Journal of Advances in Science and Technology

Vol. VII, Issue No. XIII, May-2014, ISSN 2230-9659

AN ANALYSIS UPON VARIOUS SECURITIES OF ELECTRICAL POWER SYSTEMS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

Journal of Advances in Science and Technology
Vol. VII, Issue No. XIII, May-2014, ISSN 2230-9659

An Analysis upon Various Securities of Electrical Power Systems

Prof. Ravi Shankar Pandey[1] Prof. Bikash Chandra Saha[2]

[1]Assistant Professor, R.C.I.T. Bishrampur, Jharkhand

[2]Assistant Professor, C.I.T. Tatisilwai Ranchi

Abstract – Security of supply has been always a key factor in the development of the electric industry. Adequacy, quality of supply, stability, reliability and voltage collapse along with costs have been always carefully considered when planning the future of the electric power system. Since 1982, when world's deregulation process started, the introduction of competition at generation level brought new challenges, while the proper operation of the electric power system still require physical coordination between non cooperative agents. The increasing development of SCADA/EMS systems, the growing number of market participants, and the development of more complex market schemes have been more and more relying on Information Technologies, making the physical system more vulnerable to cyber security risks. Now cyber security risks look bigger than the physical ones. We developed a review of some of the vulnerability risks that actual electric power systems face, showing some implementation issues of it. We also comment some the steps that NERC is leading to ensure a secure energy sourcing to the U.S. Economy.

Disruption of electric power operations can be catastrophic on the national security and economy. Due to the complexity of widely dispersed assets and the interdependency between computer, communication, and power systems, the requirement to meet security and quality compliance on the operations is a challenging issue. In recent years, NERC's cybersecurity standard was initiated to require utilities compliance on cybersecurity in control systems - NERC CIP 1200. This standard identifies several cyber-related vulnerabilities that exist in control systems and recommends several remedial actions (e.g., best practices). This paper is an overview of the cybersecurity issues for electric power control and automation systems, the control architectures, and the possible methodologies for vulnerability assessment of existing systems.

----------♦----------

INTRODUCTION

LECTRIC power systems and automation systems include process control and supervisory control and data acquisition systems (SCADA) that operate safe, reliable, and efficient physical processes for the energy system. These systems are connected via a highly automated network. A variety of communication networks are interconnected to the electric grid for the purpose of sensing, monitoring, and control. Computer and communication devices are widely installed in power plants, substations, energy control centers, company headquarters, regional operating offices, and large load sites. These devices and systems are increasingly networked and complex.

Computer, communication, and power infrastructures are interdependent in a power grid. The measurements and control signals acquired by SCADA are utilized in an energy management system (EMS) of the power grid to perform a wide range of system functions, including real-time control of the power grid. Failure of an important communication channel in the operational environment could result in an inability to control or operate important facilities, leading to possible power outages. Congestion of the communication networks could delay the transfer of power system data or control signals that may be critical in some scenarios.

Although the complex infrastructure provides great capabilities for operation, control, business, and analysis, it also increases the security risks including power system cybersecurity (PSC) threats and vulnerability. A cyber-attack on the control center computer systems could lead to undesirable switching operations, resulting in widespread power outages. Another cyber-attack scenario is to penetrate the substations and alter protective relay settings, which could result in undesirable switching actions. Currently the system may not have strong measures against cyber-attacks and, therefore, vulnerabilities exist. Consequently, there is a growing

demand to address these cybersecurity issues in a comprehensive and systematic manner.

SCADA protocols have advanced from point-to-point links to newer protocols and communication methods. These newer methods allow for a higher level of redundancy and speed of transmission. An important issue is that the current practice has to be a hybrid of the original 1970s practices and today's standards. The reason for this is the expected life of SCADA devices. Since a device has to operate for 15–20 years, a wide variety of devices based on different technologies could end up in the field. Some may be "smart" devices with a processor onboard and others "dumb" with a hardwired set of tasks. Sometimes a site might be retrofitted and brought up to date, but in most cases that only happens when other maintenance work is required or the device is near the end of its lifetime. An understanding of the integration issues is important when both past and future SCADA protocols are involved.

Due to the technological changes over the last decade, the trend of protocols has been refined to be more flexible and accommodating to industrial needs, specifically in the open architecture with high-speed communications. The interoperability and maintainability of the standard protocols ensure communication security and stability. The interoperability also improves its interactions with other systems. However, these improvements may also lead to PSC vulnerabilities.

Various SCADA attacks through communication channels in the recent past have highlighted the extent to which the SCADA systems are vulnerable and the need to protect them against cyber-attacks. Recent findings report the plans to disrupt the U.S. power grid. In addition, the North American Electric Reliability Corporation (NERC) directives make it mandatory to undertake cyber security vulnerability assessment at the operator locations and to take corrective measures. The NERC security document and the ISO/IEC17799 standard specify guidelines for cyber security in power systems.

The decentralization of the property and also the decentralization of the decision making process rely every day in more complex and evolving Information Technologies IT. In parallel to the increase of the number of market participants, we have faced an increase in the number of SCADA/EMS systems operating in the electric industry, raising the interdependency between the operation of the whole electric grid (including generation, transmission, distribution) and the operation of the wholesale electric market. The electric market and the electric power system are every day more closely tight. The operation of one depends on the continuous and reliable operation of the other.

Now the vulnerability of the power system is not mainly a matter of bulk power electric system or physical system, is every day more a matter of cyber security. A market participant unable to see accurately the market or a SCADA/EMS unable to control properly some facilities could be as disastrous as a terrorist attack to some key power plants or transmission lines.

Since September 11, 2001 the threat of terrorist attack has raised as a big threat to many areas of the US economy. Almost every economic and social function is based in some way on the sourcing of energy, telecommunication services, transportation, etc. An attack to these infrastructures would bring devastating effects on the economy and in the people's life.

As Massoud Amin explains in, from the power systems we can reflect on mainly three kinds of threats over society:

a) Attacks upon the power system - Here the target is the electric infrastructure. For example, terrorists could attack simultaneously two substations or key transmission towers in order to cause a black out in a big area of the grid. Other example could be an attack to the electric market.

b) Attacks by the power system - Terrorists could use some installations of the power system to attack the population, for example, using power plant cooling towers to disperse chemical or biological agents.

c) Attacks through the power system - Terrorists could use some installations of the power system to attack civil infrastructure, for example, terrorists could couple an electromagnetic pulse through the grid to damage computer or telecommunications infrastructure.

We will focus our analysis in the first kind of threat, attacks on the electric power system itself. To contribute in this assessment, herein we develop an analysis of the existing material about vulnerability focusing in the interaction of the power systems with communication technologies.

EVOLUTION OF SCADA SYSTEM

The architecture of SCADA system has evolved through 1960s with the integration of new computing technologies into the grid environment. The evolution of SCADA system involves in three stages: (1) monolithic, (2) distributed, and (3) networked. The involvement of networking using TCP/IP has become prominent due to the economic, common deployment.

A. Monolithic **-** This is the earliest SCADA architecture using mainframe systems with redundancy by installing identical mainframe systems. It is a standalone system with no connectivity to others. The communication of remote terminal units (RTUs) was implemented using vendor-proprietary protocol and equipment. Hence the limitation of

functionality depends on the specific types of equipment and protocols.

B. Distributed - The distributed architecture of the SCADA system distributes the computing burden to a number of machines in a network. Each machine is configured with different functions and roles. The redundancy of each machine can be provided through other machines in the network. Comparing to the earlier systems, the communication protocols between the field and control center are similar. As a matter of fact, the system can still be limited by the vendors supporting the hardware, software, and peripheral devices.

C. Networked - The networked architecture has been widely used due to the nature of open system architecture that facilitates the compatibility to connect three party devices, even though some are still vendor-proprietary. Its major improvement is the open system architecture that utilizes the standardized protocols. This has been shifted from locally redundant systems to wide area networking (WAN) with the use of Internet protocol (IP) for multi-site control centers. This is used for disaster survivability that improves reliability of the facility housing the SCADA master by distributing the processes across physically separate locations.

From point-to-point links to newer protocols and communication methods. These newer methods have the advantages of greater redundancy and speed of transmission. As mentioned, an important issue is that the current practice has to be a hybrid of the 1970s practice and today's standards. An understanding of the integration issues is important when both past and future SCADA protocols are involved. Table 1 is a summary of the SCADA protocol evolution from 1970s.

Years	Protocols
1970s	*No standard protocol*: Point-to-point, hardwired remote control and tone telemetry
1980s	*Proprietary and industrial protocols*: Modbus, Modbus plus, and proprietary or vendor specific protocols
1990s	*Open protocols*: DNP by Westronics (GE); UCA by EPRI for EMS mainly in North America; IEC 60870 by International Electrotechnical Commission (IEC).
2000s	*Promoting standard protocols*: DNP primarily in North America. UCA merged into the main stream of standard protocols, IEC61850.

TABLE 1: EVOLUTION OF THE SCADA PROTOCOLS.

Due to the technological changes over the last decade, the trend of protocols has been refined to become more flexible and accommodating to industrial needs, specifically in an open architecture with high speed communications. The interoperability and maintainability of standard protocols ensure communication security.

VULNERABILITIES

Smart grid network introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of attacks. These vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable. As proposed in, the following vulnerabilities are the most serious in smart grids:

1) ***Customer security*:** Smart meters autonomously collect massive amounts of data and transport it to the utility company, consumer, and service providers. This data includes private consumer information that might be used to infer consumer's activities, devices being used, and times when the home is vacant.

2) ***Greater number of intelligent devices*:** A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the smart grid network (100 to 1000 times larger than the internet) makes network monitoring and management extremely difficult.

3) ***Physical security*:** Unlike the traditional power system, smart grid network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.

4) *The lifetime of power systems*: Since power systems coexist with the relatively short lived IT systems, it is inevitable that outdated equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.

5) ***Implicit trust between traditional power devices*:** Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a

device sending a false state makes other devices behave in an unwanted way.

6) ***Different Team's backgrounds*:** Inefficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability.

7) ***Using Internet Protocol (IP) and commercial off-the- shelf hardware and software*:** Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

8) ***More stakeholders*:** Having many stakeholders might give raise to a very dangerous kind of attack: insider attacks.

NERC-CIPAG & SECURITY

NERC has been in charge of the reliability (including safety and security) of the interconnected grid since 1968. It has developed many initiatives such as the followings:

Establishment of an Information Sharing and Analysis

Center for the Electric Sector (ES-ISAC).

Development of a Public Key Infrastructure (PKI).

Development of spare equipment database.

Development of security guidelines for the electric sector.

1) Information Sharing and Analysis Center for the Electric Center

Due to interdependences between the different sectors of the economy, coordination between the private parties and the government is required to face the terrorist threat. The ISACs (Information Sharing and Analysis Centers) were created in the different industries to build a cooperative security planning and analysis, these ISACs are the communication channel within industry and government.

NERC hosts the ISAC of the Electric System (ISACES), it was working on September 11 and facilitated the necessary communication to secure key electric industry assets.

2) Public Key Infrastructure (PKI).

As Gent and Constantini explained in, PKI is a systematic approach to information security that connects policy and technology to establish a trusted environment to electronic businesses. It is based on public key cryptography and public key certificates, PKI provides privacy, authentification, integrity, and non-repudiation1 in the digital market place.

3) Spare equipment database.

In order to help electric companies to recover after a terrorist attack one decade ago NERC created a spare equipment database. It helps to locate spare equipment for loan under emergencies, ensuring a rapid recovery.

C. Security Guidelines

The *Security Guidelines* are mainly a compendium of practices, commonly accepted as best practices, to protect the critical facilities and functions, where each company define its own critical facilities. The Guidelines should be adapted to each company by themselves and should evolve through the time (as technology, organization of the market, power system and threat do). Also people in the company should be trained to success in protecting the company from the different threats.

The main focus of the guidelines is Physical and Cyber Security

The main components of the security guidelines are the followings:

a. Vulnerability and Risk Assessment

b. Threat Response Capability

c. Emergency Management

d. Continuity of Business Processes

e. Communications

f. Physical Security

g. Information Technology / Cyber Security

h. Employment Screening

i. Protecting Potentially Sensitive Information

CHALLENGES FOR NEW SECURITY SOLUTIONS

Security solutions developed for traditional IT networks are not effective in grid networks because of the major differences between them. Their security objectives are different in the sense that security in IT networks aims to enforce the three security principles (confidentiality, integrity and availability), while the security in automation (grid) networks aims to provide human safety, equipment and power lines protection, and system operation. Moreover, the security

architecture of IT networks is different than that of the Grid network since security in IT networks is achieved by providing more protection at the center of the network (where the data resides), while the protection in automation networks is done at the network center and edge. Their underlying topology is also different where IT networks use a well-defined set of operating systems (OSs) and protocols, while automation networks use multiple propriety OSs and protocols specific to vendors. Finally, their Quality of Service (QoS) metrics are different in the sense that it is acceptable in IT networks to reboot devices in case of failure or upgrade, while this is not acceptable in automation networks since services must be available at all times.

POWER SYSTEM CYBERSECURITY VULNERABILITIES

PSC vulnerabilities involve three main components, i.e., computer, communication, and power system. Attacks can be targeted at specific systems, subsystems, and multiple locations simultaneously from remote. These components are highly interdependent. The security level indicates the severity of the damage that might be done if there is a penetration into the power system. At the level of computer systems, security is divided into three sub-categories, i.e., Internet, Intranet, or individual computers. The PSC threats arise from the various attacks discussed here. They represent the different attack types, mechanisms and other potential pitfalls that need to be considered in the design of a secure SCADA network.

1) *Cyber Attackers*: PSC threats to SCADA systems may arise from two sources, namely internal disgruntled employees and external malicious hackers. The threat from internal employees is real but not very likely as it would be easier to identify the attacker in most cases and the fear of the consequences would in itself reduce the likelihood of such attacks. However, it is still necessary to take preventive measures to avoid such occurrences. On the other hand, it is easier for an external hacker to launch cyber-attacks and the attack could go undetected, thereby making the SCADA systems more vulnerable.

2) *Targeted Cyber Attack Types*: Malicious attackers can launch targeted attacks such as sniffing packets at an Internet service provider (ISP) or carrier and then maliciously modifying the packets in the network to achieve the expected results. They could proactively exploit software bugs and other vulnerabilities in various systems, either in the corporate network or the SCADA network, to gain unauthorized access to places such as control center networks, SCADA systems, interconnections, and access links. Openly available vendor documentation for proprietary power systems control software also makes them vulnerable to software exploits. They could configure unauthorized access points to send false information to confuse the SCADA systems in order to trigger unwanted countermeasures. They could target RTUs, intelligent electronic devices (IEDs), uplink connections, and other physical entities to disrupt services. They could exploit the deterministic nature of the inter-center control communications protocol (ICCP) messaging protocol to achieve the desired effects on the SCADA network and the electric grid.

3) *Flood-based Cyber Attack Types*: Cyber-attacks that are based on denial of service (DoS) mechanisms, and others that spread due to viruses and worms by causing a traffic avalanche in short durations, can potentially bring down systems and cause a disruption of services. There is no well-known, fool-proof, defense against such cyber-attacks in the computing literature. Various effective ad-hoc solutions have been adopted on traditional computer networks. If the access links that connect the SCADA network to the Internet are swamped by heavy traffic caused by such attacks, it could prove disastrous as the control and supervisory data (including alarms, IED data) flowing to the SCADA network could be lost in the network. The gateway or firewalls installed to monitor the incoming traffic could be overloaded by the large volumes of attack traffic. Thus the ability of the SCADA network to respond to actual failures can be significantly affected. Also, the traffic flood could contain malicious ICCP messages that could confuse the SCADA systems to a great extent.

CONCLUSION

The interconnection of old SCADA systems to internet, networks or telephone lines, and the ever more intensive use of computer networks and wireless systems have risen the fact that potential terrorists, bored hackers, unhappy employees, and smart kids around the world, could access the controls of power systems and hurt countries in one of the key factors of their economies, producing billionaire losses in almost all the sectors of their economies.

We have presented the scale of this problem, some examples, and the main measures and practices that the electric industry must be taken in order to reduce these risks as much as is economically desirable.

Cyber-power system security is a critically important issue today and for the future. In this context, several research challenges must be addressed, which include vulnerability assessment, security framework, modeling, and validation.

This paper presented an overview of the research issues, ongoing research, and future areas of research. Specifically, the future work includes (1) integrated modeling techniques that capture the cause-effect relationship between cyber-physical systems, (2) metrics to quantitatively assess the survivability of the system and to carry out a security investment analysis quantifying the cost benefits, and (3) real-world data and tested evaluations to validate the models.

REFERENCES

- Amin Massoud, Modeling and Control of Complex Interactive Networks. *IEEE Control Systems Magazine*, February 2002.
- Brown Alan, SCADA vs the hackers, can freebie and a can of Pringles bring down the U.S. power grid?, Mechanical engineering, New York, December , vol. 124, issue 12
- G. N. Ericsson and A. Torkilseng, "Management of information security for an electric power utility – On security domains and use of ISO/IEC17799 standard," *IEEE Trans. on Power Delivery*, vol. 20, no. 2, Apr. 2005, pp. 683-690.
- Gent Michael, Constantini Lynn, Reflections on Security, IEEE power & energy magazine, January/February 2003.
- M. Berg and J. Stamp, "A reference model for control and automation systems in electric power," Sandia National Laboratories.
- S. Pudar, M. Govindarasu, C.-C. Liu, "PENET: A pragmatic method for attack modeling and validation," submitted for publication, 2007.
- "Understanding SCADA system security vulnerabilities," Symantec White Paper, 2005.