Vaasan yliopisto
UNIVERSITY OF VAASA

MIKE MEKKANEN

On Reliability and Performance Analyses of IEC 61850 for Digital SAS

ACTA WASAENSIA 336

COMPUTER SCIENCE 15

Reviewers

Professor Matti Lehtonen
Aalto University
Department of Electrical Engineering and Automation
P.O.Box 13000
00076 Aalto
Finland

Dr. Faisal A. Mohamed
Libyan Authority for Research,
Science and Technology
Tripoli, Libya

Julkaisija Vaasan yliopisto	**Julkaisupäivämäärä** Lokakuu 2015	**Julkaisun tyyppi** Monografia

Tekijä(t)
Mike Mekkanen

Julkaisusarjan nimi, osan numero
Acta Wasaensia,336

ISBN
978-952-476-644-9 (painettu)
978-952-476-645-6 (verkkojulkaisu)

Yhteystiedot
Vaasan Yliopisto
Teknillinen tiedekunta
Tietotekniikan yksikkö
PL 700
65101 Vaasa

ISSN
0355-2667 (Acta Wasaensia 336, painettu)
2323-9123(Acta Wasaensia 336, verkkojulkaisu)
1455-7339 (Acta Wasaensia. Tietotekniikka 15, painettu)
2342-1282 (Acta Wasaensia. Tietotekniikka 15, verkkojulkaisu)

Sivumäärä	**Kieli**
202	Englanti

Julkaisun nimike
Yhteentoimivuus- ja suorituskykyanalyysi IEC 61850 sähkönjakeluautomaatiolle

Tiivistelmä

Viime vuosina sähkölaitoksilla on ollut vahva suuntaus kohti uusia teknologioita ja standardeja vastatakseen yhä suuremman energiantarpeen tuomiin uusiin vaatimuksiin. Lisäksi on odotettavissa, että uusiutumattomista energianlähteistä tulee tulevaisuudessa pula. Yksi merkittävimmistä tehtävistä on kehittää uusi ratkaisu, joka tukee parempaa sähkönjakelun laatua ja hajautetun sähköntuotannon kehitystä kohti älykästä sähköverkkoa. Standardoitu ratkaisu (IEC 61850) tarjoaa energiajärjestelmille lupaavan automaatio- ja suojeluratkaisun, jolla on suuri vaikutus sähköasemien asennus-, käyttö- ja huoltotoimintoihin. Lisäksi se lisää luotettavuutta, saatavuutta ja joustavuutta sähköverkkoon, joka liittää sähköntuotannon ja tehonkulutuksen yhteen uudella dynaamisella tavalla. IEC 61850 -standardiin perustuvat kommunikointiprotokollat mahdollistavat sähköasema-automaatiolle uudenlaisia ratkaisuja, jotka tarjoavat myös tehokkaan suorituskyvyn. Tämä tehokkuus mahdollistaa reaaliaikaisen tiedonjakamisen, elinkaarikustannusten vähentämisen sekä tarjoaa yhteentoimivuutta, joka on todettu yhdeksi tärkeimmistä motiiveista sen käyttämiseen. Sarjamuotoinen asynkroninen viestintä ja perinteiset protokollat, joita nykyään käytetään, kaipaavat uudistusta.

Tutkimus analysoi ja arvioi melko uuden IEC 61850 standardin suorituskykyä sähkönjakeluautomaatiojärjestelmissä (SAS). Tutkimuksessa määritellään aiemman sukupolven sähköjärjestelmien piirteet ja tarve täsmentää tehokas tapa sähköjärjestelmien päivittämiseen, siirtämiseen ja sovittamiseen uuteen. Kirjassa ehdotetaan uutta luotettavuuden ja vikatodennäköisyyden arviointimenetelmää RaFSA:ta, joka voi helpottaa energiajärjestelmien suunnittelua. Kirjassa on toteutettu laaja intensiivinen simulointi, joka osoittaa ehdotetun tekniikan mahdollisuuksia. Simulointi on todettu tärkeäksi menetelmäksi, joka mallintaa todellisen reaaliaikainen järjestelmän käyttäytymistä kun simuloidaan sekä varsinainen prosessi ja järjestelmän satunnainen käyttäytyminen. Tämän lähestymistavan auttamiseksi määritellään luotettavuusmittarit ja testataan IEC 61850:n toimintoja. Useita SAS-viestinnän väylätopologioita testattiin katkaisijavikasuojan turvatehtävän (BFP) toimintatilanteissa. Ne osoittivat, että rengastopologia tarjoaa parhaan luotettavuuden ja pienemmän todennäköisyyden epäonnistua. Lisäksi työssä suunniteltiin ja rakennettiin kokeellisia SAS-kokoonpanoja eri valmistajien laitteiden yhteentoimivuuden testaukseen. Työssä on esitelty useita DEMVE laboratoriossa suoritettuja käytännön SAS-testauskokeiluja ja tuloksia. Saavutetut tulokset ovat auttaneet tunnistamaan tarpeen toimittajavapaan järjestelmän konfigurointityökaluun, sekä määritelleet rajat ja kapasiteetin SAS-viestintäjärjestelmäverkolle. Suuri määrä uutta teknistä ja käytännön tietoa SAS-suunnittelu- ja kokoonpanoprosesseista on saatu aikaan. Työn aikana tunnistettiin myös useita tulevia tutkimusaiheita ja -kysymyksiä.

Asiasanat
IEC 61850, sähköasema-automaatio SAS, yhteentoimivuus, GOOSE, SV, älykäs sähköverkko.

Publisher
Vaasan yliopisto

Date of publication
October 2015

Type of publication
Monograph

Author(s)
Mike Mekkanen

Name and number of series
Acta Wasaensia, 336

Contact information
University of Vaasa
Faculty of Technology
Department of Computer Science
P.O. Box 700
Fi-65101 Vaasa
Finland

ISBN
978-952-476-644-9 (print)
978-952-476-645-6 (online)

ISSN
0355-2667 (Acta Wasaensia 336, print)
2323-9123(Acta Wasaensia 336, online)
1455-7339 (Acta Wasaensia. Computer Science 15, print)
2342-1282 (Acta Wasaensia. Computer Science 15, online)

Number of pages
202

Language
English

Title of publication
On Reliability and Performance Analyses of IEC 61850 for Digital SAS

Abstract

During the last years utilities have been facing a strong trend towards new technologies and standard to meet the new requirements of higher energy demands at expected shortage of the nonrenewable sources of energy. One of the most significant tasks is to bring a new solution that supports better quality electricity supply and to support the evolution of the decentralized electric generation towards smart grid approached. Standardized solution (IEC 61850) in terms of auto¬mation and protection within energy system is a promising solution that provides a great impact on substation installation, operation and maintenance. Furthermore, it increases the reliability, availability and flexibility of the electric energy grid that linked power generation with power consumption in a dynamic manner. The communication protocols based on the IEC 61850 standard in the substation automation enables a new kind of solutions that provides an efficient performance. This efficiency has been introduced by means of sharing real-time information; reducing life-cycle costs; and providing interoperability, which is identified as one of the main motivations for its use. Serial asynchronous communication and legacy protocols are the existing solutions that being used today in which that needs to refurbish.

This work analyzes and evaluates the performance of the relatively new approach IEC 61850 standard within the Substation Automation System (SAS). Furthermore, it defines the existing legacy power system and the needs to specify the efficient way to upgrade, migrate and retrofit the legacy power system. A novel reliability and probability of failure estimation method RaFSA, which may facilitate the energy systems design has been proposed. An intensive simulation approach to demonstrate the proposed techniques have been given. The simulation is a high valuable method that simulates the actual behavior of the real time system upon simulating both the actual process and the system random behavior. To assist this approach and defined the reliability of the IEC 61850 functions. Several SAS communication bus topologies upon breaker failure protection function (BFP) are tested. They have been shown that ring topology provides the higher reliability and less probability of failure result values. Moreover, designing and construction of the experimental SAS, configurations and interoperability testing between multi-vendor devices. Several SAS practical testing experiments and results thorough DEMVE laboratory are presented and discussed. The achieving results have identified the need for the vender-natural system configuration tool and specified the limits and capacity of the SAS communication system network. High technical and practical experiences have been achieved through the SAS design and configuration processes, several future work issues were identified.

Keywords
IEC 61850, SAS, Interoperability, GOOSE, SV, IED, Smart Grid.

ACKNOWLEDGEMENT

I would first like to thank my advisor Professor Mohammed Salem Elmusrati, whose vision, open mind, technical support and guidance during my study. I deeply admire his encouragements and advisements from the initial to the final state of the work.

I would be also very much thankful to my co-supervisor Professor Erkki Antila, his research approach within DEMVE project and genuine interest in understanding the true nature of things, his advising style that always provides positive attitude help me to discover a new research area.

I also want to thank Mr. Reino Virrankoski for his advices, valuable discussion and great efforts to explain questions clearly and simply.

I am particularly indebted to University of Vaasa, Telecommunication engineering group, and DEMVE project Vaasa University group, whom gives me a chance to continue and financial support during my study from 2011-2014, Vaasa University Foundation during 2014-2015.

I would like to thank the Department of Computer Science members and the Faculty of Technology for the support and providing friendly and encouraging work atmosphere, Dr. Jari Töyli, Professor Timo Mantere, Professor Kimmo Kauhaniemi , Mr. Petri Ingström, , Professor Jarmo Alander, and Miss. Johanna Annala. Also I would like to thank the Lab engineers. Mr. Veli-Matti Eskonen and Mr. Juha Miettinen for helping and supporting. Moreover, I would like to thank all my friends in the ComSys Group and VAMK, for instance, Tomas Höglund, Omar Abu-Ella, Tobias Glocker, Matti Tuomala, Caner Cuhuc, Ruifeng Duan, Ahmmed Elgargure, Timo Rinne, Jari Koski, Sami Karpiniemi, Matias Mäkinen and Peilin Zhang.

Finally, I am extremely grateful to my wife, Leila my daughter Dina and my son Romeo for their eternal love, encouragement, understanding and supporting, making it possible for me to complete this thesis.

Contents

Figures

Tables

Abbreviations

ACSI	Abstract communication service interface
AVR	Automatic voltage regulator
CSMA	Carrier sense multiple access
CUT	Coordinate universal time
DER	Distributed Energy Resources
DNP	Distributed network protocol
EPS	Electrical power system
FACT	Flexible alternating current transmission system
GOOSE	Generic objective oriented substation events
GPS	Global positioning system
GSSE	Generic service substation events
HMI	Human machine interface
HVDC	High-voltage direct current
IEC	International Electrotechnical Commission
IED	Intelligent electronic devices
IRIG-B	Inter-Range instrumentation group time code B
ISO	International system organizer
LAN	Local area network
LD	Logical device
LN	Logical node
MMS	Manufacturing message interface
MU	Merging unit
OSI	Open system interconnection
PLC	Programmable logical controller
PMU	Phasor measurements unit
RSTP	Rapid spanning tree protocol
RTU	Remote terminal unit
SAP	Service access points
SAS	Substation automation system
SCADA	Supervisory Control and Data Acquisitions
SCL	Substation configuration language
SCAM	Specific communication service mapping
SNTP	Simple network time protocol
SPS	Special protection scheme
SV	Sampled value
TS	Time Synchronization
UCT	Universal Co-ordinated time
VLAN	Virtual local-area network
VMD	Virtual manufacturing device
VPN	Virtual private network
WAMC	Wide-area monitoring and control
WAN	Wide area network
XML	eXtensible Markup Language

1 BACKGROUND

This chapter considers existing power systems and presents a promising solution for them (IEC 61850 standard) by highlighting the initial publication review as a background for my research. It considers how existing power systems operate and future demands, with a view to discovering and highlighting the bottleneck of existing power systems, and whether the available solutions associated with their implementation challenges are suitable to upgrade, retrofit or migrate to these new solutions, which eliminate existing power systems' limitations. Challenges that might prevent the implementation of the new solution are specified and settled via experimental verification, which is presented in detail in the rest of this thesis.

1.1 Introduction

Recently, utilities have witnessed a strong trend towards new standards and technologies, fundamentally transforming their capabilities and bringing a new solution that supports and meets their existing and future demands. However, existing power systems' automation and protection have traditionally used proprietary manufacturer-specific communication protocols carried over other protocols for various applications. According to these infrastructure interfaces among power system nodes, intelligent electronic devices (IEDs) from various manufacturers may require huge investment based on developing a costly and complicated protocol convertor. Consequently, conditional power quality supply has been highlighted in recent years, and new laws, taxes and deregulation have been issued for instance, in Finland penalties have been regulated for non-delivered energy, while Sweden has issued a new law such that no interruptions longer than 24 hours are allowed after the year 2011 (Brändström & Lord 2009). Therefore, one of the most dominant considerations of current and future power system design comprise the standardization solution, product-featuring, smooth integration and a higher degree of adaptability, such that it may be used to revolutionize power systems' operation, improving reliability as well as maintenance, and reducing the installation time and effort. In order to address these issues, in 2003, the International Electro-technical Commission (IEC) Technical Committee (TC)-57 has published the IEC 61850 standard, entitled "Communication Networks and Systems in Substation" (IEC 61850 standard), which is defended as a common inter-national standard and one of the most promising powerful solutions to existing power industry limitations, and which is expected to support power systems' evolution. As far as the IEC 61850 standard is concerned, it is a promising solution to existing power systems' limitations; however, various aspects are not specified within the IEC 61850 standard and are left for end-use for instance, the highly reliable substation automation system (SAS) communications bus topology, types of redundancy, etc. Moreover, researchers and developers have noted that the open nature of the IEC 61850 standard gives broad freedom for manufacturers to operate with. Further, the interpretations of the IEC 61850 standard from different manufacturers remain different based upon the ambiguity that still exists. These issues may vary the interoperation of the standard from one manufacturer to another and may increase the complexity of the interoperability tasks within the SAS. In addition, many of the available automation and protection functions are grounded upon the emerging concept of a smart grid (SG) based on the IEC 61850 standard are whether need to be developed, or initially invented in which that softly amendment solutions are no more feasible. This is because several principles of conventional power systems, such as the radial topology, passive nodes, one-way power flow, etc., are not maintained anymore. Therefore, further discussion and testing works need to be processed, and revolutionary energy system infrastructure changes might need to be based upon the IEC 61850 standard in order to meet end users' requirements and prove the feasibility of the IEC 61850 standard (i.e., that it possesses high-energy system reliability and is fault-tolerant).

Meanwhile, the global acceptance of the IEC 61850 standard has raised its profile as an interesting area of research, from both the academic- and the industry-side. This wide acceptance has stimulated researchers and developers to go further towards plug-and-play-based IEC 61850 implementations within SAS and beyond to an SG. For coping with these demands, various research groups and pilot projects have been carried out globally - for instance, the University of Vaasa has set-up an in-house research and testing laboratory, the Development of Education Services of IEC 61850 in a Multi-Vendor Environment (DEMVE). All my research activities have taken place under the umbrella of two projects, namely DEMVE I and DEMVE II. These projects raise the vision and the spirit of the IEC 61850 standard based on sharing data among various manufacturers' intelligent electronic devices (IEDs) and executes the information that has been shared by this data (i.e., interoperability). Interoperability is one of the main concerns regarding the IEC 61850 standard. Moreover, it has also been considered as the major challenge faced by SAS design engineers in establishing seamless communication among various manufacturers' IEDs. However, initially, substation automation and protection was the main focus of the IEC 61850 standard's first version. The key point is that it provides a uniform framework for all the related system levels. IEC 61850 takes into consideration all the various aspects that are common at the substation site, such as data models, communication solutions, engineering and conformity testing. The legacy protocols concentrate on how the data is transmitted on the channel. Meanwhile, it organizes the data - in terms of applications - by means of syntax and semantics in the devices where they do not specify it. The main aspect that IEC 61850 adopts based on its architectural construct is “abstracting” the data object’s definition and services. Independently of any underlying protocol, it creates data objects and services that support a comprehensive set of substation functions and it provides strong services to facilitate substation communication. The abstract definitions of the data object allow its mapping to any protocol that can meet the best data and service requirements, as IEC 61850 does not specify any protocol. IEC 61850 specifications focus on three major issues, namely standardizing the available information, services (write, read, etc.) and communication services. Further, the IEC 61850 standard in Part 8 and Part 9 (IEC 61850-8; IEC 61850-9) specifies Ethernet communication technology based on the open system interconnection (OSI) model for the station and the process level within the SAS. Ethernet technology has been defined as an appropriate communication solution for power automation usage based on its high flexibility, bandwidth and speed.

This thesis provides guidelines and facilitates the design and implementation of the IEC 61850 standard within an SAS. It first considers the relatively new IEC 61850 standard from different perspectives. An explorative study and analysis of the IEC 61850 standard and the legacy power system are conducted which demonstrate the impact of the IEC 61850 standard on the legacy power system’s infrastructure, such that it might not meet the requirements imposed by electricity utilities’ deregulation. Furthermore, various reliability and availability analyses have been carried out on different SAS communications bus topologies. Secondly, several practical testing experiments for the SAS based on the IEC 61850 standard are designed, constructed and carried out. These practical testing experiments are implemented to evaluate and prove the feasibility of the IEC 61850 standard as a promising solution for the communications system within the energy system. Lastly, a favorable communication solution based on a new communication technology, cognitive radio (CR), for a future SG is proposed. Strong practical experience was gained through the SAS configuration process, several contributions were made based upon these analyses and some future work issues were identified (more details about these contributions are presented in Section 1.6).

1.2 Power System New Opportunities for Protection and Automation

Growing world economies and populations are expected to increase electrical energy consumption two-fold by 2050, and according to the International Energy Agency study climate change is the gravest global challenge facing energy utilities (VTT 2009). Energy systems produce energy services for society's needs. An energy system can be seen as a complex of many interlinked units or chains. Typically, the chains are composed of elements (e.g., power generation, a substation, conversion, transmission, etc.). Meanwhile, protection and automation in power systems are two of the main infrastructures supporting the reliability and flexibility of electrical grids that link power generation units with power consumptions in a dynamic manner. Energy systems, based on a growing and changing market, have been forced to retrofit and update legacy energy systems. Utilities now look at methods for efficient utilization that incentivize power quality improvements, permitting higher profits by increasing interest in state-of-the-art solutions that decrease outage costs. This is the case where the capacity for controlling energy flows from source to consumers and the stability and maintainability of the energy grid are the main concern, whether or not the solutions are based on conventional methods or new technologies.

A few years ago, managing the energy system's infrastructure was the main focus and it occupied the attention of utilities. The objective of conventional power system control is to maintain system stability. In order to achieve this goal, it may require conventional actuators (e.g., an automatic voltage regulator (AVR), power system stabilizers (PSSs) and a flexible alternating current transmission system (FACTS). These instruments have to be considered within the control algorithm, which is based on a single, independent control loop. The outputs of these algorithms are then used as a combination of advanced controlling techniques' solutions as illustrated in Figure 1.

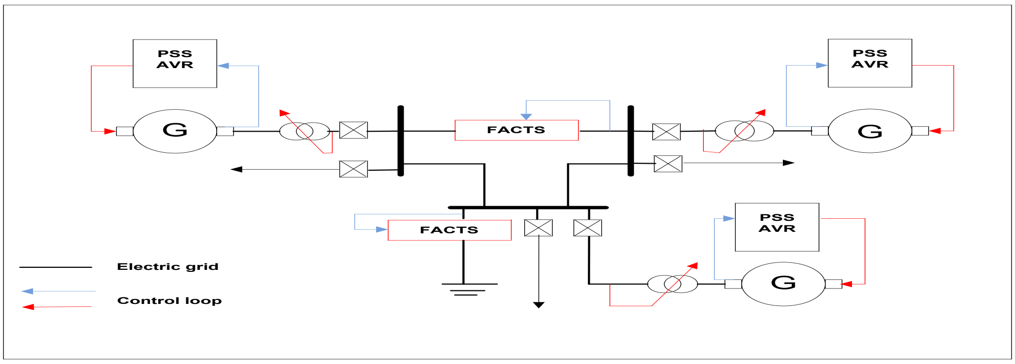


Figure 1. Traditional control of EPS single independent local control loops.

This incomplete vision has changed given the concept that two infrastructures must be managed, along with the energy system infrastructure and the communication information system infrastructure (Korba et al. 2005). Existing SAS communication and information systems are mainly designed according to the electricity production and consumption infrastructure which existed several decades ago, and they lack coordination among various operational entities. These entities are introduced into the energy grid by an incoming burst of distributed renewable energy resources (an SG).

The emerging concept of an SG has set completely new requirements for energy systems. Distributed production requires distributed automation, which in turn requires advanced communication solutions to operate reliably. Communications networks within energy systems enables a new kind of solution that provides intelligent performance. This intelligence has been introduced by means of exchanging real-time information, whereby different active nodes are linked with a bidirectional communications network system. Today, communication technology offers the possibility of opening the circuit breaker far from detected deviations. These abilities open the door to remote or wide-area monitoring and control (WAMC) platforms and central management services that pre-process the aggregated information throughout the entire power system. Furthermore, they permit the sharing of information between different utilities, which allows for a real-time view of the entire energy grid (Kezunovic 2007).

As such, the future trends in terms of energy system protection and automation are to mi-grate from a local measurements supervisory control and data acquisition (SCADA)-based approach to a dynamic measurement system. To realize such a system, synchronized phasor measurement units will be implementing together with the stability assessment and stabilization algorithms. Phenomena such as frequency deviation, thermal line overheating, circuit breaker status, voltage in-stability, etc., will be dynamically monitored and shared among the energy system nodes. Furthermore, power system stability can be characterized in real-time and the protection solution setting can be selected from the available entities based on learning. The WAMC power system is shown in Figure 2 (Tholomier & Jones 2010) (Korba etc. 2005) (Selim etc 2012).

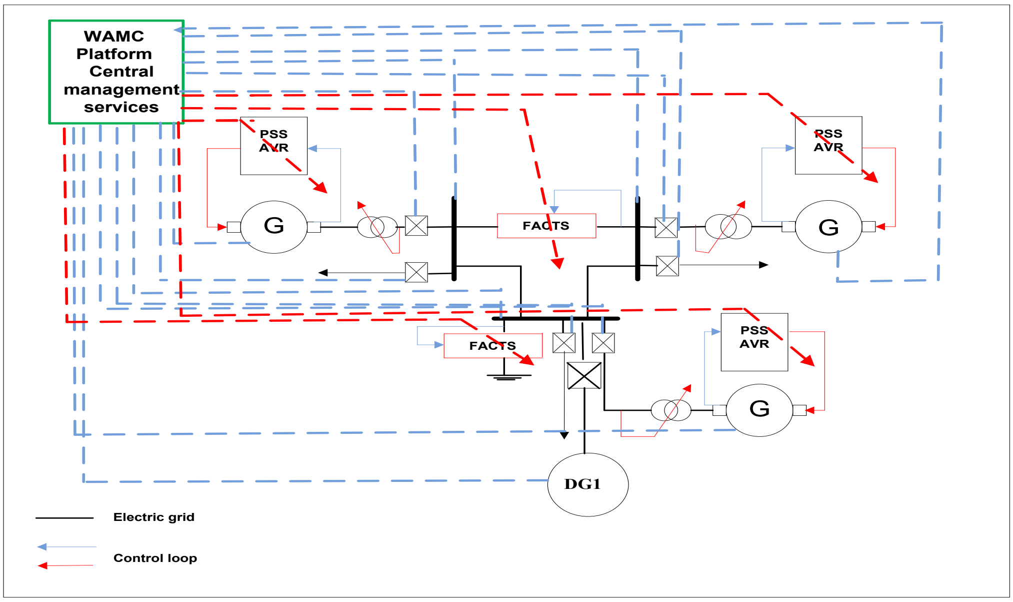


Figure 2. Future trend in protection and automation of EPS

1.2.1 Power System Model

For over a century, synchronous machines have been used by electricity power systems to generate electricity. However, recently, renewable-energy sources such as wind and solar power have begun to expand at increasing pace. Power systems have one or more sources of power (generators). Traditional generators are rotating machines which, in a steady state, rotate at 50-60 Hz or else at a synchronous speed. However, not all AC power systems are always in a steady state and they may exhibit defects such as harmonic distortion, sags, swells, etc., or else they may the power system tray may try to correct the imbalances between generation and loads so as to stay close to a synchronous speed, i.e., in synchronism (Rasmussen 2003). In some cases generator machines deviating from the ideal behaviour may become unstable. The main reasons for deviation are as follows:,

1. Network configuration variation, whereby there are alternating operations of the distribution network between closing and opening based on local needs or protection system's operation (local events).

2. Load variation, frequent operations of loads such as connecting and disconnecting alternating machines.

3. Physical unsymmetrical faults, individual fault in part of the system, for instance in the lines, the transformer, a single phase load or a short circuit in a single phase.

4. Nonlinearities of the electrical equipment, upon the fact, the instantaneous values of voltage, current, magnetic fluxes etc.

Obviously, losing synchronization is not desirable. However, large disturbances do happen, even if infrequently (Devos & Rowbotham 2001) (Saccomanno 2003).

The dynamics of a rotating machine can be modelled in a manner that, in case of the load, increases. The machines will require more accelerating power, Pa, which is the difference between the mechanical power, Pm, and electrical power, Pe, to rotate at synchronous speed, as follows,

(1.1) $$M\acute{\omega} + D\acute{\delta} = Pa = Pm - Pe$$

where δ represents the deviation of the shaft's rotational angle from synchronous, ω = δ' is the deviation from synchronous speed, M is the rotation inertia and D is the damping. Pm is controlled by the manufacturer while Pe is the real electrical power which is injected into the transmission network and which transmits power from the generator to the distribution feeder. The modelling of this transmission network can be done as a standard mesh circuit as follows,

(1.2) $$I = Y . V$$

where I is the injected current, Y is the conductance and V is the single phase voltage based on the frequent assumption that the three phases are balanced. Therefore, only a single phase is required to be modelled. For electricity power transition, injection is a more interesting term than the I current injection, given that the main consideration is the transition of the electrical power from the generators to the consumer. Thus, the transmission network can be modelled as,

(1.3) $$S = g\ (V)$$

where S is the power injected into the node voltage and g indicates the nonlinear functions that relate power injections to the node voltages. Finally, the power system has to be modelled in such a way that provides immunities to credible disturbances and avoids outages (Bose 2003).

1.2.2 Structure of Energy System

An energy system in the most general terms comprises a generation station, a high voltage medium and low voltage power networks (the grid). Based on the concept of distributed generation and the location of the renewable power sources - which are constructed far away from the consumption area - the greater the need for extensive and reliable transmission networks. A transmission network consists of a power line, a control centre and substations. The substations are the most crucial nodes in the transmission and distribution networks, and the first version of IEC 61850 concentrated on substation automation. Electricity utilities' deregulation as regards power generation, transmission and distribution in each country has com-promised many different companies involved in it. In order to perform their func-tions and provide secure, stable and reliable power services, all power stations, substations, power lines and related control centers are interconnected, forming an electrical energy grid. In the past, this interconnection was poorly formed. How-ever, based on future electricity demands, this interconnection must now become stronger and rise to a national level, forming a national energy grid with an asso-ciated reliable communications system network (EWICS 2006).

Electrical energy trading businesses have increasingly tended to build up strong synchronous connections between separate electrical energy systems. Here, the observation may be made that the power consumed no longer needs to be generated locally. Consequently, a greater quantity of electrical power now is transported over the transmission network over longer distances as a part of the energy trading business. The energy-related policy of the European Union has opened the door to a competitive electricity market by building trans-European networks so as to provide a highly secure and stable power supply. For instance, the Nordic energy system comprises the grids of Finland, Sweden, Norway and Eastern Denmark, Table 1. In addition, there is an internal HVDC between southern Finland and southern Sweden, various HVDC connections between the Nordic power system and the Eastern and Western European and Russian grids. The weak point of the Nordic power system is the ageing of the transmission lines, which have turned into a major risk as regards undesirable power flows and oscillation, the occurrence of which has increased significantly (Turunen 2008, 2011).

Table 1. Interconnection from Finland to the Nordic energy system and neighbors

To Sweden	Two 400 kV AC lines One 220 kV AC lines One 400 kV DC cable
To Norway	One 220 kV AC line
To Russia(asynchronous)	Back-to-back HVDC of 1400MW One 400kV and two 110 kV radial AC lines to power plants
To Estonia (asynchronous)	HVDC light of 350 MW

1.2.3 Legacy Communication System Infrastructure

Existing communication and information system infrastructures for energy grids lack coordination among various operational entities. This infrastructure had been designed based upon the needs of traditional energy systems, whereby various subsystems are separated and data and information sharing is limited, which is usually the case with slow or else delayed restoration. Further, it has been highly focused on vertical communications between a control centre and individual sub-system for local and remote monitoring and data acquisition (Gopalakrishnan & Thomas; Xie et al. 2002).

A simple star network topology - hardwired point-to-point - in which SCADA are used today, carries a status such as “switch open” or “switch close” and commands, bidirectional between the control centre and poll substation remote terminal unit (RTU). Figure 3 illustrates the traditional energy grid. Consequently, this communication structure, given the concepts of distributed power generation sources and grid-wide phenomena, has a limited ability to cope with. This is particularly important in a deregulated environment where the huge amount of information generated from distributed renewable generation resources needs to be shared for the protection and automation functions.

Sharing information will increase the opportunities to limit spread of disturbances throughout the energy gird, which becomes more vulnerable to the phenomenon of cascading. In order to overcome these drawbacks, special protection schemes have been developed. Several monitoring and measurement technologies have been implemented with the continuing development of IEDs.

Communications systems network media play a critical role within the energy grid infrastructure. In the present case, Ethernet technology has been considered as a simpler means to transfer data, and the widespread adoption of it as a faster, less expansive and better standardization effort - as brought by the IEC 61850 communication protocol - has seen a marked improvement in interoperability scenarios (PULSECOM 2010).

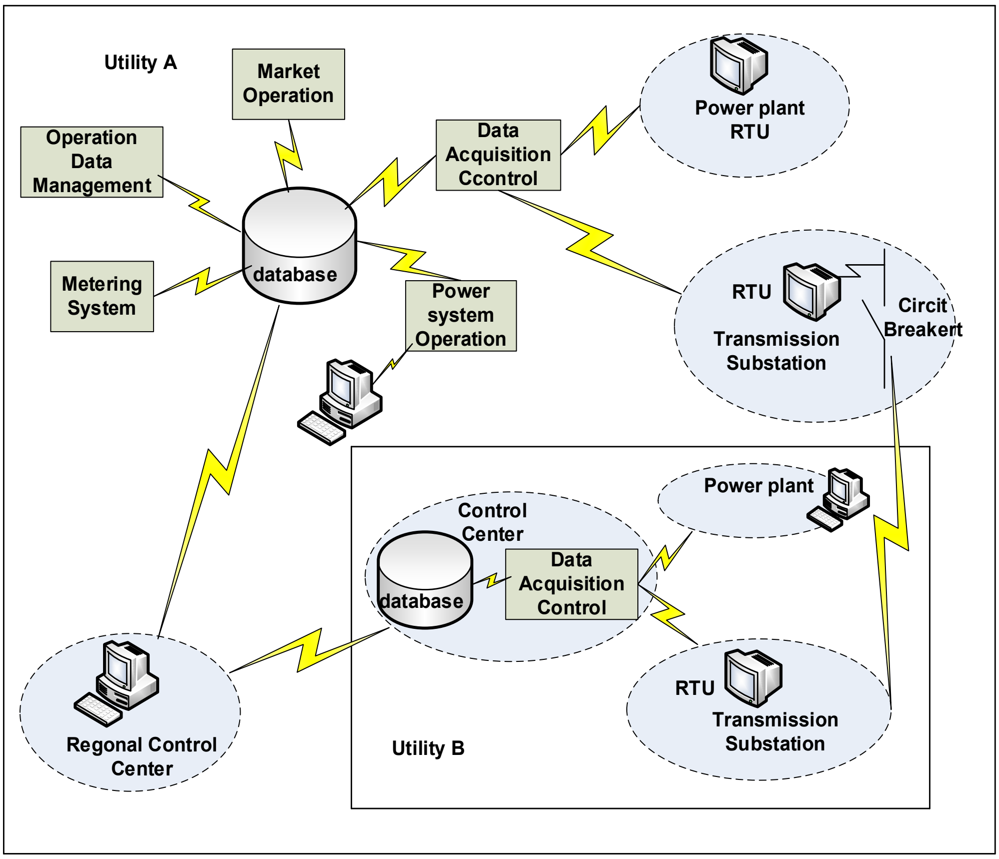


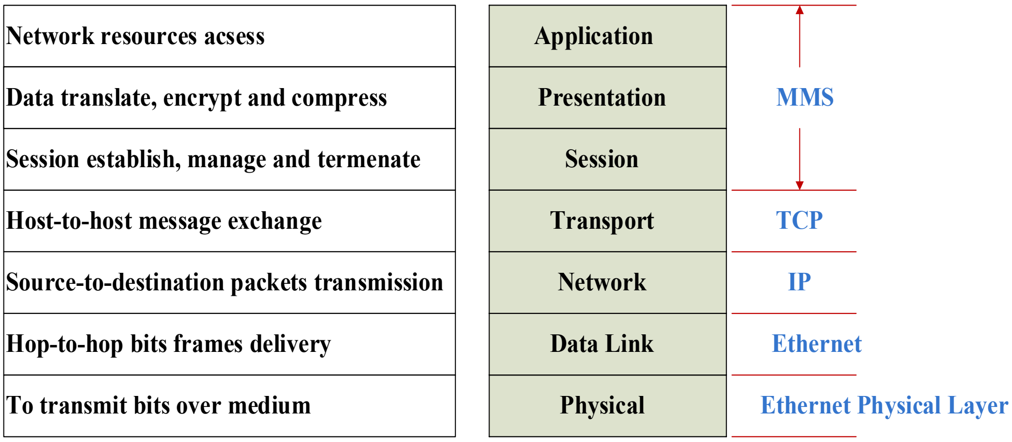
Figure 3. Traditional energy system communication network.

1.2.4 An Open System Interconnection Model

The OSI model was developed by the International Organization for Standardization (IOS). In the late 1970s, the OSI model was first presented as a set of protocols that covered all aspects of network communications. The OSI model provides for open networking environments that allow various manufacturers' systems to communicate regardless of their underlying structure. Nowadays, different network technologies are in use, exhibiting beneficial operational understanding and a strong ability to integrate different communications systems with each other. In truth, facilitating communications without requiring changes to the logic of the underlying hardware and software is the reason for the high degree of acceptance of the OSI model in several technologies (Stalling 2007).

The layered framework is an OSI model, being the most basic form that divides the system architecture into seven hierarchical layers that became the standard for most communications systems' architectures. The seven layers of the OSI model are separated but are highly interconnected. Each layer provides a subset of functions related to its operations and needs to communicate with other systems. Within a single system, each layer performs services for the upper layer and implements services performed by the lower layer.

The OSI model provides for the idea of dividing the communications process into separated layers within the telecommunications network. Each layer adds a specific segment of data that is related to its functions. Consequently, in a given message, there is no direct connection between peer layers. However, the physical layer deals with the physical aspect of carrying the data that flows down from the application layer through each layer at the sending ends to the receiving ends, where the data flows up through each layer to the application layer. In addition, direct connections are not the only way that is specified by the OSI model; for instance, connection links can be established through a packet switch or a circuit switch. Figure 4 illustrates the OSI architecture and provides a summary of each layer's functions.



Network resources acsess	Application	MMS
Data translate, encrypt and compress	Presentation	
Session establish, manage and termenate	Session	
Host-to-host message exchange	Transport	TCP
Source-to-destination packets transmission	Network	IP
Hop-to-hop bits frames delivery	Data Link	Ethernet
To transmit bits over medium	Physical	Ethernet Physical Layer

Figure 4. Open system architecture and summary of the layers functions

Communications technologies comprise a broad and dynamic field that has evolved and is growing rapidly. The strong evolution of communications technology can be integrated into the power industry. Therefore, the data services and applications of the power system substations based on IEC 61850 are built over the standard OSI model's seven layers in order to accomplish interoperability and to become future proofed, which is the basic requirement for any standardization process (Sidhu & Gangadharan 2005) (Bose 2003).

1.2.5 Substation Communication Protocols

Conceptual frame work based communications among systems are provided by a network communication model. However, a specific communication method does not. Network communication protocols are defined as the actual communication based on a formal set of rules that enable to computing systems understand, accept and talk to each other. A short introduction to some of the substation communication protocols will be presented so as to better understand the need for a new global standard.

1. Modbus

Modbus is a protocol that represents the common defined language that has been implemented by Modicon devices in order to link between each other and other devices through different types of communications networks. The first appearance was in 1979, for use in a programmable logical controller. It can be considered to be the first industrial open-file bus that a developer could implement with its products without limitations. Now, it is one of the de facto standards used for connecting industrial electronics devices. Client/Server communication services include the Modbus communications schema, which is provided by an application layer protocol. Therefore, the standard Modbus system may consist of up to 247 servers and one client. It is simple and easy to understand and implement. How-ever, its simplicity given the data model that has been used by Modbus cannot support complex object structures, nor can various automation functions be executed by different types of substation devices. These issues are the main drawback of its implementation and have forced manufacturers to define their own functions, leading to a reduction in operability and compatibility among multivendor products (Rev 1996).

2. DNP3 Distributed Network Protocol

The DNP3 protocol was developed by Westronic Inc. between 1992 and 1994. It was designed to achieve open, standard-based interoperability between substation devices such as computers, IEDs and central stations. DNP3 is built based on the IEC 60870 standard. Its partially completed protocol specifications have been used to provide a more easily implementable protocol that supports newer functions within centralized SCADA systems. DNP3 was specifically created for North American requirements and was widely carried out by typical electrical utilities. Such utilities may have a centralized operations centre for monitoring and controlling all devices within the energy system. One of the mean drawbacks that limits using the DNP3 protocol in modern substations is its processing latency. Extra time is required when a transport layer breaks long messages into smaller frames, or when reassembling frames based on longer messages. Further, the time that is required for receiving confirmation messages, or the time spent waiting for multiple retries when retries are configured, is unacceptable (Curtis 2005) (Fieldsever Technology).

3. IEC 61850

IEC 61850 is a relatively new international standard, which has been developed to define the communication infrastructure within the substation for the first version, and has been extended to support the protection and automation for the energy system within the second version. The IEC 61850 standards have been expected to provide and ensure seamless communication as well as integration between IEDs from various manufacturers into a hierarchical level. The rest of this chapter explores the standards in details.

1.2.6 Substations Topologies

Energy systems have to be adapted according to needs. It has become necessary to transmit power for longer distances at higher voltages. Direct high voltage from a power plant cannot be used in homes or by businesses. In such systems, various types of substations are implemented to adapt the distributed voltages. Further, they are used to split the flow of electrical power among the outgoing lines based on their topologies, which makes the electrical power usable for end users. Therefore, substations can be classified based on their size and functions (ABB 2012).

Typically, transmission and distribution comprise the two types of substation. A transmission substation is usually supplied with a transmission-level feeder (100 kV and higher) which can connect two or more transmission lines that allow a single source of electrical power to be split into more outputs. In the simple case, all transmission lines are of the same voltages. In another case, it may have a transformer to step up or step down voltages based upon needs.

The size of a transmission substation ranges from small (which may consist of a bus plus some circuit breakers) or large (consisting of multiple voltage bus levels, many circuit breakers and an enormous amount of monitoring protection and numerous control devices). In this case, it may require a redundant communication link among the transmission substation devices, as well as between transmission substations and a control centre, to increase reliability. Figure 5 illustrates the two types of transmission substations (Shoemarker & Mack 2002).

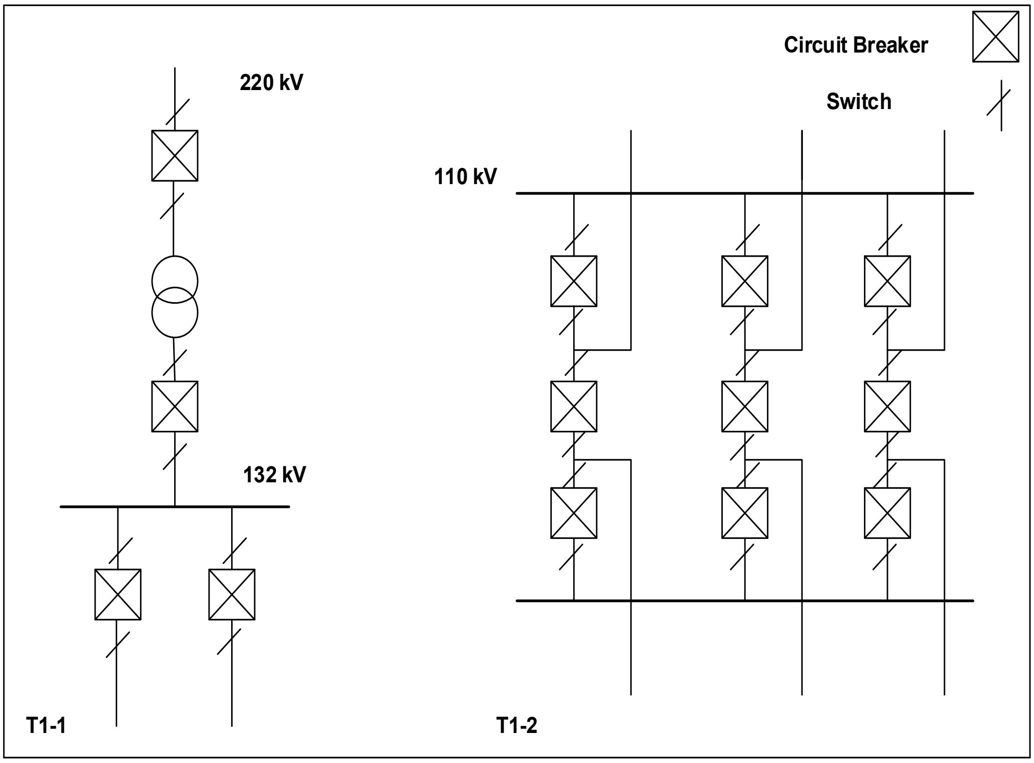


Figure 5. Small transmission substations.

Once the electric power reached its distention, the distribution substation is used to step down the transmitted voltage to lower level and to split the electric power in order to be shared by the end users. The ranges of the distribution substation voltages are between 3.4 kV- 33 kV depending on the size and coverage area served by the local utility. Figure 6 illustrates two types of the distribution substations (IEC 61850-1 2003).

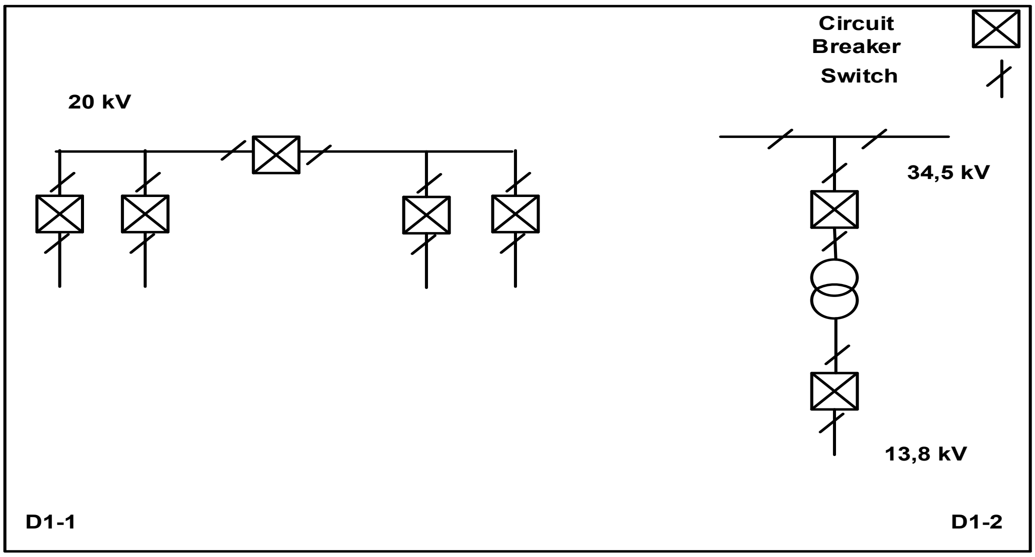


Figure 6. Small distribution substation.

1.2.7 Substation Monitoring and Control

Monitoring and control are the key features of an SAS allowing electrical utilities to coordinate any disturbance devices installed in the substation remotely. Different types of devices are utilized within the SAS. These devices are integrated into a functional group based on their communication scheme for the purpose of moni-toring and control. SASs seen rapid evolution in the last two decades. The main factors in this evolution have been considered based on, firstly, the development of high-speed microprocessor-based IEDs implementing digital technology and its massive usage - for instance, protective relays, meters, programmable logical controller PLCs, transducers and other devices that can be dedicated to specific functions in an SAS. Secondly, the vast amount of data and information provided by IEDs, which encourages researchers towards significant developments in communications systems based on the agreed and accepted usage of communications standards and protocols. This allows for the use of equipment from the various manufacturers. Thirdly, the merging of the objective of a sharing data be-tween various devices inside SASs as well as outside them to limit cascade phenomenon based energy system failure. Different types of the monitoring and control schemes have been implemented within SASs; however, they are outside the scope of this study. Figure 7 illustrates the conventional substation architecture where the centralizing scheme simplifies an SAS based upon the fact that all the interfaces are centered around the SCADA RTU. According to this classification, substation architectures can be divided into three hierarchical levels. A substation's primary equipment, such as circuit breakers, power transformers, switch-gears, etc., and their link elements, such as instrument CTs, VT transformers, circuit breakers, etc., represent the level zero process level (Mesmaeker etc. 2005) (Prasoon etc. 2009).

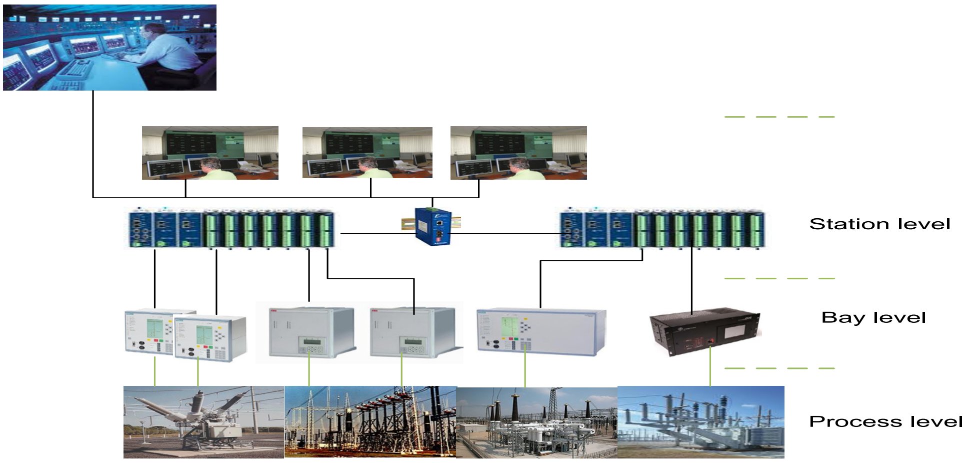


Figure 7. Conventional substation architecture.

Consequently, automation, control and protection can be considered according to two levels. Level 1, which represents the bay-level devices such as IEDs, protection, measuring, PLCs, QoS, etc., is directly connected to devices at the process level. Level 2 corresponds to the human machine interface (HMI) and the control centre, which is interfaced digitally with the bay-level devices. Based on this level, all the substation functions, such as local operation, macro commands, central-ized automatic functions and incident recording, are performed. Further, for HMI with the SCADA center and with the managing engineering center of the utility, bay devices at this level may be represented as Level 3 (Amantegui et al. 2005). Interfaces inside and between substation levels are created by the communications system in which it plays the key role in exchanging information and functions, and so it can be considered as the glue that binds the substation levels together. All systems' performance, reliability, speed and supported functions can be determined and defined by its communications networks. Serial, asynchronous communications and legacy protocols are the existing solutions that are being used today and which require upgrades or retrofits (UIS 2007).

1.2.8 New SAS Technologies

With today's rapid developments, technologies essentially share significant aspects such as faster speeds (computers), Broadband (communications) and better electronic power control (FACTS). These developed technologies bring a combination of multidisciplinary skills and experiences that have driven the substation automation project to meet the diverse needs of today's utilities. Here, we briefly outline several modern technologies that may be used in new substation design.

1.2.8.1 Intelligent Electronic Devices

An IED is a single device that can perform functions such as protection, control, metering and sending/receiving data to/from an external device, resulting in more compact designs with reduced wiring and high reliability. The associated enhanced microprocessor and modern communications technologies with the new IEDs have increased the capabilities for remote/local control and data acquisition for use in network analysis. Further, different IEDs raise the possibility of integrate between one another so that they can function together and share information locally as well as beyond the gate with other systems. One of the main key features is that they are programmable, i.e., the embedded function can be changed or updated by downloading a new software version when available so as to take advantage of new functionality. Figure 8 illustrates the functions that have been merged with the new IEDs (Hor & Crossley 2005).

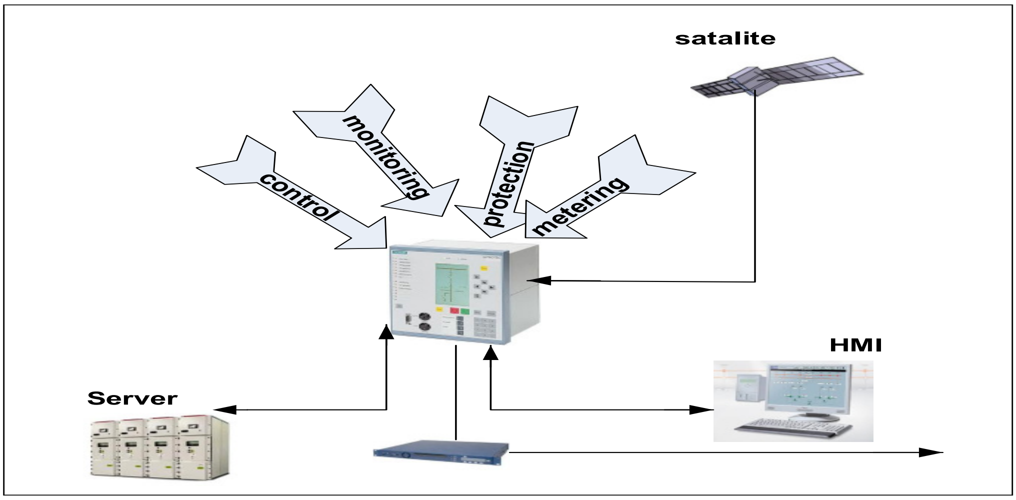


Figure 8. IED merging functions.

1.2.8.2 Communication Media

Utilities have acquired numerous communication media options that have been implemented in modern energy system grids, such as microwave transmission, fibre optics, spread-spectrum techniques, wireless radio and various high-speed process buses. Each utility has always had a proprietary communications system which is used to connect various subsystems. The utilities have been considered as among the largest users of data and real-time information based on shifting their focus to client services. This scheme requires delivering the specific data to the selected client within the assigned period of time, requiring data communication over the extended communications network. The main focal point for the communications network is comprised by the merging requirements, raising issues for various types of proprietary subsystems' communication solutions as regards a hybrid SG (Kezunovic 2010). A hybrid communications network has been adopted in the new SAS, merging a modern process bus with high-speed fibre optic technology. Broadly, the fibre optic medium is replacing copper wire since it is suitable in the substation environment and it has been recognized as a backbone for many network systems. There are two options for fibre optics that might be chosen. First, there is a single mode, which has one source laser-generated light with a core diameter of less than a tenth of the wavelength of the propagating light and which can be implemented in the case of long-distance transmission up to 3,000 m. Second, there is a double mode with a relatively larger core and generated light from multiple streams and which can be implemented for medium or short distances. Several benefits can be realized by using fibre optics, as it supports long-distance communications with less loss, a high data rate, a high bandwidth, smaller sizes, lighter weights and strong immunity to electromagnetic interference (Kezunovic 2007).

1.2.8.3 Synchronized Sampling

The Global Positioning System (GPS) had been integrated in the utilities industry to provide a reference time signal. The reference time signal provided by the GPS system is very important for signal processing analysis - for instance, in order to correlate the disturbance event reports received from a single IED, and when integrating data from different IEDs in different locations. Further, it exhibits a high degree of synchronization with universal coordinated time (UCT) with an accuracy of up to 1 μs, which in turn can be received over a wide area such as that covered by a power system network through a GPS receiver. The purpose of utilizing this technology is to carry out a synchronized sampling clock within the input data acquisition system in IEDs and to provide a time tag to the data polled by IEDs. Consequently, modern substation operations based on protection and automation functions may require synchronization for a successful implementation, for instance the digital current differential protection function (Kezunovic 2007).

1.2.9 Upgrade Migrate and Retrofit

In Finland, many regional substations are ageing as the average age is more than 40 years old - for instance, the substation in Vöyri has a static relay technology for protection and control SPAJ 3A5 J3, SPAA 3A5 J40 and a switchgear system manufactured by Strömberg (now merged with ABB) from the 1980s. Utilities try to extend the lifetimes of aged substations by maintenance scheduling and repair strategies. The system's maintenance and services costs are going up every year given the obsolescence of substations' secondary devices and the complexity of software (which affects the system's reliability negatively). These issues have forced utilities to retrofit the existing legacy SAS (Beaupre et al. 2000; ABB 2008). Another crucial issue facing utilities for upgrading ageing energy system units is that the lifecycle of the secondary devices is half that of the primary apparatus. In industrialized countries, such a retrofit scenario is quite common (for instance, the Vöyri substation retrofit project). Utilities have realized that automation based on state-of-the-art secondary devices, as well as the global standard IEC 61850, has proven to be a good approach to extending the lifecycle of substations and their primary apparatus. Further, by using this step-by-step approach, they can ensure that they minimize investment costs in addition to serving the needs of the next 10-15 years as regional electrical power demand steadily increases (ABB 2010; Lenzin 2011). Optimizing substation operations within a developed and competitive environment forces utilities to initiate the need to establish continuity of services during any transition. Outages should be minimal and only used where there is no other option - for instance, in the Vöyri substation, and based on the concept of reducing outages, an auxiliary bus bar for contingency and maintenance has been utilized, while a backup generator assesses when the full load is ready to operate and whether an interruption has occurred to the incoming power supply. As regards upgrading all legacies' secondary devices and migrating the SAS to the IEC 61850 standard with a fully factory-tested solution, bay-by-bay might not be a big challenge as built from scratch. A retrofit project is more challenging by its nature, it requires that legacy devices and new IEDs must be compatible and operate smoothly. Due to these challenges, the sub-station retrofit project can be characterized based on two cases. In the first case, with the extensive use of IEDs, utilities have been worried based on that they could not specify what was necessary, since the new standard IEC 61850 does not standardize functions. Further, the principle task of specification raises concerns that certain requirements will be met besides whether the maximum possible benefits are ensured based on use. Therefore, the main question arises as to what must be changed, since the boundary is the existing substation automation system's requirements, which need extensive knowledge as regards the existing substation's automation and future demands in addition to hands-on training and clear operational instructions. This results in specifying the needed functions based on either a functional point of view only or by referring to some dedicated existing devices, meaning control, protection and monitoring units. The available functionality based on the new standard needs to be covered and it may require one or else multiple IEDs.

The IEDs in the substation can be divided based on the above concept into two groups: 1) performing data acquisition and processing, which are installed through the control house, such as protective relays, and 2) mounting and collecting the data from the primary apparatus, which is called the 'switchyard monitoring' of devices, and installing them afterwards onto the primary apparatus. The system is established by enabling the interconnection of various advanced IEDs and processing the incoming data from these IEDs at both the substation and the control centre. Utilities have new opportunities in terms of interoperability and interchangeability that have been achieved based on new standard advantages, enabling utilities to select IEDs that best fit their needs. The result is that utilities do not have to worry about compatibility, even when they select IEDs chosen from multiple vendors or versions, since the new SAS standard ensures this (Janssen & Brand 2010; Kezunovic et al. 2010). Consequently, utilities have to initiate their selection process criteria - for instance, if the selection had been made based upon the evaluation of the data that is provided by the vendor manuals. Taking a decision by means of what are the most strongly related performance characteristics might be a hard task, but it might also be necessary to develop tools to measure this data. Therefore, the criteria for the selection process must be initiated up to the task, requiring the utilities-side to provide appropriate tools and methodologies for evaluating the design of the new SAS. As a result, the requirements for retrofit projects based on the first case solution can be encapsulated as,

1. Considering all operational parameters, maintenance and asset management requirements based on analyzing and consulting to achieve the optimal specification for a cost-effective solution.

2. Providing integrator engineers, for whom the main role is to implement all the substation devices (existing and new IEDs) as one integrated system by using appropriate tools which enable users and devices to share data.

3. Coordinating between all the groups involved throughout the project to ensure the most efficient and timely project management implementations.

4. Creating laboratory setup with modelling and simulating capabilities to provide IED evaluations before implementation so as to achieve fully tested solutions that are future-proof and ready for implementation.

5. Hands-on-training and education to facilitate the transitions from the legacy system to modern IEC 61850 in order to ensure optimal implementation and usage for added and extended functions.

In the second case, consideration had been given to the extreme implementation of fibre optics cables within the updating task of the legacy substation. Clearly, in legacy substations' cables, damage is often caused by rodents, since substations might be established in rural areas. Another crucial issue is the weight of copper wire, which is high, especially in larger substations that use longer cables to connect all their subsystems. Further, the environmental challenges due to implementing copper wires, such as high voltages, relatively high resistance, extreme temperatures, current faults and harsh environments. Therefore, the most viable option in the case of upgrading or maintenance (damaged copper cable) and in order to overcome all these limitations is fibre optic, which has many advantages as mentioned earlier.

1.2.10 Towards a Smart Grid

An SG is a common objective for a variety of types of development, since today's grids are heavily based on a hierarchical architecture with a unidirectional top-down power flow that was built between the 1970s and the 1980s. Energy grid operating methods have not changed, even though demand has increased drama-ti-cally over time, mostly due to environmental and economic concerns. As regards a SG, this can be defined as an upgrade in the electrical grid's transmission, with distribution networks that link power generation units and power consumption in a dynamic manner, and which attempts to operate intelligently based on their be-haviour and actions. On the other hand, the broad expectation for the future of a SG has led the European Commission to realize and set its policy to move to-wards a SG. This approach has been approved by merging the new technologies, which will allow electrical power to flow exactly where it is needed (when it is needed) in a cost-effective manner. In addition, it will be possible to improve consumer services in compliance with shifting its behaviour from a passive receiver for power into an active participant by means of allowing sharing information and monitoring. This real-time monitoring of its status and communication with the grid operator and the energy supplier allows the consumer to directly control and manage their individual consumption as well as introducing the concept of 'return power' to the grid from small resources (VTT 2009; Energy Future Coalition 2010; MEMO 2011). Eventually, there will be significant great benefit for all actors, such as the grid operator, with the merging of the concepts of centralized and decentralized power generation. This approach allows for the connecting of all renewably generated power from a variety of generation sites and players scattered over wide areas. Another crucial issue which becomes increasingly important is energy storage and load management based on increasing the share of the intermittent power in the system. However, storing electricity relatively is difficult based on its nature. Nonetheless, renewable power generation plants from neighbouring areas, such as solar power from North Africa, could be used to store energy by means of using pump storage plants for managing fluctuating power supplies and loads, resulting in high reliability and flexibility. Figure 9 illustrates the future electrical energy grid (Larsson 2009) (Battagöini etc. *2008*).

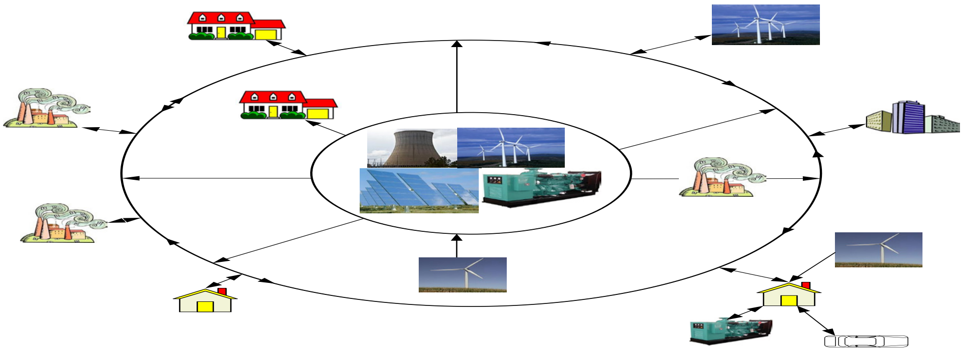


Figure 9. Future electrical energy grid.

1.3 The IEC 61850 Standard for Energy Systems

1.3.1 Background to the IEC 61850 standard

Sharing real-time data becomes a dominant task for any successive system operation. In a substation, the real-time data needs to be shared speedily and accurately among the substation devices as well as with other energy subsystems. This con-cept has generated a demand to integrate and consolidate IEDs. This task may require a standardized communications language among devices in order to facili-tate interfaces, since the existing solutions have reached their limits. In particular, the Electrical Power Research Institute (EPRI) and IEEE raised the concept of a utility communication architecture (UCA) in the early 1990s. The idea behind the concept is to identify the requirements, structure and specific communications technologies that can be used to implement the standardization scheme deemed suitable for future extension. The first version concentrated on the interfaces be-tween the control centres and the substations and the control centre (Proudfoot 2008) (IEC 61850 2003).

In 1994, the next phase of UCA (UCA 2.0) started to define the substation's communications bus. The UCA architecture comprised data objects on the application layer. The service interface was the middle layer, providing tasks such as defining, retrieving and logging process data in the bottom communication profile's layer. The IEC 57 Technical Committee began its activity in 1996 using the same concept as that for IEC 61850. In 1997, the IEC 61850 standard was defined as the common international standard when the two groups merged their work. As a result, the harmonization process comprises the current IEC 61850 specifications, which include UCA 2.0 as well as offering additional features. The first version of the IEC 61850 standard was published in 2003. Figure 10 illustrates the merging process of the two working groups (Adamiak &Premerlani 1999) (Ozansoy 2009).

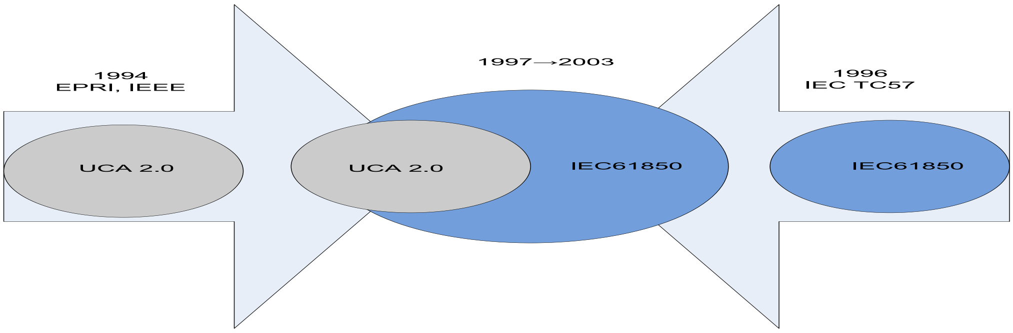


Figure 10. Merging process.

1.3.2 Overview of the IEC61850 standard and Basic Concepts

Nowadays, the IEC 61850 standard has become one of the most promising and powerful solutions for the power industry's existing limitations and is expected to support energy systems' evolution. The key point is that it provides a uniform framework for all the related system levels. IEC 61850 considers the various aspects that are common at the substation site, such as data models, communication solutions, engineering and conformity over the channel. Although organizing the data in terms of applications by means of syntax and semantics within the devic-es, they did not specify it.

The main aspect that IEC 61850 adopts is the associated architectural construct, "abstracting" the data object's definition and its services. These data objects and their associated services are abstracted independently from any underlying proto-col, which supports a comprehensive set of substation functions and provides strong services in order to facilitate the energy system's communication. The abstract definitions of the data object allows its mapping to any protocol that can meet the best data and service requirements, as the IEC 61850 standards do not specify any protocol. Therefore, the IEC 61850 specification can be encapsulated according to three major focusing issues, 1 Standardizing the available information (the data object model), substation functions (the functional model) and the IEDs name, thereby providing the IEDs with a shared vocabulary that supports the intended semantic meaning.

2 Standardizing different ways of the accessing the scheme for the available data's abstract communication services interface (ACSI). These ways are defined as services. Further, specifying the mapping scheme according to the communication services and the data according to a number of protocols.

3 Defined a language eXtendable Markup Language (XML) implemented to describe all the configuration information exchanged between the IEDs, the network and the power system.

The scope of the first version of the IEC 61850 standard is composed of 10 major parts that together define the various aspects and the requirements that must be fulfilled by the SAS. The main goal is to achieve interoperability among the IEDs within the SAS, as illustrated in Table 2 (IEC 61850 2003) (Mackiewicz 2006).

Table 2. Scope of the first version of the IEC 61850 standard.

Part	Definitions
1	*Introduction and Overview*: this provides an introduction to IEC 61850 and a general overview of all the parts.
2	*Glossary*: this gives definitions of the specific terms used in the SAS.
3	*General Requirements*: this defines quality requirements-based system operations.
4	*System and project management*: this specifies engineering service requirements.
5	*Communication Requirements for Functions and devices Models*: this defines the virtualizations aspect and its performance requirements.
6	*Configuration Description language for communication in Electrical Substation*:this specifies a file format for describing system configuration and relation between devices.
7	*Basic Communication Structure for Substation and feeder Equipment*:
7-1	*Principle and Models*: it defines the communication and information model principles also mapping scheme.
7-2	*Abstract Communication Service Interface (ACSI)*: it defines the cooperation of various devices.
7-3	*Common Data Classes (CDC)*: it defines the common attribute type and common data classes related to substation applications.
7-4	*Compatible logical nodes and data classes*: it specifies the data classes with regard to syntax and semantics.
8	*Specific Communication Service Mapping (SCSM)*
8-1	*Mapping to MMS (ISO/IEC 9506-1 & 2) and to (ISO/IEC8802-3)*: it describes the communication mapping for the entire system.
9	*Specific Communication Services Mapping (SCSM)*
9-1	*Sampled Values over Serial Unidirectional Multi-drop Point-to-Point Link*: it describe the point-to-point unidirectional communication mapping services.
9-2	*Sampled values over ISO/IEC 8802-3*: it describes the SCSM for bus-type.
10	*Conformance testing*: it specifies the implementations conformance testing techniques and the declared performance parameters measurements techniques.

1.3.3 IEC 61850's Impact on and its Benefits for Substation Operations

The positive impact of the IEC 61850 standard on substation operational costs is clearly known in terms of increasing the power quality and reducing the outage response. However, this goal requires paying attention to how to implement the IEC 61850 standard in order to build, integrate and operate the SAS. Energy systems are moving into the digital environment, where huge amounts of real-time information is available, allowing a new kind of calculation for higher level substation functions-based protection and automation. The IEC 61850 standard is unique, designed from the base up in order to operate over state-of-the-art technologies. It provides a novel set of functionalities which do not exist within legacy SAS operations. From an IEC 61850 implementation point of view that attempts to utilize the fullest functionality, numerous of benefits will be achieved (Janssen 2008; Holbach et al. 2007), such as:

1 An open system for protection, automation and data sharing from the use of the standard representation for all the objects of the energy system and a common technology infrastructure to eliminate procurement ambiguities.

2 Interoperability between devices from various manufacturers within the energy system and the ability to configure the system with the available configuration system tools independently of on-site manufacturer support.

3 A secure and dependable overall system by means of several techniques that allow for flexible information transfers

4 Reducing the overall system costs for operation and maintenance

5 Flexible and expandable functions, and easy adaptation by means of self-description in a standardized manner.

1.3.4 IEC 61850-7-420

The incoming global boom in distributed energy resources (DERs) systems needs to be integrated into the energy grid, and its impact on distribution power systems in turn raises challenges. These challenges have stimulated utilities and DER manufacturers to announce a growing need to define and standardize communications outside the individual SAS, which may include various DER IEDs. As a result, the standard IEC 61850-7-420 was published in 2009 as an extension of the IEC 61850 standard and in order to address these issues. The IEC 61850-7-420 specifies various types of LNs and information modelling suitable for different DERs – for instance, wind farms, fuel cell systems, photovoltaic, combined heat and power (CHP), etc. Via information modelling, the LNs facilitate communications and the integration of the DERs into the utilities protection and automation systems. However, the other specifications (ACSI, communication mapping) are still based on the existing IEC 61850 standard. Utilities and DERs manufacturers are expected to achieve benefits from utilizing the IEC 61850-7-420 in terms of reducing installation and maintenance costs. Furthermore, by offering the standardization of all DERs data models, this will improve interoperability among distributed automation systems (DASs) and DERs and increase the reliability of the energy grid (IEC 61850-7-420 2009).

1.3.5 The IEC 61850 Information Model

The information model in IEC 61850 is hierarchically structured, whereby LNs are the essential elements of this model. Modelling is performed in a standardized way in order to provide an opportunity for interoperability among IEDs within the system. IEC 61850 models virtualize the real devices in energy systems as logical devices (LDs) such that the LNs are hosed by. An LN represents a specific function within a device where the function can be split into multiple LNs that can be located in various physical devices which, in terms of this infrastructure, are called distributed functions. Therefore, an LN may be considered as the small part of function that possesses the capability to exchange data. The hierarchy information modelling can be classified as five levels in order to perform applications within SAS. The levels have an inheritable relationship. In a substation, one or more physical devices can be defined. The individual physical device may have zero or multiple servers (typically at least one server). The server object based on the hierarchical data model is located on the topmost level, as illustrated in Figure 11, which may have one or multiple access points. In compliance with the data model, the server class can be described as a collection of the objects below it in the data model. Further, it possesses methods that can create all the underlying objects. Based on a server implementation perspective, in order to access the objects of the data model from the server, the list of object references and corresponding references to instances of the objects are stored in the server class, which allows for the performing of this task. The definition of an LD and a server is left to the manufacturer or administrator of the substations. Standardization is the way that the LNs are predefined with. This fact makes LNs the most crucial point of the information model. In terms of this restriction, interoperability between different IEDs from various manufacturers can be achieved (IEC 61850-7-2 2003) (IEc 61850-7-4 2003) (Zhang etc. 2009).

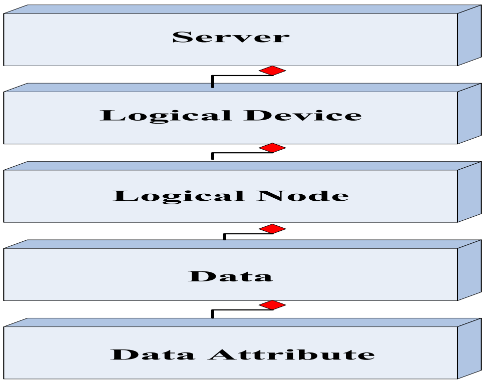


Figure 11. Hierarchy of the IEC 641850 data model.

As such, the data are grouped into 13 different groups. According to these groups, all of the substation operation data can be assigned to one of these groups, for instance, the metering and measurements function data group is begun with "M" and the protection function data group is begun with "P", etc. In addition, the groups are further divided into LNs which are named based on their associated services that are logically related to functions in the substation. LNs can be defined in terms of 86 different types. For instance, the "Switchgear" function group which begins with "X" comprises two different LNs: "XCBR" and "XSWI". Each LN is constructed by seven categories of data classes, such as status information, measured information, etc. Each of the data classes consists of a number of data attributes, as we have 355 different data attributes that have a specific name, a specific type and various purposes, as illustrated in Figure 12. Browsing to individual objects may be simple in this model given the fact that the data object is named by means of its place and path through the information tree model. For instance, as in Figure 12 from the left to the right, the first name is the device name and the second part represents the LN. The third part is a functional constraint which is used to group the individual attribute which has a predefined function based on its functionality - in our example, "ST" stands for status attributes. Lastly, the "Pos" attribute represents the position of the circuit breaker and "q" contains the quality to the value of the status that has been sent (IEC 61850-5 2003) (IEC 61850-7-1 2003).

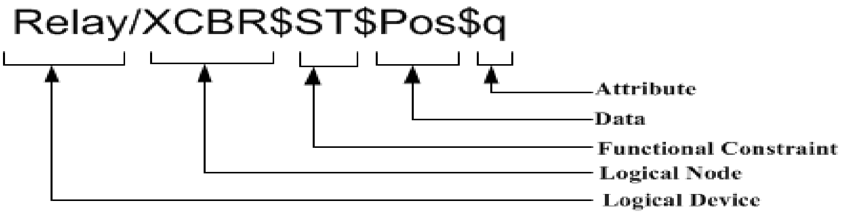


Figure 12. IEC 61850 Object Name Structure.

1.3.6 Virtualization of the Physical Devices and LN, LD Concept

The IEC 61850 standard provides for notion of an LN that can be considered as the major role of the standard, which by means of virtualization, is able to virtual-ize the substation's physical device in the data model. This data model consists of a number of LNs. These LNs, by a reasonable distributed allocation, can build the LD. The LD is often initiated in one physical device that cannot be distributed. The specific function in the SAS is often performed by different physical devices which are called "distributed functions" while the devices are called "distributed devices". In order to implement the distributed function correctly, the sharing of information is required among these devices. The interfaces are performed based on the IEC 61850 standard's communications services. These interfaces follow the predefined rules and the assigned performance requirements. The rules allow for interoperability between devices from various manufacturers. Figure 13 illustrates the modelling approach were the real physical substation devices in the right side are modelled into a virtual model. The virtual model contains the LDs that have hosted the LNs, which encapsulates the real device and services. The data model and services with their associated information are mapped to a network communications protocol, such as manufacturing message specification (MMS), transmission control protocol TCP/IP, Ethernet, etc. (Zhang etc. 2009) (IEC 61850-7-1 2003).

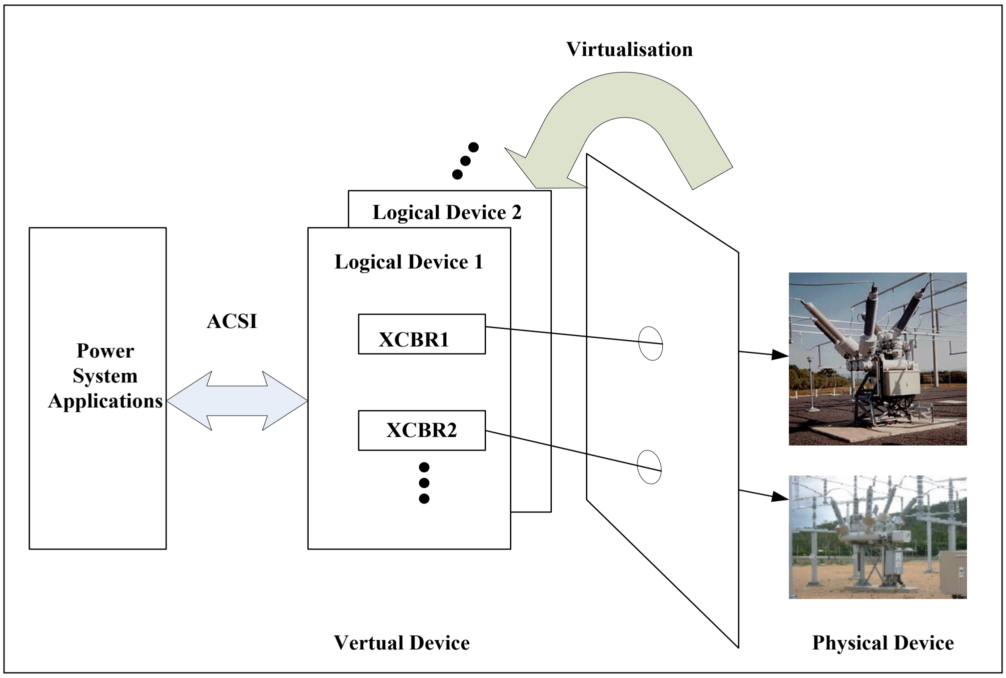


Figure 13. The virtualization process.

The LNs - based on their functionality - consist of a list of data associated with dedicated data attributes. These data have a predefined structure (a syntax and semantics). The LNs with the associated data are crucial for the description and for information sharing for the energy system's protection and automation. Figure 14 illustrates more clearly the concepts of an LD, an LN, a CDC and a data attribute that map to the real world. The virtualization task started by specifying the container for the physical device containing one or more LD; each LD may contain one or more LNs, while each LN may comprise a set of CDCs. The idea be-hind introducing the CDCs was to group and a construct larger data object. The data classes may contain a set of data attributes. The terms "LD", "logical nod" and "data object" are all virtual, representing real data. This real data is used by the energy protection and automation systems over a reliable, high-speed communications system network that links between the defined physical devices. Further, the information modelling and the sharing data are defined independently of the programing software, the operating system and the storage device, which thus provides for the ability to use state-of-the-art technologies (Brand 2004).

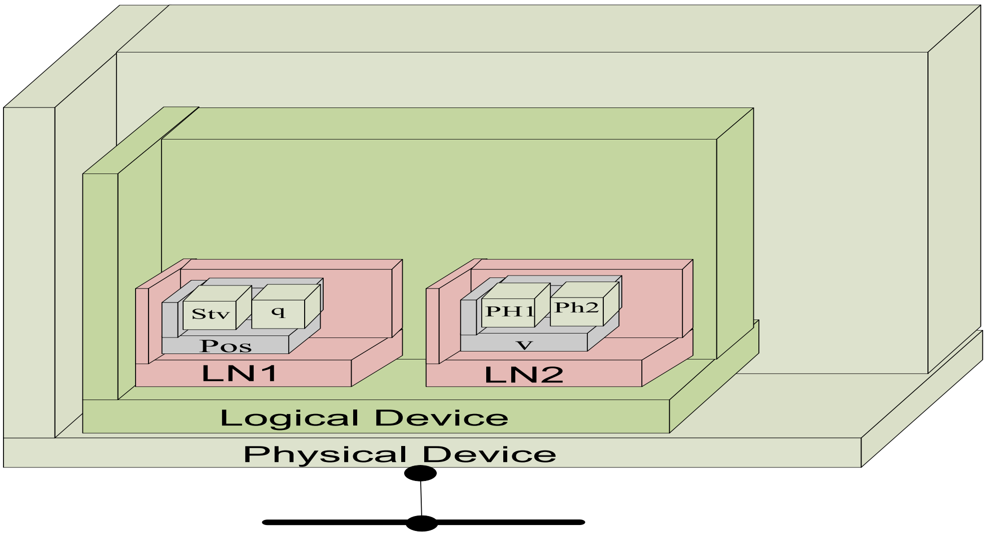


Figure 14. IEC 61850 logical grouping**.**

1.3.7 Communication and Logical Interfaces within SAS

A substation architecture can be divided into three levels: station, bay and process. These levels have been distinguished based on their functionalities. However, they are nonetheless highly interconnected based on several logical interfaces. Figure 15 illustrates the three levels in addition to the associated logical interfaces numbers, from bottom to up. The process level has been linked to the bay level by interface numbers four and five. These logical interfaces provide the ability to exchange control commands and information data. Usually, the primary apparatuses, such as circuit breakers, transformers, switchgears, etc., are located at the process level, which may also have IEDs such as intelligent sensors and actuators. The input and output messages of these apparatuses basically consist of information, such as the transformer voltage and current values, as an analogue signal format, and control commands from the bay relays as a binary signal format. In order to convert the analogue signal into a digitalized standard packet, this is done by a so-called “merging unit” (MU). The MU might be located in the yard next to or else be integrated with the instrument transformer, and should contain the LNs’ voltage and current transformer (TVTR, TCTR). This conversion has many advantages - for instance, increasing the reliability of the protection and automation systems in terms of broadcasting the data, making it available for the entire system. Further, it reduces the overall SAS cost in terms of limiting the copper wires’ utilization. This reduction can be achieved by replacing the electrical wires’ connection with the logic interfaces. The output packet stream samples that the MU may transfer over the point-to-point-type connection to any IED are broadcasted over the local area network (LAN) in a similar manner to GOOSE messages (IEC 61850-9-1 2003) (Brand 2008).

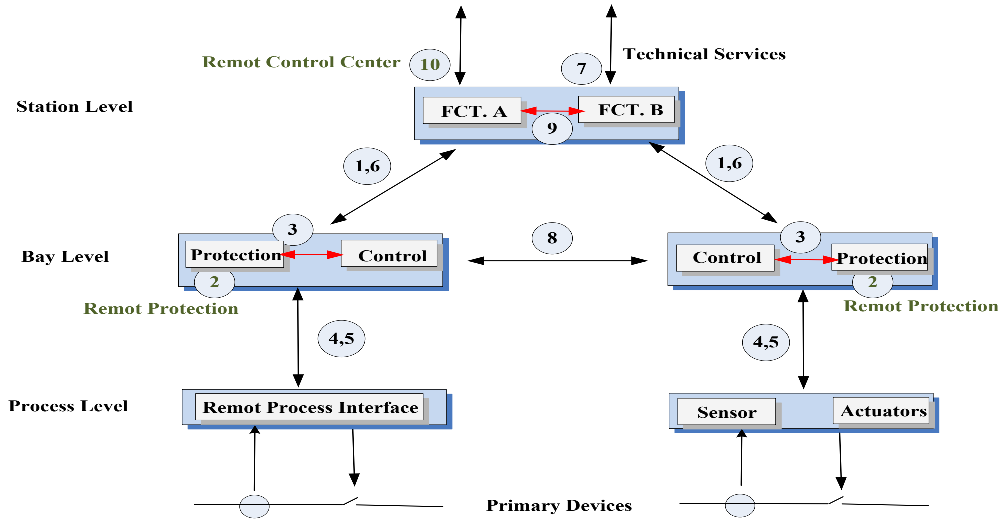


Figure 15. SAS levels and logical interfaces.

Within the bay-level, IEDs such as the protection and control units provide protection functions by means of implementing the functions' output signals initiated on one bay such that they may perform an action on the primary apparatus of the primary (level one) bay. The IEC 61850 standard offers the feature whereby the SAS functions may be freely or logically allocated between IEDs. Nowadays, state-of-the-art IEDs may provide multiple functions such as monitoring, protection and control within an individual IED. On the other hand, different functions within an individual bay unit have the ability to share data, as illustrated by interface number three. Various bays - in terms of the horizontal communication GOOSE messages - are able to communicate with each other by interface number eight. Interfaces four and five illustrate the communication between the bay level and the process level, and interfaces one and six illustrate the communication between the bay level and the station level. The station level equipment, such as the HMI, the station workplace, the alarm unit and its features, the remote control centre, the database, etc., communicates with the bay level within interface one to exchange protection data and interface six to exchange control data. Further, interface nine illustrates the sharing data within the station level. Interfaces seven and 10 illustrate the sharing data outside the local station operator. These tasks have been carried out using the second version of standard IEC 61850-7-420.

1.3.8 The IEC 61850 Communication Protocols

The main idea behind the IEC 61850 standard is that the data object model and services are separated from the communication ISO/OSI layers' stack. This approach offers the opportunity to implement the state-of-the-art of communication technologies. The mainstream technologies are the communication schemes that have been used for the ISO/OSI reference model. The ISO/SOI stack is based on the concept of layering communication functionality, consisting of seven layers as illustrated in Figure 16. Layers one and two are the Ethernet physical and link layer, layers three and four comprise the TCP/IP layer, and layers six and seven comprise the MMS layer. The IEC 61850 object models are mapped over different layers in terms of their services and requirements. The object model based on the client/server services ACSI is mapped to the five-seven MMS layers, whereas the high-speed time-critical messages, such as SV, the status indications blocking the trip commands and GOOSE, are mapped directly to the Ethernet link layer (IEC 61850-8-1 2003) (Brand 2004).

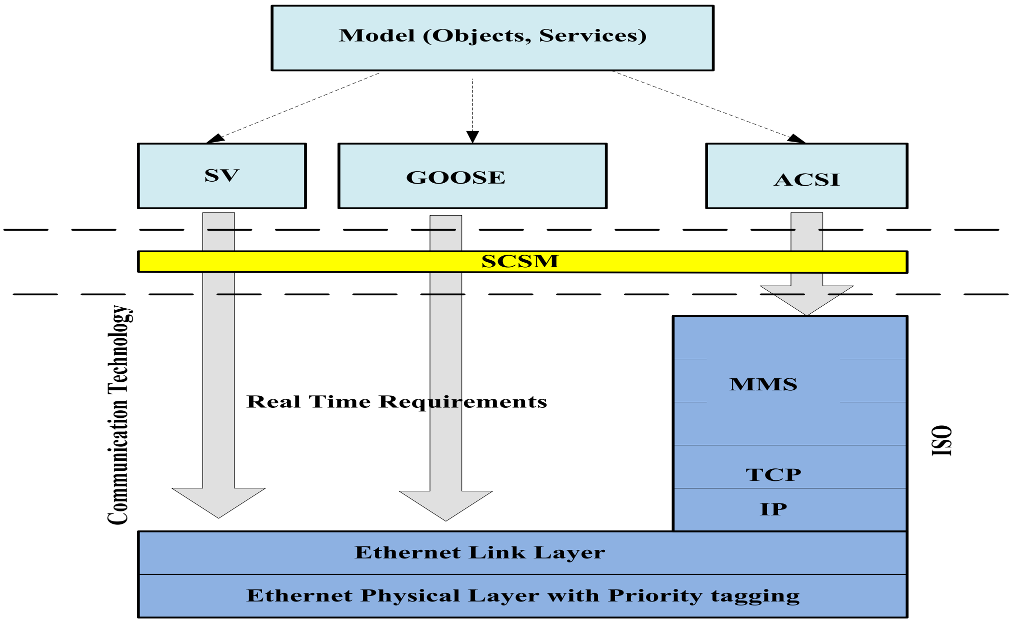


Figure 16. IEC 61850 application messages mapping to the OSI layers.

1.3.8.1 The Abstract Communication Service Interface

The IEDs are described by the standardized method that allows all of them to share data by means of an identical structure that is related to their functions. From the network behaviour perspective, the ACSI provides the specification for the basic model that represents the definition for the substation-specific information models. Further, it specifies a set of information exchange service models and the response to those services. This specification allows various IEDs to exhibit identical behaviour. The abstraction technique that has been adopted by IEC 61850 is one of the most significant features which separates the SAS application from the underlying communication protocol and operating systems, as illustrated in Figure 17. (Adamiak etc. 2009).

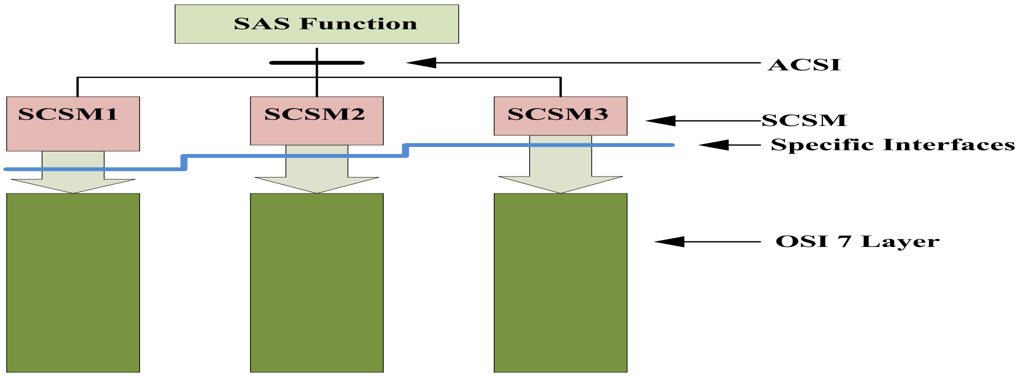


Figure 17. Abstract communication service interface concept.

An ACSI concept has two approaches. Firstly, based on the basic information model, only aspects of real devices or real functions that are visible and accessible over the network are modelled, resulting in hierarchical class models, such as LOGICAL-DEVICE, LOGICAL-NODE, DATA and DataAttribute. Secondly, based upon the exchange service model, the abstraction can be defined from the way in which the devices are able to share the information in terms of the definition, focusing on aspects of the purpose of the services instead of describing how the services are built (IEC 61850-7-2 2003). In a real implementation, the basic information model and services' model are mapped into an existing communication stack. The mapping schemes are achieved through the SCSM. In IEC 61850, two mapping schemes are specified (IEC 61850-9-1 2003) for the transmission of the SV (IEC 61850-8-1 2003) and for the transmission of wide station events and all other communication services. Further, the ACSI provides abstract interfaces that describe communications between client and server. This type of interface can be used for real-time applications, such as data access, data recovery, device control, publisher/subscriber applications, event reporting and transferring, self-description, self-healing, data typing and data reading. Further, it describes communications between applications on one device as a publisher to many applications on various devices as a subscriber for fast and reliable system-wide event distributions, such as GOOSE, generic substation events (GSEs) and SV. The ACSI interfaces which are defined above allowed the client to observe the data model, to get and set data, to manipulate data-sets, to log, etc., by means of a calling method such as GetDataValues or SetDataValues. These methods employed in the programing language are reasonably traditional methods, with assigned arguments leading to returned output values (Pedersen 2010). Consequently, the ACSI model defined the services set within the client application while the server application defined the response to the requested services. It also defined the concept of “application associations”. This feature represents the controlling access mechanisms to an object within a device. In order to restrict a particular devices’ visibility, different access-control schemes can be used.

1.3.8.2 GSSE, GOOSE and SV

The GSE service model is one of the main features of IEC 61850 that offers fast and reliable real-time applications to deliver SAS data values over the communications system network. The GSE service model is based on the concept of independency decentralization. It uses a multicast/broadcast services model based on an efficient method. This multicast/broadcast services model provides for the simultaneous distribution of the SAS event values to all of the SAS subscriber IEDs. The generic substation event distributions also support peer-to-peer and client/server communication models. IEC 61850-7-2 defines two control classes and the structures of two messages, such as,

1. GOOSE, which supports a wide variety of the SAS’s common data, such as analogue, binary and integer value data-types grouped by Data-Set.
2. GSSE, which supports only the status change information events, fixed structure binary events and bit pairs.

Therefore, the type of shared information is the major difference between the GOOSE and GSSE services. The flexible GOOSE model is used by all new systems, and conveys a wide range of messages and binary and analogue data. Meanwhile, GSSE is older and only delivers binary values within its messages. Figure 18 illustrates the GOOSE model. The message is based on the publisher/subscriber exchange mechanism. From an implementation point of view, at the publisher side the values are written in the local buffer, while at the receiving side the subscribers read the values from the local buffer. The local buffers of the sub-scribers are updated by the communications system where the GSE control class has been used as a controller for the procedure from the publisher side (IEC 61850-7-2 2003).

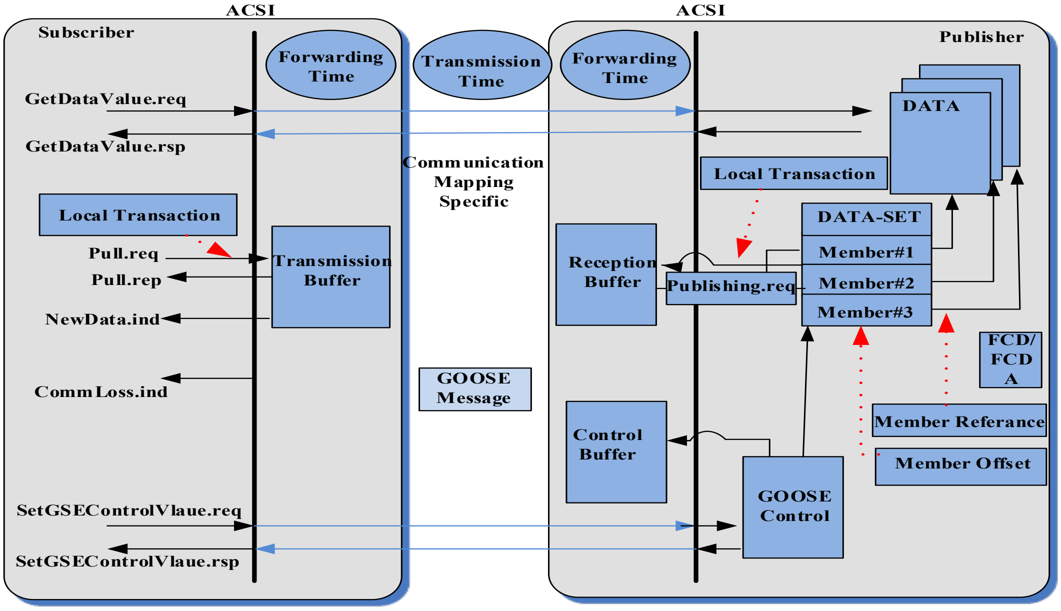


Figure 18. GOOSE service operation mechanism.

The substation IEDs recognize the changing status as well as when the last status changes occur upon receiving the GOOSE messages, which contain all the needed information. Further, the local timer of the subscriber can be set based on the related time of the latest status change event. At this point, GOOSE has been identified as having one of the fastest times for critical messages within an SAS. Therefore, GOOSE messages are mapped directly to the Ethernet layer in order to support the real-time operation requirements. Typical protection events, such as trip, interlock and status indication, are recognized as high priority services in which the processing time must be less than a quarter of a cycle. For instance, the message transmission time for the 50 Hz cycling frequency system is specified as <4 ms. Moreover, since the GOOSE messages are directly mapped over the Ethernet layer, which does not guarantee delivering services. The retransmission scheme should be used to ensure that the messages are received based on a multicast transmission. Lastly, since the GOOSE message can serve various applications with different performance requirements and various data types, it may be considered as a flexible tool, (Zhang & Kumal 2008).

Another high-speed time-critical message within the SAS are the SV messages, which are used to deliver measured values from switchyard-to-bay IEDs in a digitized form. Multicast is a transmission scheme whereby the measured values at one location can be delivered to any number of subscribers. Either an intelligent instrument or the MU is responsible for the digitalization process. A particular target may require a distinctive sampling rate which can be freely selected based upon their needs (Hou & Dolezik 2008). More details about SV are provided in Chapter Three.

1.3.8.3 Manufacturing Messaging Specification (MMS)

The object model and service that are defined in IEC 61850-7-x are mapped over the application layer of the MMS (layer seven), which is a part of ACSI that does not utilize time-critical messages. The MMS is an international standardized mes-saging system (ISO 9506) that has been used to exchange real-time data and ser-vices among network devices. The mean feature of the MMS is that it is ind-pendent of the application function being performed as well as the device and software manufacturer. Further, based on the highly generic nature of the message services provided by MMS, it is appropriate for different types of functions, de-vices and industries - for instance, based on ACSI's implementation requirements the information modelling and services that are provided by MMS precisely meet its needs (Stalling 2007). When looking at the benefit of implementing MMS messaging services, three major effects that can be evaluated contribute to reduce costs. First, there is interoperability, which allows network applications and IEDs to share their real-time information without the need to create information environments. Second, there is independence, which provides interoperability independently of the developer of the application, network connectivity and functions based on provide common communication services. Last, there is data access, which facilitates applications to provide useful functions by obtaining the information that is required through the network application (IEC 61850-7-2 2003). From the implementation perspective as regards MMS services, the object of the ACSI server class is mapped based on IEC 61850-8-1 by SCSM one-to-one over the virtual machine device (VMD) object. The VMD is the key feature of the MMS services, specifying how the server behaves based upon the client application's point of view. Moreover, it represents that part of an application task that enables the monitoring and control of services by means of a set of resources and functionality associated with one or more devices. Generally, the VMD defines the objects that the server consists of. Further, the services enable a client to access and manipulate these objects by means of assigning one or multiple communication addresses that create service access points (SAPs) where the MMS services can be exchanged. Figure 19 illustrates the VMD concept (SISCO 1995).

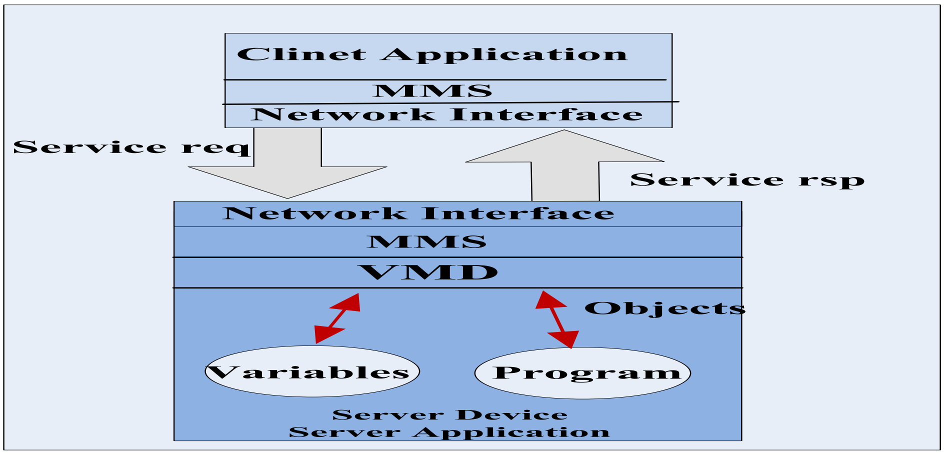


Figure 19. MMS concept.

1.3.9 GOOSE Retransmission deterministic approach

The GOOSE message structure clarifies that it is a routable message which is delivered to the assigned IED subscriber network address as opposed to the IED address which uses a multicast scheme. The network address represents the mail group subscription address and not the IED address, which routes the GOOSE messages inside the LAN rather than via the WAN. The multicast scheme creates technical challenges inside the LAN for the message delivery process. The challenge in conventional LAN is when the substation event is broadcast by the IED inside the LAN and other IEDs receive the message and duplicate to the same LAN, such that data collisions with the sending IED and transmission delays may accrue. Therefore, the unpredictable behaviour for the LAN makes each IED responsible for handling various LAN network circumstances, such as message drop, message delay, asynchronous delivery and outages (McDonland 2003). The Ethernet network is based on carrier sense multiple access collision detection (CSMA/CD), which is a non-deterministic protocol that is based on its implementation, and senses the channel and detects other transmission signals if they appear to eliminate data collisions. This concept is used within the existing Ethernet network, which introduced the queuing scheme and which increases the non-deterministic factor and latency. Further, it can be very difficult to predict the number of data across the network (Curtis 2000). Increasing the number of devices connected into the LAN sees that the expected data collision is increased exponentially. Modern Ethernet switching, token ring and token bus, retransmission scheme and priority tagging are used to enhance the real-time deterministic performance suitable for the SAS (Thomas & Ali 2010).

IEC 61850-8-1 defined the retransmission scheme to achieve a proper level of reliability, as illustrated in Figure 20. GOOSE messages are constantly published and indicated to substation actions that request a SendGosse service which contains a set of data that may consists of binary and analogue data entities. Within the substation configuration processes, every GOOSE message is associated with a specific max time (mt) parameter as a waiting time between the first GOOSE message publication and the retransmission event in a stable condition as a T0 GOOSE heartbeat transmission. The next retransmission of the GOOSE message happens when the data element is changed or else T0 expires. In this case, the data element that will have changed the time of transmission (tot) that separates the GOOSE messages is reduced to a very short period, as illustrated in Figure 20, as (T1) to increase the probability of receiving GOOSE messages by all the sub-scribers. After a few retransmissions, the (tot) will increase gradually until reaching the assigned T0 parameter. For each message in the retransmission process, the publisher assigned a time to live (ttl), which is used to calculate the time to wait (ttw) by the subscriber. When the ttw interval has expired and the message has not been received by the subscriber, it indicates that the association is lost, which is one of the most intelligent features added by the IEC 61850 standard to the SAS.

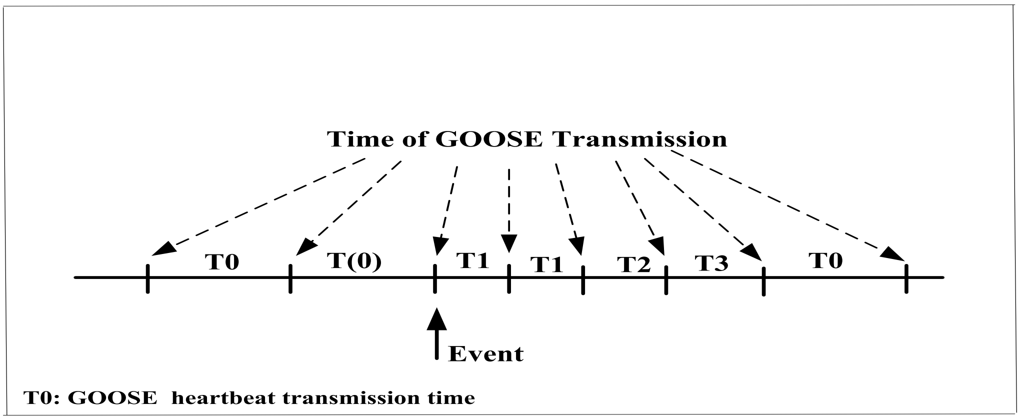

Time of GOOSE Transmission
T0
T(0)
T1
T1
T2
T3
T0
Event
T0: GOOSE heartbeat transmission time

Figure 20. GOOSE retransmission concept.

1.3.10 Substation Configuration description Language (SCL)

IEC 61850-6-1 specifies the substation configuration language SCL based on the XML. The system integrator may need to configure the system devices both before utilizations and also in the case of adding new devices to the system. The SCL exhibits a hierarchical file configuration in which it allows unambiguous descriptions within multiple levels of the system based on the standardized XML files. It is a uniform description of the system configuration and the relation between the system and the allocated functions. Therefore, using the SCL file format makes it possible to describe - in a standardized manner - communication and function-related device capability, the device parameters, the communications system configuration and the allocation of the system devices. These descriptions' files for the entire system and its devices can be shared between devices, engineering tools and various system engineering tools to build up the automation system (Brand 2004).

In order to achieve the systems' integration in the standardized way in compliance with the IEC 61850 data model, the SCL defined an object model that describes the IEDs' connection, allocation and how the object model can be published with-in various SCL files. These files can be exported or imported with various system engineering tools. Six different SCL files data types are defined based on the configuration step, their content and their needs. They are constructed using an identical format and method; however, they have varying scope and numerous extensions. From these files' system configuration tool can be obtained all the needed information, such as the substation network topology, the IED's description, the communications system's description and the data-type templates. Table 3 describes the six file types and their extinctions (IEC 61850-1 2003).

Table 3. SCL file types and extinctions.

Ex.	Name	Description
.icd	IED Capability Description	Describe the capabilities of an IED, IED allocation, IED communication description and system description
.ssd	System Specification Description	Describe the SAS and the required LNs
.scd	Substation Configuration Description	Specify all IEDs, communication configuration and substation description
.cid	Configured IED Description	Facilitate the communication between an IED configuration tool, IED allocation within the substation
.IID	Instantiated IED Description	Describe the configuration for an IED
.SED	System Exchange Description	Describe the exchanging configuration between substations

1.3.11 Time Synchronization (TS)

The digitization of the SAS based upon the IEC 61850 standard with the associated strict performance requirements deems that all devices in the substation should be accurately synchronized for the time stamping of data and motion control. For a better understanding of the TS approach, lets us ask a most important question: where, in an SAS, several IEDs are connected together, how will accurate and coordinated time services with a vast amount of information be made available at a fast rate? In addition, there are most of the substation functions - for instance, the distance function which requires the voltage and the current to be synchronized, and the synchrony-check function which needs to make a comparison between voltages in order to possess a common reference, etc. This function will not operate properly if their events are not organized in a way such that the accruing order is the same as when they are published.

Time reference is one simple solution, where by means of electing one IED as a time reference all the other IEDs should synchronize with it. However this solution works satisfactorily with small SASs, since the IED time will lag from the time reference with the LAN's delayed value, which is the time that the messages need to travel from the time reference to their destination (Ozansoy et al. 2008).

IEC 61850 states that the TS model is needed to provide a synchronized coordinated universal time (CUT) to all IEDs in the LAN based on use of the simple network time protocol (SNTP) which can achieve accuracies within the range of 1 ms. The TS requirements should be met whether the SNTP or another protocol has been used. Figure 21 illustrates the TS model with a time-server that has been externally synchronized with an external resource, such as a GPS receiver. All the IEDs in the substation are synchronized with the time-server, which represents the source for the substation's internal TS and time stamping (IEC 61850-7-2 2003).

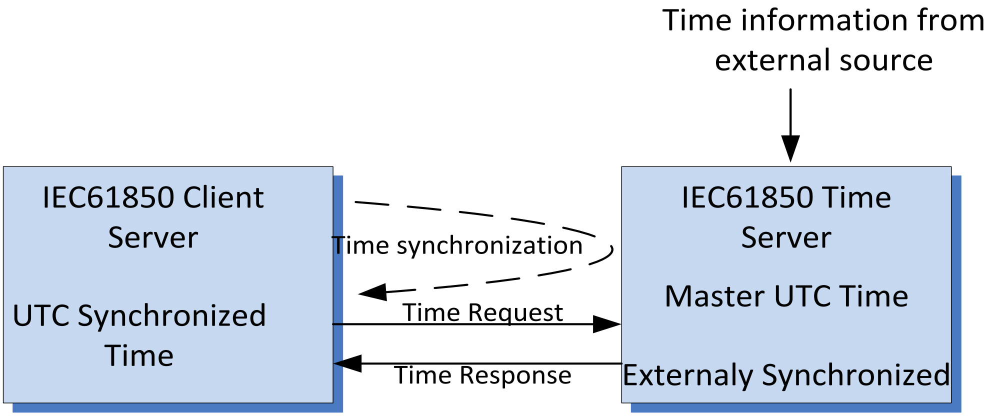


Figure 21. Time synchronization model.

Various classes of TS accuracy have been defined by the IEC 61850 standard, as illustrated in Table 4. The first two time-performance classes (T1, T2) are defined for normal events that are not time-critical events. The rest (T3, T4 and T5) are defined for the critical time events, such as protection and metering. As regards, the TS protocol that is chosen and the performance of the underlying hardware plays a critical role in the accuracy of the TS model. Therefore, the accuracy that is provided by the conventional solution is 1 ms, which does not meet the requirements that are assigned for the raw data SV.

Alternatively, one solution is to use the Inter-Range Instrumentation Group time code B (IRIG-B) which is not a time source itself. It provides accuracy of 5 µs and requires an external time source, such as GPS. Another solution is to use precision time control (PTC), which was defined in IEEE 1588. It is a standard control mechanism for ensuring interoperability between IEDs while meeting the best individual application requirements and provides accuracy of 0.5 µs. The PTC has been considered as a form of network core synchronization with a minimum hardware assist and soft-ware (Dominicis etc. 2011).

Table 4. Time performance requirements**.**

Performance Class	Accuracy	Application
T1	± 1ms	Events
T2	± 0.1ms	Synchrocheck
T3	± 25µs	Sampled Values
T4	± 4µs	Sampled Values
T5	± 1µs	Sampled Values

1.3.12 Reliability Criteria and Redundancy

Redundancy has been identified as a key enabling reliability criteria for SASs in terms of avoiding taking down the whole system due to a single failure. However, the IEC 61850 standard does not specify the required architecture issues in order to achieve an extremely reliable SAS. The result is that discussion and testing work is left to the end users in order to make this approach available in practice and provide a highly fault-tolerant system. Therefore, in order to achieve a high degree of system tolerance, redundancy in devices and communication paths should be ensured at each substation level. The extent of the redundancy provided is based upon the size of the substation - for instance, large, high-voltage substations often have two individual parallel communication paths and redundant protection IEDs, whereas, in a small substation with a lower voltage, no parallel communication paths are used but redundant IEDs may be implemented. The redundancy scheme is a way to increase reliability. However, in other hands it creates system complexity in hardware and software and also increases costs. Therefore, it requires more practical and careful implementation (IEC 61850-6 2003).

From the single device perspective, redundancy can be provided by duplicating relays or IEDs - for instance, a high-voltage transmission line may require duplicated mains protection with a duplicate HMI, either for operational reasons or redundancy. Both duplicated HMIs have the capability to switch-over upon a failure event. An alternative solution is to provide redundancy in the communication path where the modern Ethernet switch with be used. An Ethernet switch is an IED that has multiple ports which may require configuration based on its operating system, firmware and power supply. This provision of the Ethernet switch creates genuine full-duplex communication between the operator and the process level with a high data rate, a minimum number of collisions and a high degree of reliability (Hou & Dolezilek 2008) (Kasztenny 2006).

According to IEC 61850-6, all the substation devices can be connected in a ring topology and based on network redundancy, whereby each IED has two Ethernet ports to create redundant network communication, as illustrated in Figure 22. Here, we can observe that each IED has been connected with a separate connection port to each closed-loop ring. These closed-loop rings are redundantly established in parallel in order to limit the cause of failure by offering an alternative connection link within the bay IEDs. However, in the communications performance requirements mentioned before, fast GOOSE messages have a strict performance requirement that the messages should be delivered in less than 4 ms.

A virtual local area network (VLAN) is a one of the technical solutions that attenu-ates the effect of the broadcast/multicast phenomenon in LAN. This can be done by originating a needed network segment by dividing the physically connected network and reducing the traffic flow by restricting it into a single individual VLAN (Ali & Thomas 2006).

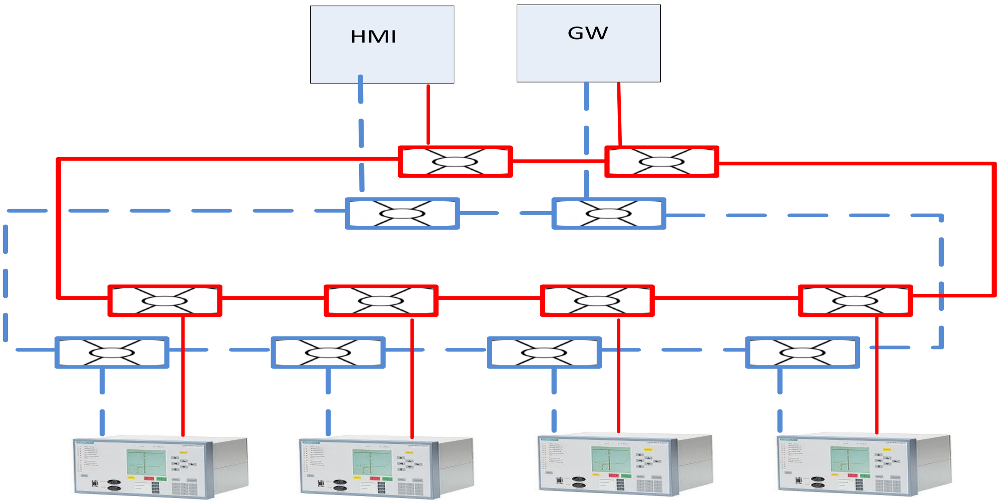


Figure 22. Double parallel redundant ring.

1.3.13 Cyber Security

Cyber security is a term that is introduced with respect to the digital environment, whereby devices with an embedded microprocessor are now commonly used for control and automation functions. Since SASs based on IEC 61850 were firstly designed to operate within a secure network - the individual substation – the IEC 61850 standard does not provide a security solution (and so it is not covered by the first version of the standard). However, in terms of a WAN, where the client is located outside the secured LAN and attempts to access the SAS's functions, in this case data security is a critical issue. As such, different control access schemes, such as secure connection, authentication and encryption, should be considered (Apostolov 2003). IEC 61850-7-2 provides an access control model that addresses the data security aspect. The data-access process can be restricted at various levels throughout the access control model in relation to a specific server. Therefore, for instance, the group of data attributes might be visible with accessible permissions for a selected client; however, they are invisible to the other clients through the access control model restriction. As a result, the access control specification of the server and the identification of the client play a key role in the restriction process. The set of restrictions is called a "virtual access view". The virtual access view also provides the capability to restrict supported services in addition to the restriction on the visibility of the instances to a specific client. Various proposed security schemes have been investigated recently (Prematratne et al. 2010); however, they are not covered by this work.

1.4 IEC 61850 Technical Challenges Implementation Issues

From the first step, since the IEC 61850 standard has been published, the major scope of the standard has been to clarify the communication issues within the SAS that compose various manufacturers' devices. This task has been fulfilled by defining several communication protocols that facilitate the sharing of information among those various manufacturers' devices. However, several implementation issues have been left to the researchers' design engineers to deal with, such as the reliability of the SAS and the reliability of the IEC 61850 distributed functions, improving system reliability based on a redundancy approach and the type of redundancy, the commissioning of various manufacturers' devices' tasks, the clarification of actual complete system designs and their operation and maintenance issues. Moreover, the open nature of the IEC 61850 standard gives a wide ranging freedom for manufacturers to operate with that may increase the complexity of the IEC 61850 implementation task. In addition, the emerging concept of the SG places a high degree of pressure on existing utilities' infrastructure operations. Following several of the available automation and protection functions, their fundamental operational schemes have been collapsing, as mentioned earlier. Therefore, further discussions and testing works need to be processed in order to meet end users requirements and for the successful implementation of the IEC 61850 standard. In this section, the technical challenges and the IEC 61850 standard's implementation issues have been highlighted, and in the rest of this thesis these issues are analysed and appropriate solutions are developed. These developing solutions have been carried out to facilitate and bring about a complete SAS that has the ability to utilize the vision of the IEC 61850standard.

1.4.1 IEC 61850 SAS Functions Reliability Estimation Challenging

An automation system's reliability is directly related to the reliability of its IEDs, protection and automation functions. The IEC 61850 standard defines the concept of a distributed function to allow for the free allocation of functions within various IEDs (IEC 61850-1). As a result, functions may split into parts, executed within various IEDs. These functional parts need to communicate with each other to implement the assigned function successfully. Further, based on IEC 61850's defined reliability restriction, no such single point of failure should exist that can cause the whole system to enter into a failed state. However, to my knowledge the reliability of IEC 61850's functions have not been discussed or analysed before the present literature. Most of the available previous research focused on the whole system's reliability calculation using various existing calculation methods. Kanber and Sidhu (2009), Andersson et al. (2005) and Yunnis et al. (2008) have been using the reliability block diagram (RBD) and fault-tree methods based on their system reliability calculations for different SAS topologies. Further, Jisng and Singh (2010) add another parameter (repair rates) to the system reliability calculation. A Markov model was used for a reliability estimation model in Anderson et al. (1997), Anderson et al. (1992) and Singh and Patton (1980). Therefore, it is important to carry out an estimation of the reliability and probability of failure for IEC 61850 functions based on different practical Ethernet communications bus topologies to prove the feasibility of the IEC 61850 distributed function. Furthermore, it is also important to develop a novel reliability and probability of failure estimation method RaFSA that may facilitate the reliability and probability of failure estimation tasks, as well as well as facilitating the system reliability estimation with various adding parameters (e.g., the repairing time, the load flow, reconfiguration, optimization, etc.) were these parameters are hard to estimate within the analytical approach.

1.4.2 IEC 61850 SAS Performance Analysis and Evaluation Challenging

1.4.2.1 IEC 61850 Communication System Network Latencies Estimation Challenging

The IEC 61850 standard defines a high priority and specific time delay for the high-speed time-critical messages' latencies, such as GOOSE and SV, that need to reach their destinations in less than 3-4 ms. In order to reduce the processing time for the high-speed messages, the IEC 61850 standard specifies a direct implementation over the OSI layers, whereby these high-speed messages have to mapped directly over the Ethernet link layer. However, given the dynamic behaviour of the IEC 61850 communications network, the overall system performance and traffic latency cannot be easily estimated. Moreover, in IEC 61850-5, the part-estimated messages' latencies within the communications network were defined based on a simple approach. This simple latency estimation approach (one-way messages, publisher-to-subscriber) actually does not reflect or guarantee the actual system's performance, which is really important for an SAS's practical, real-time applications. Sidhu and Yin (2007), Chen et al. (2012), Ali et al. (2012) and Ridwan et al. (2012) analysed the performance of the IEC 61850 communications network using various simulation tools based on the defined simple latencies estimation approach. Therefore, there is a need to develop a proper approach for estimating the critical-time messages' latencies which reflects the real behaviour within the system (a round-trip approach) (Steinhauser et al. 2010). Moreover, it is possible to utilize this round-trip development approach within an actual physical SAS rather than a simulation environment, which increases the challenges to the system's commissioning, especially when the actual AS devices come from various manufacturers. In addition, several assumptions were made by the author in order to facilitate the communications system's network latencies estimation task.

1.4.2.2 Challenges for System Interoperability and Commissioning

One of the most challenging issues is evaluating and confirming the performance of the complete AS composed of a set of various manufacturers' IEDs. This is because the IEC 61850 standard specifies the performance of a single IED based on the required response times for various events within the SAS (the conform-ance test). From the cumulative experiences that have been gained by working with the DEMVE 1 and DEMVE 2 projects, wide ranging issues are raised based on the various manufacturers' IEDs' integration tasks, such that IEDs which con-form to the IEC 61850 standard and which also pass the conformance test still risk being incapable of operating with each other. Researchers and developers have noted that the open nature of the IEC 61850 standard gives wide ranging freedom for manufacturers to operate with. Further, the interpretation of the IEC 61850 standard by different manufacturers remains different based upon the ambiguities that still exist. These issues may vary the interoperation of the standard from one manufacturer to another and may increase the complexity of the interoperability tasks within the SAS. Therefore, IEDs passing the conformance test cannot ensure interoperability and are not sufficient for end users' requirements. End users must include the interoperability test as an element through the IED acceptance process. Ali, Mini and Thoma (2012), Holbach et al. (2007), Chen et al. (2012), Ridwan et al. (2012), Ridwan et al. (2014), Niejahr, Englert and Dawidczak (2010), Hong et al. (2013), Mekkanen et al. (2013) and Falk (2011) have identified the importance of end user interoperability testing based on various practical pilot projects. Therefore, the University of Vaasa has set up an in-house research and testing laboratory, DEMVE. This project supports the vision and spirit of IEC 61850 based on SASs' sharing information and executing it is in the mean concern view. The outputs of this project offer a complete guide as to how to integrate various manufacturers' IEDs and how to characterize data sharing among the whole integrated system. Moreover, they offer a solution for the most complicated system integration tasks by developing a novel approach to the vendor/natural system configuration tool.

1.4.2.3 Challenges for the System's Configuration

A practical system interoperability testing project requires various methods and tools. However, the IEC 61850 standard defines the IEDs model, communication services and their various common files in order to describe those models and it does not try to specify the IED or the system configuration tool. The various manufacturers' IEDs and system configuration tools present significant challenges for protection and integration engineers while configuring individual IEDs or even the whole system. The challenges have been raised based on the IED protection and configuration settings' parameters and are different for each manufacturer, requiring proprietary software for each IED. Moreover, engineers need to be trained to implement different proprietary configuration tools for the same pur-pose. Ali, Mini and Thoma (2012), Holbach et al. (2007), Chen et al. (2012), Ridwan et al. (2012), Ridwan et al. (2012), Niejahr, Englert and Dawidczak (2010), Hong et al. (2013), Mekkanen et al. (2013) and Falk (2011) have identified the major challenges facing the implementation of the IEC 61850 standard in multi-vendor IEDs, such that the most costly and time-consuming process was the configuration task (based on the available SAS configuration tools). Most of the above-mentioned works were pilot projects that were used commercial IEDs on a designed laboratory platform and commercial software configuration tools. Moreover, the commissioning task needs the full support of manufacturers' products lines. Therefore, in order to reduce costs, the effort involved and the time taken, a novel approach for a new SAS configuration tool must be developed that is independent of any commercial IED brand. In addition, it must have the ability to import SCL files from various manufacturers, IEDs, systems and databases, creating and increasing the IEDs' configuration to the system level. As a result, in this thesis the vendor's natural system configuration tool approach is invented and proposed in order to enhance the SAS configuration task. In addition, it may go beyond the SAS that it supports - for example, large utilities composed of various manufacturer units, IEDs or the SG concept.

1.4.2.4 Technical Challenges IEC 61850-9-2 Process Bus Implementation

The evolution of the IEC 61850-9-2 process bus as a high data-rate communications network has greatly improved the capability of SASs. This evolution has led to significant growth in product development and process bus commissioning. Several process bus projects have been commissioned worldwide. However, regardless to this growth, the available knowledge about the real behaviour of the process bus network (especially when there is a large number of SV traffic resources connected within the same communications system network) remains slight. Moreover, the dynamic behaviour and the traffic latencies within the process bus operation have been considered as a unique critical characteristic. These characteristics have hard real-time requirements and can be increased and decreased based on changes in the network topology and traffic in the network being tested. As a result, process bus network analysis is a focus of research for both industry and academia, and several network process bus models have been subject to testing. However, their hard assumptions limit their effectiveness (Amelot et al. 2011). In Sidhu and Yin (2007), the modelling and simulation of the distribution substation regards 69 kV and 220 kV; however, the raw data of the SV traffic's characteristics that has been used is not compliant with IEC 61850-9-2LE. In Gurbiel et al. (2009), several studies are conducted based on a test bench that calculates and compares the characteristics of the SV traffics' differences between the two paths direct from the MU and the source of the digital reference signal. David Ingram has performed several studies that have discussed the process bus's critical issues, such as TS, routing and process bus traffic analysis. Most of the studies were done using the GTNET card with the SV firmware to generate the MU stream, and the Endace DAG7.5G4 network card to monitor the traffic. The weak point of those works is that they cannot reflect the real behaviour of the system, since they generate streaming traffic based on a mathematical calculation (the number of MUs in the network multiplied by the traffic that each MU can generate every second) and they then injected the traffic into the process bus net-work. Accordingly, the injected traffic calculation of the behaviour of the rest of the network components was performed (Ingram et al. 2013; Ingram et al. 2012). However, none of these above-mentioned above works presents or reflects the real dynamic behaviour of the process bus communications networks or assesses the limits of the process bus networks based on this dynamic behaviour. There-fore, as a first step, it is important to assess the limits and simulate the dynamic performance of the process bus communications system network using OPNET, which is and industry-trusted simulation tool. This task requires modelling various IEDs, such as MU, ESW, the communication link and the receiving IED, which they have not developed yet and which do not exist in the simulation tool library. These modelled IEDs' various communications network parameters need to be considered (e.g., various communication link speeds, the IED's microprocessor processing time, the packet the enter-arrival time, the switch buffers' sizes, the number of queues, the capacity of the queue, etc.). Within the second step, a hardware laboratory for a typical IEC 61850-9-2LE process bus network using commercial physical devices is set up. Various MUs, SV traffic sources, media convertors, a network synchronizer and a network analyser are constructed with this developed laboratory testing facility. This practical test attempts to reflect actual SASs' real behaviour in the process bus network and to assess their performance within each SAS. Moreover, the practical testing process offers complete guidance for the real challenges that are faced during the process bus analysis. Firstly, the hardware challenges based on integrating various commercial merging MUs' IEDs and media converters. Further, the number of the SV traffic sources is not enough to assess the limit and capacity of the process bus network, whereby the testing steps require 1-22 SV traffic sources. Secondly, the SV traffic stream latencies' estimation challenges based on developing a novel approach for estimating the sample value packets' stream latencies for the publishing/subscribing time analysis for a series of successive receiving packets. This novel SV estimation latency approach needs to be implemented over various network analyser tools to test the performance of the novel approach with the help of MATLAB. Finally, comparisons between the IEC 61850-9-2LE process bus practical experiments and the IEC 61850-9-2LE process bus OPNET simulation models' result outputs have been carried out. By implementing the comparison, two benefits have been noted. From a practical experiment point of view, it proves the correctness of the design and the implementation of the IEC 61850-9-2LE process bus; from an OPNET simulation model point of view, it shows the rightness of the IEC 61850-9-2LE process bus modelling and the novel time analysis of the SV traffic stream latency. Further, it demonstrates the power of the OPNET simulation tools that can model a high data-rate, real-time system based on the new IEC 61850-9-2LE.

1.5 Motivation

The positive impact of the IEC 61850 standard on automation system offers a reduction in the overall labour and operational costs, and can be clearly seen in terms of increasing the power quality and reducing the outage response. However, this goal requires paying attention to how to implement this relatively new IEC 61850 standard in order to upgrade, build and operate the energy system's automation in an efficient way. Further, it should involve solving the ambiguity issues that are related to the implementation of the IEC 61850 standard. This is because we are moving towards the concept of an SG energy system and a digital environment that sets completely new requirements for electricity distribution and production automation. Distributed production requires distributed automation, which in turn requires standardization and advanced communications solutions in order to operate reliably. Therefore, one of the significant challenges is to examine the feasibility of the IEC 61850 standard for the energy system in terms of the reliability of the protection functions and the performance of the SAS considering the high-speed messages' critical latencies within the energy system communications network.

1.6 Contributions of the Thesis and Methodology

According to these motivations, an analysis and investigation were carried out based on a comprehensive research work to present the impact of the IEC 61850 standards on SASs' operations considering the reliability of the SASs' functions and the robustness of the SASs' communications system network in various circumstances. The highlights of the research tasks were classified based on the theoretical and practical tests variously throughout Chapters 2-4 as mentioned earlier, and are listed below.

1 To investigate the impact of the IEC 61850 standards on SASs' reliability, the availability of the breaker failure protection (BFP) function has been analyzed. Reliability and availability are two of the primary considerations in current and future SAS design. The importance for this investigation has been to provide the reliability and availability of the BFP function in which, with n = 1, the other protection-related SAS functions are a subset of the BFP function. The analysis was carried out over the small transmission substation 220/132 kV platform classified as T1-1 with a single bus which is assigned by the IEC 61850 standard using an RBD method. Comparisons between the reliability and availability results for various substation communications network topologies have been carried out. Redundancy has been identified as key to increasing SASs' reliability (Mekkanen etc. 2012).

2 A generic, novel reliability and probability of failure estimation algorithm (RaFSA) had been invented. The RaFSA estimation method is suitable for estimating the reliability and probability of failure for any individual device, function, subsystem or system. The RaFSA estimations are implemented over a practical, small transmission substation, T1-1. Various SAS communications bus topologies are considered. A stochastic simulation approach is the way in which RaFSA estimations are implemented. The RaFSA estimation method attempts to examine and predict the actual behaviour pattern for each device in the automation system. Various advantages were noted through the implementation of the novel method RaFSA, as illustrated in Chapter 2.2. (Mekkanen etc. 2013a).

3 To evaluate the system's reliability and probability of failure functions, it was developed based on the simulation of a novel approach to various SAS communications bus topologies and experimental tests were carried out. A sequential Monte Carlo simulation method was used based on the reliability and probability of failure evaluations of the RaFSA estimation

method. These evaluations were implemented over the small transmission substation T1-1 for the BFP function. According to the developed solution, various advantages were achieved (e.g., it is a flexible solution that has the ability to change, expand input data and include various parameters in the calculation without the need to change the underlying process) (Mekkanen et al. 2013b). In addition, comparisons between the mathematical and RaFSA reliability and probability of failure results' output values were carried out, showing that significant variations in the RaFSA results values about the true value occur when the number of trials is small. In contrast, the number of variations is significantly reduced as the number of trials increases, converging on the true values.

4 Within the practical analysis and in the first step, a proper approach for estimating the high-speed priority messages' latencies has been developed which is suitable for the dynamic characteristics of the SAS communications network (a round-trip approach). Further, this approach reflects the real behaviour of the devices in the system. In the next step, the utilization of the developing approach is carried out based on the design of the actual physical SAS. The output results values from these practical experiments show that the devices under testing (DUTs) are compliant with the IEC 61850 criteria. Furthermore, it proves the interoperability concept such that the DUTs subscribe to the GOOSE messages from a third-party IED within the designed SAS (Mekkanen etc. 2013d). (Mekkanen etc. 2014a).

5 The second issue related to the practical study was, firstly, to enhance and relax the system configuration task using a novel approach for which a new vendor/natural SAS configuration tool has been invented which is independent of any commercial IED brand. The vendor/natural system con-figuration tool has the ability to import various types of IEC 61850 specific configuration files from different manufacturers, IEDs, systems and da-tabases, and increases the relay configuration to the system level based on the full IEC 61850 standard, including the protection and feature setting levels. Further, this tool is expected to reduce costs and effort involved as well as the time taken for AS configuration and commissioning tasks. Secondly, the vendor/natural system configuration tool has been proposed for large utilities that comprise various manufacturer units and IEDs to re-lax the system configuration task and support the expansion of the IEC 61850 standard so as to go beyond SASs, emerging towards the SG concept (Mekkanen etc. 2014b) (Mekkanen etc. 2014c).

6 The last issue related to the practical study was, firstly, to facilitate the design of the SAS by assessing the capacity of the process bus communications network. For testing purposes, the modelling of various IEDs, such as MUs, ESW, the communication link and the receiving IED (which have not been developed yet and do not exist in the OPNET simulation tool library) has been carried out. Within these modelled IEDs, various communications network parameters need to be considered in order to simulate a typical IEC 61850-9-2LE process bus. The SV traffic stream latencies were successfully measured in two scenarios that confirmed that the first Ethernet switch experienced more latency than the subsequent switches, such that the limits and capacity of the process bus network's critical components (such as the communication links and the Ethernet switch) have been assessed successfully. Secondly, a novel approach for estimating the SV packets' stream latencies based on a time analysis for a series of successive receiving packets has been developed. The developed SV packets stream latency approach has been implemented and tested over the typical designed IEC 61850-9-2LE process bus communications network. Lastly, comparisons between the IEC 61850-9-2LE process bus laboratory's practical experiments and the IEC 61850-9-2LE process bus OPNET simulation models' output results have been carried out (Mekkanen etc. 2014d) (Mekkanen etc. 2014e) (Mekkanen etc. 2014f).

7 To reduce and enhance the energy system's operational costs, an alternative novel framework for the communications system in an SG has been proposed. The novelty of the proposed communications model is that it at-tempts to bring about a reasonable change in SG's communication infra-structure. The study considers wireless communication as a medium and introduces the CR technology. Further, the feasibility of CR in identifying the available spectrum (even with a very low SNR based on subscribing and sensing) has been demonstrated. This task was carried out by using the feature detection method "cyclostationary" within the MATLAB soft-ware environment. The alternative novel framework has many advantages that can be summarized as a reduction in the network's communications system infrastructure costs based on avoiding wired applications and reusing the licensed frequency bands, thereby providing more affordable services (Mekkanen etc. 2013c).

1.7 Organization of the Theses

The rest of this thesis is organized as follows. In Chapter 2, SAS communications network bus topologies are illustrated. The analysis of the various SAS communications network bus topologies attempts to explore some fundamental issues with-in the SAS design. The thesis's analysis is carried out based upon the BFP func-tion. Reliability and availability are identified and calculated for the various SAS topologies. Further, a novel RaFSA estimation method is presented. The novel RaFSA estimation method attempts to examine and predict the actual behaviour pattern for each IED in the system.

In Chapter 3, we design and discuss various practical testing experiments. In the first section, an analysis and methodology for measuring and calculating the high-speed GOOSE messages' latencies within the multi-vendor SAS communications network is presented. A novel approach to the vendor-independent SAS configu-ration tool (which has the ability to import different SCL files) is proposed in the second section. In the third section, the modelling of the modern IEDs is present-ed and discussed in order to build an SAS process bus network and evaluate the performance of the simulated network under different circumstances using OPNET. Lastly, we present a novel approach to estimate the SV packets' stream latency within a LAN based on IEC 61850-9-2LE by means of implementing var-ious practical laboratory tests. Further, a comparative evaluation of the practical and simulation SV traffic streaming latencies' results values is carried out.

In Chapter 4, we propose an alternative framework for the communications system network within an SG. This proposed communications model attempts to bring about a reasonable change in the SG's communications infrastructure with the introduction of CR technology, where it has various advantages.

Chapter 5 concludes this work and highlights several steps for future research.

2 RELIABILITY AVAILABILITY AND PROBABILITY OF FAILURE

The performance of electrical generation, transmission and distribution are directly related to the reliability of their components, mainly IEDs and the SAS's pro-tection functions. Modern IEDs and protection functions can fail for any reason. As such, 100% reliability is impossible. Therefore, in order to assess the system's performance parameters, several reliability, probability of failure and availability analyses were carried out on different SAS communications bus topologies.

2.1 Reliability Availability of IEC 61850 BFP

This part of Chapter 2 analyses the reliability and availability computation of the typical protection BFP function, which requires that all of the communications systems' network paths work properly upon the successful implementation of the assigned function. Reliability and availability computations are implemented over a typical transmission substation T1-1 using the RBD method, considering various communications system network bus topologies. The computational results' values are compared with each other in order to specify and facilitate the SAS design task.

2.1.1 Introduction

The IEC 61850 standard offers a feature whereby the substation's automation functions may be freely or logically allocated between IEDs. Nowadays, based on current microprocessors, individual bay IEDs may provide multiple functions, such as protection and automation. Various bays grounded on GOOSE messaging are able to communicate with each other via so-called "horizontal communication". Communications system networks in substations based on substation buses comprise a wide and involved topic, since no specific solution is identified by the IEC 61850 standard. Further, IEC 61850 standards are thus based on an Ethernet network implementation, which provides flexible physical variants. Therefore, various solutions need to be determined and tested in order to fulfil an SAS's functional requirements based on performance, reliability and availability. In addition, based upon the IEC 61850 reliability requirements, there should not be a single point of failure that can cause the whole system to enter a failed state. However, and to the best on my knowledge, the reliability of IEC 61850's functions have not previously been discussed or analysed by other researchers. Therefore, there needs to be a study of the reliability and availability of IEC 61850 functions' profiles over various SAS communications bus topologies in order to evaluate the SAS's performance.

According to the implementation perspective, substation bus topologies have various advantages and disadvantages, and usually an appropriate trade-off can be made (Brand et al. 2004). A typical substation bus architecture comprises cascad-ed, star and ring topologies. Often, in order to meet the best standard requirements, mixed solutions such as a star/ring topology may be implemented within the SAS design project. In this chapter, we investigate the reliability and availability of the BFP function in relation to various SAS communications system network bus topologies for the T1-1 small transmission substation that is assigned by IEC 61850 using the RBD method. The RBD method represents a success-oriented system network based on simplifying the function's integration within the system by showing the logical connections among the system's components. The other protection or automation functions related to the SAS's operation (except command sequence interlocking) are mostly a subset of the BFP function, with n = 1 (Andersson et al. 2005). The parameter n represents the number of paths that the function-action entities need to use upon a successful implementation of the assigned function. Therefore, the impact of the various SAS communications system network bus topologies and redundant bus networks on reliability and availability are investigated. Comparisons between the reliability and availability estimation and computation output results values for various SAS communications system network bus topologies are carried out in order to identify the most reliable SAS bus topologies (Zima etc. 2005).

2.1.2 Possible Failure of the SAS Protection Functions

Stability is an essential part of successful design, whereby each system has a stability margin. Lost stability can be accrued in cases where the stability margin is less than the disturbance. Accordingly, for the SAS operation this case leads to the collapse of the electrical power system either partially or entirely, which is called "blackout" .Typically, unexpected disturbances can occur in the case of the sudden plugging of a new load across the network or the tripping of one of the mean transmission lines upon a failure within the substation apparatus or else upon the assigned energy systems' maintenance schedule. These possibilities imply that the stable states to the energy system will be disrupted.

Failure within a switchyard apparatus could cause significant damage to crucial operational components, such as power transformers, switchgear, transmission lines, etc. Therefore, protection and control devices are often employed by SASs to allow for the faster isolation of failed subsystems, which can reduce the damage and can prevent bringing down the entire system. As a result, one of the main crucial protection functions related to an SAS's operation is switching operation control. These switches (disconnectors), based on its design restriction, have the ability to connect or disconnect very low currents - for instance, loaded lines are not allowed to switch on or off by themselves if they follow the right sequences. Figure 23, for instance, illustrates a sequence that must be followed in order to switch off a loaded line. Firstly, cut off the current using circuit breaker Q11. Secondly, switch off the line disconnector Q23. This step attempts to clear and isolated the transmission line from the active side of the circuit breaker. Thirdly, switch off the bus bar disconnector Q21 or Q22, depending on which bus bar is the feeder that the line connects with. This step performs isolation clearance between the circuit breaker and the feeder.

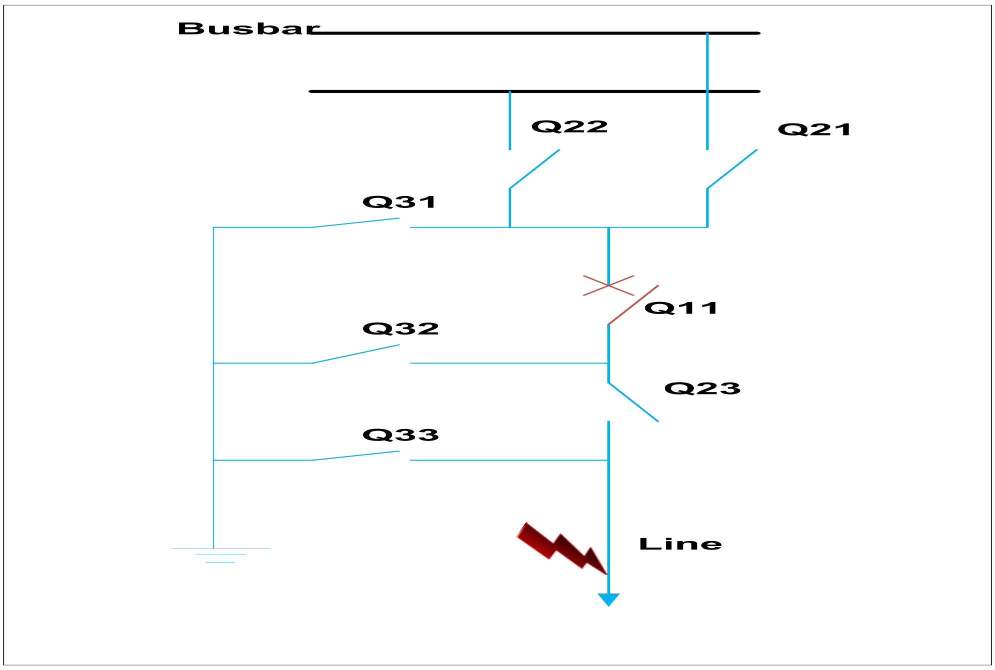


Figure 23. SAS protection function serious actions.

In the case of clearing the line fault upon applying this sequence in the wrong way by sending a command to switch off the disconnector Q21 or Q22 initially, the damage will occur to the disconnector contact points based on an electrical arc arising between them. This fault leads to an interphase short circuit. In addition, it may cause considerable material loss due to the fact that the complete damage to the disconnector might affect (partially or completely) other apparatuses within the substations. According to this example, we might consider that such an absence in the following entities within an SAS operation may increase the probability of failure, 1 The measurement of analogue quantities in the substation may cause a very serious result in terms of loss or delay.

2 Protections based on the quick detection and elimination of faults.

3 Controls of the sequence of switching operations based on programmable interlocking, synchronization and continuity checking of the control circuit of the circuit-breaker and disconnectors.

4 Monitoring, control and automated fast acting based on alarms or warning messages.

5 Communication and sharing information in order to facilitate efficient decision-making.

Therefore, one of the main tasks for consideration for energy system planning is maintaining stability (Brand & Wimmer 2008).

2.1.3 The Typical Small Transmission Substation Architecture T1-1

IEC 61850 specifies T1-1 as a typical, small transmission substation 220/132 kV layout, as illustrated in Figure 5. T1-1 comprises five bays, three line bays, one transformer bay and one bus bay. Each bay may have a protection IED (PIED), a control IED (CIED), even for the bus bay which may require these IEDs based upon the distrusted function allocation that is assigned by IEC 61850. These IEDs may be used to clear faults related to any breaker (Kezunovic 2007). Further, the bus and the transformer bays may have two MUs for each of them based upon the CTs'/VTs' primary three-set apparatus measurements, whereas there is one MU for each feeder. The MU is responsible for the digitalization of the CTs'/VTs' measured values in which is requires a TS source IED. In this case study, the TS source for each MU has been considered. Table 5 tabulates the T1-1 IEDs' specification.

Table 5. T1-1 substation IEDs specification

Bay name	P. IED	C. IED	MU	TS
Line-1	1	1	1	1
Line-2	1	1	1	1
Line-3	1	1	1	1
Transformer	1	1	2	2
Bus	1	1	2	2

2.1.4 The Breaker Failure Protection Function BFP

SAS functions and devices are often employed by a substation to prevent failure and allow for the faster isolation of failure subsystems, which reduces damage and prevents bringing down the entire system. Various types of functions are implemented for this reason, such as interlocking, BFP, fast auto-recluse, inter-tripping, disturbance recorders, etc. All these functions, upon successful execution, require that all the communications system network paths are operated successfully. According to the BFP function, the hosted bay that represents the location where the BFP function resides (protection unit, control unit) is called the "local bay". In case of failure, when the local circuit breaker is in a non-operational state or where there are unexpected measurement values (CTs/VTs), a distributed trip signal from the BFP to adjacent n bays must be achieved in order to execute the BFP function successfully. Four circuit breakers within the T1-1 layout are each connected with a single-bay Ethernet switch. In case of a breaker failure and upon successful execution of the function, the current measurement from the MU in the local bay, to the PIED in the path (MU-ESW-PIED), and the trip signal to other bays in the paths (PIED-ESW-(ESW-BIED) * n), are initiated. Hence, the trip signals to initiate the BFP function might be initiated from different protection functions either within or outside the protection terminal (ABB 2002). Therefore, various communications system network bus topologies have been analysed and it is assumed that the trip signal might be sent directly to the breaker BIED based on the merging concept of the process bus to the station bus.

2.1.5 Reliability and Availability Definition and Calculations

The common meaning of the used term "reliability" indicates the capability to successfully execute the assigned function within the defined period upon the stated condition. Observations and analyses of the available test data related to performance, under either actual or simulated conditions, comprise the parameters that are used in order to assess reliability. These data are governed by a parametric probability distribution which represents the probability that the given system will or will not fail within a specified time (Billinton & Allan 1992). Another commonly used reliability index is the failure rate λ(t), which represents the instantaneous rate of failure per unit time.

A typical failure rate curve for the many physical components is the bath-tub curve, which can be separated into three distinct regions, as illustrated in Figure 24. Region I represents a burn-in that is characterized by a varying, higher failure based upon manufacturing faults or else unsuitable design. Region III represents a wear-out fatigue phase such that the failure rates are increased rapidly with time upon the device ageing. Region II represents the useful life or normal operation, which might be specified by a constant failure rate, and the failure rates are independent of each other where the Poisson curve and exponential distribution are acceptable and used for the availability and reliability calculations.

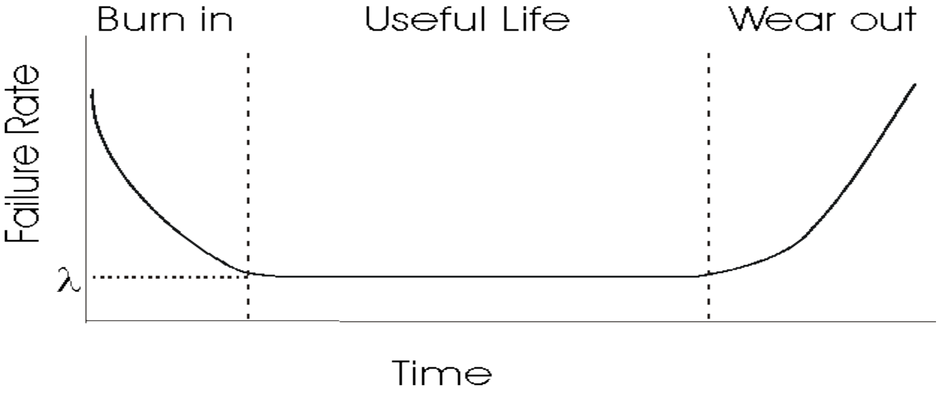


Figure 24. Physical device typical failure rate curve.

In addition, the mean time to fail (MTTF), the mean time to repair (MTTR) and the mean time between failures (MTBF), etc., might be used to represent reliability and availability (for simplicity). The mathematical representation of the data can be implemented by one of the specific statistical probability distribution functions. For instance, if we assume that the underlying failure distribution is exponential (Region II), the reliability representation equations are,

$$Q(t) = \int_0^t f(t)d(t) \tag{2.1}$$

$$R(t) = 1 - \int_0^t f(t)dt \tag{2.2}$$

$$Q(t) = \int_0^t \lambda . e^{-\lambda t} dt \ = 1 - e^{-\lambda t} \tag{2.3}$$

$$R(t) = \int_t^\infty \lambda . e^{-\lambda t} \, dt \ = e^{-\lambda t} \tag{2.4}$$

$$E(t) = \int_0^\infty \lambda t . e^{-\lambda t} dt = \frac{1}{\lambda} = MMTF \tag{2.5}$$

where Q(t) is the cumulative failure distribution function, R(t) represents the reli-ability over time, t, and E(t) is the mean.

Other crucial SAS operation parameters are availability, which is usually estimated based on two separated event failures, and repair as time-to-failure and time-to-repair, which can be considered as reliability-representing components. The simple definition of availability based upon time-to-repair is the probability that the system will be available based on demand. As to the time-to-failure concept, this is the capability of the system being used over a given time. Consequently, determining the availability of the system depends on the communications system network bus topologies and the interconnections between the devices within the system. Two typical devices' interconnection conditions may be considered. First, there is a series interconnection if a failure in one device causes a failure to another device. Second, there is a parallel interconnection if a failure in one device leads to other devices operating over the failed one within the system. The equations for the calculation of availability upon the MTTF and MTTR are as follows,

$$A = \frac{MTTF}{MTTF + MTTR} \tag{2.6}$$

Availability for series systems is,

$$A_s = A_{1.}.A_2 \tag{2.7}$$

Availability for parallel systems is,

$$A_p = A_1 + A_2 - A_1.A_2 \tag{2.8}$$

where A represents the availability. Clearly, 100% availability indicates a fully operable case while 0% indicates the unavailability (i.e., failure) case (Yunus et al. 2008). The failure case might be considered as a component of failure when it is not working as intended or else some functions within an IED do not operate successfully. These inoperable function cases may occur due to an application within an IED no longer being integrable or reachable in the case of failure within the communications system network buses.

The calculation of the reliability and availability was carried out based upon the following assumptions. Firstly, we assume that the failure event modes exhibit independence. Secondly, the reliability for substation functions has been represented by the MTTF while the reliability of the communication links is 100%-connectable based on its higher MTTF value of 300 y. Lastly, it is assumed that the MTTR is eight hours based on the availability calculation for individual components. The MTTF values and the availability for various devices within the SAS are calculated and tabulated in Table 6 (Billionton & Allan 1992) (Kanbar & Sidhu 2009) (Andersoon etc.2005).

Table 6. Reliability and availability for Individual devices.

SAS component	MTTF/y	Availability
PIED	150	0.999993911757006
CIED	150	0.999993911757006
MU	150	0.999993911757006
E. Switch	50	0.999981735493416
TS	150	0.999993911757006

2.1.6 Substation Communications Network Bus Topologies and Reliability Availability Calculation Results

In this section, the impact of the various communications network bus topologies and different redundant communications network concepts on the reliability and availability of the BFP function is analysed using the RBD method. Firstly, the reliability (based upon the MTTF data observation) and the availability (based up Equation (2.6) for individual devices) are calculated, as illustrated in Table 6. Secondly, the individual bay typical general protection function, reliability and availability are calculated for simplicity and the purpose of demonstration. Lastly, various communications network bus topologies' reliability and availability are calculated in the rest of this chapter.

2.1.6.1 General Bay Protection Function

Regardless of the substation communications network bus topologies, a typical general bay protection function within an individual bay may comprise an Ethernet switch, PIED, CIED, an MU, BIED and TS, since it is typical for various substation communications network bus topologies. The general bay protection func-tion typically requires measurements from the primary devices, the analysis of these measurements within the protection IED, and taking decisions based upon the pre-assigned protection function parameters.

The trip signal is sent directly to the BIED to trip the circuit breaker. Figure 25 illustrates a typical general protection function and the required IEDs. Therefore, upon successful implementation of the general bay protection function, the signal needs to deliver across the paths TS-MU-PIED-ESW-BIED such that all the contributed IEDs have to operate successfully. This indicates that the IEDs within the system are connected according to the series connection concept, as illustrated by the RBD in Figure 26. The MTTF and the availability results values presented by the RBD of the general bay protection function are as follows,

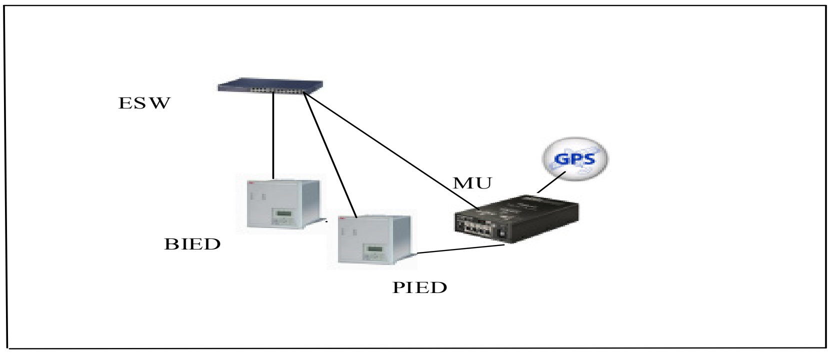


Figure 25. Typical bay protection function.

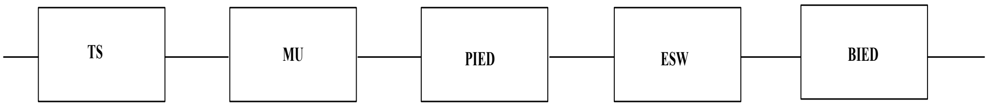


Figure 26. RBD for typical bay protection function.

The calculation of the MTTF and the availability based upon the RBD in Figure 26 of the general bay protection function is:

$$(2.9) MTTF_{System} = \frac{1}{MMTF_{TS}} + \frac{1}{MMTF_{MU}} + \frac{1}{MMTF_{PIED}} + \frac{1}{MMTF_{ESW}} + \frac{1}{MMTF_{BIED}}$$

MTTF =21.428571428 y

From Equation (2.7) the availability of the general bay protection function is,

A= 0.999957383

From the results value of the MTTF, this indicates that the reliability of the general bay protection function has only one-seventh of the MTTF for an individual PIED. Therefore, we can argue that it varies its configuration and any redundancy should be considered and analysed as essential aspect in order to improve overall system reliability and availability.

2.1.6.2 An SAS Cascaded Topology

After analysing the general bay protection function from the reliability and availability perspective, various substation communications network bus topologies should be analysed. Firstly, a cascaded architecture that indicates all six substation bays is connected via a chain upon an open-loop bus topology, as illustrated in Figure 27, whereby all the bays' IEDs based upon the proper implementation of the BFP function need to operate successfully. Therefore, the RBD in Figure 28 illustrates the merging process bus and station bus concept as well as the assumption that the trip signal can be delivered directly to the BIED (worst case condition).

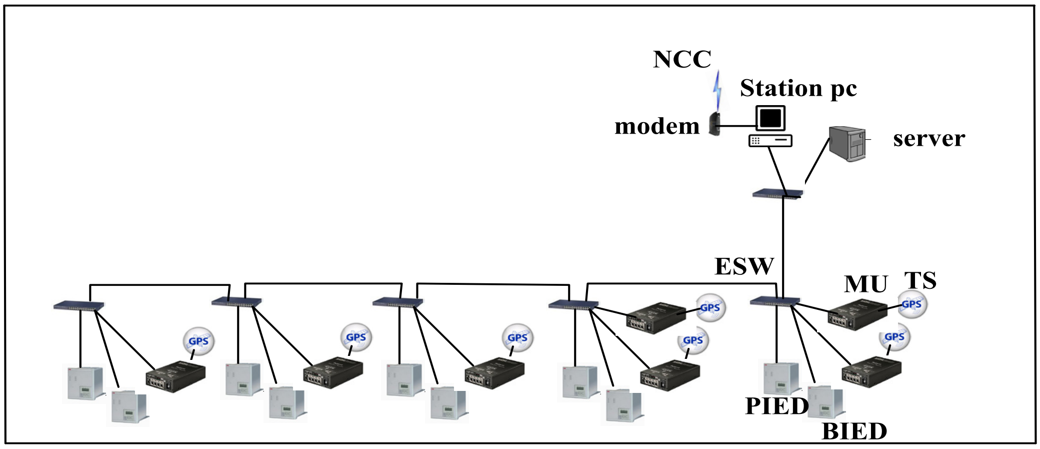


Figure 27. SAS cascaded topology.

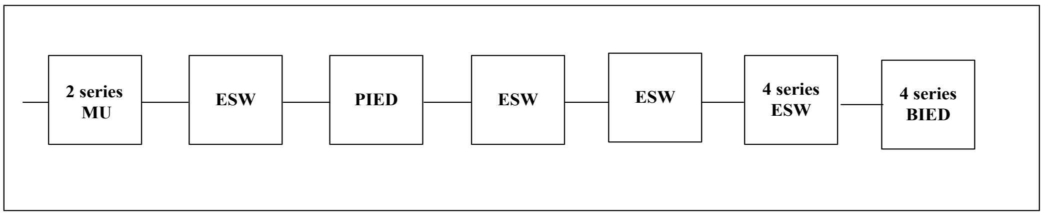


Figure 28. SAS RBD cascaded topology.

The reliability and the availability calculation values for the cascaded SAS topology are as follows:

MTTF= 5.357142895 y

A= 0.999829543

2.1.6.3 An SAS Ring Topology

The ring topology (ring redundancy) is illustrated in Figure 29, such that the Ethernet switches for the SAS's six bays are linked together in a closed-loop. The RBD of the SAS ring topology based upon the rapid spanning tree protocol (RSTP) provides automatic pickup paths in case of any failure in an active link. Therefore, four Ethernet switches out of five are required to execute the BFP function properly, as illustrated in Figure. 30.

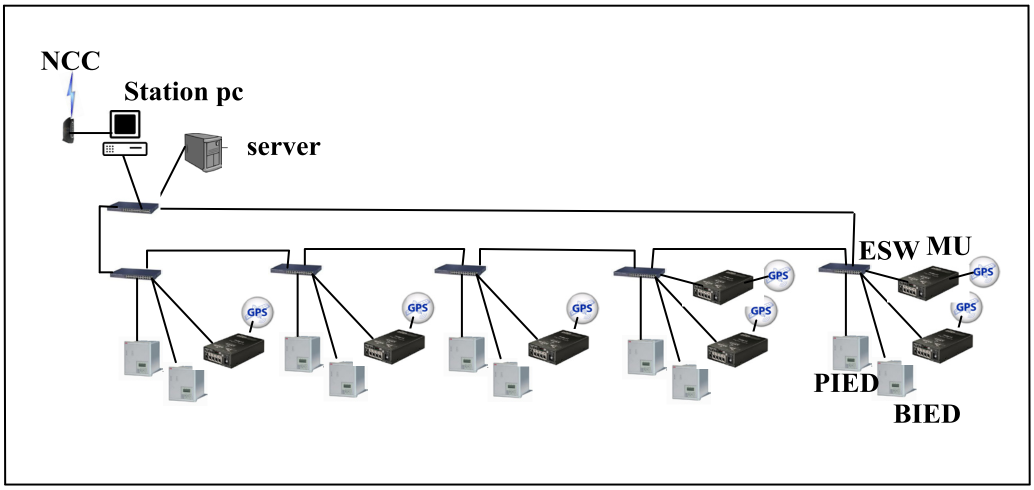


Figure 29. SAS ring topology.

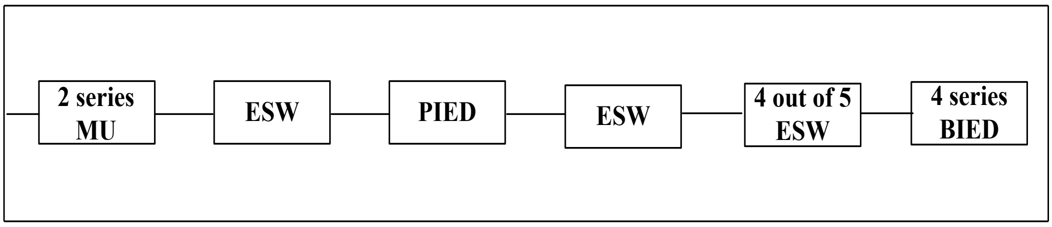


Figure 30. SAS RBD ring topology

The reliability and the availability calculation results values for the SAS ring topology are as follows:

MTTF= 7.627118644 y

A= 0.999920852

2.1.6.4 An SAS Redundant Ring Topology

Mixing SAS topologies - such as a star/ring topology - can introduce two additional, redundant Ethernet switches connected in a star to the six SAS Ethernet switch bays. With this SAS star/ring topology, each SAS bay's IEDs have tow paths, one with the main Ethernet switch and the other with the Ethernet redundant switch; both the main and the redundant Ethernet switches are connected in parallel, as illustrated in Figure 31. In Figure 32, the SAS star/ring topology RBD is illustrated. The RBD specifies the required paths to deliver the trip signal over the SAS topology communications network bus and facilitate the reliability and availability calculation upon the concepts of series and parallel combinations.

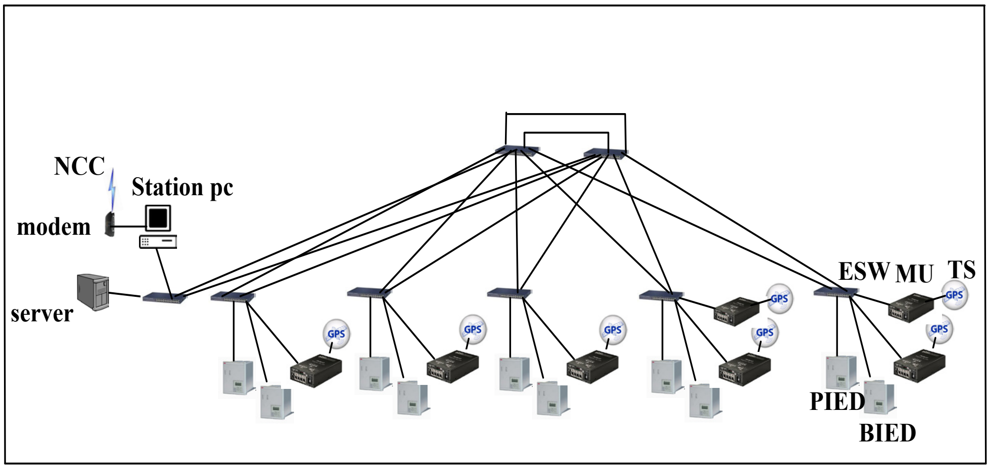


Figure 31. SAS star ring topology.

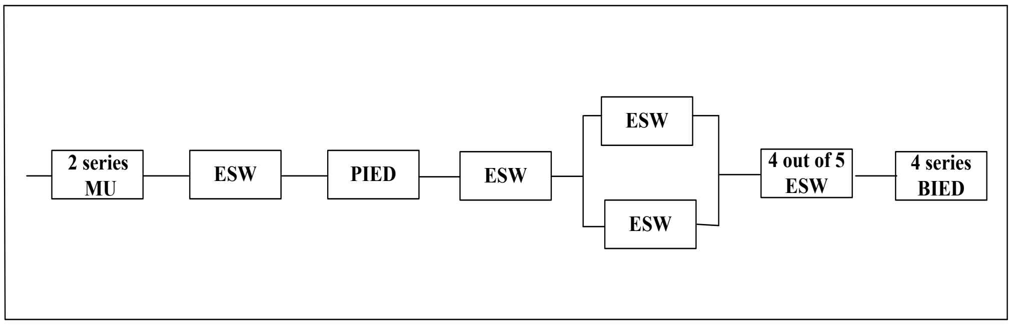


Figure 32. SAS RBD star ring topology.

The reliability and availability calculation results values for the SAS star/ring topology are as follows,

MTTF= 6.923076923 y

A= 0.999920852

According to the MTTF and availability calculation output results values for the SAS BFP within the star/ring topology, it had lower MTTF and availability values compared with the ring architecture. The reasons for this degradation within the MTTF and availability calculation's results values are due to the introduction of two additional Ethernet switches. Although these switches are connected in parallel with each other, they are connected in series with the rest of the system.

2.1.6.5 An SAS Full Redundant Ring Topology

In the case of achieving a higher level of redundancy, each IED within the SAS's six bays should be connected to two redundant Ethernet switch communications network ring topology buses. Theses redundant Ethernet switch communications network ring topology buses are connected with a common HMI, which is often used within the protection function (Brand et al. 2004), as illustrated in Figure 33. Based upon these redundant Ethernet switch communications network ring topol-ogy buses, the six bays' IEDs have tow paths in two separated Ethernet switch communications network ring topology buses. Figure 34 illustrates the RBD of the fully redundant ring topology.

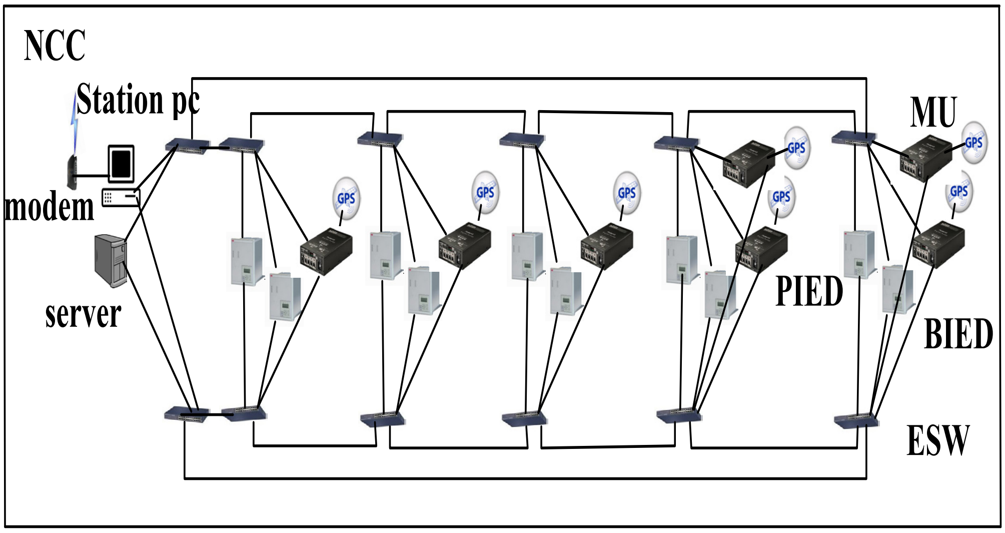


Figure 33. SAS Full redundant ring topology.

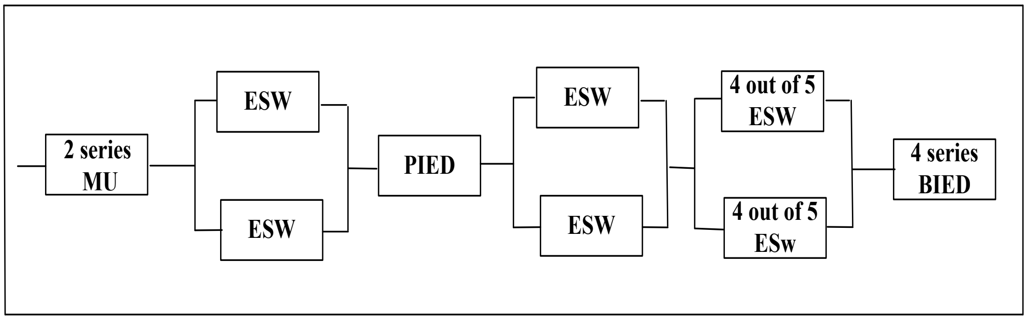


Figure 34. SAS RBD Full redundant ring topology.

The reliability and the availability calculation results values for the fully redundant ring topology are as follows:

MTTF= 9.712230215y

A= 0.999957382

2.1.7 Discussion

Up to this point, the analysis of the reliability and availability of the BFP function in the SAS communications network bus topologies has been carried out using the RBD method. From among the four practical, typical topologies, Table 7 presents a summary of the four analyses' (MTTF, availability) output results values.

Table 7. SAS reliability and availability calculation result values.

SAS bus topologies	MTTF (years)	Availability
Cascaded	5.357142857	0.999829543
Ring	7.627118644	0.999920852
Star/Ring	6.923076923	0.999920852
Fully Redundant-Ring	9.712230215	0.999957382

According to the calculation results values of the MTTF and availability in Table 7, we observe that the BFP function in the SAS cascaded communications network bus topology provides the lowest values (5.357142857, 0.999829543), since the cascaded topology has non-redundant Ethernet switches which constitute the bottleneck of the communications system's reliability. Furthermore, all Ethernet switches within the SAS cascaded communications network bus topology should work properly (series connection) in order to execute the BFP function successfully. The advantages that can be achieved by an SAS cascaded communications network bus topology are a lower cost and a simpler configuration.

For comparison of the ring communications network bus topology calculation output results values (7.627118644, 0.999920852) with the cascaded communications network bus topology, we can observe that there is an improvement in the BFP function's reliability and availability results values. The reason for this is that four-out-of-five Ethernet switches should operate properly in order to execute the BFP function successfully. However, the SAS ring communications network bus topology requires RSTP to give a suitable performance upon the preassigned protection function requirements.

In the case of the SAS star/ring communications network bus topology, there is an improvement in the BFP function's reliability and availability results values (6.923076923, 0.999920852) compared with the cascaded architecture, whereas there is some degradation in the BFP function's reliability and availability results values compared with ring architecture. The reason for this is that we have introduced two additional Ethernet switches that do not affect the performance of the overall communications network bus topology Ethernet switches upon execution of the BFP function. Although these two Ethernet switches are connected in parallel, they are connected in series with the rest of the SAS.

Finally, a fully redundant ring SAS communications network bus topology that provides for higher BFP function reliability and availability results values (9.712230215, 0.999957382) saw increased reliability compared with the cascaded by (4.3551 y) and the availability by (1.278384253e-004). From the above analysis of the BFP function's reliability and availability calculation output results values, it is indicated and clearly proven that introducing redundancy within the Ethernet network has a greater impact on improving an SAS's reliability and availability. However, and on the other hand, it also increases the SAS's complexity and cost. Therefore, we argue that varied SAS communications network bus topologies should be analysed in various circumstances, and that the trade-off between simplicity, lower costs and lower reliability and availability SAS values as against complexity, higher costs and higher reliability and availability SAS values should be made, so that the overall SAS reliability and availability values and the cost of the SAS are not compromised.

2.1.8 Conclusion

Analysis of the SAS communications network bus topologies attempts to explore some fundamental analyses in an SAS's design. These analyses were carried out using the BFP function by investigating several practical SAS bus topologies from a reliability and an availability point of view. The overall system reliability and availability are based upon combinations of use-cases within SAS communications network bus topology design. Reliability and availability have been identified and calculated for various SAS topologies. Comparisons among these SAS topologies were made based on the reliability and availability calculation output results values. Redundancy has been identified as a key feature to increase the reliability and availability of the SAS upon addressing the feasibility, performance and implementation of the BFP function in various SAS communications network bus topologies.

2.2 Reliability and Probability of Failure Simple Algorithm RaFSA Estimation Method

In the second part of Chapter 2, for reliability and probability of failure, a simple algorithm (the RaFSA estimation method) was invented. This task was based upon the estimation of the reliability and probability of failure extant in individual

IEDs, the typical general bay protection function and the BFP function further based upon several SAS communications network bus topologies. The RaFSA estimations are implemented over a practical, small transmission substation, T1-1. Various practical SAS topologies are considered. The RaFSA estimations are im-plemented with a stochastic simulation approach.

2.2.1 Introduction

The traditional way to evaluate the reliability or probability of failure for a system is by using one of two basic approaches: direct analytical techniques and stochastic simulations. In the previous sections, we were concerned with the analytical approach, which instantiates the system based on a mathematical model that sim-plified it. According to this system simplification, the direct implementation of the mathematical solutions over the mathematical model needs to be made based upon the calculation of the reliability, probability of failure and availability. On the other hand, the simulation approach is a highly valuable method. This method is widely used to simulate the actual behaviour of real-time systems by simulating both the actual process and the system's random behaviour. Therefore, simulation techniques provide solutions for the simulated system as a sequence of real testing events sorted by the simulation time. Both approaches have advantages and dis-advantages. The analytical technique has a relatively short solution time and al-ways gives the same numerical results for the same model and the same input data, whereas the simulation technique has the ability to handle huge amounts of input data with different kinds of probability distribution models, and not only the exponential ones. In addition, a simulation solution has the ability to include other analysis tools and parameters, such as the repairing time, the load flow, reconfiguration, optimization, etc., while changing the input data or expansion is easily implemented without modification during the simulation process. From the above-mentioned points, we can see that each approach has its own merits and demerits. Moreover, neither approach can be considered better than the other. In selecting any solution from the announced approaches, it must be based upon the system, its characteristic and on meeting the depth and detail of the analysis requirements. A mixed solution of the two approaches can be implemented in different circumstances and in particular cases (Billinton & Allan 1992). It is important to note that, in the rest of this chapter, the evaluation of the reliability and probability of failure for a small transmission substation protection function (BFP) (rather than the availability and downtime of the system) are carried out.

The mathematical representation of the observation data can be implemented by one of the specific statistical probability distribution functions. The system's reliability can be determined by taking the integral of it, which represents the area below the curve of the probability density function (Kezunovic & Popovic 2005). Table 8 shows the analytical calculation output results values for the reliability and probability of failure considered for each individual SAS IEDs.

Table 8. Reliability and probability of failure for each individual SAS IEDs.

SAS	MTTF/y	Failure rate f/y	Reliability	Probability of failure
PIED	150	0.006666666	0.935506985	0.064493014
CIED	150	0.006666666	0.935506985	0.064493014
MU	150	0.006666666	0.935506985	0.064493014
E-switch	50	0.020000000	0.818730753	0.181269246
TS	150	0.006666666	0.935506985	0.064493014

From Table 8, it might be considered that the analytical calculation output results values indicate an identical reliability and probability of failure for identical IEDs, which represent a weak point of the analytical solution method. This is because in real-time operations each IED within the SAS (even if they are identical) may experience different reliability and probability of failure profiles.

Therefore, the estimation of the reliability and probability of failure was carried out upon inventing a novel RaFSA estimation method. The analysis and discussion of the estimation of the system's reliability and the probability of failure using the RaFSA estimation method takes place for one protection IED, a general bay protection function and the BFP function in various SAS communications network bus topologies. The novel RaFSA estimation method is implemented over a practical, small transmission substation, T1-1. The RaFSA estimation method is implemented with a stochastic simulation approach.

2.2.2 The RaFSA Estimation Method

In general, the novel RaFSA estimation method has been developed under the assumption that the failure rate distribution function is based on an exponential distribution (useful life) in Region II of the bath-tub curve in Figure 24. The most unconvincing fact derived from the analytical calculations of the reliability and probability of failure is the calculation of the output results values - for instance, the reliability and probability of failure for n identical IEDs in the same environment are identical. However, the behaviour patterns for n identical IEDs in the real world will all be different. These differences can exist in varying functionalities, including the survival time, the number of failures, the time between failures, the restoration time, etc. Therefore, the strongest aspect of the novel RaFSA has been considered, since it intended to examine and predict the actual behaviour pattern for each IED in the system. These examination and prediction features are provided based on nature, although the process that is involved in the RaFSA is random.

2.2.2.1 RaFSA Individual IED

To better understand the novel RaFSA estimation method, individual IED is considered firstly. According to the RaFSA process's steps, we generate a set of uniform pseudo-random numbers based on a deterministic algorithm. The generated numbers are distributed randomly over the interval (0, 1), as follows:

(2.10) $$X_{i+1} = (A * X_i + C)(mod\ B)$$

where A is the multiplier, B is the modulus and C is the increment, and where all are non-negative integers. After generating the sequence of pseudo-random numbers, a uniform random number can be found by dividing the generated numbers over the modulus as follows:

(2.11) $$U_i = \frac{X_i}{B}$$

The uniform input data can be converted into another distribution by using one of the converting methods. The main procedures that are used for conversion are the inverse transform method, the composition method and the acceptance rejection method. Within the novel RaFSA process, the inverse transform method was used - it is the most efficient converting method. However, the inverse transform method can be used only if the distribution can be inverted analytically. This method is suitable for the exponential distribution that we assumed for the failure rate distribution function for the proposed IED model. Therefore, the converted operation time for the IED is based on the inverse transform method, and can be achieved from the formula as follows (Billinton & Allan 1992),

(2.12) $$T_i = \frac{1}{\lambda_i}\ln(U_i)$$

where T is the operation time (TTF) based on an exponential distribution and λ is the failure rate. The classical modelling of the system's IEDs is based on two states of probability models, namely "operate" and "failed". Transitions between states are defined based on the probability distributions over the TTF and TTR. After developing the operation time, as the next step, we need to examine whether the SAS's IEDs are in the operative state or else whether they enter into the failure state. This task can be performed by comparing the operation time with the assumed mission time. In order to specify the success events, we need to consider the operating time in which the IED remains in its up (or operating) state before it fails. Next, if the operating time is greater than or equal to the mission time, we mark these events as successes (reliable). If the operating time is less than the mission time, we sign these events as failures. In order to estimate the values of the reliability and probability of failure for an individual IED or SAS (considering the internal connection between the SAS's IEDs), success and failure events should be defined and counted. Figure 35 illustrates the flowchart of the novel RaFSA estimation process,

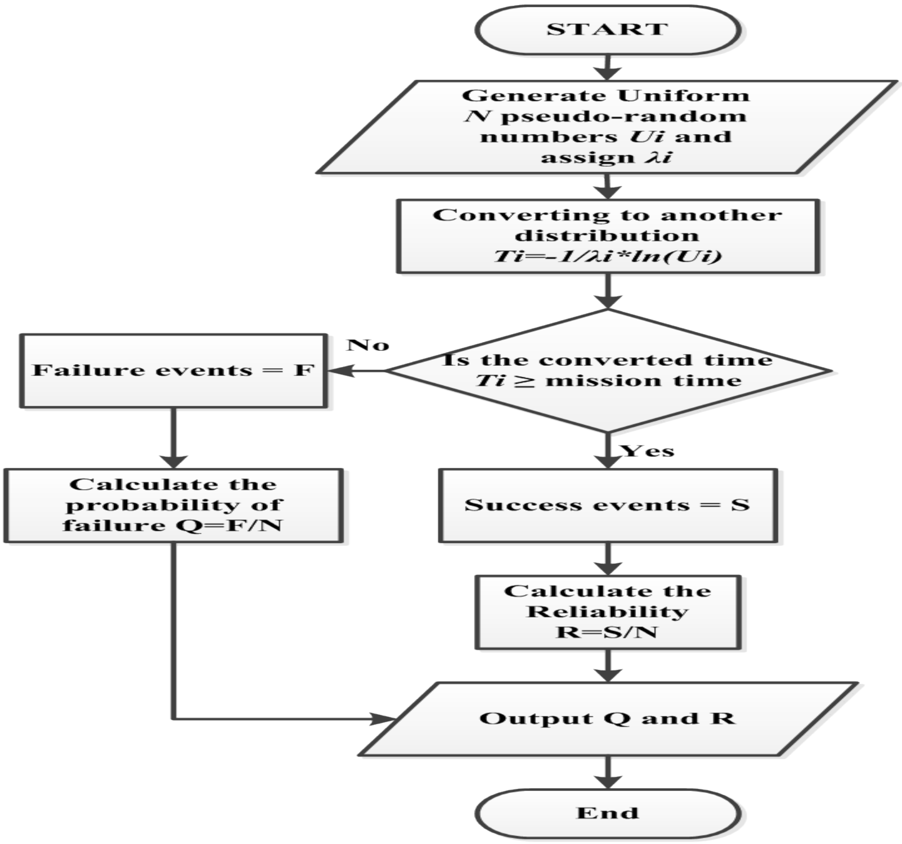

START
Generate Uniform N pseudo-random numbers Ui and assign λi
Converting to another distribution Ti=-1/λi*ln(Ui)
Is the converted time Ti ≥ mission time
No
Failure events = F
Yes
Success events = S
Calculate the probability of failure Q=F/N
Calculate the Reliability R=S/N
Output Q and R
End

Figure 35. RaFSA flow chart estimation process for an individual IED.

The estimated output results values can be processed in many ways, including plots. A plot is one of the most significant representation methods and is one of the merits of Mont Carlo simulation (MCS). Therefore, in order to give a clear pictorial representation of the way in which the reliability or probability of failure can vary, we plot the estimated results values to give a clear pictorial representation of the ways in which the reliability or probability of failure can vary.

Firstly, the reliability of the individual IED is estimated based upon the novel RaFSA estimation method. The estimation reliability results values for the analyt-ical and novel RaFSA are plotted in the MATLAB environment. From Table 8, the analytical results given by Equation (2.4) for the reliability of the single IED are (R(t) = 0.935506985) (true value). Figures 36-40 illustrate both the true value and the reliability estimation output results values based upon the RaFSA estimation method for t = 1 year for 100, 1,000 and 10,000 trials for an individual IED.

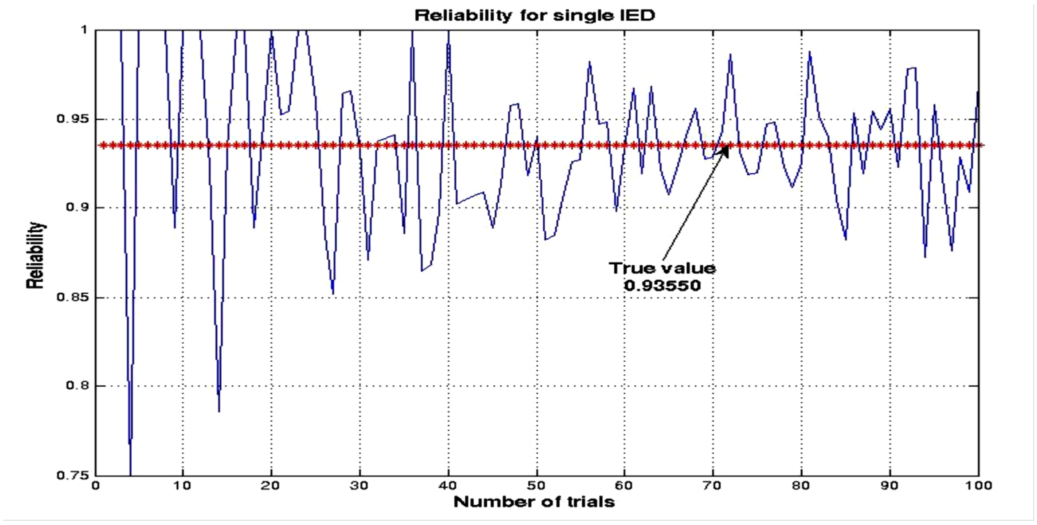


Figure 36. Reliability for individual IED within 100 trials.

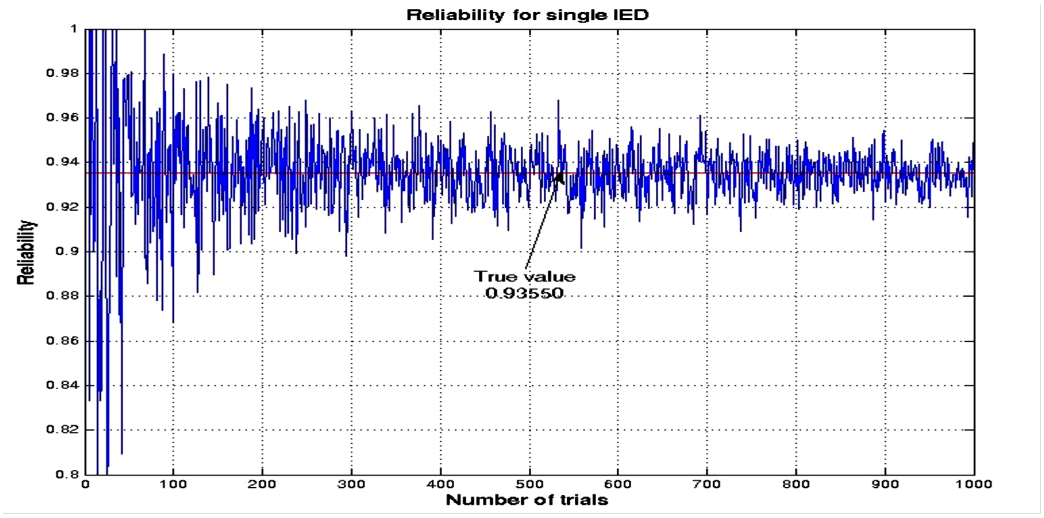


Figure 37. Reliability for individual IED within 1000 trials**.**

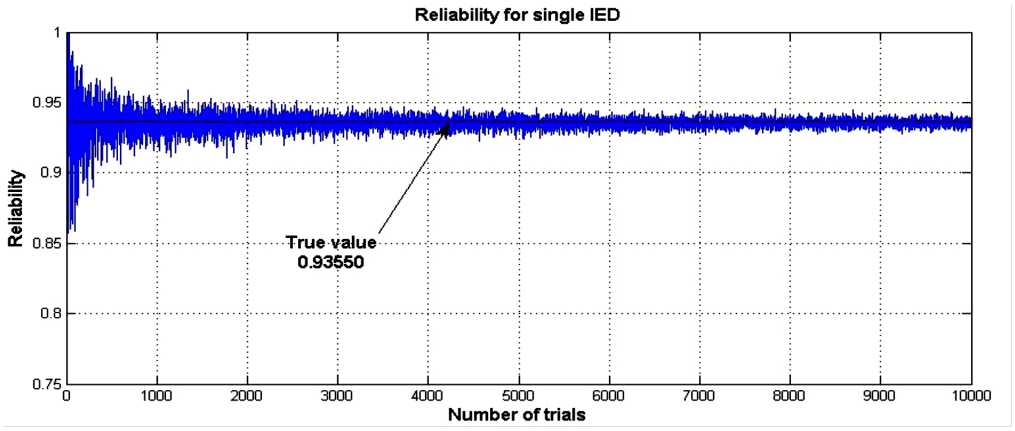


Figure 38. Reliability for individual IED within 10000 trials.

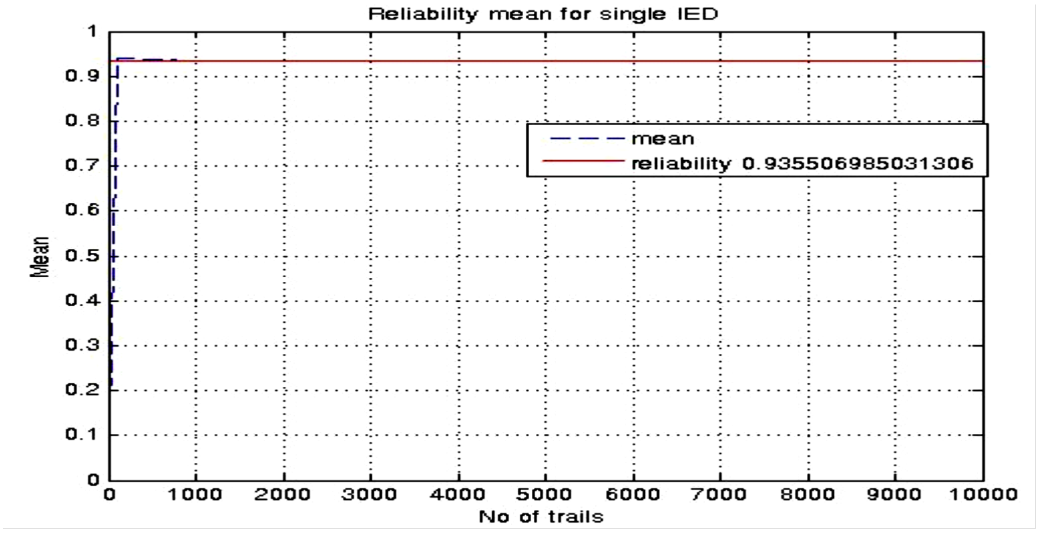


Figure 39. Reliability and the mean for single IED.

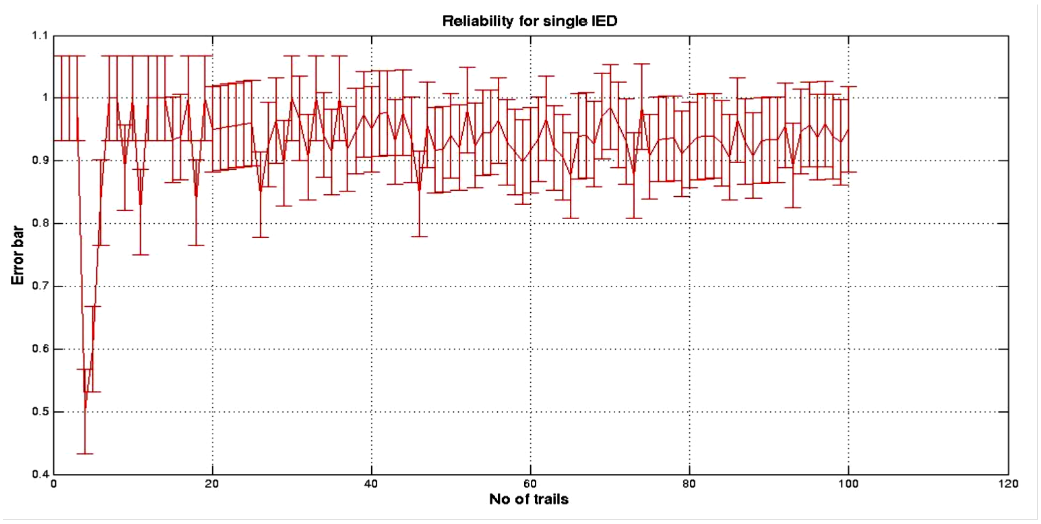


Figure 40. Reliability error bar for single IED.

Several observations can be made from Figures 36-40. Firstly, based on the analytical results, the true value of the reliability is (R(t) = R = 0.935506985), which occurs in the trials (15, 30, 32 and 60) within the RaFSA estimation results values. However, this would not be known for a real system, as illustrated in Figure 36, at 100 trials. Secondly, from Figure 36, the RAFSA estimation output results values are randomly variate about the true value when the number of trials is small (±0.0350) at 100 trials. Thirdly, the number of instances whereby the values of the reliability are greater than the true value is approximately equal to the number of instances where the reliability values are less than the true value. The mean of the reliability values is (0.940196437) and the standard deviation is (0.054404264). Lastly, as the number of trials was increased, the variations in the RaFSA estimation reliability results values is reduced. However, the values of the reliability remain variable even at trial 10,000, although the variation is reduced significantly and has a tendency towards the true value. The mean is (0.935524025) and the standard deviation is (0.007278546), as illustrated in Figure 38.

2.2.2.2 The RaFSA General Bay Protection Function

In this subsection, the typical general bay protection function in the SAS is considered. According to the IEC 61850 standard, an SAS's functions are distributed over different IEDs based on specific real-time restrictions. The typical general bay protection function may consist of a single Ethernet switch, PIED, an MU, BIED and TS, as illustrated in Figure 25. Regardless of the SAS topology, the general bay protection function is identical and needs the same set of IEDs for various SAS topologies. Therefore, the general bay protection function always needs IEDs that are interlocked in a path, such as (TS-MU-PIED-ESW-BIED), upon the successful implementation of the protection function. Moreover, all the interlocked-path IEDs must work successfully. Within these interlocking paths and with successful IED working conditions, the underlying SAS communications network bus for all these IEDs is considered as a series connection.

Reliability and probability of failure for an SAS series connection are,

(2.13) $$R_s(t) = R_1(t) * R_2(t)$$

(2.14) $$Q_s(t) = Q_1(t) + Q_2(t) - Q_1(t) * Q_2(t)$$

while the reliability and probability of failure for an SAS parallel connection are,

(2.15) $$R_P(t) = R_1(t) + R_2(t) - R_1(t) * R_2(t)$$

(2.16) $$Q_p(t) = Q_1(t) * Q_2(t)$$

where R is the reliability and Q is the probability of failure. The same procedure within the RaFSA can be followed as in the case of the above individual IED. However, in this case, two failure rates (λ1, λ2) need to be assigned and another check condition (the same type as for the SAS communications network bus IEDs' connection) needs to be considered. By counting the success and failure events, we are able to estimate the value of the reliability and the probability of failure, as explained in Figure 41 which shows the flowchart of the RaFSA estimation process for a typical general bay protection function. More details about the analytical calculation made be found in (Mekkanen etc. 2012).

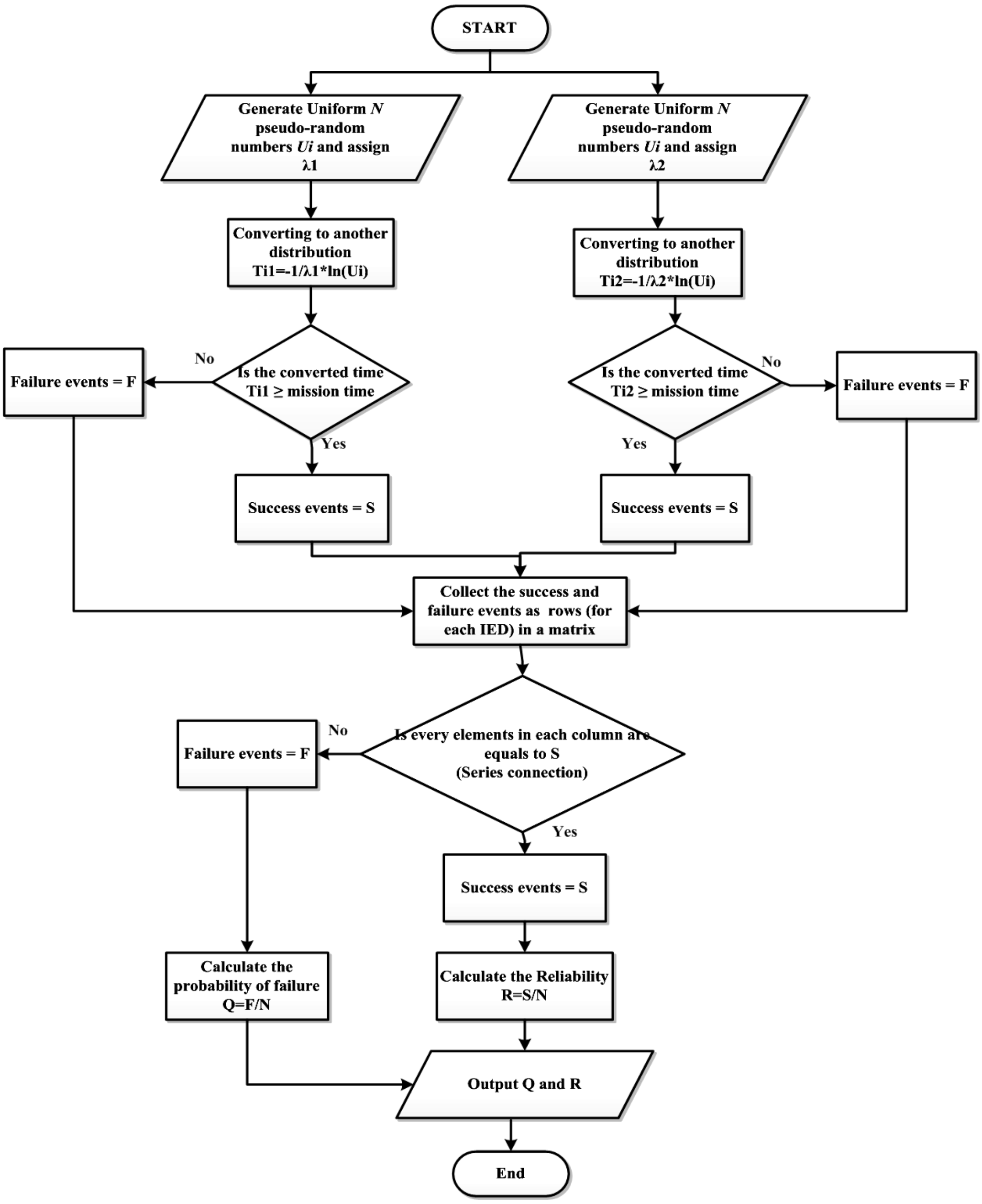

START
Generate Uniform N pseudo-random numbers Ui and assign λ1
Generate Uniform N pseudo-random numbers Ui and assign λ2
Converting to another distribution Ti1=-1/λ1*ln(Ui)
Converting to another distribution Ti2=-1/λ2*ln(Ui)
Is the converted time Ti1 ≥ mission time
Is the converted time Ti2 ≥ mission time
No
No
Yes
Yes
Failure events = F
Failure events = F
Success events = S
Success events = S
Collect the success and failure events as rows (for each IED) in a matrix
Is every elements in each column are equals to S (Series connection)
No
Yes
Failure events = F
Success events = S
Calculate the probability of failure Q=F/N
Calculate the Reliability R=S/N
Output Q and R
End

Figure 41. RaFSA flowchart for an SAS's typical general protection function.

From Equation (2.13), the analytical output results value for the reliability of the typical general bay protection function based on t = 1 year is (R(t) = 0.954405479), where the novel RaFSA estimation results values for the estimation of the reliability for a typical general protection function after 100, 1,000 and 10,000 trials is illustrated in Figures. 42- 46.

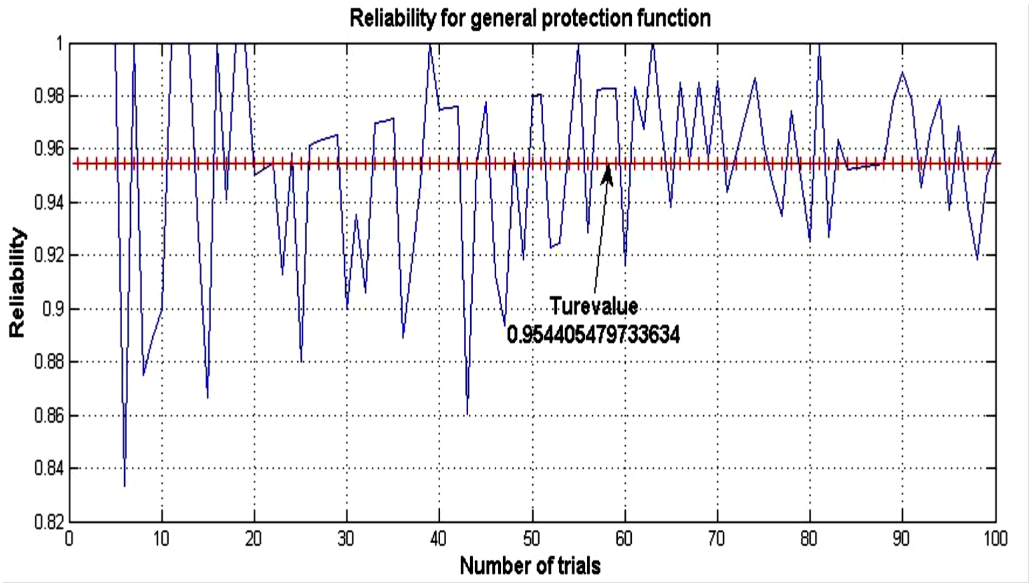


Figure 42. Reliability for general bay protection function within 100 trials.

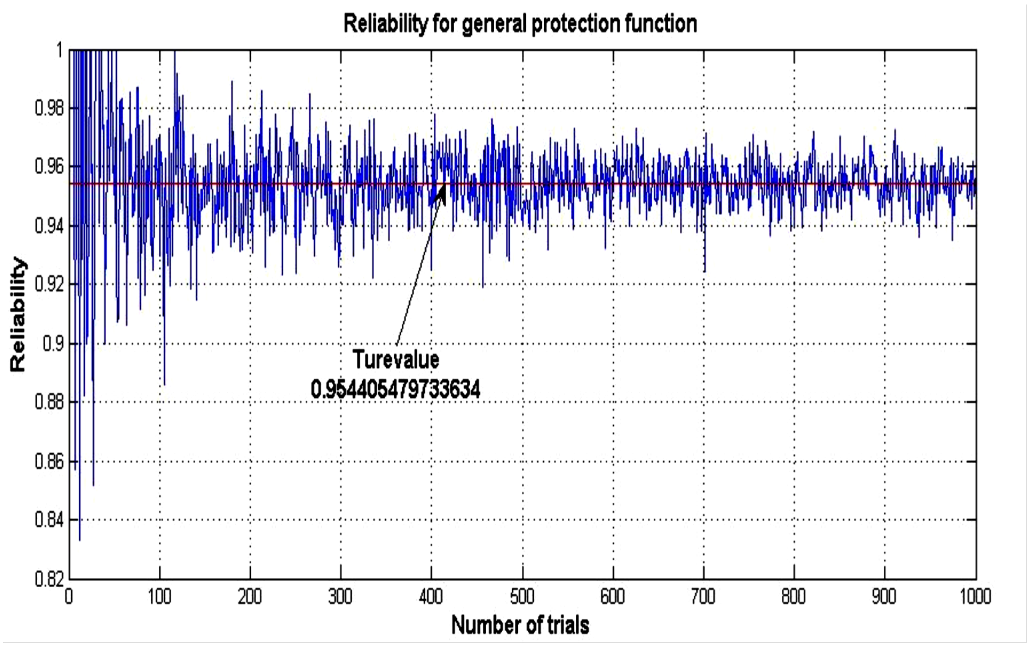


Figure 43. Reliability for general bay protection function within 1000 trials.

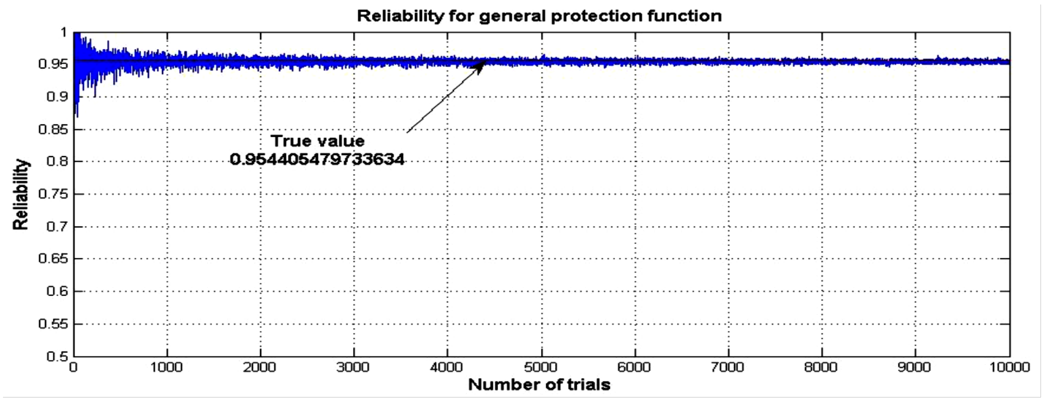


Figure 44. Reliability for general bay protection function within 10000 trials.

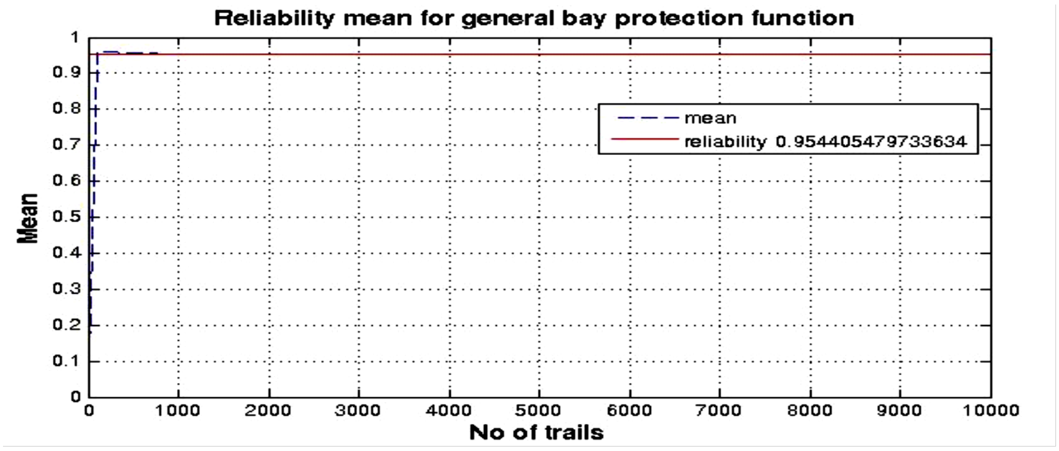


Figure 45. Reliability and the mean for general bay protection function.

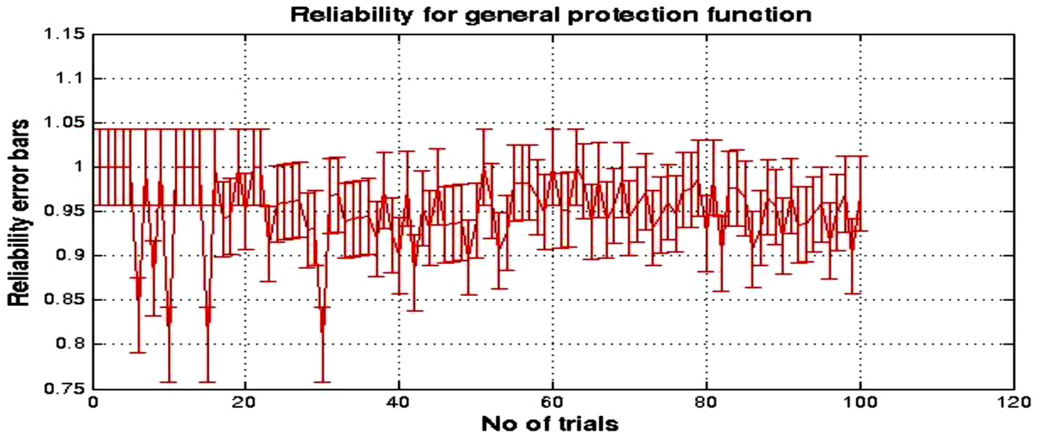


Figure 46. Reliability error bar for general bay protection function.

The observation that we discussed above can also be made for the reliability estimation for the typical general bay protection function. From the reliability analyt-ical results value, the true value of the reliability is (R(t) = 0.954405479). From Figure 42, the RaFSA reliability estimation results values are randomly variate about the true value when the number of trials is small (±0.00559) at trial 100. In addition, and infrequently, the true value occurs in some trials (22, 44, 67, 87 and 88) and the number of instances where the value of the reliability is greater than the true value is approximately equal to the number of instances where the reliability values are less than the true value.

The mean of the reliability values is (0.959896583) and the standard deviation is (0.032408827). Lastly, as the number of trials is increased, the variations in the RaFSA reliability estimation results values are reduced. However, the values of the reliability remain variant, even at trial 10,000, although the variation is reduced significantly and has a tendency towards the true value. The mean is (0.954452063) and the standard deviation is (0.006022050), as illustrated in Figure 44.

2.2.2.3 An RaFSA Cascaded Communication Network Topology

Within this subsection, we consider the reliability RaFSA estimation for the BFP function in the SAS communications network cascaded topology for the small transmission substation T1-1. The BFP function, upon successful implementation in a typical SAS cascaded topology, requires that all six bays be connected via a chain upon an open-loop SAS bus topology, as illustrated in Figure 27. Therefore, based upon the SAS cascaded topology, it may require that all the path IEDs (such as Ethernet, switches, TS, MUs, related PIEDs and BIEDs) work successfully (a series connection).

The same procedure can be followed as in the cases above. However, in the cascaded SAS topology with various failure rates of IEDs numbering more than two, the RaFSA estimation method needs to assign various (λj) failure rates for each participant SAS IED. Further, the SAS communications network topology needs to be considered within the RaFSA implementation process. By counting the success and failure events, we are able to estimate the values of the reliability and the probability of failure as explained in Figure 47, which shows the flowchart of the novel RaFSA estimation process for a cascaded SAS topology,

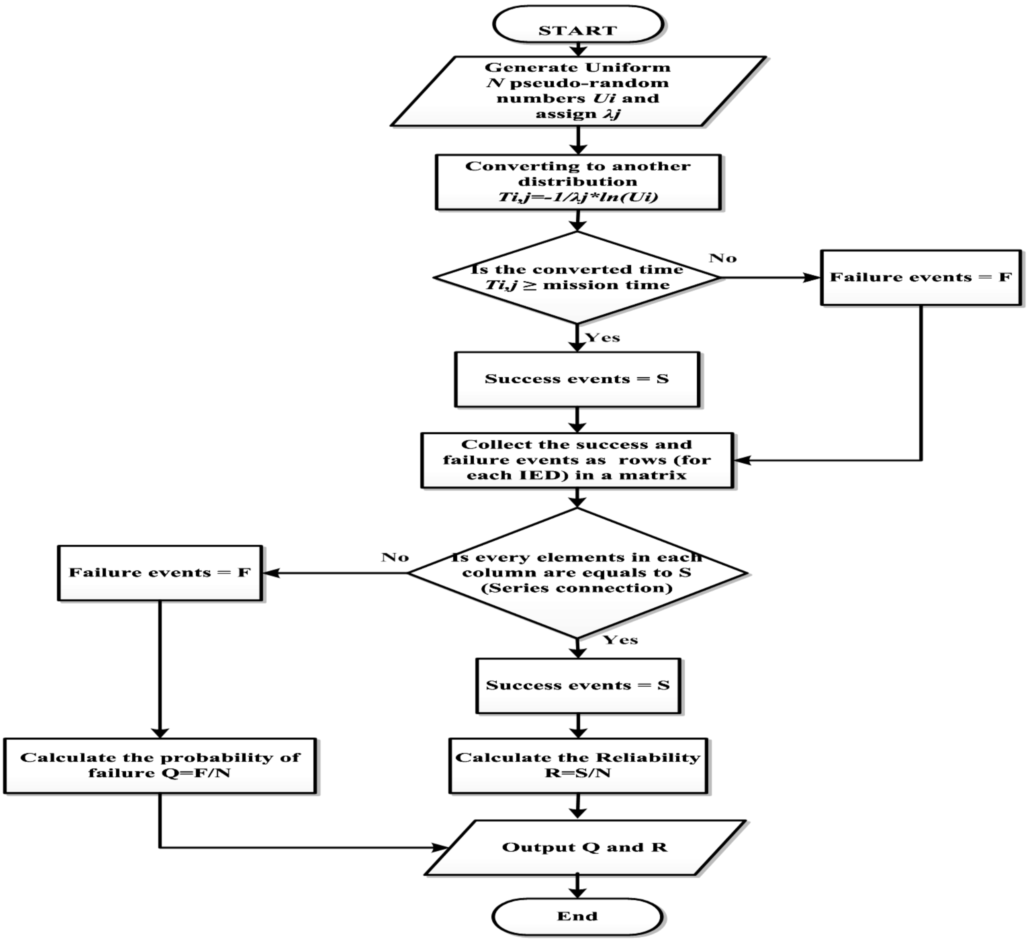


Figure 47. RaFSA Flow chart estimation process for SAS cascaded topology.

The analytical result based on t = 1 year is (R(t) = 0.829720263), while the novel RaFSA reliability estimation results values for 100, 1,000 and 10,000 trials are illustrated in Figs. 48-52,

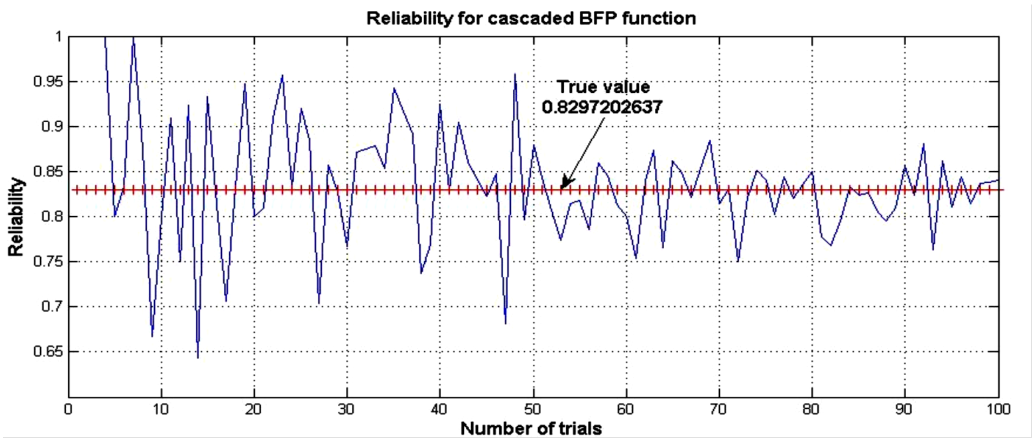


Figure 48. Reliability for BFP SAS cascaded topology within 100 trials.

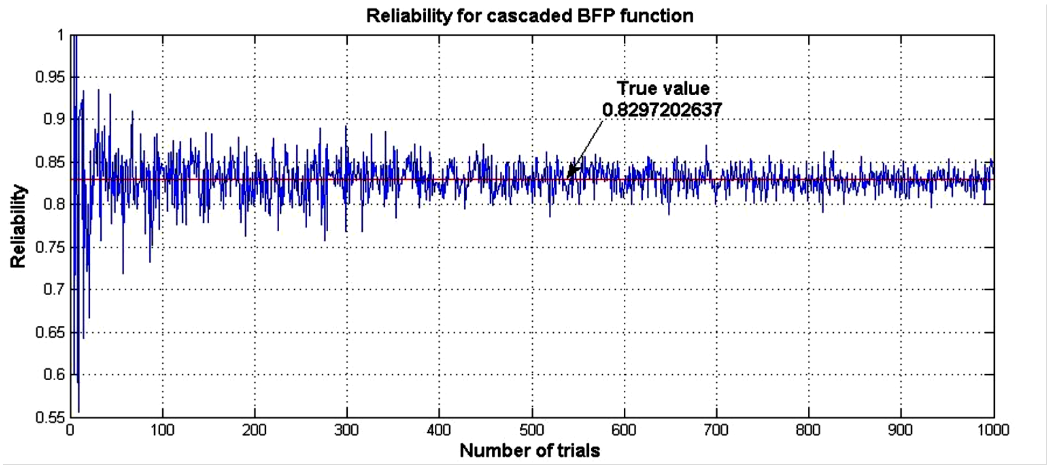


Figure 49. Reliability for BFP SAS cascaded topology within 1000 trials.

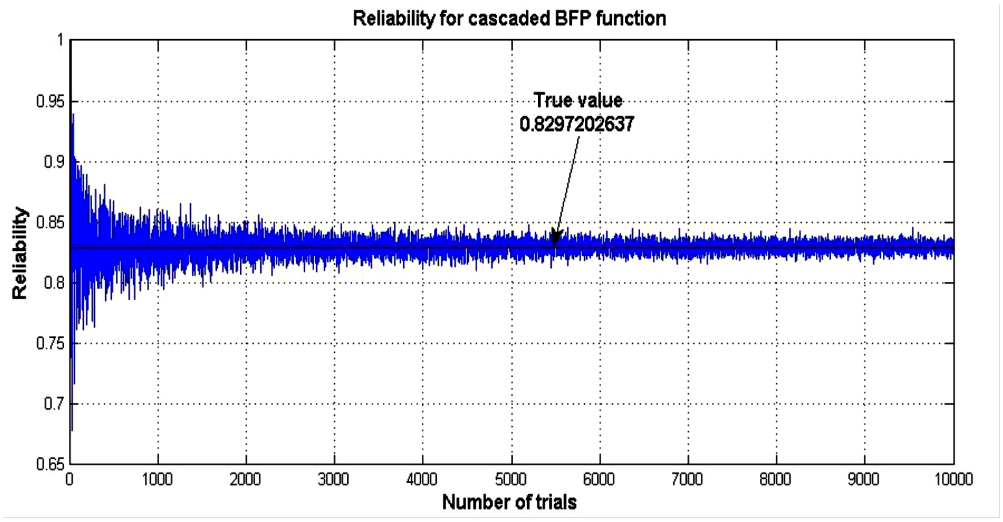


Figure 50. Reliability for BFP SAS cascaded topology within 10000 trials.

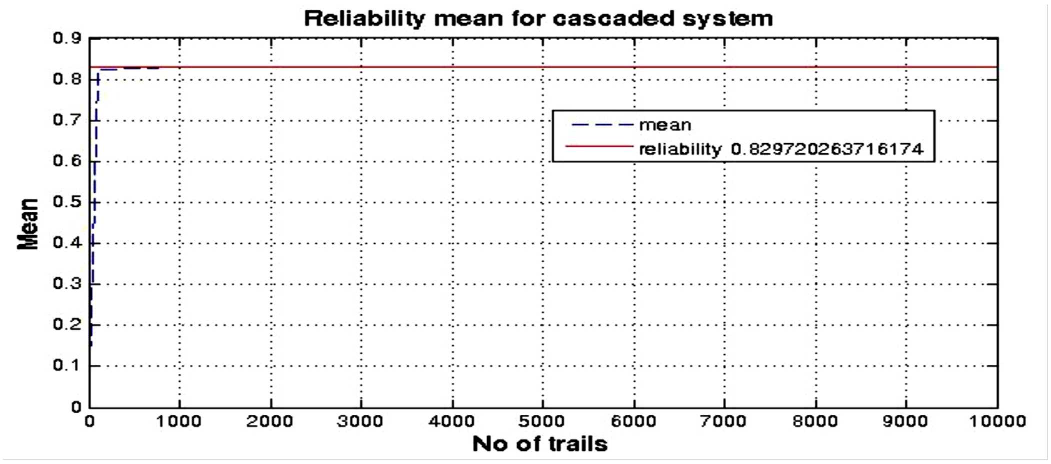


Figure 51. Reliability mean for BFP function for the cascaded SAS topology.

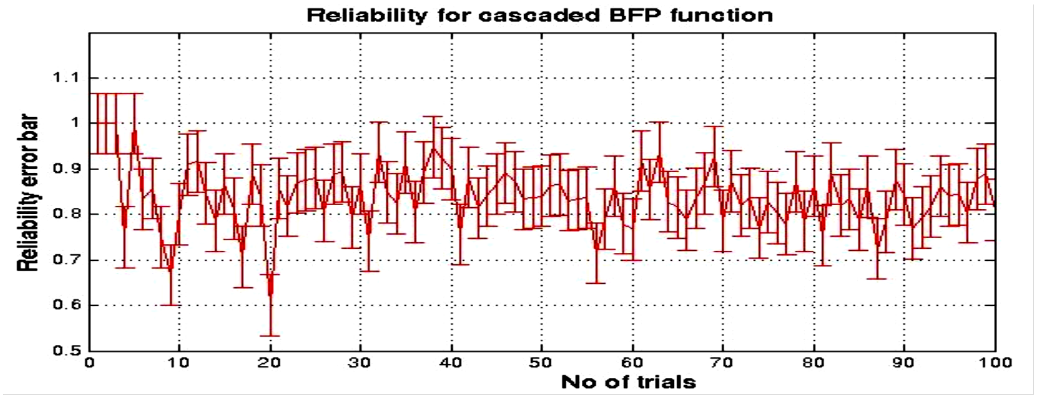


Figure 52. Reliability error bars for BFP function SAS cascaded topology.

We can observe from Figure 48 that the RaFSA reliability estimation results values of the BFP function for the cascaded SAS topology are randomly variate about the true value (R(t) = 0.829720263) when the number of trials is small (± 0.0102) at trial 100. In addition, and infrequently, the true value occurs in trials (6, 18, 24, 27, 29, 41 and 71), and the number of instances where the values of the reliability are greater than the true value is approximately equal to the number of instances where the reliability values are less than the true value, whereby the mean of the reliability values is (0.823838307) and the standard deviation is (0.082451292). Moreover, as the number of trials increases, the variation in the reliability values is reduced. However, the values for reliability remain variable, even at trial 10,000, but the variation is reduced significantly and has a tendency towards the true value. The mean is (0.829789372) and the standard deviation is (0.011974237), as illustrated in Figure 50.

2.2.2.4 An RaFSA Redundant Ring Communication Network Topology

Lastly, the novel RaFSA estimation process for the BFP function of the redundant SAS ring topology is carried out. In order to achieve a higher level of redundancy, each IED is linked within the SAS with two redundant communications network ring topologies. Based upon this SAS communications network topology, all the IEDs have tow paths within two separated ring networks, as illustrated in Figure 33. The same procedure can be followed as in the cases above. However, in the redundant ring system with different failure rats for the IEDs, the novel RaFSA needs to assign different (λj) failure rates for each SAS participant IED. The IEDs' connections within each communications network subsystem need to be considered, since we have mixed series and parallel IED connections. For instance, for parallel IEDs, a failure in one IED leads to other IED operating over the failed one. Moreover, for any other intermediate situation, four-out-of-five IED subsystems can be modelled as three IEDs in series with two IEDs in parallel (Billinton

& Allan 1992). By counting the success and failure events, we are able to estimate the value of the reliability and the probability of failure, as illustrated in Figure 53, which presents the flowchart of the novel RaFSA estimation process for a redundant ring SAS topology,

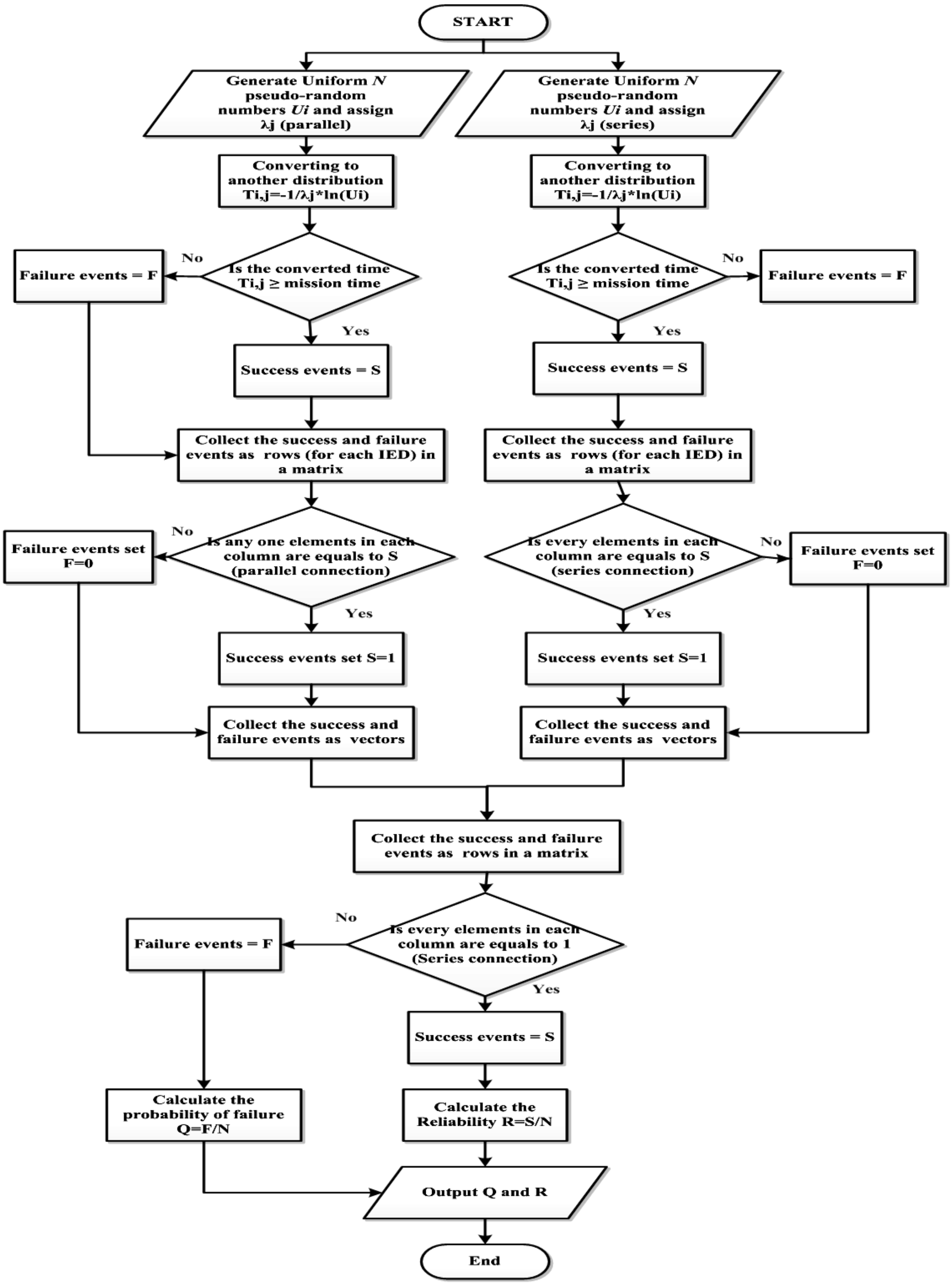

START
Generate Uniform N pseudo-random numbers Ui and assign λj (parallel)
Generate Uniform N pseudo-random numbers Ui and assign λj (series)
Converting to another distribution Ti,j=-1/λj*ln(Ui)
Converting to another distribution Ti,j=-1/λj*ln(Ui)
Is the converted time Ti,j ≥ mission time
No
Failure events = F
Yes
Success events = S
Is the converted time Ti,j ≥ mission time
No
Failure events = F
Yes
Success events = S
Collect the success and failure events as rows (for each IED) in a matrix
Collect the success and failure events as rows (for each IED) in a matrix
Is any one elements in each column are equals to S (parallel connection)
No
Failure events set F=0
Yes
Success events set S=1
Is every elements in each column are equals to S (series connection)
No
Failure events set F=0
Yes
Success events set S=1
Collect the success and failure events as vectors
Collect the success and failure events as vectors
Collect the success and failure events as rows in a matrix
Is every elements in each column are equals to 1 (Series connection)
No
Failure events = F
Yes
Success events = S
Calculate the probability of failure Q=F/N
Calculate the Reliability R=S/N
Output Q and R
End

Figure 53. RaFSA flowchart for an SAS redundant ring topology.

The redundant ring architecture has (R(t) = 0.902160386) as a true value based on t = 1 year using the reliability analytical solution, whereas the novel RaFSA esti-mation reliability results values based upon the SAS redundant ring topology are illustrated in Figures 54-58 for 100, 1,000 and 10000 trials.

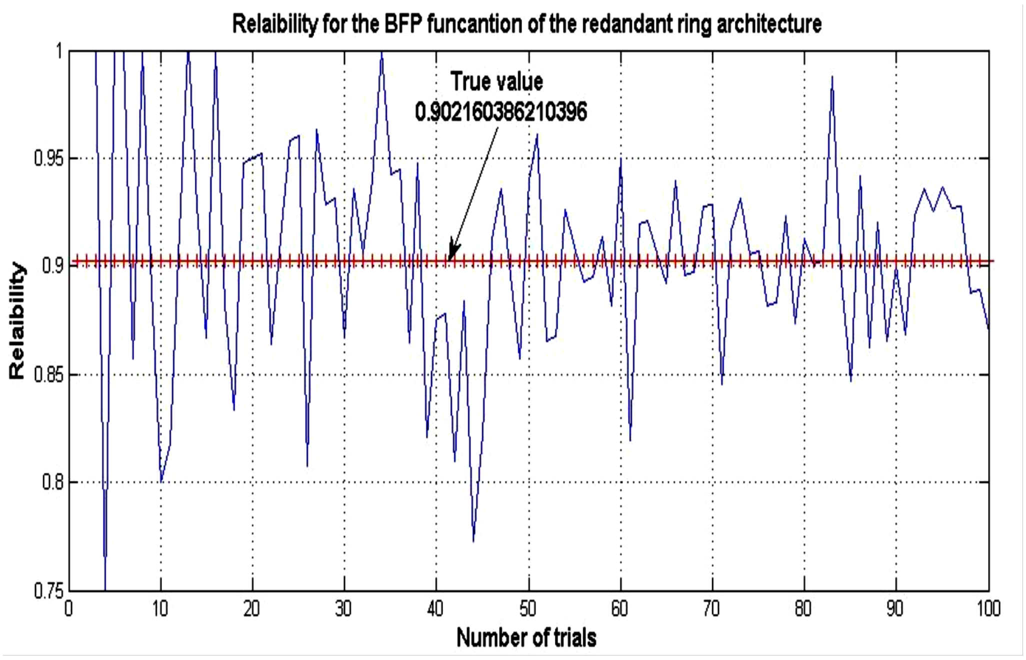


Figure 54. Reliability for BFP SAS redundant ring topology within 100 trials.

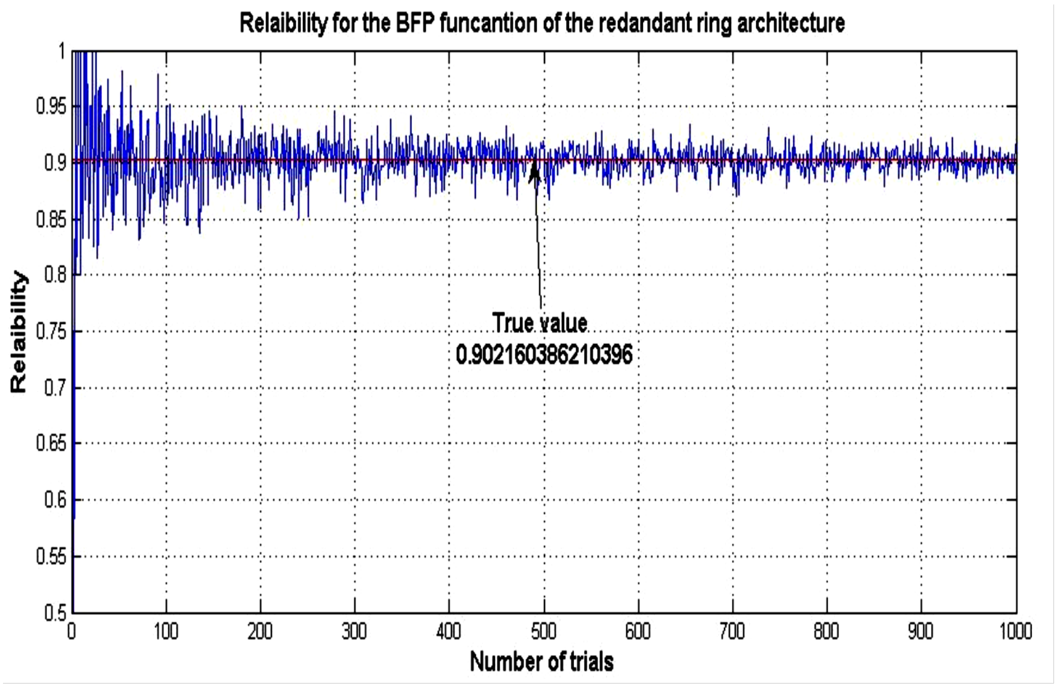


Figure 55. Reliability for BFP SAS redundant ring topology within 1000 trials.

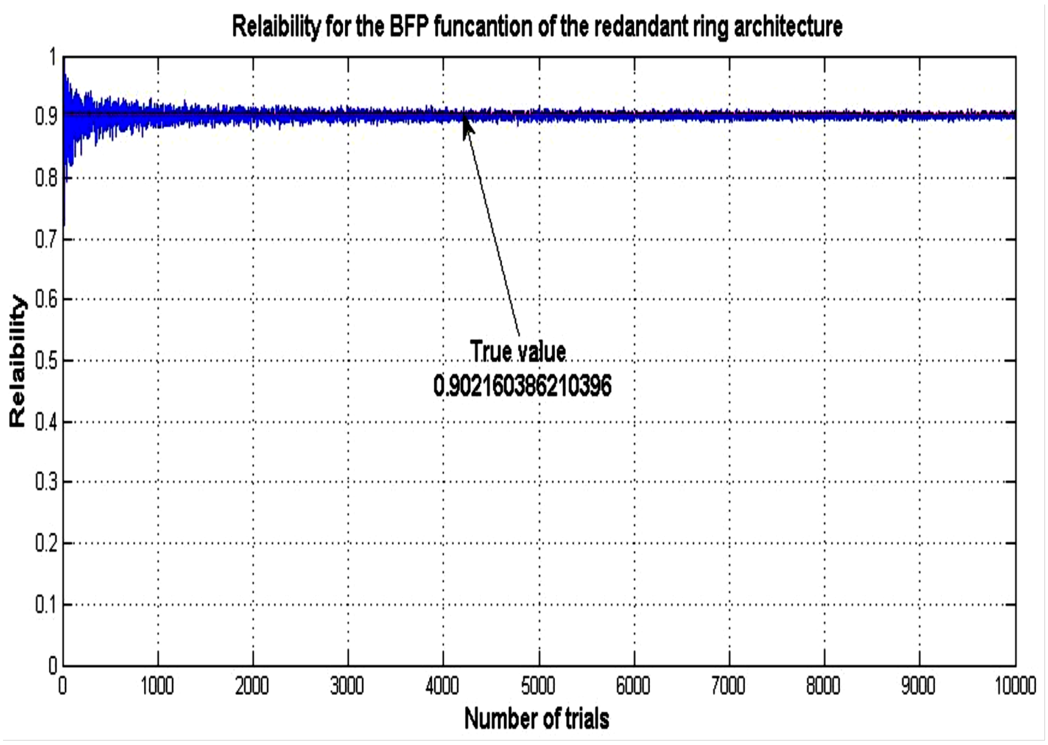


Figure 56. Reliability for BFP SAS redundant ring topology within 10000 trials.

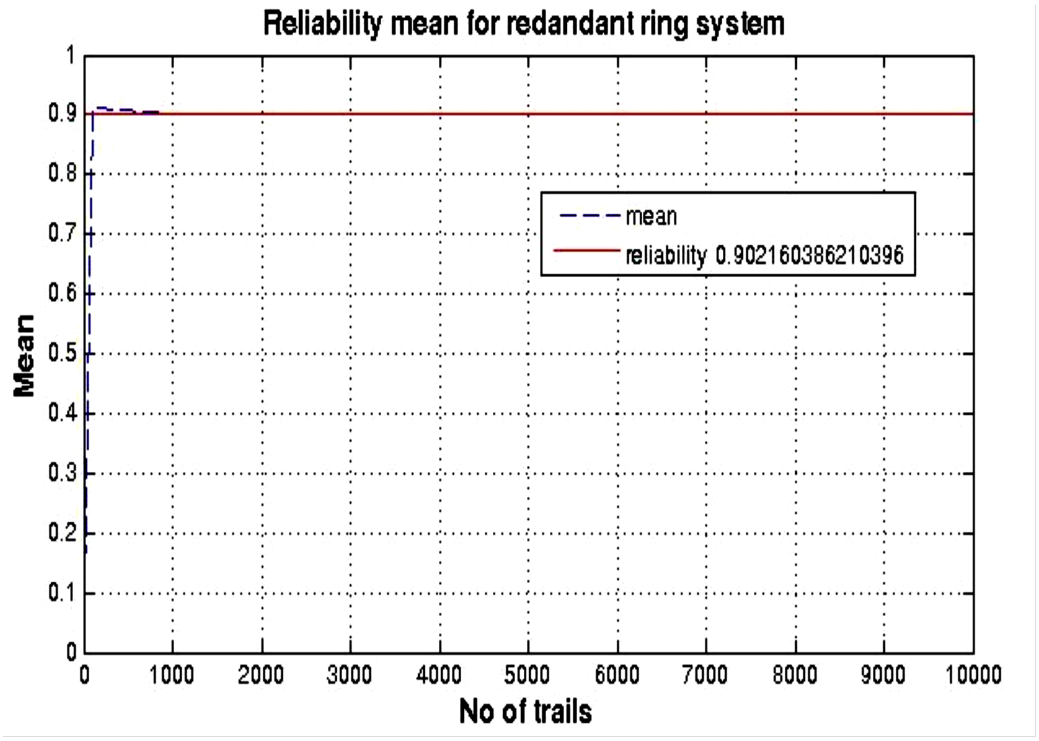


Figure 57. Reliability mean for the BFP function of the redundant ring topology.

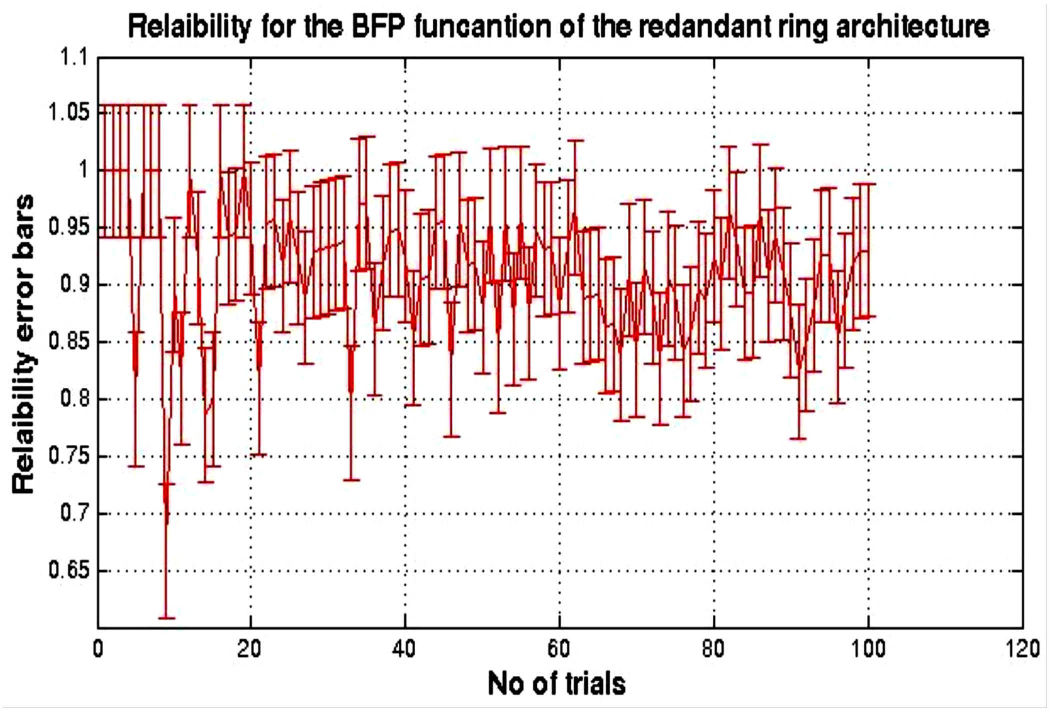


Figure 58. Reliability error bar of the redundant ring topology.

We can observe from Figure 54 that the RaFSA estimation reliability output results values for the SAS redundant ring topology are randomly variate about the true value (R(t) = 0.902160386) when the number of trials is small (±0.0316) at trial 100. In addition, and infrequently, the true value occurs in trials (32, 55, 75, 81, 82 and 90) and the number of instances where the values of the reliability are greater than the true value is approximately equal to the number of instances where the reliability values are less than the true value. The mean of the reliability values is (0.910451766) and the standard deviation is (0.058272275). Moreover, as the number of trials increases the variations in the reliability values are reduced. However, the values of the reliability remain variant even at trial 10,000, although the variation is reduced significantly and has a tendency towards the true value. The mean is (0.902201402) and the standard deviation is (0.009636179), as illustrated in Figure 56.

2.2.3 Discussion and Comparison of the Analytical Reliability, Probability of Failure and the RaFSA Estimation Method Results Values

From the novel RaFSA reliability estimation method, the mean and standard deviation output results values and the reliability analytical output results values for the above SAS communications network topologies are tabulated in Table 9.

Table 9. Reliability, analytical results, means and standard deviations.

Single IED trials	Mean	STD	Reliability anaytical result
100	0.940196437	0.054404264	0.935506985
1000	0.935590617	0.017980619	0.935506985
10000	0.935524025	0.007278546	0.935506985
GBPF trials			
100	0.959896583	0.032408827	0.954405479
1000	0.954447701	0.016076721	0.954405479
10000	0.954452063	0.006022050	0.954405479
Cascaded trials			
100	0.823838307	0.082451292	0.829720263
1000	0.829630730	0.031831826	0.829720263
10000	0.829789372	0.011974237	0.829720263
Ring trials			
100	0.910451766	0.058272275	0.902160386
1000	0.901740971	0.037374331	0.902160386
10000	0.902201402	0.009636179	0.902160386

Further, based upon our observation about achieving results values, we were able to conclude as follows:

- Generally, significant variations (errors) in the RaFSA reliability estimation results values about the true value occur when the number of trials is small.

- Infrequently, the true value occurs, in particular during random trials. However, for a real system this would not be known.

- The number of instances where the values for the RaFSA reliability estimation results values is greater than the true value is approximately equal to the number of instances where the reliability values are less than the true value. Therefore, the mean of the reliability values is approximately equal to the true value.

- The variation of the RaFSA reliability estimation results values away from the true value was reduced as the number of trials increased. Moreover, the reliability estimation values remained variant even after 5,000 trials; however, the variation was reduced significantly to the lowest value.

- For each analysis procedure, we needed to estimate the reliability values from several simulations. Each simulation had different output data (results). However, all the simulation results shared the same characteristic such that the results had a tendency to move towards the true values.

According to the results values for reliability based on the analytical and RaFSA estimation solutions, we observed that the SAS cascaded topology provided lower values than the SAS redundant ring bus topology, since it had non-redundant Ethernet switches (which constitute the bottleneck of the SAS's reliability). Furthermore, all the Ethernet switches needed to work successfully (in series) in order to execute the SAS BFP function. The advantages that are exhibited by the SAS cascaded topology are that it is less expensive and has a simple configuration, whereas the redundant SAS ring provides higher values that increase reliability. This result indicates that introducing redundancy to the Ethernet network has a greater impact on improving the SAS's reliability. However, and on the other hand, it also increases the SAS's complexity and cost. Therefore, it needs more practical and careful consideration upon its implementation.

It is important to note that the probability of failure estimation results values through the RaFSA estimation method for the BFP in various SAS communications network bus topologies based upon various numbers of trials are illustrated in Appendix 1.

2.2.4 Conclusion

The performance of electrical generation, transmission and distribution is directly related to the reliability of the components involved, mainly IEDs and the SAS's protection functions. Modern IEDs and protection functions can fail for any rea-son. As such, 100% reliability is impossible. Therefore, in order to assess the reli-ability and stability of the system, an actual system behaviour estimation method is required. This can be achieved by implementing the invented novel RaFSA estimation method.

The novel RaFSA estimation method attempts to examine and predict the actual behaviour pattern of each IED in the system. These examination and prediction features are provided given that the nature of the process that is involved in the RaFSA process is random. RaFSA provides specific benefits: it is easy to carry out in various PC software environments (such as MATLAB, C, C++, etc. Further) and it supports different kinds of probability distribution models (not only the exponential one). It can handle a huge amount of input data. Moreover, other analysis tools and parameters, such as the repairing time, the load flow, reconfiguration, optimization, etc., can be considered whereby these parameters are very difficult to carry out under the analytical solution approach. Lastly, changing the input data can easily be applied throughout RaFSA without major modifications to the underlying process.

2.3 Conclusions

In this chapter, SAS communications network bus topologies were discussed and analysed and several of their designs were tested. These tests attempted to explore some fundamental issues in SAS design based upon analysis of the BFP function. Meanwhile, reliability, the probability of failure and availability were also identified and calculated for these SAS topologies. Comparisons among these SAS topologies were then carried out based upon the reliability and availability calculations output results values. Redundancy was identified as a key feature in increasing the reliability and availability of SASs. Further, a novel RaFSA estimation method was presented. This method attempts to examine and predict the actual behaviour pattern of each IED in the system, and it has many advantages. These advantages are that it is easy to perform in various PC software environments, it supports different kinds of probability distribution models, it can handle a huge amount of input data, and other analysis tools and parameters (such as the repairing time, the load flow, reconfiguration, optimization, etc.) can be considered in the system's reliability, probability of failure and availability calculations.

3 PRACTICAL PERFORMANCE ANALYSIS

The proper operation of the planned SASs may require different testing levels, especially when trying to implement new technologies or standards in the initial version. Therefore, in Chapter 3, several practical testing experiments for an SAS based on the relatively new IEC 61850 standard are designed, constructed and carried out. These practical testing experiments are implemented to evaluate and prove the feasibility of the IEC 61850 standard as a promising solution for communications system networks in energy system

3.1 Performance Evaluation of IEC 61850 GOOSE Based Interoperability Testing

In this section, we analyse the timed response of the SAS by implementing one of the fastest possible critical messages in the IEC 61850 standard, namely a GOOSE message. GOOSE messages are published over a designed prototype SAS platform that presents the various manufacturers' IED environments. Upon this designed prototype SAS, interoperability testing is performed. The GOOSE messages' timed responses are successfully measured based upon the proposed round-trip method for the DUTs. The achieved output results values show that the DUTs were compliant with the IEC 61850 criteria. Furthermore, they prove the concept of interoperability such that the DUTs subscribe to the GOOSE messages from the third-party IEDs. A discussion of the various IED configuration tools, network load issues and deterministic GOOSE completes the vision.

3.1.1 Introduction

There are many steps involved in order to achieve the proper operation of a complete, designed SAS based on the specific assigned requirements from a development and production (of the IEDs) point of view. In IEC 61850 draft part (10), the standard defines a methodology for testing IEDs (the conformance test). Such IEDs must be compliant with the standard before they are accepted and implemented by end users. The IEC 61850 conformance test refers to a communications test that could significantly decrease any associated interoperability issues. It establishes the SAS communications network based upon laboratory testing and increases confidence that the DUT has complied with the IEC 61850 standard. Moreover, it also shows that the DUT is capable of operating with third-party IEDs in a specified way. It certified by the UCA International User Group (UCAlug). However, from the cumulative experiences that have been gained by employing it in DEMVE I-II since 2011, such DUTs which passed the conformance test still risked possibility that they would be incapable of operating in a multi-vendor environment. This is because various other factors might affect the integration and commission of IEDs in an SAS. Moreover, the conformance test might be considered as a form of product testing. This kind of testing can be handled by the manufacturers themselves. Furthermore, it is a specific type of test that only considers the functions and services that are requested by the IED vendor. Testing the functions and services may not be enough to cover the end user's requirements. As such, the most important aspect of the open nature of the IEC 61850 standard is that it gives wide ranging freedom for manufacturers to operate. Further, the interpretation of the IEC 61850 standard by different manufacturers remains different given the ambiguity that still exists. These issues may vary the interoperation of the standard from one vendor to another and may increase the complexity of the interoperability tasks within an SAS.

In addition, it requires various methods and configuration tools in order to configure IEDs from different manufacturers in order to achieve interoperability. Therefore, DUTs passing the conformance test cannot ensure interoperability suf-ficiently to meet end users' requirements. End users must include the interopera-bility test as a part of the IED acceptance process. The University of Vaasa has set up an in-house research and testing laboratory, the "Development of the Education Services of IEC 61850 in a Multi-Vendor Environment", DEMVE. This project maintains the vision and spirit of IEC 61850 for SASs such that sharing in-formation and executing it is the main concern.

3.1.2 The GOOSE Model

Multicasting GOOSE messages are designed to replace hardwired legacy interlocking signals with a logic interconnection. GOOSE is a high-speed time-critical message with high priority that should be transferred to the final destination with-in <4 ms. In order to increase the reliability of the GOOSE messages, several rep-licas of the original GOOSE message must be published when the status changes. This mechanism is used to guarantee that the subscriber IED is able to receive a copy of the originally published GOOSE messages and operate successfully.

The GOOSE protocol can be considered as a multicast publisher/subscriber model such that the published GOOSE messages can be received by various IEDs which have been configured to subscribe to them. Further, GOOSE supports the sharing of wide types of any available common data (binary, analogue measured values etc.) that are grouped into the GOOSE DATA-SET. IEC 61850-7-1 part defines the GOOSE model such that several parameters are used to control the publishing process, as follows;

DataSet: comprising various object references whereby the values of the dataset member groups can be published using GOOSE Control Block (GoCB).

GoEna: to remotely enable/disable the publishing of the GOOSE messages.

AppID: associated within the GoCB such that it may use GOOSE as an identifier of the LOGICAL-DEVICE, as well as with a handler for the selection of and subscription to various GOOSE messages from different IEDs at the same time.

ConRev: containing the configuration revision, which indicates any changes or updates within the dataset associated with the GoCB.

StNum: a state number that presents a counter which increments whenever there are changes within the GOOSE dataset's member values, such that these changes are detected and the GOOSE messages are published.

SqNum: a sequence number consisting of a counter which increments by a fixed number in the case of the publishing of GOOSE messages for instant ABB IED SqNUm increment by 100 each time.

GoRef: representing the reference for the GoCB.

Test: indicating the implementing of the values to the message based on TRUE (testing purpose) or FALSE (operation purpose).

NdsCom: this needs commissioning - it would indicate that the GoCB requires furthe configuration.

3.1.3 Measuring Latencies The Round-Trip Concept

A common starting point for the discussion comprises the issues relating to the time taken for transferring the time-critical GOOSE messages. The transfer time should be less than 4 ms for a GOOSE command. IEC 61850-5 part highlights the different times involved in the transfer process of the messages from one point to another, as illustrated in Figure 59.

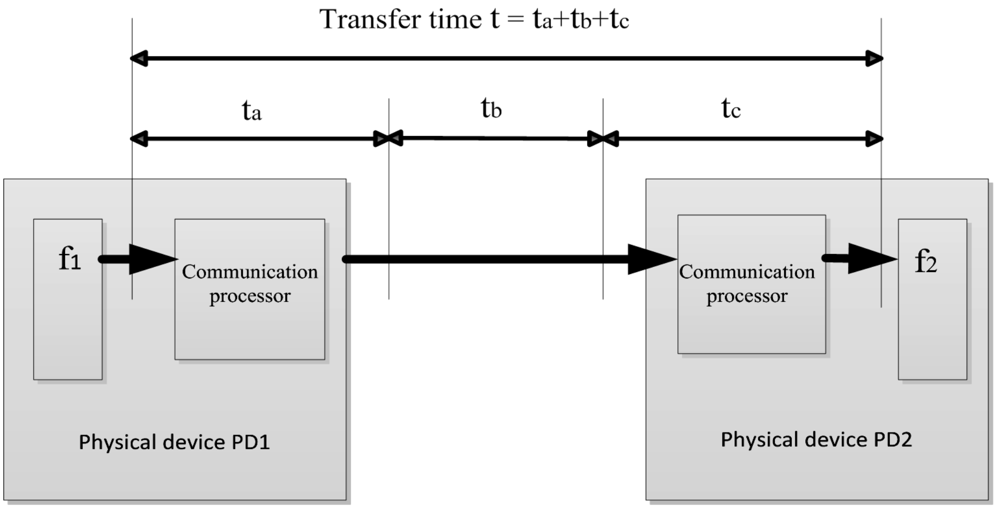


Figure 59. Overall transfer time IEC 61850-5.

In Figure 59, the performance evaluation of the SAS communications network based upon the above process may not reflect or guarantee the actual system performance, which is particularly important for practical, real-time applications. Therefore, the idea of achieving an appropriate evaluation of GOOSE's performance within the DUT might be by measuring the round-trip time, as illustrated in Figure 60 (Steinhauser etc. 2010).

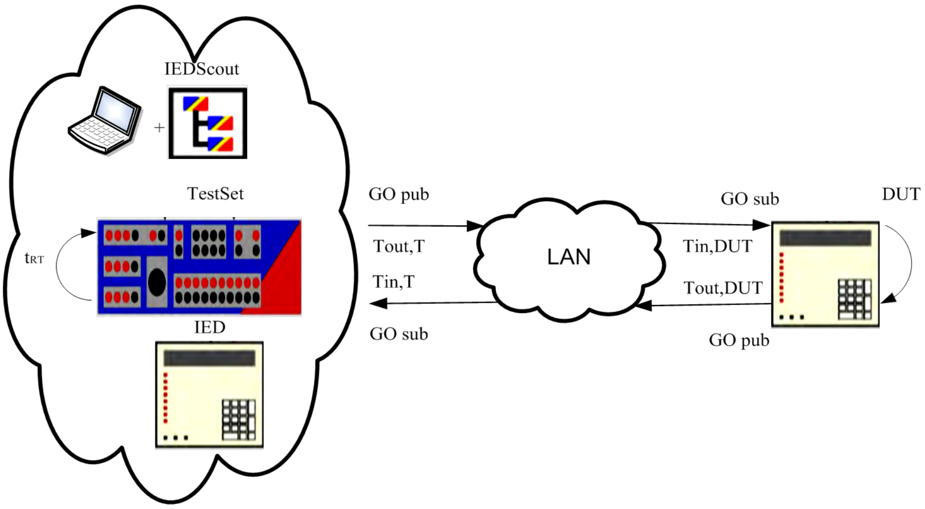


Figure 60. The round_trip concept

According to the proposed round-trip measuring process for the DUT response, firstly, stimulus GOOSE messages are published to the DUTs over the SAS communications network. The DUTs were configured to subscribe to the published GOOSE messages. Secondly, the DUTs next attempt to extract and execute the associated information and then try to publish other GOOSE messages as quickly as possible. Measuring the round-trip time involves seven individual times that may affect GOOSE's performance. Therefore, two assumptions have to be made in order to achieve useful measuring results. The first assumption that can be fulfilled in most cases is that the network time t_LAN can be neglected under the condition that the communications network between the test set and the DUT is kept as simple as possible while using a single high-performance Ethernet switch within a 100 Mbit/s network. This is because the GOOSE message is very short at several hundred bits (for instance, Vamp IED is 952 bits, ABB IED is 1,280 bits, etc.).

The second assumption is that of the symmetry of t_in and t_out for both the DUT and the test set, since the processing time for the same number of data (packet size) within the same processor and the same environment is expected to be constant, as illustrated bellow (Ingram etc. 2013)

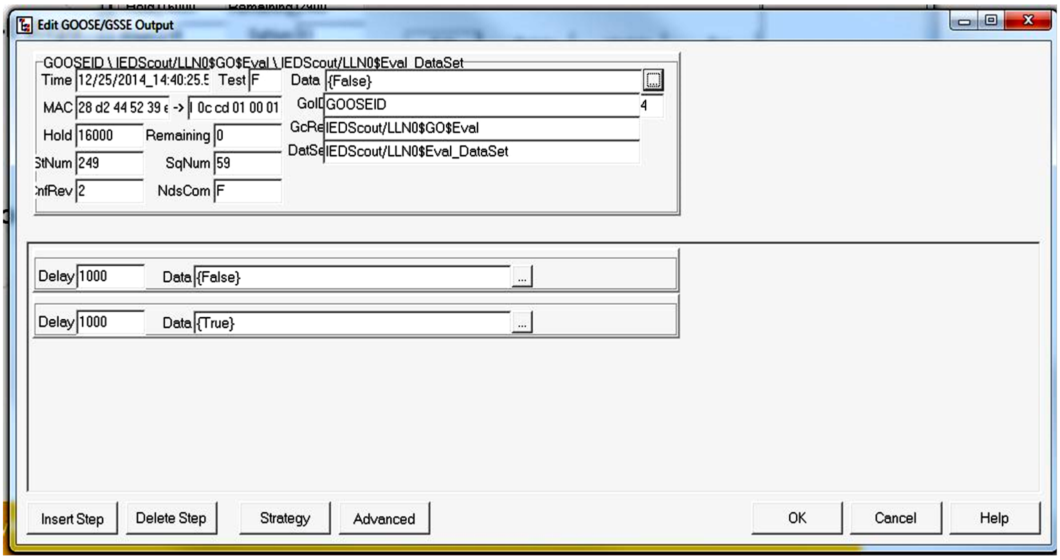
(3.1) $$\bar{t}_{RT} = \bar{t}_{out.TS} + \bar{t}_{LAN} + \bar{t}_{in.DUT} + \bar{t}_{App} + \bar{t}_{out.DUT} + \bar{t}_{LAN} + \bar{t}_{in.TS}$$

(3.2) $$\sigma^2{}_{RT} = \sigma^2{}_{out.TS} + \sigma^2{}_{LAN} + \sigma^2{}_{in.DUT} + \sigma^2{}_{App} + \sigma^2{}_{out.DUT} + \sigma^2{}_{LAN} + \sigma^2{}_{in.TS}$$

3.1.4 Performance Evaluation of the DUT Using GOOSE Messages

In this section, the practical performance evaluation of the DUTs using GOOSE messages and their timed response needs to be assessed. The main objective of the testing task is to verify that the DUTs' performance given a timed response such that the publishing of the GOOSE messages is compliant with the IEC 61850 requirements (i.e., not exceeded 4 ms). Furthermore, the DUT has the ability to operate within a multi-vendor environment for interoperability testing.

In terms of implementation, the first scenario is to design the testing of a multi-vendor environment for modern IEDs employed within an SAS. The experimental testing begins by designing a small SAS consisting of hardware and software. The hardware instruments are an Ethernet switch (MiCOM H35x), a Vamp 257 feeder protection IED and a PC. The Software comprises the Vampset configuration tool, Omicron IEDScout, Wireshark and Sigra (Siemens) or TransView (Omi-cron). According to the testing process, the first step is to configure IEDScout, which attempts to generate the GOOSE messages as a Boolean value and publish them based on the assigned GOOSE parameters to the communications network, as illustrated in Figure 61.


Edit GOOSE/GSSE Output

GOOSEID \ IEDScout/LLN0$GO$Eval \ IEDScout/LLN0$Eval_DataSet

Time 12/25/2014_14:40:25.5 Test F
Data {False}
MAC 28 d2 44 52 39 ε -> I 0c cd 01 00 01
GoID GOOSEID 4
Hold 16000 Remaining 0
GcRe IEDScout/LLN0$GO$Eval
DatSe IEDScout/LLN0$Eval_DataSet
StNum 249 SqNum 59
nfRev 2 NdsCom F

Delay 1000 Data {False}

Delay 1000 Data {True}

Figure 61. IEDScout GOOSE messages.

In the second step, configuration of the Vamp 257 IED with the Vampset configuration tool takes place, assigning all the subscription GOOSE parameters that are related to the IEDScout GOOSE messages' parameters. Furthermore, Vamp 257 IED attempts to publish other GOOSE messages. This task can be achieved by designing a GOOSE receiving function within the Vampset IED configuration tool (the logic view window) to execute the round-trip scenario. We use the outputs of these functions within the signal matrix to associate these values with the GoCB dataset for publishing the Vamp 257 GOOSE messages, as illustrated in Figure 62.

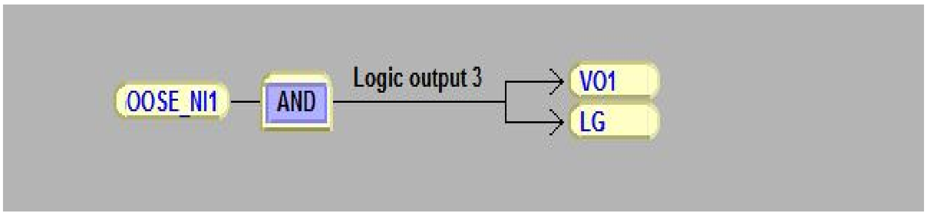
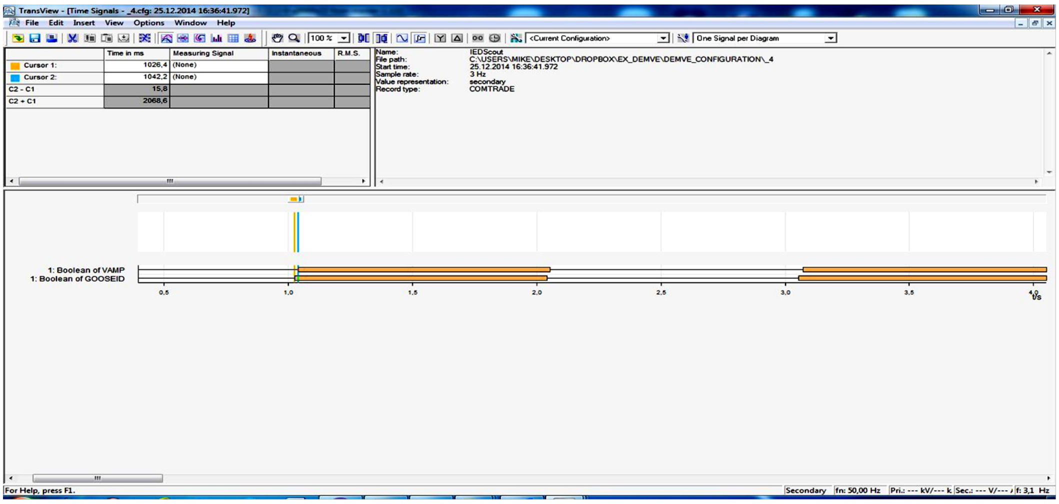


Figure 62. Vampset configuration tool.

The t_App IED sequence is related to the subscribing GOOSE messages and Boolean values can be extracted from the EVENT BUFFER within the Vampset configuration tool. Further, Vamp 257 IED is synchronized based on the PC internal clock within the Vampset configuration tool. It is credible to assume that the GOOSE status change occurs at the same time as it is seen in IEDScout and the DUT. The visualization and analysis of the recorded GOOSE messages is implemented within the TransView software, as illustrated in Figure 63. This shows the t_RT, which is the time from publishing the GOOSE messages by IEDScout until the time of receipt of those GOOSE messages within the DUT, which executes the internal functions and publishes other GOOSE messages through the SAS communications network.



	Time in ms	Measuring Signal	Instantaneous	R.M.S.
Cursor 1:	1026,4	(None)		
Cursor 2:	1042,2	(None)		
C2 - C1	15,8			
C2 + C1	2068,6			

Name: IEDScout
File path: C:\USERS\MIKE\DESKTOP\DROPBOX\EX_DEMVE\DEMVE_CONFIGURATION_4
Start time: 25.12.2014 16:36:41.972
Sample rate: 3 Hz
Value representation: secondary
Record type: COMTRADE

For Help, press F1. | Secondary | fn: 50,00 Hz | Pri.: --- kV/--- k | Sec.: --- V/--- / | f: 3,1 Hz

Figure 63. Fault analyzer software.

From Equation (3.1) the time t_DUT is calculated as follows,

$$t_{\_DUT} = t_{\_RT} - t_{\_App} \qquad (3.3)$$

where the outcomes from Equation (3.3) are divided into two based on the assumption that was mentioned earlier, namely that t_in and t_out for the DUT are symmetric. Table 1 shows the calculation for the DUT GOOSE performance evaluation output results values.

Table 10. Measuring of DUT GOOSE messages latencies.

Experiments	Time ms		
	t_RT (ms)	*t_App (ms)*	*DUT GOOSE (ms)*
1	22.4610	20	1.2305
2	24.4610	20	2.157
3	16.0610	10	3.0305
4	18.7060	10	4.353
5	22.1140	20	1.057
6	23.8410	20	1.9205
7	17.2800	10	3.640
8	15.5660	10	2.830
9	18.9510	10	3.4755
10	24.8030	20	2.4015

Using a normal distribution probability density function, the mean and the stand-ard deviation of the DUT GOOSE timed response was calculated, such that (mean = 2.6095) and (std = 1.06). From the GOOSE performance evaluation output results values, it can be observed that the testing trials have successfully measured the timed response and publishing of the GOOSE messages for the DUT through the communications network, and it shows that the DUT is compliant with the IEC 61850 criteria. Furthermore, it proves the interoperability concept, such that the DUT subscribes to the GOOSE messages that were published by the third-party IED simulated by the Omicron IEDScout.

Consequently, according to the second scenario, we design a multi-vendor testing environment for the DUT IEDs within a modern SAS. The experiment begins by designing a small SAS from hardware and software. The hardware comprises an Ethernet switch (MiCOM H352), two Vamp 257 IEDs as GOOSE message subscribers and publishers, ABB REG 670 as the GOOSE message publisher, and a PC. The software comprises the Vampset configuration tool, ABB PCM 600, the IET600 configuration tools, Omicron TransView, Wireshark and Sigra. In terms of the test implementation process, the first step is to configure the Vamp 257 relays with the Vampset IED configuration tool and assign all the GOOSE parameters for subscribing and publishing.

The ABB REG 670 IED is configured by the ABB IED configuration tool PCM600 as the GOOSE publisher. The entire system is configured by the ABB system configuration tool IET600. Furthermore, we design protection functions and use their outputs with the signal matrix to associate those values with the GoCB dataset of the GOOSE messages within the Vamp IEDs as before. In the second step, the status indication within the ABB REG 670 occurred based on connecting the external signal to the digital input (DI) ABB REG 670 connectors. These status indicators must be published upon the GOOSE messages through the SAS communications network. In the third step, Vamp 257 relays must subscribe to the REG670, thereby publishing the GOOSE messages, extract the information from them, and then execute the de-signed functions. Furthermore, the Vamp 257 IEDs attempt to publish other GOOSE messages. All the IEDs are synchronous, and the time reference for calculation is the PC internal clock. Lastly, the visualization and analysis of the recorded GOOSE messages are implemented within the TransView application. The achieved output results values show the t_RT, which is the time from publishing the GOOSE messages by REG 670 until the receipt of those GOOSE messages within the DUTs and their publishing of another GOOSE to the SAS communications network, as illustrated in Figures 64-65.

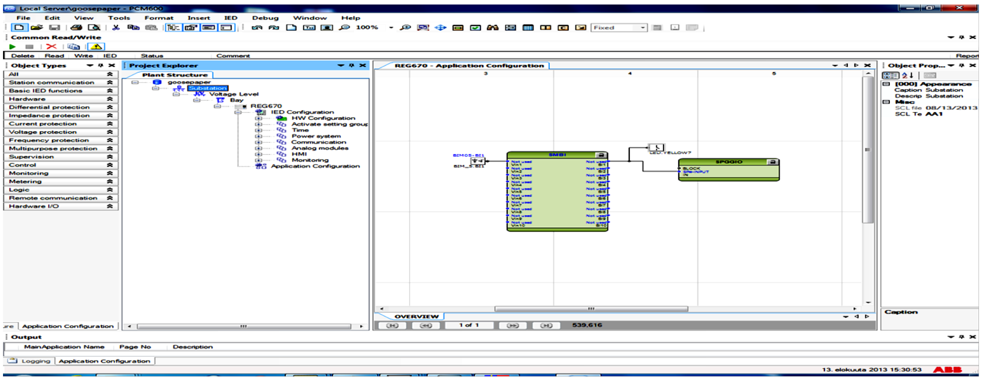
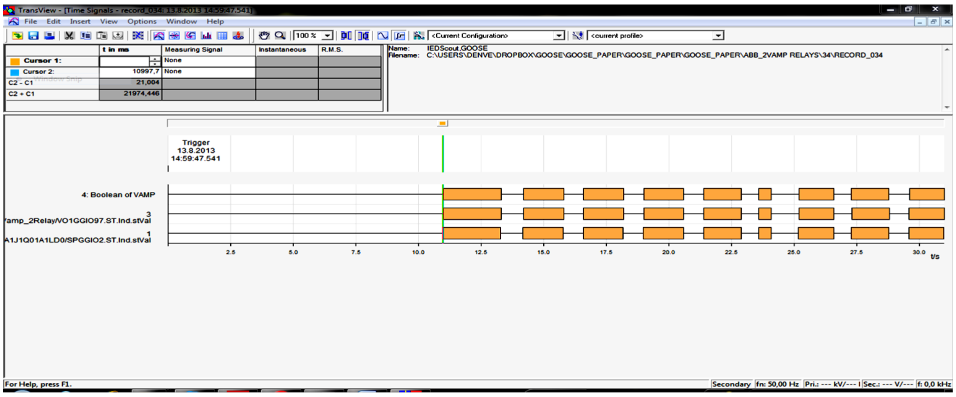


Figure 64. ABB PCM 600 IED configuration tool.


TransView - [Time Signals - record_034: 13.8.2013 14:59:47.541]
File Edit Insert View Options Window Help
<Current Configuration>
<current profile>

	t in ms	Measuring Signal	Instantaneous	R.M.S.
Cursor 1:		None		
Cursor 2:	10997,7	None		
C2 - C1	21,004			
C2 + C1	21974,446			

Name: IEDScout.GOOSE
Filename: C:\USERS\DENVE\DROPBOX\GOOSE\GOOSE_PAPER\GOOSE_PAPER\GOOSE_PAPER\ABB_2VAMP RELAYS\34\RECORD_034

Figure 65. Fault analyzer tool.

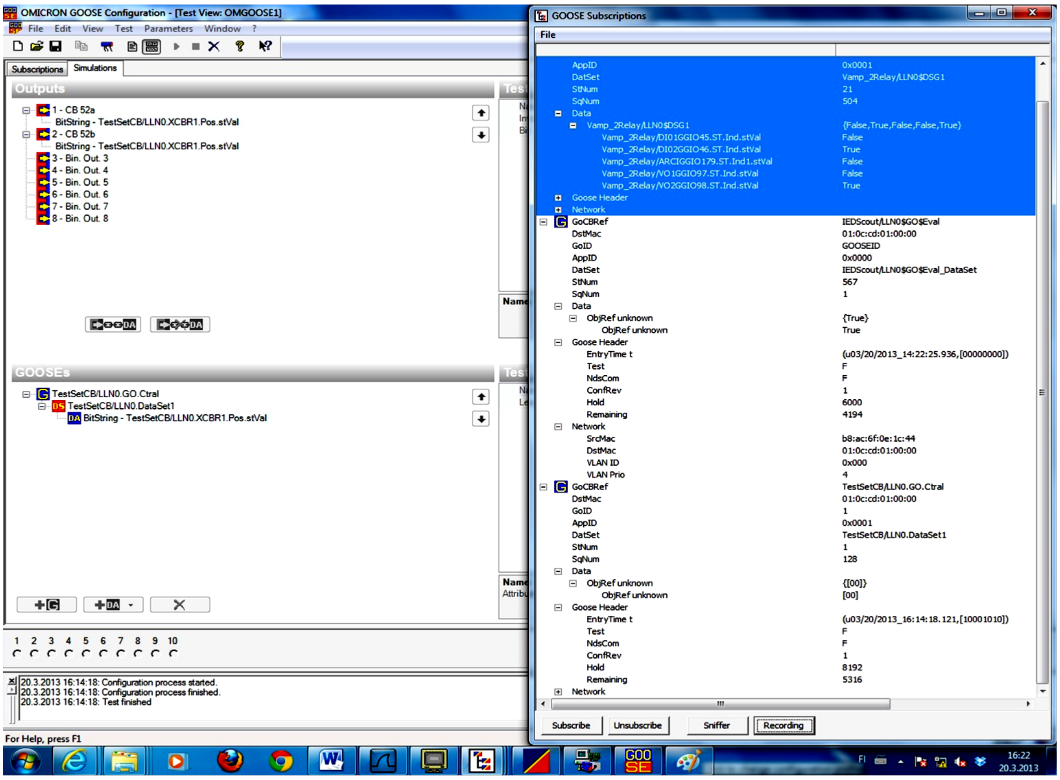
The same procedure as the first scenario can be implemented here, such that the performance evaluation of the timed response of the DUTs upon receipt of the GOOSE messages is carried out. The main difference between scenario one and scenario two is that the GOOSE messages were published by IEDScout as the publisher to the Vamp 257 IED DUT as the subscriber. In scenario two, however, the GOOSE messages were published by ABB REG 670 as the publisher and two DUTs, namely Vamps 257 IEDs, as the subscribers. Table 11 shows the calculation for the GOOSE performance evaluation output results values for DUT1 and DUT2.

Table 11. Measuring of DUTs GOOSE messages latencies.

Ex	*t_RT 1*	*t_App 1*	*DUT1 GOOSE*	*t_RT2*	*t_App2*	*DUT2 GOOSE*
1	22.477	20	1.2385	23.029	20	1.5145
2	22.078	20	1.039	22.715	20	1.3575
3	21.220	20	0.61	21.663	20	0.8315
4	19.636	10	4.818	15.814	10	2.907
5	19.382	10	4.691	15.615	10	2.8075

Using a normal distribution probability density function, the mean and the stand-ard deviation of the timed response GOOSE DUT1 are calculated, such that (mean = 2.4793) and (std = 2.0898). Further, the mean and the standard deviation of the timed response GOOSE DUT2 are calculated, whereby (mean = 1.8836) and (std = 0.9248). From the timed response GOOSE performance evaluation output results values, it can be observed that the experiment has successfully measured the timed response of the GOOSE messages for the DUTs, and it shows that the DUTs are compliant with the IEC 61850 criteria. Furthermore, a comparison between the responses of the DUTs for the same stimuli signal can be made. Lastly, it proves the interoperability concept such that the DUTs subscribe to the GOOSE messages from the third-party IED ABB REG 670. The main advantage of using Vamp IEDs as subscribers is that all the subscription GOOSE parameters can be assigned manually based on the ABB REG 670 GOOSE publishing parameters within the Vampset IED configuration tool.

The third scenario involves configuring modern test devices (the Omicron CMC test set) based on the subscribing and publishing of GOOSE messages, such that they can be used the measure the round-trip time of the GOOSE messages for different DUTs' IEDs. In terms of the testing implementation process, the first step is to design the testing prototyping platform environment for the multi-vendor modern IEDs. The prototyping platform consists of hardware and software. The hardware comprises an Ethernet switch (MiCOM H35-V2), ABB REG670, the Omicron CMC356 test set, two Vamp 257 IEDs and a PC. The software comprised PCM600, IET600, the Vampset configuration tools, Omicron Test Universe, IEDScout, Wireshark and Sigra (Siemens) or TransView (Omicron). During the second step, ABB REG670 is configured as a GOOSE message publisher using the PCM600 and IET600 system configuration tools. The CMC356 test set, based on the GOOSE configuration module, is configured as a subscriber and publisher for the REG670 GOOSE messages using the Omicron Test Universe software. The CMC356 inverts the received signal from REG670 and sends it to the SAS communications network. In the third step, the two Vamp 257 IEDs are configured as subscribers for the Omicron CMC356 test set GOOSE messages. The subscription process needs to extract the information from the GOOSE messages and execute the internal function; it then publishes other GOOSE messages through the SAS communications network using the Vampset configuration tool. The two Vamp 257 IEDs are synchronized based on the PC internal clock. All the measuring and latency calculations are based on the same reference time (the network analyser). It is credible to assume that the GOOSE status change occurred at the same time as seen in the network analyser tools and the DUTs. The same configuration steps as for scenarios one and two are used in scenario three. The CMC356 configuration is illustrated in Figure 66.



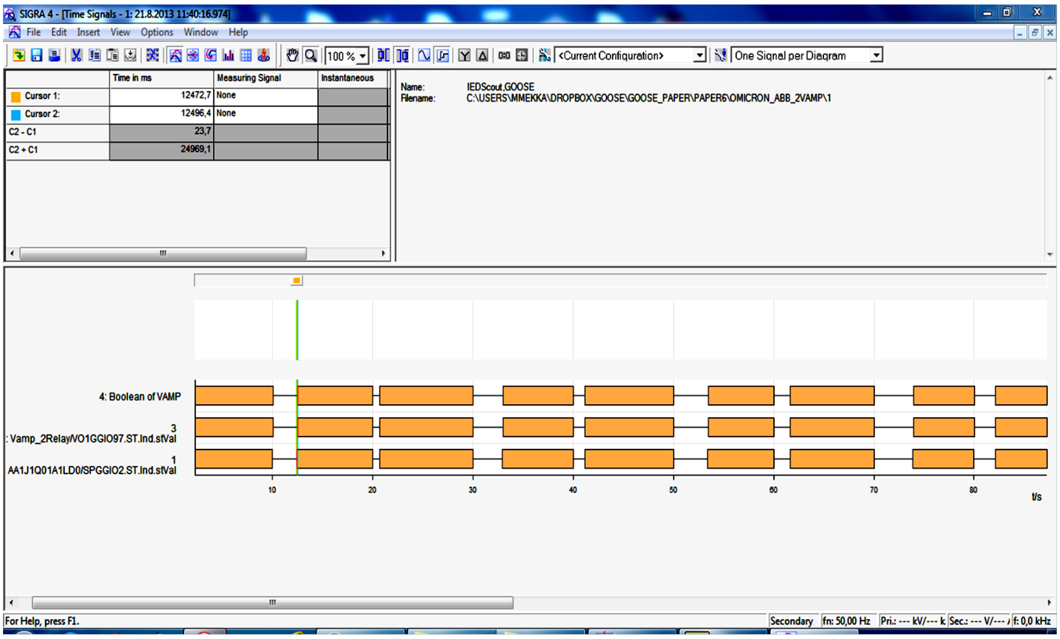
```
1 - CB 52a
    BitString - TestSetCB/LLN0.XCBR1.Pos.stVal
2 - CB 52b
    BitString - TestSetCB/LLN0.XCBR1.Pos.stVal
3 - Bin. Out. 3
4 - Bin. Out. 4
5 - Bin. Out. 5
6 - Bin. Out. 6
7 - Bin. Out. 7
8 - Bin. Out. 8

TestSetCB/LLN0.GO.Ctral
  TestSetCB/LLN0.DataSet1
    BitString - TestSetCB/LLN0.XCBR1.Pos.stVal
```

```
20.3.2013 16:14:18: Configuration process started.
20.3.2013 16:14:18: Configuration process finished.
20.3.2013 16:14:18: Test finished
```

```
    AppID                                   0x0001
    DatSet                                  Vamp_2Relay/LLN0$DSG1
    StNum                                   21
    SqNum                                   504
    Data
      Vamp_2Relay/LLN0$DSG1                 {False,True,False,False,True}
        Vamp_2Relay/DI01GGIO45.ST.Ind.stVal      False
        Vamp_2Relay/DI02GGIO46.ST.Ind.stVal      True
        Vamp_2Relay/ARCIGGIO179.ST.Ind1.stVal    False
        Vamp_2Relay/VO1GGIO97.ST.Ind.stVal       False
        Vamp_2Relay/VO2GGIO98.ST.Ind.stVal       True
    Goose Header
    Network
  GoCBRef                                   IEDScout/LLN0$GO$Eval
    DstMac                                  01:0c:cd:01:00:00
    GoID                                    GOOSEID
    AppID                                   0x0000
    DatSet                                  IEDScout/LLN0$GO$Eval_DataSet
    StNum                                   567
    SqNum                                   1
    Data
      ObjRef unknown                        {True}
        ObjRef unknown                      True
    Goose Header
      EntryTime t                           (u03/20/2013_14:22:25.936,[00000000])
      Test                                  F
      NdsCom                                F
      ConfRev                               1
      Hold                                  6000
      Remaining                             4194
    Network
      SrcMac                                b8:ac:6f:0e:1c:44
      DstMac                                01:0c:cd:01:00:00
      VLAN ID                               0x000
      VLAN Prio                             4
  GoCBRef                                   TestSetCB/LLN0.GO.Ctral
    DstMac                                  01:0c:cd:01:00:00
    GoID                                    1
    AppID                                   0x0001
    DatSet                                  TestSetCB/LLN0.DataSet1
    StNum                                   1
    SqNum                                   128
    Data
      ObjRef unknown                        {[00]}
        ObjRef unknown                      [00]
    Goose Header
      EntryTime t                           (u03/20/2013_16:14:18.121,[10001010])
      Test                                  F
      NdsCom                                F
      ConfRev                               1
      Hold                                  8192
      Remaining                             5316
    Network
```

Figure 66. The CMC GOOSE configuration module.


SIGRA 4 - [Time Signals - 1: 21.8.2013 11:40:16.974]

	Time in ms	Measuring Signal	Instantaneous
🟧 Cursor 1:	12472,7	None	
🟦 Cursor 2:	12496,4	None	
C2 - C1	23,7		
C2 + C1	24969,1		

Name: IEDScout.GOOSE
Filename: C:\USERS\MMEKKA\DROPBOX\GOOSE\GOOSE_PAPER\PAPER6\OMICRON_ABB_2VAMP\1

For Help, press F1.

Figure 67. The fault analyser tool.

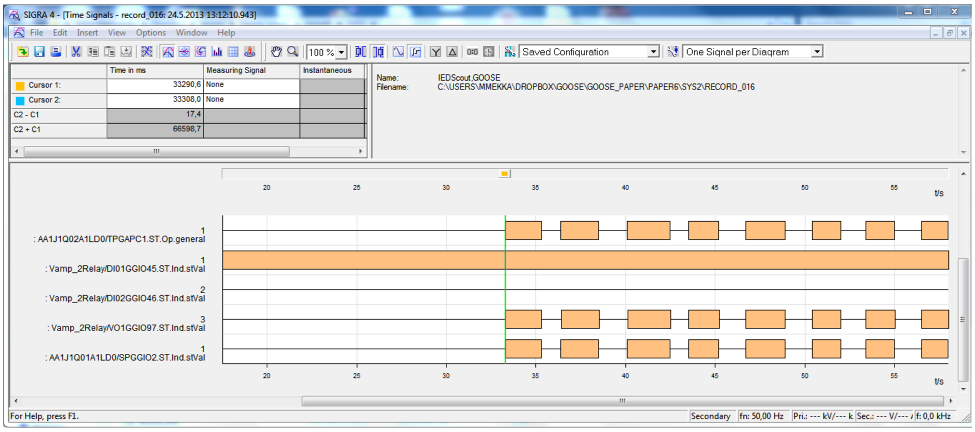
The timed responses of the GOOSE messages for the DUTs have been calculated and the output results values are tabulated in Table 12.

Table 12. Measurements of the DUTs GOOSE message latencies.

Ex	*t_RT 1*	*t_App1*	*DUT1 GOOSE*	*t_RT2*	*t_App 2*	*DUT2 GOOSE*
1	23.628	20	1.814	24.549	20	2.274
2	21.498	20	0.749	21.508	20	0.754
3	16.499	10	3.249	17.600	10	3.800
4	15.499	10	2.749	16.674	10	3.337
5	21.632	20	0.816	22.653	20	1.326
6	21.592	20	0.796	22,710	20	1.355
7	17,626	10	3.813	18.819	20	4.409
8	16.558	10	3.279	16.558	10	3.279
9	23.474	20	1.737	24.503	20	2.251
10	18.839	10	4.3195	19.994	10	4.997

Using a normal distribution probability density function, the mean and the stand-ard deviation of the timed responses of GOOSE for the DUTs are measured and calculated, such that DUT1 (mean = 2.3321) and (std = 1.3267), while for DUT2 (mean = 2.7782) and (std = 1.4124). For the GOOSE timed response performance evaluation output results values s, it can be observed that the experiments successfully measured the timed responses of the GOOSE messages for the DUTs based on the measurement of the round-trip time for the GOOSE messages. Furthermore, the results show that the DUTs are compliant with the IEC 61850 criteria. Moreover, it proves the concept of interoperability such that the DUTs sub-scribe to the GOOSE messages from the third-party CMC 356, as simulated by the Omicron Test Universe GOOSE configuration module. CMC 356 subscribes to the GOOSE messages that are published by ABB REG670, inverts them and then publishes further GOOSE messages to the DUTs.

In the last scenario, we design and test a prototype platform multi-vendor environment for a modern SAS. The prototype platform consists of hardware and software. The hardware comprises an Ethernet switch (MiCOM H35-V2), ABB REG670, ABB REF615, Vamp 257 IED and a PC. PCM600, IET600, the Vampset configuration tools, Omicron IEDScout, Wireshark and Sigra (Siemens) or TransView (Omicron) are the software. According to the testing initialization, the first step is to configure REG670 as a GOOSE message publisher. As a second step, we configure the VAMP257 relay and ABB REF615 as subscribers for the ABB REG670 GOOSE messages, we then extract the information that is associated with these messages, execute the internal functions and then publish other GOOSE messages to the SAS communications network. All the timed responses, measurements and calculations are based on the same reference time (the network analyser). It is credible to assume that the GOOSE status change occurred at the same time as seen in the network analyser tools and the DUTs.



SIGRA 4 - [Time Signals - record_016: 24.5.2013 13:12:10.943]

	Time in ms	Measuring Signal	Instantaneous
🟧 Cursor 1:	33290,6	None	
🟦 Cursor 2:	33308,0	None	
C2 - C1	17,4		
C2 + C1	66598,7		

Name: IEDScout,GOOSE
Filename: C:\USERS\MMEKKA\DROPBOX\GOOSE\GOOSE_PAPER\PAPER6\SYS2\RECORD_016

Saved Configuration
One Signal per Diagram

For Help, press F1.

Secondary | fn: 50,00 Hz | Pri.: --- kV/--- k | Sec.: --- V/--- / | f: 0,0 kHz

File
Edit
Insert
View
Options
Window
Help
100 %
1
: AA1J1Q02A1LD0/TPGAPC1.ST.Op.general
1
: Vamp_2Relay/DI01GGIO45.ST.Ind.stVal
2
: Vamp_2Relay/DI02GGIO46.ST.Ind.stVal
3
: Vamp_2Relay/VO1GGIO97.ST.Ind.stVal
1
: AA1J1Q01A1LD0/SPGGIO2.ST.Ind.stVal
20
25
30
35
40
45
50
55
t/s

Figure 68. The fault analyser tool.

The GOOSE messages timed responses for the DUTs are tabulated in Table 13.

Table 13. Measuring of DUTs GOOSE messages latencies.

Ex	*t_RT 1*	*t_App 1*	*DUT1 GOOSE*	*t_RT2*	*t_App 2*	*DUT2 GOOSE*
1	2.763	1	0.881	24.029	20	2.224
2	2.654	1	0.827	24.086	20	2.043
3	2.648	1	0.824	24.000	20	2.000
4	2.593	1	0.796	23.730	20	1.865
5	2.605	1	0.802	23.500	20	1.750
6	2.589	1	0.7945	23.163	20	1.581
7	2.462	1	0.731	22.885	20	1.442
8	2.530	1	0.765	22.615	20	1.307
9	2.445	1	0.722	22.533	20	1.266
10	2.411	1	0.705	22.272	20	1.136

Using a normal distribution probability density function, the mean and the stand-ard deviation for the timed response GOOSE messages of the DUTs is measured and calculated, such that DUT1 (mean = 0.7848) and (std = 0.0545), while for DUT2 (mean = 1.6614) and (std = 0.3710). From the timed responses of the GOOSE performance evaluation output results values, it can be observed that the experiments successfully measured the timed responses of the GOOSE messages for the DUTs based on the measurement of the round-trip time for the GOOSE messages. Furthermore, it shows that the DUTs are compliant with the IEC 61850 criteria. In addition, it proves the interoperability concept such that the DUTs sub-scribe to the GOOSE messages from the third-party IED.

3.1.5 Conclusion

Performance evaluation and interoperability testing are an important issue that must be realized by utilities in the design and implementation of modern SAS processes based on the IEC 61850 standard. Performance evaluations and interoperability testing comprise crucial tasks that may require special efforts based on several modern hardware and software tools which have to be used. One element of such performance evaluation and interoperability testing involves the timed responses for the DUT based upon GOOSE messages. Therefore, the analysis of the timed response of the DUTs was carried out by implementing one of the quickest high-speed time-critical messages under the IEC 61850 standard, namely the GOOSE message. The obtained output results values show the successful measurement and calculation of the timed responses of the GOOSE messages for the DUTs based on the proposed round-trip approach. Furthermore, it shows that the DUTs are compliant with the IEC 61850 criteria. Moreover, it proves the concept of interoperability such that the DUTs subscribe to the GOOSE messages from the third-party IED as well as from the CMC test set. In addition, a comparison between the timed response GOOSE messages of the DUTs was made. Cumulative experiences were gained based upon designing, configuring and implementing an SAS within a laboratory environment using modern IEDs and modern configuration software tools. For future work, several assumptions are made in this part so as to simplify what work could be waived. Furthermore, the measurement of the latencies for the round-tip time of the GOOSE messages based on various bus topologies with more than one Ethernet switch may need to be considered. Similar issues can be raised to calculate the accumulation jitter for the GOOSE messages when there is interference with traffic propagating within the same SAS communications network.

3.2 A Novel Approach to the Needs of a Vendor-Neutral System Configuration Tool

In this section, we demonstrate a novel approach to a new SAS configuration tool which is independent of any commercial IED brand. It has the ability to import SCL files from various manufacturers’ IEDs, systems and databases, and creates and raises the IEDs' configuration to the system level based upon the full IEC 61850 standard approach, including the protection and feature-setting level.

3.2.1 Introduction

The internationally accepted IEC 61850 standard has stimulated researchers and developers to go a long way towards plug-and-play IEDs within SASs. However, and on the other hand and from cumulative experiences, broad issues have been raised as regards SASs' integration and commissioning, especially where the SAS consists of various manufacturers' IEDs, as mentioned in Section 3.1.1. Moreover, this task needs full support from manufacturers. Several research works (Ali et al. 2012; Holbach et al. 2007; Chen et al. 2012; Ridwan et al. 2012; Englert & Dawidczak 2010; Hong et al. 2013; Mekkanen et al. 2013; UCA 2011) have identified that the major challenges facing the implementation of the IEC 61850 standard among multi-vendor IEDs are the cost, effort involved and time required for the configuration of the IEDs as well as the entire SAS based on the existing SAS configuration process (in order to achieve smooth communication and interoperability). The challenges have been raised based upon IED protection and configuration settings parameters as regards the differences for each vendor, who require proprietary software for each IED. Moreover, engineers need to be highly trained in order to utilize different proprietary configuration tools for the same purpose. Most of the above-mentioned works are pilot projects that have considered commercial IEDs for designed laboratory platforms and commercial software configuration tools. Therefore, in order to reduce costs, effort and the time taken, a novel approach for a new proposed SAS configuration tool is adopted. The novel configuration tool is independent of any commercial IED brand. It has the ability to import SCL files from different vendors, IEDs, systems and databases, creating and increasing the relay configuration to the system level based on the proposed full IEC 61850 standard, including the protection and feature setting levels. Moreover, it can separate the SAS configuration tasks between various SAS engineer groups. For instance, the protection engineer is able to focus for the design and implementation of the protection scheme rather than the underlying communications infrastructure.

3.2.2 Challenges Within the Existing IEDs and System Configuration Tool

The IEC 61850 standard assigns several SCL files to describe the SAS's aspects. Each IED within the SAS has the ability to generate the SCL files with different extinction to describe its capabilities and to define itself relative to the system configuration tool. According to the existing SAS configuration process, the SCL files need to be created by a proprietary IED configuration tool or else are provided by the vendors. In order to configure the entire SAS, all the SCL files for the various manufacturers' IEDs have to be imported to one of the available system configuration tools as chosen by any the IED manufacturers participating in the SAS project, as illustrated in Figure 69.

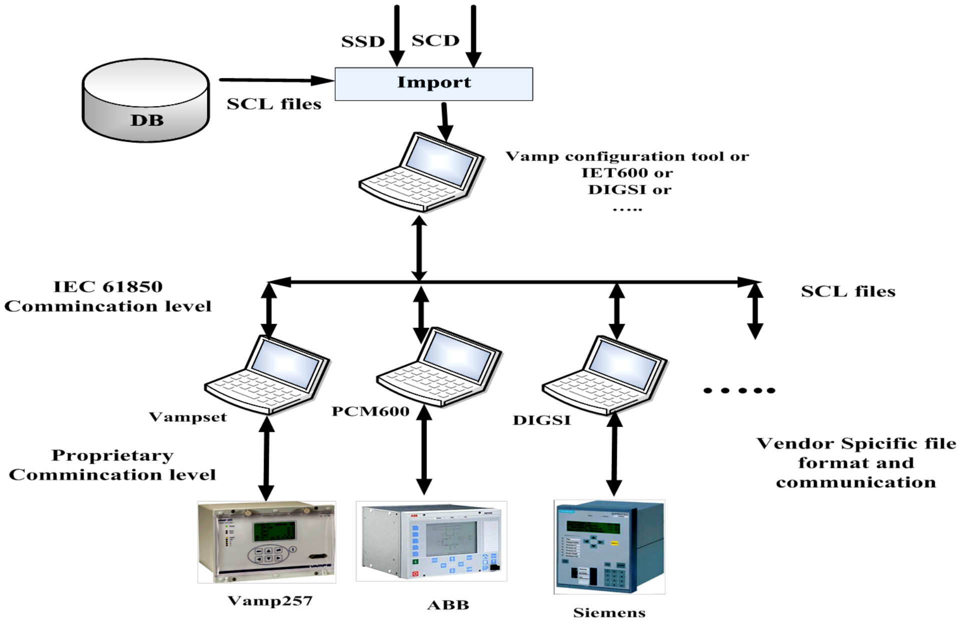
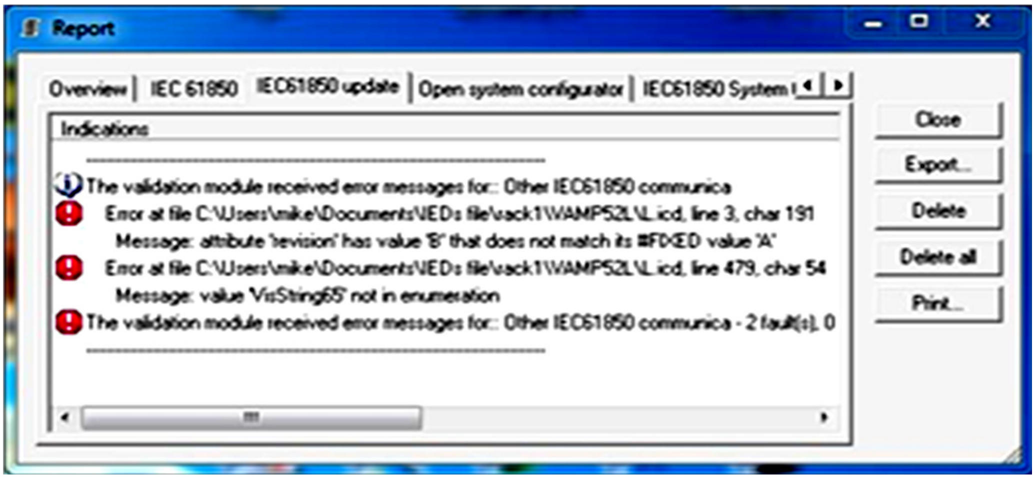


Figure 69. The existing SAS configuration process.

However, these imported SCL files have to be updated constantly during the system configuration process to a final configuration containing the protection settings parameters as well as the final communications settings. It was considered that, during the importing process, an error report might be produced by the IEC 61850 validator tool such that some of the created SCL files would have some format errors based upon the ambiguity explained earlier, and as illustrated in Figure 70. These errors were the first hurdle that had to be resolved.



```
------------------------------------------------------------
The validation module received error messages for:: Other IEC61850 communica
   Error at file C:\Users\mike\Documents\IEDs file\rack1\VAMP52L\L.icd, line 3, char 191
    Message: attribute 'revision' has value 'B' that does not match its #FIXED value 'A'
   Error at file C:\Users\mike\Documents\IEDs file\rack1\VAMP52L\L.icd, line 479, char 54
    Message: value 'VisString65' not in enumeration
The validation module received error messages for:: Other IEC61850 communica - 2 fault(s), 0
------------------------------------------------------------
```

Figure 70. An SCL files Validator Tool error report.

Even if the final system configuration is established, in some cases there will still be a chance that the configured IEDs will not be able to receive the GOOSE messages that they were configured to subscribe to. The reason for this is that the GOOSE messages' description is different to what was actually described in the imported SCL files. In addition, based on the different vendors' system configuration tools, in some cases the system configuration tool will not show all the GOOSE parameters for the publisher and subscriber to match between themselves. Moreover, in some other cases the system configuration tool may not offer the modification of the GOOSE parameters (offering it only for the native IED within the SAS). In order to analyse the problem, it is necessary to use a network analyser tool (Wireshark, Ethereal, IEDScout, etc.) that has the ability to detect the network traffic based on the specific protocol. It must display the entire GOOSE structure so that a view of the specific relay GOOSE parameters can be analysed and so that the GOOSE messages can be subscribed to manually – for example, within the Vamp relays, GOOSE parameters can be entered manually based on the Vampset configuration tool.

The next step of the existing SAS configuration process is to export the final SCL file that contains all the system configuration parameters to the different proprietary IED configuration tools. Each proprietary IED configuration tool needs to update its native IEDs based upon the final system SCL file (associated with GOOSE). The reason for this is that each manufacturer has a proprietary way of linking the configuration tool with their IEDs. Moreover, they have a proprietary file format to describe their features and settings.

At the time of publishing of this thesis, interoperability has not yet reached this level (i.e., the parameter settings level). Furthermore, such proprietary parameter settings' file formats and specific means of communicating between IEDs and vendor software tool booths underlie vendors' business strategies, such that they prefer to keep a particular setting file format and they may also look to develop their own products without being constrained by the restrictions of the standard.

Another crucial issue within the system configuration process is the need to buy and install all the different manufacturers' software configuration tools and then jump from the proprietary IED configuration tools to the system configuration tool, and vice versa. In relation to this task, in some cases, it may be necessary to make backup files for the project before proceeding through the system configuration process because, if any fault within the system configuration occurs, returning to the previous configuration will not be available.

According to the previous overview of the existing SAS configuration process and the associated crucial issues deriving from the proposed full IEC 61850 standard (all the levels are standardized, including the parameter settings level), the existing SAS configuration methodology needs to be modified. The modification can be achieved by using a novel, vendor-neutral configuration tool.

3.2.3 A Vendor-Neutral System Configuration Tool

The novel, vendor-neutral system configuration tool is independent of any commercial IEDs brand. It has the ability to import SCL files from manufacturers, IEDs, systems and databases, and creates and increases the relay configuration to the system level based on the proposed full IEC 61850 standard, including the protection and feature setting level, as illustrated in Figure 71.

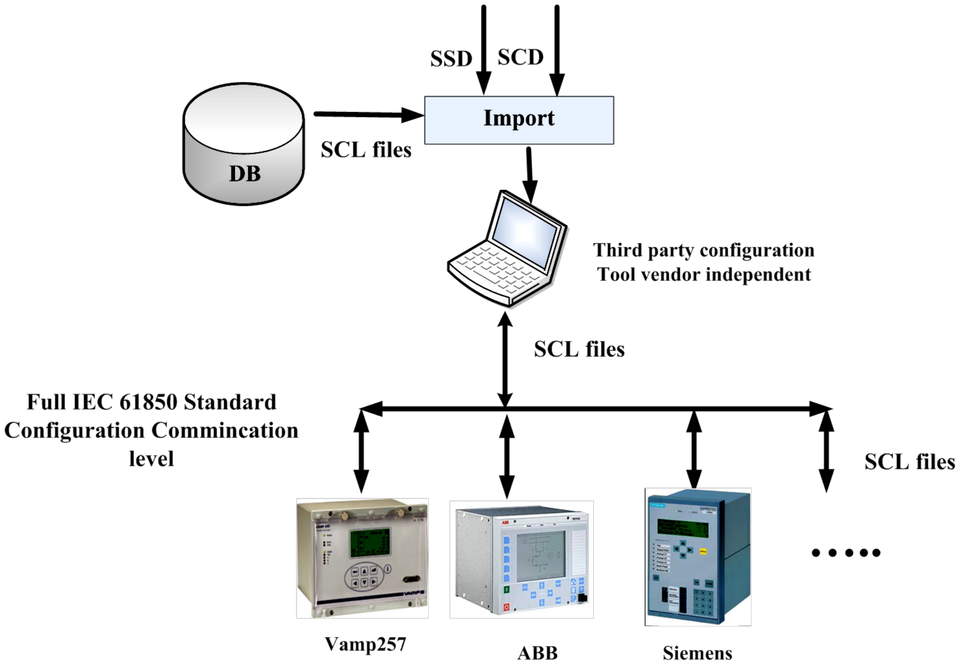
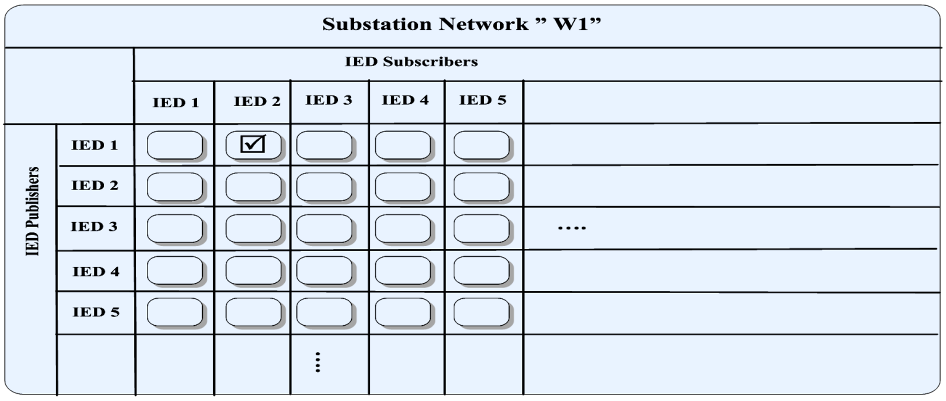

SSD
SCD
Import
DB
SCL files
Third party configuration Tool vendor independent
SCL files
Full IEC 61850 Standard Configuration Commincation level
SCL files
Vamp257
ABB
Siemens
•••••

Figure 71. A novel approach for the SAS configuration tool vendor independent.

3.2.4 The Vendor-Neutral System Configuration Tool Process

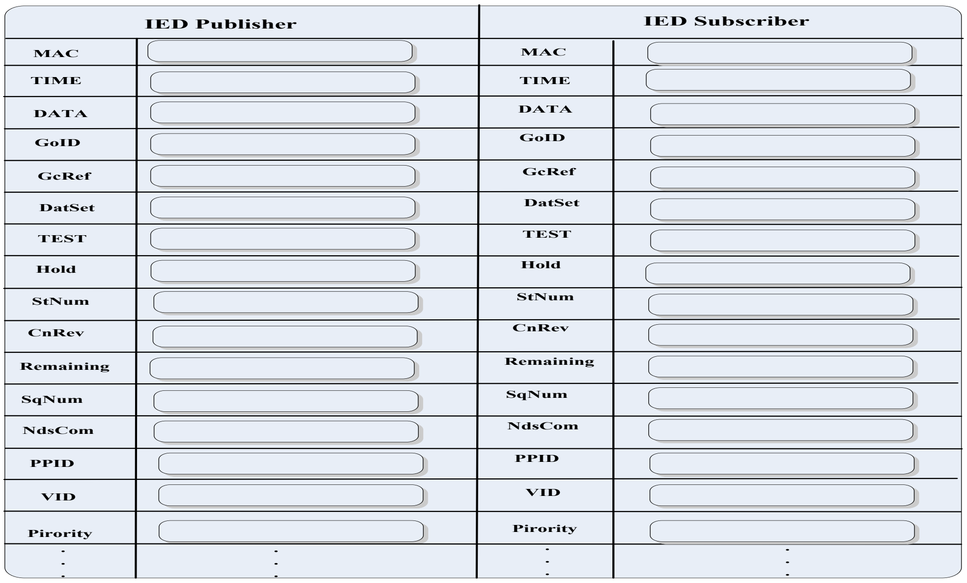
According to the proposed novel, vendor-neutral system configuration tool, Figure 72 presents the table of the SAS's participant IEDs within the sub-network "W1". The participating IEDs are listed vertically for the subscriber IEDs and horizontally for the publisher IEDs. The listed IEDs are taken from the imported SCL files (from the SCD, the SSD system files, or else by manually adding IEDs to the system based on the ICD files). As a result, when the checkbox is checked (for instance, between IED1 and IED2, as illustrated in Figure 72), another window pops out, as illustrated in Figure 73. This window, for instance, shows all the communication GOOSE parameters for the publisher (IED1) and the subscriber (IED2) based on the preprogramed GOOSE messages. Those GOOSE parameters are the most important parameters that have to be assigned to achieve smooth communication between multi-vendor IEDs. These parameters are either filled automatically upon the imported SCL file or else manually. Moreover, these parameters can be modified for the different manufacturers' IEDs based upon the proposed novel, vendor-neutral SAS configuration tool within the system level to update the entire SAS. For the last step, it has the ability to write the final SAS SCL file to the various manufacturers IEDs since, based upon the proposed full IEC 61850, all the SAS system levels are standardized; therefore, there is no need for the proprietary IED configuration tools in order to write the final system SCL to the native IEDs.



Substation Network ” W1”

		IED Subscribers					
		IED 1	IED 2	IED 3	IED 4	IED 5	
IED Publishers	IED 1	□	☑	□	□	□	
	IED 2	□	□	□	□	□	
	IED 3	□	□	□	□	□	....
	IED 4	□	□	□	□	□	
	IED 5	□	□	□	□	□	
				⋮			

Figure 72. The SAS configuration process IEDs.



IED Publisher		IED Subscriber	
MAC	□	MAC	□
TIME	□	TIME	□
DATA	□	DATA	□
GoID	□	GoID	□
GcRef	□	GcRef	□
DatSet	□	DatSet	□
TEST	□	TEST	□
Hold	□	Hold	□
StNum	□	StNum	□
CnRev	□	CnRev	□
Remaining	□	Remaining	□
SqNum	□	SqNum	□
NdsCom	□	NdsCom	□
PPID	□	PPID	□
VID	□	VID	□
Pirority	□	Pirority	□
⋮	⋮	⋮	⋮

Figure 73. The SAS configuration process GOOSE parameters.

3.2.5 Utilities Operation Enhancements Upon the Vendor-Neutral Tool

From the proposed novel, vendor-neutral system configuration tool, several bene-fits can be realized by reducing the cost and effort involved and the time taken, as follows,

- Creating a simplified system Vendor-Natural tool by raising the IED configuration to the system level which does not requires any proprietary (configuration tools and communication links).

- Offering a cost-effective solution based on reduction within the tools that can be used to configure the automation system.
- Reducing the operation and maintenance costs associated with staff training, such that interoperability and interchangeability are applicable among the technical staff.
- Reducing the operation and maintenance costs associated with the adding, to upgrading and expanding of the AS functionality (IED interchangeability).
- Implementing the Vender-Natural tool and based on the full IEC61850 standard the AS is reliable and independent of the vender and vendors' product lines.
- Allocating AS engineering tasks between different AS engineers. For instance, the protection engineer is able to focus on the design and implementation of the protection scheme rather than the underlying communication infrastructure.
- Vendor-Natural tool provides full AS interoperability including all the AS levels.

Furthermore, it can be extended to include the entire SAS events (SV, report control block, etc.), as well as the future extension of the IEC 61850 standard's functions.

3.2.6 Practical Example for Utility with Various Manufacturers Nodes

For the purpose of our discussion, let us consider a large energy company that has extensive internal multi-vendor electrical nodes. These nodes are connected within an enterprise communications network (for instance, Interconexion Electrica S.A.E.S.P., which is a Colombian energy company). The company's main product is the transmission of electricity. Table 15 describes the various manufacturers' substations in ISA.

Table 15. Various substations in ISA (MacDonald etc. 1999).

Substation	Vendor	LAN
San Marcos 230kV	Schneider	APRILNet
Primavera 230 kV	AEG	Modbus Plus
La Sierra 230 kV	AEG	Modbus Plus
Pumio 230 kV	Schneider	Ethway
San Marcos 230 kV	Automatizacion Avanzada	Ethway
Paez 230 kV	Alstom	ILSA
Sabanalarga 230kV	Schneider	LAN 7000
Fundacion 230 kV	Schneider	JBUS
Cerromatoso 230 kV	Schneider	Modbus Plus
Sochagota 230 kV	ABB	LON
Guatiguara 230 kV	ABB	LON
Chinu 500 kV	Siemens	SINEC-HI
La Virginia 230 kV	Cegelec	CONTRONET
San Marcos 500 kV	Automatizacion Avanzada	Ethway
Controlled from Sabanalarga		

The company has 10 different digital control system (DCS) solutions from six different manufacturers and, as realized in MacDonald et al. (1999), "there was a need for a change to a standardized design." Now, let us consider that the company upgrades its DCS and SAS to the existing IEC 61850 standard and links all the electrical nodes to the standard communications system network. Based on the above proposed framework, the management (operation and maintenance) centre will be filled with dozens of independent proprietary configuration tools for each manufacturer's instruments. Moreover, each manufacturer's tools and instruments will require their own staff, who will need to undergo intensive training for them. Further, any extensions or changes made in order to provide the required functionality impose complications, since they requires specific knowledge and details of each different manufacturer's particular system (tools and instruments). Therefore, one consideration can be raised such that the utilities will become dependent upon the manufacturers, since it is impossible to add and integrate IEDs or functions from other manufacturers to the existing system. This underlies the manufacturers' business strategies.

On the other hand, staff can be knowledgeable; however, such knowledge will only be about a subset of any given instruments and tools (of a specific manufacturer). Moreover, the staff themselves will be neither interoperable nor interchangeable. Therefore, the design, operation and maintenance of a large system comprises instruments and tools from different manufacturers (as anticipated for large utilities and based on the SG concept) and, given the above-mentioned example, may also require a huge staff; fault isolation may require combined efforts, coordinating among multiple proprietary system tools and providing information based on different proprietary formats. High levels of investment may be required given the needs of multiple IEDs and system configuration tools, as well as a large stock of different specific spare parts for each manufacturer's system.

From the earlier discussion, it can be noted that even if a utility has been upgraded to a standard solution (existing IEC 61850), it will still suffer from high lifecycle costs and investment needs based on the impositions of various manufacturers (staff, training, tools and various instruments and spare parts). As a result of the above discussion and given the increased demand to overcome the lack and limi-tations of existing (IED, system) configuration tools, a platform for a simple net-work vendor-neutral configuration tool had been invented which can be used to design and configure different vendors' instruments and systems. The vendor-neutral configuration tool provides an answer to a genuine end user need. Therefore, the vendor-neutral configuration tool is expected to supplant almost every vendor-proprietary configuration tool, since it provides several benefits as mentioned earlier,

3.2.7 Conclusion

The lack of an existing SAS configuration process was studied and analysed based on the cumulative experiences that have been gained from the DEMVE I-II projects, as well as the study of several previous pilots of IEC 61850 multi-vendors projects. This section presents a novel approach for a vendor-neutral SAS configuration tool. It has the ability to import SCL files from various vendors, IEDs, systems and databases, and makes and raises the relay configuration to the system level based on the full IEC 61850 standard, including the parameter and feature setting levels. Moreover, it separates out the SAS configuration tasks among different SAS configuration engineers. The vendor-neutral configuration tool provides a simple, cost-effective solution for multi-vendor (IEDs, nodes) integration. Several benefits overcome the lack and limitations of vendors' proprietary (IED, System) configuration tools, such as the reduction in the number of utilizing configuration tools, the operation and maintenance costs associated with staff training, and the interoperability and interchangeability as applicable among technical staff. Further, based on the reduction of operation and maintenance costs, the adding to and upgrading and expanding of the AS functionality is applicable, with the result that IED interchangeability can be achieved. Further, it provides AS, which has better reliability and is independent of the vendors' product lines. The vendor-neutral tool separates out the AS engineering tasks. Moreover, it provides for full AS interoperability, including all the AS levels.

3.3 Performance Evaluation of IEC 61850-9-2LE Process Bus Using OPNET

In this section from Chapter three, we discuss the modelling concepts of the IED using the OPNET modeller simulation tool. Simulation tools offer extensive and adaptable environments for the systems under study. Considering the specifications for modelling, the system simulation also facilitates the performance evaluation of the system under study. The performance evaluation of the various system topologies can be handled easily, thereby providing an initial guide to the SAS network engineers based on planning and design. Several tests were performed based on the modelled MU and IED which reflect the behaviour of the Ethernet switches within the SAS by delivering the SV traffic stream. In addition, the SV traffic stream latencies are evaluated to assess the limits and capacity of the process bus network's critical components.

3.3.1 Introduction

The growth of IEC 61850-9-2 process bus as high data-rate communications networks have increased in number has greatly improved the capability of SASs. IEC 61850-9-2 provides distributed measurements for monitoring, control and protection functions. In both industry and academia, engineers have been attempting to establish and test new approaches, taking advantage of PC-based technology to build individual test situations based on modelling and simulating systems' components. However, there are several another feasible system performance evaluation methods, such as analysis, mathematical modelling, test-bed emulating and hybrid simulation. These methods have several advantages and disadvantages - for instance, analysis and mathematical modelling can provide rapid answers to the problem being studied, but in general many of the cases are inapplicable and lack accuracy in terms of the approximation process. Moreover, it cannot reflect the real behaviour of the system, especially when it is related to the communications network issues - such as queues and protocols - in which it can be decomposed or approximated by reducing the studied model to a typical model (to re-duce the analytical difficulties). Meanwhile, test-beds involve implementing the studied case on real-world hardware on a much smaller scale which may still suffering from other real-world difficulties that may be completely irrelevant to the case in question. Moreover, the cost may be significant and unsuitable for analysing a large system (Brand & Wimmer 2008; Sethi & Hanatyshin 2013).

Given the above discussion, system simulation provides a way to model a system's behaviour and analyse the interactions between the modelled components by using discrete event simulation (DES). DES is considered as the typical method in large-scale simulation studies, providing modelling and solutions in a more accurate and realistic manner, since it reflects the real behaviour of the system under study by creating extremely detailed system networks and a packet-by-packet model of the events taking place within the network under study. As a result, this work takes the simulation approach to determine and predict the real behaviour of the process bus network by using OPNET, which is more suitable for development engineers than end users. OPNET offers an extensive and adaptable environment for the systems under study, with a wide range of support for different communications technologies and systems, starting from individual LANs to global communications system networks (satellite networks).

3.3.2 The SV Testing Methodology

According to the process bus simulation process and as the first step, we provide for the modelling of the MU, which is an IEC 61850-9-2LE-compliant device that publishes digital measuring signals (such as current and voltage) from primary SAS components' current and voltage transformers (CTs and PTs) to the bay controllers and protection IEDs within the SAS. The MU is an interface between the existing analogue primary SAS components and the new command, control and protection digital IEDs based on the IEC 61850-9-2LE for building the digital bays or else a full digital SAS. It also allows for the replacement of expensive copper cables by optical fibres. In the second step, a series of tests for the process bus network under different circumstances and based on various scenarios are implemented. These scenarios are used to illustrate and determine the real behaviour of the process bus network based on calculating the latencies of the SV packets' traffic stream through their transition from publishers to subscribers. The SV latencies have been considered as a unique critical characteristic that is a hard real-time requirement and which can be increased and decreased based on changing the network topology and traffic in the network under consideration.

Significant growth within the process bus network based on product development and several process bus SASs was commissioned. However, regardless of this growth, knowledge about the real behaviour of the process bus network especially when there is a large number of traffic resources connected within the same network - is slight. The process bus network analysis is the focus of much research by both industry and academia. Several network process bus models have been subject to testing; however their hard assumption limits their effectiveness (Amelot et al. 2011). In Sidhu and Yin (2007), they model and simulate distribution substation of 69 kV and 220 kV; however, the raw data of the SV traffic characteristics that has been used is not compliant with IEC 61850-9-2LE. In Gurbiel et al. (2009), several studies were performed based on a test bench that calculates and compares the characteristics of the SV traffic differences between the two paths direct from the MU and the source of the digital reference signal. David Ingram has done several studies that discuss the process bus's critical is-sues, such as TS, routing and process bus traffic analysis. Most of the work was done by using the GTNET card with the SV firmware to generate the MU stream and the Endace DAG7.5G4 network card to monitor the traffic. The weak point of these works is that they cannot reflect the real behaviour of the system, since they generate streaming traffic based on mathematical calculation (the number of MUs within the network multiplied by the traffic that each MU can generate every second) and then inject the generated traffic into the communications network. Accordingly, the injected traffic calculation of the behaviour of the rest of the network's components was performed (Ingram et al. 2012, 2013).

The strengths of the present work are that every node in the process bus network has been modelled using OPNET, which simulates the real physical SAS components. Moreover, the traffic that was generated by every node was compliant with the IEC 61850-9-2LE standard, and the interactions between those nodes reflected the real behaviour of the SAS, since every node was connected to the network one-by-one. Furthermore, the interactions between the connected nodes were monitored based on the measurement of the end-to-end (ETE) latencies from the publisher's and the subscriber nodes' points of view.

3.3.3 The SAS Time Critical Messages Sample Value

SVs are peer-to-peer messages which are used to deliver measured values from the switchyard to bay IEDs in digitized form within the SAS. It is a multicast message such that, within the LAN, the measured values at one location can be delivered to any number of subscribers. An individual target may require an individual sampling rate, which can be freely selected according to their needs. For instance, 80 samples per nominal period for a protection application the sample rate of which is 4 kHz/s for 50 Hz frequency in which one set of samples can be sent in a single SV packet every 250 µs, and 256 samples per nominal period for a metering application in which eight sets of samples can be sent in a single SV packet every 78,125 µs. These sample values are located in the application service data unit (ASDU), where the application protocol data unit (APDA) may consist of one or more ASDUs within the SV packet frame. According to the IEC 61850-9-2-LE, an ASDU consists of a sequence of bits that may translate to obtain the related information, such as the “tag”, “length” and “values” that may represent the actual information - for instance, svID, which is a unique SV identity. In addition, smpCnt is an SV counter that counts from 0-3999 for 4 kHz sample/s, and confRve is one the value of which increases each time that the SV parameters are reconfigured. A sample synchronization flag (smpSynch) represents the synchronization status of the SV packet frame, while a sequence of data represents the actual dataset as illustrated in Figure 74. InnATCTR1.Amp.instmag.i, in Figure 75, represents the magnitude of the instantaneous measured value of current phase one (Gurbiel etc. 2009).

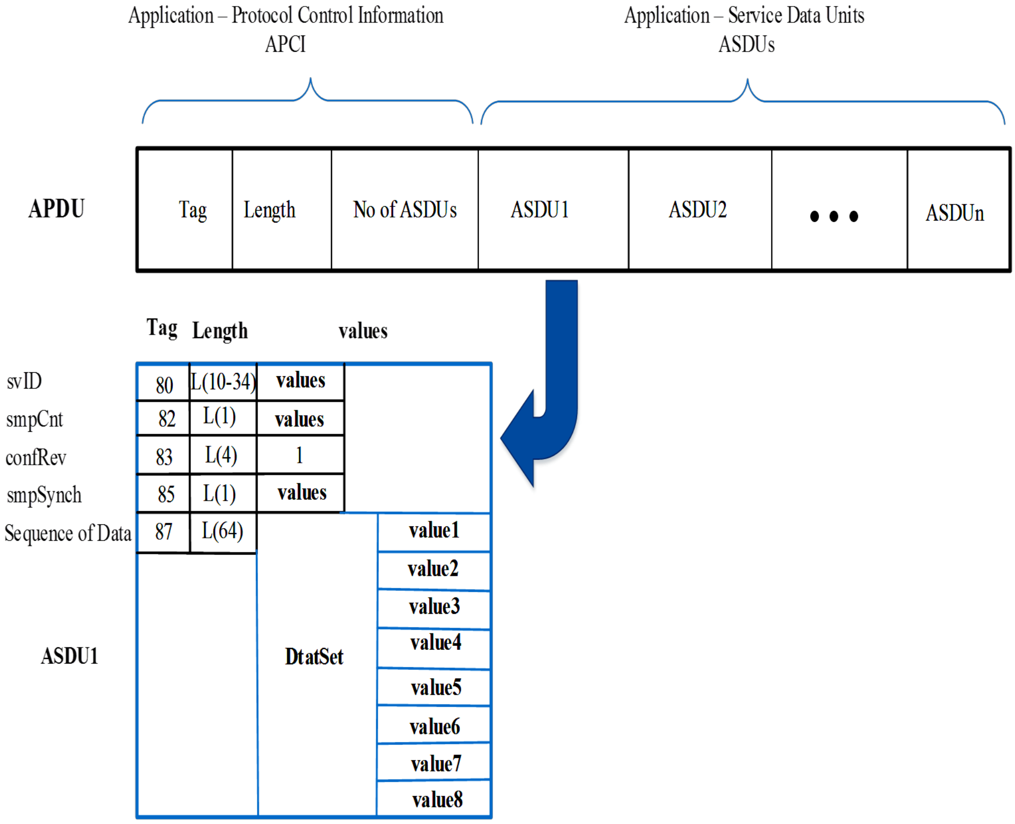


Figure 74. Packet Application Data Unit and Application Service Data Unit.

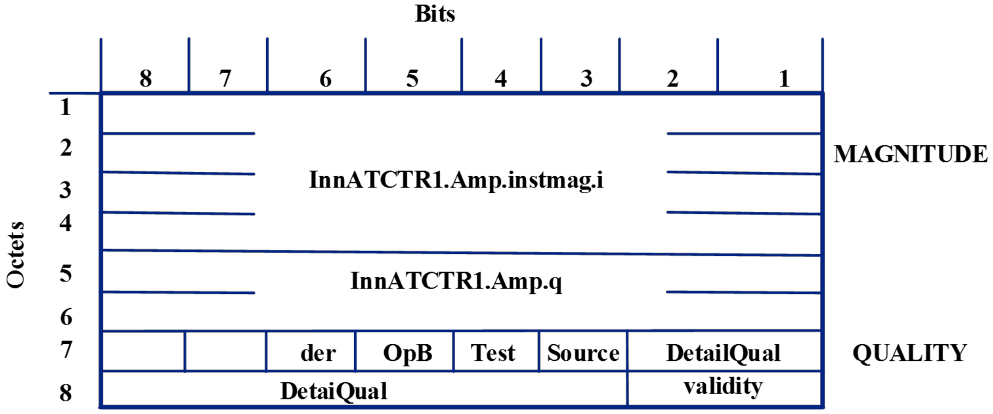


Figure 75. Magnitude and quality of SV of phase A current.

3.3.4 OPNET Simulation Tool

In order to build a simulation model that can produce results within an acceptable timeframe, the real-life system network must be simplified. The simplification of the real-life system network can be made based on the simulation goals that were identified previously. The simulation goals are to examine and predict the real behaviour of the system under testing with respect to different parameters, such as the mean delay, delay variations, traffic lost, traffic dropped, error, etc. In this work, OPNET is used to model the IEC 61850-9-2LE process bus network in a simplified way, such that different SAS components are modelled and connected in several scenarios using the OPNET modelling tools. OPNET provides several editors that facilitate and simplify modelling tasks. In this section, a description of the most commonly used editors is given as an overview. These editors are organized in a hierarchical manner, from down to up, namely a parameter editor, a process editor, a node editor and a project editor. The parameter editor (including the packet format editor) is always considered as a utility editor rather than modelling the domains by which the user could configure the modelled node parameters and traffic generation parameters, such as the MAC address, the destination address, the start time, the stop time, the inter-arrival time, the packet size, etc. Meanwhile, the OPNET process model editor is used to represent the logic flow that reflects the processors' behaviour, protocols, resources, applications, algorithms and queues' modules using a finite state machine (FSM) approach. The process model consists of a state transition diagram (STD) that is expressed in the languages Proto-C (with an extensive library of kernel procedures) and C. The graphical representation of the states and transitions describes the process steps. These state transitions accrued according to the stimulus state response. In each state, the predefined library (or the more flexible language C) can be used to identify the general logic, even linking to an external program. Figure 76 illustrates the process model for the traffic generation source module for the MU.

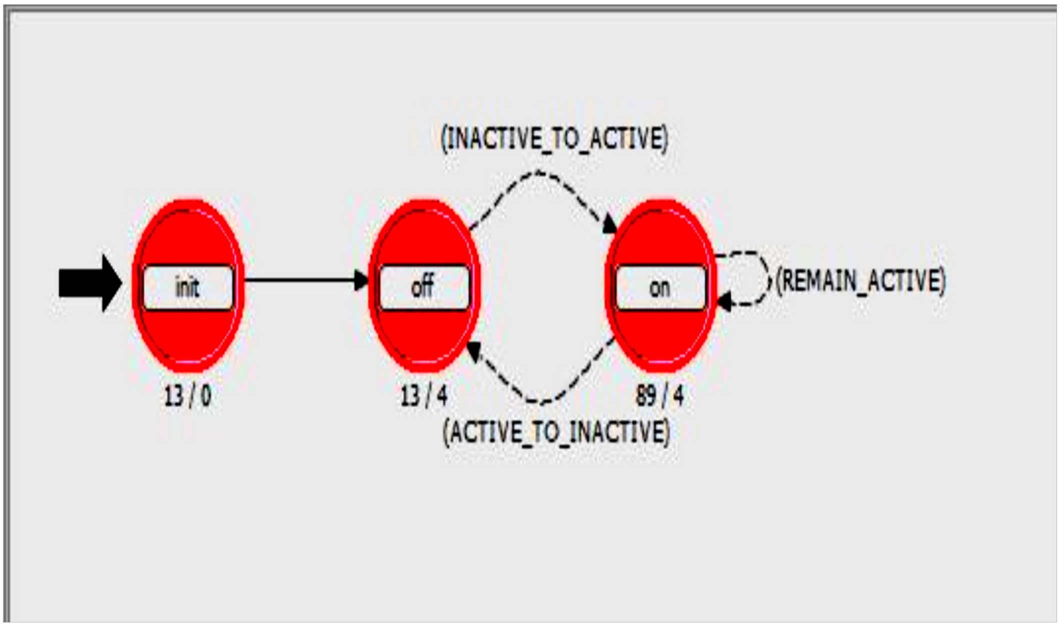


Figure 76. The OPNET process model.

The node editor was considered as a user interface tool in which a user might model a physical device and edit the internal structure of that device or node. A node model consists of several modules separated by logical functionalities. These modules might be connected through a packet stream or else be connected with static wires. Each particular node function can be represented by a particular module in which that module can be used to transmit packets, receive packets, process data, store data, route packets, etc. Figure 77 illustrates the modelled MU IED node model diagram that can be used within the process bus network to simulate the SAS. Where the Ethernet MAC node model is provided with OPNET nodes, the model library implements CSMA/CD and the retransmission mechanisms specified in the IEEE 802.3 and IEEE 802.3z standards (Lu & Yang 2011). Within the Ethernet MAC model, the following features provide for the serialization of bit transfers to and from the physical layer, namely first input first output (FIFO) processing of the transmission request, propagation delay based on the distance between the connected nodes, carrier sensing and collision detection within the physical layer, and full- and half-duplex transmission. Ethernet MAC node models were used within these work process bus network test models.

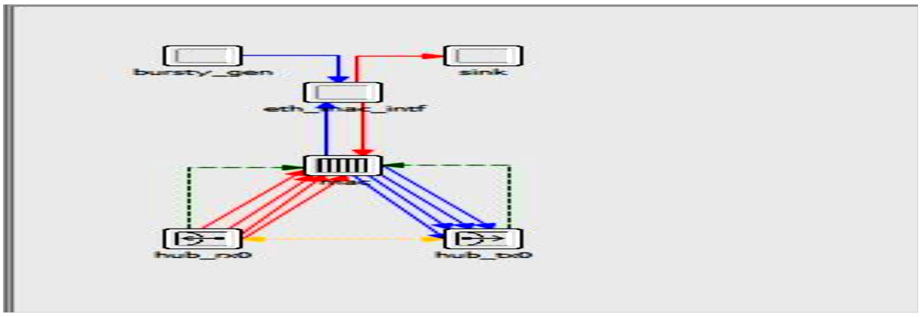


Figure 77. The OPNET node model.

Within the project editor, the system topology can be specified for the communications network under consideration as the one that might be used for every simu-lation task. In the project editor, the user can define the position and the intercon-nection of the modelled nodes that the system consists of. The network of the modelled system can be complex, since the project editor can support different kinds of nodes, such as fixed, mobile and satellite. However, complexity can be eliminated by implanting the sub-network approach, which can be arranged in a hierarchical manner. In the sub-network's lower level, this may only consist of nodes and communication links. The project editor can group all these sub-networks where the communications links facilitate communication between those sub-networks. Figure 78 illustrates the MU IED nodes in the SAS.

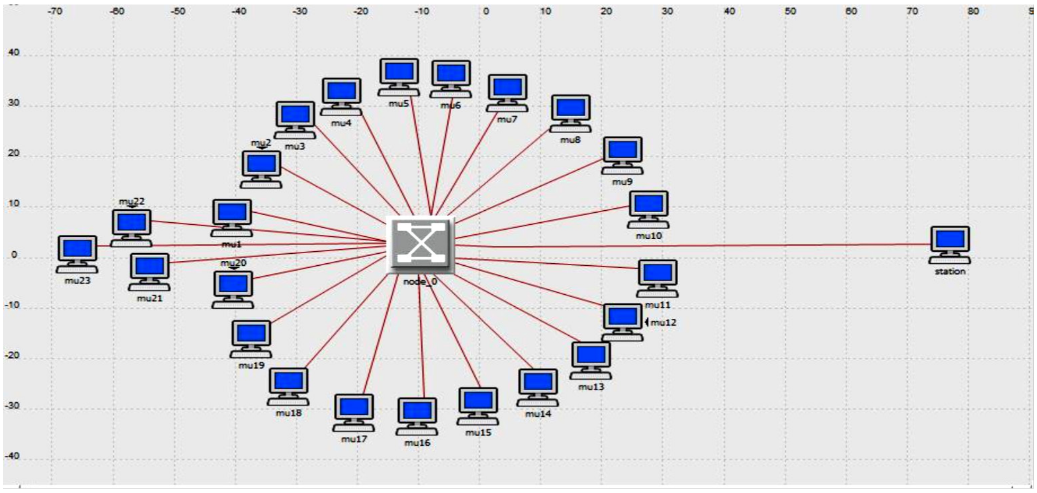


Figure 78. The OPNET project model.

3.3.5 Modeling and Simulating of the IEC 61850-9-2LE Process Bus SAS

The MU's reliability and proper functionality plays a major role within the SAS. For instance, incorrect measurements, delays and errors may lead to the incorrect resolution of protective and control IEDs, which may cause serious damage. Therefore, in this section, the SV traffic stream latency is evaluated. The purpose of this evaluation and testing is to assess the limits and capacity of the process bus network's critical components. These components include the communication links, the Ethernet switch publishing IEDs, and the subscribing IEDs. Various SAS circumstances were considered in various scenarios, such as the number of SV packets that the traffic stream may pass to reach their destination along with the associated latency experience when passing the same number of Ethernet switches. In addition, it includes the capacity of an individual process bus net-work in relation to the number of MUs that might be created and handled.

In the first scenario, and for the first step, the MU has been modelled as an SV messages' publisher and the receiving IED has been modelled to subscribe to the publishing MU's SV traffic stream, as illustrated in Figure 79. These nodes (the MU and the IED) have been used in both scenarios. A number of Ethernet switches are connected through the SAS communications network, one-by-one, in series between the MU and the receiving IED. The calculation and measurement of the SV packets' traffic stream ETE latency associated with the addition of an Ethernet switch each time that may the SV traffic experienced based on different LAN speeds of 10 Mb/s and 100 Mb/s are carried out. It is worth noting that all nodes for both scenarios are synchronous based on the assigned simulation start time and stop time.

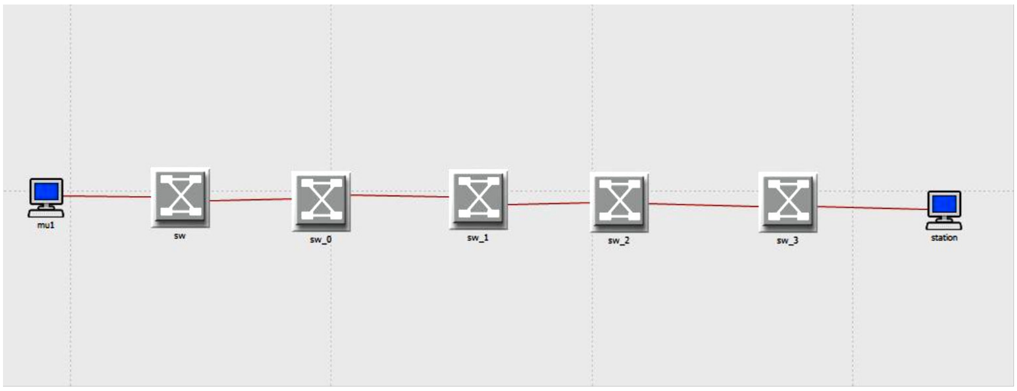


Figure 79. A large SAS consisting of five Ethernet switches.

MU SV packets are created based on IEC 61850-9-2LE such that the MU can send 4,000 packets per second as the sampling period (50 Hz and 80 samples/c) and the packet size is 126 bytes plus the header. This SV traffic was created within the custom MU modelled node in which it allows SV traffic key parameters to be assigned specifically. Priority tagging has not been considered, since there is no other traffic within the simulated process bus network. Moreover, according to the modelled Ethernet switch quality of service (QoS) parameters, it has one queue with a packet service rate of 100,000 packets/s. This scenario presents and simulates the approach of a large SAS when the SV packets need to pass more than one switch to reach their destination.

3.3.6 Numerical Results and Discussion

Within the first system project configuration, which consists of a single Ethernet switch, the SV traffic stream latency ETE was 245,534,992 µs, whereas in the second trial, when adding a second Ethernet switch to the SAS communications network, the SV packets' traffic stream latencies were increased by 110 µs. As a result, we recognized that every Ethernet switch added to the SAS communications network increases the SV traffic stream latencies by an almost-fixed amount of latency 110-120 µs. Figure 80 illustrates the latencies for five SAS configurations starting from the latencies of the SV packets' traffic stream that have passed through a single Ethernet switch in the 10 Mb/s LAN to the fifth Ethernet switches.

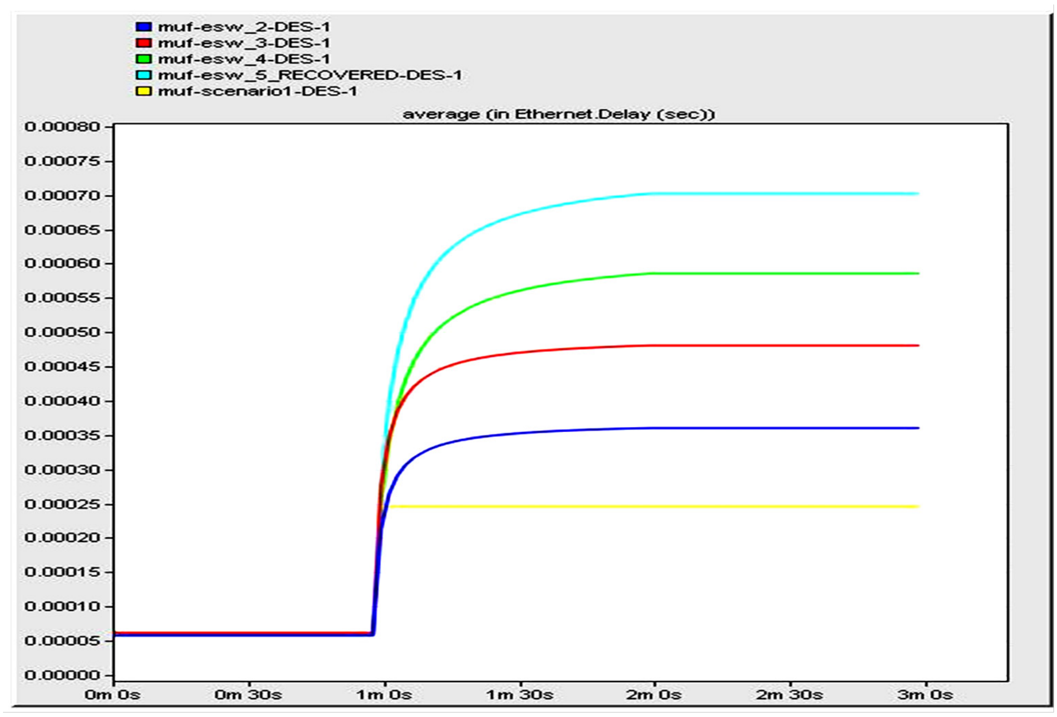


Figure 80. SV Traffic stream average latencies LAN 10Mb/s.

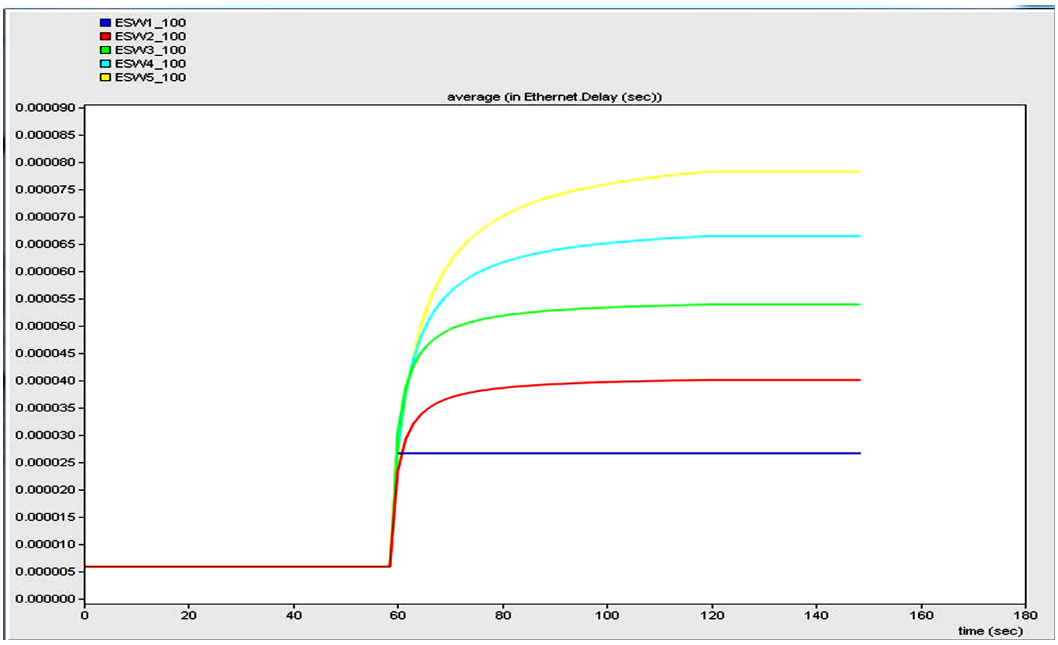


Figure 81. SV Traffic stream average latencies LAN 100Mb/s.

This result has been considered as significant since the first Ethernet switch expe-rienced more latencies than the subsequent switches based on its serialized, bunched SV packet frames, whereas the subsequent switches experienced less latency such that they could be used to connect a large SAS efficiently without significantly increasing the overall latency of the SV traffic stream. Therefore, according to Figure 80, the latest Ethernet switch increases the SV traffic stream latency to 693.8105 µs. Meanwhile, Figure 81 illustrates the latencies for five SAS configurations, starting from the latencies of the SV packets' traffic streams that have passed through a single Ethernet switch within the 100 Mb/s LAN to the fifth Ethernet switches. The latency that the SV packets' traffic stream experienced when passing the first switch was 2.6654 µs, whereas every Ethernet switch adds an almost fixed amount of latency of 11-13 µs. The latest Ethernet switch increases the SV traffic stream latency to 78,274175 µs.

3.3.7 Modeling and Simulating of the IEC 61850-9-2LE Process Bus Increasing the Number of MU within the SAS

According to the second scenario process, several modelled MUs were connected to the process bus network by increasing the number of MUs by one for each trial, as illustrated in Figure 78. The purpose of these tests was to evaluate the limits and capacity of the process bus network's crucial components, such as the communication links and the Ethernet switch. The calculation of the SV packets' traffic stream ETE latencies associated with adding MUs that may be SV packets are experienced based on different LAN speeds of 10 Mb/s and 100 Mb/s. It is worth noting that all the nodes are synchronous based on the assigned simulation start time and stop time. In the first step, where the LAN speed is 10 Mb/s, several modulated MUs were connected to the process bus network. Each test, the number of MUs within the process bus network was increased by one and calculations for the SV packets' traffic stream ETE latencies was associated with adding MUs that the SV packets may have experienced.

In the second step, where the LAN speed was 100 Mb/s, the same procedure as mentioned above in step one was repeated. Calculations for the SV packets' traffic stream ETE latencies were associated with adding MUs by which the SV packets might be experienced. These tests might reflect the real behaviour of the process bus network when the SV packets' traffic stream increases with an in-crease in the number of MUs within the SAS communications network. Moreover, it shows the capacity of the process bus network based upon the assigned speed of the LAN network as well as the process bus tolerance based on the limitation of the number of MUs that have to be connected within the individual SAS and which can be handled.

3.3.8 Numerical Results and Discussion

Under the first configuration, where the LAN speed was 10 Mb/s, the first MU was connected in the process bus network. 60,000 SV packets were created based on 15 seconds of traffic generation, where the SV packets' traffic stream latency was 250.5581 µs. This SV traffic stream latency is within the acceptable range, since the specified requirement latencies in the case of no packet losses was anticipated to be 250 µs. In contrast, by connecting two MUs, the SV traffic stream latencies increased linearly to 0.72237s in 15 seconds, as illustrated in Figure 82. The theoretical throughput that every MU can create is 4.418 Mb/s with a 50 Hz 80 sample/c and a 126 bytes frame size plus a header, which may lead the LAN communications network to reach its limits.

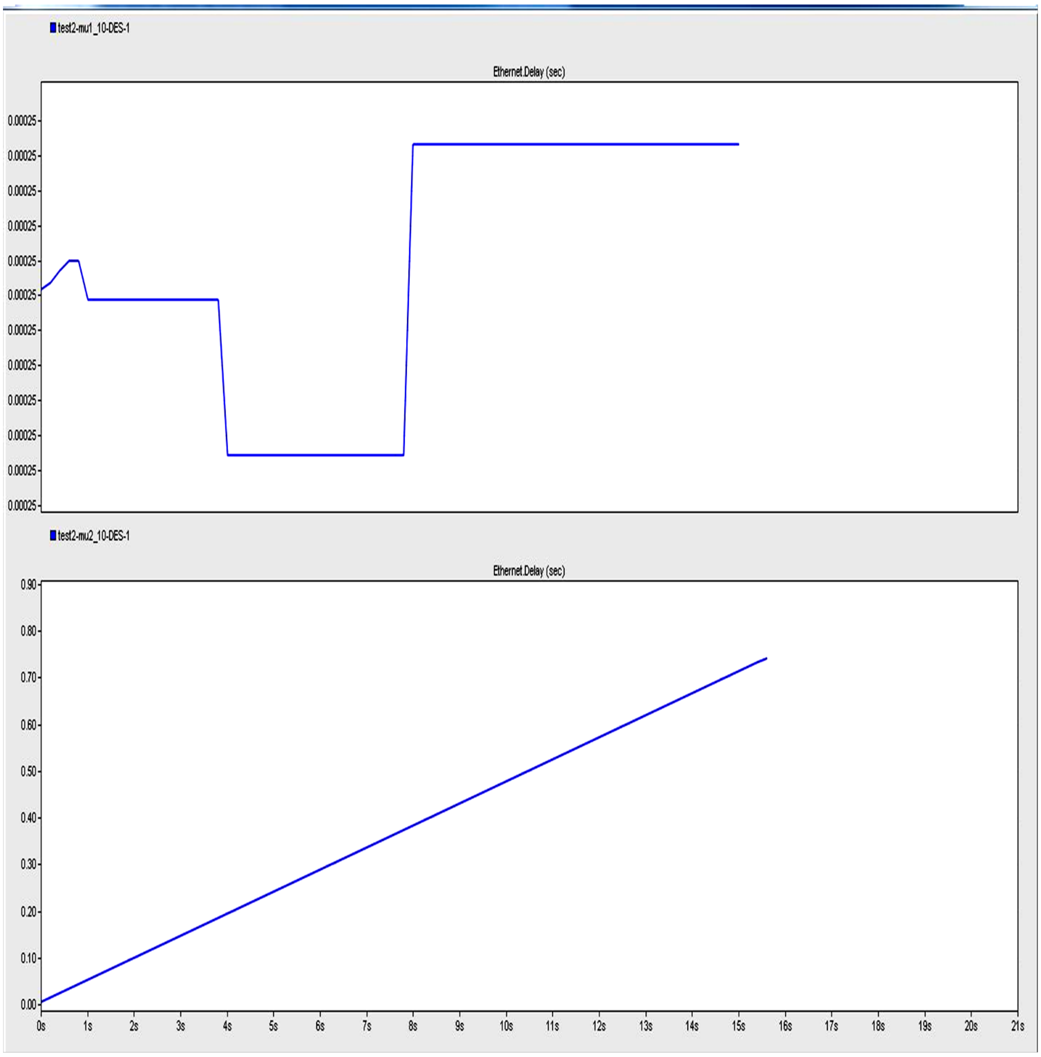


Figure 82. SV Traffic stream average latencies LAN 10Mb/s.

In the second step, with a LAN speed of 100 Mb/s, each MU generates an SV traffic stream of 4,000 packets/s. As a result, 19 MUs generate 1,140,000 packets in 15 seconds, as illustrated in Figure 83. From Figure 83, the first MU latency was 26.6613 µs whereas each MU adds an almost-fixed amount of latency to the SV traffic stream ≈ 6 µs. Further, the 19 MU increased the SV packets' latency to 144,914,583 µs, which is within the acceptable latency range of 250 µs. However, based on adding MUs 20-23, the latencies increased significantly, as illustrated in Figure 84. Table 16 tabulates the output results values which are not acceptable based on the SV limitation (the SV traffic stream without packet loss is 250 µs).

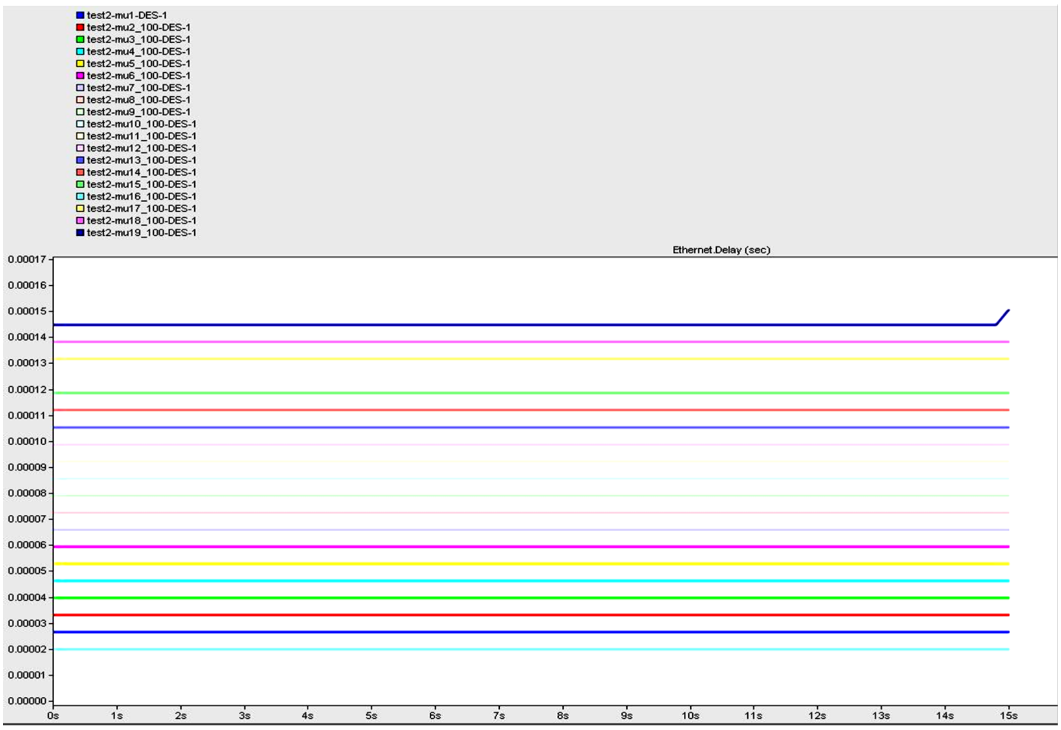


Figure 83. SV Traffic stream average latencies LAN 100Mb/s 19 MUs.

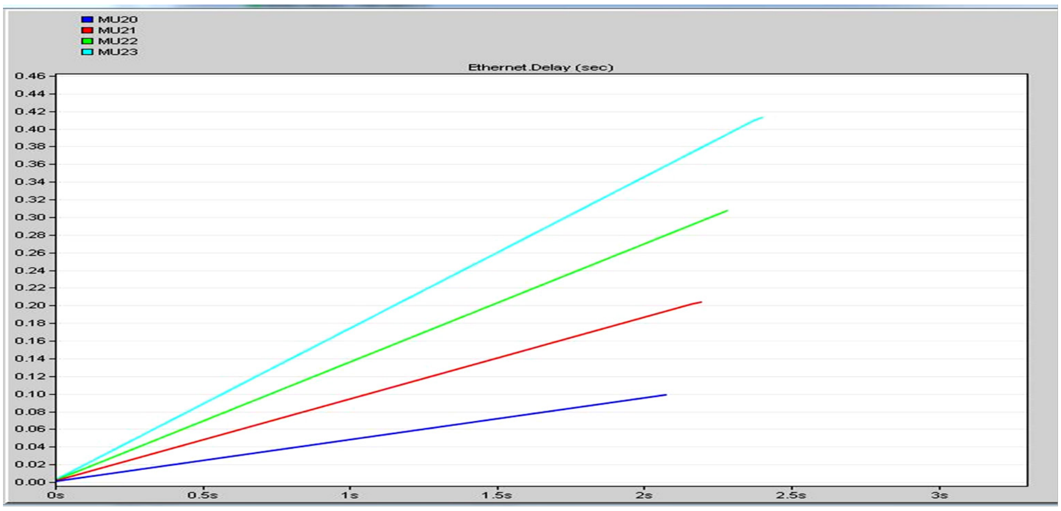


Figure 84. SV Traffic stream average latencies LAN 100Mb/s 20-23 MUs.

Table 16. MUs SV traffic stream latencies.

	MU20	*MU21*	*MU22*	*MU23*
T(s)	0.0958	0.1960	0.2712	0.3629

These latencies have been recognized and defined such that they occur upon reaching the limits of the LAN speed of 100 Mb/s, whereas the Ethernet switch still operates in a normal manner without dropping packets (23 MUs generate 184,004 packets within two seconds; the station sink destroys 184.002 packets: OPNET statistic), since it can serve SV packets based on a processing rate of 100,000 packets/s. The Ethernet queue size is 100 packets.

3.3.9 Conclusion

In future, mixed buses (process bus, station bus) promise to be seen within SAS networks since the process bus shows more reliability and flexibility for high data-rate network traffic. This can be achieved by utilizing modern technologies and network components, such as IEDs, links and Ethernet switches. In this work, the modelling of modern IEDs has been discussed in order to build an SAS process bus network and evaluate the performance of the simulated network under different circumstances using OPNET. OPNET has been proven to be an efficient simulation tool for modelling and facilitating crucial performance evaluation issues within SASs. According to the simulation of the process bus network, the unique characteristic of the SV networks is that it has hard real-time requirements, which were modelled and evaluated in several scenarios. Measurements from the modelled IEDs and several process bus network were confirmed such that the first Ethernet switch experienced more latency than the subsequent switches based on it serializing the bunched SV frames, whereas the subsequent switches experienced less latency, such that it can be used to connect a large SAS efficiently and without significantly increasing the overall latency of the SV traffic stream. Latencies were measured based on connecting several MUs in a process bus network to evaluate the limits of the capacity of the process bus network's critical components, such as the communication links and the Ethernet switch (which may facilitate design and guide engineers to build the SAS in an efficient way).

3.4 Laboratory Analysis and Methodology for Measuring IEC 61850-9-2LE Process Bus Packet Stream Latencies

In this section, we present and discuss a novel approach to estimate the sample value SV packets' stream latency within the process bus network. Moreover, it shows the successful implementation of the novel SV packets' stream latencies estimation approach based on designing a practical IEC 61850-9-2LE process bus using commercial physical devices to evaluate their performance within the de-signed SAS.

3.4.1 Introduction

IEC 61850-9-2 provides distributed measurements for monitoring, control and protection functions by using the MU. The MU has the ability to connect the analogue world to the digital world within the SAS by converting the analogue data signals that are gathered from the primary instruments' current and voltage trans-formers (CT, VT) into digitalized standard packets for subsequent transmission through the process bus LAN. It can transmit over the point-to-point-type connection to any IED or else broadcast over the LAN in a similar manner to GOOSE messages. According to IEC 61850-9-2, it specifies how SV measurements can be transmitted over the LAN, whereas IEC 61850-9-2LE (Light Edition) reduces the ambiguity of the first version and facilitates the standard implementation tasks. These improvements had been achieved by assigning the size of the datasets that need to be transmitted. Further, the sampling rates have been specified. The as-signed dataset consists of measurements for four voltages and four currents. These measurements represent the three phases' lines and a neutral line, as illustrated in Figure 85.

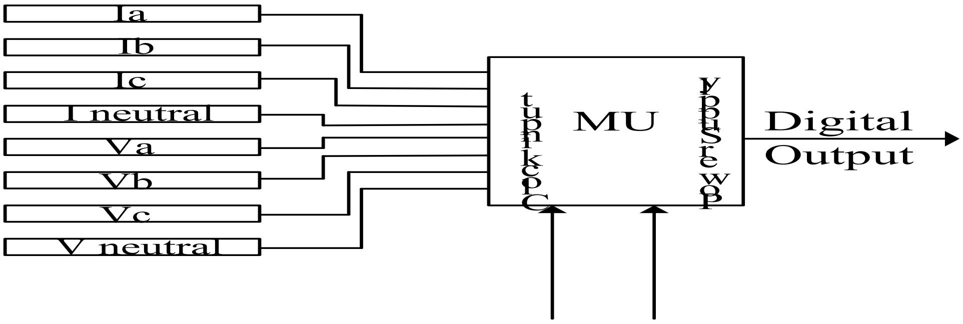


Figure 85. The merging unit concept.

3.4.2 A Novel Approach to Estimating the SV Traffic Stream Latencies

The overall estimated SV traffic stream latency comprises three different estimated latencies, as illustrated in Figure 86. As a result, the estimated SV traffic stream latency (TESV) for each packet within the process bus network can be estimated as follows;

$$T_{ESV} = T_{MU} + T_{LAN} + T_{PC} \quad (3.4)$$

where, TMU is the processing time for the MU to process (sampling, encapsulating) the data set and transmit the SV Ethernet packet to the various destinations within the process bus network. TLAN is the estimated time required for the SV packets to travel from the source to their destinations within the assigned process bus network, and TPC is the estimated time required for the received node (PC in this work) to process and present the received data.

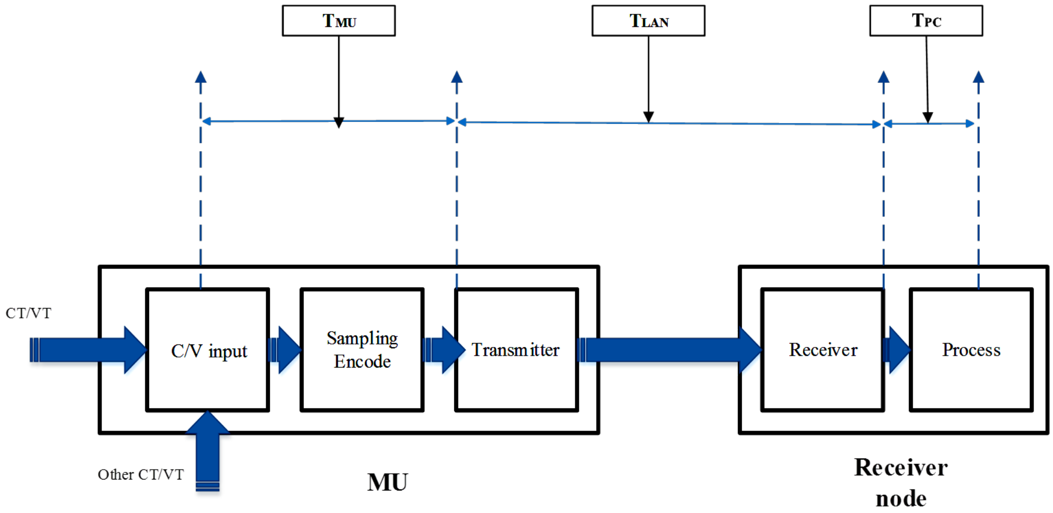


Figure 86. The SV packets latencies within the process bus network.

As a result the estimated SV packet latency TELAN for every packet within the assigned communication process bus network based on the novel latency estimation approach is such that the SV packet latency can be estimated from each of two successively received SV packets, as follows:

$$T_{ELAN} = T_{ESV2} - T_{ESV1} \tag{3.5}$$

where, TESV2 is the second successive received SV packet, and TESV1 is the first successive received SV packet.

Since T2MU1 and T1MU1 and T2PC1 and T1PC1 are expected to be constant based on the assumption that the processing time for the same length sequence of data within the same processor and within the same environment are expected to be constant (Ingram etc. 2013) this supports this assumption. Nowhere, after substituting Equation (3.4) in Equation (3.5) the estimated latency (TELAN) that is experienced by each SV packet within the process bus communications network can be estimated as follows:

$$T_{ELAN} = T_{2LAN} \;- T_{1LAN} \tag{3.6}$$

As regards the inter-arrival time between the sequences of successively published SV packets (250 µs), it is necessary to considered the calculation of the TELAN. This consideration has to be measured in the calculation in case the SV packets stream from one source, such that there is a processing time between every gener-ated packet. However, in the case where several SV packet streams are generated from one source (as in CMC356 and CMC850) this consideration does not need to be measured in the calculation between (SV2-SV1), (SV3-SV2) and (SV3-SV1). From the discussion that has been mentioned above, the SV packets' latencies within the assigned process bus communications network have been success-fully proven. Moreover, the implementation of the SV novel latencies estimation approach has been carried out based upon practical testing experiments in two further scenarios, as now follows.

3.4.3 Design and Implementation of the Process Bus Network on VAMP Merging Unit

According to the first scenario, the design and implementation of the IEC 61809-2LE process bus network was made within the DEMVE laboratory. The process bus network consists of OMICRON CMC356, VAMP MU, CMC850, CMIRIG-B, a modern intelligent Ethernet switch, media convertors, cables and a PC, as illustrated in Figure 87. VAMP MU was connected to the process bus network as the SV packets publisher, OMICRON CMC 356, and based on the Quick CMC module within the Test Universe software, it was used to inject the voltages and currents to the VAMP MU. The PC was configured to subscribe and analyse the receiving SV traffic stream packets using Wireshark to sniff the process bus net-work and define the SV packets receiving time. The CMC850 test set was used as the SV packets' streams subscriber and analyser. Based on the subscription task CMC850, it has the ability to analyse the SV traffic and define the number of received and lost SV packets. Moreover, it has the ability to read the voltage and current values that are associated with the SV packet frames based on the metering and oscilloscope view options. It is worth noting that all nodes are synchronous, based on the assigned pulse per second (PPS) signal that is generated from the CMC356 as a reference time based on its internal time-based (CMC) master clock.

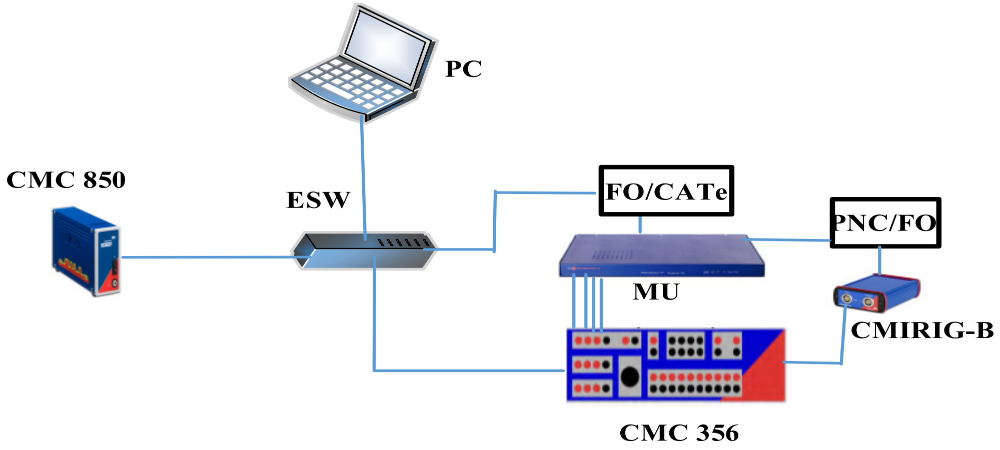


Figure 87. SV process bus design and connection diagram.

From Figure 87, the PPS signal is generated from CMC356 and connected to the CMIRIG-B interface box. CMIRIG-B enables the connection between the CMC test set and those devices that have the ability to send or receive the PPS or IRIG-B protocol signals. Moreover, it performs the level conversion between the CMC test set and the sources or receivers. The PPS signals output from the CMIRIG-B need to be converted from PNC/FO using a media convertor (an E/O convertor). A fibre optic medium has been used to connect the CMIRIG-B PPS port and the MU's PPS port. The MU is synchronized based on the CMC test set master clock. Within each PPS signal, the MU sample counter starts from 0 and goes to 3,999, which leads to a synchronous SV that is different from the MU and which also lets us know the order of sequential samples.

Testing was performed on a live SAS such that the MU provided the SV packets over 1GBASE-FX, which needed to be converted to CAT5e using a media convertor FO/CAT5e (BlackBox). The CMC356 test set was used based on the QuickCMC test module to inject the analogue three-phase voltages and currents into the VAMP MU. The VAMP MU SV output packets were recorded for four seconds, resulting in four arrival measurements.

These measurements were synchronized within the 1-PPS synchronizing signal. The VAMP MU published 4,000 SV packets every second with a packet frame length of 144 bytes. The inter-arrival between frames was 250 µs, resulting in 16,000 SV packet measurements. The SV packets' arrival measurements were recorded using Wireshark, which has the ability to filter the network traffic. As such, the SV packets' traffic stream was captured and exported to MATLAB. Within the MATLAB environment, code was written to analyse the recorded measurements.

From Equation (3.6), calculations based on the novel approach to find the estimated latency TELAN were applied to each SV packet within the designed SAS process bus network. Figure 88 illustrates the TELAN for the 16,000 MU VAMP SV packet frames. Every packet experienced a different latency based on the process bus communications network, which is normal since every packet is sent independently. These TELAN are within the acceptable range, since the maximum requirement latency was 250 µs. The mean and standard deviation of the TELAN for the captured frames were (mean = 2.50033 µs) and (σ = 6.30073*10^-6). Moreover, in Figure 89 the TELAN for the SV-captured frames was filtered based on smpCnt = 0-3999 and was averaged to illustrate the behaviour of the SAS process bus network, whereby the SV traffic stream latencies were shown every second.

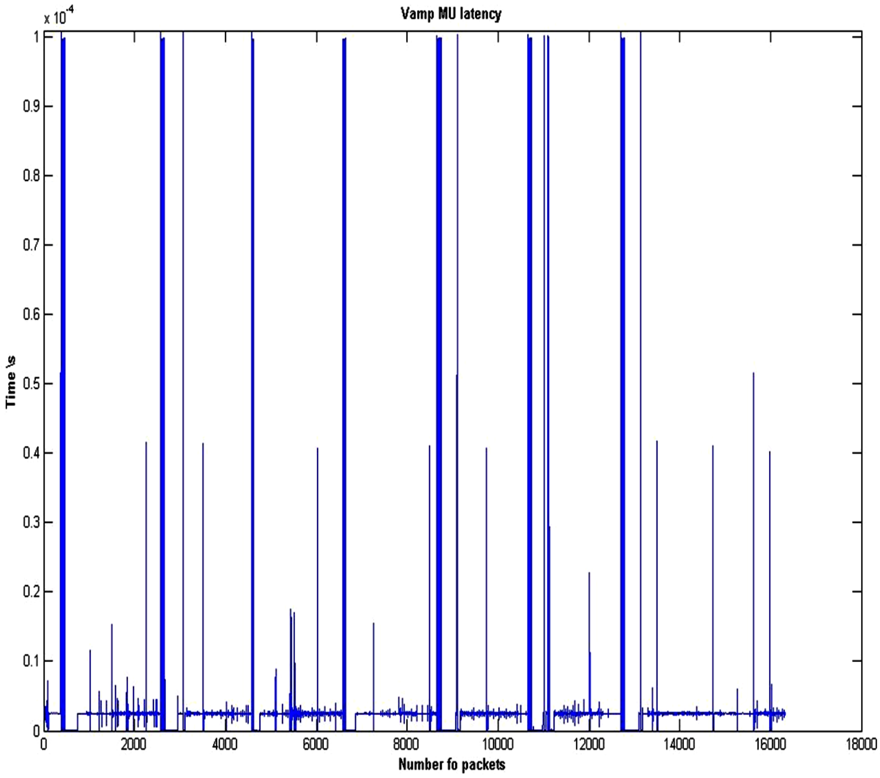


Figure 88. VAMP MU SV packets latency for 16000 packets.

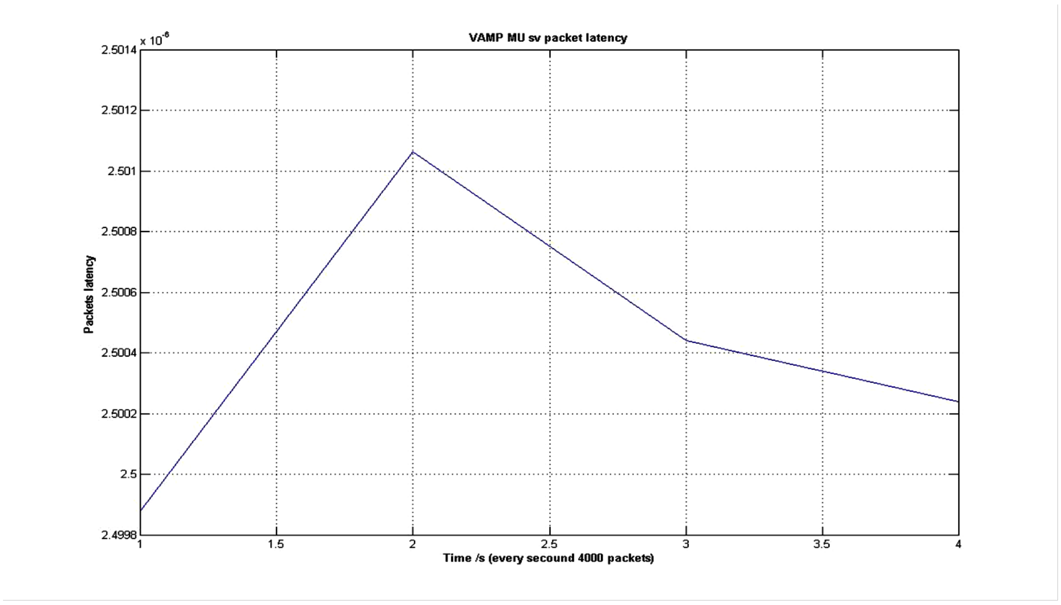
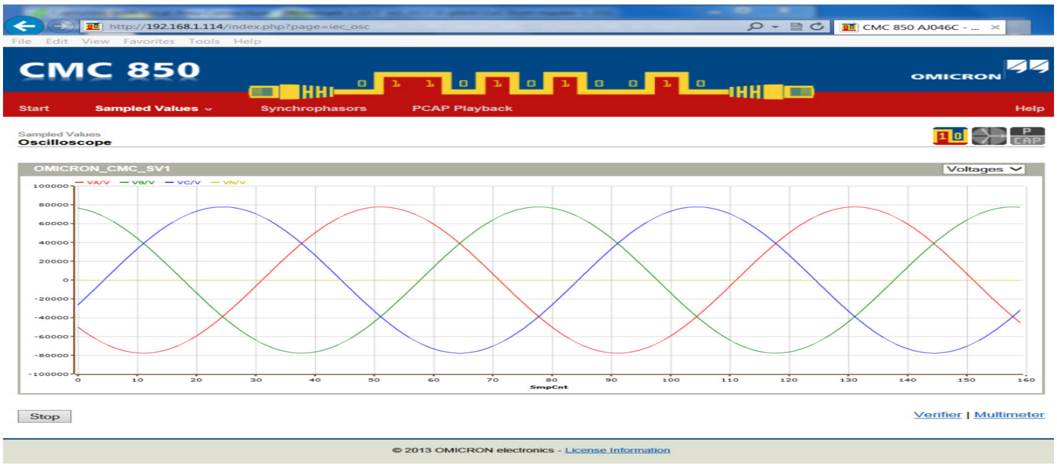


Figure 89. VAMP MU SV packets latency filtered and averaged.

Concerning the second scenario employing OMICRON and CMC356 and based on the SV module, the Test Universe software was used as the MU SV publisher. The QuickCMC module in the Test Universe software was used to inject the voltages and currents, such that the SV module needs to publish their values within the SV packets stream. The PC was configured to subscribe and analyse the receiving SV packets using Wireshark to sniff the SAS process bus network and define the SV packets' receiving time. CMC850 was used as the SV subscriber and analyser, as illustrated in Figure 90. All the nodes were synchronized as in scenario one. In the case of using the CMC test set as the SV publisher, there is no need for the media convertor since the CMC test set provides their SV packets over the RJ45 ETH1 or ETH2 ports.


http://192.168.1.114/index.php?page=iec_osc

CMC 850 AJ046C - ...

Figure 90. The Test set CMC850 subscriber and SV traffic analyzer.

Testing was performed in a live substation and the CMC356 test set was used to publish the SV traffic stream. The SV output packets were recorded for eight seconds, resulting in eight arrival measurements. These measurements were synchronized to the 1-PPS synchronizing signal. The CMC356 published 4,000 SV packets every second with a packet-frame length of 127 bytes. The inter-arrival between frames is 250 µs, resulting in 32,000 SV packet measurements. The SV packets' arrival measurements were recorded using Wireshark, which has the ability to filter the network traffic. As regards the SV traffic stream, this was captured and exported to MATLAB. Within the MATLAB environment, an analysis was made and calculations were performed for the recorded measurements to find the actual estimated latency of the TELAN experienced by every SV packet within the process bus network. Figure 91 illustrates the TELAN for the 32,000 SV packet frames. Every packet experienced a different latency based on the process bus communications network, which is usual since every packet is sent independently. These TELAN are within the acceptable range, as mentioned earlier. The mean and standard deviation of the TELAN for the captured frames were (mean = 2.49700 µs) and (σ = 0.725500*10^(-6)). Moreover, in Figure 92, the TELAN for the captured frame was filtered based on smpCnt = 0-3999 and averaged to illustrate the behaviour of the process bus network such that the SV traffic stream latencies were shown every second.

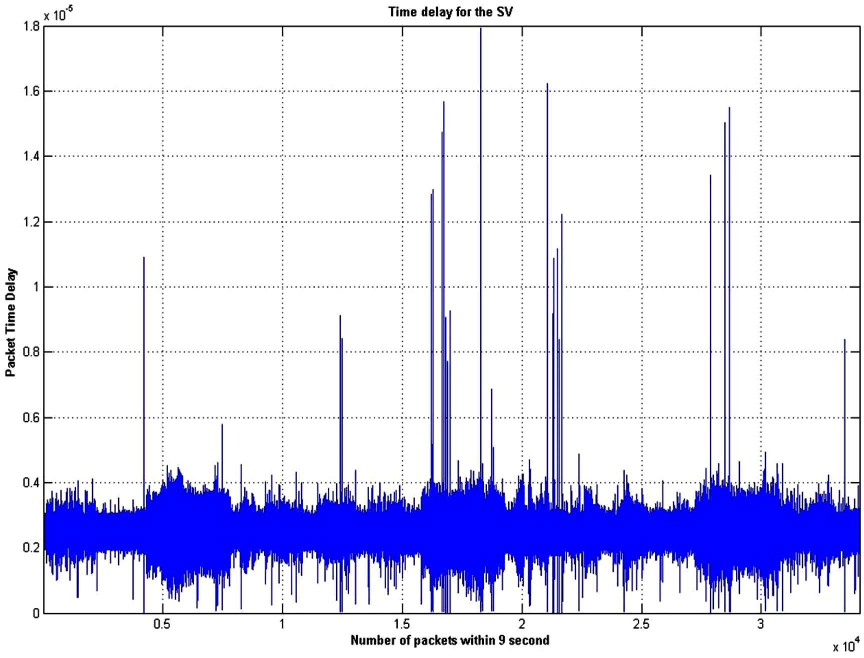


Figure 91. CMC356 SV packets latencies.

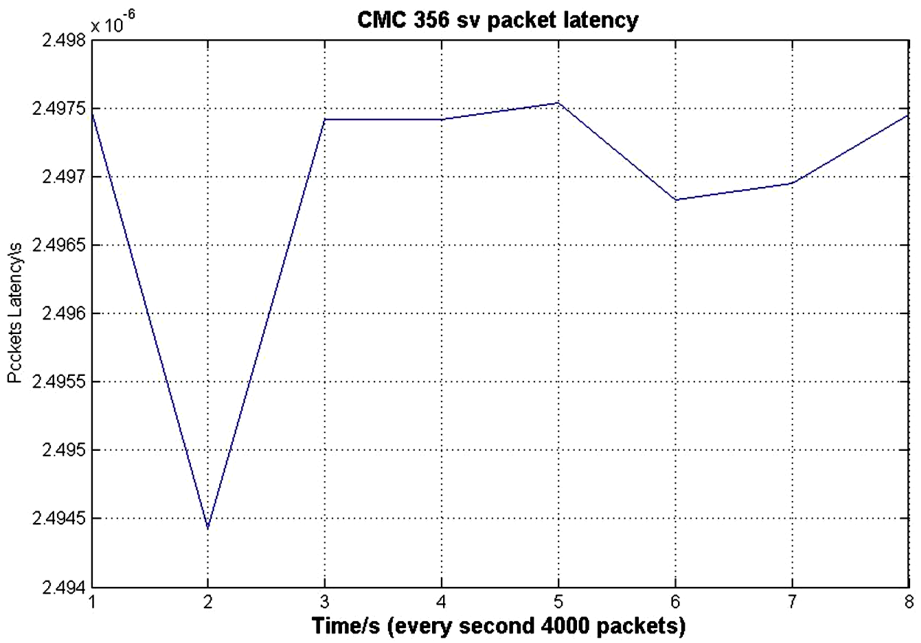


Figure 92. CMC 356 SV packets filtered and averaged**.**

3.4.4 Design and Implementation of the Process Bus Network Based on the CMC356, CMC850 and VAMP SVs

In this section, testing was performed on a live substation, as illustrated in Figure 87, such that five SV traffic streams were generated from the CMCs test sets and the Vamp MU, as follows: three SVs from the CMC850, one SV from CMC356, and one from Vamp MU, as before and according to the above-mentioned scenarios. Figure 93 illustrates the TELAN for the SVs' captured frames and was filtered based on smpCnt = 0-3999 and was averaged to illustrate the behaviour of the process bus network such that the SV traffic stream latencies were shown every second. The mean and standard deviation of the SV traffic stream latencies has been tabulated in Table 17. From Table 17, the mean latency that was added by each MU is ≈ 9.96 µs, which is almost the same as the result from the simulation model (≈ 6-9 µs).

The small differences that may appear between the two output results values were based upon the simulation made in the PC environment, in which that means the generated SVs packets even they are from different simulated MUs, however, the processing time to generate these SV packets is the same for every MU. In contrast, from a practical experiments point of view, every generated MU

SV packet stream was generated from a different source, such that the SV packet streams were related to the processing time and were characteristic of each generated source. Moreover, the standard assigned an SV packet length of 126 bytes plus the header; however, the SV packet generated from the CMC instruments was 127 bytes in length and the SV packet length that was generated from Vamp MU was 144 bytes. These differences in the SV packets' lengths are strongly related to the differences in the SV latency results, since the latencies are directly proportional to the packet length.

Table 17. The Mean and standard deviation of the SV packet streams.

	SV1	*SV2*	*SV3*	*SV4*	*SV5*
Mean (μs)	229	236	249	256	269
STD	1.53×10^{-6}	0.746×10^{-6}	0.10×10^{-6}	1.065×10^{-6}	1.574×10^{-6}

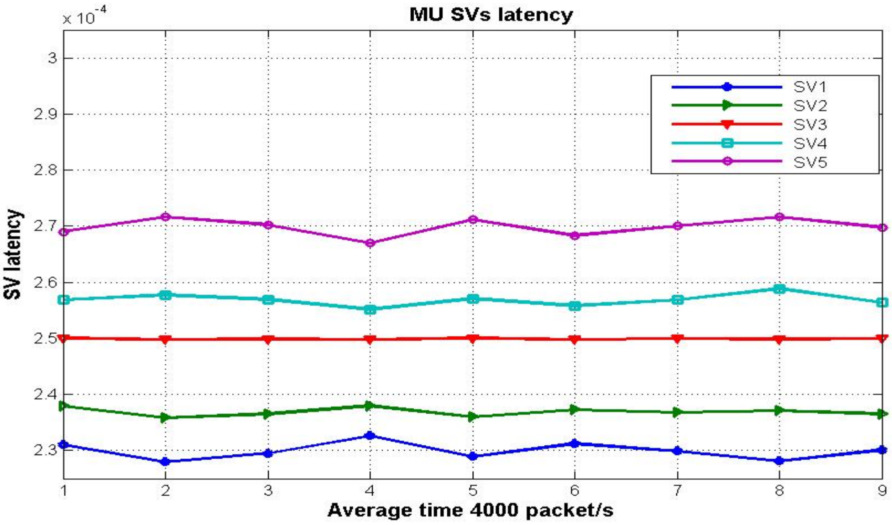


Figure 93. Filtered and averaged SV packets stream latencies.

3.4.5 Comparative Evaluation of practical and Simulation SV Traffic Streaming Latencies Results within Process Bus Network IEC 61850-9-2LE

In this section, comparisons between the output results values of the performance testing of the practical (i.e., using commercial physical devices) prototype SAS process bus network and the simulated SAS process bus model based on OPNET are carried out. These comparisons show that there are small differences between the output results values of both experiments, as mentioned above. By implement-ing the comparison, two benefits were achieved from the practical experiments point of view, thereby proving the correctness of the design and the implementa-tion of the IEC 61850-9-2LE process bus as well as the novel time analysis of the SV traffic stream latency. From the OPNET simulation models point of view, it shows the correctness of the IEC 61850-9-2LE process bus modelling as well as the power of the OPNET simulation tools (which can model a high data-rate, real-time system based on the new standard IEC 61850-9-2LE). Within the work, cer-tain technical issues are confronted, such as that there are not enough SV re-sources to assess the limitations of the process bus network based on the number of MUs that can connect within the SAS. In addition, within the Wireshark environment, although the recorded traffic can be filtered based on the source address and destination address, etc., the calculation (for instance, the packet latency based on the previously received packet) is implemented upon the all received packets rather than upon the filtered received packets view. Therefore, MATLAB code was written to analyse, calculate and draw the SVs' traffic stream latencies.

3.4.6 Conclusion

In this section, from Chapter 3 , we present a novel approach to estimate the SVs' packets' stream latencies within the SAS LAN based on IEC 61850-9-2LE by means of implementing various simulations and practical laboratory tests. Testing is an important issue for the SAS process bus on IEC 61850-9-2LE in view of highlighting the capability of the process bus network and ensuring that the SVs' packets' latencies are within the acceptable range before the full-scope integration of the SAS in reaching "plug and play" solutions. During the laboratory testing, advanced hardware and software configuration tools are demonstrated and used. The obtained output results values show that the successful implementation of the novel SV packets' latencies estimation approach is based on designing a practical SAS IEC 61850-9-2LE process bus using commercial physical devices. Furthermore, it proves that the SV packet frames are compliant with the IEC 61850-9-2-LE criteria and that the average SV packet latencies are within an acceptable range where no loss occurs. Lastly, the comparative evaluation of the practical and simulation SVs' traffic streaming latency output results values was carried out. The obtained results show that, by implementing the comparison, two benefits are achieved. From the practical experiments point of view, it proves the correctness of the design and the implementation of the IEC 61850-9-2LE process bus as well as the novel time analysis of the SV packets' stream latencies.

From the OPNET simulation, and from a modelling point of view, it shows the correctness of IEC 61850-9-2LE process bus modelling as well as the power of the OPNET simulation tools (which can model a high data-rate, real-time system based on the new standard IEC 61850-9-2L). Moreover, the work illustrates that the latencies of the practical and simulation SVs' packets' streaming output results values are almost the same, as well as explaining the reasons for the small differences that may appear between them.

3.5 Conclusions

In this chapter, the design and discussion of various practical testing experiments for IEC 61850, GOOSE and SV messages were carried out. Firstly, the analysis and methodology for the measurement and calculation of the high-speed GOOSE messages' latencies within the multi-vendor SAS communications network were presented. The obtained output results values demonstrated the successful measurement and calculation of the timed response GOOSE messages for the DUTs based on the proposed round-trip approach. Furthermore, it showed that the DUTs are compliant with the IEC 61850 criteria. Moreover, it proved the interoperability concept that the DUTs subscribe to, namely the GOOSE messages from the third-party IED. Secondly, a novel approach for the vendor-independent SAS configuration tool (which has the ability to import different SCL files) was proposed.

The vendor-neutral configuration tool provides a simple, cost-effective solution for multi-vendor (i.e., IEDs, nodes) integration by which several benefits can be achieved, such as a reduction in the number of configuration tools utilized, a reduction in the operational and maintenance costs associated with staff training, and the implementation of interoperability and interchangeability applicable to technical staff, showing that adding, upgrading and expanding SAS functionality is applicable, with the result that IED interchangeability can be achieved. Thirdly, the modelling of the modern IEDs was presented and discussed so as to build the SAS process bus network and evaluate the performance of the simulated network under different circumstances using OPNET.

Lastly, the novel approach to estimate the SVs' packets' stream latencies in SAS process bus network based upon IEC 61850-9-2LE was proposed. The proposed approach was implemented within various practical laboratory tests. Further, the comparative evaluation of practical and simulation SV traffic streaming latencies' results values was carried out. The obtained results show that, by implementing the comparison, two benefits are achieved. From the practical experiments point of view, it proves the correctness of the design and implementation of the IEC 61850-9-2LE process bus and the novel time analysis of the SV traffic stream latency. From the OPNET simulation modelling point of view, it shows the appropriateness of the IEC 61850-9-2LE process bus modelling. In addition, an explanation for the small differences upon the comparative evaluation of the output results values was given.

4 COMMUNICATION SYSTEM FOR SMART GRID

4.1 Spectrum Sensing Techniques for Smart grid Communication System

In this Chapter, alternative novel framework for the communication system network within the smart grid has been proposed. The novelty of the proposed communication model attempts to bring about a reasonable change in smart grid communication network infrastructure with the introduction of Cognitive Radio (CR) technology. Moreover, the alternative novel framework has many advantages such as providing a cost-effective solution, increase reliability, availability of the smart grid and reducing scarcity of the available resources by implementing of the most powerful sensing method (cyclostationary) within CR in which that has been described based on various simulation scenarios.

4.1.1 Introduction

The emerging concept of SG sets completely new requirements for the electricity distribution and production automation. Distributed production requires distributed automation, which in turn requires advanced communication solutions to operate reliably. On the same time, there is a common global tendency in the legislation to tighten the company's responsibilities in the case of reduce resource consumption and emission, while improve power quality. These issues put great demands and lead to emerge the new wireless communication technologies within the SG concept to enhance the reliability and flexibility of the energy systems. Where, wireless communications based CR not just provides valuable advantages over wired, it also enhanced the spectrum utilization.

There are several reasons that we need to migrate to SG. As existing communication and information system infrastructure for power grid today, lack coordination among various operational entities. According to the existing infrastructure, various subsystems are separated. Data and information sharing is limited, which is usually the case of slow, delayed restoration. In addition, it was highly focused on vertical communications between control center and individual substation for local remote monitoring and data acquisition (Xie etc. 2002).

To overcome these drawbacks and improve the energy system service quality, emphasis has been placed upon the development of the SG communication system network. SG communication system network is consisted from a communication media and the assigned communication protocols, for instance, standardization effort brought by IEC 61850 communication protocols that have a mark shift improvement within the interoperability scenario. Communication system network within the SG must be robust enough to address the enhancement in energy system efficiency as well as reliability and quality of power distribution.

4.1.2 Cognitive Radio Technology for SG Communication System

In concern about the limitations of the existing energy systems communication technologies, and according to the SG structure where most of distribute automation system and (DASs) and distributed energy resources (DERs) are scattered randomly and located within the rural areas, wireless communications are the most feasible solution. Since, most of the available communication technologies infrastructures are not existed in these areas.

Technical issues arise based on implementing of the wireless technologies due to the fact that these technologies occupy the same spectrum with the licensed users. Since the licensed spectrums permit transmission over a higher power and cover a wide area which is suitable for rural area requirements (Gungor & Lambert 2006). Therefore, the typical way of utilizing the licensed spectrums is by using the CR approach as proposed in this thesis to minimize the cost, overcome the restriction of utilizing the licensed spectrum. Moreover, communication system network upon CR technology increases the reliability, availability of the power supply, reduce outages and offering a fast outage detection and restoration with the help of bidirectional communication, since DAS networks had almost negligible outage detection mechanism. In addition, wireless communication technologies contribute in increasing the communication redundancy as using these technologies as redundant communication system networks.

In this chapter, the proposed SG communication system network can be divided into two levels higher-level and lower-level. Regardless to the lower-level communication system technologies (wired, wireless). Wireless communication system network based on CR technology has been used within the higher level. This proposed communication system network provides a full bidirectional communication system among the smart grid nodes as illustrated in Figure 94.

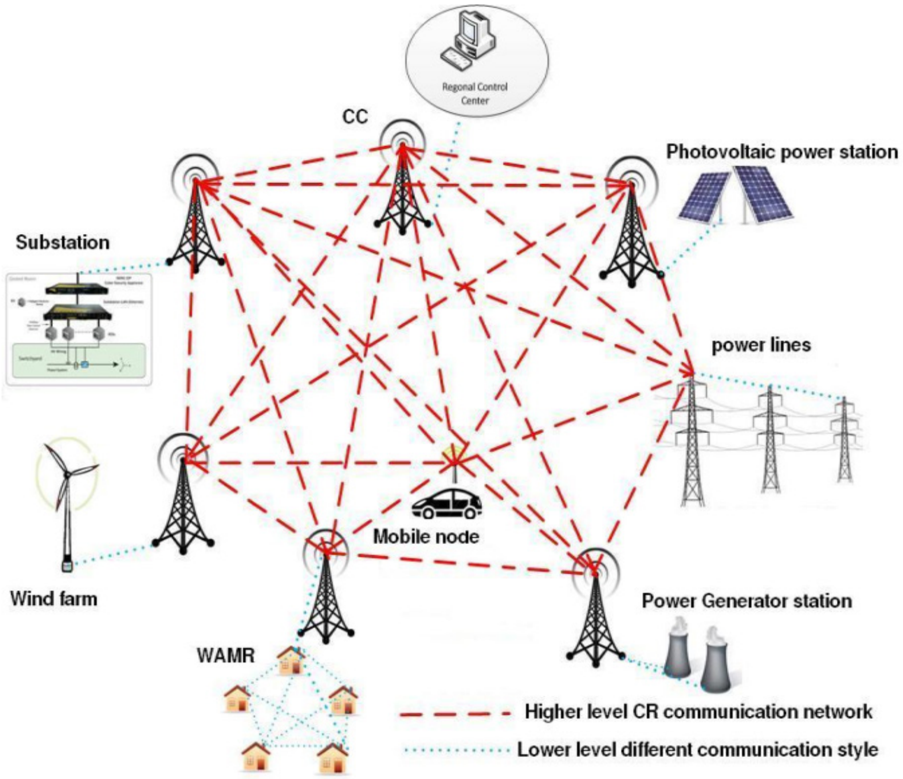

Regonal Control Center
CC
Photovoltaic power station
Substation
power lines
Wind farm
Mobile node
Power Generator station
WAMR
Higher level CR communication network
Lower level different communication style

Figure 94. CR in Smart-Grid communication system network

According to Figure 94 the higher-level communication system enables sharing the information among all the smart grid nodes. In case of disturbance or failure in one node, immediate actions need to be taken in order to substitute the failure node and limit the cascaded phenomenon in which that increase the reliability and availability of the power systems and enhanced the quality of service for the SG.

4.1.3 Cognitive Radio Approach

CR is the novel technology that significantly extends the user support functionality by makes the software functionality available for various classes of adaptivity. It is intelligent as much as it can select the best and lowest-cost service for radio transmission. For instance, in case the control center, want to send data to DASs and there are several communication system networks available within the SG for use upon the redundant communication system network concept, CR automatically selects the reliable and lowest-cost network based on identifying the available network characteristics and learning from the previous state. Moreover, it can predict about the current transmission status or soon available other resources. As a result, CR can be defined as, the smart radio that able to sense the outer environment, learn from past events and attempt to specify a smart decision to adapt the operation parameters upon the available environment vision (Mekkanen 2010). From CR definition, two main features are arisen. These features can be illustrated as cognitive capability and reconfigurability in which that simply implemented in software supported by Software Defined Radio (SDR) development. Cognitive capability refers to the ability to continuously sense, extracting information from the radio environment to independently specify the occupancy of the licensed spectrum by the licensed users, through this process. Reconfigurability, exhibit software control of the radio gives an advantage to an individual system to operate over multiple assigned configurations. This functionality offers flexibility upon operation over various modulation techniques that meet the best user communication demands supported by its hardware design. As regards, the fundamental issue of cognitive radio is to get an unutilized spectrum in certain time and specific location through cognitive capability and reconfigurability as illustrated in Figure 95 and make it available for unlicensed users by two concepts. First, since not all the licensed spectrums are utilized all the time in every location CR search for those targets which are referred as spectrum holes or white spaces. In case of suddenly licensed user claim the assigned band CR move to another spectrum hole if it is possible or searching for other opportunities. Second, the cognitive user shares the same spectrum band and adapting the transmission parameters in concentrate and to be sure there is no harmful interference provided to the active licensed users. In general we can capsulate the CR primary tasks in the three main tasks as fallows. First task, radio scene analysis (RSA), which includes, estimates of interference, detects spectrum holes and predicts modelling for the state. Second task, channel identification, which enhanced spectral utilization and third task, dynamic spectrum management (DSM) and transmit power control (TPC).This DSM can be seen when cognitive radio attempts to access the white space or when CR shares the licensed bands with the licensed users by adapting its transmission parameters upon the receiver environment observation, feedback stimulis.

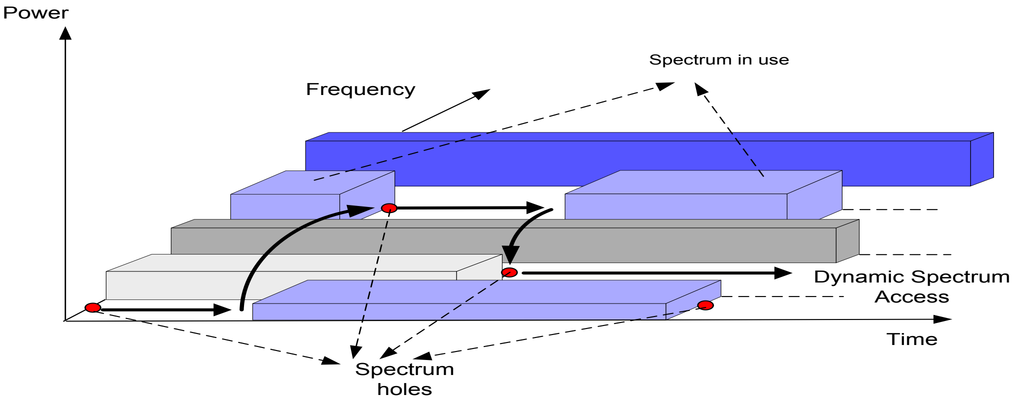


Figure 95. CR concept

4.1.4 Spectrum Sensing Method

Manmade signals such as, telemetry, radar, sonar system and communication signals exhibit periodicity. Typically, periodicity can be introduced in the signal parameters such as phase of the sinusoidal carrier signal, time pulses, or direction of arriving, kind of modulation and coding, etc. These underlying periodicities can be used to detect and identify the licensed user signals in case of a noisy environment and other modulating signals. Therefore, modulating signals are characterized as a cyclostationay in condition that the mean and autocorrelation are periodic. Since most modulated signals are constructed from information data, which is random, time varying stationary process and sinusoidal carrier wave that is deterministic and predictable. The final modulated signal is neither stationary nor deterministic, it is cyclostationary upon the underling periodicity. From the cyclostationary signal processing perspectives, which are characterized by mean and autocorrelation function that are periodic in time, the mean and autocorrelation are implemented to achieve a spectral correlation function (SCF). The SCF of the cyclostationary signals provides a highly rich frequency domain that can be used to implement the sensing task, by detecting a unique cyclic frequency of different modulated signals as illustrated in Figure 96.

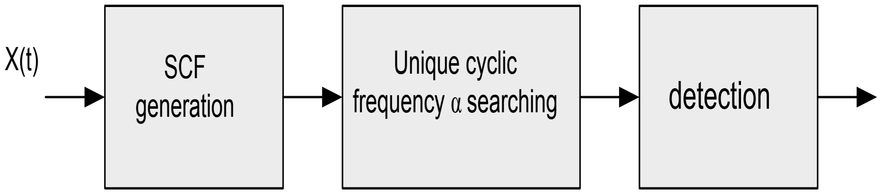


Figure 96. Cyclostationary signal detection procedure.

4.1.5 Simulations of Signals Based Spectrum Sensing

The distinctive features of the signals can be seen easily in the frequency domain rather than the time domain in which that can be used for detecting the presence of the licensed user signals. In practice, two methods can be used to accomplish this goal. One is called the FFT Accumulation method (FAM), and the other is Strip Spectral Correlation Algorithm (SSCA). Both methods shared the same characteristic and implemented upon the modifications into the cyclic cross autocorrelation. In this section, we present the experimental result based on implementation of the FAM to the several analog and digital modulated signals, also compare the resultant SCD function in which it is obtained as output from those methods with the theoretical results. Finally, this work explores the feasibility of the sensing method (cyclostationary) based on detecting licensed signals within a very low signal to noise ratio (SNR) and background of noise. Firstly, note that, the main characteristic of a Wight Gaussian noise (WGN) and interferences have no spectral correlation only at cyclic frequency equal to zero (α=0) as illustrated in Figure 97. According, to this fact feature detection (cyclostationary) allows cognitive radio to detect the licensed signals in case of a noisy environment or other modulated signals with a specific modulation variety. Secondly, we consider within the rest of this chapter various modulated signals with a fundamental carrier frequency (fc) in Hz.

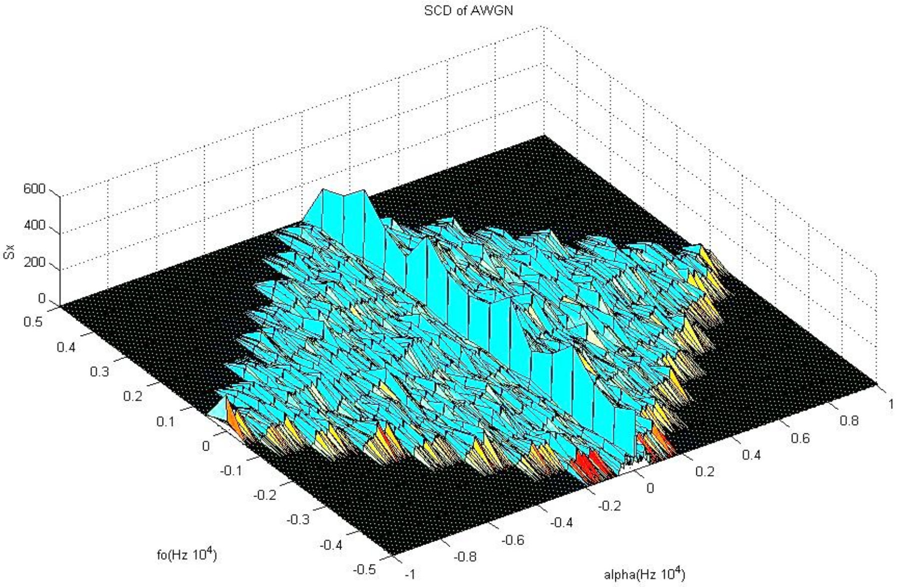


Figure 97. WGN Spectral correlation density function.

4.1.5.1 Pure Sinewave

Let first consider a pure analog sinewave signal as a carrier with the fundamental frequency (fc) in Hz,

(4.1)
$$p(t) = \cos(2\pi f_c t)$$

The spectral correlation density function SCD for the sinewave and from the signal processing theory is given as,

(4.2)
$$S_x^\alpha(f) = \left\{ \begin{array}{ll} \frac{1}{4}[\delta(f+f_c)+\delta(f-f_c)] & \alpha = 0 \\ \frac{1}{4}\delta(f) & \alpha = \pm 2f_o \\ 0 & others \\ & \end{array} \right\}$$

All details of the mathematical derivations are given in (William 1986). Therefore, based on the fc= 1000Hz, the sampling frequency fs= 8000 and from Equation (4.2) in which that leading to the following result,

(4.3)
$$S_x^\alpha(f) = \left\{ \begin{array}{ll} \frac{1}{4}[\delta(f-1000)+\delta(f+1000)], & \alpha = 0 \\ \frac{1}{4}\delta(f) & \alpha = \pm 2000 \end{array} \right\}$$

Based on theoretical result and the above mentioned information, we expect to obtain peaks at f=±1000Hz for α=0 and at α=±2000Hz for f=0 in which that agree with the achieving experimental results as illustrates in Figures 98, 99.

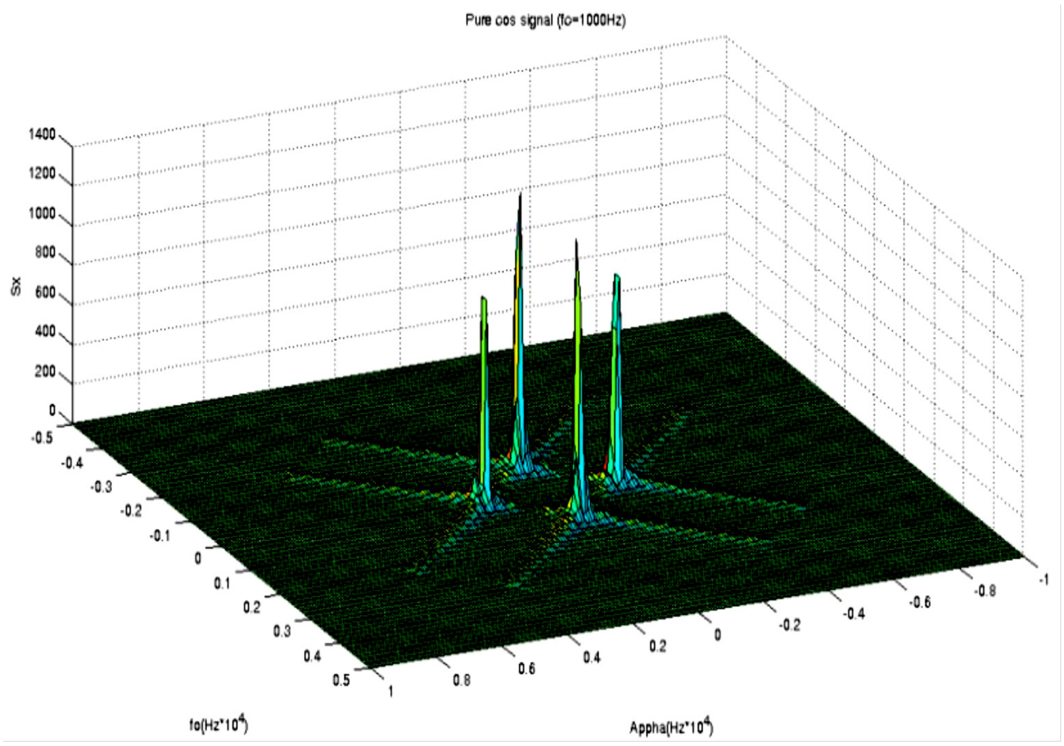


Figure 98. Surface plot of the SCD estimate magnitude for pure sinewave**.**

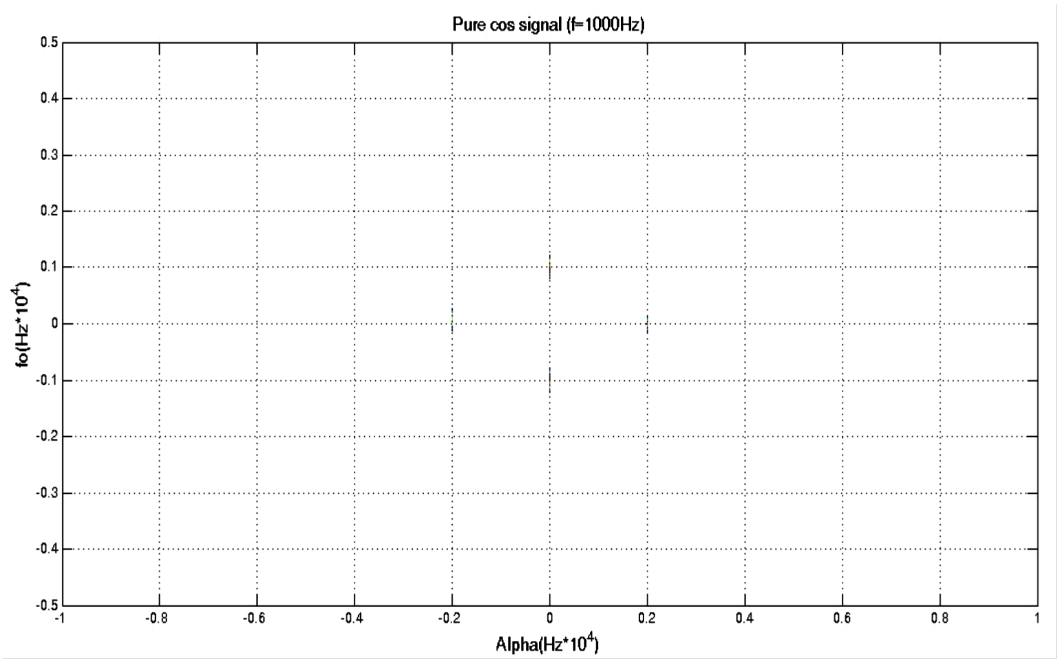


Figure 99. Contour plot of the SCD estimate magnitude for pure sinewave.

In case of adding the WGN to the signal with the SNR (-5), the SCD for the original signal did not mask by noise. Most of the noise peaks are replicas of the fundamental frequencies as illustrated in Figures 100, 101.

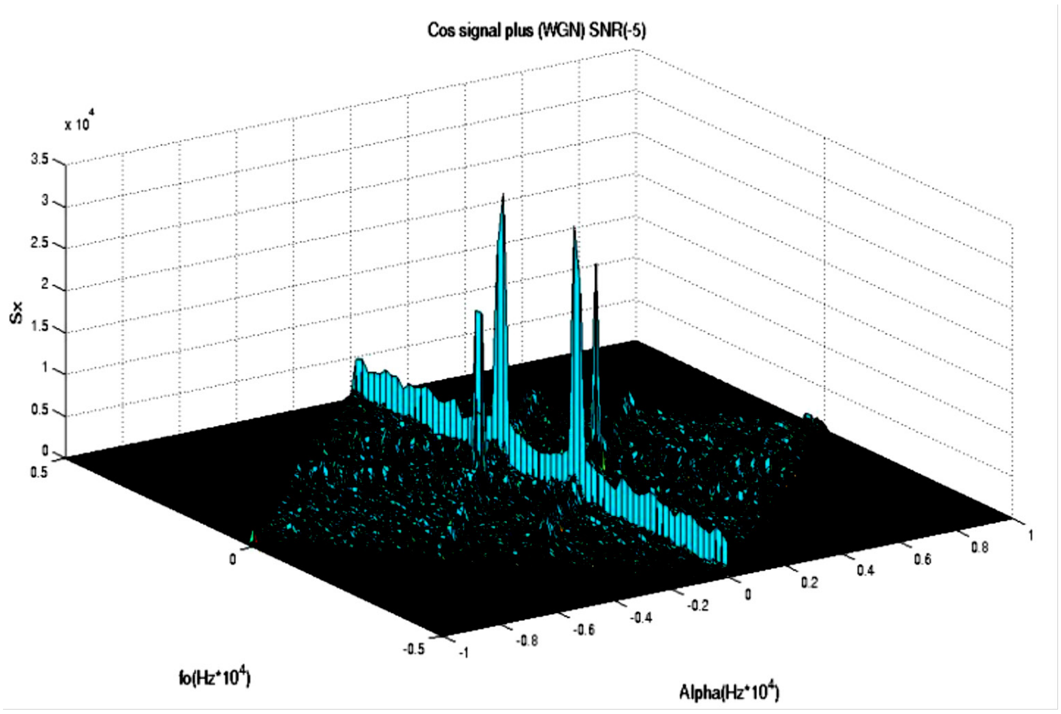


Figure 100. Surface plot of the SCD estimate magnitude for noisy sinewave

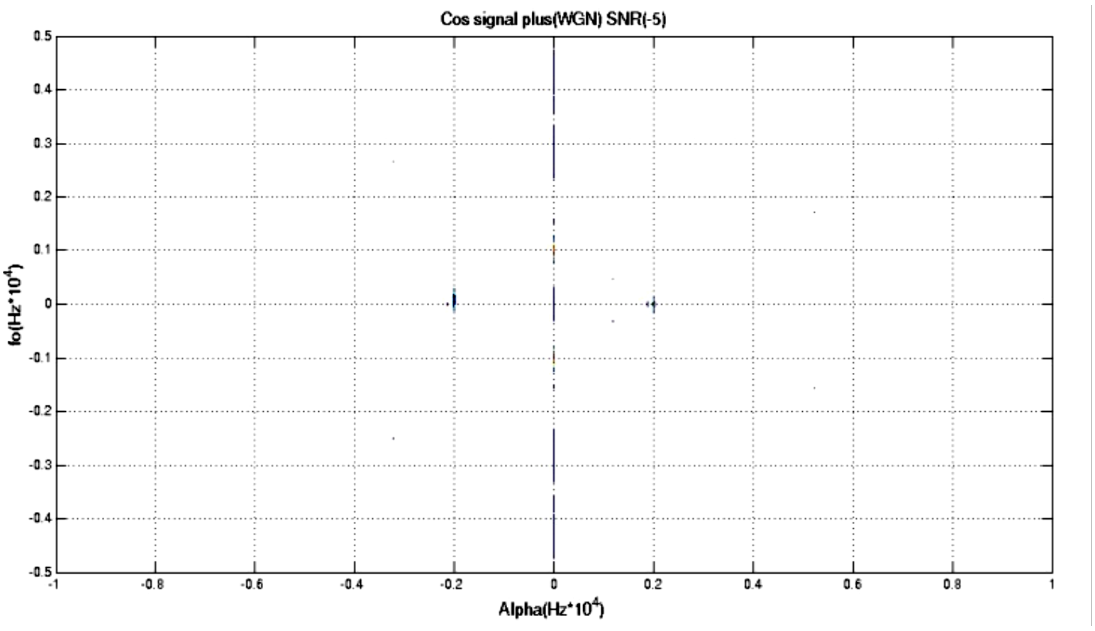


Figure 101. Contour plot of the SCD estimate magnitude for noisy sinewave.

In case of increasing the noise gradually and considering the SCD for the tested signal it could be seen that the SCD for the tested signal is not fully masked by the noise since the SNR(-25db) as illustrated in Figures 102, 103.

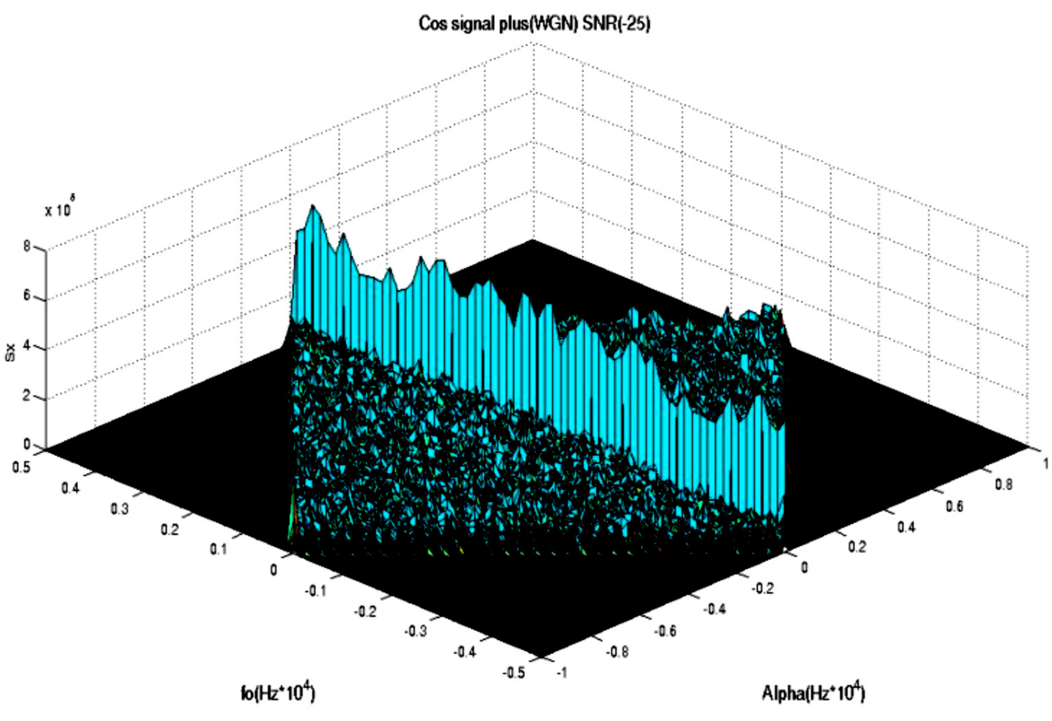


Figure 102. Surface plot of the SCD estimate magnitude for noisy sinewave.

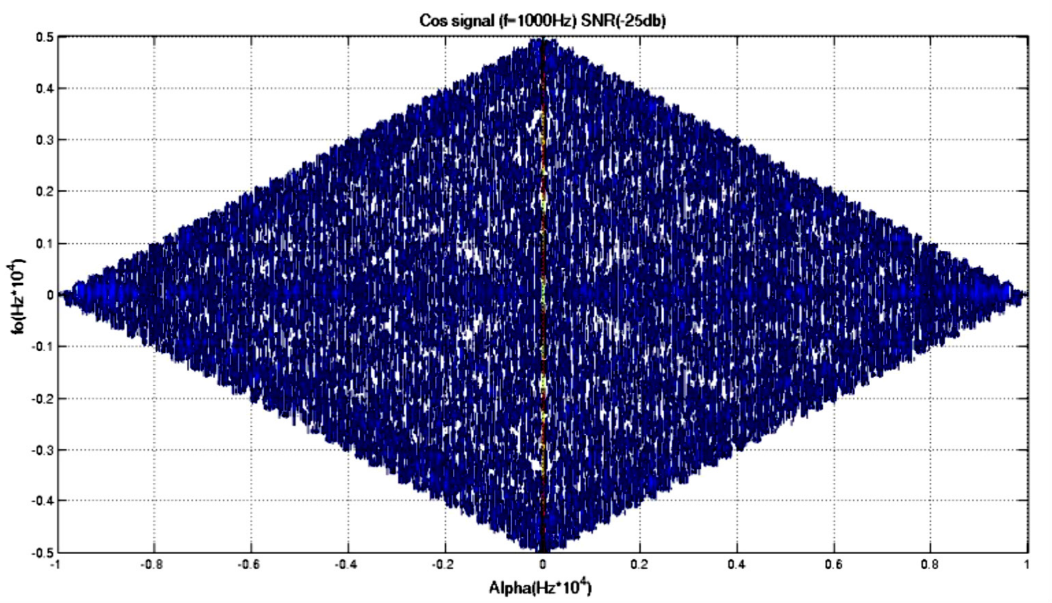


Figure 103. Contour plot of the SCD estimate magnitude for noisy sinewave.

4.1.5.2 Amplitude Modulation Single Side Band (AMSSB)

Within the second scenario, the SCD function for the Amplitude Modulation Single Side Band Signal (AMSSB) has been analyzed. Assume a massage signal as a tone for simplicity and to show the exact frequency of the massage fa= 1000Hz such as (a(t)=cos(2*pi*fa*t)) and fc=2000Hz, as a result the signal of the AMSSB is x(t)=a(t)p(t) where p(t) is given in Equation (4.1) and the SCD function based the analytical derivation results are,

$$S_x^{\alpha}(f)=\left\{\begin{array}{ll}\frac{1}{8}[\delta(f-f_o+f_a)+\delta(f+f_o-f_a)] & \alpha=0\\ \frac{1}{8}\delta(f)e^{\pm i2\varphi_o} & \alpha=\pm 2(f_o-f_a)\\ 0 & others\end{array}\right\} \qquad (4.4)$$

Therefore, according to Equation (4.4) we expect to obtain peaks at f=±1000Hz for α=0, and at α=±2000Hz for f=0, in which that agree with the achieving experimental results as illustrated in Figures 104, 105.

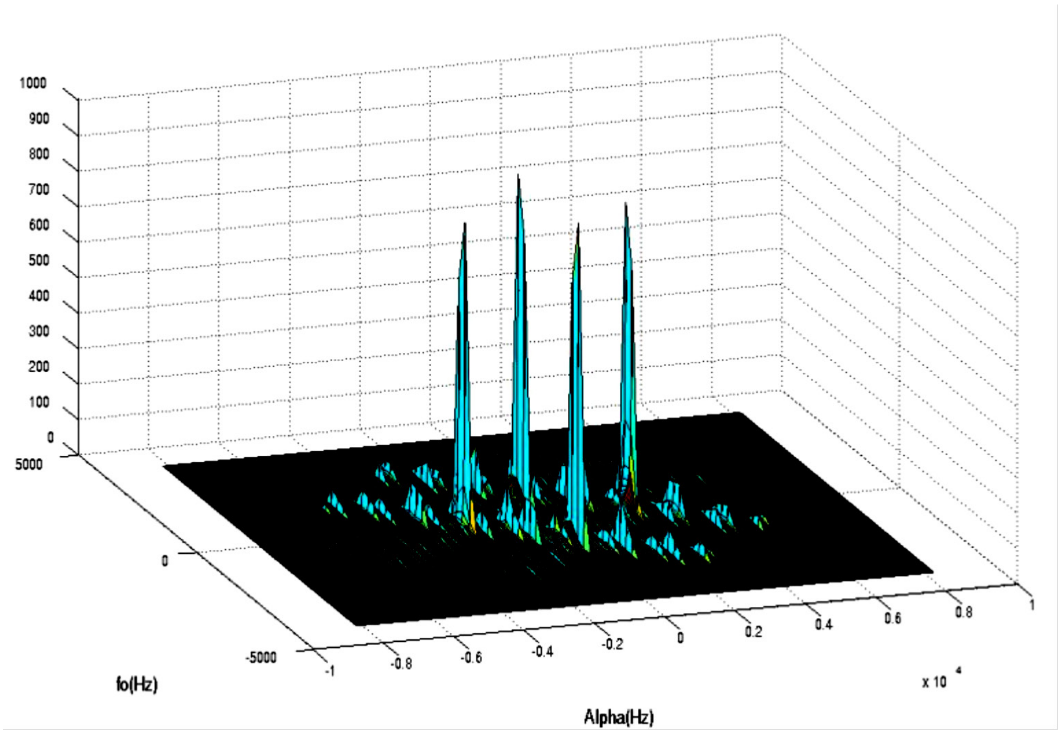


Figure 104. Surface plot of the SCD estimate magnitude for AMSSB.

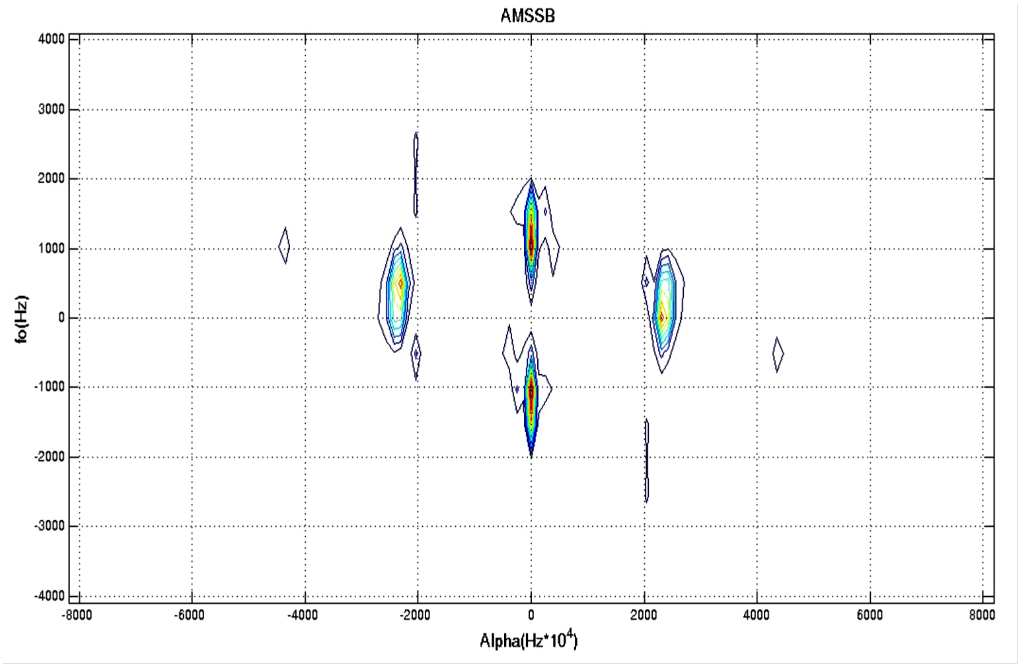


Figure 105. Contour plot of the SCD estimate magnitude for AMSSB.

In case of adding a (WGN) to the signal with the SNR (-5), the SCD for the original signal did not masked by noise, most of the noise peaks are replicas of the fundamental frequencies as illustrated in Figures 106, 107.

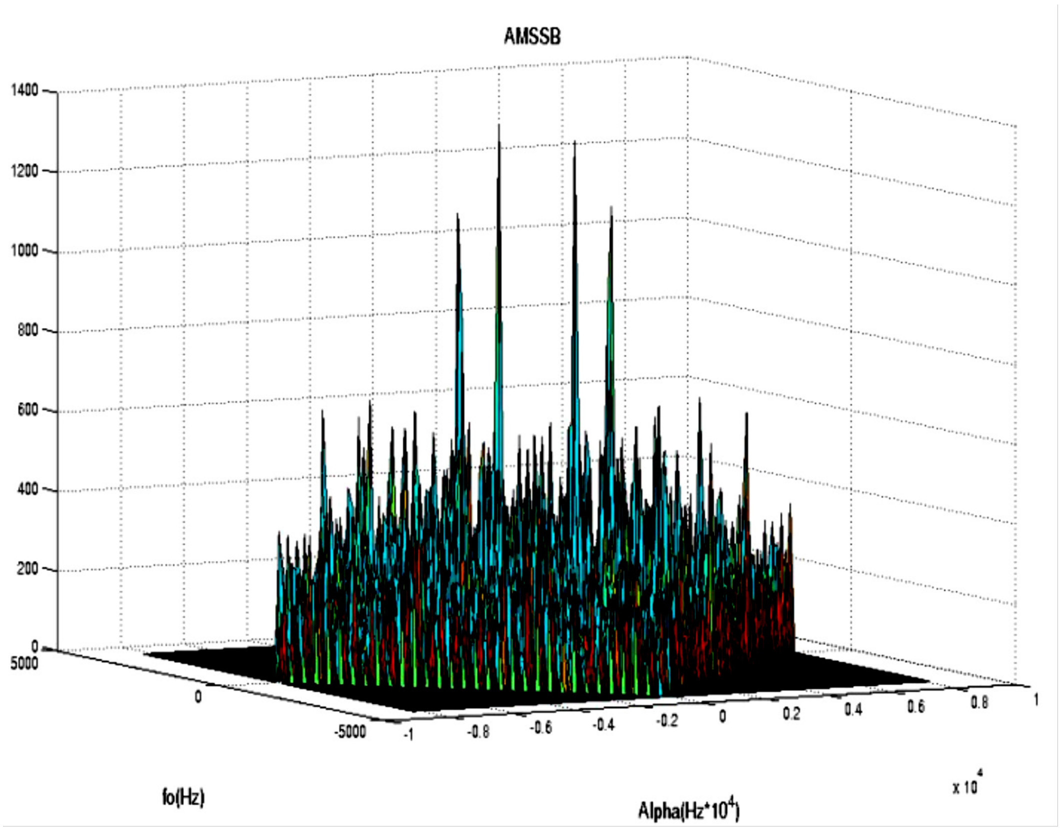


Figure 106. Surface plot of the SCD estimate magnitude for noisy AMSSB.

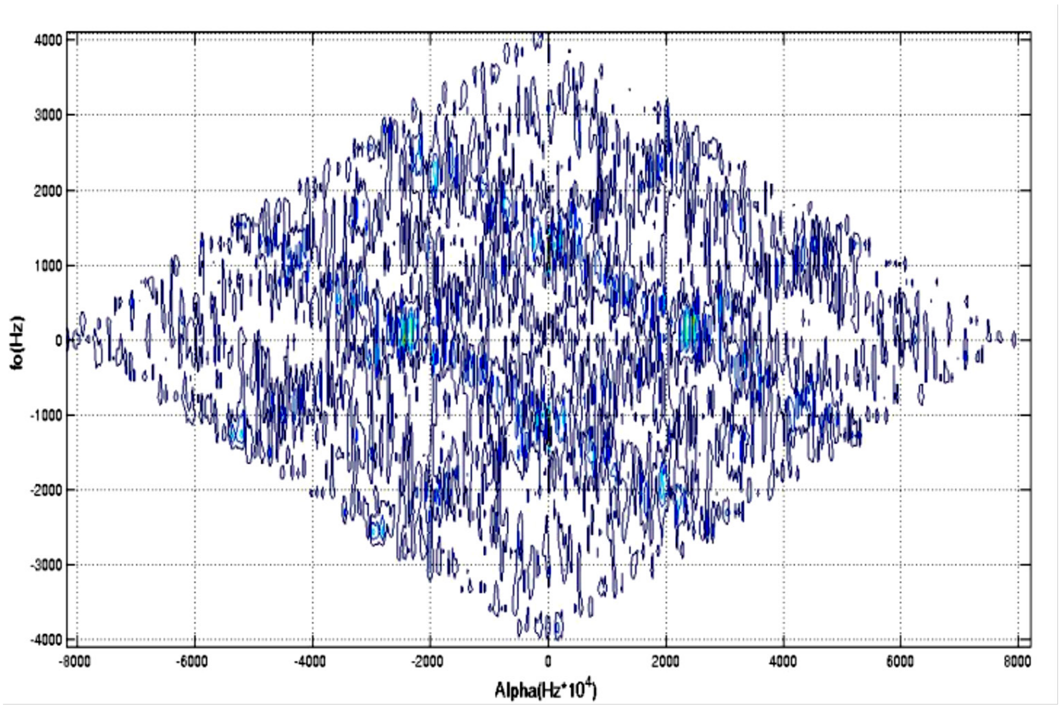


Figure 107. Contour plot of the SCD estimate magnitude for noisy AMSSB.

In case of increasing the noise gradually and considering the SCD for the tested signal it could be seen that the SCD for the tested signal is not fully masked by the noise since the SNR(-25db) as illustrated in Figures 108, 109.

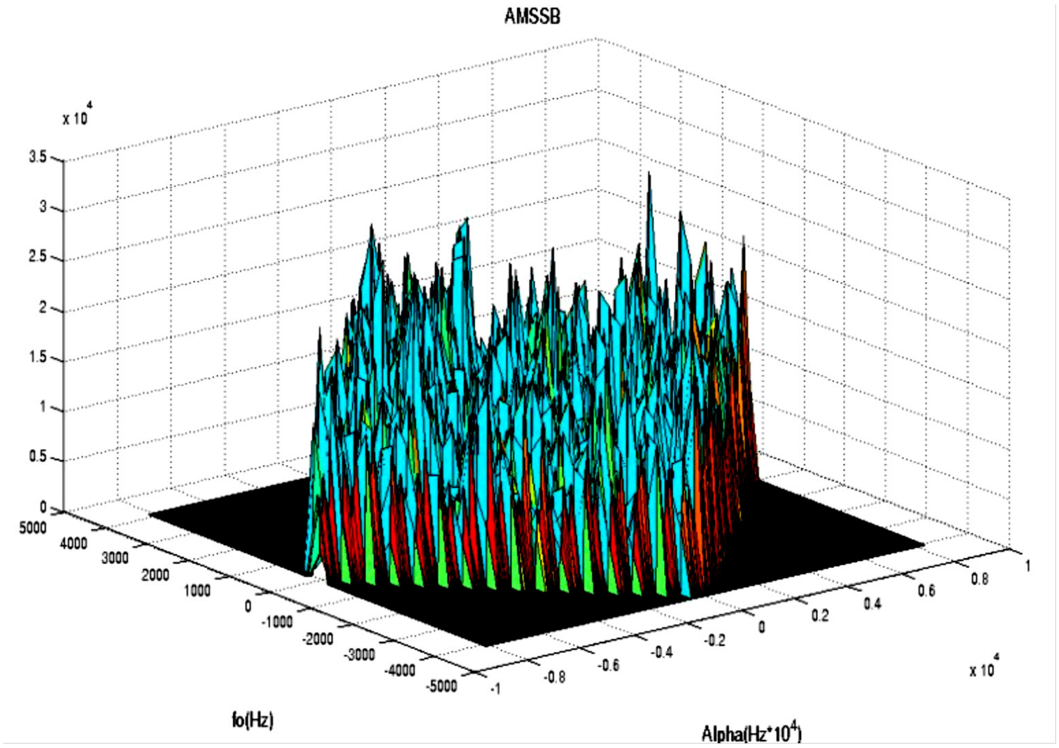


Figure 108. Surface plot of the SCD estimate magnitude for noisy AMSSB**.**

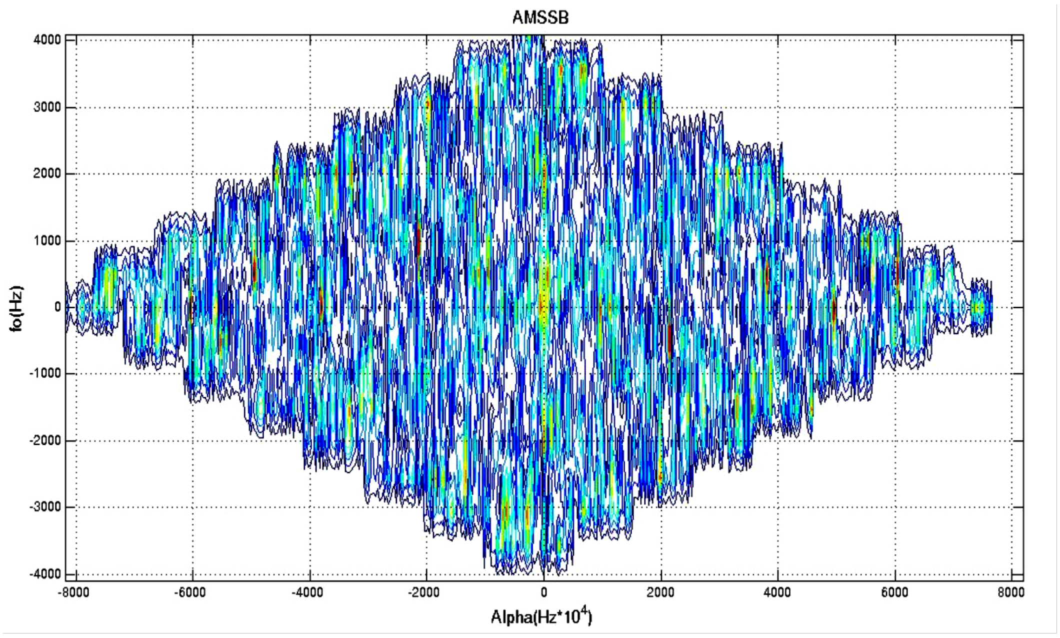


Figure 109. Contour plot of the SCD estimate magnitude for noisy AMSSB.

4.1.5.3 Binary Phase Shift Keying (BPSK)

In this subsection, SCD function for a digital signal binary phase shift keying (BPSK) has been analyzed. The signal with a PSK is simply a phase modulated (PM) carrier such as;

$$x(t) = \cos[2\pi f_o t + \varphi(t)] \tag{4.5}$$

Where the phase ϕ(t) is a digital phase amplitude modulation (PAM) signal as;

$$\varphi(t) = \sum a_n q(t - nT_o - t_o), \quad a_n = (0, \pi) \tag{4.6}$$

The SCD function for the BPSK signal based on analytical result is,

$$S_x^\alpha = \begin{cases} \frac{1}{4T_o} Q\,(f + {}^{\alpha}\!/\!_{2} \pm f_o).Q^*\,(f - {}^{\alpha}\!/\!_{2} \pm f_o)\,e^{-i\,[2\pi\,(a+2f_o)\,t_o \pm 2\,\varphi_o\,]}, \alpha = \pm 2f_o + k/T_o \\ \frac{1}{4T_o} [Q\,(f + {}^{\alpha}\!/\!_{2} \pm f_o).Q^*\,(f - {}^{\alpha}\!/\!_{2} + f_o) \quad + \\ Q\,(f + {}^{\alpha}\!/\!_{2} - f_o).Q^*(f - {}^{\alpha}\!/\!_{2} - f_o)\,e^{-i2\pi t_o}], \qquad \alpha = k/T_o \\ 0 \qquad\qquad o\ t\ h\ e\ r\ s \end{cases} \tag{4.7}$$

From Equation (4.7) we expect to obtain four entities of the SCD function forms. Four peaks at the points at f= ±fo = ±2000Hz, for α=0 and at the points α= ±2fo = ±4000Hz in which that agree with the achieving experimental results as illustrated in Figures. 110, 111.

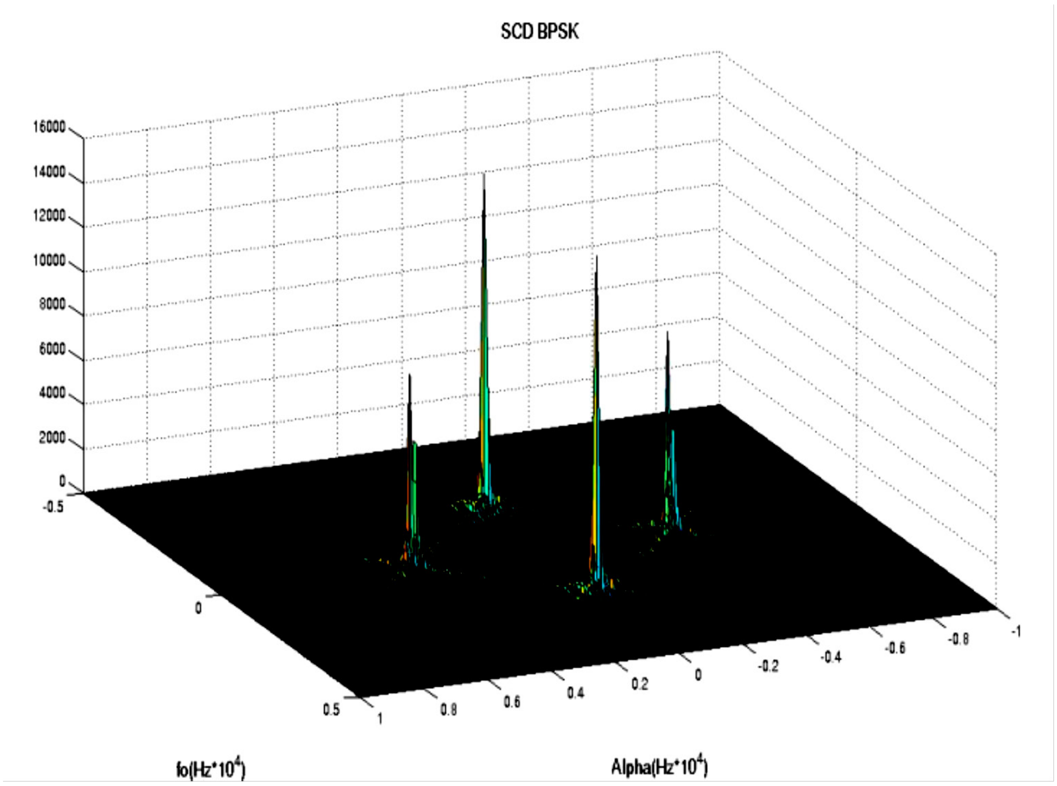


Figure 110. Surface plot of the SCD estimate magnitude for BPSK.

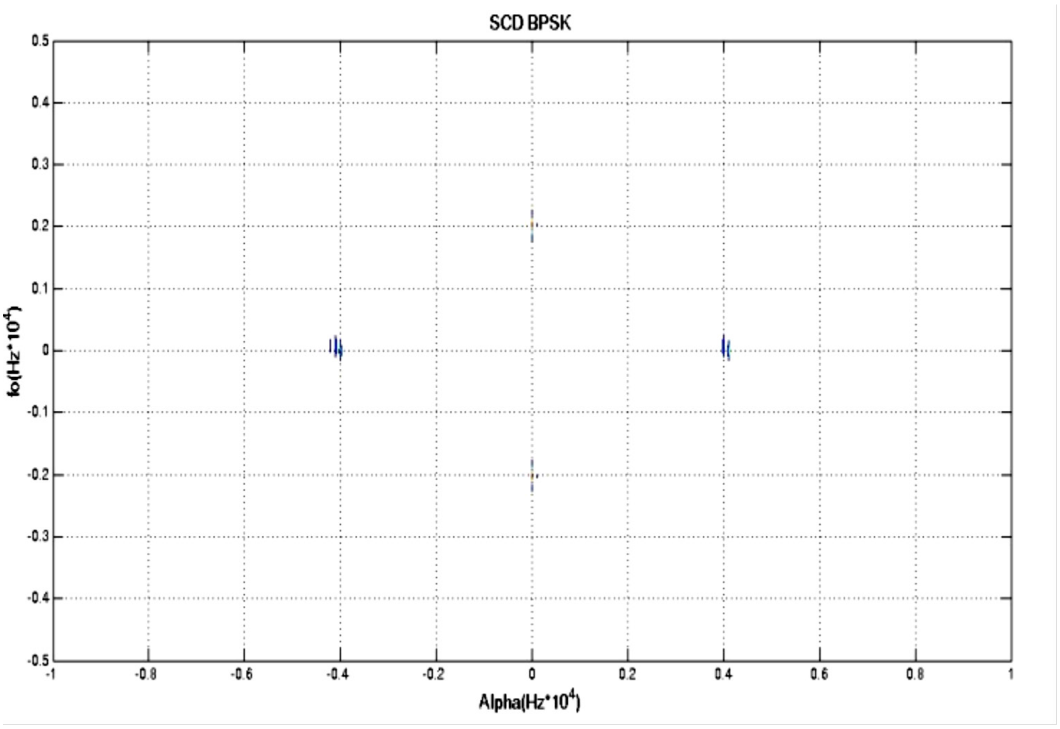


Figure 111. Contour plot of the SCD estimate magnitude for BPSK.

In case of adding a Wight Gaussian Noise (WGN) to the signal with the SNR (-5), the SCD for the original signal did not masked by noise, most of the noise is concentrated where alpha equal to zero and replicas of the fundamental frequencies as illustrated in Figs. 112, 113.

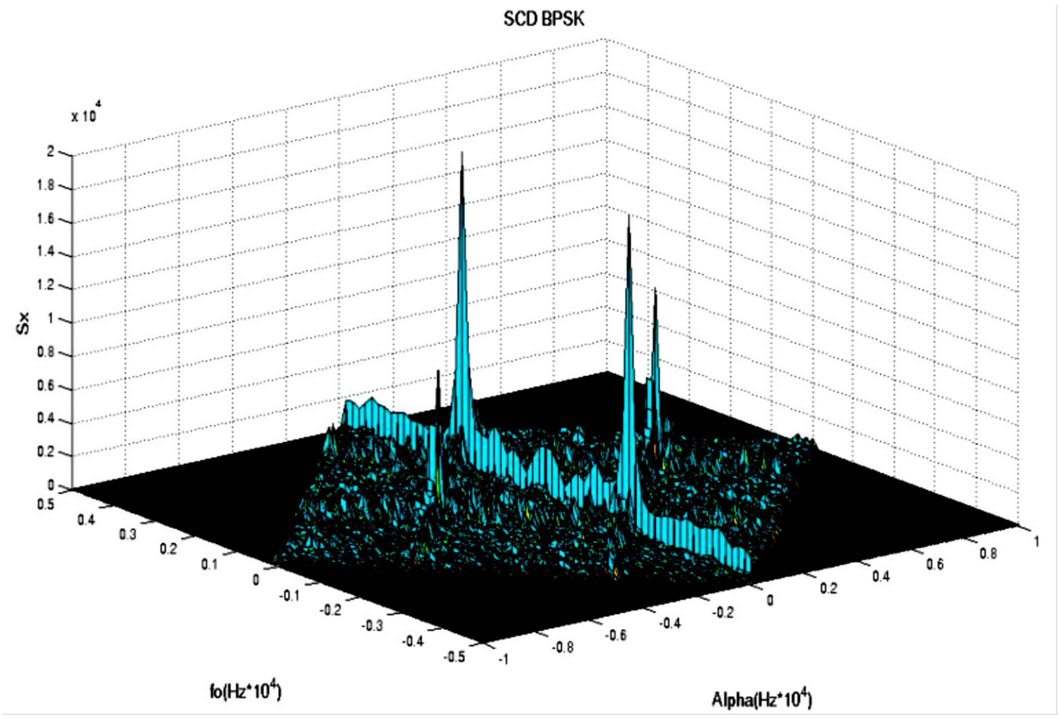


Figure 112. Surface plot of the SCD estimate magnitude for noisy BPSK.

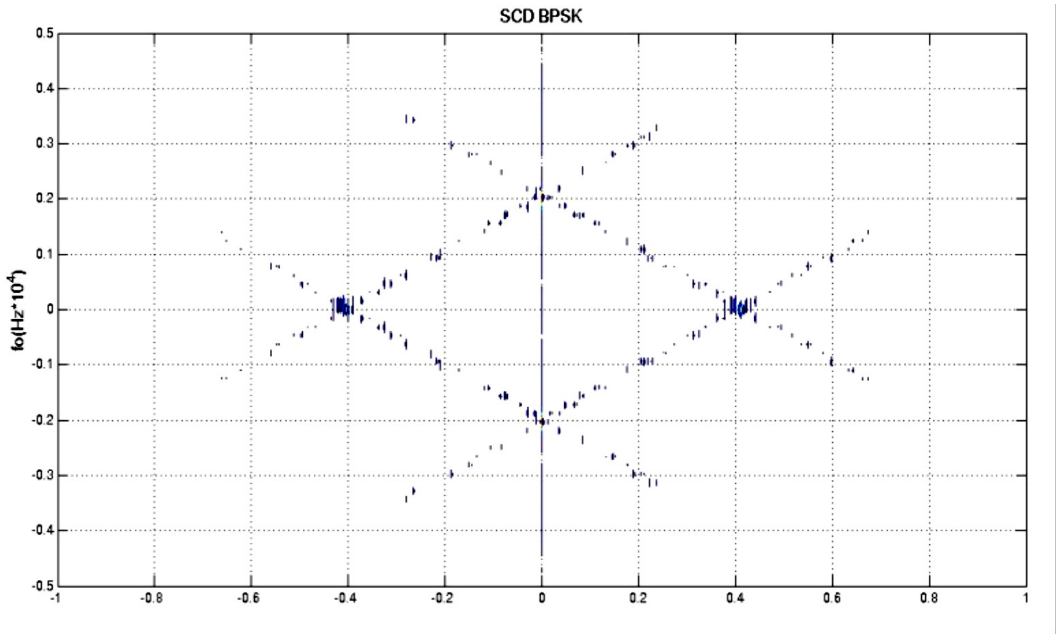


Figure 113. Contour plot of the SCD estimate magnitude for noisy BPSK.

In case of increasing the noise gradually and considering the SCD for the signal under test, it could be seen that the SCD for the tested signal is not fully masked by the noise since the SNR(-25db) as illustrated in Figures 114, 115.

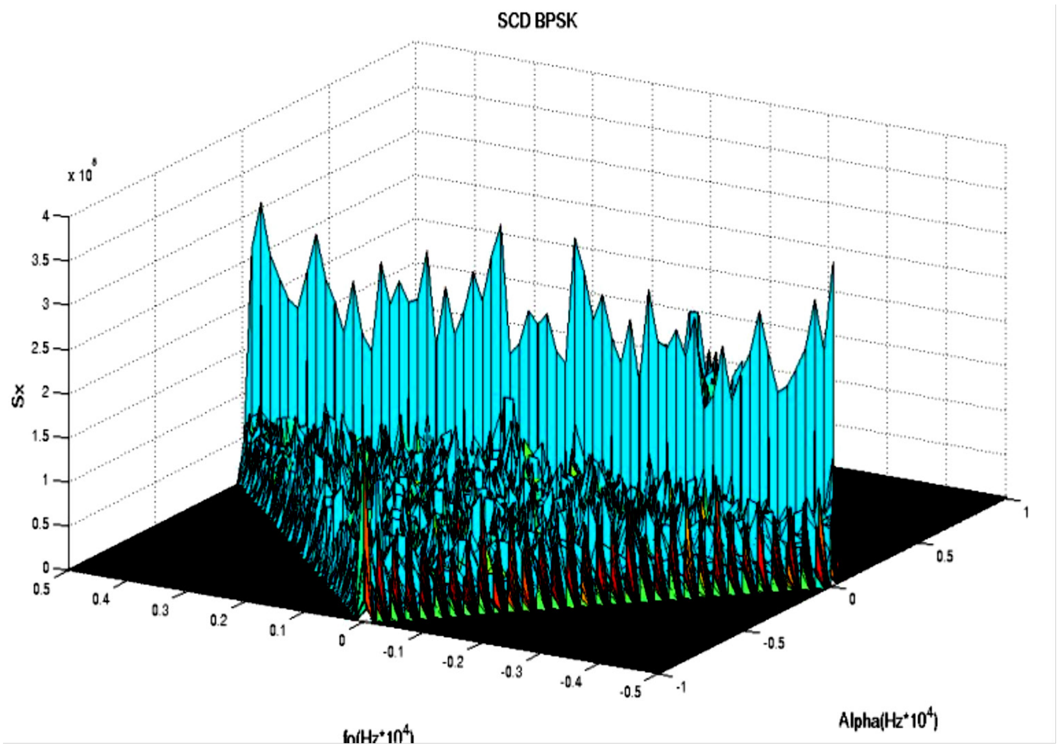


Figure 114. Surface plot of the SCD estimate magnitude for noisy BPSK.

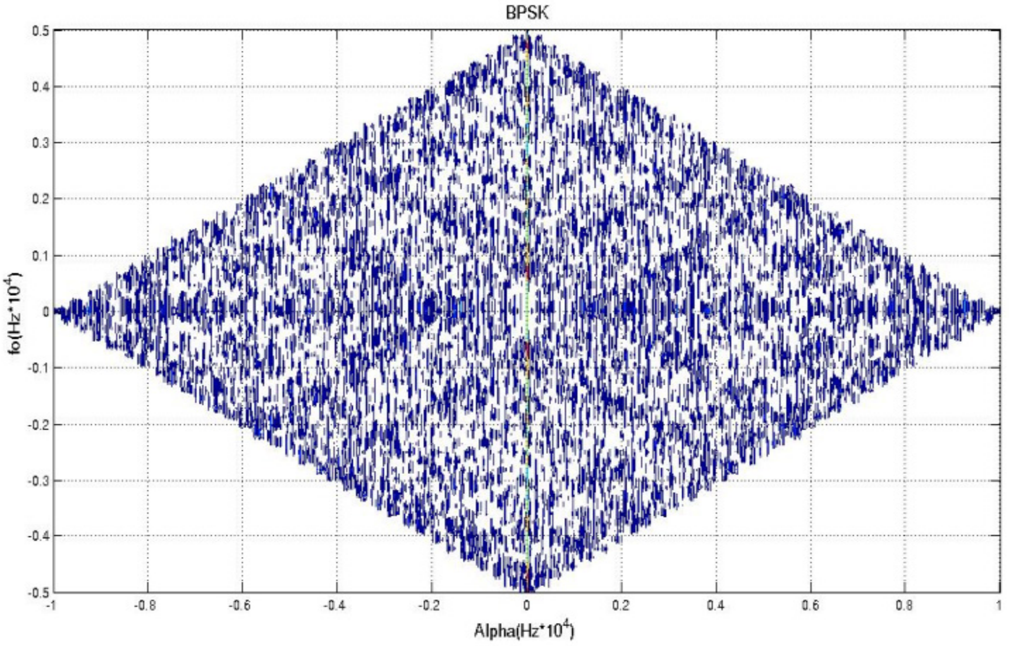


Figure 115. Contour plot of the SCD estimate magnitude for noisy BPSK.

4.1.6 Conclusions

The alternative framework for the communication system network within the SG has been proposed. This proposed communication system network model attempts to bring about a reasonable change in SG communication infrastructure with the introduction of CR technology. Moreover, it has various advantages such as; firstly, offering the cost-effective solution for the communication system within the SG through avoiding the wired applications and reusing the licensed frequency bands that provided more affordable services. Secondly, high reliability, availability upon the full bidirectional wireless communication among all nodes within the SG that support the decentralized decision approach. Thirdly, it might reduce the scarcity within the available resources. Fourthly, introduce the concept of reusing the favorable low licensed frequency bands through utilizing the spectrum holes or sharing the available frequency band with the licensed users within some restrictions. Lastly, the feasibility of the proposed alternative framework for the communication network to detect the licensed spectrum occupancy was examined within various scenarios. These testing show that the license user singles can be detected in a noisy environment and even with a very low SNR, in which that prove the feasibility of the proposed solution for the SG communication system network as a mean solution for the communication network or as a backup for the existing one (redundancy concept).

5 CONCLUSIONS AND FUTURE WORK

This research work investigated some fundamental questions related to legacy power system infrastructures and the IEC 61850 standard's implementation issues. The existing power system infrastructure does not meet the requirements imposed by electrical utility deregulation power generation, transmission and distribution or ancillary services, which compromises various parties. Achieving the required power system flexibility, reliability and availability will entail the merging of new technologies and standards that can handle all the functions needed. The continuous development of the technology and standards (such as digital communications, microprocessors, IEC 61850, etc.) has a significant impact on the feasibility and usefulness of SAS performances and designs. The new IEC 61850 standard for SASs provides tangible benefits in terms of more measured and calculated real-time information in relation to substation operations. This real-time information is available and easily accessed through the IEC 61850 standard for use by operating, maintenance and engineering in order to troubleshoot substation events. However, based on the new SAS design approach and the related evaluation studies investigated in this work, several challenges raise.

SAS communications network bus topologies based on the IEC 61850 BFP function's analysis were considered in Chapter 2, part one. This work investigates several practical SAS bus topologies from the reliability and availability points of view. Reliability and availability were calculated for various SAS bus topologies and comparisons were made among the achieved reliability and availability results values. Redundancy was identified as a key feature to increase the overall reliability and availability of an SAS. In part two, the novel RaFSA estimation method was introduced. The novel RaFSA estimation method attempts to examine and predict the actual behaviour pattern of each IED within an SAS. These examination and prediction features are provided based on the nature of the process that is involved within the RaFSA process being random. RaFSA provides specific benefits, such as being easy to carry out within various PC software environments, supporting different kinds of probability distribution models and handling large numbers of input data, in addition to other analysis tools and parameters, such as the repairing time, the load flow, reconfiguration, optimization, etc. Changing the input data can easily be applied through RaFSA without major modifications to the underlying process.

In Chapter 3, several practical tests were carried out. In part one, the analysis and the methodology for measuring and calculation of the GOOSE messaging latencies in the multi-vendor SAS communications network were carried out. Firstly, we introduced the round-trip calculation method to calculate the GOOSE messag-es' latency. The achieved results show the successful measurement and calculation of the GOOSE messages' latency for the DUTs based on the proposed round-trip method. Furthermore, they show that the DUTs are compliant with the IEC 61850 criteria and prove the interoperability concept. In part two, a novel approach to a vendor-independent SAS configuration tool was presented. This approach creates and increases the relay configuration to the system level based on the full IEC 61850 standard, including the parameter and feature setting level. Several advantages can be noted in its implementation, such as overcoming the lack and limitation of vendors' proprietary (IED, system) configuration tools, the reduction of the operation and maintenance costs associated with the number of used IEDs and system configuration tools and the amount of staff training. Further, interoperability and interchangeability are applicable among the technical staff. In addition, it provides for the adding, upgrading and expanding of AS functionality, and provides AS that has better reliability and which is independent of the vendors' product lines. In part three, modelling of modern IEDs to build an SAS process bus network and evaluate the performance of the simulated network under different circumstances using OPNET was carried out. The achieved results from the modelled SAS process bus indicate that the first Ethernet switch experienced more latency than the subsequent switches based on its serialized, bunched SV frames, whereas the subsequent switches experienced less latency. This result facilitates the connection of a large SAS, which might consist of more than one Ethernet switch. Further, several MUs within a process bus network were connected one-by-one to evaluate the limits and capacity of the process bus network. The achieved results show that no more than 19 MUs are able to be connected in one 100 Mb/s SAS communications network. In part four, a novel approach to estimate the SV packets' stream latency in a LAN based on IEC 61850-9-2LE was presented. The implementation of this approach was based on considering the successful reservation of a sequence of an SV packet stream. The obtained results demonstrate the successful implementation of the novel SV latency estimation approach. Lastly, the comparative evaluation of practical and simulated SV traffic streaming latency results was carried out. The obtained results show that, by implementing the comparison, two benefits are achieved. From the practical experiments point of view, it proves the correctness of the design and the implementation of the IEC 61850-9-2LE process bus in addition to the novel time analysis of the SV traffic stream's latency. From the OPNET simulation modelling point of view, it shows the correctness of the IEC 61850-9-2LE process bus modelling, as well as the power of the OPNET simulation tools (which can model a high data-rate, real-time system based on the new standard IEC 61850-9-2L).

In Chapter 4, the alternative framework for the communications system network based upon the SG approach was proposed and analysed. The main feature of the proposed communications network model was introduced with the CR technology. The CR technology has several advantages, such as offering a cost-effective solution to the communications system in an SG, high reliability and availability based upon bidirectional wireless communication among all the nodes within the SG. It might also reduce the scarcity evident among the available resources and introduce the concept of reusing favourable, licensed low-frequency bands. Further, the feasibility of the proposed alternative framework for the communications network in detecting licensed spectrum occupancy was examined, showing that the license user's signals can be detected in a noisy environment, even with a very low SNR. These results maintain the spirit of CR by sharing the available license spectrum while also offering a cost-effective solution for the SG communications network as a primary solution to the communications network or else as a backup for an existing one. Although this work has investigated several fundamental questions relating to legacy power systems and the IEC 61850 standard's implementation, there remain certain areas for which future work needs to be considered, such as:

- Several assumptions have been made in this work to simplify the calculations, which perhaps should be waived.

- It may be necessary to consider measuring the latencies for the round-trip time of the GOOSE messages based on different bus topologies with more than one Ethernet switch.

- Similar issues relate to the calculation of accumulation jitter for the GOOSE messages where they interfere with traffic propagated within the same SAS communications network.

- The development and investigation of new (or the enhancement of) existing SAS digital automation and protection functions based upon IEC 61850 that offer unique characteristics. For instance, the islanding detection protection function can be improved significantly upon monitoring the CB status, DG status, etc., through the central ser-vices manager. This developed function was carried out in a sup-plementary work submitted to the pacworld conference (Glasgow, UK) and accepted for oral presentation on 29 June-2 July, 2015. The underlying functional developments were carried out based on the MATLAB/Simulink simulation. As a next step, we need to imple-ment and test the developed solution on the practical micro-grid (MG) using the commercial ABB COM600 and various IEDs.

REFERENCES

ABB, (2002). Breaker Failure Protection, [Web document]. Sweden: ABB Automation Technology Products. Available at: http://www05.abb.com/global/scot/ http://www05.abb.com/global/scot/scot296.nsfvertydiplay/c1256d32004634ba c1256e28005f594b/$file/1mrk580139ben_en_reo_517_2.4_breaker_failure_protection.pdf.

ABB, (2008). Smarten up your assets Enhanced substation automation, control and protection for continuous and secure power delivery. [Web document]. Baden: Power System. Available at:http//www05.abb.com/global/scot/scot221/nsf/ /veritydisplay/7633bab7ce7895e1c12574ff003bd9b1/$file/sa%20systems%20retrofit%20pamphlet%2011%2008.pdf.

ABB, (2010). Power system protection and automation reference Extending substation life cycle with IEC61850. [Web document]. Vaasa: Distribution Automaton. Available at:http://www05.abb.com/global/scot/scot229.nfs.

ABB, (2012). Transmission and distribution substation Customized solutions and modular concepts for utility and industrial applications. [Web document]. Power System. Available at:htpp: //www02.abb.com/global/gad/ /gad02181.nsf.

Adamiak, M., & Premerlani, W. (1999). The Role of Utility Communication in a Deregulated Environment. In *Proceeding on the 32nd Annual Hawaii International Conference on System Science.*

Adamiak, M., Baigent, D. & Mackiewicz, R., (2009). EC61850 communication Network and Systems In Substation. [Web document]. Available at:http//www.gedigitalenergy.com/ multilin/journals/issues/spring09/iec61850.pdf

Ali, I., & Thomas, S., (2006). Ethernet Enabled Fast and Reliable Monitoring Protection and Control of Electric Power Substation. In *Proceeding International Conference on Power Electronics, Drives and Energy Systems (PEDES '06).* 1-6.

Ali, I., Thomas, M., S., & Gupta, S., (2012). Methodology & Tools for Performance Evaluation of IEC 61850 Goose based Protection Schemes. In *IEEE 5th Power India Conference.* 1-6.

Amelot, J., Li-Baboud, Y., Vasseur, C., Fletcher, J., Anand, D., & Moyne, J., (2011). An IEEE 1588 performance testing dashboard for power industry requirements. In *International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS'11).* 132.137.

Amntegui, I., Ojanguren, C. De Calos, F., & Quintanilla, R. (2005). Automation of HV Substation in Iberdrola. Experience and Plans. In *Proceeding 58th Protective Relay Engineers Conference.* 194-200.

Anderson, P., M., & Agarwal, K., S., (1992). An improved model for protective system reliability. In *IEEE Transaction on Reliability*. 41:3. 422-426.

Anderson, P., M., Chintaluri, G., M., Maghbuhat, S., M., & Ghajar, R., F., (1997). An improved reliability model for redundant protective systems Markov models. In *IEEE Transaction on Power System*.12:2. 573–578.

Andersson, L., Brand, K., Drunner, C., & Wimmer, W., (2005). Relaibility investegatiion for SA communication architectures based on IEC 61850. In *IEEE Power Technology*. 1-7.

Apostolov, A., Brunner, C., & Clinard, K., (2003). Use of IEC61850 Object Models for Power System Quality Security Data Exchange. In *CIGRE/IEEE PES International Symposium on Quality and Security of Electric Power Delivery Systems*. 155-164.

Battagöini, A., Lilliesstam, J., Bals, C., & Haas, A. (2008). The SuperSmart Grid. European Climate Forum, [Web document]. Available.at: http//germanwatch.org/ /klima/ssg08.pdf.

Beaupre, J., Lehoux, M., & Berger, P. (2000). ADVANCED MONITORING TECHNOLOGIES FOR SUBSTATIONS. In *Proceeding 9th IEEE International Conference maintenance Proceedings*. 287-292.

Billinton, R., & Allan, N., (1992). Reliability Evaluation of Engineering Systems. USA: Springer Science Business Media.

Bose, A. (2003). POWER SYSTEM STABILITY: NEW OPPORTUNITIES FOR CONTROL. [Web document]. Boston. Available at:http://www.gridstat.net/publications/Bose-GridComms-Overview-Chapter.pdf.

Brand, K. (2004). The Standard IEC 61850 as Prerequisite for Intelligent Applications in Substation. In *Proceeding IEEE Power Engineering Society General Meeting*. 714-718.

Brand, K., & Wimmer, W. (2008). Approach to optimized Process Bus architectures. [Web document]. Switzerland: ABB power System. Available at:http://www05.abb.com/global/scot/scot221.nsf/veritydisplay/4cc6f6baabd4815dc12574f9004ca837/$file/abb%20iec9%202%20profiline%202008%20offprint.pdf.

Brand, K., P., Brunner, C., & Wimmer, W., (2004). DESIGN OF IEC61850 BASED SUBSTATION AUTOMATION SYSTEM ACCORDING TO CUSTOMER REQUIREMENTS. In *CIGRE Session. Paris*, 2004.

Brändström, F. & Lord, W. (2009). THE FUTURE SUBSTATION-REFLECTION ABOUT DESIGN. Prague: In *Proceeding of CIRED 20th International conference on electricity distribution,* 1-4.

Chen, S., J., Hsiang, Y., Hung, C., Sheng, T., & Fang, R., (2012). Using Multi-Vendor IEDs for IEC6180 Interoperability and HMI-SCADA Applications. *In International Symposium on Computer Consumer and Control (IS3C)*. 745-748.

Curtis, K., (2005). A DNP3 Protocol Primer. [Web document]. DNP Users Group. Available at:http//www.dnp.org/aboutus dnp3%20primer%20rev%20a.pdf

Devos, A. & Rowbotham, C. (2001). Knowledge Representation for Power System Modelling. In *Proceeding IEEE Power Industry Computer Applications (PICA 2001)*. 50-56.

Dominicis, C., M., Ferrari, P., Flammini, A., Rinaldi, S., & Quarantelli, M., (2011). On the Use of IEEE 1588 in Existing IEC 61850-Based SASs: Current Behavior and Future Challenges. In *IEEE Transaction on Instrumentation and Measurement*. 60:9., 3070-3081.

Energy Future Coalition, (2010). CHALLENGE AND OPPORTUNITY CHARTING A NEW ENERGY FUTURE. [Web document]. Washington DC. Available at:http://www.energyfuturecoalition.org/files/webfmuploads/EFCreport

Englert, H., & Dawidczak, H., (2010). Improving IEC 61850 Interoperability: Experiences and Recommendations," in *CIGRE, Power System Conference, Canada*.

EWICS, (2006). Electric Power Systems Cyber Security: Power Substation Case Study. [Web document]. European Workshop on Industrial Computer System. Available at:http://www.energycentral.com/download/products/ EPSCyberSecurity.pdf

Falk, H., (2011). IEC 61850 INTEROPERABILITY. [Web document]. USA: UCA International Users Group. Available at:http//testing.uca.org/IOP_Registrati on/2011%20CIM61850%20IOP/IOP%20Rports/IEC%2061850%20IOP,%20Pari s,%20France%20UCAIug-63-111Rv1.pdf.

Field Server Technologies, DNP3 Protocol Serial. [Web document]. Field Server Technologies. Available at:http://www.fielsserver.com/products/drivers/DNP3-protocol.php#DNP3_Tested.

Gopalakrishnan, P. & Thoms, J. Introducing Protocol Converter in a Sub-Station Communication Environment for IEC 61850 Compatibility. [Web document]. India: Kalki Communication Technologies Ltd. Available at:http://www.kalkitech.com/wpcontent/files/WhitePaper_Impact_Of_Protocol _Converter_InSS_Comm.pdf.

Gungor, V., C., & Lambert, F., C., (2006). A survey on communication networks for electric system automation. In *ELSEVIER Computer Networks 50*, 877-897.

Gurbiel, M., Komarnick, P., Styczynski, Z., Gatzen, F., W., & Dzienis, C., (2009). Merging Unit Accuracy Testing. In *IEEE Power Energy General Meeting*. 26-30.

Holbach, J., Rodriguez, J., Wester, C., Baigent, D., Frisk, M., Kunsman, S., & Hossenlopp, L., (2007). STATUS ON THE FIRST IEC61850 BASED PROTEC-

TION AND CONTROL MULTI-VENDOR PROJECT IN THE UNITED STATES. In *Proceeding 60th Annual Conference for Protective Relay Engineering's*. 283-306.

Hong, Q., Blair, S., Catterson, V., Dysko, A., Booth, C., & Rahman, T., (2013). Standardization of power System Protection Settings Using IEC 61850 for Improved Interoperability," in *IEEE Power and Energy Society General Meeting*.

Hor, C., & Crossley, P. (2005). Knowledge Extraction from Intelligent Electronic Devices. Berlin: Springer-Verlag. 82-111.

Hou, D., & Dolezike, D., (2008). IEC61850-What it Can and Cannot offer to Traditional Protection Schemes. [Web document]. Schweitzer Engineering Laboratories. Available at:http//www.ucaiug.org/Meeting/CIGRE_2014/USB%20.

IEC 61850-1, (2003). Communication Network and System in substation-part 1: Introduction and Overview.

IEC 61850-5, (2003). Communication Network and System in Substation-part 5: Communication Requirements for Functions and devices Models, (2003).

IEC 61850-6, (2003). Communication Network and System in Substation-part 6: Configuration Description language for communication in Electrical Substation.

IEC 61850-7-1, (2003). Communication Network and System in Substation-part 7-1: Principle and Models.

IEC 61850-7-2, (2003). Communication Network and System in Substation-part 7-2: Basic Communication Structure for Substation and feeder Equipment- -Abstract Communication Service Interface (ACSI).

IEC 61850-7-4, (2003). Communication Network and System in Substation-part 7-4: Basic Communication Structure for Substation and feeder Equipment--Compatible logical nodes and data classes.

IEC 61850-7-420, (2009). Communication Networks and System for Power Utility Automation for Distributed Energy Resources.

IEC 61850-8-1, (2003). Communication Network and System in Substation-part 8-1: Specific Communication Service Mapping (MCSM)- Mapping to MMS (ISO/IEC 9506-1 & 2) and to (ISO/IEC8802-3).

IEC Standard for Communication Network and Systems in substation, IEC 61850 (2003).

Ingram, D., M., E., Tylor, R., R., Schub, P., & Campbell, D., A., (2013). Performance Analysis of IEC 61850 Sampled Value Process Bus Network. In *IEEE Transaction Industrial Information*. 9:3. 1445-1454.

Ingram, D., M., E., Steinhauser, F., Marinescu, C., Tylor, R., R., Schub, P., & Campbell, D., A., (2012). Direct evaluation of IEC 61850-9-2 process bus network performance. In *IEEE Transaction Smart Grid*. 3:4. 1853-1854.

Ingram, D., Steinhauser, F., Marinescu, C., Tylor, R., Schub, P., & Campbell, D., (2013). Direct evaluation of IEC 61850-9-2 process bus network performance. In *IEEE Transaction on Industrial Information*. 3:4. 1853-1854.

Ingram, D., Tylor, R., Schub, P., & Campbell, D., (2013). Performance Analysis of IEC 61850 Sampled Value Process Bus Network. In *IEEE Transaction on Industrial Information*. 9:3. 1445-1454.

Janssen, M., & Apostolov, A. (2008). IEC61850 Impact on Substation Design. In *Proceeding IEEE/PES Conference and Exposition on Transmission and Distribution*. 1-7.

Janssen, M., & Brand, K., P., (2010). THE SPECIFICATION OF IEC BASED SUBSTATION AUTOMATION SYSTEMS. [Web document]. Switzerland: ABB Power System. Available at: http.www05.abb.com/global/scot/scot221.nsf.nsf/veritydisplay/b0dc46b17050d26bc125705a004de6d5/$file/Brand_Janssen_DistribuTech2005.pdf.

Jiang, K., & Singh, C., (2010). Reliability modeling of all-digital protection systems including impact of repair. In *IEEE Truncations on Power Delivery*. 25:2. 579-587.

Kanbar, M., G., & Sidhu, T., S., (2009). Reliability and Availability Analysis of IEC 61850 Based Substation Communication Architecture. In *IEEE Power & Energy Society General Meeting. PES '09*. 1-8.

Kasztenny, B., Whatley, J., & Udren, E., Burger, J., Finney, D., & Adamiak, M., (2006). IEC61850: A Practical Application Primer for Protection Engineers. In *Proceeding 60th Annual Georgia Tech Protective Relay Conference*.

Kezunovic, (2010). New concept and solution for monitoring and control system for the 21th century substation. In *Proceeding Intrnational Conference onPower System Technology*. 1-7.

Kezunovic, (2010). The Next Generation of Monitoring and Control System Using Synchronized Sampling Technology and Multifunctional IEDs. In *40th. International Conference on System Science*. 117.

Kezunovic, M. (2007). The next generation of monitoring and control system using synchronized sampling technology and multifunctional IEDs. In *Proceeding international conference on System Scenic*. 117.

Kezunovic, M., Guan., Y., & Ghavamt, M., (2010). The 21st century substation design: Vision of the Future. In *Proceeding Bulk Power System Dynamics and Control Conference (iREP.)* 1-8.

Korba, P, Larson, M., Oudalov, A. & Preiss, O. (2005). Looking ahead the future of power system control. [Web document]. ABB Review. Available at:http://www05.abb.com/global/scot/scot271.nsf/veritydisplay/e7fc5528cafb93b0c125701a00495e0d/$file/35-38%202M532%20ENG-72dpi.pdf

Larsson, M. (2009). ABB and Corporate Research Future Challenges. In *Proceeding Next Generation Conference.*

Lenzin, M. (2011). Substation retrofit: Retrofitting Sils subssation with IEC61850 technology. [Web document]. Baden. Power System. Available at:http//www05.abb.com/global/scot/scot299.nsf/veritydisplay/bb15bf73f39cda47852578e000675b7e/$file/Substation%20retrofitfromABBReview.pdf.

Mackiewicz, R. (2006). Overview of IEC61850 and benefits. In *IEEE Power Engineering Society General Meeting*.

McDonald, J., Caceres, D., Borlase, S., Carlos, J., &Janssen, M., (1999). ISA Embraces Open Architecture. In *Transmission and Distribution World*. 51:11. 68.

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2015). Design Principles and Practical Implementation of an Islanding Preventing algorithm Based on IEC 61850-7-420. under review *IEEE* International Conference on Advanced Networks & Telecommunications Systems.

(ANTS 2015) Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2015). Data Modeling in IEC 61850-7-420 for Smart Control Islanding Detection., under review in *IEEE* Transactions on power systems.

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2015). Islanding Detection Algorithm Using IEC 61850-7-420., in Protection Automation & Control pacWorld Conference Galsgow UK 29 June- 2 July 2015.

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2014). Comparative Evaluation of Practical and Simulation SV Traffic Streaming Latency Results within Process Bus Network IEC 61850-9-2LE., in 3rd International Conference on Future Energy, Environment, and Materials October 27-28, 2014, Paris, France (FEEM2014).

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2014). Using OPNET to Model and Evaluate the MU Performance based on IEC61850-9-2LE., in Conquering Complexity: Challenges and Opportunities conference November 3-5, 2014, Missouri University of Science & Technology Philadelphia, PA, USA.

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2014). Novel Approch to Estimate the SV Traffic Streaming Latency Based on IEC 61850-9-2LE in International Conference on Industrial Technology, Management and Education Research Shanghai, China, August 21-22, (ICITMER 2014).

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2014). Enhancing the Configuration of the SAS Task by Using the Vendor-Natural System Configuration Tool, in *IEEE* Canadian Conference on Electrical and Computer Engineering., Toronto, Canada, May 5-8, CCECE2014.

Mekkanen, M., (2014). Interoperatibility and Analysis Issues Based on IEC61850, in proc Vaasa EnergyWeek, Renewable Efficient Energy (REE IV) 20.3.2014/ " , REE IV 2014

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2014). The Needs for the Vendor-Neutral System Configuration Tool based on IEC61850: Introduction and Concept " in proc 1st International Conference on Electrical Engineering and Applications Athens, Greece , MIC electrical 4-6 April 2014 . ,. MIC Electrical 2014

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2014). Analysis and Methodology for Mesuring the IEC61850 GOOSE Messages Latancey: Gaining Interoperability Testing " in proc International Conference on Network Computing and Applications., Hammamet, Tunisia, January 17-19, 2014 , WCCAIS2014

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2013). Communication System in Smart Grid Using Spectrum Sensing Techniques" in proc IEEE Conference PEOCO,2013 Malaysia .PEOCO2013

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2013). Simple Algorithms RaFSA Estimation Method Based on IEC61850" in proc IEEE Conference PEOCO,2013 Malaysia.PEOCO2013

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., Relaibility Evaluattion and Comparison for Next-Generation Substation Function Based on IEC 61850 Using Montecarlo Simulation".IEEE Conference, ICCSPA, UAE, 2013 . UAE_ICCSPA,

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E.,(2012). Reliability and Availability Investigation for Next-Generation Substation Function Based on IEC 61850. (WoWCA2012), Vaasa Finland 2012.

Mekkanen, M., (2010). SPECTRUM SENSING TECHINQUES IN COGNITIVE RADIO: CYCLOSTATIONARY METHOD. [Web document]. Vaasa: Vaasa University Libraray. Available at: http://www.tritonia.fi/?d=248&g=abstr_act&abs=3738.

Mekkanen, M., Virrankoski, R., Elmusrati, M., & Antila, E., (2013). Performance Evaluation of IEC 61850 GOOSE based Interoperability. In *WIT Transaction on Engineering Sciences*. 209-217.

Mekkanen, M., Virrankoski, R.,Elmusrati, M., & Antila, E., (2013). Performance Evaluation of IEC 61850 GOOSE based Interoperability. In *Proceeding International Future Energy Environment Conference FEEM'13*. 209-217.

MEMO, (2011). Q&A on the deployment of smart electricity grids and smart meters. [Web document]. Brussels: MEMO. Available at:http//ec.europa.eu/energy/gas_electricity/smartgrids/doc/20110412_memo.pdf.

Mesmaeker, I., Reitmann, P., Brand, K., & Reinhart, P. (2005). Substation Automation based on IEC 61850. In *Proceeding* 6th *Cigre Conference on SCB5*. Cairo.

Niejahr, J., Englert, H., & Dawidczak H., (2010). Improving IEC 61850 Interoperability: Experiences and Recommendations. In *Proceeding CIGRE, Power System Conference*.

OPNET Modeler, OPNET Technologies. [Web document]. Available at: http://www.opnet.com.

Ozansoy, C., R., Zayeg, A., Kalam, A., (2008). Time Synchronization in a IEC 61850 Based Substation Automation System. In *Power Engineering Conference (AUPEC'08)*. 1-7.

Ozansoy, R. C., Zayegh, A., & Kalam, A. (2009). Object Modeling of DataSet in the International Standard IEC61850. In *IEEE transactions on Power Delivery* 24:3, 1140-1147.

Pedersen, A., Hauksson, E., & Anderson, P., (2010). "Facilitating a Generic Communication Interface to Distributed Energy Resources: Mapping IEC 61850 to RESTful Services. In *Proceeding IEEE First International Conference on Smart Grid Communication*. 61-66.

Prasoon, A., Pratyush, B., Ratnesh, C., Ruchika, D., & Nalini, A. (2009). Substation Automation using IEC 61850. [Web document]. Mgree Project. Available at:http://scribd.com/doc/21058909/Substation-Automation.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, R., Tan, J., (2010). Security Analysis and Auditing of IEC61850-Based Automated Substations. In *IEEE Transaction on Power Delivery*. 25:4., 2346-2355.

Proudfoot, D. (2008). UCA and 61850 For DUMMIES. [Web document]. Available.at:http//www.nettedautomation.com/download/UCA%20and%2061850%20 for%20dummies%20V12.pdf.

PULSECOM, (2010). SUBSTATION COMMUNICATION. [Web document]. Available at:http//www.pulse.com/pdf/datasheets/Substatic.pdf.

Rasmussen, N. (2003). Reliability Models for Electric Power System. [Web document]. Schneider Electric white paper library. Available at:http://www.apcmedia.com/salestools/SADE-5TNQYW/SADE-5TNQYW_R1_EN.pdf.

Rev, J., (1996). Modicon Modbus Protocol Reference Guide. Massachusetts: MODICON.

Ridwan, M., Zarmani, M., Miswan, N., Laijim, R., Awang, H., & Musa, A., (2014). Testing of IEC 61850 Compliant Smart Grid Devices: A Malaysian Experience. [Web document]. CIGRE Technical meeting. Available at: Http//www.cigre-thailand.org/tncf/events/ aorc2014/full_paper/1093R.pdf.

Ridwan, M., Zarmani, M., Miswan, N., Laijim, R., Awang, H., & Musa, A., (2012). Testing the Interoperability of IEC 61850 Intelegent Electronic Devices A Tenaga Nasional Berhad Experience. In *Proceeding OMICRON, Asia-Pacific Protection and Testing Conference*.

Ridwan, M., Zarmani, M., Miswan, N., Laijim, R., Awang, H., & Musa, A., (2012). Testing the Interoperability of IEC 61850 Intelegent Electronic Devices A Tenaga

Nasional Berhad Experience. In *OMICRON, Asia-Pacific Protection and Testing Conference.*

Saccomanno, F. (2003). ELECTRIC POWER SYSTEM Analysis and Control. USA: IEEE Press.

Selim, T., Cagil, O. & Zayegh, A. (2012). Modeling of a Centrallized Micrgrid Protection System and Distributed Energy Resources According to IEC 61850-7-420. *IEEE Transactions on Power System* 27:3, 1560-1567.

Sethi, A., & Hnatyshin, V., (2013). The Practical OPNET User Guide for Computer Network Simulation. New York: CRC Taylor and Francis group.

Shoemaker, T., & Mack, J. (2002). Substations. 12th. USA: McGraw Hill. 85-107.

Sidhu, T., & Gangadharan, P. (2005). Control and Automation of Power System Substation using IEC61850 Communication. In *proceeding IEEE conference on Control Application.* 1331-1336.

Sidhu, T., S., & Yin, Y., (2007). Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems. In *IEEE Transaction on Power Delivery.* 22:3. 1482-1489.

Sidhu, T., Yin, Y., (2007). Modelling and Simulation for performance Evaluation of IEC61850-Based Substation Communication System. In *IEEE Transaction on Power Delivery.* 22:3. 1462-1489.

Singh, C., & Patton, A., D., (1980). Protection system reliability modeling: Unreadiness probability and mean duration of undetected faults. In *IEEE Transaction.* 29:4.,339–340.

Stallings, W., (2007). Data and Computer Communication. 7th. USA: Prentice Hall. 497-530.

Steinhauser, F., Schossing, T., Klien, A., & Geiger, S., (2010). Performance Measurements for IEC 61850 IEDs and Systems. [Web document]. Protection Automation Control World. Available at:https//www.pacw.org/no-cach/ issue/december_2010_issue/performance/implementing_firewalls_for_modern_ substation_cybersecurity/complete_article/1/print.html.

Tholomier, D. & Jones, L. (2010). VISION FOR A SMART TRANSMISSION GRID. In *Proceeding international conference on bulk Power System Dynamics and Control (iREP).* 1-12.

Turunen, J. (2011). A Wavelet-based Method for Estimating Damping in Power System. Helsinki. Alto University library. Available at:https://aaltodoc.aalto.fi /bitstream/handle/123456789/4930/isbn9789526040516.pdf?sequence=1

Turunen, J., Larsson, M., Korba, P., Jyrinsalo, J. & Haarla, L. (2008). Experiences and Future Plans in Monitoring the Inter-area Power Oscillation Damping. In *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century.* Pittsburgh. 1-8.

UCA, (2011). INTEROPERABILITY TEST IEC61850 INTEROPERABILITY. [Web document]. Available at: http://testing.ucaiug.org/IOP_Registration/ /2011%20CIM61850%20IOP/IOP%20Reports/IEC%2061850%20IOP,%20Paris ,%20France%20UCAIug-63-111Rv1.pdf.

UIS, (2007). Substation Automation. [Web document]. Utility Information System. Available at:http://usico.net/substationautomation.htm.

VTT, (2009). Energy visions 2050. [Web document]. Porvoo: WS Bookwell Oy. Available at:http://www.vtt.fi/files/publications/EnergyVisions_2050.pdf

William, A., G., (1986). STATISTICAL SPECTRAL ANALYSIS A NON PROBABILISTIC THEORY. NJ: Prentice-Hall.

Xie, Z., Manimaran, G., Vittal, V., Phadke, A., & Centeno, V. (2002). An Information Architecture for Future Power System and Its Reliability Analysis. *IEEE transaction on Power System* 17:3, 857-863.

Yunus, B., & Musa, A., Ong, H., S., Khalid, A., & Hashim, H., (2008). Reliability and availability study on substation automation system based on IEC 61850. In *IEEE 2nd Power and Energy Conference, 2008. PECon*. 148-152.

Zhang, C., Tan, J., Kirby, B., Thompson, S., & Bo, Z. (2009). Modeling and Implementation Device Based on IEC61850. In *Proceeding IEEE Conference on Electrical engineering*.

Zhang, L., X., & Kumal, N., (2008). Testing Protective Relays in IEC61850 Framework. In *Proceeding Power Engineering Conference (AUPEC'08)*. 1-6.

Zima, M., Larsson, M., Korba, P., Rehtanz, C., & Andersson, G., (2005). Design Aspect for Wide-Area monitoring and control systems. In *IEEE Proceedings*. 93;5. 980-996.

APPENDICES

Appendix 1

In this part, we intended to present the simulation scenarios for the evaluation of the probability of failure for one protection IED, general bay protection function and BFP function upon different SAS communication network bus topologies. The same concepts of our observation that had been discussed in Chapter 2 for the reliability estimation analysis can be made here for the probability of failure estimation. Let's first consider a single IED. According to the analytical results the true value of the probability of failure is (Q(t)=0.0644930149) for single IED as illustrated in Table 8. Where, the RaFSA estimation result values for the probability of failure for single IED are illustrated in Figures 114-118. From Figure 116 the probability of failure values are significantly random variated about the true value when the number of trials was small, ±0.02450 at trial 100. Further, infrequently the true value (Q(t)=0.0644930149) occurs in trials (32, 47 and 75). Where, the number of instances that the values of the probability of failure were greater than the true value was approximately equal to number of instances when the probability of failure values were less than the true value. As a result, the main of the probability of failure values was 0.06283720836 and the standard deviation was 0.06441576092. Lastly, as the number of trials was increased the variations of the probability of failure result values were reduced. However, the result values of the probability of failure were still remaining variant even at trial 10000, but the variation was reduced significantly and had a tendency towards the true value. A a result, the main was 0.06455271952 and the standard deviation was 0.00710325701 as illustrated in Fig. 118.

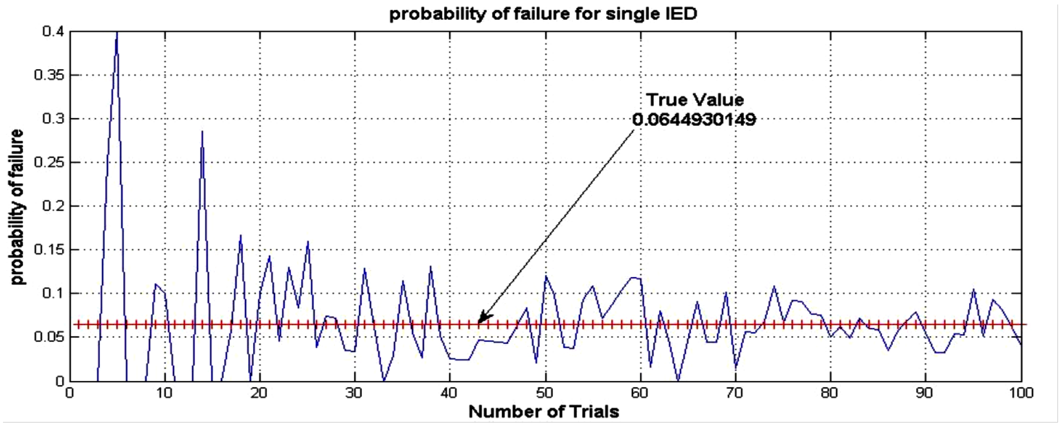


Figure 116. Probability of failure for single IED 100 trials**.**

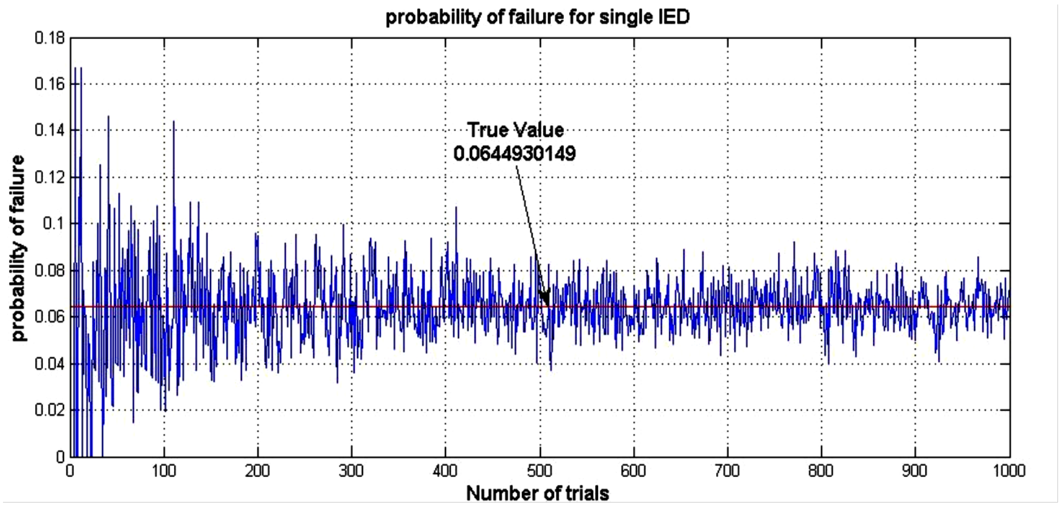


Figure 117. Probability of failure for single IED 1000 trials.

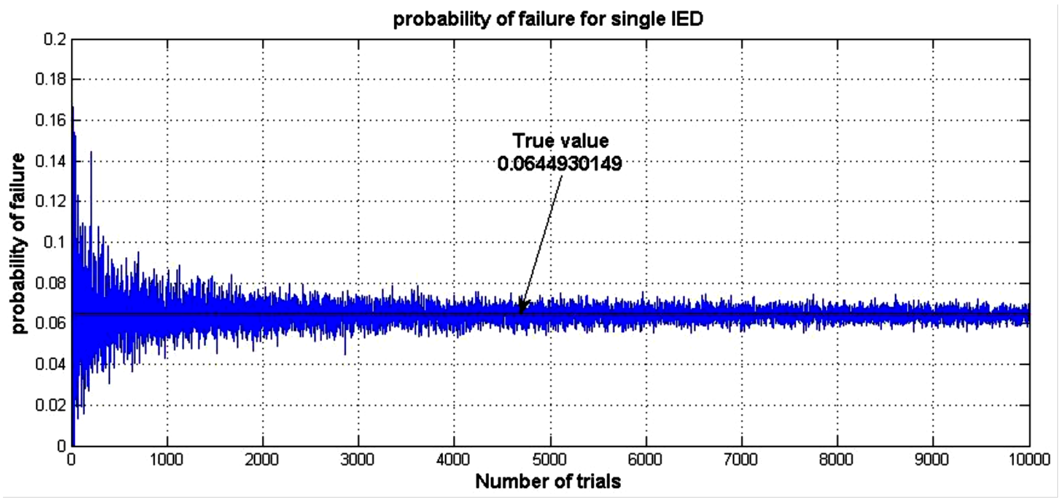


Figure 118. Probability of failure for single IED 10000 trials.

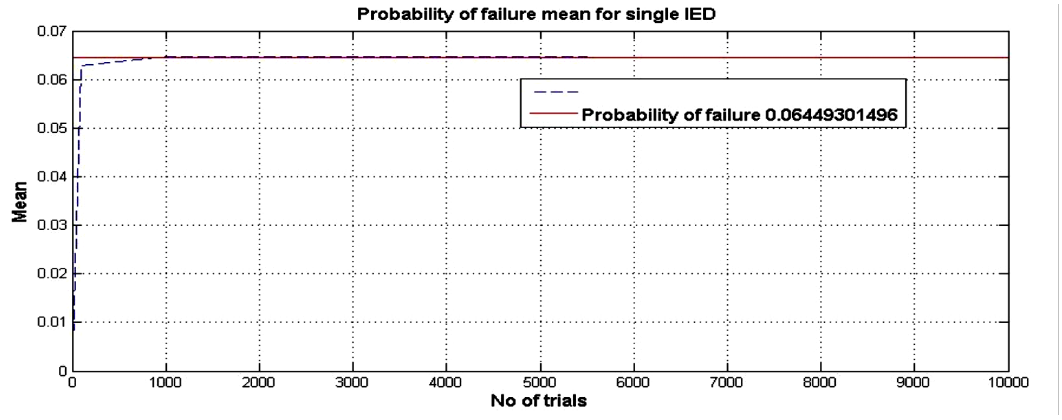


Figure 119. Probability of failure mean for single IED.

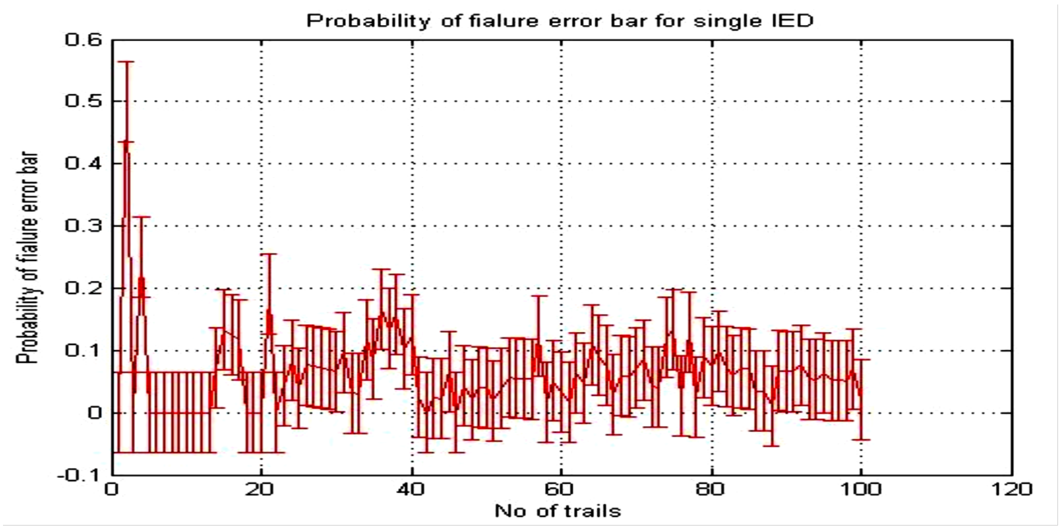


Figure 120. Probability of failure error bar for single IED.

Secondly, in case of the probability of failure estimation through RaFSA method for general bay protection function, the estimation result values were illustrated in Figures 119-123, the true value upon the mathematical calculations for the probability of failure result value was (Q(t)=0.045577538). From Figure 121 the probability of failure result values were significantly random variated about the true value when the number of trials was small, ±0.00057 at trial 100. Further, infrequently the true value Q(t)=0.045577538 was occurs in trials 44 and 86. Where, the number of instances that the result values for the probability of failure were greater than the true value is approximately equal to number of instances when the probability of failure result values were less than the true value. As a result, the main of the probability of failure values was 0.04950890549 and the standard deviation was 0.05990042920. Lastly, as the number of trials was increased the variations of the probability of failure values were reduced. However, the values of the probability of failure were still remaining variant even at trial 10000, but the variation was reduced significantly and had a tendency towards the true value. Therefore, the main was 0.06455271952 and the standard deviation was 0.00710325701 as illustrated in Figure 125.

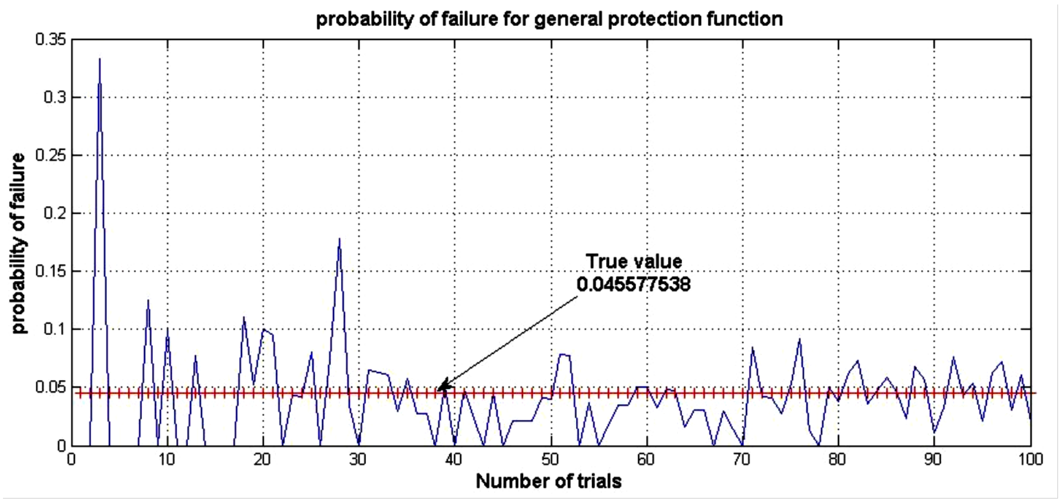


Figure 121. Probability of failure for GBPF 100 trials.

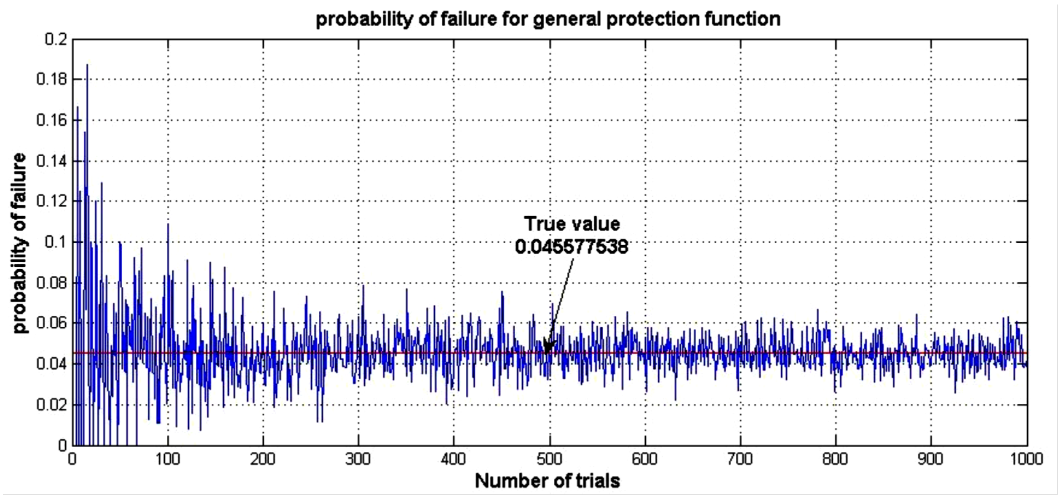


Figure 122. Probability of failure for GBPF 1000 trials.

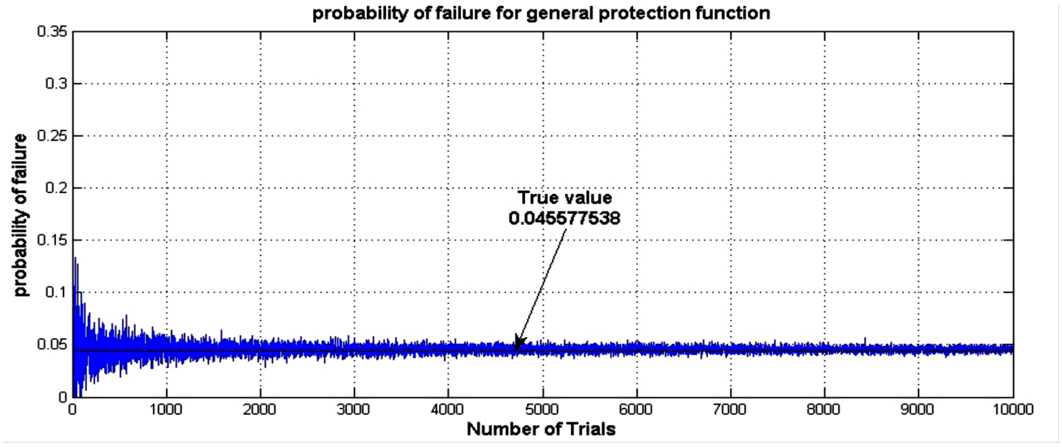


Figure 123. Probability of failure for GBPF 10000 trials.

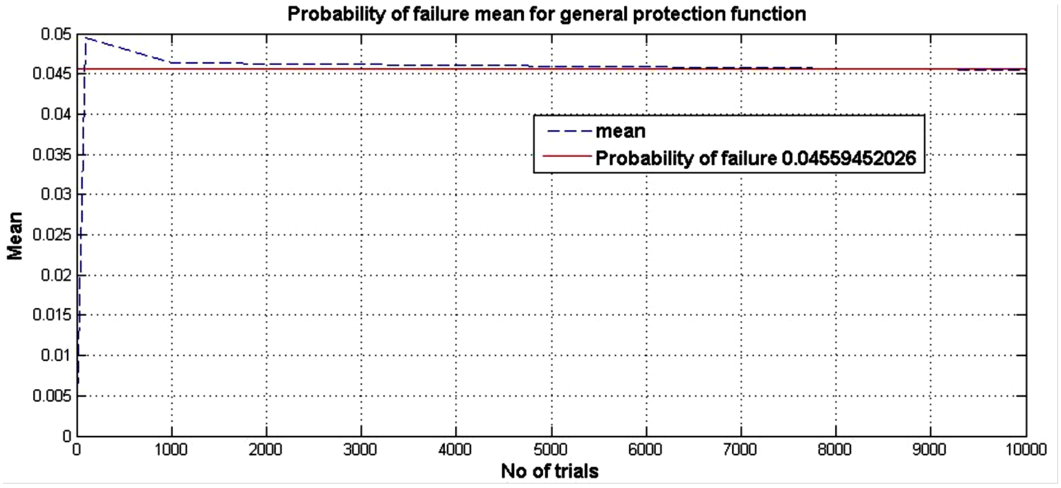


Figure 124. Probability of failure mean for GBPF function.

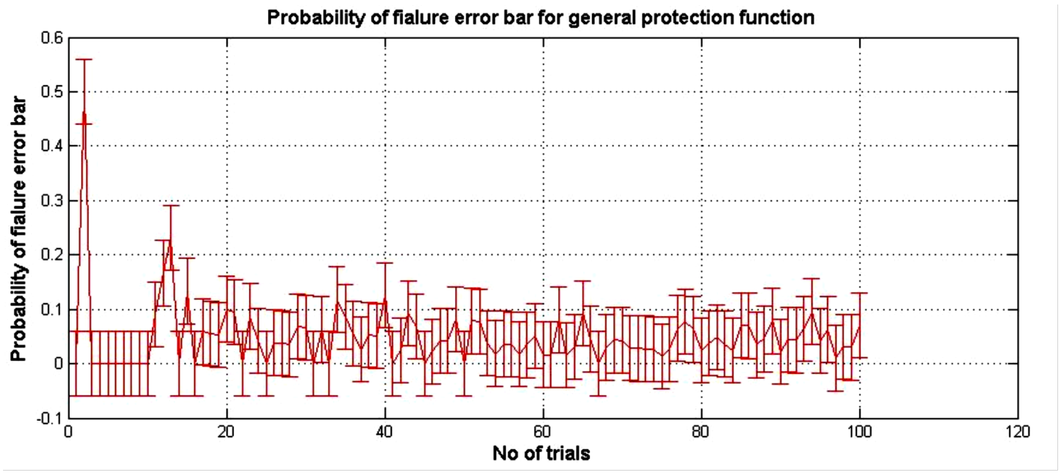


Figure 125. Probability of failure error bar for GBPF function.

Thirdly, we consider the probability of failure estimation for the BFP function for the cascaded SAS communication network bus topology through RaFSA estimation method. The estimation result values were illustrated in Figures 126-130. The true value upon the mathematical calculations for the probability of failure was Q(t)=0.01702797362. From Figure 126 the probability of failure values were significantly random variated about the true value when the number of trials was small, ±0.020 at trial 100. Further, infrequently the mathematical result true value Q(t)=0.01702797362 was occurs in trials (70, 77, 82 and 88). Where, the number of instances that the values of the probability of failure were greater than the true value is approximately equal to number of instances when the probability of failure values were less than the true value. As a result, the main of the probability of failure values was 0.16159198450 and the standard deviation was 0.08025559475. Lastly, as the number of trials was increased the variations of the probability of failure values were reduced. However, the values of the probability of failure were still remaining variant even at trial 10000, but the variation was reduced significantly and had a tendency towards the true value. Therefore the main was 0.17034559108 and the standard deviation was 0.01408304809 as illustrated in Figure 128.

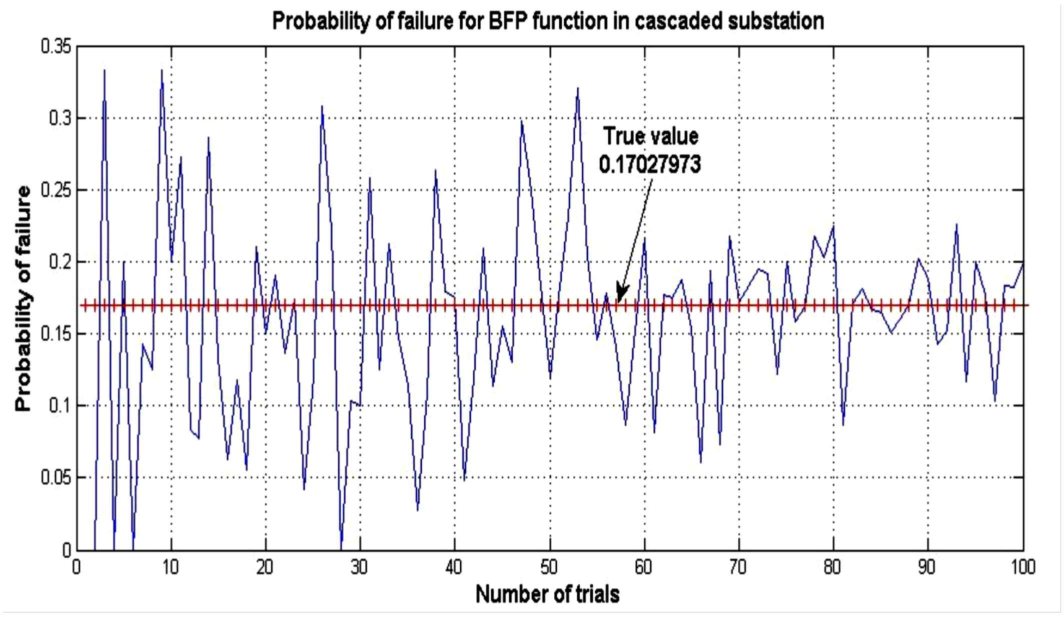


Figure 126. Probability of failure for BFP for the cascaded SAS 100 trials.

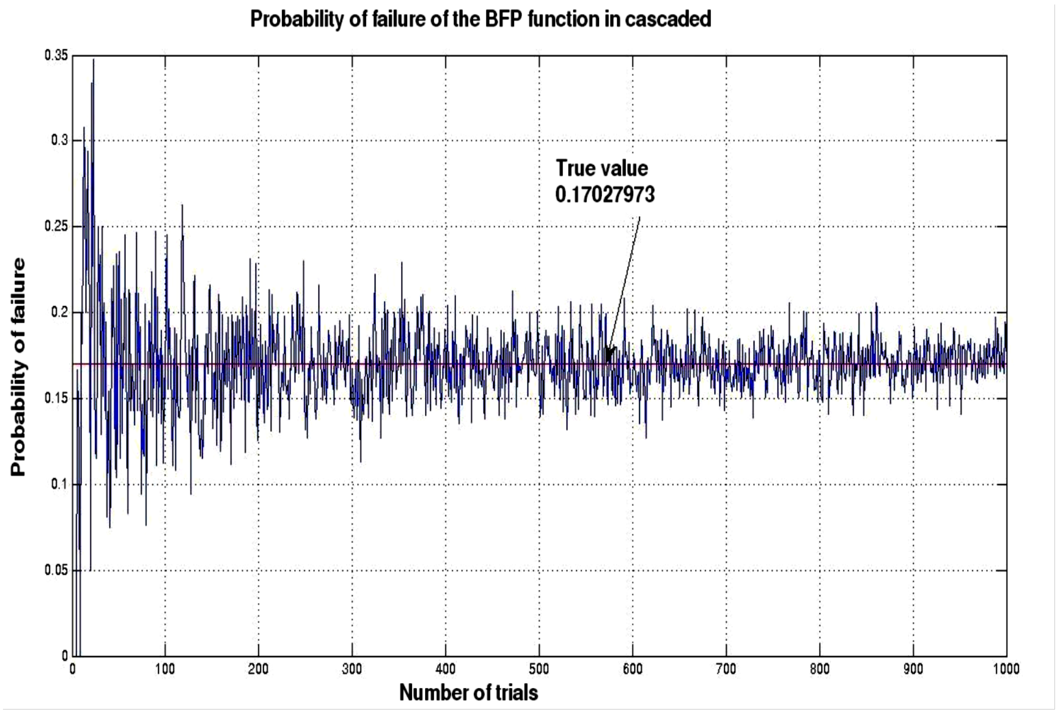


Figure 127. Probability of failure for BFP for the cascaded SAS 1000 trials.

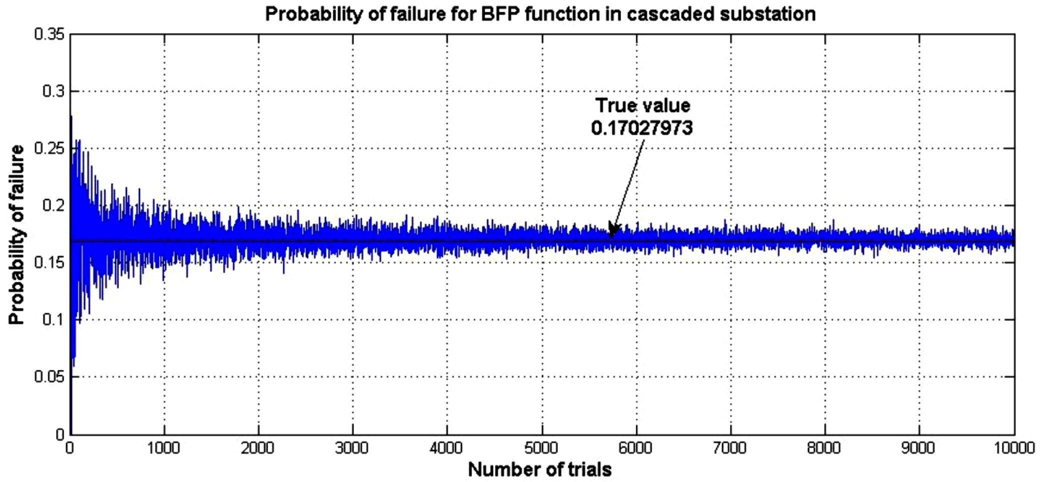


Figure 128. Probability of failure for BFP for the cascaded SAS 10000 trials.

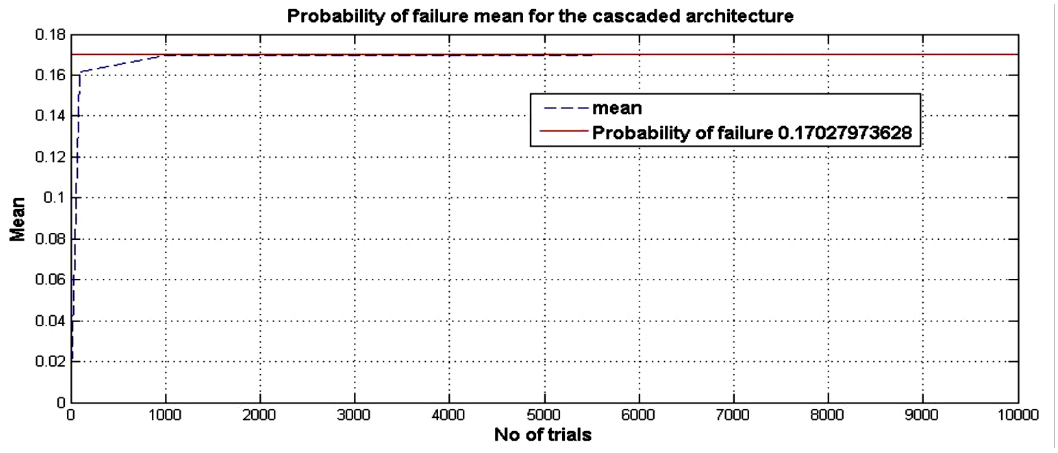


Figure 129. Probability of failure mean for BFP for the cascaded SAS.

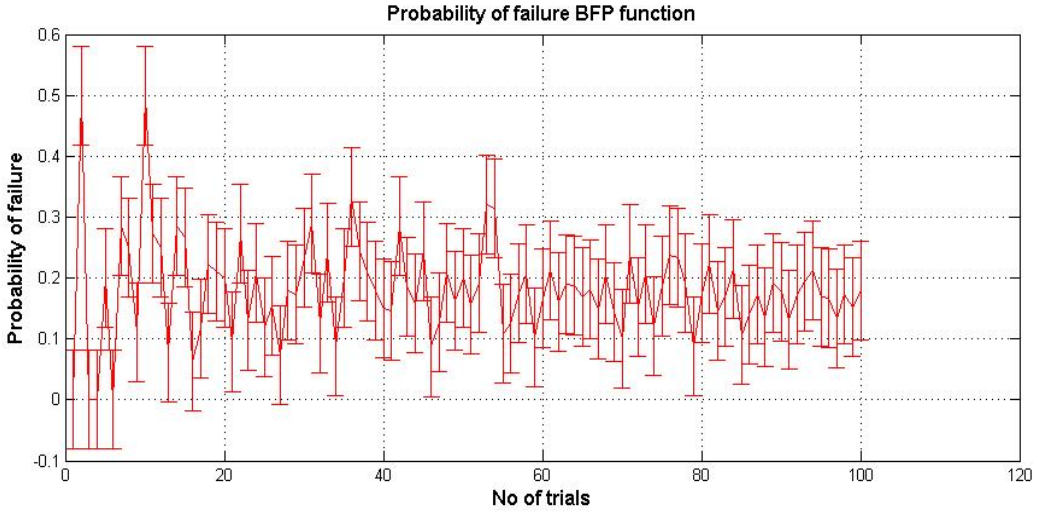


Figure 130. Probability of failure error bar for BFP for the cascaded SAS.

Lastly, in case of the probability of failure estimation through RaFSA method for the redundant ring SAS communication network bus topology, the estimation result values were illustrated in Figures 131-135, the true value upon the mathematical calculations for the probability of failure result value was (Q(t)=0.0978396137). From Figure 131 the probability of failure result values were significantly random variated about the true value when the number of trials was small, ±0.0316 at trial 100. Further, infrequently the true value Q(t)=0.0978396137 was occurs in trials 72 and 92. Where, the number of instances that the result values for the probability of failure were greater than the true value is approximately equal to number of instances when the probability of failure result values were less than the true value. As a result, the main of the probability of failure values was 0.10016937835 and the standard deviation was 0.07320785920. Lastly, as the number of trials was increased the variations of the probability of failure values were reduced. However, the values of the probability of failure were still remaining variant even at trial 10000, but the variation was reduced significantly and had a tendency towards the true value. Therefore, the main was 0.09768267111 and the standard deviation was 0.00937645051 as illustrated in Figure 133.

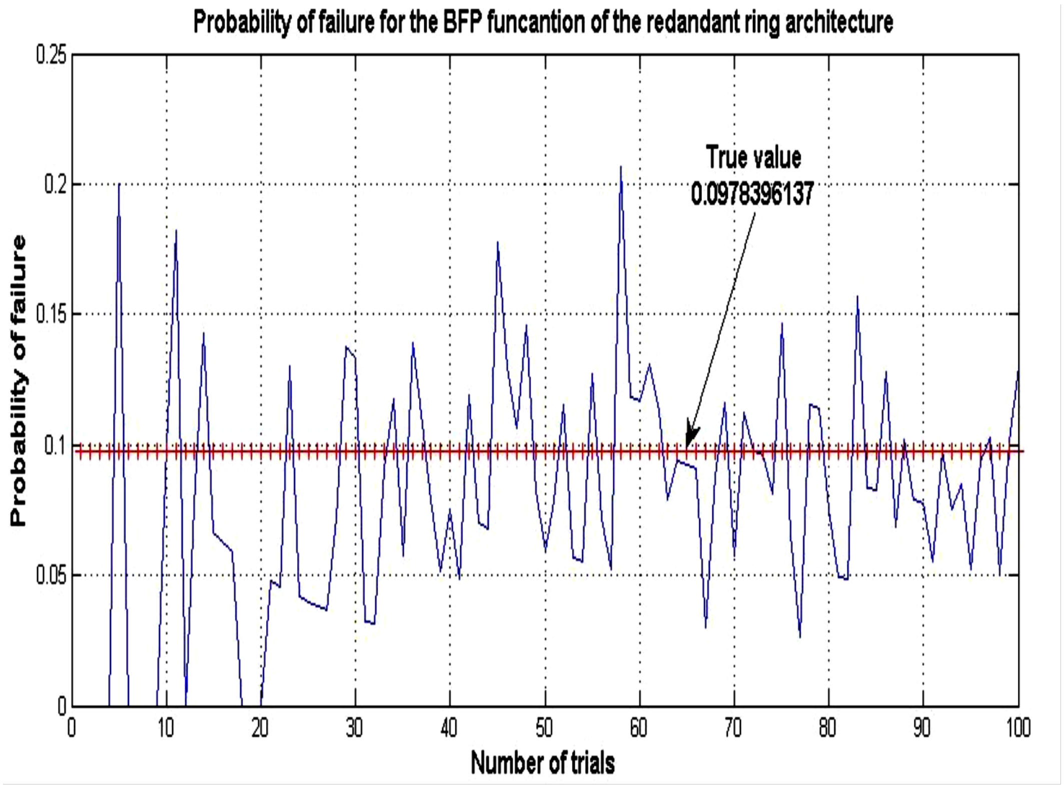


Figure 131. Probability of failure for BFP for the redundant ring SAS 100 trials.

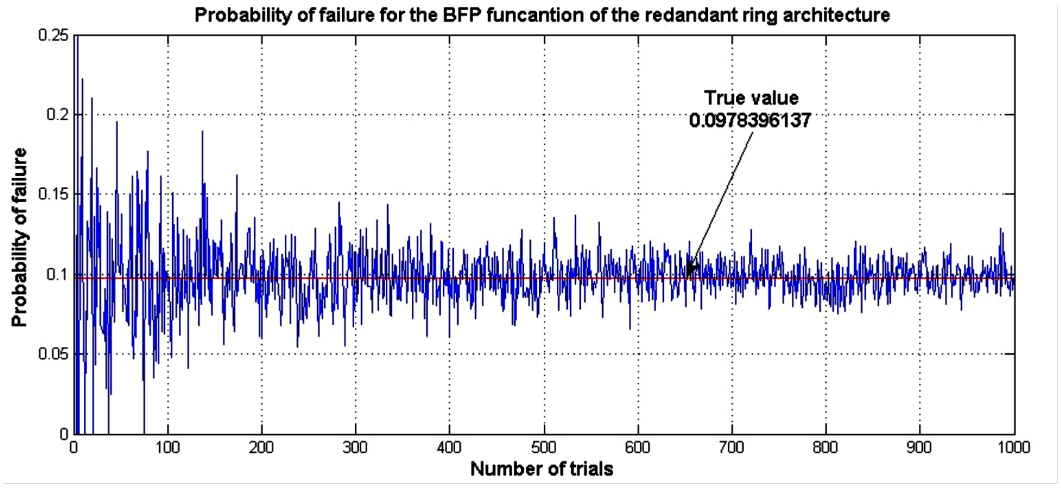


Figure 132. Probability of failure for BFP for the redundant ring SAS 1000 trials.

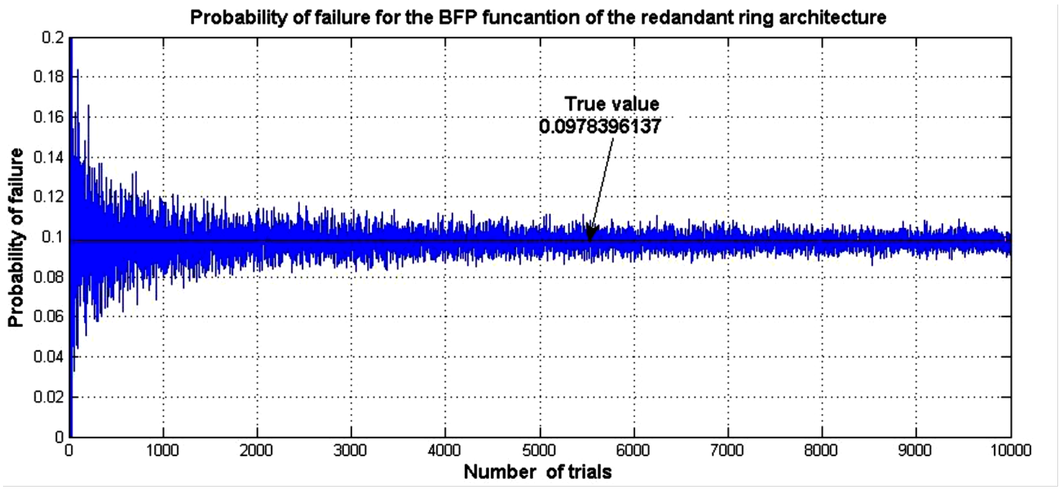


Figure 133. Probability of failure for BFP for redundant ring SAS 10000 trials.

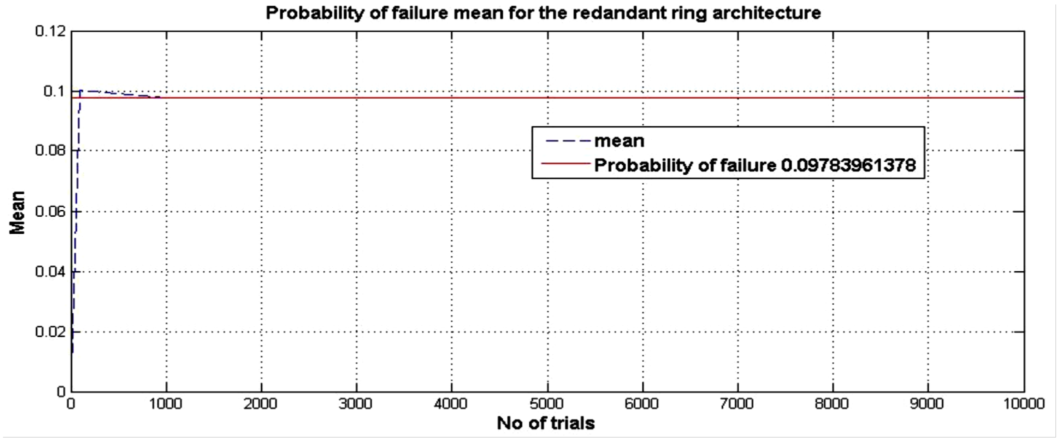


Figure 134. Probability of failure mean for BFP for redundant ring SAS.

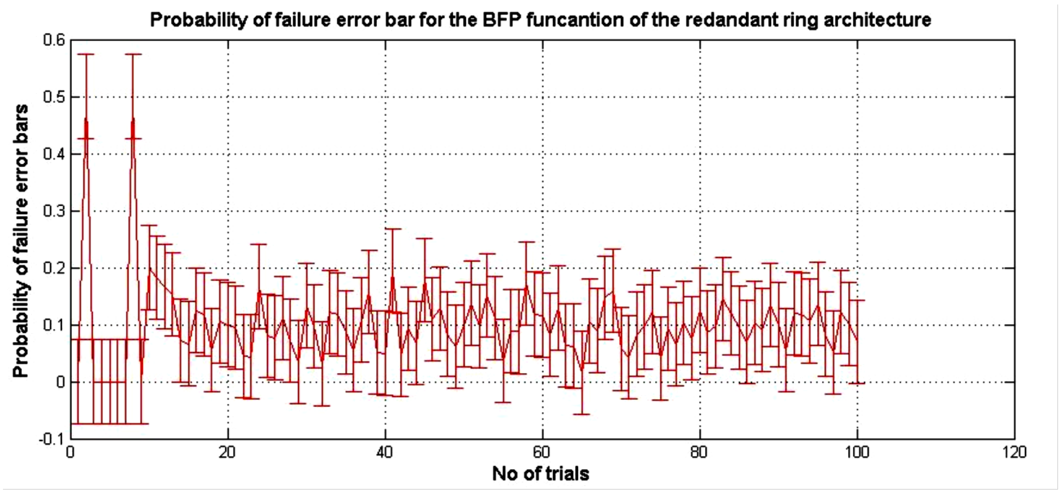


Figure 135. Probability of failure error bar for BFP for redundant ring SAS.

From the novel RaFSA probability of failure estimation method, mean and standard deviation result values with the probability of failure analytical result values for the above various SAS communication network bus topologies were illustrated in Table 18.

Table 18. Probability of failure, analytical result values, means and standard deviations for Various SAS bus topologies.

Single IED trials	Mean	STD	Probability of failure analytical result values
100	0.06283720836	0.06441576092	0.06449301496
1000	0.06463912439	0.02127783774	0.06449301496
10000	0.06455271952	0.00710325701	0.06449301496
GBPF trial			
100	0.04950890549	0.05990042920	0.04559452026
1000	0.04641035280	0.02554942821	0.04559452026
10000	0.04553403984	0.00578643601	0.04559452026
Cascaded trials			
100	0.16159198450	0.08025559475	0.17027973628
1000	0.16967653843	0.02881141111	0.17027973628
10000	0.17034559108	0.01408304809	0.17027973628
Ring trials			
100	0.10016937835	0.07320785920	0.09783961378
1000	0.09768792123	0.02303774519	0.09783961378
10000	0.09768267111	0.00937645051	0.09783961378

Further, upon our observation about the achieving result values we are able to conclude that as follows:

- Generally, significant variations (errors) of the RaFSA probability of failure estimation result values about the true value occur when the number of trials is small.

- Infrequently, the true value occurs, in particular, random trials. However, for real system this would not be known.

- The number of instances that the values for the RaFSA probability of failure estimation result values are greater than the true value is approximately equal to the number of instances when the probability of failure values are less than the true value. Therefore, the main of the probability of failure values is approximately equal to the true value.

- The deviation from the RaFSA probability of failure estimation result values had been reduced as the number of trials is increased. Moreover, the probability of failure estimation values are still variant even after trial 5000, however the variation is reduced significantly to least value.

- In each analysis procedure, we need to estimate the probability of failure values from several simulations. Each simulation has different output data (result). However, all simulation results share the same characteristic that these results have the tendency toward the true values.

According to the result values of the probability of failure based on the analytical and RaFSA estimation solutions, we observed that the SAS cascaded topology provided higher values than the SAS redundant ring topology, since it has non-redundant Ethernet switches, which constitute the bottleneck of the SAS reliability. Furthermore, all Ethernet switches need to work successfully (series) to execute the SAS (BFP) function. The advantages that can be achieved by SAS cascaded topology is less expensive and simple configuration. Whereas, the redundant SAS ring provides the lower values in which that increase the reliability of the SAS. This result indicates that introducing redundancy in the Ethernet network has a greater impact on improving SAS reliability. However, on the other hand, it increases SAS complexity and costs. Therefore, it needs more practical and careful upon its implementation.