INEEL/EXT-04-01710

Introduction To SCADA Protection And Vulnerabilities

Ken Barnes
Briam Johnson

March 2004

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC

INEEL/EXT-04-01710

Introduction to SCADA Protection and Vulnerabilities

Ken Barnes
Briam Johnson

March 2004

Idaho National Engineering and Environmental Laboratory

Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Under DOE/NE Idaho Operations Office
Contract DE-AC07-99ID13727

CONTENTS

FIGURES

TABLES

ACRONYMS

AGC	Automatic Generation Control
ANSI	American National Standards Institute
CSI	Computer Security Institute
DOE	Department of Energy
EMS	Energy Management System
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas, Inc
FERC	Federal Energy Regulatory Commission
IEEE	Institute of Electrical and Electronics Engineers
INEEL	Idaho National Engineering and Environmental Laboratory
ISAC	Information Sharing and Analysis Center
ISO	Independent System Operator
NERC	North American Electric Reliability Council
NRC	Nuclear Regulatory Commission
OASIS	Open Access Same-Time Information System
RTO	Rural Transmission Organization
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition System

Introduction to SCADA Protection and Vulnerabilities

1. ELECTRIC UTILITY AND SCADA/EMS SYSTEM OVERVIEW

Even though deregulation has changed the landscape of the electric utility industry to some extent, a typical large electric utility still owns power generation facilities, power transmission and distribution lines, and substations. Figure 1 shows a block diagram of these components.

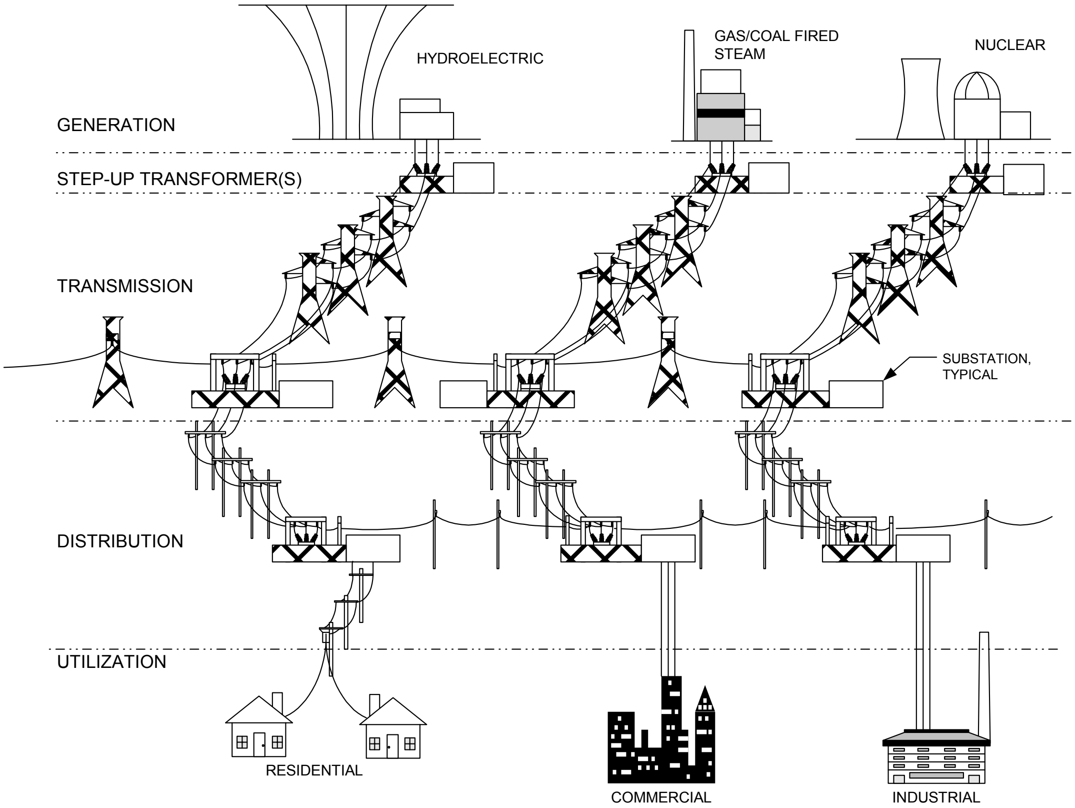


Figure 1. Utility block diagram.

Transmission and distribution lines form the segments or spokes of a utility's grid. Power flow may change through these lines, but control of the system occurs at the nodes of the grid, the generation facilities, and substations. This section discusses each of these node types in more detail as well as how each is controlled.

1.1 Power Generation

Although power supplying the grid comes from many sources, the majority of power is generated by large, investor-owned public utilities. Figure 2 shows the makeup of the types of utilities and the amount of power they provide.[1]

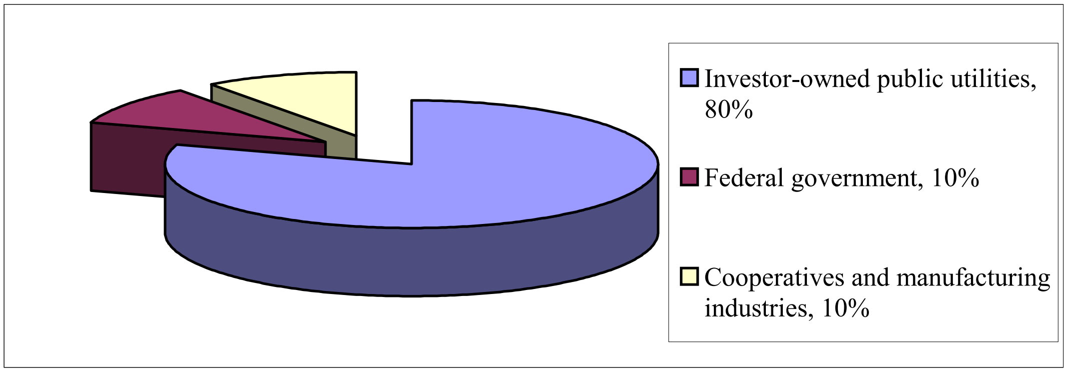


Figure 2. U.S. power providers.

Fuel for power generation in the U.S. also comes from several sources. The primary source is coal, accounting for more than 50% of the total generation. Nuclear power accounts for the next largest portion of power produced, at approximately 20%. Natural gas, hydroelectric, and petroleum round out the top five energy sources. Other sources, including renewables (wind, solar, geothermal, etc.), account for the remaining 2%. Figure 3 depicts these generation sources.[1]

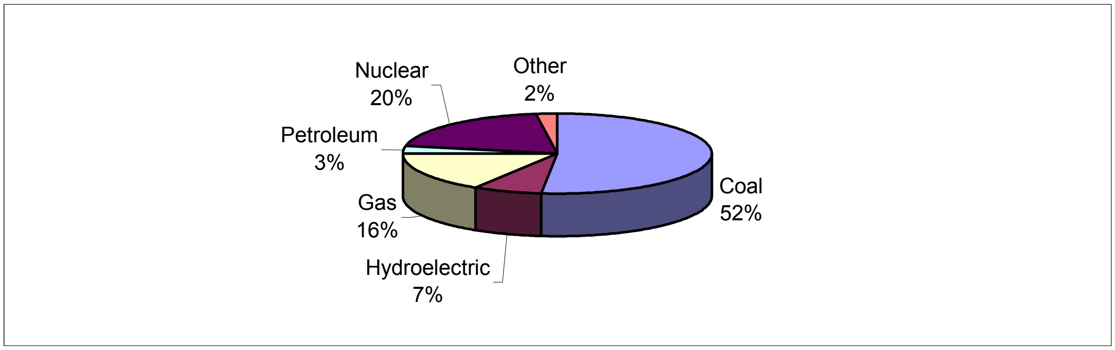


Figure 3. U.S. production by energy source – 2000.

Figure 4 shows a block diagram of a typical electric power plant. From a control standpoint, a large plant typically has a local, dedicated control system linked with a Supervisory Control and Data Acquisition System (SCADA) Remote Terminal Unit (RTU) via a communications link or by discrete inputs and outputs. The SCADA RTU receives status and power flow data from the plant and, depending on the power plant, may send control signals to increase or decrease power output based on the current load on the system and whether import/export of power from the system is required. The generator typically has one or more protective relays to prevent damage to the generator or system. Newer protective relays are microprocessor based, and one relay can incorporate all the functions necessary to protect the generator. With older electromechanical relays, several relays are required to perform the same function.

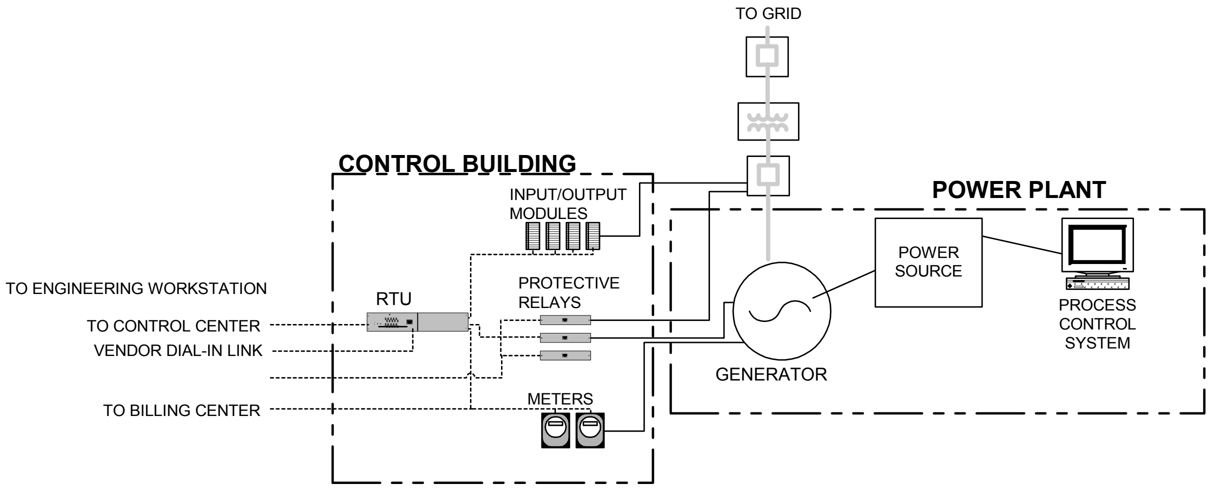


Figure 4. Generation plant block diagram.

1.1.1 Coal

The U.S. has one quarter of the world's coal reserves, which account for more energy content than all of the world's known oil reserves.[2] It is no surprise then, especially considering that most of it is close to the surface and easy to mine, that coal supplies more electrical energy than any other power source in the U.S. A typical coal-fired power plant has a dedicated process control system to manage fuel feed and combustion, emissions, and power output. Little data was found on the manufacturers of control systems in existing plants, but Bailey (now owned by ABB), Honeywell, and Foxboro are examples of companies that have traditionally supplied systems of this type.

1.1.2 Nuclear Power

There are currently 104 nuclear power plants in the U.S., 103 of which are operational. As mentioned above, these plants account for approximately 20% of the power generation in the U.S., or approximately 98,000 MW. All of these plants were built by one of four companies (Combustion Engineering, Babcock and Wilcox, Westinghouse, or General Electric) and fall into two types: pressurized water reactors or boiling water reactors. Like coal-fired plants, nuclear plants almost always have a local process control system for monitoring and controlling the plant. Some of the same companies that provide control systems for coal-fired plants also supply systems for nuclear power plants.

Commercial nuclear reactors are tightly controlled by the Nuclear Regulatory Commission (NRC). The NRC is responsible for codifying requirements and licensing plants, as well as performing regular inspections to ensure compliance with safety and security requirements. Nuclear plants are likely the most secure of any electric generation facilities. Plants are required to have dedicated security forces, and all employees must pass rigorous background checks.

Nuclear plants must comply with the design basis threat determined by the NRC. The design basis threat includes conceivable, credible attacks that could result in the release of radioactive contamination. The threat includes attacks by airplanes, trucks loaded with explosives, and many other scenarios. Plant security forces often perform force-on-force exercises to prove their resistance to such attacks.

1.1.3 Hydroelectric

Hydroelectric power is currently the largest renewable energy resource in the U.S. Much of this hydropower is operated and managed by the federal government through the Tennessee Valley Authority, Bureau of Reclamation, and Bonneville Power Administration. Although the generators and dams that make up this system are large, the controls for these systems are relatively simple. Water flow is the main control variable and this is usually determined by downstream water needs or a certain reservoir level, rather than electric power demand. Still, a large hydroelectric plant typically has its own dedicated control system. Smaller plants may have only an RTU to control the system.

1.1.4 Gas

Natural gas is the nation's fastest growing fuel for consumption and utilization. Gas is used for manufacturing, heating, and power production. During the last decade, the demand for natural gas increased 19% to levels that are difficult to sustain under current supply and production constraints. This demand growth has occurred despite improvements in energy efficiencies during the past several years. Total natural gas demand is projected to grow 50% during the next 25 years. Natural gas is likely to be a primary fuel for distributed power generators – mini-power plants that would be sited close to where the electricity is needed.

1.1.5 Petroleum

Petroleum is used in manufacturing, transportation, heating, and power generation. Only 3% is used in power production; the majority is used for transportation. Currently, it supplies more than 40% of the total energy demands and more than 99% of the fuel used in automobiles for the U.S.

1.2 Power Substations

There are many similarities between transmission substations and distribution substations, but a few differences as well. The following two sections describe their features, similarities, and differences.

1.2.1 Transmission Substations

Figure 5 shows a diagram of a somewhat typical transmission substation. Major power system components include circuit breakers, transformers, switches, and, possibly, capacitor banks. Major control and monitoring components include RTUs and their associated input/output modules, protective relays, and meters. Newer protective relays and meters are microprocessor-based and are often called intelligent electronic devices (IEDs).

RTUs interface with input modules to gather status data including circuit breaker open/closed status, transformer alarms, protective relay trip status, and other data. RTUs interface with outputs to control circuit breakers, switches, and transformer tapchangers. Depending on the size of the system and manufacturer, input/ouput modules can either be separate, standalone modules or cards that slide into the RTU.

Protective relays prevent damage to major equipment in the event of an abnormal condition such as a short circuit. These relays monitor each transformer in the substation as well as lines going to other substations or generation plants. For lines going to other substations or plants, a relay is required at each end, with communication between them so that if there is an abnormal condition, both ends of the line can be opened to remove it from service and prevent damage to equipment. Communications channels can be via phone line, microwave, fiber optics, pilot wire, power line carrier, or wireless technologies.

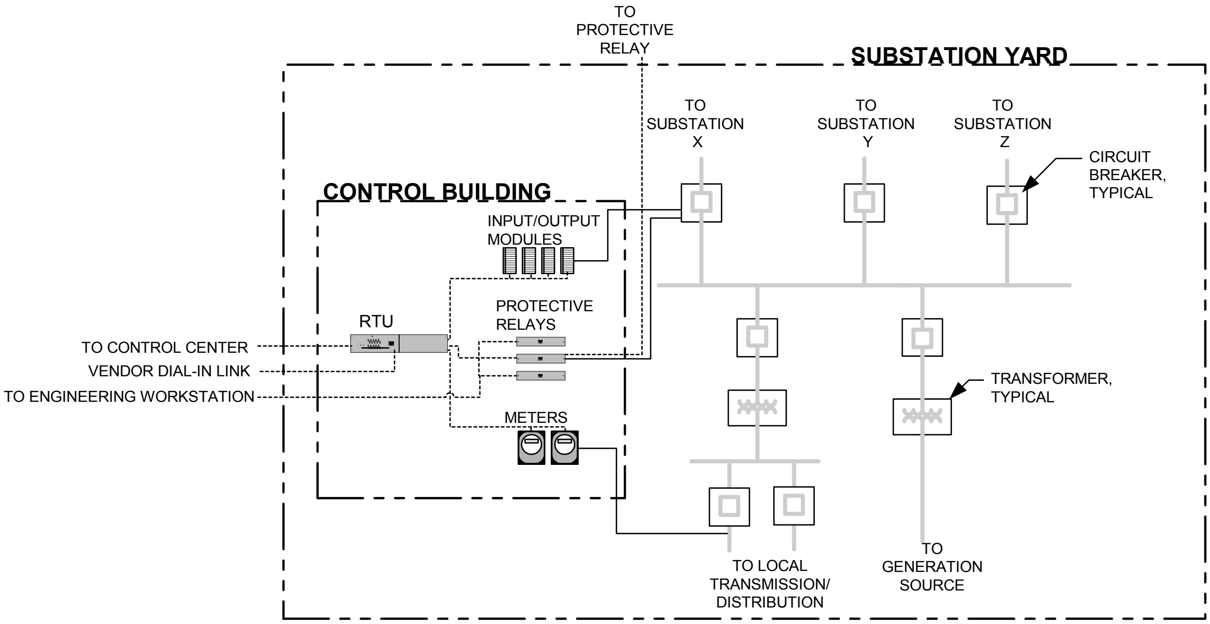


Figure 5. Typical transmission substation.

Newer relays not only communicate with each other, but have communications channels that are often tied into the RTU to gather metering data (line voltage, current, and power). They are also often tied into an engineering workstation so that engineers can access the relay if it trips a circuit breaker. The integration of protective relays into SCADA systems has raised the stakes, somewhat, with regard to cybersecurity. While utilities are able to operate their system if the SCADA system is taken out of commision, they are much less likely to operate their system without protective relays and risk damage to major, long-lead equipment. If an attacker breaks into a SCADA system and trips a breaker via an RTU, it can be closed again remotely. However, if an attacker gains access to a protective relay to trip a breaker, the relay often triggers a lockout relay that prevents a breaker from being closed again until the lockout is reset at the substation.

Meters at the transmission level are used to determine energy flowing into and out of a substation. This is particularly important when the energy is flowing out of a utility's system into another utility's system or vice-versa. Newer meters are connected to RTUs via a communications link; older meters are connected via analog channels.

1.2.1.1 Distribution Substations. Distribution substations are similar to transmission substations in that they have circuit breakers and transformers as their primary electrical components. From a control standpoint, they have RTUs, protective relays, and meters that perform basically the same functions as those used in transmission substations. There are a few differences, however. Figure 6 shows a typical distribution substation.

A distribution substation typically steps the incoming voltage from transmission levels down to medium voltage levels (2,400 to 69,000 volts) for utilization. Since lines at this level typically feed loads directly, protective relays typically do not have a communications link to another relay. These relays are also more likely to be the older, electromechanical type that do not have communications capability.

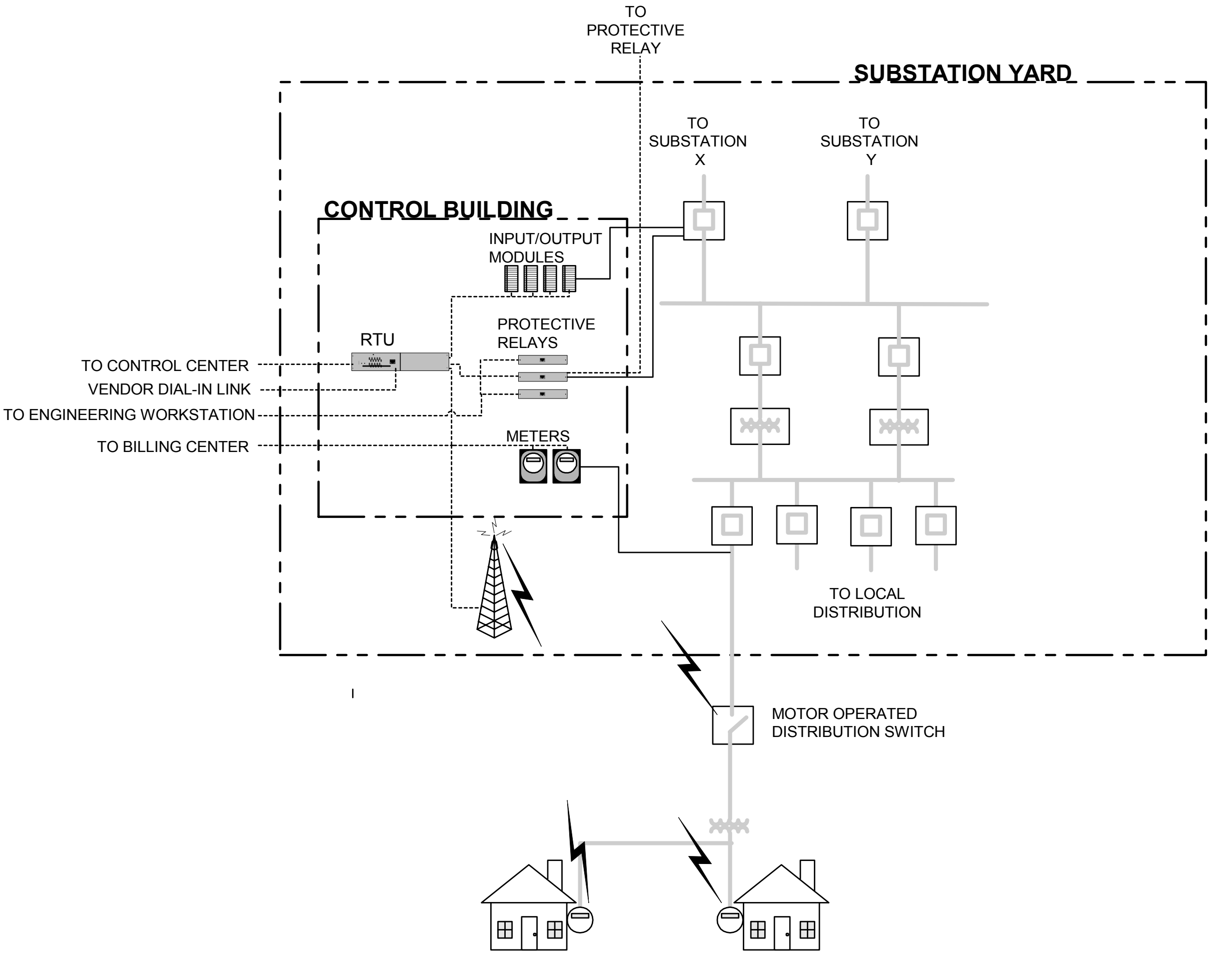


Figure 6. Typical distribution substation.

In recent years, automated meter reading and wireless control of distribution switches have become cost effective. Many utilities employ one or both of these functions to reduce manpower requirements and streamline operations. Automated meter reading gathers billing information via either a wireless or power-line-carrier communications link. The information is then uploaded to the utility's billing center, which may or may not be collocated with the control center. Automated pole-top distribution switches are typically controlled by a substation RTU via a wireless communications link. According to a recent survey, the popularity of these switches is increasing.[3] The survey shows that respondents had 3,823 of these switches currently installed, with plans to install 2,272 more. The additional communications channels provide more pathways for potential attackers to exploit.

1.2.2 Electric Utility Control Center

A centralized control and monitoring system is key to the operation and maintenance of a modern utility's generation, transmission, and distribution resources, as described in the previous sections. For most utilities, this system is housed in one or more control centers. Figure 7 shows a diagram of a control center typical of a large utility. For utilities serving many thousands or millions of customers, several of these control centers may be used to monitor regional portions of the system. Smaller utilities and rural electric cooperatives typically have a subset of the equipment shown in Figure 7. Components of the control center include the SCADA system, Energy Management System, and other application servers and/or workstations.

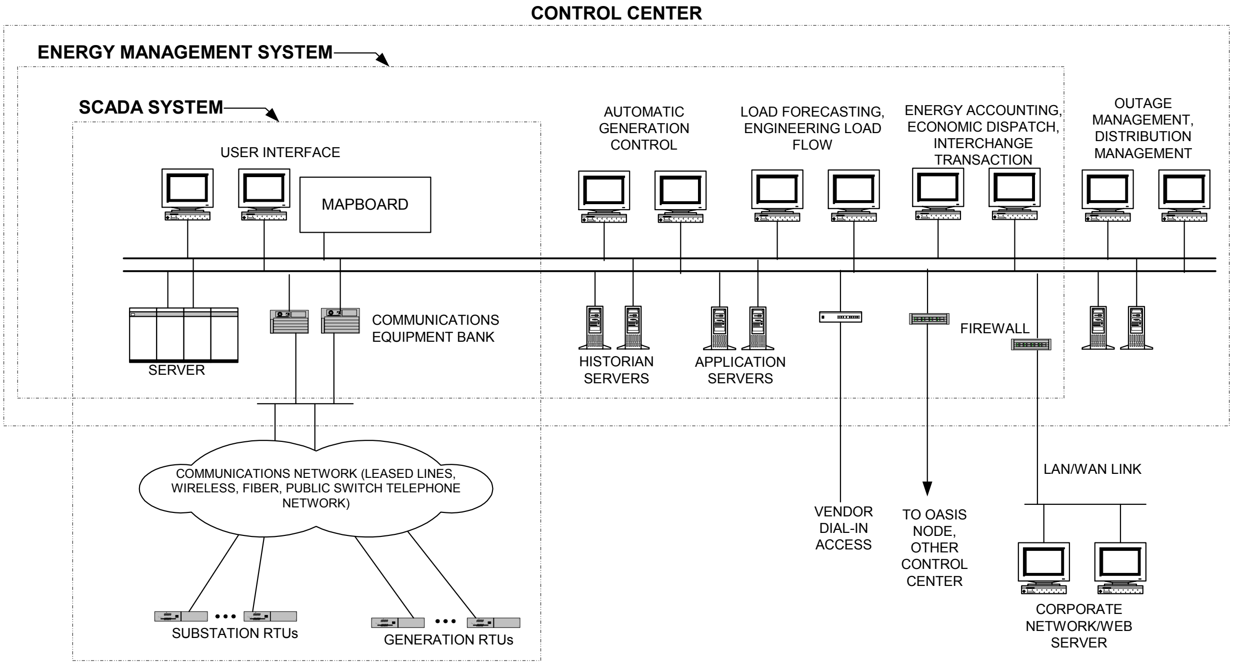

CONTROL CENTER
ENERGY MANAGEMENT SYSTEM
SCADA SYSTEM
USER INTERFACE
MAPBOARD
AUTOMATIC GENERATION CONTROL
LOAD FORECASTING, ENGINEERING LOAD FLOW
ENERGY ACCOUNTING, ECONOMIC DISPATCH, INTERCHANGE TRANSACTION
OUTAGE MANAGEMENT, DISTRIBUTION MANAGEMENT
SERVER
COMMUNICATIONS EQUIPMENT BANK
HISTORIAN SERVERS
APPLICATION SERVERS
FIREWALL
COMMUNICATIONS NETWORK (LEASED LINES, WIRELESS, FIBER, PUBLIC SWITCH TELEPHONE NETWORK)
LAN/WAN LINK
VENDOR DIAL-IN ACCESS
TO OASIS NODE, OTHER CONTROL CENTER
CORPORATE NETWORK/WEB SERVER
SUBSTATION RTUs
GENERATION RTUs

Figure 7. Typical utility control center block diagram.

Figure 8 shows a graphical depiction of a typical control center. A large control center is typically staffed by several operators, with each operator commonly dedicated to a portion of the system, such as transmission, distribution, or generation. The control center is often set up with separate areas for each of these functions.

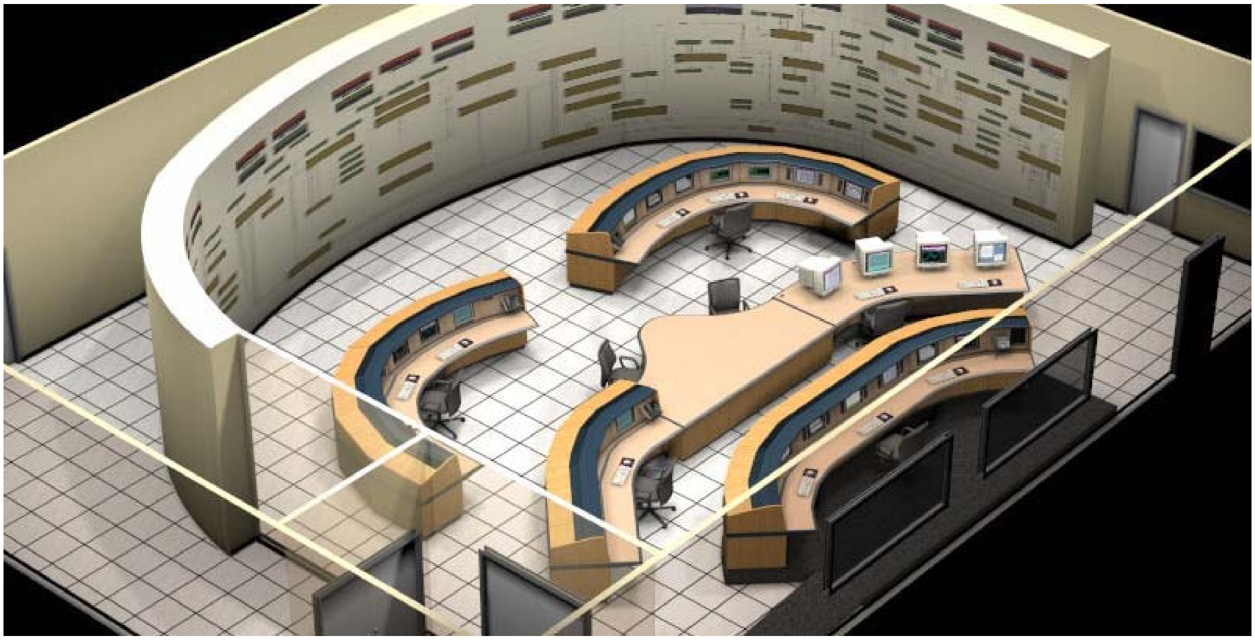


Figure 8. Typical utility control center.

1.2.2.1 SCADA System. SCADA is a term used in several industries fairly generically to refer to a centralized control and monitoring system. In the electric utility industry, SCADA usually refers to the basic control and monitoring of field devices, including breakers, switches, capacitors, reclosers, and transformers. As shown in Figure 7, a SCADA system includes data collection computers at the control center and RTUs in the field that can collectively monitor and control anywhere from hundreds to tens of thousands of datapoints. It also includes a user interface that is typically monitored around the clock. The user interface, in addition to one or more computer displays, usually includes a mapboard or large group displays to provide an overview of system status.

Also included in the SCADA system are the communications channels required to transmit information back and forth from the central computer(s) to the RTUs. The physical media used to create these channels typically consist of leased lines, dedicated fiber, wireless (licensed microwave or unlicensed spread spectrum radio), or satellite links.

1.2.2.2 *Energy Management System.* Most utilities have, in addition to a SCADA system, a computer system that coordinates and optimizes power generation and transmission. The system that performs this function is called an Energy Management System (EMS).

As shown in Figure 7, the EMS can include applications such as automatic generation control (AGC), load forecasting, engineering load flow, economic dispatch, energy accounting, interchange transaction, reserve calculations (spin and non-spin), and volts amps reactive (VAR)/voltage control.

AGC controls generation units in real time to maintain the system frequency at or very near 60 Hz. It also balances overall power generation with overall load. AGC is also used to import or export power from a utility's system. Increasing system frequency will cause power to be exported; decreasing frequency causes power to be imported.

Load forecasting uses real-time data like outside temperature and historical data to predict the load hours or days in advance. Economic dispatch is concerned with determining which generators should be operated, based on system load and fuel costs, among other things. Interchange transaction manages the import and export of power from a utility's system. The reserve calculation compares actual generator output to rated output in order to determine reserve. The spinning reserve counts only those generators currently online. The non-spinning reserve includes those generators that are currently offline.

Figure 9 shows the results of a survey of utilities regarding which EMS applications they currently use or have plans to use.[3]

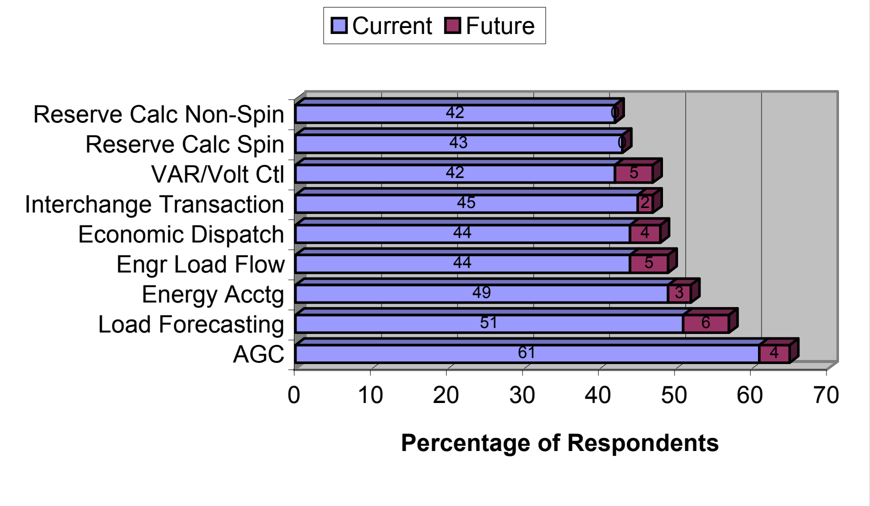


Figure 9. Current/future plans for EMS applications and functions.

1.3 SCADA Standards

No single standard covers all SCADA systems and applications. Many additional standards exist that discuss specific hardware and software components of SCADA systems, such as communication hardware, protocols, database compliance, and human machine interfaces. Some standards related to SCADA systems are summarized in Tables 1 through 4.

1.3.1 American National Standards Institute/Institute of Electrical and Electronic Engineers

Table 1. SCADA-related ANSI/IEEE standards.

Standard	Title	Description
ANSI C37.1	IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control	Contains useful definitions and features for SCADA systems.
IEEE 802.3	Standard for information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications	Standard describing requirements for twisted pair (10Base-T) ethernet
IEEE 999	IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Systems	Establishes recommended practices for master station equipment communications protocols to remote equipment
IEEE 1379	Recommended Practice for Data Communications between Remote Terminal Units and Intelligent Electronic Devices in a Substation	Provides implementation recommendations for the Distributed Network Protocol (DNP) 3.0 and IEC 60870-5-101 protocols in substations
IEEE 1402	Guide for Electric Power Substation Physical and Electronic Security	Provides recommendations and survey data for electronic and physical security of power substations

1.3.2 Electronic Industries Alliance/Telecommunications Industry Association

Table 2. SCADA-related Electronic Industries Alliance/Telecommunications Industry Association standards.

Standard	Title	Description
EIA/TIA-232-F	Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange	Contains requirements for serial communications standard typically referred to as RS-232

EIA/TIA-485-A	Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems	Contains requirements for serial communications standard typically referred to as RS-485

1.3.3 International Electrotechnical Commission

Table 3. SCADA-related International Electrotechnical Commission standards.

Standard	Title	Description
IEC 60870-5	Telecontrol equipment and systems - Part 5-101: Transmission protocols	Describes serial and network version of protocol upon which DNP 3.0 is based
IEC 60870-6	Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations	Describes TASE.2 protocol typically referred to as Intercontrol Center Communication Protocol (ICCP) in U.S.
IEC 61850	Communication networks and systems in substations	Describes protocol similar to UCA 2.0.

1.3.4 North American Electric Reliability Council

Table 4. SCADA-related North American Electric Reliability Council standards.

Standard	Title	Description
Urgent Action Standard 1200	Cyber Security	Temporary standard relating to cyber security for NERC members. Applies to computers, installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations. It does not apply to nuclear facilities.

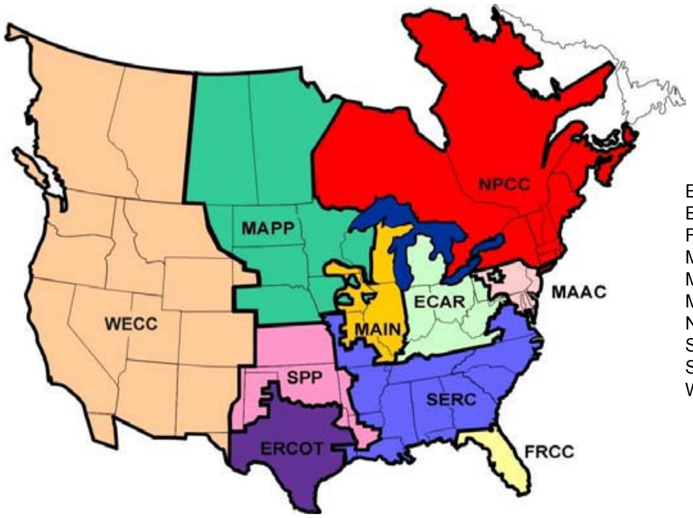
2. GOVERNMENT AND INDUSTRY AGENCIES AND ORGANIZATIONS INFLUENCING THE POWER INDUSTRY

Several regulatory and non-regulatory agencies, corporations, and institutions control and influence the generation, transmission, and distribution of power in the U.S. Two of the most visible are the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Council (NERC). Other organizations include the Department of Energy (DOE), Nuclear Regulatory Commission (NRC), Rural Electric Association (REA), Edison Electric Institute, the Electric Power Research Institute (EPRI), and the Utility Telecommunications Council.

2.1 North American Electric Reliability Council

The North American Electric Reliability Council (NERC) is a non-profit corporation that is primarily concerned with the reliability of electric power in North America. It was organized in 1968 following blackouts that left nearly 30 million people in the northeastern U.S. without power. NERC's members represent all segments of the electric utility industry, from rural electric cooperatives to large investor-owned utilities. Federal, state, and Canadian provincial utilities, power marketers, independent power producers, and some large-end users are also members. These members account for nearly all of the power generation, transmission, and distribution for the U.S, Canada, and portions of Mexico. Although membership in NERC is technically voluntary, nearly all entities that make up the North American grid are members and comply with the policies and standards generated by NERC.

NERC members are segmented geographically into ten Regional Coordinating Councils, as shown in Figure 10. Each of the councils provides input to the development of NERC policies and reliability criteria and oversees compliance among its members. It also serves as a planning resource for future system upgrades.



ECAR - East Central Area Reliability Coordination Agreement
ERCOT - Electric Reliability Council of Texas
FRCC - Florida Reliability Coordinating Council
MAAC - Mid-Atlantic Area Council
MAIN - Mid-America Interconnected Network
MAPP - Mid-Continent Area Power Pool
NPCC - Northeast Power Coordinating Council
SERC - Southeastern Electric Reliability Council
SPP - Southwest Power Pool
WECC - Western Electricity Coordinating Council

Figure 10. The 10 Regional Coordinating Councils of NERC.

NERC has been active in protecting electric utility systems. One of its subcommittees, the Critical Infrastructure Protection Advisory Group (CIPAG), is made up of industry experts in cyber, physical, and operational security, and works with DOE and the Department of Homeland Security to help ensure the security of the nation's supply of electricity.

According to Presidential Directive PDD-63, eight critical infrastructures exist in the U.S. Electric power is one of those eight infrastructures. Per the directive, each critical infrastructure is required to operate an Information Sharing and Analysis Center (ISAC). NERC is responsible for operating the ISAC for the electricity sector (ES-ISAC). The ES-ISAC website (www.esisac.com) provides information regarding current threat levels and incidents as reported by the Department of Homeland Security, tools to help in vulnerability assessments, and other information regarding security of electrical systems.[4]

2.2 Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) is the primary regulatory agency for the electric power industry, natural gas industry, oil pipelines, and non-federal hydroelectric projects.

Along with Congress, FERC has been instrumental in the deregulation of the power industry. Its landmark Orders 888 and 889, issued in 1996, provided open access to the nation's transmission grid. Order 888 required utilities to publish non-discriminatory tariffs for transmitting, or "wheeling," power over their transmission lines. Order 889 established the Open Access Same-Time Information System (OASIS). OASIS is a web-based computer system that provides real-time information regarding a utility's available transmission capacity and total transmission capability. These two orders opened the way for other utilities, independent power producers, power marketers, and others to purchase and deliver power regardless of who owns the transmission resources between buyer and seller.

Implementation of OASIS has not been uniform. In some cases, utilities have their own OASIS site. In the majority of cases, however, multiple utilities share an OASIS site; in several cases, one OASIS site serves an entire NERC region. Access to data on OASIS sites is also not uniform. PJM's OASIS node (website https://esuite.pjm.com/mui/index.htm), for instance, requires that a registration form be filled out, reviewed, and approved before access is granted. CAISO's node (website http://oasis.caiso.com), on the other hand, provides anyone who visits its website open access to information about existing conditions, load forecasts, and expected outages.

Subsequent to the issue of Order 889, FERC encouraged voluntary establishment of independent system operators (ISOs) among utilities. The primary purpose of creating ISOs was to ensure the non-discriminatory nature of open access. With an ISO, utilities would retain ownership of transmission resources but allow the ISO to manage these resources. Since the ISO is a non-profit organization operated independently of any single utility, it should, in theory, give non-preferential treatment to all buyers and sellers.

FERC, in its Order 2000, further defined the role of the transmission system administrators by calling for the creation of regional transmission organizations (RTOs). RTOs are similar to ISOs, but are more rigidly defined. Among the requirements for RTOs is that each RTO must have a single OASIS site that provides transmission availability for all of its members. Figure 11 shows current RTOs and the regions they cover. Note that some RTOs retained "ISO" in their name (e.g., California ISO) but fulfill the requirements of RTOs and function as such.

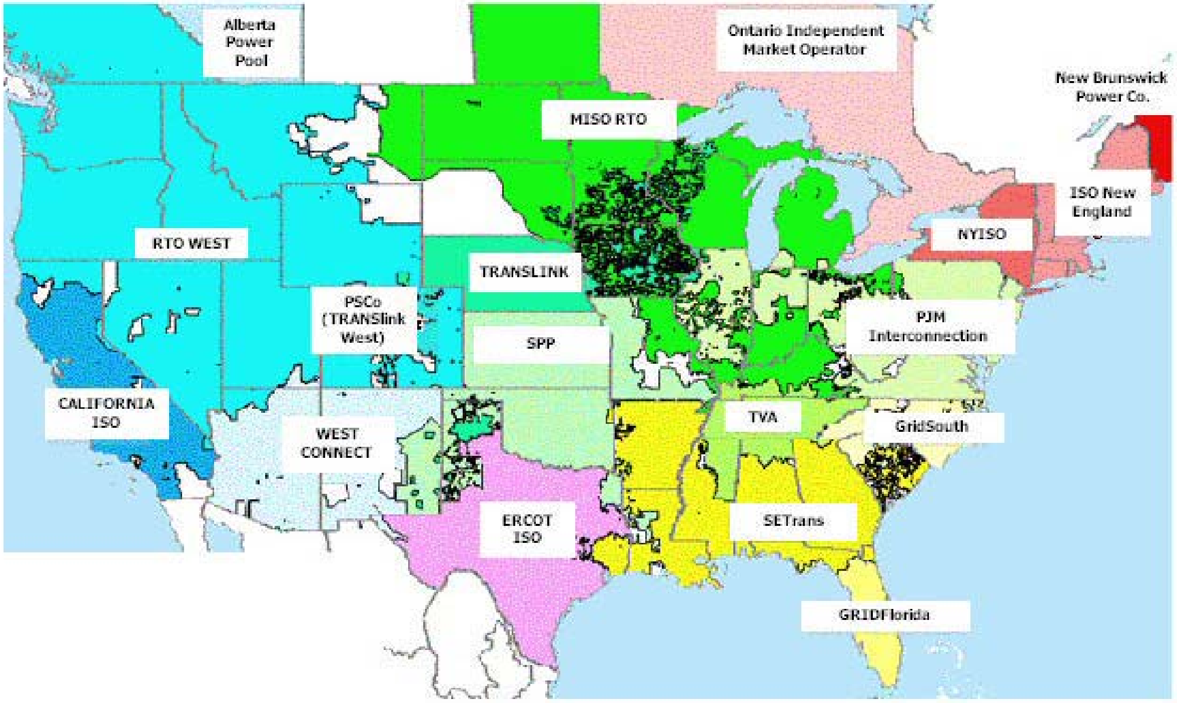


Figure 11. Current Regional Transmission Organizations (RTOs).

2.3 Other Organizations

In addition to FERC and NERC, there are many other organizations involved in various aspects of the electric power industry, including federal, state, and industry/other organizations. Following is a list of these organizations with a brief description of their purpose.[1]

- Federal

  - Department of Energy—provides basic research in energy-related fields, including generation, conversion, and emissions; provides basic research in national security; helps ensure reliable and affordable sources of energy; promotes renewable energy and conservation, helps shape energy policy

  - Department of Homeland Security—focuses on reducing terrorist vulnerabilities, preventing terrorist attacks, and minimizing damage from terrorist attacks and natural disasters. Disseminates information on terrorist threats as well as vulnerabilities

  - Environmental Protection Agency—oversees electric power transmission and distribution with regard to power plant emissions

  - National Institute of Standards and Technology—provides research into new security devices and methodologies, evaluates commercial security devices, administers the Process Control Security Requirements Forum (PCSRF)

    - Nuclear Regulatory Commission—oversees nuclear power generation, as well as transportation and production of nuclear fuels

    - Tennessee Valley Authority—America's largest public power company, with generation facilities that include 11 fossil plants, 29 hydroelectric dams, 3 nuclear plants, a pumped-storage facility, and 17,000 miles of transmission lines that serve more than 8 million customers

    - Bonneville Power Administration—Federal agency under DOE responsible for operating a transmission grid in the Northwestern U.S. and marketing power from 31 federally owned dams, one nuclear power plant, and a large wind energy program.

- State

    - State Public Utility Commissions—control rate structure for all municipal utilities, investor-owned utilities, and rural electric cooperatives.

- Industry/Other

    - Electric Power Research Institute—focuses on discovering, developing, and delivering technical advances in power technology through partnership with its membership of more than 700 utilities

    - Utility Telecommunications Council—represents telecommunications interests of electric, gas, and water utilities before Congress, the Federal Communications Commission (FCC), and other agencies

    - National Rural Electric Cooperative Association—represents investor-owned electric cooperative on issues affecting electric service industry and the environment

    - American Public Power Association—represents the interests of approximately 2,000 municipal and other state and locally owned public utilities before Congress, federal agencies, and courts. Disseminates information to member utilities

    - Edison Electric Institute—provides information exchange and develops informational resources and tools.

3. METHODS OF SCADA SYSTEM PROTECTION

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 received 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 of these centers are collocated; others are 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 was the most significant obstacle for maintaining a high level of information security.

Several tools are available to defend systems. These tools include passwords, firewalls, intrusion detection systems, virtual private networks, and access control. The following sections provide a brief description of each of these tools.

3.1 Passwords

Passwords can be an effective security method. Two factors that influence their effectiveness are strong passwords and encryption. Strong passwords are defined as passwords of six characters or more that do not form a pronounceable word, name, date or acronym, and have at least one special character or digit and one mixed-case character.[5] Table 5 shows a comparison of the time it takes a password cracking program to crack passwords of different lengths for strong passwords (require brute-force cracking) and dictionary passwords. Dictionary passwords in this case are based on the 25,143-word UNIX spell-check dictionary that contains words, numbers, common names, and acronyms. Strong passwords are based on a 90-character set of letters, numbers, and special characters.[5]

Table 5. Comparison of times to crack dictionary vs. strong passwords.

Attack	Number of Possibilities	2400 bps	9600 bps	19200 bps	38400 bps	10 Mbs
Dictionary Passwords						
4 char.	11,022	2.4 hr	1.9 hr	1.4 hr	1.3 hr	0.9 hr
6 char.	20,721	4.6 hrs	3.5 hr	2.7 hr	2.5 hr	1.7 hr
8 char.	23,955	5.3 hrs	4.0 hr	3.1 hr	2.9 hr	2.0 hr
Strong Passwords						
4 char.	66,347,190	14,707 hrs	11,168 hr	8,625 hr	7,961 hr	5,528 hr
6 char.	5.3741×10^{11}	13,598 yr	10,326 yr	7,975 yr	7,361 yr	5,112 yr
8 char.	4.3530×10^{15}	110,150,114 yr	83,647,831 yr	64,599,315 yr	59,630,136 yr	41,409,817 yr

As one can see from the table, strong passwords, especially those of six characters or longer, are almost impossible to crack using brute force methods. Of course, if a potential intruder can sniff a network and see the password in clear text, the strongest password is no better than a weak password. It is therefore important that passwords not be transmitted in clear text.

Several tools are available for password encryption for workstations and servers. Intelligent devices in substations, however, often do not support a full character set for passwords, nor do they support password encryption.

3.2 Firewalls

A firewall serves as a barrier to traffic crossing the boundary of a network. Firewalls allow only packets satisfying predetermined rules to get from outside a network to the inside or vice versa. Firewalls can be either standalone devices or software running on a computer. They are often set up with a buffer zone, or DMZ, between the protected network and the outside world. The DMZ allows web servers, for instance, to provide information to outside customers without having to get through the firewall. Standalone firewalls are manufactured by companies like Cisco Systems and Nokia. A simple software firewall called TinyFirewall is available to run on Microsoft Windows-based machines.

3.3 Intrusion Detection Systems

Intrusion detection systems are used to detect unauthorized use of a computer network. They can be set up to detect internal abusers, external abusers, or both. Intrusion detection systems fall into one of two categories: signature detection systems or anomaly detection systems. Signature detection systems match packets with known intrusion characteristics and, based on sensitivity settings, determine whether an attack is occurring. Anomaly detection compares system behavior with a profile of past behavior to determine whether an intrusion is taking place. Both system types require care in setting sensitivity, as well as monitoring of event logs.

3.4 Virtual Private Networks

Virtual private networks (VPNs) tunnel through open IP-based networks by encrypting data to provide a secure connection. VPNs can encrypt just the data packet payload or the whole packet, including the source and destination address. In the latter case, a new packet header with a new IP address is added. VPN devices, in this case, are matched so that each has a compatible address. Once a packet is received by a VPN device, the packet is decrypted and, if the entire packet was encrypted, the dummy address is stripped off. The packet is then routed to its proper destination. VPNs typically use the triple data encryption standard (3DES or triple DES) with 128- to 168-bit encryption. Vendors of these systems include Cisco Systems, Netgear, and Nokia.

3.5 Access Control

Access control can include the control of physical access to computer systems. It can also refer to electronic access. For electronic access, control measures are identified as one, two, or three factor authentication. The three factors are:

1. Something you have (e.g., ID card)

2. Something you know (e.g., password)

3. Something you are (e.g., fingerprint).

Obviously, the most secure authentication and access control would incorporate all three, but this is seldom the case in actual systems. Two-factor authentication is sometimes used, but single-factor authentication is still commonplace for many systems. RSA Security is a leader in two-factor authentication systems. According to the RSA website (www.rsasecurity.com), their SecurID cards are the most popular two-factor identification system in the world.

Biometrics is the term typically used to describe the third factor. Several methods are available that use biometrics to verify identity. Factors checked by various systems include fingerprints, retinas, iris, face patterns, hand geometry, signature, or voice recognition.[13] Although costs for these devices is decreasing, they do not appear to be used widely. Perhaps one of the reasons is that at least some of them are quite easy to spoof. According to a recent PC Magazine article, fingerprint scanners could be spoofed by simply breathing on the sensor, making the last fingerprint reappear. Some face recognition sensors could be spoofed by a still photo. Iris sensors could similarly be fooled by placing a photograph of a person's eye on someone else's face.[6] Newer products are addressing some of these problems but current biometric devices alone do not provide adequate protection.

3.5.1 Actual Usage of Defense Tools

Respondents to the Computer Security Institute (CSI)/FBI survey report use several tools to defend against attacks (see Figure 12). The most commonly used tools are anti-virus software, firewalls, access control, and physical security. Intrusion detection and encryption are also becoming more common. Most of the technologies in Figure 12 were discussed in the previous section or are fairly self-explanatory. One technology not discussed earlier but shown in Figure 12 is the PC Memory Card [PC Memory Card International Association (PCMCIA)]. The security feature of the PCMCIA card is its removable function. The card with its stored memory can be removed when not needed, thereby eliminating any pathway of attack. Reusable passwords, also shown in Figure 12, are static passwords that do not change on a regular basis.

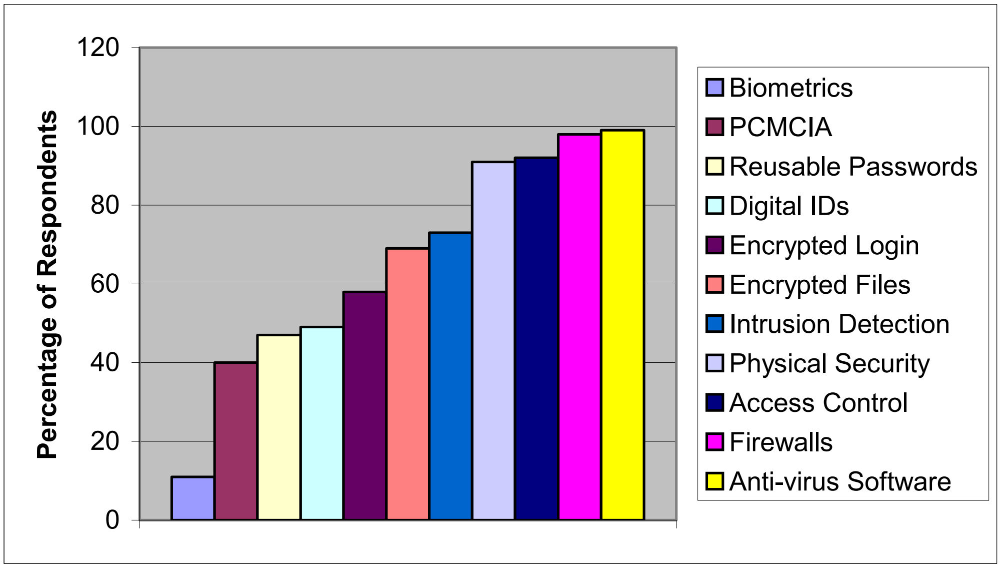


Figure 12. Security technologies used.

Information specific to electric utilities indicates that perhaps this industry is falling behind. According to the Newton-Evans report, use of defense tools among utilities lags well behind industry in general. Figure 13 shows that most respondents use passwords as a primary means of protection. Only 67% of the respondents use virus protection as compared to 99% in the CSI/FBI study.[7] Less than half of the respondents use any measure other than passwords and virus protection to defend against attacks.

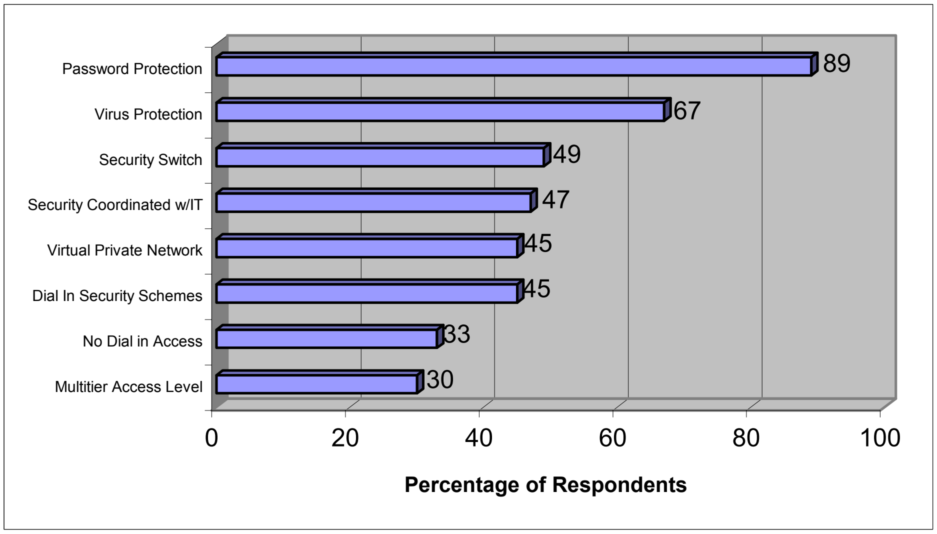


Figure 13. Approach utilization for reducing vulnerability on operational networks in the utility.

A trend that exacerbates the problem for utilities is the increasing use of the Internet for applications. Figure 14 shows current and planned implementation of applications using Internet technology. Notice that expansion in the use of the Internet is being planned for in every category. Of the respondents, nearly 40% either currently use the Internet for supervisory control (17%) or plan to do so (21%).

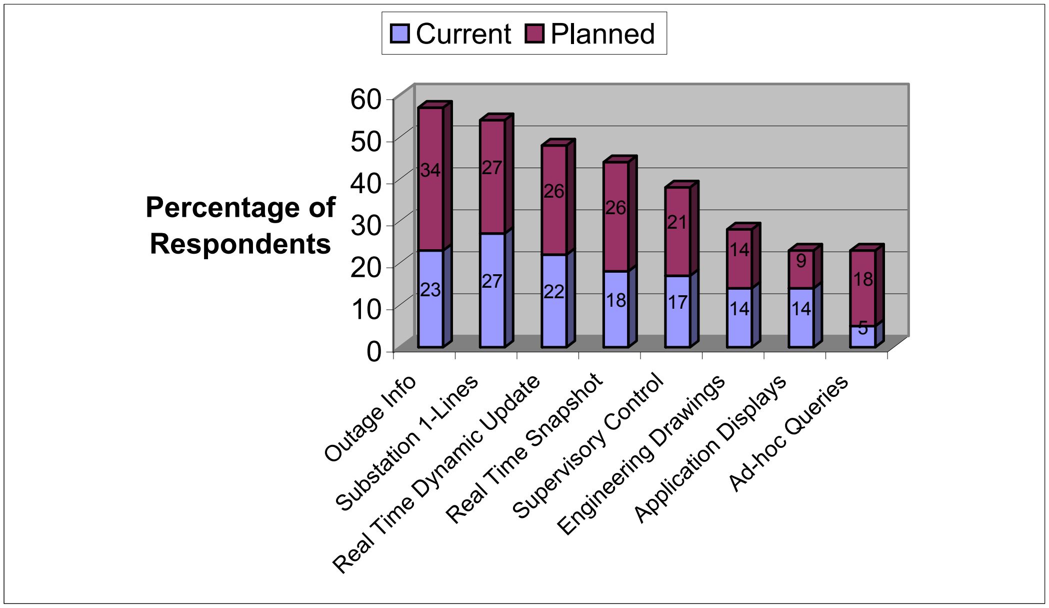


Figure 14. Current/future implementation of functions using Internet technology.

As mentioned previously, NERC has been involved with the security of electric utility systems. Its Urgent Action Standard 1200, which was issued in August 2003, is an attempt to standardize and enforce compliance with cybersecurity principles. The standard mandates that every entity involved with the generation, transmission, or distribution of electric power must perform the following steps:

1. Identify its critical cyber assets.

2. Identify its physical and electronic perimeters.

3. Implement physical and electronic access controls.

4. Monitor physical and electronic access.

5. Identify response actions for physical and electronic incidents.

6. Identify recovery plans in the case of an attack.

Urgent Action Standard 1200 does have limitations, however. It is only effective for one year (can be extended another year) and does not apply to all utilities or equipment in the grid. NERC is working on future standards that will be more encompassing, but approval of Urgent Action Standard 1200 will not happen quickly.

4. VULNERABILITIES

An organization's systems are most vulnerable at the point where the connectivity is the greatest and the access control is the weakest. 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. Potential access points include but are not limited to modem access, network access, wireless network, and power line. The following sections address the nature of each vulnerability, any trends affecting the vulnerability, and likely avenues of attack.[1]

4.1 Control Center Vulnerabilities

There is no "standard" control center system configuration. Systems 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, in order 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.

An electronic intruder can 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 of these interfaces.

4.1.1 Corporate Management Information System

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 their information systems to access control center data necessary for business purposes. One utility interviewed considered the business value of access to data within the control center worth the risk of open connections between the control center and the corporate network. More common solutions used include 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. Internet connectivity, modem pools, and individual modems can all 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, 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. They were surprised to learn about the experiences of the telecommunications industry where hackers had defeated these measures.

4.1.2 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. The creation of Independent System Operators (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.

4.1.3 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 the company’s products with a dial-in port allow the manufacturer’s engineering staff to connect to the system to perform software updates and 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.

4.1.4 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.

4.1.5 Impacts

Regardless of the access point, once in the control system network, the intruder can 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 to open and close relays, shutting down lines, and potentially affecting power 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, though a costly measure to take, most utilities can revert to manual coordination if all control center functions are lost.

4.2 Substation Vulnerabilities

A substation serves as a clearinghouse for power as it transforms high voltages used to transmit the power across the service area to lower voltages that are 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. 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.

4.2.1 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 identifies the telephone line serving such a device, could dial into an unprotected port and reset the breaker to a higher level of tolerance. 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 be indicated by nothing more than an alarm on a control system.

4.2.2 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.

4.3 Communications Vulnerabilities

Utilities rely on a mix of private microwave radio, private fiber, and 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.

4.3.1 Private Infrastructure Vulnerabilities

Microwave systems operating in the 2- and 6-gigahertz range and using 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 a public network. Utilities reported instances of theft of voice services, as well as the loss of voice and data services 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 that was finally traced to frequency spillover from a cellular service provider. Despite all of this, utilities have stated that their private systems are safe and secure because they are isolated from public networks.[1]

4.3.2 Public Infrastructure Vulnerabilities

Roughly one-third of the electric utility control communications traffic is carried on public networks. Most utilities use public networks 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 public networks 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 public network 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 public network is in the 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.

5. EXAMPLES OF CYBER ATTACKS

5.1 SCADA System Attacks

While there isn't a great deal of anecdotal evidence of SCADA system attacks, there are some examples. A Schweitzer Engineering Technical Paper, "Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems,"[5] gives three examples:

1. Hackers have attacked electric utilities' business and information systems.

2. In Texas a disgruntled ex-employee posted a note in a hacker journal that he had sufficient information to electronically attack the power grid.

3. A radical environmental group was caught trying to hack into a utility's information system.

Other stories have circulated as well. An oft-quoted example is that of a disgruntled ex-employee of a SCADA vendor who gained access to one of their customer's control systems via a wireless link and opened valves to dump raw sewage onto the grounds of a Hyatt Regency Hotel. He did this numerous times and in fact wasn't caught until the 46th occurrence.[8,9]

A story about a young teenager gaining access to the Roosevelt Dam's SCADA System has also circulated. However, cyber expert Joe Weiss of KEMA Consulting states that this story is a fabrication and never happened.[8,9]

The fact that there are not many publicly available examples of SCADA system break-ins does not mean they do not happen. The 2003 CSI/FBI Computer Crime and Security Survey provides an overview of the computer security methods used and types of attacks experienced by a cross-section of U.S. companies.[2] While this survey is not focused on the electric utility industry (only 4% of respondents were from utilities), it does provide a baseline for the types of attacks perpetrated and the damage done by unauthorized users. According to the CSI/FBI survey, approximately 56% of respondents reported unauthorized computer use in the past 12 months, slightly less than the numbers reported in the previous 4 years. Figure 15 shows the data gathered from 2003.

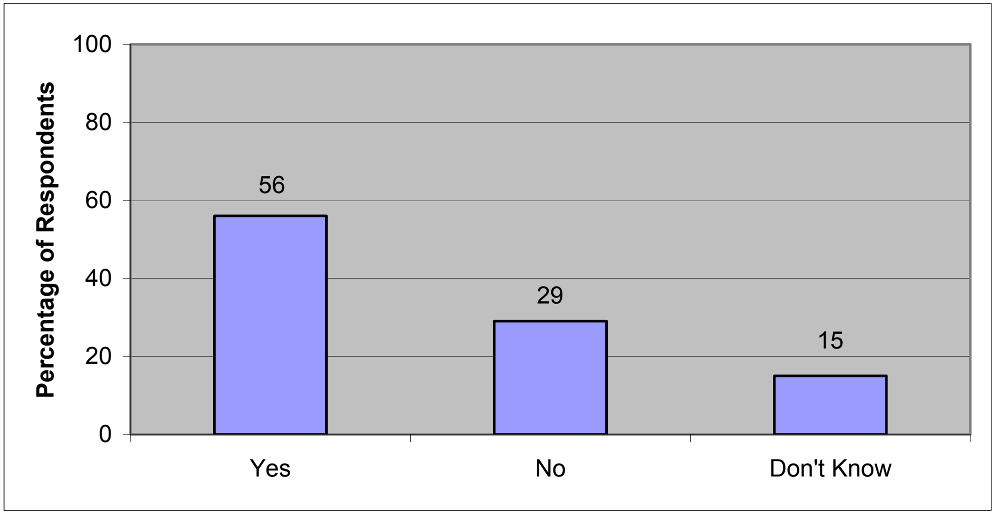


Figure 15. Unauthorized use of computer systems within the last 12 months.

The downward trend in reported attacks could be somewhat misleading. The report also shows an increasing trend toward not reporting unauthorized use of computer systems. Respondents cited fear of negative publicity or exploitation by competitors as primary reasons for not reporting. Figure 16 shows the actions taken by respondents when they were attacked.[7]

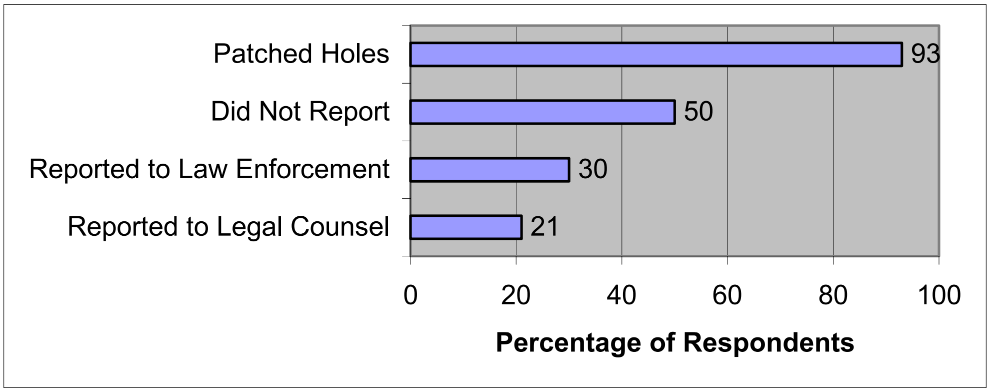


Figure 16. Response to cyber attacks.

Although documented evidence of attacks on utility systems is sparse, the threat is real. According to security firm Riptech (now owned by Symantec), 70% of their electric utility clients experienced at least one major attack in the first half of 2002, compared with 57% in the last half of 2001. Riptech also reports that when they try to penetrate a utility's network, they are successful 95% of the time.[10]

Types of attacks and/or misuse include viruses, laptop theft, net abuse, system penetration, denial of service, and others. Figure 17 shows types of attacks/misuse according to the CSI/FBI survey.[2] As one can see from the figure, viruses are the most common type of attack. According to the survey, several attack types show an increasing trend, including system penetration and denial of service. These two attack types, in addition to viruses, typically use the Internet as a source of attack. Indeed, the survey found an increasing trend toward Internet-based attacks, compared to inside attacks or remote dial-in (see Figure 18).[7]

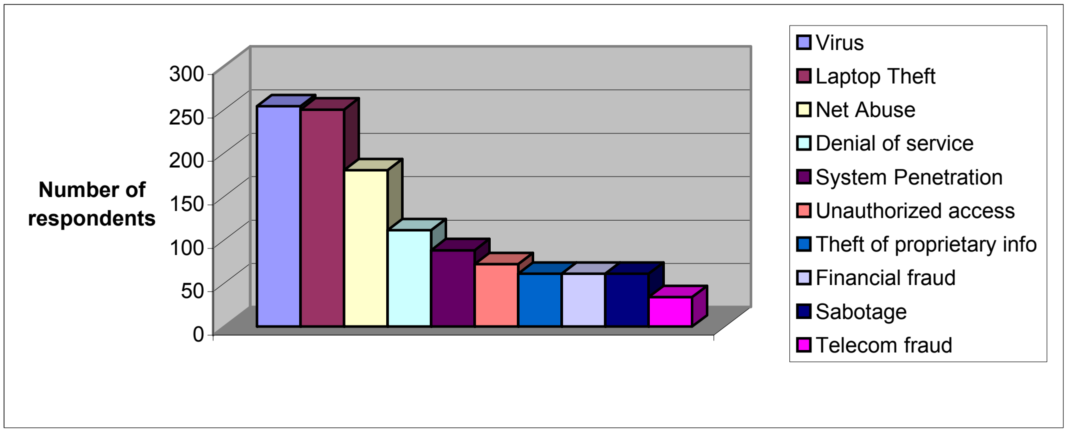


Figure 17. Types and cyber attacks/misuse.

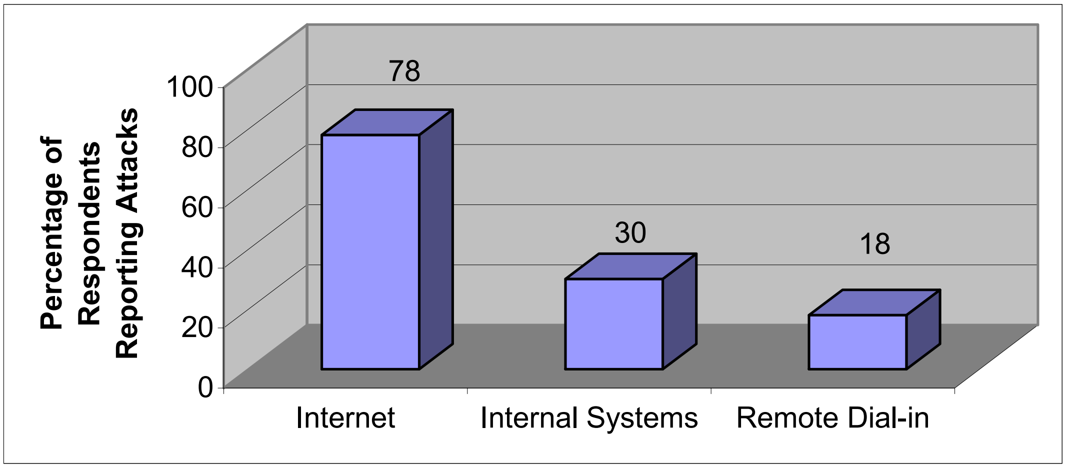


Figure 18. Communications media utilized for attacks.

Regarding types of attackers, survey respondents, as shown in Figure 19, pointed to independent hackers and disgruntled employees as the most common.[2] Domestic competitors, foreign corporations, and foreign governments were also identified as significant sources of attack. Since many attackers are not caught, it is not clear whether this data is based only on those who are caught or whether these numbers are based on conjecture by the respondents.

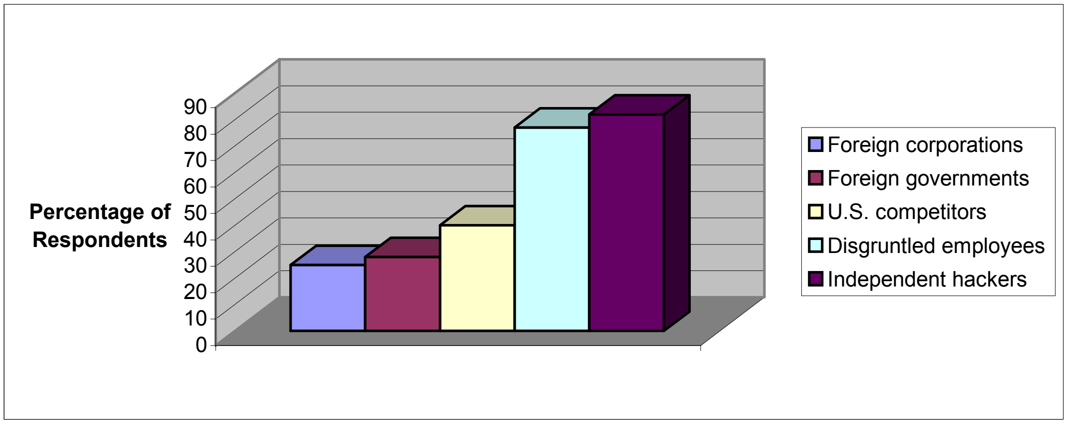


Figure 19. Types of cyber attackers.

5.2 General History of Computer Attacks

Following is a general history of computer milestones, viruses, and attacks as compiled in a recent Washington Post article.[11]

1945: Rear Admiral Grace Murray Hopper discovers a moth trapped between relays in a Navy computer. She calls it a “bug,” a term used since the late 19th century to refer to problems with electrical devices. Murray Hopper also coined the term “debugging” to describe efforts to fix computer problems.

1949: Hungarian scientist John von Neumann (1903-1957) devises the theory of self-replicating programs, providing the theoretical foundation for computers that hold information in their “memory.”

1960: AT&T introduces its Dataphone, the first commercial modem.

1963: Programmers develop the American Standard Code for Information Interchange (ASCII), a simple computer language that allows machines produced by different manufacturers to exchange data.

1964: AT&T begins monitoring telephone calls to try to discover the identities of “phone freaks,” or “phreakers,” who use “blue boxes” as tone generators to make free phone calls. The team's surveillance chief tells Newsweek magazine in 1975 that the company monitored 33 million toll calls to find phreakers. AT&T scores 200 convictions by the time the investigation ends in 1970.

1969: Programmers at AT&T's Bell Laboratories develop the UNIX operating system, the first multi-tasking operating system.

1969: The Advanced Research Projects Agency launches ARPANET, an early network used by government research groups and universities, and the forerunner of the Internet.

1972: John Draper, soon to be known as “Captain Crunch,” discovers that the plastic whistle in a box of breakfast cereal reproduces a 2600-hertz tone. With a blue box, the whistle unlocks AT&T's phone network, allowing free calls and manipulation of the network. Among other phreakers of the 1970s is famous future hacker Kevin Mitnick.

1972: Future Apple Computer co-founder Steve Wozniak builds his own “blue box.” Wozniak sells the device to fellow University of California-Berkeley students.

1974: Telenet, a commercial version of ARPANET, debuts.

1979: Engineers at Xerox Palo Alto Research Center discover the computer “worm,” a short program that scours a network for idle processors. Designed to provide more efficient computer use, the worm is the ancestor of modern worms—destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted.

1983: The FBI busts the “414s,” a group of young hackers who break into several U.S. government networks, in some cases using only an Apple II+ computer and a modem.

1983: University of Southern California doctoral candidate Fred Cohen coins the term “computer virus” to describe a computer program that can “affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself.” Anti-virus makers later capitalize on Cohen's research on virus defense techniques.

1984: In his novel, “Neuromancer,” author William Gibson popularizes the term “cyberspace,” a word he used to describe the network of computers through which the characters in his futuristic novels travel.

1986: One of the first PC viruses ever created, “The Brain,” is released by programmers in Pakistan.

1988: Twenty-three-year-old programmer Robert Morris unleashes a worm that invades ARPANET computers. The small program disables roughly 6,000 computers on the network by flooding their memory banks with copies of itself. Morris confesses to creating the worm out of boredom. He is fined $10,000 and sentenced to three years' probation.

1991: Programmer Philip Zimmerman releases “Pretty Good Privacy” (PGP), a free, powerful data-encryption tool. The U.S. government begins a three-year criminal investigation on Zimmerman, alleging he broke U.S. encryption laws after his program spread rapidly around the globe. The government later drops the charges.

1991: Symantec releases the Norton Anti-Virus software.

1994: Inexperienced e-mail users dutifully forward an e-mail warning people not to open any message with the phrase “Good Times” in the subject line. The missive, which warns of a virus with the power to erase a recipient's hard drive, demonstrates the self-replicating power of e-mail virus hoaxes that continue to circulate in different forms today.

1995: Microsoft Corp. releases Windows 95. Anti-virus companies worry that the operating system will be resistant to viruses. Later in the year, however, evolved “macro” viruses appear that are able to corrupt the new Windows operating system.

1998: Intruders infiltrate and take control of more than 500 military, government, and private sector computer systems. The incidents—dubbed “Solar Sunrise” after the well-known vulnerabilities in computers run on the Sun Solaris operating system—were thought to have originated from operatives in Iraq. Investigators later learn that two California teenagers were behind the attacks. The experience gives the Defense Department its first taste of what hostile adversaries with greater skills and resources would be able to do to the nation's command and control center, particularly if used in tandem with physical attacks.

1999: The infamous “Melissa” virus infects thousands of computers with alarming speed, causing an estimated $80 million in damage and prompting record sales of anti-virus products. The virus starts a program that sends copies of itself to the first 50 names listed in the recipient's Outlook e-mail address book. It also infects Microsoft Word documents on the user's hard drive, and mails them out through Outlook to the same 50 recipients.

2000: The “I Love You” virus infects millions of computers virtually overnight, using a method similar to the Melissa virus. The virus also sends passwords and usernames stored on infected computers back to the virus's author. Authorities trace the virus to a young Filipino computer student who goes free because the Philippines has no laws against hacking and spreading computer viruses. This spurs the creation of the European Union's global Cybercrime Treaty.

2000: Yahoo, eBay, Amazon, Datek, and dozens of other high-profile Web sites are knocked offline for up to several hours following a series of so-called “distributed denial-of-service attacks.” Investigators later discover that the DDOS attacks—in which a target system is disabled by a flood of traffic from hundreds of computers simultaneously—were orchestrated when the hackers co-opted powerful computers at the University of California-Santa Barbara.

2001: The “Anna Kournikova” virus, promising digital pictures of the young tennis star, mails itself to every person listed in the victim's Microsoft Outlook address book. This relatively benign virus frightens computer security analysts, who believe it was written using a software “toolkit” that allows even the most inexperienced programmer to create a computer virus.

2001: The Code Red worm infects tens of thousands of systems running Microsoft Windows NT and Windows 2000 server software, causing an estimated $2 billion in damages. The worm is programmed to use the power of all infected machines against the White House Web site at a predetermined date. In an ad hoc partnership with virus hunters and technology companies, the White House deciphers the virus's code and blocks traffic as the worm begins its attack.

2001: Debuting just days after the September 11 attacks, the “Nimda” virus infects hundreds of thousands of computers around the world. The virus is considered one of the most sophisticated, with up to five methods of infecting systems and replicating itself.

2001: Melissa virus author David L. Smith, 33, is sentenced to 20 months in federal prison.

2002: The “Klez” worm—a bug that sends copies of itself to all of the e-mail addresses in the victim's Microsoft Outlook directory—begins its march across the Web. The worm overwrites files and creates hidden copies of the originals. The worm also attempts to disable some common anti-virus products and has a payload that fills files with all zeroes. Variants of the Klez worm remain the most active on the Internet.

2002: A denial-of-service attack hits all 13 of the “root” servers that provide the primary roadmap for almost all Internet communications. Internet users experience no slowdowns or outages because of safeguards built into the Internet's architecture. But the attack—called the largest ever—raises questions about the security of the core Internet infrastructure.

2003: The “Slammer” worm infects hundreds of thousands of computers in less than three hours. The fastest-spreading worm ever wreaks havoc on businesses worldwide, knocking cash machines offline and delaying airline flights.

6. REFERENCES

1. President's National Security Telecommunications Advisory Committee, Information Assurance Task Force, *Electric Power Information Assurance Risk Assessment*, March 1997.

2. Department of Energy (see website http://www.doe.gov/engine/content.do?BT_CODE=COAL)

3. Newton-Evans Research Company, Worldwide Market Survey of SCADA, Energy Management Systems and Distribution Management Systems in Electrical Utilities: 2003-2005, Volume 1, North American Market, June 2003.

4. North American Electric Reliability Council (see website www.nerc.com)

5. Paul Oman, Edmund O. Schweitzer III, Deborah Frincke, "*Concerns about Intrusions into Remotely Accessible Substation Controllers and SCADA Systems,*" 27th Annual Protective Relay Conference, Paper #4, 2000: http://www.selinc.com.

6. Glass, Brett, "*Biometric Security,*" PC Magazine, January 20, 2004.

7. Computer Security Institute/Federal Bureau of Investigation, *2003 Computer Crime and Security Survey*, 2003.

8. Gellman, Barton, "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," Washington Post, June 27, 2002 p. A01.

9. Lemos, Robert, "Cyberterrorism: The Real Risks," CNET News.com, August 27, 2002.

10. Green, Sian. 2002, *REPORT: Cybersecurity—Prime Targets*, Power Engineering International, August 2002.

11. Krebs, Brian. *"A Short History of Computer Viruses and Attacks,"* Washington Post, Friday, February 14, 2003.