Australasian Universities Power Engineering Conference, AUPEC 2020, Hobart, TAS, Australia, 29 November – 3 December 2020

Communication and Information Security Assessment of a Digital Substation

Joevis J. Claveria and Akhtar Kalam
College of Engineering and Science
Victoria University
Melbourne, Australia
joevis.claveria@live.vu.edu.au
akhtar.kalam@vu.edu.au

***Abstract*— The Internet of Things (IoT) has enabled the rapid pace of the use of communication technology and infiltration of technical systems in a digital world. In terms of power systems generation and operation, a reliable solution for substation automation and smart grid communication is the IEC 61850 standard. It has a robust modelling structure for monitoring, protection, and control and management systems in substations and across the grid. Modern communication technologies are destined for internet use for remote monitoring, settings, and data recovery. However, the communication network is exposed to cyber threats and evident risks in security defense of automated power systems. To tackle these vulnerabilities, the IEC 62351 standard aims to improve security in handling the communication and data transfers in power system automation. This paper discusses the different security measures in communication, information and cyber security solutions in power systems. To further illustrate the novel communication and security schemes of digital substations, a case study using the Victoria University Zone Substation (VUZS) simulator for cybersecurity assessment has been instigated.**

Keywords - IEC 61850; Generic Object-Oriented Substation Events (GOOSE), Manufacturing Message Specifications (MMS), Sampled Value (SV), IEC 62351; Communication Security; Information Security; Cyber Security

Introduction

The deployment of IEC 61850 standard protocols has been widely recognised and used in digital substation and smart grid applications for a more reliable and efficient form of communication protocols. This allows the smart equipment Intelligent Electronic Devices (IEDs) to communicate in high-speed peer-to-peer communication through GOOSE messaging in the substation [1]. The IEC 61850 protocols use Ethernet and optical fibre cables as a medium of communication among the protective relays. This eliminates or lessens the use of standard hardwired copper wires in the system.

Switch-based Ethernet network manages the communication better than hubs in real-time communication. This shows that a data link layer is more reliable than a physical layer in terms of handling real-time data communication. Industrial Ethernet has dominant and high-speed properties which make it an interesting communication technology for substation automation [2]. On the other hand, optical fibre technology is used as a sensor for real-time line current monitoring on various locations in power systems. It is used for fault detection in protective devices without relying on coordination curves of time-current [3]. The optical fibre connection enables clean and fast communication of data which has an electromagnetic immunity in the event of surges. These days, optical fibres are used for extremely high-speed data transfer over long distances for industrial controls and power systems automation.

However, this communication network is exposed to cyber threats and risks through physical layer connection (Ethernet, optical fibre, etc.). To mitigate the risks and vulnerabilities in the communication network, the IEC 62351 standard is utilised. The IEC 62351 standard was developed by IEC TC57 (Working Group 15) for the purpose of securing the transmission of data across the network. The security objectives include data authentication, and detection of intrusion, eavesdropping and spoofing. The IEC 62351 standard is not limited to securing the communication protocols of IEC 61850 but also of other standards such as IEC 60870 and others [4].

I. Communication and Information Systems Standard

A. *Communication Protocol Standard*

Communication protocols are the most critical and important parts of power system operations in transmitting and receiving information from different levels of a substation. Despite its significance, until now, communication protocols are rarely incorporated with cyber security and security measures against disturbances and power and equipment failures [5]. These threats are common to different communication protocols if the transmission of data is unsecured. Power utilities now clearly understand the risks and chaotic results of unsafe data. **Figure 1** illustrates the evolution of most common IED communication protocols that are widely used in the substation environment. These are the Modbus, Distributed Network Protocol 3 (DNP3), IEC 60870, Utility Communication Architecture (UCA) and the IEC 61850 [6].

- Modbus – Master / Slave protocol (Request/Reply)
- DNP3 – widely used in North America and uses Master / Slave protocol
- IEC 60870 – widely used in European countries for SCADA, etc.
- UCA - Basis for IEC 61850
- IEC 61850 – Communication protocol for substation automation

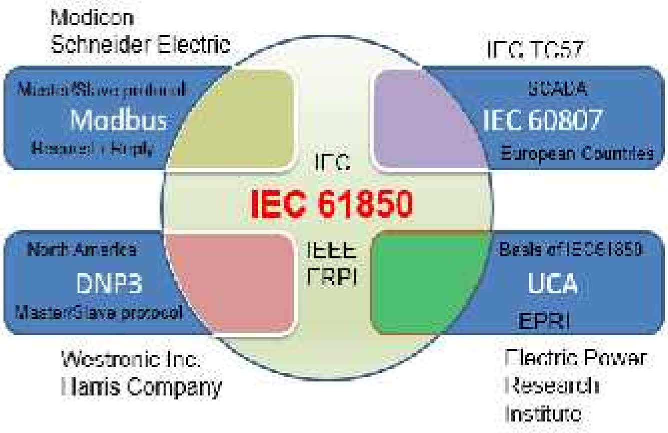

Figure 1: Communication Protocol Standards

B. *Communication Security Mechanisms of Power Systems*

The development of information and communication technology has been at the forefront of every enterprise in the digital age, from banking and finance, national security, health systems, telecommunication systems, energy and power industry, and many more. However, the application of information and communication technology in the market leads to data and information breaches on the internet. Information must be secured during operation, application and transmission of data. Due to alarming threats to and cyber-attacks of electrical grid and power plants in the power industry, information and communication security has become necessary. The focus lies on the security of information, networking and cybersecurity.

1. *Information Security*

It is a process of securing all forms of information – from electronic, paper print documents, other forms of confidential evidence such as private or sensitive data, and even information in people’s heads – that need protection from unauthorized access, use, disclosure, modification, disruption, and destruction.

2. *Network Security*

It is a process of securing the software and hardware underlying the networking infrastructure of a system, as a preventive measure for protection of computers, users, and programs from unauthorized access, use, modification, destruction and improper disclosure. It is also a configuration designed to protect the confidentiality, integrity and accessibility of computers either in public or in private networks.

3. *Cyber Security*

It is a process of securing the network systems and programs from threats and digital attacks during transmission and receiving of digital information across the internet. Unauthorized attack could be carried out to infiltrate sensitive information to extort money from users, destroying evidence, modifying status, and interfering in normal business processes.

C. *Sources of Cyber Threats and Attacks*

Cyber-attacks are progressively becoming sophisticated and are evolving threats to restricted areas such as government infrastructure, power utilities and large network organizations. However, these threats and attacks can be intentional or unintentional, and can come from – but are not limited – to the following sources [7] [8]:

- espionage and information warfare
- political activism
- foreign nations engaged in crime
- organization insider and corporate attacker
- unintended mistake of employee due to lack of training
- recreational hackers, virus writers and crackers
- criminal groups and terrorists
- internet threats such as viruses, spywares and worms

These sources of threat and attack may vary in terms of their motives and capabilities. Some may have different attack techniques that may adversely affect the operations of an organization or industry.

II. Safety Assessment Method of Power Systems

A. *Fault Tree Analysis (FTA)*

Fault tree analysis is a type of analysis based on possible sources of faults or accidents that lead to system failure. This method is a top to bottom empirical analysis that branches out downwards and illustrates a logical diagram of events like leaves and demonstrates a step by step logical relationship to find the events that cause a fault or undesired result.

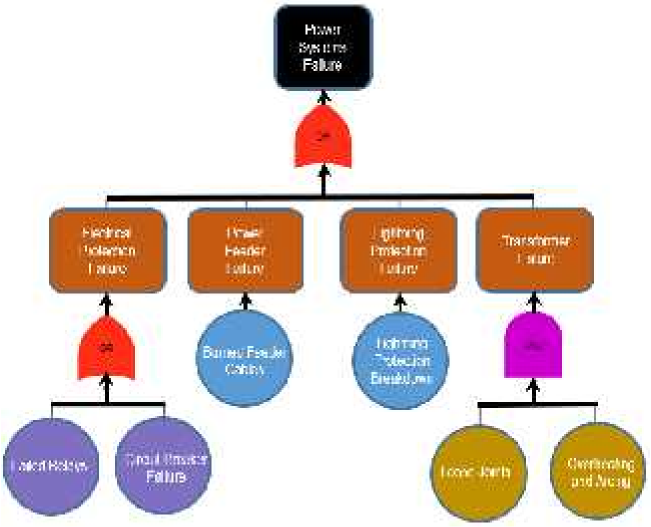

Figure 2: Fault Tree Analysis on a Power System Failure

Figure 2 illustrates a simple power system failure based on a fault tree analysis. The analysis starts from top to bottom – What caused the power system to fail? What were the possible sources of faults or accidents? Was it an electric protection failure, power feeder failure, lightning protection failure or transformer failure? What were the underlying events that caused the faults? Was it failed relays or circuit breakers that caused the electrical protection system to fail? Or was it due to the blend of loose connection and overheating of the wire that caused the transformer to fail? These are the basic procedures in analysing a fault tree scheme. Basically, it is based on a deductive type of reasoning that is compliant leading to a critical analysis of an undesired state of event.

Cao *et al* (2010) [9] proposed a method by illustrating a case study using a power distribution system with multiple outputs and outlining the weak parts in the fault tree. The method illustrates that the systems unreliability is directly associated with the systems component. Langer *et al* (2016) [10] conducted a risk assessment using event tree analysis on cyber physical attacks on a smart grid. The case study focused on the voltage controller of the power systems that could be exploited, leading to incorrect readings of the line voltage being sent to power equipment and Distributed Energy Resources (DER) that caused them to go off the safety limit.

One of the weaknesses of the fault tree analysis is the creation of the logical fault tree diagram. The larger the fault tree, the higher the difficulty and complexity in finding the events fault.

B. *Attack Tree Analysis (ATA)*

Attack tree analysis is a method of investigating an attack using a conceptual diagram and modelling a threat in a system. In the attack tree, the root node indicates the status of the node being attacked while the leaf node represents the purpose of the attack. ATA has been used in different applications, one of which is the use of control systems relating to smart grids. ATA exposes security threats in attacks, which can be mitigated when properly addressed.

Ten *et al* (2007) [11] proposed a method using attack trees to systematically evaluate the susceptibility and enhancements of cybersecurity for SCADA systems. The case study illustrated the capability of the attack tree method as a penetration testing of an attack, assessment of security flaws and confirmation of hypothesis. Li *et al* (2010) [12] presented a hydroelectric power plant model case study to demonstrate the vulnerability of industry control computers and that electric power devices in the system can be manipulated. Thus, the attack tree was constructed to mitigate flaws of a network and prevent future occurrences.

Attack trees can mitigate and predict faults during an event. This process offers clarity and transparency in decision making.

III. Communication and Security Schemes for Power Systems

A. *IEC 61850 Standard Communication Protocol*

IEC 61850 has an all-inclusive structure, and abstract data models that can be defined and mapped to different protocols. These data models can be mapped to GOOSE, MMS and SV. **Figure 3** shows the communication protocol of IEC 61850 being mapped and stacked based on the Open System Interconnection (OSI) model. The OSI network layer model [13] [14] is classified into parts, the data / information processing and communication functions.

The communication stack mapping in **Figure 3** shows the GOOSE and SV protocols being mapped directly via high-speed messaging on LAN thru Ethernet. The network transmission implies that data messages carried out are of a high level of importance, such as time-critical protection relaying, interlocking data between IEDs, alarms, signals and others. Both the GOOSE and SV are under the layer 2 multicast which means that it skips other data and communication layers for immediate processing. The MMS is present in most devices for operational reporting and monitoring functions. MMS is positioned through the Transmission Control Protocol /Internet Protocol (TCP/IP) stack which means the transmission of data is not of high importance.

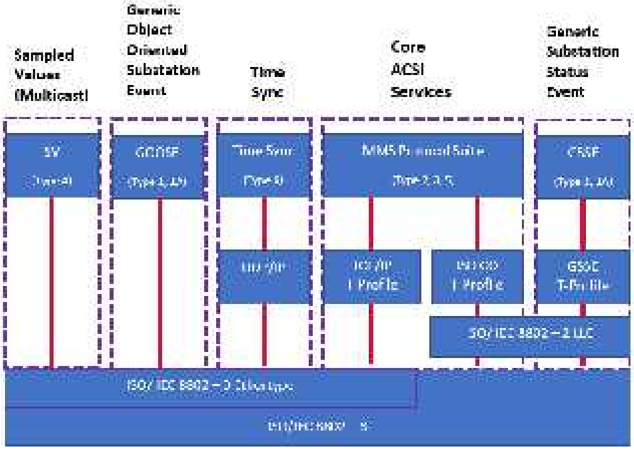

Figure 3: IEC 61850 Communication Protocol Stack [15]

B. *IEC 62351 Security Standard*

IEC 62351 standard has the specific details to carry out a task in securing the three most important communication protocols of IEC 61850, the GOOSE, MMS and SV [4].

IEC 62351 – 3 – Security for any profiles including TCP/IP
- Transport Layer Security (TLS) Encryption
- Node Authentication using x.509 certificates
- Message Authentication

IEC 62351 – 4 – Security for any profiles including MMS
- Authentication for MMS
- TLS to provide transport layer security

IEC 62351 – 6 – Security for IEC 61850 profiles
- VLAN mandatory for GOOSE
- Simple Network Time Protocol (SNTP)
- Message Authentication

With these types of security under IEC 62351, researchers are moving forward to develop a new security scheme for IEC 61850 and other standard protocols. Recent publications proposed an improved security scheme for MMS [16], SV and GOOSE messaging [17] [18]. The results of the study verify that successful authentication, and management of keys and certificates in communication protocols can be safely used in the substation [19].

IV. Cybersecurity Assessment of a Digital Substation: A Case Study

Power systems are one of modern digital society's most complex and vital infrastructures, acting as a backbone for economic activities. More and more models have been studied regarding information and cyber security for digital substations, especially now that the IEC 62351 standard is extensively used to secure the IEC 61850 communication protocols. Understanding their effect on cyber-attacks is a critical problem in the evaluation of security risks.

An assessment of information and cyber security is being conducted in the Victoria University Zone Substation (VUZS) Simulator [6]. **Figure 4** presents the single line diagram of the VUZS simulator.

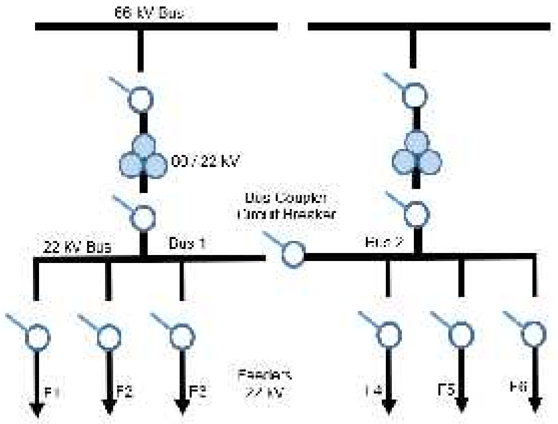

Figure 4: VUZS Simulator Single Line Diagram

A digital substation is associated with IED relays distributed to protect and control the whole substation so that no part of the substation is left unprotected. IED relays are controlled and monitored through a sophisticated protection scheme.

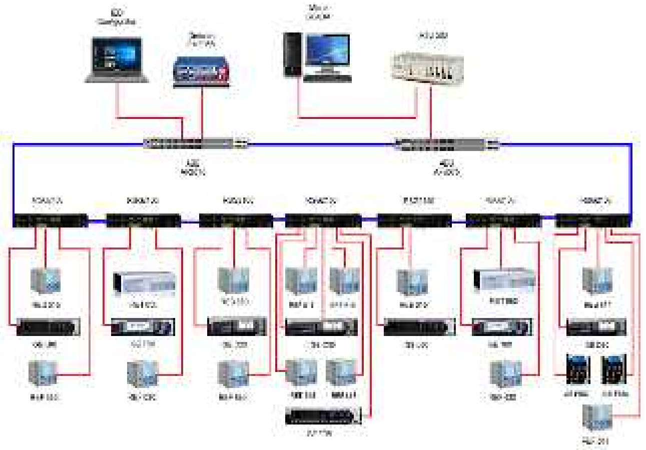

Figure 5: VUZS IED Protection and Control Scheme

Figure 5 illustrates the sophisticated protection and control scheme of the VUZS simulator. Unfortunately, the VUZS simulator deals with station and bay level only. The process level is emulated using real time digital devices to produce sampled values injected to the IEDs and into other parts of the system.

To gain a better standing of cyber security in a substation, a case study was instigated to assess the weaknesses, vulnerabilities, and counter measures in securing the communication protocols of the IEC 61850 standard.

A. Application of Security Measures

There are simple security measures and techniques that can be implemented inside a substation environment. For instance, personnel working in the station level must be knowledgeable in computers and know the substation process. Personnel working on SCADA and HMI must be properly oriented and must abide with the security policy of the organization. An inclusion of a Graphical User Interface (GUI) for security measures like biometrics and others will make computer access more protected. On the side of Operating Systems (OS), the CTRL-Alt-Del combination keys is called a secure attention key. This implies trust in the integrity of the systems in filling-up a password in a real log-in form. The station level must be protected and secured appropriately due to the severity of contained information.

GOOSE messages are sent from a publisher IED to multicast configured users known as subscriber IEDs. The GOOSE messages sent by the publisher do not need an acknowledgment acceptance coming from the subscriber. A security breach can be recognized when a GOOSE message being re-transmitted shows that the status and sequence number parameters have changed. On the other hand, the MMS uses Transport Layer Security (TLS) protocol to secure the transmission of data between a client/server. The TLS retains the integrity, authenticity, and confidentiality of the data transferred.

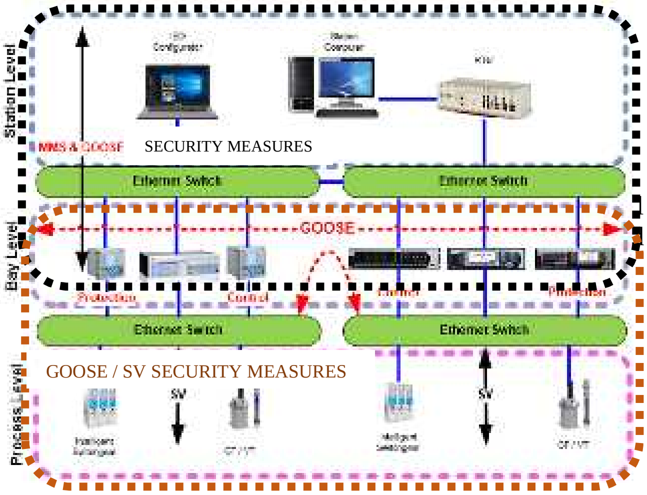

Figure 6: IEC 61850 Substation Architecture

Figure 6 illustrates the flow of the GOOSE, MMS, and SV protocols across the substation and their limitations. This shows where the security measures for the GOOSE, MMS and SV will be implemented in the substation.

B. Attack Tree Modelling in a Digital Substation

In the field of information technology, attack tree modelling is used to analyze potential threats and attack paths against a specific system.

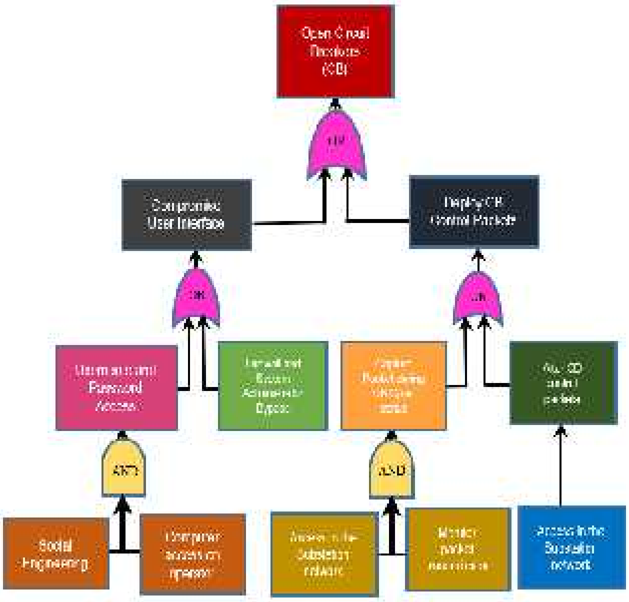
Open Circuit Breakers (CB)
OR
Compromise User Interface
Deploy CB Control Packets
OR
OR
Password Access
AND
AND
Social Engineering
Access in the Substation network

Figure 7: Attack Tree Analysis of a Digital Substation

However, attack tree modelling can be extended and applied to other structures such as power systems in the electrical sector. **Figure 7** illustrates an attack tree model for the VUZS simulator. The main goal for the attack is to open a circuit breaker which is the root node. The leaf nodes contain sub goals or stages of events that can be executed to achieve the final goal. Attack tree models are analyzed generally from the bottom to top. This will give the operators ability to mitigate threats and attacks, and efficiently identify the relevant intrusion events in a power system control network.

C. Message Authentication Code (MAC) Methodology

The MAC is used to verify the validity and consistency of a message coming from a sender.

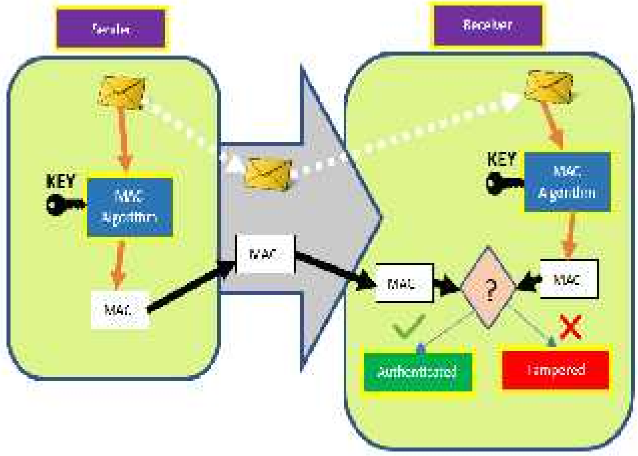

Figure 8: MAC Authentication Method

Figure 8 shows the process of MAC authentication method. The sender IED will send a GOOSE message to a MAC algorithm and will generate a secret key. The GOOSE message and the new generated MAC are sent through an Ethernet link to the IED receiver. The IED receiver will also generate its own MAC with the same key from the IED sender. If the MAC of the receiver is the same as the sender, the GOOSE message will be processed accordingly. Otherwise, the GOOSE message will appear to be tampered during transmission and will be discarded.

D. Application of Python Programming Language and Wireshark Packet Analyzer in the Case Study

The Wireshark software will be used to analyze the packets from the communication protocols, GOOSE, MMS, and SV. The packets of the GOOSE message will be monitored from the physical ports of Ethernet and wireless network. The GOOSE message will be decoded using Basic Encoding Rules (BER) and other available tools for decoding. The MAC authentication can be written with a Python script which contains data and code for secret key generation.

1. Python Programming Language

Python is a universal open source programming language which supports multiple user interface design models. The structure is based on concept of "objects" which contains data and code. The Python program has a wide range of standard library tools that support several formats and protocols for automation and networking applications.

Cui *et al* (2018) [20] used a Python-based software called ANDES to bridge the gap between power system analysis and cybersecurity performance. The method used is suitable for research and implementation of cyber-physical power system simulation. Adhikari *et al* (2017) [21] developed a test bed using a real time digital simulator for hardware and software combined with Python and other programming languages. The design was to model realistic power system eventualities and cyber-attacks using a script to capture the data from the system.

Python and other programming languages have their strength and weaknesses in terms of their suitability and functionalities. However, Python contains multiple packages with a range of functionality from automation, networking, graphical user interface and many more.

2. Wireshark Packet Analyzer

Wireshark is a free and open source packet analyser that can capture live packet data from a network interface and is used for troubleshooting network faults, errors and for communication protocol analysis. It can also save and display packet, search, filter and create various statistical packets in the network.

Wang *et al* (2010) [22] used Wireshark to analyse TCP/IP protocols using a request and reply function in the network. The detailed characteristics of a packet data, physical address, packet framework, and transmission of data were investigated. Yang *et al* (2015) [23] built a comprehensive testbed to investigate the impact and vulnerabilities of cyber-attacks on IEC 61850 based substations. The testbed tested an IED communication protocol, from end to end testing of cyber-attacks through packet length analysis of Wireshark.

V. Conclusion

The IEC 62351 standard is still in its infancy stage in handling the communication and information security of the IEC 61850 standard protocol. The GOOSE, MMS and SV are critically vulnerable during transmission and application of messages across the substation. To further address these security challenges, a case study was initiated to illustrate the importance of fault and attack tree methods in effectively mitigating intrusion and detecting event anomalies in a substation. Furthermore, an authentication method for MAC was also projected in generating a secret key using a Python script which contains data and code. For packet analysis, Wireshark was chosen due to its popularity and capability for various statistical packet analysis in a network. The assessment has a practical significance in communication and cybersecurity modelling of security, control and protection of IEDs in a digital substation.

VI. Bibliography

Joevis Claveria received his Master of Engineering from Victoria University, Melbourne, Australia in 2014. He is currently pursuing his Doctor of Philosophy (Ph.D.) in Engineering - in Power Systems, Cybersecurity and Substation Automation at Victoria University, Melbourne. His key interests include renewable energy, industrial automation systems, distributed generation and power systems protection.

Akhtar Kalam completed his Master's in Science (M.S.) from the University of Oklahoma, Norman, and Doctor of Philosophy (Ph.D.) from the University of Bath, Bath, U.K. He has been actively engaged in teaching of power systems for more than 30 years in Victoria University, Australia and overseas. He has conducted research, provided consultancy on power system protection and independent power generation systems in Australia and overseas. His major areas of interest are power system analysis, communication, control and protection, and cogeneration systems.

VII. References

[1] L. Sevov, Z. Tony W and I. Voloh, "The Power of IEC 61850: Bus-transfer and Load shedding Applications," *IEEE Industry Application Magazine* , no. JAN/FEB, pp. 60 - 67, 2013.

[2] T. Skeie, S. Johannessen and C. Brunner, "Ethernet Substation Automation," *IEEE Control Systems Magazine,* vol. 22, no. 3, pp. 43-51, June 2002.

[3] C. T. Law, K. Bhattarai and D. C. Yu, "Fiber-Optics Detection in Power Systems," *IEEE Transactions on Power Delivery,* vol. 23, no. 3, pp. 1271-1279, July 2008.

[4] IEC-TC57, "IEC 62351: Power Systems management and associated information exchange - Data and communications security - PArt 6: Security for IEC 61850," International Electrotechnical Commission, 2007.

[5] F. M. CLeveland, "IEC 62351-7: Communications and Information Management Technologies - Network and System Management in Power System Operations," in *IEEE/PES Transmission and Distribution Conference and Exposition*, Chicago, Il, USA, 2008.

[6] J. Claveria and A. Kalam, "GOOSE Protocol: IEDs Smart Solution for Victoria University Zone Substation (VUZS) Simulator Based on IEC 61850," in *IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC),* Kota Kinabalu, Malaysia, 2018.

[7] G. C. Wilshusen, "U.S. Government Accountability Office," 24 April 2012. [Online]. Available: https://www.gao.gov/products/GAO-12-666T. [Accessed 13 April 2020].

[8] A. Hadbah, A. Kalam and A. Zayegh, "Powerful IEDs, Ethernet Networks and their effects on IEC 61850-based Electric Power Utilities Security," in *Autralian Universities Power Engineering Conference (AUPEC),* Melbourne, Australia, 2017.

[9] K. Cao, K. Xie and B. Hu, "Unreliability Tracing Technique for System Components Based on the Fault Tree Analysis," in *2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems*, Singapore, 2010.

[10] L. Langer, P. Smith, M. Hutle and A. Schaeffer-Filho, "Analysing cyber-physical attacks to a Smart Grid: A voltage control use case," in *2016 Power Systems Computation Conference (PSCC)*, Genoa, Italy, 2016.

[11] C. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems using Attack Trees," in *2007 IEEE Power Engineering Society General Meeting*, Tampa, Florida, 2007.

[12] W. Li, J. Huang and W. You, "Attack modeling for Electric Power Information Networks," in *2010 International Conference on Power System Technology*, Hangzhou, 2010.

[13] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications,* Vols. COM-28, no. No. 4, pp. 425-432, 4 April 1980.

[14] J. D. Day and H. Zimmermann, "The OSI reference model," *Proceedings of IEEE,* vol. 71, no. 12, pp. 1334-1340, Decemeber 1983.

[15] I. 61850, Part 8-1: Specific Communication Service Mapping (SCSM) –Mapping to MMS (ISO 9506-1 and ISO 9506-2), First Edition: IEC, 2004.

[16] T. S. Ustun and S. M. S. Hussain, "An Improved Security Scheme for IEC 61850 MMS Messages in Intelligent Substation Communication Networks," *Journal of Modern Power Systems and Clean Energy,* in press.

[17] J. Zhang, J. Li and e. al, "A security scheme for intelligent substation communications considering real-time performance," *Journal of Modern Power System and Clean Energy* , vol. 7, no. 4, pp. 948-961, 2019.

[18] S. M. Farooq, S. M. S. Hussain and T. S. Ustun, "Performance Evaluation and Analysis of IEC 61850-6 Probabilistic Signature Scheme for Securing GOOSE Messages," *IEEE Access,* vol. 7, pp. 32343-32351, 2019.

[19] S. M. S. Hussain, T. S. Ustun and A. Kalam, "A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges," *IEEE Transactions on Industrial Informatics,* 2019.

[20] H. Cui and F. Li, "ANDES: A Python-Based Cyber-Physical Power System Simulation Tool," in *2018 North American Power Symposium (NAPS)*, Fargo, ND, 2018.

[21] U. Adhikari, T. Morris and S. Pan, "WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining," *IEEE Transactions on Smart Grid,* vol. 8, no. 6, pp. 2744-2753, 2017.

[22] S. Wang, D. Xu and S. Yan, "Analysis and application of Wireshark in TCP/IP protocol teaching," in *nalysis and application of Wireshark in TCP/IP protocol teaching," 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, Shenzhen, 2010.

[23] Y. Yang and e. al., "Cybersecurity test-bed for IEC 61850 based smart substations," in *2015 IEEE Power & Energy Society General Meeting*, Denver, 2015.