INEEL/EXT-04-01517

Review Of Supervisory Control And Data Acquisition (SCADA) Systems

Ken Barnes
Briam Johnson
Reva Nickelson

January 2004

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC

INEEL/EXT-04-01517

Review of Supervisory Control and Data Acquisition (SCADA) Systems

Ken Barnes
Briam Johnson
Reva Nickelson

January 2004

Idaho National Engineering and Environmental Laboratory

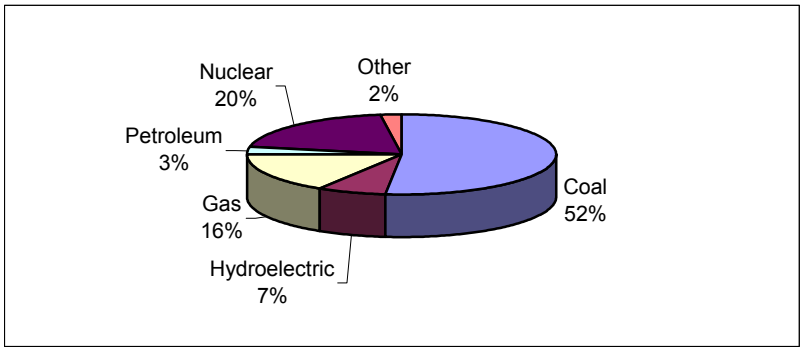
Idaho Falls, Idaho 83415

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

SUMMARY

A review using open source information was performed to obtain data related to Supervisory Control and Data Acquisition (SCADA) systems used to supervise and control domestic electric power generation, transmission, and distribution. This report provides the technical details for the types of systems used, system disposal, cyber and physical security measures, network connections, and a gap analysis of SCADA security holes.

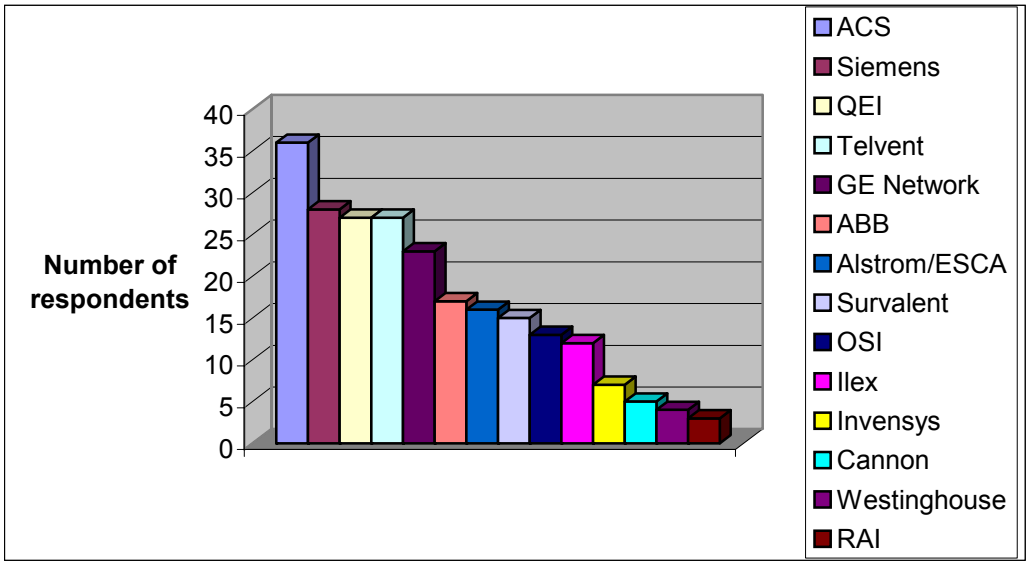
The United States has three transmission power grids, which are comprised of public, private, and government-owned utilities and rural and municipal cooperatives. Eighty percent of the power is generated by investor-owned public utilities. Domestic power generation comes from several sources as shown below.



SCADA systems come in a myriad of types, sizes, and applications. There are many SCADA system manufacturers and most provide a multitude of SCADA systems. Following is a table of major manufacturers and current, major SCADA systems.

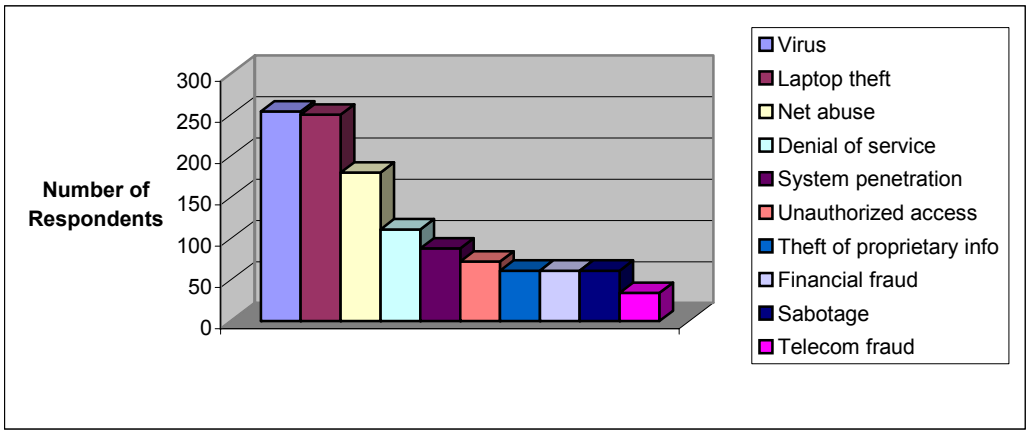
Manufacturer	Current SCADA
ABB	Process Portal A/Operate IT, Ranger
Advanced Control Systems (ACS)	Prism
Alstom	ESCA
C3-Ilex	EO SCADA
Citect	CitectSCADA
Foxboro	Invensys I/A series
GE Fanuc Automation	iFix 32
GE Network Solutions	XA21, Swift
Honeywell	Smart Distributed System
Metsoautomation (formally Neles)	metsoDNA
Motorola	MOSCAD
Open Systems International (OSI)	Monarch
QEI, Inc	TDMS-2000
Siemens	PowerCC EC and SIMETEC PCS 7

A survey[2] of more than 200 SCADA, Energy Management System (EMS), and Distributed Management System (DMS) owners was performed to determine the vendor representation for the respondent installations. The following figure provides the results.

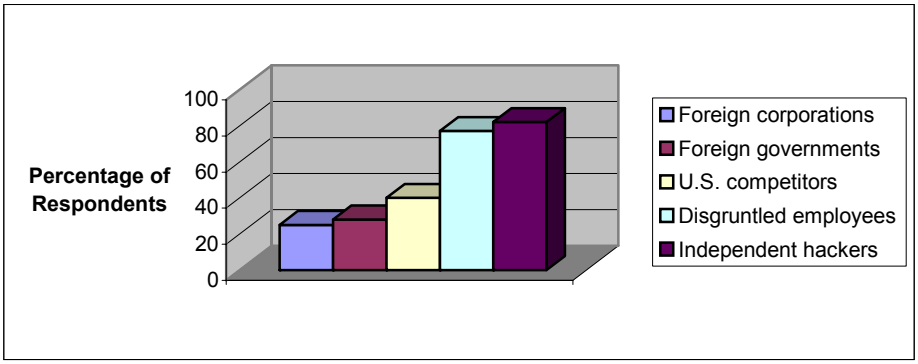


The average life of a SCADA system is typically 8 to 15 years. This long life is due to the time- and capital-intensive process required to replace the systems. There is almost no aftermarket for SCADA hardware except in the nuclear industry. Substation and control center hardware, once removed, is typically discarded or stored indefinitely in a warehouse or back room.

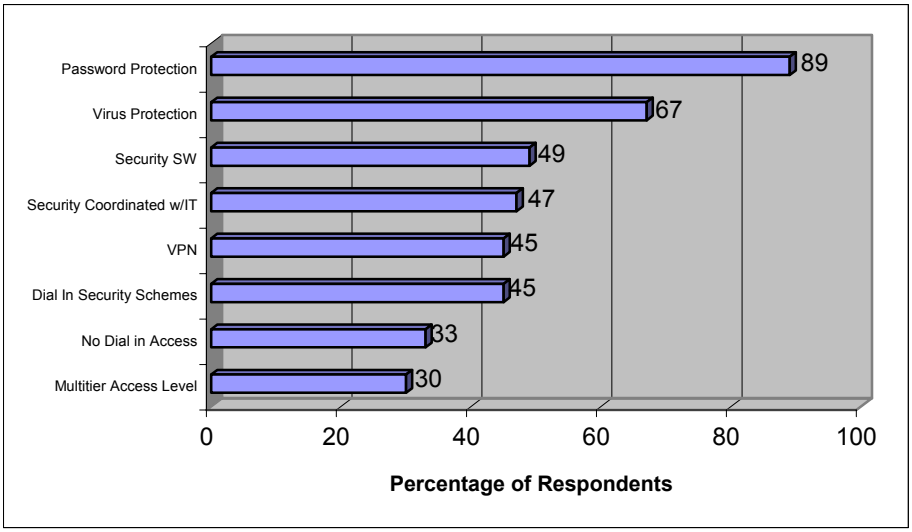
Cyber attacks have become a reality for many companies, and electric utilities are no exception. According to the security firm Riptech, 70% of their electric utility clients experienced at least one major attack in the first half of 2002, compared to 57% in the last half of 2001. Riptech also reports that when they try to penetrate a utility's network, they are successful 95% of the time.[6] The following figure shows the types of cyber attacks experienced by more than 398 respondents in 2003.[7]



The majority of attacks are internet-based, followed by internal system-based and remote dial-in.[7] Cyber attacks are coming from a variety of sources as shown below.[7]



A number of cyber security measures are used to defend against attacks. The following figure shows the results of a survey to more than 200 utilities for the types of cyber security measures they currently employ.[2]



Physical security at electric power substations varies from installation to installation depending on level of risk, level of impact, and cost of implementation. IEEE Standard 1402-2000, "IEEE Guide for Electric Power Substation Physical and Electronic Security,"[5] contains examples of physical barriers, electronic barriers, and other security measures. Examples of physical barriers include fences, walls, and locks. Examples of electronic barriers include photo-electric/motion sensing, video surveillance systems, building systems, computer security systems, passwords, dial-back verification, selective access, virus scans, encryption, and encoding. Utilities also use other types of security measures, such as lighting, landscaping, buildings, patrols, communications, and internal and external information restrictions.

The architecture of large electrical SCADA systems is moving towards distributed processing. EMS tends to be large and require many network interfaces. Typical EMS applications include Automatic Generation Control

(AGC), load forecasting, energy accounting, outage management, Sequence of Events (SOE), etc. The architecture of smaller electrical systems tends to be more simplified and contains fewer network connections such as servers, operator interfaces, Remote Terminal Units (RTUs)/Programmable Logic Controllers (PLCs), and Intelligent Electronic Devices (IEDs). The SCADA network is formed when the clients, servers, and RTUs/controllers communicate using some type of protocol and network connections.

Modern SCADA systems typically have multiple network connections. Network connections for SCADA systems can be subdivided into two general categories: "Outside" and "Inside." Inside connections refer to connections within the system; outside connections refer to connections from one SCADA or EMS system to another. Network connections may consist of modem, leased lines, optic microwave, radio, or direct network connections. The most popular protocol within a substation is Distributed Network Protocol (DNP) 3.0. For outside SCADA network connections, the most popular protocol is Intercontrol Center Communication Protocol (ICCP).

There has been considerable focus recently on cyber security of the electrical power grid, but there is still much to be done. Some of the outstanding needs are:

1. Develop security methods that work well with low bandwidth communications channels in real-time control networks.
2. Integrate better security into substation devices, including RTUs and IEDs.
3. Develop testing criteria for control systems to ensure to the extent possible that vulnerabilities do not exist.
4. Perform real-world testing on live or test systems to isolate and mitigate vulnerabilities of integrated systems.
5. Incorporate cyber security into the most widely used SCADA protocols (e.g., DNP and ICCP).
6. Streamline patch management of control systems.
7. Reduce potential consequences of cyber attack by strengthening the power grid.
8. Develop standards that apply to all systems and components critical to the operation and maintain continued reliability of the electrical power grids.
9. Invest in intelligence on the configuration of potential adversarial systems.
10. Invest in the development of smart systems that in the event of a cyber attack would either alert and block the attack (defense) or alter the attack depending on system configuration (offense).

FOREWORD

The Idaho National Engineering and Environmental Laboratory (INEEL) has unique capabilities related to Supervisory Control and Data Acquisition (SCADA) systems and operations, and is recognized by the Office of Energy Assurance as the SCADA Testbed within the Department of Energy (DOE) complex. The INEEL Testbed is one of the first SCADA test beds; the National Infrastructure Simulation and Analysis Center provides modeling and other laboratories supporting the SCADA Testbed. INEEL staff support the design, development, and operations of SCADA systems for internal and external customers. As a national SCADA resource, the INEEL can be relied on by DOE, other government agencies, and industry for expert information, science, development, or recommendations.

This report summarizes information obtained on SCADA systems and operations within the infrastructure of the United States. Types of SCADA systems reviewed include those for electric power generation, electric power transmission, electric power distribution, and process control. A two-fold process was used to obtain this intelligence. First, information was gathered regarding the types of infrastructure components, uses, interdependencies, access methods, etc. Second, analyses were performed on this information to determine commonalities, gaps, vulnerabilities, and risks.

The scope of this report includes:

1. An overview of SCADA equipment and uses (see Section 2).

2. Major manufacturers, vendors, and software for SCADA systems used to supervise and control domestic electric power generation, electric power transmission, electric power distribution, and various process systems. Vendors for SCADA systems and an overview of the current usage of these systems are provided (see Section 3).

3. A discussion of average/expected service life of domestic SCADA systems, after-market use of SCADA equipment, and methods used by industry to dispose of SCADA equipment (see Section 4).

4. Types of cyber security measures used by industry and industry's perceptions of what cyber security measures are necessary (see Section 5).

5. Types of physical security measures used by industry and industry's perceptions of what physical security measures are necessary (see Section 6).

6. Network connections normally used by domestic SCADA systems and the security protocols used between inside and outside connections (see Section 7).

7. A gap analysis that identifies current holes in the security of SCADA systems (see Section 8).

CONTENTS

SUMMARY iii

FOREWORD vii

1. INTRODUCTION 1

1.1 Purpose 1

1.2 Scope 1

2. Electric Power Industry Overview 1

2.1 Overview of U.S. Power Grid 2

2.2 Key Industry Players 3

2.2.1 North American Electric Reliability Council 3
2.2.2 Federal Energy Regulatory Commission 4
2.2.3 Other Organizations 5

2.3 Electric Utility Overview 6

2.3.1 Power Generation 7
2.3.2 Power Substations 9
2.3.3 Electric Utility Control Center 12

2.4 SCADA Standards 14

2.4.1 American National Standards Institute/Institute of Electrical and Electronic Engineers 14
2.4.2 Electronic Industries Alliance/Telecommunications Industry Association 15
2.4.3 International Electrotechnical Commission 15
2.4.4 North American Electric Reliability Council 16

3. SCADA MANUFACTURERS AND VENDORS 17

3.1 SCADA Hardware and Operating Systems 17

3.2 SCADA Evaluation Process 18

3.3 SCADA Vendors 20

4. SCADA EXPECTED LIFE AND DISPOSAL 23

5. ELECTRONIC SECURITY 24

5.1 Attacks 24

5.2 Attack Tools 26

5.2.1 Password Crackers 26
5.2.2 War Dialers 26
5.2.3 Ping Sweep and Port Scan Programs 26
5.2.4 Packet Sniffers and Protocol Analyzers 27
5.2.5 Denial of Service Tools 27

5.3 Attack Scenarios 27

5.4 Defense Tools 27

5.4.1 Passwords 28
5.4.2 Firewalls 28
5.4.3 Intrusion Detection Systems 28
5.4.4 Virtual Private Networks 29
5.4.5 Access Control 29
5.4.6 Actual Usage of Defense Tools 29

6. PHYSICAL SECURITY 32

6.1 Physical Security 32

6.2 Effectiveness of Security Methods 32

7. NETWORK CONNECTIONS AND PROTOCOLS 34

8. GAP ANALYSIS 37

9. REFERENCES 39

FIGURES

Figure 2-1. The three U.S. transmission interconnections. 2
Figure 2-2. The 10 Regional Coordinating Councils of NERC. 3
Figure 2-3. Current Regional Transmission Organizations (RTOs). 5
Figure 2-4. Utility block diagram. 7
Figure 2-5. U.S. power providers. 7
Figure 2-6. U.S. production by energy source – 2000. 8
Figure 2-7. Generation plant block diagram. 8
Figure 2-8. Typical transmission substation. 10
Figure 2-9. Typical distribution substation. 11
Figure 2-10. Typical utility control center block diagram. 12
Figure 2-11. Typical utility control center. 12
Figure 3-1. Choices of acceptable operating systems. 17
Figure 3-2. SCADA CPU platforms. 18
Figure 3-3. Vendor representation for respondent installations for SCADA, EMS, and DMS systems. 21
Figure 3-4. Vendors likely to be considered for future EMS procurements. 21
Figure 5-1. Unauthorized use of computer systems within the last 12 months. 24
Figure 5-2. Response to cyber attacks. 24
Figure 5-3. Types of cyber attacks/misuse. 25

Figure 5-4. Communications media utilized for attacks. 25
Figure 5-5. Types of cyber attackers. 26
Figure 5-6. Security technologies used. 30
Figure 5-7. Use of approaches for reducing vulnerability on operational networks in the utility. 30
Figure 5-8. Current/future implementation of functions using internet technology. 31
Figure 7-1. Current/future choice of protocol from substation to external EMS/SCADA/DMS network. 35
Figure 7-2. Current/future choice of protocol from substation to external EMS/SCADA/DMS host network. 35
Figure 7-3. Communications protocols used/planned to use to communicate between RTO/ISO systems. 36

TABLES

Table 2-1. SCADA-related ANSI/IEEE standards. 14
Table 2-2. SCADA-related Electronic Industries Alliance/Telecommunications Industry Association standards. 15
Table 2-3. SCADA-related International Electrotechnical Commission standards. 15
Table 2-4. SCADA-related North American Electric Reliability Council standards 16
Table 3-1. Minimum SCADA test requirements. 19
Table 3-2. List of SCADA manufacturers and their current SCADA system. 20
Table 5-1. Comparison of times to crack dictionary vs. strong passwords. 28
Table 6-1. Three sample electric power utilities and implementation of IEEE Std. 1402-2000 32
Table 6-2. Results of security survey on effectiveness of security methods 33

ACRONYMS

AGC	Automatic Generation Control
ANSI	American National Standards Institute
CORBA	Common Object Request Broker Architecture
DC	Direct Current
DCS	Distributed Control System
DMS	Distributed Management System
DNP	Distributed Network Protocol
DOD	Department of Defense
DOE	Department of Energy
EMS	Energy Management System
ERCOT	Electric Reliability Council of Texas, Inc
FTP	File Transfer Protocol
ICCP	Intercontrol Center Communications Protocol
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
INEEL	Idaho National Engineering and Environmental Laboratory
ISO	Independent System Operator
NERC	North American Electric Reliability Council
NISAC	National Infrastructure Simulation and Analysis Center
NRC	Nuclear Regulatory Commission
NTP	Network Time Protocol
OASIS	Open Access Same-Time Information System
PLC	Programmable Logic Controller
REA	Rural Electric Association
RTO	Rural Transmission Organization
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition System
SOE	Sequence of Events
TCP/IP	Transmission Control Protocol/Internet Protocol
T&D	Transmission and Distribution
WAN	Wide Area Network

DEFINITIONS

The following definitions are used throughout this report.

- ANSI C37.1 defines **SCADA** as a system operating with coded signals over communication channels so as to provide control of Remote Terminal Unit (RTU) equipment. The supervisory system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of RTU equipment for display or for recording functions.

- ANSI C37.1 defines **Remote Terminal Unit (RTU)** as the entire complement of devices, functional modules, and assemblies that are electrically interconnected to affect the remote station supervisory functions. The equipment includes the interface with the communication channel but does not include the interconnecting channel. During communication with the master station the RTU is the subordinate in the communication hierarchy.

- ANSI C37.1 defines **protocol** as a strict procedure required to initiate and maintain communication.

- ANSI C37.1 defines **Intelligent Electronic Device (IED)** as any device that incorporates one or more processors with the capability to receive or send data/control from, or to, an external source (e.g., electronic multifunction meter, digital relays, controllers).

- An **Energy Management System (EMS)** houses the utility systems databases, operational applications and displays, and report-generation functions. An EMS consists of a SCADA system, automatic generation control (AGC) system, applications and database, and a user-interface system.

- A **Server** consists of computer hardware and software that communicates with many devices on the SCADA network. Servers can be set up such that they provide redundancy. Servers store the SCADA information that is presented using other applications.

- A **Router** consists of hardware and software that when programmed, allows communication to flow (or not to flow) in configured networks.

- A **firewall** consists of hardware and software that allows communication from devices “inside” the firewall to communicate with devices “outside” the firewall. It is typically programmed to prevent communication from outside the firewall to inside the firewall unless pre-configured security requirements are met.

Supervisory Control and Data Acquisition (SCADA) Support and Development Program

1. INTRODUCTION

1.1 Purpose

This report summarizes information obtained on SCADA systems and operations within the infrastructure of the United States. Types of SCADA systems reviewed include those for electric power generation, electric power transmission, electric power distribution, and process control. A two-fold process was used to obtain this intelligence. First, information was gathered regarding the types of infrastructure components, uses, interdependencies, access methods, etc. Second, analyses were performed on this information to determine commonalities, gaps, vulnerabilities, and risks.

1.2 Scope

The scope of this report includes:

- An overview of SCADA equipment and uses (see Section 2).
- Major manufacturers, vendors, and software for SCADA systems used to supervise and control domestic electric power generation, electric power transmission, electric power distribution, and various process systems. Vendors for SCADA systems and an overview of the current usage of these systems are provided (see Section 3).
- A discussion of average/expected service life of domestic SCADA systems, after-market use of SCADA equipment, and methods used by industry to dispose of SCADA equipment (see Section 4).
- Types of cyber security measures used by industry and industry's perceptions of what cyber security measures are necessary (see Section 5).
- Types of physical security measures used by industry and industry's perceptions of what physical security measures are necessary (see Section 6).
- Network connections normally used by domestic SCADA systems and the security protocols used between inside and outside connections (see Section 7).
- A gap analysis section that identifies current holes in the security of SCADA systems (see Section 8).

2. Electric Power Industry Overview

This section provides an overview of the U.S. power grid, discusses organizations involved in various aspects of the electric power industry, and provides an overview of SCADA standards.

2.1 Overview of U.S. Power Grid

The electric power grid in the U.S. is made up of more than 3,000 public, private, and government-owned utilities and rural and municipal cooperatives. Physically, the power grid is separated into three nearly autonomous transmission grids: the eastern interconnection, the western interconnection, and the Electric Reliability Council of Texas, Inc. (ERCOT) (see Figure 2-1). Because each of these grids operates asynchronously with respect to the others, power cannot be interchanged directly among them. There are a few direct current (DC) links that connect the grids, but for the most part each of them operates independently.

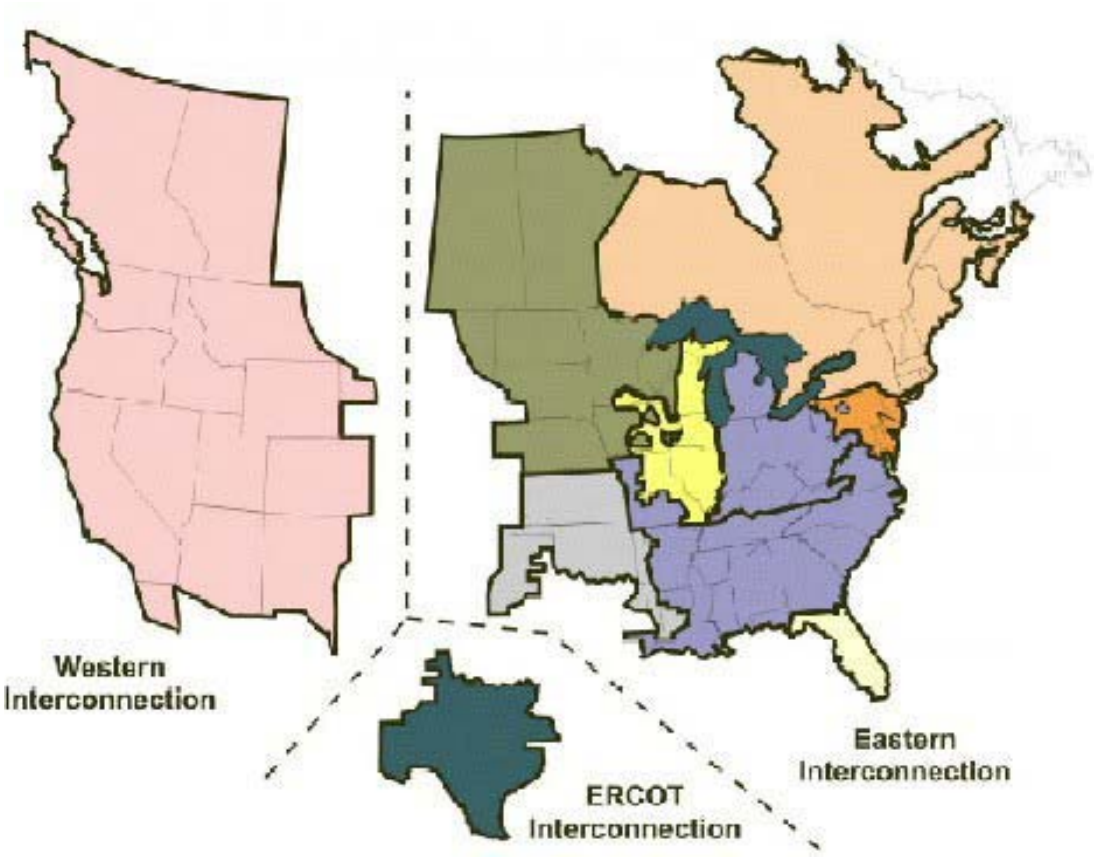


Figure 2-1. The three U.S. transmission interconnections.

The utilities that make up the power grid have traditionally been highly regulated, vertically integrated public or private corporations or government-owned entities responsible for everything from the generator to the customer's meter. This picture has changed significantly in the last several years. The deregulation that began with the Energy Act of 1992 has removed some of the restrictions and encouraged competition in the generation and delivery of power. Competition has forced utilities to cut costs to the extent possible. One of the results of competitive pressures and the advent of the internet has been a rapid increase in the extent that automation is used at a typical utility and the amount of data that is being collected.

Another result of deregulation has been an increased fragility of the power grid. A good share of deregulation has been focused on generation as opposed to transmission or distribution. As a result, many new generation facilities have been built but transmission resources have not kept pace and are routinely

stretched beyond their normal limits.[8] Recent events including the east coast blackout of 2003 have brought new focus to solving this problem. However, building new transmission lines or increasing the capacity of existing lines is a time-and capital-intensive process, and so the problem persists.

2.2 Key Industry Players

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), Electric Power Research Institute (EPRI), Edison Electric Institute, and Utility Telecommunications Council.

2.2.1 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 2-2. 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.

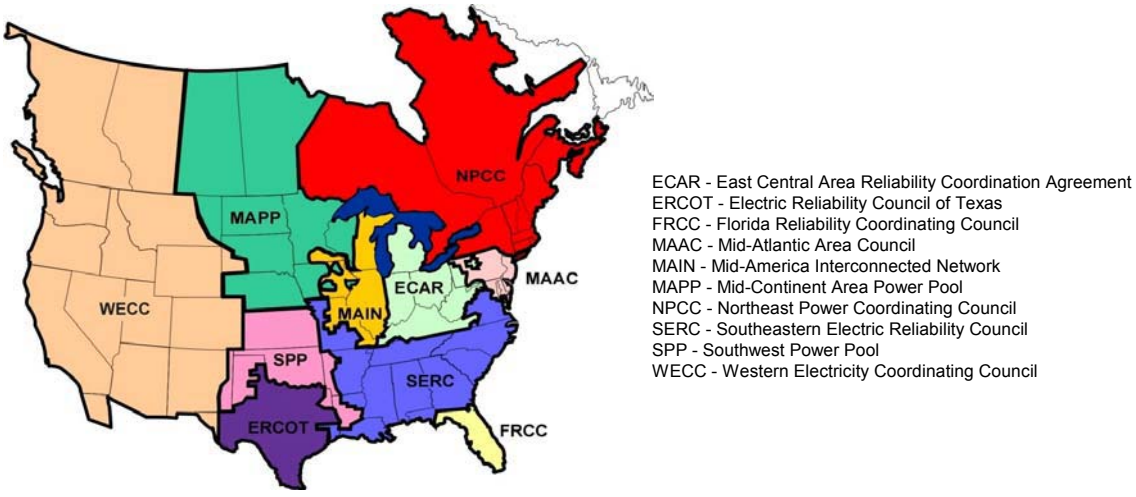


Figure 2-2. The 10 Regional Coordinating Councils of NERC.

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, known as "ES-ISAC." The ES-ISAC website (http://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.[11]

2.2.2 Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) is the primary regulatory agency for the electric power industry, as well as for the 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, provides open access to the nation's transmission grid. Order 888 requires utilities to publish non-discriminatory tariffs for transmitting, or "wheeling," power over their transmission lines. Order 889 establishes 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 have 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 Interconnection'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. California ISO's (CAISO's) node (website http://oasis.caiso.com), on the other hand, allows anyone who visits its website open access to information about existing conditions as well as 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 players.

FERC, in its Order 2000, further defines 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 2-3 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.

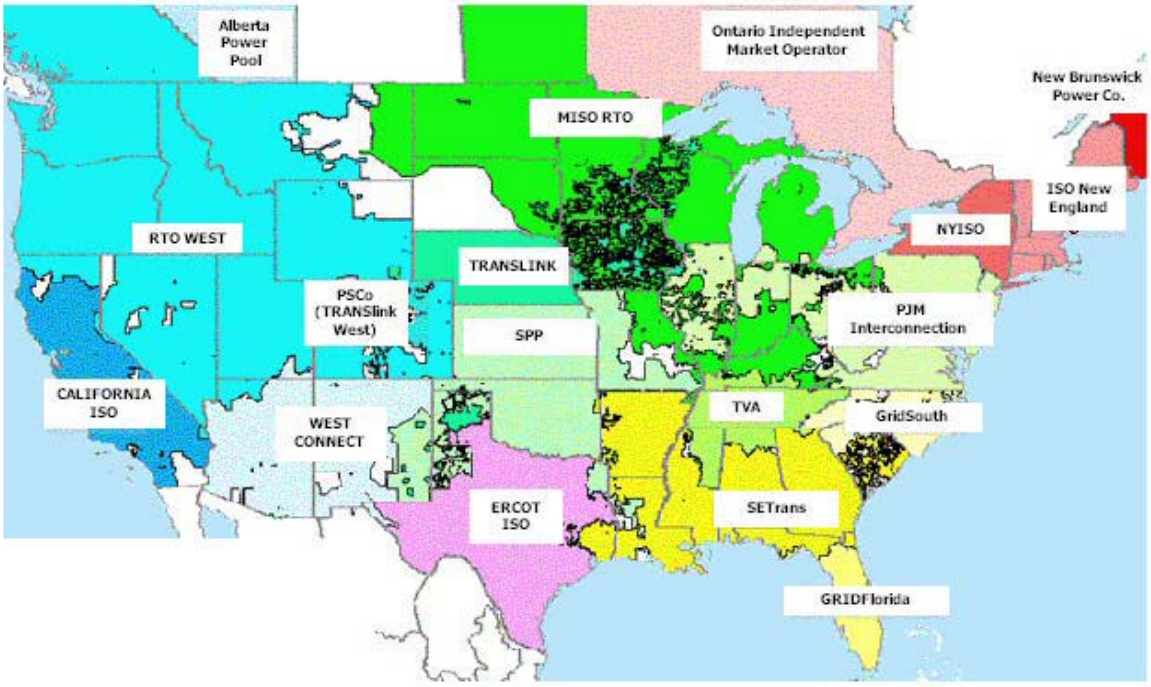


Figure 2-3. Current Regional Transmission Organizations (RTOs).

2.2.3 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 as well as 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

- 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, three 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.

2.3 Electric Utility Overview

Even though deregulation has changed the landscape to some extent, a typical large electric utility still owns power generation facilities, power transmission and distribution lines, and substations. Figure 2-4 shows a block diagram of these components. 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.

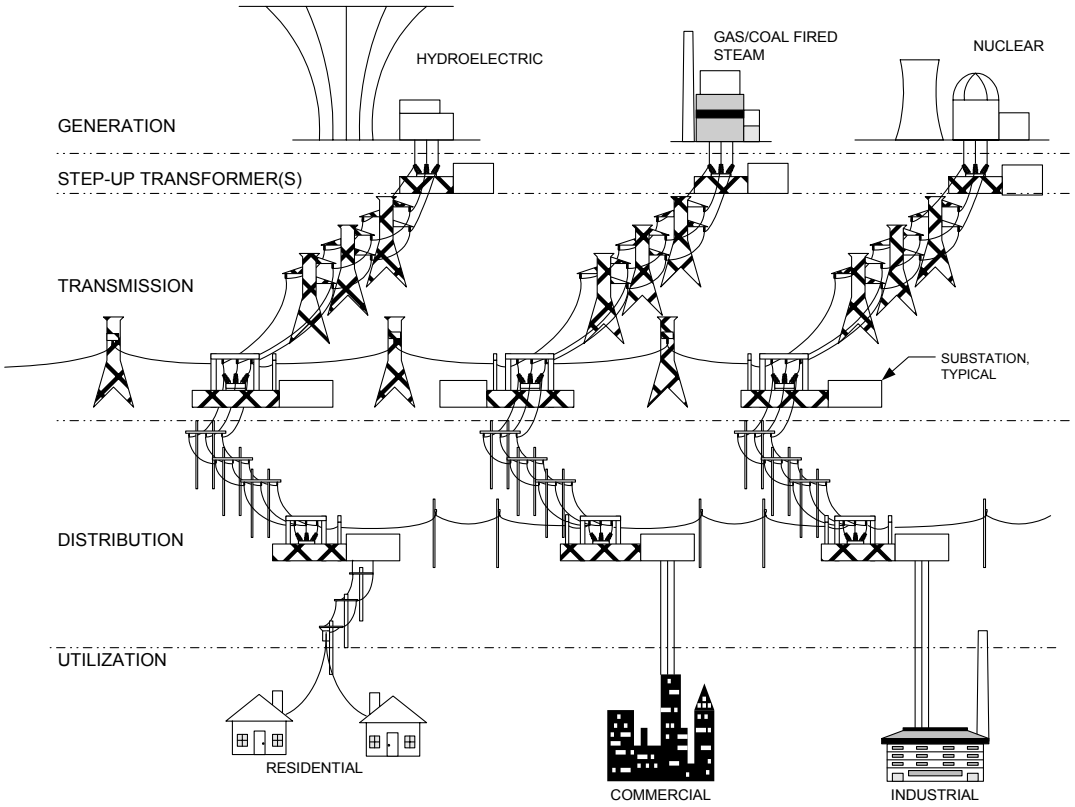


Figure 2-4. Utility block diagram.

2.3.1 Power Generation

Although power supplying the grid comes from many sources, the majority of power is generated by investor-owned public utilities. Figure 2-5 shows the makeup of the types of utilities and the amount of power they provide.[1]

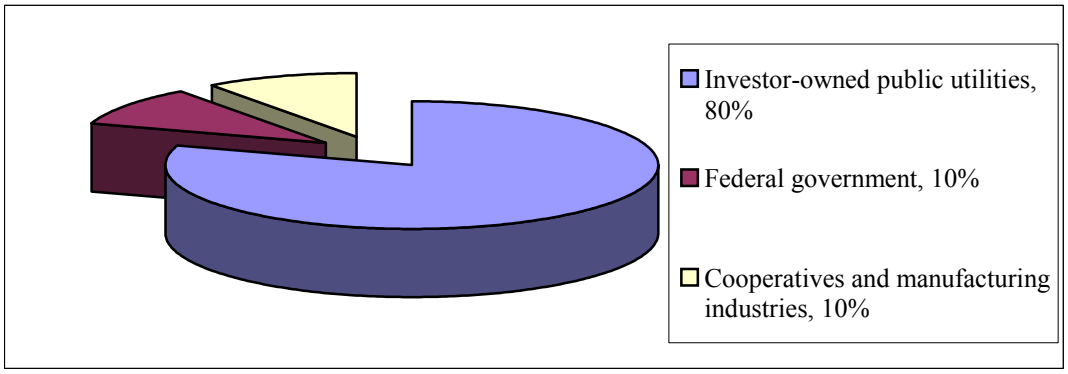


Figure 2-5. U.S. power providers.

Fuel for power generation in the U.S. 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 2-6 depicts these generation sources.

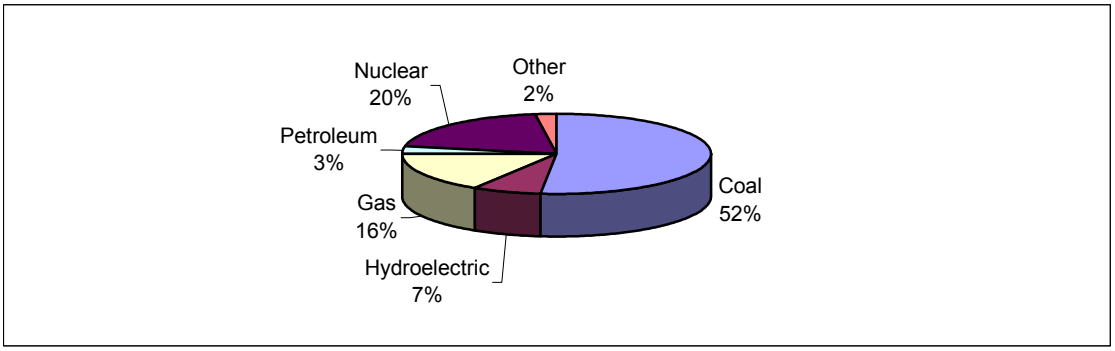


Figure 2-6. U.S. production by energy source – 2000.

Figure 2-7 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 SCADA RTU via either 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 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 to the 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.

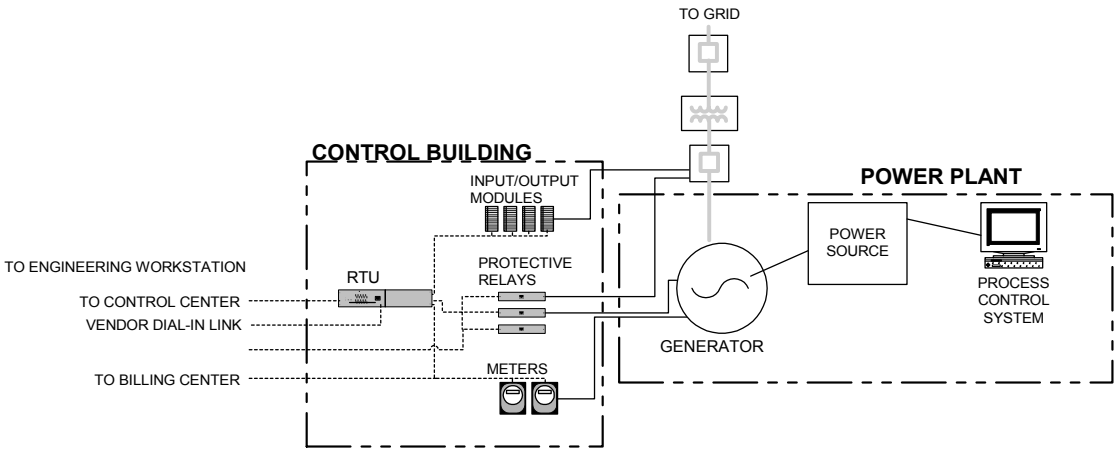


Figure 2-7. Generation plant block diagram.

2.3.1.1 ***Coal.*** The United States has one quarter of the world's coal reserves, which account for more energy content than all of the world's known oil reserves.[15] 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.

2.3.1.2 ***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 to monitor and control 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.

2.3.1.3 ***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.

2.3.2 Power Substations

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

2.3.2.1 ***Transmission Substations.*** Figure 2-8 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).

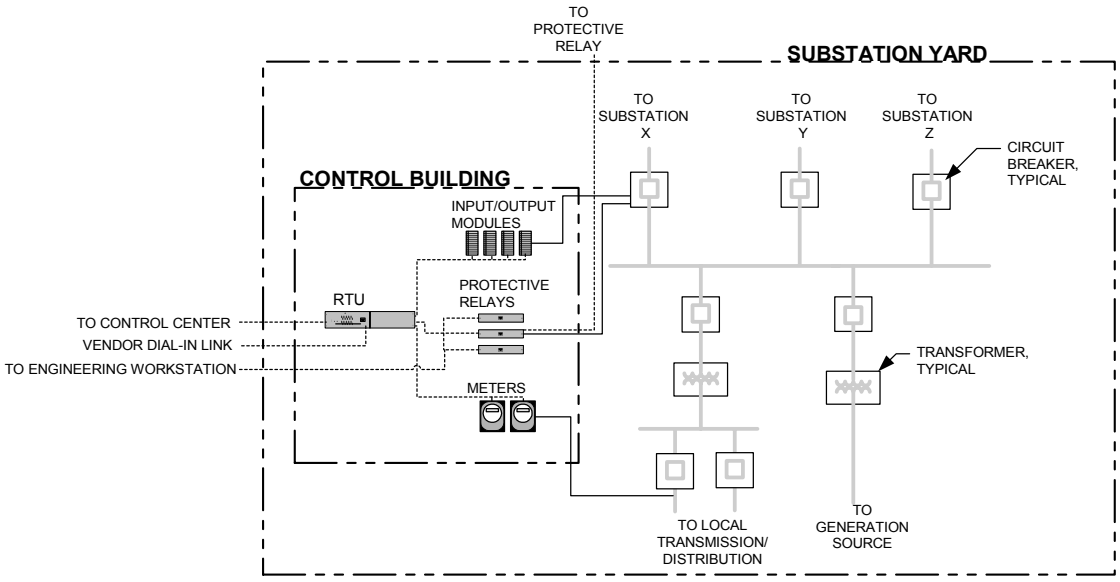


Figure 2-8. Typical transmission substation.

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 function to 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, or power line carrier.

Newer relays, in addition to communicating with each other, 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 in the event it trips a circuit breaker. The integration of protective relays into SCADA systems has raised the stakes somewhat with regard to cyber security. Utilities are much less likely to operate their system without protective relays and protection against 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. On the other hand if an attacker could gain 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 if 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.

2.3.2.2 ***Distribution Substations.*** Distribution substations are similar to transmission substations in that they still have circuit breakers and transformers as their primary electrical components. From a control standpoint, they still have RTUs, protective relays, and meters that perform basically the same functions as in transmission substations. There are a few differences, however. Figure 2-9 shows a typical distribution substation.

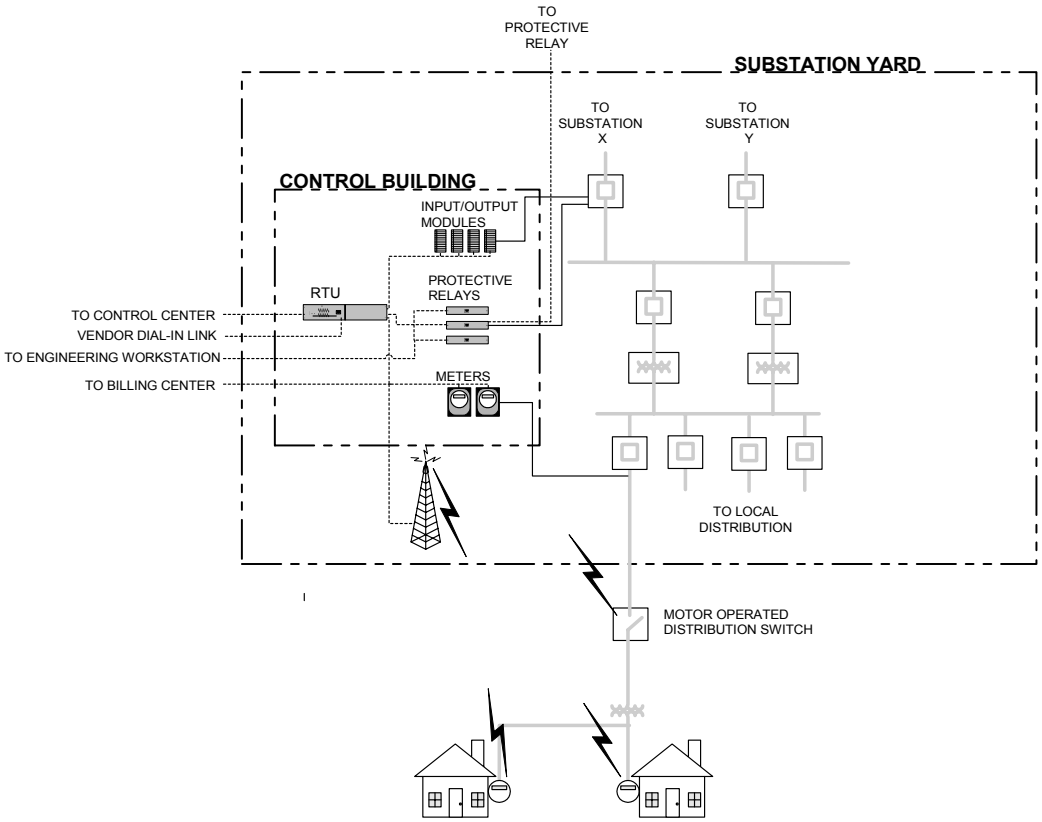


Figure 2-9. Typical distribution substation.

A distribution substation typically steps the incoming voltage from transmission levels down to medium voltage levels (2,400-69,000 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 with no communications capability.

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 colocated 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,[2] the popularity of these switches is increasing. 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.

2.3.3 Electric Utility Control Center

Key to the operation and maintenance of a modern utility's generation, transmission, and distribution resources as described in the previous sections is a centralized control and monitoring system. For most utilities, this system is housed in one or more control centers. Figure 2-10 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 2-10. Components of the control center include the SCADA system, the energy management system, and other application servers and/or workstations.

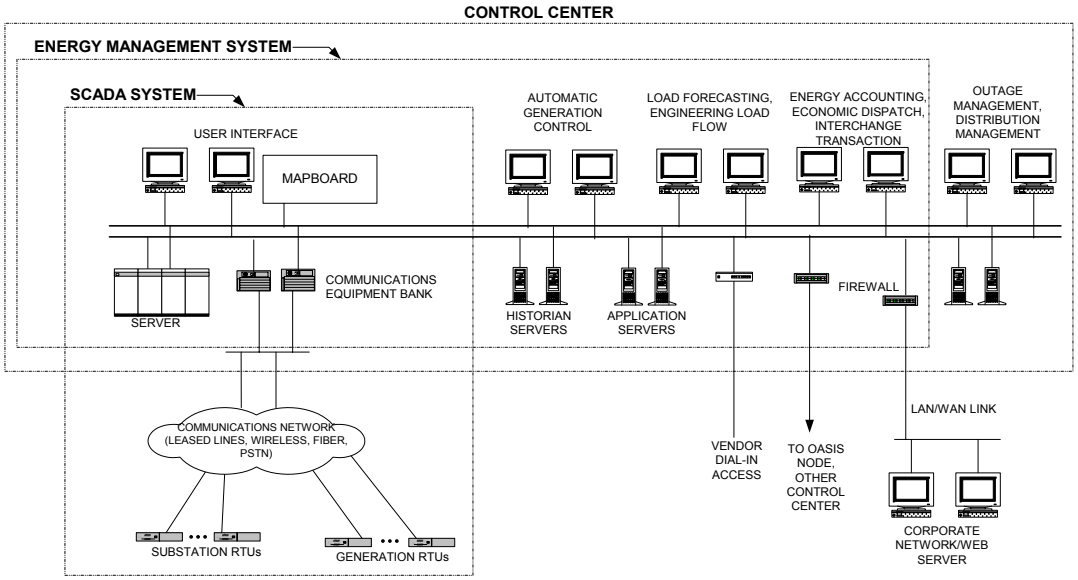


Figure 2-10. Typical utility control center block diagram.

Figure 2-11 shows a graphical depiction of a typical control center. A large control center typically is staffed by several operators. Each operator is often 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 as well.

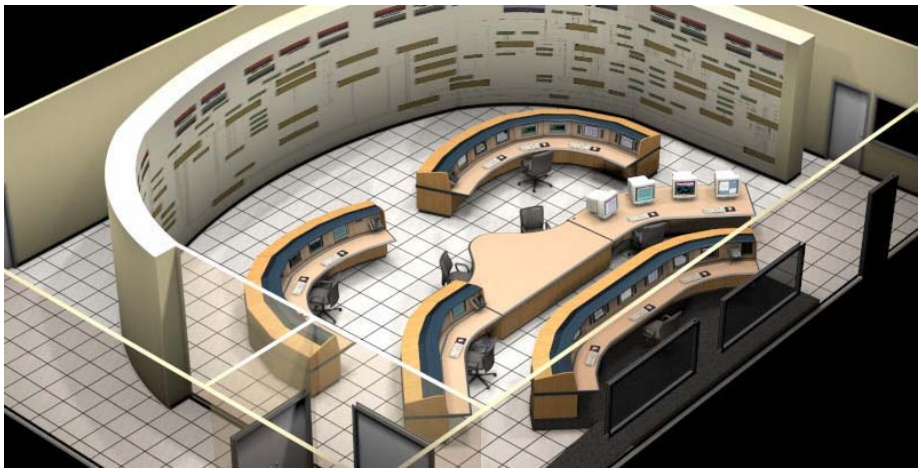


Figure 2-11. Typical utility control center.

2.3.3.1 ***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 basic control and monitoring of field devices including breakers, switches, capacitors, reclosers, and transformers. As shown in Figure 2-10, a SCADA system includes data collection computers at the control center and remote terminal units (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.

2.3.3.2 ***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 2-10, 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 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. Reserve calculation compares actual generator output to rated output to determine reserve. Spinning reserve counts only those generators currently online. Nonspinning reserve includes those generators that are currently offline.

Figure 2-12 shows the results of a survey[2] of utilities regarding which EMS applications they currently use or have plans to use.

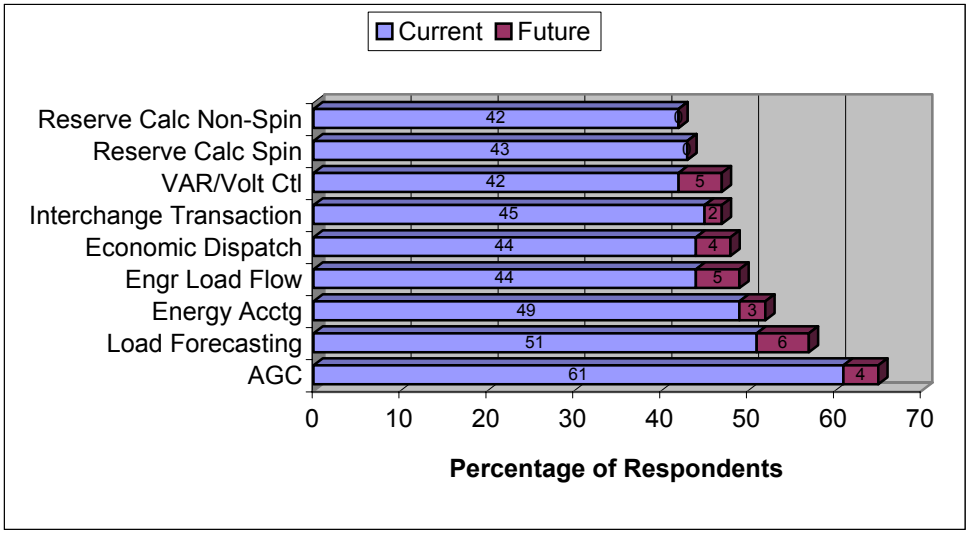


Figure 2-12. Current/future plans for EMS applications and functions.

2.4 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 the following tables.

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

Table 2-1. 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

Standard	Title	Description
IEEE 1379	Recommended Practice for Data Communications between Remote Terminal Units and Intelligent Electronic Devices in a Substation	Provides implementation recommendations for the 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

2.4.2 Electronic Industries Alliance/Telecommunications Industry Association

Table 2-2. 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

2.4.3 International Electrotechnical Commission

Table 2-3. 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 ICCP in U.S.
IEC 61850	Communication networks and systems in substations	Describes protocol similar to UCA 2.0.

2.4.4 North American Electric Reliability Council

Table 2-4. 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 also not apply to nuclear facilities.

3. SCADA MANUFACTURERS AND VENDORS

3.1 SCADA Hardware and Operating Systems

SCADA vendors provide both computer hardware and software for a new system. Traditionally, SCADA computers have been large, UNIX-based servers. As personal computers (PCs) have become more powerful and Microsoft Windows-based operating systems have become more popular, the trend in new systems has shifted toward Windows-based PCs (see Figure 3-1). This is especially true of smaller systems. While some vendors offer a choice of platform between Linux, UNIX, and Windows, very few vendors offer their SCADA software for operation solely on a UNIX-based system. Linux-based systems are offered by some vendors and have increased in popularity recently. Larger SCADA systems still tend to rely on UNIX, TRU 64, VMS, or others in lieu of Windows systems for large complex applications. Even on bigger systems, though, ancillary applications are often run on Windows.

Regarding computer hardware vendors, HP tended to be most popular followed by IBM with Dell becoming more popular (based on a study by Newton-Evans Research; see Figure 3-2). The study placed HP and its predecessor companies DEC and COMPAQ in the same category. Since some respondents to the study used both types of platforms for different applications, the percent total does not total 100%.

Many of the systems utilize UNIX-based operating system software on either server, workstation, or PC hardware platforms with either Windows- or workstation-based client front ends. The older, traditional, medium- to large-scale EMS utilize UNIX-based servers and terminal equipment where newer systems are moving to Windows-based servers and front-end hardware. Many systems that are transitioning to newer technologies include mixed UNIX- and Windows-based hardware. The vendors specified in Figure 3-2 are major suppliers of hardware that support Windows, UNIX, and Linux operating systems software but the figure does not distinguish among them. UNIX and Windows OS software variants can be used in their various forms on server, workstation, and PC hardware.

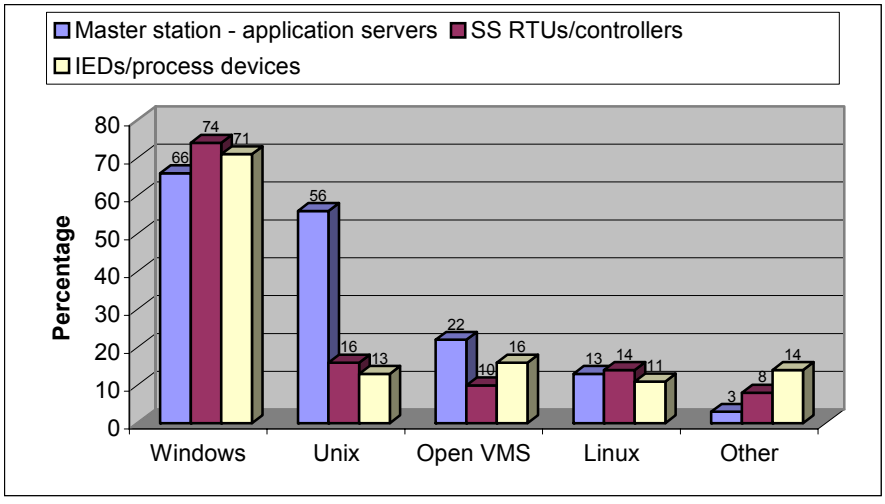


Figure 3-1. Choices of acceptable operating systems.

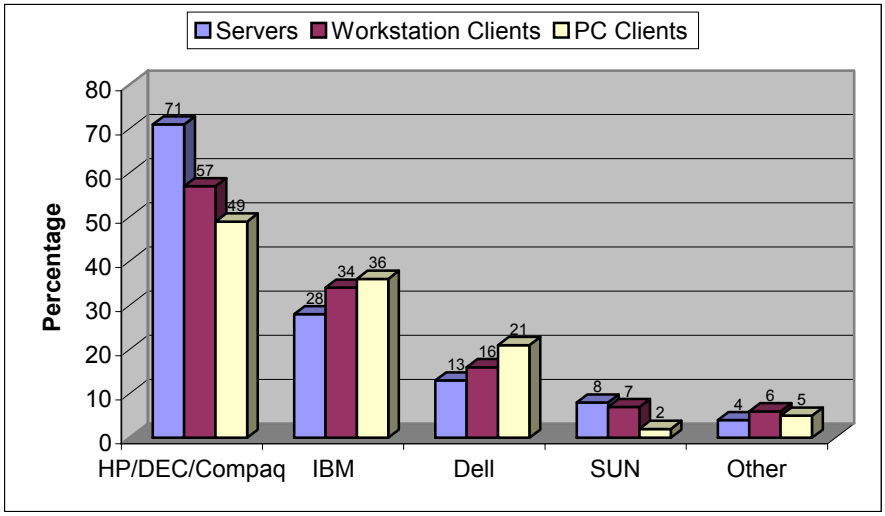


Figure 3-2. SCADA CPU platforms.

As SCADA hardware is upgraded, SCADA software usually follows. As users upgrade hardware, the vendor of the software must have previously tested the version of software with the proposed hardware. The typical sequence of testing is outlined in Section 3.2. A typical problem users may run into is when upgrading only one (either the hardware or software). The legacy hardware or software may not be upgradeable depending on whether the vendor is still in business. Extensive testing is required by users to ensure the legacy system is still operable. The vendor will typically recommend upgrading both simultaneously to alleviate this problem (it doesn't hurt their bottom line, either).

When interfacing to legacy RTUs, the issue of what type of protocol is used becomes critical (see Section 7). Whether hardware or software can be upgraded depends on whether the RTU communicates using an "Open" or "Propriety" protocol. If a user has legacy hardware at the RTU level, and decides to upgrade the SCADA, the protocol must be available to the SCADA software (e.g., DNP, Modbus). If the protocol is proprietary, then the user must decide whether to upgrade the RTU or spend additional costs implementing communications. For some protocols that are proprietary, the upgrade may not be possible because the vendor is no longer in business or due to legal issues.

Other hardware of SCADA systems may consist of vendor-specific RTUs, PLCs, other servers, firewalls, routers, meters, relays, and controllers. See Figure 2-10 for a typical SCADA system.

3.2 SCADA Evaluation Process

The SCADA testing and evaluation process is outlined in IEEE C37.1-1994. This standard outlines the test stages and classes of tests to be performed on a SCADA system. See Table 3-1 for a description of the tests.

Table 3-1. Minimum SCADA test requirements.

Test Stages	Classes			
	Interface Tests and Inspections	Environmental Tests and Inspections	Functional Tests and Inspections	Performance Tests and Inspections
Certified Design Tests	Power Input SWC Dielectric	Temperature Humidity Acoustic (opt)	None	None
Factory Tests and Inspections	Mechanical Power Source (opt.) Dielectric (opt)	Temperature (opt) Humidity (opt) Acoustic (opt) Altitude (opt) Dust (opt) EMI (opt) EMC (opt) Shock/vibration (opt)	I/O point C/O Comm. User Interface Special Functions	Loading Data Acquisition-Control User Interface Computer & Disk Stability (opt) Maintainability (opt) Expandability (opt)
Field Tests and Inspections	None	None	I/O point C/O Comm. User Interface Special Functions	Availability (opt)

Newly installed SCADA systems go through a vendor-recommended user-defined evaluation process. Vendors and users implement IEEE C37.1 as applicable. Newer systems today do not require all of the tests identified in the IEEE standard because the equipment and software are designed and built to additional standards. The evaluation process is typically a three-tiered approach. Out of the numerous sites that were interviewed, the users of the sites had implemented all or part of each phase of the evaluation process.

The first phase of testing is performed in the development facility. The SCADA system is interfaced with a mock-up of a substation, usually an RTU or PLC. Testing of communication, I/O points, and control functions are verified. The second phase consists of testing the SCADA system with a vendor-provided simulation package. The Factory Acceptance Test (FAT) commonly encompasses all or part of these. The simulation software validates control points and interface points. The last phase of testing is also known as system operability (SO) testing. This is performed after installation of all applicable control and field devices. All discrete points are toggled and all control points are operated on the "on-line system" to verify proper operation of the SCADA system. Upon completion of the SO test, the SCADA system is placed on-line.

After initial installation, periodic testing is performed to verify that the SCADA system continues to operate properly. This testing is part of preventative maintenance procedures.

3.3 SCADA Vendors

SCADA systems come in a myriad of types, sizes, and applications. They may monitor/control only a few hundred points or tens of thousands of points. For the scope of this report, only SCADA systems that apply to electrical transmission, distribution, and generation and were of substantial size were evaluated. EMS contain a suite or modularized set of applications such as AGC, outage coordination, load forecasting, remote clients, and business applications.

Table 3-2 lists utility related SCADA manufacturers and their current, major SCADA system(s). The list is not intended to be all-inclusive as most manufacturers provide a multitude of SCADA systems. Frequently, many vendors enter or leave the SCADA market based on corporate buy outs.

Table 3-2. List of SCADA manufacturers and their current SCADA system.

Manufacturer	Current SCADA
ABB	Process Portal A/Operate IT, Ranger
Advanced Control Systems (ACS)	Prism
Alstom	ESCA
C3-Ilex	EO SCADA
Citect	CitectSCADA
Foxboro	Invensys I/A series
GE Fanuc Automation	iFix 32
GE Network Solutions	XA21, Swift
Honeywell	Smart Distributed System
Metsoautomation (formally Neles)	MetsoDNA
Motorola	MOSCAD
Open Systems International (OSI)	Monarch
QEI, Inc	TDMS-2000
Siemens	PowerCC EC and SIMETEC PCS 7

Figure 3-3 shows the percentage of manufacturer use from the respondents of a recent survey on existing systems.[2] Figure 3-4 identifies future vendors being considered for new EMS procurements. The term “EMS” in Figure 3-4 represents a consolidation of the existing installations (SCADA, DMS, EMS, etc.) shown in Figure 3-3. The number of vendors in the legend of Figure 3-4 is less than shown in Figure 3-3 due to industry consolidation and vendors no longer providing SCADA systems.

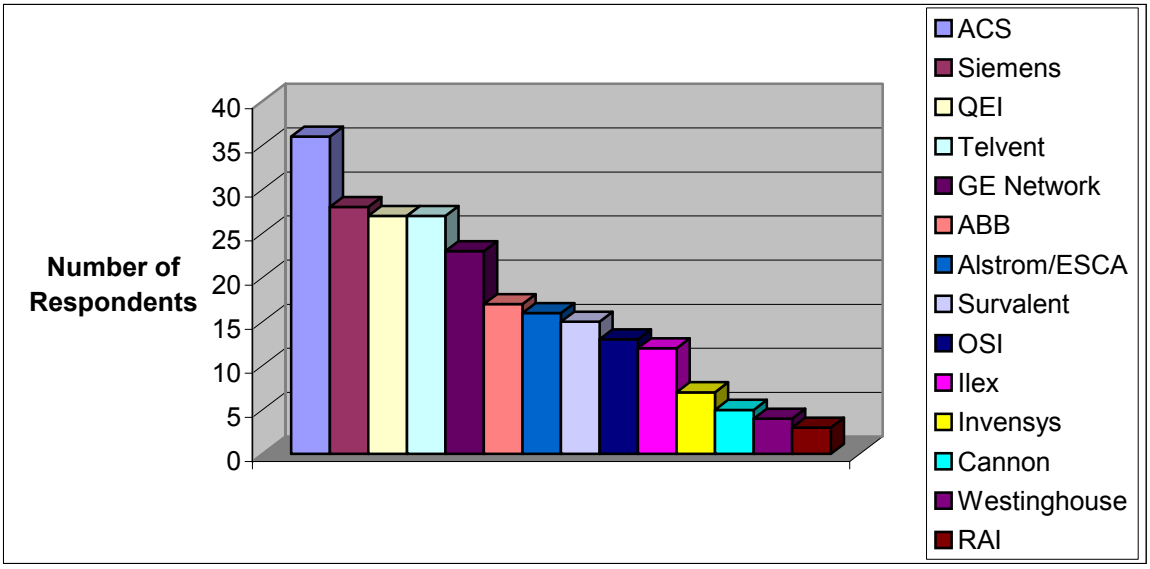


Figure 3-3. Vendor representation for respondent installations for SCADA, EMS, and DMS systems.

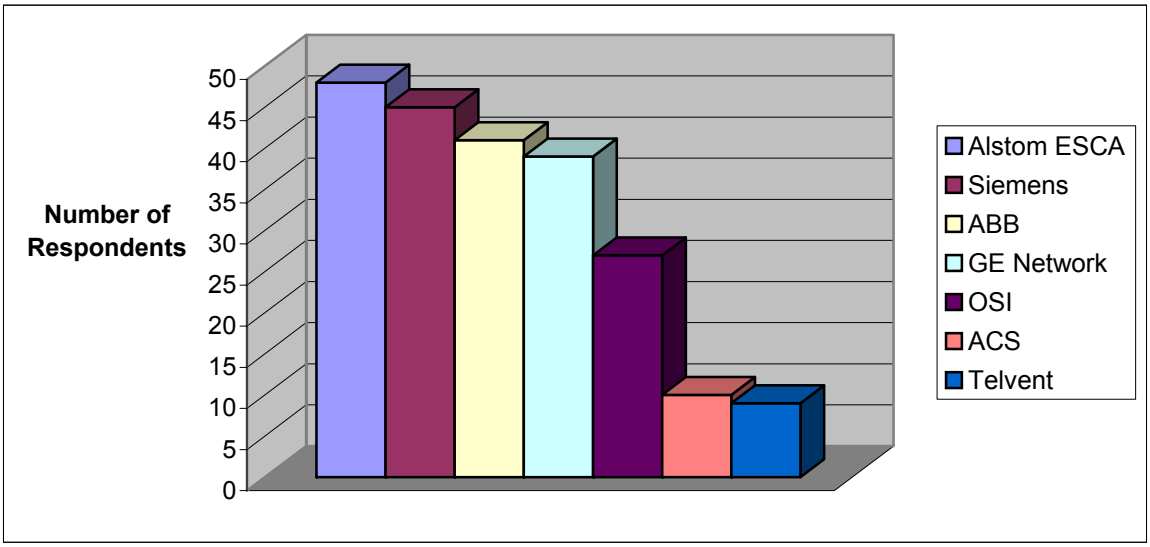


Figure 3-4. Vendors likely to be considered for future EMS procurements.

The following are vendor profiles of the top six SCADA suppliers shown in Figure 3-3.

Company: Advanced Control Systems (ACS)

Background and Strengths: ACS was founded in 1975 to supply real-time control systems and equipment to the electric utility industry. ACS has delivered more than 470 SCADA, SCADA/AGC, DMS, and EMS masters and 11,000 RTUs.

Their current masters are based on UNIX software and workstations or workstations and servers using RISC processors in an open network environment. A full line of RTUs is supplied, all with IED interface

	capabilities and various communications protocols, including DNP 3.0. A full line of substation equipment is offered from legacy RTUs to protocol's converters/data concentrators to substation automation systems with or without graphical user interface
Company:	Siemens
Background and Strengths:	Siemens Power Transmission and Distribution was formed to focus specifically in the operations and needs of domestic and international electric utility markets. Semens provides a complete range of products. Siemens is a supplier of SCADA and automation systems to the electric, water, and gas utility industries as well as to industrial customers worldwide. TeleGYR is now part of Siemens. Other products include SICAM controllers and RTUs.
Company	QEI
Background and Strengths	Founded in 1960 as Quindar Electronics, QEI designs and manufactures SCADA equipment and systems. The company supplies industries such as water, gas, power, petroleum, pipeline, railroad, steel, communication, traffic control, and telemetry. Products include the TDMS 2000 and RTUs.
Company	GE Network Solutions
Background and Strengths	Currently owned by GE Power systems. GE provides complete solutions to support T&D automation programs. They provide both hardware and software solutions.
Company	ABB
Background and Strengths	ABB is one of the world's largest suppliers of automation systems for the electric power industry. The ABB network management specializes in SCADA/DMS/EMS applications software. Major products include the RANGER system. ABB also integrates their own microprocessor-based relays with SCADA systems. They have installed more than 5,000 substation automation systems worldwide.
Company	Alstom ESCA
Background and Strengths	Alstom provides small- and large-scale SCADA/EMS/DMS systems. Primarily focused on the electric power industry, they provide hardware and software in substation automation and real-time energy information systems. They are a worldwide industry leader in SCADA technology. Products include e-terra Global energy solutions.

4. SCADA EXPECTED LIFE AND DISPOSAL

Procurement, installation, and commissioning of a SCADA system is a time- and capital-intensive process. As a result, major upgrades and/or replacements are performed infrequently. The average life of a SCADA system is typically 8 to 15 years. This corresponds with the expected life of typical hardware used. As a result, there is almost no aftermarket value for these components. A web search for aftermarket SCADA hardware confirmed this. The only exception is in the nuclear industry. Many nuclear plants still have original control system hardware that could be 20 to 30 years old. Much of it still uses analog technology as compared to newer digital hardware. With the multitude of requirements that need to be met for a control system replacement, in addition to the complexity of these systems, many plant owners choose to limp along with older controls rather than upgrade. This is especially true of plants that are near the end of their operating licenses.

Substation and control center hardware, once removed, is typically discarded or stored indefinitely in a warehouse or back room. One utility in fact gave its old RTU cabinets to its employees to use as smokers, which apparently works quite well.

5. ELECTRONIC SECURITY

5.1 Attacks

Attacks on electronic systems have become a reality for many companies and electric utilities are no exception. This section discusses the types of attacks typically seen and the defense tools used to ward off these attacks. The 2003 Computer Security Institute (CSI)/Federal Bureau of Investigation (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. While this survey is not focused on the electric utility industry (4% of respondents were from utilities), it does provide a baseline for the types of attacks perpetrated and 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 5-1 shows the data gathered from 2003.

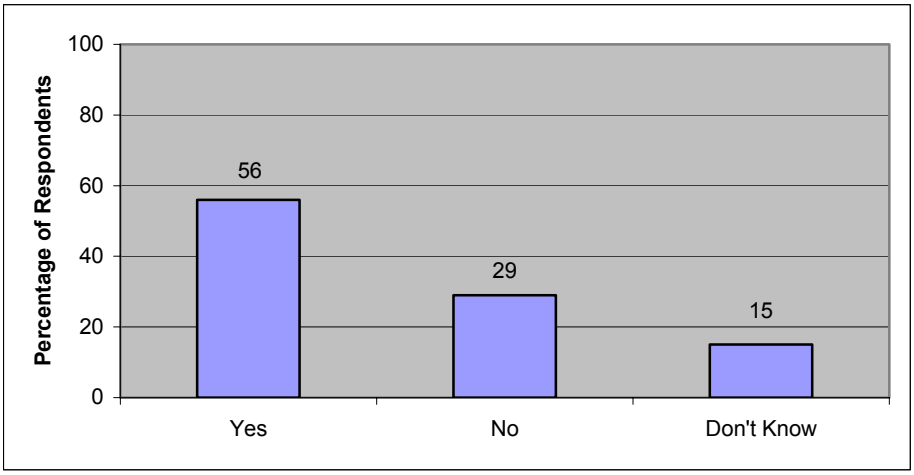


Figure 5-1. Unauthorized use of computer systems within the last 12 months.

The downward trend in reported attacks may 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 5-2 shows the actions taken by respondents when they were attacked.

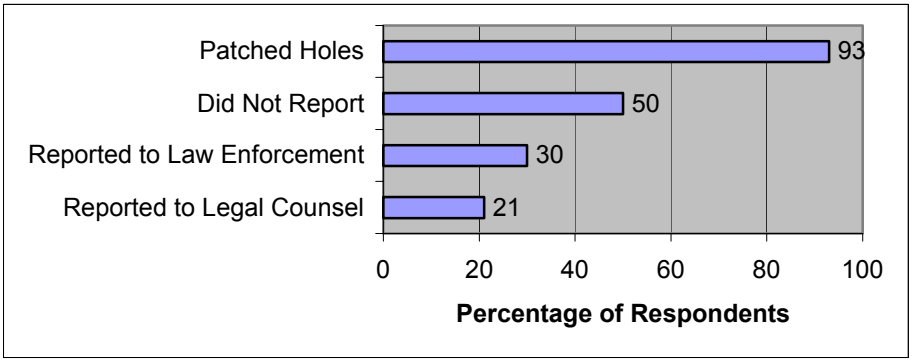


Figure 5-2. Response to cyber attacks.

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.[6]

Types of attacks and/or misuse include viruses, laptop theft, net abuse, system penetration, denial of service, and others. Figure 5-3 shows types of attacks/misuse and their trends during the past four years. Viruses are the most common type of attack. One can also see from this figure that 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 5-4).

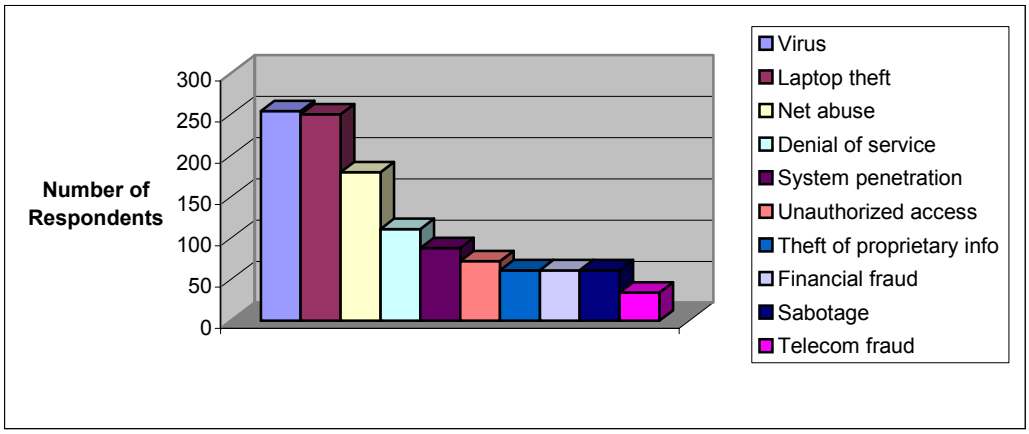


Figure 5-3. Types of cyber attacks/misuse.

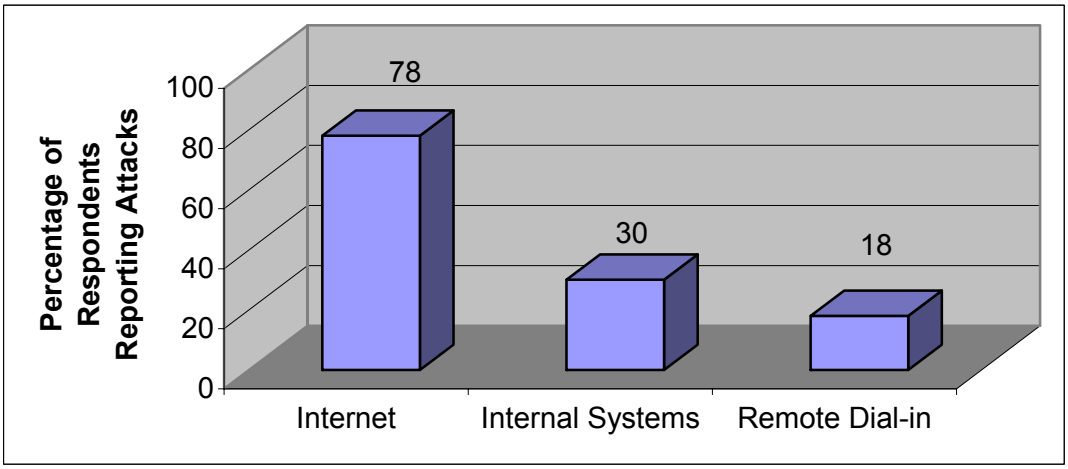


Figure 5-4. Communications media utilized for attacks.

Regarding types of attackers, survey respondents, as shown in Figure 5-5, pointed to independent hackers and disgruntled employees as the most common. Domestic competitors, foreign corporations, and foreign governments were also 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 base on conjecture by the respondents.

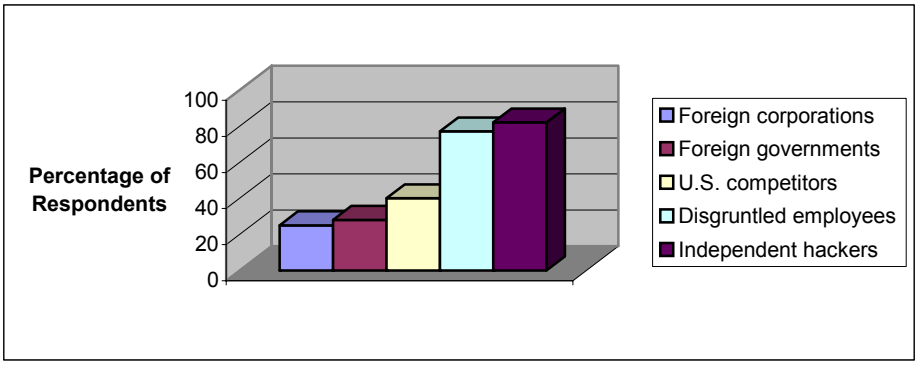


Figure 5-5. Types of cyber attackers.

5.2 Attack Tools

An attacker need not be an accomplished programmer to penetrate a network or computer system. Several tools are available to either gain access to or learn more about a system targeted for attack. This section gives a brief description and some examples of several types of tools of this nature.

5.2.1 Password Crackers

The term password cracker is basically self explanatory. The intent of this software is to try multiple login attempts, typically using one of two methods, dictionary or brute force. Dictionary attack tools use common words or phrases that often appear in passwords. Brute force attack tools simply try every possible character combination that could be entered as a password. Brute force attacks can obviously take longer but also have the ability to crack more passwords. A bevy of password cracking programs is available free on the internet. Lophtcrack is a commercially available program that costs about $250 and is capable of performing brute force and dictionary attacks.

5.2.2 War Dialers

War dialers use a single modem or a bank of modems to dial a range of numbers to determine whether a particular phone line has a modem connected to it. If this is the case, the attacker can then attempt to gain access to this modem using a password cracker or other tool. Like password crackers, war dialers can also be downloaded from the internet. Examples include ToneLoc and THC-Scan. PhoneSweep is a commercially available program that can differentiate between modems and faxes. Cost for this program is approximately $1,000.[10]

5.2.3 Ping Sweep and Port Scan Programs

Ping sweep and port scan programs work on TCP or UDP networks. Ping sweep programs work similarly to war dialers, except instead of dialing phone numbers they ping ranges of IP addresses to determine which ones are used. Port scan programs can then be used to determine which ports are being used. Nmap is an example of a tool that can do ping sweeps and port scans. It is freely available on the internet and works on Windows-based machines. Ethereal is a UNIX/LINUX version that is also freely available.

5.2.4 Packet Sniffers and Protocol Analyzers

Packet sniffers intercept data being transmitted between computers in a TCP/IP network. This requires that the packet sniffer be in the path between sender and receiver. Protocol analyzers take raw packet data and attempt to determine the protocol used and the information being transmitted by each packet. Like other tools, many products are available freely from the internet. Ethereal, mentioned in the previous section, also performs sniffing and protocol analysis.

5.2.5 Denial of Service Tools

Denial of service (DOS) attack tools work by flooding a network with either legitimate or malformed packets of data, thereby effectively locking out legitimate traffic. Some tools come with several malformed packet types known to cause certain systems to crash. Examples of these tools are smurf, fraggle, and SYNflood. SYNflood sends connection requests (SYN packets) to the intended target, but never acknowledges the connection so that many ports are left open on the target machine(s).[10]

5.3 Attack Scenarios

As shown in the previous section, there are several ways to gain access to a networked system. Once a system has been penetrated, an attacker has several options to choose from if his or her target is an electric utility. He or she could:

1. Take direct control of devices in substations and/or generation plants, shutting these facilities down.

2. Plant malicious code or a "logic bomb" that executes on a given event or at a preselected time to disrupt the system.

3. Plant code that opens a "back door" to allow easy access in the future.

4. Change data such as billing information to disrupt financial operations.

5. Perform a "man in the middle" attack to intercept and change data to deceive system operators into thinking the system is in a condition that it is not (e.g., circuit overload). The operators may therefore take unnecessary or damaging action to mitigate this condition.

6. Change protective device settings to make a protective relay trip when it shouldn't, not trip when it should, or both, thus taking the system out of service and/or causing damage to equipment.

7. Take resources hostage for other purposes (e.g., game hosting), degrading performance of the system for the tasks it was designed to do.

Of course, system penetration is not necessarily even required. An attacker could initiate a denial of service (DOS) or distributed denial of service (DDOS) attack that basically ties up all network resources and prevents legitimate traffic from getting through a network.

5.4 Defense Tools

Several tools are also 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.

5.4.1 Passwords

Passwords can be an effective security method. Two factors that influence their effectiveness are whether the passwords are strong passwords and whether they are encrypted. Strong passwords are defined as passwords of six characters or more, with at least one special character or digit and mixed-case character, that do not form a pronounceable word, name, date, or acronym.[12] Table 5-1 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 for 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.[12]

Table 5-1. Comparison of times to crack dictionary vs. strong passwords.

Attack	# Words	2400 bps	9600 bps	19200 bps	38400 bps	10 Mbs
Dictionary						
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
Brute Force						
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, on the other hand, often do not support a full character set for passwords, nor do they support password encryption.

5.4.2 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 stand-alone 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. Stand-alone 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.

5.4.3 Intrusion Detection Systems

Intrusion detection systems (IDS) 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.

5.4.4 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.

5.4.5 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 (http://www.rsasecurity.com/), their SecurID cards are the most popular two-factor identification systems in the world.

Biometrics is the term typically used to describe the third factor. Several methods of using biometrics to verify identity are available. Factors checked by various systems include fingerprints, retinas, iris, face patterns, hand geometry, signature, or voice recognition.[13] Although costs for these devices are 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.[14] Newer products are addressing some of these problems but it appears for the most part that biometric devices are not quite ready for prime time.

5.4.6 Actual Usage of Defense Tools

Respondents to the CSI/FBI survey report use several tools to defend against attacks (see Figure 5-6). Most common among these are anti-virus software, firewalls, access control, and physical security. Intrusion detection is also becoming a more commonly used tool, as well as encrypted files. Most of the technologies in Figure 5-6 were discussed in the previous section or are fairly self-explanatory. PCMCIA is one exception, although ostensibly the security feature of PCMCIA is that memory stored on a PCMCIA card can be removed when not needed, thereby eliminating a pathway for attack. Reusable passwords are static passwords that do not change on a regular basis.

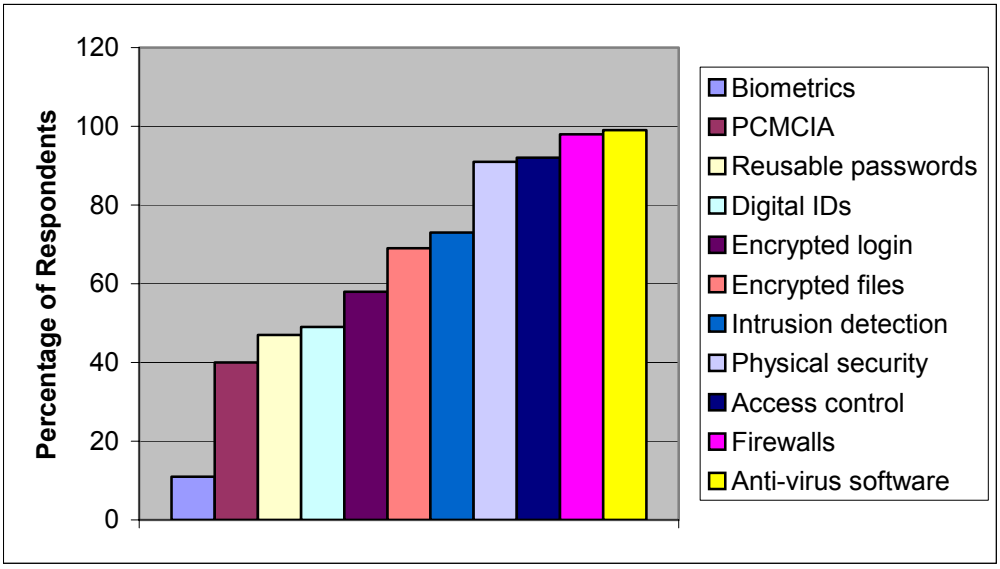


Figure 5-6. Security technologies used.

Information specific to electric utilities in comparison 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 5-7 shows that most respondents use passwords as a primary means of protection. Only two-thirds of respondents use virus protection as compared to 99% in the CSI/FBI study. Less than half of the respondents use any measure other than these to defend against attacks.

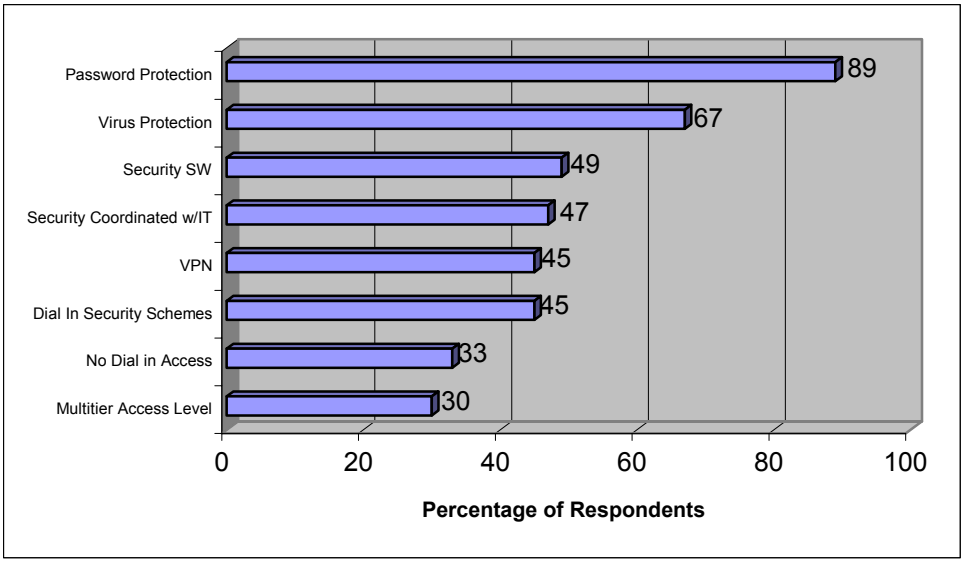


Figure 5-7. Use of approaches for reducing vulnerability on operational networks in the utility.

A trend that exacerbates the problem for utilities is the increasing use of the internet for applications. Figure 5-8 shows current and planned implementation of applications using internet technology. Notice that in every application category there is planned expansion in the use of the internet. Of the respondents, nearly 40% either currently use the internet for supervisory control (17%) or plan to do so (21%).

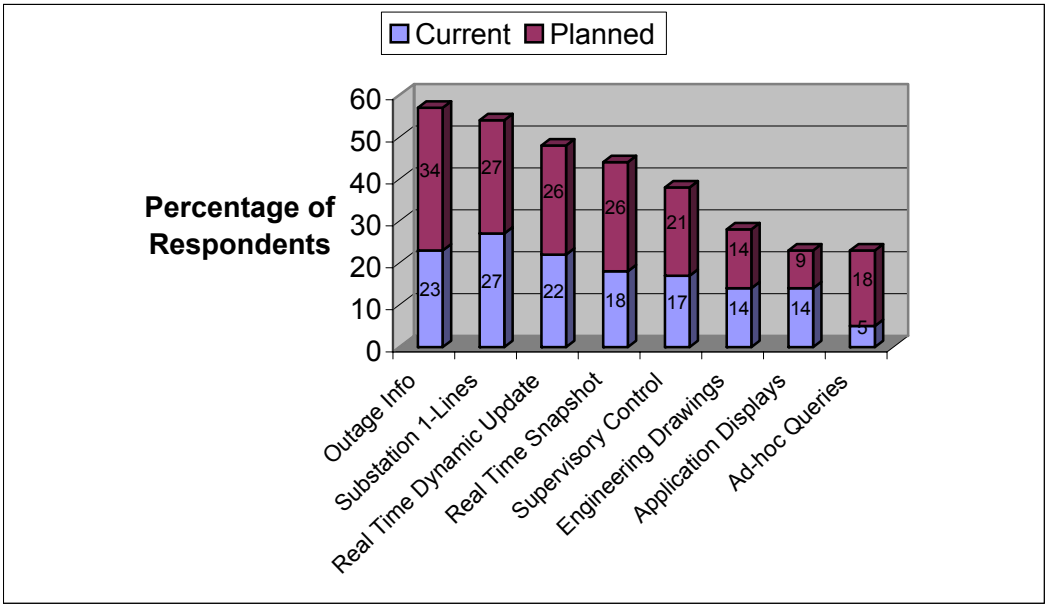


Figure 5-8. Current/future implementation of functions using internet technology.

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 cyber-security principles.[9] The standard mandates that every entity involved with the generation, transmission, or distribution of electric power must perform several steps, including:

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.

The 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 this standard will not happen quickly.

6. PHYSICAL SECURITY

6.1 Physical Security

Physical security at electric power substations and generation facilities varies from installation to installation depending on level of risk, level of impact, and cost of implementation. Cost is a particularly important factor as a result of the competitive pressures brought on by deregulation. IEEE Std. 1402-2000, "IEEE Guide for Electric Power Substation Physical and Electronic Security," is available as a resource for planning and implementing security measures. The main categories of physical security at electric power substations are physical barriers and electronic barriers. Examples of physical barriers include fences, walls, and locks. Examples of electronic barriers include photo-electric/motion sensing, video surveillance systems, building systems, computer security systems, passwords, dial-back verification, selective access, virus scans, encryption, and encoding. Examples of other types of security measures are lighting, landscaping, buildings, patrols, communications, and internal and external information restrictions.

Table 6-1 identifies three sample electric power utilities and their implementation of IEEE Std. 1402-2000. The three utilities are a hydro-electric utility, a utility performing transmission, distribution, and generation, and a utility performing transmission and distribution only.

Table 6-1. Three sample electric power utilities and implementation of IEEE Std. 1402-2000.

Method	Hydro-Electric	Utility Transmission and Distribution	Utility Transmission, Distribution, and Generation
Lights	X	X	X
Signs	X	X	X
Special Locks	X	X	X
Security Guard		X	X
Solid Walls	X	X	X
Manned Substations	X	X	X
Fence	X	X	X
Video Cameras	X		X
Optical Alarms			
Special Equipment (metal-cladding, polymers)	X		X
Door Alarms to SCADA	X	X	
Alarm System			X

6.2 Effectiveness of Security Methods

A security survey was performed and documented in IEEE Std. 1402-2000. The survey results, shown in Table 6-2, provide an indication of the effectiveness of security methods used by respondents in an urban substation. One general observation is that lights, signs, and special locks are the most common security methods employed. Although generally effective according to the majority of the respondents, these methods were not found to be completely effective and can be defeated. Some of the methods used least often (alarms systems, motion detectors, and electronic protection) were reported to be completely effective. The respondents were from various utilities.

Table 6-2. Results of security survey on effectiveness of security methods.

Method	Number of respondents reporting to survey	Not effective (%)	Somewhat effective (%)	Very effective (%)
Lights	31	7	77	16
Signs	27	7	78	15
Special Locks	18	1	66	33
Solid Wall	7	0	57	43
Security Guard	5	0	60	40
Manned station	4	0	100	0
Optical alarms	4	0	75	25
Fence	4	0	75	25
Video Camera	3	0	100	0
Special Equipment (metal-clad, polymer)	3	0	67	33
Door Alarm (to SCADA)	2	0	0	50
Alarm System	2	0	0	100
Motion Detectors	1	0	0	100
Electronic Security	1	0	0	100

7. NETWORK CONNECTIONS AND PROTOCOLS

The architecture of large electrical SCADA systems is moving towards distributed processing. EMS tends to be large and require many network interfaces. Servers handle AGC, load forecasting, energy accounting, outage management, SOE, etc. (see Figure 2-10). The architecture of smaller electrical systems tends to be simpler and contain fewer network connections such as servers, operator interfaces, RTUs/PLCs, and IEDs. The SCADA network is formed when the clients, servers, and RTUs/controllers communicate using some type of protocol and network connections.

Modern SCADA systems typically have multiple network connections. Network connections for SCADA systems can be subdivided into two general categories: "Outside" and "Inside." Network connections may consist of modem, leased lines, optic microwave, radio, or direct network connections.

Inside network connections may communicate with many type of devices, including RTUs, IEDs, other SCADAs, modems, PLCs, and GPS clocks. Inside network protocols include Distributed Network Protocol (DNP) 3.0 (Serial and Ethernet), Modbus, TCP/IP, legacy protocols, proprietary protocols, and others.

Outside network connections may communicate with multiple systems including other EMS and RTOs. Outside network protocols include Intercontrol Center Communications Protocol (ICCP), FTP, DNP 3.0 (Serial and Ethernet), TCP/IP, Modbus, and IEC 61850. Note that TCP/IP is not a substation protocol but rather an underlying data transfer method comprised of a suite of protocols for application in internet/intranet.

Substation protocol selection depends on a variety of factors, such as the selected SCADA system, user preference, and available protocols in other SCADA system/devices. SCADA systems have the availability to communicate with more than one protocol. A SCADA system can communicate with one device with one protocol and another device with a different protocol.

The most popular protocol for outside SCADA network connections is ICCP. ICCP is based on an international standard (IEC60870-6 TASE.2) that enables integration of real-time data between the control centers of different utilities over Wide Area Networks (WANs). Leased lines are another popular network connection between control centers. ICCP-TASE.2 is being used world wide within the electric and gas utility industries to provide exchange of real-time data between control centers, substations, power plants, EMS, SCADA, and metering equipment. Applications range from small regional power dispatching networks to large multi-national transmission systems.

The protocol information in the following three figures was obtained from the Newton-Evans Research Group.[2] Figure 7-1 identifies types of protocol used within a substation, typically from RTUs to IEDs; Figure 7-2 identifies percentages of use for protocols from substation to external SCADA/EMS/DMS; and Figure 7-3 indicates percentages of communications protocols between SCADA and RTO/ISO systems.

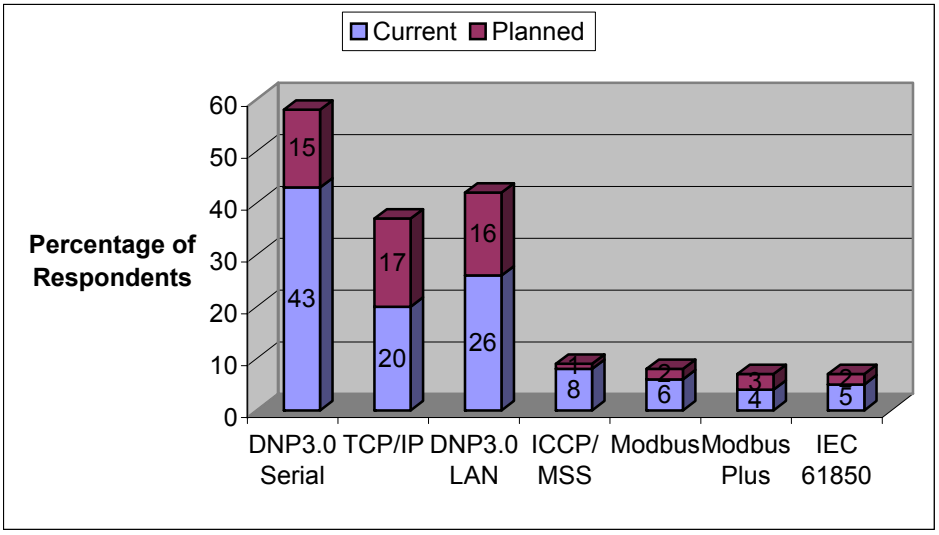


Figure 7-1. Current/future choice of protocol from substation to external EMS/SCADA/DMS network.

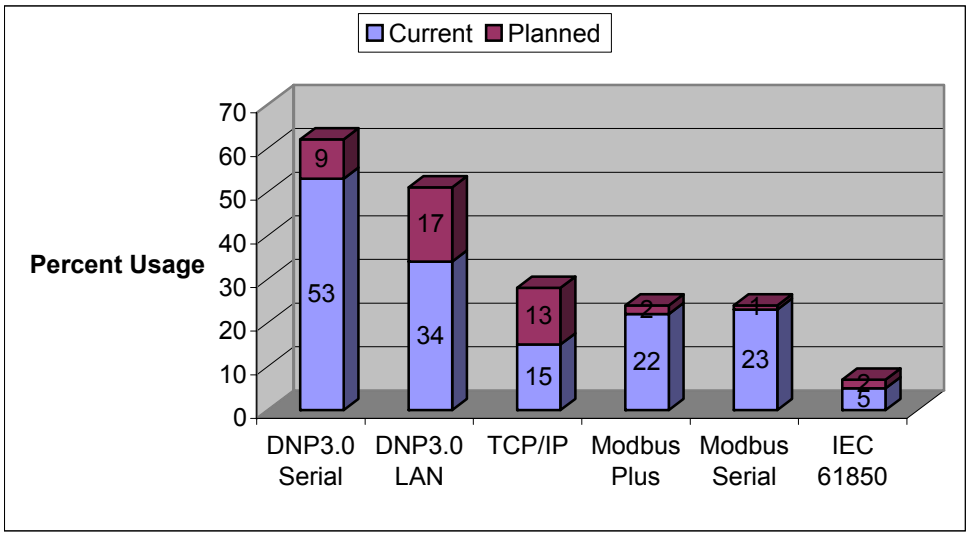


Figure 7-2. Current/future choice of protocol from substation to external EMS/SCADA/DMS host network.

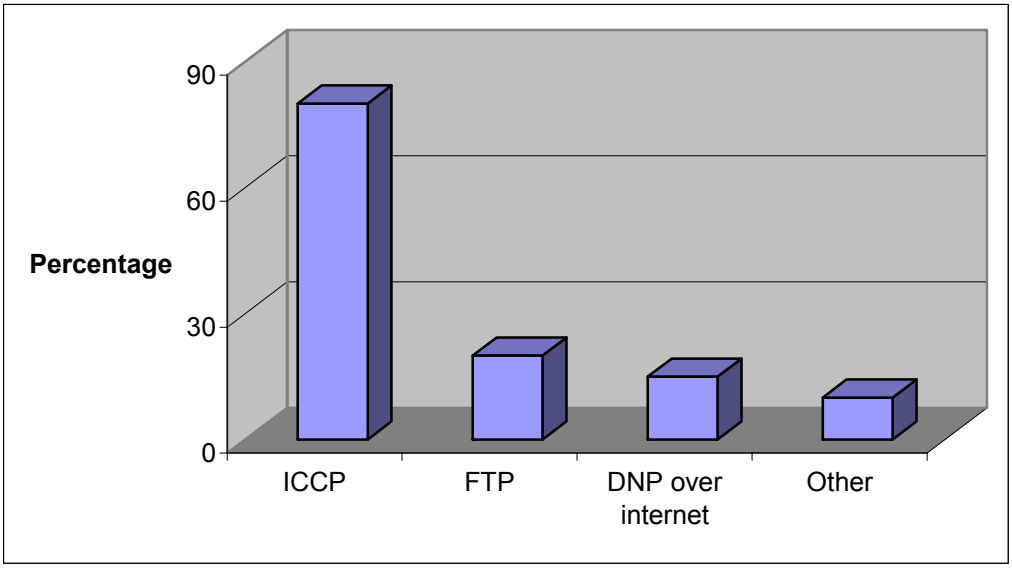


Figure 7-3. Communications protocols used/planned to use to communicate between RTO/ISO systems.

8. GAP ANALYSIS

Although there is currently a fair amount of effort being dedicated to reducing and mitigating the risks of electronic attack to electric power systems, there is still much to be done. Some of these gaps include:

1. Lack of comprehensive approach to security that includes policies and procedures that apply to all devices, connections, and likely scenarios.

2. Lack of communication and cooperation between the utility's information technology (IT) department and SCADA engineers and operators.

3. Lack of regular assessments of SCADA vulnerabilities.

4. Lack of ways of performing real-world tests on systems without risking interruption of service to customers.

5. Lack of security devices for low-bandwidth, real-time control networks.

6. Lack of common testing methods for identifying vulnerabilities.

7. Lack of methods to quantify cyber-security risk.

8. Lack of reliable, inexpensive sensors and devices to ensure physical security of substations.

9. Quantity of operating system and application security patches makes staying current a difficult task.

10. Bottlenecks in power grid make widespread outages more likely.

The following are some potential solutions to help eliminate the gaps:

1. Develop security methods and devices that work well with low bandwidth communications channels in real-time control networks.

2. Implement better security in substation devices (e.g., RTUs, IEDs).

3. Develop testing criteria for control systems vulnerabilities.

4. Perform real-world testing on live or test systems to isolate and mitigate vulnerabilities of integrated systems.

5. Implement cyber security in the most widely used SCADA protocols (e.g., DNP, ICCP).

6. Streamline patch management of control systems.

7. Reduce potential consequences of cyber attack by strengthening power grid.

8. Implement security requirements that apply to all systems and components critical to the operation, maintenance, and continued reliability of the electrical power grids.

9. Intelligence on configuration of potential adversarial systems.

10. Development of smart systems (alert and block – defense or alter attack based on configuration – offense).

9. REFERENCES

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

2. 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.

3. IEEE Std. C37.1-1987, "IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control," Institute of Electrical and Electronics Engineers, 1987.

4. IEEE Std. 999-1992, "IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Systems," Institute of Electrical and Electronics Engineers, 1992.

5. IEEE Std. 1402-2000, "IEEE Guide for Electric Power Substation Physical and Electronic Security," Institute of Electrical and Electronics Engineers, 2000.

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

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

8. U.S. Department of Energy, 2002, *National Transmission Grid Study*, May 2002.

9. NERC, "Urgent Action Standard 1200 – Cyber Security," August 2003.

10. Paul Oman, Allen D. Risley, Jeff Roberts and Edmund O. Schweitzer III, "*Attack and Defend Tools for Remotely Accessible Control and Protection Systems in Electric Power Systems,"* Schweitzer Engineering Laboratories.

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

12. 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.

13. IEEE Computer Society (see website http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm#d7)

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

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