WILEY

Securing SCADA Systems

Ronald L. Krutz, PhD

Introduction

Computer-based supervisory control and data acquisition (SCADA) systems have evolved over the past 40 years, from standalone, compartmentalized operations into networked architectures that communicate across large distances. In addition, their implementations have migrated from custom hardware and software to standard hardware and software platforms. These changes have led to reduced development, operational, and maintenance costs as well as providing executive management with real-time information that can be used to support planning, supervision, and decision making. These benefits, however, come with a cost. The once semi-isolated industrial control systems using proprietary hardware and software are now vulnerable to intrusions through external networks, including the Internet, as well as from internal personnel. These attacks take advantage of vulnerabilities in standard platforms, such as Windows, and PCs that have been adopted for use in SCADA systems.

This situation might be considered a natural progression of moderate concern—as in many other areas using digital systems—if it were not for the fact that these SCADA systems are controlling a large percentage of the United States’ and the world’s critical infrastructures, such as nuclear power plants, electricity generating plants, pipelines, refineries, and chemical plants. In addition, they are directly and indirectly involved in providing services to seaports, transportation systems, pipelines, manufacturing plants, and many other critical enterprises.

A large body of information-system security knowledge has accumulated concerning the protection of various types of computer systems and networks. The fundamental principles inherent in this knowledge provide a solid foundation for application to SCADA systems. However, some of the characteristics, performance requirements, and protocols of SCADA system components require adapting information-system security methods in industrial settings.

In order to present a complete view of SCADA system security concepts and their important role in the nation’s critical infrastructure, this text begins by defining SCADA system components and functions, and providing illustrations of general SCADA systems architectures. With this background, specific SCADA implementations in a variety of critical applications are presented along with a determination of security concerns and potential harmful outcomes of attacks on these operations.

The text follows these illustrations with a detailed look at the evolution of SCADA protocols and an overview of the popular protocols in use today. Then the security issues and vulnerabilities associated with these protocols are examined.

With the criticality of SCADA system security established, the chapters that follow explore SCADA system vulnerabilities, risk issues, attacks, and attack routes, and they provide detailed guidance on countermeasures and other mechanisms that can be applied to effectively secure SCADA systems. In addition, related information, security standards, and reference documents are discussed. These publications provide extremely useful information for securing SCADA systems from cyberattacks.

The book concludes with an examination of the economics of implementing SCADA system security, organizational culture issues, perceptions (and mis-perceptions) of SCADA vulnerability, and current state of SCADA system security. This last topic is addressed in detail by examining SCADA security issues in the oil and gas industry, rail systems, and seaports. Finally, current advanced development programs, additional countermeasures, and legislation targeted to increase the effectiveness of SCADA security in the present and future are described.

CHAPTER 1
What Is a SCADA System?

Supervisory control and data acquisition (SCADA) systems are vital components of most nations' critical infrastructures. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations.

SCADA provides management with real-time data on production operations, implements more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. However, these benefits are acquired at the price of increased vulnerability to attacks or erroneous actions from a variety of external and internal sources.

This chapter explores the evolution of SCADA systems, their characteristics, functions, typical applications, and general security issues.

History of Critical Infrastructure Directives

In 1996, Presidential Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) to explore means to address the vulnerabilities in the U.S. critical infrastructure. Internet-based attacks and physical attacks were two of the major concerns that were to be considered by the committee. As a result of the committee’s efforts, the FBI National Infrastructure Protection Center (NIPC) and the Critical Infrastructure Assurance Office (CIAO) were established in May 1998 by Presidential Decision Directive 63 (PDD 63). The main function of the NIPC was to conduct investigations relating to attacks against the critical infrastructure and issue associated warnings, when appropriate. The CIAO was designated as the main entity for managing the U.S. critical infrastructure protection (CIP) efforts, including coordinating the efforts of the different commercial and industrial entities affected.

As a consequence of the CIAO activities, the Communications and Information Sector Working Group (CISWG) was established with the mission to “promote information sharing and coordinated action to mitigate CIP risk and vulnerabilities in all levels of the Information and Communications (I&C) Sector.” In addition, companies in eight critical industry sectors established a related entity, the Partnership for Critical Infrastructure Security (PCIS). The PCIS was formed to mitigate the vulnerabilities caused by the interdependence of many commercial and industrial organizations.

In response to the September 11, 2001 attacks, the president, on October 8, 2001, established the President’s Critical Infrastructure Board (PCIB), the Office of Homeland Security, and the Homeland Security Council with Executive Order 13228. Also in October 2001, the USA Patriot Act was passed to provide U.S. government law enforcement agencies with increased authority to perform searches, monitor Internet communications, and conduct investigations.

On the economic front, in February 2003, President George W. Bush appointed the 30-member National Infrastructure Advisory Council (NIAC) from the private sector, state and local governments, and academia. NIAC’s charter is to advise the president on information system security issues related to the various U.S. business sectors. Around the same time, President Bush issued Executive Order 1327, which discontinued the PCIB. This action was necessary because the functions of the PCIB were assumed by the Department of Homeland Security.

President Bush, in December 2003, announced Homeland Security Presidential Directives HSPD-7 and HSPD-8. HSPD-7 is a modification of PDD 63 that delineates the national policy and responsibilities of the executive departments, government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service relating to protection of the critical infrastructure. These are the executive departments:

- The Department of Homeland Security
- The Department of State
- The Department of the Treasury
- The Department of Defense
- The Department of Justice
- The Department of the Interior
- The Department of Agriculture
- The Department of Commerce
- The Department of Labor
- The Department of Housing and Urban Development
- The Department of Transportation
- The Department of Energy
- The Department of Education
- The Department of Veterans Affairs

HSPD-8 focuses on preparedness to prevent and respond to domestic terror attacks, disasters, and emergencies.

Figure 1-1 illustrates the timeline of the major activities relating to CIP in the United States.

SCADA System Evolution, Definitions, and Basic Architecture

Supervisory control and data acquisition (SCADA) means different things to different people, depending on their backgrounds and perspectives. Therefore, it is important to review the evolution of SCADA and its definition as understood by professionals and practitioners in the field.

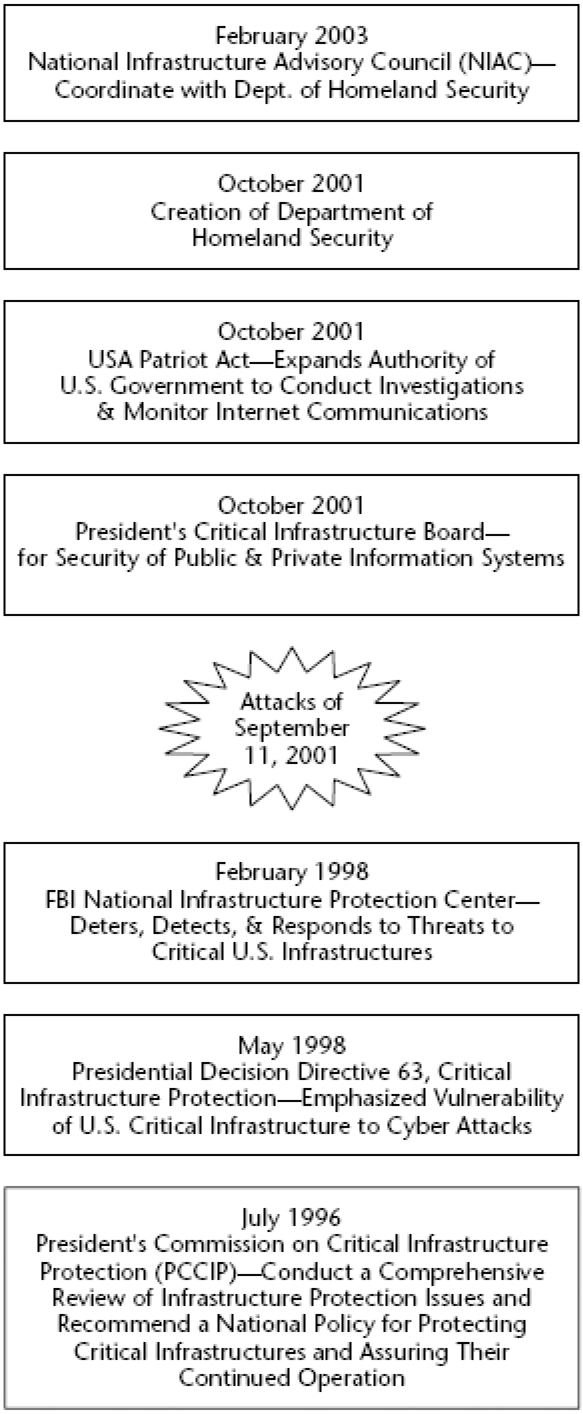
February 2003 National Infrastructure Advisory Council (NIAC)—Coordinate with Dept. of Homeland Security
October 2001 Creation of Department of Homeland Security
October 2001 USA Patriot Act—Expands Authority of U.S. Government to Conduct Investigations & Monitor Internet Communications
October 2001 President's Critical Infrastructure Board—for Security of Public & Private Information Systems
Attacks of September 11, 2001
February 1998 FBI National Infrastructure Protection Center—Deters, Detects, & Responds to Threats to Critical U.S. Infrastructures
May 1998 Presidential Decision Directive 63, Critical Infrastructure Protection—Emphasized Vulnerability of U.S. Critical Infrastructure to Cyber Attacks
July 1996 President's Commission on Critical Infrastructure Protection (PCCIP)—Conduct a Comprehensive Review of Infrastructure Protection Issues and Recommend a National Policy for Protecting Critical Infrastructures and Assuring Their Continued Operation

Figure 1-1 Timeline of U.S. critical infrastructure protection activities

SCADA Evolution

The scope of SCADA has evolved from its beginnings in the 1960s. The advent of low-cost minicomputers such as the Digital Equipment Corporation PDP-8 and PDP-11 made computer control of process and manufacturing operations feasible. Programmable logic controllers (PLCs) progressed simultaneously. These latter devices implemented traditional *relay ladder logic* to control industrial processes. PLCs appealed to traditional control engineers who were accustomed to programming relay logic and who did not want to learn programming languages and operating systems. When microcomputers were developed, they were programmed and packaged to emulate PLCs in function, programming, and operation. In fact, competition developed between the two approaches and continues to this day.

Initially, control systems were confined to a particular plant. The associated control devices were local to the plant and not connected to an external network. The early control systems consisted of a central minicomputer or PLC that communicated with local controllers that interfaced with motors, pumps, valves, switches, sensors, and so on. Figure 1-2 illustrates this architecture.

This architecture is sometimes referred to as a *distributed control system*. Such systems are generally confined to locations close to each other, normally use a high-speed local network, and usually involve closed loop control. As a necessary requirement for the operation of these systems, companies and vendors developed their own communication protocols, many of which were proprietary.

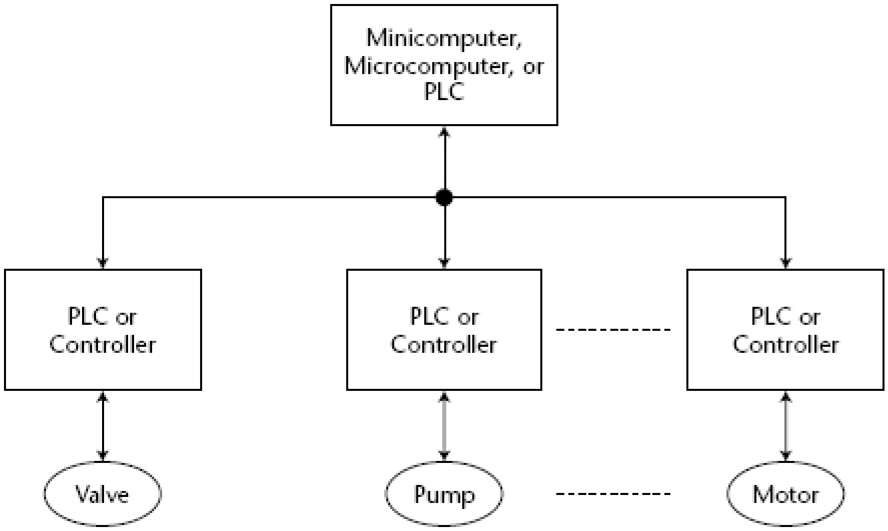

Figure 1-2 Typical local control system

As the technical capabilities of computers, operating systems, and networks improved, organizational management pushed for increased knowledge of the real-time status of remote plant operations. Also, in organizations with a number of geographically separated operations, remote data acquisition, control, and maintenance became increasingly attractive from management and cost standpoints. These capabilities are known collectively as *supervisory control and data acquisition* or SCADA.

SCADA Definition

Listed here are two typical definitions of a SCADA system and the source of each definition:

- SCADA is the technology that enables a user to collect data from one or more distant facilities and/or send limited control instructions to those facilities. *SCADA: Supervisory Control and Data Acquisition* by Stuart A. Boyer, published by ISA The Instrumentation, Systems, and Automation Society; 3rd edition.

- A system operating with coded signals over communication channels so as to provide control of RTU (Remote Terminal Unit) equipment. *IEEE Standard C37.1-1994, Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control*. (The RTU is discussed in the next section.)

Additional definitions associated with SCADA systems are given in Table 1-1. This listing is not meant to be all-inclusive, but describes some important terms used in the application of SCADA systems.

Table 1-1 SCADA-Related Definitions

TERM	**DEFINITION**
deterministic	Degree to which an activity can be performed within a predictable timeframe.
DeviceNet	An Allen Bradley control network protocol that is used to connect PLCs and local controllers.
ControlNet	An Allen Bradley communications protocol applied to control systems.
Data Highway, Data Highway +	Allen Bradley communications protocols.
fieldbus	Communication protocols that facilitate interchange of messages among field devices. Some examples of fieldbus protocols are Foundation Fieldbus, Modbus, DeviceNet, and Profibus.
hot stand-by system	A duplicate system that is kept in synchronism with the main system and that can assume control if the main system goes down.
proportional, integral, derivative (PID) control	Method used to calculate control parameters to maintain a predetermined set point. Mathematical techniques are used to calculate rates of change, time delays, and other functions necessary to determine the corrections to be applied.
real-time (adjective)	An action that occurs at the same rate as actual time; no lag time, no processing time.

TERM	DEFINITION
real-time operating system (RTOS)	A computer operating system that implements process and services in a deterministic manner.

SCADA System Architecture

Specific terminology is associated with the components of SCADA systems. These SCADA elements are defined as follows:

■ **Operator:** Human operator who monitors the SCADA system and performs supervisory control functions for the remote plant operations.

■ **Human machine interface (HMI):** Presents data to the operator and provides for control inputs in a variety of formats, including graphics, schematics, windows, pull-down menus, touch-screens, and so on.

■ **Master terminal unit (MTU):** Equivalent to a master unit in a master/ slave architecture. The MTU presents data to the operator through the HMI, gathers data from the distant site, and transmits control signals to the remote site. The transmission rate of data between the MTU and the remote site is relatively low and the control method is usually open loop because of possible time delays or data flow interruptions.

■ **Communications means:** Communication method between the MTU and remote controllers. Communication can be through the Internet, wireless or wired networks, or the switched public telephone network.

- **Remote terminal unit (RTU):** Functions as a slave in the master/slave architecture. Sends control signals to the device under control, acquires data from these devices, and transmits the data to the MTU. An RTU may be a PLC. The data rate between the RTU and controlled device is relatively high and the control method is usually closed loop.

A general diagram of a SCADA system is shown in Figure 1-3.

Modern SCADA architectures rely heavily on standard protocols and digital data transmission. For example, a communications protocol such as the Foundation Fieldbus, which is discussed in Chapter 3, is applied in conjunction with industrial Ethernet radios. These Ethernet radios provide data rates of 512 Kbps, a large increase over those provided by EIA-232 serial links. For security, industrial Ethernet access points use spread-spectrum frequency hopping technology with encryption.

As discussed previously, a SCADA architecture comprises two levels: a master or client level at the supervisory control center and a slave or data server level that interacts with the processes under control. In addition to the hardware, the software components of the SCADA architecture are important. Here are some of the typical SCADA software components:

- SCADA master/client
  - Human machine interface
  - Alarm handling
  - Event and log monitoring
  - Special applications
  - ActiveX or Java controls

- SCADA slave/data server
  - Real-time system manager
  - Data processing applications
  - Report generator
  - Alarm handling
  - Drivers and interfaces to control components
  - Spreadsheet
  - Data logging
  - Archiving
  - Charting and trending

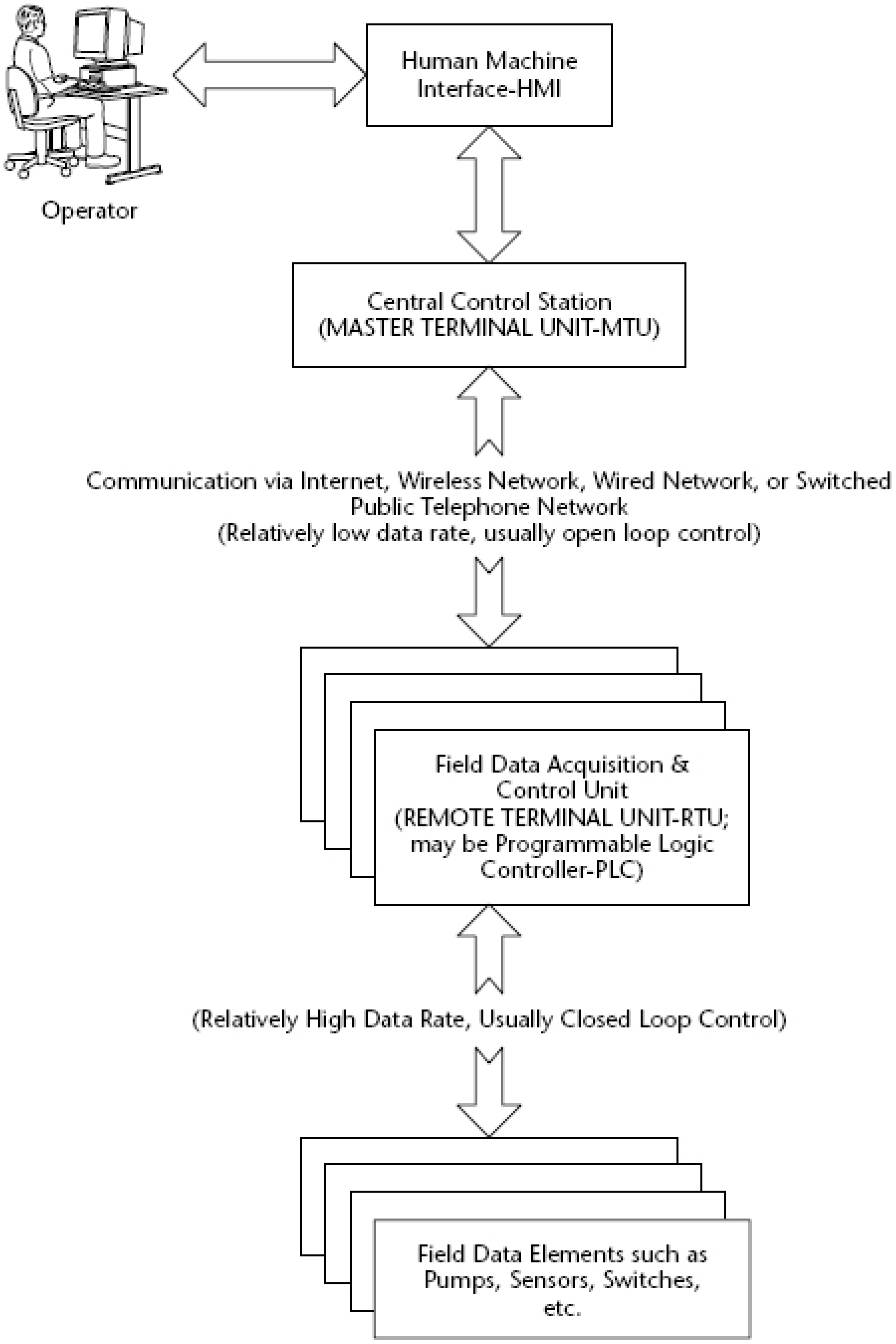
Operator
Human Machine Interface-HMI
Central Control Station (MASTER TERMINAL UNIT-MTU)
Communication via Internet, Wireless Network, Wired Network, or Switched Public Telephone Network
(Relatively low data rate, usually open loop control)
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
(Relatively High Data Rate, Usually Closed Loop Control)
Field Data Elements such as Pumps, Sensors, Switches, etc.

Figure 1-3 Typical SCADA system architecture

SCADA Applications

SCADA is pervasive throughout the world. As discussed previously, it permeates the world’s critical infrastructures, monitoring and controlling a variety of processes and operations. Examples of common SCADA systems are shown in Figures 1-4 through 1-8 to illustrate the diversity of their application domains. However, it is useful to note the similarities in their architectures.

In some of the examples, the EIA-232 and EIA-485 standards are used. EIA-232, formerly known as RS-232, was developed in the 1960s by the Electronic Industries Association (EIA) as a data communications standard. EIA-232 addresses serial data links and specifies the data exchange protocol, signal voltages and timing, signal functions, and the mechanical connectors to be used. EIA-232 signals are asynchronous with typical data rates of 20 Kbps.

EIA-485 is also an asynchronous serial data communications standard with typical data rates of 10 Mbps and the ability to transmit data over longer distance links than EIA-232. It was formerly known as RS-485.

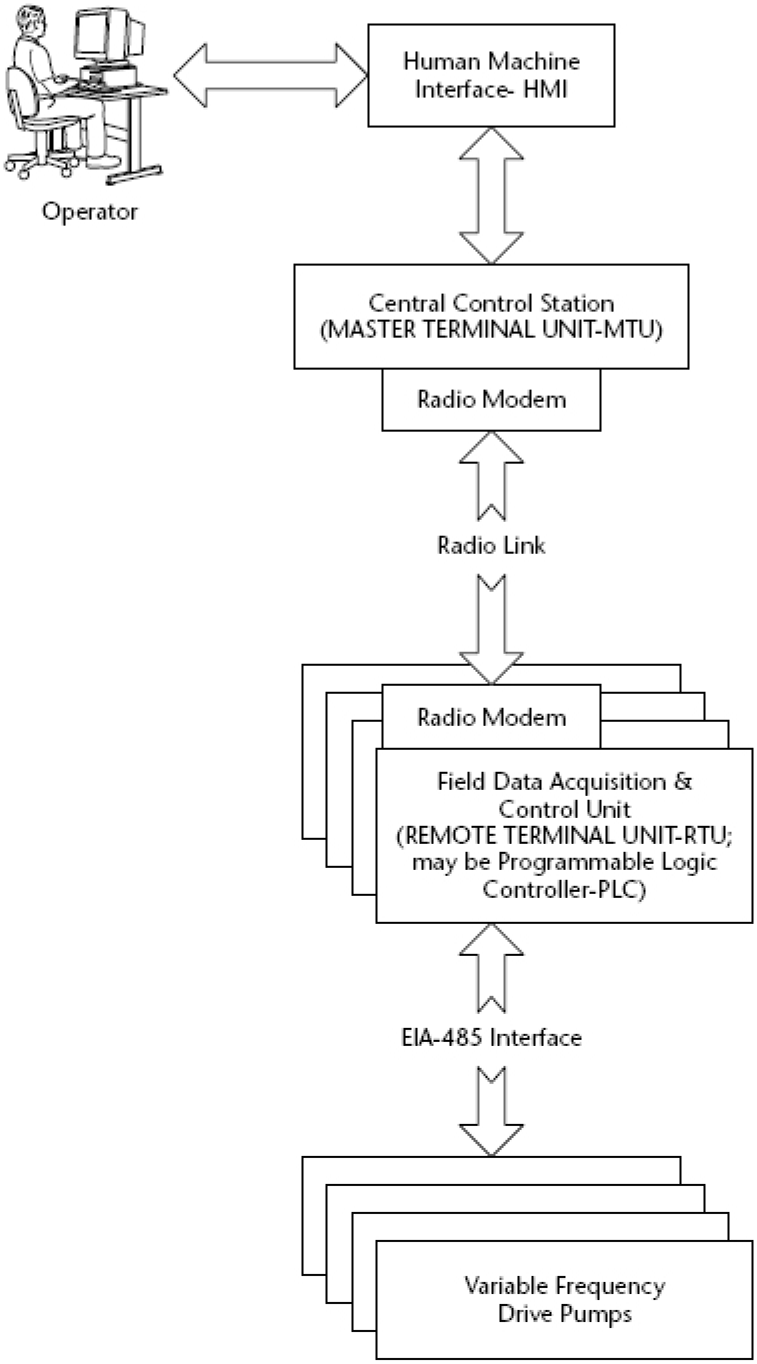
Human Machine Interface- HMI
Operator
Central Control Station (MASTER TERMINAL UNIT-MTU)
Radio Modem
Radio Link
Radio Modem
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
EIA-485 Interface
Variable Frequency Drive Pumps

Figure 1-4 Typical variable frequency drive pump oil field SCADA system

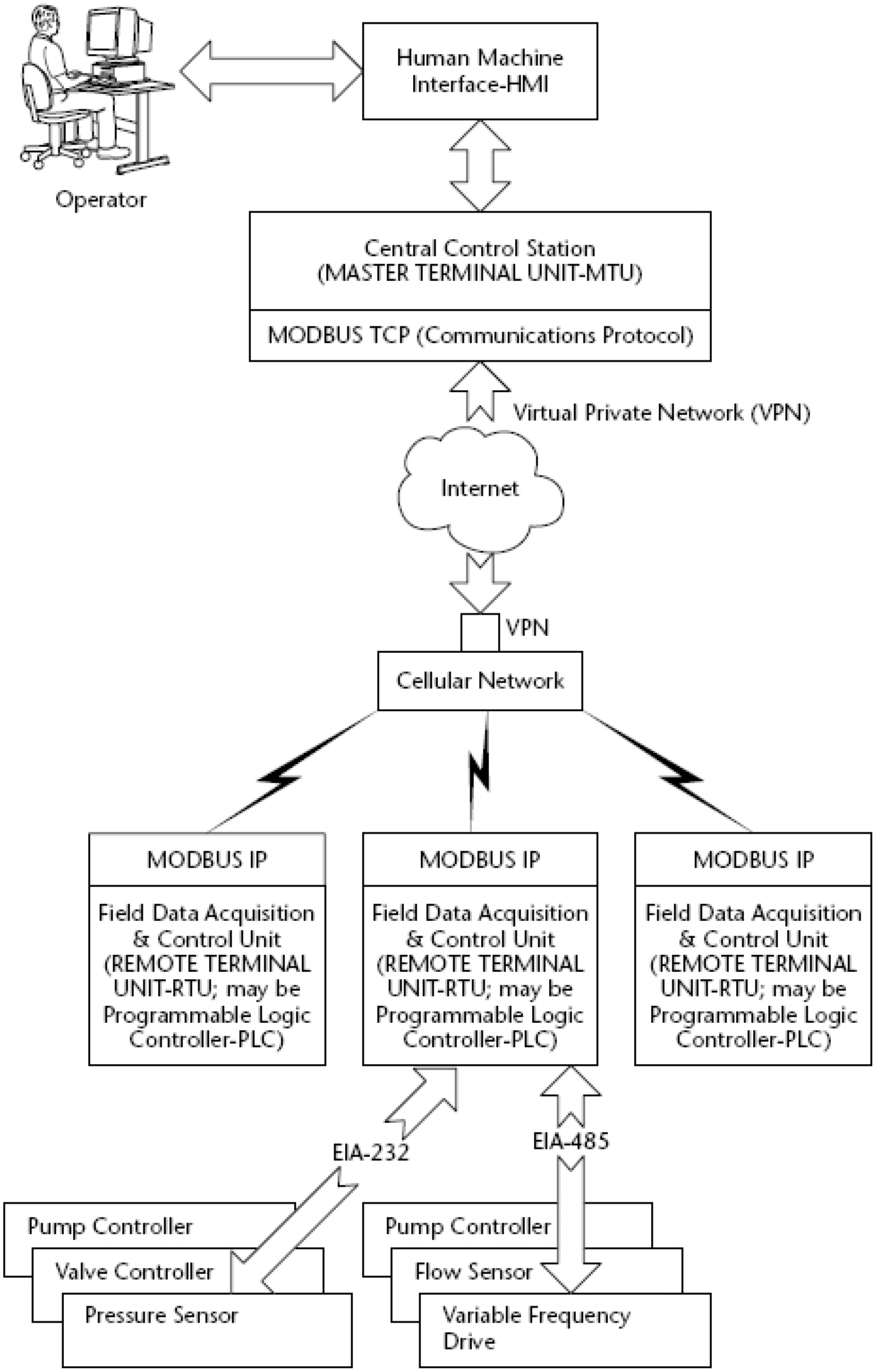
Operator
Human Machine Interface-HMI
Central Control Station (MASTER TERMINAL UNIT-MTU)
MODBUS TCP (Communications Protocol)
Virtual Private Network (VPN)
Internet
VPN
Cellular Network
MODBUS IP
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
MODBUS IP
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
MODBUS IP
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
EIA-232
EIA-485
Pump Controller
Valve Controller
Pressure Sensor
Pump Controller
Flow Sensor
Variable Frequency Drive

Figure 1-5 SCADA system using the Internet and cellular network

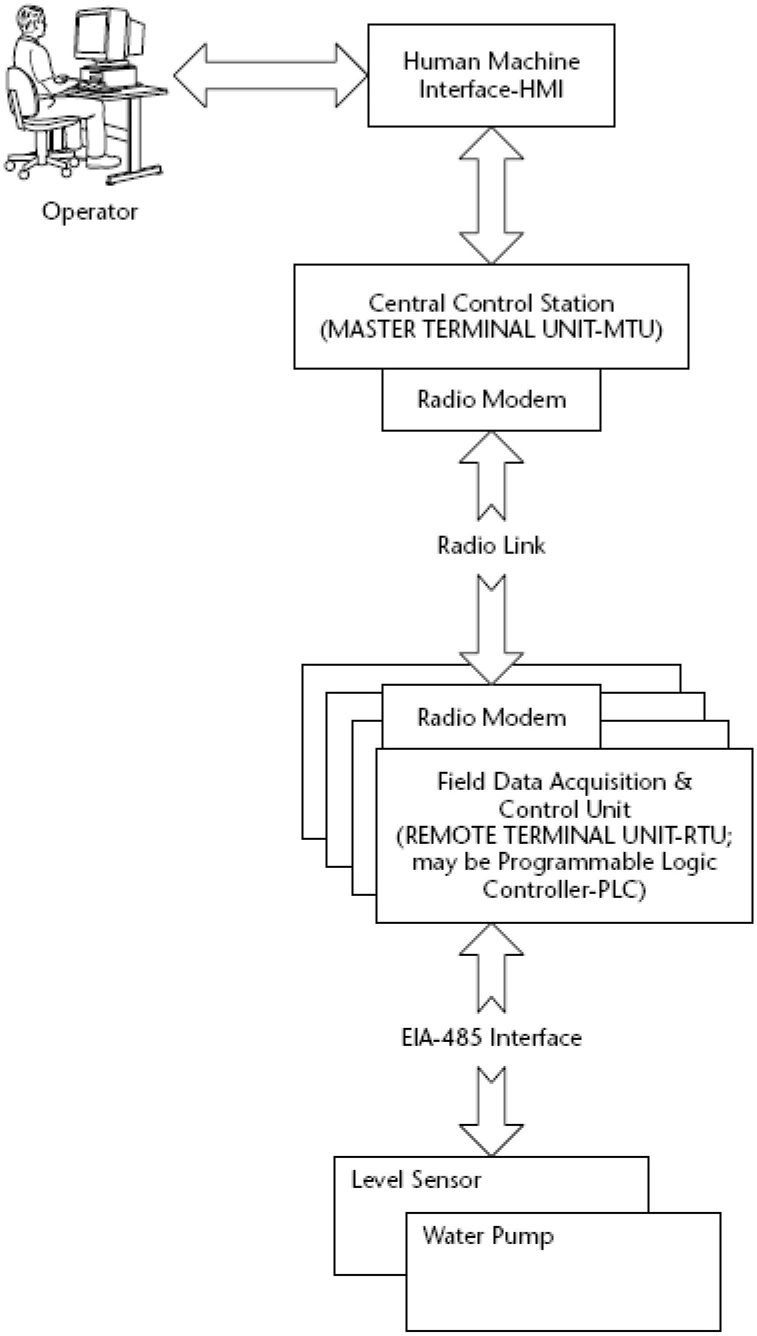
Operator
Human Machine Interface-HMI
Central Control Station (MASTER TERMINAL UNIT-MTU)
Radio Modem
Radio Link
Radio Modem
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
EIA-485 Interface
Level Sensor
Water Pump

Figure 1-6 Water reservoir SCADA system

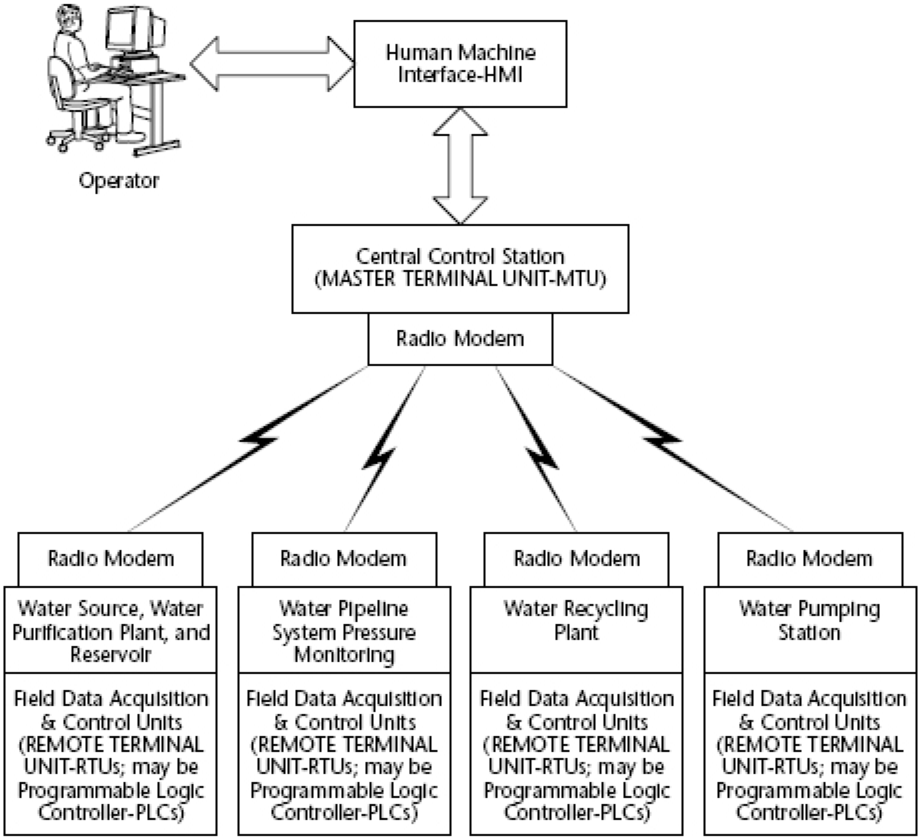
Operator
Human Machine Interface-HMI
Central Control Station (MASTER TERMINAL UNIT-MTU)
Radio Modem
Radio Modem
Radio Modem
Radio Modem
Radio Modem
Water Source, Water Purification Plant, and Reservoir
Water Pipeline System Pressure Monitoring
Water Recycling Plant
Water Pumping Station
Field Data Acquisition & Control Units (REMOTE TERMINAL UNIT-RTUs; may be Programmable Logic Controller-PLCs)
Field Data Acquisition & Control Units (REMOTE TERMINAL UNIT-RTUs; may be Programmable Logic Controller-PLCs)
Field Data Acquisition & Control Units (REMOTE TERMINAL UNIT-RTUs; may be Programmable Logic Controller-PLCs)
Field Data Acquisition & Control Units (REMOTE TERMINAL UNIT-RTUs; may be Programmable Logic Controller-PLCs)

Figure 1-7 General SCADA water treatment facility

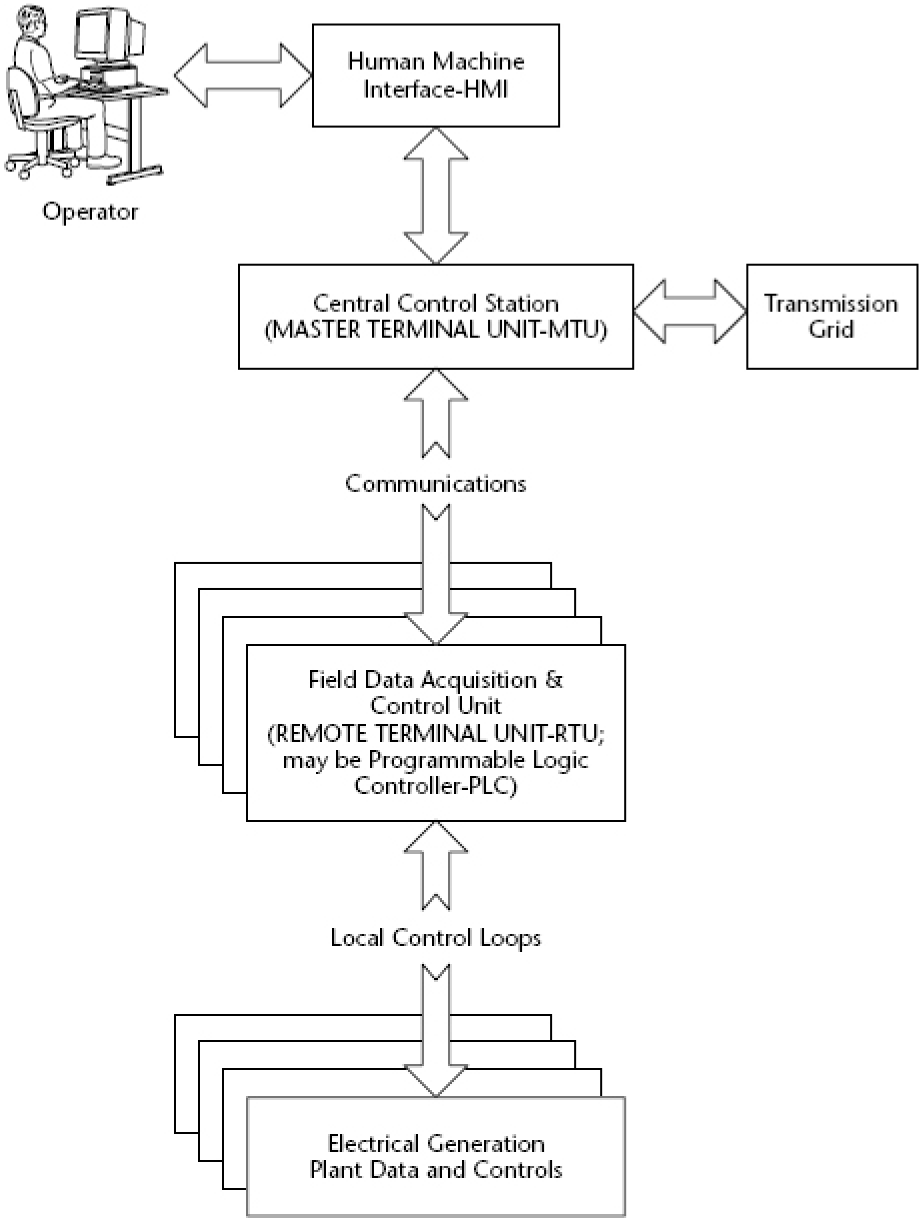
Operator
Human Machine Interface-HMI
Central Control Station (MASTER TERMINAL UNIT-MTU)
Transmission Grid
Communications
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
Local Control Loops
Electrical Generation Plant Data and Controls

Figure 1-8 Electrical generating plant SCADA system

SCADA System Security Issues Overview

For reasons of efficiency, maintenance, and economics, data acquisition and control platforms have migrated from isolated in-plant networks using proprietary hardware and software to PC-based systems using standard software, network protocols, and the Internet. The downside of this transition has been to expose SCADA systems to the same vulnerabilities and threats that plague Windows-based PCs and their associated networks. Some typical attacks that might be mounted against SCADA systems that employ standard hardware and software are listed here:

- Malicious code such as viruses, Trojan horses, and worms
- Unauthorized disclosure of critical data
- Unauthorized modification and manipulation of critical data
- Denial of service
- Unauthorized access to audit logs and modification of audit logs

Most SCADA systems, particularly the local PLCs or controllers, have to operate in real-time or near real-time environments. Thus, they cannot afford delays that might be caused by information security software and that interfere with critical control decisions affecting personnel safety, product quality, and operating costs. Also, plant SCADA system components do not usually have excess memory capacity that can accommodate relatively large programs associated with security monitoring activities.

In summary, conventional information technology (IT) systems are concerned with providing for internal and external connectivity, productivity, extensive security mechanisms for authentication and authorization, and the three major information security principles of confidentiality, availability, and integrity. Conversely, SCADA systems emphasize reliability, real-time response, tolerance of emergency situations where passwords might be incorrectly entered, personnel safety, product quality, and plant safety.

SCADA and IT Convergence

There is an emerging trend in many organizations comprising SCADA and conventional IT units toward consolidating some overlapping activities. For example, control engineering might be absorbed or closely integrated with the corporate IT department. This trend is motivated by cost savings achieved by consolidating disparate platforms, networks, software, and maintenance tools. In addition, integrating SCADA data collection and monitoring with corporate financial and customer data provides management with an increased ability to run the organization more efficiently and effectively.

This integration, however, comes with some difficulty. Relative to information security for example, the security architectures of SCADA and corporate IT systems traditionally have focused on different priorities. With a merging of the two systems, both SCADA and corporate IT use the same security model. Issues such as modems connected to one system compromising the other, the possibility of the corporate Internet connection exposing the SCADA system, the real-time, deterministic requirements of SCADA systems, and the round-the-clock operation of SCADA systems require merging of the disparate cultures of SCADA and IT. A good example of this sort of problem is the routinely scheduled downtime for IT organizations to upgrade software, perform backups, and so on. Such downtime cannot be tolerated in most SCADA systems.

Conventional IT Security and Relevant SCADA Issues

Over the years, information system security professionals developed a number of generally accepted best practices to protect networks and computing infrastructures from malicious attacks. However, these practices cannot be applied directly to SCADA systems without accounting for the different requirements of IT and SCADA systems. The following list provides examples of IT best practices and the state of their application to SCADA systems:

Audit and monitoring logs: After-the-fact analysis of audit trails is a useful means to detect past events. Monitoring, on the other hand, implies real-time capture of data as a system is operating. Both techniques are successfully employed in IT systems. Their application to SCADA systems will yield benefits similar to those derived from their use in IT systems. Because of the varying ages and sophistication of some SCADA system components, many do not have logging capabilities. The cost of installing, operating, and maintaining extensive auditing and monitoring capabilities in a SCADA application must be weighed against the potential benefits.

Biometrics: Biometrics are attractive because they base authentication on a physical characteristic of the individual attempting to access relevant components of a SCADA system. Currently, biometrics are promising, but are not completely reliable. Depending on the characteristic being examined, there might be a high number of false rejections or false acceptances, throughput problems, human factor issues, and possible compromises of the system. However, the technology is progressing and biometrics should become a viable option for controlling SCADA system access.

Firewalls: Firewalls can be used to screen message traffic between a corporate IT network and a SCADA network. Thus, in many instances, a firewall can protect SCADA systems from penetrations that have occurred on the corporate side. Some issues that have to be considered when applying firewalls to SCADA systems are the delays introduced into data transmissions, the skill and overhead required set up and manage firewalls, and the lack of firewalls designed to interface with some popular SCADA protocols.

Intrusion detection systems: Intrusion detection systems (IDSs) are either host-based or network-based. A host-based IDS can detect attacks against the host system, but does not monitor the network. Alternatively, a network-based IDS views the network by monitoring network traffic and assesses the traffic for malicious intent. IDSs are useful in protecting SCADA systems, but cannot be universally applied because, at this time, IDSs are not available for some SCADA protocols. As with other safeguards, IDSs might slow down certain SCADA operations and their cost and operation have to be weighed against the potential benefits derived from their use.

Malicious code detection and elimination: The computational overhead associated with detecting and eliminating malicious code that might infect a SCADA system can seriously affect the real-time performance of SCADA system components. Activities such as running antivirus software, updating virus signature databases, and quarantining or deleting malicious code require time and computing cycles that might not be available on SCADA system components. Updating virus databases from the Internet also exposes the SCADA systems to additional viruses and attacks from the Internet. Again, the cost of antivirus implementations must be weighed against the perceived SCADA risks and benefits of such software.

Passwords: In a SCADA environment, a control operator might need to enter a password to gain access to a device in an emergency. If the operator types in the password incorrectly a few times, a conventional IT security paradigm, which presumes an intruder trying to guess the password, is to lock out the operator. Locking out the operator is not a good thing in real-time control environments. For operators on local control devices, passwords might be eliminated or made extremely simple. At the supervisory level, better and longer passwords might be used, two-factor authentication employed, and challenge-response tokens used. In situations where the passwords might be subject to interception when transmitted over networks, encryption should be considered to protect the password from compromise.

Public-key cryptography: With public-key or asymmetric-key cryptography, there is no need to exchange secret keys between sender and receiver. A public key is available to anyone wishing to communicate with the holder of the corresponding and mathematically related private key. The private key is protected and known only to the receiving party. The main feature of public-key cryptography is that it is virtually impossible to derive the private key from the known public key. Public-key cryptography also provides the ability for a sender to digitally sign a document and transmit it for anyone to read who can access the sender’s public key. This signing guarantees that the document was sent by the owner of the private key of the public-key-private-key pair. As one can deduce, key management, including certification that the public key actually belongs to the named person, is an important issue that has to be handled by the organization. Relative to SCADA operations, public-key cryptosystems require relatively long processing times that are incompatible with the real-time requirements of control systems. Symmetric-key cryptosystems, discussed in the next section, are more suitable for use in the SCADA environment.

Symmetric-key cryptography: With symmetric-key cryptography, also known as secret-key cryptography, the sender and receiver have to share a common, secret key. This key is used to encrypt the message at the transmitting end and decrypt the message at the receiving end. Thus, the secret keys have to be distributed securely from all transmitters to all receivers. This distribution is a concern. One popular solution is to use public-key cryptography to distribute the secret key and then use symmetric-key cryptography to send the message. Because the key length is relatively short compared to the messages, time is not an issue with public-key cryptography. Symmetric-key cryptography is orders of magnitude faster in operation than public-key cryptography. Symmetric-key cryptography has not yet been widely applied to SCADA systems. It is applicable to data transmitted over a long-distance SCADA network and is not as important in local plant control loops. Symmetric key encryption will be applied to the critical portions of a SCADA network.

Role-based access control: This type of access control is gaining popularity in government and industry sectors because of its ability to accommodate changes in personnel and organizations. In this type of security control, access is based on the role of a person in an organization rather than the identity of the individual. It has not yet been widely applied to SCADA systems but holds promise for use at the supervisory level of SCADA operations.

Redundancy as a Component of SCADA Security

In addition to technical and administrative security controls, various physical security measures can be applied to protect SCADA systems.

Backup, duplicate, geographically separated control centers can provide redundancy and, therefore, protection against human attacks and natural disasters. On a smaller scale, a hot backup standby SCADA system at the supervisory control center provides a means to continue operating if the primary system is disabled. As an additional security layer, the SCADA control center could be located in a remote area in an unmarked, inconspicuous building.

SCADA System Desirable Properties

Figure 1-9 summarizes the general state of SCADA at this time. The figure depicts a typical SCADA system that incorporates standard hardware and software platforms, such as PCs and Windows. The SCADA system is linked to external networks, corporate IT operations, and remote, possibly insecure, access points such as modems. Because standard hardware and software are used, the equipment is vulnerable to the same attacks that historically have been mounted against PCs and Windows.

A successful, unauthorized penetration of a SCADA system could result in an intruder taking control of a master or slave unit, disrupting critical processes, falsifying data, and even initiating actions that could result in the loss of human life and destruction of the plant under control.

A good description of the desired properties of a SCADA system is given in the North American Electric Reliability Council (NERC) definition of SCADA reliability objectives. Even though the definition addresses the electric utility industry, the properties can be extrapolated to all components of a nation’s critical infrastructure. NERC Form 715 defines reliability as:

- **Adequacy:** The capacity to meet system demand within major component ratings in the presence of