SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2014; **7**:175–194
Published online 24 January 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.698

SPECIAL ISSUE PAPER

SCADA communication and security issues

Jingcheng Gao[1], Jing Liu[1], Bharat Rajan[1], Rahul Nori[1], Bo Fu[1], Yang Xiao[1]*, Wei Liang[2] and C. L. Philip Chen[3]

[1] Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA
[2] Shenyang Institute of Automation Chinese Academy of Sciences, Shenyang, Liaoning, China
[3] Faculty of Science of Technology, University of Macau, Macau

ABSTRACT

Supervisory control and data acquisition (SCADA) systems are widely used to monitor and control industrial processes. They provide the key functionality of real-time monitoring, logging/archiving, report generation, and automation for smart grid, which is a promising power delivery system for the near future. On the basis of these functionalities, various SCADA architectures, including hardware and software architecture, have been proposed and standardized; however, the most open and expediently growing areas in the smart grid are the infrastructure and technologies for the SCADA communication and security. In this paper, we provide a review for many documented standards in SCADA, and we also review its state-of-the-art communication and security aspects. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS
SCADA; smart grid; communication; security

***Correspondence**
Prof. Yang Xiao, Department of Computer Science, The University of Alabama, 101 Houser Hall, Tuscaloosa, AL 35487–0290, USA.
E-mail: yangxiao@ieee.org

1. INTRODUCTION

The technical aspects of a power grid are fast changing and generally inspired by the technological evolutions in the market and in the corresponding usage on informational technologies (ITs). To stand up to these changes, computer systems, which is also called supervisory control and data acquisition (SCADA) systems, are being developed. Closed, isolated, and single user-based architectures are changing into interlinked, standardized systems that support new functionalities, and they are also user friendly and cost efficient. SCADA systems are widely used in industry for monitor and control industrial processes, especially for a plant or for its equipment, such as telecommunications, water and waste control, energy, oil and gas refining, and transportation [1–3]. SCADA systems were deployed among power delivery systems several decades ago in the United States. To date, many such advanced systems and their applications have been developed worldwide. Smart grid is a promising power delivery system for the near future. Building a robust and secure SCADA system is therefore a key to the development of the smart grid.

SCADA systems in power grids have been in use in the United States for long enough—the past five decades. The development in corresponding IT resources has very rarely made its way into the power industry. The grids and, for that matter, even the SCADA systems still remain old in age. An interest in improving the national power grids to make them smart and productive has cropped up in the past 10 years. SCADA systems are a general sensory network with a distributed control system coupled on them. It forms the basic component of control, and it acts as an interface between the user and the actual systems. The systems are generally designed to be event driven. For example, the sounding of an alarm or a warning signal requires a corresponding action. This property of the SCADA systems tends to make it domain specific.

Besides SCADA, there are some other similar systems. For example, process control systems (PCSs) are complete sets of systems that from a centralized location are able to monitor remotely and take measurement of some remote sensors. The major distinguishing factor is that SCADA systems are spread in a very large geographical area. These systems make the critical structure that is related to power, water and sewage utilities, transportation services, and many more facilities that make our daily life lot easier. Distributer control systems (DCSs) and industrial control systems also form a subset of the major PCS systems. They differ in the fact that they offer many more geographically based services when compared with SCADA. There are many related works in these areas [4–55].

In this paper, we provide a review for many documented standards in SCADA, and we also review its state-of-the-art communication and security infrastructure. SCADA architectures are vulnerable to security attacks by humans or malicious software programs. We intend to account for various possibilities that can occur in a smart grid system and to suggest strategies to tackle these threats. Security breaches in smart grid systems may result in large scale blackouts, and in some cases, they may also be a threat to national security. Analyzing causes for these threats becomes a necessity before a designer can actually implement a smart grid system. A detailed study on SCADA system security acts as the preliminary requirement to any smart grid system implementation. This survey covers web-based, Internet-based, asynchronous transfer mode (ATM)-based, Terrestrial Trunked Radio (TETRA) network-based, wireless-based, and even cell phone-based SCADA communication networks.

The rest of the paper is organized as follows. We provide an introduction of SCADA in Section 2. Section 3 introduces SCADA architecture. We discuss SCADA communication standards and technologies in Section 4. Some SCADA communication applications are discussed in Section 5. We discuss SCADA security issues in Section 6. Section 7 presents some securing SCADA communication standards. The examples of SCADA security applications are in Section 8. We conclude our work and present future work in Section 9.

2. INTRODUCTION OF SCADA

1.1. SCADA functionality

This section was base on the materials in [3]. SCADA functionality includes access control, multimedia interface, trending, alarm handling, logging/archiving, report generation, and automation explained as follows [3].

Access control: users are allocated among groups that have defined read/write access privileges to the process parameters in the system and often to specific product functionality [3].

Multimedia interface: multimedia interface supports multiple screens, which can display combinations of synoptic diagrams and text [3].

Trending: most of the SCADA products provide trending facilities, and one can use it to summarize the common capabilities in a chart or a figure [3].

Alarm handling: alarm handling is based upon limit and status checking, and it is performed centrally in the data servers [3]. In other words, the information only exists in one place, all users see the same status (e.g., the acknowledgement), and multiple alarm priority levels (in general many more than three levels) are supported. It is usually possible to group alarms and to handle these as aggregation. E-mails can be generated, and predefined actions can be executed automatically in response to alarm conditions.

Logging/archiving: logging can be described as the medium-term storage of data on a disk, and archiving can be described as the long-term storage of data either on a disk or on another permanent storage medium [3]. Logging is typically performed on a cyclic basis. In other words, once a certain file size, period, or number of points is reached, the data are overwritten [3]. Logging of data can be performed at a set frequency, or it can be initiated only if the value changes or if a specific predefined event occurs. Logged data can be transferred to an archive once the log is full. The logged data is time stamped and can be filtered when viewed by a user. The logging of user actions is, in general, performed together with either a user ID or station ID.

Report generation: one can send reports by using Structured Query Language (SQL) type queries to the archive, real-time database, or logs [3].

Automation: many of the products allow actions to be triggered automatically by events [3].

1.2. Advanced SCADA systems

SCADA systems have been evolving since they were created. The paper [56] summarizes that distributed architecture and multimedia are two dominate techniques that would influence the SCADA systems. The paper [3] reviews that SCADA is adopting Web Technology, ActiveX, and Java in the products and also adopting object linking and embedding for process control as a means of communication between client and server modules. The paper [57] argues that the future SCADA is not a stand-alone system, but rather, it is incorporated with a deep level implementation of information flows within the substation system featuring the advanced communication technologies.

Recent SCADA systems have shown a feature that many new technologies have applied into systems to make them more real-time, productive, robust, and secure. For example, those new technologies include advanced systems such as SCADA systems based on Internet [58–60], Intranet-based SCADA [61], web-based SCADA [62], industrial Ethernet-based SCADA [63], web-based SCADA display system via Internet [64], and so forth.

1.3. SCADA communications

SCADA systems in smart grid are designed to monitor the states and to control behaviors of all the plants over the power delivery systems. Therefore, real-time, precise, robust, and secure communication is the key to the monitoring and controlling processes. It is vital to have an overview of applied and potential SCADA communication standards and technologies. For example, different types of SCADA communication infrastructures within the whole SCADA architecture are the blueprints for building among certain communication standards and technologies.

SCADA communication standards are created by several national organizations:

IEEE C37.1: this standard is designed as an American national automation systems prototype in substations, specification, and analysis of systems used for SCADA and its automation control. It has four versions right now, and they are ANSI/IEEE C37.1-1979, ANSI/IEEE C37.1-1987, IEEE Std. C37.1-1994, and IEEE Std. C37.1-2007 [65].

IEEE Std. 999–1992: this standard provides a recommended practice for SCADA communication [66].

NCS TIB 04–1: the National Communication System (NCS) has released a Technical Information Bulletin 04–1 for the SCADA systems. It covers recent overviews of the SCADA architectures and protocols that implement the communication [1].

Other than the aforementioned national standards, many researchers have either proposed new communication technologies for the SCADA communication system or adopted advanced communication techniques for existing SCADA communication infrastructures.

1.4. SCADA security

Like any system, a SCADA system tends to be prone to attacks of various forms including physical attacks by a human or by malicious software that can harm the system or use up the system's resources. Any of these forms of disruption that happens to a SCADA system can be highly dangerous [67]. Threats, such as fiddling with billing information of particular users, can cause a major economical disturbance if not monitored carefully [67]. The power grids, on the other hand, are a major resource to national defense, and any form of attack on these can cause havoc. Attacks on SCADA systems have increased by at least 10 times since the beginning of the 21st century [67].

The major issue is that most of the SCADA systems were set up years before advances of computers and communication networks so that SCADA systems did not evolve as fast as those in the computer systems and communication networks. Although restriction on the physical access to early SCADA systems was believed to be secure, current communication capability and remote access capability cause harder security issues. The common methods are prevention methods via restriction on the unauthorized access. People tend to undermine vulnerabilities in the SCADA systems caused by the complex network infrastructures. Therefore, many security breaches occur recent year.

It becomes a difficulty to justify how secure a SCADA/power system is. It is possible to define security levels by analyzing the reliability of a power system. The analysis provides us with a means to analyze when and if power failures occur, and this analysis becomes a major factor in providing service to the customers [68]. Failure of a SCADA system generally occurs when the operator of a power system is unable to retrieve data from or send data to the basic productivity plant or even the controlling units and the customer accessible infrastructures of the grid [68]. To restore any of the loads, the control information and the usage or failure information is very crucial. The bus system connecting the various infrastructures is analyzed by comparing the availability of the controlling paths throughout the SCADA systems [68]. This system would contain the master stations, communication networks, remote terminal units (RTUs), wide area networks (WANs), and the other basic infrastructure components of the grid.

3. SCADA ARCHITECTURE

The traditional SCADA system is composed of a central host computer and a number of RTUs, the operator terminals, and/or programmable logic controllers (PLCs) [1,2], which are shown in Figure 1. Some key components are as follows [1,2]:

SCADA meter: used for gathering data from a plant (acquiring) and sending commands (control) to a plant.

RTU: used for connecting to sensors in the plants, converting sensor signals to digital data, and sending digital data to the supervisory system.

PLCs: used as field devices because they are more economical, flexible, and configurable than special-purpose RTU.

Communication infrastructure: used for connecting the supervisory system to the RTUs and/or PLCs.

A proper understanding of SCADA is necessary to analyze the various security threats that need to be addressed. Figure 2 shows scada architecture in modern power grids.

A SCADA system is a centrally controlled master system that commands terminal RTUs, and these RTUs include relay devices, actuators and sensors, circuit power breakers, voltage regulators, and so forth. Master terminal units (MTUs) are higher level units, including supporting applications, human machine interfaces (HMIs), data storage, and acquisition systems. PLCs are used as control sensory devices and RTUs. Programmable automation controllers are used as the basic controlling unit.

There are three generations of SCADA system architectures. The first generation uses the WAN for communication between MTUs, which execute decision making, and RTUs, which serve the end users. The second generation uses local area networks (LANs) to communicate between MTUs and RTUs. The third generation uses WAN and Internet protocol (IP).

The components of the SCADA architecture include the following: (i) on-field devices, for example, RTUs, PLCs, intelligent electronic devices (IEDs), and Process Automation Controllers (PACs); (ii) monitoring and controlling equipment, for example, HMI, historian, controller for SCADA, and real-time data processor; and (iii) communications, for example, Inter-Control Center Communications Protocol (ICCP), Odyssey Commutation Processor (OCP), Ethernet, wireless networks, serial network connections, and Modbus and DNP3 protocols. The terminal controller unit is responsible for communicating, analyzing the data, and displaying the occurring events to the users as well as the service providers. The

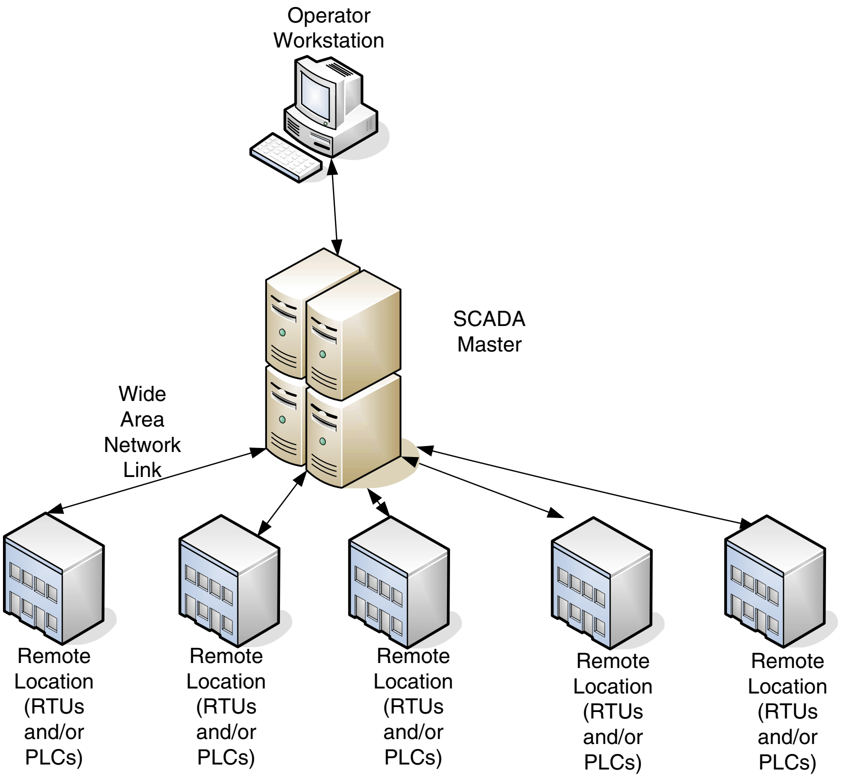

Operator Workstation
SCADA Master
Wide Area Network Link
Remote Location (RTUs and/or PLCs)
Remote Location (RTUs and/or PLCs)
Remote Location (RTUs and/or PLCs)
Remote Location (RTUs and/or PLCs)
Remote Location (RTUs and/or PLCs)

Figure 1. A typical SCADA system [1].

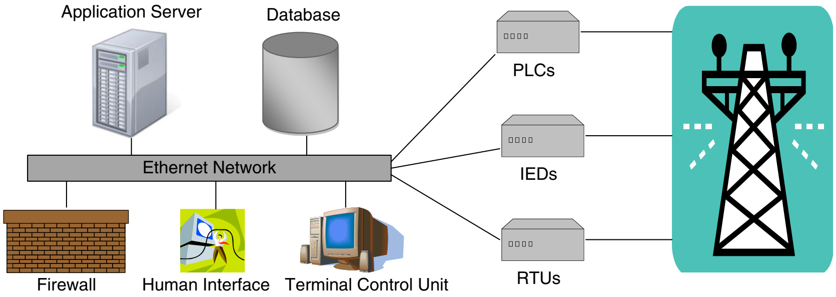


Figure 2. SCADA architecture in modern power grids.

devices are generally controlling and controlled devices, which run on embedded operating systems to communicate data using various controlling protocols, such as Modbus and DNP3.

To ensure that SCADA systems are well maintained, security measures should be given special importance [69]. Attacks on the SCADA system can cause threat to people's safety, a loss of productivity, and even some environmental damage [69]. Some basic network systems (e.g., ports, hubs, switches, routers, firewalls, and the Simple Network Management Protocol (SNMP)) are also general, electrical power grid components that are at risk of being attacked.

The interconnection of microprocessors used in SCADA has been an increasing trend in recent times, and this interconnection makes the SCADA system less secure [69]. PLCs and DCSs used as process controllers have been replaced by IEDs, which are generally applied to control power meters, to control power stations, and to trace heat [69]. Power meters, wireless LANs, IEDs, relay networks, and Master Control Centers (MCCs) are interconnected in SCADA when setting up power grids [69]. With all these devices being interconnected, the network of a SCADA system is becoming less isolated and, thus, becoming prone to attacks [69].

3.1. Hardware architecture

One is able to distinguish between two basic layers in a SCADA system: the *client layer*, which caters to the human–machine interaction and the *data server layer*, which handles most of the process data control activities. The data servers communicate with devices in the field through process controllers. Process controllers (e.g., PLCs) are connected to the data servers either directly or via networks or fieldbuses that are proprietary (e.g., Siemens H1) or nonproprietary (e.g., Profibus) [3]. Data servers are connected to each other and to client stations by means of an Ethernet LAN. The data servers and client stations are NT platforms, but for many products, the client stations may also be Win95 machines. Figure 3 shows typical hardware architecture.

3.2. Software architecture

The products are multitasking and are based upon a real-time database that is located in one or more servers. Servers are responsible for data acquisition and handling (e.g., polling controllers, alarm checking, calculations, logging, and archiving) on a set of parameters, which are typically those to which they are connected [3]. Figure 4 shows the software architecture [3].

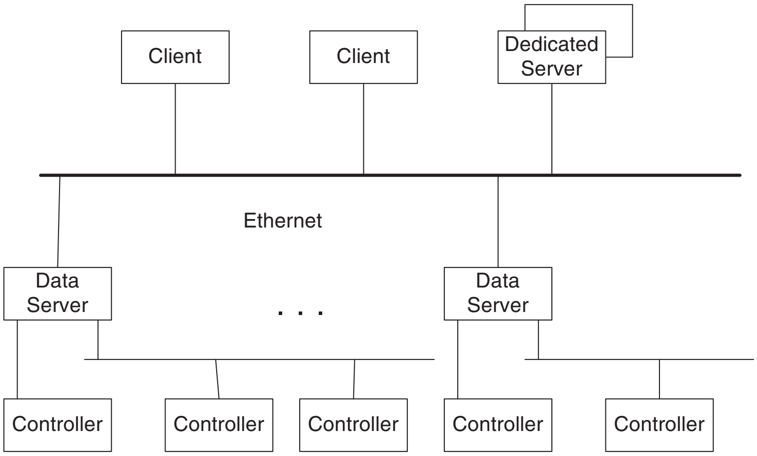


Figure 3. A typical SCADA hardware architecture [3].

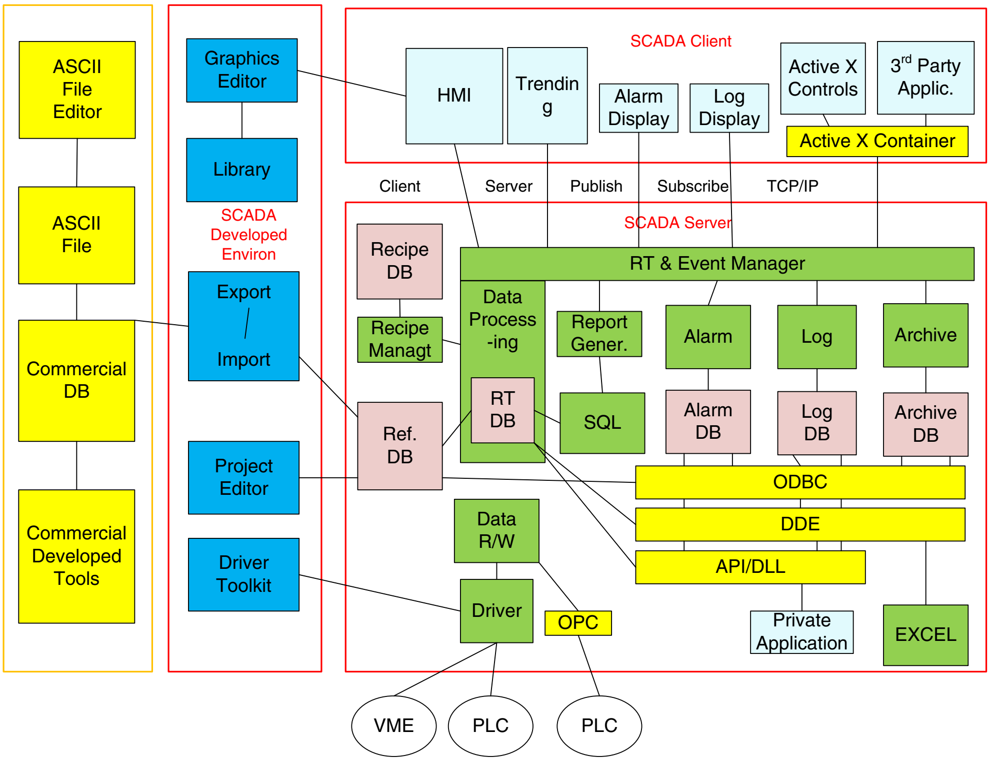
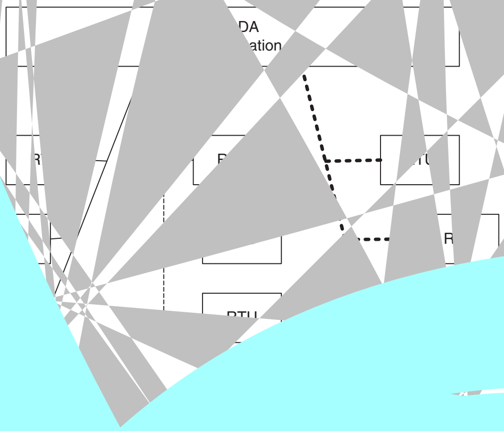


Figure 4. Generic software architecture [3].

3. Co[illegible]ation i[illegible]astruct[illegible]

[illegible] typical SCA[illegible] [illegible]mmunication sy[illegible] [illegible]en[illegible] [illegible] c[illegible]is of a master statio[illegible] and [illegible]y other distributed R[illegible] [illegible]. The RTUs [illegible]e interconnec[illegible] to the master sta[illegible] thr[illegible] variety of [illegible]nic[illegible]on channels, such as [illegible]adio [illegible] [illegible]ased lines, [illegible] (as show[illegible] [illegible]5), an[illegible] others [2]. H[illegible] of [illegible]e greates[illegible] [illegible]ication challenges



that [illegible] channel [illegible]its the speed [illegible]f [illegible]ta a[illegible] [illegible]nt[illegible] that can be [illegible] [illegible]d. Furth[illegible]rmor[illegible] [illegible]e channel [illegible] another challe[illegible] [illegible] [illegible]unicati[illegible]n [2].

[illegible] COM[illegible]UN[illegible]CATIO[illegible] S[illegible]S AND T[illegible]ECHNO[illegible]

1[illegible] [illegible]7

[illegible]E Std. C37[illegible] [illegible]HE s[illegible] [illegible]tom[illegible]ation [illegible]n o[illegible] [illegible]ADA system [illegible] system. However th[illegible] [illegible]ernal protectio[illegible] int[illegible] [illegible]own i[illegible] Fi[illegible] SC[illegible]DA system main[illegible] [illegible]s[illegible] [illegible]rt, [illegible]e[illegible] [illegible]ys[illegible]em [illegible]co[illegible] [illegible]e and [illegible] applic[illegible] [illegible]SCADA [illegible]e subsyst[illegible] [illegible]ced [illegible]cation [illegible] datab[illegible] [illegible]igurat[illegible] management) c[illegible] [illegible]d used data [illegible]isition fro[illegible] [illegible]ment, an[illegible] ter[illegible]l [illegible] [illegible]d[illegible] [illegible] o[illegible] [illegible]te (subst[illegible] functions and architecture include HMI, RTU, data concentrator to collect the required data from all substation IEDs and to provide data exchange to other systems, and remote access controller: to enable remote access to substation IEDs for remote configuration, access, and data retrieval, shown in Figure 7 [65].

4.2. IEEE Std. 999–1992

This standard allows geographically dispersed terminals to conduct serial digital transmission in the SCADA systems [66]. These types of systems typically utilize dedicated communication channels, such as private microwave channels or leased telephone lines that are limited to data rates of less than 10 kb [66]. Wideband local networks used for high-speed data acquisition and control functions are excluded. This standard covers communication channels, channel interfaces, message format, information field usage, and communication management [66].

4.3. NCS TIB 04–1

The goal of this Technical Information Bulletin (TIB) is to examine SCADA systems and their potential usage by the NCS to support national security and emergency preparedness communications and critical infrastructure protection [1]. Therefore, after reviewing SCADA architectures, protocols and communication media, and vulnerabilities, they focused on possible strategies for NCS with regard to SCADA systems and their application in a national security and emergency preparedness and critical infrastructure protection environment [1].

4.4. Internet based

Traditional SCADA systems for power utilities relied on data transmission rather than fixed analogue circuits and modems, as shown in Figure 8 [59]. On the other hand, the traditional ones become unfit for today's requirements. Therefore, the use of the Internet or Transmission Control Protocol (TCP)/IP can overcome the limitations of analogue communications and can achieve higher bandwidth and quality communication [58–60].

In particular, the paper [63] proposes that the Ethernet can also be utilized to implement the SCADA communication. Furthermore, the paper [61] applies Intranet technology to the SCADA communication system for a real-time performance and for reliability of supervisory control.

4.5. Web based

Users in electric power companies need to access SCADA data, but problems arise concerning the provision of access to the SCADA data from various locations cheaply and securely [62]. The paper [62] argues that web-based interface from the Intranet can bring SCADA real-time and historical information to users via a single front-end with a familiar web browser, shown in Figure 9.

The paper [64] describes a unique web-based application, which is implemented on the basis of client/server

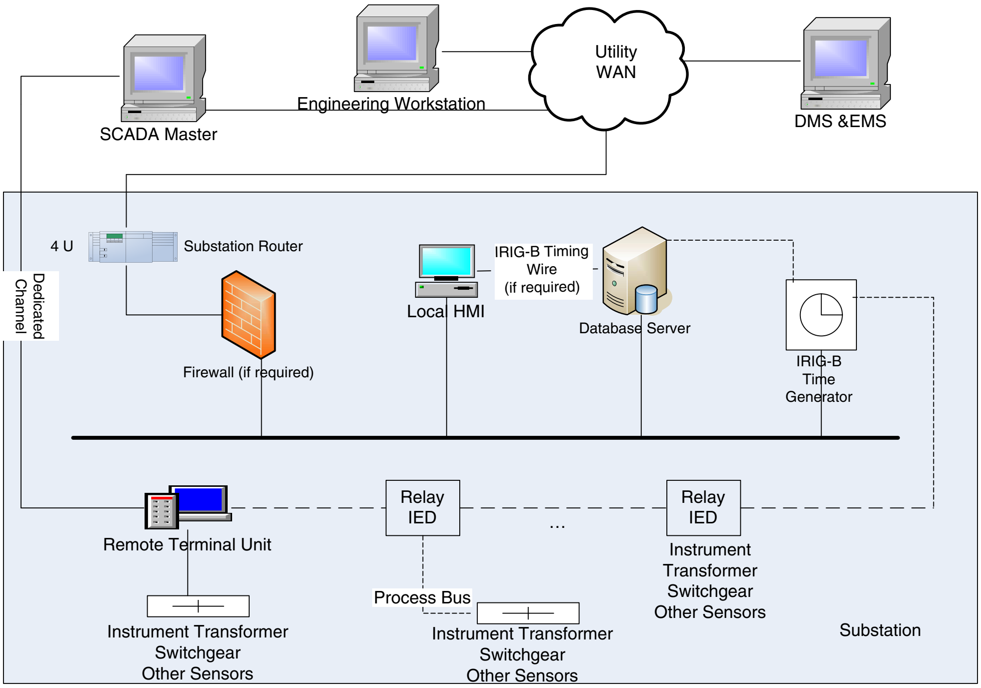


Figure 7. Substation automation system architecture without security shown [65].

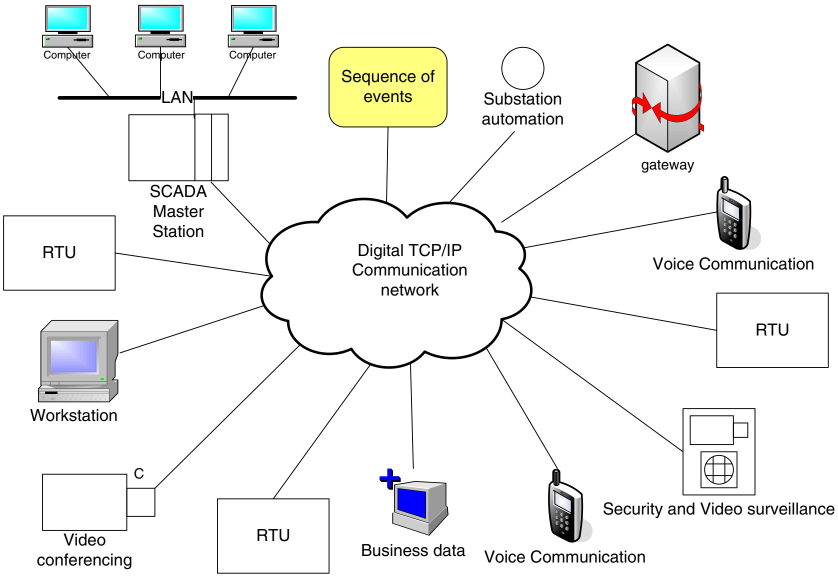


Figure 8. Integrated TCP/IP communication network [59].

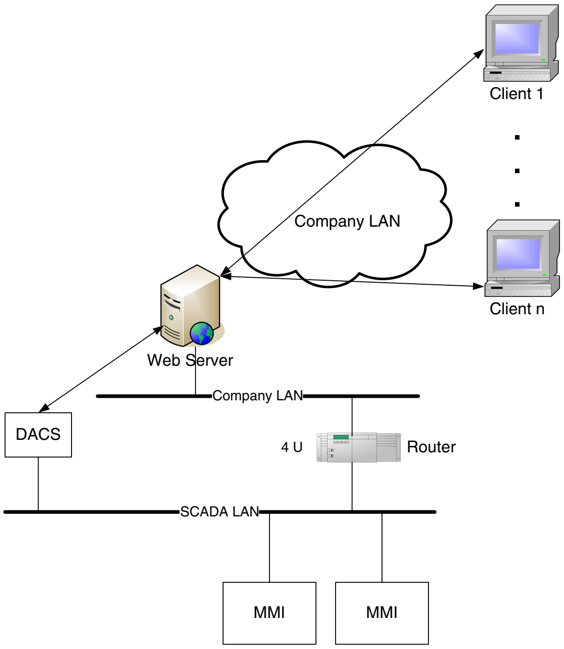


Figure 9. Intranet and SCADA system interconnection [62].

architecture. The user can view the real-time data and can control the operation of the substation at the server site.

4.6. ATM based

ATM network is a true multiservice network that provides broadband services and meets different qualities of service requirements. Therefore, the paper [70] applies it as the communication backbone between geographical information system and SCADA as shown in Figure 10.

4.7. Open and distributed SCADA

On the basis of recent development of computer and communication technology, the authors [71] have developed an open distributed energy management system (EMS)/SCADA system, as shown in Figure 11.

4.8. Wireless SCADA

Wireless technologies have been integrated to SCADA communication systems for monitoring and accessing the performance of remote devices for certain parameters or for remote control of the substations. This technology is known as automation [72–75]. The paper [72] claims that wireless technologies can bring SCADA an inexpensive yet adaptable and easy-to-use infrastructure by using general packet radio service. The hardware components are not complicated, but the customer-written software makes it reprogrammable over the air. It is also able to send and receive control and data signals at nonpredetermined time [72]. The paper [73] applies the wireless SCADA system to conduct the automated meter reading. The papers [74] and [75] both propose that cellular phone networks can be applied to SCADA systems.

4.9. Key management

For efficient and secure requirements of the SCADA network, the papers [76–78] discuss several methods of managing cryptographic keys and give sample cryptographic algorithms that are appropriate for the SCADA system. The paper [77] describes a cryptographic protocol for SCADA links that leverages the cyclic redundancy checks transmitted by existing SCADA equipment to achieve strong integrity with minimal latency. The paper [78] proposes advanced key management architecture for secure SCADA communications.

4.10. Communication technology for SCADA system

The paper [79] provides a technical guideline paper to provide a summary of different communication media available for SCADA communication in terms of advantages and disadvantages, including twisted-pair metallic cables, coaxial metallic cables, fiber optic cables, distribution line carrier, power line carrier, satellites, leased telephone service, very high frequency (VHF) radio (mobile), and microwave radio.

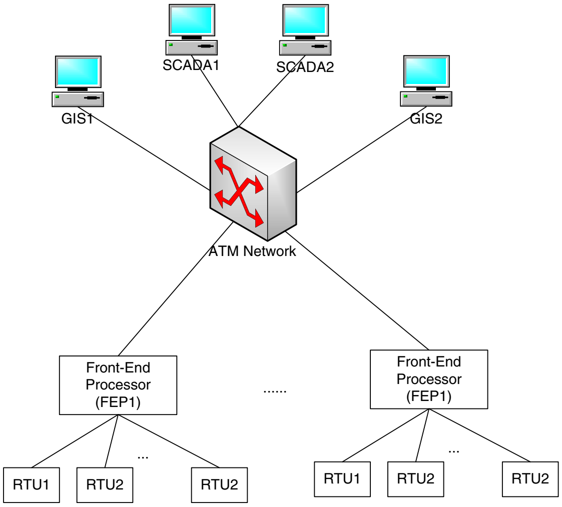


Figure 10. GPS-based SCADA architecture [70].

5. SCADA COMMUNICATION APPLICATIONS AND DATA

5.1. SCADA-based applications

Many new SCADA communication techniques have been developed. Speed and accuracy of under frequency load shedding play a vital role in preserving system stability. The paper [80] utilizes the new SCADA scheme to overcome the shortcomings of previous adaptive under frequency load shedding procedures and to provide a fast but reliable method to maintain the system integrity.

5.2. Data format

This data format is based on the IEEE Std. 999–1992 [66] by which a message protocol is defined to the octet level rather than to the bit level. The paper [2] proposed the same message format with a concise version. Message format, as shown in Figure 12, includes message establishment, information, and message termination [2]. Figure 13 shows the sequence of message for control [2]. Figure 14 shows the sequence of messages for batch data transfer [2]. Figure 15 shows the sequence of message data acquisition [2].

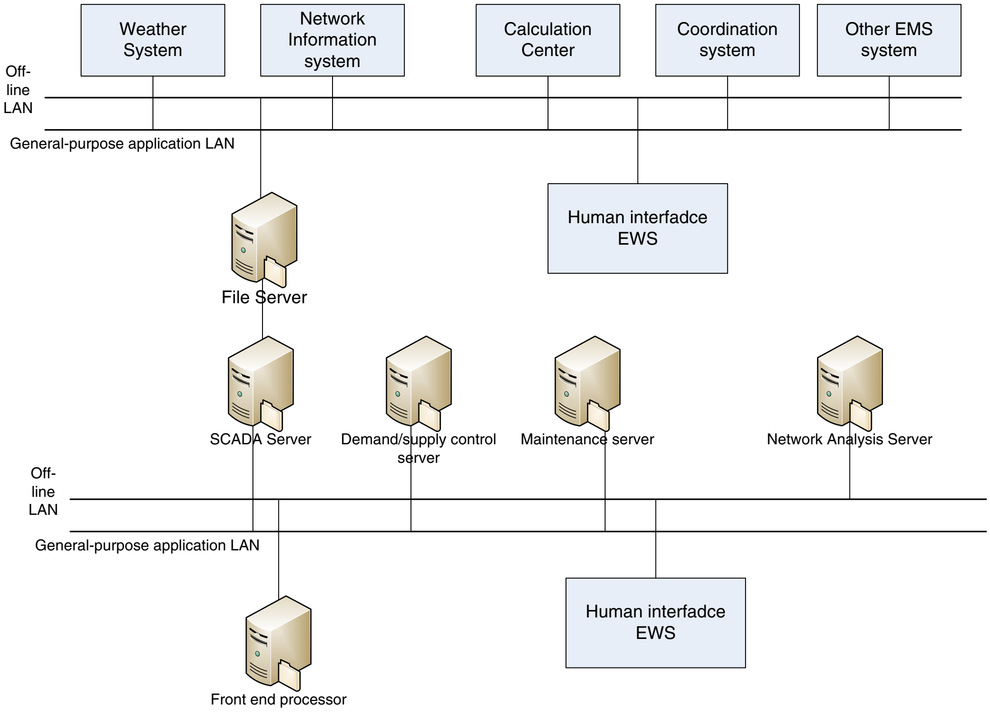


Figure 11. EMS/SCADA system [71].

DOI: 10.1002/sec

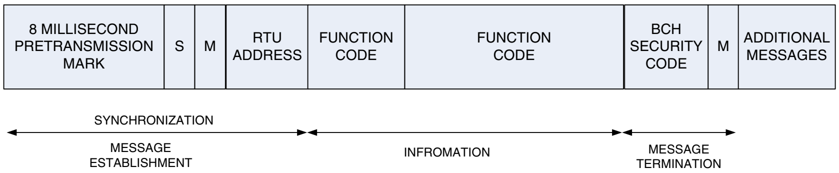


Figure 12. Typical asynchronous message format [2].

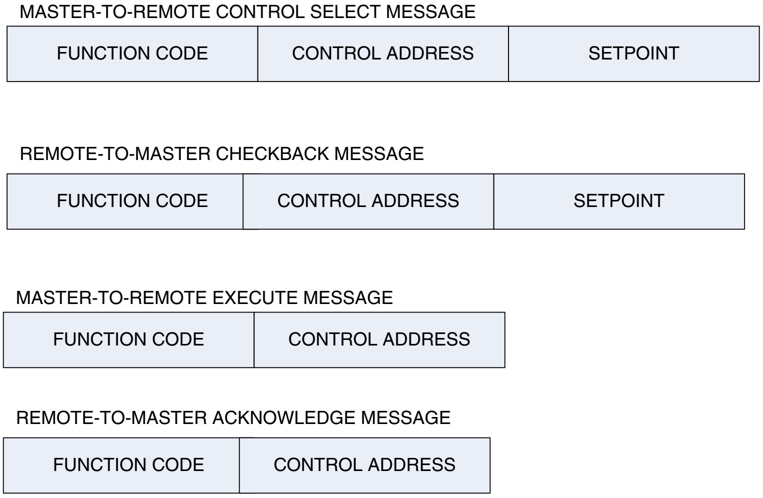

MASTER-TO-REMOTE CONTROL SELECT MESSAGE
FUNCTION CODE
CONTROL ADDRESS
SETPOINT
REMOTE-TO-MASTER CHECKBACK MESSAGE
FUNCTION CODE
CONTROL ADDRESS
SETPOINT
MASTER-TO-REMOTE EXECUTE MESSAGE
FUNCTION CODE
CONTROL ADDRESS
REMOTE-TO-MASTER ACKNOWLEDGE MESSAGE
FUNCTION CODE
CONTROL ADDRESS

Figure 13. Sequence of message for control [2].

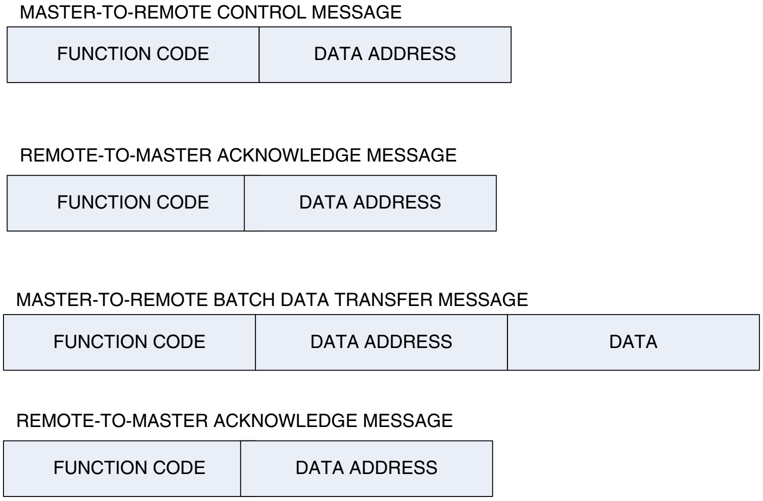

MASTER-TO-REMOTE CONTROL MESSAGE
FUNCTION CODE
DATA ADDRESS
REMOTE-TO-MASTER ACKNOWLEDGE MESSAGE
FUNCTION CODE
DATA ADDRESS
MASTER-TO-REMOTE BATCH DATA TRANSFER MESSAGE
FUNCTION CODE
DATA ADDRESS
DATA
REMOTE-TO-MASTER ACKNOWLEDGE MESSAGE
FUNCTION CODE
DATA ADDRESS

Figure 14. Sequence of messages for batch data transfer [2].

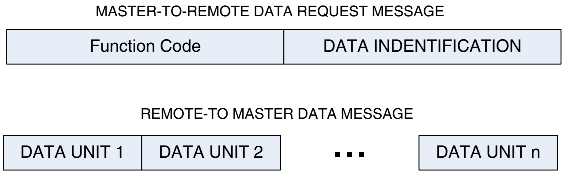


Figure 15. Sequence of messages data acquisition [2].

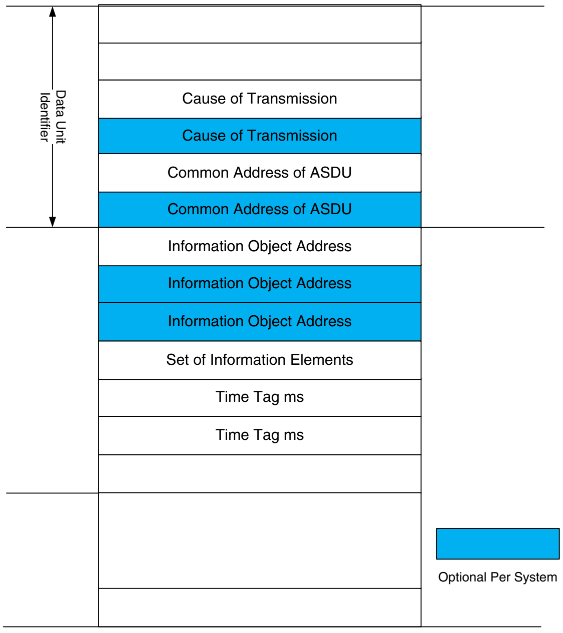


Figure 16. IEC 60870-5-101 [1].

5.3. SCADA protocols

Figure 16 shows IEC 60870-5-101, and Figure 17 shows DNP3 [1].

6. SCADA SECURITY

Because of the isolated nature of the data transfer infrastructure and the systems processing the data, the security of a SCADA system cannot be simply solved by using IT security mechanisms.

Real-time information reporting systems, interconnected systems, and control processing and monitoring systems of SCADA need the Internet, whereas the internetworking increases vulnerabilities. SCADA systems adopt less expensive TCP/IP, Ethernet, and Microsoft Windows for financial reasons, which have a wide variety of vulnerabilities.

Encryption and data access authorization are required for secure communication between the master systems and the RTUs to prevent intruders and malicious software from damaging the system security. System security can

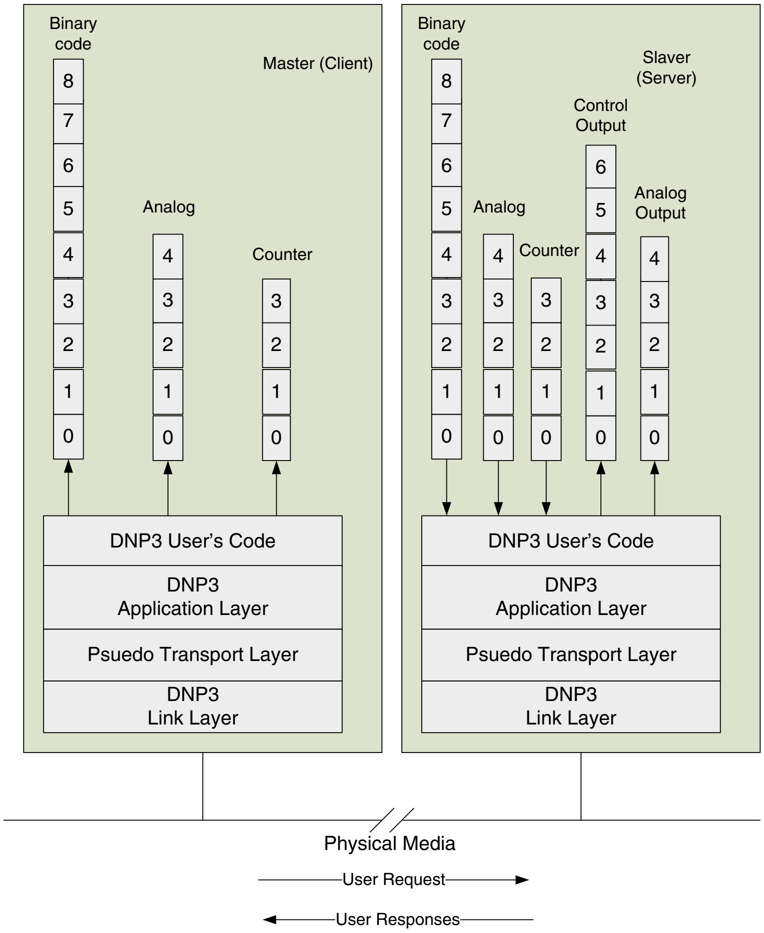


Figure 17. DNP3 layers [1].

be classified into three levels: enterprise, process control, and embedded system [81].

Although being well protected at enterprise level, SCADA security at process control level and embedded system level has rarely been addressed well, and thus, they become major targets of attacks [81]. Before considering the higher level network security issues, we need to review SCADA system requirements: (i) electrical and environmental requirements, (ii) network resilience, that is, the ability of the systems to overcome circuit failures, and (iii) limited response times for the real-time SCADA systems [81]. The design of a system according to the electrical specifications and the general environmental specifications set by the government thus becomes necessary [81].

Security issues in SCADA systems fall into two main categories: direct security threats (e.g., terrorist attacks, destruction of industrial infrastructures, and field device theft) and indirect security threats (e.g., attack by viruses, spywares, and causing system operating code logic errors) [67].

6.1. Attack data

In a realistic situation of a power grid being attacked, data collected by PLCs, DCSs, and RTUs are generally sent to a management group, which is composed of PCs, which can be hacked easily [69]. The British Columbia Institute tracks industrial issues addressing cyber security, and it builds an Internet security incident database (ISID) that has information relating to security-related attacks on networking systems and PCSs [69]. The data of attacks stored in this database are for future reference and for avoiding similar attacks [69]. Attacks to operating systems, applications, and multiple connected networks have been major causes recently [69].

The authors of [81] and [82] presented some examples of attacks that have been reported to ISID. For example, one record shows an SQL slammer worm using four paths in the control systems to attack: (i) a nuclear power plant-processing computer with a contractor's telephone line, (ii) a power SCADA system through a virtual private network (VPN), (iii) a petroleum control system using a laptop, and (iv) a machine HMI using a dial-up modem [81].

6.2. Pathways

The following concludes some pathways by which a SCADA system can be attacked [81]:

- Modems—most modems have been found to have no passwords or only trivial passwords [81].
- Wireless networks—the vulnerability of the systems exposes when an intruder acts as a remote node that is trying to communicate with the central management host [81].
- Third-party connections—the remote support of systems that are accessible by utility vendors or of third-party connections makes the system vulnerable [81].
- VPNs—their level of security is dependent upon the degree of security of the VPN server system. This is a major threat to the overall system safety [81].
- Mobile devices—mobile devices, such as laptops, personal digital assistants (PDAs), and flash drives, come with different security policies and practices [81].
- Internet—many studies, such as those based upon the ISID, have shown that some SCADA control systems get directly connected to the Internet [81].

6.3. Insecurities

There have been many factors that lead to insecurities. The use of embedded operating systems in SCADA results in many additional expenditures because it is tougher to interact with these systems [83]. Therefore, SCADA systems tend to use common operating systems such as UNIX, Solaris, or Windows in control center systems [83]. To increase the bandwidth capacity of the communicating networks, TCP/IP are used instead of the specialized protocols [83]. All these standardizations in SCADA systems cause SCADA security to face the same challenge in traditional IT technologies [83].

With a system connected to share networks, it is becoming difficult to curtail the attacks, and solving these problems is a major goal of SCADA security [84]. The authors of [4] explained the significance of a power relay and the reason why they are the major targets of attackers. Power relays, which are the second most important part of the SCADA RTU, control or isolate the issues in the power grid when some electrical discrepancy arises in the grid [84]. Power relays cut off the faulty area and create an isolation pool that is then restored by general smart grid error correction mechanisms [84]. Power relay is a major target for the attackers to collapse the grid [84].

The following lists some of the common causes of insecurities in SCADA systems [67]:

- Dependency on encrypted messages—the use of IP causes vulnerability [67].
- Segmentation—if one network and control center, which is protected by firewall, is breached, it becomes easy for the other network-connected components to be just as easily attacked [67].
- Unsolved threats—the known vulnerabilities of Windows or UNIX become major entry points for the attackers [67].
- Personnel development—the employees of power grid companies need to be given proper training to maintain the security [67].
- Absence of antivirus software—antivirus tools should be installed and connected to the Internet for downloading updates [67].
- Remote observations disabled—remote control helps to notice attacks executed on the remote system. There are chances of intrusions into the substation or SCADA system that can be accessed remotely [67] [85].

- Inefficient protocols—most of the protocols are not initially designed for security [67].

The easy accessibility of hacking tools causes a rapid increase in interests to misuse the services available to people to save money [86]. It is not surprising that the governments of various countries work together to attack the utility networks of their rival countries [87], [88].

There have been mainly three threats that have been identified [85]:

- Hacking—it can be from individual motivation, and this is where the hackers may simply want to prove to the world that they can cause a threat to the public [85].
- Espionage—it is an outcome of completion between industrial utility service providers or rivaling countries [85].
- Sabotage and vandalism—they are the results of employees motivated to create loss for their companies [85].

In SCADA system, valves are devices that help prevent failures, and circuit breakers are devices that are responsible for preventing the spread of faults through the grid by islanding the faulty part of the connection [85]. After intruding into a grid, the hacker may operate these devices by changing the operational settings [85].

The typical ways of intruding a system are carried out by finding a modem over the available devices or by finding out the company's IP address, which can be publically accessible [85]. Then, the hackers send multiple input messages to figure out the connection type by using the popular dictionary, tools, or brute force password detection algorithms [85]. The length of the password is proportional to the level of the system [85]. The brute force algorithm generates all the possible combinations to find the correct password [85].

6.4. Vulnerabilities

Here, we summarize some key issues of SCADA security. The vulnerabilities in security of software and networks include [89]:

- Viruses, malware, and Trojan horses.
- Logical errors—they are generated during the code writing of the system and may cause unintended or undesired output [89].
- Convenient features for user—they are infections, such as file downloading, from features used by most users [89].
- Reconfiguring the authentication permissions.
- Administrator access.
- Key loggers—install software to log the key-type.
- Denial of Service—use denial of service attack to cause authentic requests to be denied [89].
- Eavesdropping.
- Unsecured wireless network setup.
- Remote access without authentication.
- Leak of confidential information.

Vulnerabilities related to the business staff and personnel include the following [89]:

- Lack of discipline and professional ethics.
- Insider.
- Setting simplified passwords.
- Unnecessary use of SCADA resources.
- Confidential information provided to third parties.

6.5. Solutions

Security could be achieved by password authentication to devices and role-based multiple access control. There are also protocols, for example, IEC-61850, used for communication in a protective relay, better accuracy, and faster performance with improved automated capabilities.

Besides password protections, there are other mechanisms to protect system access [85]:

- Smart cards—smart cards are used to generate a time-varying key or a password [85].
- Encryption—encryption uses public or private encryption-keying mechanisms to achieve secure transmission [85].
- Firewalls—firewalls prevent the transmission of malicious data into the secure parts of the network [85].

The usage of the Internet or Ethernet for communication in SCADA causes the existing threats [81]. It is a necessity to avoid attacks in these networks such as firewalling, VPN, tunneling, authentication, cryptography, and intrusion detection system in these networks [81]. For example, employing a firewall or proxy system may avoid the denial of service attack on SCADA servers [81]. The feature, which is that SCADA systems usually are equipped with their own subnets and IP segments, makes them more secure when compared with general systems built off the Internet, but an attack that gains physical access to the system can rarely be avoided [81].

7. SECURING SCADA COMMUNICATION STANDARDS

This section lists some securing SCADA communication standards that were released by the International Electrotechnical Commission (IEC). These stands are used to avoid massive network collapses and to recover the grid from any insecure issues.

IEC 62351-1 and 62351-2 are used to provide a formal introduction and glossary about the existing security standards in SCADA communications.

IEC 62351-3 introduces security standards for profiles that use TCP/IP. It specifies the usage of transport-level security for all the issues related to confidentiality and authentication-related information.

IEC 62351-4 was used to provide security standards to the profiles by using manufacturing message specification, which is specified in ISO-9506. It allows both secure and nonsecure communications to simultaneously use transport-level security.

IEC 62351-5 deals with IEC-60870-5 and its add-ons. IEC 60870-5 and IEC 60870-6 are the SCADA communication protocols used in the United States and other parts of the world, respectively.

IEC 62351-6 and 62351-7 provide security for peer-to-peer protocols and network system management.

These standards act as a base in determining the respective security threats.

8. EXAMPLES OF SCADA SECURITY SCHEMES

We present some examples of SCADA security applications in this section. Some of these applications require a certain process when applying the system requirement, such as the model-based system [89] and four-step process mechanism [83], and some applications require the use of specific technologies, such as a compromising graph [89] and a firewall [90].

8.1. Model-based system

Industrial service providers often hire consultants to assess system requirements and maintain security [91]. Because the SCADA system generally has a limited number of protocols and applications, some researchers build a model to monitor system behaviors and to find attacks when unexpected behaviors occur [89]. Modbus protocol is used in PLCs and IEDs to provide effective communications in SCADA systems [89].

The researchers build a particular set of models that are supposed to characterize the normal behavior of the systems in normal environments [89]. The approach analyzes the system at constant intervals and computes the system behavior [89]. The model is applicable to networking structures using Modbus protocol [89]. The model-based approach is able to detect all forms of attacks even those that are not expected, such as unknown intrusions [89].

The model is built at protocol level and is characterized by responses given by the system to the requests sent in by the users based upon the service document of the Modbus protocol [89]. The patterns of this model are based upon the predicted communications and historical data [89]. The modeled system observes a change in the expected attack behavior and reports to the control center that there has been an attack [89].

There are a few drawbacks to utilizing a model-based approach. One major problem is the difficulty to maintain all the models that keep track of each of the unexpected attacks [89]. Another major problem is that it might not be possible to provide accurate tracking results if there are too many systems connecting to the network, and as a result, a false positive is generated [89]. This false positive implies a possible attack on the system, and it may cause an unnecessary back-up [89].

8.2. A four-step process mechanism

A four-step process mechanism for SCADA security as shown in Figure 18 is proposed in [83] to mitigate SCADA system errors.

The chain in Figure 18 includes four steps, which have their own individual significances [83]:

- Establishment—to establish a secured system, it is important to build a plan for necessary security features [83]. The assessment of architectures, networks, applications, and infrastructures helps identify potential threats [83].
- Education—the clients and users obtain training from operators of service providers along with consultants and social welfare firms [83]. This process also requires educating the operators, system programmers, and maintenance staff [83].
- Enforcement—to detect an intrusion or malfunction in the system, it is necessary to have the enforcement of detection tools that perform the system scan in an automated fashion [83].
- Evaluation—constant reevaluations of the security measures are also needed [83]. This helps to analyze the success of the security features [83].

8.3. Strategies in control architecture

Various strategies to deal with security issues in control architecture and their application are proposed in [69]. The major stages in the assessment procedure are as follows [69]:

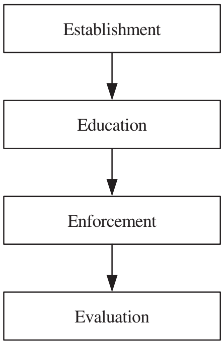


Figure 18. A four-step process mechanism [83].

- Assessment procedure—it has three stages, which are *assess and define current systems*, *risk assessment*, and *gap analysis* [69].
- Human element—survey a particular set of people about the cyber security issues at a particular location [69].
- List of devices—a list of all the devices used is maintained to assess the various regions that might have security threats based upon the vulnerability of each of the devices [69].
- Architecture—a detailed architecture of the network and the SCADA systems is helpful for the IT administration to realize if the devices are properly functioning [69].
- Device assessment—it examines the devices in SCADA network, such as PLCs, DCSs, IEDs, modems, firewalls, routers, and HMIs [69].

8.4. A schema using compromising graph

A schema to reduce the risks of having a cyber attack quantitatively is proposed in [89], and this security risk is measured quantitatively [89]. The authors of [89] implemented the compromising graph for understanding the risk measurements. A compromising graph is a graph that has nodes as stages of potential attack and edges as the causes for the attack [89]. The causes for the attacks, vulnerabilities, and skill level of the attacker are also considered in this graph [89]. The measurement inspections are made for the following purposes [89]:

- To find an estimation of risk and to find an optimal methodology to reduce the risk along with the framework [89].
- To employ the methodology and to find the risk reduced [89].
- To prove that hackers are assumed in the measurement and to prove that the methodology found has better efficiency [89].

The authors of [89] recognized that the risk associated with the particular attack is also related to the time elapsed to attack the system completely. In other words, the risk varies with time depending upon whether the scenarios are large or small [89].

An example of a compromising graph is shown in Figure 19 [89]. In this compromising graph for SCADA, there are several roots: OC is operator console, DEVW is the developer workstation, APPS is the application server, and DAS is the data acquisition server [89]. The user-level interfaces are the nodes in between, and the targets are the perimeter nodes [89]. Figure 19 represents all the possible ways the attacker can reach the RTU, which is the primary target in the SCADA system [89]. The attacker can potentially reach the RTU by using access to find the root access or by going directly to the root access [89]. It is easy to find the shortest distance in this compromising graph by using existing traditional algorithms [89]. These steps for finding the possible ways an attacker can reach the RTU are repeated for all the other targets in a control system [89].

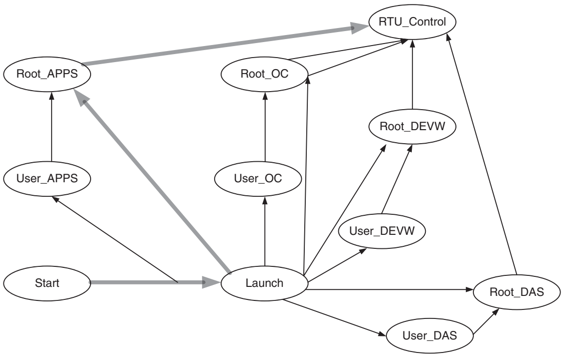


Figure 19. Compromising graph for SCADA [89].

8.5. Firewalls

A survey on firewall deployment for SCADA networks was conducted by the National Infrastructure Security Coordination Center through the British Columbia Institute of Technology [90]. The firewall technique is used to monitor and control data packets to and from a network, and they are designed by keeping the security issues in mind [89]. A firewall can be implemented either by separate hardware connected externally to the network or by software integrated into the operating system of SCADA, which is being secured in the network [89]. Firewalls are utilized to protect process control network (PCN) and enterprise network (EN) from attacks [89]. PCN is a closed system with HMI systems, some data historians, workstations, and also the connecting networking medium [89].

There are several types of firewalls [89]:

- The packet-filtering firewall is the simplest firewall, and it filters the packets depending upon the constraints on the activity control list of the firewall [89].
- The stateful firewall accepts the anticipated data packets that belong to the previous types of firewalls faced [89]. Therefore, stateful firewall is complex to design. It is also called dynamic packet-filtering [89].
- The application proxy firewall segments sections of the data packets depending upon the application that uses the data packet [89]. They also put the data packet together and send it to the requesting application available on the same network [89].
- The hybrid firewall is a combination of the stateful firewall and application proxy firewall [89].
- The deep packet inspection firewall provides deep filtering in the application layer, and this type of firewall still remains in the development phase [89].

Utility companies use remote access authorization to the controlling stations of third parties to fix outages in the PLCs [89]. Wireless network access is also common in the SCADA system. A firewall for SCADA should be implemented to secure remote access and wireless access [89]. Firewalls are also used to monitor data packets entering the PCN [89].

Security, manageability, and scalability are three evaluation criteria for SCADA firewalls [89]. On the basis of these criteria, there are eight architectures that have been proposed for firewalling SCADA systems [89]:

- A dual-homed computer uses two network interface cards, which connect to EN and PCN, to access information from both networks, but this architecture exposes the dual-homed computer as the main target for the attacks [89].
- A dual-homed server with a personal firewall is similar to a dual-homed computer, but it is employed in a server rather than a computer [89].
- A network layer switch firewall is implemented by employing a network layer switch between PCN and EN [89]. It typically allows one kind of packet across them, but managing these firewalls is a difficult task [89].
- A firewall within two ports of the respective networks is similar to the previous architecture, but a modifiable firewall is utilized instead of a network layer switch [89]. This type of firewall could filter TCP packets [89]. For this architecture, the firewall is in between the two ports, and therefore, it makes management and scalability easy [89].
- The combination of routers and firewalls is used for security purposes [89]. The routers are firewalled from the network, and thus, the external router takes care of the incoming packets with vulnerabilities by filtering them, and the firewall takes care of the application proxy and stateful inspection [89]. The advantage is that it is easy to implement [89].
- Demilitarized zones (DMZs) between networks create subnetworks for security reasons by using firewalls so that attackers can only be connected to the subnetwork [89]. In SCADA systems, DMZ is formed by employing a firewall in between the switches of the two networks [89]. It is more secure and can be easily managed and scaled [89].
- Firewall pairing in between networks uses two firewalls to separate two networks [89]. The first firewall blocks packages from the compromised server from entering into the control network. The second firewall blocks the arbitrary packages instead [89]. The disadvantage is that this system exposes the server to attacks even when the networks connected to this DMZ are safe [89].

PCN virtual LAN (VLAN) firewall is similar to the aforementioned but focuses on PCNs. It also decomposes them into several VLANs [89]. These VLANs interconnect themselves to DMZ through the packet filter and network layer switch [89]. These VLANs avoid the transmission of unwanted traffic across the entire PCN [89]. The disadvantage of this architecture is the cost [89].

9. CONCLUSION

SCADA systems are the basic controlling units in the majority of the industrial systems that need a medium to connect the actual generating stations to the small units that the resource is supplied to. SCADA systems are widely used to monitor and control industrial processes. They provide the functionality of real-time monitoring, logging/archiving, report generation, and automation among other things. On the basis of these functionalities, various SCADA architectures have been proposed and standardized, including hardware and software architecture.

However, the most open and expediently growing area is the communication infrastructure and technologies in SCADA communication. In this paper, we collected almost every documented standard in SCADA and its communication infrastructure, including IEEE Std. c37.1 and IEEE Std. 999–1992. Furthermore, many communication technologies and applications are developed on the basis of the standards. They provide faster speed as well as more secure, robust, and scalable communication for the SCADA systems. Those technologies cover web-based, Internet-based, ATM-based, TETRA network-based, wireless-based and even cell phone-based SCADA communication networks.

In addition, we analyzed the architecture of SCADA networks in modern day smart grids or power grids so that we could have a better understanding of the systems. Also, we observed the various security threats to a SCADA system in power grids. We, then, analyzed various forms of threats pertaining to the grid. We listed the various forms of attacks that are possible and that generally occur on a system, and we provided what needs to be carried out to stop these threats in the future. Also, we addressed the ways to mitigate such attacks.

SCADA systems have evolved with the development of both IT technology and communication technologies. The paper [92] argues that SCADA systems have evolved from mainframe-based systems to flat client–server architecture now and that even flatter architecture and more distributed computing will be the direction for progression. Meanwhile, advancements in server Operating System (OS), databases, and communication tools will be the power drive for SCADA systems.

The paper [93] believes that traditional SCADA systems will become an integrated SCADA and substation/distribution automation system. The paper [94] applied artificial intelligence techniques, such as multiagent, to practice the SCADA automation. The paper [95] suggests the implementation of the SCADA DC motor with a fuzzy logic controller on a neural network.

Extensibility and interoperability are also two of the future trends of SCADA system. The paper [96] argues that there are two major drawbacks to current SCADA systems. First, wireless sensor networking is a promising technology in SCADA communication, which can significantly improve the sensing capability; however, it is difficult to integrate sensor networks with current SCADA systems because of their lack of interoperability. Then, current SCADA systems limit extensibility to new applications. For example, if a company should want to extend its SCADA system by adding a safety alarm system, it would be very difficult to add that application [96]. Therefore, it is very important to enable the interoperability and extensibility of the future SCADA system.

ACKNOWLEDGEMENT

This work is supported in part by the US National Science Foundation under grants CNS-0716211, CCF-0829827, CNS-0737325, and CNS-1059265. Dr. Liang's work is supported in part by the Special Foundation for National Fundamental Research 973 Program of China under 2010CB334705 and the National High Technology Research and Development 863 Program of China under 2011AA040101. Prof. Chen's work is supported in part by the National Fundamental Research 973 Program of China under grant 2011CB302801 and the Macau Science and Technology Development Fund grant number 008/2010/A1.

REFERENCES

1. Tib N. 04-1, Technical Information Bulletin 04–1, National Communications System, SCADA Systems. October, 2004.
2. Gaushell D, Block W. SCADA communication techniques and standards. *Computer Applications in Power IEEE* 2002; **6**:45–50.
3. Daneels A, Salter W. What is SCADA? International Conference on Accelerator and Large Experimental Physics Control Systems. 1999.
4. Xiao Y. Editorial. *International Journal of Security and Networks (IJSN)* 2012; **7**(2):71–72.
5. Neji NB, Bouhoula A. Managing hybrid packet filter's specifications. *International Journal of Security and Networks (IJSN)* 2012; **7**(2):73–82.
6. Baig ZA. Rapid anomaly detection for smart grid infrastructures through hierarchical pattern matching. *International Journal of Security and Networks (IJSN)* 2012; **7**(2):83–94.
7. Boyer S, Robert J, Otrok H, Rousseau C. An adaptive tit-for-tat strategy for IEEE 802.11 CSMA/CA protocol. *International Journal of Security and Networks (IJSN)* 2012; **7**(2):95–106.
8. Butun I, Wang Y, Lee Y, Sankar R. Intrusion prevention with two level user authentication in heterogeneous wireless sensor networks. *International Journal of Security and Networks (IJSN)* 2012; **7**(2):107–121.
9. Kolesnikov V, Lee W. MAC aggregation resilient to DoS attacks. *International Journal of Security and Networks (IJSN)* 2012; **7**(2):122–132.
10. Wong D, Tian X. E-mail protocols with perfect forward secrecy. *International Journal of Security and Networks* 2012; **7**(1):1–5. DOI:10.1504/IJSN.2012.048491
11. Vespa LJ, Chakrovorty R, Weng N. Lightweight testbed for evaluating worm containment systems. *International Journal of Security and Networks* 2012; **7**(1):6–16. DOI:10.1504/IJSN.2012.048478
12. Kandah F, Singh Y, Zhang W, Wang T. A misleading active routing attack in mobile ad-hoc networks. *International Journal of Security and Networks* 2012; **7**(1):17–29. DOI:10.1504/IJSN.2012.048492.
13. Alsubhi K, Alhazmi Y, Bouabdallah N, Boutaba R. Security configuration management in intrusion detection and prevention systems. *International Journal of Security and Networks* 2012; **7**(1):30–39. DOI:10.1504/IJSN.2012.048493
14. Xiao Z, Xiao Y. PeerReview re-evaluation for accountability in distributed systems or networks. *International Journal of Security and Networks* 2012; **7**(1):40–58. DOI:10.1504/IJSN.2012.048494
15. Al-Salloum ZS. Defensive computer worms: an overview. *International Journal of Security and Networks* 2012; **7**(1):59–70. DOI:10.1504/IJSN.2012.048479
16. Mu Y, Chen L, Chen X, *et al*. Editorial. *International Journal of Security and Networks* 2007; **2**(3/4):171–174.
17. Tartary C, Tartary H. Efficient multicast stream authentication for the fully adversarial network model. *International Journal of Security and Networks* 2007; **2**(3/4):175–191.
18. Bhaskar R, Herranz J, Laguillaumie F. Aggregate designated verifier signatures and application to secure routing. *International Journal of Security and Networks* 2007; **2**(3/4):192–201.
19. Hsu H, Zhu S, Hurson AR. LIP: a lightweight interlayer protocol for preventing packet injection attacks in mobile ad hoc network. *International Journal of Security and Networks* 2007; **2**(3/4):202–215.
20. Oliveira LB, Wong H, Loureiro AAF, Dahab R. On the design of secure protocols for hierarchical sensor networks. *International Journal of Security and Networks* 2007; **2**(3/4):216–227.
21. Michail HE, Panagiotakopoulos GA, Thanasoulis VN, Kakarountas AP, Goutis CE. Server side hashing core exceeding 3 Gbps of throughput. *International Journal of Security and Networks* 2007; **2**(3/4):228–238.
22. Hoeper K, Gong G. Preventing or utilising key escrow in identity-based schemes employed in mobile ad hoc networks. *International Journal of Security and Networks* 2007; **2**(3/4):239–250.
23. Cheng Z, Chen L. On security proof of McCullagh–Barreto's key agreement protocol and its variants. *International Journal of Security and Networks* 2007; **2**(3/4):251–259.

24. Finnigin KM, Mullins BE, Raines RA, Potoczny HB. Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks. *International Journal of Security and Networks* 2007; **2**(3/4):260–271.
25. Huang D. Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks. *International Journal of Security and Networks* 2007; **2**(3/4):272–283.
26. Abdalla M, Bresson E, Chevassut O, Moller B, Pointcheval D. Strong password-based authentication in TLS using the three-party group Diffie–Hellman protocol. *International Journal of Security and Networks* 2007; **2**(3/4):284–296.
27. Chen H, Guizani M. Editorial. *International Journal of Security and Networks* 2007; **2**(1/2):1–2.
28. Li R, Li J, Chen H. DKMS: distributed hierarchical access control for multimedia networks. *International Journal of Security and Networks* 2007; **2**(1/2):3–10.
29. Sakarindr P, Ansari N. Adaptive trust-based anonymous network. *International Journal of Security and Networks* 2007; **2**(1/2):11–26.
30. Malaney RA. Securing Wi-Fi networks with position verification: extended version. *International Journal of Security and Networks* 2007; **2**(1/2):27–36.
31. Sun F, Shayman MA. On pairwise connectivity of wireless multihop networks. *International Journal of Security and Networks* 2007; **2**(1/2):37–49.
32. Erdogan O, Cao P. Hash-AV: fast virus signature scanning by cache-resident filters. *International Journal of Security and Networks* 2007; **2**(1/2):50–59.
33. Rabinovich P, Simon R. Secure message delivery in publish/subscribe networks using overlay multicast. *International Journal of Security and Networks* 2007; **2**(1/2):60–70.
34. Chen Z, Ji C. Optimal worm-scanning method using vulnerable-host distributions. *International Journal of Security and Networks* 2007; **2**(1/2):71–80.
35. Pan J, Cai L, Shen X. Vulnerabilities in distance-indexed IP traceback schemes. *International Journal of Security and Networks* 2007; **2**(1/2):81–94.
36. Korkmaz T, Gong C, Sarac K, Dykes SG. 8 Single packet IP traceback in AS-level partial deployment scenario. *International Journal of Security and Networks* 2007; **2**(1/2):95–10.
37. Ling H, Znati T. End-to-end pairwise key establishment using node disjoint secure paths in wireless sensor networks. *International Journal of Security and Networks* 2007; **2**(1/2):109–121.
38. Artan NS, Chao HJ. Design and analysis of a multipacket signature detection system. *International Journal of Security and Networks* 2007; **2**(1/2): 122–136.
39. Zhu Y, Fu X, Bettati R, Zhao W. Analysis of flow-correlation attacks in anonymity network. *International Journal of Security and Networks* 2007; **2**(1/2):137–153.
40. Gu Q, Liu P, Chu C, Zhu S. Defence against packet injection in ad hoc networks. *International Journal of Security and Networks* 2007; **2**(1/2):154–169.
41. Hwu J, Hsu S, Lin Y-B, Chen R. End-to-end security mechanisms for SMS. *International Journal of Security and Networks* 2006; **1**(3/4):177–183.
42. Wang X. The loop fallacy and deterministic serialisation in tracing intrusion connections through stepping stones. *International Journal of Security and Networks* 2006; **1**(3/4):184–197.
43. Jiang Y, Lin C, Shi M, Shen X. A self-encryption authentication protocol for teleconference services. *International Journal of Security and Networks* 2006; **1**(3/4):198–205.
44. Owens SF, Levary RR. An adaptive expert system approach for intrusion detection. *International Journal of Security and Networks* 2006; **1**(3/4):206–217.
45. Chen Y, Susilo W, Mu Y. Convertible identity-based anonymous designated ring signatures. *International Journal of Security and Networks* 2006; **1**(3/4):218–225.
46. Teo J, Tan C, Ng J. Low-power authenticated group key agreement for heterogeneous wireless networks. *International Journal of Security and Networks* 2006; **1**(3/4):226–236.
47. Tan C. A new signature scheme without random oracles. *International Journal of Security and Networks* 2006; **1**(3/4):237–242.
48. Liu Y, Comaniciu C, Man H. Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection. *International Journal of Security and Networks* 2006; **1**(3/4):243–254.
49. Karyotis V, Papavassiliou S, Grammatikou M, Maglaris V. A novel framework for mobile attack strategy modelling and vulnerability analysis in wireless ad hoc networks. *International Journal of Security and Networks* 2006; **1**(3/4):255–265.
50. Xiao Y, Jia X, Sun B, Du X. Editorial: security issues on sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4):125–126.
51. Wang H, Sheng B, Li Q. Elliptic curve cryptography-based access control. *International Journal of Security and Networks* 2006; **1**(3/4):127–137.
52. Zheng J, Li J, Lee MJ, Anshel M. A lightweight encryption and authentication scheme for wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4):138–146.
53. Al-Karaki JN. Analysis of routing security-energy trade-offs in wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4): 147–157.

54. Araz O, Qi H. Load-balanced key establishment methodologies in wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4):158–166.
55. Deng J, Han R, Mishra S. Limiting DoS attacks during multihop data delivery in wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4):167–178.
56. Duong T. “The design of next generation SCADA systems,” in Power Industry Computer Application Conference, 1995. Conference Proceedings, 1995 IEEE. 1995; 431–436.
57. Sciacca SC, Block WR. Advanced SCADA concepts. *Computer Applications in Power IEEE* 1995; **8**:23–28.
58. Medida S, *et al*. “SCADA-EMS on the Internet,” in Energy Management and Power Delivery, 1998. Proceedings of EMPD ’98. International Conference on, 1998. 1998; **2**: 656–660.
59. Kwok-Hong M, Holland BL. Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking. *Power Engineering Journal* 2002; **16**:305–311.
60. McClanahan RH. “The benefits of networked SCADA systems utilizing IP-enabled networks,” in Rural Electric Power Conference, 2002. 2002 IEEE. 2002; **7**: C5–C5.
61. Ebata Y, *et al*. “Development of the Intranet-based SCADA (supervisory control and data acquisition system) for power system,” in Power Engineering Society Winter Meeting, 2000. IEEE. 2000; **3**: 1656–1661.
62. Zecevic G. “Web based interface to SCADA system,” in Power System Technology, 1998. Proceedings. POWERCON ’98. International Conference on, 1998. 1998; **2**: 1218–1221.
63. Zhihao L, Jinshou Y. “The design of SCADA based on industrial Ethernet,” in Intelligent Control and Automation, 2002. Proceedings of the 4th World Congress on, 2002, pp. 2786–2789 vol.4.
64. Qiu B, Gooi HB. Web-based SCADA display systems (WSDS) for access via Internet. *Power Systems, IEEE Transactions on* 2000l; **15**:681–686.
65. “IEEE Standard for SCADA and automation systems,” IEEE Std C37.1-2007 (revision of IEEE Std C37. 1-1994). 2008; c1–133.
66. “IEEE recommended practice for master/remote supervisory control and data acquisition (SCADA) communications,” IEEE Std. 999–1992, p. 0_1, 1993.
67. IBM Internet security systems. Available: http://www.iss.net/
68. Bruce AG. Reliability analysis of electric utility SCADA systems. *IEEE Transactions on Power Systems* 1998; **13**(3):844–849 Aug.
69. Creery A, Byres EJ. Industrial cybersecurity for power system and SCADA networks. Paper No. PCIC-2005-34.
70. Shyh-Jier H, Chih-Chieh L. Application of ATM-based network for an integrated distribution SCADA-GIS system. *Power Systems IEEE Transactions on* 2002; **17**:80–86.
71. Toshida N, *et al*. Open distributed EMS/SCADA system. *Hitachi Review* 1998; **47**:208–213.
72. Goel A, Mishra R. Remote data acquisition using wireless-SCADA system. *International Journal of Engineering (IJE)* 2009; **3**:58.
73. Molina F, *et al*. “Automated meter reading and SCADA application for wireless sensor network,” Ad-Hoc, Mobile, and Wireless Networks. 2003; 223–234.
74. Ozdemir E, Karacor M. Mobile phone based SCADA for industrial automation. *ISA Transactions* 2006; **45**:67–75.
75. Ozimek I, Kandus G. SCADA system using TETRA communication network. Recent advances in computers, computing and communications. 164–166.
76. Beaver C, *et al*. “Key management for SCADA,” Cryptog. Information Sys. Security Dept., Sandia Nat. Labs, Tech. Rep. SAND2001-3252. 2002.
77. Wright A, *et al*. Low-latency cryptographic protection for SCADA communications. 2004; 263–277.
78. Donghyun C, *et al*. Advanced key-management architecture for secure SCADA communications. *Power Delivery IEEE Transactions on* 2009; **24**:1154–1163.
79. Marihart DJ. Communications technology guidelines for EMS/SCADA systems. *Power Delivery IEEE Transactions on* 2001; **16**:181–188.
80. Parniani M, Nasri A. “SCADA based under frequency load shedding integrated with rate of frequency decline,” in Power Engineering Society General Meeting, 2006. IEEE, 2006; 6.
81. “Trends in security incidents in the SCADA and process industries: a summary – part II” Eric Byres, David Leversage, Nate Kube, Symantec Corporation. 2007.
82. “SQL slammer worm lessons learned for consideration by the electricity sector,” North American Electric Reliability Council, Princeton NJ, June 20. 2003.
83. IBM internet security systems white paper, “A Strategic Approach to Protecting SCADA and Process Control Systems”.
84. C1Working group members of power system relying committee. Cyber Security Issues for Protective Relays, Power Engineering Society general meeting. 2007.
85. Oman P, Edmund O. ll S, Frincke D. Concerns about intrusions into remotely accessible substation controllers and SCADA systems. 2000.

86. IEEE Power Engineering Society. IEEE Standard 1402–2000: IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE. New York, NY, Apr. 4, 2000.
87. National Security Telecommunications Advisory Committee Information Assurance Task Force. Electric Power Risk Assessment. March, 1997.
88. Poulsen K. "Lights out: NIPC unveils plan to monitor cyber attacks on the power grid," an InfoSec News Article Ported to Security Focus Web Page. May 25, 2000: http://www.securityfocus.com/news/41
89. McQueen MA, Boyer WF, Flynn MA, Beitel GA. Quantitative cyber risk reduction estimation methodology for a small SCADA control system. International Conference on System Sciences. 2006
90. NISCC good practice guide, "Firewall Deployment for SCADA and Process Control Networks 1.4" British Columbia Institute of Technology. 2005.
91. "Trends in security incidents in the SCADA and process industries: a summary – part I" Eric Byres, David Leversage, Nate Kube, Symantec Corporation. 2007.
92. Marcuse J, *et al*. Servers in SCADA applications. *Industry Applications IEEE Transactions on* 1997; **33**:1295–1299.
93. Gacek D, *et al*. "Migrating from SCADA to automation," in Transmission and Distribution Conference and Exposition, 2001 IEEE/PES. 2001; **1**: 343–348.
94. Davidson EM, *et al*. "Applying multi-agent system technology in practice: automated management and analysis of SCADA and digital fault recorder data ," in Power Engineering Society General Meeting, 2006. IEEE. 2006; 1.
95. Horng J. SCADA system of DC motor with implementation of fuzzy logic controller on neural network. *Advances in Engineering Software* 2002; **33**:361–364.
96. Ye W, Heidemann J. "Enabling interoperability and extensibility of future SCADA systems," University Southern California, USC/ISI Technical Report, ISITR-625, 2006.