Analysis of Vulnerabilities in the Protocols used in SCADA Systems

Krushna Chandra Mahapatra, S.Magesh

***Abstract*— As the need for reliable Electric Power became greater with the technology advancement and as the labor became a more significant part of the cost of providing electric power, technologies known as Supervisory Control and Data Acquisition or SCADA were developed that allowed remote monitoring and even control key system parameters. As the technologies further increased hence a whole power system would be controlled by a SCADA system. Hence there came the urge for security which is the major concern currently. So here we analysis some of the Vulnerabilities found in the current protocols in SCADA systems by which a system can be compromised and also patch to it so that it can't be further compromised.**

***Index Terms*— SCADA, MODBUS, DNP3, TCP/IP, Firewall, IDS.**

I. INTRODUCTION

Supervisory control and data acquisition system or SCADA refers to the combination of telemetry and data acquisition. SCADA includes the collecting of the information via a RTU (remote terminal unit), PLC's (Programmable Logic Controllers) and IED's (Intelligent electronic devices), transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. Three of the most important part of a SCADA system is Master Station, Remote Terminal (RTU, PLC, and IED) and the communication between them. In order to have good Communication between them, there must be a communication protocol. DNP3 and T101 are two of the most common protocols today. It is important to determine which protocol should be applied if you are planning a SCADA system.

A. Purpose

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

***Manuscript received March, 2015*.**

***Krushna Chandra Mahapatra** is pursuing Masters of Technology in Information Security and Cyber Forensics in SRM University SRM Nagar Kattankulathur603203 India.*

***S.Magesh** is currently the Asst. Professor (Sr.G), Department of Information technology SRM University SRM Nagar, Kattankulathur-603203, India.*

II. SCADA SYSTEMS

SCADA is a system operating with coded signals over communication channels so as to provide control of Remote Terminal Unit (RTU) equipment. The supervisory system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of RTU equipment for display or for recording functions. As the requirement for smaller and smarter systems grew, sensors were designed with the intelligence of PLCs and DCSs. These devices are known as IEDs (intelligent electronic devices). The IEDs are connected on a fieldbus such as Profibus, DeviceNet or Foundation Fieldbus to the PC. They include enough intelligence to acquire data, communicate to other devices and hold their part of the overall program. No single standard covers all SCADA systems and applications. Many additional standards exist that discuss specific hardware and software components of SCADA systems such as communication hardware, protocols, database compliance, and human machine interfaces [1].

A. SCADA Networks

SCADA systems are often complex networks with multiple components. These systems may be fully automated, where all control is performed by computers, fully manual, where control is performed by human operators, or a hybrid system, where some control is performed automatically and some is performed by human operators. To perform all of these functions, many SCADA systems include:

1) Field interface devices: Sensors detecting and reporting power levels, flow rates, temperature, pressure, and local control devices such as motor controls, valve actuators, and control switchboxes.

2) Operating equipment: Motors, pumps, automated factory systems, and valves controlled by the SCADA network.

3) Control computers: Embedded computers or dedicated PCs receiving information from the sensor networks, reporting this information to the management systems and controlling the associated operating equipment. These computers may make decisions automatically based on the information derived from sensors, or may relay commands received from management computers.

4) Management computers: Computer terminals with an HMI (Human Machine Interface) connected to the SCADA network. These computers provide an interface for operators to monitor and control the devices on the SCADA network.

5) Networked communication (local and remote): SCADA networks use a variety of communication technologies. Serial communication, USB or proprietary wired networks are used for short range communication. Ethernet, TCP/IP, Wi-Fi, dial-up networking, cellular packet data and other methods are used for long range communication. Increasingly, SCADA networks utilize the Internet for long range communications and remote access.

6) Interconnection to business process systems: Frequently, SCADA networks are connected to corporate networks to allow them to interconnect with business process systems.

SCADA networks may contain a mix of PCs and special-purpose embedded systems running real-time operating systems such as VxWorks, INTEGRITY, or MQX. Many of the PCs used in SCADA networks were installed when the SCADA system was first deployed and have not been updated with newer operating system versions or software patches. As a result they are often vulnerable to attack. Most embedded computers in SCADA networks were designed before security was a major concern and contain few, if any, security measures

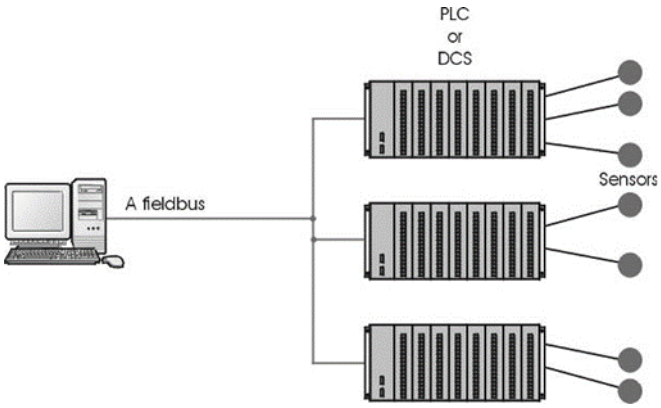

Fig. 1 Simple SCADA System

B. Protocols in SCADA Communication

In order for SCADA systems to obtain its functionality, it needs a protocol for transmitting data. Some of the SCADA protocols include Modbus RTU, RP-570, Profibus, ABB, Conitel, etc. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850 (in which T101 branched out), IEC 60870-5-101 or 104, and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols is now improved and contain extensions to operate over TCP/IP [2]. It is good security engineering practice to avoid connecting SCADA systems to the Internet so the attack surface is reduced. RTUs and other automatic controller devices were being developed before the advent of industry wide standards for interoperability [3]. The result is that developers and their management created a multitude of control protocols.

1) T101 or IEC 60870-5-101 (IEC101): It is an international standard prepared by TC57 for power system monitoring, control & associated communications. This is compatible with IEC 60870-5-1 to IEC 60870-5-5 standards and uses standard asynchronous serial tele-control channel interface between DTE and DCE. The standard is suitable for multiple configurations like point-to-point, star and multidropped.

Distributed Control System components are usually included in SCADA. IEDs, RTUs or PLCs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these RTUs and PLCs [1]. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC.

2) DNP3: The DNP3 or Distributed Network Protocol is used for communications between SCADA masters (control centers) and remote terminal units (RTUs) and/or intelligent electronic devices (IEDs). It is a set of communications protocols used between components in process automation systems. It is usually used is in utilities such as water and electric companies. It is also technically possible to use it in other utilities. It was specifically developed to facilitate communications between various types of data acquisition and control systems. It plays a crucial role in SCADA systems. It is used by SCADA Master Stations or Control Centers, Remote Terminal Units, and Intelligent Electronic Devices. It is primarily used for communications between a master station and IEDs or RTU's.

DNP3 supports multiple-slave, peer-to-peer and multiple-master communications. It supports the operational modes of polled and quiescent operation. The latter is also referred to as reporting by exception. Although the protocol was designed to be very reliable, it was not designed to be secure from attacks by hackers and other malevolent forces that could potentially wish to disrupt control systems to disable critical infrastructure. This was a major oversight. Because smart grid applications generally assume access by third parties to the same physical networks and underlying IP infrastructure of the grid, much work has been done to add Secure Authentication features to the DNP3 protocol.

Layer 7	Application	Defines types of services, communications and security	Application
Layer 6	Presentation	Converts the data from one format to another, such as from a text file to a pop up window displaying the text	Presentation
Layer 5	Session	Exchanges of data between two applications, opens, coordinates and ends sessions	Session
Layer 4	Transport	Manages error checking and services that packets are delivered	Transport
Layer 3	Network	Routes and forwards data to proper destinations	Network
Layer 2	Data Link	Builds and synchronises data packets	Data Link
Layer 1	Physical	Converts the bit stream across the network, manages the hardware and the mechanical process for sending and receiving data	Physical

Fig. 1 DNP3 Build

The DNP3 protocol is now compliant with IEC 62351-5. Some vendors, such as Itron, implement elliptic curve cryptography which the US NSA considers sufficient to protect information as "top secret" with only 384 bits. Implementation of ECC over DNP3 is not very widespread yet. The DNP3 protocol is also referenced in IEEE Std. IEEE 1379-2000, which recommends a set of best practices for implementing modern SCADA Master-RTU/IED communication links. These include not just encryption but other practices that enhance security against well-known intrusion methods [1].

3) Modbus: The Modbus transmission protocol was developed by Gould Modicon (now Schneider) for process control systems and use with its programmable logic controllers (PLCs). It has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices [4]. The main reasons for the extensive use of Modbus over other communications protocols are: It is openly published and royalty-free, relatively easy industrial network to deploy and it moves raw bits or words without placing many restrictions on vendors. Modbus allows for communication between many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer. Modbus is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. Besides the standard Modbus protocol, there is another Modbus protocol, called Modbus Plus [10].

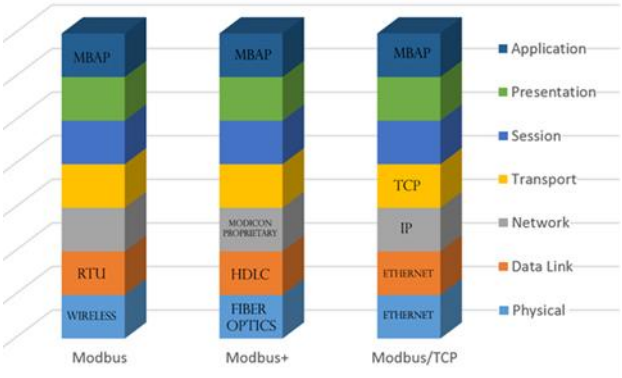

Fig. 2 MODBUS Protocol

4) RP570: It is a protocol used between an RTU (Remote Terminal Unit) in a substation and the FE (Front End), which is usually the SCADA software in the Control Center. RP570 was developed by ABB in beginning of 1990. It was based on IEC 57 part 5-1, presently known as IEC 60870. Known variations are RP571, ADLP80 and ADLP180.

5) HDLC: High Level Data Link Control) has been defined by the International Standards Organization for use on both multi-point and point-to-point links. Other descriptions of it include SDLC (synchronous data link control used by IBM) and ADCCP (advanced data communication control procedure used by ANSI). HDLC will be the reference used throughout the following text. In contrast to the BSC, a character-based protocol, HDLC is a bit-based protocol. It is interesting to note that it is a predecessor to the local area network protocols such as Ethernet.

C. Vulnerability in SCADA Systems

In the past, when SCADA systems were independent and vendor-controlled systems with no connections to other systems and when the network protocol was proprietary, only a few people, such as developers and hackers, knew of the existence of SCADA installations. However, the present SCADA systems are widely distributed and networked [5]. Since the systems are dependent on open protocols for the internet, they are vulnerable to external remote cyber threats. SCADA systems are different from general information systems in terms of security management. In the risk and security management of general information systems, after analyzing the assets, threats, and vulnerabilities of information systems and calculating the degrees of a risk, security measures are prioritized for calculating the remaining risk. In contrast, for SCADA systems, the analysis of the assets is performed not from the viewpoint of systems but from the viewpoint of target facilities managed and operated [11].

D. Underlying Security Issues

Security issues underlie each the path of least resistance in achieving each of the attack goals:

1) Lack of Confidentiality: All MODBUS messages are transmitted in clear text across the transmission media.

2) Lack of Integrity: There are no integrity checks built into the MODBUS application protocol, and as a result it depends on lower layer protocols to preserve integrity.

3) Lack of Authentication: There is no authentication at any level of the MODBUS protocol, with the possible exception of some undocumented programming commands.

4) Simplistic Framing: MODBUS/TCP frames are sent over established TCP connections. While such connections are usually reliable, they have a significant drawback for the MODBUS application: TCP does not preserve record boundaries.

5) Lack of Session Structure: Like many request/response protocols (i.e. SNMP, HTTP, etc.) MODBUS/TCP consists of short-lived transactions where the master initiates a request to the slave that results in a single action. When combined with the lack of authentication and poor TCP initial sequence number (ISN) generation in many embedded devices, it becomes possible for attackers to inject commands with no knowledge of the existing session [5].

III. ATTACKS ON SCADA NETWORKS

There is little dispute that additional protection is needed for SCADA networks. The FBI recently acknowledged that hackers gained access to SCADA systems in many different countries. Other reported attacks on SCADA systems include:

- Train system delays.
- Sewage system spillage caused by an employee.
- Automotive manufacturing plant shutdown.

Given the large number of deployed SCADA devices and the slow migration to modern, secure SCADA devices, the SCADA marketplace needs the ability to add security to both existing legacy devices and new designs in a cost-effective manner for both remote SCADA devices located outside of a corporate network and for local SCADA devices such as

those residing on the factory floor. The Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security Survey provides an overview of the computer security methods used and types of attacks experienced by a cross-section of companies. While this survey is not focused on the electric utility industry (4% of respondents were from utilities), it does provide a baseline for the types of attacks perpetrated and damage done by unauthorized users. According to the CSI/FBI survey, approximately 56% of respondents reported unauthorized computer use in the past 12 months, slightly less than the numbers reported in the previous 4 years.

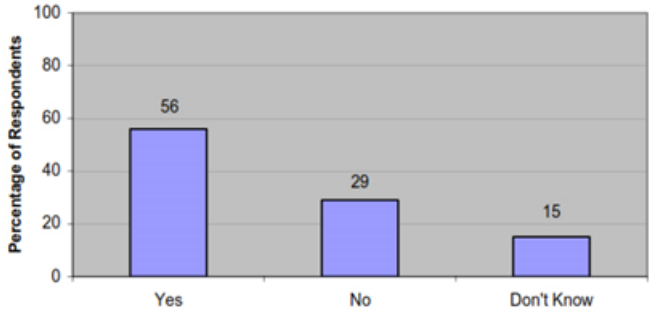

Fig. 3 Unauthorised use of Computers

The downward trend in reported attacks may be somewhat misleading. The report also shows an increasing trend toward not reporting unauthorized use of computer systems. Respondents cited fear of negative publicity or exploitation by competitors as primary reasons for not reporting. Fig. 5 shows the actions taken by respondents when they were attacked.

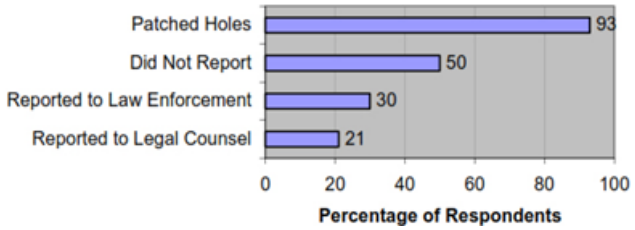

Fig. 4 Response to Cyber Attacks

Types of attacks and/or misuse include viruses, laptop theft, net abuse, system penetration, denial of service, and others. Fig. 6 shows types of attacks/misuse and their trends during the past four years.

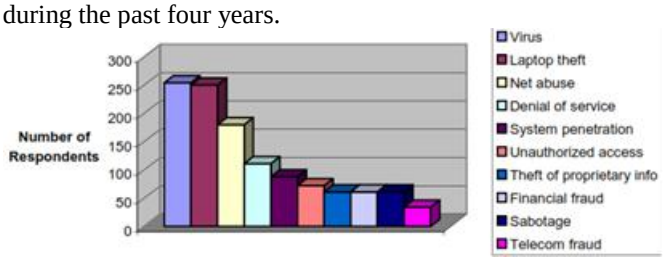

Fig. 5 Types of Cyber Attacks

Seen from this figure that several attack types show an increasing trend, including system penetration and denial of service. These two attack types, in addition to viruses, typically use the internet as a source of attack. Indeed, the survey found an increasing trend toward internet-based attacks compared to inside attacks or remote dial-in (see Fig. 7).

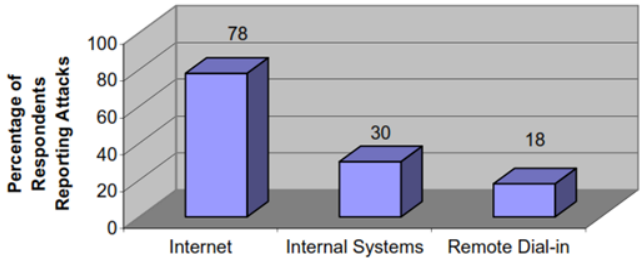

Fig. 6 Communications media utilized for attacks

Regarding types of attackers, survey respondents, as shown in Figure 8, pointed to independent hackers and disgruntled employees as the most common. Domestic competitors, foreign corporations, and foreign governments were also significant sources of attack. Since many attackers are not caught, it is not clear whether this data is based only on those who are caught or whether these numbers are based on conjecture by the respondents [6].

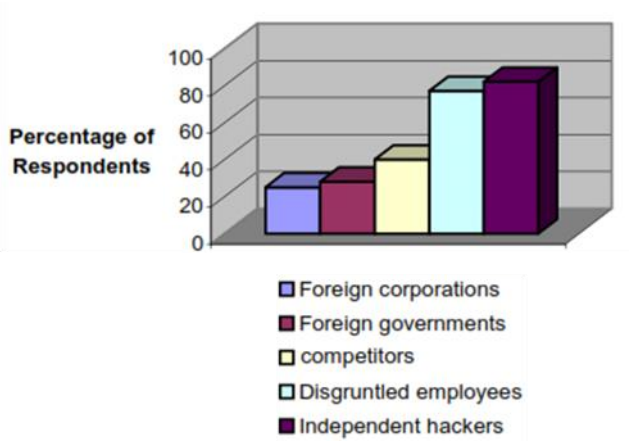

Fig. 7 Types of Cyber Attackers

A. Attack Tools

An attacker need not be an accomplished programmer to penetrate a network or computer system. Several tools are available to either gain access to or learn more about a system targeted for attack. This section gives a brief description and some examples of several types of tools of this nature [12].

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

2) Denial of Service Tools: Denial of service (DOS) attack tools work by flooding a network with either legitimate or malformed packets of data, thereby effectively locking out legitimate traffic. Some tools come with several malformed packet types known to cause certain systems to crash.

Examples of these tools are smurf, fraggle, and SYNflood. SYNflood sends connection requests (SYN packets) to the intended target, but never acknowledges the connection so that many ports are left open on the target machine(s).

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

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

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

B. Mitigations to the Vulnerabilities

Several tools are also available to defend systems. These tools include passwords, firewalls, intrusion detection systems, virtual private networks, and access control. The following sections provide a brief description of each of these tools [12].

1) Firewalls: Unlike enterprise firewalls that protect all of the computers on a corporate network, a SCADA firewall protects just a single SCADA device. Since the firewall is filtering traffic for a single SCADA device only, it does not need to perform any routing functions and can be customized specifically for the requirements of protecting a specific SCADA device. It only requires two Ethernet ports and can be implemented on low cost hardware, providing a customized yet cost-effective solution. The device is simply plugged into the network in front of the SCADA device, inserting a layer of protection.

2) Passwords: Passwords can be an effective security method. Two factors that influence their effectiveness are whether the passwords are strong passwords and whether they are encrypted. Strong passwords are defined as passwords of six characters or more, with at least one special character or digit and mixed-case character, that do not form a pronounceable word, name, date, or acronym. Table 5-1 shows a comparison of the time it takes a password cracking program to crack passwords of different lengths for strong passwords (require brute-force cracking) and for dictionary passwords. Dictionary passwords in this case are based on the 25,143-word UNIX spell-check dictionary that contains words, numbers, common names, and acronyms. Strong passwords are based on a 90-character set of letters, numbers, and special characters.

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

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

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

6) Security Status Monitoring: Security monitoring controls shall issue automated or manual alerts when they detect something out of the norm

- Processes for enabling ports on hosts, routers, and firewalls
- Alerts generated by the should be logged
- Logs must be maintained for a minimum of 90 days

C. Physical Security

Physical security at electric power substations and generation facilities varies from installation to installation depending on level of risk, level of impact, and cost of implementation. Cost is a particularly important factor as a result of the competitive pressures brought on by deregulation. The main categories of physical security at electric power substations are physical barriers and electronic barriers. Examples of physical barriers include fences, walls, and locks. Examples of electronic barriers include photo-electric/motion sensing, video surveillance systems, building systems, computer security systems, passwords, dial-back verification, selective access, virus scans, and encryption.

IV. CONCLUSION

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

Some of these gaps include:

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

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

• Lack of regular assessments of SCADA vulnerabilities.

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

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

• Lack of common testing methods for identifying vulnerabilities.

• Lack of methods to quantify cyber-security risk.

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

• Quantity of operating system and application security patches makes staying current a difficult task. Bottlenecks in power grid make widespread outages more likely.

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

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

• Implement better security in substation devices (e.g., RTUs, IEDs).Develop testing criteria for control systems vulnerabilities. Perform real-world testing on live or test systems to isolate and mitigate vulnerabilities of integrated systems.

• Implement cyber security in the most widely used SCADA protocols (e.g., DNP, ICCP). Streamline patch management of control systems.

• Reduce potential consequences of cyber-attack by strengthening power grid.

REFERENCES

[1] Practical modern SCADA protocols - dnp3, 60870-5 and Related Systems by Gordon Clarke and Deon Reynders.

[2] Byres, E., Carter, J., Elramly, A., and Hoffman, D.; "Worlds in Collision-Ethernet and the Factory Floor", ISA 2002 Emerging Technologies Conference, Instrumentation, Systems and Automation Society, Chicago, October 2002

[3] Stamp, J., Dillinger, J., Young W., and DePoy, J.; "Common Vulnerabilities in Critical Infrastructure Control Systems", Sandia National Laboratories, Albuquerque, NM, May 2003

[4] MODBUS Application Protocol Specification V1.1, Modbus Organization, June 12, 2002

[5] Byres, E. and Lowe, J.; "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE 2004 Congress, VDE, Berlin, October 2004

[6] Computer Security Institute/Federal Bureau of Investigation, 2003 Computer Crime and Security Survey.

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

[8] Franz. M; "Flexible Threat Modeling." www.io.com/~mdfranz/papers/unpub-may04-flexible-threat-modeling.pdf.

[9] Moore, A.P., Ellison, R.J. and Linger, R.C.; Attack Modeling for Information Security and Survivability, www.cert.org/archive/pdf/01tn001.pdf.

[10] MODBUS Application Protocol Specification V1.1, Modbus Organization.

[11] G. Ericsson, "Information Security for Electric Power Utilities (EPUs) – Cigré Developments on Frameworks, Risk Assessment and Technology," Paper TPWRD-543-2008, IEEE Transactions on Power Delivery, Vol. 24, No. 3, July 2009.

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

