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

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 (ICT) and legacy power systems. With increasing awareness on vulnerabilities of smart grids to cyber-attacks, cybersecurity is becoming a prime concern. Earlier, it was assumed that 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with the standardization of communication protocols for power utilities and emergence of power market, this approach is no longer valid.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 paper, a detail 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 (R-GOOSE), Routable-SV (R-SV) and Manufacturing Message Specification (MMS) messages have been presented in great detail.**

Index Terms—**IEC 61850, IEC 62351, Security requirements, Cyber Physical Systems, Cybersecurity, Availability, Confidentiality, Message Integrity, GOOSE.**

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 power system domain enables greater control and operation with smaller margins. All these schemes require some sort of communication and coordination between different components of the power grid. This communication needs to take place between 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 has propelled the automation of smart grids.

S.M.S. Hussain and T.S. Ustun are with Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan. (email: suhail.hussain@aist.go.jp, selim.ustun@aist.go.jp).
A. Kalam is with the College of Engineering and Science, Victoria University Melbourne 8001, Australia (e-mail: akhtar.kalam@vu.edu.au).

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, controller Intelligent Electronic Devices (IEDs) and servers. Although initially proposed for substation automation only, IEC 61850 standard has emerged as the most promising communication standard for smart grids [2]. This is thanks to its object-oriented design which serves for interoperable operation between instruments from different vendors. It has the ability to design new smart grid components and report several data sets 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, 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, is not considered to be as valuable as 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. Secondly, in addition to 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 disruption of bids in highly competitive electricity markets for example European Power Exchange (EPEX) issue in June 2019 [10]. Lastly, 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 International Electrotechnical Commission (IEC) 62351 standard puts it: And the desire to disrupt 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 security model for power system communication is required. IEC Technical Committee (TC) 57 WG 15 developed IEC 62351 standard series which 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 mitigates 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 over-current relay coordination, or distributed energy resources 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 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 paper the cybersecurity recommendations by IEC 62351 standard parts (especially part 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 uses cases are discussed. Based on this background, relevant cybersecurity schemes, how they mitigate these vulnerabilities and practical implementation considerations are discussed.

Rest of the paper is organized as follows: Section II gives an overall background of IEC 61850. Section III presents the security requirements, challenges and potential attacks in 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 draws the conclusions.

II. IEC 61850 BACKGROUND

The first edition of IEC 61850 standard series had 10 main parts [11]. The Table I gives the brief description of different parts of IEC 61850 standard for 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 below in detail, enable interoperability in smart grids and pave the way for plug-and-play (PnP) capability.

TABLE I
DESCRIPTION OF IEC 61850 STANDARD PARTS FOR SUBSTATION
AUTOMATION SYSTEMS (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] IEC 61850-7-2 [14] IEC 61850-7-3 [15] IEC 61850-7-4 [16]	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 61850-8-1 [17] IEC 61850-8-2 [18] IEC 61850-9-2 [19]	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 61850-9-3 [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.

A. IEC 61850 for power utility automation beyond SAS

Considering the popularity of IEC 61850 [22] and its capability to exchange 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 distributed energy resources (DERs), IEC 61850 evolved from a SAS standard into a communication standard that covers 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 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], multi-agent management [37]–[39], control and optimization [40], Electric Vehicle (EV)- Photovoltaic (PV) coordination [41]. 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 comprehensive overview of the different aspects that need to be considered for inter-substation and substation to control center communication, respectively. For inter-substation information exchange over a Wide Area Network (WAN), IEC 61850-90-1 specifies either mapping of GOOSE and SV messages over TCP/IP layers (but using UDP at the transport layer) or tunneling them across WAN. Using these techniques exchanging GOOSE and SV in a WAN different protection schemes requiring inter-substation 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 Rate of Change of Frequency (ROCOF) and sampling rate. Additionally, IEEE C37.118.2 [52] PMU information exchanges were replaced by 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. In [53], [54] authors developed and implemented R-GOOSE and R-SV gateways for synchrophasor communication. In [55] the performance of the IEC 61850-90-5 PMU communication networks in comparison to IEEE C37.118.2 communication networks is presented. Similarly, the IEC 61850-90-7 [56] extension provided information models for power converters of DER systems.
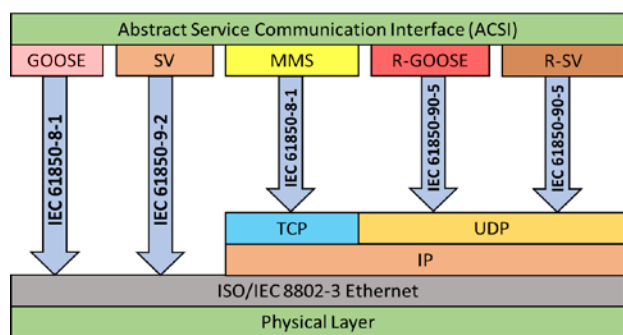

Fig. 1. R-GOOSE and R-SV protocol stack.

Authors in [3], developed 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 PnP integration of EVs to the grid. Utilizing the IEC 61850-90-8 information models, communication-based energy management strategy in microgrids with high penetration of EVs is developed in [58]. In [59], a charging management strategy of EVs based on 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 non-exhaustive 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 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 61850's 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 differs to 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 power system communication are narrow band with throughput constraints, hence the security measures resulting is additional overheads such as key exchanges, digital signatures etc. Further, the power communication equipment such as controllers are limited by processing powers and memory, hence security measures such as encryption etc. becomes very difficult. 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 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 catastrophic effects. Hence, the denial of service to authorized entity in power utility automation systems is much more severe than 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 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: 1) Confidentiality – prevention of unauthorized access to information; 2) Integrity – prevention of any modification or theft of information; 3) Availability – preventing denial of service and availability of information to authorized users; 4) Non-repudiation – 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. Security field cannot be disintegrated into smaller, 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 61850's popularity can be attributed to two main factors: ease of connection via ethernet instead of traditional hard-wired systems and standardized message structures which ensures interoperability. An unwanted consequence of these is the increased vulnerability to cyber-attacks. It is easier to access 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 or
2. Gaining access to confidential information.

Different attacks on substation communication network are carried out targeting a specific protocol or device/node. In [61], [62] authors showcased the malicious Fault Injection Attack (FIA) and false data injection on target IEDs by injecting computation errors through invasive or noninvasive techniques. Further, the impact on substation security and, eventually, power grid integrity and availability are discussed.

In [63] authors developed a scheme to audit the security of IEC 61850 automated substation. The audit scheme consists of security metrics which quantify the security of the network. From the security audit, it was concluded that 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 which 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 *stNum* value is updated with a new event. Fig. 2 shows how *sqNum* and *stNum* values change with periodic publication and an event. With the event, stNum is incremented to 2 and sqNum is initialized to zero.

In [65] authors describe about three types of attacks on GOOSE messages called GOOSE poisoning. First one is the high-status number attack where spoofed GOOSE messages with high *stNum* are sent by a hacker. The subscriber, after processing these spoofed GOOSE messages, discard the other legitimate GOOSE messages with *stNum* equal to or less than that of spoofed messages. Figure 3 shows that when the subscriber receives the spoofed GOOSE message with *stNum* value 2, it rejects legitimate GOOSE messages with *stNum* value 1. Second one is high rate flooding attack. 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 status number flooding attack.
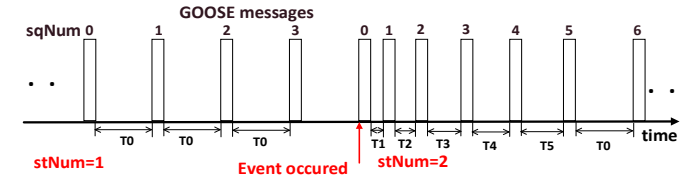

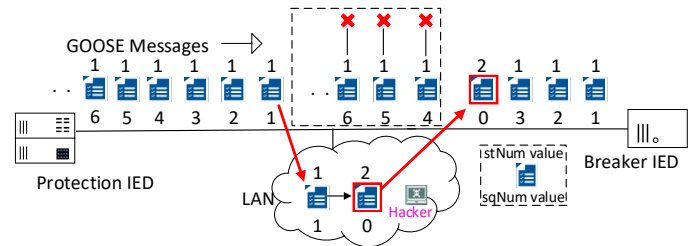Fig. 2. *stNum* and *sqNum* parameters of GOOSE message.

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

The last one is called 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 second phase, attacker multicasts spoofed GOOSE messages with a different rate. These spoofed GOOSE messages prevent subscriber from processing the legitimate GOOSE message. Similar replay and tampering attacks on 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 (ADS) was proposed in [69] to prevent intruders gaining access to SAS. Similarly, in [70] an intrusion detection system based on 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].

In [72] authors, 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 series of new attacks such as eavesdropping, masquerade, false data injection, replay and DoS. SYN flood attacks and buffer overflow attacks as a DoS attack are showcased in [73]. Review of cybersecurity attacks, challenges and measures for IEC 61850 message exchanges is presented in [74]–[76]. Table II provides summary of different types of security attacks and the security requirements in IEC 61850 automated systems.

Figure 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 same type of attack may be used to realize different security threats. In order to achieve end-to-end security, security measures must be employed to mitigate all of 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 cybersecurity concerns in IEC 61850-based communication networks, IEC TC 57 published IEC 62351 standard which is presented below.
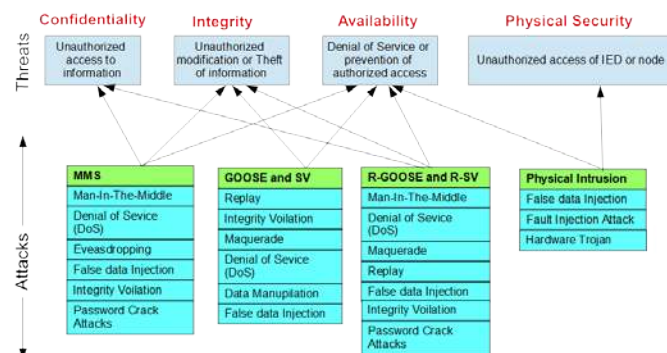

Fig. 4. Different security threats with their corresponding security attacks.

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]

IV. IEC 62351 OVERVIEW

IEC 62351 standard aims to provide smart grids end-to-end 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:

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

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

1. 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 use of TCP/IP. Among IEC 61850 messages, this part relates to MMS messaging.

2. IEC 62351-4:2018:

IEC 62351-4:2018 specifies 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 handshake and only supports Open Systems Interworking (OSI) protocol stack. IEC 62351-4:2018 was revised to provide more information on extended integrity and authentication both for handshake phase and the data transfer phase in MMS communication. Furthermore, it provides support for application protocols using other protocol stacks, e.g. an Internet protocol suite. Currently, the IEC 62351-4:2018 supports application protocols with OSI and eXtensible Messaging and Presence Protocol (XMPP) stacks.

3. IEC 62351-7:2017

IEC 62351-7:2017 defines network and system management (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 UML model principles, a thorough review is performed on NSM object data with new data introductions; MIBs translation of SNMP protocol is added as Code Components.

4. 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 asymmetric and symmetric keys that are used in different algorithms specified in other parts of IEC 62351 standards such as 3, 4 and 6.

Specific parts of IEC 62351 deals 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 NSM object model for determining the security and reliability of the network and role-based access control at application layer common to all types of IEC 61850 messages. Figure 5 summarizes the security mechanisms defined in different parts of IEC 62351 series corresponding to the different IEC 61850 messages.
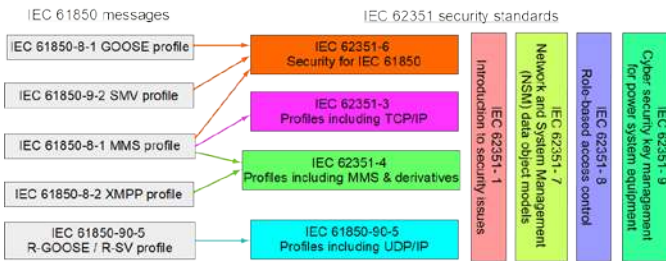

Fig. 5. IEC 62351 security mechanisms corresponding to the different IEC 61850 messages.

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 messages types used in IEC 61850 based communication. First category includes GOOSE and SV messages which can be unicast and multicast messages that are only used within a LAN. Second category includes R-GOOSE and R-SV messages which are essentially the same as 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 which are routable yet used for point-to-point communication, not multicast messaging.

A. GOOSE and SV messages

IEC 62351-1 identifies message authenticity and integrity as two important security requirements for IEC 61850 GOOSE and SV messages. Considering that 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 processing times for encryption of GOOSE messages would be high with the limited computation

capacity of the IEDs. The security threats countered by implementation of these security requirements include unauthorized modification of data, tampering, replay and MITM attacks [9]. To achieve these security requirements, IEC 62351-6:2007 standard recommends use of Digital Signatures (DS) generated by SHA256 and RSA public key algorithms. For DS generation, RSA algorithm as per RFC 2313 [84] is stipulated. Further, IEC 62351-6:2007 specifically mentions 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 stating 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 2nd byte of 2-byte "Reserved1" field. Hence, the value in 2nd byte of 'reserved1' field specifies the length of the 'Extension' (i.e. DS) appended to the message. "Reserved2" field is used to specify 16-bit CRC value, which is calculated for first 8 bytes of the GOOSE/SV PDU (i.e. 'Ether-type', 'APPID', 'Length' and 'reserved 1' fields).
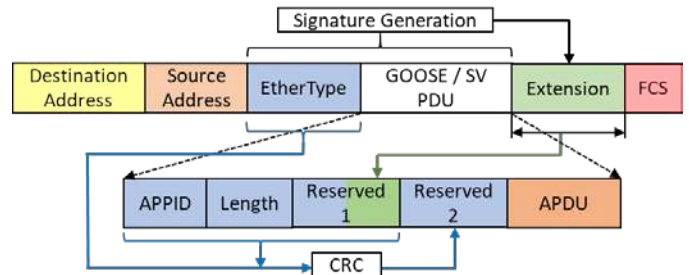

Fig. 6. Extended GOOSE/SV frame format.

In [86], authors implemented RSA based digital signatures as per IEC 62351-6:2007 specifications to mitigate 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 literature [86]–[91]. Table III shows the computational times for signing the DS with RSA and ECDSA algorithms reported in literature. From Table III it is quite evident that both RSA and ECDSA algorithms do not meet the 3 ms timing 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 to 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 IEC 62351-6:2007 standard.

TABLE III
TIME TO GENERATE AND VERIFY A DIGITAL SIGNATURE FOR DIFFERENT SCHEMES

DS Algorithm	Key Size (bits)	DS Signing time (ms)	DS verification time (ms)	Processor	Reference
RSASSA-PKCS1-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	[88]

				(1GB RAM)	
	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		

Alternatively, in [95]–[97] authors proposed use of Message Authentication Code (MAC) algorithms for GOOSE/SV security. IEC 61850-90-5 [50] already stipulates MAC algorithms for securing R-GOOSE and R-SV. Hence, the MAC algorithms are included in the draft of IEC 62351-6:2020 standards which will be published in 2020. MAC algorithms and their corresponding sizes of MAC values are given in Table IV.

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

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 the Fig. 7.
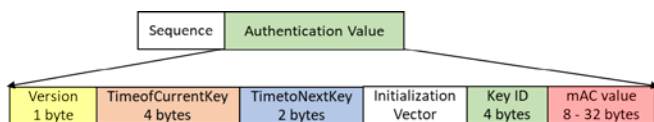

Fig. 7. Structure of the "Extension" field.

The average computational processing times and size of secure GOOSE messages for different MAC algorithms are listed in Table V. The communication delays for exchanging secure GOOSE messages based on different MAC algorithms in a typical substation communication network obtained through network simulator is also given in Table V. It can be noticed that, End-to-End (E2E) delays (including communication and computational delays) for secure GOOSE messages employing any variants of MAC algorithms is 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 requirement of pre-shared keys. Future research pertaining to safe distribution of keys or proposing of new algorithms

without the need of pre-shared 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 encryption 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 61850's use beyond SAS to power utility automation such as DERs [25], Virtual Power Plants [42], energy management [30], electric vehicles [59], smart meters [5]; sensitive data is 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 appropriate encryption algorithms for GOOSE messages must be investigated. Also, the encryption algorithms must adhere to the stringent GOOSE timing requirements of 3 ms.

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

B. R-GOOSE and R-SV messages

Figure 1 shows the mapping of GOOSE and SV protocols over 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 is mandatory requirement, while the confidentiality is left as optional. The IEC 61850-90-5 recommends use of MAC algorithms to generate digital signatures for APDU authentication and integrity. The process of authentication and integrity verification using the digital signatures is similar to that of 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 requires a pre-shared 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.

Figure 8 shows the packet format of the secure R-GOOSE and R-SV as specified in 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 payload field. The security fields in session header are "TimeofCurrentKey", "TimetoNextKey", "Security Algorithms" and "Key ID". The "TimeofCurrentKey" has 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 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 HMAC algorithm used for signature generation for achieving message authentication and integrity. Table VII lists different encryption and MAC signature generation algorithms corresponding to 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.

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 any one of the algorithms listed in Table VII. The signature field starts with tag value of 85 hexadecimal (1 byte), next byte contains the length of calculated MAC signature and then followed by the calculated MAC signature value.

The publisher 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 (ISAKMP) [99]. The GDOI communication between Publisher/Subscriber and KDC also called as "GROUPKEY-PULL" for obtaining Key is accomplished in 3 phases:

1. Connection establishment and authorization through exchange of X.509 certificates between the KDC and GDOI client (R-GOOSE/R-SV subscriber or publisher)
2. Determining the encryption and signature algorithms that are supported. Initially the GDOI client sends GDOI identification payload request, to which KDC responds by sending the Key Encryption Key (KEK) Payload contain the information on 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.

In [53], authors present the technical details and also implementation of IEC 61850-90-5 and GDOI mechanisms for exchanging the keys between GDOI clients and KDC.
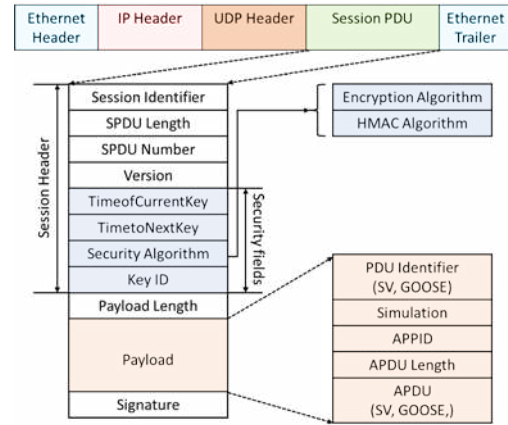

Fig. 8. Packet format of R-GOOSE/R-SV message.

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

C. MMS client-server messages

The IEC 62351-1 identifies confidentiality, integrity and authentication security requirements 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 takes consists of two phases: handshake phase and data transfer phase. The IEC 62351-4 provides support for integrity and authentication during handshake phase and data encryption during the data transfer phase.

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

5.3.1. Security for transport profile:

For securing the transport profiles the IEC 62351-4 recommends 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 message authentication code. 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 Internet Protocol 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 mode 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 compatibility mode of operation are given in Table VIII. However, the IEC 62351-4:2018 specifies the 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 any more. Similarly, Table IX lists the recommended cipher suites for native mode of operation by IEC 62351-4:2018. Further, the IEC 62351-4:2018 also specifies that all the implementations that claim conformance to native mode shall support cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256 as a minimum.
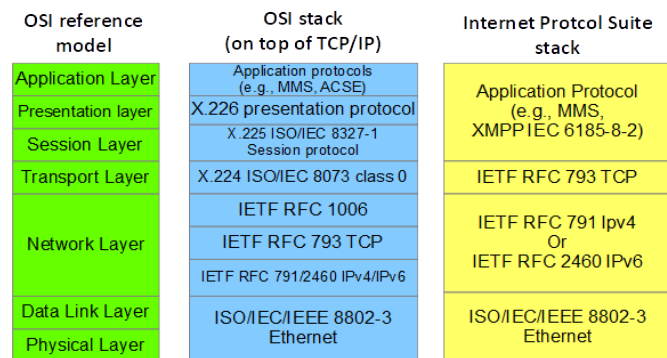

Fig. 9. MMS message protocol stacks.

When the above-mentioned 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.

5.3.2. Security for application profile:

The security specifications for application profile has two classes:

1. Peer-to-peer security specification (A-security profile) specified by the IEC 62351-4:2007 standard which supports the MMS messages implemented over OSI stack. This profile provides peer authentication at the application layer during association establishment. It doesn't provide any confidentiality or integrity check mechanism for subsequent data transfer. The peer authentication carried out by exchanging the Association Control Service Element (ACSE) AARQ and AARE PDUs containing the calling-authentication-value and responding-authentication-value data as defined in ISO 8650.

2. End-to-end 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 end-to-end 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. Further, IEC 62351-4:2018 provides the option of using the E2E security with or without encryption. The Table X list the different cryptographic algorithms specified by the IEC 62351-4:2018 for E2E security profile.

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

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	

VI. CONCLUSIONS

This paper presents an overview of IEC 61850 message structures and the related cybersecurity concerns in detail. It shows how IEC 61850's use has been 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 are discussed for each message type. A succinct explanation is given to understand these security schemes and put them into perspective in power system automation.

In addition to these analyses, timing performance of the security mechanisms recommended by IEC 62351 is examined for power system scenarios that use IEC 61850-based communication. It has been found that the use of RSA digital signatures 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 is being considered in the revised edition of IEC 62351-6, has been presented. The IEC 61850-90-5 security recommendations for securing R-GOOSE and R-SV messages have also been analyzed. For an up-to-date discussion, the latest editions of the IEC 62351-4 for securing IEC 61850 messages has been described.

This paper would be very useful for 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 on using 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. Informatics*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[2] *Communication networks and systems for power utility automation*, 2.0. IEC 61850, IEC, 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*, 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. Farooq, S. Hussain, S. Kiran, and T. Ustun, "Certificate Based Authentication Mechanism for PMU Communication Networks Based on IEC 61850-90-5," *Electronics*, vol. 7, no. 12, Dec. 2018.

[9] "Power systems management and associated information exchange – Data and communications security Part 1: Communication network and system security – Introduction to security issues," IEC 62351-1, IEC, 2007.

[10] "European Power Exchange (EPEX) SPOT." [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*, 2.0. IEC 61850-5, IEC, 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*, 2.1. IEC 61850-6, IEC, 2018.

[13] *Communication networks and systems for power utility automation - Part 7-1: Basic communication structure - Principles and models*, 2.0. IEC 61850-7-1, IEC, 2011.

[14] *Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)*, 2.0. IEC 61850-7-2, IEC, 2010.

[15] *Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes*, 2.0. IEC 61850-7-3, IEC, 2010.

[16] *Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes*, 2.0. IEC 61850-7-4, IEC, 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*, 2.0. IEC 61850-8-1, IEC, 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)*. IEC 61850-8-2, IEC, 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*, 2.0. IEC 61850-9-2, IEC, 2011.

[20] *Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation*, 1.0. IEC 61850-9-3, IEC, 2016.

[21] *Communication networks and systems for power utility automation - Part 10: Conformance testing*, 2.0. IEC 61850-10, IEC, 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. 2017.

[23] *Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes*, 1.0. IEC 61850-7-420, IEC, 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.*, 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 Deliv.*, 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 *2011 IEEE PES Innovative Smart Grid Technologies*, 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 *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 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, 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. Informatics*, 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. Informatics*, 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.

[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. Transm. 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*, 1.0. IEC 61850-90-1, IEC, 2010.

[46] *Communication networks and systems for power utility automation - Part 90-2: Using IEC 61850 for communication between substations and control centres*, 1.0. IEC 61850-90-2, IEC, 2016.

[47] M. A. Aftab, S. Roostaee, S. M. Suhail 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. Transm. Distrib.*, vol. 12, no. 18, pp. 4089–4098, Oct. 2018.

[48] B. Falahati, Z. Darabi, and M. Vakilian, "Implementing distance line protection schemes among IEC61850-enabled substations," in *2014 IEEE PES T&D Conference and Exposition*, 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. 2018.

[50] *Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*, 1.0. IEC 61850-90-5, IEC, 2012.

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

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

[56] *Communication networks and systems for power utility automation - Part 90-7: Object models for power converters in distributed energy resources (DER) systems*, 1.0. IEC 61850-90-7, IEC, 2013.

[57] *Communication networks and systems for power utility automation - Part 90-8: Object model for E-mobility*, 1.0. IEC 61850-90-8, IEC, 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. 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. Informatics*, 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 *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 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 Deliv.*, 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," in *ISGT 2014*, 2014, pp. 1–5.

[65] E. Kush,N., Ahmed, E., Branagan,M. and Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol," in *Twelfth Australasian Information Security Conference (AISC 2014)*, 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, p. 3731, Sep. 2019.

[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 Deliv.*, 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. CRC Press, 2001.

[72] B. Kang *et al.*, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, 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. 5, 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 *Proceedings of the 6th International Conference on Information Technology and Multimedia*, 2014, pp. 5–10.

[75] J. Cai, Y. Zheng, and Z. Zhou, "Review of cyber-security challenges and measures in smart substation," in *2016 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 2016.

[76] A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, "Security Challenges in Control Network Protocols: A Survey," *IEEE Commun. Surv. Tutorials*, pp. 1–1, 2018.

[77] *Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP*. IEC 62351-3, IEC, 2018.

[78] *Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives*, 1.0. IEC 62351-4, IEC, 2018.

[79] *Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850*, 1.0. IEC 62351-6, IEC, 2007.

[80] *Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models*, 1.0. IEC 62351-7, IEC, 2017.

[81] *Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control*, 1.0. IEC 62351-8, IEC, 2011.

[82] *Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment*, 1.0. IEC 62351-9, IEC, 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*. RFC 2313, IETF, 1998.

[85] J. and B. K. Jonsson, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*. RFC 3447, IETF, 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 *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, pp. 266–270.

[88] F. Hohlbaum, M. Braendle, and A. Fernando, "Cyber Security Practical considerations for implementing IEC 62351," in *PAC World Conference*, 2010.

[89] D. Ishchenko and R. Nuqui, "Secure Communication of Intelligent Electronic Devices in Digital Substations," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2018.

[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*. IEC 61850-9-2 LE, UCA International User Group, 2004.

[93] *ACSELERATOR RTAC SEL-5033 Software Instruction Manual*. Schweitzer Engineering Laboratories, 2018.

[94] B. J. Matt, "The cost of protecion measures in tactical networks," in *Proc. of the 24th Army Science Conference*, 2005.

[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 *2018 Conference on Design of Circuits and Integrated Systems (DCIS)*, 2018, pp. 1–6.

[98] M. Baugher, B. Weis, T. Hardjono, and H. Harney, *The Group Domain of Interpretation*. RFC 3547, IETF, 2003.

[99] D. Piper, *The Internet IP Security Domain of Interpretation for ISAKMP*. RFC 2407, IETF, 1998.

[100] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246, IETF, 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*. RFC 4055, IETF, 2005.

[102] S. Turner, D. Brown, K. Yiu, R. Housley, and T. Polk, *Elliptic Curve Cryptography Subject Public Key Information*. RFC 5480, IETF, 2009.

BIOGRAPHIES

S. M. Suhail Hussain (M'13) received his Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India in 2018. He is currently AIST Postdoctoral Researcher at Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, Japan. His research interests include power system communications, cybersecurity in power systems, substation automation, IEC 61850 standards, electric vehicle integration and cyber-physical energy systems.

Dr. Hussain is Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. He was a recipient of IEEE Standards Education Grant approved by the IEEE Standards Education Committee for implementing project and submitting a student application paper in 2014-15.

Taha Selim Ustun (M'04) received his Ph.D. degree in electrical engineering from Victoria University, Melbourne, VIC, Australia. Currently, he is a researcher at Fukushima Renewable Energy Institute, AIST (FREA) and leads Smart Grid Cybersecurity Lab. Prior to that he was an Assistant Professor of Electrical Engineering with the School of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. His research interests include power systems protection, communication in power networks, distributed generation, microgrids, electric vehicle integration and cybersecurity in smartgrids. Dr. Ustun is an Associate Editor of the IEEE ACCESS and Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. He is a member of IEEE 2004, IEEE 2800 Working Groups and IEC Renewable Energy Management Working Group 8. He has edited several books and special issues with international publishing houses. He is a reviewer in reputable journals and has taken active roles in organizing international conferences and chairing sessions. He has been invited to run specialist courses in Africa, India and China. He delivered talks for Qatar Foundation, World Energy Council, Waterloo Global Science Initiative and European Union Energy Initiative (EUEI).

Akhtar Kalam is a Professor at Victoria University (VU), Melbourne since 1985 and a former Deputy Dean of the Faculty of Health, Engineering and Science. He is currently the Head of Engineering and Director of Externalization at the College of Engineering and Science, VU. He is also the current Chair of the Academic Board and lectures in the Masters by coursework program in the Engineering Institute of Technology, Perth, Australia. Again he is the Editor in Chief of Australian Journal of Electrical

& Electronics Engineering. Further he has Distinguished Professorship position at the University of New South Wales, Sydney, Australia; MRS Punjab Technical University – Bhatinda, India; Crescent University – Chennai, India; VIT – Vellore, India and 5 Malaysian universities. He has wide experience in educational institutions and industry across four continents. He received his B.Sc. and B.Sc. Engineering from Calcutta University and Aligarh Muslim University, India. He completed his MS and Ph.D. at the University of Oklahoma, USA and the University of Bath, UK. His major areas of interests are power system analysis, communication, control, protection, renewable energy, smart grid, IEC61850 implementation and co-generation systems. He provides consultancy for major electrical utilities, manufacturers and other industry bodies in his field of expertise. Professor Kalam is a Fellow of EA, IET, AIE, a life member of IEEE and a member CIGRE AP B5 Study Committee.