Journal of Power and Energy Engineering, 2015, 3, 16-22
Published Online April 2015 in SciRes. http://www.scirp.org/journal/jpee
http://dx.doi.org/10.4236/jpee.2015.34003

An Algorithm for Optimal Firewall Placement in IEC61850 Substations

Hermes Eslava[1], Luis Alejandro Rojas[1], Danny Pineda[2]

[1]Universidad Distrital, Bogotá, Colombia
[2]Openlink Sistemas De Redes De Datos S.A.S, Bogotá, Colombia
Email: hjeslavab@udistrital.edu.co

Received November 2014

Abstract

Recently, most electric power substations have adopted production control systems, such as SCADA systems, which communicate with field devices and remotely control processes from a computer screen. However, these systems together with protection measures and additional control actions (using protocol IEC61850) seem not to be enough to free substations of security attacks (e.g. virus, intruders, forgery or unauthorized data manipulation). This paper analyzes the main features of an electric power substation together with the aspects that might be significantly affected by cyber-attacks. The paper also presents the implementation of a specific security system (*i.e.* firewall-wise system) intended to protect a target distribution network.

Keywords

Firewall, Security, Substations, Electric Power, IEC61850

1. Introduction

Demographic expansion and industrial growth have boosted the demand for electric power. Additionally, this increased demand is further exacerbated by the use of new technologies and the complexity involved in the various solutions implemented within electric power systems. In most cases, companies have diverted their efforts to complying with standards in order to implement the corresponding better practices. However, the aforementioned demand added to the particular economic and social conditions of customers has forced companies to operate near critical-security levels, also under reduced generation rates [1].

2. Identification of the Needs

Various factors associated to both customers and electric power generation companies have contributed to an increase in complexity when attempting to control and operate electrical power systems. Thus, the need for using more-advanced computational tools at power control centers has emerged. The main purpose of an electric power distribution system is to deliver energy from the distribution substation to the corresponding users (*i.e.* end clients). In this context, a drawback might be associated to the fact that these systems are distributed over large geographic areas. Thus, in order to achieve a stable energy supply, the power system must be extremely

How to cite this paper: Eslava, H., Rojas, L.A. and Pineda, D. (2015) An Algorithm for Optimal Firewall Placement in IEC61850 Substations. *Journal of Power and Energy Engineering*, **3**, 16-22. http://dx.doi.org/10.4236/jpee.2015.34003

reliable. However, failure events and other operational disturbances are almost inevitable, which leads to subsequent electrical supply interruptions in particular areas. Whenever system failure occurs, such an event is alleviated through the joint actions of circuit-breakers and protection relays. During such situations, the operator's task at a control center is to interpret the associated cascade of protection measures so as to locate the potential failure point where failure actually occurred. Then the operator makes a decision that should lead to successfully restoring the system.

Nevertheless, there might be uncontrollable situations when the operator is unable to identify dangerous actions due to the type of interconnection between corporative informatics systems and industrial control systems. This implies that security failure associated to traditional operating systems (*i.e*. Windows, Linux, Unix, protocols TCP/IP, etc.) has a direct impact on the types of control systems that, until recently, operated in a centralized and isolated fashion (e.g. electrical power substations) [2].

Some centers incorporated control and instrumentation devices (e.g. SCADA). Despite exhibiting excellent performance in terms of security, such devices were not intended to support features like antivirus, intruder detection, authenticity, and access control. In 2010, an informatics worm, known as Stuxnet, was discovered. This worm was capable of reprogramming PLC (Programmable Logic Devices) equipment and also of hiding the changes applied. Stuxnet is proof that malicious software can cause physical damage to real operating elements (namely energy overloads, improper manipulation of robotic elements, damage to electrical-mechanical equipment, alterations or fake representations of digital signals, etc.). Other reports show evidence of cyber-attacks that have succeeded in changing official energy-consumption reports (figures of lower consumption) and have also manipulated the information of users at a massive scale in order to commit fraud and cause supply-service denial by companies.

3. Distribution Networks, Substations, SCADA and Standard IEC61850

To date, the operation of transmission and generation substations (linked to a distribution network) make it possible to transport energy to consumption areas so that it can be delivered to either industrial or residential clients. In such networks, three voltage levels can be identified and associated to three types of sub-network: delivery sub-network, mid-voltage sub-network and low-voltage sub-network. Such a distribution activity involves the following [3]:

Operation of the distribution network in order to ensure that electric power is delivered to clients through distribution networks with adequate quality standards and supply warranties.

Supplying electrical power to the users that are connected to their corresponding networks, always promoting a rational use of energy as well as ensuring pre-established quality of service.

Maintenance of equipment and facilities in order to provide continuous operational capacity.

Electrical balance measurements (*i.e*. each client's consumption). This is carried out with smart counters and tele-management devices. These processes are guaranteed to be modernized.

Planning and building new facilities for energy distribution in order to cope with newer energy demand.

Doping with all the information requirements demanded by the regulatory bodies and their associated institutions.

In addition to these activities, large electrical power distribution companies must pay close attention to and be aware of the social and commercial impact that results from providing electrical services that deliver adequate voltage values (always available and ready to use). Thus, as already mentioned, distribution networks will always be exposed to various risks that crystallize into occasional system failure.

Electrical energy substations allow flexibly driving the energy flow within a power system. This guarantees a level of security through the use of control and protection automatic devices. Such devices allow changing voltage levels, adjusting voltage regulation as well as activating/deactivating the connections of the system with various circuits [4]. The constituent parts of these systems include switches, protection devices, instrumentation transformers, section dividers, lightning rods, measurement systems, control systems, and also auxiliary services [5].

All substations require electrical energy supply for their own motors, lighting systems, and control systems control. Additionally, substations need other types of public utilities such as gas, water and compressed air, including the corresponding drainage systems. All these utilities co-exist within any substation [6], and their function is to provide energy to carry out various processes. Coexistence of such systems is acknowledged by the Federal Energy Regulatory Commission (FERC), which is a federal agency in the United States that has a juris-

diction over all electrical power borders among states; this is also acknowledged by the North American Electric Reliability Council (NERC). The latter organization refers to these utilities as the Interconnected Operations Services (IOS), since the term adequately refers to the natural essence and the costs implied in these utilities [7].

3.1. SCADA (Supervisory Control and Data Acquisition)

Within these auxiliary services, alternating current services serve low-voltage loads that are only associated to mid-voltage electrical equipment or installations. Additional direct current services also exist; these services consist of a charger, a bank of batteries, and distribution boards. This represents a safe energy source that relies on banks of energy or a batteries collection with their corresponding alternating-current charger, which is exclusively used to this end and remains always connected. The minimum voltage value that should be kept at the end of the battery discharge period must coincide with the tolerance range of the target equipment (*i.e*. its target load).

In order to keep track and control of these operations, it is necessary to include a 24/7 battery monitoring system, which will report the performance of the batteries on a permanent basis. The main purpose is to provide information that allows determining the current state of the batteries as well as the remaining capacity with the given load conditions. Additionally, the system makes use of automatic alarms intended to warn of possible battery-associated problems, either by using local or remote alarms. All this is currently applied by using adaptive algorithms that are specially developed to recognize unusual behavior that may occur in any of the cells before such behavior causes any noticeable damage in the system [8].

At this point, the use of tele-control remote terminal units (RTU) becomes essential. These units are basically data acquisition devices together with control devices on the field; their main purpose is to serve as an interface between local control-and-instrumentation equipment and the actual supervising/control data acquisition system [9]. Terminal units are capable of monitoring a number of input/output (I/O) signals that are related to process. These units also analyze and store data in real time as well as running user-programmable control algorithms. Furthermore, the units communicate with a master station and, in some cases, with other remote units. A particular RTU explores the process variables on a regular basis and, through a communication module, allows information exchange with a master terminal unit (MTU) that is located in a central control room. This latter process may use a range of communication media such as a telephone wire, UHF/VHF, micro-waves, satellite links, optical fiber and other media since the terminals have auxiliary ports that link them to other remote (sometimes mobile) terminal units. The communications protocol governs the structure of the messages as well as the corresponding error correction techniques, which are mostly proprietary. Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

The system in charge of supervision, control and data acquisition (*i.e*. SCADA) allows visualizing the variables sent by the RTU. It is based on a software application for production control, which communicates with the devices on the field and controls the process automatically from a computer screen. This system provides various users with information about the process, namely: operators, quality control supervisors, surveillance staff, maintenance staff, etc. [10].

Some of the most widely known applications (either associated or not with SCADA) include Aimax (by Design Instruments S.A.), CUBE (by Orsi España S.A.), FIX (by Intellution), Lookout (by National Instruments), Monitor Pro (by Schneider Electric), SCADA InTouch (by LOGITEK), SYSMAC SCS by Omron, Scatt Graph 5000 (by ABB), and WinCC (by Siemens).

Some of these systems implement protocols such as DNP3, ModBus, IEC60870-5-101, 103 and 104 or IEC61850. In this particular study, protocol IEC61850 was chosen since it allows protection and control functionalities within substations to be modeled in different logic nodes, and also grouped in various logic devices. This leads to important savings in terms of time when implementing the newer protection devices, since it requires no newer points to be assigned to the points of SCADA devices, which represents an advantage over other protocols like DNP.

3.2. Standard IEC61850

IEC61850 consists of the following detailed parts, which are further described in separate documents. IEC61850-5

provides general definitions of the models for equipment as well as the communication requirements. IEC 61850-7-4 and 7-3 provide specific definitions of the information models. EC61850-7-2 defines the services and functions for proper information exchange.

Within the standard, the fundamentals of the communications system are established (sections 5 and 7-1). These documents provide a functional description of the system by providing representations of the essential elements. Section 7-2 provides a more detailed definition of the communications system using the so called ACSI (Abstract Communication Service Interface). Such a description is given at an abstract level by using a comprehensive definition of the objects that constitute the communications system **Figure 1**.

Sections 7-3 and 7-4 provide further object definitions. Specifically, section 7-4 shows the development of nearly 100 models using more than 2000 attributes. Section 7-3 defines the most common attributes that appear in a large set of objects. Section 6 also fulfills very important complementary purposes by defining a configuration language. This new language, based on XML, allows extending the definitions of the objects provided by the standard, avoiding the inconveniences of a stiff model. The correspondence between the abstract communications interface and the specific communications protocols is displayed in sections 8 and 9. Specifically, section 8 provides the details of the substation's bus. Sections 9-1 and 9-2 provide a new correspondence, particularly for the process bus. Regarding the acquisition of real-time measurements, performed over analog signals so far, the standard proposes a shift towards digital signaling, using Ethernet and optical fiber as the underlying technology. In particular, section 9-1 puts forward an organization of communications through one-direction links, whereas section 9-2 suggests the classical bus-wise architecture.

3.3. Security Scheme

A firewall represents a traffic control and monitoring system within a network or between different networks. This system is initiated by capturing traces of traffic as they pass over the links. Then this traffic is compared with a set of control and access rules that have been previously established (Access Control Lists-ACLs). When the traffic fails to match the rules, the firewall rejects or disregards the incoming information.

The equipment must be of industrial type, it should be manageable and reliable to operate under harsh environmental conditions. It should also be highly resistant to electromagnetic interference and electrical currents. Ideally, this equipment should meet the following requirements:

1) *A wide range of industrial standards*

a) *IEEE*1613: Electric Utility Substations.

b) *IEC*61850-3: Electric Utility Substations.

c) *IEC*61800-3: Variable Speed Drive System.

d) *IEC*61800-6-2: Generic Industrial.

e) *NEMA TS*-2: Traffic Control Equipement.

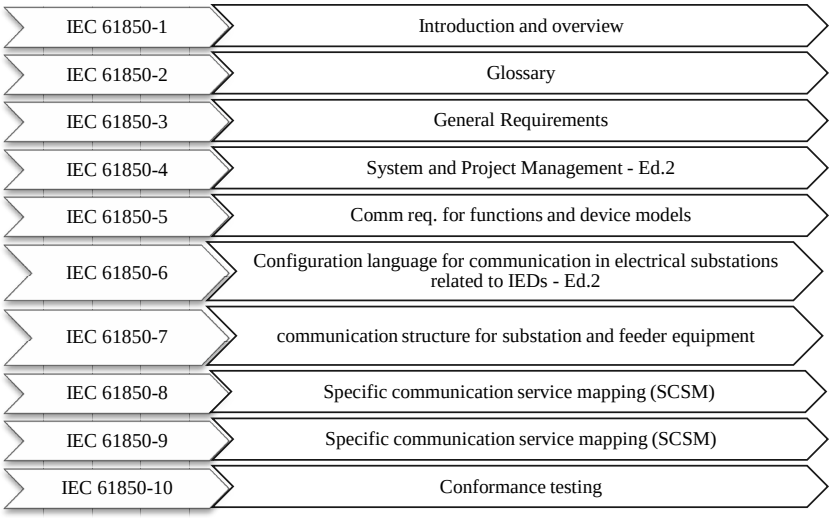

Figure 1. IEC61850 structure.

2) *Networking features*

a) *User authentication*: it should maintain password construction rules (password length, valid characters and validation time spans among other features).

b) *Access control*: it should provide various access levels based on user identity (read, read-and-write, run).

c) *IP spoofing*: it should protect the system against intruder attacks that intend to configure false IP addresses in order to acces the system's network.

d) *Prevention of Denial of Service* (*DoS*): qit should protect the system against denial of service resulting from packet rejection in situations where attacks can be recognized (exceeding the length of the buffer, the maximum firewall-disc capacity and the size of register files).

e) *Packet filtering*: it should retransmit or reject a packet based on the information contained in the packet's header and in its source/destination IP addresses.

f) *State inspection*: it should allow identification of the port numbers that are being used for the connections established by authorized users only; communication should be terminated when failing to identify the port numbers.

g) *Proxy servers*: it should include proxy applications that allow controlling Internet acces in order to meet performance and sequirity requirements (HTTP, TCP, Telnet, FTP).

h) *Network Address Translation* (*NAT*): it should protect the system from external access to the IP addresses that have been assigned within the local area network of the system.

i) *Notifications*: it should inform users of any attempt of itruders to enter the system, also storing relevant informtaion of such intrusion attempts.

Despite the basic security conditions presented above, some cases of vulnerability have been reported, particularly occurring during packet exchange. Traditionally, the main communication components in a firewall correspond to source IP, destination IP and the communication protocol. For instance, if only Internet traffic is to be allowed (*i.e*. http traffic) from a client to IP address 192.168.1.10 located in a web server whose IP address is 192.168.1.20, the corresponding ACL rule might look as follows: "*Allow Src* = 192.168.1.10 *Dst* = 192.168.1.20 *Port = HTTP*". If the three criteria are met, the ACL lets the message pass.

The problem arises when, despite establishing the rules, it is impossible to thoroughly inspect the conditions that validate the rule, that is, the firewall validates the message through the ACL and accepts it, but the message turns out to be a firmware update, which actually carries information about the Human Machine Interface-HMI (*as a fake component of the SCADA system*) intended to manipulate a particular PLC device. This may represent a serious security problem. In this context, it is necessary that the firewall supports a thorough inspection of the packets (referred to as Deep Packet Inspection-DPI).

4. Laboratory: Equipment and Recommendations

In order to optimize resources and allow the prototype Implementation to be as portable as possible, a low-level design was suggested. This design makes use of a single physical processor together with an operating system capable of hosting two virtual machines in order to simulate the type of traffic that flows between two entities of a SCADA system (HMI-PLC/RTU) and two additional virtual machines. The virtual machines must play the role of the SCADA firewall and that of the administration console table, respectively as it is shown in **Figure 2**.

Subsequently, a general check list for the security of SCADA networks must be verified since there is no current testing protocol for firewalls included in this type of devices as it is shown in **Table 1**:

With no commercial interest whatsoever and also considering the aforementioned definitions, it was concluded that one of the most complete and sophisticated pieces of equipment (in terms of security) corresponded to the Cisco ASA 5500 Series. This ASA series provides advanced Stateful Firewall and VPN concentrator functionality in one device, and for some models, an integrated Intrusion Prevention System (IPS) module or an integrated Content Security and Control (CSC) module. The ASA also includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPsec VPN, SSL VPN, clientless SSL VPN support, and many more features.

Firewalls protect inside networks from unauthorized access by users on an outside network. A firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such as a web or FTP

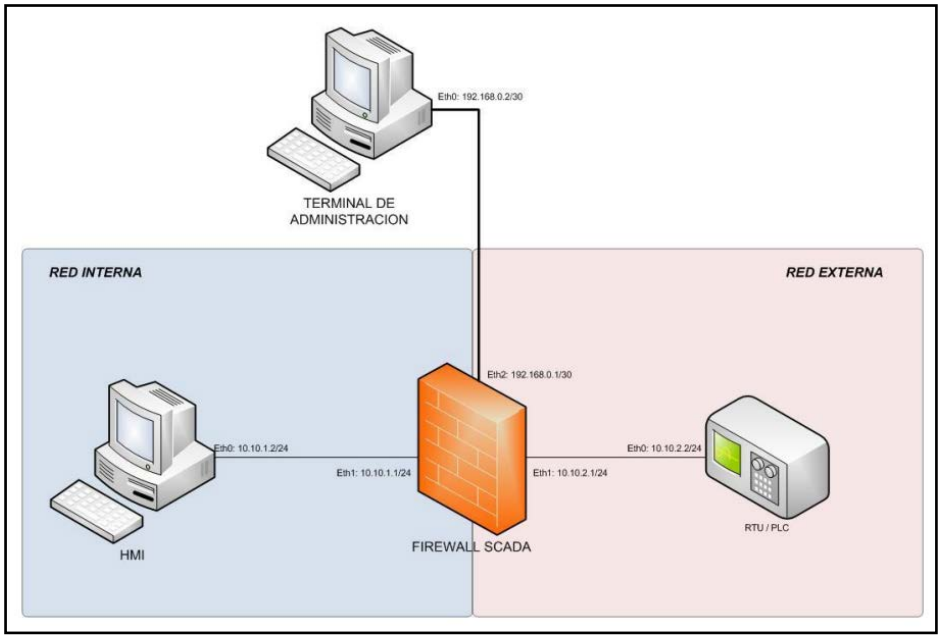

Figure 2. Sample of logical topology for the SCADA firewall prototype.

Table 1. Check list activities for the security of SCADA networks.

No	Activity	Status
1	Identify all connections to SCADA networks	
2	Disconnect unnecessary connections to the SCADA network	
3	Evaluate and strengthen the security of any remaining connections to the SCADA network	
4	Harden SCADA networks by removing or disabling unnecessary services	
5	Do not rely on proprietary protocols to protect your system	
6	Implement the security features provided by device and system vendors	
7	Establish strong controls over any medium that is used as a backdoor into the SCADA network	
8	Implement internal and external intrusion detection systems and establish a 24/7 incident monitoring	
9	Perform technical audits over SCADA devices and networks, and any other connected networks, to identify security concerns	
10	Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security	
11	Establish SCADA “Red Teams” to identify and evaluate possible attack scenarios	
12	Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users	
13	Document network architecture and identify systems that serve critical functions or contain sensitive information that requires additional levels of protection	
14	Establish a rigorous, ongoing risk management process	
15	Establish a network protection strategy based on the principle of defense-in-depth	
16	Clearly identify cyber security requirements	
17	Establish effective configuration management processes	
18	Conduct routine self-assessments	
19	Establish system backups and disaster recovery plans	
20	Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance	
21	Establish policies and conduct training to minimize the likelihood that staff will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls	

http://www.controlscada.com/scada-security-checklist-free-download

server, you can place these resources on a separate network behind the firewall, called a demilitarized zone (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks. You can also control when inside users access outside networks (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server. When discussing networks connected to a firewall, the outside network is in front of the firewall, the inside network is protected and behind the firewall, and a DMZ, while behind the firewall, allows limited access to outside users. Because the ASA lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

5. Conclusions

The adoption of a firewall-wise system in Colombian substations is recommended due to the new 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 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.

6. Acknowledgements

The authors would like to thank OPENLINK SISTEMAS DE REDES DE DATOS S. for the permanent support in the design, development and implementations of this study. Their experience in the electrical power sector allowed the successful ensemble of a multi-disciplinary team that will certainly lead to the formulation of novel future studies intended to favor the interests of all electrical supply companies and also of the general public in Colombia.

References

[1] Martínez, E.V. (2010) Academia de Ingenieria de México. http://academiadeingenieriademexico.mx/archivos/coloquios/9/Diagnostico%20de%20Ubicacion%20de%20Fallas%20en%20Sistemas%20Electricos%20de%20Potencia.pdf

[2] Endesa, G. (2013) Endesa-Electricidad-La red de Distribución. http://www.endesa.com/es/conoceendesa/lineasnegocio/Electricidad/Red_distribuci%C3%B3n

[3] Short, T.A. (2004) Electric Power Distribution Handbook. CRC Press.

[4] Lehtonen, M. (2010) Electric Power Quality and Supply Reliability Conference. In: *Fault Rates of Different Types of Medium Voltage Power Lines in Different Environments*, Kuressaare.

[5] Pabón, J.D., Zea, J., León, G., Hurtado, G., González, O.C. and Montealegre, J.E. (2001) La atmósfera, el tiempo y el clima. In: Leyva, P., Ed., *El medio ambiente en Colombia*, Bogotá IDEAM, 35-91.

[6] Castaño-Unimedios, L. (2013) Ciencia y tecnología: Colombia tendrá norma para predicción de rayos. http://www.unperiodico.unal.edu.co/dper/article/colombia-tendra-norma-para-prediccion-de-rayos.html

[7] Keraunos (2013) Keraunos-Innovación tecnológica en predicción de rayos. http://keraunos.co/

[8] Bechard, P. (2013) Localización de fallas eléctricas. PdMA Corporation. http://confiabilidad.net/articulos/localizacion-de-fallas-electricas/

[9] Rivas, A.A. (2012) Visiones de Telefónica-Innovaciones que muestran el valor de la tecnología. http://visionesdetelefonica.cl/paper/4/esp/index.html

[10] D. The United States Department of Energy, Grid 2030—A National Vision for Electricity's Second 100 Years, Washington, 2003.