International Journal of Smart Grid and Clean Energy

Cyber security strategies for substation automation systems and their implications

Sugwon Hong *

Department of Computer Engineering and Next-Generation Power Technology Center
116 Myongji-ro, Cheoin-gu, Yongin, Gyeonggi-do, S. Korea

Abstract

As cyber security in the substation automation system and the smart grid has been recognized critical, a plethora of documents related to cyber security have been published. This paper intends to sort out all security approaches and derive the high-level security strategies which can cover all possible specific security measures applied for actual implementation. All security measures ultimately come under three security strategies: network separation, communication message security, and monitoring. Network separation is involved in physical separation and logical network separation, which are located in the front line of defense. As the last line of defense, communication message security is involved in data authentication, data integrity, and optionally data confidentiality. Monitoring should be an integral part of security strategies for detection and reporting of attacks. The intrusion detection system (IDS) is a main tool to realize security monitoring. To design the domain-specific IDS can be a viable security solution to enhance security capabilities of the current substation automation system. The concept of network management can be expanded to enhance security monitoring capability as well as integrated operation of IT and OT systems. Considering the fact that the substation automation system is the main building block of the smart grid and IEC 61850 protocols will be an essential part of data modeling and communication in the smart grid, the security strategies analyzed in the paper can provide reasonable validity to address security issues of the smart grid.

Keywords: cyber security, substation automation system, smart grid, security strategy, IEC 61850 security

1. Introduction

Over the years, substation automation, protection and control systems are gradually moving to the substation automation system (SAS) built on the international standard IEC 61850. These substations are heavily dependent on information exchange on the overlaying IT networks. For this reason, cyber security is not treated as an optional issue to provide reliable operation any more, but a 'must-have' requirement. As the cyber security issue is gaining its importance and attention, a plethora of works have been published to address this issue by government organizations, international standard bodies, utilities, venders, and academic researchers. Here, we mainly focus on the documents published by international bodies and government organizations, not because individual researchers' works are of little significance but those organizations' efforts have more realistic impacts on driving future implementation to install cyber security solutions at the level of utility system as well as equipment.

We classify these cyber security-related documents by two criteria. One is the degree of technological details by which the documents fall under management-oriented or technology-oriented categories. The other is the target or domain on which the documents are intended. A few of them are specifically targeted on substation security or broadly smart grid security, while some are addressing security on the industrial automation and control system (ICS), and the others are directed on overall IT system security.

* Manuscript received December 3, 2018; revised July 17, 2019.
Corresponding author. *E-mail address*: swhong@mju.ac.kr.
doi: 10.12720/sgce.8.6.747-756

For example, the IEC 62351 standards are directed towards cyber security solutions to substation communication based on the IEC 61850 [1-6]. Unlike other standards mentioned above, the IEC 62351 are normative standards which means they are providing security measures for achieving secure operations in the IEC 61350 substations. Originally the standards aim at providing security measures for IEC 61850 communication protocols. But later their scope of the works was expanded beyond the specific IEC 61850 communication protocols.

As for the management or operation, IEEE standards, "Cyber Security Requirements for Substation Automation, Protection, and Control Systems," directly focuses on the security of the substation automation system [7]. The NIST 7628 (vol.1-3) three parts documents, "Guidelines for smart grid cybersecurity" are regarded as a good reference to understand cyber security requirements for the smart grid because they contain exhaustively detailed actors and interfaces, considering all possible services in the smart grid domains including the substation automation system [8]. The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) provide useful guidance for smart grid security. This utility-driven, public-private collaborative project has published security profiles for Advanced Metering Infrastructure (AMI), Distribution Management (DM), Wide-Area Monitoring Protection and Control (Synchrophasor), Substation Automation, and Embedded Devices [9-12]. Cigre also published the informative technical reports which help to understand cyber security requirements for substation automation, protection and control [13-15].

Table 1. Classification of cybersecurity-related documents

target	Management (operation)	Technology
Substation (smart grid)	IEEE C37.240 [7] NIST IR7628 [8] ASAP-SG [9,10,11,12] Cigre D2.31[13] Cigre B5/D2.46 [14] NERC-CIP [16]	IEC 62351 [1-6] Cigre WG B5.38 [15] IEEE P1686 [17] IEEE P1711.1 [18] IEEE P1711.2 [19]
ICS	ISA 62443 [20] IEC 62443 [21] NIST 800-82 [22] DHS IC-CERT [23]	
IT	ISO/IEC 27000 [24] ISO 17799 [25] NIST 800-53 [26]	NIST 800-130 [27] ISO/IEC 9798 IETF RFCs

Table 1 shows which categories these documents come under according to these two criteria [1-27]. All the organizations and standardization bodies do not try and are not willing to come up with new security measures to meet the security requirements and achieve security goals. The reason is that all the useful security solutions are already out there in the IT systems and networks, and they do not want to reinvent the wheel. What they want is to piece the puzzles together to solve security problems for specific assets or systems of the substation and more broadly the smart grid.

In this paper, we claim that all these puzzles to solve security tasks for substation automation systems can be classified into three categories: *network separation*, *communication message security*, and *monitoring*. We claim that all the security measures in the substation automation system eventually can come under one of the categories, and these approaches, which we call the security strategies here, help to understand interrelation between security requirements and specific security measures, and ultimately provide the pillars to construct security solutions for the substation automation system, furthermore the smart grid.

In the next section, we consider the security requirements or goals which are proposed for the ICS systems. In the following sections, we explain each strategy respectively, and then evaluate the suitability of these strategies in the substation automation system, and possibly the smart grid.

2. Security Requirements

Among all imaginable attacks from primitive probing to manipulating an internal system, any sophisticated attackers or intruders' ultimate goal is to lead to malfunction of primary field devices, consequently causing to disrupt normal operation and to degrade service quality, or to degenerate to the complete shut-down of system operation to the extreme. In the same vein, operators try to do the best to defend any possible threats to cause abnormal operations. Any research papers which study cyber security issues of SCADA systems put forward all possible security threats or attacks in the SCADA system, and those list of threats or attacks are similar to typical IT network threats. So, we do not feel the need to enumerate a list again here.

Instead, we want to look into attack vectors that was exposed in the Stuxnet attack which is considered one of the most sophisticated attacks so far [28]. The attack vector means a path by which intruders gain access to a system in order to accomplish an attack goal, exploiting the system's vulnerabilities. The penultimate goal of the Stuxnet is to change file system and alter the system setting and status of the target devices to control field devices, taking advantage of vulnerabilities of OS and programmable logic controller (PLC) software. Access could be obtained via installation of malware on the computers inside the SCADA system.

Similar attack vectors can be utilized by any sophisticated intruders to gain access to the IEC 61850-based substation [29, chap 4.1]. Most studies concern the GOOSE message communication mechanism, which is one of the most critical vulnerabilities in the IEC 61850 protocol. Delivery of false GOOSE message to Intelligent Electronic Devices (IED), which control primary field devices, could entail the same effect that we saw in the Stuxnet attack. Spoofing or false GOOSE message injection may cause the modification of IED file system or altering of status settings, ultimately disrupting operations of primary field devices. Intruders can also flood GOOSE messages into IEDs with intent to achieve Denial of Service (DoS). As far as detection and report of abnormal behaviors is the security monitoring's goal, a monitoring system should detect this kind of critical attacks once they take place in the system.

The international Society of Automation (ISA) proposed seven security requirements for industrial control systems (ICS), which encompass overall aspects of security requirements and are also well suited to SCADA systems [20]. These ISA requirements are similar to the typical IT network security requirements, but they are more specialized in the SCADA/ICS system. The seven security requirements are: *Access Control*, *Use Control*, *Data Integrity*, *Data Confidentiality*, *Restrict Data Flow*, *Timely Response to Event*, and *Network Resource Availability*.

The *access control*, which is called the identification and authentication control in the ISA document, means to verify the identity of users (humans, software processes, devices) requesting access before activating communication. The aim is to prevent illegitimate (unauthenticated) access of selected devices or data. The *use control* means to enforce the assigned privileges of an authenticated user to perform the requested action on the system, and monitor the use of privilege. This is aimed to prevent unauthorized access of selected devices or data. *Data integrity* means to prevent unauthorized manipulation of data, and *data confidentiality* is to prevent unauthorized disclosure of information on communication channel and in data repository. The *restricted data flow* means to determine necessary information flow restriction and thus determine strictly managed configuration of communication paths used to deliver information. The *time response to event* means to respond to security violation by notifying, reporting, and taking timely corrective actions. Lastly, the *network resource availability* is to ensure the availability of the system against degradation or denial of essential services.

Among these seven requirements, availability has the highest priority in the SCADA system because the ultimate goal of attackers is to disrupt normal operation. These requirements are not mutually exclusive. For example, since system availability may be caused by false message injection or intentional overflow of messages, system availability is closely related to user (or device) authentication and data integrity. Network separation strategy is directly related to the restricted data flow and partially related to access control. The role of communication message security strategy is to verify the correctness of message contents and legitimate originators of messages. Meanwhile, monitoring is aimed at the time response to events and prevention of system breakdown, not completely though. Thus, the main task of security monitoring would be how to achieve its intended goals to maintain system availability without any involvement of data authentication and integrity.

3. Network Separation

3.1 First line of defense: Physical separation

Physical network separation is the first line of defense in the sense of providing the ‘air gap’, which means that a network has no outside connections. Any IT devices outside of the network cannot connect the network, crossing a physical gap. But nowadays this belief of the air gap is relegated to be a myth, because complete physical network separation is considered to be untenable. It is claimed that in real life, in no cases can we find any SCADA/ICS networks which are not connected with enterprise networks. Firmware update, OS patches, new logic update to address design flaw, and other maintenance and support activities are highly likely to be implemented by remote access or by using laptops, and sometimes by wireless.

Having said the dark side about physical separation, we claim that the first and foremost strategy is to build as physically separate networks as possible. This means that the design of substation operational networks should be directed to this goal. For this purpose, it is desirable to disconnect any unnecessary network connections, and to remove unneeded services. And we should identify and designate reliable ‘access points’ to the outside of the substation, only through which information should be exchanged with the outside. For this case, security policy will play an important role. For example, security policy enforces that USB connection is not permissible, or can be used only after the USB is examined for any compromise on the designated PC. So is the case of any remote access by any employee.

3.2 Access control at entry points: Virtual separation

If the physical air gap is not achievable, we can resort to logical network separation. The network can be divided into different domains depending on criticality or functionality or any other purposes. Each domain constitutes a virtually separated network which is only connected to other domains via dedicated entry points. Neighboring network domains have clearly defined such security entry points, only on which all information flows are exchanged and strict security policing is enforced. The primary goal is that when attackers try to penetrate deeper networks, it can reduce the probability of attack success, i.e., attacks are as isolated into a penetrated network domain as possible, mitigating attack impacts.

The concept to separate one network into several segmented zones or domains depending on criticality or functionality is nothing new in the network design of IT world. Firewall and intrusion prevention system (IPS) are common equipment used for this purpose, and virtual Private network (VPN) is a common network design technique used for deploying dedicated networks. The network separation, which is often called ‘defense in depth,’ is the major security strategy which the current SCADA/ISC systems depend on, and it will keep on being so in the foreseeable future [22, 23].

At the dedicated entry points, access control such as identification and authentication will be major tasks. The major function of the firewall and IPS is to filter packets based on network protocol information and other information. We might need more sophisticated authentication servers at the entry points which can interpret more semantics of data command flow. For authorization which is a part of the use control of the security requirements mentioned in section 2, the role-based access control (RBAC) scheme can be employed, which is commonly used by many operating systems to control computer resource access. In this scheme, a central RBAC server allows each user to access a specific device, verifying each user’s authentication and authorization based on its identity and privilege assigned to the device. The IEC 62351 part 8 specifies the control of user access to data in the system by means of role-based access control [6].

4. Communication Message Security

While physical network separation is the first line of defense, security at the level of communication messages is said to be the last line of defense from the viewpoints of substation automation systems. Any intruder's final attack goal is to impair the functions of primary field devices in substations and ultimately disrupt proper operations of substations. The goals of message security is to guarantee message integrity, message authentication, and/or message confidentiality. That is, message security prevents intruders from manipulating messages by modifying message contents, injecting false messages, reusing old messages, and hijacking communication sessions. So, this security strategy can level up the substation security capability at the same level of online banking or online transaction in the IT network.

In substation automation systems there are three kinds of message exchanges: between control devices such as IEDs inside a substation, between different substations, between substations and control centers. The IEC 61850 standards define the communication protocols for information exchange in the substations [30]. The IEC 62351 standards target developing security solutions for specific IEC 61850 communication protocols. Unlike other standards, these standards specify the technical details of security measures to satisfy the following security requirements: data authenticity, data integrity, and optionally data confidentiality.

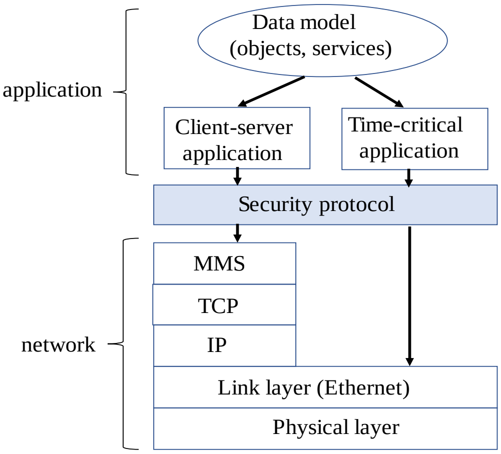

Fig. 1. Substation communication model

The IEC 62351 standards adopt the common IT security algorithms and protocols to derive security measures, such as crypto algorithms, keyed-hash message authentication code (HMAC), digital signature, and Transport Layer Security (TLS). There are two factors to be considered to choose proper security solutions. One is the underlining network stacks as in Fig. 1. The client-server application is running over the TCP/IP stacks, while the time-critical application relies on broadcast communication on the Ethernet LANs. TLS is commonly used in every application running over the TCP/IP in the current IT network. We can also choose TLS as the security protocol for client-server application running over the TCP/IP stacks, since TLS provides all the flavors required for message security. The other factor to select proper security solutions is to meet the performance criteria for each application. IEC 61850 Ed 2 specifies 7 classes of message transfer times depending applications as shown in table 2 [30]. Thus, the time-critical application based on the bare Ethernet communication may choose any message authentication protocols such as HMAC, digital signature, or others, avoiding heavy computing loads involving in encryption/decryption. Practically speaking, we can say that to find proper security measures is not a difficult task because the task is mainly involved in piecing together these algorithms or protocols to meet specific security requirements, considering the underlining network stacks.

A major challenge lies in implementation. Embedded devices in substations have limited computing resources and can devote only a part of their resources for security processing. This fact raises difficulty to meet performance criteria specified in IEC 61850 for processing real time messages such as GOOSE and sample value data. The GOOSE message is designed for peer-to-peer exchange between devices, and need to be transmitted within 3 milliseconds. Digital signature is involved in public key crypto algorithm, which places heavy computing burden on devices. The performance evaluation shows that both software and hardware implementation of the pubic key crypto algorithm could not satisfy this stringent response time requirements [31, 32, 33]. Thus, other message authentication methods should be considered as viable options. Currently TC57 WG15 is reviewing the performance issues. Keyed-hash MAC may replace digital signature for message authentication and integrity to avoid public key crypto computation.

In addition to implementation, migration is another daunting challenge since installing security functions into legacy devices overnight is not possible. Replacement or even retrofitting process will be difficult and time-consuming because SCADA systems should be in 24/7 operation. To circumvent installing built-in security functions into devices, an ad-hoc approach can be considered. This approach is to retrofit legacy devices by developing separate security module, which is often called bump-in-the-wire (BITW) approach [34, 35]. In reality, considering implementation and migration challenges, it will be hard to expect to adapt the communication message strategy to the SCADA/ICS system in the foreseeable future.

Table 2. Message transfer classes

TT class	Transfer Time (ms)	Application Examples
0	>1000	Files, events, log contents
1	1000	Events, alarms
2	500	Operator commands
3	100	Slow automation interactions
4	20	Fast automation interactions
5	10	Releases, status changes
6	3	Trips, blockings

5. Security Monitoring

Combined with two aforementioned security strategies, monitoring is also an integral part of the substation security because it can provide detection and reporting functions. Network security monitoring is to do the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. Monitoring is a way of finding intruders on the network and do something about them before they damage the system [36]. In a nutshell, monitoring is involved in detecting and reporting any illegal behaviors in the system, consequently providing the necessary high-level of security and reliability in the SCADA/ICS system.

5.1. Intrusion Detection System (IDS)

The intrusion detection system (IDS) is a main tool to do security monitoring. The technique of IDS in which we are interested for the substations is the anomaly-based detection. The anomaly detection is the process to determine which observed events are to be identified as abnormal because it has significant deviation from normal behavior which is called profile. As always, the difficult part is how to decide or derive profiles which reflect all characteristics of the system. Thus, the main task to do security monitoring is to design domain-specific IDS which is conscious of the target domain semantics. Here, we can classify domain-specific information into four kinds of information to derive profiles for SCADA-specific IDS: *network features*, *application protocols*, *device characteristics*, and *other domain-specific normal activities*. The paper [37] explains how to design IDS to utilize the domain specifics for each case and the related references.

The first information to be considered is the information about target network features. The SCADA networks have very predictable patterns compared to IT networks [38]. In the IT network, it is not possible to completely predict a list of allowable communication paths. A large portion of the traffic occurring in the IT network is involved in human actions, leading to dynamic traffic patterns. On the contrary, the SCADA network configuration is stable and has the fixed IP addressing schemes. Unless there is any abrupt change in the system configuration, intentional or unintentional, communication paths are deterministic since data exchanges take place between fixed nodes such as IEDs, servers, and other devices, which is mostly machine-to-machine communication.

The second useful information is the application protocol header information. The semantics of each fields of the header in the application protocol data unit (PDU) can be used to verify the validity of the incoming packets. Any correlated rules between different fields of the same packet or between the fields of subsequent packets are also utilized as effective criteria to decide whether incoming packets obey the logic of the application protocols. For example, if the sequence number field exits in the header, the sequence numbers of all packets should be in order, and the following packet's number should be incremented by one. Time stamp field is also useful to check the correctness of a series of arriving packets. In this way, the extracted header information of incoming packets is compared with profiles by simple matching or sometimes checking rules between headers or between a sequence of packets.

The effectiveness of IDS will increase as we can derive profiles which are more aware of semantics of the target system. If we can find out features of field devices to help to monitor traffic, we can enhance the performance of IDS. Another possible way of deriving profile is to use machine learning techniques. In this approach, we can use known data traffic as training data, and derive profiles using machine learning techniques. The validity of profiles still should be verified, but we expect that more researches will be carried out on this approach.

5.2. Network and system management

Traditionally, network management is an indispensable tool to manage complex IT network systems. Network management enables a human manager to have a big picture of complex systems by monitoring the status and operation of all network components in real-time. So, this leads to obtain up-to-date information about system components at the right time. The operation of network management is based on client-server model. Agents residing on network components are collecting information in real time on data objects which are pre-defined at configuration time. A manager residing at a central management station requests data object information to the agents. Then, agents send the collected information, and a manager can combine all data object information into a single database, which is called management information base (MIB) in the network management jargon. The IETF's SNMP protocol specifies the way of exchanging data between agents and a manager. In this way, a manager can get the whole picture of the network system.

Currently substation operation management and IT network management are separated as in Fig. 2. Substation operation servers or EMS collect operation information from IED over the IT network. Then the substation operation manager takes necessary actions based on this information about the system. On the other hand, the IT network manager collects information about network components such as switches, routers, and transmission equipment which consist of the IT network overlaying the substation. The substation operation manager is blind to the IT network, and at the same time the IT network manager is also unaware of the substation device operation. For example, when operation managers detect a problem, they could not decide whether it is caused by the IT network or an IED failure [39].

To expand the concept of network management to the substation automation system can enhance the capability of monitoring IT/OT system in an integrated way. The agent residing in the substation component, mainly Intelligent Electronic Devices (IEDs), collects information regarding physical access, communication security, application protocols, clock, and environment, so that the IT/OT network manager can have an integrated view of the substation devices as well as IT communication components. For this purpose, we need to expand the network and system management (NSM) data objects to reflect what information is needed to manage the substation reliably. The abstract NSM data objects can then be mapped to any appropriate protocol. At present, some of SCADA system device vendors define private MIBs and try to utilize them for monitoring SCADA operations. In order to provide interoperability and approach NSM in a unified way, IEC defines the standard MIBs for the substation automation devices [5].

NSM can enhance monitoring capability of the substation. The operator can track down all configuration status of deployed devices such as their serial number, firmware versions, current setting, resource status, and physical/network access. It enables the operator to have ability to detect any unauthorized manipulation of devices and take proper actions to correct situation.

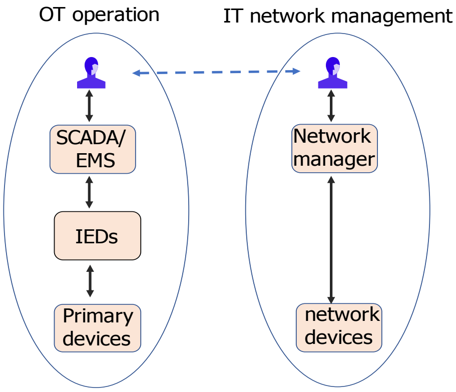

Fig. 2. Current IT/OT system management

6. Conclusion

Network separation is currently the dominant security strategy which the SCADA/ICS systems including the substation rely on. Physical network separation still has validity, and should be the first design goal of network configuration of the substation automation system. For this purpose, it is desirable to disconnect any unnecessary network connections, and to remove unneeded services unless possible risks are fully understood.

The most important thing to design virtually separated networks is to identify and designate reliable access points to the outside of the substation and between the network subdomains inside the substation, only through which the exchange of information flow is admissible. Security policy should be enforced on the access points. However, the devil is always in the details. We have a high degree of ambiguity of how to implement access control at the entry points, so that we can achieve the high-degree of virtually separated networks. This strategy cannot guarantee complete prevention from any unauthorized access. It can only reduce the possibility of attack success, mitigating attack impacts. Even though it may not achieve the full capacity of the security goals, it should be an essential part of security strategy to make secure communication domains for the substation automation system. The logical network separation is the go-to strategy that is being implemented in the current substation automation systems, and maybe it will continue to be so for a long term.

The communication message security can lift the SCADA/ICS security to the same level of the IT network such as routing information exchange between routers in the backbone Internet or client-server message exchange of online banking system. However, the major challenges of message security lie in implementation and migration. Embedded devices in substations have limited computing power and can devote only a part of their resources for security processing. Some messages have very stringent transfer time requirements in the substation. For this reason, the message authentication algorithms or protocols are workable choices. In reality, it will take a long time to make its way of deploying the built-in security functions into field devices.

Security monitoring is a viable solution to enhance security capability in the current SCADA system, since the intrusion detection system as a main tool for monitoring can be easily deployed without any change of the current substation configuration. The main task is how to design the domain-specific IDS reflecting network features and application protocols which are characteristic of the target system. Furthermore, Network and system management which incorporates the IT network management into the substation not only can help to manage and maintain the IT/OT system in a unified way, but it will also enhance the security capability of the SCADA system with collaboration with IDS.

The substation is the main building block of the smart grid. The smart grid consists of several domains each of which has specific asset information and applications, and allows for information of all assets in the domains to be known and being able to influence actions in each domain by means of applications. This information sharing and flows should take place at the right time as well as in an active manner. For this reason of more intimate connectivity and information sharing, network separation has a more significant role in the security. The connection points between domains should be identified and designated, and all the information flows should be monitored and the strict security policy should be enforced on these connection points. The IEC 61850 standard provides a standardized way of defining and exchanging data objects in the substation. IEC 61850 Edition 2 covers Distributed Energy Resources (DERs) and it supports that interoperable applications can be developed for distributed generation as an integrated part of the smart grid. The standard will be expanded to other domains in the smart grid. In this sense, network and system management (NSM) will do a critical role of management and monitoring of the smart grid since it provides a way of monitoring all the assets and their information in a unified way as well as tracking configuration and access status of all the devices. It will take time for NSM to make a way of being utilized in full capacity in the substation and beyond. However, IDS can be a viable tool to be applied for the smart grid security. As IDS can be deployed in the substation without any change of the current substation configuration, it can also be applied to any domain or subdomain in the smart grid as long as we understand the features of the target domains.

Acknowledgements

This research was supported by Korea Electric Power Corporation. (Grant number: R18XA01)

References

[1] *Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security – Profiles including TCP/IP*. IEC TC57 WG15, IEC 61850-3. (2014).

[2] *Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS*. IEC TC57 WG15, IEC 61850-4. (2017).

[3] *Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives*. IEC TC57 WG15, IEC 61850-5. (2013).

[4] *Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850*. IEC TC57 WG15, IEC 61850-5. (2007).

[5] *Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models.* IEC TC57 WG15, IEC 62351-6. (2017).

[6] *Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control.* IEC TC57 WG15, IEC 62351-8. (2011).

[7] IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control System. IEEE Power and Energy Society, IEEE Std C37.240-2014. (2014).

[8] *Guidelines for Smart Grid Cyber Security: Vol.1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*. NIST, NISTIR 7628 Revision 1. (2014).

[9] *Security Profile for Substation Automation*, The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). (2012).

[10] *Security Profile for Advanced Metering Infrastructure*. The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Version 2.1. (2012).

[11] *Security Profile for Distribution Management*, The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). (2012).

[12] *Security Profile for Wide*-Area Monitoring Protection, and Control, The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). (2011).

[13] *Security Architecture principles for Digital Systems in Electric Power Utilities*. Cigre WG D2-31. (2015).

[14] *Application and Management of Cybersecurity Measures for Protection and Control*. Cigre JWG B5/D2.46. (2014).

[15] *The Impact of Implementing Cyber Security Requirements using IEC 61850*. Cigre WG B5.38. (2010).

[16] *Critical Infrastructure Protection (CIP) Standard – CIP 002-009*. NERC Standard CIP 002-009. (2008).

[17] *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*. IEEE Power and Energy Society, IEEE Std 1686-2013. (2013).

[18] *Trial Use Standard for a Crytographic Protocol for Cybersecurity of Substation Serial Links*. IEEE p1711.1. (2013).

[19] *Standard for Secure SCADA Communication Protocol (SSCP)*. IEEE P1711.2.

[20] *Security for industrial and Automation Control Systems - Terminology, Concepts and Models*. ISA Standard ISA-62443-1-1. (2007).

[21] *Industrial Communication networks − Network and system security − Part 1-1: Terminology, concepts and models*. IEC TS 62443-1-1. (2009).

[22] *Guide to Industrial Control Systems (ICS) Security*. NIST special Publication 800-82. (2015).

[23] *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. DHS IC-CERT. (2016).

[24] *Information technology − security techniques − Information Security Management Systems − Overview and vocabulary*. ISO/IEC 27000. (2018).

[25] *Information technology − Security techniques − Code of practice for information security management*. ISO/IEC 17799. (2005).

[26] *Security and Privacy Controls for Information Systems and Organizations*. NIST 800-53.

[27] *A Framework for Designing Cryptographic Key Management Systems*. NIST 800-130. (2010).

[28] Falliere N, Murchu L. O, Chien E, W32.Stuxnet Dossier, Symantec, 2011.

[29] Kabir-Querrec. M. Cyber security of the smart grid control systems: intrusion detection in IEC 61850 communication networks. PhD dissertation. Thesis. Grenoble Alpes University, Grenoble, France; 2017.

[30] *Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device model*. IEC 61850-5 Ed.2. (2013).

[31] Schlegel R, Obermeier S, Schneider J, Assessing the Security of IEC 62351. Presented at: 2015 the 3rd International Symposium for ICS & SCADA Cyber Security Research.

[32] Fuloria S, Anderson R. The Protection of Substation Communications. Presented at: 2010 SCADA Security Scientific Symposium.

[33] Hohlbaum F, Braendle M, Alvarez F. Cyber security practical consideration for implementing IEC 62351. Presented at: 2010 PAC World.

[34] Ishchenko D, Nuqui R. Secure communication of intelligent electronic devices in digital substations. Presented at: 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D).

[35] Tsang PP, Smith SW. YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems. Presented at: 2008 IFIP TC 11 23rd International Information Security Conference.

[36] Bejtlich, R. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press; 2013.

[37] Hong S. Monitoring and network management for SCADA security and its implications. Presented at: 2019 International Conference on Natural Science, Engineering, and Technology.

[38] Lemay A, Rochon J, Fernandez J. A practical flow white list approach for SCADA systems, Presented at: 2016 the 4th International Symposium for ICS & SCADA Cyber Security Research.

[39] *Network System Management: Implementations and Applications of the IEC 62351-7 Standard*. EPRI 3002003738. (2014).