ISSN No.: 2454- 2024 (online)

International Journal of Technical Research & Science

# IEC61850: a Lingua Franca for Substation Automation Systems

**Sajad Amjadi*, Akhtar Kalam**
Sajad.AmjadiZeynalhajelo@vu.edu.au
College of Engineering and Science
Victoria University
Melbourne, Australia

**Abstract**-The last few years has seen numerous studies pointing to the IEC61850 as a worthwhile international standard for substation automation systems. The standard incorporates the use of logical nodes to resolve problems related to interoperability and interchangeability in multi-vendor zone substation systems. The standard also initiated a cost-effective Generic Object Oriented Substation Event (GOOSE) messaging technology to replace the traditional copper wiring. This paper provides a synopsis of communication protocols and their development over the time. The authors elucidate core elements of telemetry communications, structures of protocols and the significance of standards for communication protocols within substation automation systems. This paper aims to endorse and publicise the IEC61850 protocol as the latest and improved communication standard opposed to other substation protocols like DNP and Modbus.

**Index Term-** Generic Object Oriented Substation Event (GOOSE), Interoperability, IEC61850 Standard, Substation Automation Systems (SAS).

## 1. INTRODUCTION

Over the past decades power protection systems have seen numerous studies due to the host of critical equipment such as IEDs in Substation Automation Systems. An appropriate and well-designed communication structure is required to make these intelligent devices interconnect and exchange data. This has categorised communication technology as one of the crucial contributing factors to guarantee unfailing, reliable and cost-effective protection systems. Therefore, development of a robust and reliable protocol for communication applications has grown into a foremost objective in power communication and protection systems.

## 2. PROTOCOLS

When language is a media for communication, there is a need of systematic rules to follow in order to achieve the communication between parties [1]. A protocol plays the role of a rulebook prepared with a chain of instructions to help two or more communication parties talk to and understand each other.

Communication in a multi-vendor environment, a place where devices come from different vendors, often is causing challenges due to the use of multi-language technologies in programming of vendors' devices. Overcoming to this problem requires an expensive interface for communication applications. The International Standard Organisation Network Model known as OSI (Open System Interconnection) introduced a 7 network-layered hierarchy to show how data is transferred from one communication platform to another end and vice versa (Fig. 2.1).

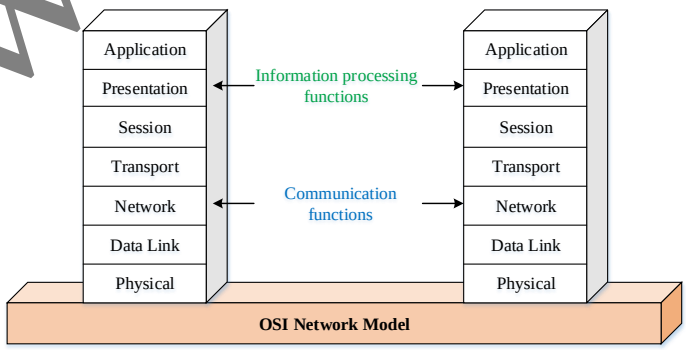


**Fig. 2.1 OSI 7 network- layered hierarchy [2]**

- Application layer provides a cluster of interfaces to be utilised for getting access to network services.
- Presentation mainly transforms the data of application into a generic framework for network broadcasting and vice versa.
- Session layer allows two communication parties to maintain ongoing exchange of data across a network.

- Transport layer is to manage the data transmission over the network.
- Network layer converts logical network address into the format to be used within physical devices and also controls the addressing for message delivery.
- Data Link layer initiates specific data frames between the Physical Layer and the Network.
- Physical layer converts data format from bit into signals to be sent as outgoing messages and vice versa.

### 2.1 Modbus

Modbus is a client/server massaging protocol located in application layer of OSI Network Model [3]. It supports different types of physical layers categorised in OSI. Modbus was originally introduces by Modicon (now Schneider Electric) in 1976 to support different fields of applications such as: industrial automation, infrastructure, and substation automation and transportation applications. Modbus makes the use of master/slave structure to establish communication between devices connected together. One of the advantages of Modbus protocol is that the flow of data exchange can be either from client to server or vice versa [3].

Modbus is also known as master/slave protocol which works with request/reply rule. In order to perform the request/reply operation in Modbus based systems, two different types of frames namely: Application Data Unit (ADU) and Protocol Data Unit (PDU) are initiated [4]. PDU includes a code specifying the function to be operated and ADU provides the information to be used for PDU operation. The process of exchanging data starts by initiating a command which contain both ODU and ADU frames and ends by receiving a response packet from client (Fig. 2.2).

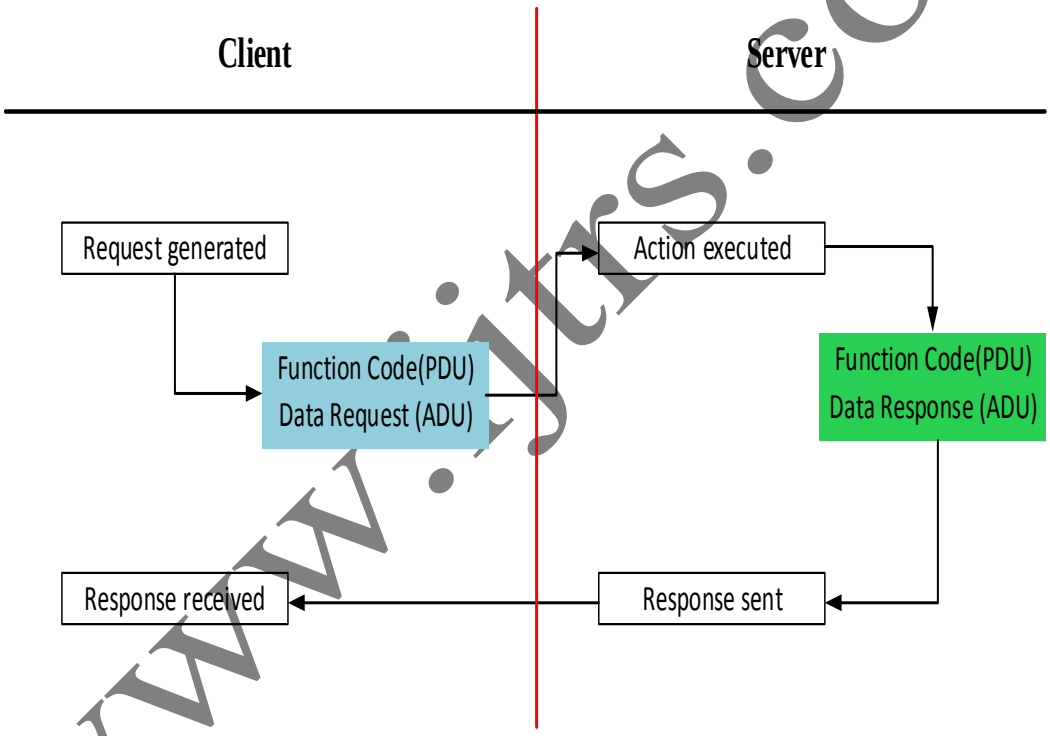


**Fig. 2.2 Client/Server data exchange in Modbus protocol** [4]

Modbus is designed with combination of layered protocols, such as Modbus RTU (Remote Terminal Unit) and Modbus TCP/IP (Transmission Control Protocol/Internet Protocol), to offer a trustworthy data exchange mechanism between microprocessor based devices. Modbus RTU employs the serial physical layer using RS232 or RS485, to transfer data between devices [5]. The disadvantage of Modbus RTU is its limit to transfer different types of information. The information packets that can be sent through Modbus RTU are only data. This means that Modbus RTU is not able to exchange other types of parameters such as units, resolution, point name, status value, etc. These types of information require a modern Ethernet based protocols such as EtherNet/IP or IEC61850. Modbus protocol eliminated this drawback by introducing Modbus TCP/IP driver. Modbus TCP (Modbus Ethernet/IP) is well industry accepted protocol that utilises the Ethernet TCP/IP physical layer, the top level of the physical layer in OSI, to achieve the communication between devices [3]. Figure 2.3 illustrates the structure of Modbus communication network which employs Modbus TCP, Modbus RTU and RS232 Modbus RTU485 (Fig. 2.3).

**Modbus Communication Network Structure**

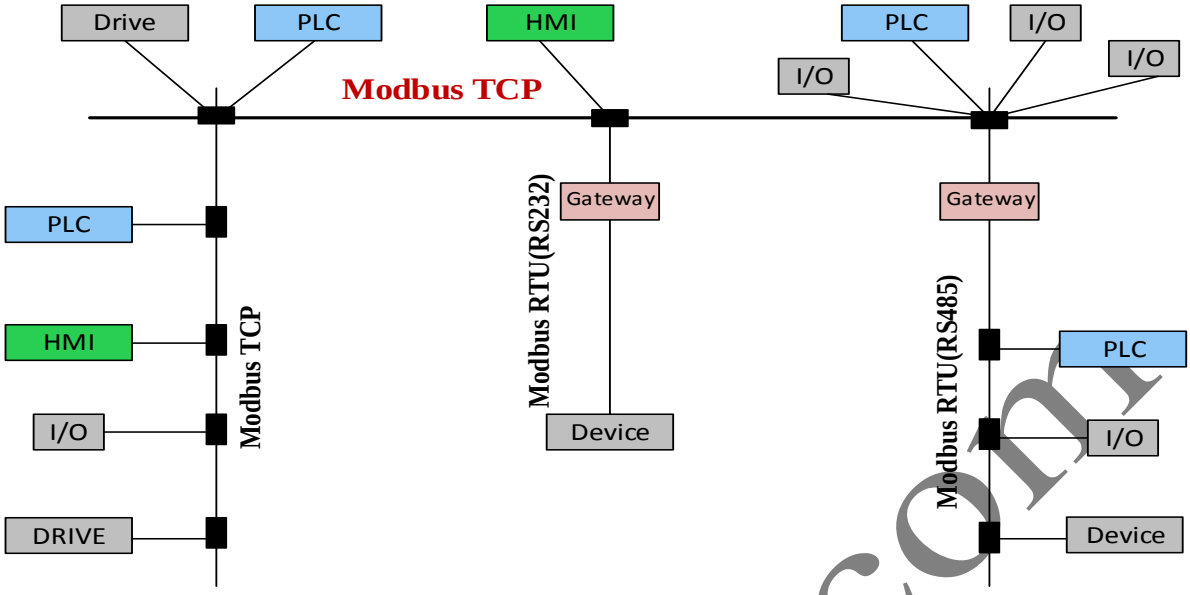


**Fig. 2.3 Modbus communication architecture** [3]

One of the challenges with Modbus protocol is the upgrading of Modbus devices from physical layer (RS232 or RS422) to Modbus TCP/IP (Ethernet layer). This requires a gateway device to convert the communication format from physical layer to upper layer such as Ethernet layer. This conversion causes an unwanted time delay in the process of function's operations.

In Modbus protocol based systems, server employs a controller as a middleware to collect data from other devices and send it to the master through programming panel or host processor. The controllers used by server also follow the master/slave communication architecture. The only difference between controller and server of Modbus is that, the controllers can only interact with one master simultaneously, whereas server can interact with master and controller at the same time.

In the recent decades Modbus TCP/IP is employed as one of the industry accepted standard to operate client/server based communication application [3]. In the context of substation automation it is used to monitor, supervise and control the performance of the intelligent devices- IEDs, Circuit breakers, Transformers- through a middleware gateway and controller. Although interoperability was one of the targets to achieve in Modbus, still there are many challenges and failure in a multi-vendor environment that Modbus fails to resolve them.

### 2.2 DNP3

Distributed Network Protocol (DNP3) is another open[1] and public communication protocol originally introduced by Harris, Distributed Automation Products in 1993 [6]. DNP3 located in second layer of OSI Network Model employing a series of communication protocols to achieve interoperability between devices under (IEC) Technical Committee 57 [6]. The DNP3 protocol is compliant with IEC 62351-5 and is mainly established as a standard for utilities including electrical and water industries. Despite Modbus protocol, it is not commonly used in other industries. DNP3 utilises SCADA to control and monitor the performance of intelligent devices through a Remote Terminal Unit (RTUI), also known as gateway, under master station/gateway/intelligent devices communication structure. One of the primary purposes of DNP3 was to provide a reliable protocol in terms of interoperability and long term stability. Therefore, network security and cyber security issues were not initially considered in the development of DNP3. This resulted in being easily attached and hacked by hackers and malevolent in smart grid application. This is due to the fact that smart grid is a platform runs by IP interfaces and provides open admission to third party to the IP infrastructure and physical network. Therefore failure to secure the IP infrastructure will cause series interruption and/or damage in the network. Therefore, DNP3 has been forced to resolve this drawback by adding secure authentication parameters to its architecture.

[1] Open architecture is an expression that describes an interoperable networks between software and hardware interfaces and accordingly between vendors.

The DNP3 protocol has been widely utilised by companies due to its numerous proven merits such as its efficiency, robustness and better interoperability compared to Modbus or older protocols. For instance, from the point of OSI Network Model, DNP3 is a layer 2 protocol whereas it supports layer 4, layer 5 and layer 7 of the OSI Network Model. This gives it superiority over Modbus protocol, positioned in Application Layer. Furthermore; in contrast to Modbus or other older protocols, Time synchronization is achieved for the first time using RTU in DNP3 protocol. It initiates a frame contains time stamped variation of data which are pulled out and transferred through RTU [2]. In addition; despite Modbus protocol, DNP3 is capable of communicating with multiple masters and pee-to-peer[2] communication simultaneously. Furthermore, DNP3 has the capacity of transferring different types of data in a single massage packet with a defined time frame.

### 2.3 UCA

It goes without saying that the developments of the Modbus and DNP3 protocols have been recognised as favourable achievements in the field of communication systems. These protocols have enabled utilities to implement their applications using open protocols with free of exorbitant charge access to their license. However, the drawback of these protocols is their complexity in terms of substation and instrument configuration. Due to a convoluted structure used by these protocols, configuration of an interoperable system in amulet-vendor environment substation was an irresistible time consuming procedure [7].

In addition, due to lack of restriction, vendors tend to implement their infrastructure using different communication protocols. Consequently, interoperability still remained an issue between vendors' intelligent devices and needed a huge amount of effort to tackle this problem. For instance, if devices as well as RTU from different vendors are configuring through different protocols, the peer-to-peer communication will be failed due to lack of understanding of the protocols used between devices [8]. Therefore, an idea of developing a framework to resolve these downfalls and eliminate the interoperability challenges resulted in introducing UCA (Utility Communication Architecture) as a systematic communication structure for utilities in 1990 [6, 9]. In the development of the UCA protocol, it is intended to make use of all "off-the shelf" existing protocols to achieve a friendly, reliable, flexible and robust protocol capable of fully supporting interoperability in a multi-vendor environment. The idea of splitting a massive problem into small pieces with defined detailed solution for each segment is used as an object-oriented model in UCA [9]. The object-oriented model of UCA describes the format, description and meaning of utility data in communication systems.

In UCA protocol, the Manufacturing Message Specification (MMS), is used to enable the SCADA performances using real-time data. The MMS is internationally standardised with IEC9509. It employs Application Layer of OSI Network Model. With the help of MMS mapping, a common based messaging format has been initiated which offers multiple range of services to the applications. For instance, it provides the operation of reading, writing, and reporting of variable, as well as downloading or uploading programs.

### 2.4 IEC61850

In recent decades, to a great extend interoperability have been a topmost challenge in a multi-vendor-based substation automation systems. Existing protocols were unable to fully warrant different vendor IEDs to communicate with one another[10, 11]. The reason behind this was that manufacturers purposely designed their products using their own proprietary tools, meaning customers had to favour one vendor more than another[2, 12]. In doing so, manufacturers practically configured their products in such a way that if one piece of equipment failed, then all or some accompanying devices required replacement. This was a major downfall for substations as a great deal of auxiliary equipment which was rather expensive needed to be stockpiled. Therefore, an urgent need for an international communication protocol as a Lingua Franca[3] has become an essential but hot topic for power protection and substation automation systems. The International Electrotechnical Committee (IEC) and IEEE worked together to advance the existing communication protocols for substation communication. The objectives were to achieve a protocol capable of free configuration, interoperability and long term proof interoperability and free configuration. As a consequence, the first version of IEC 61850 was announced in 2004 as an international standard which provides a detailed specification of layered substation automation architecture. The communication architecture is composed of abstract definition of classes and services which are independent of underlying concrete protocol stacks and deployment platforms. The protocol incorporates the use of logical nodes to resolve problems related to interchangeability, but also physical character mappings to overcome IED proprietary restrictions. The protocol does not describe any individual implementations, communication architectures or product functionalities. It instead focuses on the visible specifications of both primary and secondary equipment. The Second Edition of the IEC61850 Standard is published in 2014 which is encapsulated in a series of 20 documents spanning over ten parts.

[2] Peer-to-peer communication refers to the exchange of data directly between two devices where their functionality come with same capacity. There is no client/server order in the pee-peer-communication.

[3] Lingua Franca refers to a systematic common language to achieve communication or make exchange of data between two or more communication parties where they do not share a native (same) language.

## 3. IEC61850-based Substations' Architecture

IEC61850 has made use of the hierarchal substation automation structure to develop three levels namely: Enterprise or Station Level, Bay Level and Process level (Fig. 3.1).

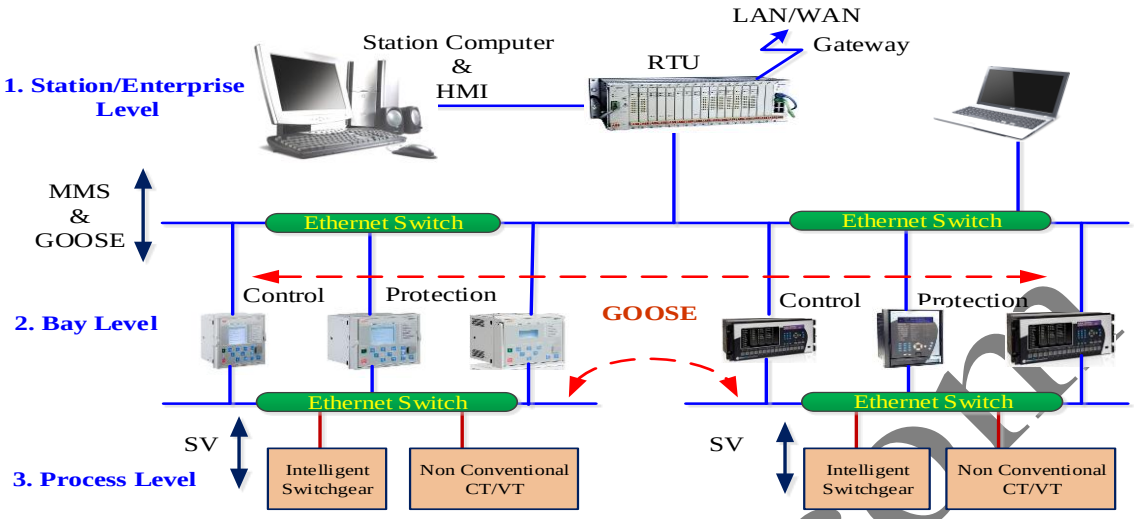


**Fig. 3.1 Architecture of an IEC61850-based substation [13]**

### A) Station Level

Station Level is used for the archiving, automation, data storage and management of countless bay level devices through the use of dedicated software tools. The hardware necessary to carry out such tasks is sheltered in a separate room away from all switchgear equipment. The station level allocates HMI computers, printers, modems, GPS receivers and Ethernet switches. The large storage capacity provided by these peripherals allows significant amounts of data files to be stored in real-time databases. These databases are continuously updated through station level modems, which act as a communications gateway to the Network Control Centre (NCC). The modems require physical coupling of Wide Area Networks (WAN), but also demand the presence of protocol converters capable of decoding incoming software commands [7].

### B) The bay level

The Bay Level connects a wide range of control and protections IEDs using station level Ethernet switches. The serial connection of these devices isolates various substation objects (i.e. lines and transformers) from the rest of the substation. These digitally manufactured IEDs have in-built LCD screens, push buttons and LEDs for the indication of measured data [7, 13]. Depending on the communication commands received from the station level, these IEDs are capable of performing functions such as bay control, bay protection, bay monitoring, and fault recording. All bay level automation systems are housed in standalone kiosks away from primary and secondary switchgear equipment [7, 13].

### C) The Process Level

The Process Level interlinks all primary and secondary switchgear equipment together with the substation automation systems located in the bay level kiosks. A large quantity of serial communication links are essential to carry out such manipulation, especially when connecting countless number of actuators, sensors, voltage transformers (VTs) and Resistance Thermal Detectors (RTD). The use of equipment that utilises both input and output (I/O) terminals is a clever way to reduce hardwiring in the process level.

### 3.1 Interoperability and SCL language

Prior to the standardization of the IEC61850 protocol, it was impossible for different vendor IEDs to communicate with one another. The reason behind this was that manufacturers purposely designed their products using their own proprietary tools, meaning customers had to favour one vendor more than another. In doing so, manufacturers practically configured their products in such a way that if one piece of equipment failed, then all or some accompanying devices required replacement. This was a major downfall for substations as a great deal of auxiliary equipment which was rather expensive needed to be stockpiled.

IEC61850-6 introduces XML-based Substation Configuration Language (SCL) as a common language to accomplish interoperability between devices. Accordingly different forms files using the common based language are brought together in part 6 of the IEC61850 standard. These files are as follows [14]:

- Description of Configured IED (CID)
- Capability Description of IED (ICD)
- Instantiated IED Description (IID)
- Description of System Exchange (SED)
- Description of Substation Configuration (SCD)

System Specification Description (SSD)

### 3.2 GOOSE Messaging in IEC61850-based Substations

The GOOSE message is the most important and beneficial feature of the IEC61850 Standard [15]. The GOOSE is a time critical message which is directly mapped onto the Ethernet, to make it fast and efficient. GOOSE works on a publisher/subscriber model, which means that the devices that have subscribed for this service can send and publish it as well (Fig. 3.6).

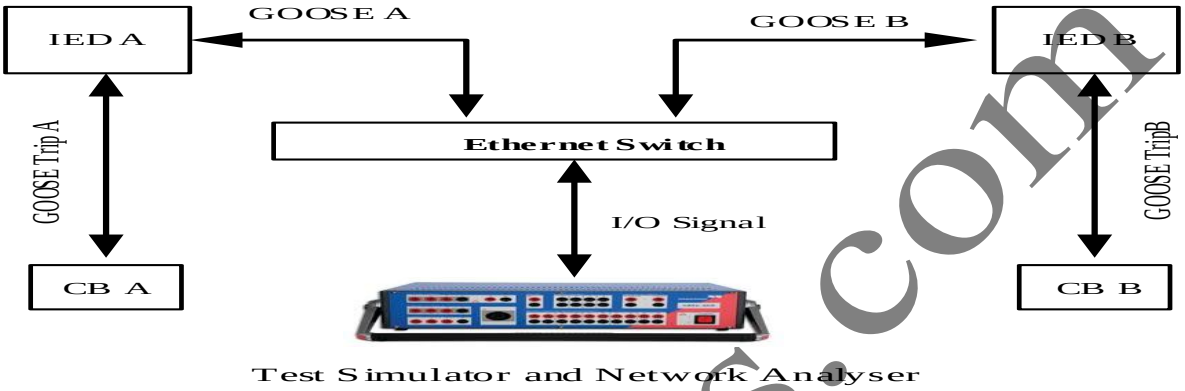


**Fig. 3.2 Peer-to-peer communication between IEDs via GOOSE messaging [14]**

Although GOOSE is already used in the UCA protocol, the IEC61850 GOOSE is a more advanced version of the UCA GOOSE message. The additional features are as follows:

- High level of flexibility
- Capability of either publishing or subscribing multiple messages from one IED
- Containing much more data attribute types (Boolean, BitString, Coded Enum, Integer, floating, etc.)
- Exchange of data is much faster
- Use for protection and control
- Messages are published by multicasting on the network.
- IEDs subscribe (or listen) to selected multicast messages
- Messages are sent or published periodically (heartbeat or maximum transmission time of 60s, 10s, 1s, etc.) under normal conditions

Messages are sent multiple times when an event occurs, following a transmission pattern until the maximum time is reached or until another event occurs.

## CONCLUSION

This paper emphasised the importance of an international communication protocol for substation automation. Over the past decades there has been a great deal of efforts to achieve a Ligula Franca for communication applications. However, this paper has shown that IEC61850 is more superior to other protocols endorse and publicise the IEC61850 protocol as the latest and improved communication standard opposed to other substation protocols such as DNP, Modbus and UCA due to numerous advantages that it has introduced such as cost reduction, GOOSE messaging and fully interoperability.

## REFERENCES

[1] J. Espina, T. Falck, A. Panousopoulou, L. Schmitt, O. Mülhens, and G.-Z. Yang, "Network topologies, communication protocols, and standards," in Body sensor networks, ed: Springer, 2014, pp. 189-236.

[2] A. Kalam and D. P. Kothar, Power systems protection and communications, First ed. Kent, UK: New Age Science Limited, 2010.

[3] I. Modbus, "Modbus application protocol specification v1. 1a," North Grafton, Massachusetts (www. modbus. org/specs. php), 2004.

[4] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES, 2011, pp. 1-7.

[5] W. S. Going, B. Thigpen, P. Chok, A. B. Anderson, and G. Vachon, "Intelligent Well Technology: Are we ready for closed loop control?," in Intelligent Energy Conference and Exhibition, 2006.

[6] A. W. Blackett, B. J. Gilbert, and M. A. Hancock, "Method and system for master slave protocol communication in an intelligent electronic device," ed: Google Patents, 2004.

[7] B. Stojcevski, "Implementation of the IEC61850 international protocol for accurate fault location in overhead transmission lines," College of Engineering and Science, Victoria University, Australia, 2013.

[8] C. Wester and M. Adamiak, "Applications of peer-to-peer messaging in industrial facilities," in Pulp and Paper Industry Technical Conference (PPIC), Conference Record of 2012 Annual IEEE, 2012, pp. 1-10.

[9] A. Bakhtar and M. Kooshavar, "Implementation of UCA Based Inter and Intra Substation Communication Architecture."

[10] I. Bermudez, A. Tongaonkar, M. Iliofotou, M. Mellia, and M. M. Munafò, "Towards automatic protocol field inference," Computer Communications, vol. 84, pp. 40-51, 2016.

[11] E. Udren, S. Kunsman, and D. Dolezilek, "Significant substation communication standardization developments," in 2nd Annual Western Power Delivery Automation Conference (WPDAC) Proceedings, 2000.

[12] B. Stojcevski and A. Kalam, "Fault Location in Overhead Power Lines Using the IEC61850 International Protocol," International Review on Modelling and Simulations (IREMOS), vol. 3, pp. 888-899, 2010.

[13] S. Amjadizeynalhajelo and A. Kalam, "Device Isolation in IEC61850 Based Substation Protection Systems," International Journal on Recent Technologies in Mechanical and Electrical Engineering (IJRMEE), pp. 43-48, 2015.

[14] S. Amjadi and A. Kalam, "IEC61850 GOOSE Performance in Real Time and Challenges Faced by Power Utilities," in PowerTech, 2015 IEEE Eindhoven, 2015, pp. 1-6.

[15] A. Apostolov, "To GOOSE or not to GOOSE?-that is the question," in Protective Relay Engineers, 2015 68th Annual Conference for, 2015, pp. 583-596.

**Sajad Amjadi** received the B.Sc. Engineering degree from University of Tabriz, Iran in 2008 and completed Master of Electrical and Electronic Engineering from Royal Melbourne Institute Technology (RMIT), Melbourne in 2011. He is a member of Engineers Australia and he is currently pursuing his PhD at Victoria University, Melbourne, in the area of Power Protection and Communication Systems, in particular designing the Victorian Zone Substation Simulator Centre based on IEC61850 standard under the supervision of Professor Akhtar Kalam. His area of technical expertise is power protection, SCADA, substation automation systems and IEC61850 in particular, GOOSE messaging technology.

**Akhtar Kalam** (MIEEE '1981) received the B.Sc. degree from Calcutta University, Calcutta, India, and the B.Sc. Eng. degree from Aligarh Muslim University, Aligarh, India, and M.S. from the University of Oklahoma, Norman, and Ph.D. degree from the University of Bath, Bath, U.K. His Ph.D. work focused on the application of distance protection to series-compensated extra high-voltage lines. He has been actively engaged in the teaching of power systems for more than 30 years in the College of Engineering and Science, Victoria University, and overseas. He has conducted research, provided consultancy, and has more than 450 publications on power system protection and independent power generation. His major interests are power system analysis, power system protection, zone substation and expert system application in power systems, cogeneration, and renewable energy.