

# Infrastructure Assurance

## Natural Gas Security Issues Related to Electric Power Systems

by Bill Buehring  
Argonne National Laboratory

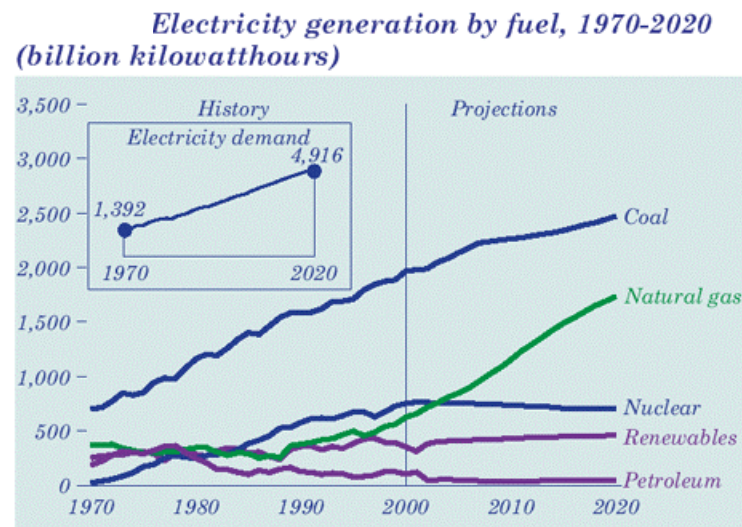
for  
Carnegie Mellon University  
Electricity Security and Survivability Workshop

November 28, 2001



## Natural Gas and Electric Infrastructures are Tightly Linked

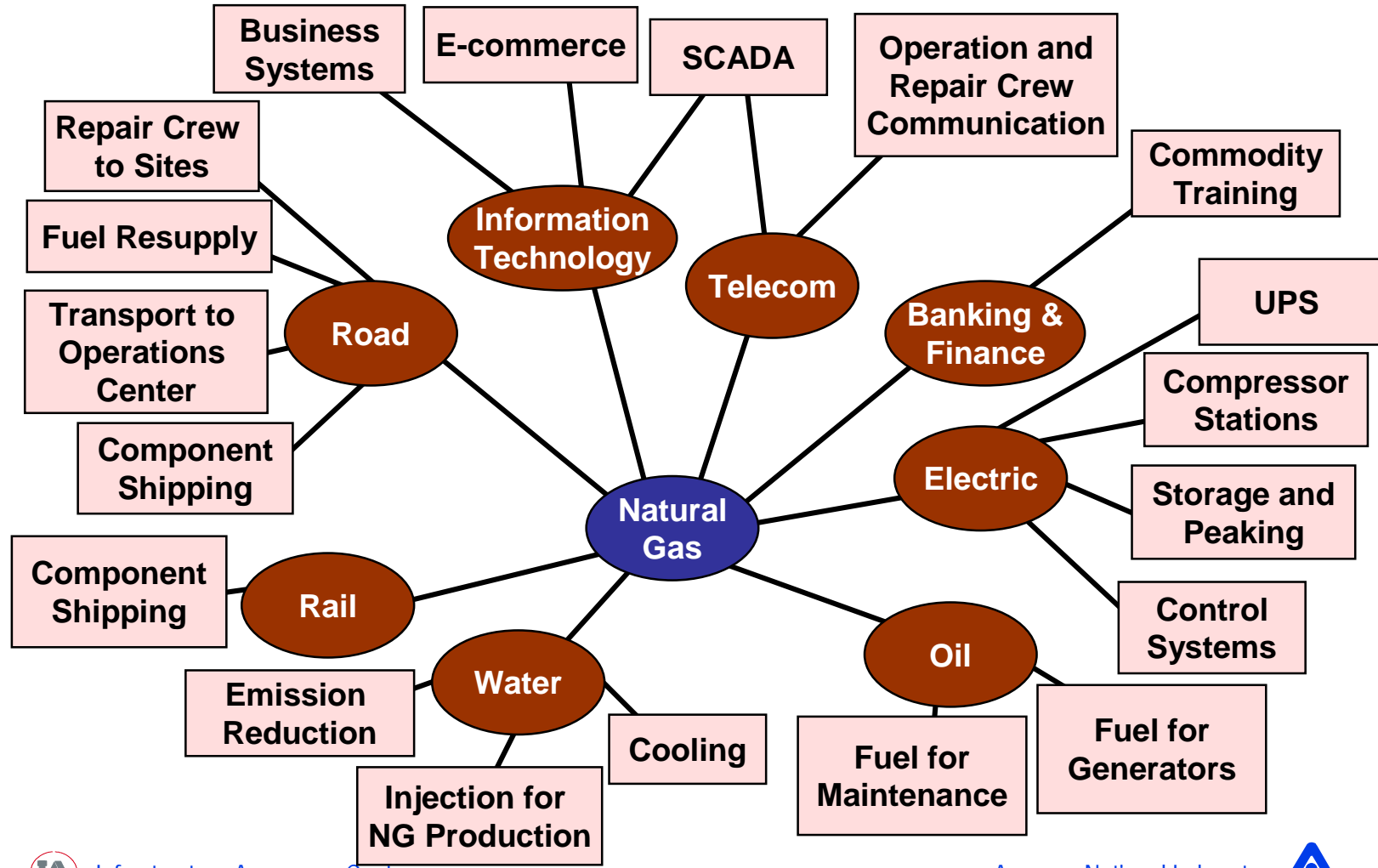
- Natural gas accounted for 16 percent of U.S. utility and non-utility electrical generation in 2000; 20 percent in July 2001
- In most regions, natural gas has become much more than a fuel source for peakers, e.g., gas accounts for over one-third of utility generation in the major gas-producing states
- Natural gas is expected to account for two-thirds of new generating capacity over the next 20 years and one-third of total U.S. electrical generation by 2020
- Conclusion: natural gas security issues are electric security issues



Source: DOE/EIA



# Illustrative Natural Gas Dependencies on Other Critical Infrastructures



## Broad Categories of Natural Gas Infrastructure

- **Physical facilities that either produce or deliver natural gas from production to consumption**
- **Automated control systems, such as Supervisory Control and Data Acquisition (SCADA), for physical facilities that produce or deliver natural gas**
- **Information databases, including but not limited to, corporate financial data, customer records, facility records, proprietary information, trade secrets, and any other records deemed critical to the success of the organization**



## Two Recent Energy Industry Reports Examined Infrastructure Protection

- ***Securing Oil and Natural Gas Infrastructures in the New Economy***, National Petroleum Council, Committee on Critical Infrastructure Protection (June 2001), available at [www.npc.org](http://www.npc.org)
- ***An Approach to Action for the Electricity Sector***, North American Electric Reliability Council, Working Group Forum on Critical Infrastructure Protection (June 2001), available at [www.nerc.com](http://www.nerc.com)



# Definition of Infrastructure Criticality

- **Enterprise Level**
  - Loss of the asset from intentional act would result in substantial financial harm to the enterprise and affects the enterprise as a whole
- **Industry Level**
  - Loss of the asset from intentional act would result in a failure to deliver essential public services, failure to ensure the general public health and safety, and cause long term harm to the viability of the industry
- **National Security Level**
  - Loss of the asset from intentional act would adversely impact the minimum operations of the economy and government



## Categories of Vulnerabilities Analyzed (NPC)

- **Growing reliance on information technology & telecommunications**
- **Acceleration of the global, interconnected economy**
- **Changes resulting from business restructuring**
- **Growing interdependence of all infrastructures**
- **Impact of changing political and regulatory environment**
- **Impact of physical and human factors on reliable operations**
- **Impact of natural disasters**



## **NPC Recommendations: Company & Industry Preparedness**

- **Each company should regularly conduct vulnerability assessments of its own systems and operations and take action as appropriate. Each company should also conduct assessments of its partners' vulnerabilities.**
- **Industry and government should advocate the development, adoption, and implementation of global IT processes to reduce vulnerabilities of cyber and other electronic systems.**
- **The oil and natural gas industries should enhance their response and recovery plans, including participation in regional response and recovery planning and exercises to deal with disruptions to physical and cyber infrastructures.**



## **NPC Recommendations: Information Sharing & Sector Coordination**

- **The oil and natural gas industries should establish a secure information-sharing mechanism using an industry-directed service provider.**
- **Under the current law and legal environment, the Information Sharing and Analysis Center (ISAC) would only share information with members from the oil and natural gas industry.**
- **Individual companies in the oil and natural gas industry will take the lead in establishing a board, which will investigate, develop, and implement an ISAC for the sector.**
- **The NPC recommended that the Secretary of Energy formally acknowledge the designee of the governing body of the Energy-ISAC as the permanent sector coordinator.**



## **NPC Recommendations: Government Actions**

- **The federal government should enact legislation to facilitate information sharing with and among sector components. Specifically, the issues of FOIA exemptions, anti-trust and liability relief need to be properly addressed.**
- **Government and industry should work together to develop processes that ensure industry's access to law enforcement and intelligence information that is actionable in real-time.**
- **The federal government should use all means available to encourage countries to enact globally consistent laws addressing the interconnected, electronic commercial marketplace.**
- **All components of U.S. energy sectors should be viewed as a single energy infrastructure for critical infrastructure protection.**



## **NPC Recommendations: Government Actions (continued)**

- **Response and recovery preplanning should be undertaken to minimize jurisdictional conflicts among government entities (federal, state and local) during the response to and recovery from a major emergency.**
- **Government-funded research and development should address national security and other key critical infrastructure protection, mitigation, response and recovery needs that transcend individual companies.**
- **The government should continue its critical infrastructure protection initiatives and organize itself to effectively interact with industry on a broad range of mutual critical infrastructure protection issues.**



# ENERGY/ISAC Vision & Founding Members

## Vision

To provide a unique and customized set of information sharing and analysis services that will enhance the capability of the energy industries to identify and reduce infrastructure vulnerabilities, to protect from cyber or physical attacks or disruptions, and to respond to and recover from attacks or disruptions restoring service to customers as quickly as possible.

[www.energyisac.com](http://www.energyisac.com)

## Founding Members

- Anadarko Petroleum Corp.
- British Petroleum
- Conoco Inc.
- Duke Energy Corporation
- El Paso Corporation
- Enron Corporation
- Halliburton Company
- Peoples Energy Corporation
- Phillips Petroleum Company
- Shell Oil Company

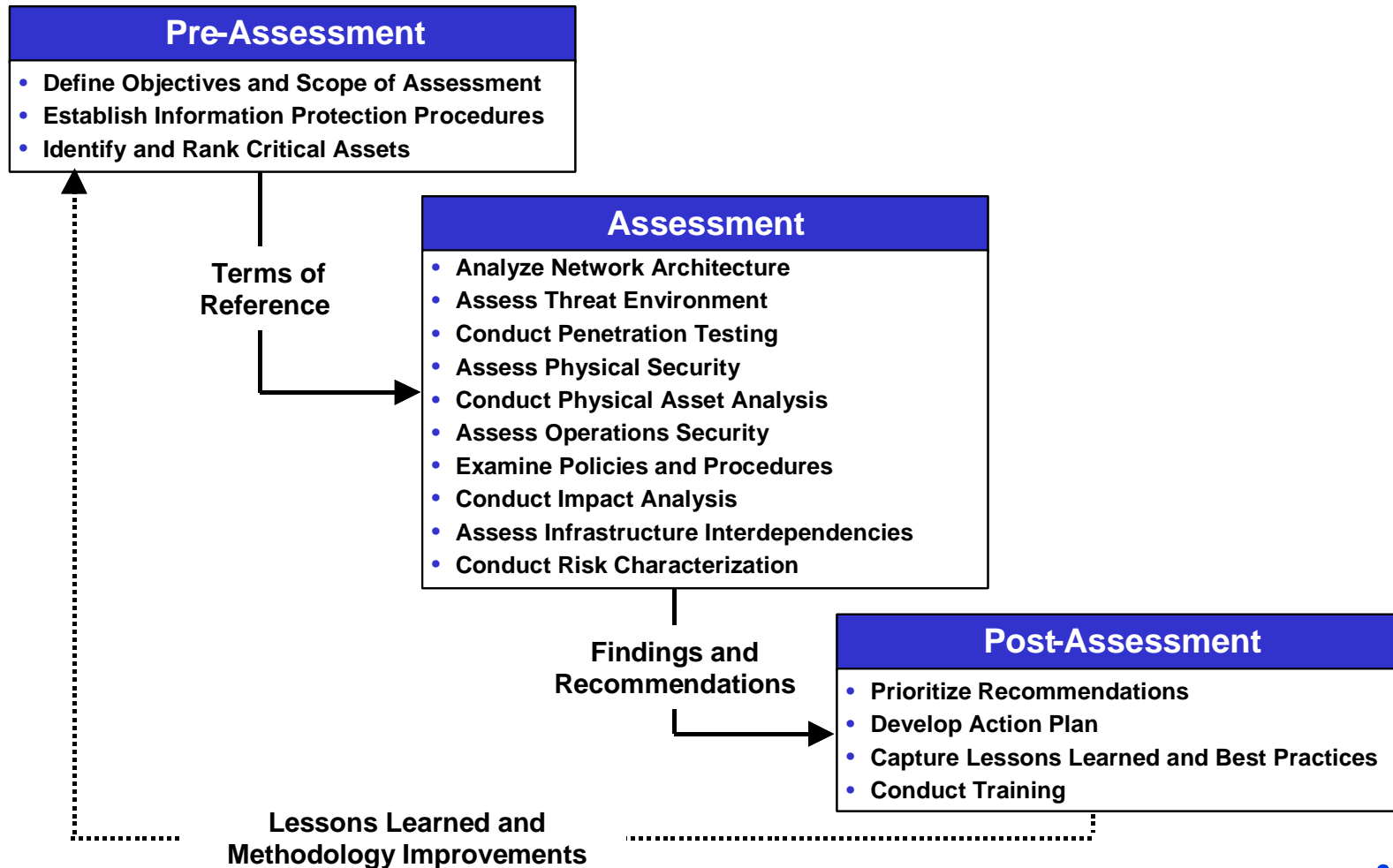


## **U.S. Department of Energy Vulnerability and Risk Analysis Program (VRAP)**

- **Initiated program in FY 1998**
- **Intended to raise awareness of threats and vulnerabilities**
- **Focused initially on electric power information technology systems**
- **Expanded program to all energy sources and to include physical, cyber, and interdependencies**
- **Conducted 11 assessments at electric and natural gas utilities and organizations to date**



# DOE VRAP Vulnerability Assessment Process



# Vulnerability Assessment Lessons Learned

- **Network Architecture** – Network perimeter should be defined and external connections minimized. Mission critical systems should have added security and protection
- **Threat Environment** – Background investigations for new hires and periodic updates for current employees are crucial
- **Penetration Testing** – Security measures such as traffic filtering, authorized controls, encryption, and access controls, minimizing or disabling of unnecessary services and commands, email filtering and virus control should be implemented
- **Physical Security** – A formal physical security program is essential. Such a program should include listing critical assets, developing a mission statement, defining threats, defining acceptable risks, and applying a vulnerability assessment methodology.
- **Physical Asset Analysis** – Companies should compare their operating procedures with best practices and procedures used throughout the industry

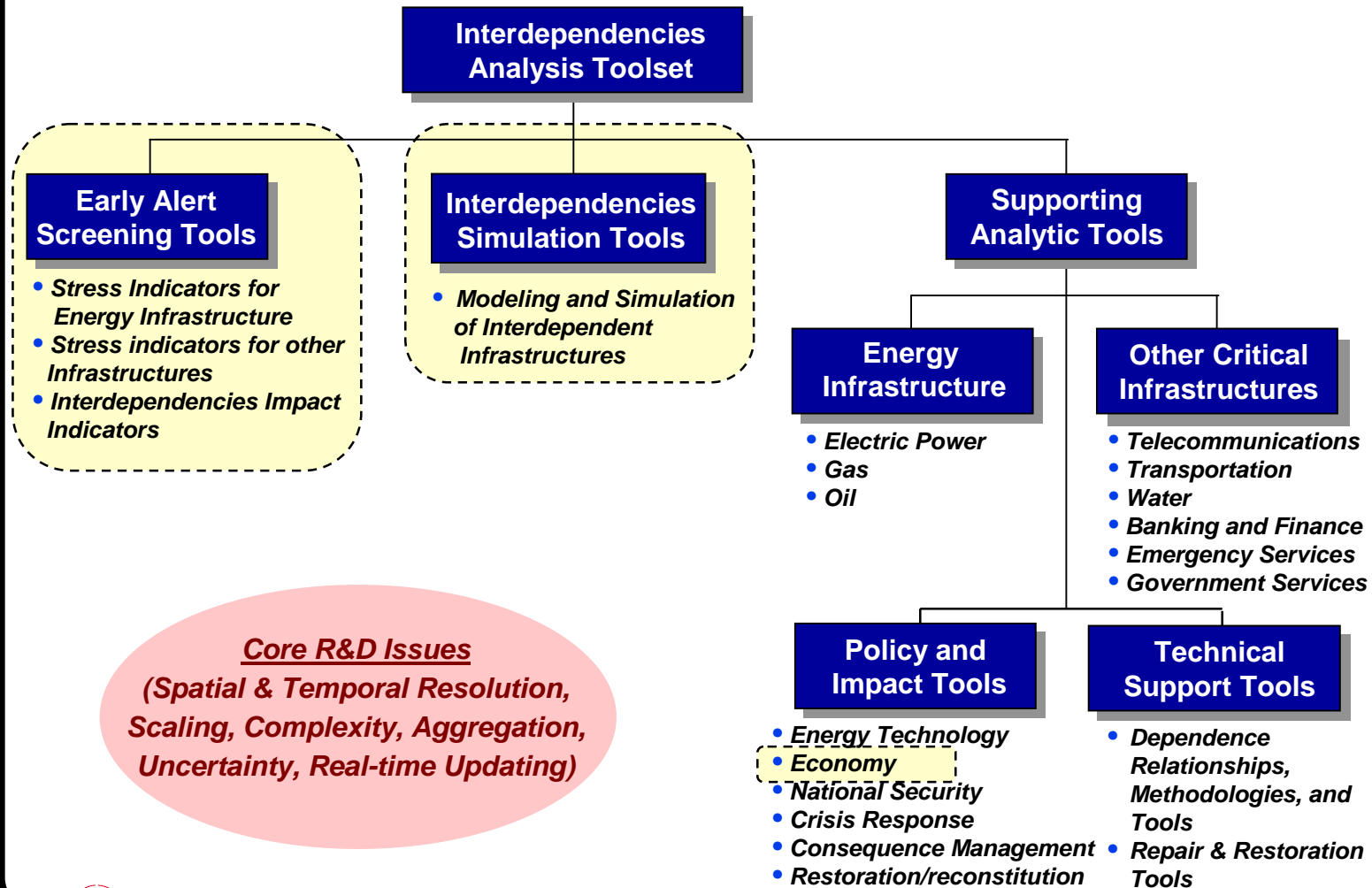


## Vulnerability Assessment Lessons Learned (Cont'd)

- **Operational Security** – A five step program of identifying critical assets, analyzing threats, analyzing indicators and vulnerabilities, assessing risk, and applying appropriate countermeasures should be implemented to enhance the security of a company's sensitive assets
- **Policies and Procedures** – Formalized policies and procedures provide a foundation for achieving the desired level of security
- **Impact Analysis** – Estimates of the potential consequences, including economic implications, of not mitigating identified vulnerabilities or addressing security concerns are necessary in order to effectively apply risk management approaches to evaluate mitigation and security recommendations
- **Infrastructure Interdependencies** – Contingency and response plans need to be evaluated from an infrastructure interdependencies perspective and coordination with other infrastructure providers needs to be enhanced
- **Risk Characterization** – The risk management process for addressing security concerns should be integrated into the corporate risk management process



# Initial Development Activities for DOE's Energy Infrastructure Interdependencies Program



# ALERT: Assessment of Levels of Energy-Infrastructure Reliability Threats

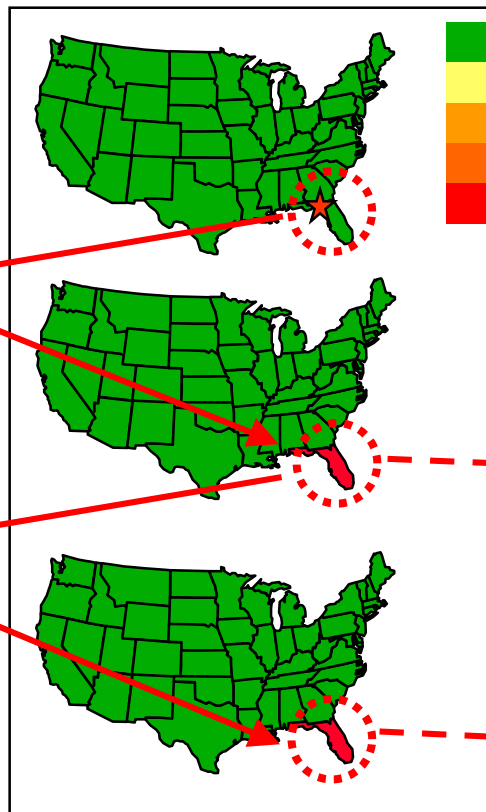
## Illustration: Major Natural Gas Compressor Station Outage in Florida

### Lightning Strike on Perry Compressor Station

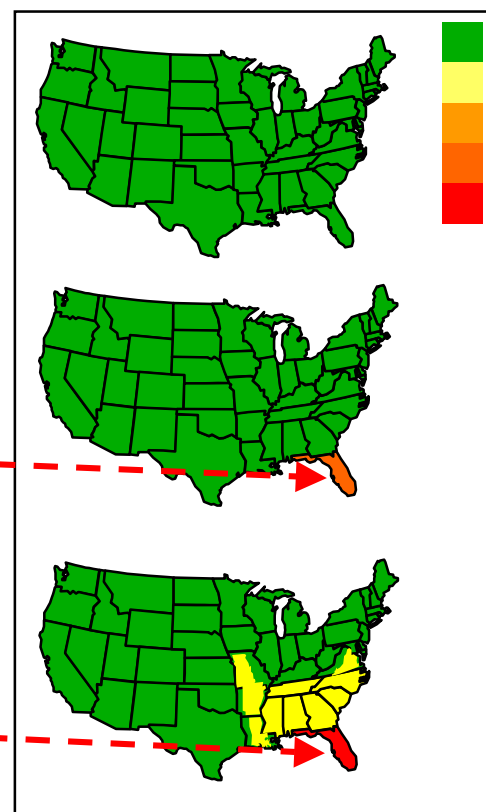
- August 14, 1998
- Florida Gas Transmission Co.
- Three pipelines ruptured
- Partial service within 70 hours



### Baseline Health Indicators: Natural Gas



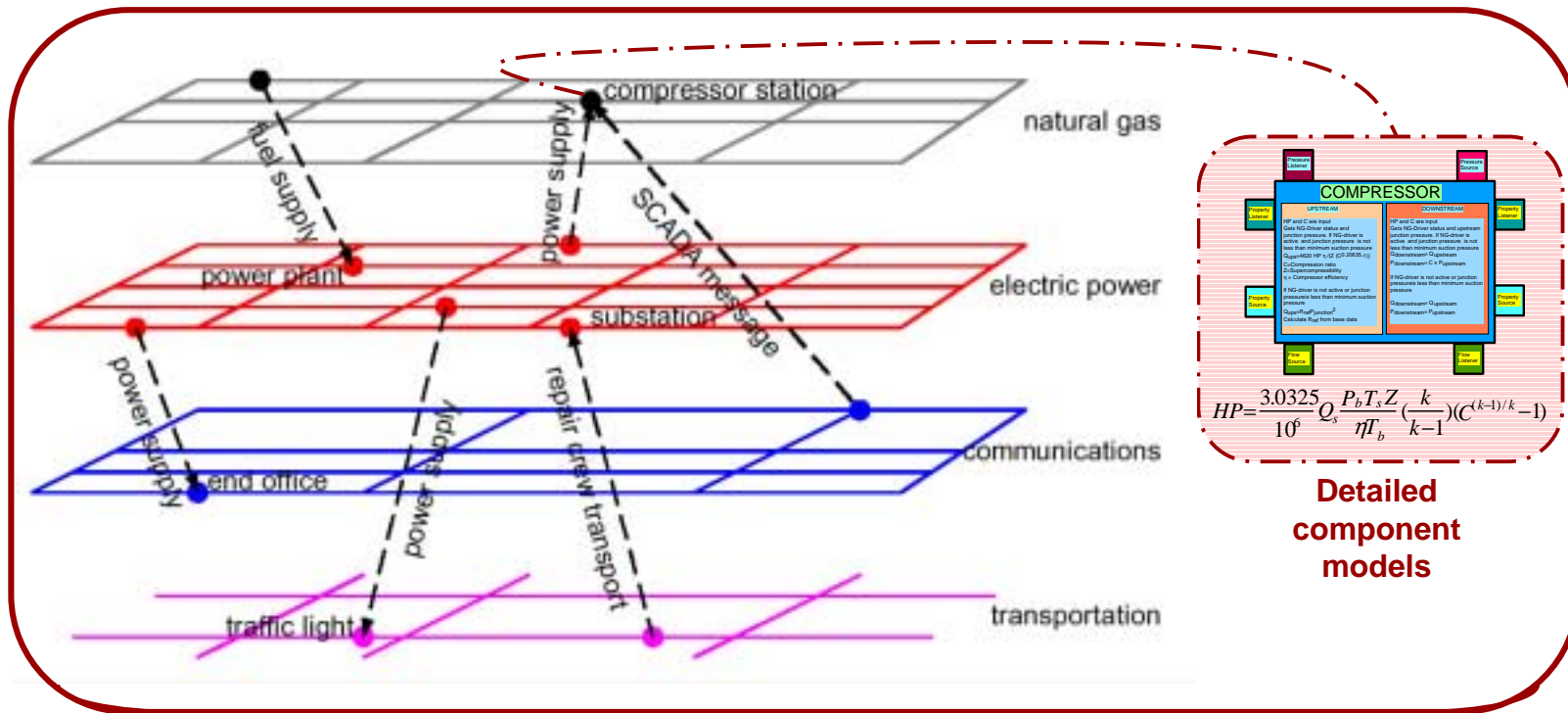
### Baseline Health Indicators: Electric Power



Possible  
Implications of  
Extremely Hot  
Weather



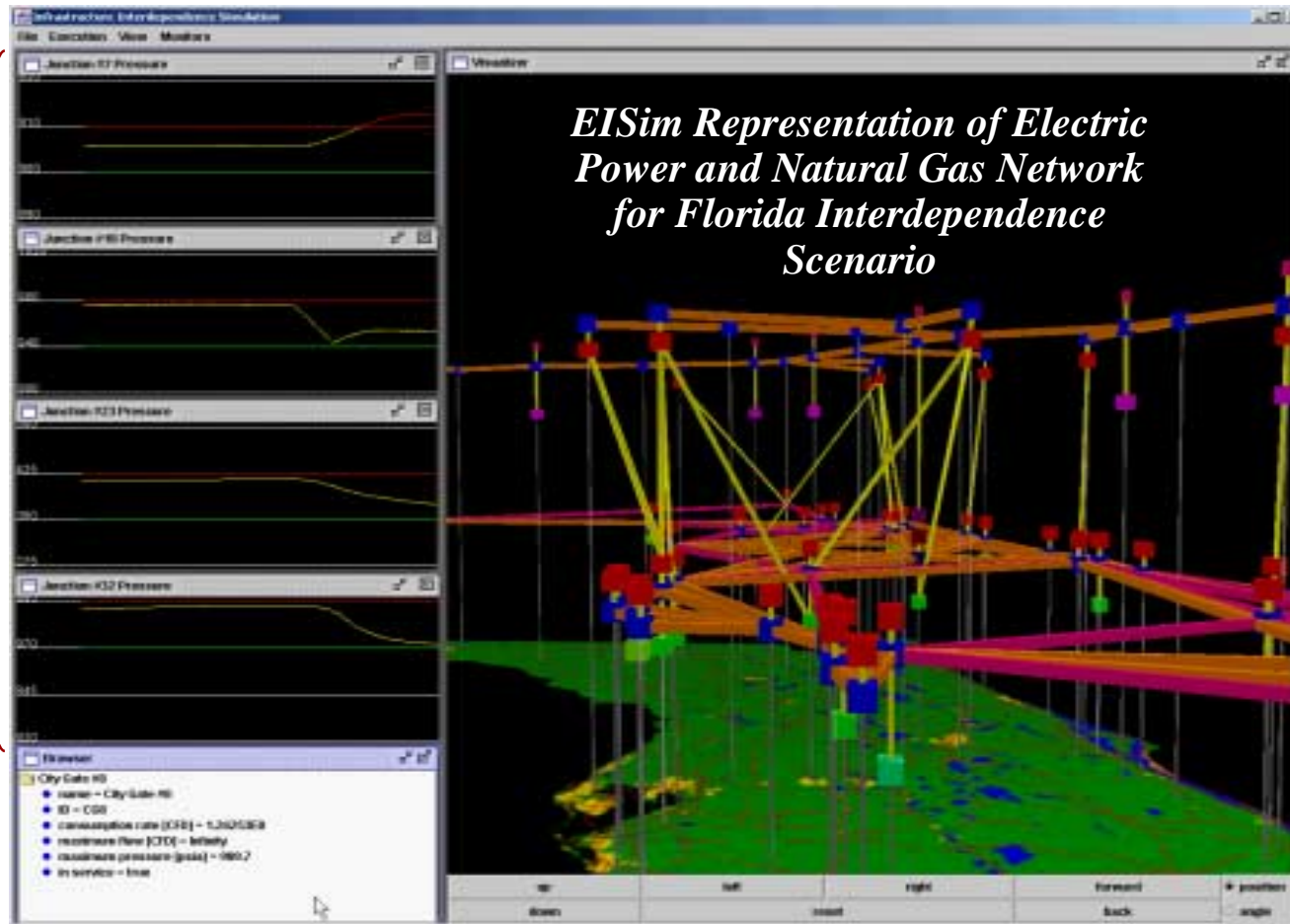
# Energy Infrastructure Simulation (EISim) Concept



- **Critical system components and vulnerabilities**
- **Interdependence propagation pathways and degree of coupling**
- **Spatial and temporal system behavior**
- **Evaluation of protection, mitigation, response, and recovery options**
- ...



# EISim Visualization



*Natural Gas Infrastructure*

*Electric Power Infrastructure*

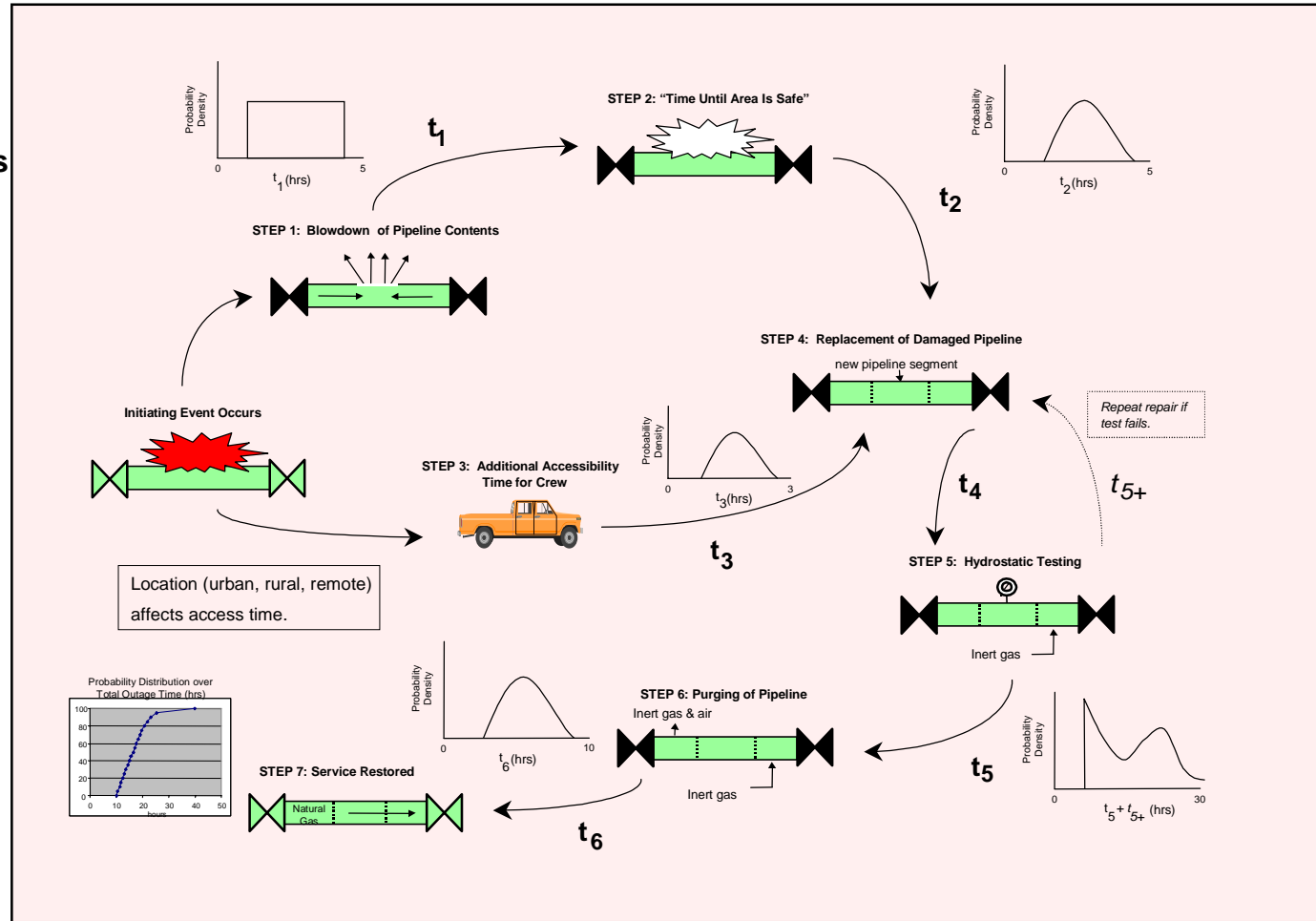
*GIS Layer*

*Component Behavior Monitors*



# CI<sup>3</sup> Example: Repair and Restoration of a Damaged Natural Gas Pipeline

CI<sup>3</sup> is the Critical Infrastructures Interdependencies Integrator

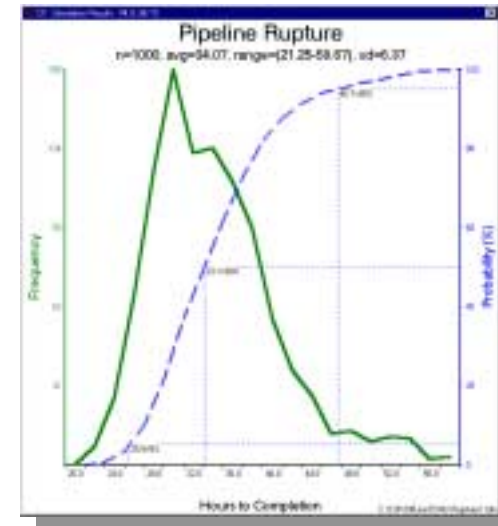
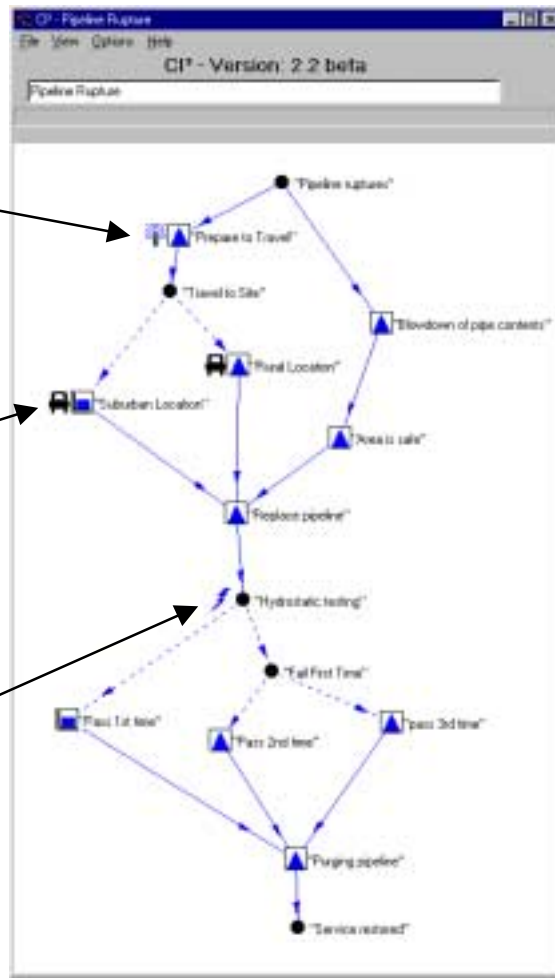


# Repair and Restoration of a Damaged Natural Gas Pipeline — A CI<sup>3</sup> Transition Diagram

Dependence on Telecommunications

Dependence on Transportation (Road)

Dependence on Electric Power

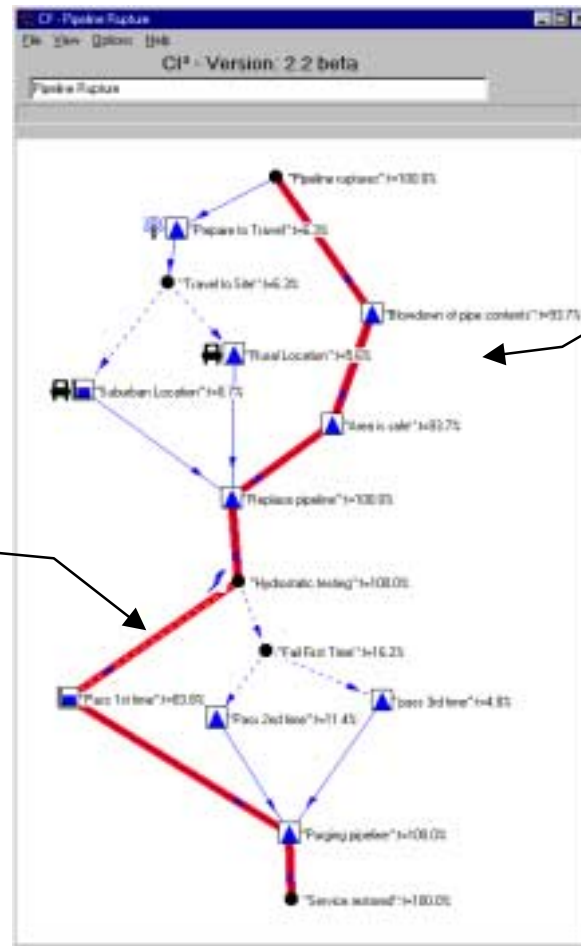


This graph tells us that:

- Outage duration range 21-59 hrs
- Most likely value is about 30 hrs
- Probability that duration  $\geq 25$  hours is 95%



## A CI<sup>3</sup> Transition Diagram Showing the “Most Active” Path



Testing is usually successful on the first attempt

Blowdown and time until area is safe usually takes more time than travelling to the site



## Benefits of Interdependencies Analysis Tools

- **Facilitate understanding of how disruptions—**
  - Propagate (cascade) among infrastructures
  - Exacerbate repair and restoration problems
- **Identify critical components and vulnerabilities from interdependencies perspective (transcends single infrastructure perspective of asset criticality)**
- **Determine consequences of disruptions (e.g., economic impacts)**
- **Allow “what if” analyses**
- **Support exercises, training, and education**



## The NPC Report Outlined Research and Development Needs

- Information assurance
- Interdependencies and system complexity
- Physical protection assessment
- Multisensor and warning technologies
- Protection and mitigation
- Risk management
- Critical consequence analysis
- SCADA protection enhancement
- Monitoring and detection
- Modeling and simulation
- Decision support
- Institutional barriers



## **The CIAO Identified Interdependency and Complexity R&D Topics and Roadmaps**

- **Identification and characterization of dependencies**
- **Analysis of scale, complexity and trends**
- **System analysis and simulation tools**
- **Consequence analysis and risk management methodologies and tools**
- **Protection and mitigation**
- **Response and recovery**

***Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures, Critical Infrastructure Assurance Office (July 1998), available at [www.ciao.gov](http://www.ciao.gov)***

