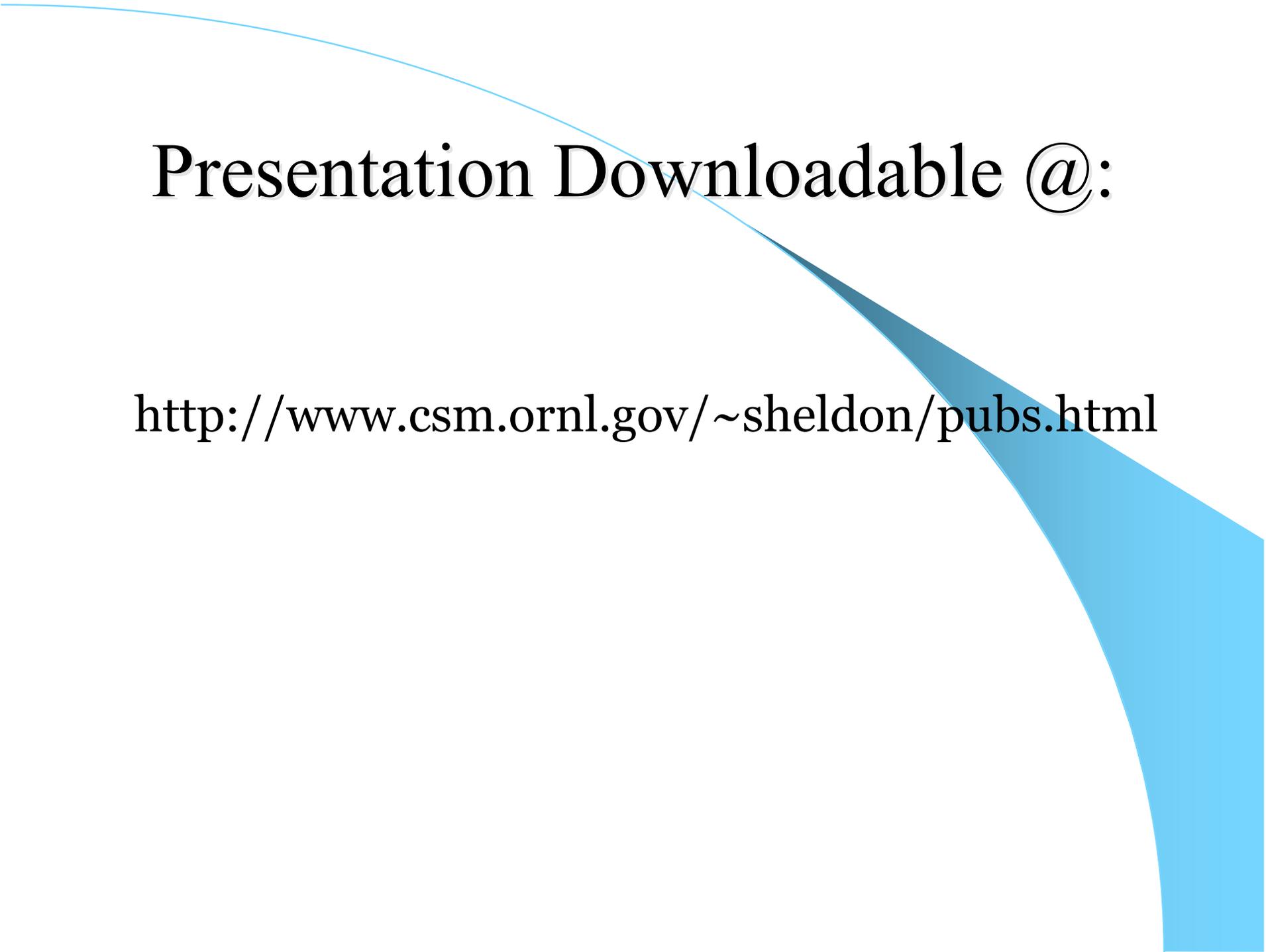
# Reliable Core Ensures System Stability

- However, due to the complexity of the power grid the actuation of one portion of the control network can cause rolling instabilities.
- A contained scheme will be devised to ensure that system improvements are only made around a reliable core, whose dynamics and correlations are rigorously specified and analyzed.
- Thus, while applied enhancements may take some time to take effect, *the reliable core ensures that the system is within stable operating ranges at all times.*

# Conclusion:

## Applications/ Prospects

- Survivability is pervasive in large complex systems (e.g., CIs), evolved within an ever changing context which is poorly understood.
- In this paper/ talk, *we have offered no solutions*, but shared our interest and our ideas on creating survivable/cyber-secure CIs.
- Our preliminary investigations show rationale that elicit the need for further investigation, development and validation.



Presentation Downloadable @:

<http://www.csm.ornl.gov/~sheldon/pubs.html>