SAND98-2220C

TOWARDS A STANDARD FOR HIGHLY SECURE SCADA SYSTEMS

Rolf Carlson
09/25/98

Abstract

The critical energy infrastructures include gas, oil, and electric power. These infrastructures are complex and interdependent networks that are vital to the national security and social well being of our nation. Many electric power systems depend upon gas and oil, while fossil energy delivery systems depend upon electric power. The control mechanisms for these infrastructures are often referred to as SCADA (*Supervisory Control and Data Acquisition*) systems. SCADA systems provide remote monitoring and centralized control for a distributed transportation infrastructure in order to facilitate delivery of a commodity. Although many of the SCADA concepts developed in this paper can be applied to automotive transportation systems, we will use transportation to refer to the movement of electricity, gas, and oil.

Recently, there have been several reports suggesting that the widespread and increasing use of SCADA for control of energy systems provides an increasing opportunity for an adversary to cause serious damage to the energy infrastructures[1,2]. This damage could arise through cyber infiltration of the SCADA networks, by physically tampering with the control networks, or through a combination of both means.

SCADA system threats decompose into cyber and physical threats. One solution to the SCADA security problem is to design a standard for a highly secure SCADA system that is both cyber, and physically secure. Not all-physical threats are possible to guard against, but of those threats that are, high security SCADA provides confidence that the system will continue to operate in their presence. One of the most important problems in SCADA security is the relationship between the cyber and physical vulnerabilities. Cyber intrusion increases physical vulnerabilities, while in the dual problem, physical tampering increases cyber vulnerabilities. There is potential for feedback and the precise dynamics need to be understood.

As a first step towards a standard, the goal of this paper is to facilitate a discussion of the requirements analysis for a highly secure SCADA system. The framework for the discussion consists of the identification of SCADA security investment areas coupled with the tradeoffs that will force compromises in the solution. For example, computational and bandwidth requirements of a security standard could force the replacement of entire SCADA systems. The requirements for a real-time response in a cascading electric power failure could pose limitations on authentication and encryption mechanisms.

The shortest path to the development of a high security SCADA standard will be achieved by leveraging existing standards efforts and ensuring that security is being properly addressed in those standards. The Utility Communications Architecture 2.0 (UCA), for real-time utility decision control, represents one such standard. The development of a SCADA security specification is a complex task that will benefit from a systems engineering approach.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

SCADA Systems

The critical energy infrastructures include gas, oil, and electric power. These infrastructures are complex and interdependent networks that are vital to the national security and social well being of our nation. Many electric power systems depend upon gas and oil, while fossil energy delivery systems depend upon electric power. The control mechanisms for these infrastructures are often referred to as SCADA (Supervisory Control and Data Acquisition) systems. The IEEE Std C37.1-1994 specification for the electric power industry defines SCADA systems as "a system operating with coded signals over communication channels so as to provide control of RTU [Remote Terminal Unit] equipment."[3]

In an IEEE tutorial course on the fundamentals of supervisory systems, a less formal working definition of a supervisory system is given to be "a collection of equipment that will provide an operator at a remote location with enough information to determine the status of a particular piece of equipment or an entire substation or power plant, and case actions to take place regarding that equipment or facility without being physically present."[4] Many of the recent changes to SCADA systems have come from advances in the computing and telecommunications industries. The evolving SCADA systems are becoming more efficient and cost effective but arguably less secure. SCADA architectures are a moving target.

Consequently, our definition of SCADA systems will be sufficiently broad to capture the stationary features of representative systems in the gas and oil as well as the electric power industries. We will define a SCADA system as *a system that provides remote monitoring and centralized control for a distributed transportation infrastructure in order to facilitate delivery of a commodity*. Although many of the SCADA system concepts developed in this paper can be applied to automotive transportation systems, we will use transportation to refer to the movement of electricity, gas, and oil. In the electric power industry, the commodity is electricity while in the gas and oil industry the commodities are gas and oil. The critical energy infrastructures use SCADA systems to control and optimize their respective operations. The SCADA systems activity does not include payroll or billing, but more office systems are using SCADA system information to improve efficiency in billing and customer operations. The definition we offer in this paper is an augmentation of the IEEE definitions and meant to emphasize that SCADA systems exists to deliver a commodity. One of the fundamental problems in developing a standard will be ensuring that security does not hinder the mission of the SCADA system, and therefore does not hinder delivery of the commodity. Security solutions for SCADA systems could result in a variety of requirements that exceed the capacities of current systems.

The more a SCADA system security requirement exceeds the capability of existing systems, the more it will cost for a given company to upgrade, and the longer it will take before the standard becomes ubiquitous. Equipment that includes a higher initial cost often entails more maintenance and operational expense. Widespread acceptance could be important if the ultimate goal is to achieve an overall improvement in the stability of the critical infrastructures.

Historically, SCADA systems have consisted of four components: the supervisory system, remote terminal units, a communications network, and field instruments. Next, we discuss the four major SCADA subsystems.

SCADA Subsystems

Master Systems

The SCADA master system at the supervisory site processes information received form the SCADA network to form a digital representation of the infrastructure state. Control directives are then issued back to the infrastructure directly from the supervisory site. Under reregulation in the power industry, SCADA data is often shared outside of the originating organization and the supervisory site might be contained at a regional ISO (Independent System Operators) facility.

Different topologies for the supervisory site are possible. The central site can consist of a peer network of computers, as in a substation or refinery, or in a hierarchical configuration where a supervisory computer has several subordinate sites, each with a respective master system controlling a subset of the infrastructure. Many different applications can run on computers at the central site in order to take advantage of data.

Remote Terminal Units (RTU)

The RTUs acquire data from sensors on the infrastructure, deliver control signals to the field equipment, and communicate with the master stations. The RTU can be considered a condensation point for data that is aggregated and delivered to the control center. Remote Terminal Units (RTU) are referred to synonymously as Remote Telemetry Units. As the RTUs become more capable, decisions and responsibility are being delegated to the RTU, offloading many decisions formerly made by the master site. Each master station has one or possibly many RTUs reporting to the station. Examples of communication mediums that could be used include radio, dedicated landline, leased line, satellite links, microwave both analog and digital, cabling such as RS-232, and dial-up modem. RTU's can be as complex as a general purpose computer hosting a collection of dedicated controller cards housed in expansion slots, or as simple as stand alone devices with a fixed number of input and outputs. Programmable Logic Controllers (PLC) are sometimes used instead of RTUs. Functionally, PLCs and RTUs are merging. Hardware PLC and RTU packages with limited functionality may be vulnerable to certain attacks, such as direct tampering with jumper configurations, or remote reprogramming. PCs operating as an RTU with a common operating system such as Windows NT, have significantly more and well documented vulnerabilities as many hacker WWW sites will attest. Such systems could pose a significant security risk in the SCADA network.

Communication Links

The communication system links the master unit with the remote terminal units. Common methods of communication include radio, leased line, landline, and digital and analog microwave. More recently analog and digital cellular communication has been introduced. For remote service, satellite communication is sometimes employed. SCADA security in communication typically refers to the ability to perform error correction, rather than authentication or encryption. As late as 1994, the IEEE gave the following definition of communication security on a SCADA network, "Security is the ability to detect errors in the original information transmitted, caused by noise on the communication channel."[5] In today's world such a definition is incomplete, however, the need for security in utility communication

has been recognized in other forums EPRI (Electrical Power Research Institute) is developing the UCA (Utility Communications Architecture) to facilitate communications between the components of an electric power system. Although the UCA purports a security model, it has not been widely assessed and it remains to be seen whether the security of the UCA will be sufficient for its stated purpose.

Field Equipment

The field equipment consists of sensors and controllers that directly interface with the infrastructure and report to the RTU. A typical measurement could result in a simple binary yes or no, or it could be an analog signal representing a real-valued parameter. The analog signal is often digitized to around 12 bits of information at the RTU. The communication media between the supervisory site and the RTUs are designed to handle packets of this size, often on a report by exception basis.

Electric Power

There are four major components to the generation and delivery of electric power: the generation system, transmission system, distribution system, and control center. Substations are considered part of the transmission system. The control center monitors the entire network including power generation, transmission, distribution, and load.

Several systems that are often viewed as different flavors of SCADA for the electric power industry include AM/FM (Automated Mapping/Facilities Mapping), EMS (Energy Management Systems), GIS (Geographic Information Systems), DMS (Distribution Management Systems), and SAS (Substation Automation Systems). In the case of AM/FM and GIS, the differences can be viewed as different application sets on the supervisory site. AM/FM for example refers to the management of spatially distributed assets and facilities and GIS systems are used to monitor data with an associated geographic position.

In the case of EMS, DMS, and SAS, the differences are both spatial and functional. If we add software to the supervisory site to include AGC (Automatic Generation Control) and PSSA (Power System Security Analysis), then in addition to SCADA we have EMS. DMS refers to the SCADA control and monitoring functions that start from the substations and finish with the end users. GIS and CIS (Customer Information Systems) are often regarded as portions of the DMS. Regardless of the application name, information is acquired by the infrastructure, processed at a supervisory site, and then control signals are dispatched. We will refer to this collection of activities of remote monitoring and control as SCADA.

Gas and Oil

The dependence upon SCADA systems by the gas and oil industry is not as great as that in the electric power industry. Nonetheless, SCADA systems in the gas and oil industry are increasingly used to monitor and regulate gas and fluid flow. Formerly, such regulation was performed by the manual adjustment of valves and compressors. Pressure meters provide information about the state of the flow, while valves and regulators ensure against over pressure. SCADA systems monitor pipe flows in order to optimize pipeline operations.

High Security SCADA Systems

We defined a SCADA system as a system that provides remote monitoring and centralized control for a distributed transportation infrastructure in order to facilitate delivery of a commodity. Building on this, we define *a highly secure SCADA system as a SCADA system that is both cyber secure and physically secure.* A highly secure SCADA system will be synonymously referred to as a high security SCADA system. There are limitations on what it means for a SCADA system to be physically secure. Physical SCADA system security means component authentication, tamper resistance, and in certain contexts proximity detection. Behind a substation fence, proximity detection makes sense. Along a transmission line, proximity detection might be less useful. Physically guarding each section of an electric power transmission system is not feasible and therefore not included in this definition. These limitations will be explored in later sections. There are no limitations on the use of the term cyber security in the definition on SCADA system security. One of the most important problems in SCADA system security is the relationship between the cyber and physical vulnerabilities. Cyber intrusion increases physical vulnerabilities, while in the dual problem, physical tampering can increase cyber vulnerabilities. There is potential for feedback and the precise dynamics needs to be understood. Let us next examine a definition of electric power infrastructure security so that we may compare this with our definition of SCADA system security.

Electric Power Infrastructure Security defined by NERC in form 715

According to NERC (National Energy Regulatory Commission) The primary reliability objectives in the electric power industry are adequacy and security. They can be defined as follows:

> Adequacy - which is the capacity to meet system demand within major component ratings in the presence of scheduled and unscheduled outage of generation and transmission components or facilities, and
>
> Security - which is a system's capability to withstand system disturbances arising from faults and unscheduled removal of bulk power supply elements without further loss of facilities or cascading outages.

The definition of security for electric power is really robustness, or resiliency. We can see that the definition of security according to NERC is quite different from the definition of security for SCADA systems. A highly secure SCADA system provides confidence in the infrastructure state measurements and the subsequent delivery of control. Such confidence might be the difference between halting and not halting a cascading outage in an emergency. Not only is the definition of SCADA system security significantly different from that of traditional electric power security, but SCADA system security is also different from modern computer network security.

SCADA System Security Is Not Computer Network Security

It is tempting to suggest that the SCADA system security problem is simply a computer network security issue. This may be true in 10 years, but for now there is a large collection of SCADA systems that need to be evolved from their present state. Wholesale replacement of

existing SCADA systems may not be an economic possibility for many operators in the new restructured environment.

There are real differences between contemporary computer networks and SCADA systems. For example, SCADA systems tend to be spread out over large geographic regions, terminated by sensors of limited intelligence rather than general purpose workstations. SCADA components often communicate to the master station on a report by exception basis, or a polled basis, rather than as peers. Data packets tend to be small. Components can be isolated geographically with low power constraints, and a human security presence is not possible at all sensor sites. These differences lead to real concern over tamper resistance, data packet authentication, and key management and certification techniques for SCADA networks. An important operational constraint of a SCADA network is that it functions as specified under maximum load. Security cannot hinder such operation. For example, how much computational capability will it take at the supervisory site to authenticate 50,000 sensors on a SCADA network that are all reporting by exception simultaneously? What does it mean to do this in real time so that the authenticated information can be processed into a control directive for the network in sufficient time to be effective? Are certain certificate authority models better suited for this challenge than others are? These are some of the questions that need to be answered if we are to achieve a standard for a highly secure SCADA system. Next, we discuss a collection of problems that need to be addressed in order to develop a requirements analysis for high security SCADA systems.

SCADA Systems Challenges

Legitimate User Access and Remote Control

In an infrastructure emergency, such as the cascading failure of a power grid, SCADA operators are often off site and need to gain immediate remote access to the command facilities of the network. A typical mechanism that is currently used to protect against remote unauthorized entry is a password scheme through a dial-in port. Internet access is becoming a popular alternative. The passwords are often simple so that they are easy to remember and unchanged over time so that the operator can be guaranteed access when the moment is critical. One of the primary threats voiced by SCADA operators is that of former insiders. With increased connectivity to the Internet, the hacker threat could also increase. Biometrics and smart card identification technologies could increase legitimate user-access security to SCADA networks while maintaining the reliability and efficiency of current methods. Other applications of user identification technology include network service. Any individual replacing or maintaining SCADA components should be authenticated at the location of service. A balance needs to be struck between assuring authorized use while assuring against unauthorized use.

Unattended Monitoring and Component Tamper Resistance

Sensitive SCADA equipment often operates unattended in remote sites for months without local inspection. Remote Telemetry Units (RTU), Programmable Logic Controllers (PLC), sensors, and communication equipment currently are easy prey for physical damage or tampering. Within a restricted area, such as a substation, one of the goals of a highly secure SCADA system is that the system be able to detect and authorize the presence of any human within a close physical proximity to the system. Another related goal of a highly secure

SCADA system is to provide tamper resistance on each SCADA system component. Even if proximity detection is successfully bypassed, each component of a highly secure SCADA system needs to be able to deter successful replacement or impersonation and manipulation through carefully structured seals and access mechanisms. The SCADA system operator needs confidence that the physical state of the SCADA network reflects the logical-reported state of the network.

Component Authentication and Inventory Control

A pivotal technology for a highly secure system is data authentication. It is not possible to make a credible assessment of the health of a system without authenticating the identity of each component and the correctness of each message. Sensor and control signal spoofing coordinated with a physical attack can cause damage that might not become visible for an extended period. Because sensor messages can be quite small, often only a few bits of information, the authentication requirements are unique and available security techniques need to be adapted. There does not exist a methodology for packaging small messages for transmission that guarantees the authentication of the message for a given message length with minimal overhead at a specified level of security. Signing a message using the Digital Signature Algorithm (DSA) requires 160 bits in the message, forcing a pad of the original 12 bits with random "salt". It is not clear whether a traditional SCADA system communication channel would support such a 13-fold increase in the bandwidth requirements. If we are to evolve the security of SCADA communications networks, a more subtle approach needs to be developed.

In addition, the real-time response requirements of a SCADA control system, combined with the report on exception behavior of SCADA sensors produces a unique collection of monitoring requirements. On a network with up to 50,000 sensors, an event such as a cascading failure will cause a large proportion of the sensors to generate exceptions simultaneously. The computational requirements of the supervisory system need to be accounted for if the authentication and control mechanisms are both to succeed.

Supervisory Computer Security and Firewalls

Much of the information processing occurs at the supervisory site. There currently are no special purpose firewalls for supervisory sites that accommodate SCADA systems. Unsecured protocols such as DDE (Dynamic Data Exchange), and active content such as OLE (Object Linking and Embedding) and ActiveX objects are passing directly to the supervisory site.

A Standard SCADA System Applications Framework

With each new SCADA installation, there is a need for a standard collection of applications to produce reports, database information, make decisions, and link with other computer systems, all while facilitating security. Having each utility build value-added components from fifth generation tools such as Java or Visual Basic introduces additional potential for system weakness.

Key Management Techniques and Certificate Authorities

All cryptographic techniques, whether used for encryption, identification, or digital signatures, ultimately rely upon some form of cryptographic key. Often keys are grouped in one location

for safekeeping. The management and maintenance of these keys so that they may be used efficiently by a legitimate user is an ongoing problem. One aspect of a highly secure SCADA system is key management for the keyed component members of the system. This will require a certificate authority. SCADA systems have real-time response requirements that make building a key management strategy on top of a working system a challenge. A SCADA network might have 30,000 – 50,000 nodes that need authentication. In an emergency, many of the nodes may be simultaneously reporting exceptions. In order to mount an effective control-response strategy, these messages must be authenticated and decoded immediately. A certification structure that allows for such large volume on a real-time basis will almost certainly rule out some of the widely proposed certificate handling standards. The computational requirements of the supervisory system need to be accounted for if the certification and control mechanisms are to succeed.

SCADA System Support for a National Indications and Warnings Center

One important component of a complete SCADA system security model is the ability to securely transfer sensor data to an indications and warnings center (I&W) for analysis. Many infrastructure state measurements originate on SCADA systems, so it is natural to consider linking SCADA systems with an I&W. Although still in the proposal stage, developing an I&W will be an important step in resolving security issues that cannot be addressed by single infrastructure operators. Since most SCADA system operators claim their systems are unrelated to SCADA systems on competing infrastructures, transfer of such sensor data facilitates analysis of events occurring on disjoint SCADA systems. Even as SCADA systems begin to use more of the Internet for information transfer, their association will remain indirect at best. The proprietary nature of the data and cost of an all-to-all information transfer between SCADA systems will be prohibitive and not in the interest of any one infrastructure operator to manage. An I&W might allow early detection of a coordinated attack upon our domestic critical energy infrastructures as well as provide the privacy demanded by industry.

Secure Communications Protocols for SCADA networks

A highly secure SCADA system requires that the communication protocols between supervisory systems and other SCADA components withstand a complete security analysis. One family of protocols in the utilities industry that has a security model is the Utility Communications Architecture (UCA). EPRI (Electric Power Research Institute) developed the UCA based on International Standards Organization (ISO) standards for data communications. The UCA provides interconnectivity and interoperability between utility data communication systems for real-time information exchange to reduce operating costs, increase operational flexibility, and decrease installation and integration costs of new components. A thorough security analysis of the UCA needs to be performed.

Internet Technologies for SCADA Systems

Several Internet security technologies are maturing and need to be evaluated for inclusion into SCADA networks. SSL stands for Secure Socket Layer and is used almost exclusively between Web browsers and Web servers, but could be adapted for use on a SCADA network. Currently, Web browser clients rarely have certificates leading to weaknesses in the communications. SCADA objects on the other hand could easily be issued certificates.

At the network layer, IPSEC (Internet Protocol Security Protocol) could provide security to the SCADA network and allow legacy communications protocols to continue at the application and transport layers. One problem that will need to be addressed is the routing of information through untrusted intermediary nodes. Routing attacks can provide at least denial of service. Depending on the strength with which the information has been encrypted and authenticated, routing attacks can provide a threat more serious than denial of service.[6]

New Trends and Issues

Traditional problems associated with securing a SCADA network, include exposed-gangly transportation systems, low power constraints, remote locations, and the need for convenient-emergency access to the control systems. There is a collection of new issues, however, that could significantly influence the future security of electric power SCADA systems. The most important influence is reregulation of the electric power market.

Reregulation

In an effort to reduce power prices, the electric power industry is being restructured to spur competition. Vertically integrated utilities are being split into separate entities. SCADA data may be shared outside the originating organization with several companies, including a power market such as California PX (Power Exchange) and the California ISO (Independent System Operators). The operational data that was once minimally valued outside the utility is now used to price complex derivative securities. FERC (Federal Energy Regulatory Commission) has developed orders 888 and 889 to help clarify collaboration and competition in the new environment. There is no coherent framework for securing the shared information.

Offloading Communications Infrastructure

In response to increased competition and a tightening power market, many companies are offloading their communication needs when possible. By migrating to a medium such as digital cellular, the utility shifts the burden of maintaining the communication infrastructure to the cellular operator, thus decreasing their fixed costs. Another benefit is the possible inheritance of a security model for communications. For example, Cellular Digital Packet Data (CDPD) is a wireless digital packet service that has been scrutinized.[7] Alternatively, the Global System for Mobile Communications (GSM) digital standard, which is now being used by over 79 million telephones worldwide has been found to have weaknesses. Although rare in the U.S. GSM is widely used in the rest of the world. Communication methods for SCADA networks currently tend to be of limited bandwidth with little or no security model.

Transition to Open Systems

Historically, SCADA systems have been developed with proprietary hardware, communication protocols, and software. Vendors could gain a market advantage by adding features that add value above a competing product. The features would be kept intentionally proprietary to tie the customer to the vendor. Customers are now expressing a desire for open standards. Instead of asking vendors to develop specific features, in house software experts customize their open systems using fifth generation languages and development platforms, such as Visual Basic, to add the features that are necessary for the particular utility. Consequently, we are

moving from proprietary systems that deliver security through obscurity to open systems based on common operating systems such as Unix and Windows NT, and communication methods that include DDE, Java, and ActiveX. Wide standardization upon technologies with well-known security weaknesses will cause as many holes as they close but these systems are no longer stand-alone. Open technologies are also yielding unprecedented opportunities for connectivity with the Internet, which multiplies the weaknesses of the new open systems. In the next generation SCADA system, not only could there be open platforms that are widely accepted and weak, but also easily accessible from geographically distant locations. Open systems and connectivity are not the only reason to adopt high standards for SCADA security, there is another reason. SCADA systems are typically long lived, some on the order of 25 years or older.

Foreign Trader Barriers

There is an economic need for standards. According to Raymond G. Kammer, Director, NIST, before the Subcommittee on Technology, Committee on Science, House of Representatives, April 28, 1998, on International Standards: Technical Barriers to Free Trade. "The United States needs an effective national standards strategy if we are to compete effectively in the global market....It is fair to say that European governments and industries believe that they can create a competitive advantage in world markets by strongly influencing the content of international standards."[8] Competing standards can keep American companies out of foreign countries. An international standard would level the playing field so that American companies could enter a foreign market knowing they are compliant. As the SCADA market grows, it is a national security issue that the SCADA systems controlling our critical energy infrastructures meet evaluation criteria determined by the United States.

National Security Agency Efforts

One problem with rating a SCADA network is that there is no generally accepted way to measure the quality of the network security. The Network Rating Model (NRM)[9] being produced by the NSA is an attempt to define a comprehensive methodology for assessing the security protection provided by a network within the context of its mission and operational environment.

Another program that might be useful for arriving at a SCADA system standard is the Trust Technology Assessment Program (TTAP). The TTAP is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. TTAP is working to provide for a smooth transition to the Common Criteria. The Common Criteria contains criteria that can be used as the basis for assigning information technology security properties. SCADA systems designed around the common criteria might allow a more consistent comparison of security performance between networks.

Systems Engineering

The problems outlined in this paper begin to develop a discussion that will lead to the requirements analysis for a highly secure SCADA system. An analysis of the security mission, operational environments, and user requirements has not been addressed. These need to be

well defined before the identification of functional and performance requirements can be obtained.

System verification in the context of SCADA security is a challenge that needs further investigation. The likely requirements for security verification include a mutable infrastructure that can serve as a testbed for pilot technologies. For reliability reasons, an operational electric power grid is unlikely to allow such active security challenges, or red teaming.

Acknowledgements

I would like to thank the Sandia staff and management for their support, and in particular, Doug Nicholls for his discussions and insights on vulnerabilities.

References

[1] The Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

[2] Critical Infrastructure Assurance Office, *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*, May 22, 1998.

[3] IEEE Std C37.1-1994, *IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control*, IEEE Power Engineering Society, Sponsored by the Substations Committee, Institute of Electrical and Electronics Engineers, Inc., New York, New York, p. 12.

[4] IEEE Tutorial Course: Fundamentals of Supervisory Systems, 94 EH0392-1 PWR, Sponsored by the Data Acquisition, Processing, and Controls Systems Subcommittee of the Substations Committee of the IEEE Power Engineering Society, 1994, Chapter 1, p. 3.

[5] Ibid, p. 38.

[6] Bellovin, Steven M., *Cryptography and the Internet*, Advances in Cryptology - CRYPTO '98., 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1998, Lecture Notes in Computer Science 1462, Springer, Hugo Krawczk (Ed.), p. 46-55.

[7] Yair Frankel, Amir Herzberg, et. al., *Enhanced Security Protocols for the CDPD Network: Security Issues in a CDPD Wireless Network*, IEEE Personal Communications, August 1995, p. 16 - 27.

[8] http://www.nist.gov/testimony/intstnds.htm

[9] http://www.radium.ncsc.mil/nrm/nrmovrvw.html