International Journal of Electrical and Computer Engineering (IJECE)
Vol.8, No.6, December 2018, pp. 4423~4431
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp4423-4431

A Defense-in-depth Cybersecurity for Smart Substations

M. N. Dazahra, F. Elmariami, A. Belfqih, J. Boukherouaa
Department of Electrical Networks and Static Converters, National superior School of Electricity and Mechanics, Morocco

Article Info

Article history:

Received Mar 27, 2018
Revised May 27, 2018
Accepted Jun 10, 2018

Keyword:

Cybersecurity
Defense in depth
IEC61850
Smart substation
Substation automation

ABSTRACT

The increase of cyber-attacks on industrial and power systems in the recent years make the cybersecurity of supervisory control and data acquisition and substation automation systemsa high important engineering issue. This paper proposes a defense in depth cybersecurity solution for smart substations in different layers of the substation automation system. In fact, it presents possible vulnerabilities in the substation automation system and propose a multiple layer solution based on best practice in cyber security such as the hardening ofdevices, whitelisting, network configuration, network segmentation, role-based account management and cyber security management and deployement.

Corresponding Author:

Dazahra Mohamed Nouh,
Department of Electrical Networks and Static Converters,
National superior School of Electricity and Mechanics,
Road El Jadida, Km 7, BP: 8118, Oasis–Casablanca, Morocco.
Email: m.n.dazahra@gmail.com

1. INTRODUCTION

The power grid is a national critical infrastructure that plays an important pillar for the development of a nation, when electricity stops everything stop. The growth of power grid and the use of communication technologies make it vulnerable to cyber-attacks, terrorist attacks, vandalism and other threats. According to National Institute of Standards and Technology NIST the threats of cyber-attacks on Supervisory control and data acquisition SCADA has increased four times in the last years.

The first attack on a power grid was the attack on a Ukrainian utility (Ivano-Frankivsk) SCADA in December 2015. First, the hacker got access to the SCADA and started disabling the power backup system. Then, he blocked the customer call centres. Finally, he started opening circuit breakers and deleting user's accounts which prevent the operators from closing the circuit breakers to restore normal state. the damages of these attack were a disconnection of 30 substations which impacted 225 000 customers for 3 hours [1]. The impact of this attack shows the necessity of taking actions to secure the power grid against cyber-attacks.

Substations are the hearth of the power grid, and the security of the power grid needs to be done first at the substations level. As new modern substations or smart substations are based on IEC61850 standards and Ethernet communication; also, they are connected to SCADA and corporate network, which make them more vulnerable to cyber-attacks [2]. Recently, the cyber security in substations has received more and more attention [3]-[4].

There have been many researches and actions on the cybersecurity of substations. In fact, the Technical Committee Number 57 TC57 of the International Electrotechnical Commission IEC has already developed several standards to solve security problems in the automation system IEC 62351 standards for Power systems management and associated information exchange-data and communications security [5]-[6]. The IEC 62443 standard defines security for industrial control systems of the power systems. These standards give a guideline on how to apply cybersecurity in operation and maintenance [7].

More researches have been done on the cybersecurity of the substations. In [8]-[10] authors presented solutions for intrusion detection based on IEC61850 protocol. In [8]-[11] some cybersecurity test-bed where presented to test and detect vulnerabilities in the Substation Automation System SAS based on fuzzy test. Some researches presented physical security using unidirectional gateways [12], while others were interested in adding encryption to protocol [13].

However, these works stay insufficient for cybersecurity of SAS because it will be too late to detect an intrusion if it is not stopped at first place because until the zero day attack the hacker can cause severe damages on the substation. Moreover, the standards have not been implemented by manufactures because they are focusing on operation more than security, for example the application of the encryption proposed in standards IEC62351-5 caused a time delay to the packets which is not accepted in the operation of SAS. The proposed solutions in literature for cybersecurity in substation are in most time not practical or complex to be implemented in the SAS. Most researches focused on external attacks but not much on how to prevent from internal attacks. In reality, there is more requirements of in-depth investigation, analysis and practical solution for cybersecurity. To this end, this paper proposes a realistic defense in depth solution for cybersecurity in smart substations based on best practices in cybersecurity in order to prevent internal and external treats of cyber-attacks at different levels of the SAS.

The remainder of this paper is organized as follow. Section 2 presents the architecture of smart substations with the IEC61850 protocol. Section 3 gives an overview of the cyber vulnerabilities in substation automation systems and their impact on substation operation. Based on the vulnerabilities presented in section 2, section 4 presents a framework of cybersecurity for substation. Finally, section 5 concludes this paper and suggests future research work.

2. SUBSTATION AUTOMATION SYSTEM ARCHITECTURE

The substation automation system in smart substation uses a three-layer architecture formed of substation level, bay level and process level. The substation level contains Human Machine Interfaces that displays the status of IEDs, bay controller and other devices, it allows operators to control the primary equipment such as circuit breakers and disconnectors. The substation level contains also engineering workstation that allows configuration and settings of all devices in the substation. The substation is monitored remotely by control centre connected via a gateway, and the communication is ensured according to some protocols such as IEC 60870-5-104, IEC 60870-5-101, DNP3 or the new protocol IEC61850-90-2 [14]-[15].

The bay level comprises Intelligent Electronic Devices IED such as numeric protective relays, bay controllers and network analyser. The process level contains margin unit that sends periodical sampled value of three phases current and voltage using the Sampled Measure Values SMV; also, the process comprises intelligent circuit breaker that controlled by Generic Object-Oriented Substation Event GOOSE [16]-[17]. The interfaces between these three levels are two networks.

The substation network connects equipments in substation level with devices in bay level. In the substation network the Manufacturing Message Specification MMS is adopted for the client/server communication, the Precision Time Protocol PTP defined in IEEE 1588 is used for high precision time synchronisation for the SAS [18], other protocols such as Simple Network Management Protocol SNPM is used for Management of SAS network, File Transfer Protocol FTP is used to transfer setting to IEDs and The Hypertext Transfer Protocol is used to get access to embedded web server in some IEDs. The process network connects the bay level and the process level, while GOOSE and SMV are adopted for real time high speed communication. Figure 1 presents the architecture of a smart substation.

3. SUBSTATION AUTOMATION SYSTEMVULNERABILITIES

The substation is exposed to wide range of cyber threats, these threats can be external threats such as terrorist, spying or hackers; also, they can be internal threats intended by disgruntled employees or inadvertently threats caused in maintenance phases. Figure 2 depict the several points from where an intruder can get access to the SAS.

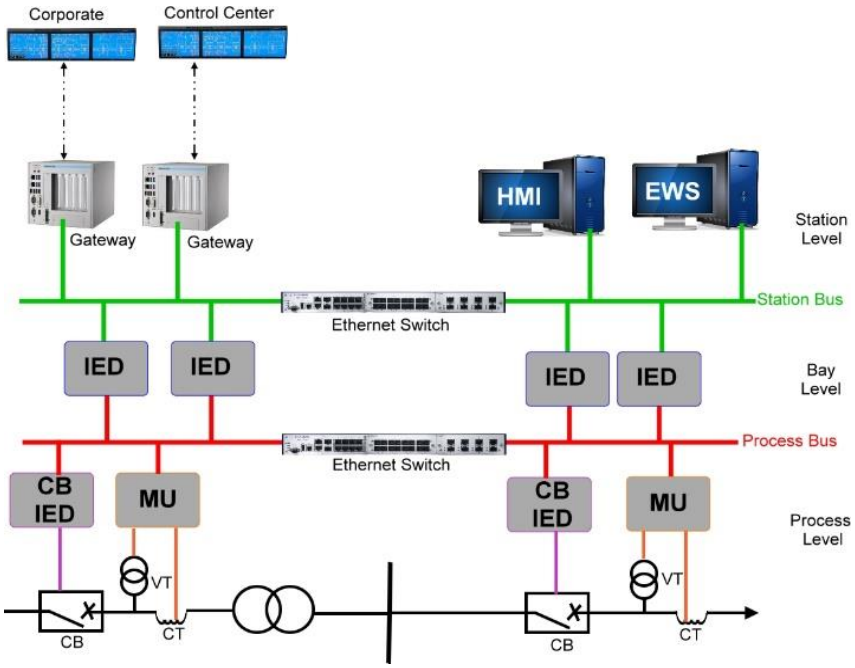

Figure 1. Smart substation architecture

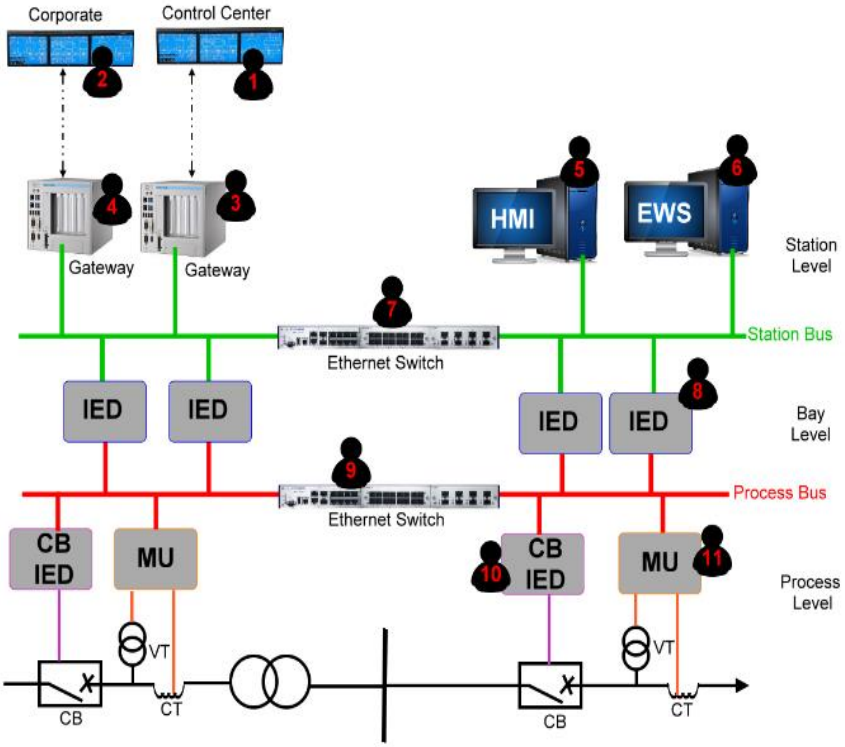

Figure 2. Vulnerable points in a smart substation

The signification and the impact of the intruder in each point from Figure 2 is described below.

a. Point 1: Control centre

If the intruder get access to the control centre, he can send control orders to the substation's primary equipments, which will cause a disturbance or a blackout to the power system.

b. Point 2: Corporate Network

If the intruder get access to the enterprise corporate network, he can get data that are confidential from the substation such as real energy consumption.

c. Point 3: Gateway for communication with control centre

The intruder can do an attack in two ways. First, a malware in USB key because gateways often use an embedded operating system which will make it easily implemented. The malware can send false data to control centre and control orders to the primary equipments. Second, the intruder can pretend to be the gateway by using a simulator of legacy protocol such as IEC60870-5-101, IEC60870-5-104 or DNP3 and send false measurements and data to the control centre, which can affect applications installed in control centre that use these data such as energy management system or distribution management system. Also, the intruders can interrupt control orders from control centre and send false feedback, which can disturb the power system for example in the case of isolating a heavy load.

d. Point 4: Gateway for communication with enterprise

The same case at point 3, the intruder can pretend to be this gateway and send false measurements which will affect reports used by the enterprise or infect the gateway by USB key malware.

e. Point 5: Human Machine Interface

The HMI is one of the crucial point to be protected in a substation because it contains interfaces to control the primary equipment and have many vulnerabilities. In fact, the intruder can do several attacks in the HMI, for instance, he can crack the password of the user's accounts and starts executing control orders to shut down the substation; also, he can use a fake IEC61850 client and send controls to different IEC61850 servers. Besides, he can delete archives and user's accounts or inject a malware via a USB key.

f. Point 6: Engineering Work station

The EWS is often used to change the setting and parameters of protective relays, bay controller and gateways. If the intruder get access to the EWS, he can send false setting to relays which will cause trips or can change communication parameters for the communication with control centre which will lead to communication interruption. Also, he can change the Substation Configuration Language of IEDs which will disturb the whole SAS.

g. Point 7: station bus

If the intruders get access to the station bus switches he can use an IEC61850 simulator in order to interrupt, tamper, pretend and replay the MMS, SNMP or PTP ethernet packets which can lead to trips, Denial of service DoS by packet storm or erroneous synchronisation for the entire system.

h. Point 8: IED

The intruder can get access to the IED directly from the communication front port, available in the totality of IEDs, by using unsecure communication protocol such as telnet.

The intruder can change the setting, parameters or update faulty firmware to the IED which will cause an equipment failure or trips of circuit breakers.

i. Point 9: Process bus

If the intruders get access to the process bus switches he can interrupt, tamper, pretend and replay the GOOSES and SV messages which can lead to trips, DoS.

j. Point 10: IED CB

As the control of IED CB is connected to the process bus by Ethernet, the intruder can pretend to be the IED of a circuit breaker and send false position which will cause problems to the operation of the substation and the power system.

k. Point 11: Mergin Unit

The intruder can pretend to be the MU and send false measurements of current and voltage to protective relays which will cause trips.

In addition to these points, there still other inadvertently threats than can affect the security of the substations such as equipment failure, disconnection of equipment's, loss of servers or misconfiguration of IED which must be taken in consideration of cybersecurity of substation.

4. DEFENSE IN DEPTH SOLUTION

Defense in depth is a concept inspired from the military where an enemy cannot defeat effortlessly a compound and multi-layered defines system than to puncture a single fence. The same Principle is applied in the domain of information systems by the use of multiple security countermeasures to protect the integrity of the information network.

Defense in depth reduce the probability that an intruder can succeed to penetrate the system. Defense in depth can also help to identify intruders who attempt to the system. If an intruder gains access to a system, defense in depth reduce the harmful impact and gives administrators and engineers time to update

countermeasures and prevent future attacks. In this paper, we propose a defense in depth solution for the cybersecurity of substation automation system in smart substation. Figure 3 depict the proposed defense in depth solution. The different layers of this defense in depth are explained in Figure 3.

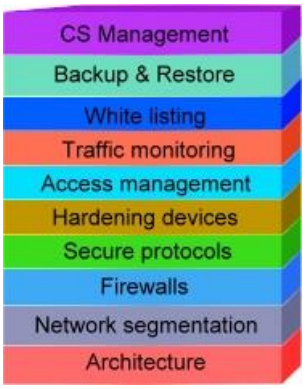

Figure 3. Defense in depth solution

4.1. Architecture

The loss of a GOOSE or SV in the case of communication cable failure can lead to disastrous damages to the substation. As a mitigation to this problem, we encourage the use of redundancy architecture for the SAS. For the process bus, it is recommended to use High availability seamless redundancy (HSR) protocol and for the substation network, it is recommended to use the Parallel Redundancy Protocol (PRP) as described in IEC 62439-3 standards [19]. These two seamless protocols offer more security to the SAS as any loss of GOOSE or SV packets can be recovered in 0ms.

Security of protective relays can be enhanced using local backup protection as presented in [20] which offer a backup of protective relay in case of their failure or a trip failure. Also, we encourage to use PTP for synchronisation as it offers a better synchronisation accuracy of 1us comparing to IRIG which offers a synchronisation accuracy of 1ms.

4.2. Network Segmentation

We propose to segments the network of substation to three zones separated by firewalls as it will offer more security because if an intruder compromise the perimeter zone he must compromise the other zones behind it to get control of physical equipment. These zones are presented in Figure 4.

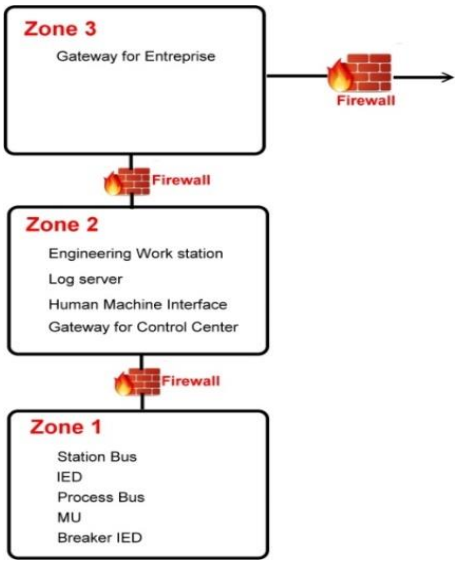

Figure 4. Network segmentation in smart substation

Zone 3: Is a Demilitarized Zone which contains the gateway for communication with enterprise network, and it should be via a Virtual Private Network.
Zone 2: Contains the EWS, Log servers, HMI and gateway for communication with the control centre.
Zone 1: Contains the station bus and the process bus with MU, IED and Circuit breaker.

4.3. Firewalls

Firewall must be configured to authorise only needed services or protocols for communication between the three segmented zones. These will hide the network structure and devices from outside view.

4.4. Secure Protocols

All unsecure protocol or clear text protocols must be disabled because data such as username and password are transferred without encryption and a simple sniffing can get them. we encourage to use only the secure version for example. For the network management the use of Simple Network Management Protocol V3 SNMPv3 instead of SNMPv1 or v2. For file transfer the use of Secure File Transfer Protocol SFTP instead of FTP. For web server the use of the secure Hypertext Transfer Protocol HTTPS instead of HTTP. For device configuration the use of SSH Secure Shell instead of Telnet.

4.5. Hardening Devices

One of best solution 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 we 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, we suggest to associate ports with media access control (MAC) address for all devices in the 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.

Computers: Gateways and HMI are industrial computers that are running on windows operating system. The first action is to be sure that the operating system is installed from trusted and certified CD because engineers often install windows form materials downloaded from the internet, so these materials could be infected or have some vulnerabilities. The second action is to install the latest updates from the operating system provider that correct all vulnerabilities detected in previous version. The third Action is to disable all USB port as malwares and virus can be injected via USB key drivers. Action 4 is to disable all unused services, application or ports in the computer. IED: for the bay controllers or numeric protective relays we suggest to delete default user and password and use more complex password.

4.6. Access Control Management

Another solution for protection against internal treats can be done by using access control management. For this aim we suggest to apply the recommendation of part 8 form IEC62351, which is Role-based access control. For every device in the substation the RBAC should be deployed, so for every user in the substation access should be grunted only for object concerning this user operation. for example, some operator will have access only to open or close primary equipment but will not have access to change setting of relay settings. The RBAC allows to divide access by areas of expertise which prevent from unintentional operation fault and from disgruntled employees. For computers based on windows operating system, we suggest to use a domain controller to secure authentication requests.

4.7. Monitor Traffic

The Monitoring of logging activities and unsuccessful login attempts can give an idea about the way user are operating the SAS. For this aim, we suggest to deploy logs system manager which will collect logs from all devices using Syslog protocol following standard RFC3164 and RFC 5424. This will give the possibility to create historical audit trails of individual user account access activity.

4.8. White-listing

In addition to the antivirus that should be installed on computer we suggest to add a white listing program, this will allow only trusted applications and services declared in the list to be executed, which will Blocks any malicious software, even if it is unknown.

4.9. Backup & Restore

One way to enhance the SAS security from equipment's failure is to have a backup and restore policy. The backup and restore of computers will be automatic using dedicated software. In the case IED

setting are stored in their internal memory, so the backup will be manually by taking a copy of the last known validated settings. In the case of an equipment failure, for example, a computer or a IED damaged due to an overvoltage in the auxiliary power supply, the maintenance team can change the equipment and inject to backup setting which will offer them better time in comparison to the case if they don't have a backup and should configure it from zero.

4.10. Cybersecurity Management

Cyber security is an ongoing process that encompasses procedures, policies, software, and hardware. We suggest to implement a plan for managing incidence response in case of any external or internal vulnerability reported from the vendor on any device in the SAS. Figure 5 presents the propose plan.

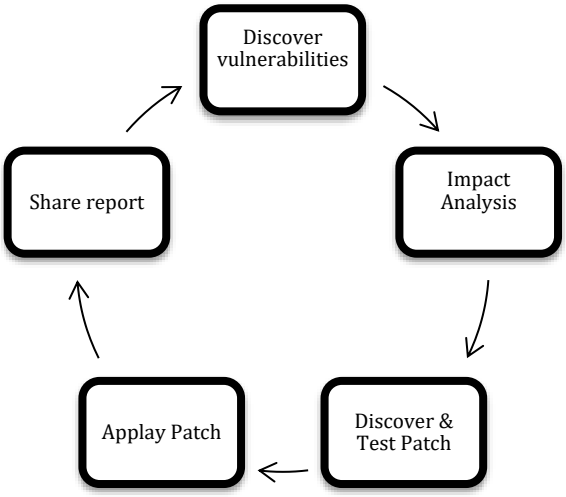

Figure 5. Cybersecurity management plan

First, if a detection of a vulnerability occurs, an impact analysis on the SAS should be carry out. Then, a Patch to fix the vulnerability should be found and tested before being applied to the SAS. Finally, a report about the vulnerability should be shared with other vendors. Cybersecurity procedures and policies should have applied in early phase of SAS project following the cyber security life cycle presented in Figure 6.

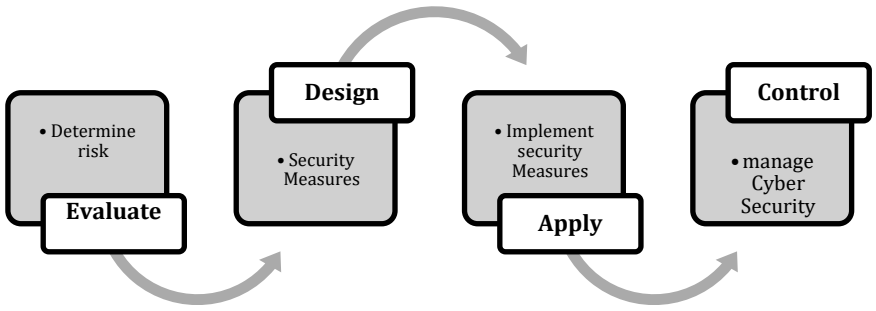

Figure 6. Cybersecurity life cycle

The first step is to determine baseline risk and security levels. The second step is to design the system using the appropriate security measurements as we recommended. The third step is to implement the security measurements and procedures with the purpose to obtain the minimal impact on the operation of substation. Finally, the cybersecurity should be managed by an incidence response plan.

5. CONCLUSION

Although the fact that the defense in depth comes into sight to be a complex and fatiguing solution to implement in substation automation systems, it is mandatory to apply it on power grids because the cyber-attacks become dangerous to substations; also, the multiple layers of security is an efficient way to prevent from external attacks and especially from internal treats that are hard to be detected or prevented as the major element in internal treats are human whether attacks are intended or unintentional wrong operations.

In this paper, first, we present the smart substation architecture based on the IEC61850 protocol. Second, we present different vulnerable point in the substation automation system of a smart substation. Finally, we present the defense in depth solution. In the future, the development of intelligent cryptographic algorithms will make the application of IEC62351 standards easier and will give more security to substation automation systems.

REFERENCES

[1] "Analysis of the Cyber Attack on the Ukrainian Power Grid", Defense Use Case , March 18, 2016.
[2] Hyunguk Yoo, Taeshik Shon, Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture, In Future Generation Computer Systems, Volume 61, 2016, Pages 128-136, ISSN 0167-739X.
[3] J. Cai, Y. Zheng and Z. Zhou, "Review of cyber-security challenges and measures in smart substation", 2016 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Chengdu, 2016, pp. 65-69.
[4] R. Dorothy, Sasilatha, "Smart Grid Systems Based Survey on Cyber Security Issues", Bulletin of Electrical Engineering and Informatics ,Vol. 6, No. 4, December 2017, pp. 337~342.
[5] Roman Schlegel, Sebastian Obermeier, Johannes Schneider, A security evaluation of IEC 62351, Journal of Information Security and Applications, Volume 34, Part 2, 2017, Pages 197-204, ISSN 2214-2126.
[6] Cleveland F. IEC 62351 security standards for the power system information infrastructure. White paper, ver. 14. International Electrotechnical Commission; June 2012.
[7] Industrial Communication Networks - Network and System Security, IEC Std. 62443.
[8] Yi Yang, K. McLaughlin, Lei Gao, S. Sezer, Yubo Yuan and Yanfeng Gong, "Intrusion detection system for IEC 61850 based smart substations", 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, 2016, pp. 1-5.
[9] U. Premaratne, C. Ling, J. Samarabandu and T. Sidhu, "Possibilistic decision trees for Intrusion Detection in IEC61850 automated substations", 2009 International Conference on Industrial and Information Systems (ICIIS), Sri Lanka, 2009, pp. 204-209.
[10] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh and J.C. Tan, "An Intrusion Detection System for IEC61850 Automated Substations", in IEEE Transactions on Power Delivery, vol. 25, no. 4, pp. 2376-2383, Oct. 2010.
[11] Y. Yang et al., "Cybersecurity test-bed for IEC 61850 based smart substations", 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.
[12] Introduction to waterfall unidirectional security gateways: true unidirectionality, true security. Technical report. Waterfall Security Solutions Ltd.; August 2012.
[13] Naiara Moreira, Elías Molina, Jesús Lázaro, Eduardo Jacob, Armando Astarloa, Cyber-security in substation automation systems, In Renewable and Sustainable Energy Reviews, Volume 54, 2016, Pages 1552-1562
[14] IEC 61850-1 Standard ed2.0. Communication networks and systems for power utility automation—Part 1: Introduction and overview; March 2013.
[15] IEC 61850-90-2 Standard ed1.0. Communication networks and systems for power utility automation—Part 90-4: Network engineering guidelines; August 2013.
[16] IEC 61850-8-1 Standard ed2.0. Communication networks and systems for power utility automation—Part 8-1: Specific communication service mapping (SCSM)—mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802- 3; June 2011.
[17] IEC 61850-9-2 Standard ed2.0. Communication networks and systems for power utility automation—Part 9-2: Specific communication service mapping (SCSM)—sampled values over ISO/IEC 8802-3; September 2011.
[18] IEEE C37.238-2011. Standard profile for use of IEEE 1588 precision time protocol in power system applications; July 2011.
[19] IEC 62439-3 ed2.0. Industrial communication networks—high availability automation networks—Part 3: Parallel redundancy protocol (PRP) and highavailability seamless redundancy (HSR); July 2012
[20] M.N. Dazahra, F. Elmariami, A. Belfqih, J. Boukherouaa ."Smart Local Backup Protection for Smart Substation",International Journal of Electrical and Computer Engineering (IJECE) ,Vol 7, No 5

BIOGRAPHIES OF AUTHORS

Dazahra Mohamed Nouh has obtained its state electricity engineering degree in 2012 from the superior National School of electricity and Mechanics (ENSEM). Currently Dazahra is pursuing his Ph.D. Degree programme in Electrical Power Engineering at ENSEM. He is a member of Laboratory of Electrical Networks and Static Converters in ENSEM. His research interests include power systems stability using FACTS, Smart Grid and Smart substation.

Elmariami Faissal Professor at the Superior National School of electricity and mechanics Casablanca, electrical engineering department. Member of the study team "Electrical Networks and Static Converters". He works onthe stability of the electricity network and smart grids

Belfqih Abdelaziz Professor at the National High School of Electricity and Mechanics (University Hassan II of Casablanca - Morocco). PhD, Engineer and holder of the University Habilitation searches (HDR). Head of the research team "Electrical Networks and Static Converters. “Teacher researcher currently working on electricity network and smart grids

Boukherouaa Jamal Professor Ability to Direct Research at the National School of Electricity and Mechanics (ENSEM - Hassan II University of Casablanca). Doctor Engineer and holder of HDR. RECS Research Team Leader. Currently working on high-frequency static converters.