Paper 0030

CYBERSECURITY RECOMMENDATIONS FOR COMMUNICATION SYSTEMS IN THE COLOMBIAN ELECTRICAL SECTOR

PhD (c) Hermes Javier Eslava
Universidad Distrital – Colombia
hjeslavab@udistrital.edu.co

Luis Alejandro Rojas
Universidad Distrital – Colombia
larojasc@udistrital.edu.co

Danny Pineda
OPENLINK - Colombia
dpineda@oplk.com

ABSTRACT

Communication systems are essential for the proper operation of the electrical sector in Colombia. However, these systems are still unprepared to face the problems caused by cyber-*terrorism attacks*. The threat of cyber-terrorism emerged in this very century as one of the biggest challenges for the electrical sector. In fact, improvements in efficiency in this sector have been achieved by acquiring *new equipment that is compliant with communication networks standards (e.g. Internet remote controllers). In this article we present a proposal for implementing Cyber-security strategies at typical Colombian power substations by following the international standards in the field. This paper promotes the implementation of best practices for the electric power sector in order to face one of the major challenges of the* 21st *century in terms of safe operation at any electrical sub-station, namely* cyber-*terrorism.*

INTRODUCTION

The common approach of the electric power industry in Colombia has been based almost exclusively on the implementation of equipment to maintain the reliability of the power systems; however, this aspect of development has come together with the incorporation of automation techniques. These techniques are supported by an information infrastructure based on robust electronic devices, which, although highly-reliable, are the target of potential threats to the confidentiality, integrity, availability and access to authorized personnel of a company. The issue of cyber security in the electric power industry is fairly new and has appeared in the literature only until this decade [1]. Around the world, several events that compromised the security of communication networks performing telecontrol tasks (from a control center via SCADA applications) have taken place [2]. Overcoming such a challenging situation has led to the creation of new standards (in terms of cyber security and more stringent equipment specifications) associated to the new elements involved in the control of electric power substations. The set of standards issued by NERC in the USA are among the most widely recognized standards [3]. In order to identify the gap in Colombia, this paper offers a review of the present infrastructure of a typical power substation in Colombia regarding Cyber-security issues. Additionally, we develop a proposal for improving security in Colombian power substations by embracing international standards such as NERC. The purpose is to identify potential problem areas and provide guidance on the implementation of a Cyber-security strategy for communication networks associated with power substation telecontrol.

PROBLEM STATEMENT

The threat of cyber terrorism, whose deliberate actions are aimed at attacking and damaging critical information-and-control systems, has increased because the necessary efforts to successfully carry out activities of this nature are not as demanding when compared to the existent preventive actions.

Electric companies are particularly vulnerable when considering the natural tendency for their infrastructure critical control systems to be connected through the Internet. For example, in 2003, computer hackers developed the fastest-growing computer virus in history (called "slammer") which was spread via Internet [4]. When this virus began to circulate on the Internet, it doubled its size every 8.5 seconds, infecting more than 90 percent of the vulnerable main computers within 10 minutes. The virus [5] was first released in a nuclear plant in Ohio (USA), where it seized the SCADA system, causing operators to lose control for about six hours, which clearly compromised the interconnected power system of the United States.

More recently, a computer worm called stuxnet was discovered in June 2010[6]. This is the first worm capable of reconfiguring Supervisory Control and Data Acquisition (SCADA) systems. It is highly dangerous because it might even affect critical infrastructures such as nuclear power plants, military facilities and electric power substations.

In Colombia, communication networks between substations as well as remote control centers and power substations themselves were all constructed in the past century, therefore they were designed without considering communication-associated Cyber-security aspects required for the proper operation of electrical systems. This fact makes it necessary to update systems architecture (especially in terms of Cyber security) according to new standards and also to real implementations that have emerged worldwide during this century.

INTERNATIONAL STANDARDS

The following is a summary of the standards that represent

the most relevant recommendations for the electricity sector [7]:

- ISO/IEC17799:2005 and ISO/IEC 27001:2005 Standards that focus on information security management
- ISA-99.00.02-Part 2: Establishing Industrial Automation and Control Systems Security.
- IEC 62351 Data and Communication Security regarding electric power systems management and information exchange.
- NISCC Good Practice Guide on Firewall, Deployment for SCADA and Process Control Networks, National Infrastructure Security Coordination Centre (NISCC).
- NISTIR 7628: Developed and published guidelines for Smart Grid cyber security (Guidelines for Smart Grid Cyber Security, NISTIR 7628, published, August 2010)
- NERC CIP 1300: NERC is the North American Electric Reliability Corporation which it is committed to ensuring the reliability of the bulk power system in North America.

These standards are considered to be international best practices, especially because they focus on cyber security and proper integration with other existent standards that govern the international electric power sector at present. In short, these standards provide an overall approach to this global phenomenon.

CYBERSECURITY IMPLEMENTATION IN COLOMBIAN ELECTRIC POWER SUBSTATIONS

Present situation in Colombia

In Colombia, electric power substations rely on communication networks which provide the following services:

- Tele-control: It refers to the connection of Remote Terminal Unit equipment (RTUs) whose functionality is to send electrical variables typically routed by using the IEC 60870-101 protocol for services within the substation, and the IEC 60870-104 protocol for communicating with the control center.
- Standard telephony: It is based on analog communications that are used for safety-critical orders, which are recorded by the control center.
- Tele-protection equipment in critical substations: These are point-to-point communications between the different protective circuit breakers. Response times for this equipment range from 20 to 50 ms.
- Security-camera systems: This service involves communications for special purposes, particularly to monitor security events within the facilities of substations.
- Tele-management in substations equipment: Equipment with RS232 and RS485 serial connections whose information is required by and transported along the network to a management center. The data informs the management center about the status of the equipment parameters and allows making remote modifications as necessary.
- Access control systems: This service refers to the elements employed to remotely grant authorized personnel physical access to the facilities of a substation.
- Energy meters: These are the elements that record the energy consumption of the system. Subsequently, the recorded information is sent to the control center in order to calculate global energy consumption.
- Bus networks: In some substations, networks of this type have been built according to the IEC 61850 standards, which provide substation interoperability. This service has been available only until recently.

Communications associated to these services are implemented in two different fashions, namely real time elements, which use independent networks with protocols such as IEC 104, and management-and-energy-measurement elements, which employ the proprietary protocols of the different components in order to gather and handle information over serial wired networks such as RS232 or RS 485.

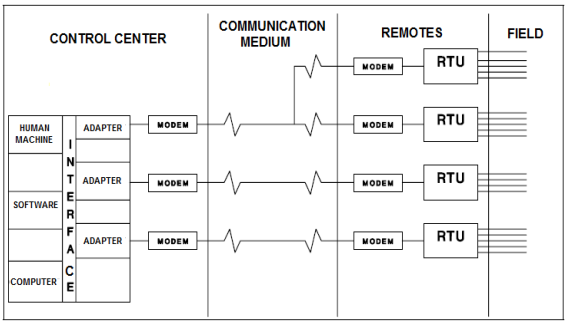

Figure 1. A traditional telecontrol system in Colombian substations

In general, today's substations do not have encryption systems (applied to control processes) intended for critical elements such as protection circuit breakers, whose function is to avoid fault extension to other elements of the national

electric system. According to official estimates, as many as 75% of Colombian power substations do not have secure encrypted connections, principally because substation design was made several years ago, mindless of security issues. Moreover, the security elements employed do not implement simple security key-protection measures such as passwords or periodic system rebooting.

Expected scenario

A survey of best practices for improving power substations security, including the different risks associated with cyber terrorism as well as the way communications systems were built and services were implemented in the past, suggests the following guidelines:

a) Substation communication networks shall be implemented using up-to-date, secure protocols, such as IEC 61850 (Fig. 2) [8].

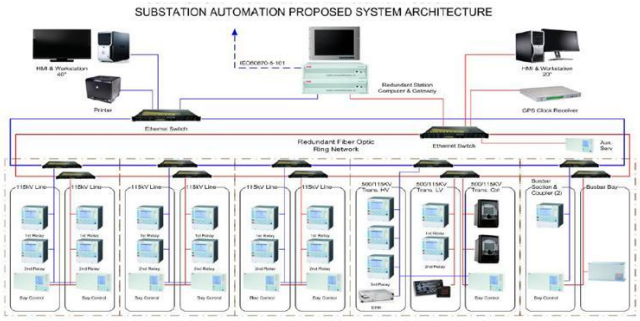

Figure 2. IEC 61850 substation architecture.

b) In order to face the different security risks associated to power substations, the recommendations from IEC 62351standards [9] must be adopted.

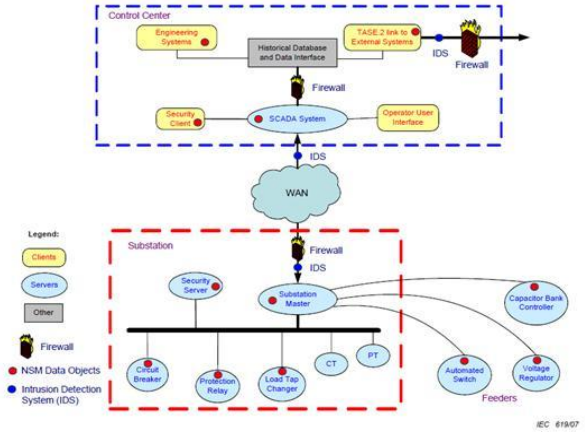

Figure 3. Optimal arquitecture according to IEC 62351

As shown in figure 3 (architecture proposed by IEC 62351), security elements such as firewalls and IDs have become increasingly necessary in electric power substations [10], allowing more flexibility and functionality when dealing with the substation's local control, which ultimately prevents important networking risks for the Colombian electric power substations.

c) Cyber-security control mechanisms must follow what is indicated in the NERC standards [11]. By implementing such recommendations, a whole management cycle is created in terms of Cyber-security, which extends to aspects such as critical-asset systematic identification, personnel controls, the procedures, and the technologies employed in critical cyber-assets of both the power substations and the control centers.

TABLE I. NERC STANDARDS REQUIREMENTS

STANDARD	
CIP-002-3	Critical Cyber Assets Identification
CIP-003-3	Security Management Controls
CIP-004-3	Personnel and training
CIP-005-3	Electronic Security Perimeter(s)
CIP-006-3	Physical Security of Critical Cyber Assets
CIP-007-3	Systems Security Management
CIP-008-3	Incident Reporting and Response Planning
CIP-009-3	Recovery Plans for Critical Cyber Assets

In general terms, the standards described herein are mature enough to be reliably implemented in the Colombian electric power sector in the short and medium term.

CONCLUSIONS AND RECOMMENDATIONS

The adoption of NERC in Colombia is recommended due to the new security vulnerabilities associated to Cyber-security issues in the electric power industry. Also, an exhaustive review of the different threats, which are mainly present in real-time networks communications, is necessary.

This work evidences a considerable gap between the electrical infrastructure to be implemented in power substations (protected from Cyber-security attacks) and the present situation of the Colombian electrical power systems, whose design was made in the past century mindless of any kind of cyber terrorism. Furthermore, equipment in power substations and communications systems that can be operated and monitored from an automated control center must be updated to fulfill international standards.

A progressive removal of old electrical connections, such as RS485 and RS232, from electric power substations is also recommended. The new approach must be to focus on a protocol-wise migration toward IP communications in order to reduce special efforts as well as promoting the adoption of Cyber-security implementation policies.

ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions and support of OPENLINK Sistemas De Redes De Datos, a company that has led the promotion and development of this study. This company has expressed a particular interest in strengthening and encouraging Cyber-security developments for the Colombian electric power sector.

REFERENCES

[1] C.W Ten, J.Hong, and C.C. Liu, "Anomaly Detection for Cybersecurity of the Substations", *IEEE Transactions on smart grid*, issue 99, August 25, 2011.

[2] A. Hahn, G. Manimaran, "An Evaluation of Cybersecurity Assessment Tools on a SCADA Environment." Proceedings of IEEE PES General Meeting, pp1-6. July, 2011

[3] D. Dolezilek and L. Hussey, "Requirements or recommendations?. Sorting out NERC,CIP,NIST, and DOE Cybersecurity," Proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[4] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, "Inside the slammer worm", *IEEE* Security & Privacy, 2003: 33-39.

[5] S.M, Cherry, "Internet slammed again (hacking), IEEE spectrum, Mar 2003, vol 40, p 59

[6] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon", *IEEE* Security & Privacy, 2011, vol 9,pp 49-51

[7] T. Sommestad, G.N. Ericsson, J. Nordlander, "SCADA system cyber security-A comparison of standards", Proceedings of IEEE Power and Energy Society General Meeting 2010, pp 1-8.

[8] H. Englert, H. Dawidczac, "IEC 61850 Substation to Control Center. Communication – Status and Practical. Experiences from Projects", PowerTech, 2009 IEEE Bucharest, June 28- July 2.

[9] S. Hans, J. Hof, M. Seewald, "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments", Fifth International Conference on Internet and Web Applications and Services (ICIW), 2010, 9-15 May, pp 135-142.

[10] L. Lei-Jun, P. Hong, "A defense model study based on IDs and Firewall linkage", International Conference of Information Science and Management Engineering (ISME), 2010 , 7-8 Aug, vol 2, pp 91 – 94.

[11] J. Lim, Consolidated Edison Co. of New York, Inc., New York, NY, USA "NERC CIP version 4 background", Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES, 20-23 March 2011