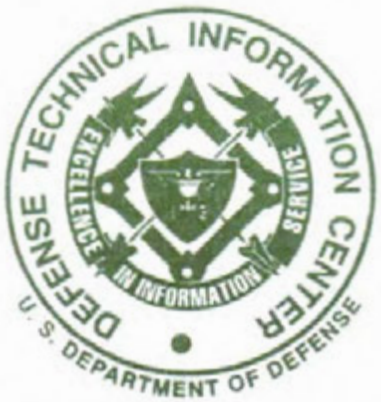
(3)

UNCLASSIFIED/LIMITED

DEFENSE TECHNICAL INFORMATION CENTER



UNCLASSIFIED/LIMITED

DEFENSE INFORMATION SYSTEMS AGENCY
DEFENSE TECHNICAL INFORMATION CENTER
8725 JOHN J. KINGMAN ROAD, SUITE 0944
FORT BELVOIR, VIRGINIA 22060-6218

UNCLASSIFIED/LIMITED

Policy on the Redistribution of DTIC-Supplied Information

As a condition for obtaining DTIC services, all information received from DTIC that is not clearly marked for public release will be used only to bid or perform work under a U.S. Government contract or grant or for purposes specifically authorized by the U.S. Government agency that is sponsoring access. Further, the information will not be published for profit or in any manner offered for sale.

Non-compliance may result in termination of access and a requirement to return all information obtained from DTIC.

NOTICE

We are pleased to supply this document in response to your request

The acquisition of technical reports, notes, memorandums, etc. is an active, ongoing program at the **Defense Technical Information Center (DTIC)** that depends, in part, on the efforts and interest of users and contributors

Therefore, if you know of the existence of any significant reports, etc., that are not in the **DTIC** collection, we would appreciate receiving copies or information related to their sources and availability.

The appropriate regulations are Department of Defense Directive 3200.12, DoD Scientific and Technical Information Program, Department of Defense Directive 5230.24, Distribution Statements on Technical Documents; National Information Standards Organization (NISO) Standard Z39.18-1995, Scientific and Technical Reports - Elements, Organization and Design, Department of Defense 5200.1-R, Information Security Program Regulation

Our **Acquisitions Branch, DTIC-OCA** will assist in resolving any questions you may have concerning documents to be submitted. Telephone numbers for the office are (703)767-8040 or DSN427-8040. The **Reference and Retrieval Service Branch, DTIC-BRR** will assist in document identification, ordering and related questions. Telephone numbers for the office are (703)767-8274 or DSN424-8274

DO NOT RETURN THIS DOCUMENT TO DTIC

EACH ACTIVITY IS RESPONSIBLE FOR DESTRUCTION OF THIS DOCUMENT ACCORDING TO APPLICABLE REGULATIONS.

UNCLASSIFIED/LIMITED

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Information Assurance Task Force

Electric Power Information Assurance Risk Assessment

FINAL

NOT FOR EXTERNAL DISTRIBUTION

December 1996

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

National Security Telecommunications Advisory Committee
Information Assurance Task Force
Electric Power Risk Assessment

Executive Summary

The security of electric power control networks represents a significant emerging risk to the electric power grid. This risk assessment is the result of a 6-month effort by the Information Assurance Task Force (IATF) of the National Security Telecommunications Advisory Committee (NSTAC), that included interviews and discussions with representatives throughout the electric power industry.

The electric power grid is a highly interconnected and dynamic system of over 3,000 public and private utilities and rural cooperatives. These utilities have incorporated a wide variety of information and telecommunications systems to automate the control of electric power generation, transmission, and distribution.

The electric power industry is undergoing significant change, fueled by marketplace forces and Federal legislative and regulatory activities. New players are entering the power generation and delivery market, and existing utilities are being required to offer open access to their transmission systems. The functions of power generation, transmission, and marketing—which traditionally have been tightly integrated—are now being separated within utilities and, in some cases, even spun off into new companies. Competition, aging proprietary systems, and reductions in staff and operating margins are leading utilities to rapidly expand their use of information systems and to interconnect previously isolated networks.

Physical destruction is still the greatest threat facing the electric power infrastructure. Compared to this, electronic intrusion represents an emerging, but still relatively minor, threat. Insiders are considered to be the primary threat to information systems. Downsizing, increased competition, and the shift to standard protocols will add to the potential sources of attacks, whether from inside, or outside, a utility.

Recent legislation increases the jurisdiction of Federal, state, and local law enforcement authorities over attacks on electric power control systems. However, the lack of effective reporting mechanisms, inconsistent use of logins, passwords, and warning banners, and a low probability of being detected, caught, and prosecuted hinder effective deterrence of potential attackers.

Substations represent the most significant information security vulnerability in the power grid. Many of the automated devices used to monitor and control equipment within transmission and distribution substations are poorly protected against intrusion. Interconnections between control centers and corporate data networks, widespread use of dial-up modems, and use of public networks (PN) are other sources of vulnerabilities.

Utilities use a variety of mechanisms to protect the electric power grid from disruption, including contingency analysis, redundant control centers, dial-back modems, and firewalls. However, few utilities have an information security function for their operational systems, and the lack of convincing evidence of a threat has led senior managers to minimize information security investments.

The recent U.S. western power outages left 2 million people without power for up to 6 hours on July 2, 1996, and 5.6 million people without power for up to 16 hours on August 10, 1996. A critical node analysis, combined with knowledge of weak protections on substation automation elements, could allow an electronic intruder to achieve similar effects. A major coordinated attack could disrupt activities at a national level.

The study found no evidence of a disruption of electric power caused by an electronic intrusion Three trends, however, will increase the exposure of electric power control networks to attacks:

- The shift from proprietary mainframe control systems to open systems and standard protocols
- Increasing use of automation, outside contractors, and external connections to reduce staff and operating costs
- The requirement to provide open access to transmission system information dictated under FERC orders 888 and 889.

The probability of a nationwide disruption of electric power through electronic intrusion short of a major coordinated attack is extremely low, but the potential for short-term disruptions at the regional level is increasing.

The report closes with a number of recommendations for the President, the electric power industry, and the NSTAC. Of these, the most important recommendation is that the President should consider assigning to the appropriate Department or Agency the mission to develop and conduct an ongoing program within the electric power industry to identify the threat and increase the awareness of vulnerabilities and available or emerging solutions.

1.0 INTRODUCTION

In January 1995, the Director of the National Security Agency briefed the National Security Telecommunications Advisory Committee (NSTAC) on threats to U.S. information systems and the need to improve the security of critical national infrastructures. The NSTAC principals discussed those issues and subsequently sent a letter to the President in March of that year stating that "[the] integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack . . . [and that] other national infrastructures . . . [such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk."[1] President Clinton replied to the NSTAC letter in July 1995, stating that he would "welcome NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications systems."[2] The President further asked "the NSTAC's principals—with input from the full range of NII users—to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information infrastructure."[3]

In May 1995, the NSTAC formed the Information Assurance Task Force (IATF) to work closely with the U.S. Government to identify critical national infrastructures and their importance to the national interest. Following several meetings with elements of the national security community, civil departments and agencies, and the private sector, the task force determined that electric power, financial services, and transportation were some of the most critical of the infrastructures. The task force determined that it would study these infrastructures to assess the extent to which their dependence on information and information systems puts them at increased risk to denial-of-service attacks.

This document is a report of the findings of the IATF's Electric Power Risk Assessment Subgroup's assessment of the risk that electronic intrusions pose to electric power distribution systems, specifically examining the vulnerability of the systems that manage and control generation, transmission, and distribution. This study represents a 6-month effort that included interviews with representatives from the operations, security, and information systems elements of eight utilities, one power pool association, the Utility Telecommunications Council (UTC), the North American Electric Reliability Council (NERC), the Electric Power Research Institute (EPRI), the Federal Energy Regulatory Committee (FERC), and a number of industry consultants. The utilities interviewed ranged in size and location and included both publicly held companies and government-owned and -operated power administrations.

---

[1] Letter from Mr. William Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States dated March 20, 1995.

[2] Letter from the President of the United States to the NSTAC dated July 7, 1995.

[3] Ibid.

During the course of the study, interview teams worked under the assumption that the risk to the electric power infrastructure was a function of four factors: threat, deterrence, vulnerabilities, and protection measures. In this model, a threat is any circumstance or event with the potential to cause harm to a system in the form of unauthorized destruction, disclosure, modification of data, or denial of service. A deterrent is an attempt to prevent or discourage an action before it is taken, thus mitigating a threat. Vulnerabilities are points of weakness within a given system and are mitigated by protection measures.

Interviews with the utilities and power pool were conducted in a nondisclosure/nonattribution environment, and utility staff were all forthcoming and helpful throughout the process. In addition, EPRI provided invaluable support to this study, undertaking its own survey of industry managers to assess their views on information security concerns. The UTC also assisted by arranging a meeting at its 1996 annual conference in Kansas City, Missouri, and identifying contacts in a number of utilities.

2.0 OVERVIEW OF POWER GENERATION AND DISTRIBUTION

This chapter provides an overview of the electric power transmission and distribution industry. This overview describes the structure of the electric utility industry, identifies the roles of key industry players, and explains the basic structure of an electric power transmission and distribution system with an emphasis on the mission, functions, and system components of a typical electric utility control center. Finally, it highlights major legislative and industry trends causing change within the electric power industry and reviews previous studies of the security of electric power networks and information systems.

2.1 BACKGROUND

Since Thomas Edison opened the New York City Pearl Street Station in 1882, the U.S. and Canadian electric power grid has grown into a highly interconnected, international asset composed of 3,000 independent utilities. The goal of the modern-day power systems is to generate and deliver electric energy to customers as reliably, economically, and safely as possible while maintaining the important operating parameters (voltage, frequency, and phase angles) within permissible limits. To achieve this goal, electric utilities use centralized automation technology incorporating high-speed digital computers, supervisory and control systems, and a variety of communication systems.

2.2 OVERVIEW OF THE ELECTRIC POWER INDUSTRY

There are about 3,000 independent electric utilities in the United States. Each is interconnected with coordinated controls, operations, telecommunications networks, and sophisticated control centers. These utilities include investor-owned public utilities, government-owned systems, cooperatives, and manufacturing industries that also produce power. Nearly 80 percent of the Nation's power generation comes from the approximately 270 investor-owned public utilities. The Federal Government generates another 10 percent of the Nation's power, primarily through large facilities such as the Tennessee Valley Authority. However, the Federal Government owns few distribution facilities. The remaining power supply is generated by the cooperatives and manufacturing industries. There are approximately 1,000 cooperatives, which generally have limited power-generation capacity and focus primarily on transmission and distribution systems. In addition, some manufacturing industries generate power for their own use but sell surplus power to utilities, accounting for a small portion of the industry total.

The 3,000 companies that compose the North American power grid are divided into four regions: Eastern, Western, Texas, and Quebec. Figure 1 depicts these regional divisions. The Eastern, Western and Quebec regional power grids are linked through an alternating

Figure 1: Interconnections of Utility Systems

current/direct current (AC/DC) interconnection—the Texas regional power grid is not linked to the other regional power grids. The four regions are further broken down into 15 "power pools" that share generation capacity with one another and are generally located within the same geographic region.

Several Federal organizations are involved in various aspects of the electric power industry. The Department of Energy's (DOE's) mission is to formulate a comprehensive energy policy encompassing all national energy resources, including electricity. The Federal Energy Regulatory Commission (FERC) is an independent agency overseeing the natural gas industry, the electric utilities, non-Federal hydroelectric projects, and oil pipeline transport. FERC was created in October 1977 through the Department of Energy Organization Act and replaced the Federal Power Commission. FERC's principal mission is to regulate the wholesale sales of electricity in interstate commerce. Other Federal agencies that oversee the electric power transmission and distribution industry include the Nuclear Regulatory Commission (NRC), the Rural Electrification Agency (REA), the Environmental Protection Agency (EPA), and the Securities and Exchange Commission (SEC).

State public utility commissions (PUCs) play the most significant role regulating the electric power industry. PUCs control the rate structure for all municipal utilities, investor-owned utilities, and rural electric cooperatives that own, maintain, or operate an electric generation, transmission, or distribution system within a state. By controlling what constitutes an allowable charge, classifying accounts, and structuring rates, the PUCs

can exert significant influence over utilities. The PUCs also regulate reliability for both operational and emergency purposes, oversee territorial agreements, and resolve territorial disputes between utilities.

The North American Electric Reliability Council (NERC) is the organization most involved in "keeping the lights on" in North America. NERC does this by reviewing the past for lessons learned; monitoring the present for compliance with policies, criteria, standards, principles and guides; and assessing the future reliability of the bulk electric systems. NERC is a nonprofit corporation composed of nine regional councils focusing on interregional and national electric reliability issues. The members of the regional councils are electric utilities, independent power producers, and electricity marketers. The electric utility members are drawn from all ownership segments of the industry—investor-owned, Federal, State, municipal, rural, and provincial. These members account for most of the electricity supplied in the United States, Canada, and Mexico. NERC was formed in 1968 in response to a cascading blackout that left almost 30 million people in the northeastern United States and southeastern Canada without electricity. Although it is a voluntary industry consortium, the NERC Engineering and Operating Committees set standards for the planning, engineering, and operating aspects of electric system reliability.

While NERC handles operational issues, the Electric Power Research Institute (EPRI) is another significant industry player, with a research and development (R&D) focus. EPRI's mission is to discover, develop, and deliver high-value technological advances through networking and partnership with the electric industry. Founded in 1972, EPRI has more than 700 member utilities, representing approximately 70 percent of the electricity generated in the United States.

The UTC is another technology-focused industry association. UTC represents the telecommunications interests of the Nation's electric, gas, and water utilities before Congress, the Federal Communications Commission (FCC), and other Federal and State agencies. UTC promotes cooperation among its member companies in all matters concerning telecommunications, including the development and improvement of telecommunications media.

Other significant electrical power industry bodies include the following:

- The National Rural Electric Cooperative Association (NRECA)
- The American Public Power Association (APPA)
- The Edison Electric Institute (EEI).

NRECA is a national service organization representing private, consumer-owned cooperative electric utilities. NRECA provides legislative representation on issues affecting the electric service industry and its environment. The APPA represents 2,000 municipal and other state or locally owned public electric utilities. The APPA primary

objective is to expand the publicly held utility base. The APPA lobbies to improve public utility access to other power networks. The association also markets public utilities as the non-profit, low-cost, and innovative alternative to their private competitors. The EEI is an association of shareholder-owned electric companies. The association provides a forum for these companies to exchange information and acts as a representative on issues of public interest. In addition, the association develops informational resources and tools.

2.3 OVERVIEW OF ELECTRIC POWER SYSTEMS

The basic structure of an electric power transmission and distribution system consists of a generating system, a transmission system, a subtransmission system, a distribution system, and a control center. This configuration is illustrated in Figure 2. Power plant generation systems may include steam turbines, diesel engines, or hydraulic turbines connected to alternators that generate AC electricity. Generators produce three-phase current at voltages ranging from 2,000 to 24,000 volts. This electricity must be transformed to higher voltages for efficient long-distance transmission. Modern transmission systems operate at voltages from 69,000 to 765,000 volts. It is the interconnection of the transmission systems that forms the "power grid," which permits the interchange of electricity between utilities. Transmission lines terminate at substations in which the

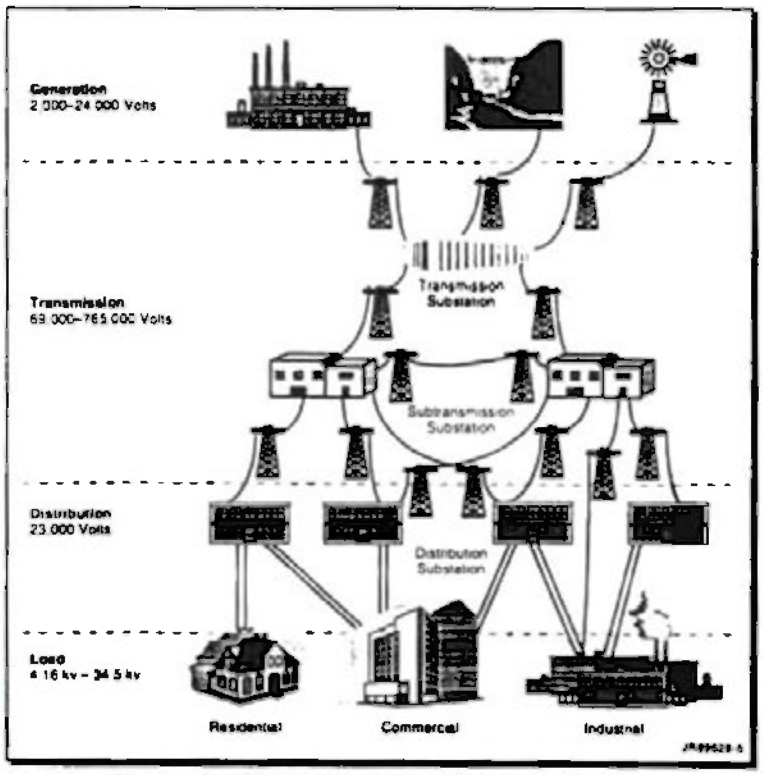


Figure 2. Overview of Electric Power Systems

voltage is reduced to the primary distribution voltage of 34.5 kv to 115 kv. This voltage is then supplied directly to large industrial users or further transformed down to 4.16 kv to 34.5 kv for local distribution.

2.3.1 The Control Center

The control center monitors a utility's generating plants, transmission and subtransmission systems, distribution systems, and customer loads. The primary functions of an electric utility control center is to provide centralized monitoring of power system operations, retain historical data, and allow for the manual and automatic control of field equipment. The control center system presents the electric system data to operations personnel via a modern, graphical user interface. Based on the data gathered, the operators may initiate control signals to various control points in the power system. The control center system may also automatically initiate controls to the field equipment, such as control of generating unit output. Figure 3 provides a schematic of a typical modern, distributed control center configuration.

Generally, the communications between the control center system and the field equipment takes place over utility-owned communications networks. Today, the majority of these networks are based on analog and digital microwave technology, although fiber optics is becoming increasingly more popular among the electric utilities. Other communications media include dedicated leased lines, power line carrier, satellite, spread-spectrum radio, and two-way radio.

Control center systems acquire the electric system data through communications with hardwired or programmable equipment in the field. This field equipment, called remote terminal units (RTUs), acts as a clearinghouse for incoming data by continuously collecting the electric system data directly from the field equipment involved in the generation, transmission, and distribution of electric power. The RTUs in turn support the transmission of this information to the control center system when requested.

Newer, more intelligent data collection equipment is now being deployed in substations by electric utilities as new substations are being built and as the old substations are being refurbished. These computerized field devices that are directly involved with the generation, transmission, and distribution systems are called intelligent electronic devices (IEDs). These devices represent the growing trend in the industry of pushing the intelligence and decision making capabilities farther and farther out into the field, closer to the data collection point. The IEDs are typically networked together at the substation, and communicate with a PC-based unit that replaces the remote terminal unit for the transmission of field data to the control center system.

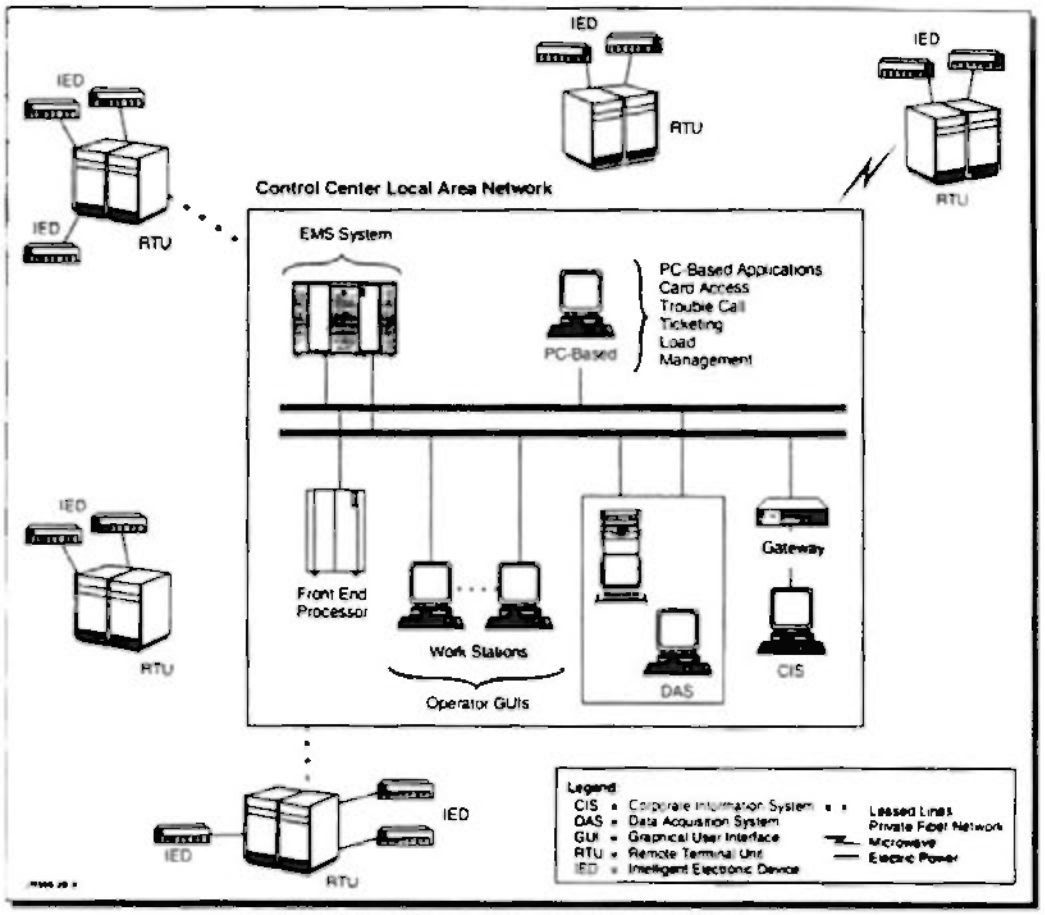


Figure 3: Typical Control Center Configuration

2.3.2 Energy Management System

A control center energy management system (EMS) typically houses the utility's systems' databases, the operational applications and displays, and the power system report-generation function. The need to disseminate valuable electric system data within a utility has resulted in many utilities connecting their EMS systems to their corporate local area network (LAN) or wide area network (WAN) to facilitate data sharing with other departments. Significant historical information systems have been developed to support this requirement. A control center energy management system (EMS) generally consists of four major elements:

- The supervisory control and data acquisition (SCADA) system
- The automatic generation control (AGC) system
- The energy management applications and database
- The user interface (UI) system.

These elements are depicted in Figure 4.

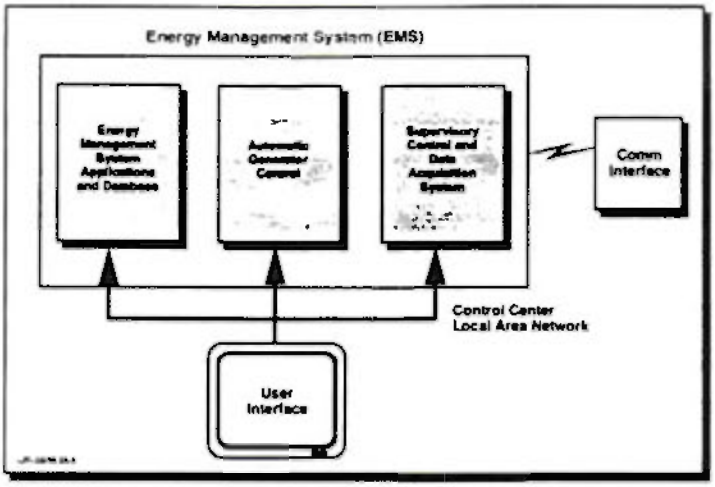


Figure 4: Energy Management System

The SCADA system manages the RTU communications, collects the electric system data from the field through a series of front-end processors, initiates alarms to the operations personnel, and issues control commands to the field as directed by the applications in the control center system. The SCADA system typically consists of a host or master computer, one or more field data-gathering and control units (RTUs), and a collection of standard and/or custom software used to monitor and control remote field data elements. SCADA systems may have 30,000 to 50,000 data collection points and may transmit analog information (e.g., generator megawatts) as well as digital or status information (e.g., breaker open/close state). SCADA systems can also send a control signal (e.g., start a pump) as well as receive a status input as feedback to the control operation (e.g., the pump is started). Current computing power allows SCADA systems to perform complex sequencing operations and provides for frequent collection (e.g., every 2 seconds) of power system data.

The AGC system controls the utility's generating units to ensure that the optimal system load is being met, with the most economical generation available. The AGC system submits supplementary control signals to the generating units to adjust their output based on the load forecast, unit availability, unit response rate, and scheduled interchange with other utilities.

The energy management applications and database are the programs and associated data sets that utility operations personnel use to manage state estimation, power flow, contingency analysis, optimal power flow, load forecasting, and generation unit allocation.

The UI system provides operational personnel with an interactive interface to monitor electric system performance, manage system alarm conditions, and study potential system conditions to ensure that network security criteria are met.

2.4 INDUSTRY LEGISLATIVE ENVIRONMENT

The electric power industry is in the midst of a revolution driven largely by a mix of marketplace forces, and Federal legislative and regulatory activity. An understanding of the legislative actions driving these changes in the U.S. electric power industry is vital to comprehending where these dynamic changes will lead.

The Federal Power Act of the 1950s laid a foundation for a self-sufficient vertically integrated electric utility structure. The late 1960s and 1970s experienced the beginning periods of rapid inflation, higher nominal interest rates, and higher electricity rates. This resulted in the government-sponsored construction of expensive generation facilities. Later, the oil cartel collapse resulted in a glut of low-priced oil, inflation, and surging interest rates. All of these elements substantially increased the costs of these high capacity generating plants resulting in rapidly rising electrical rates.

Congress recognized that the utility-owned generating facilities were increasing rates and harming economic growth and responded by enacting legislation and encouraging electric utilities to develop alternative generation sources. A new class of generating firms, such as independent power producers (IPPs), single-asset generation companies, and utility-organized affiliated power producers (APPs) sprang into existence.

Through these developments, the seeds for a free-market economy were being sown. While consumer-based rates helped to develop competitive bulk power markets, two issues remained: customer access to the transmission services and barriers hindering open access to third parties. The Energy Policy Act of 1992 (EPAC) opened up power generation to competition, while leaving power transmission and distribution a regulated, natural monopoly. In March 1995, FERC clarified the EPAC language by stating that all utilities under the commission's jurisdiction would be required to file nondiscriminatory open-access transmission tariffs available to all wholesale buyers and sellers of electric energy. Concurrently, FERC ruled that transmission owners and their affiliates did not have an unfair competitive advantage over the wholesale buyers and sellers in using transmission to sell power. This rule requires that public utilities obtain information about their transmission system for their own wholesale power transactions, via an open-access same-time information system (OASIS) available on the Internet.

In July 1996, in an effort to complete the deregulation of the power industry, Congress enacted the Electric Consumers' Power to Choose Act of 1996. The bill establishes federal mandates for all electric utilities, including electric cooperatives and municipal utilities, to provide retail choice to all classes of customers by December 15, 2000. After

retail choice in a state has been established, state commissions would be prohibited from regulating the rates for retail electricity services. Reasonable and nondiscriminatory access to local distribution facilities would be provided on an unbundled basis to any supplier seeking to provide retail electricity service. These mandated government actions will soon provide the consumers, generation and distribution firms, and power marketers open access to an unregulated electric power industry.

2.5 INDUSTRY TRENDS

The structure of the electric power industry is changing. The traditional attributes of the power industry, such as monopoly status, government ownership, and government regulations are yielding to free-market forces. The future of the U.S. power industry will be driven by competition, privatization, and deregulation. Global competition, increasing customer demands, capital liquidity, the relatively low price of natural gas, and environmental concerns are all driving forces that, when coupled with deregulation of the industry, will create great change.[4]

A number of key trends are affecting the use of networks and information systems in the power industry. These include the rise of IPPs, significant downsizing and restructuring, the advent of consumer choice, rate restructuring, and structural reorganization of access to transmission lines.

Transmission capacity is controlled by the investor-owned utilities. Under FERC order 888, transmission system operators must provide fair and equal access to their lines. A number of utilities view the creation of independent system operators (ISOs) as the answer to FERC order 888. ISOs would coordinate and schedule transmission service independently of electric companies to ensure fairness and promote reliable operations. ISOs would take over management of regional electric transmission grids owned by various electric companies, though the companies would continue to own their own parts of the regional grid.

Information technology will be the integrating force for many of the initiatives that utilities have undertaken to prepare for deregulation. To prepare for this new focus, industry organizations are successfully instituting standards and inter-utility protocols for the development of utility systems. The Utility Communications Architecture (UCA) and Database Access Integration Service (DAIS) have emerged as *de facto* industry communications and database protocols for data exchange. UCA and DIAS allow the development of more sophisticated and interoperable systems; however, the technical information about these open protocols will be available to a much larger population—and thereby a much larger number of potential attackers.

---

[4]Silverman, Lester, "Electric Power—The Next Generation," *McKinsey Quarterly* (January 1, 1994)

The Telecommunications Act of 1996 also affects the power utilities by allowing public utilities to enter the telecommunications services market. The act allows public utilities to enter the market so long as they do not subsidize their telecommunications activities with moneys from the power side of the business. Some utilities are already exploring using their private, fiber optic networks to offer services ranging from cable TV to telephone service to leased lines.

The deregulation of the electric power industry will force the utilities to move farther and faster than ever before. The next 4 years hold considerable promise for the industry but also portend significant challenges and changes. To succeed, utilities must offer value-added services; optimize the efficiency of their power systems; and develop strong customer ties, an aggressive economic development plan, and a winning corporate culture.

2.6 PREVIOUS STUDIES

This assessment builds on several previous studies of the security of information systems and networks in the electric power industry. These previous studies include the Defense Advanced Research Projects Agency's (DARPA's) 1995 Defensive Information Warfare study, EPRI's analysis of the security of the UCA and DAIS, the National Information Infrastructure (NII) risk assessment prepared by the Reliability and Vulnerability Working Group (RVWG) of the IITF, and a study of electric power's dependence on (PN) by the Air Force's Air Command and Staff College (ACSC). In addition, investigations by the Joint Program Office on Special Technologies Countermeasures (JPO-STC) and the Office of the Secretary of Defense (OSD/Policy) into overall infrastructure vulnerabilities have addressed the security of electric power networks. Although none of these studies were comprehensive, they have all reached similar conclusions.

First and foremost, these independent studies appear to agree that the transition from proprietary systems to standardized systems based on well-known, unsecure protocols and architectures will greatly reduce the security of utility control systems. These studies also noted potentially worrisome trends, such as the reduced skill levels of operations and maintenance personnel, near universal minimal front-end security, and increased interconnectivity through the use of dial-in modem ports and the Internet. One report bluntly stated that "data security is negligible to non-existent." These studies also noted the inherent risk to the utilities resulting from single point-of-failure systems. None of the studies predicted any significant improvements in the near future because tighter operational budgets and efforts to trim costs have made it difficult to justify security expenditures.

3.0 THREAT

This section addresses threats to the electric power grid. A threat is any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service. Generally speaking, threats can be placed into two broad categories— physical and electronic.

3.1 PHYSICAL THREAT

Despite the growing concern about cyberspace attacks, the physical destruction of utility infrastructure elements is still the predominant threat to electric utilities. Physical threats to the infrastructure elements of an electric power utility fall under the general categories of accidental and deliberate events. Natural emergencies are the most significant accidental physical event to affect a utility and are the single greatest cause of outages in the electric power system. However, the impact of natural hazards on the power grid is the most manageable because utilities have years of experience with this threat and have designed facilities and infrastructure elements to minimize the impact of such events. Additionally, service providers design systems and operational procedures to allow them to respond to outages and restore service quickly. Most utilities have extensive experience with storms and other natural disasters and exercise their response systems periodically.

After natural hazards, deliberate physical attacks on utility infrastructure elements cause the most damage to the electric power grid. Transformers, microwave communications towers, and transmission substations can often be found in isolated, unpopulated areas. These pieces of equipment have proven to be popular targets for vandals, criminals, ecological terrorists, and amateur sharpshooters. Every utility visited during the course of this risk assessment recounted anecdotes about teenagers breaking into substations, ecological terrorists blowing up or damaging towers supporting transmission lines, or bored hunters taking potshots at insulators, transformers, and lines. However, transmission and distribution infrastructure elements are not the only target for physical attack—as recently as February 1996, pipebombs were used to attack a SCADA system at a hydroelectric plant in Oregon.[5]

3.2 ELECTRONIC THREAT

The electric power industry does not acknowledge a single incident of a power outage caused by an electronic intrusion. However, a majority of utility members agree that an electronic attack capable of causing regional or widespread disruption lasting in excess of

[5]Bureau of Alcohol, Tobacco and Firearms, *Explosive Incident Listing*,(21 March 1996.)

24 hours is technically feasible.[6] The source for such an attack could come from within the utility or from an external source.

3.2.1 Insider Threat

Insiders can be employees, contractors, or anyone else with legitimate access to system components and/or premises. Generally, insiders are granted varying degrees of access to the software and databases and may use legitimately or surreptitiously acquired computer access privileges to compromise them. The primary motives that drive an insider to exploit a system are usually financial gain or revenge.

Electric utility personnel believe that alienated employees pose the most significant insider security threat to information systems.[7] Considering that between 1986 and 1992 the number of employees working for electric utilities has dropped from 529,664 in 1986 to 506,068 in 1992,[8] there are significant numbers of potentially bitter former utility employees with system knowledge who could attack the power grid. As evidence of this, a letter appeared in the hacker magazine *Phrack* in which the author claimed to be an employee of an electric utility in Texas. In the letter the author claimed to know quite a bit about the systems and hinted that his knowledge would be helpful if someone wanted to attack a utility's systems.[9]

3.2.2 Outsider Threat

An outsider is anyone not legitimately associated with the system in question. Outsiders could be rival companies, criminal elements, or foreign national intelligence agencies. Examples include technical hackers motivated by the challenge; terrorist groups motivated to inflict damage to systems for a variety of political, ideological, or personal reasons; or rival companies seeking competitive information.

Until the passage of the Energy Policy Act, the Electric Consumers' Power to Choose Act, and the FERC rulings, most utilities operated as natural, regulated monopolies. This has changed significantly, and utilities are now competing for customers, power, and transmission capacity. In this newly competitive environment, rivals in the electric power market will have significantly more motivation to collect information, through whatever means possible. As one respondent to the EPRI Electronic Information Security Survey

---

[6] EPRI, *Electronic Information Security Survey* (Summer 1996).

[7] Ibid.

[8] Moulton, Curtis, "More Customers, Fewer Workers," *Electric Perspectives* (September 1, 1995), pg. 68

[9] Letters to the Editor, *Phrack* (April 15, 1995).

said, "As the utility industry has been heavily regulated, many are naive to (the) potential risk of info security violations."

While there have been instances of hackers breaking into electric utilities' business and support systems, the utilities have not encountered the full-scale attacks that the telecommunications services providers have experienced. In the EPRI Electronic Information Security Survey, 35 percent of those polled were not aware of any breaches of information and control systems at any electric utility, and 60 percent were aware of only minor security breaches. This is not to say the hacker community has not tried to enter the utilities' systems—members of a radical environmental group were arrested for trying to hack into a data network.[10] However, with industry deregulation, the stakes are getting higher, perhaps high enough to attract more attention. Stanley Klein, an industry consultant, estimates that the profit at an energy derivative delivery point could be as high as $10 million a day[11]—certainly enough to attract the attention of market manipulators and the intruder community.

Furthermore, if an outside organization had goals beyond financial gain, a structured electronic attack targeting the utility's operations systems could be a way to cause widespread disruption to a given geographic region. Organizations have used structured physical attacks on utility infrastructure elements around the world to achieve a variety of goals—a Department of Energy database records 10,200 incidents over the past 16 years. An organization with sufficient resources, such as a foreign intelligence service or well-supported terrorist group, could conduct a structured attack on the electric power grid electronically—without having to set foot in the target nation and with a large degree of anonymity.

It is important to note that information systems do not just represent a way to directly attack the electric power grid. During the course of this study, many of the electric utility officials interviewed expressed a concern about the amount of information about their infrastructure elements that is readily available to the public. Utility officials felt that the information on the various FERC forms, which are currently available in the public reading room at FERC in Washington DC, and are posted on FERC electronic bulletin boards, would be of value in planning an attack on the power grid. Additionally, the information that FERC is requiring utilities to post on their OASIS node will further simplify the process of target analysis. One utility official was asked to supply a Federal agency with a list of their top ten most vulnerable locations as part of an infrastructure study—the utility refused to supply the agency with the requested information.

---

[10] *Foreign Broadcast Information Service-Western Europe Edition*, #058, (28 March 1989).

[11] Klein, Stanley, *Information Security Implications of FERC Orders 888 and 889 and Related Industry Restructuring*, Stanley Klein Associates, August 1996.

3.3 THREAT CONCLUSIONS

The electric power industry clearly recognizes and has considerable experience in dealing with the risks to the energy infrastructure from physical threats. However, the implications of electronic intrusions are understood less well. Given the limited experience with electronic attacks, government efforts to identify and scope these threats must be coordinated with an industry effort to identify and report intrusion incidents. A clear threat identification, combined with an infrastructure vulnerability assessment and guidelines for protection measures, is critical to stimulating effective response by individual utilities.

4.0 DETERRENTS

A deterrent is an attempt to prevent or discourage an action before it is initiated—generally through fear or doubt. The ability of law enforcement to investigate, prosecute, and convict is the principle deterrent to computer crime. Recent and pending legislation increases the jurisdiction of Federal, state, and local law enforcement authorities over attacks on electric power control systems. However, the lack of effective reporting mechanisms, inconsistent use of logins, passwords, and warning banners, and a low probability of being detected, caught, and prosecuted hinder effective deterrence of potential attackers

The proposed National Information Infrastructure Protection Act (H.R. 4095) would greatly expand the jurisdiction of Federal law enforcement authorities over attacks against the computer systems of critical infrastructures such as electric power. In particular, the act would

- Broaden the jurisdiction of Section 1030 of Title 18 of the U.S. Code from "Federal interest" computers to that of "protected" computers, which would include any use in interstate or foreign commerce or communication

- Expands the definition of "damage" to include any impairment to the integrity or availability of a system that threatens public health and safety or causes any loss over $5,000 in value.

In addition, the recent passage of the Economic Espionage Act of 1996 increases the penalties related to improper disclosure of proprietary information, providing an improved deterrent against electronic intrusions aimed at gaining competitive advantage.

A number of factors tend to greatly reduce the effectiveness of these deterrents. Most network and systems administrators lack efficient tools to detect intrusions reliably. Only 25% of the respondents to EPRI's information security survey reported use of any intrusion detection methods. Even when intrusions are detected, the majority of the organizations effected do not report these events. In a recent survey conducted jointly by the Computer Security Institute, the FBI, and the International Computer Crime Squad, less than 17 percent of the 428 respondents said that they would notify law enforcement if they thought they had been attacked. Most of the respondents, 70 percent, said they feared negative publicity. Furthermore, more than 70 percent of the respondents do not have warning banners stating that computing activities may be monitored, hampering

investigations because law enforcement officials would likely not be able to tap computers or prove trespassing.[12] Use of shared logins and relatively weak passwords further complicates this situation for the electric power industry.

[12] "Computer Study Finds Concern, But Insufficient Action," *Telecom & Network Security Review* (May 1996)

5.0 VULNERABILITIES

An organization's systems are most vulnerable at the point where the connectivity is the greatest and the access control is the weakest. Figure 5 depicts the electric power generation, transmission, and distribution infrastructure with the supporting communications and control systems. If someone opted to attack the electric power grid electronically, rather than physically, he or she would have several options to consider—the **control center**, the **substation,** and the **communications infrastructure**. The following sections address the nature of each vulnerability, any trends affecting the vulnerability, and likely avenues of attack.

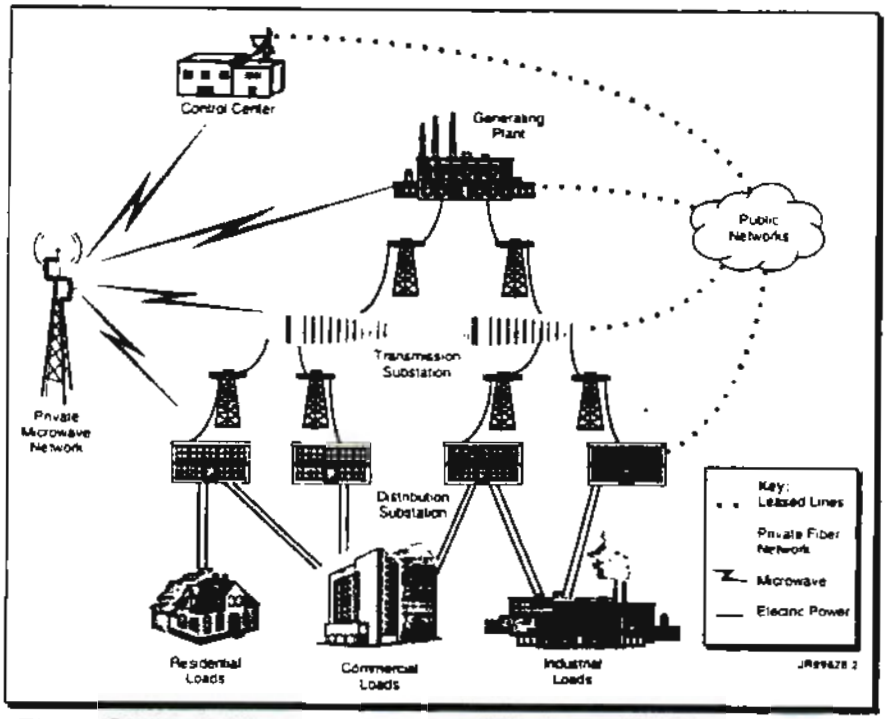


Figure 5: Electric Power Infrastructure With Supporting Communications and Control Systems

5.1 CONTROL CENTER VULNERABILITIES

There is no "standard" control center system configuration—they range from isolated, mainframe-based systems developed in-house more than 20 years ago to off-the-shelf, commercially developed, networked, Unix client/server systems. The industry trend is for utilities to procure "standard" vendor system products, based on the distributed client/server technology, to reduce schedule risk and minimize project costs. They continue to use their private communications networks to support remote data acquisition,

although the use of the public networks is increasing to interconnect corporate facilities, neighbor utilities, and the Internet.

As seen in Figure 6, an electronic intruder may access the control center through several interfaces:

- Links to the corporate information system
- Links to other utilities or power pools
- Links to supporting vendors
- Remote maintenance and administration ports.

The following paragraphs review the details of industry practices for each interface.

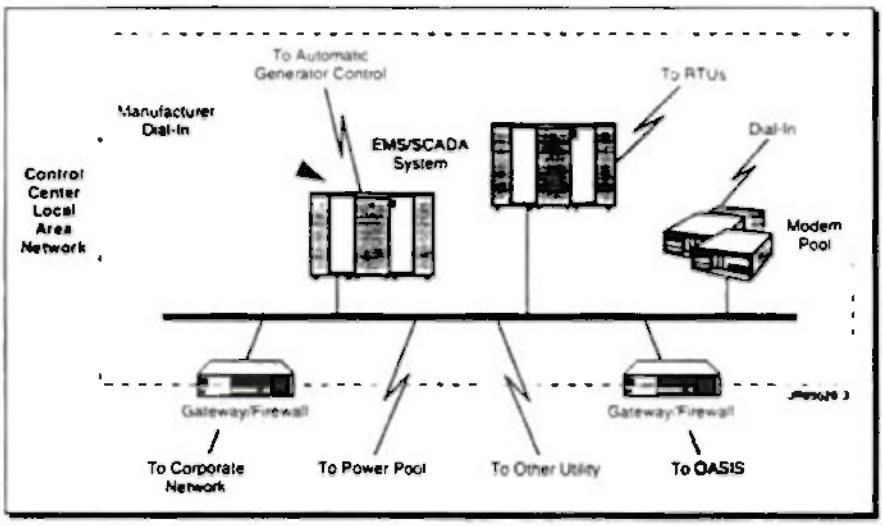


Figure 6: Typical Control Center Interfaces

5.1.1 Corporate MIS

Although not all utilities have an interface between the control center and the corporate information system, the distinct trend within the industry is to link the systems to access control center data necessary for business purposes. One utility interviewed considered the business value of access to the data within the control center worth the risk of open connections between the control center and the corporate network. More common solutions used firewalls or masked subnet routing schemes to create a secure link between the corporate information system and the EMS.

Current trends towards interconnectivity further increase the chances of an attack through the corporate network by providing more access routes into the corporate network.

Internet connectivity, modem pools, and individual modems all can serve as points of access for an electronic intruder into the corporate system and subsequently into the EMS. Despite the protective measures taken to isolate the control center network from the corporate information system, the control systems are still vulnerable to an attack through the corporate system. Utility operations personnel interviewed believed that firewalls and dial-back modems were sufficient to protect their systems from intruders, and they were surprised to learn about the experiences of the telecommunications industry with hackers defeating these measures.

5.1.2 Other Utilities and Power Pools

Many utilities have links between their control room and the control centers of adjacent utilities and the regional power pool. Most of these links are one-way connections carrying system data that operators use to balance the load on the power grid, schedule transmission, compute economic dispatch, and perform security analysis. Application-level controls and proprietary protocols make these links difficult targets for an electronic attack.

Several trends within the industry will increase the risk posed by these links. As the industry migrates to standard protocols, the pool of people with the knowledge to attack the system will grow significantly. The flurry of mergers resulting from deregulation of the industry further creates a need for merger partners to communicate electronically, increasing exposure.[13] The creation of ISOs will significantly increase the amount of traffic exchanged between the utilities and their ISO. In all likelihood, this traffic will require two-way data flows. Furthermore, the information flowing between the organizations (e.g., line capacity and scheduling information) will have significant economic value and will enable a potential attacker to identify critical nodes in the transmission and distribution system. Disabling these links would not, however, cause any direct disruption of the power system.

5.1.3 Supporting Vendors

As they move to client-server architectures, utilities are using more commercially developed software and are outsourcing the customization and maintenance of EMS and supporting applications. To support the installation, debugging, and ongoing maintenance of these new systems, utilities are providing remote access to manufacturers and integrators. Remote access is generally accomplished through a dial-in port on the system, although some utilities have dedicated links in place. These remote access links represent a potential point of access for an intruder. A representative of a major EMS manufacturer confirmed that all of his company's products with a dial-in port will allow the manufacturer's engineering staff to connect to the system to perform software updates and

[13] EPRI. *Electronic Information Security Survey* (Summer 1996).

other maintenance functions. These products frequently share a simple password that has not been changed in years.

One electric utility reported that an intruder accessed a chemistry-monitoring system in its nuclear division through a dedicated link between the system and its manufacturer. Once in the chemistry system, the intruder moved into the utility's nuclear engineering support network, accessed database entries, and altered audit logs to elude detection. Another utility increased access control on a dedicated line to a system integrator after it detected intrusion attempts.

5.1.4 Remote Maintenance and Administration

Many utilities are allowing operations and information systems personnel to access systems remotely for after-hours support. Generally, this is accomplished by configuring dial-up modems on the EMS network. Operations and support personnel can dial into the EMS network through these modem pools and log in to the EMS system. Once in, they can assist in troubleshooting, perform system administration functions, and, in some cases, operate EMS applications.

These dial-in links represent a point of access for electronic intruders. Although some utilities have taken measures to limit the operations that can be performed remotely or have further strengthened access control with token-based authentication systems, other utilities have only minimal protective measures in place.

5.1.5 Impacts

Regardless of the access point, once in the control system network, the intruder may crash the EMS system—a knowledgeable intruder can employ other, more subtle, options. For example, a sophisticated attacker could corrupt the databases, causing significant economic damage to the utility by disrupting billing operations. A knowledgeable intruder could issue false commands to the system—opening and closing relays, shutting down lines, and potentially affecting generation. An extremely knowledgeable attacker could manipulate the flow of data to the control center, causing the control center operators to respond to spurious indications. Fortunately, the technical skills and specific knowledge of an individual utility's applications and procedures limit this kind of attack to a very small number of potential attackers. Furthermore, most utilities can revert to manual coordination if all control center functions are lost—however, this is a costly measure for the utility.

5.2 SUBSTATION VULNERABILITIES

A substation serves as a clearinghouse for power as it is stepped down from the high voltages used to transmit the power across the service area and then directed to

distribution systems for delivery to residential and commercial customers. In an effort to provide higher service levels to customers and reduce staffing requirements, the electric power industry is automating substation operations with remote terminal units and a variety of intelligent electronic devices. An automated substation is depicted in Figure 7. Digital programmable breakers, switches, and relays are being produced by several manufacturers, and utilities are now using them in place of fixed, or manually set, devices Both the RTUs and the new automated devices are susceptible to electronic attack.

5.2.1 Digital Programmable Devices

By dialing into a port on a digital breaker, a utility engineer can reset the device or select any of six levels of protection. An electronic intruder who could identify the telephone

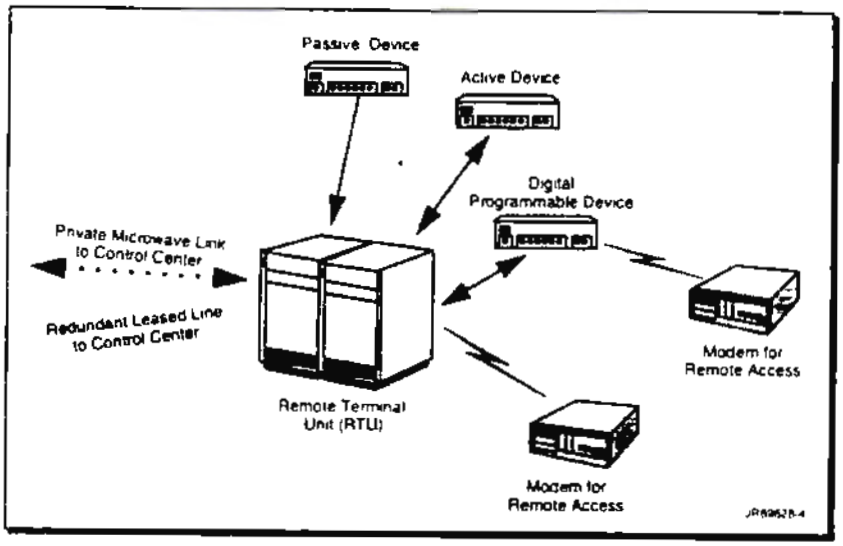


Figure 7: Typical Substation Interfaces

line serving such a device could dial into an unprotected port and reset the breaker to a higher level of tolerance than the device being protected by the breaker can withstand. By doing this, it would be possible to physically destroy a given piece of equipment within a substation. The intruder could also set the device to be more sensitive than conditions for normal operations and cause the system to shut down for self-protection. Several of the utilities visited did not have any type of security or access control on these dial-in devices. In either case, utilities reported that such an intrusion, capable of a major impact, would result in no more than a minor alarm.

5.2.2 Remote Terminal Units

Besides collecting data for the control center, an RTU operates as a clearinghouse for control signals to transmission and distribution equipment. A number of utilities reported having maintenance ports on substation RTUs that can be remotely accessed through a dial-up modem—some without even dial-back protection. An intruder could dial into this port and issue commands to the substation equipment or report spurious data back to the control center. Due to the highly networked nature of the power grid, knocking out an RTU can have a significant impact on any systems or customers "downstream" from the substation housing the RTU.

5.3 COMMUNICATIONS VULNERABILITIES

Utilities rely on a mix of private microwave radio, private fiber, and the public networks for communications among control system elements. Any one of these mediums could be exploited in an electronic attack. In most cases, an attack on the communications infrastructure alone would constitute a nuisance attack. In such an event, most utilities would equip personnel with cellular phones and mobile radios and dispatch them to key sites to report operating data back to the control center.

However, an attack on the communications infrastructure in conjunction with an attack on the electric power control system was characterized by one utility official as a "nightmare scenario." Restoring power would be extremely difficult and dangerous if all means of coordination between the control center and generation and transmission elements were lost.

5.3.1 Private Infrastructure Vulnerabilities

Microwave systems operating in the 2 and 6 gigahertz range and aerial or buried fiber optics make up the majority of utility private communications networks. Utilities view their private communications network as a key asset—several utilities stated that they would rather lose access to the public networks than to their private systems. In several cases, utilities sell excess capacity on these networks to commercial carriers, or plan to use these infrastructures to enter the telecommunications market.

A utility's private communications infrastructure is nearly as vulnerable to intrusion and physical attack as the public network. Utilities reported instances of theft of voice services, as well as the loss of voice and data service resulting from physical damage. One utility lost access to most of its private fiber network when a truck knocked down a pole at a critical juncture in the system. Microwave communications can be intercepted or jammed quite easily. There are multiple sites on the Internet with direction for assembling an inexpensive microwave jamming unit. One utility interviewed was experiencing severe disruption of its microwave communications system which it finally traced to frequency

spillover from a cellular service provider. Despite all of this, utilities seem to believe that because their private systems are isolated from the public networks, they are safe and secure.

5.3.2 Public Infrastructure Vulnerabilities

Roughly a third of the electric utility control communications traffic is carried on the PN. Most utilities use the PN to augment their private networks in the form of redundant communications lines to key substations, in geographically remote regions, or in "last mile" situations. Utilities appear to be aware of the threats to the PN and take risk mitigation measures on critical control links, such as requiring diverse routing in leased line contracts or providing for redundant transmission media. Several utilities reported that PN outages had isolated parts of their control networks and led them to increase private networking to key facilities.

It is worth mentioning that the single greatest source of interdependence between the electric power infrastructure and the PN is in their use of common rights-of-way. In many cases, public carriers lease spare conveyances or share transmission paths with utilities. In such a situation, a physical attack is more likely to disrupt multiple infrastructures than an electronic attack would.

6.0 PROTECTION MEASURES

Electric utilities use a variety of mechanisms to protect the electric power grid from disruption. The most significant measure is a double contingency analysis system, which uses a real-time simulator to look for the two worst things that could happen to the grid at any instant and offers operators corrective actions to consider and initiate. These "security" systems are powerful; however, the system does not look at elements beyond the power grid and is only as accurate as the data that it receives from the field. If the flow of this information from the field is cut off, the value of this system is reduced drastically.

Beyond actively monitoring the status of the power grid, most utilities have taken measures to guard their control centers and EMS systems from both physical attack and system failure. Practically all utilities have established back-up control centers—some collocated, others in separate facilities—that include uninterruptible power supplies and backup generators. Other utilities have installed completely redundant telecommunications facilities with their own telecommunications control center. In most cases, wherever the EMS interfaces with the outside world, utilities have installed dial-back modems and firewalls. Furthermore, most EMS systems support individual logins and passwords, and have extensive alarms and event logs.

Organizationally, all utilities have a robust physical security department, and most utilities have some information systems security function to handle the information security requirements for corporate systems. The corporate information system security office in conjunction with the internal auditing departments will generally conduct, or contract for, security evaluations and audits of corporate systems. But these audits rarely extend into the operational elements of the utility, and few utilities have an equivalent information security function for their operational control systems.

In an effort to improve security, utilities reported that they are considering a variety of improvements:

- Conducting intensive security evaluations and audits
- Ensuring dial access control (i.e., modem security)
- Using existing security features
- Eliminating security holes
- Evaluating and deploying new security technologies

- Improving coordination between operations staff and corporate information security staff
- Improving skills of the security staff
- Establishing security awareness programs.

However, utility personnel consistently stated that such investments were difficult to sell to senior managers, who were often unaware of, or skeptical of, the risks to their information systems. Many expressed concern that reduced operating margins would further threaten their ability to implement effective security. Forty percent of the respondents to the EPRI Summer 1996 Electronic Information Security Survey believed that internal priorities in a competitive environment were the most significant obstacle to maintaining a high level of information security.

7.0 POTENTIAL IMPACTS

The electric power grid is a complex, highly networked entity, whose elements are highly interdependent. A by-product of the highly networked power grid is the potential for a cascading power failure. When transmission capacity is unexpectedly lost, generation must immediately be taken off-line; otherwise, the generator's output will reroute and overload remaining transmission lines. This creates "voltage oscillations" that will ripple through the power grid. Unless corrective action is taken, these oscillations can pull down significant portions of the electric power grid.

The largest instance of such a widespread event was the famous New York City blackout of November 9, 1965, which knocked out power for up to 13 hours and affected 30 million people in eight States and Canada. More recently, on July 2, 1996, a cascading power failure in the Western Interconnect region affected 2 million customers in 14 States, Canada, and Mexico. Most customers had power restored within 30 minutes, but some did not regain service for over 6 hours. This situation was repeated on August 10, 1996, when all major transmission lines between Oregon and California were dropped. This outage affected 5.6 million users for up to 16 hours in 10 western States (see Figure 8).

Even regional outages can have wide-ranging effects. On May 14, 1996, an improper setting on a high-voltage circuit breaker at a single substation resulted in an 8-hour blackout affecting 290,000 customers through southern Delaware and across the eastern shores of Maryland and Virginia. Michael Conte, an economist at Towson State

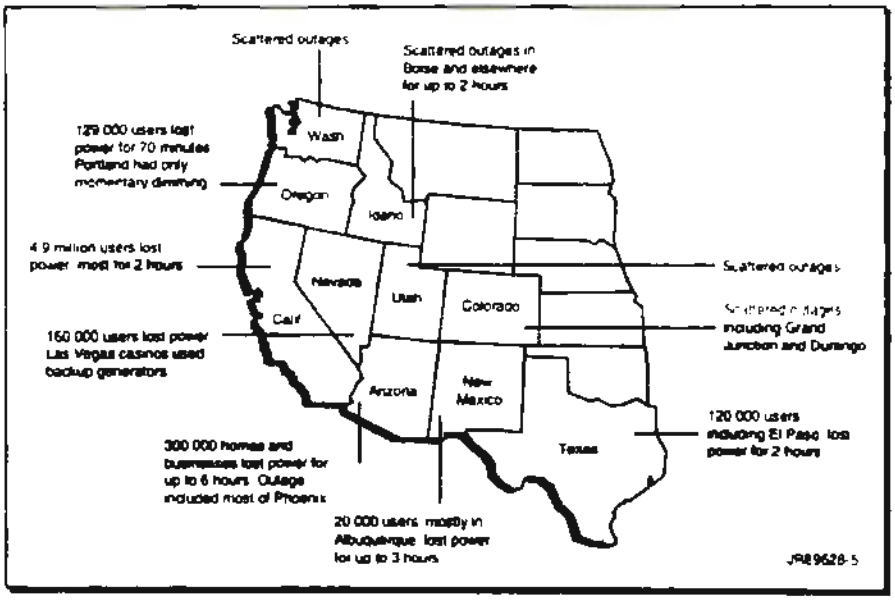


Figure 8: Effects of August 1996 Western Outage

University, estimated the loss for regional businesses to be as high as $30.8 million.[14]

These outages illustrate the tremendous effects a disruption of the electric power system can have on a given region. Significant portions of the U.S. economy and infrastructure are dependent on electric power, including, and certainly not limited to, transportation, financial services, health care, and telecommunications services. While many facilities have back-up generators, these systems are not foolproof and in many cases are not exercised on a regular basis. During these aforementioned outages, traffic lights stopped working, flight operations were suspended, schools were closed, and nuclear reactors were shutdown. In addition, a sewage treatment plant released six million gallons of sewage into the Pacific when electrically powered pumps stopped working.

Critical node analysis combined with an attack on poorly protected elements of substation automation systems can achieve effects equivalent to these recent outages. More than 50 percent of the electric utility personnel who responded to the EPRI survey believed that an intruder in the information and control systems at an electric utility could cause "serious impact on, or beyond, the region for more than 24 hours." Open sources, including FERC filings, electric industry publications, regional maps, and the Internet would provide enough information to identify the most heavily loaded transmission lines and most critical substations in the power grid. Relatively simple hacking techniques could then be used to locate dial-in ports to these points and modify settings to trigger an outage. Only a detailed review of logs or the elimination of all other factors would lead to the detection of such an attack.

[14]Humphrey, Theresa, "Power Outage Darkens Delmarva Peninsula," *The News-Times* (May 15, 1996)

8.0 CONCLUSIONS

The Electric Power Risk Assessment subgroup found no evidence of power outages attributed to deliberate electronic intrusion into utility control systems. The greatest risk facing the electric power infrastructure of the United States remains physical damage and destruction. Compared to the threat posed by natural disasters and physical attacks on electric power infrastructure elements, electronic intrusion represents an emerging, but still relatively minor, threat. However, changes within the electric power industry and in technology are increasing the risk posed by electronic intrusion.

As detailed in the preceding sections, the security of electric power control networks and information systems varies widely from utility to utility. In general, though, three trends will increase the exposure of electric power control networks to attacks and raise the probability of disruptions due to electronic intrusions.

- First, the shift from mainframe-based control applications relying on proprietary communications protocols to client-server applications using the Utility Control Architecture or other publicly documented protocols built on the transmission control protocol/Internet protocol (TCP/IP) expands the population of attackers with sufficient technical knowledge to attack these systems. This migration to client-server applications also introduces a potential for extended disruptions as the complexity of interactions continues to outpace the skills and tools of systems administrators.

- Second, the pressures to downsize, streamline, automate, and cut costs resulting from increased competition in the wholesale—and eventually, retail—power market will drive utilities to rely even more on remote automation, administration, and maintenance; on outside contractors for applications development and support; and on internetworking of control systems with corporate networks. Without a clear business case to support investments in information security, the relatively immature level of information assurance within the industry is likely to continue.

- Third, the requirement to provide open access to transmission system information dictated under FERC orders 888 and 889 introduces two new sources of exposure to attack—the interface to the OASIS host and new links required for the separate power marketing effort.

Having to post transmission system information on a World Wide Web server connected to the Internet requires utilities to establish some kind of interface between their EMS and the Internet. Although in all known cases this will be an indirect connection tightly controlled with firewalls, screened subnets, or proxy servers, the individual utility's

interface to its OASIS host creates a new and significant point of exposure. Apart from insider attacks, the Internet is the greatest potential source of information system attacks Utilities are, in many cases, relatively new to Unix and TCP/IP security, and the short timeline given for activating an OASIS site increases the opportunity for vulnerabilities to be introduced in the rush to meet FERC's deadline.

These rulemakings are forcing utilities to separate power marketing from transmission system management. These functions were formerly tightly integrated and operated on the unquestioned principle that system reliability always took precedence over economic profit. The procedures for resolving system problems between utilities were relatively informal, which was understandable given the consistency of operating philosophies and exposure to risk of the players involved.

At the information systems level, the separation of these functions is forcing utilities to disconnect networks and applications, often in the midst of already ongoing redesign efforts. Under great pressure to meet deadlines and minimize costs, information systems staffs may resort to workarounds that could ultimately introduce major vulnerabilities

At the operational level, it is not clear that the industry will be able to maintain the principles and procedures that have guided it for the past 30 years. Today, utilities resolve imbalances of generation, load, and transmission system capacity on a relatively informal basis, relying on phone coordination and recognized rules of conduct. In the new OASIS environment, this arrangement may not suffice, especially when transmission system operators may begin driving their lines further towards capacity.

At the industry level, these rulemakings will certainly lead to a major restructuring, as vertically integrated utilities spin off functional elements and a new set of players—power marketers, independent system operators, derivatives traders, retail power resellers—develops. The interactions of these businesses create new and unforeseen tensions, motivations, and risks. With vertically integrated utilities, the responsibility for the reliability of electric power was clear. The responsibility for reliability in a restructured industry is, for the moment, largely theoretical.

In sum, these trends suggest that, in the future, the electric power industry and its infrastructure will become more complex, and networks and information systems will play a major role in how individual utilities deal with the new business environment. As a result, electric power control networks will be exposed to a considerably wider range of attacks and potential attackers. Although the probability of a nationwide disruption of electric power through electronic intrusion will remain extremely low for any but a major structured attack, short-term disruptions up to the regional level may become easier to achieve—unless appropriate precautions are taken.

9.0 RECOMMENDATIONS

The recommendations of this study are directed toward three different groups—the President, the power industry, and the NSTAC. Each set of recommendations is further organized into three categories that reflect increasing levels of maturity in a program of information assurance:

- Awareness
- Information sharing
- Mechanisms for prevention, detection, response, and restoration.

Before effective mechanisms for coordinating information assurance activities between Government and industry can be established, there must be a consensus on the threats, risks, technical issues, business considerations, legal constraints, and other factors involved. This consensus cannot be established if the two parties disagree on whether a problem exists in the first place. For that reason, the recommendations aimed at increasing awareness of network and information systems security should be given first priority.

9.1 RECOMMENDATIONS TO THE PRESIDENT

9.1.1 Awareness

The President should consider assigning to the appropriate Department or Agency the mission to develop and conduct an ongoing program within the electric power industry to identify the threat and increase the awareness of vulnerabilities and available or emerging solutions. The program should be coordinated with other Departments, Agencies and advisory groups as appropriate to insure completeness and to maximize effectiveness.

9.1.2 Information Sharing

The President should consider establishing an NSTAC-like advisory committee to enhance industry-Government cooperation in light of significant regulatory changes affecting power generation, transmission, and distribution and the critical importance of electric power to National and Economic security, the government, and its citizenry. The committee should advise the head of the Department or Agency assigned the lead role for National Security and Emergency Preparedness (NS/EP) protection of the national electric power infrastructure. Such an advisory committee could perform a number of functions, to include the following:

- Provide information on factors affecting the reliability of the electric power infrastructure

- Provide the means for sharing information between Government and industry on potential electric power system faults, vulnerabilities and protection measures

- Provide a forum for recommending Government support activities to help ensure a highly reliable and available nationwide electric power capability

- Review existing or proposed legislation and advise the Government on the potential NS/EP implications for the electric power infrastructure.

9.1.3 Mechanisms for Prevention, Detection, Response, and Restoration

The Government should provide threat information and consider providing incentives for industry to work with government to develop and deploy appropriate security features for the electric power industry.

9.2 RECOMMENDATIONS TO THE POWER INDUSTRY

9.2.1 Awareness

Electric power associations, executive bodies, and individual organizations need to promote information systems security within the industry as a whole. With industry restructuring, and the interoperability of systems and networks, a lack of security in one element of the electric power industry could likely impact other providers or power transporters.

9.2.2 Information Sharing

Electric power associations should establish procedures for sharing sensitive information among member companies. This sensitive information might include threat and vulnerabilities; data security processes, procedures, tools, and techniques; and lessons learned.

9.2.3 Mechanisms for Prevention, Detection, Response, and Restoration

A secure network communications and computing environment will be important to the continued reliability of the electric power infrastructure. Security needs to be considered in communications and systems architectures and standards; in products that are purchased; and in employee methods, procedures, and training. Additionally, industry should consider establishing an electronic incident reporting and clearing function for electronic intrusions, similar to what is already done for power outages and physical attacks.

9.3 RECOMMENDATIONS TO THE NSTAC

9.3.1 Awareness

The NSTAC should reach out to the electric power industry and offer its support, expertise, and assistance in establishing an NSTAC-like capability. NSTAC should share past reports and recommendations to the President, provide advice on lessons learned throughout its tenure, and perhaps sponsor joint meetings to discuss common concerns.

9.3.2 Information Sharing

The NSTAC should invite representatives of the electric power industry to participate in open activities of the Network Security Information Exchange and appropriate meetings of the Information Assurance Task Force. In addition, NSTAC should actively foster opportunities for the exchange of information on protection technologies, attack trends, assurance programs, and other aspects of information security with industry associations.

9.3.3 Mechanisms for Prevention, Detection, Response, and Restoration

The NSTAC should consider the needs of the electric power control networks in its investigations of intrusion detection, indications and warnings, coordination mechanisms, and other elements of infrastructure assurance.