An Overview of the Implementation Issues of IEC 61850 Based Substation Automation System (SAS)

Dr. Muhammad Uzair
Faculty of engineering, Islamic University of Medina, KSA
uzair91@hotmail.com, muzair@iu.edu.sa

Abstract: IEC 61850 standard has gained a tremendous popularity in substation automation after its emergence. Many research papers have been published highlighting the different features and benefits of the IEC 61850. The standard offers interoperability, easy configuration, less cost, and simple architecture. However, in order to avail these features and advantages, there are many challenges during practical implementation which has been discussed in this paper. Previous papers generally discuss about one or two issues, i.e., particularly implementation and security issues, but this paper comprehensively discuss all failures and technical challenges faced by IEC 61850 based substation automation system (SAS). The paper presents a detailed overview of different kinds of issues, i.e., practical implementation issues, structural issues in hierarchical layers, security issues, interoperability and interchangeability issues, communication challenges, planning, reliability, synchronization, availability, training and functional issues, manpower skills, and other issues, etc. The paper discusses issues and challenges which need to be taken into account and should be resolved before the implementation of the standard, i.e., the criticality of IEC61850 based communications in terms of data transfer, reliability, availability and efficiency. In order to get successful implementation, and complete advantage of the standard, it is very necessary to take into account the existing issues and address them before implementing the standard in a utility. The paper also discusses about the future of IEC 61850 standard, and shows that DNP 3 protocol is still very popular among utilities, especially in the North America. The paper also discusses its possible integration with Internet of Things (IoT). Finally, the paper presents a case study of substation with respect to end-to-end delay of time critical Sampled Values (SV) messages in an Ethernet and wireless environment. This study will help the user in understanding the substation primary plants, i.e., current/ voltage transformers (CT's/VT's), circuit breakers, etc., for substation automation, control and protection.

Key words - IEC 61850, SAS, IEDs, Issues, Failures

الخلاصة: اكتسب معيار IEC 61850 شعبية هائلة في أتمتة المحطات الفرعية بعد ظهوره. تم نشر العديد من الأوراق البحثية التي تسلط الضوء على الميزات والفوائد المختلفة لـ IEC 61850. يوفر المعيار إمكانية التشغيل المتبادل، والتكوين السهل، والتكلفة الأقل، والبنية البسيطة. ومع ذلك، من أجل الاستفادة من هذه الخصائص والمميزات، توجد هناك العديد من التحديات أثناء التنفيذ العملي التي تمت مناقشتها في هذه الورقة. تناقش الأوراق السابقة بشكل عام قضية واحدة أو قضيتين، أي على وجه الخصوص قضايا التنفيذ والأمن، ولكن هذه الورقة تناقش بشكل شامل جميع الأعطال والتحديات التقنية التي يواجهها نظام أتمتة المحطات الفرعية المرتكز على IEC 61850 (SAS). تقدم الورقة نظرة عامة مفصلة على أنواع مختلفة من القضايا، أي قضايا التنفيذ العملي، القضايا الهيكلية في الطبقات الهرمية، القضايا الأمنية، التشغيل البيني وقضايا التبادل، تحديات التواصل، التخطيط، الموثوقية، التزامن، التوافر، التدريب والقضايا الوظيفية، مهارات القوى العاملة، وغيرها من القضايا، وما إلى ذلك. تناقش الورقة القضايا والتحديات التي يجب أخذها بعين الاعتبار ويجب حلها قبل تنفيذ المعيار، أي أهمية الاتصالات القائمة على IEC61850 من حيث نقل البيانات والموثوقية والتوافر والفعالية. من أجل الحصول على التنفيذ الناجح، والاستفادة الكاملة من المعيار، من الضروري جدًا مراعاة المشكلات الحالية ومعالجتها قبل تطبيق المعيار في الأداة المساعدة. تناقش الورقة أيضًا مستقبل IEC 61850 القياسي، وتبين أن بروتوكول DNP 3 لا يزال يحظى بشعبية كبيرة بين المرافق العامة، خاصة في أمريكا الشمالية. تناقش الورقة أيضًا إمكانية تكاملها مع إنترنت الأشياء (IoT). وأخيرًا، تقدم الورقة دراسة حالة لمحطة فرعية فيما يتعلق بالتأخير من طرف إلى طرف لرسائل القيم العينية ذات الوقت الحرج (SV) في بيئة إيثرنت ولاسلكية. ستساعد هذه الدراسة المستخدم في فهم المصانع الأولية للمحطات الفرعية، أي محولات التيار / الضغط (CT's / VT's) ، وقواطع الدارة، وما إلى ذلك، لأتمتة والتحكم وحماية المحطات الفرعية.

1. Introduction

Utilities, industries, commercials, and even residential consumers are transforming all aspects of their lives into the digital domain. A substation automation system (SAS) is a digital communication network that facilitates control, protection, and monitoring among various devices. Before the IEC 61850 standard, communication within the substation was established via expensive copper wires with limited proficiency. In order to address multiple SAS issues, IEC61850 standard named as Communication Networks and Systems in Substation was developed in 2003 to ensure interoperability among Intelligent Electronic Devices (IEDs) by the International Electro-technical Commission (IEC) Technical Committee Number 57 Working Group 10 (TC57WG10) and IEEE for Ethernet (IEEE802.3) based communication in electrical substations [1]. IEC 61850 was not designed just as a protocol like previous automation standards but a way of life for a substation, i.e., providing a design guideline for automation systems incorporating best industry practices as well as existing standards. IEC 61850 standard can provide interoperability among devices, reliability for the transfer of data, able to integrate monitoring, protection, and control devices in a network to perform different applications. The standard also defines data models representing all substation devices and functions, and common configuration syntax with a single configuration repository for all devices in the substation automation system using extensible markup language (XML). IEC 61850 clearly exceeds former protocols such as IEC 60870-5-103, DNP3, and other proprietary protocols, in terms of functions and capabilities. Therefore, IEC 61850 can be described as a collection of a management and specification system, a configuration language, a definition of automation services, a vocabulary of automation objects, and a conformity assurance system [2], [3].

In SAS, an IED (a physical device) is the main unit to perform all kinds of functions, i.e., protection, control and monitoring, by generating and handling analog and digital signals. IED is an embedded microcontroller systems that support Ethernet based communication and can perform several automation functions in SAS such as data and le transfer. Similarly, communication protocol, data formatting and the configuration language is defined to provide interoperability among devices. The IED is defined by the network address to start the IEC 61850 standard model. An IED can have one or more logical devices (LD), and a logical device may consist of many core functions called Logical Nodes (LNs) [3]. Hence, an IED is a standard representation of a data concentrator. In this way, a model is provided by the standard which supports devices from different manufactures due to common information approach for each logical node. The standard provides an ability to map available data and services to any available protocol for communication. The standard uses OSI 7 layer stack for communication as shown in Figure 1 [4].

As shown in the figure, standard maps the data to different protocols based on the application.

The type 4 and type 1 messages, i.e., raw data samples and time critical GOOSE, are directly mapped to low level Ethernet layer due to the nature of these real time messages. Sample Value Message (SV message-type 4) is a real time message and it is defined in IEC 61850-5 standard for protection, control, and measurement, etc. The type 6, i.e., time synchronization messages, are broadcasted using UDP/IP stack, while type 2, 3, 5 , and 7 messages, i.e., medium speed, low speed, file transfer, and command messages, are mapped to the manufacturing message specification (MMS) using TCP/IP stack. GOOSE messages run over flat layer 2 (i.e., not routable), and non-time critical messages (MMS, web services) run over layer 3 (i.e., routable). For the fast propagation of control signals (i.e., GOOSE message) in wide area networks, the IEC 61850-90-1 (an extension) provides communication among different substation for different applications, i.e., teleportation [4], [5].

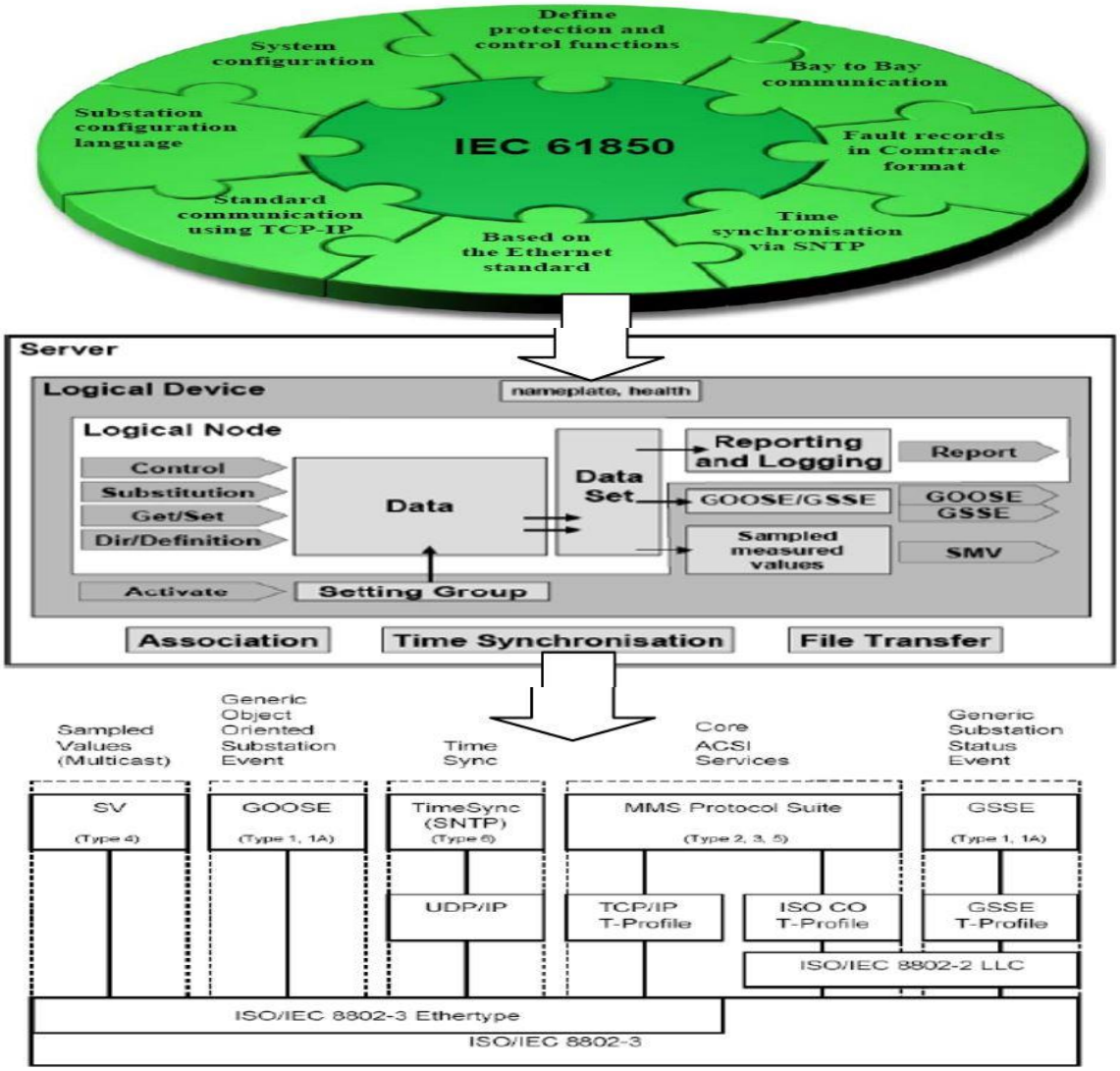

Figure 1. Conceptual model and OSI layer stack of IEC 61850 [27]

IEC 61850 is lengthy, complex and feature rich standard that facilitates the creation of powerful automation systems. The standard has already been deployed in thousands of new substation automation systems worldwide and is gaining popularity in other power system domains. However, the use of new technology and demand has also introduced new set of failures, as compared to conventional control and protection systems, i.e., wire based system. The figure 2 shows the cumulative technical issues per year [15].

There are structural, implementational, operational, data communications, and software failure issues, which were not present in the traditional hard wired systems. Unlike other standards, IEC 61850 was made operational without checking strict security features, and may introduce vulnerabilities for cyber-attacks due to the use of Ethernet based communications. Possible security breaches are password cracking, eavesdropping, replay services, data maliciousness, information interception, etc. Different other possible failures can also be infected to the system with malware by using infected devices [6]. Similarly, many external faults which although are not related to the substation but may cause many failures in the substation. In most of the cases, communication failures are figured out as the root cause of the problems in the substation automation. As Ethernet network is generally the architecture of the IEC 61850 enabled SAS, there are also numerous Ethernet faults and failures. The standard also does not define any particular system architecture and is a perfect tool to obtain interoperability, but there are also many practical limitations in this regard [7].

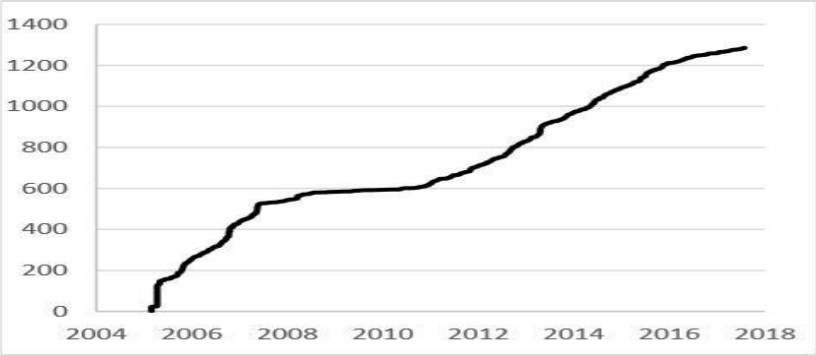

Figure 2: Cumulative technical issues by year [15]

The paper presents a detailed study of the different kinds of structural, implementational, operational, cyber, interoperable, interchangeable, and all other kinds of issues and challenges in IEC 61850 based substation automation system. Previously, different research papers have discussed these issues individually, but they are not discussed in a comprehensive way. The paper will really help researchers working to do their research while keeping in mind about these challenges. The paper will also help utilities to address these issues/challenges while

implementing the standard. Finally, the paper also discusses about the future of the IEC 61850 protocol, and its integration with IoT, while keeping in view with respect to these challenges. The paper makes it clear that if the standard really wants that it should be adopted by the utilities, the issues/challenges must be addressed.

The remainder of the paper is organized as follows: Section 2 describes the failures in hierarchical levels of the substation automation systems (SAS). Section 3, and 4 presents the interoperability and inter-changeability issues, respectively. Section 5 presents cyber-security issues and failures. Section 6 and 7 discusses subscription configuration language and manpower training issues. Section 8 discusses other issues and technical challenges. Section 9 discuss about the future of the IEC 61850 standard. Section 10 discuss about the integration of Internet of things (IoT) with the IEC 61850 standard. Section 11 presents a case study of substation for the end-to-end delay measurement of SV message for wired and wireless architecture. Section 12 presents a discussion, and section 13 presents conclusion. In the following section, the structural issues of the substation automation system have been discussed.

2. Failures in hierarchical levels of Substation Automation Station (SAS)

There are three hierarchical levels in a substation, i.e., station, bay and process level, as shown in the Figure 3 [4]. For communication between these levels, substation uses station and process buses. Following section discusses different issues and challenges related to the substation levels and buses [8].

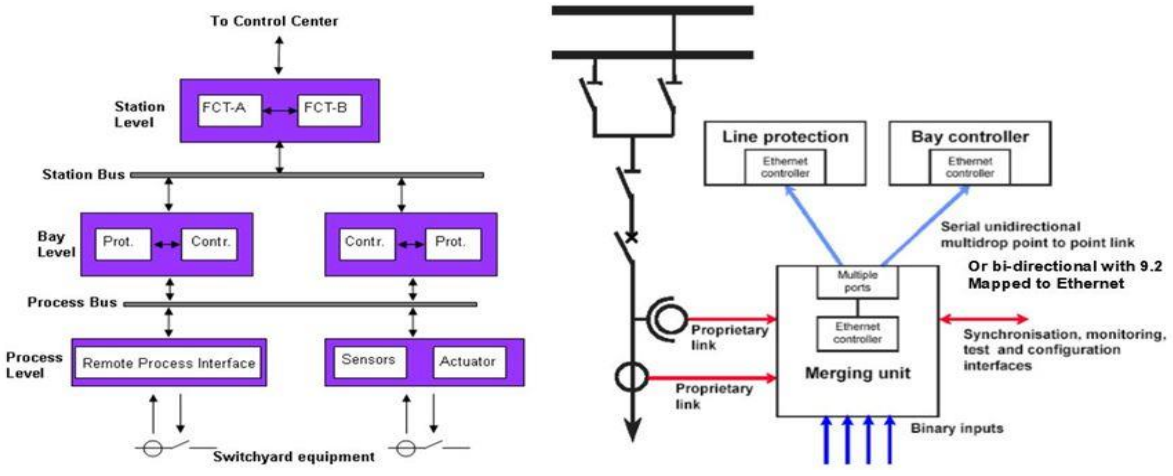

Figure 3. Interface model of a SAS (left) [4], basic Process bus and Sample Measured Value concept (right) [35]

2.1 Failures at the station level: The station level implements those functions which require data from more than one bay. Station level has human machine interface (HMI) computers, communication interfaces, and device configurations. Failures at station level are very

challenging and hard to recognize, which can occur in SCADA (supervisory control and data acquisition) centre and in remote user, and are ultimately transferred to SAS. The server at station level is the most critical part as whole data can be lost if there is a server failure. Therefore, redundant human machine interfaces, and servers should be implemented to avoid failures [4], [9].

2.1.1 Station bus failure: The communication between the station and the bay level is done through station bus. Station bus also provides communication among different bays. There are always communication issues at station bus. Therefore, for time critical protection and control messages, i.e., breaker failure trip, bus differential trip, etc, performance evaluation is needed. Generally devices from a single manufacturer are used in a complete single zone of substation, and protection and control functions are not distributed, so minimum coordination is needed among devices. However, if IEDs are from different manufacturers then it is a big challenge for design engineers to execute the SAS successfully by coordinating all the distributed functions in a single zone of substation. IEC 61850-90-1 and IEC 61850-90-2 discusses about the communication between substations and control centers, respectively [8], [4].

2.2 Failures at the bay level: The IEDs such as bay control units (BCUs), bay protection units (BPUs), phasor measurement units (PMUs), measuring centers (MCs), switch gears, metering gauge, etc., are all placed at the bay level. All of the important tasks such as data collection, protection and controlling the power network, i.e., IEDs receiving data from switches and sending them to servers, and also transferring instructions from HMIs to the interface devices are performed through these IEDs. The bay level has the central position in the hierarchical structure of the SAS; therefore any failure at the bay level has more severe effects on the operation and performance of the substation as compared to other levels. Bay level can have revealed and hidden failures. In revealed failure, if an IED responsible for complete protection and control fails, then whole system may fail. In hidden failures, a failure remain hidden during normal operation until unless some fault occur, i.e., a device may start working when it is not required or may not work when it is required, such as a protective relay which cannot detect or cannot respond when a failure occurs in the system. Self-testing and certain diagnostics should be carried out routinely in order to avoid hidden failures [10], [11].

2.3 Failures at the process level: The power equipment at the lowest level, i.e., switch yard equipment, such as current transformer (CTs), voltage transformers (VTs), protection transformers (PTs), remote I/O, circuit breakers, smart sensors, and actuators, and MUs, are connected to the substation through the process level. The process level is responsible of collecting data in a timely manner from power equipment for proper control. Due to this importance, if any failure occurs then communication among power networks and the SAS is affected. Digital communication is provided by IEC 61850-9 at the process level through the process bus to other station levels reducing the cost and complexity of the traditional hard wires.

Inputs (analog and binary) from switchgear equipment and status information from transducers are gathered using merging units (MUs). The analog values are first converted to digital before sending to the protection and control IEDs at bay level using Ethernet based communication. MU also time stamps each data using time synchronization (GPS clock) in order to estimate accurate phasors for protection and control IEDs. If there is any failure in the data transmission from the merging units to the control and protection IED's, then control (e.g., interlock logic) and protection (e.g., auto-reclosing) functions will be affected. Similarly, sensors and indicators check the power system equipment (transformers and breakers) to acquire, mention, and update to the SAS for any kind of failure. Therefore, if there is any failure in the sensor and indicator, it can also affect the reliability of the substation indirectly [4], [8].

2.3.1 Failure at process bus: Process bus is responsible for the time critical communication i.e., sampled values, and also facilitates communication between IEDs at the bay and the process level, i.e., switchyard equipment. Process bus issues are critical, i.e., handle time critical GOOSE and RAW messages, as all protection and control functions depend on the reliability of the process bus. Figure 3 also shows the basic process bus and sample measure value concept [35]. But on the other hand, utilities still do not have a mature practical experience to work with process bus, and there are still many issues/challenges related to process level communication as described below.

2.3.2 Issues with process bus topologies: There are different ways, called topologies, in which workstations can be connected with each other using Ethernet based communication. The topology really determines the nature and performance of Ethernet local area networks (LANs). The standard did not impose any restriction on the architecture of the process bus. Therefore, different architecture was developed by different manufacturer to achieve greater reliability at process bus but without ensuring interoperability between them. Ethernet topologies offers a speed of 100MBits/s for communication but time critical messages has to be in compliance with the allowable message delivery time as defined in IEC 61850 Part-5. The IEC 61850-5 I.2 studied the performance of the SAS network but without describing how the IEDs are modeled and without taking into account the worst case scenario, process bus, and network topologies. Therefore, the standard does not really specify the parameters for an overall system performance, i.e., performance of the message delivery [12]. Common Ethernet topologies such as bus, ring, star and hybrid used in substation are briefly discussed below with their issues.

a) Bus topology: IEEE 802.3 based carrier sense multiple access with collision detection (CSMA/CD) approach is used in this topology. Bus topology does not use switches, hubs or repeaters, and communicating stations are directly attached to the bus through hardware interface known as a tap. However, the topology is not feasible for large substation process bus as GOOSE and raw data packets time delay in this topology is not in compliance with IEC 61850 standard [4, 9, 12].

b) Ring topology: Ring topology uses point to-point communication links by using repeaters or switches in a closed loop. In ring topology, when one side of the loop is broken, the IEDs are not able to communicate with the IED on the other side of the loop. Although, it is easy to find a fault and rectify it as compared to the bus topology, thus making it most reliable topology. However, this topology is also not suitable for larger SAS as time delay for GOOSE and RAW data messages is the same as bus topology [4], [12], [9].

c) Star topology: In star topology, every station is connected directly to a central switch. The message delivery time for critical application are also in compliance with IEC 61850, but if the central Ethernet switch fails in this topology due to any reason, i.e. technical, environmental and EMI (electro-magnetic interference) conditions, then a major breakdown can happen at process level, and ultimately at whole SAS level [8].

d) Cascaded Star topology: Cascaded Star topology is an- other topology, in which Ethernet switches are connected in cascaded way, i.e., a switch is connected to the previous and/or next switch in a cascade way. If one of the switch fails, especially at the start of the cascade, system may face considerable delays, or total communication failure. Therefore, complete reliability is still an issue in this topology [4], [12] [8].

e) Star Ring topology: Star Ring topology provides architecture in the form of a closed loop by connecting the last switch with the first one. This topology facilitates some redundancy and reliability in case of failure, and has communicate messages within the allowable message delivery time as defined by the standard, but it is more difficult and expensive to implement this topology with respect to other topologies [4], [12] [9].

2.3.3 Other technical issues with process bus: Other technical issues are described below.

a) Time synchronization issues: Time synchronization defines how IEDs perform the synchronization of their internal clocks with a device using global positioning system (GPS) satellite. The signals sent through the process bus should be synchronized so that the protection and control functions at bay level IEDs can utilize such signals effectively from independent merging units (MUs) of various manufacturers. IEC 61850 standard first defined simple network time protocol (SNTP) to perform synchronization process but this protocol does not provide time synchronization requirements for all SAS applications, i.e., disturbance recorders, synchro phasors and data transferred through the IEC61850-9 process bus, etc. SNTP also provides an accuracy up to 1 ms, which does not meet the requirements for the raw data sampled values [13]. The standard has also proposed many other protocols to address this issue. One of the solutions is to use the inter-range instrumentation group (IRIG-B 9) synchronization which is able to provide the requirements as defined in IEEE 1588 standard and can provide accuracy in the range of 1 s. Another solution is to provide point-to-point communication between IEDs and merging units. Therefore, synchronization is very important along with latency for smooth and reliable

communication between devices inside a SAS or communication with other substations. The data is useless for monitoring, protection, and control if synchronization is lost. Therefore, there must be synchronization while collecting data from the process level [8].

b) Electromagnetic interference (EMI) immunity: Electromagnetic interferences such as switching surges, electro static discharges, etc. are commonly encountered in air insulated substation (AIS). Therefore, all the devices in a SAS must be fulfill the requirements as defined in the EMI immunity standards particularly at the process level. The general EMI immunity procedures used by industry do not follow the air insulated substation (AIS) requirements. The EMI immunity requirements are defined in the IEC 61850-3 with details by referring to IEC 6100 series (IEC 61000-6-5 and IEC 61000-4-x) or IEEE C37.90.2 [8].

c) Variations in IEC61850-9 standard: The standard defines IEC 61850-9-1 and IEC 61850-9-2 for transmitting sampled values on the IEC 8802-3 standard frame. In IEC 61850-9-1, the ASDU (Application Service Data Unit) format is fixed as defined by the IEC 60044- 8 standard. However, IEC 61850-9-2 is more versatile and programmable according to the requirements, as it uses a configurable dataset based on an encoded APDU (Application Protocol Data Unit) according to ASN.1 format. Therefore, the design engineers need to be very careful while designing the SAS [9].

d) Measurement accuracy: The available data at the process bus is analyzed according to the standards before communicating to the bay level. Therefore, the data at switchyards is sampled and then digitalized according to IEC 61850-9 standard, but this process adds quantization error. Similarly, devices such as analog to digital converters and microprocessors further add delay due to the digital signal processing. Also step and frequency response, i.e., dynamic behavior of merging units, need to be analyzed properly [9], [12].

e) Evolution of process bus: The evolution of the high data rate IEC 61850-9-2 process bus has greatly improved the performance of the SAS. However, the utilities still do not have a good understanding that how the process bus will behave under heavy traffic in a network. Therefore, various communications network parameters of the modeled IEDs need to be checked, i.e., various communication link speeds, IEDs microprocessor processing time, packet size, buffers sizes, number and capacity of the queues, etc [3], [11].

f) Interlocking: The integration of IEC 61850 in each IED eliminates the advantage of the protocol contents. Research has shown that interlocking problem occurs in the architecture using Ethernet bus and TCP/IP protocol. The interlocking is due to the delay causing an instruction from a switch to reach to another switch after delay, which is experimentally calculated around 80 msec. The design engineer has to modify TCP/IP protocol for time critical transmission [14].

g) IEC 61850-Part 10 describes conformance testing procedures to check that the IEDs provide the features as described in the subscription configuration language (SCL) file. However, network designer need to verify the other IED performance characteristics which are not

included in part 10 such as synchronization, time- stamp accuracy, control reaction time, operational and reliability criteria. The good engineering design is to select IEDs that will continue to function without delay even if network failed or it is under attack [15].

h) Research has also shown that the packet size is also one of the main factors which cause delay. Therefore, small packet size should be used, and should also avoid sending a variety of data streams at the same time in order to meet the real requirements in the substation [16].

i) Factors like distance and location of the MU and IEDs, the communication capabilities (single port, multiple ports) of the units, the availability of the network, bandwidth, and the communication topology (point-to-point, star, or ring) can make the selection of the process bus architecture quite complex.

j) IEC 61850 is based on the inter-relay communication capabilities. Therefore, redundancy of key components is very important for the overall reliability of the system, i.e., particularly dealing with protection issues.

k) There can be a delay and packet losses on process bus architecture based on IEC 61850-9-2, causing significant effect on the reliability of the protection system for whole network. Research has also shown that by increasing the frequency of the SV messages causes more packet drops [17].

l) During up gradation and migration to IEC 61850, a secondary system should be there to support both conventional and nonconventional instrument transformers [12].

m) A larger bandwidth is required as process bus needs to continuously transfer sampled values from the primary process with a quasi-real time response.

n) Electronic interfaces must be used with circuit breakers and digital switching must be used to convert switch positions, and commands.

o) There are many other issues which a designer has to take into account while using Ethernet LAN such as status of automation and protection when LAN fails, IED performance and its communication if there is a heavy traffic, hacking, denial of service, performance of the network during overload, effects of the newly connected IED on network, performance of the functionality issues of the IED as single CPU might suspend protection while servicing other network request [16], [13].

All of the above mentioned issues clearly show that there are lots of issues with process bus, i.e., ranging from its topology to technical challenges. Hence, the architecture of the process bus in the utility needs further validation due to the lack of this confidence. Following section will discuss the issues with respect to interoperability, i.e., how devices from different manufacturers will communicate with each other.

3. Interoperability

It is a big challenge to provide interoperability among devices from different manufacturers. One

of the main ideas for the formation of the IEC 61850 was to provide enhanced interoperability among IEDs from different manufacturers to perform different functions, i.e., protection, interlocking, and automation [18]. However, design and configuration is still needed for the two IEDs to interoperate with each other even with the same message type [8]. This is due to the reason that different protocols are used to perform communications between IEDs belonging to different manufacturers, which are not compatible with IEC 61850. Therefore, additional protocol inverters are required which are costly and increase failure chances. Although, the standard tells how the data will be communicated and analyzed between devices from multiple vendors but the standard does not tell which data will be available. Similarly, whenever there is upgrades in the hardware or firmware, compatibility issues occur, and even if all the configurations of two different devices match, there is still a possibility that these two may not communicate properly [13], [19], and [20]. Therefore, there can be many issues with respect to interoperability, as discussed below.

3.1 File transfer: File transfer is an issue, as IEC 61850 supports both FTP (File transfer protocol) and MMS (multimedia messaging service) file transfer but does not standardize the contents. Therefore, consistency or interoperability of these files among different vendors is still an issue, i.e., a product from one vendor may not be interoperable with other vendor. There are also other issues found between vendor files such as incorrect initialized values, unsupported XML namespace issues, support of integer 128 issues (inability to map/support such a value in the implementations memory/application), issues when a vendor attempts to import an SCD (substation configuration description) file exported by another vendor. Therefore, it becomes very challenging to confirm the performance of the substation, if IEDs belong to different manufacturers as even if IEDs pass the conformance test, there is no guarantee for interoperability and satisfaction of end users requirements. Therefore, utilities and end users must include the interoperability test for the IED acceptance process due to the existing ambiguities, i.e., different manufacturers have different interpretation of the IEC 61850 standard. These issues not only vary the interoperation of the standard from one vendor to another, but further enhance the complexity of interoperability tasks within the SAS [8], [7].

3.2 Version upgrade issues: IEC 61850 provides free configuration by separating functions of each section in the substation. Hence, the reliability of the operation in any section depends on the configuration of all devices from multiple vendors in that section. Therefore, if a version update is done for the hardware or software of a single device, then it may not interoperate with other devices belonging to other vendors leading to a need for updating of the hardware or the software of all the devices installed in the same zone causing more time, money, failures, and complexity.

3.3 Challenges for the system configuration: The IEC 61850 standard defines IEDs model, communication services and various common files but it does not specify the IED or the system configuration tool. The protection and integration engineer face severe challenges while

configuring individual IEDs or even the whole system due to various manufacturers IEDs and system configuration tools. Therefore, the configuration task is the most costly and time consuming process based on the available SAS configuration tools.

3.4 Automatically map configuration Issue*:* For a complete communication among client and server, a one to one correspondence of necessary protocol attributes is not available, therefore a manual configuration is performed as automatic configuration is not available. The system integration performed in this way is very time consuming. Similarly, some other instructions get benefit from the IEC 61850 object oriented data structures, but many data structures are not available in other protocol standards. Therefore, new data aspects are generated along with the requirement of changing current data attributes from one format to another.

3.5 Other issues regarding interoperability: Single vendor IEC 61580 interoperability is fine, but there are always challenges and problems for multivendor implementation. Utility workers need to be trained to use specific vendor tools to configure the system in a multi-vendor environment. In north American utility, there is an interoperability challenging list such as point naming differences (some vendors use generic names and others use specific contextual names), configuration parameter differences disallowing one vendors IED to subscribe to GOOSE message from the other vendors IED, challenges with respect to SCD configuration files and how to upload to devices as there is no area within the native IEC 61850 files and needed to use the private data sets to support the different settings file and IEC 61850 file. Moreover, there are different limits for number of publishing messages and number of subscribing messages for each vendor IED, as some vendor IEDs do not support priority tagging for GOOSE messages, and some do not support VLAN identifiers for network segregation. Similarly, automatic configuration using vendor SCD/ICD (IED Capability Description)/CID (Configured IED Description) files is impossible [19].

The reality of the IEC 61850 interoperability is that vendor wants coexistence and utility want interchangeability. The MMS and GOOSE messages have high maturity, while semantic model has medium maturity, and engineering tools have low maturity. Many utilities assume that products of different vendors have implemented all parts of the standard in a completely interoperable way but this is actually not right due to the reason that IEC 61850 is a large standard with multiple options from which the vendor can choose, and the marketing departments of each vendor make individual decisions concerning the features set that their customers will only use. Also, some parts of the standard can be interpreted differently by different vendors. Therefore, in order to create a successful network, a network designer has to check that the IED is able to work with the required data, protocols, and characteristics of the IED coordinate well with the other devices in the network [14]. In the following section, challenges/issues with respect to interchangeability are presented.

4. Interchangeability Issues

Interchangeability is another challenge which needs to be addressed to provide a complete flexibility to replace an IED with another IED belonging to different vendor in the same network with minimal changes. Enhancing the capability of the substation is a major challenge, i.e., augmentation, as IEDs belong to different vendors and integrating them with existing hardware (HMIs, IEDs, switches, etc) is both an economical and technical challenge. The utilities want interchangeability at the abstract communications service interface (ACSI) level so that they can select IEDs whichever they want from different vendors, as the IEC 61850 standard never ensured interchangeability of IEDs. The standard also does not define which logical nodes or contents will be supported making interchangeability more complex. Integration efforts can be minimized using standardized names and attributes in LN, but reconfiguration is still needed when devices are changed with different logical nodes, GSE characteristics, database, and interfaces. The integration can be reused if the characteristics are same, but device interchangeability is limited due to reason that logical device name is not configurable. Although, IEC 61850 is not just a protocol; it is a way of life, but utilities should avoid big changes as it may lead to strong disagreements between users, implementers, consultants, and manufacturers [17].

4.1 Observations regarding different vendor's equipment implementation: IEC 61850 needs to be continuously assessed for reliability. This is due to the reason that understanding and implementation of standard varies between from one vendor to another. Therefore, devices may behave differently even working under same condition. The research has also shown that the implementation of the GOOSE on commercial IEDs and on the open source libiec61850 library shows different results even under the same conditions, which sometimes provides an opportunity of cyber-attack on the devices under the study [7].

Cyber security is another big issue for reliable and secure operations as described in the following section.

5. Cyber security

Cyber security is always a big threat, i.e., pirate intrusion attacks leading to a compromise of data security, consistency and integrity. In cyber-attacks, PCs are infected, files are encrypted, and ransomed is asked. Also, NISTIR 7628 (a guideline for smart grid cyber security) has specified IEC 61850 as an insecure protocol, i.e., substation LANs are vulnerable if there is no implementation of firewalls, intrusion prevention system (IPS), intrusion detection system (IDS), data gateways or demilitarized zone (DMZs). Cyber-attacks on substation automation systems are real and increasing, leading to large financial losses. There was a cyber-attack in Ukraine in 2015 and 2016, where adversaries gained full control to SCADA and control room functions, and interrupted power to several customers in both attacks, and implemented a telephone denial of

service (DoS), uninterruptable power supply (UPS) shutdown and kill disk phenomenon [21]. IEC 61850 does not define any mechanism against cyber attacks, and it is up to the manufacturers to fulfill the requirements as specified in IEC 62351. Ethernet based communication has made SAS more vulnerable to cyber-attacks. Automation system has been opened to external world and can be misused for cyber-attacks. Automation industry should follow regulatory directives or industry best practices to avoid any liability. The automation industry will not be in position to offer required customer needs, high level of security for all products and solutions, fast response and reliable partner in case of a cyber-attacks. The vulnerabilities can be on the device level and on the network level. On the device level, when firmware of the subscribing devices are configured, i.e., GOOSE message communication, it must be properly tested and verified that it must follow the requirements as defined by the IEC 61850-8-1 and IEC 62351-6 standards. The subscribing devices must not process any messages which has repeated or old status numbers. The libIEC61850 has a function, i.e., IsValid(), to make sure that no duplicated or old numbers messages are processed, but commercial IEDs do not perform this verification and process fictitious messages. Similarly, any message must not be published and/or processed, until the time stamp with current status number is verified. On the network level, MAC (Media access control) address spoofing is a big issue. MAC filters should be used at all switches in a network in order to stop publishing fictitious GOOSE messages using a spoofed MAC address. However, this thing has not been addressed in both IEC 61850 and IEC 62351 standards [7], [1], [22].

Cyber security is very challenging in the power communication system as IEC 61850 is vulnerable to different attacks, i.e., denial of service, password cracking/swamping, eaves-dropping, interceptions (Man-In-The-Middle) and viruses, etc [23]. These attacks cause delays in message deliveries, and also loss of data and data security becomes more critical while communicating with components in the network whether inside or outside. The standard 61850-3 refers security details in section 304 of the IEC 60870-4. The WT15 of TC57 provides some measures against cyber-attacks, i.e., firewalls, encryption, and authentication, which can provide security up to some level. However, any process to improve the safety of the network will also increase the processing time sacrificing the network performance [1], [21]. Few examples of cyber-attacks are described below.

5.1 Denial of service attacks: During denial of service, large numbers of fake requests are sending from many devices in the network to a particular device in the same network, which ultimately can consume the resources of the network. A denial of service attack prevents an authorized user or machine from accessing the services due to insufficient bound checking, i.e., by disrupting or exploiting the services of an IED. In disruption, a malicious message is sent by the attacker to the attacked IED, which aimlessly writes extra data and causes a buffer overflow and/or an unauthorized data modification. In exploitation, multiple sessions are opened by an attacker on either the file transfer protocol (FTP) or telnet services and then do not use

them and ultimately interrupt the services of the IED [9].

5.2 GOOSE poisoning: GOOSE poisoning is another way of denial of service attack having three different kinds: high status number, high rate flooding, and semantic attacks. The sender and receiver of the GOOSE messages are described as the publisher and the receiver, respectively. Every GOOSE message has a status and sequence number field (stNum, sqNum). In high status number attacks, the attacker tries that the receiver should accept those GOOSE messages which have a higher stNum and consider the actual GOOSE messages as outdated, i.e., creating a possibility of accepting the messages only from the attacker. These kinds of attacks are really dangerous and can damage devices and even cause loss of human life. This kind of attack model is represented in Figure 4 (left). Similarly, an attacker might block legitimate messages and inject messages with altered content leading to GOOSE message manipulation.

Denial of service could also happen due to the high rate flooding attack. The high rate flooding can happen due to the congestion of the channel and utilizing the available computational means of the network, and ultimately delaying messages above the critical delay, i.e., 3-4 ms. Flooding attacks are done at the network or application layer, and can be classified as broadcast flooding or unsolicited flooding, or flooding to a third node [1], [12].

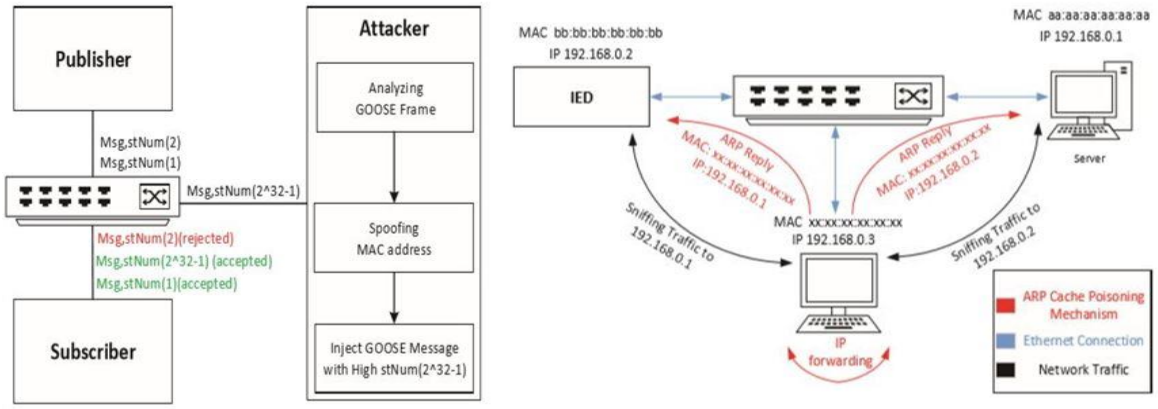

Figure 4: GOOSE Poisoning Attack (left), ARP Cache Poisoning mechanism (right) [1]

5.3 Password cracking attacks: These attacks happen when attacker gets the unapproved control to a system. Brute force attack or dictionary attacks are the two ways to figure out an authorized user password. In brute force attack, a time consuming process is done to find out the actual password by trying all probable combinations of a password, until an actual one is found. Dictionary attacks guess the password by properly constructing words that would be found in a dictionary, and take less time to crack the system [1].

5.4 Packet sniffing attacks (eavesdropping): In these attacks, an attacker attempts to steal the packets which are transmitted on the network by reading them. The services like FTP, HTTP, and

Telnet do not protect their messages and are highly vulnerable to attackers. Packet sniffing attacks also provides an opportunity to attackers to do man-in-the-middle attacks. The attacker may also do eavesdropping by performing an address resolution protocol (ARP) cache poisoning as shown in figure 4 (right), where ARP protocol converts IP addresses into MAC addresses. Therefore, if the attack is successful an accurate IP address is attached with a fake MAC address, and then all the packets are transferred to the attacker instead of actual IP address. This is also done by filling the content addressable memory (CAM) table with fake entries by flooding it. When the CAM table becomes full, packets sent to a MAC address which is not present in the CAM table is published to the whole network providing an opportunity to the attacker to access them. Similarly, in switch port stealing (another way of eavesdropping) the attacker attacks the switch by sending fake frames to change the CAM table in order to connect the MAC address of the attacker to the interface. In this way, all the incoming packets are delivered to the attacker instead of the actual receiver [1].

5.5 Security protocol IEC 62351: IEC 62351 does not provide a complete solution to avoid cyber-attacks, as it can only avoid eavesdropping/man-in-the-middle attacks, switched network packet sniffing through TLS (transport layer security) encryption, message authentication, and describing role based access, respectively. IEC 62351 does not provide protection against denial of service, GOOSE, and SV based attacks, as IEC 62351-6 digital signatures and encryption demand more than the available 4 ms delivery constraint by the IEC 61850-9-2 standard for the generation and verification [13].

5.6 Interception: During interception, attacker gets access to the data travelling in the network by interceptions, i.e., pretending a device which belongs to the network. In this way, the interceptor is able to access the data exchanged inside the network, and can change data values.

5.7 Viruses: Viruses are malicious software that can damage computer systems. If a virus gets inside a computer, it has the capacity of creating copies of them and reaches to other systems in the network.

5.8 Other issues: Research also shows that the GOOSE messages status numbers are not implemented on the devices as specified by the IEC 62351, creating a possibility of an attack on the power systems. Similarly, using old time stamps for processing messages also creates a vulnerability of attacks. Moreover, broadcast nature of the GOOSE messages also creates an environment of the sniffing and rebroadcasting them, specifically when the attacker is sitting in the same LAN. At network level, as long as the GOOSE message has an authentic APPID (application identifier) field, it is processed whether coming from an approved device or a malicious one. The IEC 61850 and 62351 do not define any rules for the authentication of MAC addresses, the utilities have to create appropriate defense mechanisms to address this challenge [24], [2].

The following section describes the issues related to subscription configuration language.

6. Subscription Configuration Language (SCL) issues

In order to standardize the method of communication within IEDs, i.e., configuration between IEC 61850 client or server or the integration of logical nodes and generic substation event (GSE) messages, substation configuration language (SCL) files were created. Substation configuration language is based on extensible markup language (XML) as per IEC 61850-1 standard providing a common object and configuration description. The clause 9 of the standard IEC 61850-6 specifies that SCL XML has five sections [18]. Initially, there was a misconception that by using a self-description method SCL files will be acquired directly from the IEDs. However, it was quickly realized that it is not like this and the system designers has to configure the IEDs by themselves during the settings implementation phase., as most of the configuration tasks are not addressed, and even the configuration to perform primary tasks is not available by using the SCL files. Also, SCL files do not handle automatic, total application configuration and GSE configuration of the IEDs from different manufacturers. Moreover, the standard does not handle interlocking, distributed protection and specialized automation. Therefore, in order to configure each IED, software of the particular IED is required from original vendor for the creation and installation of the logics as no standardization is available [25]. Therefore, tests are required to make sure that devices from different vendors can understand the information files from each other. In some case, even when the configuration files can be easily read and understood, integration with different vendors is still difficult and complex. This happens due to the reason that many parameters of the configuration, engineering and device interconnection are different among vendors, i.e., fixed data sets versus dynamic data sets, etc. [5]. Similarly, the informal specification needs to be converted into technical documentation to do the integration in SCL, and system designer needs to be very careful during this implementation process. The compliance checking has also to be done in detail which is given in part 10 of the standard, and data sheets are provided by the suppliers describing the SCL description and its capabilities with the instructions to save the documents in the subscription configuration description (SCD) file. In fact, the SCL is one of the most difficult parts to understand, as it includes the majority of the design artifacts from the automation project [21], [26]. The following section describes the manpower training issues.

7. Manpower training issues

Other than implementation, interoperability, interchange-ability, synchronization, and cyber security, etc, there are also many other issues for the implementation of IEC 61850 standard. Study shows that the implementation of the standard by utilities is a complex process which needs proper skills, competency, required training, ability to handle challenges while applying new standards, and the deployment strategies for substation automation within existing functional organizational structures, vision, and strategy as shown in figure 5 [27]. Eskom, a

South African utility, who decided to adopt the IEC 61850 standard into its substation, found that the major hurdles for the implementation of IEC 61850 standards were skills, organizational culture, and training and competency levels. As organizational culture is very critical element, hence the implementation of IEC 61850 must be properly studied. Utilities need to train their workers with the latest technologies. The requirements for the core technical skills and competency may change the organizational culture, training and competency levels, and new engineering processes, specifications and tools may be required. Generally, following skills or understanding is required before implementing the IEC 61850 standard such as understanding of protection and control functions, SCL, communication networks (TCP/IP, Ethernet, switches, routers) and time synchronization via SNTP, network data analysis, communications services, mapping of information models, MMS etc. A team of experts from communication, protection, maintenance, and substations should train workers, focusing on the details of the standard. Similarly, devices should be chosen based upon functionality, 61850 requirements, conformance tests, and redundancy [15], [27].

Figure 5: Framework for competencies [27]

The next section presents many other technical challenges, and issues of IEC61850 standard.

8. Other miscellaneous technical issues

There are also many other issues/technical challenges as described below.

8.1 Ethernet network failure: Substation automation system uses Ethernet network which consists of connectors, routers and switches, etc., for the data communications on three different levels of the SAS. Due to the use of connectors and other switching devices, many physical faults and failures like defective network interface card (NIC), faulty cables, unnecessary termination, or extra length cable can occur in the network structure. The failure of NICs, routers, and switches at the physical layer are one of the major issues that can halt data communication in a SAS. Similarly, if a node becomes disconnected or unplugged due to cable dysconnectivity in Ethernet network, and if no redundant path is provided using either, i.e., rapid spanning tree

protocol (RSTP), high availability seamless redundancy (HSR) protocol and/or parallel redundancy protocol (PRP), then a segment of the network or whole system in SAS might get interruption, and ultimately will result a total communication failure. Due to the Ethernet network, jabbering is another inherent issue in these networks, in which a packet has to retransmit when other devices don't understand, resulting in an increased traffic and consequently network halt or failure. Also, if a network is not properly designed, then collisions may occur which generates runts (smaller packets as compared to required minimum packet size) and giants (larger packets as compared to required maximum packet size). Although, routers and switches can be used to reduce the length of the cable and collisions but these devices have their own failure rates, and other faulty issues, ultimately deteriorating the whole system reliability. The IEEE also does not allow any 100BASE-TX segment more than 80 meters in a network [8].

8.2 Commissioning issues: IEDs require lot more configuration, i.e., a complex and time consuming process as compared to a traditional electro-mechanical relays and will not work properly if setting is not done accurately. While commissioning, different kinds of functions in an IED requires validation so that all diagrams, controls, inputs/outputs, indications etc, are working as required. Also testing, which is an important part of commissioning and routine maintenance verifies the correct operation of the IEDs but requirements are altogether different than an electromechanical relays and hard-wired circuits as described in 61850-10. Testing becomes more critical and creates uncertainty in the integrated IEC 61850 based SAS when some part of the system needs to be tested without effecting the working and efficiency of the whole substation. Therefore, any inaccurate SAS engineering and design issues will ultimately lead to operational failure, and may cause the system to allow or stop the requested instructions [4].

8.3 Important things while commissioning: While commissioning, few of these things must be properly understood, i.e., how much important is testing and capturing the GOOSE during commissioning? How to monitor GOOSE message after the system is in service, and how to find the absent GOOSE messages? Is there a limitation to the number of subscribers for one GOOSE? How to visualize the source and destinations of GOOSE? How to replace the new relay of different model or different manufacturer, as testing is required to make sure that all new GOOSE and all IEDs related to this new IED is working properly. The maximum number of IEDs that can be put in one loop on Ethernet switch should be properly analyzed, and communication port of IED should be checked. Similarly, we should take proper measures to manage the files, otherwise it will be lost. Dataset sequence must be followed, as by changing the sequence of the members in the dataset of sending IED during the commissioning process, there is a possibility that corresponding function in the receiving IED will be affected. Commissioning details should be carefully planned with communication and post-communication maintenance tasks. Similarly, how to test an in-service automation system, as legacy air-gap method will not work with IEC 61850 standard [15], [26].

8.4 Data integrity issues: The connection of two points is not always sufficient to have a secure communication, as various other factors also affect proper communication. Logical problems are generally more complex and difficult to find and solve than the network structured problems [4]. Therefore, data integrity is an important issue for a consistent and reliable communication in the standard. IEC 61850-3 standard has referred IEC 60870-4 (section 3.5) for the details of the reliability of the data delivery by the substation. For consistent and reliable communication, error corrections can be performed but this process requires time synchronization further adding the reliability and consistency concerns. Similarly, software failure is another kind of failure which was not present in the traditional hardwired system, i.e., code faults due to the dedicated software of each IED to implement functions. A good level of understanding is required for effectively utilizing different features in an IED due to the complicated software design. Variables, arguments, codes, operands, and subroutines, etc., are the various variables factors which can cause failures in an IED. Moreover, use of latches and time-delays to perform protection and control functions further enhances the probability of software failure. Similarly, if a database fails, it means the massive failure for the operation of running systems. Therefore, any unauthorized access must be avoided to a database [4].

8.5 Latency issues: Latency is another critical issue for the proper operation of Ethernet based network. High speed time critical messages, i.e., GOOSE and SV, require 3-4 ms to reach the destination, as defined by the standard. Each task has some latency but some tasks like system protection must operate in quick and steady way. Two different kinds of latency can exist in a network, i.e., constant and variable. Constant latency is predictable and calculate able as it is an inbuilt delays in devices and connections and also due to the structure of the network and available bandwidth. Variable latency depends that how much is the traffic and current load on the network. The variable latency increases and throughput decreases when there are simultaneous communications or failures inside the network. The issue of latency goes critical if an intermediary device or connector fails, forcing data to travel an alternate and non-optimal path, i.e., increasing the hop count. Similarly sometimes, some intermediary nodes need to handle more traffic in order to cover up the faulty nodes in the network, ultimately increasing traffic delays [13].

8.6 External failures: There can be many external failures, which can impact or halt the operation of a SAS. Most important of them is the loss of power in an IED, as compared to the electromechanical relays. Even if power goes off for a very short moment of time, whole system is reset creating a possibility of failure. Similarly, the loss of power has same effect on network switches, routers and other devices, i.e., a disconnection of all IEDs. A redundant power source is required to avoid such situation [5].

8.7 Environmental issues: The devices at the process levels are exposed to the atmospheric conditions. The environmental requirements, i.e., temperature, humidity, pressure, pollution, and

corrosion are defined in standards IEC 61850-3, IEC 60870-2 and IEC 60694. It is very important that devices at the process level must fulfill these requirements. A build up of the stain and dust on the devices can decrease the efficiency of the cooling system bringing different components in the devices to heat up and also initiate fire in extreme weather conditions. Overheating can also cause temperature sensitive elements to damage if there is no air conditioning, especially in large facilities. Similarly, communications devices, wirings, and connectors decrease in efficiency with time and network performance is gradually reduced [8].

8.8 Planning issues: IEC 61850 standard is very comprehensive in the desired outcome for an interoperable system but the proper application of IEC 61850 standard requires a careful plan. The implementation of IEC 61850 technology requires a large degree of risk management, as learning curve for the standard can be very steep, and training costs are generally underestimated, stopping many substation industry to make transition from old system to a new standard [17]. Similarly, functions in a single section can be distributed to many devices as defined by the standard. However, random or improper allocation of distributed functions may create more traffic in the network increasing message delivery time of the critical messages. Similarly, with the increase in the power demand substations need to be expanded but standard does not specify any specific architecture, and this issue should also be taken care during planning, i.e., adding more devices should not increase and existing Ethernet LANs should be scalable [28] Therefore, for a successful substation commission and execution a complete flow chart should be prepared.

8.9 SAS structural issues: IEC61850 standard guarantee that even a single zone can have devices from different vendors as contrast to the current situation. This means that different devices and Ethernet switches will be from different manufacturers, which may cause problems of communication between each other especially when the devices have to comply with the IEC 61850 standard. Therefore, building such a structure from different vendors also brings risk and complexity to the SAS architecture [18].

8.10 Overall system reliability issues: There is no demand for redundancy in the standard even for critical applications. However, reliability and consistency requirements are defined in the IEC 61850-3, that substation must keep on working all the time and there must not be a single thing which can stop its working, i.e., no loss of any undetected function if any component fails. The details of the reliability requirements for SAS are further defined in the IEC 60870-4 Section-3.1 [8].

8.11 IEC 61850 SAS functions reliability issues: The IEC 61850-1 defines the concept of a distributed function, i.e., splitting the functions into many parts and executing within various IEDs. The reliability of the IEDs, protection, control and automation functions are responsible for the reliability of the system. Therefore, there should no single point where there can be a possibility of failure of a function to cause the whole system to stop working. Previous research papers generally focus on whole system reliability using various calculation methods, and do not

focus on the reliability of IEC 61850 functions. Therefore, understanding the reliability and probability of the failure for any function is very important for a successful operation of a substation [29].

8.12 Accessibility issues: SAS accessibility is also one of the important functional requirements for implementing the SAS according to the standard, and specific accessibility requirements are defined in IEC 61870-4 Section-3.3. Therefore, there may be a need for the back-up to maintain the current level of accessibility for critical applications, as few communication devices may have less availability in the EMI environments, and need to be added in today's architecture [29].

8.13 Sustainability issues: The sustainability issues deals with the inner workings of the IEDs and are defined in the IEC 60870-4 and referred by the IEC 61850-3. In order to fulfill the requirements of the maintainability, there will be more burdens on the manufacturers.

8.14 Cost and complexity issues: IEC 61850 based substations cannot be successful if it is expensive to run its operational functions. It is the cost equation, which finally decides what can be employed in the field rather than what is manufactured, based on what is technically possible. Cost includes engineering design, construction and material cost, availability, and maintaining extra electronic equipment. Similarly, most of the substations are not new but either expanded or upgraded. Migration to IEC 61850 requires large investment making the process long, continuous, and complex. Therefore, there should be a seamless migration during the implementation of IEC61850 standard within specified time limits [18].

8.15 Logical node issues: IEC 61850 does not standardize which logical node should exist in an IED and most of the logical node content in the standard's documentation is optional, or may not be available or mapped. Even if some or all of the logical nodes are supported by the different IEDs, IEC61850 does not standardize the contents of the data. Therefore, there can be different collections of LNs in each IED, and the same LN in different IEDs can have different data. The standard only specifies that the logical nodes are supported and data is identified in SCL by an IED. However, this thing may create many problems and network designers have to get the SCLs and/or other parameters well in advance for selecting IEDs. IED is capable of creating and providing lot of information but the information mapped to the LNs is only available to the network designer. Therefore, in the standard, there will be different data availability between different IEDs [13].

8.16 A big standard: The standard is very big, and there are more than 40 total parts in IEC 61850, 14 of them are in core edition with a variation from easy to difficult understanding for each part. The easy parts document the common understanding of users while the more difficult parts involve issues where there is no right answer for every application. The standard is still evolving as mentioning different technical issues shown at (TISSUEs) even after 15 years [30].

8.17 Miscellaneous issues: Research has shown that there are many other issues because of IED

limitations and was unsolvable and forced the network designer to change the databases and naming conventions for the devices. One of the limitations is the eight character limit of the device name, so a redefinition of the naming database, and correspondingly a reconfiguration of the whole databases are required. Similarly, generic nodes are used as there is no mapping flexibility, i.e., mapping any IED digital value to a data object in a logical node. There are also issues while configuring HMIs and SCADA gateways during functional testing, i.e., control block names cannot be configured for all IEDs, and consequently writing to the report control block name is not possible. Some IEDs also do not have the ability to report something back to the HMI. Similarly, mapping is also an issue when double point indication is done with DNP3 and Conitel 2020 for breakers and sectionalizers. Moreover, servers are not able to handle the large number of IEDs, which can be accommodated in a project. Also windows version compatibility with new version of IEDs is another issue [15], [31]. Similarly, research has shown that issues are there while testing GOOSE messages for interlocks. Control block reference (CBR) cannot be more than 32 characters for some IEDs and many vendors cannot use selected CBR as limit exceeded several times due to the used naming convention. Similarly, some vendors are not able to subscribe the GOOSE messages from different devices by (import SCL files) from other vendors without respecting all the configuration parameters [31]. The available con- figuration and certification only provide some necessary task for a successful commissioning. It is the duty of the network designer to be sure that all the required data is supported by the IED and it is aligned well with other devices in the network.

Previous sections have presented many possible issues, challenges, and failures, which a utility can face while implementing IEC 61850 standard. There are many concerns such as standard is too big, challenging, difficult to understand everything, require rigorous amount of experience, and a huge possibility that system will fail or will give lot of troubles while implementing. Therefore, all of the above mentioned challenges and issues make it more difficult for a utility to adopt this standard. Therefore, if standard really wants that it should be adopted by utilities, it must have to take into account all possible measures to address these challenges and issues. The next section discusses about the future of the IEC 61850 standard.

9. Future of the IEC 61850 standard

There are many protocols which are used inside the SAS, i.e., distributed network protocol (DNP3- IEEE Standard 1815), IEC 870-5-101, IEC 60870-5-104 and Modbus, etc. The IEC 61850 has major advantages over these legacy protocols used in the substations on the data side, but it also has lot of issues and overheads as mentioned above. DNP3 is one of the leading protocols in North America utility. DNP3 evolved from traditional SCADA requirements for remotely monitoring and controlling assets in a reliable manner over a wide area using low bandwidth and potentially unreliable communication systems. It also provides a relatively

simple data values and control commands with a high degree of integrity and resilient methods for recovery from communication system failures. DNP3 has also seen wide adoption outside of the electric power systems, particularly within water and wastewater utilities. An IED in DNP 3 command requires only two attributes to be set to work on it as compared to six or more attributes required by IEC 61850 protocol. For commissioning of the IEC 61850 substation automation system into a North American utility, it has to interconnect it to a SCADA system which uses DNP3. A new standard, IEEE 1815.1, provides guidance on mapping data and functionality between IEC 61850 and DNP3. However, this mapping process automatically associates IEC 61850 semantics with each DNP3 data object allowing the semantic information known to the DNP3 outstation and masters, although never transmitted over the channel at run time. This improves the efficiency of DNP3 by getting rich object model information available from IEC 61850 [22], [32].

Newton-Evans Research Company conducted a survey in 2016 in North American protective relay marketplace. The participants in the survey were 79 electric utilities that include 16 investor-owned, 28 public power, 26 cooperatives, 4 electric power consulting groups, and 5 Canadian electric utilities. The question was asked whether your utility control system uses IEC 61850 protocol for substation automation or SCADA system. The response of the utilities were very surprising as about 80 percent of the respondents said that they have no use or plans for IEC 61850 in any area, and 89 percent said they don't use or plan to use IEC 61850 for SCADA. These results show that IEC 61850 is more complex as compared to other protocols and industry will take time to fully adopt it. Therefore, the standard will not overpass DNP3 in North American market in the near future. Survey also shows that especially LAN based DNP3 is still the most popular protocol in the industry in their future planning [33].

Although, the IEC 61850 standard offers many advantages due to its open nature, i.e., an availability of a wide range to operate, but it also increases the complexity of the IEC 61850 implementation task. The biggest disadvantages of IEC 61850 based SAS is that this standard is complex, requires new skills and tools, adds additional burden on network management, adds cyber security overheads, etc. Therefore, complexity and overheads reduce many benefits in many applications [34]. A lot of work is still required to address the current issues and challenges in order to make the standard more acceptable and implementable. Better integration tools, interoperability/interchangeability characteristics and better naming convention will definitely enhance the acceptance of the standard, so that it is easily read by every utility. Similarly, device independent and user friendly integration software should be made along with such vendor configuration software which is able to use the created SCL configuration files. Until all of these issues are not addressed, the end user will not be able to enjoy the available interoperability/interchangeability while working with multi-vendor equipment [6]. The next section discusses integrating IoT with IEC 61850.

10. Internet of Things (IoT) and IEC 61850

Internet of things (IoTs) is a communication technology, which makes everything capable of communicating with other things existing in this world such as homes, cars, animals, humans, farms, and industry, etc. A substation has always a large number of Intelligent Electronic Devices (IEDs); therefore, it is considered a natural application for IoT. However, integrating IoT in a substation environment has many challenges. The fundamental concept behind the IoT is that lot of sensors provide data to generate useful information for the required application. Each sensor uses a unique assigned address to feed information through public internet to cloud based applications. But, if the connected devices are huge in number as in a substation, it will require a major change how the addressing of the devices is done. Similarly, use of public Internet to communicate with field devices in a substation raises serious cyber security and Quality of Service (QoS) concerns [36, 37].

Energy sector has also well-defined communications technology and protocols, i.e., DNP3, and IEC 61850, and these protocols are not used in IT, web, and Internet applications. In IoT, most widely used Advanced Message Queuing Protocol (AMQP) supports a transactional model, making it more complex and not appropriate for edge devices. Energy sector protocols typically use a Master/Slave or Client/Server approach. Although, the web uses a client/server approach, but, it is based on a different paradigm and the HTTP protocol used in web is connectionless which also reduces the efficiency. Moreover, the data acquisition approach through Internet and in automation systems is very different. Although, Intel is already proposing a protocol for communication for substation environment, but to achieve true interoperability between different vendors is a big challenge, i.e., necessary for devices and applications to share a common data model. Vendors of networking devices offer Network Management Software (NMS) to support their devices, which is generally designed to support devices from a single vendor. However, the development of a universal management platform remains a challenge, and may not even be economically feasible [36, 37].

Another important challenge of IoT is to get a sense of the large amount of data produced by the sensors. It means that applications will need to be able to figure out the meaning of the data, i.e., the semantics, is the sensor reading voltage or temperature? Also, IoT uses the concept of cloud computing, and vendors are constantly evolving their applications and adding new features to keep up with market and customer requirements in energy sector, but organizations simply cannot afford to keep up with rapid change. IoT also requires extensive computing capability. However, even the smallest utility will face it difficult to maintain the applications and install updates to address bugs or security issues, i.e., extensive computing [36, 37].

The next section presents a case study of substation.

11. Case study of substation in wired and wireless architecture for End-to-End delay measurement of Sample Value (Type 4) messages.

11.1 Wired (Ethernet) topology

A case study was done by making an architecture of the substation in the bus and star topology for the end-to-end delay measurement of the Type 4 messages, i.e., station to process level network simulation model.

11.1.1 Bus topology: MUIED (Merging unit IED), BRKIED (Breaker IED), and PCIED (Process control IED), were designed in the OPNET Modular using object oriented modeling approach. PCIED is generally placed in the bay level and MUIED is generally placed in the process level. MUIED collects data from the process area, i.e., through CT's/PT's and transfers this information to the PCIED for further processing, i.e., sending a trip command to the BRKIED to open or close a breaker accordingly. PCIED is also connected to the central station through the station bus for the data exchange so that central station can perform supervisory actions. The node models (design) of the MUIED and BRKIED for bus topology are shown in Figure 6. The communication stack for the MUIED is very simple, i.e., application layer, Ethernet layer, and physical layer.

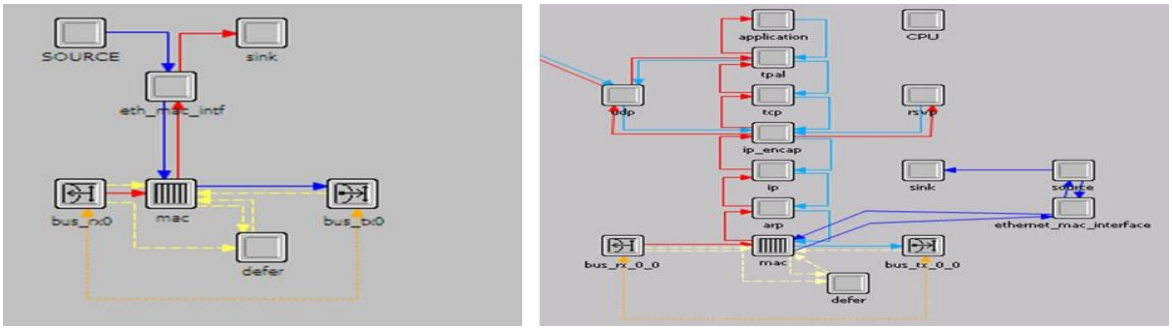

Figure 6. Node model diagram for MUIED (left), and BRKIED (Right) for Bus topology

Figure 7 shows the bus topology architecture of the substation and the end to end delay measurement of the SV messages from the process to station level.

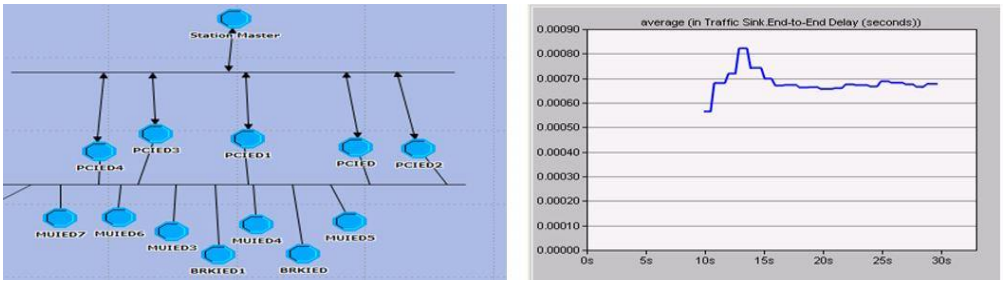

Figure 7. Bus topology architecture from station to process level (left), and SV End-to-End delay measurement

11.1.2 STAR topology: Similarly, MUIED, BRKIED, and PCIED for star topology were designed. Figure 8 shows the star topology architecture of the substation and the end to end delay measurement.

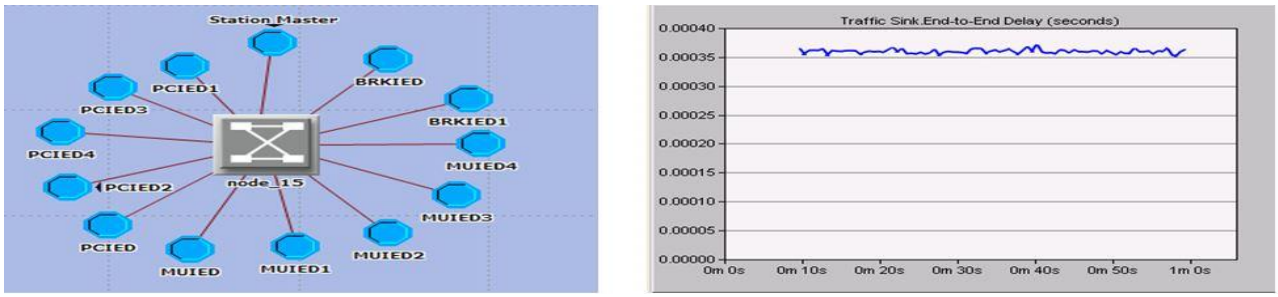

Figure 8. Star topology architecture (left), and SV End-to-End delay measurement (right)

The Ethernet standard IEEE 802.3 has been used with the CSMA/CD (Carrier sense multiple access/collision detection) media access approach for the transfer of data. The table below shows the measured values at different speed and frequency. The raw data source is the simple source with finite state machine.

Table 1. SV message End-to-End delay measurement for Bus and Star topology in wired architecture

LAN Speed (Mbps)	Sample /Sec	Sampled Value message average delay (msec) (Bus Topology)	Maximum delay (msec)	Sampled Value message average delay (msec) (Star Topology)	Maximum delay (msec)
10	480	0.8	1.4	0.3	0.35
10	960	1.0	2.0	0.3	0.37
10	1920	1.2	2.2	0.3	0.35
100	480	0.75	1.3	0.3	0.32
100	960	0.75	1.3	0.3	0.32
100	1920	0.7	1.2	0.3	0.32

Table 1 shows that for bus topology at 10 Mbps, delay increases as the number of samples increases. However, at 100 Mbps, the delay does not increase by increasing the number of samples, and its value is also less as compared to the delay at 10 Mbps. For star topology, the end-to-end delay does not increase with the increase of the samples, and delay is also less as compared to the bus topology. For the bus topology, sometimes stations find the medium busy especially for the case of the low data rate transfer and high number of nodes. The data shows that the end-to-end delay is within the allowed limits of the standard, i.e., 3-4 msec, for the time

critical messages (protection), and automation and metering application messages [16], [17]. This data also shows that it should be avoided to send larger packet size, i.e., samples, to meet the standard guidelines, especially for bus topology at low speed, i.e., 10 Mbps.

11.2 Wireless topology

Even with the advance architecture of the substation, cabling in the substation accounts for large amount of money and complexity, which can be reduced either fully or partly by performing the substation automation functions wirelessly. Therefore, a wireless topology was created as shown in figure 9, and different wireless IEDs (MUIED, BRKIED & PCIED) has been placed in the substation in an ad-hoc mode with no centre access point. The layout (design) of the MUIED for wireless topology is shown is also in Figure 9.

.

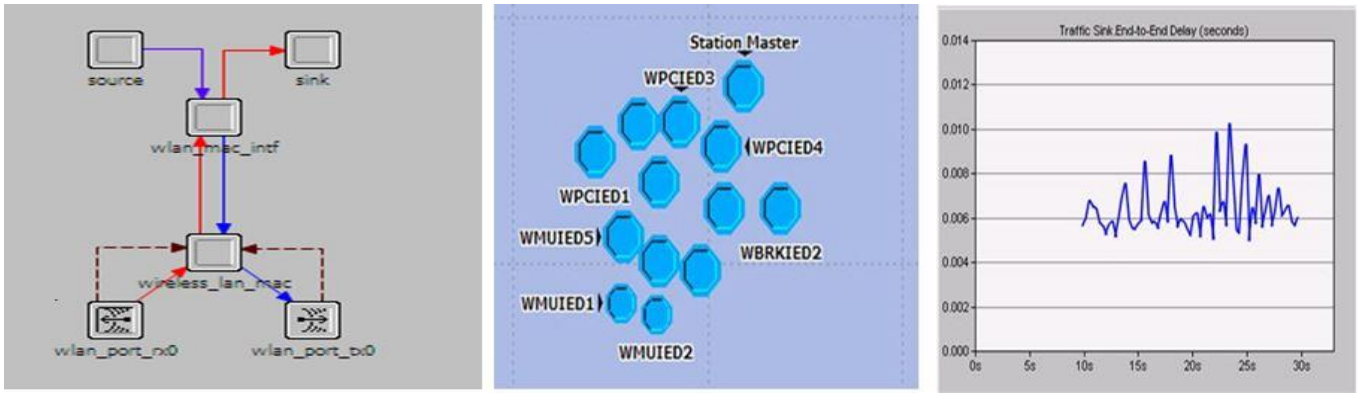

Figure 9. Node model diagram (left) for MUIED, wireless topology architecture (middle), and SV end-to-end delay measurement (right) for wireless topology architecture

Table 2 shows the results for different data rates and for different samples in case of wireless architecture.

Table 2. SV end-to-end delay measurement for wireless architecture

Data Rate (Mbps)	Sample/Sec	Sample Value Message (average delay)	Sample Value Message (maximum delay)
11	50	6 msec	10 msec
11	75	20 msec	80 msec
11	100	0.5 sec	1.0 sec
11	480	2.0 sec	3.0 sec
11	960	2.0 sec	3.0 sec
11	1920	2.0 sec	3.0 sec
54	50	5.0 msec	10.0 msec

54	75	1.0 sec	1.2 sec
54	100	2.5 sec	2.5 sec
54	480	3.0 sec	3.0 sec
54	960	3.2 sec	3.0 sec
54	1920	3.3 sec	3.0 sec

Table 2 shows that for both 11 and 54 Mbps, the delay increases as the number of samples increases. However, the maximum delay is almost the same for different data rates, as the sample size increases. The end-to-end delay for the wireless medium is more as compared to the wired medium. This is due the fact that in wireless medium, electromagnetic interference, radio frequency interference, signal fading, and the attenuation of the signal by bouncing off with the obstacles are the main reasons of the loss of signals. The data also shows that the end-to-end delay is not within the allowed limits of the standard, i.e., 3-4 msec, for the time critical messages, i.e., protection [17]. However, this delay is still within the limits of standard for the automation and metering applications [16].

The results show that for practical applications, the size of the sample should be small to ensure reliable and real time data transmission. The main factors affecting delay are samples per second, communication architecture (bus, star or wireless), and Ethernet link bandwidth. Similarly, for important messages, the specific protection IEDs should be connected on the same Ethernet switches in order to get fast and reliable delivery.

The next section provides an overall discusses.

12. Discussion

All of the issues/challenges have been described in the above sections. First of all, paper presents in detail about the physical issues, i.e., hierarchical, with a detailed analysis for process bus challenges in substation automation system, describing that how much it is important to deal with the hierarchical and topological issues. As process bus takes care of the equipment directly attached to switchyard, therefore any failure in process bus will ultimately affect the whole substation. For a secure and reliable communication within the substation network, Ethernet topology, time critical requirements, selection of the functions and performance requirements, etc., should be selected carefully. Then paper discusses in detail about interoperability and interchangeability issues when there are devices from different manufacturers. The paper describes that interoperability and interchangeability are one of the big challenges for the rapid expansion and growth of IEC 61850.

Similarly, commissioning issues have been discussed, which should be standardized and prepared according to the requirement in advance, as standard is still new. The paper then

presents a detailed analysis of the security issues, i.e., cyber security, logical, and software failures in IEC 61850 based SAS. This issue/failure can cause problems for data communications within SAS and also outside the substation, ultimately affecting the performance of the utility up to the severe level. Software failures and security issues has become a serious challenge to the IEC based SAS as compared to the existing relay based models and require a detailed study and a secure solution. Therefore, an in-depth study and solutions understanding is required before planning a new cyber physical substation infrastructure in order to build a safe and steady power energy source. The paper also discusses manpower skills and training issues for the implementation of SAS in a utility. The paper specifies the importance of workers skills, organizational culture, training and competency levels, etc. for the implementation of IEC 61850 in a utility. The paper finally discusses in detail about the future of IEC 61850 protocols, especially in North American utility, where the standard is still facing a strong competition from DNP 3 protocol. It will take a long time for the IEC 61850 protocol to widely adapt by the utilities, especially if all of these challenges are not addressed.

13. Conclusion

Many papers have been published highlighting the different technical challenges and issues for the IEC 61850 based SAS. However, these papers generally discuss one or two issues, i.e., implementation or interoperability, or cyber security, etc., and do not present a comprehensive and detailed overview of all the challenges and issues. This paper presents a comprehensive overview (all possible issues with detail) of all kinds of technical issues and challenges faced by the IEC 61850 based SAS, i.e., hierarchical structural issues, implementational issues, reliability, interoperability, interchangeability, synchronization, latency, cyber security, commissioning, manpower training and skill, and all other different issues, etc. Moreover, other issues such as good architecture, appropriate redundancy, operational and functional stuff, backup system for high availability, reliability, latency, environmental, sustainability, synchronization, comprehensive testing process, cost, substation expandability, functions allocation, reliable protocols for integration and security, etc. have been discussed in details in this paper. The paper finally also discusses about the future of IEC 61850 protocols, especially in North American utility, where the standard is still facing a strong competition from DNP 3 protocol. The paper also discusses about the challenges of integrating IoT with IEC 61850.

The paper also presents a case study of the measurement of end-to-end delay of SV messages, i.e., type 4, for the wired (bus and star topology) and wireless substation architecture. The results show that the delay is within the limits in case of Ethernet (bus and star) topology, but, the delay is not within limits for wireless topology as defined by the standard due to invariant noise and distance, and other physical factors. Therefore, which medium should be used, i.e., wired or

wireless, can be decided based on the substation environment, utility requirements and keeping in mind of the merits and demerits of both approaches.

Although, IEC 61850 is much more than a protocol, and offers communication services for real time applications, offers metadata among devices and services, multiple information models and a system configuration language, but the paper has presented it clearly that it is not possible to develop a well functional IEC 61850 based SAS without understanding and addressing all these challenges. Addressing these issues and challenges will maintain the consistency throughout the life time of the substation, i.e., checking and verifying during the commissioning process, replacing the failed IEDs, conducting preventive maintenance, and adding new IED to the existing system. The utilities still need time to move to this standard for adaptation, as it is also a big standard, still updating itself increasing its complexity, and efforts (workers training and skill, cost, management issues, utility atmosphere, etc), with all of the above mentioned issues.

14. References

[1] T. A. Youssef, M. E. Hariri, and O. Mohammed, "IEC 61850: Technology Standards and Cyber Security Threats," in Environment and Electrical Engineering (EEEIC), pp. 1-6, July 2016.

[2] A. Elgargouri, R. Virrankoski and M. Elmusrati, "IEC 61850 based smart grid security," in IEEE International Conference on Industrial Technology (ICIT), pp. 2461–2465, March 2015.

[3] P. Parikh, and T. Sidhu, "A Comprehensive Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substation Applications," IEEE Transactions on Industrial Informatics. vol. 9, no. 3, pp. 1466-1476, July 2013.

[4] T. Sidhu, M. Kanabar, and P. Parikh, "Implementation Issues with IEC 61850 Based Substation Automation Systems," in National Power Systems Conference (NPSC), pp. 473- 478, Nov. 2008.

[5] B. Adhikary, S. Rao,"Implementation aspects of substation automation systems based on IEC61850," International Conference on Control, Instrumentation, Energy and Communication, pp. 442-445, May. 2016.

[6] S. Mohagheghi, J. Stoupis and Z. Wang, "Communication protocols and networks for power systems current status and future trends**,"** in IEEE/PES Power Systems Conference and Exposition, pp. 1-9, Aug. 2009.

[7] T. Yousef and O. Mohamed, "On the implementation of the IEC 61850 standard: Will

different manufacturer devices behave similarly under identical conditions?" Journal of Electronics, vol. 5, no.85, Dec. 2016.

[8] B. Falahati and E. Chua, "Failure Modes in IEC 61850-Enabled Substation Automation Systems," in IEEE/PES Transmission and Distribution Conference and Exposition, pp. 1-5, Jan. 2016.

[9] G. Igarashi and J. Santos, "Challenges to the Implementation of a Real-Time Process Bus According to IEC61850-9," in IEEE PES Innovative Smart Grid Technologies, pp. 1-6, Jan. 2014.

[10] D. Hou and D. Dolezilek, "IEC 61850 What It Can and Cannot Offer to Traditional Protection Schemes," SEL Journal of Reliable Power, vol. 1, no. 2, pp. 266–279, Oct. 2010.

[11] J. Shin and S. Eom, "Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying," IEEE Transactions on Power Delivery, vol. 26, no. 2, pp. 725–735, March 2011.

[12] P. T. Tiago, "Emerging technologies and future trends in substation automation systems for the protection, monitoring and control of electrical substations," M.Sc. Thesis, Faculdade de Engenharia da Universidade do Porto, Portugal, Nov. 2013.

[13] D. Dolezilek, "IEC61850: What You Need to Know About Functionality and Practical Implementation," in Power Systems Conference: Advanced Metering, Protection, Control, and Distributed Resources, pp. 1-17, July 2006.

[14] M. Haffar, J. Thiriet, and E. Savary, "Modeling of substation architecture implementing IEC 61850 protocol and solving interlocking problems", IFAC Proceedings volumes, vol. 22, no. 40, Sep. 2007.

[15] B. Muschlitz, "IEC 61850 INTEROPERABILITY, THE GOOD THE BAD AND THE UGLY," Technical report, Nova tech Corporate Communications, USA, April 2015.

[16] N. Hasan, B. Mohd, and F. Hisyam, "Comparisons process-to-bay level peer-to-peer network delay in IEC 61850 substation communication systems," Journal of Electrical Systems and Information Technology, vol.1, no.3, pp.266–275, Jan. 2014.

[17] S. Kumar, and S. Islam, "Performance evaluation of a process bus architecture in a zone substation based on IEC 61850-9-2," in IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1-5, 2016.

[18] B. Adhikary, S. Rao and S. R. Balasani, "Implementation Aspects of Substation

Automation Systems based on IEC 61850," in Instrumentation, Energy and communication (CIEC), pp. 442-445, Aug. 2016.

[19] A. Hamdon, "Standards Are Note Enough! Challenges of IEC-61850 Interoperability," Tech. Report, Solutions Incorporation, Canada, Dec. 2016.

[20] I. Shin, B. Song, and D. Eom, "International Electronical Committee (IEC) 61850 Mapping with Constrained Application Protocol (CoAP) in Smart Grids Based European Telecommunications Standard Institute Machine-to-Machine (M2M) Environment," in Energies, pp.1-13, June 2017.

[21] R. MattCole, R. Arnold, "Cyber security Challenges of Implementing IEC-61850 for Automation Between the Smart Distribution Control Center and the Substation," Tech. Report, Sargent & Lundy, LLC., Feb.2017.

[22] P. Thunga, "Security aspects of smart grid communication," M.Sc. Thesis, Univ. of Waterloo, Canada, July 2012.

[23] P. Kreutzer, "Future trends substation automation and IEC 61850," Tech. Report, ABB., Germany, Aug. 2012.

[24] T. Youssef and O. Mohammed, "On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly under Identical Conditions ?", Journal of Electronics, vol. 5, no. 85, Aug. 2016.

[25] T. Robert and G. Dogger, "Hidden Challenges in the Implementation of IEC 61850 in Larger Substation Automation Projects," Tech. Rep., Cooper Power Systems, Cybectec Energy Automation Solutions, China, March 2007.

[26] A. Semjan, and J. Naibo, "Experience Sharing Challenges and Solutions on IEC 61850 Substation Commissioning in Thailand," in IEEE PES GTD International Conference and Exposition Asia (GTD Asia), pp. 228-234, July 2016.

[27] R. Madiba and L. D. Erasmus, "Organizational impact of implementing IEC 61850 standard for communication networks and systems in substations," in Proceedings of PICMET '13: Technology Management in the IT-Driven Services (PICMET), pp. 2681-2689, March 2013.

[28] D. Dolezilek, "Using information from relays to improve the power system,"SEL Journal of Reliable Power, vol. 1, no. 2, Oct. 2010.

[29] M. Mekkanen, "On Reliability and Performance Analyses of IEC 61850 for Digital SAS," M.Sc Thesis, University of VAASA, Finland, Oct. 2015.

[30] IEC 61850 Tissue Database. https://iec61850.tissue-db.com/default.mspx, 2015.

(accessed 13 Nov. 2019)

[31] V. M. Flores, D. Espinosa, J. Alzate and D. Dolezilek, "Case Study: Design and Implementation of IEC 61850 From Multiple Vendors at CFE La Venta II," in International Conference of Relay Protection and Substation Automation, pp. 307-320, Nov. 2007.

[32] A. West, "1815.1-2015 - IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]", https://standards.ieee.org/standard/1815_1-2015.html, Dec. 2015 (accessed on 19 September 2019)

[33] Newton-evans research. https://digitalsubstation.com/en/2016/09/20/newton, 2016. (accessed 21 Nov. 2019)

[34] H.F. Maragal, "Emerging Technology Roundtable Substation Automation-IEC 61850," Tech. Rep., North American Reliability Corporation - NERC, 2016.

[35] D. Baigent, M. Adamiak, R. Mackiewicz, "IEC 61850 Communication Networks and Systems in Substations: An Overview for Users", The Protection & Control Journal. 61-68, July 2009.

[36] Maciej, Integrating IoT with IEC 61850. https://www.jpembedded.eu/en/integrating-iot-with-iec-61850/, 2018. (accessed 26 April. 2020)

[37] Jacques Benoit, "The internet of things and energy sector: myth or opportunity," power and energy automation conference, Spokane, Washington, March, 2016.