Cybersecurity for Smart Substation

2020 IEEE PES Transmission & Distribution Conference and Exhibition - Latin America (T&D LA) | 978-1-7281-4155-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/TDLA47668.2020.9326174

Wagner Seizo Hokama
Smart Grid Dept.
CPFL
Campinas-SP, Brazil
whokama@cpfl.com.br

Juliane Soares de Souza
Electrical System Planning Dept.
CPFL
Campinas-SP, Brazil
julianesouza@cpfl.com.br

***Abstract* — We are currently undergoing an incredible digital transformation in our power distribution substations with the implementation of intelligent electronic devices (IEDs) in TCP / IP network in accordance with the standards established by IEC 61850 for substation protection and control. The use of information sharing and interoperability among IEDS are technical characteristics in smart substations. With the advent of this digital technology, which bring us a huge framework of opportunities for improvement in its operation and maintenance, we also have a weakness to be considered and studied that is cybersecurity, as already occurs in the corporate network of companies. The proposal of this project was to develop a diagnostics, studies, benchmarking analysis and the application of a cybersecurity action for distribution substations protection and control system.**

Keywords — Cybersecurity; IEC-61850; Smart Substation; Intrusion Detection System - IDS

I. Introduction

To improve the quality and reliability of Power Systems, the advancement of research on Smart Substation is going by the increase in resources related to information technology, communication and engineering. With the sophistication of distribution systems, both in terms of comprehensiveness, diversity and load growth, it is imperative to incorporate the concepts of smart grids particularly through the integration that the opportunities arising from this context provide [1]. Characteristic examples of these opportunities are network automation, intelligent meters and distributed generation. It is also necessary to take into account increasingly sensitive regulatory policies, which are beginning to paradigms of relationship between consumers and electric power concessionaires [2]. These opportunities give a significant effort to the incorporation of the technologies related especially by the complexity associated to the operation and the planning of the electrical networks, and the requirements of efficiency, safety and reduction of environmental impacts that must always permeate any innovation proposal in this sector [3]. The increase of distributed generation in medium and low voltage, the storage of energy, microgrids, response to demand, the immense amount of information that can be used for decision making, among others, represent some of the challenges related to the new paradigm of networks for the electricity distribution sector [4]. However, for all this to work in accordance with IEC 61850 Standard [5], it is necessary to digitalize the substation protection and control system.

The IEC 61850 apply Ethernet-based communication standard for substation communication and is has been widely used in the design of smart substation automation. This Standard specifies a series of protocols for the abstract data models, such as manufacturing message specification (MMS), generic object oriented substation event (GOOSE) and sampled measure values (SMV) [6].

The digitization leaves the system exposed to cyber-attacks that can be fatal to the power system. Cybersecurity of smart substation has been recognized as an emerging issue for the smart grid [7]. Since the smart substation employed a flexible and interoperable solution to the communication problems between devices, the excessive reliance on information and communication technologies make it be readily exposed to the malevolent cyber attackers [8].

Cybersecurity is about implementing measures to protect a computer or an automation system, such as a substation project with all its IEDs and other components even as protect ethernet communication network against unauthorized use or hacking attacks. These hackers are aimed at cyber-attack which is characterized by any internal or external method, intentional or unintentional, that may alter or damage the correct operation of the system [7].

Having defined the basic concepts, we took action to insert the cybersecurity issue into the development of the SMART SUBSTATION project, where we defined a new Full Digital Substation standard with the implementation of a process bus. This project included the standardization and implementation of cybersecurity in distribution substations at CPFL Group. The project aimed at threat mapping and risk mitigation with a focus on infrastructure, access and tracking management, and database management (Backup).

Among other actions, the idea was to implement the Hardening concept, widely used by the IT area in corporate networks, which aims to open only the ports / connections necessary for the process / system to function, leaving everything else closed / blocked.

II. Study Development

To address the cybersecurity of smart substations, looking for answers on how to put together an action plan to implement cybersecurity measures for CPFL Group substations, we searched for events held by solution providers, as well as research on international standards, manuals and systems equipment catalogs about the subject in question. At the start of this study, can mention some cybersecurity best practice for creating resilient control systems [10]:

- Know, limit, and monitor access to the control system.
- Implement the appropriate security for each level of the control system.
- Continuously monitor the control system at all levels (Baselines, alarms, logs).
- Have a continence plan.
- Patch, update, and maintain.
- Don´t forgot physical security.
- Learn from events.
- Be aware of your public information.

The studies started with the survey, events and benchmarking about what the market offers nowadays and how it can be implemented.

A. Participation in cybersecurity events

The first event we participated to research on the subject was Webinar on May 10, 2019 [9].

One of the items that drew a lot of attention in this Webinar was the information gathered from studies by insurer Allianz [11] that cyber incidents were the main reason for system shutdowns in Brazil in 2018, resulting in 43% of the incidents. Other relevant information about cyber threats was that Brazil had a loss of 32 million reais, growth of 197%, leaving our country among the 5 largest targets in the world, according to Norton's report on cyber security 2018 [12].

According to a holistic approach made by its authors, a graph was presented where about 38% of the causes are due to technology failure and physical protection used in industrial facilities. The other 62% is equally distributed between people and processes.

In this same event was discussed about some myths related to cyber security, as follows:

- “We are isolated from the Internet, so we are protected”.
- “Hackers do not know industrial protocols”.
- “Hackers are only looking for large companies”.
- “Our firewall fully protects us from intrusions”.

Certainly, these claims are myths, as they do not ensure the system protection against cyber attacks.

B. Benchmarking:

As part of the project order, we also benchmarked with other companies what they are doing in the cybersecurity division.

Utility 1 made a presentation at the event in Campinas on May 29 & 30, 2019, where we note the following topics:

Common Remarks:

- Factory default password equipment.
- Password sharing for systems and equipment.
- Managers sharing password with assistants.
- Lack of control with cleaning and maintenance personnel.
- Personal devices connected to corporate network.
- Administrator credential for workstation users.
- Third party access to sensitive information.
- The company assumes that the cloud provider protects the company.

Points to be considered:

- Legacy needs time and money to be replaced.
- Identifying internal threats is more difficult.
- Observe staff turnover.
- Implement security controls.

To ensure the proper functioning of cybersecurity it is essential sponsor culture change and discuss security at the strategic level. Some cybersecurity tips are identify the risks, have an incident response plan and the Security Officer can ensure stakeholder engagement. In the beginning, implement controls from the simplest.

C. Research of new technologies

In search of new technologies, for use in smart substations with a focus on improving our cybersecurity, we have researched some network equipment and solution for this purpose.

- Firewall:

Firewalls employ rules that permit, limit, or deny the transmission of packet-based communications and, in doing so, reduce the exposure of communications networks to external threats. Also, some firewalls that drop data packets often create an alarm or log file that notifies the user and/or administrator of the actions [14].

However, firewalls do not offer deep protection. There are many ways to bypass a firewall. Many substations employ remote access to retrieve fault records or to adapt settings in IEDs. These connections provide a route through which malware can enter devices in the substation.

Maintenance and test PCs provide another channel of infection. These PCs can be permanently installed or temporarily brought into the substation. These PCs are connected to the entire network or directly to individual protection or control devices. Files transferred to these PCs can also become attack vectors.

- Intrusion Detection Systems:

Intrusion Detection Systems (IDS) detect threats on the network, and there are several approaches in terms of technology and use. These approaches are based on BlackList, Learning, and IEC 61850 Standard.

The first two approaches are widely used today in corporate networks by IT teams around the world. However, in a well-controlled environment such as digital substations, the IEC 61850-based approach becomes the most appropriate.

For IEC 61850 substations, the entire automation system, with all of its IEDs, data models and communication parameters is described in a format known as Substation Configuration Language (SCL), defined in IEC 61850-6. This also includes the main assets and often even the substation single-line diagram. This information can be used to develop a new approach to detecting cyber attacks. One product available in the market is Omicron StationGuard, that creates a complete model of the automation system and the substation and then compares every single network packet with this live system model [13]. Fig. 1 shows the StationGuard that uses expert knowledge paired with information from the standard and the SCL files [13].

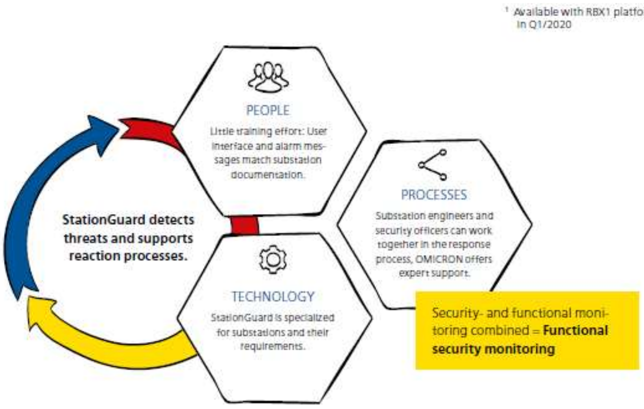
[1] Available with RBX1 platform in Q1/2020
PEOPLE
Little training effort: User interface and alarm messages match substation documentation.
PROCESSES
Substation engineers and security officers can work together in the response process, OMICRON offers expert support.
StationGuard detects threats and supports reaction processes.
TECHNOLOGY
StationGuard is specialized for substations and their requirements.
Security- and functional monitoring combined = Functional security monitoring

Figure 1. Station Guard Strategy for Cybersecurity Purpose

Even the signal values contained in the messages are evaluated using the system model. This process requires no learning phase and only uses the SCL description and some user input substations.

Station Guard is expected to launch early in the year 2020.

III. Recomendation

After surveying current market practices, we recommend that at MINIMUM the following cyber security conditions be implemented in smart substations:

A. Cybersecurity-related Event Log

Logs are a valuable tool for alerting and coordinating incident response as well as determining what happened after something goes wrong. After we deal with the immediate problem, it is critical to figure out how the problem occurred and prevent it from happening again. The same applies for a cyber attack. Properly configured logs will help us to discover how far into the network the attacker got, what they modified, and how they gained access in the first place [14].

IEDs should be able to indicate cybersecurity related events. These events must be stored internally in the event list and can be sent to the HMI (Human Machine Interfaces) system through the IEC-61850 protocol. Some examples of signals that can be monitored (they will be detailed later in the system points list):

- Successful User Login
- Successful user logoff
- Password change or removal
- Equipment firmware change
- Relay configuration / setting change
- Date and / or time change
- Wrong user login / password failed

B. Digital Signature Firmware

The IED must have digitally signed firmware. This means that only firmware developed by the IED manufacturer can be loaded on the device. Thus, software developed by hackers cannot be downloaded to the device.

C. Production Hardening:

A recommended aplication against internal attack is hardening devices in substations. Hardening devices mean that all unused ports, protocols or services in a device must be disabled. For each equipment in the architecture must be propose some actions to be taken. Switches: The first action is to disable the default admin account and create new account with complex password. The second action 2 is to disable unused ports for communication. The third action is to enable secure protocol and disable unsecure protocols such as HTTP, FTP and Telnet. Besides, is suggest to associate ports with media access control (MAC) address for all devices in the substation automation system (SAS). In this case, If the intruder tries to connect a device into a port that is assigned to MAC address the port will be disabled preventing access to the network [15].

IEDs should only be implemented with the desired functionality for the project. Soon, communication protocols not necessary for the project will be disabled. This means that the "virtual IED display surface" is limited against hacking attempts.

Industrial PCs (PAS and SCC) will have their USB ports disabled (except the dongle port) and CD / DVD drive limiting the PC access surface. Switch ports that are not active will also be disabled to prevent improper access to the network. Fig.2 present the propose of system hardening.

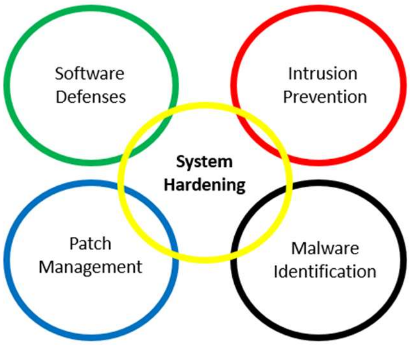

Figure 2 - Hardening Concept.

D. Crypto-CHIP:

The IED must have an internal chip to ensure encryption of sensitive information such as passwords, configuration data, etc.

E. Patch Management:

The IED provider must continually monitor cyber threats that may impact their products. As a result, it should periodically report vulnerabilities found and the firmware version that should be downloaded by the user to IED to mitigate risks.

IV. Pratical Application

Smart substation faces variety of cyber security threats, as shown in Fig. 3 [8].

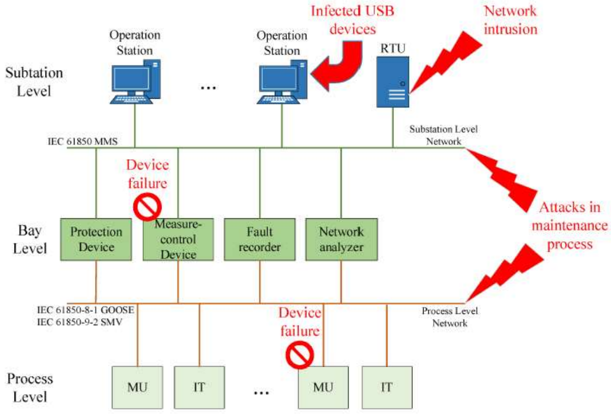

Figure 3. Cyber Security Threats in Smart Substation [8].

Here are some points we would like to highlight about these threats:

- Network intrusion: if remote control is supported by Ethernet based communication, smart substation can be intruded through the networks. Supervisory control and data acquisition (SCADA) systems and Remote Terminal Unit (RTU) are usually being the target [8].
- Malware in physical media: malicious programs generally hide in the physical media like USB devices and Compact Discs. Operation station in smart substations often become the entry for these malwares [8].
- Attacks in maintenance process: devices in smart substation need to be maintained periodically, which offers an opportunity to break the defense based on the network and the protection supported by section isolation. Once the engineer's laptop or computer which connect the target device directly has been infected by malwares or controlled by cyber attackers, maintenance process will facilitate the cyber-attacks [8].
- Security management irregularities: irregularities is also one of the major hurdle. Experience has shown that cyber security in substation is often compromised due to the fact that most of security utilities are not used and managed easily. Engineers who are responsible for the operation of automation systems are typically not security experts and they will likely find workarounds if security presents too much of a challenge. Examples are default passwords that are not changed or firewalls that are not configured correctly and not properly maintained. Most of the cyber security threats originate from the exploitation of vulnerabilities in devices or managements. Vulnerabilities in devices may lead to system exceptions in certain scenario. Negligence of substation staff members can open an illegal entrance to the backend system of a device. Cyber attacker who exploits these vulnerabilities may possibly lead to device failure, which finally results in safety incidents [8].

The cybersecurity recommendations showed in III were applied to the digitization project developed at the São Carlos 4 - Bethania Substation. To project the smart substation in Bethania was hired the Siemens Solution. The Bethânia Substation is composed of two 138 kV transmission line, a 26.6 MVA transformer with voltage level 138 / 11,9 kV and a 11,9 kV bus with 5 feeders, typical arrangement of a CPFL distribution substation. The Fig.4 depicts the single-line diagram of Bethania Substation.

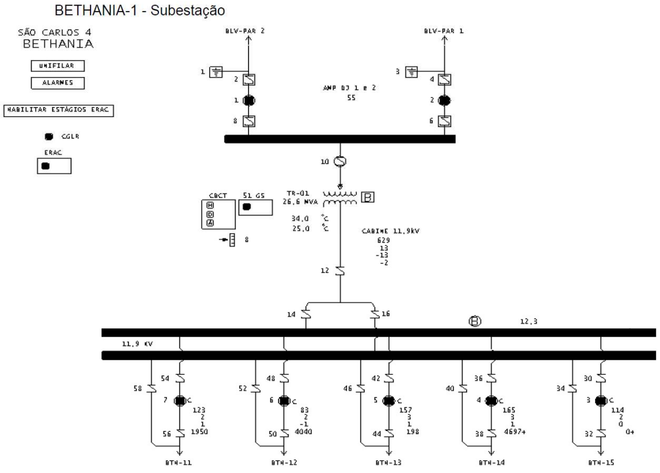

Figure 4 – Single – line diagram of São Carlos 4 – Bethânia Substation.

In this substation, a redundant solution was assembled where the yard equipment (merging units and IOBOX) receive analog signals from the CTs (current transformers) and PTs (Potential transformers) of the lines, and from the high and low voltage sides of the transformers. In addition to analog signals, all digital field signals are also acquired and sent to the control room, these digital signals are sent via GOOSE while analog signals are sent via Sample Values, always supported by the use of IEC61850. Similarly, the digital signals of the protective relays are sent to the field equipment via GOOSE to actuate the yard equipment such as tripping, reclosing, opening and closing commands etc.

In this solution, the protection actuation and the control of the lines and transformers use only the process bus system. The feeders are not using Process bus because the relays are on the same panel as the PTs and CTs. However all communication of the feeder relays use the IEC61850 standard with GOOSE exchange between them. It was adopted the use of a feeder from each manufacturer, in order to test the GOOSE exchange between equipment from different manufacturers aiming at the consolidation of interoperability as described in the IEC61850 standard.

In the implemented architecture, we can check how the communication between all substation equipment. Three panels are used, where two of them were in the yard substation and one of them in the protection and control room. A panel with 2 merging units and an IOBOX was fielded on the high side of the transformer, another with the same configurations was placed on the low side of the transformer, and the panel with protective relays was placed in the protection and control room.

The communication networks are divided into two, one being the Station Bus and the other the process bus. The Station Bus was responsible for communicating between the protective relays, the IONBOX and the supervision system. In this network the equipment can exchange GOOSE with each other and send data to the supervisory system. The network redundancy protocol known as RSTP was used. This protocol allows the network to automatically recompose itself in the event of a failure within a few miles. Similarly, the feeders also exchanged data between relays and supervisory system using the station bus.

In the station bus network were included 2 switches where these allow network access by peripheral equipment. In these switches are also connected the GPS responsible for system time synchronization and the machines where the Elipse supervisory system and Sicam control system are installed, which can be accessed remotely via CPFL System Operation Center (SOC) to execute the substation commands and to send all supervisory information to the remote center.

The process bus is responsible for communication between the line protection relays, the transformer and the merging units that were acquiring the analog and digital signals in the field. Merging units acquire the currents and voltages of the CTs and PTs respectively and send them to protection relays using Sample Values. Sample Values are analog signals digitized by merging units transformed into data packets that are standardized by the IEC61850-2 standard. This communication is unidirectional. Digital signals are exchanged between merging units and protection relays using GOOSE also defined by the IEC61850 standard. These digital signals are mainly command signals and tripping of the relays to the circuit breaker.

The network redundancy protocol used in the process bus was HSR, this protocol allows the network to automatically recompose itself in the event of failure without recomposition time. A RED box was included in this network, equipment that allows access to the HSR network by equipment that does not have this technology.

It is noteworthy that in this type of configuration, where the entire protection and control system depends entirely on the TCP / IP communication network, it is essential to have a very secure network, that is, cybersecurity is mandatory.

V. Conclusion

We can conclude that digital transformation in our power distribution substations with the implementation of intelligent electronic devices in TCP / IP network in accordance with the standards established by IEC 61850 for substation protection and control will bring us new challenges in the area of cybersecurity.

In this sense, we must guide ourselves by making use of appropriate standards to address this requirement in supervisory and control systems, which is here found to be the most appropriate international standard IEC-62443 - The safety standard for industrial control systems in the field of operational technologies (OT).

Regarding its implementation, we note that the access settings must be configured following the application "White List" or "Deny by Default", i.e. close everything and release only what is really needed. When using systemic applications, such as digital substations, we cannot accept device certifications only, but systemic certifications.

Regarding its maintenance, we note that cybersecurity must be treated as a process, not a project, to be effective in its smooth operation and sustainability over time. The responsibility for cybersecurity should lie with everyone involved in the process, not just the company's IT / TO area. Users are as responsible as system security.

In Brazil, there is a tendency to discuss cybersecurity measures and contributions to the creation of procedure that set the cybersecurity controls adopted by the operating agents connected to the supervision network and by the National Electric System Operator (ONS) in their operational environments. The Brazilian Electricity Regulatory Agency (ANEEL), has included on the 2020-2021 regulatory schedule the discussion for establishment of minimum cybersecurity requirements in Procedures of ONS. The public consultation in ANEEL is scheduled for 2021 [17].

REFERENCES

[1] EPRI - Eletric Power Research Institute, Mossé, A., Diretor Executivo da EPRI América Latina, Redes inteligentes: desafios e Realidades. Smart Grid Forum, São Paulo, 2009.

[2] ANEEL, Apresentação da ANEEL, Redes Inteligentes e Eficiência Energética Perspectiva do Regulador, III Exposição e Simpósio em Eletricidade e Tecnologias, 2011.

[3] Empresa de Pesquisa Energética, Balanço Energético Nacional, 2011

[4] Xue-song, Z., Li-qiang, C., & You-jie, M., Research on Smart Grid Tecnology. Computer Application and System Modeling (ICCASM), 2010 International Conference , 3 pp.V3-599-V3-603, 22-24, 2010.

[5] IEC 61850-3, COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –PART 3: GENERAL REQUIREMENTS.

[6] Communication Networks and Systems in Substations, IEC Std. 61850.

[7] C. W. Ten, H, 1 Hong, and C. C. Liu, "Anomaly detection for eyberseeurity of the substations," IEEE Trans. Smart Grid, 2(4), pp.865-873,2011.

[8] Chai Jiwen and Liu Shanmei, "Cyber security vulnerability assessment for Smart substations," *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Xi'an, 2016, pp. 1368-1373.

[9] WEBINAR ELIPSE E MOXA, held on 10 May 2019 <https://kb.elipse.com.br/webinar-aplicacao-da-norma-de-ciber-seguranca-iec-62443-em-sistemas-de-supervisao-e-controle/> [accessed august, 2019].

[10] J. Smith, J. Pereyda and D. Gammel, "Cybersecurity best practices for creating resilient control systems," *2016 Resilience Week (RWS)*, Chicago, IL, 2016, pp. 62-66.

[11] RELATÓRIO SOBRE RISCOS DA ALLIANZ, 2019 <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2019.html > [accessed august, 2019].

[12] RELATÓRIO SOBRE RISCOS DA NORTON, 2018 <https://us.norton.com/cyber-security-insights-2018> [accessed august, 2019].

[13] STATIONGUARD, FUNCTIONAL SECURITY MONITORING FOR SUBSTATIONS, OMICRON USER MANUAL, april, 2019.

[14] D.Whitehead, K. Owens, D. Gammel, J.Smith, “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies Sensible Cybersecurity for Power Systems”, Schweitzer Engineering Laboratories, Inc: A Collection of Technical Papers Representing Modern Solutions, 2018.

[15] Mohamed Nouh, Dazahra & Faissal, Elmariami & Aziz, Belfqih & Boukherouaa, Jamal. (2018). A Defense-in-depth Cybersecurity for Smart Substations. International Journal of Electrical and Computer Engineering (IJECE). 8. 4423.

[16] BETHÂNIA SUBSTATION WORKSTATEMENT AT CPFL, HELD ON 4 APRIL 2018 – SIEMENS SOLUTION BRAZIL.

[17] REGULATORY AGENDA 2020-2021, National Agency of Electrical Energy <https://www.aneel.gov.br/agenda-regulatoria-aneel> [accessed february, 2020].