A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges

S. M. Suhail Hussain, *Member, IEEE*, Taha Selim Ustun, *Member, IEEE*, and Akhtar Kalam, *Life Member, IEEE*

***Abstract*—Smart grid is the nexus of advanced information and communication technologies and legacy power systems. With increasing awareness on the vulnerabilities of smart grids to cyberattacks, cybersecurity is becoming a prime concern. Earlier, it was assumed that the power system communication protocols are very specialized and different, so the "security by obscurity" approach would be sufficient. However, with the standardization of communication protocols for power utilities and the emergence of the power market, this approach is no longer valid. IEC 62351 Standard has been published to provide security recommendations for different power system communication protocols including IEC 61850. IEC 61850 is emerging as the most promising and popular power system communication standard. Therefore, in this article, a detailed analysis of security threats, possible attacks, and security requirements for IEC 61850 communication is presented. Building on this, the security considerations presented in IEC 62351 for securing different IEC 61850 messages, such as generic object-oriented substation events (GOOSE), sampled values (SV), routable-GOOSE, routable-SV, and manufacturing message specification messages have been presented in great detail.**

***Index Terms*—Availability, confidentiality, cyber-physical systems, cybersecurity, generic object-oriented substation events (GOOSE), IEC 61850, IEC 62351, message integrity, security requirements.**

I. Introduction

THE traditional power system concept is evolving into smart grid with the integration of information and communication technologies (ICT). The application of advanced ICT in the power system domain enables greater control and operation with smaller margins. All these schemes require some sort of communication and coordination between the different components of the power grid. This communication needs to take place between the equipment that are manufactured by a myriad of companies that pertain to different domains. For this reason, many efforts have been made to develop different communication technologies, standards, and protocols for smart grids [1].

Advancements in ICT technologies with lower latencies and higher bandwidth have propelled the automation of smart grids. Different standards and protocols were developed for standardizing the communication in smart grids. The communication standards and protocols define how the information is exchanged between different components, such as field equipment, and controller intelligent electronic devices (IEDs) and servers. Although initially proposed for substation automation only, International Electrotechnical Commission (IEC) IEC 61850 standard has emerged as the most promising communication standard for smart grids [2]. This is thanks to its object-oriented design that serves for interoperable operation between instruments from different vendors. It has the ability to design new smart grid components and report several datasets at the same time [3]–[5]. With all these capabilities, IEC 61850 is poised to be the smart grid communication standard of the future [6], [7]. The evolution of IEC 61850 from substation to power utility domain has increased the concerns for the cyberattacks [8].

This stems from the fact that, in the past, much attention was paid to improve the performance of the communication protocols and achieve interoperability between different equipment. Cybersecurity was not really a hot research topic. This is because the communication protocols for the power system were considered to be very specialized and different. Hence, the knowledge of how to read the bits and bytes of the appropriate one-out-of-a hundred communication protocols was considered to be challenging and obscure. Therefore, it was assumed that the "security by obscurity" approach would be sufficient [9]. Furthermore, the data exchanged in these communications, such as voltage measurements of a power line, are not considered to be as valuable as the financial information.

However, with the changing paradigms in power system communications, the concept of "security by obscurity" is no longer valid. There are several reasons behind this; with the standardization of the communication protocols and interoperability, information models became uniform without any obscurity. Second, in addition to the power system measurements, financial information is exchanged in power system communications. For instance, in deregulated electricity markets, tiny misinformation about the power information can lead to the

Manuscript received May 22, 2019; revised September 11, 2019 and November 13, 2019; accepted November 24, 2019. Date of publication November 29, 2019; date of current version May 26, 2020. This work was supported in part by Fukushima Prefecture's Reconstruction under Grant 2019. Paper no. TII-19-1981.R2. *(Corresponding author: S. M. Suhail Hussain.)*

S. M. S. Hussain and T. S. Ustun are with the Fukushima Renewable Energy Institute, National Institute of Advanced Industrial Science and Technology, Koriyama 963-0298, Japan (e-mail: suhail.hussain@aist.go.jp; selim.ustun@aist.go.jp).

A. Kalam is with the College of Engineering and Science, Victoria University, Melbourne, VIC 8001, Australia (e-mail: akhtar.kalam@vu.edu.au).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2956734

1551-3203 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

disruption of bids in highly competitive electricity markets, for example, European Power Exchange issue in June 2019 [10]. Finally, with the integration of wide-area power networks with known information models and messages, power system infrastructure has become, at least in theory, a possible target for cyber attacks. This possibility is really broad, as IEC 62351 standard puts it: And the desire to disrupt the power system operations can stem from simple teenager bravado to competitive game playing in the electrical market place to actual terrorism [9].

Therefore, a complete end-to-end (E2E) security model for power system communication is required. IEC technical committee (TC) 57 WG 15 developed the IEC 62351 standard series that addresses the cybersecurity issues of the power communication standards that are under the jurisdiction of TC 57. Cybersecurity vulnerabilities of IEC 61850 communication and the recommended schemes to mitigate those are also discussed in this new standard, IEC 62351 [9]. This document is a list of guidelines and develops a framework for secure operation. However, its implementation in actual operation scenarios, such as overcurrent relay coordination or distributed energy resources (DERs) management system, is open to interpretation. In order to implement cybersecurity measures in smart grids that are modeled according to IEC 61850, a thorough study of IEC 62351 standard is required. After that, individual solutions can be developed to ensure secure communication in different fields of smart grid operation.

Standard development is a hard task as the standards are intended to be inclusive of all technologies and not to favor one over the other. For this reason, they are developed as a set of guidelines or a framework to achieve a certain goal. Specific implementations, their performances, and technology selection are not discussed. It is up to the user to study the standard, understand its stipulations, and develop a practical solution that both meets the technical needs of the operation and the requirements of the standard.

It is important to have a thorough understanding of IEC 61850 messages, their vulnerabilities, and the cybersecurity guidelines of IEC 62351. To this end, in this article, the cybersecurity recommendations by IEC 62351 standard parts (especially parts 4 and 6) for different IEC 61850 message protocols, such as generic object-oriented substation events (GOOSE), sampled values (SV), routable-GOOSE (R-GOOSE), routable-SV (R-SV), and manufacturing message specification (MMS) are analyzed in detail. Differences in the structures of these messages as well as their use cases are discussed. Based on this background, relevant cybersecurity schemes, how they mitigate these vulnerabilities, and practical implementation considerations are discussed.

The rest of this article is organized as follows. Section II gives an overall background of IEC 61850. Section III presents the security requirements, challenges, and potential attacks in the IEC 61850 based power utility automation systems. Section IV presents an overview of IEC 62351 standard. Section V discusses IEC 62351 security considerations for different IEC 61850 messages. Finally, Section VI concludes this article.

TABLE I
DESCRIPTION OF IEC 61850 STANDARD PARTS FOR SAS

Parts	Description
IEC 61850-1	"Introduction and overview"
IEC 61850-2	"Glossary"
IEC 61850-3	"General requirements"
IEC 61850-4	Specifies the system and project management for power utility automation systems with communication between IEDs.
IEC 61850-5 [11]	Specifies information on communication requirements of substation automation functions.
IEC 61850-6 [12]	Specifies a "description language for the configuration of IEDs" in SAS called System Configuration description Language (SCL)
IEC 61850-7-1 [13]	Presents detailed account of Abstract Communication Service Interface (ACSI), different Logical Nodes (LNs), Data Objects (DOs), Common Data Classes (CDCs) and how to achieve interoperability using these building blocks.
IEC 61850-7-2 [14]	
IEC 61850-7-3 [15]	
IEC 61850-7-4 [16]	
IEC 61850-8-1 [17]	"Parts specify the protocol structure and mapping of different ACSI services to MMS, eXtensible Markup Language (XML) messages transported over eXtensible Messaging and Presence Protocol (XMPP) and ISO/IEC 8802-3 (Ethernet)."
IEC 61850-8-2 [18]	
IEC 61850-9-2 [19]	
IEC 61850-9-3 [20]	Specifies a precision time protocol (PTP) profile of IEEE 1588-2008 in compliance with IEC 61850.
IEC 61850-10 [21]	Specifies procedure for "conformance testing of 61850 client, server and engineering tools."

II. IEC 61850 BACKGROUND

The first edition of the IEC 61850 standard series had ten main parts [11]. Table I gives the brief description of different parts of IEC 61850 standard for a substation automation system (SAS). The main strength of IEC 61850 standard is the common data model it uses for devices and its unique message protocols for communicating power system information in a predefined fashion. These two features, which are discussed in detail later in the text, enable interoperability in smart grids and pave the way for plug-and-play (PnP) capability.

A. IEC 61850 for Power Utility Automation Beyond SAS

Considering the popularity of IEC 61850 [22] and its capability of exchanging the high volume of data in a standardized and interoperable manner, researchers and engineers started thinking about using it beyond SAS implementations. Several extension publications, such as 7-420 for DERs, IEC 61850 evolved from a SAS standard into a communication standard that covers the entire power utility automation. IEC 61850-7-420 [23] published in 2009 presents the information modeling for different DERs in terms of logical nodes (LNs). Using these IEC 61850-7-420 information models of DERs, different researchers developed communication assisted protection schemes for the active distribution systems and microgrids with high penetration of DERs [24]–[29]. Furthermore, IEC 61850-7-420 communication-based functions/applications for smart grids and microgrids have been extensively studied and reported, such as energy management [30], [31], active and reactive power control [4], [32], [33], automation [34]–[36], multiagent management [37]–[39], control and optimization [40], and electric vehicle (EV)–photovoltaic coordination [41].

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

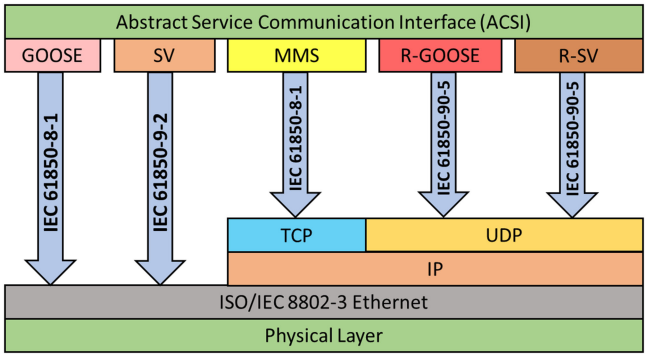

Fig. 1. R-GOOSE and R-SV protocol stack.

Similarly, the IEC 61850-7-420 information models were used to develop communication framework for virtual power plant management [42], [43], battery energy storage system [44] as well as smart meters and solar home systems [5].

IEC 61850-90-1 [45] and IEC 61850-90-2 [46] extensions present a comprehensive overview of the different aspects that need to be considered for intersubstation and substation to control center communication, respectively. For intersubstation information exchange over a wide-area network (WAN), IEC 61850-90-1 specifies either mapping of GOOSE and SV messages over TCP/Internet protocol (IP) layers (but using UDP at the transport layer) or tunneling them across WAN. Using these techniques, exchanging GOOSE and SV in WAN different protection schemes requiring intersubstation communication, such as differential and distance protection, were developed [47]–[49].

IEC 61850-90-5 [50] provides guidelines for IEEE C37.118.1 [51] based synchrophasor data transfer as per IEC 61850. The LN MMXU was augmented with new data objects (DOs), e.g., "HzRte" and "ClcIntvPer," to incorporate the synchrophasor measurement parameters, such as the rate of change of frequency and sampling rate. Additionally, IEEE C37.118.2 [52] PMU information exchanges were replaced by the R-GOOSE and R-SV messages. The layer 2 GOOSE and SV messages are mapped over UDP/IP layers to form the R-GOOSE and R-SV messages, as shown in Fig. 1. Khan *et al.* [53], [54] developed and implemented the R-GOOSE and R-SV gateways for synchrophasor communication. In [55], the performance of the IEC 61850-90-5 PMU communication networks in comparison with IEEE C37.118.2 communication networks is presented. Similarly, the IEC 61850-90-7 [56] extension provided the information models for the power converters of DER systems.

Ustun *et al.* [3] developed an information model for EVs by extending the IEC 61850-7-420 to develop a new LN EVCT. Later in 2016, IEC 61850-90-8 [57] extension specifying the object models for EV and its related equipment was published. It gives an information model for EV and its related equipment for the PnP integration of EVs to the grid. Utilizing the IEC 61850-90-8 information models, communication-based energy management strategy in microgrids with the high penetration of EVs is developed in [58]. In [59], a charging management strategy of EVs based on the harmonization of IEEE WAVE 1609 and IEC 61850-90-8 communication has been presented. IEC 61850-90-8 information model of EV only supports the charging process. In [58], IEC 61850-90-8 LNs for EV were extended by including new DOs to support the discharging process.

From the above nonexhaustive survey, it is quite evident that IEC 61850 is growing fast and poised to become the popular and preferred standard for power utility automation. The evolution of IEC 61850 from the substation to power utility domain has increased the concerns for the cyberattacks. With the standardization of the power communication exchanges and extending IEC 61850 based communication to WANs and to carry sensitive information, such as electricity market transactions, the notion of "security by obscurity" no longer holds valid. A thorough cybersecurity refurbishment is required to keep up with IEC 61850s popularity and extensions for alternative use.

III. Security Requirements, Challenges, and Attacks in IEC 61850 Power Utility Automation Systems

The security challenges for power utility automation systems largely differ from those of Internet systems. All the existing security services and technologies are primarily developed for the computer Internet, whose requirements are completely different from the power system.

Generally, the communication channels used for the power system communication are narrow band with throughput constraints; hence, the security measures resulting are additional overheads, such as key exchanges and digital signatures (DS). Furthermore, the power communication equipment, such as controllers, are limited by processing powers and memory; hence, security measures, such as encryption, become very difficult. The majority of these devices and systems have no access to Internet and are located in remote sites with no on-site personnel. All of these factors make it challenging to manage the keys, revoke certificates, or implement other security measures.

The communication in power utility automation system carries critical information related to direct actions in physical world, any hindrance in accessing any one component may lead to the catastrophic effects. Hence, the denial of service (DoS) to authorized entities in the power utility automation systems is much more severe than the normal Internet systems.

Hence, there is a potential requirement of either developing new services and technologies or modifying the existing security services and technologies of the Internet to adhere to the security and communication requirements of power utility automation systems.

A. Basic Security Requirements, Potential Threats, and Possible Attacks

The four basic security requirements in any system for preventing four basic security threats are the following:

1) confidentiality—Prevention of unauthorized access to information;
2) integrity—Prevention of any modification or theft of information;
3) availability—Preventing (DoS) and availability of information to the authorized users;

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

4) nonrepudiation—Preventing the denial of an action that took place or claim of an action that did not take place [60].

The required security countermeasures largely differ for each system and also depend on time performance. Therefore, identifying the required countermeasures beneficial to meet the security requirements is an important task. It is generally desired to have an optimal solution with adequate appropriate measures and no overkill. The security problem has been clearly explained in IEC 62351 [9] as follows.

Security represents a collection of issues that are hugely sophisticated and spread over different dimensions. The security field cannot be disintegrated into smaller and more manageable portions in a standard and clear way. This makes it, virtually, impossible to survey and deploy full security measures in a cost-effective way.

B. Review of Security Attacks in IEC 61850 Power Utility Automation Systems

IEC 61850s popularity can be attributed to two main factors: ease of connection via Ethernet instead of the traditional hardwired systems and standardized message structures that ensure interoperability. An unwanted consequence of these is the increased vulnerability to cyberattacks. It is easier to access the Ethernet-based networks and standardized messages allow hackers to know exactly what instructions to give.

The attacks on IEC 61850 based substations are carried out usually to achieve these goals.

1) Disrupt the services in substation by modifying and fabricating the information/data exchanges.
2) Gaining access to confidential information.

Different attacks on substation communication network are carried out targeting a specific protocol or device/node. Chattopadhyay *et al.* [61], [62] showcased the malicious fault injection attack (FIA) and false data injection on the target IEDs by injecting computation errors through invasive or noninvasive techniques. Furthermore, the impact on substation security and, eventually, power grid integrity and availability are discussed.

Premaratne *et al.* [63] developed a scheme to audit the security of IEC 61850 automated substation. The audit scheme consists of security metrics that quantify the security of the network. From the security audit, it was concluded that the intrusion attacks were most common and an intrusion detection system must be employed as a viable security countermeasure.

Cyber intrusion attacks on IEC 61850 GOOSE and SV messages are discussed in [64]. The intruders can modify GOOSE messages and trip circuit breakers in substations. With SV messages, an intruder can send fabricated values to control centers that can lead to false conclusions and operational decisions.

Every GOOSE message contains two parameters, status number (*stNum*) and sequence number (*sqNum*). For every GOOSE message published, the *sqNum* value is incremented by one, while the *stNum* value is updated with a new event. Fig. 2 shows how the *sqNum* and *stNum* values change with periodic publication and an event. With the event, *stNum* is incremented to 2 and *sqNum* is initialized to 0.

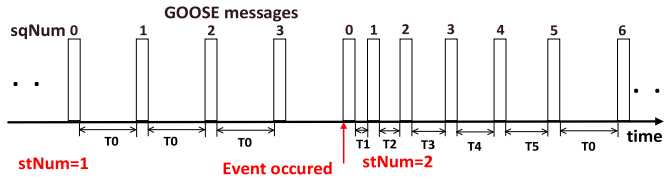

Fig. 2. *stNum* and *sqNum* parameters of GOOSE message.

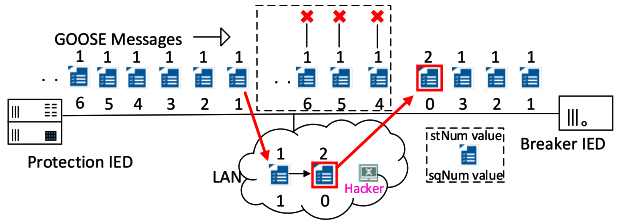

Fig. 3. GOOSE message attach with spoofed status number (*stNum*).

Kush *et al.* [65] describe three types of attacks on GOOSE messages called GOOSE poisoning. The first one is the high-status number attack where the spoofed GOOSE messages with high *stNum* are sent by a hacker. The subscriber, after processing these spoofed GOOSE messages, discards the other legitimate GOOSE messages with *stNum* equal to or less than that of the spoofed messages. Fig. 3 shows that when the subscriber receives the spoofed GOOSE message with *stNum* value 2, it rejects the legitimate GOOSE messages with *stNum* value 1. The second one is high-rate flooding attacks. In this case, several spoofed GOOSE messages are sent as multicast messages while status figures (i.e., *stNum*) are increased. This causes the subscriber to expect a very high *stNum* value for the next GOOSE message. This type of attack is summarized as a status number flooding attack.

The last one is called a semantic attack. This type of attack is carried out in two phases. In the first phase, the attacker observes the network traffic and determines the rate of status change. In the second phase, the attacker multicasts the spoofed GOOSE messages with a different rate. These spoofed GOOSE messages prevent the subscriber from processing the legitimate GOOSE message. Similarly, replay and tampering attacks on the GOOSE and SV messages are discussed in the literature [66]–[68]. The consequences of masquerade and replay attacks on power system operation are discussed in [66].

An integrated anomaly detection system was proposed in [69] to prevent intruders from gaining access to SAS. Similarly, in [70], an intrusion detection system is based on the data collected from simulated attacks on IEDs. However, still these detection systems do not fulfill the authenticity and message integrity security requirements and, hence, are prone to intrusion attacks. Node authentication of all the entities in the network solves the problem of network intrusions [71].

Kang *et al.* [72] demonstrated Man-In-The-Middle (MITM) attack on IEC 61850 MMS messages by ARP spoofing. Based on this MITM attack, the attacker may further launch the series of new attacks, such as eavesdropping, masquerade, false data

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

TABLE II
SUMMARY OF ATTACKS ON IEC 61850 AUTOMATION SYSTEMS

Attack Type	Target message / Device	Description	Security requirements	Reference
Intrusion attacks	GOOSE and SV	Replay, masquerade, data manipulation attacks	Integrity and authenticity	[64]–[69]
MITM attack	MMS	MITM attack based on ARP spoofing to further launch series of new attacks	Integrity, confidentiality and authenticity	[72]
DoS attack	MMS	SYN flood attack during TCP connection and a buffer overflow attack	Authenticity	[73]
Intrusion attacks	Substation LAN	DoS Attacks with ARP and Password crack attacks	Integrity, confidentiality and authenticity	[70]
False data injection attack	IEDs	Malicious FIA are performed by injecting computation errors in the target by invasive or noninvasive techniques	Authenticity, Physical security	[61], [62]

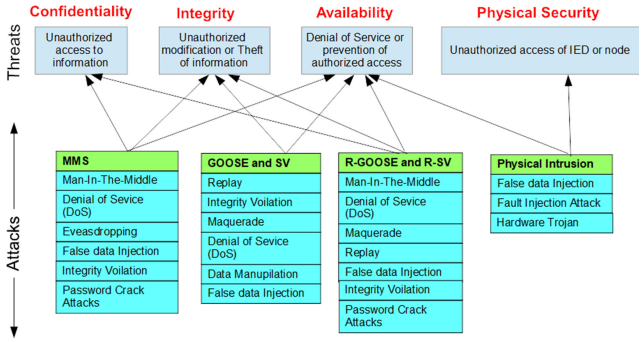

Fig. 4. Different security threats with their corresponding security attacks.

injection, replay, and DoS. SYN flood attacks and buffer overflow attacks as a DoS attack are showcased in [73]. A review of cybersecurity attacks, challenges, and measures for IEC 61850 message exchanges is presented in [74]–[76]. Table II provides a summary of different types of security attacks and the security requirements in IEC 61850 automated systems.

Fig. 4 shows the security requirements, and different security threats and security attacks pertaining to different IEC 61850 messages. Different types of attacks that lead to different security threats, which compromise security requirements, are shown in Fig. 4. It can be noticed that the same type of attack may be used to realize different security threats. In order to achieve E2E security, security measures must be employed to mitigate all of the four threats and the corresponding attacks. Mitigating a single threat would not be adequate as the same type of attack might be possible for a different threat. Hence, all the threats must be addressed at the same time in a system. To address the cybersecurity concerns in IEC 61850 based communication networks, IEC TC 57 published IEC 62351 standard, which is presented in the following.

IV. IEC 62351 OVERVIEW

IEC 62351 standard aims to provide smart grids E2E cybersecurity measures and solutions for possible attacks. It addresses the cybersecurity issues of different IEC TC 57 power communication standards, such as IEC 61850, IEC 60870-5, IEC 61970, IEC 61968, and IEC 60870-6. Currently, the standard has 16 parts, listed as follows.

1) Part 1: Introduction to security issues [9].
2) Part 2: Glossary of terms.
3) Part 3: Profiles including TCP/IP [77].
4) Part 4: Profiles including MMS and derivatives [78].
5) Part 5: Security for IEC 60870-5 and derivatives.
6) Part 6: Security for IEC 61850 [79].
7) Part 7: Network and system management (NSM) data object models [80].
8) Part 8: Role-based access control [81].
9) Part 9: Cyber security key management for power system equipment [82].
10) Part 10: Security architecture guidelines.
11) Part 11: Security for eXtensible markup language (XML) documents.
12) Part 12: Resilience and security recommendations for power systems with DER cyber-physical systems.
13) Part 13: Guidelines on security topics to be covered in standards and specifications.
14) Part 90-1: Guidelines for handling role-based access control in power systems.
15) Part 90-2: Deep packet inspection of encrypted communications.
16) Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7.

The comprehensive analysis of the different parts of IEC 62351 is made in [83]. It covers the analysis of parts 1–10. However, IEC 62351 parts 3 and 4 have been completely revised and parts 7 and 9 are recently added. A brief overview of these revisions is presented in the following.

A. IEC 62351-3:2018

The IEC 62351-3:2018 Ed. 1.1 specifies the cybersecurity procedures to achieve confidentiality, integrity, and authentication at the transport layer for different SCADA and telecontrol protocols that make the use of TCP/IP. Among IEC 61850 messages, this part relates to MMS messaging.

B. IEC 62351-4:2018

IEC 62351-4:2018 specifies the security requirements in terms of procedures, protocol extensions, and algorithms at the transport and application layer for MMS messages and its derivatives. IEC 62351-4:2007 provides limited support for authentication during a handshake and only supports open systems interworking (OSI) protocol stack. IEC 62351-4:2018 was revised to provide more information on the extended integrity and authentication both for the handshake phase and the data transfer phase in MMS communication. Furthermore, it provides support for application protocols using other protocol stacks, e.g., an IP suite. Currently, the IEC 62351-4:2018 supports application protocols with OSI and eXtensible messaging and presence protocol (XMPP) stacks.

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

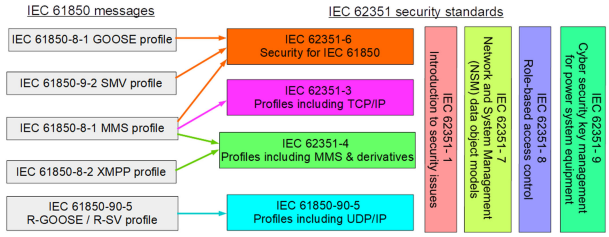

Fig. 5. IEC 62351 security mechanisms corresponding to the different IEC 61850 messages.

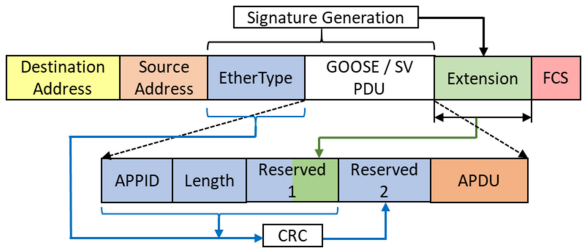

Fig. 6. Extended GOOSE/SV frame format.

C. IEC 62351-7:2017

IEC 62351-7:2017 defines the NSM data object models for determining the security and reliability of the network. These models would help in intrusion detection, monitoring the health and condition of the IEDs. This edition has been revised technically. Furthermore, NSM object description follows the UML model principles, a thorough review is performed on NSM object data with new data introductions; management information bases (MIBs) translation of SNMP protocol is added as code components.

D. IEC 62351-9:2017

IEC 62351-9 specifies the detailed process of generating, distributing, revoking, and handling of public key certificates and cryptographic keys. This includes the asymmetric and symmetric keys that are used in different algorithms specified in the other parts of IEC 62351 standards, such as 3, 4, and 6.

Specific parts of IEC 62351 deal with the security guidelines for securing the IEC 61850 communication. The IEC 61850-6 specifies the security mechanisms to secure the IEC 61850-8-1 [17] GOOSE and IEC 61850-9-2 SV [19] messages, whereas the IEC 62351-4 and 3 provide the security mechanisms required to secure the IEC 61850-8-1 MMS messages and IEC 61850-8-2 [18] XMPP messages. IEC 62351-9 contains the cryptographic key management methods for the security algorithms specified in IEC 62351-3, 4, and 6 for securing different IEC 61850 messages. In addition to the above-discussed security mechanisms, IEC 62351-7 and IEC 62351-8 provide an NSM object model for determining the security and reliability of the network and the role-based access control at application layer common to all types of IEC 61850 messages. Fig. 5 summarizes the security mechanisms defined in different parts of IEC 62351 series corresponding to the different IEC 61850 messages.

V. Security Requirements for IEC 61850 Message Exchanges

In this section, security requirements specified by IEC 62351 standard for different IEC 61850 messages are discussed. For ease of understanding, this section is structured based on three message types used in IEC 61850 based communication. The first category includes the GOOSE and SV messages that can be unicast and multicast messages that are only used within a LAN. The second category includes the R-GOOSE and R-SV messages that are essentially the same as the first category messages except that they can be routed to different LANs and WANs. This extends the operation domain considerably and adds more security vulnerabilities. Finally, MMS messages are considered that are routable yet used for point-to-point communication, not multicast messaging.

A. GOOSE and SV Messages

IEC 62351-1 identifies the message authenticity and integrity as two important security requirements for the IEC 61850 GOOSE and SV messages. Considering that the GOOSE messages have a strict time delivery requirement of 3 ms, IEC 62351-1 stipulates that encryption algorithms should not be applied [9]. The reasoning is that the processing times for encryption of GOOSE messages would be high with the limited computation capacity of the IEDs. The security threats countered by the implementation of these security requirements include the unauthorized modification of data, tampering, and replay and MITM attacks [9]. To achieve these security requirements, IEC 62351-6:2007 standard recommends the use of DS generated by SHA256 and RSA public key algorithms. For the DS generation, an RSA algorithm as per RFC 2313 [84] is stipulated. Furthermore, IEC 62351-6:2007 specifically mentions the use of SHA256 algorithm for generating HASH values and RSASA-PSS algorithm as per RFC 3447 [85] for signing the HASH value as long as it is compatible with RFC 2313.

For every GOOSE/SV message, a DS is generated starting with the EtherType field through the end of application protocol data unit (APDU) field. This generated DS is appended to GOOSE/SV message in a new field "Extension," as shown in Fig. 6. The length of "Extension" field (i.e., DS) is reflected on the second byte of 2-byte "Reserved1" field. Hence, the value in second byte of "Reserved1" field specifies the length of the "Extension" (i.e., DS) appended to the message. "Reserved2" field is used to specify the 16-bit CRC value, which is calculated for first 8 bytes of the GOOSE/SV protocol data unit (PDU) (i.e., "EtherType," "APPID," "Length," and "Reserved 1" fields).

Ustun *et al.* [86] implemented the RSA-based DS as per IEC 62351-6:2007 specifications to mitigate the replay and masquerade attacks on GOOSE messages. However, many shortcomings related to the use of RSA-based DS for securing GOOSE/SV messages were identified in the literature [86]–[91]. Table III lists the computational times for signing the DS with RSA and elliptic curve digital signature algorithm (ECDSA) algorithms reported in the literature. From Table III, it is quite evident that both RSA and ECDSA algorithms do not meet the 3 ms timing

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

TABLE III
TIME TO GENERATE AND VERIFY A DS FOR DIFFERENT SCHEMES

DS Algorithm	Key Size (bits)	DS Signing time (ms)	DS verification time (ms)	Processor	Reference
RSASSA-P KCS1-v1_5	1024	0.942	0.283	Intel i5-3210M CPU @ 2.50GHz	[91]
	2048	3.56	0.75		
RSA	1024	6.8	-	Pentium M 1.7 GHz (1GB RAM)	[88]
	1024	4	-	Intel Core 2 Duo @ 2.2 GHz (2 GB RAM)	
	1024	3.748	0.155	FPGA (100 MHz)	
	1024	1.917	0.129	FPGA (200 MHz)	
RSA	1024	0.3		Xeon server 2.53 GHz	[89]
	1024	>6	-	BeagleBone Black (TIAM3359 ARM Cortex A8 @ 1 GHz)	
	1024	>10	-	Raspberry Pi 2 with BCM2836 quad-core ARM Cortex A7 overclocked at 1 GHz	
ECDSA	112	3.431	0.223	Intel 2.8 GHz Core i7, 4 GB RAM	[90]
ECDSA $F_{2^{160}}$	320	5.7	7.2	Pentium III at I GHz	[94]
ECDSA F_P	320	4.0	5.2		
BLS $F_{3^{97}}$	170	3.5	23.0		

TABLE IV
MAC VARIANTS RECOMMENDED IN DRAFT OF IEC 62351-6:2020

S.No	MAC Algorithm	Hash Function	*MAC* value (Size in bytes)
1	HMAC-SHA256-80	SHA-256	10
2	HMAC-SHA256-128	SHA-256	16
3	HMAC-SHA256-256	SHA-256	32
4	AES-GMAC-64	-	8
5	AES-GMAC-128	-	16

requirement of GOOSE messages [11]. A typical protection IED would be required to handle about 4000 packets of SV per second [92] and about 100–150 GOOSE packets per second [93]. With this huge data rate, it is practically impossible to secure the GOOSE/SV messages with the DS scheme proposed on the IEC 62351-6:2007 standard.

Alternatively, Hussain *et al.* [95]–[97] proposed the use of message authentication code (MAC) algorithms for GOOSE/SV security. IEC 61850-90-5 [50] already stipulates the MAC algorithms for securing R-GOOSE and R-SV. Hence, the MAC algorithms are included in the draft of IEC 62351-6:2020 standards that will be published in 2020. The MAC algorithms and their corresponding sizes of MAC values are given in Table IV.

When using the MAC algorithms for authenticating the GOOSE/SV, the DS is replaced by MAC value in the "Extension" field of extended GOOSE/SV frame. The structure of the "Extension" field appended to the GOOSE/SV frame is shown in Fig. 7.

The average computational processing time and the size of secure GOOSE messages for different MAC algorithms are listed in Table V. The communication delays for exchanging secure GOOSE messages based on the different MAC algorithms in a typical substation communication network obtained through a

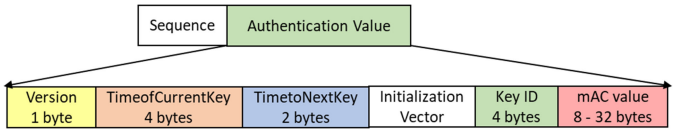

Fig. 7. Structure of the "Extension" field.

TABLE V
E2E DELAY OF DIFFERENT MAC ALGORITHMS

Algorithm		Total Size (bytes)	Computational time (ms)		Comm. Delays (ms)	E2E delay (ms)
			Publisher	Subscriber		
No security		159	0	0	0.0664	0.0664
HMAC-SHA256	80	193	0.0127	0.0141	0.0709	0.0977
	128	199	0.0127	0.0142	0.0722	0.0991
	256	215	0.0127	0.0143	0.0757	0.1027
AES-GMAC-64		205	0.0054	0.0066	0.0730	0.0850
AES-GMAC-128		213	0.0055	0.0069	0.0749	0.0873

TABLE VI
COMPARISON OF SECURITY MEASURES SPECIFIED BY DIFFERENT IEC 62351-6 STANDARDS FOR GOOSE AND SV

Standards / Parameters	**IEC 62351-6:2007**	**IEC 62351-6:2020 (draft)**
Security Measure	RSASA-PSS based signatures	MAC based authentication values
Performance	Very high computational times making it unsuitable for GOOSE and SV	Good performance with low computational time and low signature sizes
Security Extension size	128 bytes (for 1024 key) 256 bytes (for 2048 key)	8 – 32 bytes
Security Target	Authenticity and Integrity	Authenticity and Integrity
Threats and attacks countered	Unauthorized modification of data, tampering, replay and MITM attacks are countered	Unauthorized modification of data, tampering, replay attacks and MITM attacks are countered
Pros	Asymmetric algorithms (public – private key) utilized.	Low computational times and relatively lower signature sizes
Cons	• Relatively high computational times and larger signature size • No measures for confidentiality	• Requirement of pre-shared keys. • No measures for confidentiality

network simulator are also given in Table V. It can be noticed that the E2E delays (including communication and computational delays) for secure GOOSE messages employing any variants of MAC algorithms are less than 3 ms requirements. Hence, MAC algorithms can be successfully applied to both GOOSE and SV messages. However, one of the drawbacks of MAC algorithms is the requirement of preshared keys. Future research pertaining to the safe distribution of keys or proposing of new algorithms without the need for preshared keys can be investigated. Table VI presents the comparison of security measures specified in IEC 62351-6:2007 and draft of IEC 62351-6:2020 standards.

Considering that GOOSE messages have a strict time delivery requirement of 3 ms, IEC 62351-1 stipulates that the encryption

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

algorithms should not be applied [9]. The reasoning is that processing times for encryption of GOOSE messages would be high with the limited computation capacity of the IEDs. However, with the extension of IEC 61850s use beyond SAS to power utility automation, such as DERs [25], virtual power plants [42], energy management [30], EVs [59], and smart meters [5]; sensitive data are carried over IEC 61850 messages. Generally, in SAS, GOOSE messages are used to carry the breaker trip or close commands. The confidentiality of these messages inside a substation environment is not a strict requirement. However, when GOOSE messages are used to send commands to different DERs for energy management or market purposes, their confidentially becomes very important. To achieve the confidentiality requirement in these novel scenarios, the appropriate encryption algorithms for GOOSE messages must be investigated. Also, the encryption algorithms must adhere to the stringent GOOSE timing requirements of 3 ms.

B. R-GOOSE and R-SV Messages

Fig. 1 shows the mapping of GOOSE and SV protocols over the UDP and IP layers to create R-GOOSE and R-SV. The IEC 61850-90-5 specifies the security model for R-GOOSE and R-SV messages considering the security threats and functions given in IEC 62351-1. The IEC 61850-90-5 stipulates that for R-GOOSE and R-SV, the information authenticity and integrity are mandatory requirements, while the confidentiality is left as optional. The IEC 61850-90-5 recommends the use of MAC algorithms to generate DS for APDU authentication and integrity. The process of authentication and integrity verification using the DS is similar to that of the GOOSE and SV. For the optional confidentiality of R-GOOSE/R-SV messages, IEC 61850-90-5 recommends the use of encryption algorithms, such as AES-128 and AES-256 algorithms. Both the MAC authentication and AES encryption algorithms are symmetric algorithms and require a preshared key. The need to provide symmetric keys to the publishers and subscribers of R-GOOSE and R-SV is accomplished by the concept of key distribution center (KDC) in IEC 61850-90-5. The KDC provides key to the subscribers/publishers, which is valid for given time period, and also informs the subscribers/publishers of an impending key change by communicating the "TimeofCurrentKey" and "TimetoNextKey" values.

Fig. 8 shows the packet format of the secure R-GOOSE and R-SV as specified in the IEC 61850-90-5 standard. The extra fields for security are added in the session header and the signature is appended at the end after the payload field. The security fields in session header are "TimeofCurrentKey," "TimetoNextKey," "Security Algorithms," and "Key ID." The "TimeofCurrentKey" has the size of 4 bytes of unsigned integer value representing "SecondSinceEpoch," i.e., the interval "in seconds continuously counted from epoch" [54]. Similarly, the "TimetoNextKey" has 2 bytes size and is represented as a signed integer value. The "Security Algorithms" field is of 2 bytes in size, where the first byte represents the type of encryption employed, if any, and the second byte represents the hash-based message authentication code (HMAC) algorithm used for the signature generation for achieving message authentication and integrity. Table VII lists the different encryption and MAC signature generation algorithms corresponding to the value of "Security Algorithms" field. The "Key ID" field contains 4 bytes of value assigned by the KDC as a reference to the key that is in use.

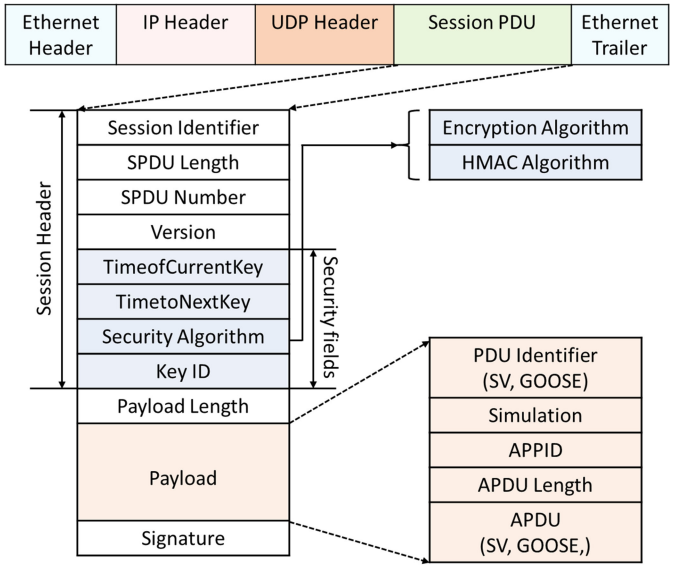

Fig. 8. Packet format of R-GOOSE/R-SV message.

TABLE VII
ENCRYPTION AND MAC SIGNATURE ALGORITHMS FOR R-GOOSE AND R-SV

1st Octet Value	Encryption Algorithm	2nd Octet Value	MAC signature Algorithm
0	None	0	None
1	AES-128-GCM	1	"HMAC-SHA256-80"
2	AES-256-GCM	2	"HMAC-SHA256-128"
		3	"HMAC-SHA256-256"
		4	"AES-GMAC-64"
		5	"AES-GMAC-128"

The signature field consists of the MAC signature value calculated for the session protocol data unit starting from the session header to the payload, as shown in Fig. 8, as per anyone of the algorithms listed in Table VII. The signature field starts with the tag value of 85 hexadecimal (1 byte), the next byte contains the length of calculated MAC signature and then followed by the calculated MAC signature value.

The publishers and subscribers' of R-GOOSE/R-SV messages receive the keys for encryption and MAC signature generation algorithms from the KDC. The IEC 61850-90-5 KDC profile is based on the RFC 3547: group domain of interpretation (GDOI) [98] and Internet security association and key management protocol [99]. The GDOI communication between the publisher/subscriber and KDC also called as "GROUPKEY-PULL" for obtaining key is accomplished in three phases.

1) Connection establishment and authorization through the exchange of X.509 certificates between the KDC and GDOI client (R-GOOSE/R-SV subscriber or publisher).

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

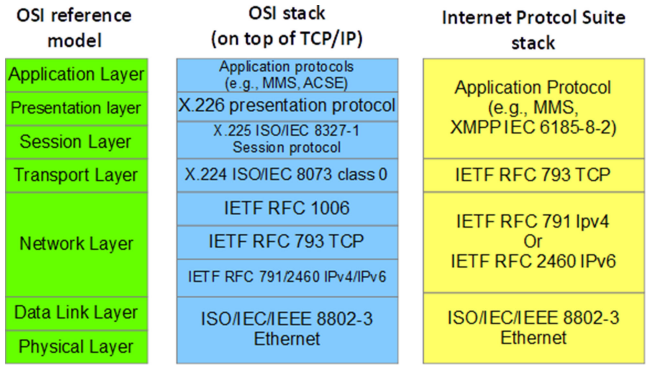

Fig. 9. MMS message protocol stacks.

2) Determining the encryption and signature algorithms that are supported. Initially, the GDOI client sends the GDOI identification payload request to which the KDC responds by sending the key encryption key payload containing the information on the encryption and signature algorithms that are supported. The GDOI client acknowledges these algorithms by issuing a key download (KD) payload request.
3) Obtain the keys. The KDC sends the response to the KD payload request to the GDOI clients.
4) Khan *et al.* [53] present the technical details and also the implementation of IEC 61850-90-5 and GDOI mechanisms for exchanging the keys between the GDOI clients and KDC.

C. MMS Client–Server Messages

The IEC 62351-1 identifies the confidentiality, integrity, and authentication security requirements that are required for the IEC 61850 MMS type messages. The IEC 62351-4:2018 provides the security considerations for achieving the above security requirements. The MMS message exchange process consists of two phases: handshake phase and data transfer phase. The IEC 62351-4 provides support for integrity and authentication during the handshake phase and data encryption during the data transfer phase.

The security to MMS messages is provided for the application and transport profiles. The application profile includes the application, presentation, and session layers of an OSI reference model, whereas the transport profile includes the transport, network, data link, and physical layers.

1) Security for Transport Profile: For securing the transport profiles, the IEC 62351-4 recommends the use of transport layer security (TLS) defined by the RFC 5246 [100]. TLS defines a cipher suite which is a set of cryptographic algorithms for peer authentication, key exchange algorithm, encryption, and MAC. The default TCP port used by IEC 61850 MMS messages is 102. When TLS security profiles are used to secure the MMS messages, the TCP port 3782 must be used as specified by the IEC 62351-4 standard.

The MMS messages can have either the OSI stack or IP suite stack (IP suite), as shown in Fig. 9. As discussed in Section IV, the IEC 62351-4:2007 (old version) supports only the OSI stack. Hence, in the new edition of IEC 62351-4:2018, which supports both the OSI and IP suite stacks, two modes of operation of communication, i.e., compatibility and native modes, are defined. The compatibility mode is compatible with cipher suites for TLS defined in IEC 62351-4:2007 for MMS messages operating with OSI stacks. The cipher suites that are recommended for the compatibility mode of operation are given in Table VIII. However, the IEC 62351-4:2018 specifies that at minimum, cipher suite TLS_DH_DSS_WITH_AES_256_SHA shall be supported. Due to security considerations, the first and last two cipher suites in Table VIII are considered as obsolete and not allowed anymore. Similarly, Table IX lists the recommended cipher suites for the native mode of operation by IEC 62351-4:2018. Furthermore, the IEC 62351-4:2018 also specifies that all the implementations that claim conformance to the native mode shall support cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256 as a minimum.

TABLE VIII
RECOMMENDED CIPHER SUITES FOR COMPATIBILITY MODE OF OPERATION [9]

"Key exchange		Encryption	Hash	Source
Algorithm	Signature			
TLS_RSA		WITH_RC4_128	SHA	RFC 2246 (TLS 1.0)
TLS_RSA		WITH_3DES_ede_CBC	SHA	RFC 2246 (TLS 1.0)
TLS_DH	DSS	WITH_3DES_ede_CBC	SHA	RFC 2246 (TLS 1.0)
TLS_DH	RSA	WITH_3DES_ede_CBC	SHA	RFC 2246 (TLS 1.0)
TLS_DHE	DSS	WITH_3DES_ede_CBC	SHA	RFC 2246 (TLS 1.0)
TLS_DHE	RSA	WITH_3DES_ede_CBC	SHA	RFC 2246 (TLS 1.0)
TLS_DH	DSS	WITH_AES_128	SHA	RFC 4346 (TLS 1.1)
TLS_DH	DSS	WITH_AES_256	SHA	RFC 4346 (TLS 1.1)
TLS_DH		WITH_AES_128	SHA	RFC 4346 (TLS 1.1)
TLS_DH		WITH_AES_256	SHA	RFC 4346 (TLS 1.1)

TABLE IX
RECOMMENDED CIPHER SUITES FOR NATIVE MODE OF OPERATION

"Key exchange		Encryption	Hash	Source
Algorithm	Signature			
TLS_RSA		WITH_AES_128_CBC	SHA256	RFC 5246
TLS_DH	RSA	WITH_AES_128_CBC	SHA256	RFC 5246
TLS_DH	RSA	WITH_AES_128_GCM	SHA256	RFC 5288
TLS_DHE	RSA	WITH_AES_128_GCM	SHA256	RFC 5288
TLS_DH	RSA	WITH_AES_256_GCM	SHA384	RFC 5288
TLS_ECDHE	RSA	WITH_AES_128_GCM	SHA256	RFC 5289
TLS_ECDHE	RSA	WITH_AES_256_GCM	SHA384	RFC 5289
TLS_ECDHE	ECDSA	WITH_AES_128_GCM	SHA256	RFC 5289
TLS_ECDHE	ECDSA	WITH_AES_256_GCM	SHA384	RFC 5289

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

TABLE X
RECOMMENDED CRYPTOGRAPHIC ALGORITHMS FOR E2E SECURITY PROFILE

Type	Algorithm	
Public key algorithms	rsaEncryptionAlgorithms [101]	
	ecPublicKey [102]	Secp256r1
		brainpoolP256r1
Signature algorithms	sha256WithRSAEncryptionAlgorithm	
	ecdsa-with-SHA256-Algorithm	
Symmetric encryption algorithms	AES128-CBC	
	AES256-CBC	
Authenticated encryption algorithms	AES128-GCM	
	AES256-GCM	
Integrity check value algorithms	HMACWithSHA256	
	AES128-GCM	
	AES256-GCM	

When the abovementioned IEC 62351-4:2018 TLS-based security profiles are implemented, the following security threats and attacks are countered: Masquerading, MITM attack, tamper detection/message integrity, unauthorized modification of data, and replay attacks.

2) Security for Application Profile: The security specifications for application profile have two classes.

1) Peer-to-peer security specification (A-security profile) specified by the IEC 62351-4:2007 standard that supports the MMS messages implemented over OSI stack. This profile provides peer authentication at the application layer during association establishment. It does not provide any confidentiality or integrity check mechanism for subsequent data transfer. The peer authentication carried out by exchanging the association control service element AARQ and AARE PDUs containing the calling-authentication-value and responding-authentication-value data as defined in ISO 8650.
2) E2E application security (E2E security), which specifies the end-to-end security for the application layer for MMS messages over IP suite and IEC 61850-8-2 XMPP messages. E2E security profile provides E2E data origin authentication and message integrity during association establishment and also the subsequent data transfer will be bound to this initial authentication, unlike the A-security profile. Furthermore, IEC 62351-4:2018 provides the option of using the E2E security with or without encryption. Table X lists the different cryptographic algorithms specified by the IEC 62351-4:2018 for E2E security profile.

VI. CONCLUSION

In this article, we presented an overview of IEC 61850 message structures and the related cybersecurity concerns in detail. It showed how IEC 6185 use was extended from sending electrical measurements in a closed LAN to WANs, several LANs and sending very sensitive information, such as ownership or financial transactions. The security recommendations specified in the IEC 62351 Standard series for securing IEC 61850 communication were discussed for each message type. A succinct explanation was given to understand these security schemes and put them into perspective in the power system automation.

In addition to these analyses, the timing performance of the security mechanisms recommended by IEC 62351 was examined for power system scenarios that use IEC 61850 based communication. It was found that the use of RSA DS as stipulated in IEC 62351-6 Standard for securing GOOSE and SV does not meet the timing considerations of IEC 61850. Furthermore, performance analysis of the HMAC algorithm, which was being considered in the revised edition of IEC 62351-6, was presented. The IEC 61850-90-5 security recommendations for securing the R-GOOSE and R-SV messages were also analyzed. For an up-to-date discussion, the latest editions of the IEC 62351-4 for securing IEC 61850 messages were described.

This article would be very useful for the researchers to understand cybersecurity vulnerabilities of IEC 61850 messages, the underlying reasons due to message structures, and solution recommendations given in IEC 62351, how these solutions map to vulnerabilities of different IEC 61850 messages as well as their practicality, in terms of timing performances. It also gives further insight into using the different approaches to mitigate these vulnerabilities in a very time-efficient manner.

REFERENCES

[1] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Inform.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.
[2] Communication *Networks* and *Systems* for *Power Utility Automation*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850, 2.0, 2013.
[3] T. S. Ustun, C. R. Ozansoy, and A. Zayegh, "Implementing vehicle-to-grid (V2G) technology with IEC 61850-7-420," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 1180–1187, Jun. 2013.
[4] S. M. S. Hussain, M. A. Aftab, and I. Ali, "IEC 61850 modeling of DSTATCOM and XMPP communication for reactive power management in microgrids," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3215–3225, Dec. 2018.
[5] S. M. S. Hussain, A. Tak, T. S. Ustun, and I. Ali, "Communication modeling of solar home system and smart meter in smart grids," *IEEE Access*, vol. 6, pp. 16985–16996, 2018.
[6] A. Apostolov, "The future is now," 2019. [Online]. Available: https://www.energycentral.com/OMICRON/future-now
[7] "IEC 61850 edition 2—The standard evolves and so does the industry," 2018. [Online]. Available: http://tiny.cc/gtsjcz
[8] S. M. Farooq, S. M. S. Hussain, S. Kiran, and T. S. Ustun, "Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5," *Electronics*, vol. 7, no. 12, Dec. 2018, [Online]. Available: https://www.mdpi.com/2079-9292/7/12/370
[9] *Power Systems Management and Associated Information Exchange—Data and Communications Security Part 1: Communication Network and System Security—Introduction to Security Issues*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-1, 2007.
[10] European Power Exchange (EPEX) SPOT, Paris, Jul. 4, 2019. [Online]. Available: https://www.epexspot.com/document/40853/190704_EPEXSPOT_Press-Release_Decoupling_final.pdf
[11] Communication *Networks* and *Systems* in *Substations*—Part 5: Communication *Requirements* for *Functions* and *Device Models*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-5, 2.0, 2013.
[12] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 6: Configuration *Description Language* for *Communication* in *Power Utility Automation* Systems *Related* to IEDs, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-6, 2.1, 2018.
[13] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 7-1: Basic *Communication Structure*—Principles and *Models*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-7-1, 2.0, 2011.
[14] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 7-2: Basic *Information* and *Communication Structure*—Abstract *Communication Service Interface* (ACSI), Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-7-2, 2.0, 2010.

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

[15] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 7-3: Basic *Communication Structure*—Common *Data Classes*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-7-3, 2.0, 2010.

[16] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 7-4: Basic *Communication Structure*—Compatible *Logical Node Cl*asses and *Data Object Classes*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-7-4, 2.0, 2010.

[17] 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, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-8-1, 2.0, 2011.

[18] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 8-2: Specific *Communication Service Mapping* (SCSM)—Mapping to *Extensible Messaging Presence Protocol* (XMPP), Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-8-2, 2018.

[19] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 9-2: Specific *Communication Service Mapping* (SCSM)—Sampled *Values Over* ISO/IEC 8802-3, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-9-2, 2.0, 2011.

[20] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 9-3: Precision *Time Protocol Profile* for *Power Utility Automation*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-9-3, 1.0, 2016.

[21] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 10: Conformance *Testing*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-10, 2.0, 2012.

[22] X. Cheng, W.-J. Lee, and X. Pan, "Modernizing substation automation systems: Adopting IEC standard 61850 for modeling and communication," *IEEE Ind. Appl. Mag.*, vol. 23, no. 1, pp. 42–49, Jan./Feb. 2017.

[23] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 7-420: Basic *Communication Structure*—Distributed *Energy Resources Logical Nodes*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-7-420, 1.0, 2009.

[24] H. Laaksonen, D. Ishchenko, and A. Oudalov, "Adaptive protection and microgrid control design for Hailuoto island," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1486–1493, May 2014.

[25] T. S. Ustun, C. Ozansoy, and A. Zayegh, "Modeling of a centralized microgrid protection system and distributed energy resources according to IEC 61850-7-420," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1560–1567, Aug. 2012.

[26] D. Della Giustina *et al.*, "Smart grid automation based on IEC 61850: An experimental characterization," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 8, pp. 2055–2063, Aug. 2015.

[27] M. H. Cintuglu, T. Ma, and O. A. Mohammed, "Protection of autonomous microgrids using agent-based distributed communication," *IEEE Trans. Power Del.*, vol. 32, no. 1, pp. 351–360, Feb. 2017.

[28] T. S. Ustun, C. Ozansoy, and A. Zayegh, "Extending IEC 61850-7-420 for distributed generators with fault current limiters," in *Proc. IEEE PES Innov. Smart Grid Technol.*, 2011, pp. 1–8.

[29] T. S. Ustun, C. Ozansoy, and A. Zayegh, "Simulation of communication infrastructure of a centralized microgrid protection system based on IEC 61850-7-420," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun.*, 2012, pp. 492–497.

[30] I. Ali and S. M. S. Hussain, "Communication design for energy management automation in microgrid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2055–2064, May 2018.

[31] W. Shi, X. Xie, C.-C. Chu, and R. Gadh, "Distributed optimal energy management in microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1137–1146, May 2015.

[32] A. Colet-Subirachs, A. Ruiz-Alvarez, O. Gomis-Bellmunt, F. Alvarez-Cuevas-Figuerola, and A. Sudria-Andreu, "Centralized and distributed active and reactive power control of a utility connected microgrid using IEC61850," *IEEE Syst. J.*, vol. 6, no. 1, pp. 58–67, Mar. 2012.

[33] A. Timbus, M. Larsson, and C. Yuen, "Active management of distributed energy resources using standardized communications and modern information technologies," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4029–4037, Oct. 2009.

[34] M. Eriksson, M. Armendariz, O. O. Vasilenko, A. Saleem, and L. Nordstrom, "Multiagent-based distribution automation solution for self-healing grids," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2620–2628, Apr. 2015.

[35] X. Pan, L. Zhang, J. Xiao, F. H. Choo, A. K. Rathore, and P. Wang, "Design and implementation of a communication network and operating system for an adaptive integrated hybrid AC/DC microgrid module," *CSEE J. Power Energy Syst.*, vol. 4, no. 1, pp. 19–28, Mar. 2018.

[36] A. Ruiz-Alvarez, A. Colet-Subirachs, F. Alvarez-Cuevas-Figuerola, O. Gomis-Bellmunt, and A. Sudria-Andreu, "Operation of a utility connected microgrid using an IEC 61850-based multi-level management system," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 858–865, Jun. 2012.

[37] G. Zhabelova, V. Vyatkin, and V. N. Dubinin, "Toward industrially usable agent technology for smart grid automation," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2629–2641, Apr. 2015.

[38] M. H. Cintuglu, T. Youssef, and O. A. Mohammed, "Development and application of a real-time testbed for multiagent system interoperability: A case study on hierarchical microgrid control," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1759–1768, May 2018.

[39] G. Zhabelova and V. Vyatkin, "Multiagent smart grid automation architecture based on IEC 61850/61499 intelligent logical nodes," *IEEE Trans. Ind. Electron.*, vol. 59, no. 5, pp. 2351–2362, May 2012.

[40] M. Manbachi *et al.*, "Real-time co-simulation platform for smart grid volt-VAR optimization using IEC 61850," *IEEE Trans. Ind. Inform.*, vol. 12, no. 4, pp. 1392–1402, Aug. 2016.

[41] T. S. Ustun, S. M. S. Hussain, and H. Kikusato, "IEC 61850-based communication modeling of EV charge-discharge management for maximum PV generation," *IEEE Access*, vol. 7, pp. 4219–4231, 2019.

[42] N. Etherden, V. Vyatkin, and M. H. J. Bollen, "Virtual power plant for grid services using IEC 61850," *IEEE Trans. Ind. Inform.*, vol. 12, no. 1, pp. 437–447, Feb. 2016.

[43] F. Nadeem *et al.*, "Virtual power plant management in smart grids with XMPP based IEC 61850 communication," *Energies*, vol. 12, no. 12, p. 2398, Jun. 2019. [Online]. Available: https://www.mdpi.com/1996-1073/12/12/2398

[44] W. Pei, Z. Qi, W. Deng, and Z. Shen, "Operation of battery energy storage system using extensional information model based on IEC 61850 for micro-grids," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 4, pp. 849–861, Mar. 2016.

[45] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 90-1: Use of IEC 61850 for the *Communication Between Substations*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-90-1, 1.0, 2010.

[46] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 90-2: Using IEC 61850 for *Communication Between Substations* and *Control Centres*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-90-2, 1.0, 2016.

[47] M. A. Aftab, S. Roostaee, S. M. S. Hussain, I. Ali, M. S. Thomas, and S. Mehfuz, "Performance evaluation of IEC 61850 GOOSE-based inter-substation communication for accelerated distance protection scheme," *IET Gener., Transmiss. Distrib.*, vol. 12, no. 18, pp. 4089–4098, Oct. 2018.

[48] B. Falahati, Z. Darabi, and M. Vakilian, "Implementing distance line protection schemes among IEC 61850-enabled substations," in *Proc. IEEE PES T&D Conf. Expo.*, 2014, pp. 1–5.

[49] I. Ali, S. M. S. Hussain, A. Tak, and T. S. Ustun, "Communication modeling for differential protection in IEC-61850-based substations," *IEEE Trans. Ind. Appl.*, vol. 54, no. 1, pp. 135–142, Jan./Feb. 2018.

[50] Communication *Networks* and *Systems* for *Power Utility Automation*—Part 90-5: Use of IEC 61850 to *Transmit Synchrophasor Information A*ccording to IEEE C37.118, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-90-5, 1.0, 2012.

[51] *IEEE Standard for Synchrophasor Measurements for Power Systems*, IEEE Standard C37.118.1-2011, 2011.

[52] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, IEEE Standard C37.118.2-2011, 2011.

[53] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid," *IEEE Access*, vol. 5, pp. 11626–11644, 2017.

[54] S. R. Firouzi, L. Vanfretti, A. Ruiz-Alvarez, H. Hooshyar, and F. Mahmood, "Interpreting and implementing IEC 61850-90-5 routed-sampled value and routed-GOOSE protocols for IEEE C37.118.2 compliant wide-area synchrophasor data transfer," *Electr. Power Syst. Res.*, vol. 144, pp. 255–267, Mar. 2017.

[55] I. Ali, M. A. Aftab, and S. M. S. Hussain, "Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks," *J. Mod. Power Syst. Clean Energy*, vol. 4, no. 3, pp. 487–495, Jul. 2016.

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.

[56] *Communication Networks* and *Systems* for *Power Utility Automation*—Part 90-7: Object *Models* for *Power Converters* in *Distributed Energy Resources* (DER) *Systems*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-90-7, 1.0, 2013.

[57] *Communication Networks* and *Systems* for *Power Utility Automation*—Part 90-8: Object *Model* for E-*Mobility*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-90-8, 1.0, 2016.

[58] M. A. Aftab, S. M. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 and XMPP communication based energy management in microgrids considering electric vehicles," *IEEE Access*, vol. 6, pp. 35657–35668, 2018.

[59] S. M. S. Hussain, T. S. Ustun, P. Nsonga, and I. Ali, "IEEE 1609 WAVE and IEC 61850 standard communication based integrated EV charging management in smart grids," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7690–7697, Aug. 2018.

[60] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. London, U.K.: Pearson, 2017.

[61] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2442–2451, Jun. 2018.

[62] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. IEEE Power Energy Soc. General Meeting*, 2016, pp. 1–5.

[63] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J.-C. Tan, "Security analysis and auditing of IEC61850-based automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2346–2355, Oct. 2010.

[64] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," *Innov. Smart Grid Technol.*, ISGT 2014, Washington, DC, pp. 1–5, 2014.

[65] E. Kush, N. Ahmed, E. Branagan, and M. Foo, "Poisoned GOOSE: Exploiting the GOOSE protocol," in *Proc. 12th Australas. Inf. Secur. Conf.*, 2014, vol. 149, pp. 17–22.

[66] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Electr. Power Syst. Res.*, vol. 143, pp. 825–833, Feb. 2017.

[67] M. Caserza Magro, P. Pinceti, L. Rocca, and G. Rossi, "Safety related functions with IEC 61850 GOOSE messaging," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 515–523, Jan. 2019.

[68] M. El Hariri, E. Harmon, T. Youssef, M. Saleh, H. Habib, and O. Mohammed, "The IEC 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using NN forecasters to detect spoofed packets," *Energies*, vol. 12, no. 19, Sep. 2019, Art. no. 3731.

[69] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.

[70] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010.

[71] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, 5th ed. Boca Raton, FL, USA: CRC Press, 2001.

[72] B. Kang *et al.*, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom.*, 2015, pp. 1–8.

[73] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM based DoS attacks using data mining in smart grid," *Energies*, vol. 2, no. 10, pp. 4091–4109, Oct. 2012.

[74] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," in *Proc. 6th Int. Conf. Inf. Technol. Multimedia*, 2014, pp. 5–10.

[75] J. Cai, Y. Zheng, and Z. Zhou, "Review of cyber-security challenges and measures in smart substation," in *Proc. Int. Conf. Smart Grid Clean Energy Technol.*, 2016, pp. 65–69.

[76] A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, "Security challenges in control network protocols: A survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 619–639, Jan./Apr. 2019.

[77] *Power Systems Management* and *Associated Information Exchange*—Data and *Communications Security*—Part 3: Communication *Network* and *System Security*—Profiles *Including* TCP/IP, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-3, 2018.

[78] *Power Systems Management* and *Associated Information Exchange*—Data and *Communications Security*—Part 4: Profiles *Including* MMS and *Derivatives*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-4, 1.0, 2018.

[79] *Power Systems Management* and *Associated Information Exchange*—Data and *Communications Security*—Part 6: Security for IEC 61850, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-6, 1.0, 2007.

[80] *Power Systems Management* and *Associated Information Exchange*—Data and *Communications Security*—Part 7: Network and *System Management* (NSM) *Data Object Models*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-7, 1.0, 2017.

[81] *Power Systems Management* and *Associated Information Exchange*—Data and *Communications Security*—Part 8: Role-*Based Access Control*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-8, 1.0, 2011.

[82] *Power Systems Management* and *Associated Information Exchange*—Data and *Communications Security*—Part 9: Cyber *Security Key Management* for *Power System Equipment*, Int. Electrotech. Commission, Geneva, Switzerland, IEC 62351-9, 1.0, 2017.

[83] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of IEC 62351," *J. Inf. Secur. Appl.*, vol. 34, pp. 197–204, Jun. 2017.

[84] B. Kaliski, Public-Key Cryptography Standards #1: RSA Encryption Version 1.5, *Internet Eng. Task Force*, Fremont, CA, USA, RFC 2313, 1998.

[85] J. Jonsson and B. Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, *Internet Eng. Task Force*, Fremont, CA, USA, RFC 3447, 2003.

[86] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156044–156053, 2019.

[87] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2016, pp. 266–270.

[88] F. Hohlbaum, M. Braendle, and A. Fernando, "Cyber security practical considerations for implementing IEC 62351," in *Proc. PAC World Conf.*, 2010. [Online]. Available: https://www.semanticscholar.org/paper/Cyber-Security-Practical-considerations-for-IEC-Hohlbaum-Braendle/c14403e717780e84395c51f8370f45446a4fe48d

[89] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic devices in digital substations," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo.*, 2018, pp. 1–5.

[90] T. T. Tesfay and J.-Y. Le Boudec, "Experimental comparison of multicast authentication for wide area monitoring systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4394–4404, Sep. 2018.

[91] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," *IEEE Access*, vol. 7, pp. 32343–32351, 2019.

[92] *Implementation Guideline* for *Digital Interface* to *Instrument Transformers Using* IEC 61850-9-2, UCA International User Group, Int. Electrotech. Commission, Geneva, Switzerland, IEC 61850-9-2 LE, 2004.

[93] ACSELERATOR RTAC SEL-5033 Software Instruction Manual, Schweitzer Eng. Lab., Pullman, WA, USA, 2018.

[94] B. J. Matt, "The cost of protection measures in tactical networks," in *Proc. 24th Army Sci. Conf.*, 2005, pp. 1–8.

[95] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," *IEEE Access*, vol. 7, pp. 80980–80984, 2019.

[96] J. Zhang, J. Li, X. Chen, M. Ni, T. Wang, and J. Luo, "A security scheme for intelligent substation communications considering real-time performance," *J. Mod. Power Syst. Clean Energy*, vol. 7, no. 4, pp. 948–961, Jul. 2019.

[97] M. Rodriguez, A. Astarloa, J. Lazaro, U. Bidarte, and J. Jimenez, "System-on-programmable-chip AES-GCM implementation for wire-speed cryptography for SAS," in *Proc. Conf. Des. Circuits Integr. Syst.*, 2018, pp. 1–6.

[98] M. Baugher, B. Weis, T. Hardjono, and H. Harney, The Group Domain of Interpretation, Internet Eng. Task Force, Fremont, CA, USA, RFC 3547, 2003.

[99] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, Internet Eng. Task Force, Fremont, CA, USA, RFC 2407, 1998.

[100] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, Internet Eng. Task Force, Fremont, CA, USA, RFC 5246, 2008.

[101] J. Schaad, B. Kaliski, and R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for *Use* in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Eng. Task Force, Fremont, CA, USA, RFC 4055, 2005.

[102] S. Turner, D. Brown, K. Yiu, R. Housley, and T. Polk, Elliptic Curve Cryptography Subject Public Key Information, Internet Eng. Task Force, Fremont, CA, USA, RFC 5480, 2009.

Authorized licensed use limited to: Ostbayerische Technische Hochschule Regensburg. Downloaded on April 17,2024 at 11:40:54 UTC from IEEE Xplore. Restrictions apply.