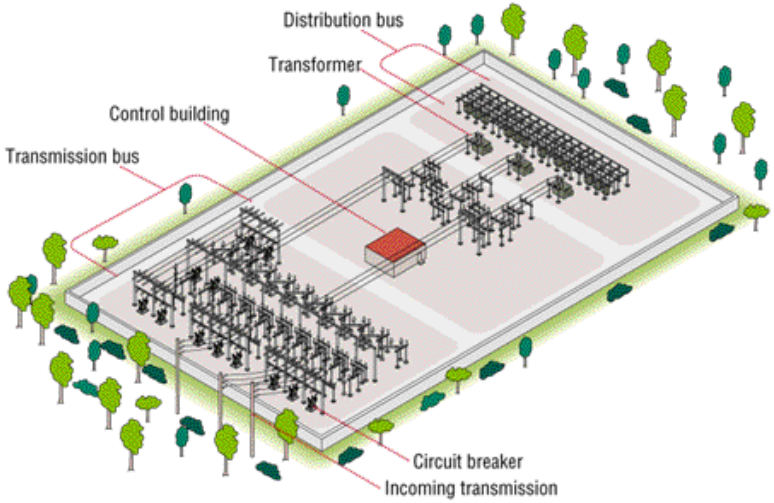
Supervisory Control and Data Acquisition (SCADA) Introduction

Jeff Dagle, PE
Pacific Northwest National Laboratory
Grainger Lecture Series for the
University of Illinois at Urbana-Champaign
September 15, 2005

Supervisory Control and Data Acquisition (SCADA)



CONTROL

- Generator Set Points
- Transmission Lines
- Substation Equipment

DATA

- Critical Operational Data
- Performance Metering
- Events and Alarms

Control Center

Provides network status, enables remote control, optimizes system performance, facilitates emergency operations, dispatching repair crews and coordination with other utilities.

SCADA is used extensively in the electricity sector. Other SCADA applications include gas and oil pipelines, water utilities, transportation networks, and applications requiring remote monitoring and control. Similar to real-time process controls found in buildings and factory automation.

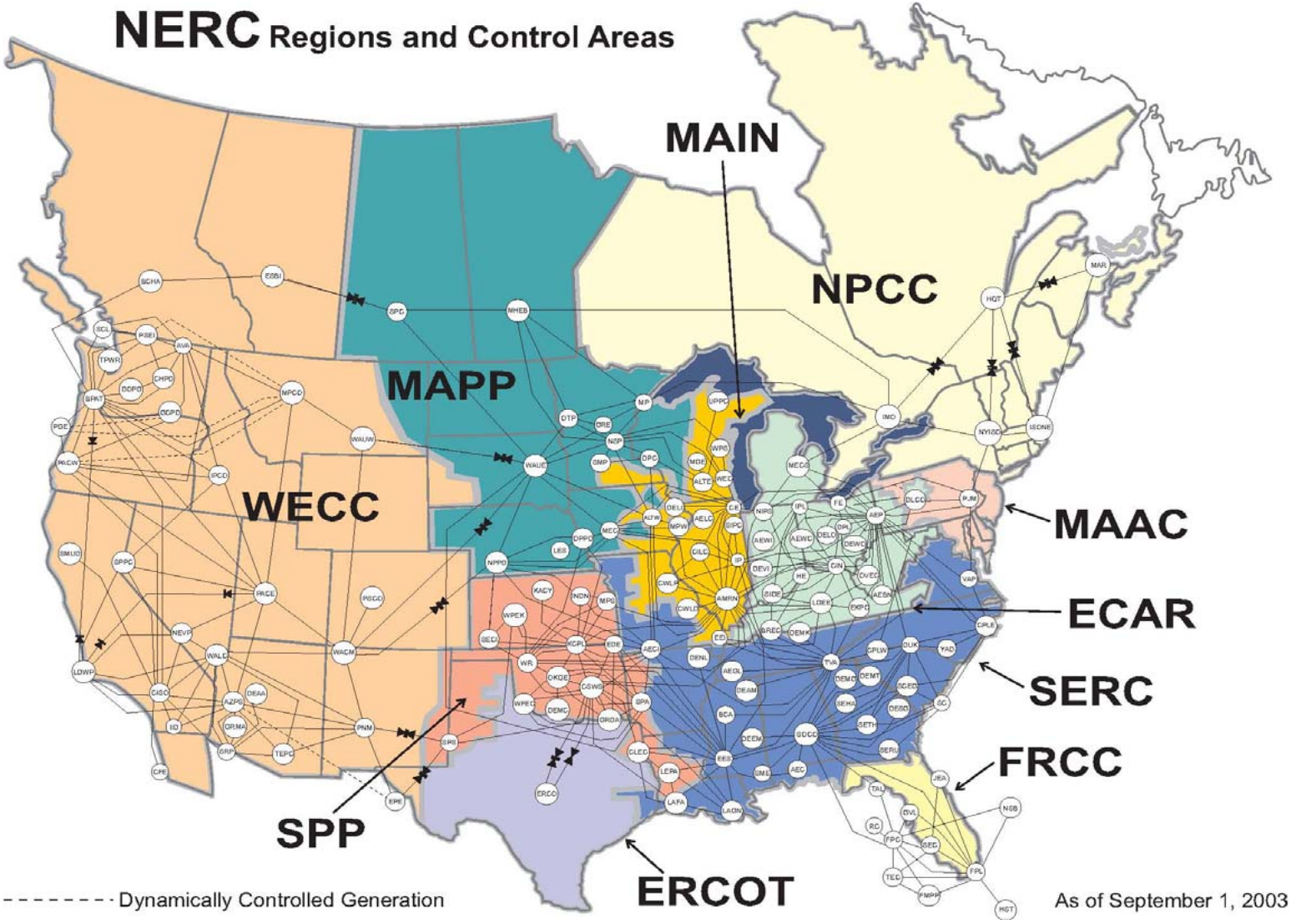
Communication Methods

- Directly wired
- Power line carrier
- Microwave
- Radio (spread spectrum)
- Fiber optic

Control Strategy

- Control Center
  - Supervisory control and data acquisition
  - Balance generation and demand (dispatching)
  - Monitor flows and observe system limits
  - Coordinate maintenance activities, emergency response functions
- Localized (Power Plants, Substations)
  - Feedback controls (e.g., governors, voltage regulators)
  - Protection (e.g., protective relays, circuit breakers)
- Key Priorities:
  1. Safety
  2. Protect equipment from damage
  3. Reliability
  4. Economics

Control Areas



Reliability Overview

- Balance generation and demand
- Balance reactive power supply and demand
- Monitor flows and observe thermal limits
- Observe power and voltage stability limits
- Operate for unplanned contingencies
- Plan, design and maintain a reliable system
- Prepare for emergencies

Reliably operate the system you have!

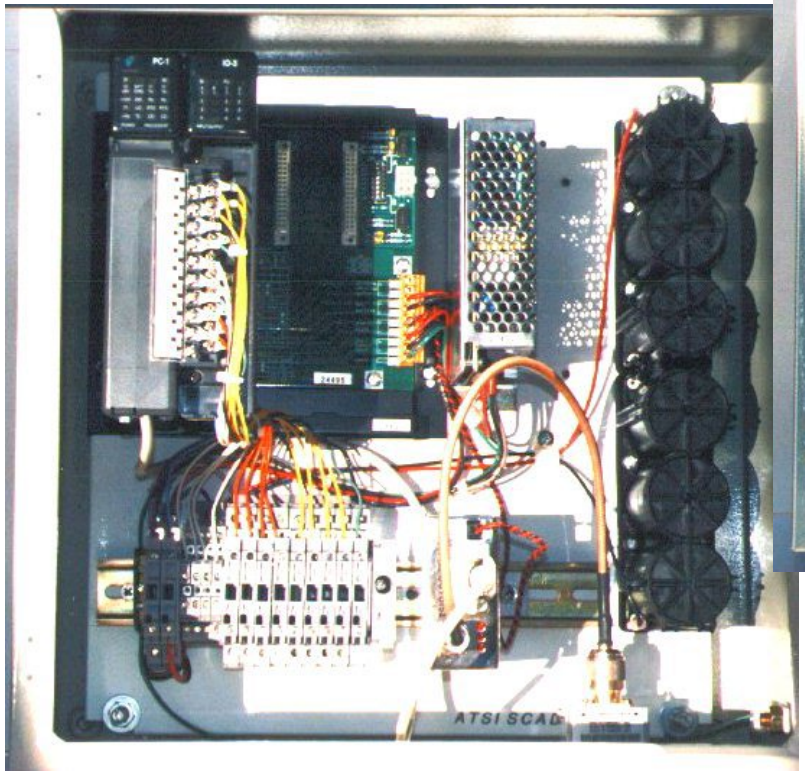
SCADA Functions

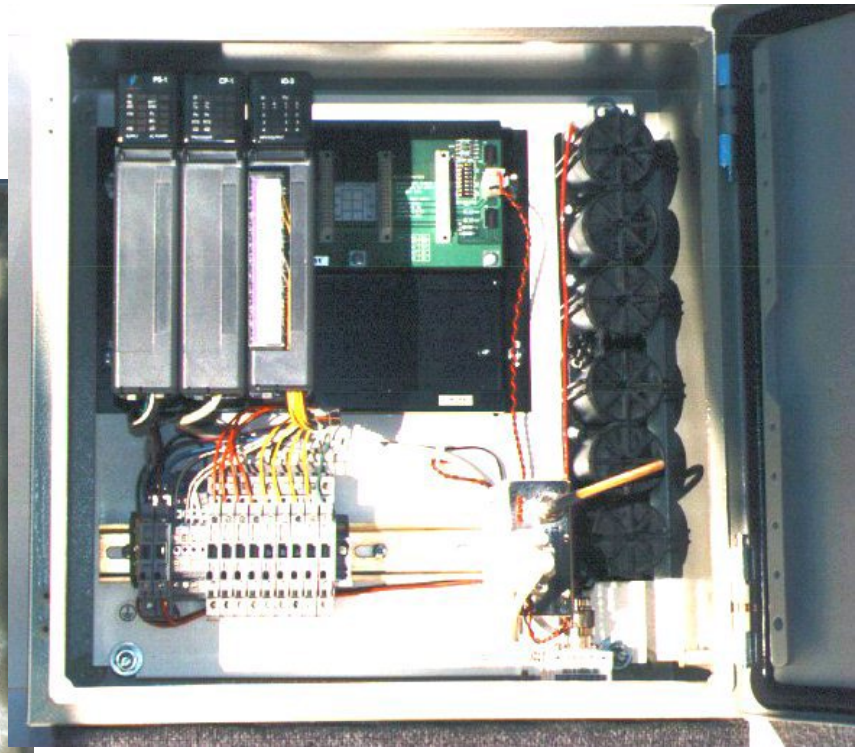
- Supervisory Control
- Data Acquisition
- Real Time Database
- Graphical Operator Interface
- Alarm Processing
- Data Historian/Strip Chart Trending
- Mapboard Interface

SCADA Principles of Operation

- Interface with Physical Devices
  - Remote terminal unit (RTU)
  - Intelligent electronic device (IED)
  - Programmable logic controller (PLC)
- Communications
  - Directly wired (typical for shorter distances)
  - Power line carrier (less common)
  - Microwave (very frequently used)
  - Radio (VHF, spread spectrum)
  - Fiber optic (gaining popularity)

Typical RTU Hardware





Typical IED Hardware

Typical PLC Hardware

Energy Management System (EMS) Functions

- Control
  - Automatic Generation Control (AGC)
  - Voltage Control
  - Interchange Transaction Scheduling
  - Load Shedding & Restoration (including special stability controls)
- Analysis
  - State Estimation/Contingency Analysis
  - Economic Dispatch
  - Short Term Load Forecasting

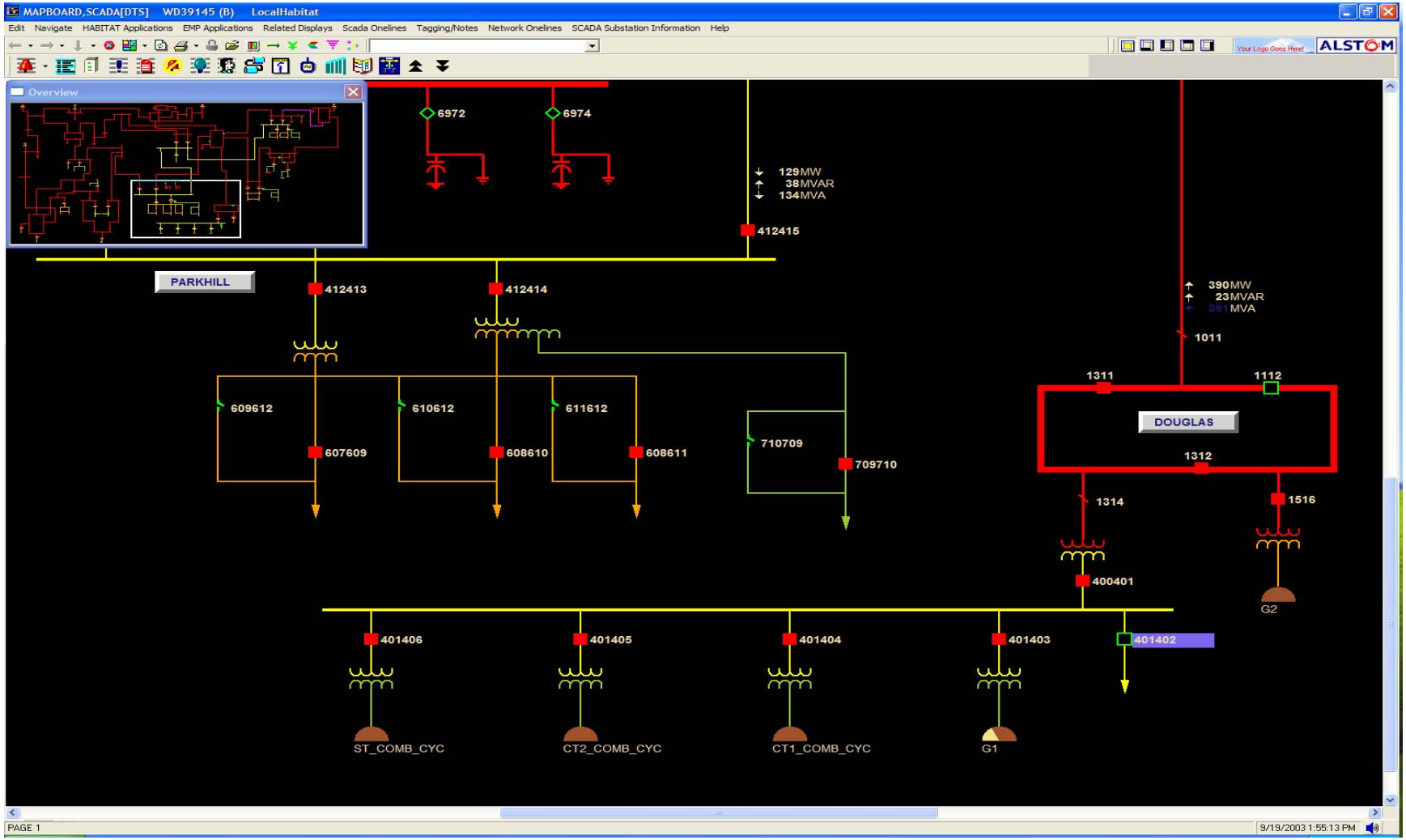
Typical Control Room Layout

Typical Operator Interface

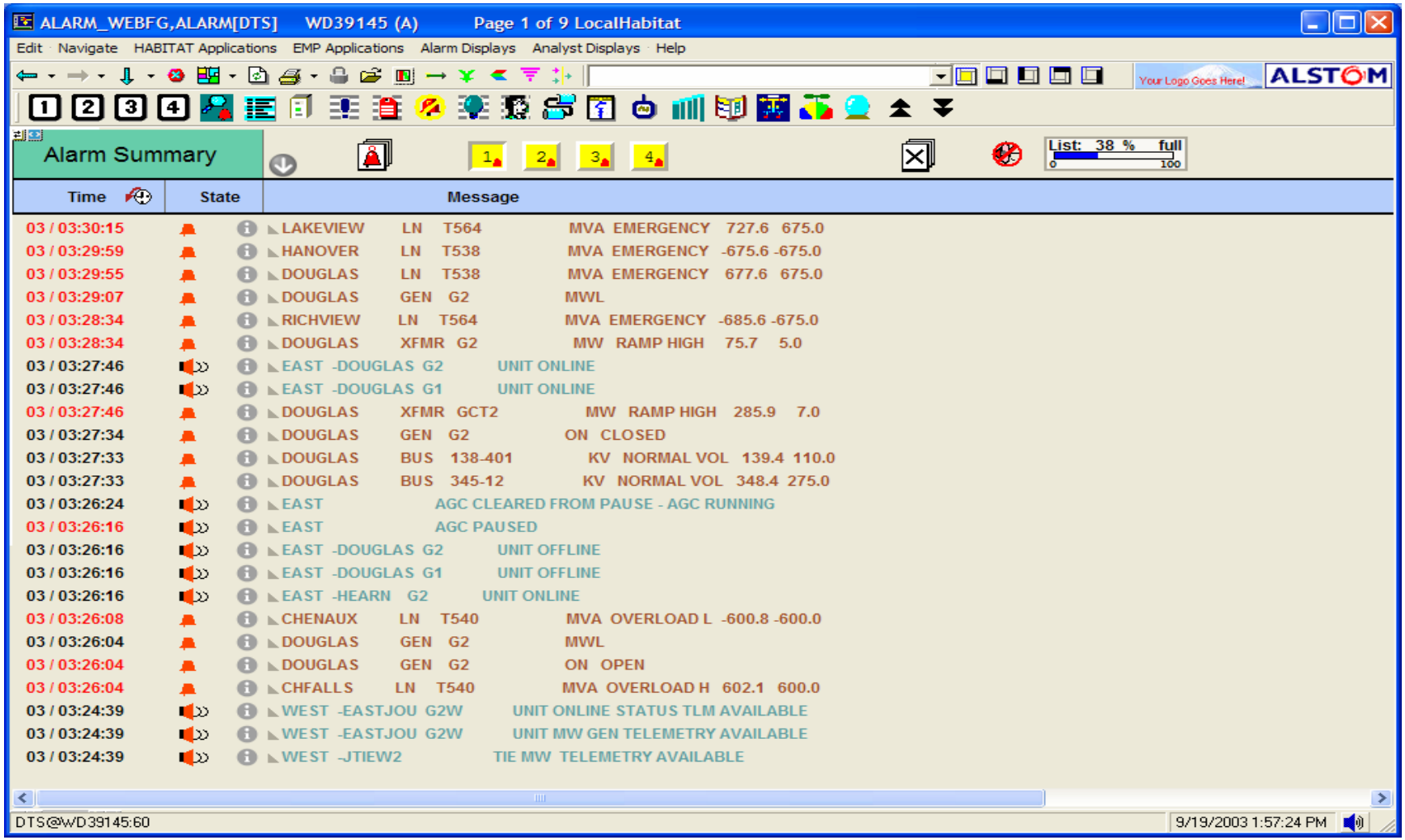
Operator Display and Control Functions

- Display real-time network status on geographic and schematic maps
- Control of circuit breakers and switches
- Graphical user interface -pan, zoom, decluttering
- Dynamic coloring to show real-time changes
- On-line data modification for construction and maintenance
- Optimization functions and decision making support

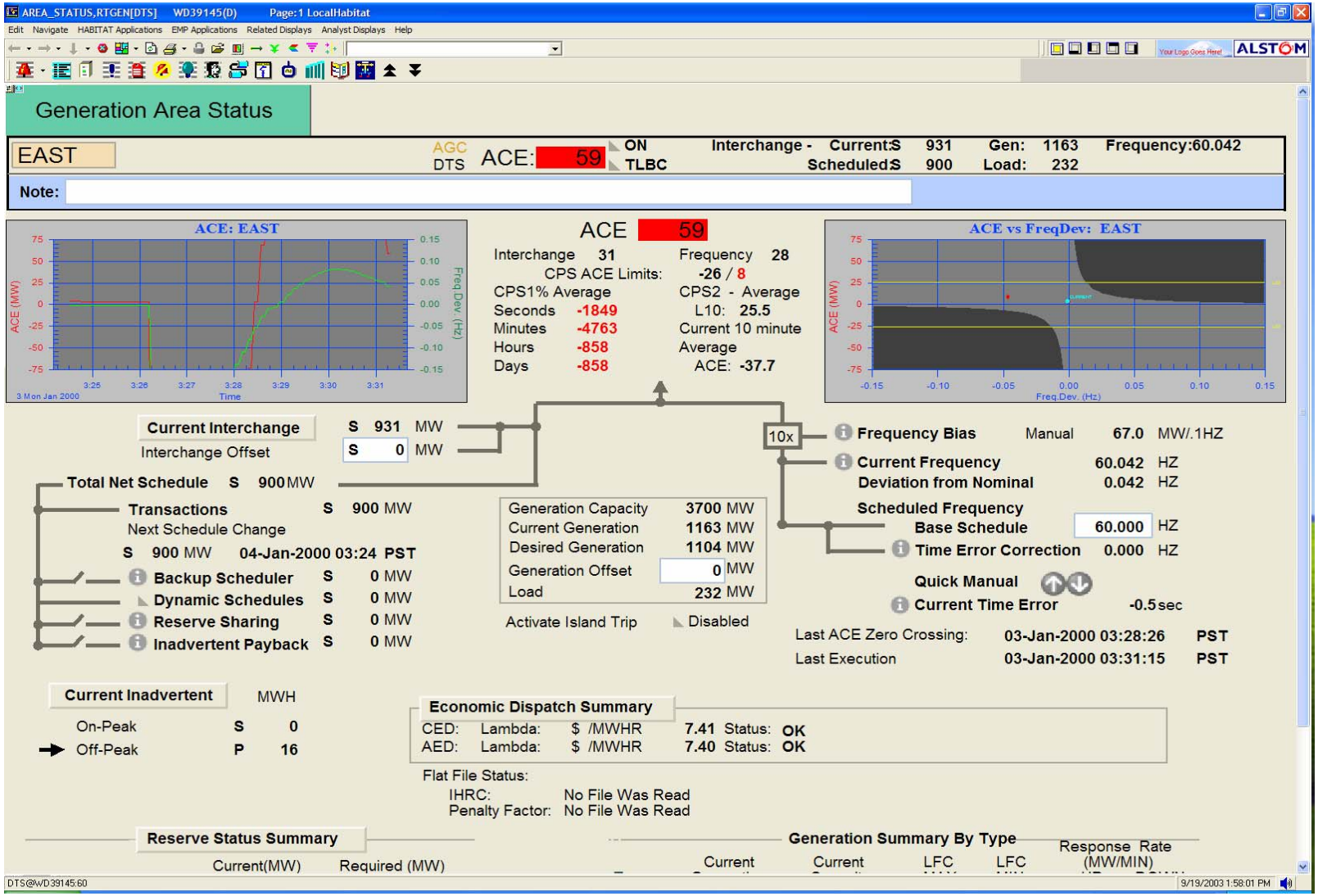
One-Line Diagram



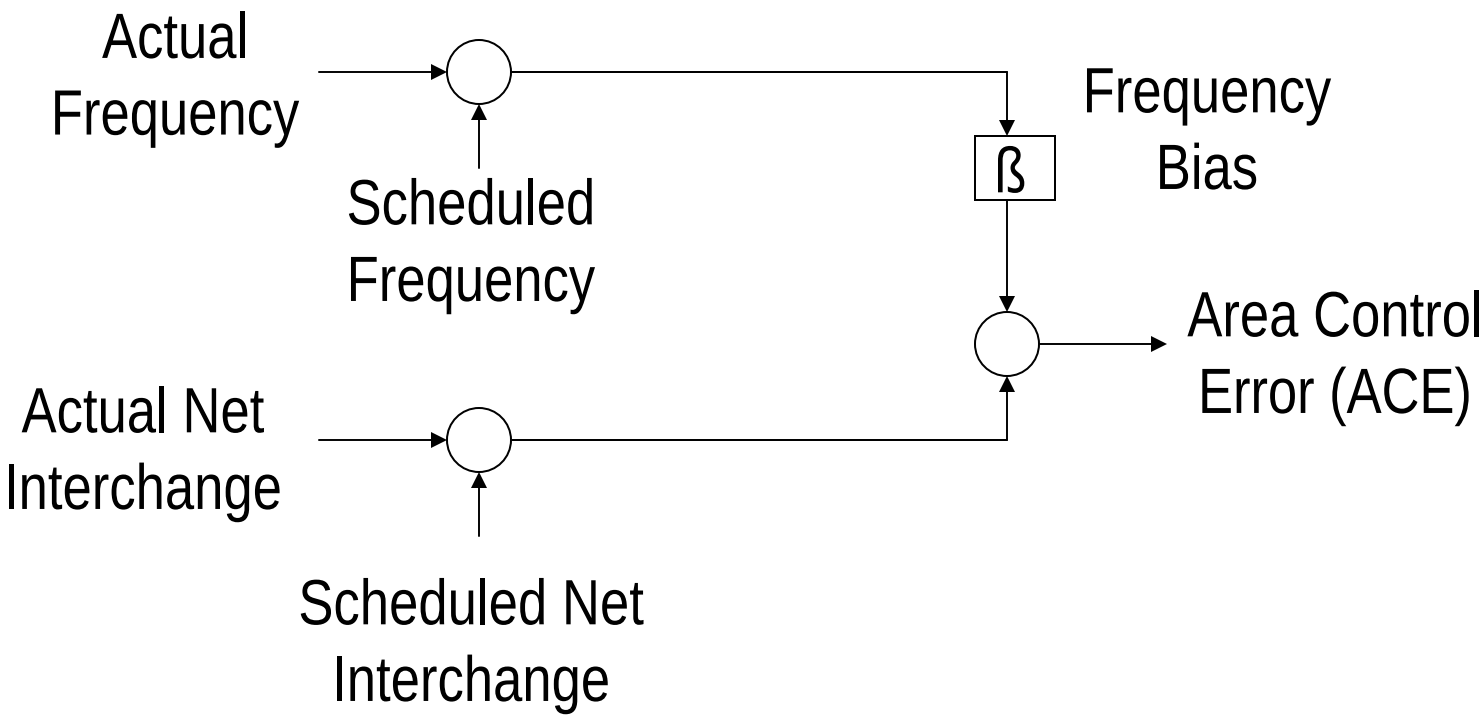
Alarm Processor



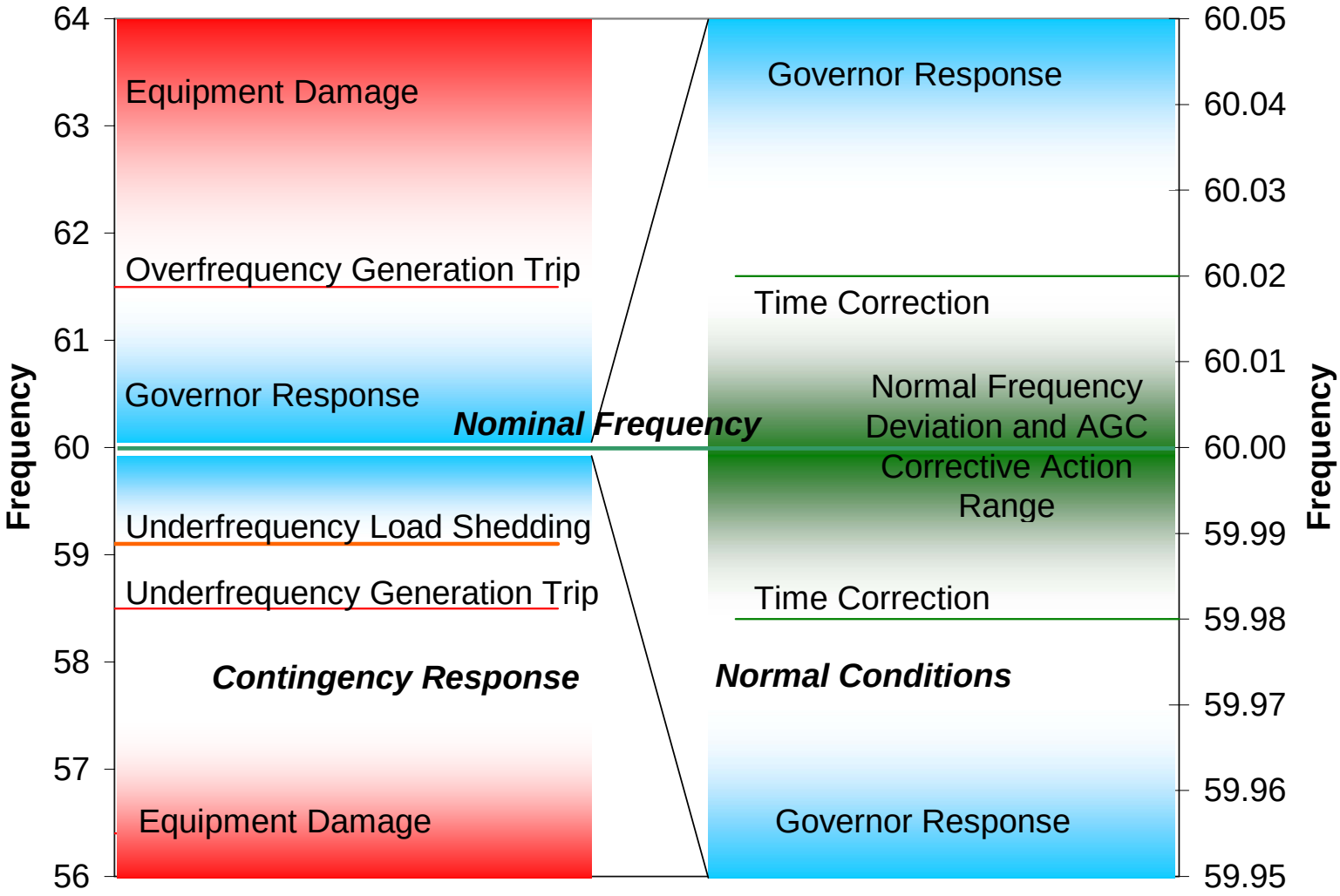
Frequency Control



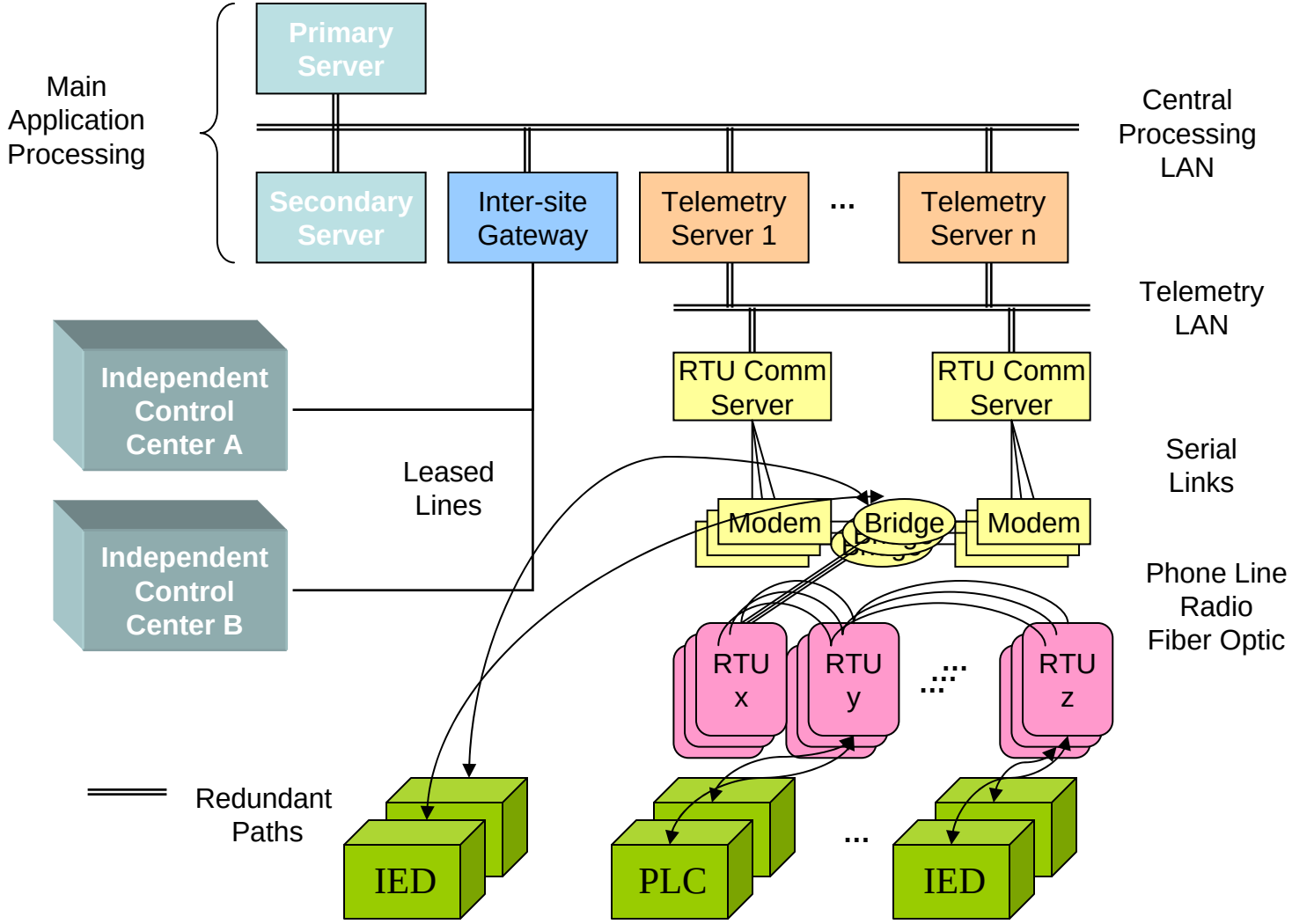
Frequency Control



Frequency Regulation



Typical SCADA Architecture



SCADA Trends

- Open Protocols
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Interconnected to Other Systems
  - Connections to business and administrative networks to obtain productivity improvements and mandated open access information sharing
- Reliance on Public Information Systems
  - Increasing use of public telecommunication systems and the internet for portions of the control system

Key Technology Drivers

- Open architectures and protocols
- Microprocessor-based field equipment
  - “smart” sensors and controls
- Convergence of operating systems
- Ubiquitous communications
  - cheaper, better, faster

Interconnections with SCADA Networks

- ***Business and Engineering Networks***
  - ***The IT link between engineering and business services is crucial for business operation***
  - ***How the link is made is crucial for security***
- ***Market Systems***
  - ***Interconnection into market systems is relatively new***
  - ***Some disagree this should be done***
  - ***Few agree on how it should be done securely***

Sharing of Telecommunication Bandwidth

- It is no longer true that utilities have stand-alone isolated systems for their SCADA communications networks, under the sole control and jurisdiction of the utility.
- In some cases, utilities have purchased bandwidth from telecommunications providers.
- In other cases, utilities sell excess bandwidth to others (either other business units within the enterprise, or outside entities).
- In many cases, there are multiple communication technologies (e.g., fiber optic, microwave, spread spectrum, twisted pair, etc.) and/or bandwidth owners/operators for a single SCADA system (particularly for larger utilities).
  - Mixture of legacy communication systems with other solutions

Major SCADA/EMS Vendors

- Asea Brown Boveri (ABB)
- Areva (formerly ESCA)
- GE Harris
- Siemens
- Advanced Control Systems (ACS)
- Open Systems International (OSI)

SCADA Protocols (Partial List!)

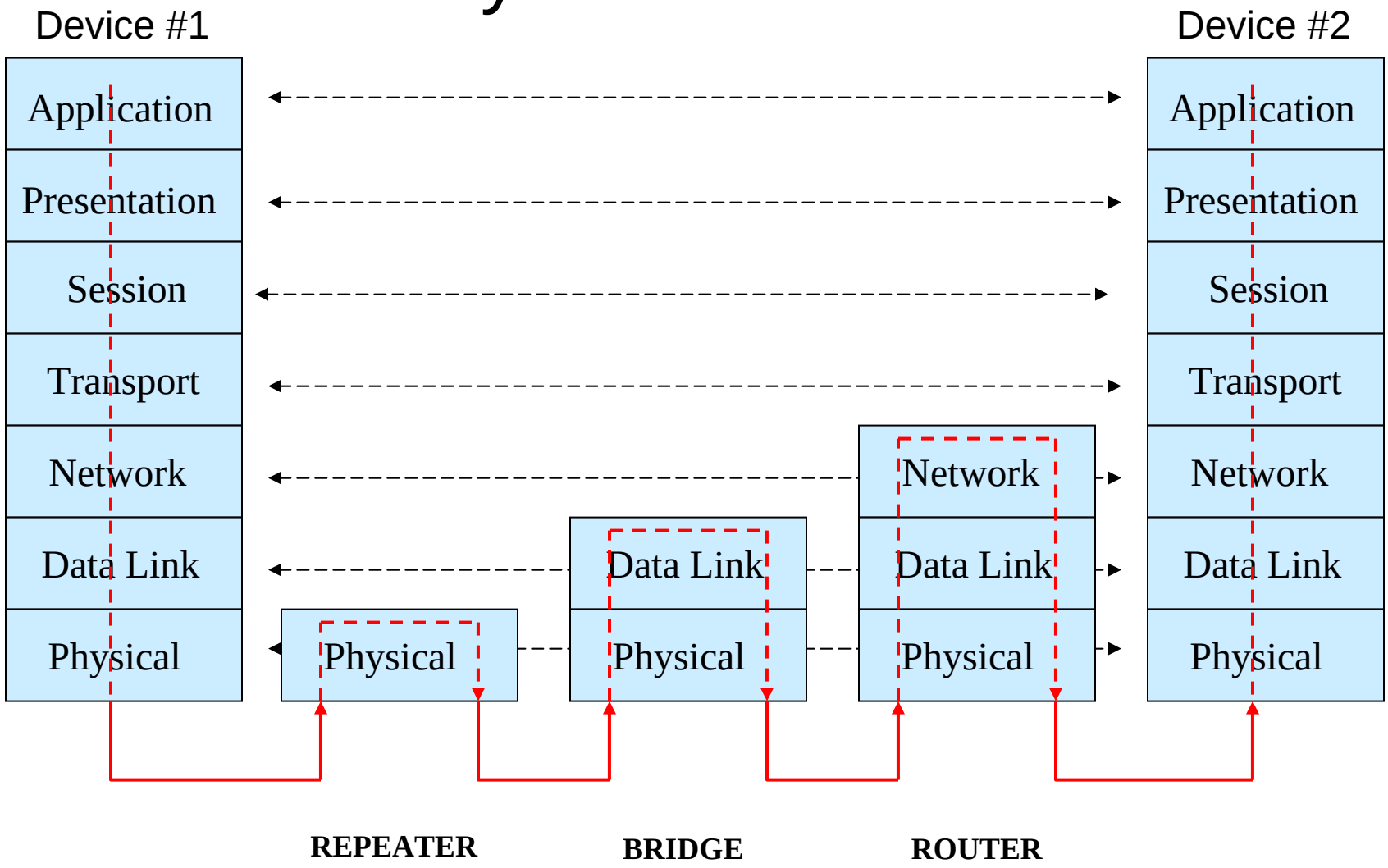
- ANSI X3.28
- BBC 7200
- CDC Types 1 and 2
- Conitel 2020/2000/3000
- DCP 1
- DNP 3.0
- Gedac 7020
- IBM 3707
- Landis & Gyr 8979
- Pert
- PG&E
- QEI Micro II
- Redac 70H
- Rockwell
- SES 91
- Tejas 3 and 5
- TRW 9550
- Vancomm

Protocol Background

International Standards Organization Open System Interconnection Reference Model
ISO OSI Reference Model (protocol stack)

7 Application	Provides interface to application services
6 Presentation	Data representation
5 Session	Starts, maintains, and ends each logical session
4 Transport	End-to-end reliable communications stream
3 Network	Routing and segmentation/reassembly of packets
2 Data Link	Transmit chunks of information across a link
1 Physical	Transmit unstructured bits across a link

Data Transmission Associated with the 7-Layer Protocol Stack



Simplified Protocol Stack

International Electrotechnical Commission (IEC)
Enhanced Performance Architecture (EPA)

3 Application	Provides interface to application services
2 Data Link	Routing and segmentation/reassembly of packets
1 Physical	Transmit bits of information across a link

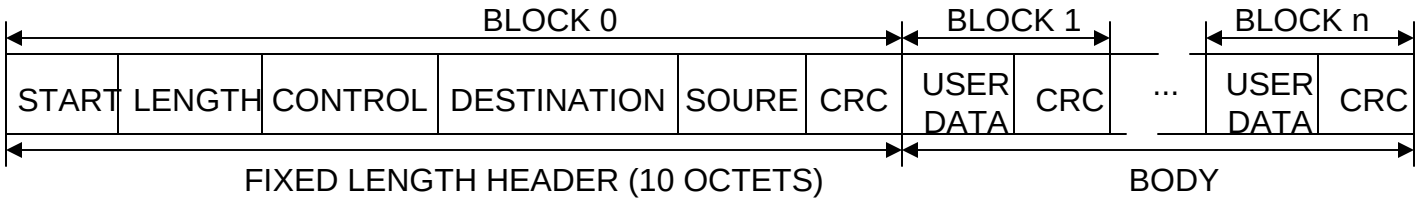
SCADA Protocol Example

- Distributed Network Protocol (DNP) 3.0
- SCADA/EMS applications
  - RTU to IED communications
  - Master to remote communications
  - Peer-to-peer instances and network applications
- Object-based application layer protocol
- Emerging open architecture standard

Distributed Network Protocol (DNP) 3.0 Data Link Layer

- Interface with the physical layer
  - Packing data into the defined frame format and transmitting the data to the physical layer
  - Unpacking frames received from physical layer
  - Controlling all aspects of the physical layer
- Data validity and integrity
  - Collision avoidance/detection
  - Perform message retries
- Establish connection, disconnection in dial-up environment

DNP 3.0 Data Link Layer

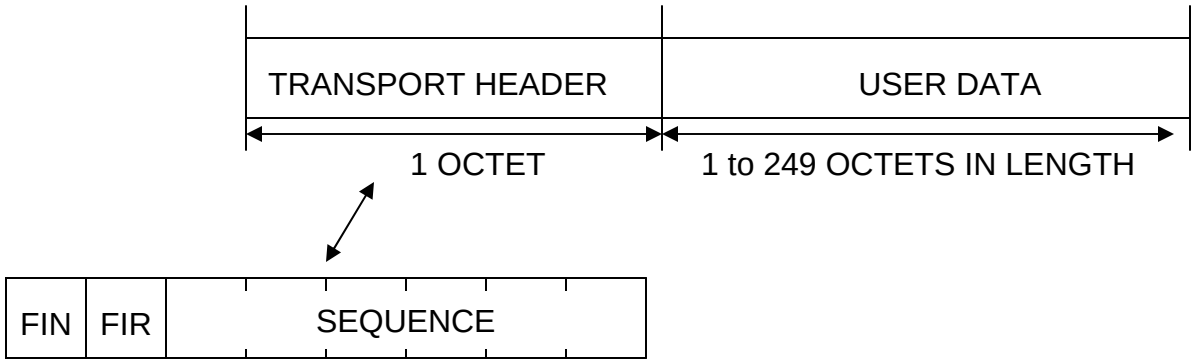


START	2 starting octets of the header
LENGTH	1 octet count of USER DATA in the header and body
CONTROL	1 octet Frame Control
DESTINATION	2 octet destination address
SOURCE	2 octet source address
CRC	2 octet Cyclic Redundancy Check
USER DATA	Each block following the header has 16 octets of User defined data

DNP 3.0 Transport Function

- Supports advanced RTU functions and messages larger than the maximum frame length in the data link layer
- Additional data integrity verification
- Packs user data into multiple frames of the data link frame format for transmitting the data
- Unpacks multiple frames that are received from the data link layer
- Controls data link layer

DNP 3.0 Transport Function



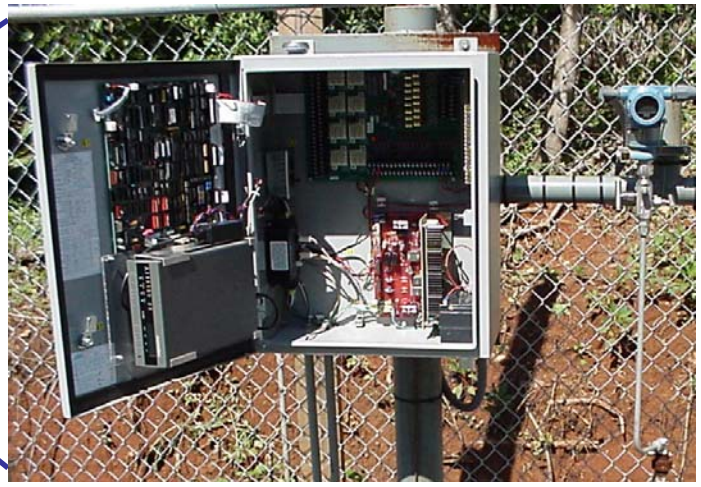
FIN	0 = More frames follow
	1 = Final frame of a sequence
FIR	1 = First frame of a sequence
	0 = Not the first frame of a sequence
SEQUENCE	Number between 0 and 63 to ensure frames are being received in sequence

DNP 3.0 Application Layer

- Communications Interface with Application Software
- Designed for SCADA and Distributed Automation Systems
- Supported functions include
  - send request
  - accept response
  - confirmation, time-outs, error recovery, etc.

Natural Gas Example

(i.e., SCADA is used in many other industries)



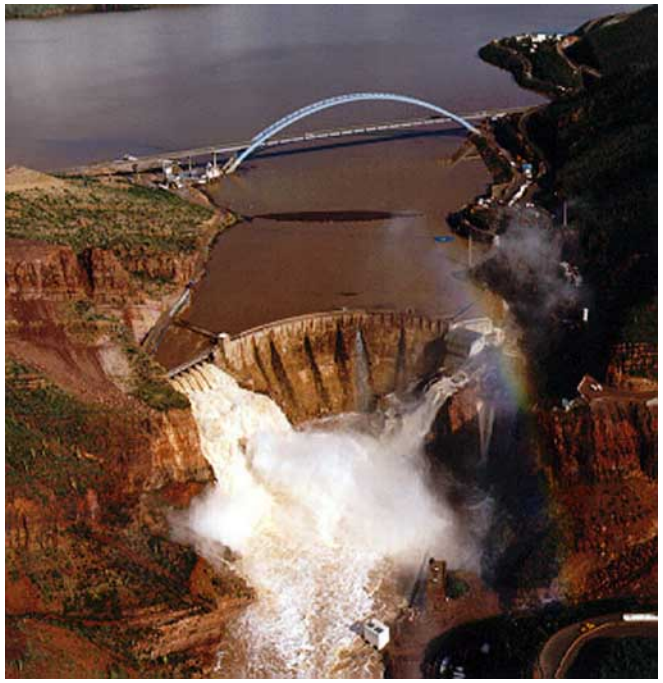
Remote Terminal Unit (RTU)

SCADA Security Case Studies

Jeff Dagle, PE
Pacific Northwest National Laboratory
Grainger Lecture Series for the
University of Illinois at Urbana-Champaign
September 15, 2005

Roosevelt Dam

- As reported by the Washington Post June 27, 2002:
- Bureau of Reclamation facility in Arizona
- SCADA system controlling dam floodgates accessed by a 12-year old hacker in 1998
- Hacker had “complete command of the SCADA system controlling the dam’s massive floodgates”
- Motivation: “exploring on a lark”



What really happened…

- The SCADA system at Roosevelt Dam is used to manage only Salt River Project's (SRP) canal system, not the floodgates at the dam.
- The hacking incident actually occurred in 1994 involving an 18 year-old.
- The hacker gained entry through a modem connected to a backup computer via a low level account, but security at the application and database level prevented the hacker from controlling any structures on the canal system.
- At no time was the hacker in a position to compromise the operation or safety of the SRP canal system.
- SRP participated with law enforcement agencies to catch the hacker.
- Law enforcement monitored phone lines while SRP installed equipment to monitor every keystroke that the hacker made. SRP went to the extent of setting up a separate fake network solely connected to the one phone line being used by the hacker. After several weeks of monitoring, the phone line was shut down, computers were rebuilt, and additional security measures were implemented.
- The evidence SRP acquired led to the arrest and conviction of the hacker.

Queensland, Australia

- April 23, 2000: Vitek Boden, 48, caught with stolen computer, radio transmitter. During his 46th successful intrusion….
- Until then, utility managers didn't know why the system was leaking hundreds of thousands of gallons of sewage into parks, rivers, and the Hyatt Regency hotel grounds.
- Attack method: software on his laptop identified itself as "pumping station 4". He then suppressed alarms, and became the "central control system" with unlimited command of 300 SCADA nodes.
- Disgruntled former employee convicted and sentenced to two years in prison.

Bellingham, Washington

- June 10, 1999: 237,000 gallons of gasoline leak from 16” pipeline, ignited 1.5 hours later. Three deaths, 8 injuries, extensive property damage.
- “Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation.”
- Warning issued to other pipeline operators by the Office of Pipeline Safety July 1999
- NTSB report issued October 2002 Key recommendation:
  - Utilize an off-line development system for implementing and testing changes to the SCADA database
- Olympic Pipe Line Co. filed for Chapter 11 Bankruptcy March 27, 2003

Computer Failures that Occurred in the Electric Power Industry August 14, 2003

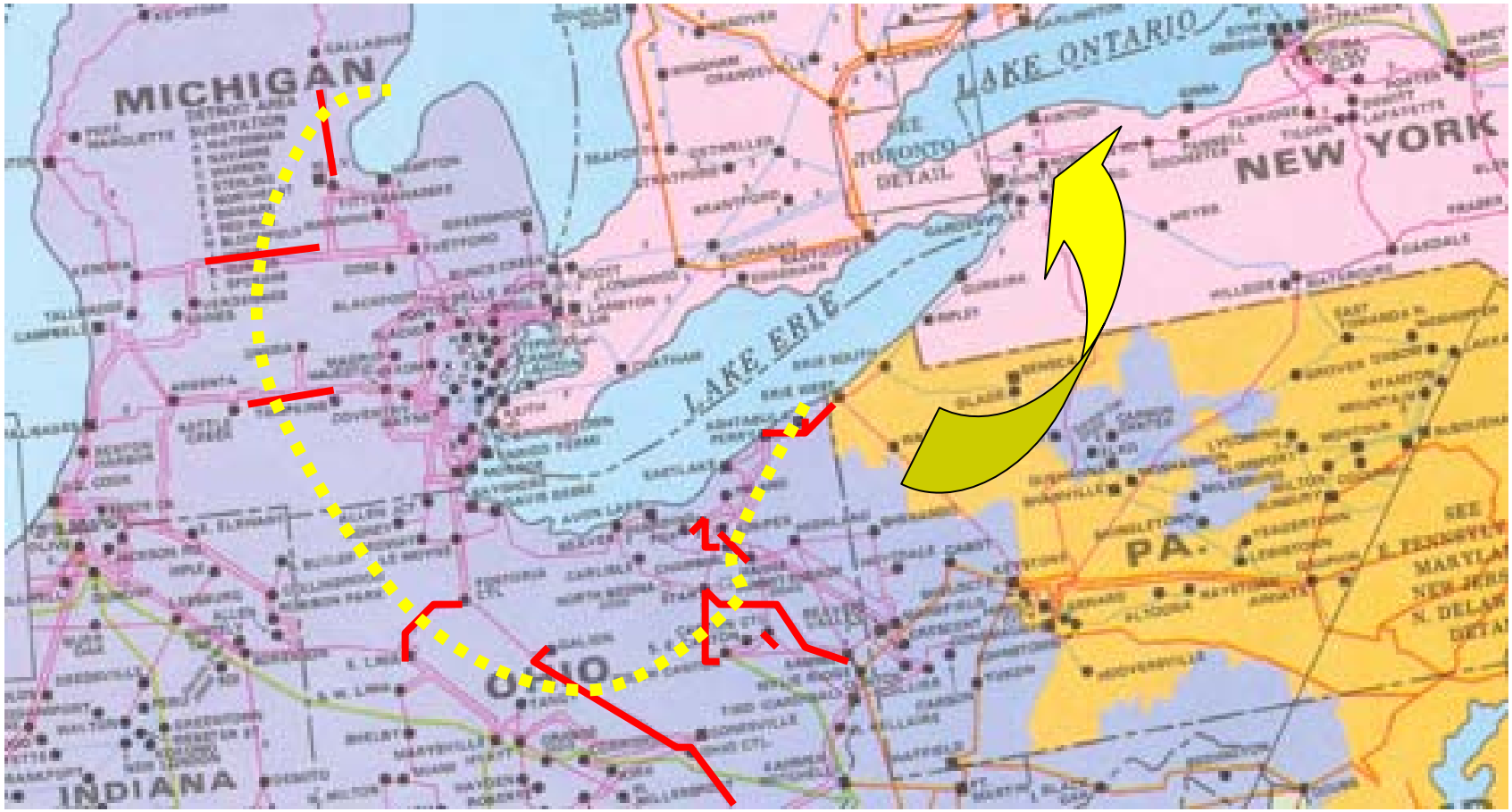
- First Energy
  - 2:14 pm alarm function fails
    - No audible or visual indications of failures are presented to power system operators
  - While technicians were working the problem, control room operators were not fully aware of the failures
  - By 2:54 pm, other failures of the energy management system caused both primary and backup servers to stop functioning
  - “Warm reboot” completed at 3:08 pm, technicians believed that they corrected the problem
    - Alarm processor still in failed condition
- Midwest Independent System Operator
  - Problems with the state estimator started at 12:15 pm, and were not fully resolved until 4:04 pm
    - This prevented the regional reliability coordinator from performing adequate contingency analyses

Major North American Blackouts

Date	Location	Load Interrupted
November 9, 1965	Northeast	20,000 MW
July 13, 1977	New York	6,000 MW
December 22, 1982	West Coast	12,350 MW
January 17, 1994	California	7,500 MW
December 14, 1994	Wyoming, Idaho	9,336 MW
July 2, 1996	Wyoming, Idaho	11,743 MW
August 10, 1996	Western Interconnection	30,489 MW
June 25, 1998	Midwest	950 MW
August 14, 2003	Northeast	61,800 MW

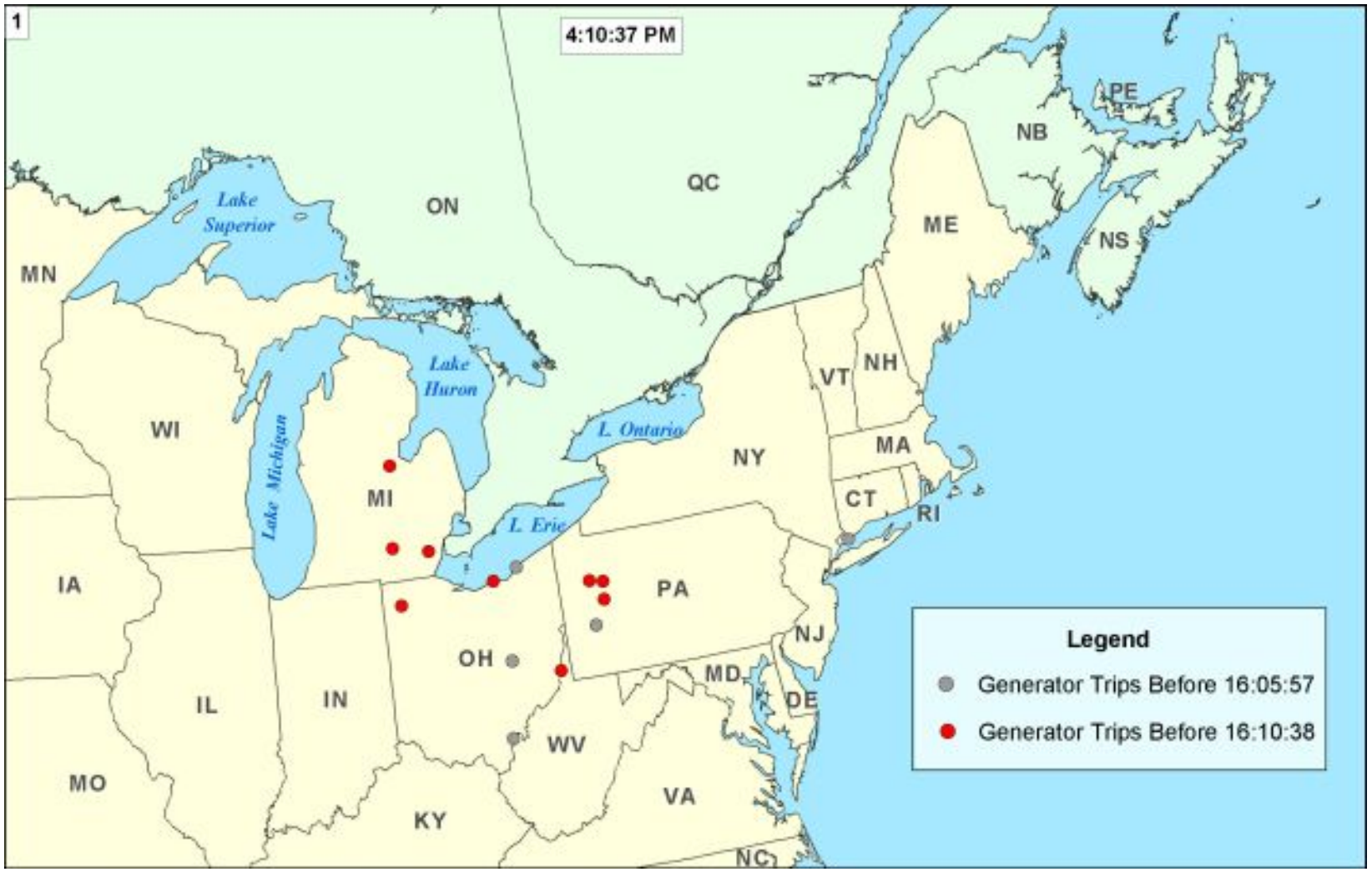
From 3:05 to 4:05 pm, several key 345kV transmission lines in Northern Ohio trip due to contact with trees in their right of way. This eventually initiates a cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid.

By 4:10 pm Northern Ohio & eastern Michigan are collapsing, many units have tripped, only connection remaining is with Ontario.

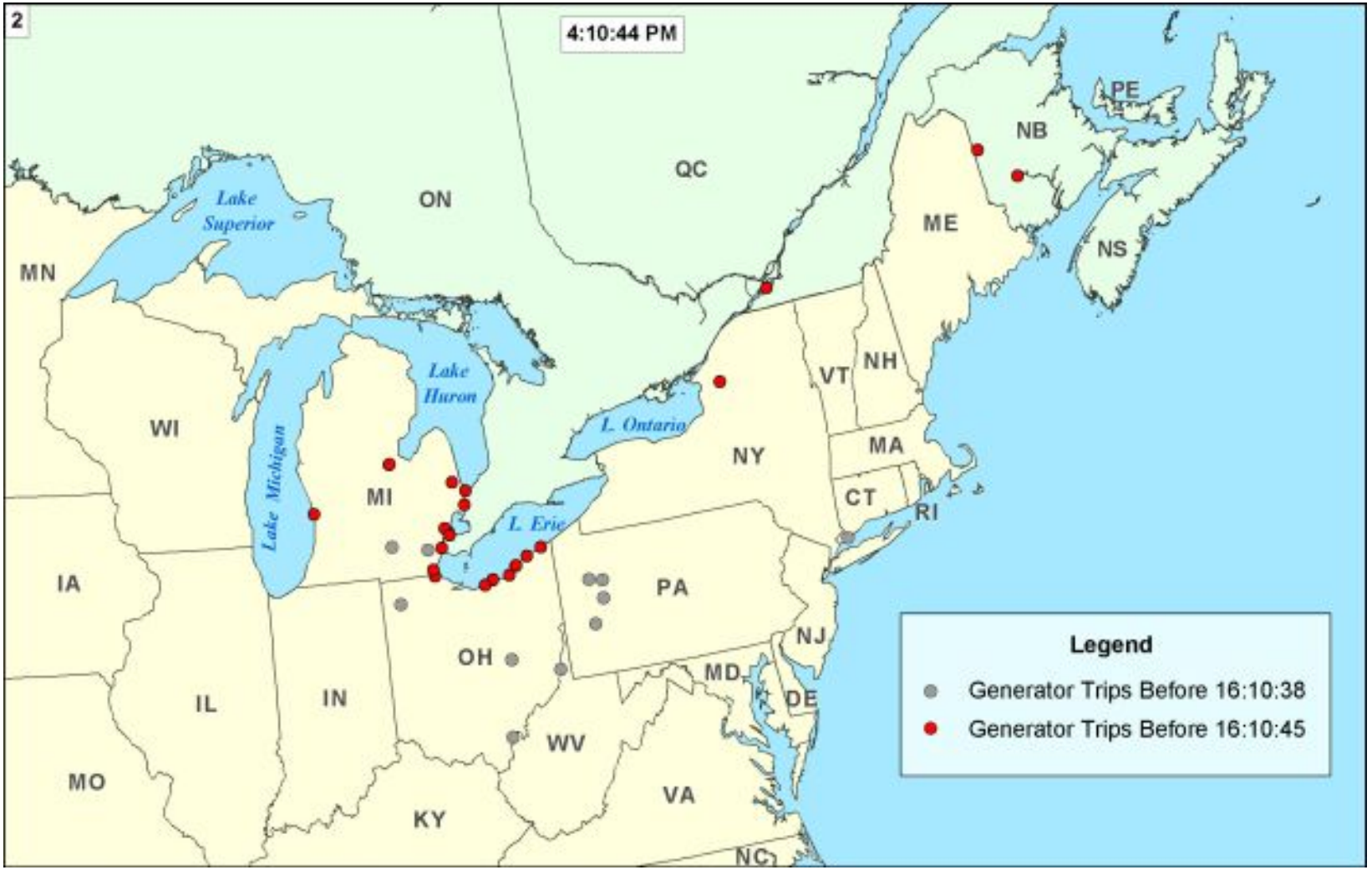


7 seconds later, the Northeast portion of the interconnected power system separates, which then breaks into multiple islands. 61,800 MW load is lost as 508 generating units at 265 power plants trip.

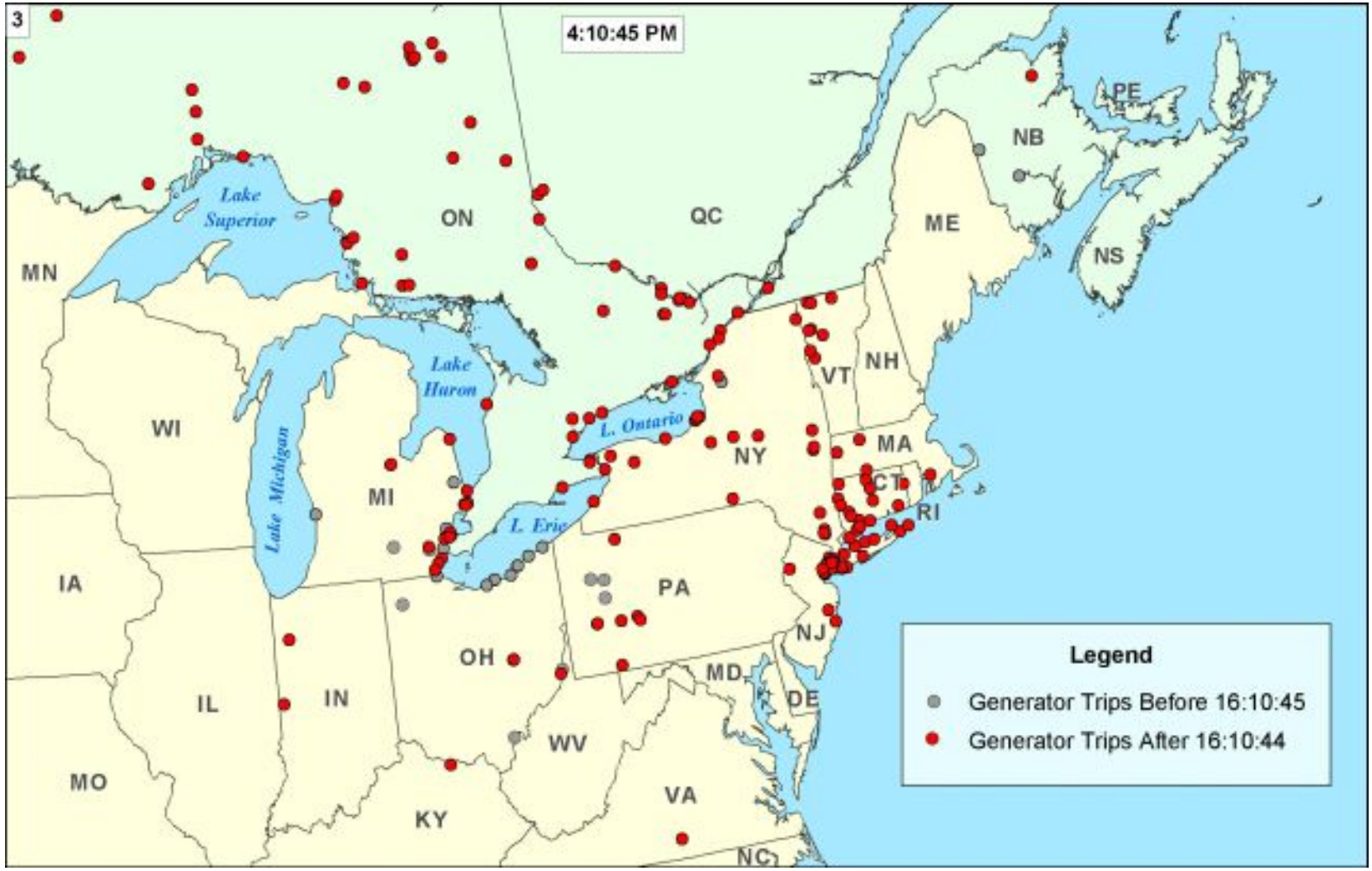
Generator Trips to 4:10:38pm



Generator Trips – Next 7 Seconds



Generator Trips – After 4:10:44pm

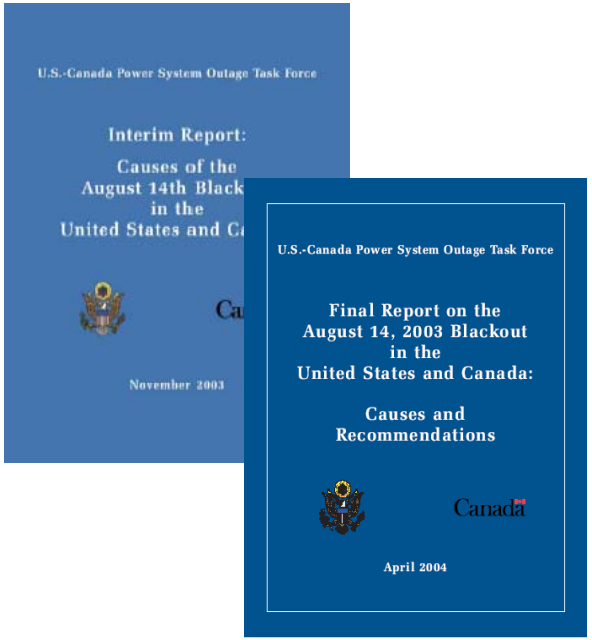


Investigation Process

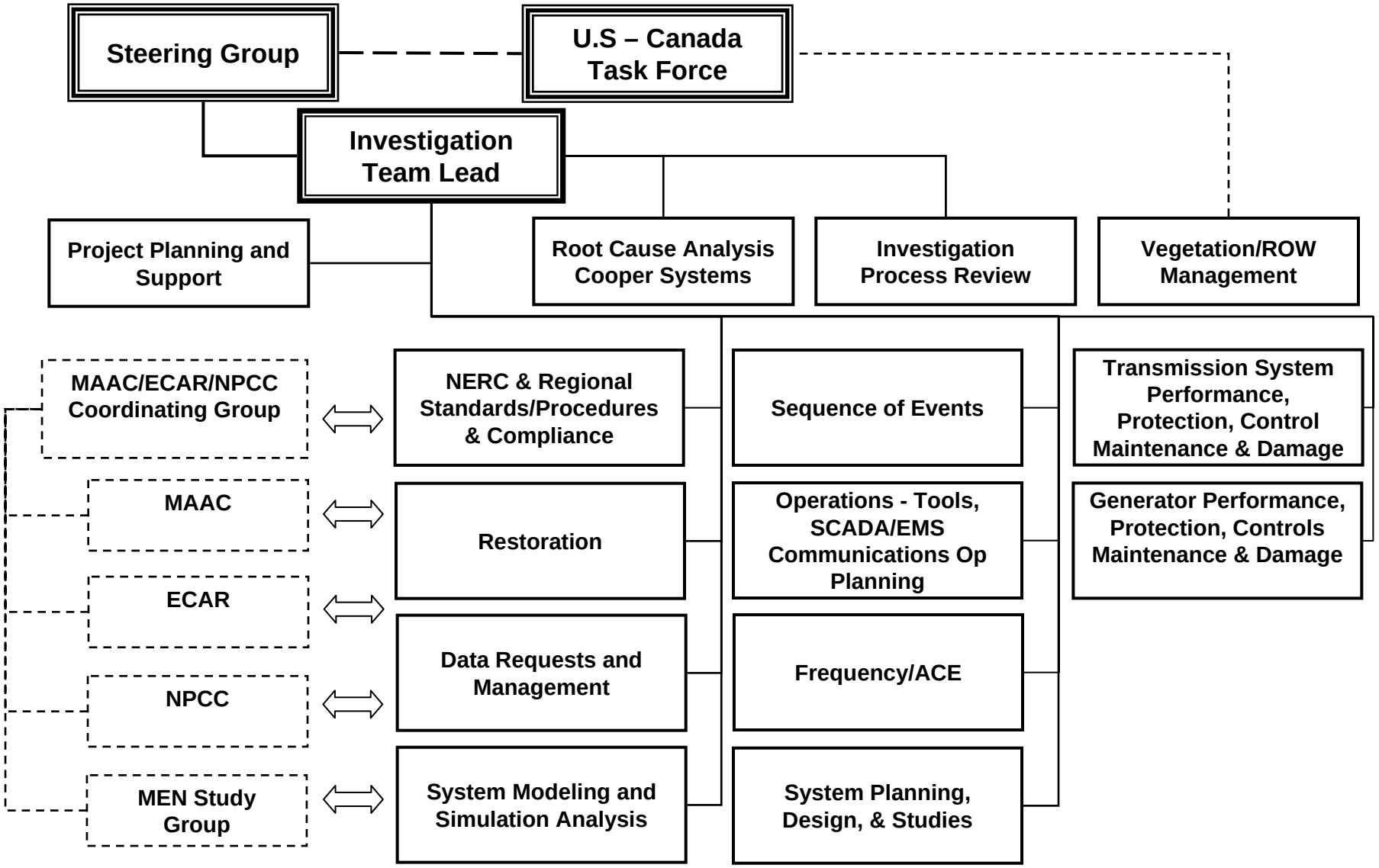
Joint U.S. - Canada Power System Outage Task Force

Electric System Working Group	Nuclear Working Group	Security Working Group
Investigate the cascading electrical failure.	**Review performance of plants and assess possibility of damage.**	**Determine if failures were caused with malicious intent.**

- Phase I
  - Investigate the outage to determine its causes and why it was not contained
  - Interim report released 11/19/03
- Phase II
  - Develop recommendations to reduce the possibility of future outages and minimize the scope of any that occur
  - Final report released 4/5/04
  - Report available at: http://electricity.doe.gov (Blackout link)



Electric System Working Group



Initial Data Request Letters

- Issued the week after the blackout
- Disseminated broadly to the reliability coordinators in the affected area
- Information requested included:
  - SCADA alarm logs, and SCADA data at the highest available sample rate
  - Data from digital fault recorders and other equipment in substations
  - Circuit breaker settings and targets (transmission lines, generators)
  - State estimator snapshots and saved contingency cases
  - Operator logs and transcripts
  - Load shedding (automatic or manual)
  - Voltage control equipment, special protection schemes, etc.

Follow-up Data Request Letters

- Targeted to specific organizations
- Topics driven by the investigation team requirements
  - System studies (voltage support, transfer capabilities)
  - Standards and compliance team
  - System planning, design, and studies team
  - Root cause team
  - Generation performance team
  - Other specific questions directed to utilities based upon the investigation team requirements

Building the Sequence of Events

- SCADA/EMS alarm logs
  - Inaccurate timing due to communication latency, time skew, buffering issues
- Substation instrumentation
  - Digital fault recorders, digital protective relays, synchronized phasor measurement units
  - Some instrument clocks were not synchronized to an established time standard
  - Data format issues

Creating a Data Warehouse

- Established at NERC
  - Dedicated server on a segmented network
  - Accessible by all members of the blackout investigation team
  - VPN access enabled for off-site members of the investigation team
- Stored data received from the utilities
  - Read-only access to the investigation team
  - Over 20 GB of information, 10,000+ files
  - Wide variety (documents, spreadsheets, special data formats, audio, …)
  - Received via email, FTP, mail (CDs and hardcopy reports)
- Working data, draft report materials, etc.
  - Read access to investigation team, write-access specified by team leaders
- Data entry and tracking procedures
- SQL-server data base developed to provide inventory and querying capabilities
  - Challenge: Database developed in parallel with the investigation process

The Blackout of August 14, 2003 Root causes associated with SCADA

- Failure of the alarm processor in First Energy's SCADA system prevented operators from having adequate ***situational awareness*** of critical operational changes to the electrical grid
- Effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes
  - Prevented contingency analysis

Suddenly, knowing a lot about the U.S. power grid became sexy at cocktail parties.

SCADA Security: Threats, Vulnerabilities and Consequences

Jeff Dagle, PE
Pacific Northwest National Laboratory
Grainger Lecture Series for the
University of Illinois at Urbana-Champaign
September 15, 2005

Vulnerability Assessment Background

- DOE Program Initiated in 1997
- Voluntary Assessments
  - Includes cyber and physical security
- Post-September 11 Activities
  - "Top 50" Energy Assets Identified (subsequently grew to 100+ assets)
  - Quick assessment surveys initiated on priority ranking, encompassing a range of assessment options
- Outreach Activities
  - Industry engagement (NERC, EPRI, etc.)
  - Federal agency liaison (NIST, NSA, etc.)

Energy Infrastructures

Electric power

Oil

Natural Gas

The threat is real!

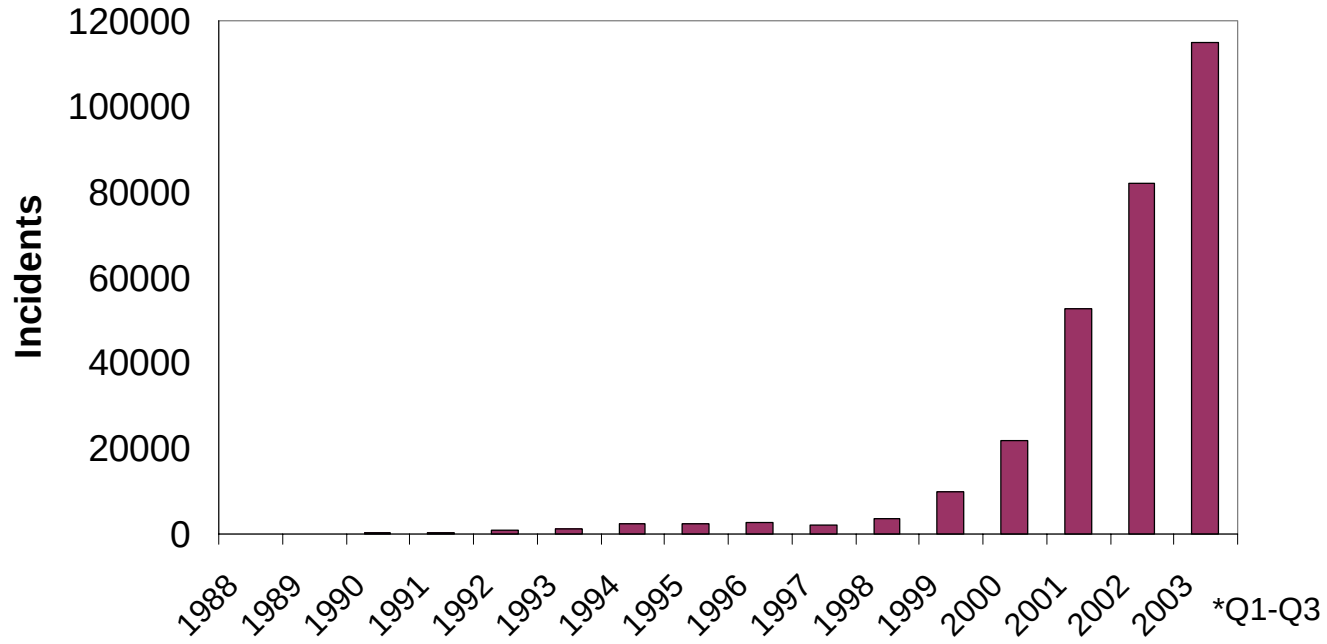
- **Unstructured adversaries**
  - **Cracker, hacker, script-kiddie**
  - **Competitors**
  - **Criminals**
- **Structured adversaries**
  - **Terrorists, hactivists**
  - **Organized crime**
  - **Foreign nations**
- **Insiders**
  - **Witting**
  - **Unwitting**
  - **Half-witting**

Anecdotes

- **2003 CSI/FBI Computer Crime and Security Survey**
  - Overall financial losses from 530 survey respondents totaled $201,797,340. This is down significantly from 503 respondents reporting $455,848,000 last year. (75 percent of organizations acknowledged financial loss, though only 47% could quantify them.)
  - The overall number of significant incidents remained roughly the same as last year, despite the drop in financial losses.
  - Losses reported for financial fraud were drastically lower, at $9,171,400. This compares to nearly $116 million reported last year.
  - As in prior years, theft of proprietary information caused the greatest financial loss ($70,195,900 was lost, with the average reported loss being approximately $2.7 million).
  - In a shift from previous years, the second-most expensive computer crime among survey respondents was denial of service, with a cost of $65,643,300--up 250 percent from last year's losses of $18,370,500.

Anecdotes *(Cont'd)*

- Carnegie-Mellon CERT

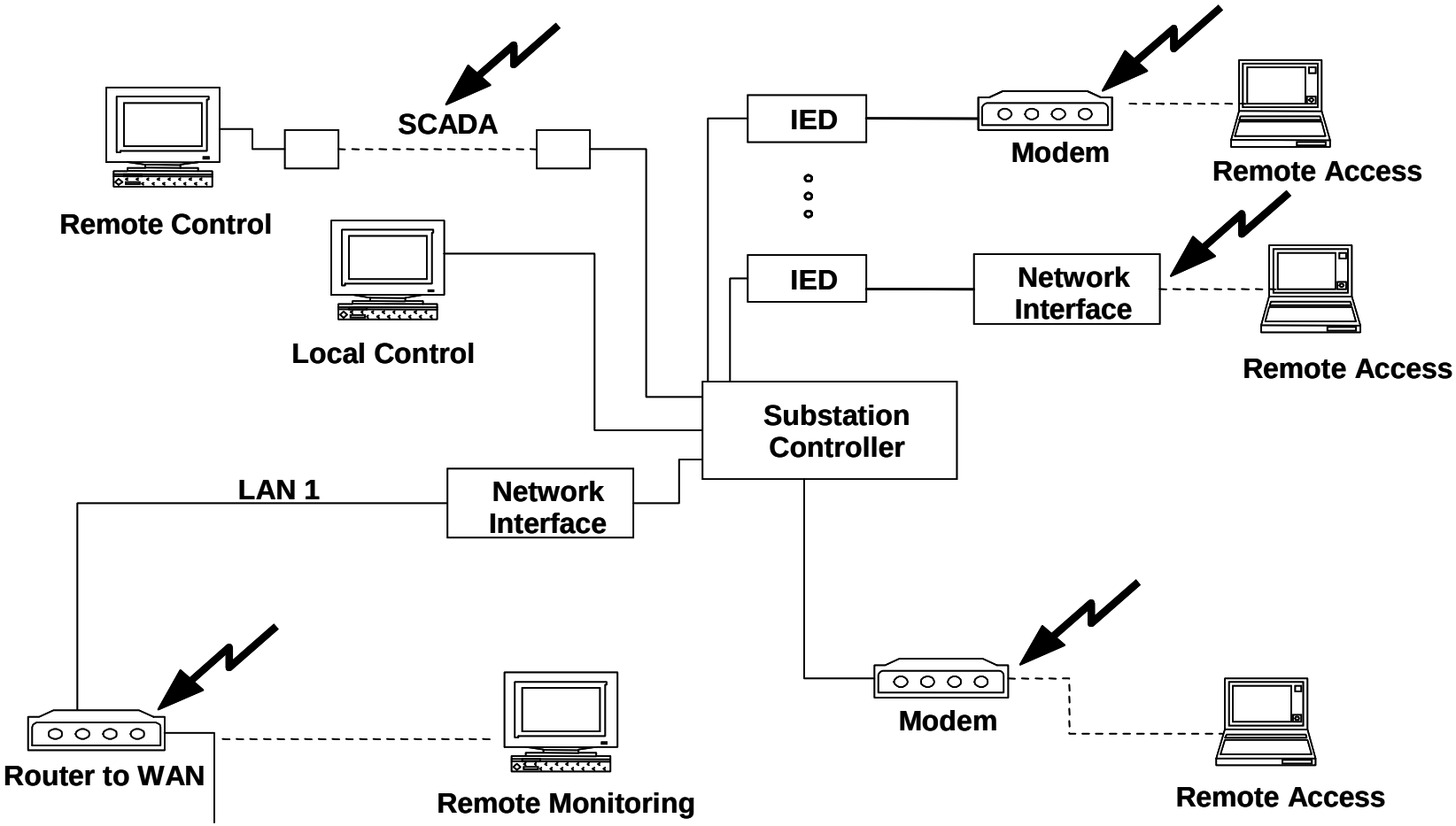


- <u>One</u> utility reported over 100,000 scans/month

Vulnerability Concerns

- **Confidentiality**
  - **Protecting information from unauthorized access**
  - **Important for deregulation, competitive intelligence**
- **Integrity**
  - **Assuring valid data and control actions**
  - **Most critical for real-time control applications**
- **Availability**
  - **Continuity of operations**
  - **Important for real-time control applications**
  - **Historically addressed with redundancy**

Vulnerable Points



Graphic courtesy of Paul Oman, Schweitzer Engineering Laboratories, Pullman Washington

Sources of Vulnerabilities

- **Exploits at the application, platform, or network level**
- **Remote *trusted* access by**
  - **Other enterprise elements (e.g., front office, support functions, etc.)**
  - **Vendors, customers, business partners**
  - **Security coordinators, neighboring control areas, etc.**
- **Unencrypted communications, lack of authentication**
- **Improper privilege escalation**
  - **Password cracking**
  - **Insider threat**
- **Lack of physical access control**
  - **Critical facilities**
  - **Remote locations (e.g., substations, communication facilities)**

Vulnerability Trends

- **Much more interconnectivity**
  - **Internal and external networks merging**
  - **Functional, organization interconnection**
- **Increased reliance on information systems**
  - **Information becoming inseparable from the core business**
- **Increased standardization**
  - **Open protocols, common operating systems and platforms**
- **Industry in transition**
  - **Deregulation, mergers, new systems and procedures**
  - **Driven to “do more with less”**

Other Vulnerability Challenges

- Configuration management is not practiced beyond systems directly affecting physical operations
- Interconnectivity and interdependencies not widely understood
  - Boundaries of systems and authorities (particularly information systems) are becoming blurred
  - Level of trust granted is frequently unwarranted
  - Partitioning logical systems to control access and limit influence is not widely practiced
  - No explicit vendor security validation
- Limited incident detection, reporting, recovery, and forensics capability

Other Vulnerability Challenges (cont)

- **Tenuous balance between public information and security needs**
  - **FERC disclosure requirements (market sensitive information)**
  - **Public franchise issues**
  - **Public-access web sites**
- **Generally vulnerabilities are greater in:**
  - **Small organizations**
  - **Organizations experiencing major culture or mission changes**
- **Need to cultivate security awareness and permeate throughout organization**
- **General observation – wide variation within industry**
  - **Need exists to adopt common protection “standards”**

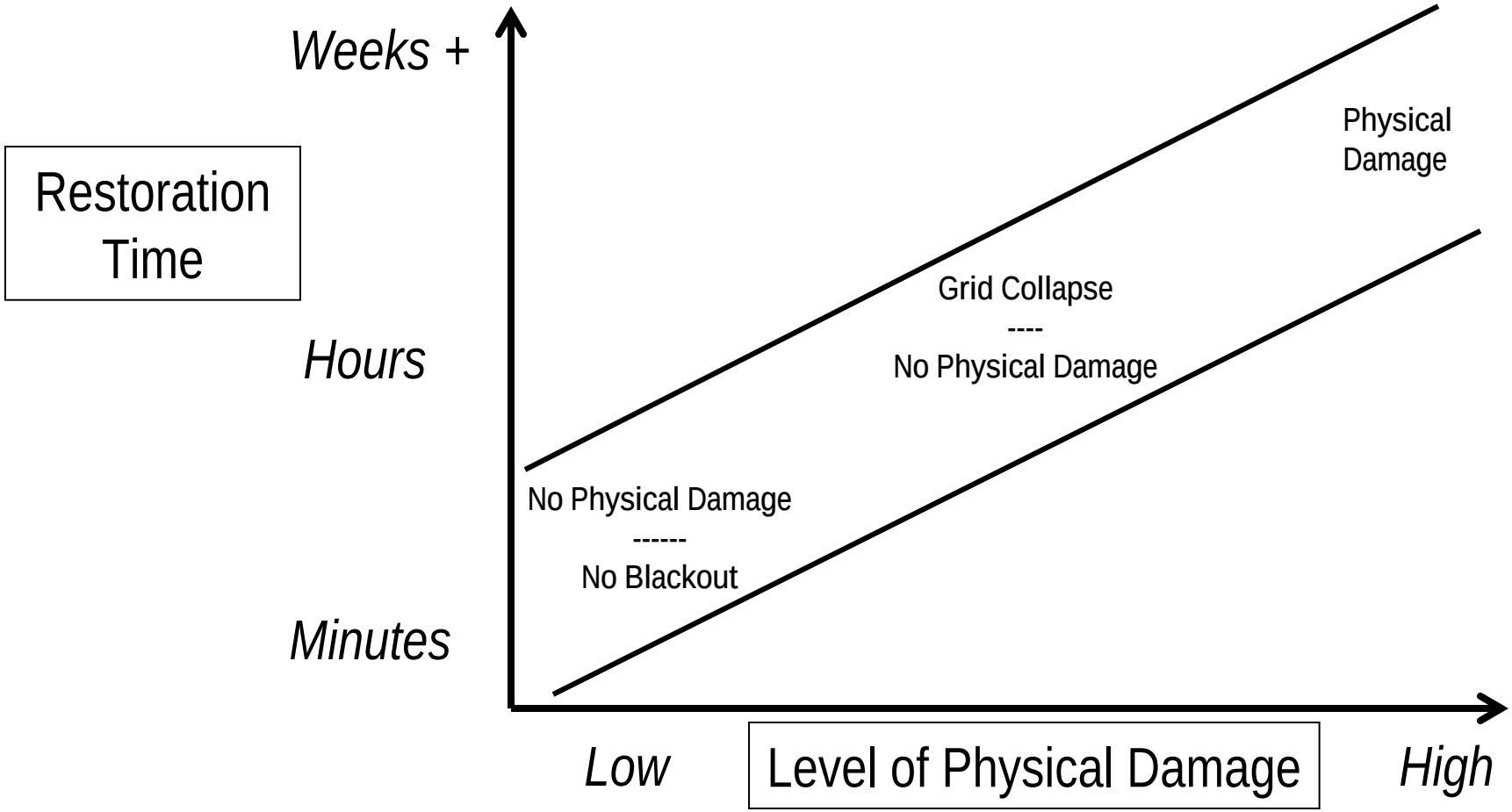
Typical Vulnerabilities Observed

- Ports and services open to outside
- Operating systems not “patched” with current releases
- Dial-up modems
- Improperly configured equipment (firewall does not guarantee protection)
- Improperly installed/configured software (e.g., default passwords)
- Inadequate physical protection
- Vulnerabilities related to “systems of systems” (component integration)

We Just Lost SCADA… So What?

- Failures within SCADA may not cause any problems on the power system
  - Impact may be limited to loss of visibility into infrastructure operations
- Redundant systems may compensate for SCADA system failures
- Consequences are a function of
  - Expected SCADA system restoration time
  - When the failure occurs (impact to power schedules)
  - System stress at time of failure
  - Whether or not redundant controls exist

Effects vs. Restoration Time



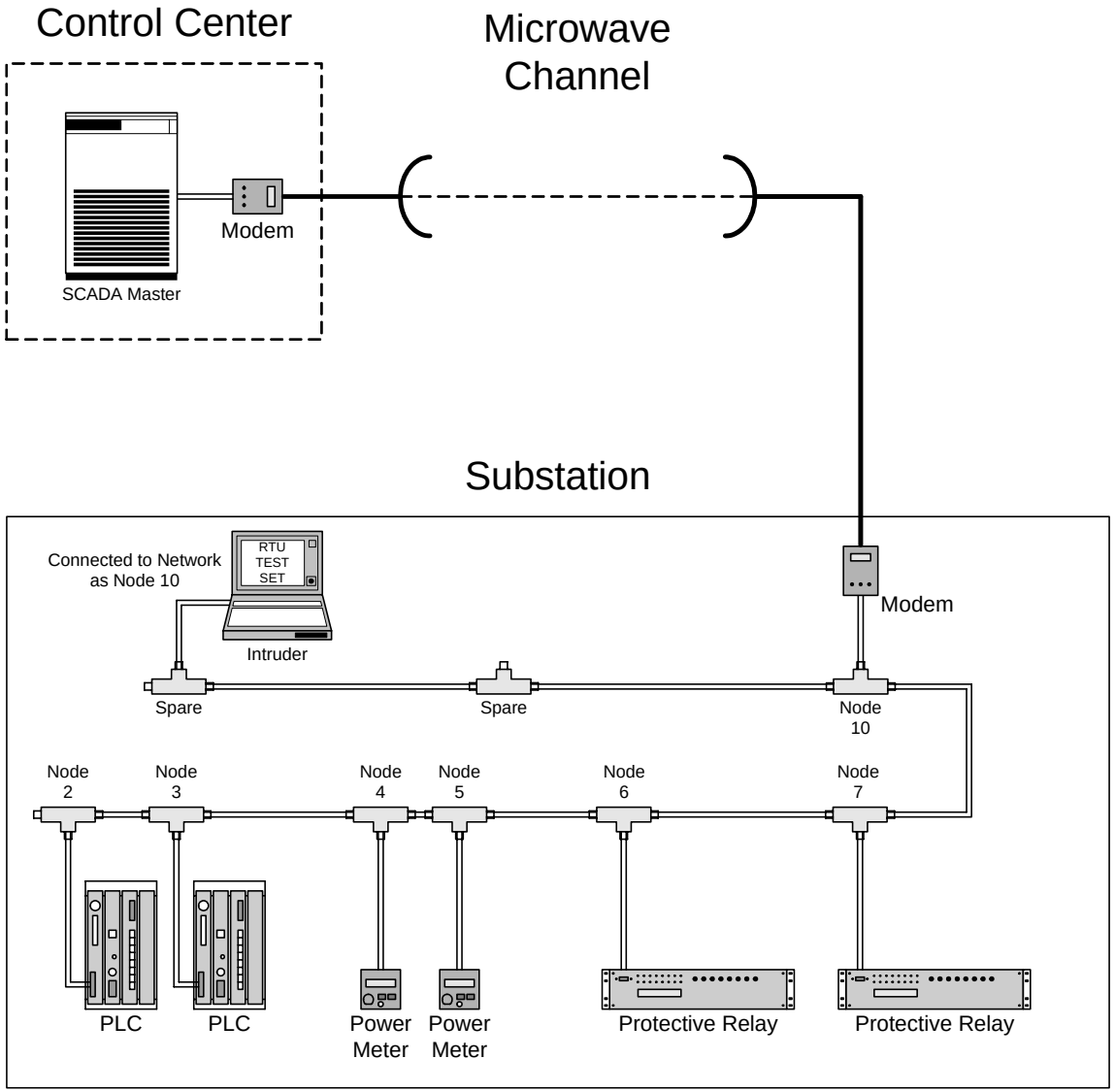
Scenario 1: Gaming the Power System

- Undercover ‘employees’ planted at various firms that market wholesale power.
- Create a targeting list for deciding which cyber systems to compromise.
- Compromise these systems through either “sniffer” software or with manual downloads.
- Profit by using this illegally gained information in power system market trading.
- Consequences
  - Unfair profiting
  - Erosion of investor confidence
  - Disruption of capital investments
  - Inadequate supply and bottlenecks within the power grid

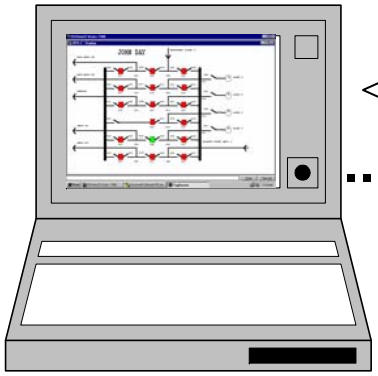
Scenario 2: Denial of Service

- In most SCADA/EMS systems, there is a gateway connecting the SCADA/EMS host with the corporate network.
- While the gateway includes access control lists and firewalls to prevent unauthorized access to the SCADA/EMS subnetwork, it has open ports that allow ping requests to pass through.
- A “ping of death” attack shuts down the SCADA/EMS host and backup systems.
- If an adversary simultaneously compromises multiple control area systems, the impact could exceed the utilities’ capabilities to respond to changing system conditions, and a cascading grid failure could occur.

Scenario 3: Exploiting Open Protocols



SCADA R&D at PNNL
Bench-Scale Vulnerability Demonstrations



SCADA Protocol (DNP 3.0)

Operator Interface

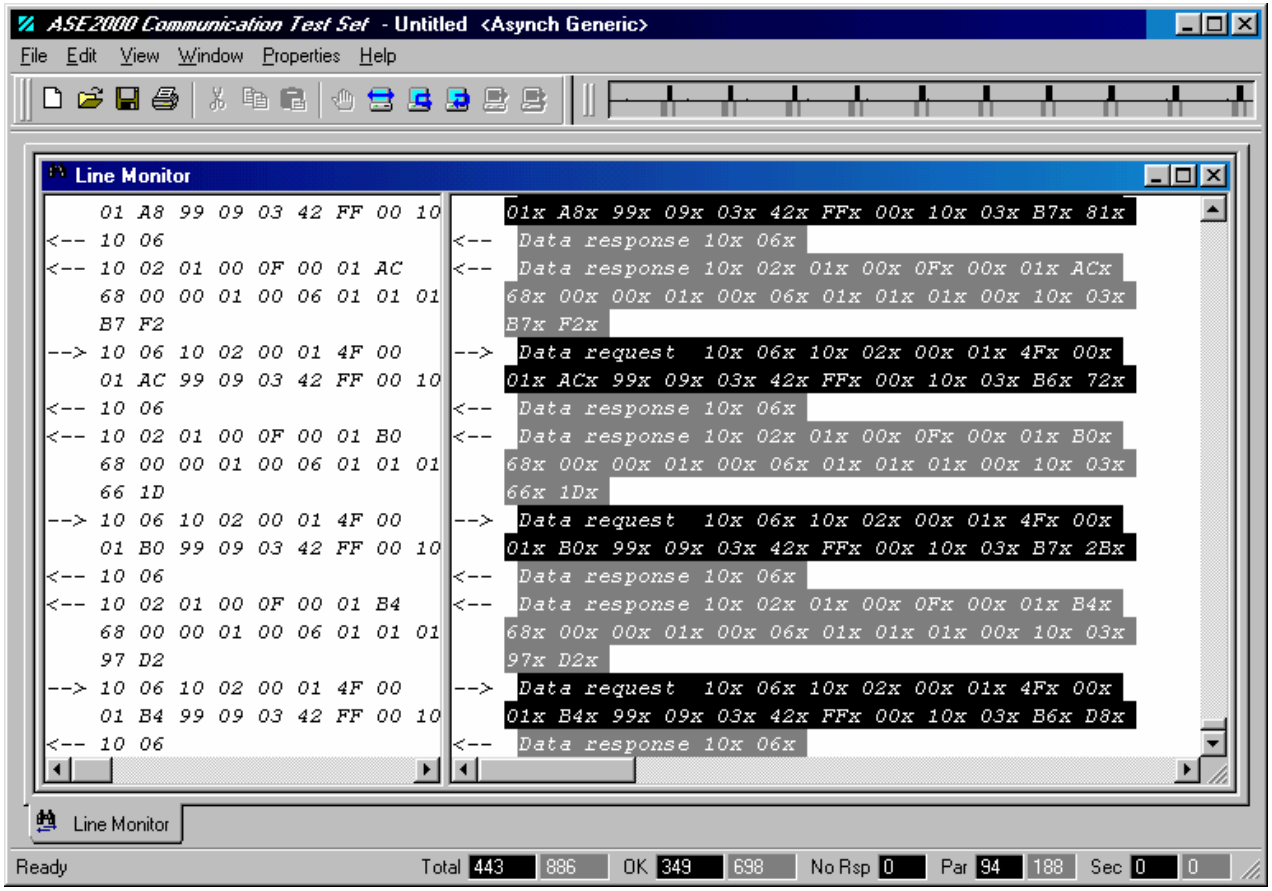
Protocol Analyzer
(Intruder)

Field Device
- Remote Terminal Unit (RTU)
- Intelligent Electronic Device (IED)
- Programmable Logic Controller (PLC)

Scenarios
- Denial of service
- Operator spoofing
- Direct manipulation of field devices
- Combinations of above

Vulnerability implications vary significantly depending on the scenario and application

SCADA Message Strings



Repeating easily decipherable format

Captured by the ASE Protocol Analyzer

Wireless SCADA Access at Substations

- Security firm Rainbow Mykotronx in Torrance, Calif., assessed a large southwestern utility that serves about four million customers.
- Evaluators drove to a remote substation. Without leaving their vehicle, they noticed a wireless network antenna. They plugged in their wireless LAN cards, fired up their notebook computers, and connected to the system within five minutes because it wasn't using passwords.
- Within 10 minutes, they had mapped every piece of equipment in the facility. Within 15 minutes, they mapped every piece of equipment in the operational control network. Within 20 minutes, they were talking to the business network and had pulled off several business reports. They never even left the vehicle.

Countermeasures to enhance security of SCADA systems

Jeff Dagle, PE
Pacific Northwest National Laboratory
Grainger Lecture Series for the
University of Illinois at Urbana-Champaign
September 15, 2005

Critical Infrastructure Protection

"Certain national infrastructures are so vital that their incapacitation or destruction would have a debilitating impact on the defense or economic security of the United States"

July 1996 - President's Commission on Critical Infrastructure Protection (PCCIP)

↓

October 1997 – *"Critical Foundations: Protecting America's Infrastructures"*

"Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future."

↓

May 1998 - Presidential Decision Directive 63: Policy on Critical Infrastructure Protection

↓

October 2001 - Executive Order 13231 "Critical Infrastructure Protection in the Information Age"

↓

November 2002 – Homeland Security Act of 2002: Formation of Dept Homeland Security

Presidential Homeland Security Documents

- National Strategy for Homeland Security
  - July 2002
- National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
  - February 2003
- The National Strategy to Secure Cyberspace
  - February 2003

Homeland Security Presidential Directives

- **HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection**

  This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

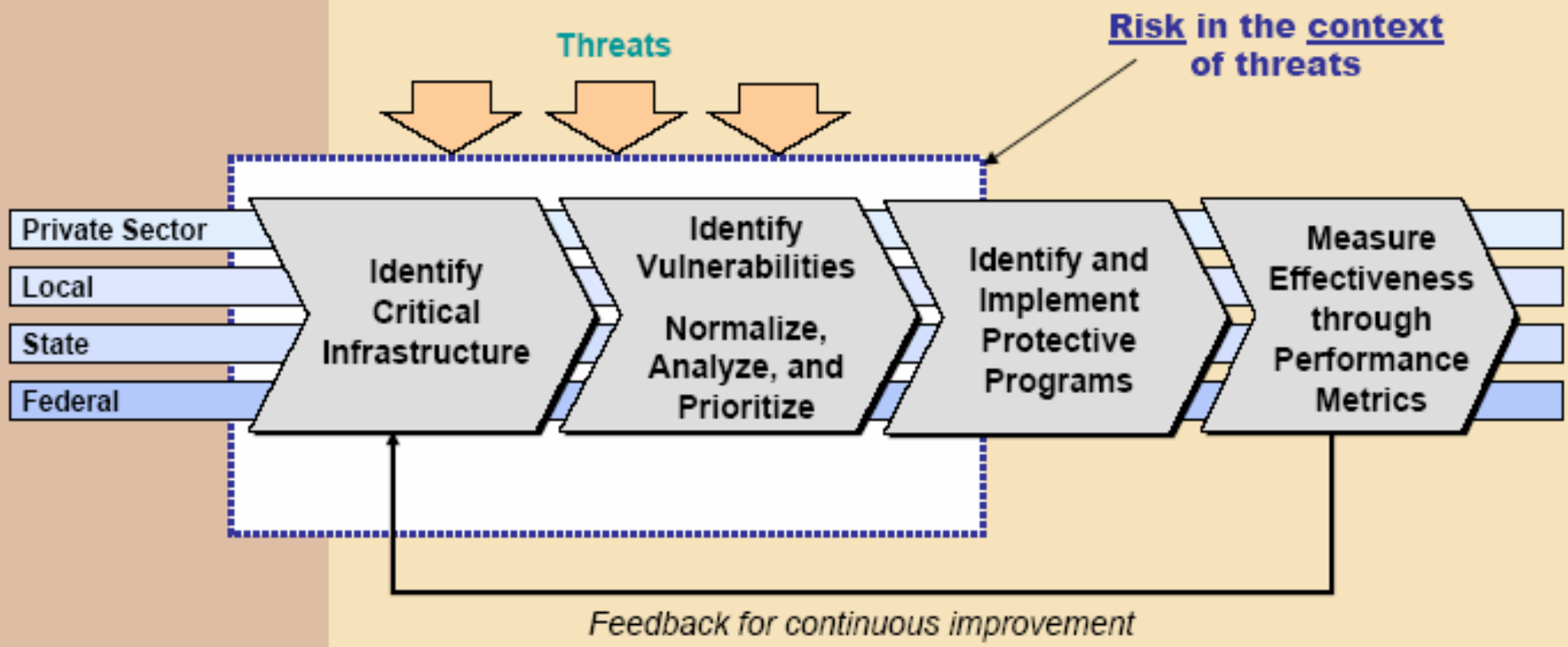
- **HSPD-8: National Preparedness**

  This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.

HSPD-7 Sector-Specific Agencies

Sector	Lead Agency
– Agriculture, Food	– Department of Agriculture
– Water	– Environmental Protection Agency
– Public Health	– Health and Human Services
– Energy	– Department of Energy
– Banking and Finance	– Department of Treasury
– National Monuments and Icons	– Department of Interior
– Defense Industrial Base	– Department of Defense

National Critical Infrastructure Protection Plan (NIPP)



This risk-based methodology drives all of our critical infrastructure protection activities at the sector and at the national level

Information Sharing and Analysis Center (ISAC)

- Link between government and private entities operating elements of critical infrastructures
- Operational ISACs
  - Chemical
  - Electricity
  - Emergency Management and Response
  - Energy (Oil and Gas)
  - Financial Services
  - Health Care
  - Highway
  - Information Technology
  - Multi-State
  - Public Transit
  - Research and Education Network
  - Surface Transportation
  - Telecommunications
  - Water

Electricity Sector ISAC (ESISAC)

- Share information about real and potential threats and vulnerabilities
  - Received from DHS and communicated to electricity sector participants
  - Received from electricity sector participants and communicated to DHS
- Analyze information for trends, cross-sector dependencies, specific targets
- Coordinate with other ISACs

Edit View Favorites Tools Help

Fri Sep 24, 2004

FAQ IAW Library Calendar Links Contact CIPC CIPIS login

NICC Contacts Bulletins/Advisories DHS Daily Reports

ESISAC

Electricity Sector Information Sharing and Analysis Center

Welcome. The ESISAC serves the Electricity Sector by facilitating communications between electric sector participants, federal government and other critical infrastructure industries. It is the job of the ESISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions.

CURRENT THREAT LEVELS (click on name for details)

Electricity Sector:	Physical	ELEVATED (yellow)
	Cyber	ELEVATED (yellow)
Department of Homeland Security		ELEVATED (yellow)
Department of Energy		SECON 3, modified with measures 33 and 38

Latest Threat Level change: January 09, 2004, 1410 EDT

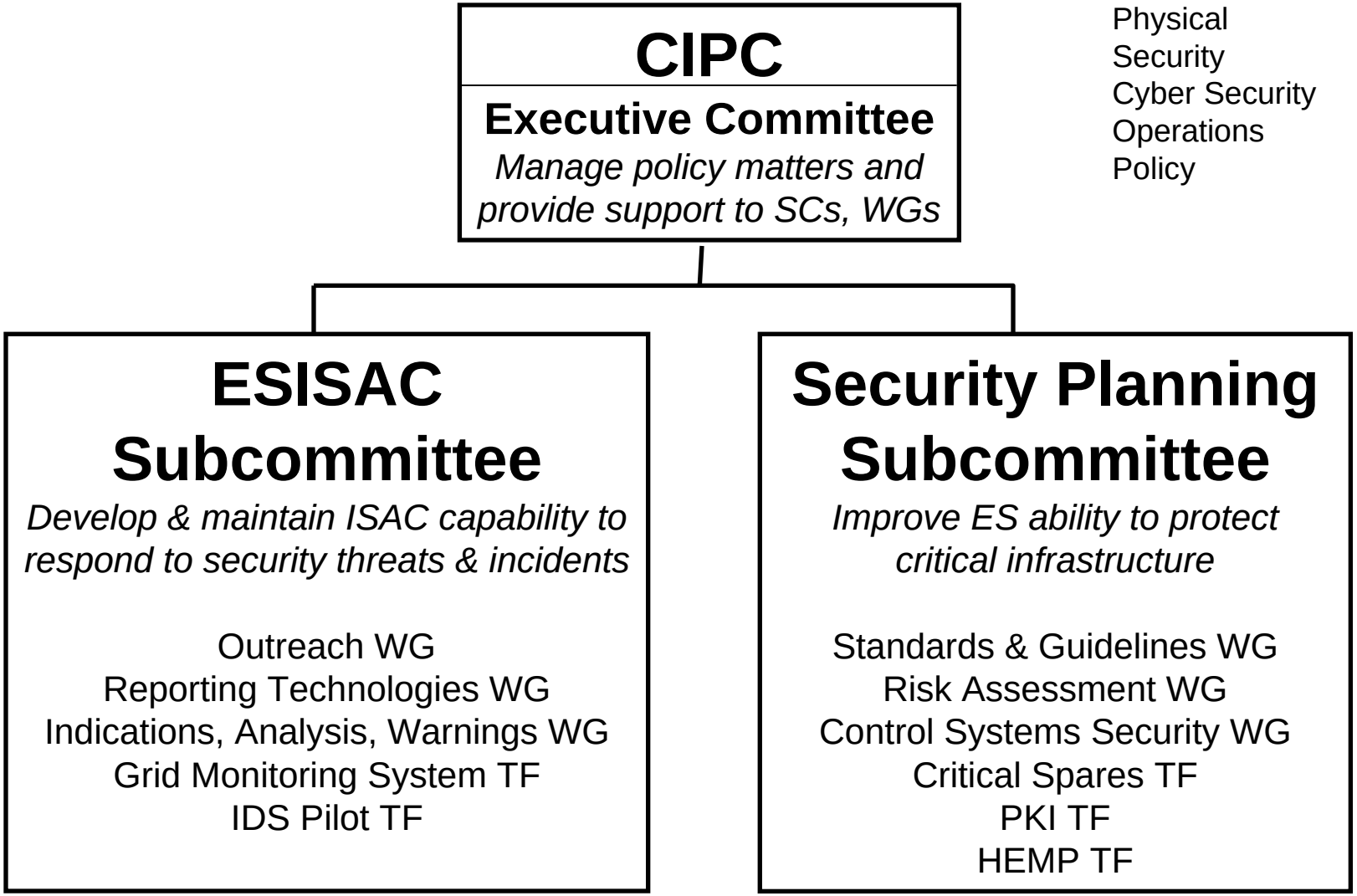
Latest update of the ESISAC Internet site: September 24, 2004

Message Board: [Archives]

- **Hurricane Jeanne**
- 01 Aug 2004: DHS has raised the HSAS to **HIGH** (**orange**) for specific Financial Sector locations in NYC, DC, Northern NJ.

http://www.esisac.com

North American Electric Reliability Council (NERC)
Critical Infrastructure Protection Committee (CIPC)



Mitigation Strategies

- Security through obscurity
  - Poor defense against “structured adversary”
- Isolated network
  - Unrealistic given today’s business demands
- Communication encryption
  - Concerns over latency, reliability, interoperability
  - Vendors waiting for customer demand
- Signal authentication
  - May provide good defense without the concerns associated with full signal encryption

Defense in Depth Strategy

- Multiple layers of defense
  - Strong network perimeter
  - Perimeter intrusion detection
  - Internal access control to mission-critical systems
  - Internal intrusion detection
  - Host-level hardening of mission-critical systems
- Good configuration management
- Effective policies and procedures
- Security awareness, training, and management control

Response and Recovery

- Contingency planning, disaster recovery drills
- Safety considerations
- Backup systems, restoration plans
- Preserve evidence
- Carefully evaluate system for changes
- Emphasizes the need for thorough and updated documentation, configuration management process

IEEE Standard 1402-2000

- IEEE Guide for Electric Power Substation Physical and Electronic Security
- Provides definitions, parameters that influence threat of intrusions, and gives a criteria for substation security
- Cyber methods considered:
  - passwords
  - dial-back verification
  - selective access
  - virus scans
  - encryption and encoding

Additional Countermeasures to Consider

- Implement access control with strong passwords
- Implement automatic reporting/intrusion detection features
- Create a multi-tiered access hierarchy
- Implement application level authentication and packet level data encryption
- Consider implementing public key infrastructure (PKI)
  - When properly implemented, PKI certificates enable authentication, encryption, and non-repudiation of data transmissions
- Implement properly configured firewalls and intrusion detection systems
- Have a defined Enterprise-level computer network security policy

Ref: *Concerns About Intrusion into Remotely Accessible Substation Controllers and SCADA Systems*, Schweitzer Engineering Laboratories, www.selinc.com

Overarching Security Policy

- Establish high-level accountability
  - Spanning both physical and cyber security
- Develop security policies
  - Address security in the context of corporate goals
- Implement security procedures
  - Actual implementation, not just on paper
- Provide adequate training
  - General employees, system administrators, etc.
- Evaluate security in the context of an overarching risk management plan

Other Issues

- Early detection is critical
  - Actively look for signs of malicious activity
  - Carefully evaluate trends, patterns
  - Notify appropriate authorities if malicious activity is detected
  - Actively participate in NERC Indications & Warnings program
  - Ensure effective mechanisms are in place to follow-through
- Conduct periodic vulnerability assessments
  - Comprehensive, independent evaluation
  - Include penetration testing, active vulnerability scanning to identify and/or validate potential vulnerabilities
  - Engage broader elements of the organization

Steps for Enhancing SCADA Security

- Establish a robust network architecture
- Eliminate trusted remote access points of entry
- Evaluate and deploy technology and approaches to enhance confidentiality, availability, and integrity
- Implement rigorous configuration management
- Provide adequate support and training
- Never become complacent!

21 Steps to Improve Cyber Security of SCADA Networks

Developed by the President's Critical Infrastructure Protection Board and the U.S. Department of Energy in 2002 as a guideline for improving the security of the Nation's SCADA systems.

Conclusion: System-Level Security Should Be Built on a Strong Foundation