Integrating the Power Transformer Protection Scheme to Telecontrol Terminal Unit (RTU)

By

Bhekinkosi Pheneas Madonsela

A thesis submitted in fulfillment of the requirements for the degree of

MASTER IN ELECTRICAL ENGINEERING

DEPARTMENT OF ELECTRICAL POWER ENGINEERING

DURBAN UNIVERSITY OF TECHNOLOGY

December 2018

Supervisor: Prof. I. E. Davidson

Co-Supervisor: Dr. T.C. Mulangu

DECLARATION OF ORIGINALITY

I, Bhekinkosi Madonsela, declare that

1. The Master's thesis entitled performance characteristics of smart substation has not been submitted for any other academic degree or diploma at any other university.
2. This thesis holds my original work and the information of other person's that is acknowledged as other person's data.
3. All graphics copied and pasted from internet are referenced accordingly
4. Moreover, this thesis symbolizes my own sentiments and not necessarily those of the Durban University of Technology.

DEDICATION

I dedicated this work in a thankful heart to my mother for her endless support during my studies. Lastly, I extend my appreciation to my father and siblings to support and encouraged me to finish this thesis.

ACKNOWLEDGEMENTS

I would like to express my appreciation to GOD for being the source of my strength physically and emotionally needed to carry out this research project. Secondly my warm regards goes to my main supervisor Professor I.E Davidson for his invaluable support, substantial remarks and career constructive advices. I also express my earnest appreciation to my co-supervisor Dr. C. Mulangu for his perceptive comments and ideas he gave me to improve my research. Lastly, my appreciation goes to my manager for me granting the access to Eskom software packages and laboratories to carry out the simulation of this research.

ABSTRACT

Automated substations and distribution networks are key element of smart grid, however not all substations and distribution networks are automated to date due to the numerous reasons such as cost related to automation and scarcity of skilful workforce. With the drive to integrate renewable energy to the national smart grid, the advanced and innovative integrating methodologies need to be investigated. Automating the power system is the effort to improve power supply security, availability and reliability. Reliability is very important in substation automation systems and is achieved through real-time monitoring of the substation data. The interconnection of substation through substation automation devices is crucial because it provide the backup link to the network in case one substation fails. The utilities has developed a remarkable interest in substation automation due to the benefit its offers such as; reduction in maintenance and, operating cost and improved revenues due to stable power system networks. Substation automation is made up of four main functions that need to be fused together; protection, control, monitoring and, local and remote communications. There are numerous communication protocols available in the market for substation automation applications. However not all of them are utilized in the current application of smart grid.DNP3 and IEC61850 are the leading communication protocols currently. DNP3 has proved its technical advantages over the past few years in substation automation applications. On other hand IEC61850 was only published in 2003 and became more popular in substation around 2006; the standard is only fifteen years old. IEC61850 define the protocols such as; GOOSE, SMV, GSSE, GSE and MMS using its communication profiles. This research will investigate the possibilities of integrating DNP3 data point into IEC61850 data model. With this approach; the legacy substation shown in figure 1.1 will inherit the advantages of IEC61850 such as high speed data exchange, interoperability and interchangeability

Key word: Interoperability, DNP3, IEC61850 standard, GOOSE, GSE, SMV, MMS

DECLARATION 2- PAPER PUBLICATIONS

The following publications emanated from this research investigation:

[1] B Madonsela, Innocent Davidson and C Mulangu, "Advances in Telecontrol and Remote Terminal Units (RTU) for Power Substations", *Proceedings of the IEEE Power Africa Conference,* 26 – 29 June, 2018, Cape Town, South Africa, pp. 504-509.

[2] B Madonsela, Innocent Davidson and C Mulangu, "Integrating DNP3 Devices into IEC61850 Server", *Proceedings of 3th Interdisciplinary research and innovation conference*, September, 2018, Peter Mokaba Ridge, South Africa, pp.1-6. Paper is accepted to be published in Interdisciplinary Journal of Economics and Business Law (IJEBL).

TABLE OF CONTENT

TABLE OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACSI	Abstract Communications Service Interface
ADU	Application Data Unit
AI	Analogue Inputs
ANSI	American National Standards Institute
AO	Analogue Outputs
ARC	Auto-Reclose
BCD	Binary Coded Decimal
CB	Circuit Breaker
CDC	Common Data Class
CID	Configured IED Description
CRC	Cyclic Redundancy Checks
CSMA/CD	Carrier Sense Multiple Access or Collision Detection
CSD	Configuration Substation Description
CT	Current Transformer
DC	Direct Current
DCA	Data Collecting Application
DFR	Digital Fault Recording
GE	General Electric
DI	Digital Input
DNP	Distributed Network Protocol
DO	Digital Output
DPA	Data Processing Application
DTA	Data Translation Application
EF	Earth Fault
FTP	File Transfer Protocol
GOMSFE	Generic Object Models for Substation or Feeder Equipment
GOOSE	Generic Object Oriented Substation Event
GSE	Generic Substation Event

GSSE Generic Substation State Event

GVRP Generic VLAN Registration Protocol

HMI Human Machine Interface

HSR High-availability Seamless Ring

ICD IED Configured Description

IDF Intermediate Distribution Frame

IEC International Engineering Consortium

IEC TC International Electrotechnical Commission Technical Committee

IEC61850 International Substation Communication Protocol

IED Intelligent Electronic Device

IEEE Institute of Electrical and Electronic Engineers

IP Internet Protocol

ISO International Standards Organization

IUG International Users Group

LAN Local Area Network

LD Logical Device

LED Light-Emitting Diode

LLC Logical Link Control

LN Logical Node

LSB Least Significant Bit

MMS Manufacturing Message Specification

MSVCB Multicast Sampled Value Control Block

MSB Most Significant Bit

NCIT Non-conventional instrument transformers

NIST National Institute of Standards and Technology

OSI Open Systems Interconnection

PC Personal Computer

PDU Protocol Data Unit

PTP Precision Time Protocols

ROS Rugged Operating System

RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
Rx	Receive
SAN	Storage Area Network
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SCC	Substation Control Centre
SCD	Substation Configuration Description
SCL	Substation Configuration Language
SCSM	Specific Communication Service Mapping
SEL	Schweitzer Engineering Laboratories
SEF	Sensitive Earth Fault
SM	Single Mode
SMV	Sampled Measured Value
SSD	System Specification Description
SV	Sampled value
TCP	Transmission Control Protocol
Tx	Transmit
UCA	Utility Communications Architecture
UDP	User Datagram Protocol
USVCB	Unicast Sampled Value Control Block
VLAN	Virtual LAN
VMD	Virtual Manufacturing Device
VT	Voltage Transformer
WAN	Wide Area Network
XML	eXtensible Markup Language

Chapter One: Introduction

This chapter provide the introduction of the proposed study including the objectives, original contribution, and definition of the problem statement and research questionnaires of the project.

1.1 Introduction

Substation Automation Systems (SAS) includes: control, monitoring, and protection for electric power generation, transmission and distribution applications. Solutions range from single function protection and control units to fully integrated, comprehensive, and high-performance substation automation systems[1]. With the current demands of electric energy on daily basis, the utilities are determined to generate, transmit and distribute electricity consistently. The constant delivery of electric energy is very crucial to the end user and is achieved through automated power system. Substation automation is used to achieve a secured point of electric supply through monitoring, control, protection and communication functions. Substation automation systems allow the collection, consolidation, processing, visualization and reporting of the system operational and non-operational data[1]. The purpose of this study is to integrate the devices operating on legacy Distributed Network Protocol (DNP3) to the newly developed IEC61850 standard to improve reliability and efficiency of existing power system. By doing so the large investments of existing devices will be not lost due to the emerging of new communication technologies. Enhancing or upgrading the existing automation systems is an economical option to adopt new communication standard other than complete replacement of existing devices. Deploying advanced technologies, leveraging the interoperability's, designing a system to meet current extensive needs - with the ability to migrate to higher level systems as our business demands - are all essential to a successful substation automation implementation[1]. In conventional substations that still exist within the power network, substation equipment such as switchgear and transformer, control, protection, and monitoring apparatus are independent of every other device.

A number of long cables are then used to complete the links between these devices in order for them to communicate. This method is uneconomical and it is therefore very important to refrain from these old technologies systems and embark on the application of new technologies. Automation engineers and technicians need comprehensive knowledge of substation automation technologies. Unfortunate, the introduction of IEC61850 standard brought numerous challenges. Beside the technical concerns related to GOOSE, the documentation of the standard as a whole is difficult to understand especially for those who are not substation automation specialist. Following are the challenges with regard to the comprehensive analysis of the standard

- IEC61850 standard adopted the most sophisticated sets of technologies for specific automation applications, which is not easily accessed by engineers and researchers that are not specializing in substation automation. The terms and definitions used to the present the standard are not similar to those generally used in legacy protocols and engineering software's for substation automation applications. That means it's difficult for engineers to read the standard, even worse for general substation operators.
- IEC61850 standard application concept is mostly defined using tables and pictures; this is a problem because it is hard for engineers and technicians to understand all tables used in the complete documentation. The concept of IEC61850 should have been easily understood if the proper comprehensive presentation was done. On other hand the standard defined twenty nine common data classed with eighty nine appropriate logical nodes, but the exact relationship between them is not clear to the end user.

Modbus, UCA and DNP3 development provided significant benefits in substation automation environment. However modbus protocols used complex communication structure and it was not possible to extend it to afford smart grid requirements. DNP3 was first established for basic serial communications network and was further extended for high speed peer to peer communication over Ethernet, because smart grid is an Ethernet driven infrastructure. According to [2] the substation automation communication standards were first introduced in late

1970’s. The standards and protocols were rapidly adopted for substation automation applications across the globe to improve the reliability of power supply. The substation automation communication network designed according to Modbus and DNP3 can be always modified to the current and future requirements[2].

1.2 Problem statement

The currently installed Intelligent Electronics Devices (IEDs) in DNP3 substations hold huge capital investments. Most of these devices were commissioned after 1993 where the DNP3 was first introduced and the general lifespan of substation power plant apparatus is between 40 to 60 years; the high voltage layout is attached to (appendix A-1). The digital relays normally last for 7 to 10 years. That alone means the oldest substation to date is 25 years remaining with 15 to 35 years more. However there is a new substation communication standard (IEC61860) that was developed few years ago to address the issues that were experienced with hardwired systems. Due to the fact that substation automation devices ranging from protection relays to telemetry systems are expensive and the currently installed DNP3 devices are having more years remaining in their lifespan, the utilities are considering the option to continue with DNP3 substation automation even though there is a new standard. DNP3 is a globally recognized standard that offered the features of smart substation such as: interoperability between devices, high speed peer to peer communication reduced software costs, easily expanded to adapt in new technologies and etc. All these advantages are adding to the reason why the utilities oppose the replacement of currently installed DNP3 devices. Beside the issue of capital investment that is held by DNP3 devices, there are numerous challenges that prevent the adoption of newly published substation communication standard (IEC61850) in South Africa. These challenges are: financial constraints, lack of knowledge with regard to IEC61850 and ambiguities with IEC61850 that still need to be explained. From the technical view not all utilities are keen to the IEC61850 standard. Even though there are these challenges, the distribution substations are the key point of customer power supply that still needs a proper automation and control.

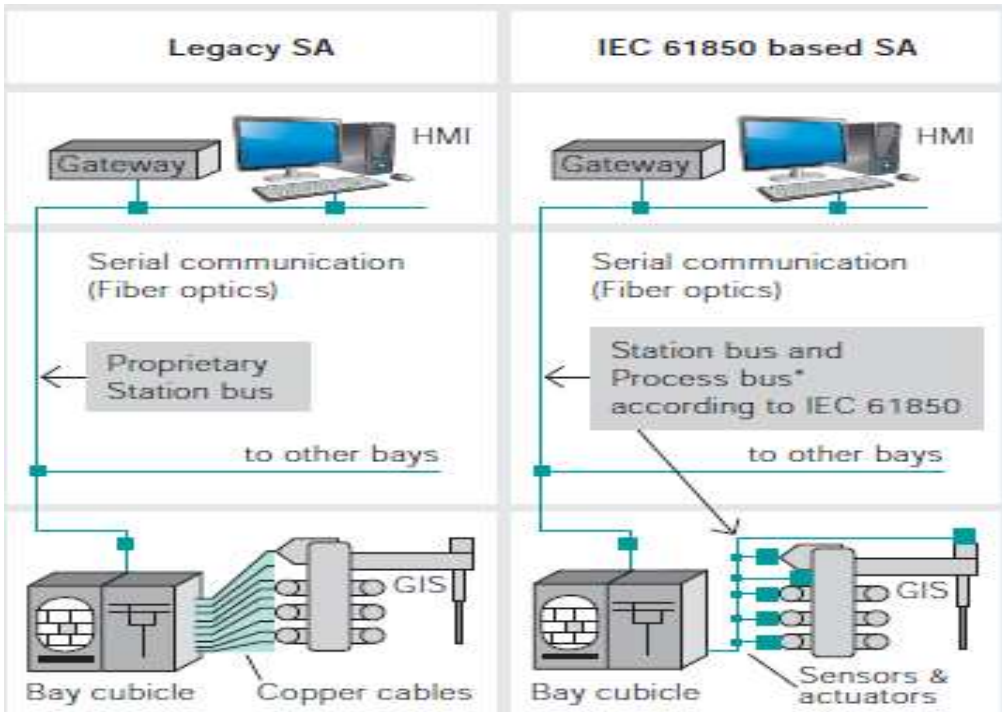


Figure 1.1: Architecture of legacy and IEC61850 substation automation systems [1]

Figure 1.1 shows the architecture for both legacy substation automation and IEC61850 based substation automation systems[1]. In terms of its architectures there is a minor difference between them, that means there is no need of replacing the legacy devices to adopt the new standard more especially if the challenges stated above still exist. However deep to the configuration of these devices there are numerous differences between these two architectures. Substation automation devices are multi-functional as they perform numerous functions such as: protection, metering, monitoring, data acquisition and control. This result to the very high installation costs of the automation systems. The electrical infrastructure is the largest and expensive infrastructure in the world that plays a crucial role in economic growth. Substations need to be interconnected to construct smart grid that is the domain requirement to ensure that adequate and reliable power supply is being generated and distributed to customers[3]. This means continuous development of substation automation is mandatory even though there are challenges. Better solutions need to be investigated taking care of the existing substation automation devices and the issue of improving the performance of those devices.

1.3 Aims and Objectives

1.3.1 Research aim

The main aim of this research is to investigate the alternatives of improving the operations of existing substation by integrating DNP3 legacy devices into IEC61850 server. This research is not aiming to support hardwired real-time control of substation devices that need the interconnection of control panels; rather offer an economical strategy to improve the performance of existing substation equipments through the manipulation of DNP3 data. The specific aim of this research work is summarized as following:

a) To deliver a feasible assessment of improving the performance of currently installed legacy devices by integrating DNP3 data points into IEC61850 server.

1.3.2 Research objectives

This research work will focus on how the legacy protocol can be incorporated into IEC61850 protocols other than the complete replacement of the currently installed huge base of DNP3 devices. The results are expected to improve utility revenues and further improve efficiency of currently installed devices. To achieve the above mentioned aim and further provide the solutions to the research key question, the research objectives of this research work will focus on the following key points:

a) Delay Performance analysis

b) Delay aware back off analysis

c) Reliability evaluation

1.4 Key Research Questions

With respect to the problem statement definition, the key question of this research is formulated as following:

"How feasible is the application of IEC61850 server in DNP3 substation in the effort of ensuring the advanced substation automation and control to some existing distributions substations? Can its application validate it as a better alternative method to modernize the legacy distribution substations, and further improves the overall efficiency and data retrieval capabilities of substation devices?"

With regard to the question above the work of this research proposed to integrate DNP3 data points into IEC61850 data model to offer a solid path toward the full implementation of the IEC6150 and ensure that the utilities will continue to utilize the remaining life span of the currently installed devices while improving revenues to address financial issues. The general idea of this research thesis develops the paradigm of integrating the devices of existing substation with the information of other bases to expedite the implementation of innovative substation automation applications. This architecture will not support the use of bulky wiring to interconnect the devices. However it will provide a cost effective and user friendly migration strategy so that, so that it will be more profitable and reliable to operate the currently installed devices.

1.5 Project Limitations and Delimitations

The research project is limited to the integration of DNP3 data points for power transformer and feeder protection relay into IEC61850 server through substation gateway and further compares the communications capabilities of serial and Ethernet based network. The following tasks form part of the project:

a) Remote Terminal Unit (RTU) and protection IEDs hardware integration;
b) RTU and protection IEDs software integration;
c) RTU configuration;
d) Simulate the master station;
e) Simulate monitor to detect data traffic;
f) IEC61850 and DNP3 Software modeling;
g) IEC61850 server to IEC61850 client communication testing;

The following activities fall outside of the scope of the research project;

a) Development and implementation of a complete IEC 61850 control model; that uses the Select-Before-Operate method;
b) Programing protection settings to protection relays;
c) Testing protections relays;
d) GOOSE protection massages testing;
e) Protective relay designing;
f) Protection relay wiring;
g) SCADA system operational development and analysis;
h) Design and installation techniques of current transformer and voltage transformer;
i) High Voltage (HV) yard designing, installation and testing;
j) Tripping of a real substation circuit breaker;
k) Management /or control of network communications within the Substation Automation Systems ;
l) Development of an IEC 61850 communication stack; and
m) Engineering access devices installation, designing and testing;
n) Sampled values analysis and mapping

1.6 Research methodology and design

From the technical point of view, there seems to be a strong link between the native IEC61850 and DNP3 standard. The link between these protocols enables the manipulation of DNP3 data and further represented in IEC61850 format. The detailed analysis of the similarities between will be done through the collection of published scientific data. The collection of published scientific data will enable the researcher to quantify and measure the feasibility of integrating DNP3 data into IEC61850. The existing literature review of DNP3 and IEC61850 will be used to further present the explanation of the proposed study. The work of this research focuses to the manipulation of specific DNP3 data that are selected to be represented in IEC61850 format. In order to provide better solution to the problem statement and research key questionnaire stated in the brief discussion above the following research methodologies are anticipated:

a) Literature review – A chronological analysis of substation communication protocols and standards will be conducted. These protocols and standards are: Modbus, DNP3 and IEC61850. Since the research focuses in DNP3 and IEC61850 a clear understanding to the similarities of these protocols is essential. A detailed review of intelligent substations and unified substation data will be conducted.

b) Software configuration methods – There are numerous software that are required to configured the whole system ranging from protection relays to IEC61850 server. To achieve interoperability between DNP3 devices there must be a clear understanding of eXtensible Mark-up Language (XML) structure.

c) Hardware interfacing – Almost all data that is needed to operate substations locally and remotely comes from integrated devices. Hence experimental investigations need to be conducted on how the substation devices can be integrated to improve their efficiency. This will also provide clear understanding of the device user applications and firmware application.

d) Performance analysis and testing – Testing is the crucial parts that will validate the whether the DNP3 has been mapped into IEC61850 using additional software's and devices. In this additional IEC61850 client is required to simulate the communication between IEC61850 server or DNP3 gateway and IEC61850 client. The performance analysis of substation devices will be done here to substantiate the feasibility of the proposed study. The results and logarithm values calculated by software testing tools will be used to draw the comparison between the performance of DNP3 serial and DNP3 LAN. Furthermore the comparison of data availability for both DNP3 serial and DNP3 LAN/IEC61850 is drawn here using values extracted from testing tools.

1.7 Significance of the study

This thesis is to provide solutions on how to adopt IEC61850 in existing substation without changing the entire automation devices in order to achieve advanced substation automation in a cheaper and reliable technique on a temporary basis. The biggest challenge with the adoption of the IEC61850 in existing substations is the costs associated with complete replacement of devices while there are some technical issues that have not been cleared with regard to IEC61850. The results of this work are expected to provide a mapping procedure between DNP3 and IEC61850 to improve the performance legacy substations. Substation automation is actually a technology that isolates operating personnel from manual handling of high voltage apparatus. If the network is not automated, the customers will experience serious power supply interruption and long downtime. This situation is not ideal and the flexibility must be added to the network to reduce the effect of supply interruption on the customer terminal. The adoption of an advanced substation automation results in a better service and greater customer satisfaction. Shorter downtimes and faster restoration of supply will increase the revenues. In other words, well designed substation automation significantly boosts profitability, electrical power reliability, availability, efficiency and safeguards power company assets. But few of above mentioned advantages has been achieved, therefore to achieve well satisfactory automation system that will meet worldwide needs. It's clear that, the application IEC61850 standard is justifiable and is a reliable solution for future substation automation systems and smart grids; however it's costly to replace the whole matured automation network within substation environment

1.8 Project Contributions

The outcome of this research will offer numerous contributions ranging from technical point of view to economical point of view and customer satisfaction. There various dynamics that forcing the electric utilities to improve the quality, and reliability of power supply and concurrently reduce the implementing and operating costs. Improved power system management, reduced plant maintenance costs, reduce power outages, better quality of supply and advanced substation automation functions are among the key benefits expected to be achieved with this study model. This research will also contribute to the academic domain, since many universities still does not have IEC61850 standard incorporated in their curriculum, hence this research will offer a detailed analysis of IEC68150 and substation automation. The contributions of the thesis for operational use can summarized as following:

a) Optimized network efficiency;
b) Improved quality of supply;
c) Enable the remote switching of substation equipments;
d) Improve the supervisory control for substations devices;
e) Increase the availability of power system data to the rightful user and further improve the integrity checking of data communicated between devices;
f) Provide interlocking functions for power transformer protections;
g) Provision of the real time information to the local monitoring machine and etc.

1.9 Publications emanating from this thesis

[1] B Madonsela, Innocent Davidson and C Mulangu, “Advances in Telecontrol and Remote Terminal Units (RTU) for Power Substations”, *Proceedings of the IEEE Power Africa Conference,* 26 – 29 June, 2018, Cape Town, South Africa, pp. 504-509.

[2] B Madonsela, Innocent Davidson and C Mulangu, “Integrating DNP3 Devices into IEC61850 Server”, *Proceedings of 3th Interdisciplinary research and innovation conference*, September, 2018, Peter Mokaba Ridge, South Africa, pp.1-6. Paper is accepted to be published in Interdisciplinary Journal of Economics and Business Law (IJEBL).

1.10 Thesis Outline

The methodology of this research consists of four main comprehensive sections: Data collection for literature review, research methodology describing the laboratory simulation, results analysis and documentation.

1.10.1 Data collection

Data collection to conduct a thoroughly literature review with regard to smart substation automation, legacy protocols (Modbus, DNP3) and new communication standard IEC61850 since the clear understanding of these systems is required along with its contributions to the substation automation applications. Literature review concludes with the remarks.

1.10.2 Laboratory set up and modelling

This research project is developed to incorporate legacy protocol DNP3 and newly developed IEC61850 standard to take the advantages of legacy devices currently installed in substations, and communicating over DNP3 Transmission Control Protocol (TCP) and further impact the adoption of the new standard. The description of devices and configuring tools used to achieve the research goals are described in the methodology. The substations IEDs are configured to perform the following functions; control, monitor protection and communications. However, this project is primarily focusing in communication function of the IED.

a) Identification of all tools required to configure communication settings to the devices;
b) Incorporation of IEC61850 server application into gateway configuration tool;
c) Configure DNP3 communications settings into protection relays and substation gateway;
d) Generate System Configuration Description (SCL) files in an eXtensible Mark-up Language (XML) format to enable the mapping between the DNP3 database and IEC61850 server;
e) Integrate the DNP3 data points into IEC61850 server.

1.10.3 Discussion and results analysis

System testing is a verification of the work that has been done providing laboratory test and other system verification measures.

1.10.4 Research documentation

The documentation of this research thesis comprises of six chapters summarized as following.

Chapter 1: Introduction

Chapter one will present the introduction of the research. It will give a preview on how the study is to be demonstrated and establish the significant points of the topic. It will cover the following: background, problem statement, objectives and aims, key research questions, significance of the study, project contributions, project delimitation and limitations.

Chapter 2: Literature Review

Chapter two will present the literature review which will be taken from the existing knowledge base, substantive findings as well as theoretical and methodological contributions made by other researchers relating to this subject. The information contained in chapter two is extracted from several journals, articles, textbook and technical papers

Chapter 3: Smart substation and system configuration

This chapter will present the description of the devices to be used for laboratory simulations and also provide descriptions of the software are used to configure the devices. Lastly is to provide a detailed procedure of step by step mapping between DNP3 and IEC61850 server.

Chapter 4: Results and Analysis

This chapter will present the discussion and analysis of the results for all experimental tests conducted with regard to the mapping between DNP3 and IEC61850. The chapter will also provide the performance comparison between DNP3 serial and Ethernet, DNP3 solicited and unsolicited.

Chapter 5: Conclusions and future work

Chapter five provides the summary of the thesis and represents the conclusion along with the recommendations for future work.

1.11 Conclusion

In conclusion this chapter presented the thesis aim and objectives, the terms and concepts used throughout the thesis. The problem statement of the research and the analysis of steps taken in order to accomplish the research objectives are given. The thesis is aimed at modelling DNP3 data into IEC 61850 server.

Chapter Two: Literature Review

This chapter will provide a comprehensive review of substations automation constitution discussing the role of substation IEDs, Distributed Network Protocol (DNP3) and IEC61850 communications as introduced in chapter one. This chapter also provides synopsis of traditional communication protocols, and standards such as; Utilities Communication Architecture (UCA) and Modbus. The balance of this chapter present the network topologies commonly used in substation applications.

2.1 Introductions

Electrical power system is a cooperative term used to describe the process of energy generation, transmission, distribution and reticulation to consumers. This requires a well built and thoroughly monitored infrastructure to ensure that; the energy reaches the consumers at an acceptable level [4]. Power system infrastructure is the largest infrastructure across the world made up of generation stations, transmission and distribution substations, pole mounted transformers, and recloser and power lines spreading across the geographical region of any country [3]. Power substations are critical components of the electric power grid where voltage transformation, line switching, line compensation and other control functions are carried out [3]. Automated substation has central role to play in stabilizing the power system network across the world. Recently, substation automation is responsible for numerous functions other than protection, monitoring and control. Those functions are the metering, operational data management and synchronization of renewable energy to the national grid [5]. The operations of production industries and other facilities rely on the electricity that is generated from centralised power stations and interconnected to each other. These power stations are connected to transmission and distribution substations where the power is regulated for the end user. The current developments with regards to climate changes have increase the energy prices; that have forced the utilities to transform the power system network into decentralised architecture. Decentralised architecture allows the bi-directional flow of electricity through the use of intelligent switching devices installed in generating and distributing stations. In order to create the reliability to the power system network; the operations of these generating units, transmission and distribution substations must be automated through the use of SCADA system since they are all over the geographical area of every country. SCADA system is used to monitor the status for each and every point of connection for the power system network.

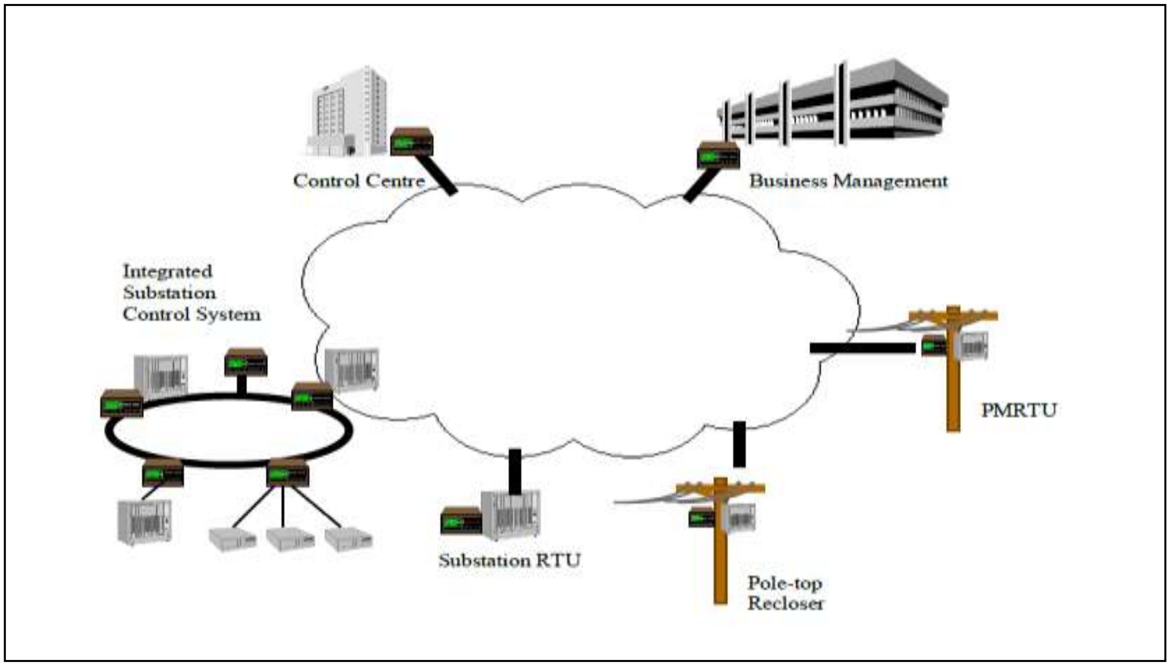


Figure 2.1: Network Integration through the addition of distributed, intelligent, real-time data servers [3].

Figure 2.1 shows the interconnection of power system network extending from substation telemetry unit to control centre and pole mounted recloser to improve the security and the reliability of the supply. Utilities has resolved to adopt the integrated and automated protection, measurement and control solutions for intelligent substations to maximize network visibility and reliability, while minimize installation and maintenance costs [3]. This thesis advocates the integration of DNP3 data points and IEC61850 data model to avoid replacement cost while providing solid path toward the full implementation of IEC61850. In Figure 2.2, the concept of substation automation system is presented that is divided into three main sections. The Interface referring to the node where all system meets, device integration and communication denoting the integration of telemetry units to protection relays and the concept of communication protocols, lastly is the real-time data networking denoting the accuracy of data communicated in station level and control centres.

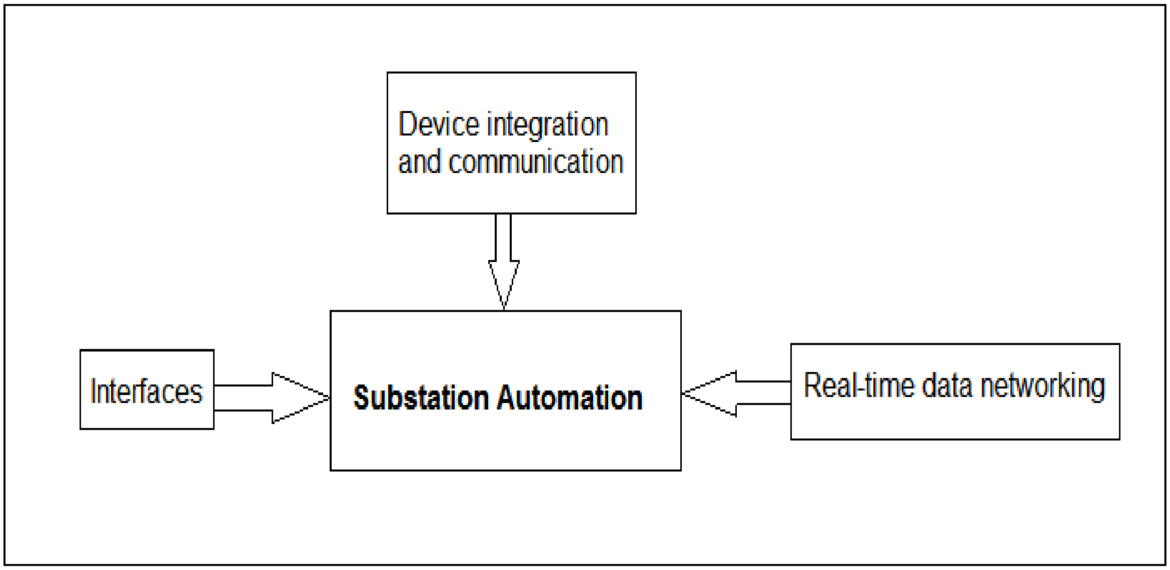


Figure 2.2: Simplified substation automation systems architecture.

This is the proposed architecture to address the problem stated in chapter one.

2.2 Substation device interface

The substation device interfacing is referring to the use of a programme, protocols and devices to enable the communication between integrated devices. In recent applications; the communication of the substation devices is driven by real-time data networking using advanced monitoring techniques so that the reliability of the power system infrastructure is improved. Therefore to improve the trustworthiness of the power supply at the substation level; the integrated substation devices must share data and communicate rapidly [6]. Figure 2.2 introduced the composition of substation automation that is further expanded as following;

2.2.1 Data and device integration system

The substation integration system must interface with all devices connected to the channel. This must include the device data retrieval, device polling and events reports [6].

2.2.3 The user interface

In order to operate substation devices a simple user interface is required to create the database library and represent the power system network in graphical display format [6]. The substation library must be coordinated with SCADA systems and control centres.

2.2.4 The substation communication interface

The integrated substation devices uses communication interface to acquire data, process data and determine the status of power system apparatus. The substation communication interface must support all communication protocols used by devices [6].

2.2.5 The fundamentals of communication protocol

The substation device needs communication protocol to exchange data and facilitate the message build up in the network [6]. The detailed concept of communication protocol is discussed in section 2.4.

2.3 The role of substation devices

Substation IEDs are used for numerous purposes within substation automation systems that fall within: protection, metering, monitoring, control and communication. Once these functions are integrated the substation automation system is formed and the system must be able to perform the following functions: data acquisition, supervision, control, data processing, advanced monitoring and remote process interface.

2.3.1 Data acquisition

This is a collection or acquiring of data within substation and outstation. The data is collected and represented in appropriate forms for further processing [7].

2.3.2 Supervision

Once the data has been collected, processed and converted, continual supervision and updating of the data is mandatory to ensure that, the data represented in control is latest [7].

2.3.3 Control

This is an exchange of commands between master station and slave substation. Controls can be executed locally using push buttons to operate [7].

2.3.4 Data processing and management

The term radical data processing is used to explain the collection of data, processing data, upload and display the data to the substation HMI. All substation data is collected from protection IEDs, and statistics meters and converted into a suitable format for further processing before is being stored in system point database. Real time monitoring enables the advanced data processing and management between substation devices and outstation devices [8].

2.3.5 Advanced monitoring and alarming

Substation data monitoring is very important and the data must be updated at all times to provide the control centers with recent substation events. The recent studies have shown that; the future substations will be able to provide an early warning alarm to authorized users via handheld mobile devices [8, 9].

2.3.6 Remote and advanced process interface

For smart substations device integration, it is valuable to outspread the process interface beyond the hardwired connections in the bay processor terminals (mostly in transmission substation) and other devices to permit remote access and advanced data processing [8].

2.4 Substation real- time data networking

Electrical substation is a key point of power supply that is used to supply customers with electric energy. Substations are secondary stations from power generations that are used to regulate the frequency and the voltage using numerous automation devices integrated in the network. To improve the security and reliability of the supply the integrated devices must reach to each other effectively to share the information that is required to operate the grid. The substation data that is collected by devices need to be distributed immediately between devices responsible for the specific function and this called real time data exchange [10]. The real time data can be stored in data warehouse for offline investigations. Real time networking provides the wide range of information from a specific device such as device location, status and event time. In recent applications the real time data networks in substations uses horizontal and vertical communications. Horizontal communications refer to the communication between protection relays whereas vertical communication refers to the communication between protection relays and substation telemetry units. The substation automation communication systems play a crucial role in the exchange of real time data exchange to operate the power system network [10]. Substation automation devices are interlinked through communication channels and buses. The real time data includes control commands, device status reports, communication status logs, exchange of protection messages (GOOSE) and transfer of sample measured values. The performance of real time data networking have got its challenges that need to be attended such network traffic and loss of data in transit. The solution to this issue is to design a reliable communication network and configure the devices to send the data continuously until arrival conformance is received. This feature is applicable with both DNP3 and IEC61850.In many applications where reliability is the prime requirement; the network interface card is used that support the concept of receiving the frames through the host computer. The data is collected using wireshark for future analysis. Network traffic can limit the speed of real time data exchange between devices. However this can be dealt with by utilizing mirror port that copies the traffic from one port to the alternative ports available in the network [6, 10]. However the mirror port technique does not provide the preservation of accurate time for data. The reliable communication network of the substation automation must have the following devices to ensure the network redundancy; Ethernet switch, hubs, routers, servers and media [11].

2.5 Communication protocols and standards

Power systems infrastructure (Generating units, Transmission and Distributions substations) is made up of expensive equipments, hence its need to be monitored and controlled remotely using the set of protocols and standards. Communication protocols are key elements of substation or distribution automation since its guide the exchange of data between IEDs within substation and control centres. Communication protocols also enable the control centres to remotely perform the following functions: load transferring, switching, load flow analysis, energy consumption analysis and anomalous event downloading. In 1980, there were at least six major shared protocols and another four proprietary protocols along with few “utility-unique” protocols such as Estel-variant that was solely developed for Eskom. Communication protocols are defined as the set of instructions that are used in substation or distribution automation to control the exchange of data between different systems of the integrated devices. Communication protocols are used for local and remote exchange of data. Substation automation protocols and technologies needs to be sustained and innovated to meet the demand of future power systems [12]. The most important protocols and standards that are related to this research are: Modbus, DNP3, UCA 2.0 and IEC 61850. Recently, all communication protocols are represented in terms of seven (7) layered Open System Interconnection (OSI) model as presented in figure 2.3. This model is used to manage data movement between system, devices and network [12].

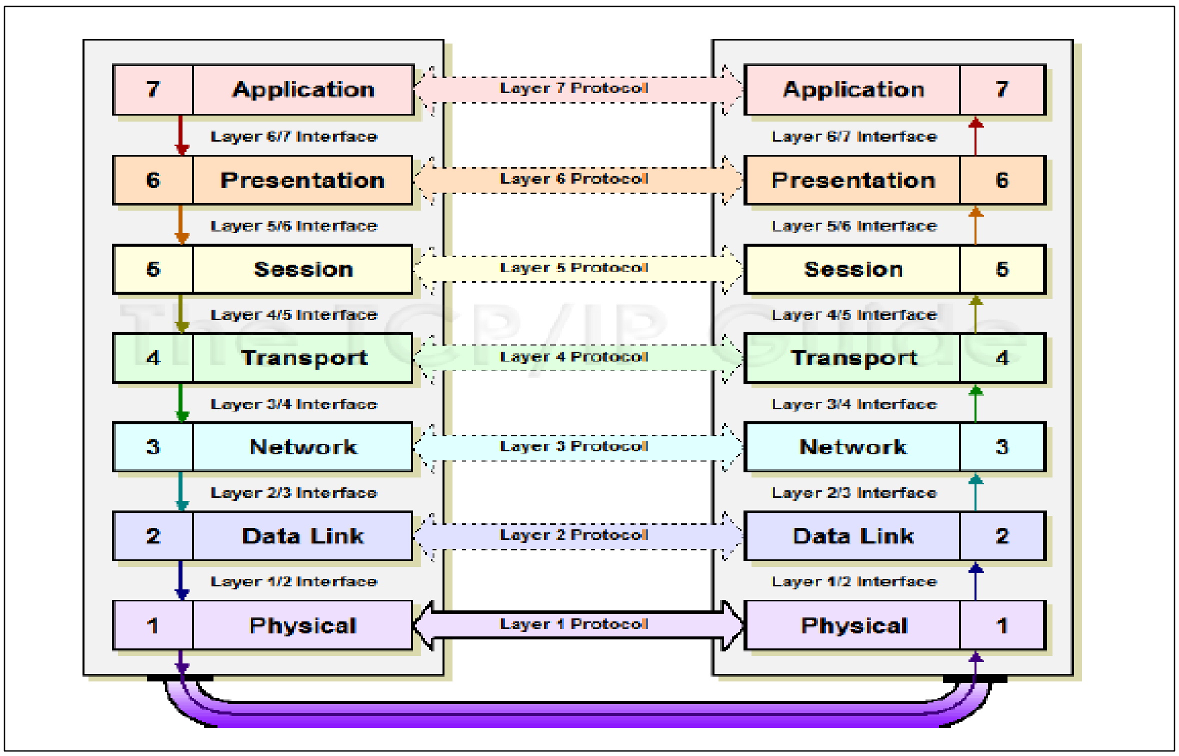


Figure 2.3: ISO models of communication protocols [12].

The OSI model provide the information needed by the operators to clarify the communication control profiles such as data sequence control, error detection control and request time out control.

a) **Application layer**: this layer is used for communication via the network.
b) **Presentation layer**: the data is transmitted one device to be received by another device in same or different network for further application in a system, presentation layer process the data so that will be recognized by receiver or receiving devices.
c) **Session layer**: this layer is used to initiate connection so that data packets will be transmitted, once all data packets has been transmitted it's terminate the connection.
d) **Transport layer**: its controls the flow of data, provide data acknowledgments notifications and facilitate the retransmission of data when there is no notification of data arrival to the recipient.
e) **Network layer**: it's provide supplementary network address to the packets and routing of data
f) **Data link layer**: this is a layer that is used to offer MAC address
g) **Physical layer**: it's used for hardwire transmission of data.

The OSI model (figure 2.3) briefly analyses the breakdown of all tasks that are required when transmitting data from one host to another in seven steps[12].

2.5.1 Communication standardization

Upon the introduction of microprocessor-based IEDs, the number of open and proprietary protocols for communication simply multiplied. By the 1980's, there were more than hundred proprietary protocols of communication available to be used in substation automation communications. This had made it difficult for utilities to achieve interoperable communication between different vendor equipment within the substation. Therefore the requirement of standardizing a substation communication became the next target for the national and international bodies of standardization (American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), IEEE, ISO and International Electrotechnical Commission (IEC). The standardization substation communication started in 1986 and resulted to the publication of UCA (Utility Communication Architecture). The introduction of UCA brought the first resolution concerning to the IEDs interoperability issues. This review will only consider four popular substation communication protocols and standards. Those are Modbus, DNP3, UCA and IEC61850.

2.5.2 Modbus

Modbus is the basic client/server communication protocol that was first published in 1970 by Schneider Electric previously known as Medicon. Those days, modbus was broadly adopted for utilities and other industrial applications owing to its client/server massaging structure. Modbus is adhering to seven layered OSI model represented in figure 2.3 and its uses application layer to host client and or server services [13, 14]. Modbus can be used over numerous set of substation communication networks; serial communications network (RS-485, RS-422, and RS-232) and Ethernet communication network (substation Local Area Network and optic fibre). Figure 2.4 below shows two crucial frames that need to be initiated by modbus in order to perform request or reply operation adhering to client or server model [15].

a) Protocol Data Unit (PDU): contain and controls the protocol operating programs that specify which function to execute at time
b) Application Data Unit (ADU): assist the PDU operation by providing applicable data.

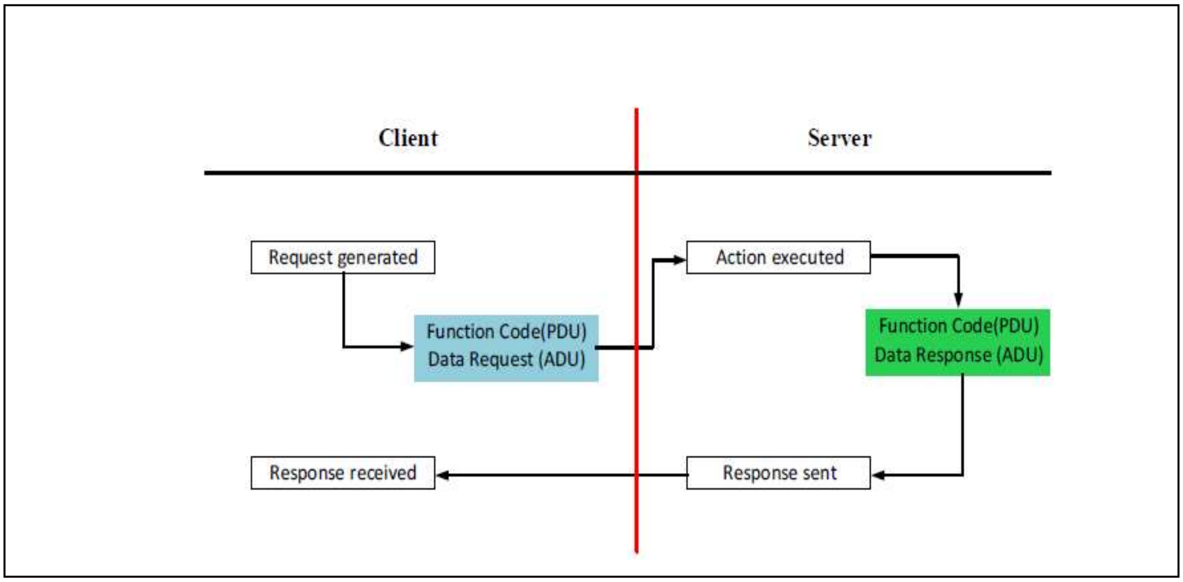


Figure 2.4: Modbus information interchanges mechanism [15].

Modbus is the one of the simplest communication protocol that allows the effective transfer of messages between devices using client – server communication model. The exchange of data in modbus protocol is based seven layered ISO model that control the communication and message construction, however the method of communication or data transfer decide which layers to be used [15].

2.5.3 Distributed Network Protocol (DNP3)

DNP3 is a proprietary and open protocol that was first published in 1993 by Harris Control (General Electric) to define the concept of data exchange between master and slaves IEDs. DNP3 is a simple master/slave communication protocol that also defines the communication standards and procedures for substation automation telecontrol. Substation telecontrol is the term used to define the remote control of substation power equipment's, using applicable protocols, standards and integrated devices. DNP3 standard or protocol was brought to achieve the interoperability between devices of different manufactures. Initially, DNP3 was established as a point-to-point serial communications protocol, due to the growing technology it was further enhanced to be a high speed peer-to-peer protocol communicating over substation Ethernet network to meet the demanding requirements of smart grid [16, 17]. DNP3 standard uses a three layer OSI model protocol called Enhanced Protocol Architecture (EPA), the improvement of seven layered OSI model (figure 2.5), where the pseudo transport layer is added transmit large amount of data [18, 19]. The data link layer is the second layer of EPA, that is used to achieve interoperability between multivendor devices [16, 19].

a) DNP3 link layer

Data link layer is used to ensure a reliable broadcasting of data through the physical layer and to provide a route for group data, this group is known as a frame. Data link layer also offers flow control and error detection. Physical layer is used to provide a clear signal passage and control the flow of bit-data [16, 20].

b) Addressing

Data transmission needs two addresses; source and receiver address. Receiver address stipulates which DNP3 device will accept the transmitted data, while source address specifies the sender [16].

c) Cyclic Redundancy Checks (CRC)

This is used to detect errors and rectify them, before the message is being lost or corrupted along the communication channel because every transmitted data is subjected to the noise, electromagnetic radiations from nearby equipments and electromagnetic induction from nearby cable [20].

d) Link Layer Confirmation

The link layer confirmation is popular in DNP3 applications. This is a DNP3 frame transmission feature that is responsible to ask for the conformance of the message arrival to the receiver [16, 20].

e) Transportation Layer

Large size of data packets need to be broken into small packets so that it can be easily transmitted by link layer, and when it reaches the destination its reassemble into one packet. Transportation layer is also used manage the communications between two end systems; Application and Physical layer [16, 21].

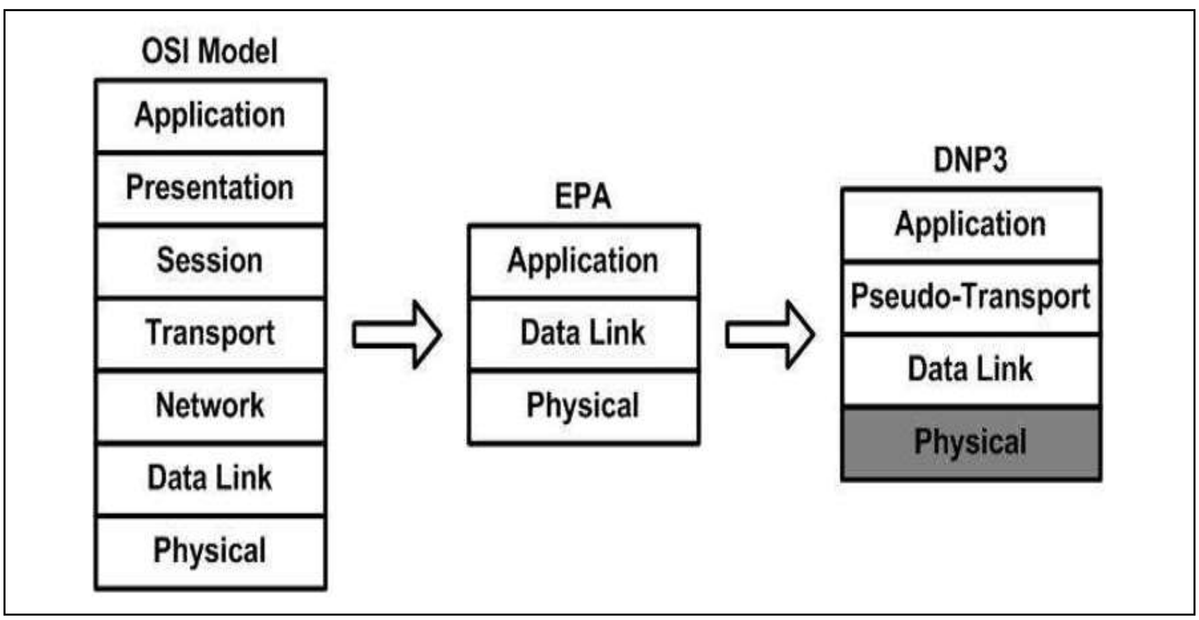


Figure 2.5: OSI model for DNP3

Figure 2.5 here demonstrate how the EPA model was derived from original seven layers OSI model shown in figure 2.3.

f) Pseudo-transport layer

Pseudo layer is added to control pseudo points. Pseudo points are not guanine points since are control by the software. Pseudo layer is also used to complete the assembling and disassembling of messages [16].

g) Physical layer

This layer can be used for network topology to characterize the communication passage.

h) Data link layer

This layer deals with the real communication medium such as copper, fibre, radio or satellite used to facilitate the communication of the protocol. Previously DNP3 communication was only described over a straightforward sequenced physical layer like RS- 232 or RS-485, however; in recent application communications are specified over Ethernet [22].

i) Application Layer

DNP3 application layer is accountable for data collision avoidance, cold restart, class data, time stamping and indications.

2.5.4 Substation Local Area Network (LAN)

If the substation is having a LAN for the purpose of communication, then the protocol being used must have the Ethernet stack to connect to the substation LAN[23]. Ethernet for substation communication network is globally adopted and the rate of its application is increasing drastically. This is a high speed communication architecture that use Logical Link Control (LLC) to provide interface to the network layers of the protocol and Carrier Sense Multiple Access or Collision Detection (CSMA/CD) as illustrated in figure 2.6 [11, 12]. This type of communication architecture needs a thoroughly analysis before is being deployed to service. Substation network topology design must be scalable and flexible so that it will be consistent and easily expanded in the future[24]. It must be easy for all interconnected devices to share information. Figure 2.6 illustrate the concept of substation LAN. Ethernet communication in substation can be carried in two approaches either Transmission Control Protocol (TCP/IP) or User Datagram Protocol (UDP/IP) it's all depend upon the requirements of data and the reliability.

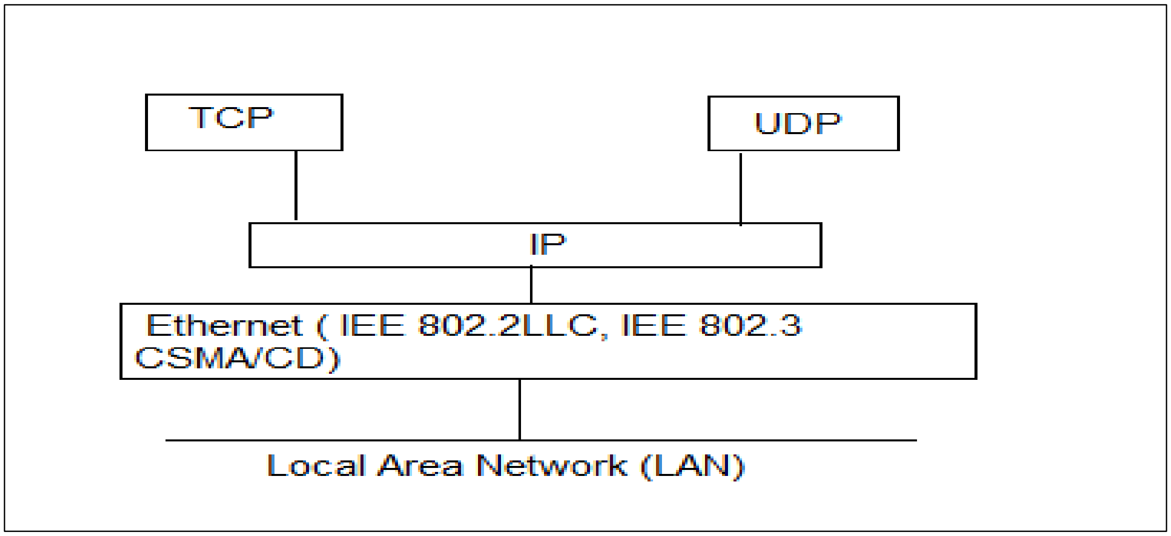


Figure 2.6: Intranet Protocol Suite

The IP provides the service called datagram to control the transmitted data from source to a specified destination. All substation IEDs connected to the substation LAN must have dedicated IP addresses to communicate over Ethernet. Transmission Control Protocol (TCP) is used when reliable connection oriented means is required to transmit data from one user to another using IP. This offers error free transmission of information. User Datagram Protocol (UDP) is used when there is a need of accessing datagram services [24, 25]. This does not offer reliable services (e.g. if the error has been detected, the data packets will be discarded) simply because this is not connection oriented. UDP is a packets based protocol. Network topologies can be loosely grouped into two main categories.

a) Broadcasting: in this architecture the message is distributed from transmitter to reach all connected devices. Then, the device will use its configuration to reach to the message. The applicable message will be accepted and if it's not applicable will be rejected. This topology is used in the application of few devices.

b) Point to point: in this architecture each node is directly communicating to only one node. The nodes can regenerate signals and pass it to nearby nodes. This type of topology is mainly applicable when too many devices will be used[24].

This review will only explore three common network architectures (star, ring and hybrid – star).

c) Star architecture

The typical star architecture uses a central node and allows the interconnection of other nodes or switches to form a star design [25].

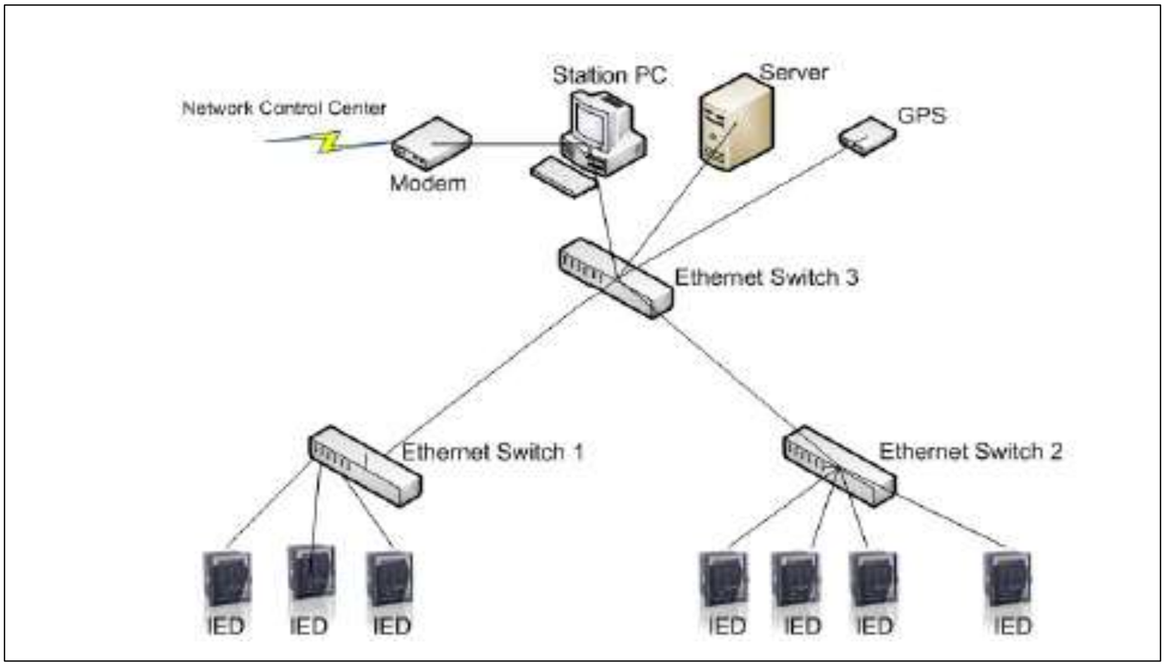


Figure 2.7: Star architecture [25].

If the central node or switch fails, the whole communication network will be lost and this designed need lots of cables. This architecture holds some major advantages such as:

I. Easy maintenances
II. Central node monitor the network traffic
III. Easily expanded (the addition and removal of nodes and cables is easy)
IV. Easily fault finding

d) Ring

Ring architecture is the most commonly used substation communication network configuration, due to its communication redundancy that is achieved using Rapid Spanning Tree protocol (RSTP) and High-availability Seamless Ring (HSR)

[26].This is widely deployed in substation applications because crucial substation messages are transmitted successively from device to device [25].

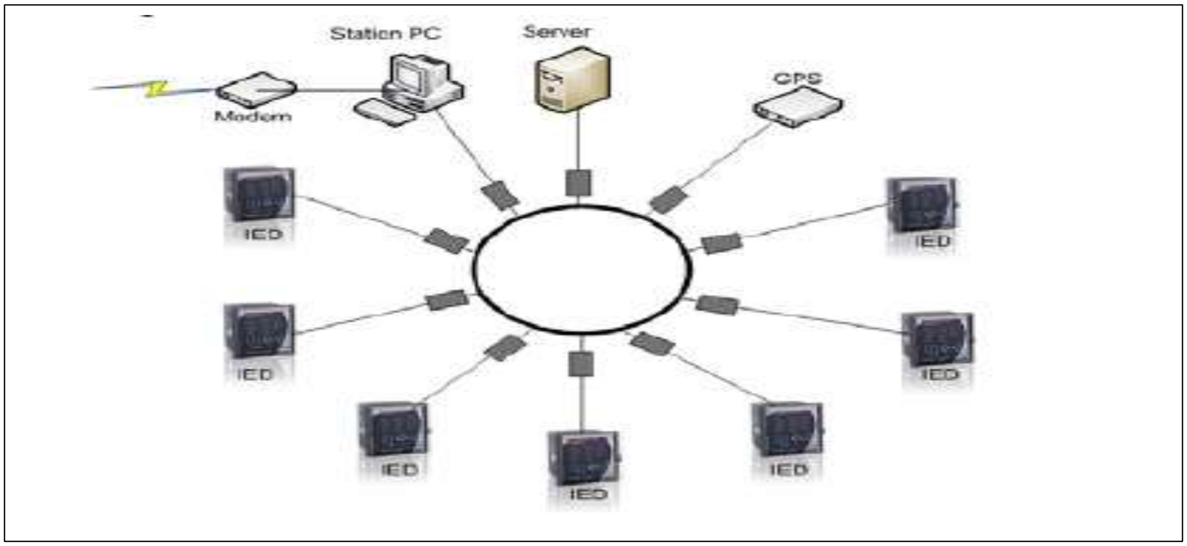


Figure 2.8: Ring architecture [25].

The loop of the ring architecture is closed that provide the high level of redundancy as shown in figure 2.8. Managed Ethernet switches must be incorporated in the design of ring architecture that helps to block the unwanted messages from circulating in loop in case one connection fails. Ring architecture has the following advantages:

I. No central node required
II. The messages can be easily and automatically recognized
III. Every node or device can regenerate the signals

The main setbacks of this design are; when one node fails, the whole network fails, not possible to add or remove any node while it in operation and difficult troubleshooting.

e) *Hybrid-Star Architecture*

This architecture has backbone switch and redundant links added to it. Hybrid star is a combination of network topologies, to improve reliability of the design. This design is complex and can bring difficulties in terms of expansion and maintenances; therefore it is difficult to achieve reliability with this design. The time delay of this architecture is acceptable [25].

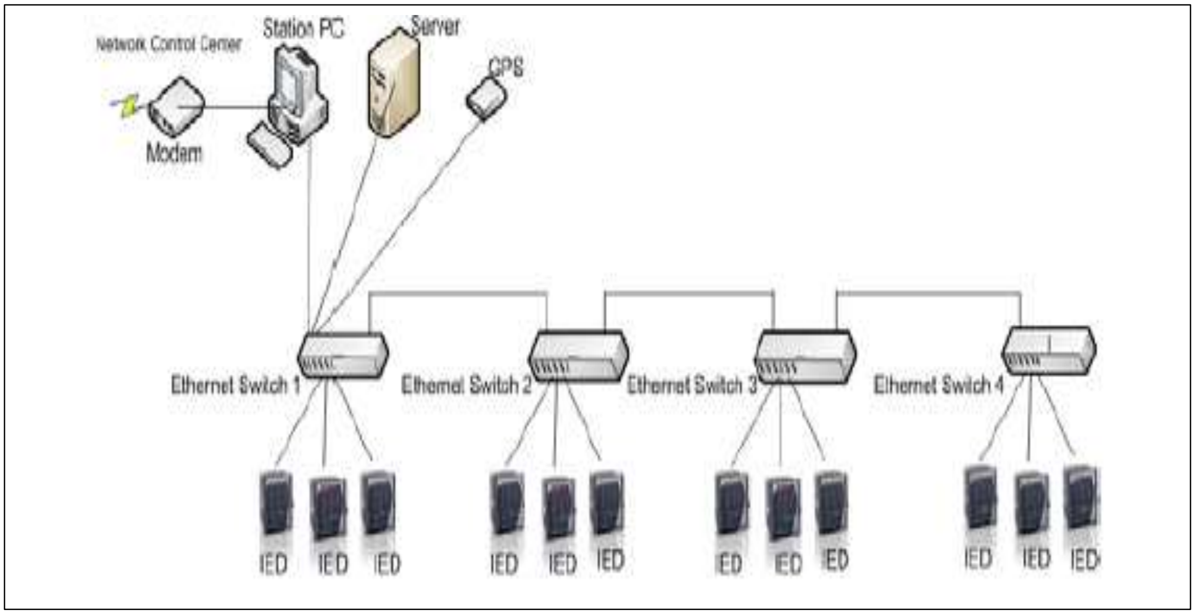


Figure 2.9: Cascaded-star Architecture [25].

Due to the complexity of this network architecture, it is not recommended to use it when few devices will be use. According to the architecture in figure 2.9 every switch has ports that provide link between previous and next switch. This network architecture is complex and its need lots of work to achieve the complete reliability.

2.5.5 Utilities Communication Architecture (UCA 2.0)

UCA is a substation communication standard that was initiated in 1988 as a utilities project and it was controlled by Electric Power Research Institute (EPRI). The UCA was initiated to define the concept of substation real-time monitoring and control. UCA became the first comprehensive standard to demonstrate the interoperability between multivendor devices integrated in the same or different networks just before the DNP3 [15, 27]. UCA was developed in order to standardize substation communication through a standardized application interface, data modelling paradigm and communication structure. UCA is not just a protocol it is a standard that also define the architecture of substation automation and further offer the option of incorporating the legacy protocols in its communication architecture [11]. UCA uses Manufacturing Message Specification System (MMS) and Generic Object Models for Substation or Feeder Equipment

(GOMSFE), to define the concept of the real-time monitoring for power system ,innovative data exchange between devices of the same or different applications and simplified substation automation architecture [27, 28].

2.5.6 IEC61850 implementation

IEC61850 is a communication standard or protocol that was published to address the issues that were not completely addressed by the introduction of UCA and DNP3 respectively. IEC61850 then became the first standard to be called a global standard owing to its comprehensive definition from physical device to communication architecture. Figure 2.11 illustrate how the UCA 2.0 and TC 57 work was incorporated to come up with one global standard.

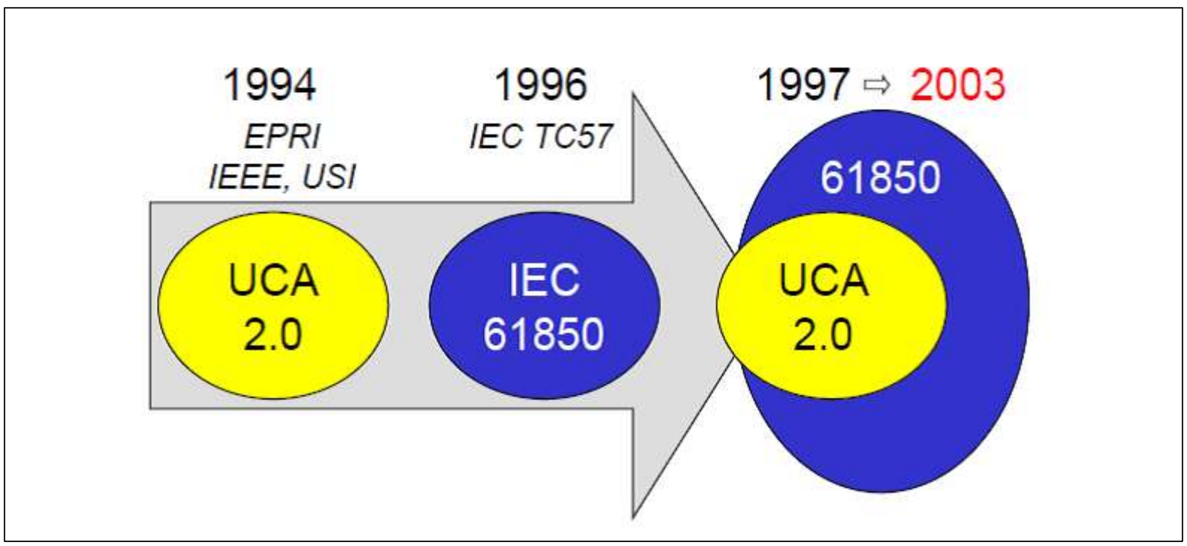


Figure 2.10: Merging of IEC 61850 and UCA 2.0 [29].

The expansion of UCA to UCA2.0 was carried by EPRI in 1994. This work was only for substation bus communications. In 1996 the Technical Committee (TC) 57 worked on the IEC61850 communication standard to further improve the work that was carried out by EPRI for substation bus communication in UCA2.0. Due to the similarity of their works, in 1997 both EPRI and TC 57 worked together to incorporate their work and develop the new communication standard called IEC61850 [29]. Their developments were completed in 2003 and the IEC61850 standard was published in 2004. This standard came as a outcome of incorporating UCA and IEC61850 [29]. IEC61850 were globally adopted owing to its numerous advantages. IEC61850 is a broad standard that simplified the communication between devices by introducing the concept of Logical Nodes (LN), Logical Devices (LD) and data classes to manage the exchange of data between devices. The issues relating to the interoperability and interchangeability were resolved once and for all by providing the advanced substation data management for all automation functions. Figure 2.11 below shows how UCA2.0 elements were incorporated into IEC61850 elements to develop IEC61850 standard [29].

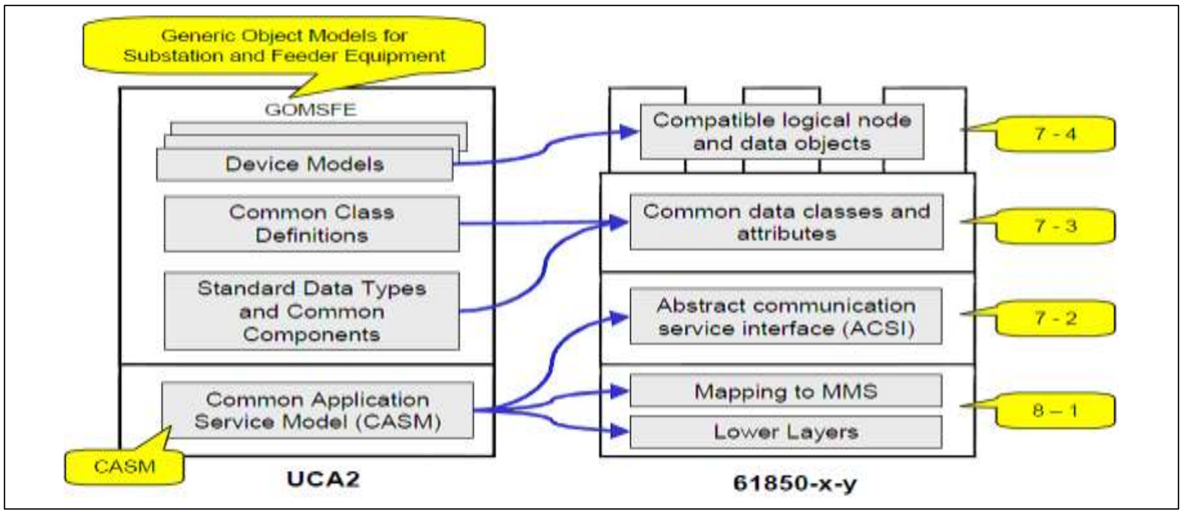


Figure 2.11: Incorporating UCA 2.0 and IEC 61850 [29].

IEC61850 is a multifaceted standard that hold the future of substation automation systems through facilitating the creation of smart automation systems up to the level of stipulating the key requirements of all devices complying to the IEC61850 standard. IEC61850 holds many new functions with others similar to those of UCA2.0 [29]. The earliest edition of IEC61850 was published in the early years of the new millennium and introduced the standardized mechanisms for:

a) Data models representing all substation devices and functions
b) A common configuration syntax with a single configuration repository for all devices in the substation automation system using eXtensible Markup Language (XML)
c) A standard set of services for reporting data, performing control operations and managing diagnostic access to data

d) Creation of specific protocols such as GOOSE and Sampled Measured Values (SMV) to support high-speed coordination of the data processes required facilitating electric network protection functions and the distribution of voltage and current waveform data between devices as a time-series of analogue measurement samples [30].

e) Mappings of the data models and services onto existing protocols (primarily MMS) and the newly developed GOOSE and SMV protocols

Figure 2.12 illustrate the communication profile and OSI model of the IEC61850

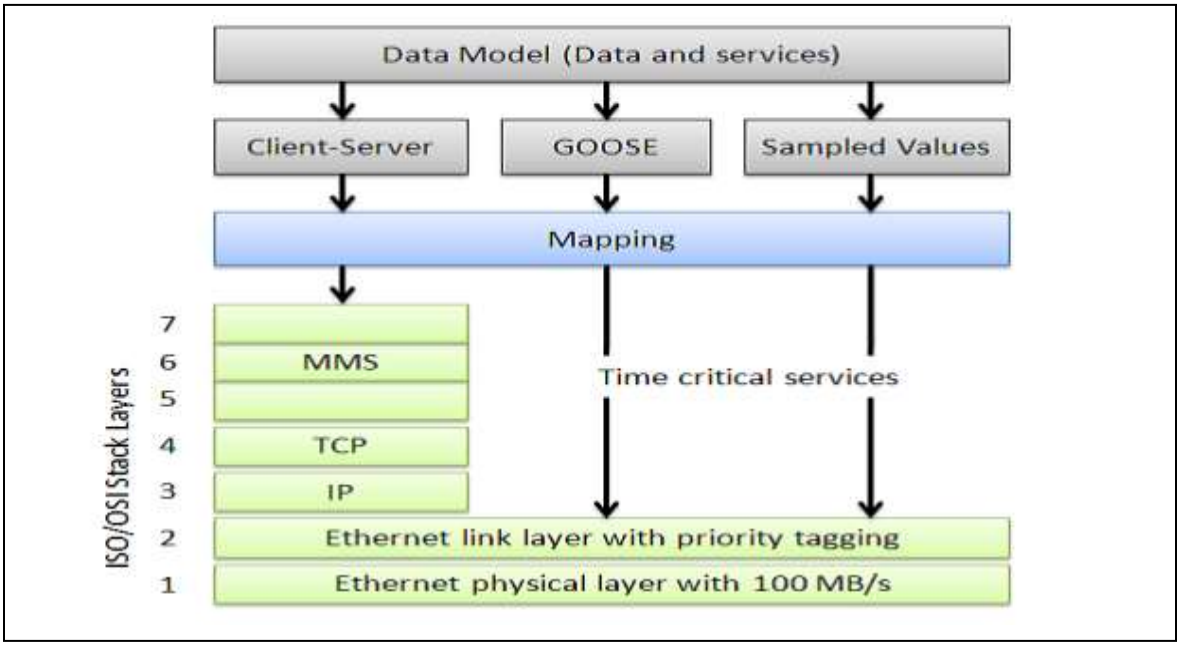


Figure 2.12: IEC 61850 ISO stack layers [31].

IEC61850 have time critical services that are mapped straight to the Ethernet link layer that offer the option of priority tagging. Those services are GOOSE and Measured Sampled Values (MSV) as shown in figure 2.12.

2.5.7 IEC61850 standard arrangement and content

This is a client/ server protocol or sometimes referred as publisher or receiver protocol depends upon the application. The scope IEC61850 standard consists of ten large sections, detailing the communication within substations and further explains the mapping procedures. The documentation of IEC61850 is very complex and it uses tables to define its concept. These standards are formally arranged in a following system [30]. Table 2.1 shows the arrangement of the IEC61850 standard.

Table 2.1: Arrangement of IEC61850 standard

Parts No.	**Standard definition and content**
	Part 1 to 5 : System aspect
1	**IEC61850 general introduction and overview**: The summary representation of the complete standard and its applicable figures
2	**Glossary** : The definitions of the special terms used in the standard
3	**General requirement :** Essentials of IEC61850 and its nature of development
4	**Project and System Management** : Description of project documentation, testing tool, confirmation of factory test, quality and system testing procedure
5	**Communication Requirements for Functions and Device models**: description of IEC61850 communication functionalities and substation devices models
	Part 6 to 10 : Configuration
6	**Basic Communication Structure for Substation and Feeder Equipment** : this is a large part of the standard consists of four sections all defining the IEC61850 abstract model
7	**Basic Communication Structure for Substation and Feeder Equipment** : this is a large part of the standard consists of four sections all defining the IEC61850 abstract model
7-1	**Modelling and Principles:** description of data modelling notation
7-2	**Abstract Communication Services Interfaces (ACSI) :** substation automation and protection system requirements
7-3	**Common Data Classes (CDC) :** description of IEC61850 hierarchical

	architecture
7-4	**Data classes and Compatible logical nodes :** description of 92 Logical Node (LN) applicable to the standard
8	**The Specific Communication Service Mapping (SCSM)**
8.1	Configuring procedure between IEC61850 and MMS (ISO or IEC 9506 and ISO or IEC 8802-3)
9	Specific Communication Service Mapping (SCSM)
9.1	**Sampled Values over serial unidirectional Multidrop point-to-point link** : the description of mapping SV over point to point
9.2	**Sampled Values over ISO or IEC 8802-3** : SV and GOOSE mapping technique
10	**Conformance Testing** : justification of test equipments for IEC61850 devices and system documentation

These sections are used to fully describe the nature and content of the standard. Part one to five describe the general information about the standard and part six to ten describe detailed services about information integration, ACSI, SCL, MMS and testing [29, 30, 32]. An overview of the all the parts are described in part one, the glossary is reflected in part two. Basic requirements for substation automation are described in part three and part four describes general information and specification of IEDs from its development to complete system engineering and quality assurance. The mapping of DNP3 data to IEC61850 standard is not defined in this document. However is an alternative option to adopt IEC61850 standard without replacing the whole substation automation networks and the procedure is defined in separate standard[33]. Undeniably most of the benefits of IEC61850 are not obtainable with legacy protocols, but the most important ones such as; interoperable between multi-vendor devices, time stamped massages for sequence of event recordings, broadcasting massages; high speed peer-peer and secure configuration or file transfers can be achieved with E-DNP3. The following are the vital advantages of IEC61850 communication standard.

a) Its offer object-oriented communication architecture
b) Lessens engineering and commissioning struggles
c) Simple communication architecture
d) Almost all functions are integrated in devices, no standalone devices required.
e) Offers a comprehensive set of all local communication services
f) Offers the function to collaborate with the legacy protocols (IEC60870, DNP3 and etc)

MMS protocol and other related services function using the OSI model of the protocol and are compliant to TCP communication profiles. Figure 2.13 illustrate the concept of mapping between IEC61850 server classes to MMS Virtual Manufacture Device (VMD).

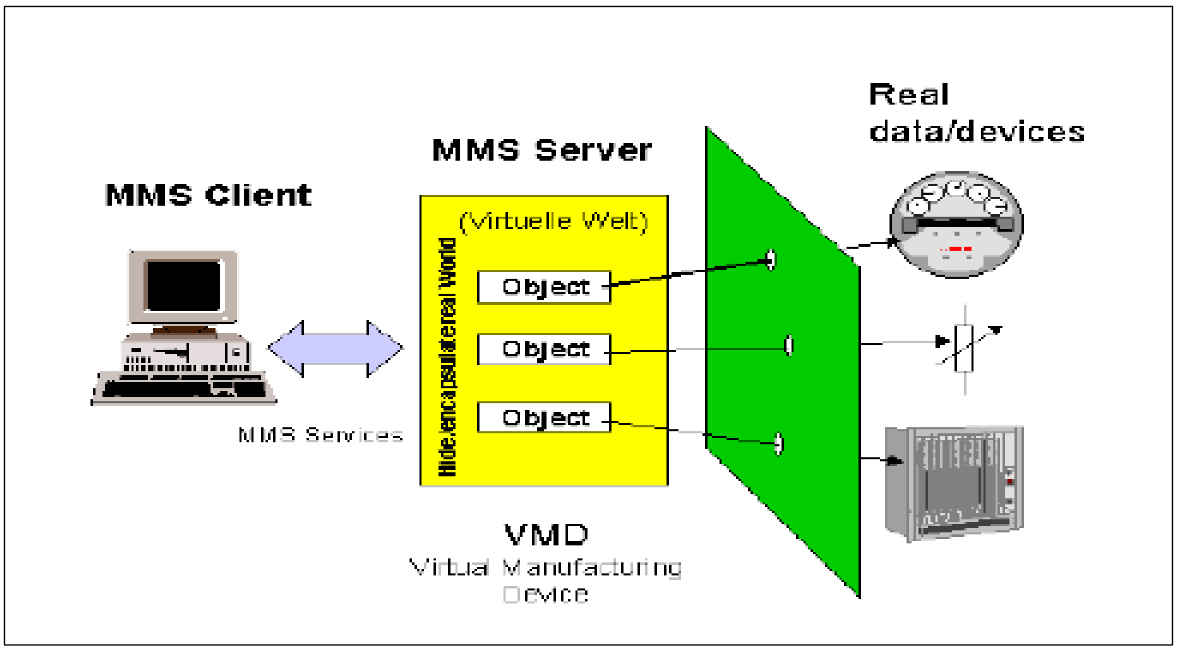


Figure 2.13: IEC 61850 VMD Model [12].

IEC61850 MMS protocol is similar to the one previous introduced in UCA.MMS protocol is used by IEC61850 standard and UCA to define communications messages between substation controllers. The concept of MMS protocol can be defined using the standardized model called VMD. VMD model clearly articulate the exchange of information between MMS clients and server[12, 30]. The distribution of input and output data values over the substation LAN needs a reliable and fast technique.

2.5.8 IEC61850 substation architecture

IEC61850 standard is currently used for local communication within substation devices [34]. Figure 2.14 illustrate the communication architecture of IEC61850 based substations with all device integrated to the network.

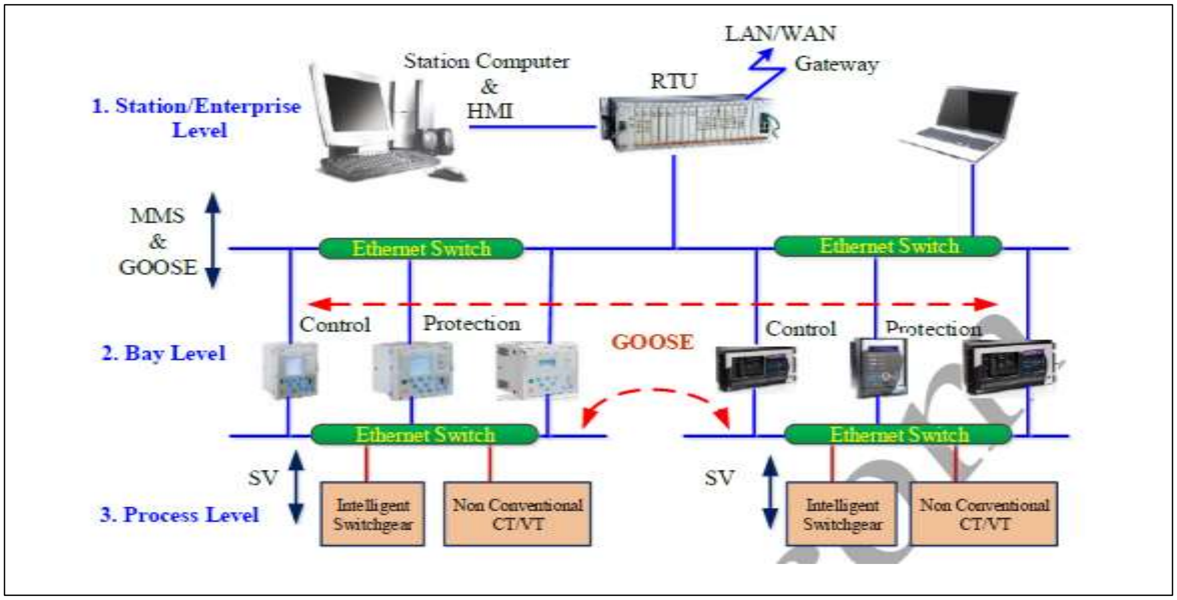


Figure 2.14: IEC61850 based substation architecture[34]

There are two directions of communications for IEC61850 based substation automation architecture; horizontal and vertical communication. Horizontal communication is referring to the exchange of data or messages within the same level of the architecture hierarchy, these messages are time critical GOOSE protection messages. Vertical communication is denoting the exchange of data or messages between substation devices positioned in different level; these messages are MMS, sampled values and GOOSE prioritizing the concept of data reliability [15, 34]. IEC61850 uses a client – server messaging model through vertical communication and publisher – subscriber messaging model via horizontal communication. The architecture of IEC61850 based substations compromises of three level of operations; Station or enterprise level, Bay level and Process bus level.

a) Enterprise level

The key functions of station level is archive data acquired from bay level, control of substation automation and control the bay level devices. It's also control the communication between remote substation and control centre, using RTUs and modems [15].

b) Bay level

This level is between station and process level, therefore its uses station level switches to interconnect control and protection IEDs. It's also host the horizontal communications [15].

c) Process Level

Process level integrates the primary and secondary equipments. This is a level where sampled values from real time monitoring are communicated to bay level [15].

2.5.9 IEC61850 data modelling paradigm

IEC61850 is a standard that directly influence the physical construction of automation devices. All IEC61850 based devices must have Logical Nodes (LN), Logical Devices (LD) and data classes as shown in figure 2.15 [1, 29, 30].

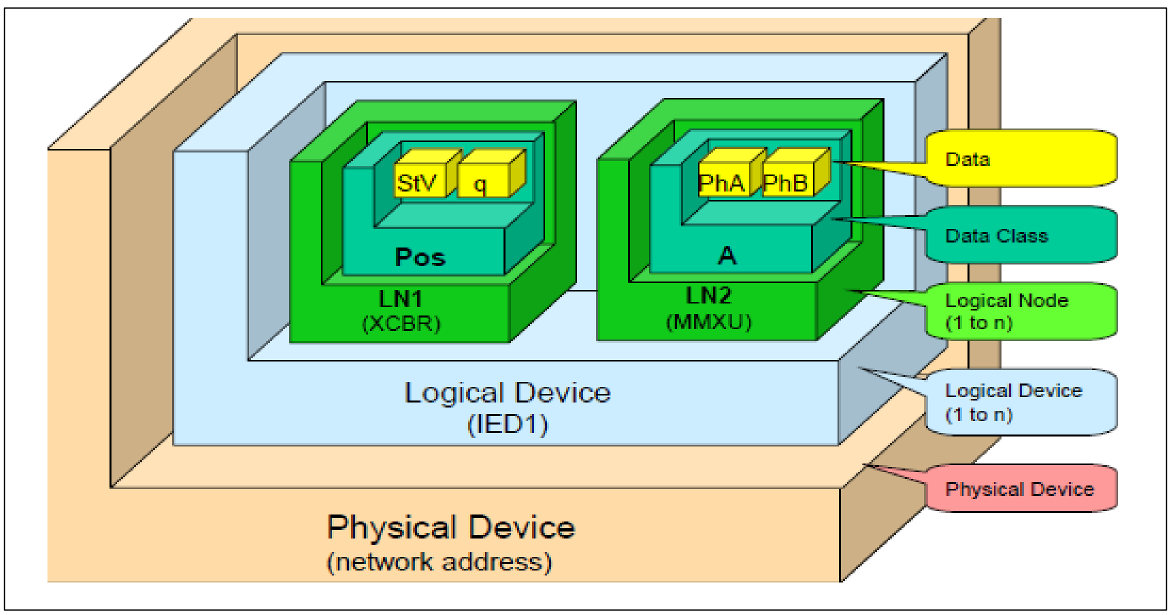


Fig. 2.15: IEC61850 device physical structure [29].

The physical device is referring to protection device that must contain all IEC61850 functions to simplify the modelling of data. Physical device is a mechanism used to link logical device to the network [33].

a) Logical Nodes

This is a grouping of power system data and its suitable services. LN controls the functions of the real device. The concepts of LNs are defined in parts 7-2 to part 7-4 of the standard. The list of logical nodes relevant to substation automation is attached in (appendix A-2 and A-3).

a) Logical Device

This is a combination of numerous logical nodes enclosed in one substation IED called physical device. These LNs are used to control the operating system of the substation physical device. LD is used to define the principal functions of physical device and is not documented in any part of the IEC61850 standard because its manufacturer responsibility [29, 33].

b) Data attribute

The quality of the data used for real- time monitoring and control is defined in terms of data attributes. This is a dedicated data value that must be exchanged [33, 35]. The common types of data attributes are quality (q) and status value (StVal)[29].

2.5.10 Substation Configuration Language (SCL)

The mechanism of data exchange to achieve interoperability in IEC61850 standard is defined via SCL [36].This is a language used to configure substation devices and its enable the IEDs to exchange the information. Interoperability is the means of exchanging data in a multivendor environment. Previously, too many tools were used to configure substation devices, because all manufactures had unique tool to configure their devices [20, 36, 37]. There are four SCL files that are currently used as represented in table 2.2. SCL uses XML file format.

Table 2.2: eXtensible Markup Language SCL files

File Description.	Files	Functions
IED Capability Description	XXX. ICD	Provide the definition of IED capabilities, all substation IEDs must have ICD files.
Configured IED Description	XXX.CID	Provide protocols definition and data format used to start up the IED
Substation Configuration Description	XXX.SCD	Provides comprehensive specification of substation automation system functional structures and the IED points description
System Specification Description	XXX.SSD	Contain single line diagrams along with its functional requirements

There numerous configurations tools that are used to configure IEC61850 and contain SCL files such as; PCS – Safety Configurator and Diagnosis (SCD) configuration tool and CET850 configuration tool. The illustration of the system and IED configurator is attached in (appendix A-4)

2.5.11 Abstract Communication Service Interface (ACSI)

ACSI is a communication mechanism that is used to regulate the interaction of IEC61850 data between integrated substation devices and it also execute data request command where it appropriate. IEC61850 was made to work together with legacy protocols when there is a need[38]. The integration of legacy protocols with IEC61850 is done via communication interface in order to achieve advanced data collection, processing, setting, monitoring and reporting. IEC61850 and legacy protocols also offer intelligent substation event grouping. The OSI model and IEC61850 communication profile represented in figure 2.12 is made up of two sections; application domain and communication stack; these sections are brought together by service mapping between applications and communications. The abstract interface in substation automation application is used to achieve the interoperability between an integrated devices, since its enables the cooperation of numerous devices in one substation. Its further describes communication between two physical devices[38]. The communication is defined as a data recovery and access, physical device control execution, configuration files transfer, device self-description, locating data types and recent substation event reporting. Abstract interface also define the concept of IEC61850 information exchange between substation to substation and to control centres [38]. The remote communication between substation and control centre for IEC61850 still not clearly explained, since IEC61850 was initially developed for communication within substation. Hence many applications use protocol translators for remote communication. Logical nodes and common data classes contained in standard are used define the basic model of substation data exchange [30]. The illustration of conceptual services for IEC61850; information model and information exchange is attached in (appendix A-5).

2.6 Comparison between legacy DNP3 and the IEC61850 standard

When the IEC61850 standard is compared with legacy communication protocol DNP3 it is more advanced and sophisticated. It is defined by object oriented modelling functionality as well as detailed defined communication interfaces. But the fact is IEC61850 is not a standalone protocol since it can be incorporated with legacy protocols where is deemed to be necessary. Again it define all features that were previously defined in legacy protocols [1, 39]. The IEC61850 standard is a multi-faceted standard that refers to many other standards (or common practices) depending on the considered issue. When implementing the IEC61850 standard on a specific embedded platform refer to a communication stack for all communication within the IEC61850 standard. The SCL capabilities of the system are assessed to describe the line diagram and provides basic configuration for communication purposes and interoperability. Table 2.3 tabulates the comparison between DNP3 and IEC61850. Comparison key: √ - means applicable and x - means not applicable.

Table 2.3: Characteristics comparison of IEC61850 and DNP3

Characteristics	IEC 61850	DNP3 (IEEE1815)
Recognized in NIST Interoperability Framework	√	√
Substation Automation	√	√
Substation to Control Center	In progress	√
High peer-to-peer	√	√
Structured Naming and Data	√	√
Data Self-Description	√	√
XML Configuration File	√	√
IP suite communication profile	√	√
Enhanced control (with reports)	√	√
Substitution (Forcing)	√	√
Files	√	√
Event logs	√	√
Read or write	√	√

Most of the crucial services offered by DNP3 and IEC61850 are similar. Both protocols were developed for similar intension as to improve and standardize substation automation, focusing on key factors such as interoperability, high speed peer-peer and secured power system controls. Both protocols use XML configuration files to achieve interoperability in multivendor substation. DNP3 offers structured data similar to IEC61850, that simplify the reporting and archiving of substation data. Furthermore DNP3 is currently used for remote application and in distribution lines where is not possible to use IEC61850 at the moment. Both

DNP3 and IEC61850 are time synchronized protocols. DNP3 is widely adopted across the world, however some application are not possible with DNP3 such as GOOSE, GSSE, MMS and MSV. According to the literature survey the IEC61850 has gained an excellent track record as the newly established communication standard. However some utilities including Eskom in South Africa are still reluctant to the standard.

2.7 Adoption of E-DNP3 and IEC61850 in South African distribution substations

Figure 2.16 represent the data on how the utilities are responding to the adoption of IEC61850 and DNP3.

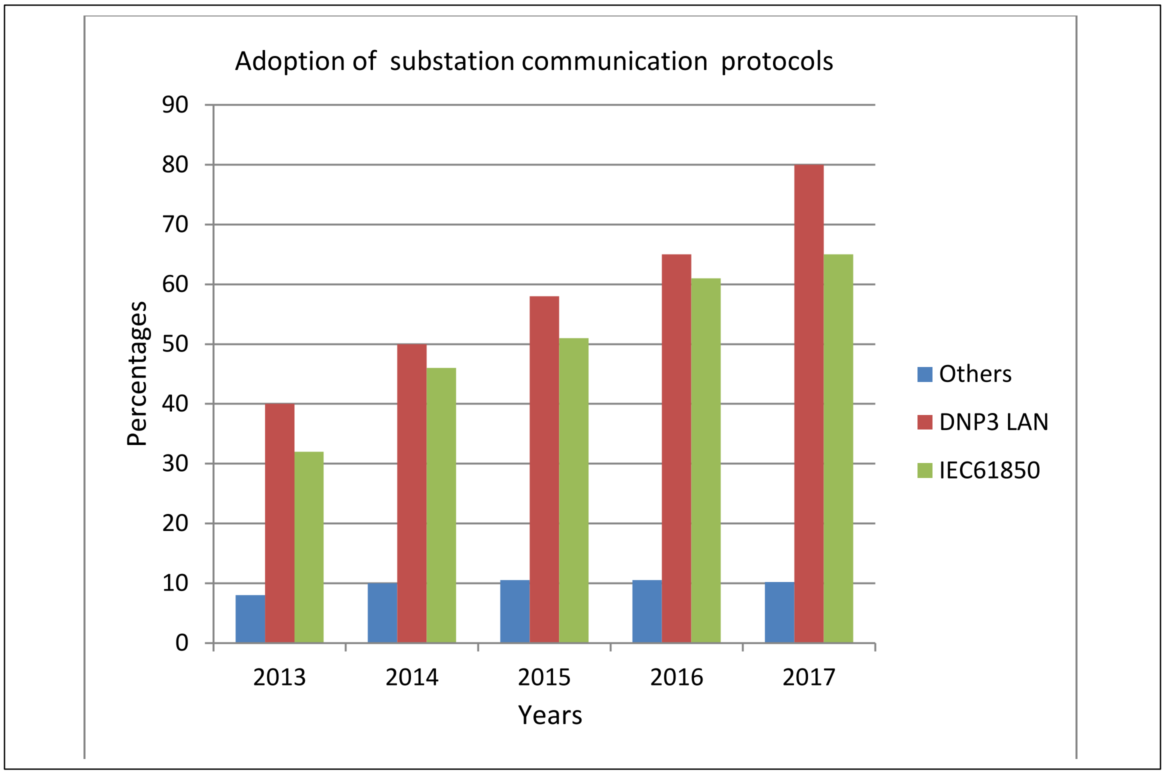


Figure 2.16: Adoption of DNP3, IEC61850 and other protocols over the past years

Figure 2.16 shows that DNP3 either serial or Ethernet communication is widely adopted in South Africa distribution substations recently. Substation automation systems are progressively modernized and the modification are undertaken as the extension of the currently installed devices to minimize costs related with complete replacement substation devices

2.8 Concerns and remarks

Engineers and technicians need comprehensive knowledge of substation automation technologies. Unfortunate, introduction of IEC61850 standard brought numerous challenges. Beside the technical concerns related to GOOSE, the documentation of the standard as a whole is difficult to understand especially for those who are not automation engineers[40]. Following are the additional challenges from those previously discussed in chapter one to define the problem statement with regard to the comprehensive analysis of the standard

a) IEC61850 suggested the integration of numerous applications such as solar, and wind power generation, remote communication using SCADA systems and etc. IEC61850 standard is more than ten years old now but some of these applications have not been practically achieved. The standard is promising; however there is more are so many assumptions used to the standard and some of its applications not practically validated. That why some utilities are struggling to cope with the practical implementation of the standard.

b) Interoperability is the one of the essential feature of IEC81850 standard that is achieved by configuring substation IEDs using standardized language called SCL. The concern is, all CID files generated using old software version to configure IEDs will be not imported into a new software version when new same vendor IED need to be configured. Even the connection cannot be established if the software installed in the Personal Computer (PC) is not the same version as the one in the relay. That means programming engineer have to restart the whole process to regenerate all new files appropriate for the software version.

IEC61850 it's a new communication standard and some utilities are still resistant to it because of its prematurity and ambiguities that are still not resolved. As much as the flexibility is improved but the security of data in IP driven communication infrastructure is still an issue to date. Whereas DNP3 is a well-known and accepted protocol that offer various services similar to that of the IEC61850. The security of DNP3 has been improved for the past few years to address the cyberattack issues. Although IEC61850 is a future rich standard, it still has challenges in terms of practical applications such as: system interoperability and configuration. These challenges need to be addressed to create the network that is smart grid ready. The key requirements of smart substations such as interoperability and high speed peer to peer were achieved in both standard IEEE1815 and IEC61850. The key advantage of IEC61850 is that, it was designed to fully co-operate with legacy protocols such as DNP3 and UCA given that DNP3 can be used over Ethernet communication. Substation automation engineers and technician are not acquainted with the technical knowledge of IEC61850. Adding to the technical issues discussed above other industries and utilities are resilient to the standard because of the financial motivated reasons. Those motives are:

a) High value of currently installed DNP3 IEDs
b) High complete replacement cost and prolonged down times
c) No formal training that are being provided (when a complete IEC61850 substation needs to be commissioned substation automation service providers such as ABB, ACTOM and etc do the 80% of the work, that is costly when compared to the cost of the internal workforce.

Due to that, there is an urgent need to investigate the alternatives to integrate DNP3 data into IEC61850 data model, since DNP3 has been around for so long and engineers are familiar with DNP3. This research is primarily focusing in the process integrating existing substation devices with IEC61850 to provide a cheap and solid path towards smart grid construction in power system. In terms of unified data access, the utilities have faced the following difficulties that need to be addressed in this research.

a) Difficulties of integration data between legacy protocols and new protocol IEC61850
b) Communication systems that do not exchange data fast enough for operational uses mostly in legacy protocol applications

About 80% of South African distribution substations are still using hardwired serial communications, which bring the difficulties in terms of monitoring the healthiness of the system. When the expansion of the substation is required, protection schemes, statistic meters and telecontrol RTUs demands extra hardwiring which may increase engineering time or plant shutdown time while in Ethernet based communication architecture it is very easy to add or delete any virtual wires within minimal time. The main goal of this research project is not to favor the hard wired substation communication architecture, but is to prolong the service life of currently installed DNP3 device and provide the strategy to decode DNP3 data into IEC61850. This research will provide a simple procedure to be used when mapping DNP3 point array into IEC61850 data model, so that legacy devices will be operated in a profitable and reliable manner.

2.9 Conclusion

Over the past years, many proprietary communication protocols were used in the substation automation environment and have hindered utilities to achieve intelligent and complete protection integration, real-time monitoring and control. The industry has reached a stage where more of interoperable, real-time data monitoring and advanced substation automation is required to improve supply reliability and security. Therefore the major challenge is to accomplish interoperability between different IEDs of multiple manufacturers. The IEC61850 standard has been developed as a future proof and adaptable communications protocol with advanced object oriented modelling structure to meet these requirements, however the some utilities are opting to integrate DNP3 data and IEC61850 to save the replacement cost, and avoid supply interruption during commissioning of large substations. The following chapter discusses the concept of smart substations and the system configuration of mapping DNP3 data into IEC61850.

Chapter Three

Smart substation and system configuration

This chapter represents the concept of smart substations adding to the structure of substation automation discussed in chapter two that include the insight over the evolution of protection relays. The last section of this chapter represents the system configuration procedure and the architecture of data collection.

3.1 Introduction

The term smart substation is defined adhering to fundamentals of communication protocols and real-time data networking discussed in chapter two. The concept of smart substations is to bring reliability and flexibility to the power system since most of the industrial operations depend upon electricity. The challenges that have been identified in legacy substation when compared to the smart substations need to be addressed by reconstructing the communication network within substations such as adopting the Ethernet communication within substations, integrating serial communication network into Ethernet network and integrate the legacy protocols such as DNP3 into IEC61850. Substation automation system is the combination three main functions; data networking, device interface, device integration and communication as discussed in chapter two. These functions are further broken down to protection, communication, control and monitoring. Therefore modernizing legacy substation automation system will bring the efficient protection, communication, control and monitoring to the power system. The simulation of this project comprises of the following devices;

a) Two protection relays (ABB REF615 and SEL 487E)
b) One Ethernet switch Ruggedcom 2100 (RSG2100)
c) DNP3 master/IEC61850 server (GE D20)
d) IEC61850 client GE D400

3.2 Smart substations

Smart substation is the substation that uses Intelligent Electronics Devices (IEDs) to monitor, control and protect the substation power plant equipments. Smart substations are a building block of the smart grid network. Smart grid is referring to the integration of intelligent devices of the power system network architecture. Smart substation uses digital communication to monitor the power system network [1, 41] . Substations were known to be a power system element used to adjust and regulate voltage in one direction. This is not the case with the recent applications, distribution networks are now designed to allow for bi-directional power flow and substations are used for advanced switching and monitoring.The integration of smart substation and the implementation of system reliability and other automation applications strongly depends upon the abilities of devices being used and the design of the communication network [42]. Devices communicating in different protocols can be used in one substation automation environment and these devices can be still joined together using a protocol translator [1, 2, 41, 43]. The following are the characteristics and operational requirements of smart substation.

3.2.1 Functional requirement of smart substations

a) Reliability and stability: Most of researchers have stressed the importance of reliability and stability for the substation automation in order to guarantee voltage and current stability.

b) Measurability and controllability: Smart grid networks must be able to sense the changes using power system sensors and execute control as soon as possible. The process of issuing a control is called controllability and is achieved through dynamic measurements and real time monitoring [8].

c) Flexibility and scalability: smart grid infrastructure must be flexible to facilitate power system data flow and execute feasible control to the network. Scalability means the system must continue to expand to meet the future demands and such expansion must not bring difficulties to the network [8].

d) Resiliency: destructions caused natural disasters and deliberate attacks are affecting the security and reliability of power supply. Therefore smart substation restores itself from such attacks as soon as possible. Smart grid infrastructure must resist to some of attacks [8].

e) Interoperability: smart power system must be driven by technologies and protocols that allow interoperability of control devices [8].

f) Maintainability: the design of the smart substation host the critical IEDs therefore must be simple and provide easily access for operations and maintenances. Any design must consider maintainability just before is even deployed.
g) Sustainability: the technology used for smart grid operation must be sustained and innovated from time to time to address recent challenges and meet the growing demand of electric energy globally.
h) Security: The security of the power systems must be tight to ensure that, there is no interruption of power supply and access to the operational data by the third part. Security must be monitored using information technology techniques to guard against cyber-attacks.
i) Optimization: it is important to make the best use of available smart grid resources, since they are expensive. The automation engineers must always make the best use available assets to minimize the capital cost and reduce network complexity so that it will be practical to deploy such solutions.

3.2.2 Technical characteristics of smart substations

Smart substation have unique technical characteristics when compared to legacy or traditional substations that is denoted by progressive data processing and communication between devices using digital platforms [8]. The following list represents the technical characteristics of a smart substation.

a) Digitalisation: fast plus reliable sensing of power measurements is achieved through digital platform. Digital platform further provide reliable and secured communication, protection and control [8].
b) Autonomy: smart substation equipments and devices must have capabilities to operate without the any human intervention with control centres and other interconnected substations. Autonomy will ensure the fast and reliable response under emergency conditions to safeguard equipment’s and operating personnel [8] .
c) Coordination: coordination of substation and control centres is very important in smart grid to improve power system stability. In the current

practise; most substation are integrated for the purpose of sharing the load and back feeding in case of maintenances or faults [8].

d) Self-healing: smart grid must have the abilities to swiftly reconfigure itself after experiencing terrorist attack, natural disasters and power outages [8].
e) Secured control: substation controls must be confirmed just before is executed. Confirmation assists the executor to send a right control command in a right device.

3.2.3 Smart sensors

Smart substations use smart sensors to control and monitor the power plant equipments. The replacement of convectional instrument transformers is underway in order to meet the current standards. Smart power system sensors have the several benefits such as wide bandwidth, high accuracy and safe operation. The recent studies shows smart power system sensors are adopted globally due to its benefits [8]. Smart sensors have led to the development of new merging units that will merge the input signal of three phases into a single phase output signal

3.2.4 Substation Human Machine Interface (HMI)

This is a Personal Computer (PC) that is situated in a substation level to perform all control functions locally. HMI is used as a local master station for the substations. This graphical user contains all substation automation elements that are required to perform controls. Some of the substation IEDs such as D400 telemetry units and etc has on-board integrated HMI. Substation events are gathered locally using integrated HMI link and stored in data archives to keep the back up of operational and non-operational data [20]. HMI is like a local control centre, the main advantage of local HMI is seen when the operation needs the data from previous time, because the data is easily pulled from the local HMI memory [31, 44].

3.2.5 Substation gateway

Substation gateway is located in substation level to interface the protection relays and master station using Supervisory Control and Data Acquisition (SCADA) systems. Substation gateways collect the data from protection relays using its Data

Collection Application (DCA) through serial or Ethernet link. The collected data is then copied to system point database through Data Translation Application (DTA) to produce new points. Its further processes the data using Data Processing Application (DPA) to make it compatible for further communication within the system. Substation telemetry units perform the following functions to the substation:

a) Collect or receive the data from IEDs in form of measurement and statuses
b) Ensure the integrity of data passing through it,
c) Concentrate the data from different IEDs,
d) Data concentrator
e) Substation gateway

3.2.6 Substation Ethernet switches

In today's application, Ethernet switches are used as a high level Storage Area Network (SAN) due to it intelligent abilities. Ethernet switch is also known as substation routing switch that offers special features such as data storage, data virtualization, remote mirroring and data sharing [45].

3.2.7 Protection relays

Power system is the most important and expensive infrastructure that drives an economic growth globally; therefore it require more sophisticated relays in terms of design and redundancy to protect, monitor and control to ensure the continuity of supply to customers (small and large power users). Protective relays have evolved over the last 60 to 70 years from basic electromechanical devices to sophisticated computer controlled equipment able to perform several operations simultaneously [46]. Electrical protection relays have been categorized and mainly fall within the following categories.

a) Phase one protection -Electromechanical relays (1950's)

Microprocessor built protection relays is also known as a numerical relays that use phase four protection technology. Computer based protection relays are software controlled and multitasking relays. Microprocessor relays have greater degree of flexibility so that, they can perform numerous functions concurrently [46]. This principle of operation is called electromagnetic induction. Electromechanical relays were main source of power system protection and were used until lately, since many protection schemes still employ this type of relay.

b) Phase two protections- Static relays (1960's)

Phase two protection relays were first introduced between late 1960's and 1970's.These types of relays brought the higher level of performances in electrical protection. Phase two protection are so called solid state technology or static relays. Static relays brought all characteristics and functions that were previously available with electromechanical relays [46].

c) Phase three protection- Digital relays (1980's)

In early 1980's digital electronics were found to have superior abilities over analogue electronics in many applications. The application of electromechanical and solid state relay gave the attention to the development of digital electronic protection relay and named phase three protection. These types of relays are flexible and faster. They can also offer simple microprocessor technology, however they have limited memory to store large configuration files and historical data [46].

d) Phase four protection- Numerical relays (1986's)

Computer or microprocessor based relays employ phase four technology. These relays are known as numerical relays, due to its greater degree of flexibility. These relays are software driven and are multitasking relays, means they perform several different functions simultaneously [46]. The core element of numerical relay is a microprocessor unit, which facilitates the process of data reading, process and displaying. Numeric relays have better capabilities compared to the previously used standard relays. Microprocessor based IEDs are no longer for limited functions in substations or power system as a whole, it has been improved to offer a wide range of functions such as metering, automation, digital fault recording (DFR), control and reporting [46]. Once the substation IEDs are networked together or integrated, they will provide information needed at control centres to monitor the network. Microprocessor based devices offers five main functions integrated in one unit namely; control function, monitoring function, metering function, communication function and protection function. But this can vary from device to device, depending in design; however for any microprocessor IED for substation automation applications, these five functions must be incorporated in a design [47].

3.2.8 Interoperability between substation devices

This is an ability of multi-vendor substation IEDs to exchange massages and make the use of information available [48]. Interoperability is one of the most important features in the incorporation of IEC61850 and DNP3 standard. The system ability to maintain certain level of freedom allowing the use of specific vendor functions is also one of the major superiority, as it allows the integration of different philosophies from each supplier[49].

3.2.9 Advantages of smart substations

The introduction of the smart technology in substation has brought numerous advantages that are not possible to achieve with traditional substations. Some of these advantages are applicable with legacy substations [50]. There are two groups of advantages in terms of smart technology, i.e., tangible and intangible benefits. Tangible benefits are referring to the financial or technical performance to benefit both the utility and the consumer [50].

a) Tangible : Financial savings to the utility

I. Increases the collection of revenues
II. Increase power system network efficiencies
III. Increase the stability of the network and minimize the breakdown or maintenance cost.

b) Tangible : Customer benefits

I. Improved supply reliability and availability
II. Improved quality of supply to customer terminals
III. Reduced supply interruption for customers (self-healing power system network in case of fault)

c) Intangible

I. More efficient plant maintenance
II. Enhanced fault detection and diagnostic study
III. Customer satisfaction because of improved quality of supply

Reducing the operational and maintenance costs to improve the reliability of the services are the key objectives of the smart technology [50]. However, the applications of substation automation systems require a considerable financial expenditure. Introducing automated systems to distribution networks will eventually make electricity more reliable, efficient, and cleaner [50].

3.3 System configuration

The first step in the communication set up is to assign the IP addresses for all devices mentioned in the introduction. The next step in the process is to configure the communication settings for terminal unit and apply default protection settings to the relays. The network mask address is 255.255.255.0 that is network type C. Table 3.1 below represent the IP and DNP3 addresses for all devices to be integrated in the substation LAN. The network architecture is represented in figure 3.1 as shown below.

Table 3.1: TCP/IP and DNP3 Communication Addresses for Devices

Substation IEDs	IP Addresses	Network mask	DNP3 addresses
IEC61850 server GE D20	192.168.1.1	255.255.255.0	260
Transformer relay SEL 487E	192.168.1.2	255.255.255.0	200
Transformer Feeder REF615	192.168.1.4	255.255.255.0	250
IEC61850 client GE D400	192.168.1.3	255.255.255.0	Not applicable

Table 3.1 above represented the model on how the integrated devices must exchange information. DNP3 data will be exchanged between IEC61850 server, GE D20, SEL 487E and REF615. IEC61850 data will be exchanged between GE D20 and GE D400 as shown in figure 3.1 below.

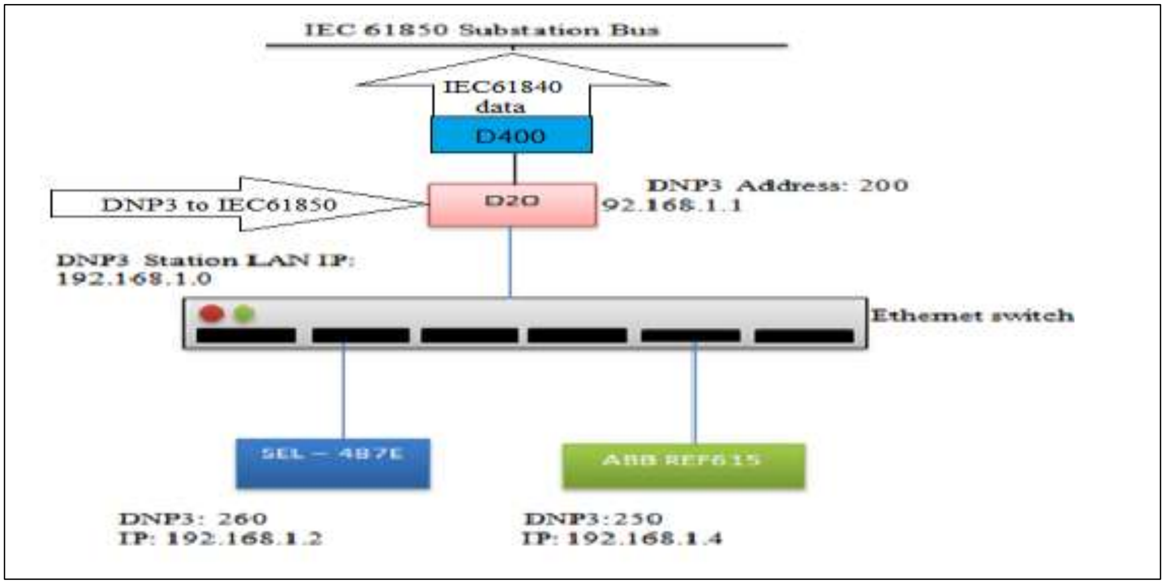


Figure 3.1: Substation network architecture

Figure 3.1 above denoted the proposed network architecture that will use the Ethernet switch to control the traffic in the network and improve the availability of time critical services to the monitoring server.

3.3.1 Ruggedcom 2100 (RSG2100) Configurations

Ruggedcom 2100 (RSG2100) is a vital device for this model to integrate protection relays and telemetry system. RSG2100 is a fully managed Gigabit Ethernet Switch that uses the operating system called Rugged Operating System (ROS) with secured communication method called Secure Socket Layer (SSL).RS2100 consist of 9- fast Ethernet ports that can be used either fibre optic or copper media with the full compliance to IEEE 802.3 used for Ethernet communication. The configuration of RSG2100 is done according to system network architecture. The initial access to the RSG2100 communication parameters is through connecting to serial port RS232 (DB9 female connector) of the Ethernet switch to the RJ45 port of the Personal Computer (PC)[51]. This connection will provides an access to set up the following communication parameters

a) Data bits equal to 8 bits
b) No parity bits and stop bits
c) Baud rate at 38400 bits per second
d) Disabling hardware and software flow settings

The settings for serial connection are chosen according to RSG2100 user manual as following;

e) Baud rate: 57600

f) no parity bits and stop bits

Once the connection has been established the authorized user is then eligible to configure the switch using Rugged Operating System (ROS) web server interface to provide permanent connections amongst substation devices using Ethernet link layer. Figure 3.2 represent the ROS web interface main menu after login in to begin with the configuration process. The station network IP address is referred as a RS2100 address which is set to 192.168.1.0 as shown in figure 3.1.

Figure 3.2: ROS web interface main menu

The ROS web server main menu have got numerous section that need to be configured, however for this research only administration and Ethernet port will be configured as highlighted in figure 3.2 above.

g) Administration

Once the administration is expanded it provides the options to configure IP interfaces and services. Access to the substation Ethernet switch is restricted to ensure that substation data is not accessible to the third part; hence RSG2100 offers different levels of access to the substation data

h) Operators access

i) Administration access

j) Guest access

Administration provides uppermost access to the substation data compare to operator and guest access. Figure 3.3 shows the extended sub-section under administrations menu for both network and devices to be integrated in the network.

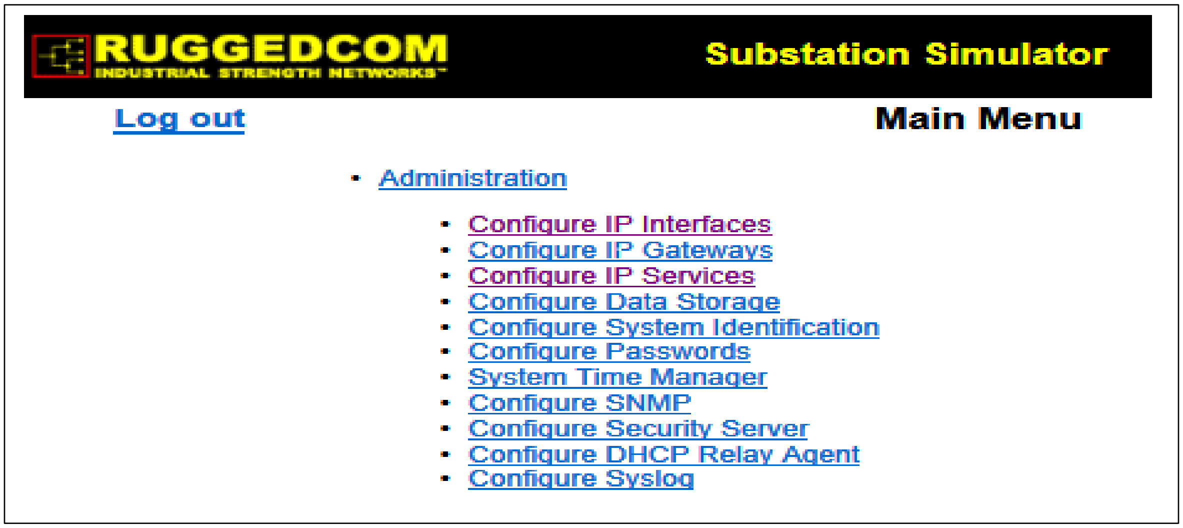


Figure 3.3: RSG2100 administration menu

Figure 3.3 above shows the administrative parameters, most importantly are configuration of IP interfaces and configuration of IP services.

3.3.2 RSG2100 Ethernet ports settings

RSG2100 is able to control up to nine Ethernet communication ports at a very high communication speed. Figure show the Ethernet port menu that is used to allocate ports to the devices, configure ports rates, statuses and alarms. It's also offers the option to configure the Virtual LAN that uses data logical frame to identify traffic. This affords the interoperability between substation devices since its permit the broadcasting of single message to multiple IEDs connected to the network. Ethernet ports allow the authorized user to configure the following settings;

a) Communication parameters

b) Port mirroring settings

c) Port link detection

d) Port rate limiting and viewing port status

Figure 3.4 illustrate the Ethernet parameters of the port allocated to SEL 487E that uses 100TX media type.

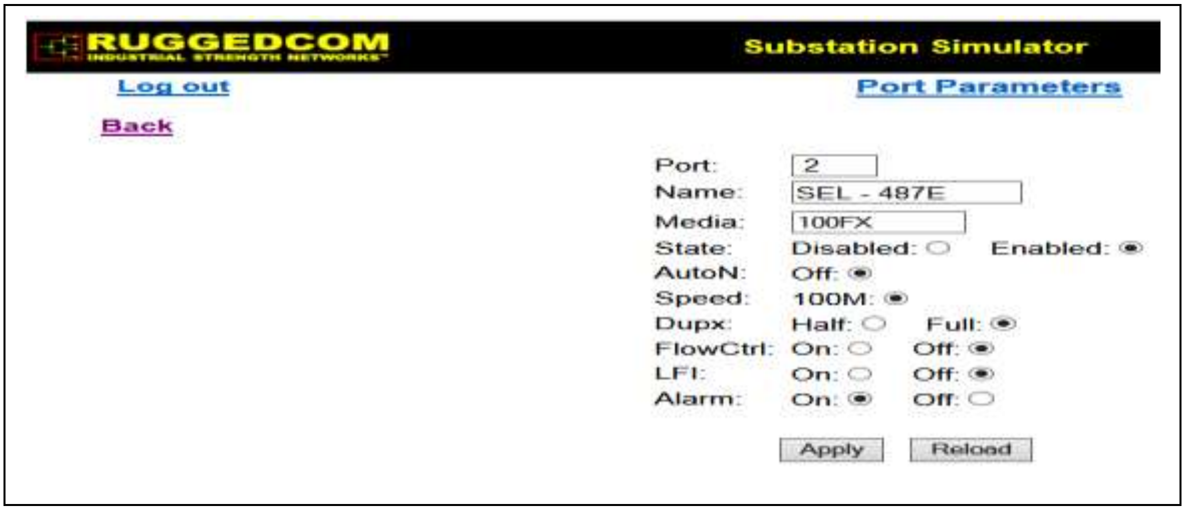


Figure 3.4: Port parameters setting for SEL 487E relay

Figure 3.4 show that port two of the Ethernet switch is used as the transmitting and receiving link for DNP3 data either from D20 or REF615 according to the communication architecture. Following are the communication parameters for ports six allocated to the REF615.

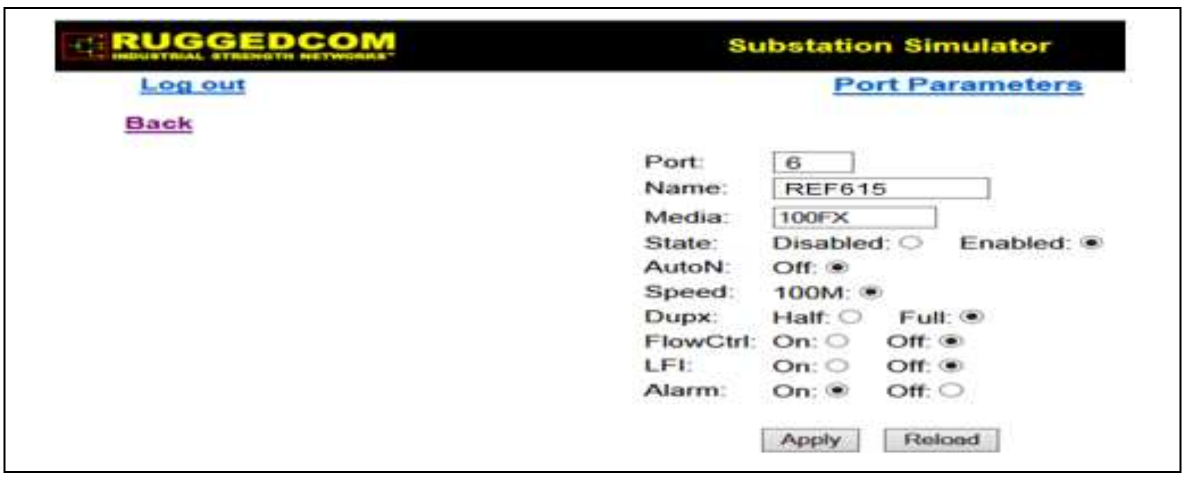


Figure 3.5: Port parameters setting for REF615 relay

The state parameter is enabled for all devices so that the frames will be sent and received during the link detection, Auto-negotiation setting set of since the ports are set to communicate over 100Mbps in full duplex as shown in figure 3.4 and 3.5 respectively. When the communication link currently configured fails the link fault detector guides the transmission of data.

3.3.3 Access from web management interface

To access the IEDs connected to the switch via web management interface, an Ethernet cable need to be connected to one of Ethernet switch ports. On the web browser, the IP address of the device or port required must be entered.

3.4 SEL 487E communication settings

SEL 487E is a transformer differential protection relay that is programmed using AcSELerator Quickset and AcSELerator Architect software's [52]. After launching the AcSELerator Quickset as illustrated in figure 3.6; the main menu provide the following selections: create new settings, read settings from connected devices and open previously saved settings.

Figure 3.6: AcSELerator QuickSet Launchpad (main menu)

SEL 487E is using a dual 100BASE-FX Ethernet card to provide E-DNP3 communication. The card is situated at the rear of the relay. SEL 487E uses SELOGIC circuit and equations to provide a wide range of functions such protection, monitoring and control. Figure 3.7 illustrate the mapping of DNP3 data points.

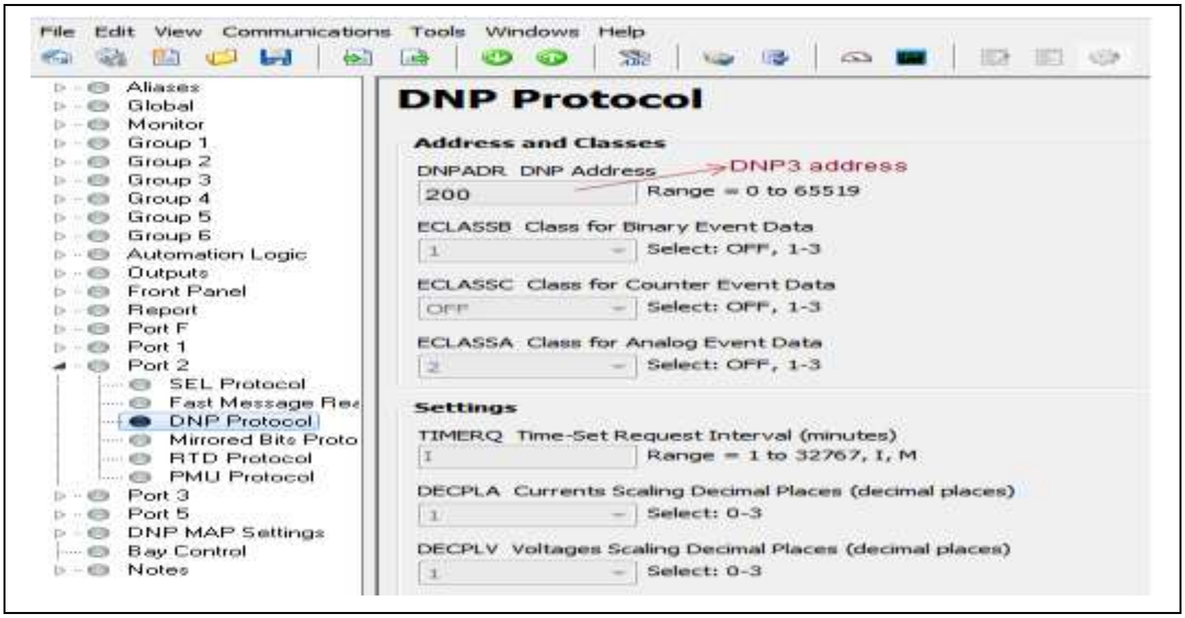


Figure 3.7: SEL 487E DNP3 setting

These communication parameters cannot be changed over Ethernet connection it need a direct RS232 connection. The DNP3 slave address is 200 communicating to the slave address of 260 as shown in figure 3.7 above. Below is table 3.2 that represent the DNP3 settings over Ethernet communication.

Table 3.2: Ethernet DNP3 Settings

DNP3 Settings	Settings Description	Recommended value
ENDNP	Enable DNP3 for Communications (Y, N)	Y
DNPPNUM	E-DNP3 Port Number for TCP and UDP	20000
DNPADR	SEL- 487E E-DNP3 address	200
DNPTR01	Data Transportation Protocol (UDP, TCP)	TCP

3.5 REF615

RED615 is an ABB relays that are used to control, monitor and protects the power system. This relay is mainly used for transformer feeder protections for medium voltage and is programmed using PCM600 software [53]. To ensure that commissioning is fast and cost effective, REF615 are provided with default communication parameters and tested from the supplier. PCM600 configuration provides the option to create new project and add the device (REF615) to the project [52]. Figure 3.8 shows the new project being created that consists of substation name, voltage level and bay level.

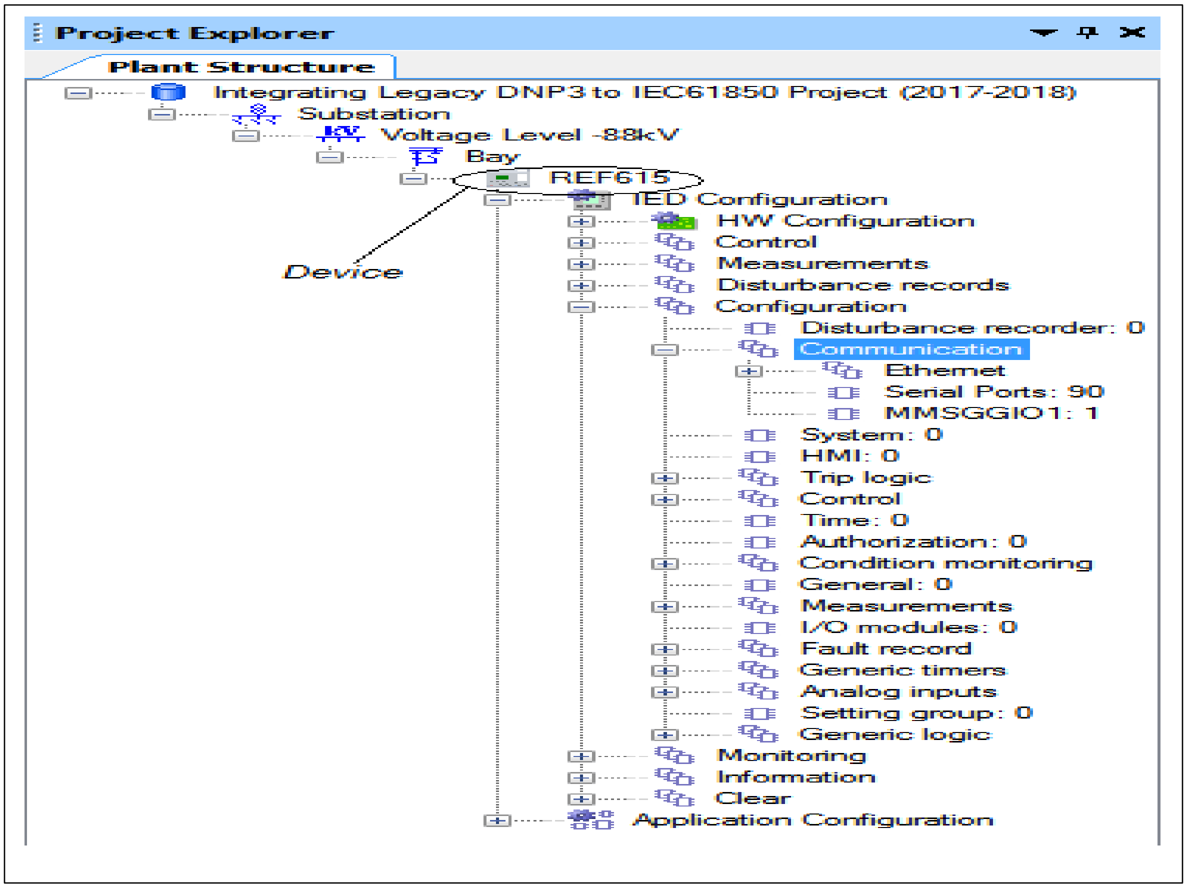


Figure 3.8: REF615 configuration main menu

Once the new project has been created it's provide the sub-sections that must be configured depending on the design requirements as it is illustrated in figure 3.8. The communication wizard is then used to configure IP address and device protocol as shown in figure 3.9 and 3.10 below. The IP address of the REF615 is set to 192.168.1.4 with the subnet mask of 255.255.255.000 similar to SEL 487E since they are in the same network. The DNP3 slave address is 250 communicating DNP3 data to master address set to 200.

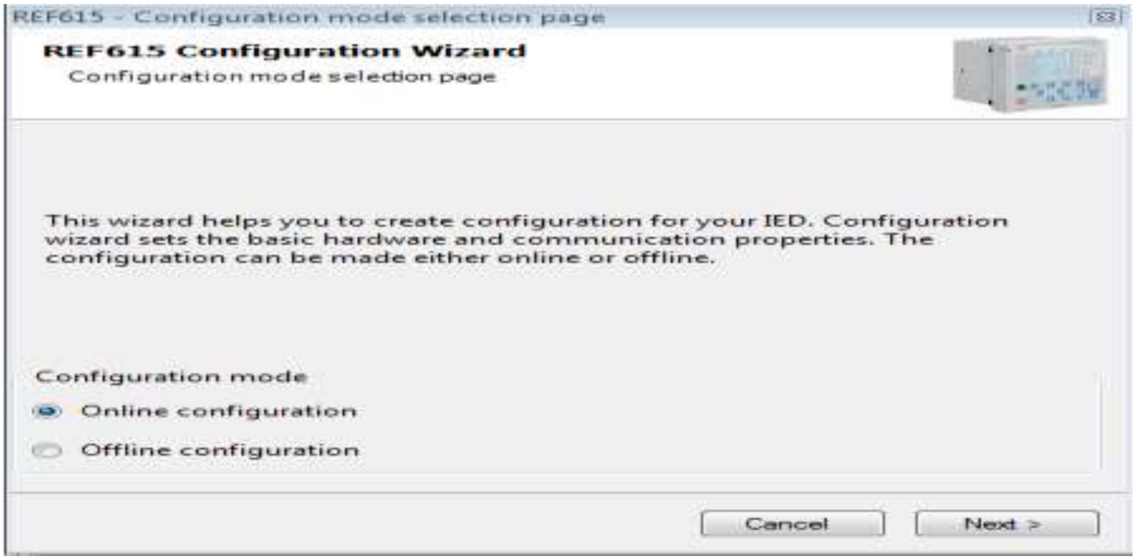


Figure 3.9: REF615 configuration wizard

There are two modes of creating the configurations for the device: online and offline mode. Figure 3.9 illustrate the online configuration mode. Figure 3.10 is the configuration of IP address and port communication medium selection.

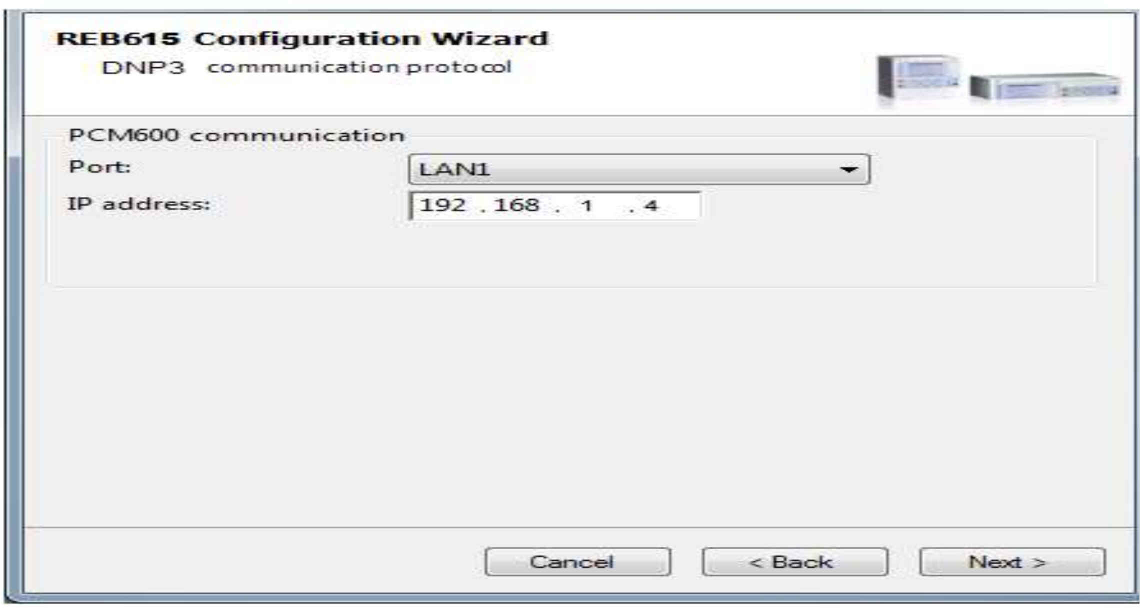


Figure 3.10: Configuration of IP address

Once the configuration steps shown in figure 3.9 and 3.10 are completed the detailed configurations files can be uploaded to the device since the list of all communication and protection functions will be visible. PCM600 software tool scan the device to acquire the serial number from integrated ABB server after completing the initial set up as shown in figure 3.11.

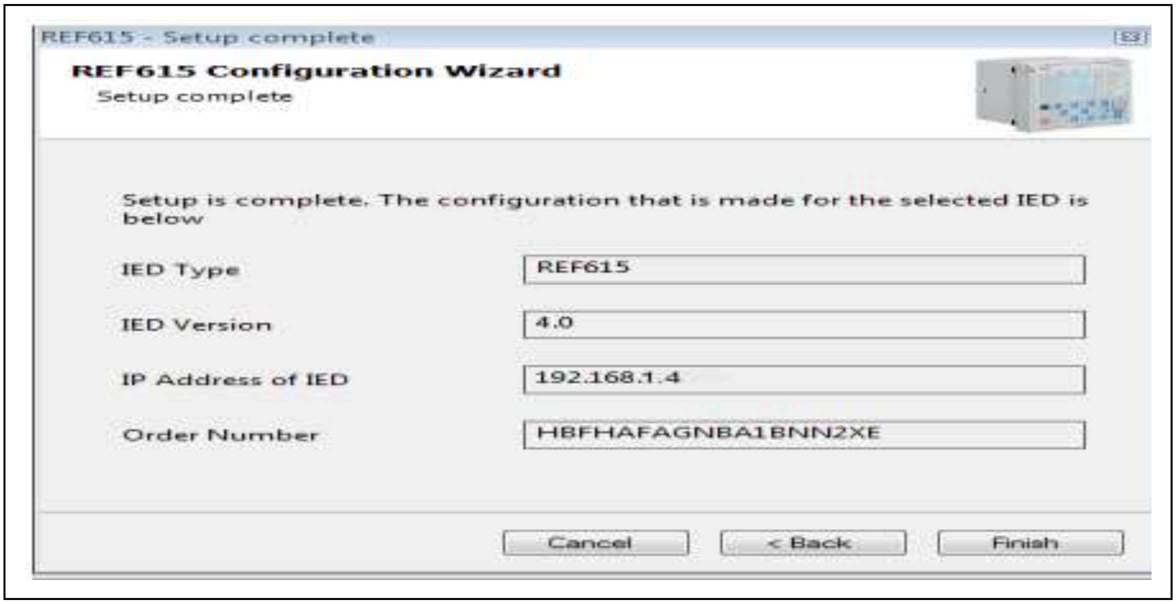


Figure 3.11: Completion of the initial set up for the REF615

Figure 3.11 above shows the relay software version, configured IP address and the order number that is: HBFHAFAGNBA1BNN2XE

3.6 GE D20 Configuration

D20 is a secure Generic Electric (GE) Remote Terminal Unit or gateway that collects substation data from protection relays and converts the data to make it compatible for further processing [54]. The device is programmed using ConfigPro Version 6. ConfigPro software program uses the Microsoft® Windows® operating system to apply and retrieve settings of substation D20 RTU. For this research D20 is used as master device to protection relay and IEC61850 server to IEC61850 client. The UCA/IEC61850 server DPA is implanted to the configPro configuration tool to map DNP3 points into IEC61850 data model.The peripheral modules are accountable for the genuine data acquisition. They directly interface to the external devices. The communications between peripheral cards is achieved via the D.20 Link. Following is the list of peripheral cards

a) D20S: Status Input Module - 64 Status Inputs and 1ms time stamping

b) D20A: Analogue Input Module - 32 Analogue Inputs and 14-bit plus sign resolution
c) D20K: control output - 24 Trip/Close and 4 Raise/Lower pairs
d) Power supply unit of 48V

Figure 3.12 shows the launching of configPro to create the new project.

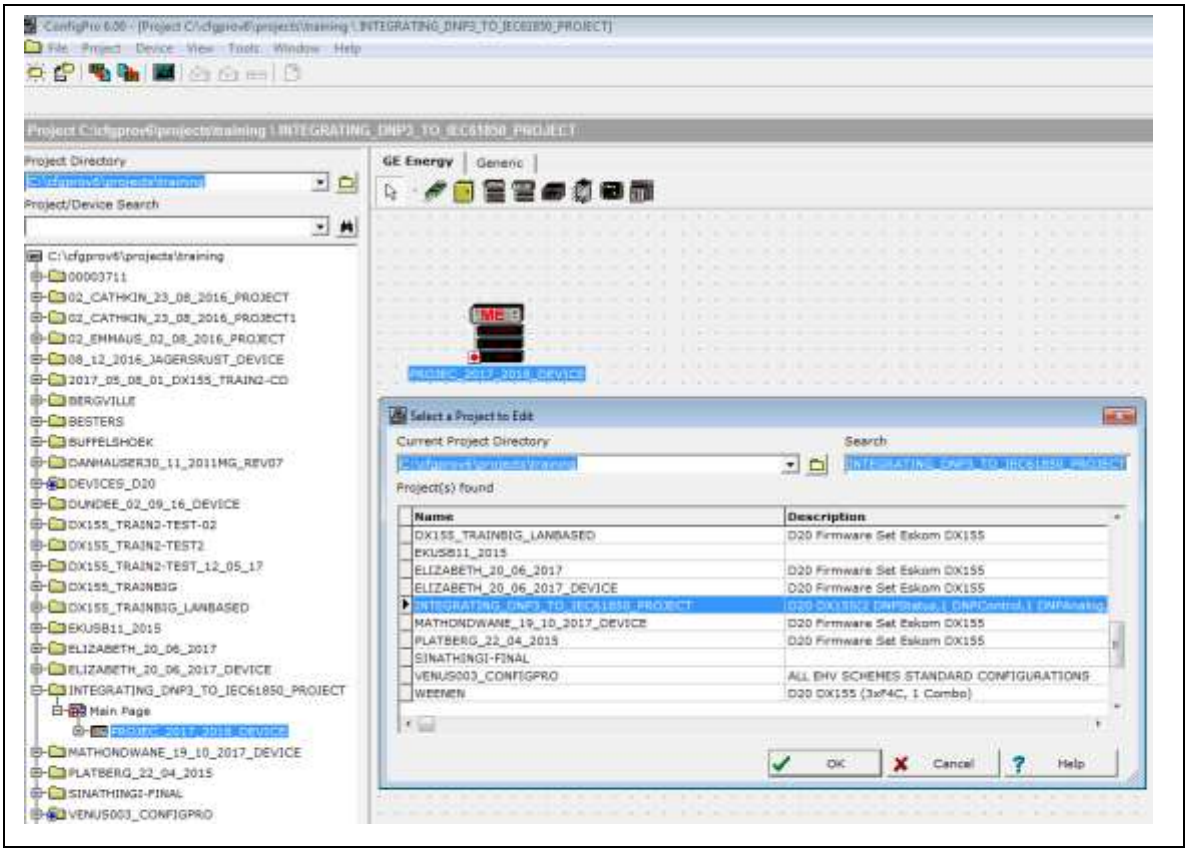


Figure 3.12: Launching of configPro

Once the new project has been created the mapping between protection relays and telemetry system can be done by double clicking to the device icon as shown in figure 3.12. ConfigPro software is built around a core of reliable and efficiently designed modules that are permanently programmed into the on-board memory of the system as firmware, and is known as the base system [53]. Figure 3.13 below illustrate the process of configuring the application that is used to collect data from Protection relays. Hardwired D20 telemetry unit is attached in (appendix A-6)

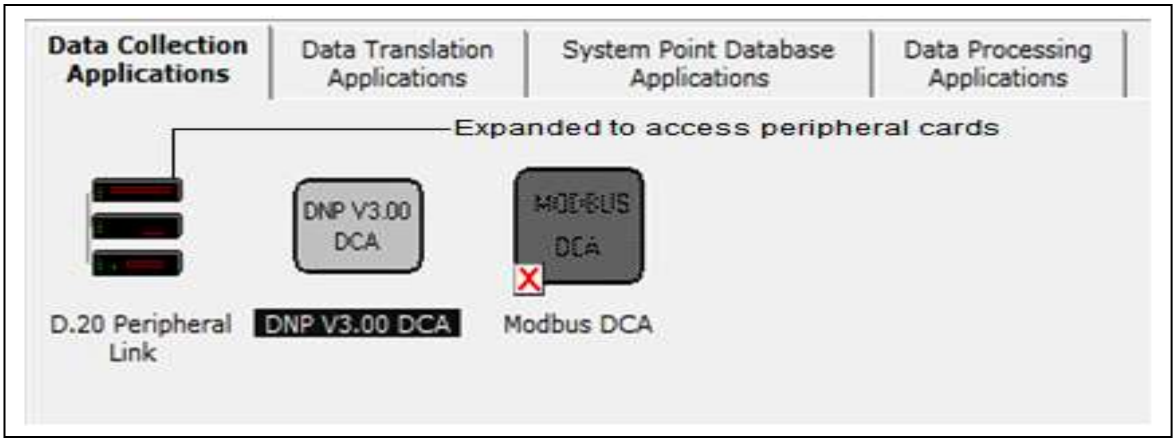


Figure 3.13: Detailed DCA mapping points

By clicking to data collection application menu, three icons will appear but only two will be used: D.20 peripheral link and DNP3 V3.00 DCA as shown in figure 3.13. Modbus DCA is disabled. When clicking to D.20 peripheral link, the software will allow the user to add the number of cards that will be required depending on the size of the database as illustrated in figure 3.14 below.

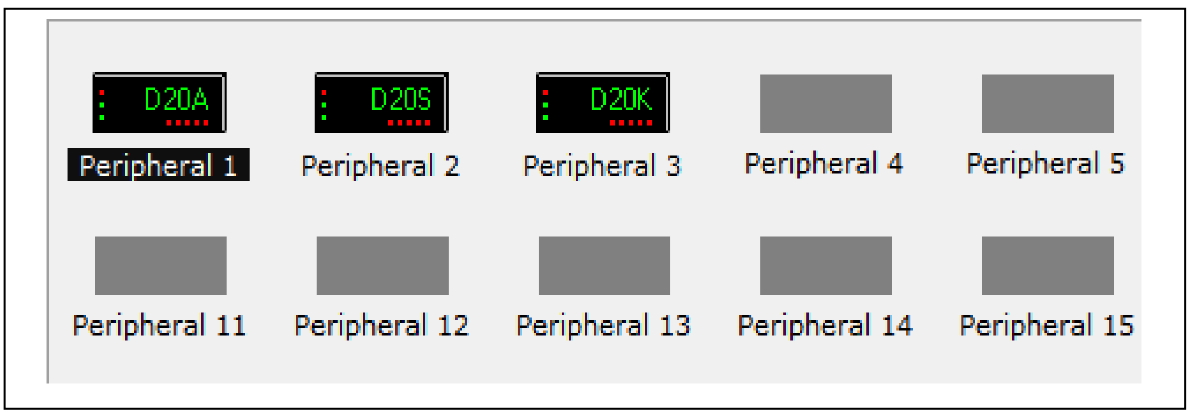


Figure 3.14: D20 Peripheral card (Analogue, Status and Control card)

Figure 3.14 shows three peripherals cards have been added to the software. Whatever that is added to the software must be wired also in the hardware architecture. From figure 3.14 it can be seen that analogue card is added to address one, status card to address two and control card to address three corresponding to the hardware architecture attached in (appendix A-6). Once the DCA has been configured, the user must click to next tab which is Data Translation Application as denoted in figure 3.15.

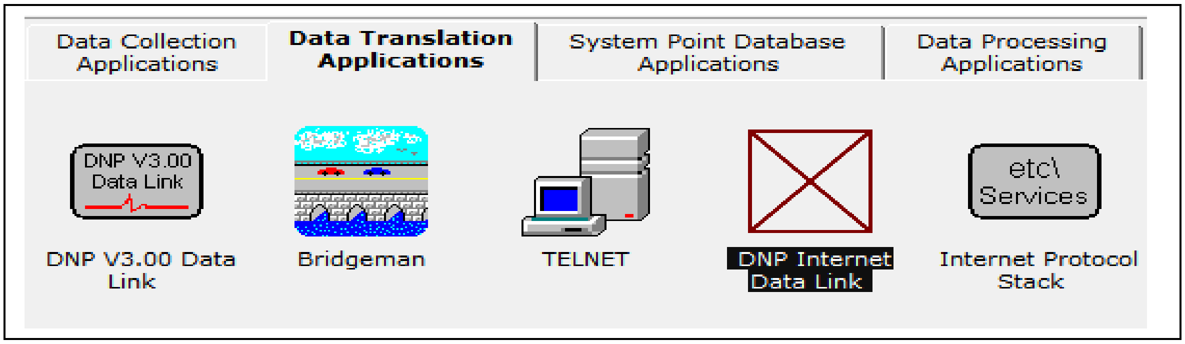


Figure 3.15: DTA configuration

All group icons accessed by clicking DTA tub are enabled. These icons are DNP3 V3 Data Link, Bridgeman, Telnet, DNP Internet Data Link and Internet Protocol Stack and are shown in figure 3.15 above. DTA is a module that duplicates existing data from the system point database, process it, and output new system points into the database. The data points created by DTA are called pseudo points, as they are not “physical” data points. The last tab is Data Processing Application tab that have three enabled group icons: DNP V3.00 PDA, file manager and UCA/IEC61850 Server DPA as shown in figure 3.16. UCA/IEC61850 server is imported to the software to carry out the simulation of this research.

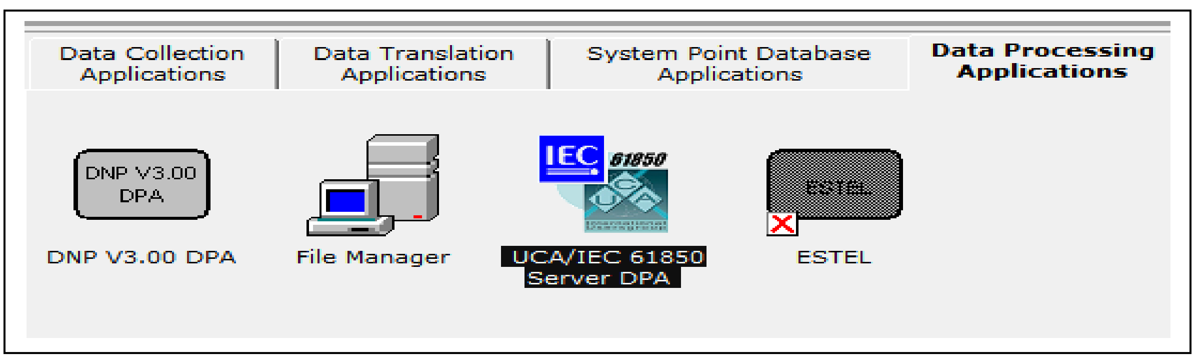


Figure 3.16: DPA configurations

The UCA/IEC61850 Server DPA shown in figure 3.16 above is used to map DNP3 data points into IEC61850. DPA is a module that takes copies of any available data in the system point database, and processes it into into a format compatible with a client protocol; in this case client protocol is IEC61850. Figure 3.17 show the binary input map table, binary output map table, analogue input map table, counter map table, frozen counter map table and internal indication map table. The list of binary input is attached to (appendix A-7).

3.7 Mapping DNP3 data into IEC61850 data model

This section represents the summary of the procedure to convert the native DNP3 data into IEC61850 data format. Specific logical nodes relevant to substation automation need to be created in table one (1) of figure 3.17. Table two (2) is group L that contain the characteristics for logical node zero (LLN0) to manage the virtual part of the device. Group L also contain the parameters for Physical Device Logical Node (LPHD) that represent physical device and communication statistics. Table three (3) is the data point table where data to be represented in IEC61850 is selected.

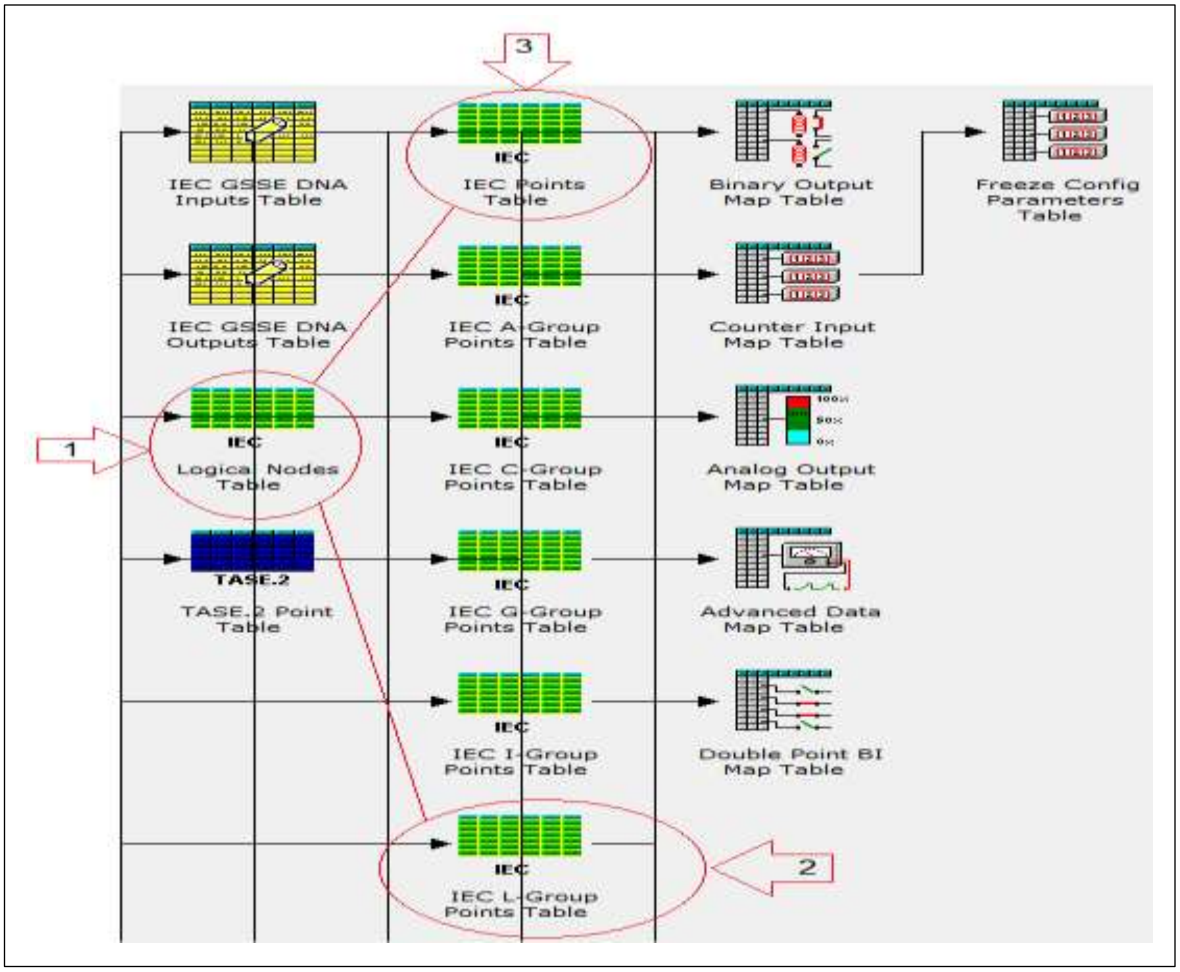


Figure 3.17: Crucial IEC61850 group tables

Figure 3.17 here represent the crucial tables and steps of configuring DNP3 master device as IEC61850 server. Following is figure 3.18 that represent the tables where the detailed mapping between these protocols is carried out including the configuration of the specialized logical nodes.

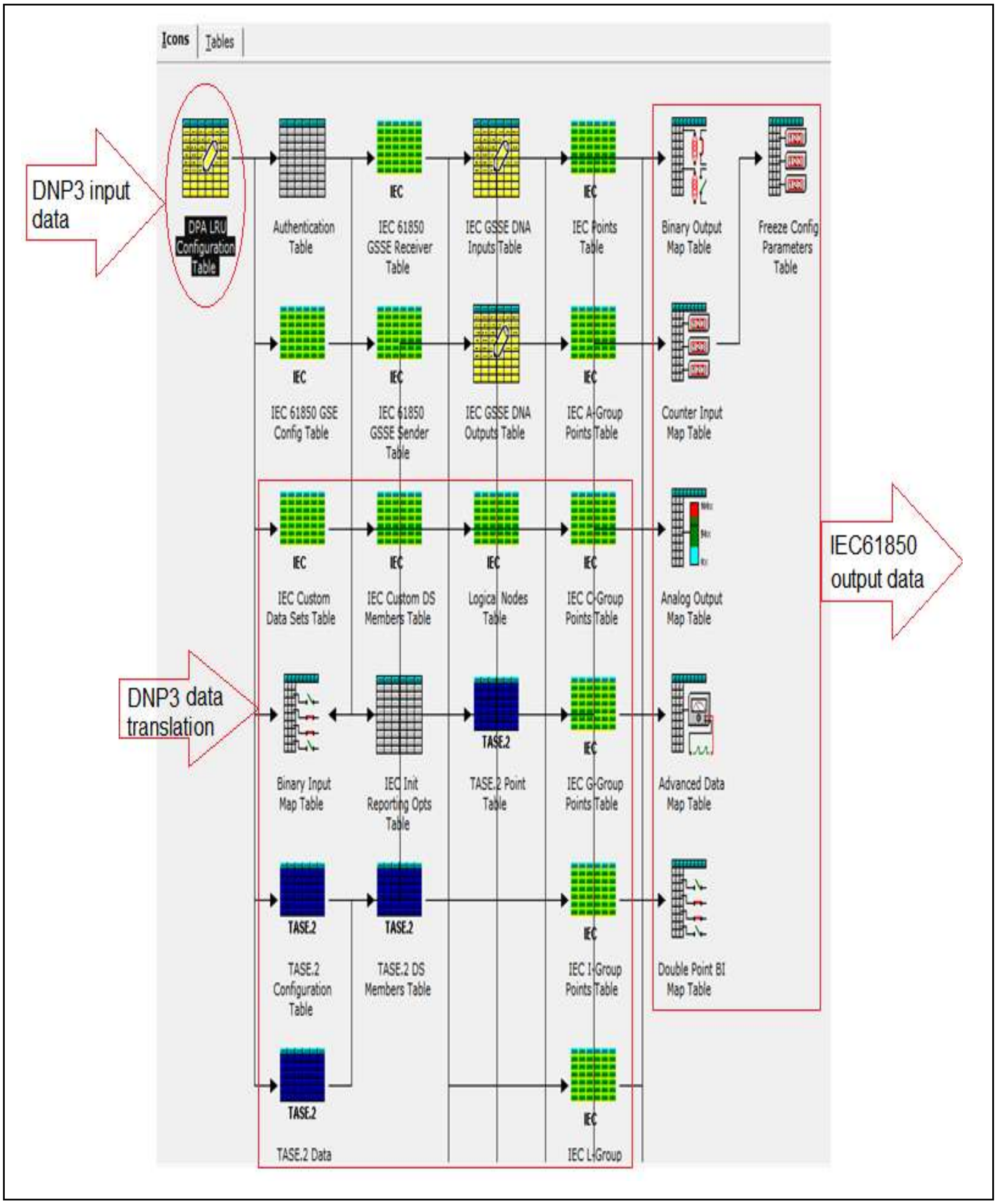


Figure 3.18: Mapping tables between DNP3 and IEC61850.

Figure 3.18 represent the summary of obtaining IEC61850 data from DNP3 input data and further highlight the tables that are used. This figure indicates the tables that are used to create and extend data object, create dataset, create control blocks, create dictionary and create the logical nodes additionally from those in figure 3.17.

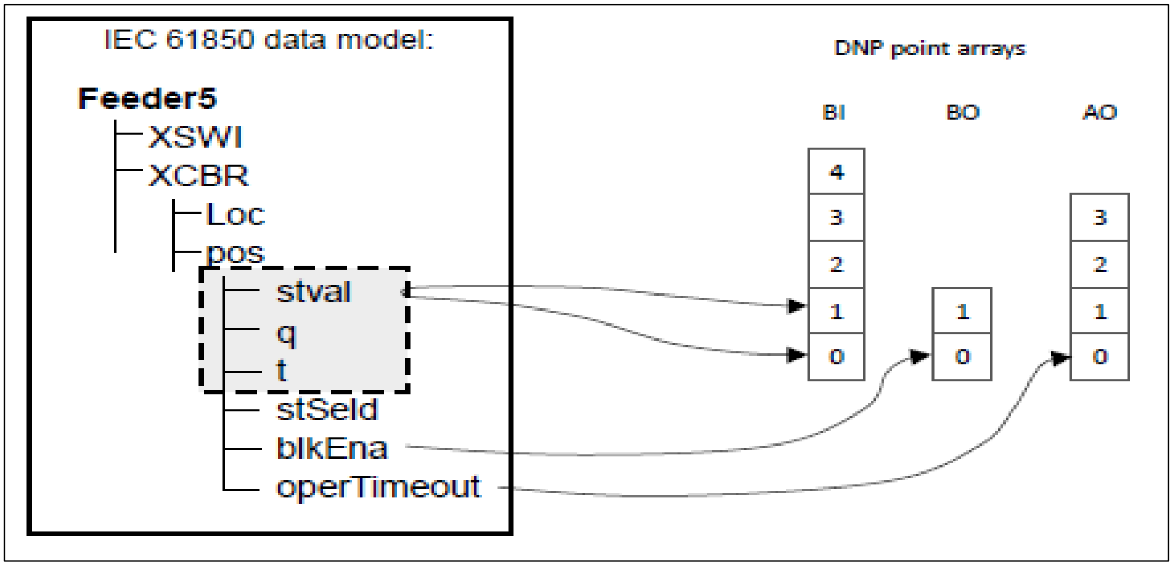


Figure 3.19: DNP3 and IEC61850 data model

Figure 3.24 represent the schematic representation of object mapping between IEC61850 and DNP3 [55].

3.7.1 Mapping of control parameters

Control parameters (“ctlVal”) carry the principal state change information for the IEC 61850 control services and these are known as pass through services. This is found in the IEC 61850-7 common data classes that have names containing the words “Controlled” or “Controllable.”

3.7.2 Data attributes ctlNum and origin mapping

a) Origin

The IEC 61850 server in the gateway shall implement the “origin” data attribute as according to the standard IEC61850-7-2, these does not need any mapping from DNP3 data points, since it originated from IEC61850 server.

b) CtlNum

The data attribute called “ctlNum” is used to identify a number of controls.DNP3 does have this concept, therefore “ctlNum” is not mapped, the IEC61850 server embedded in a configPro software used to configure gateway will be responsible for its correct use [55].

3.7.3 Data type INT32 and INT64 mapped to counters

DNP3 have 32 bits, therefore all 32 bits are mapped to lower 32 bits of the IEC61850 INT64 attribute and upper attributes are set to zero [55].

3.7.4 Mapping of configuration and description information

In this scenario, the configuration is supported by DNP3 object and can be read or written by the IEC61850 client. Some of these attributes have a corresponding entry in the DNP3-XML device profile. The IEC61850 server in the gateway is configured to provide fixed values from the DNP3-XML Device Profile [55].

3.7.5 Analogue range configuration

DNP3 has no explicit equivalent of the IEC61850 range data attribute that reports when an IEC61850 measured values reach the predetermined alarm limits. But the DNP3-XML device profile does include parameters corresponding to the minimum and maximum range for data attribute, due to that; the correspondence between DNP3 analogue output point numbers representing limits and the appropriate IEC61850 measured value are mapped together and will be internally determined in the gateway [55]. This mapping rule is called (INT_TO_AO_PROFILE).

3.7.6 Pulse configuration

It must be noted that the control services provided by DNP3 (IEEE Std 1815-2012) and IEC 61850 are the same, but the semantics of performing these services are different. The mapping or configuration of these data points enables the substation gateway to copy the current value of the IEC61850-7-3 pulse configuration parameters into a DNP3 IED in a single massage to perform the operation when the IEC61850-7-2 write to the output command value data is received [55].

3.7.7 Readable data configuration

The accessible DNP3 data objects from RTUs are mapped entirely to the intrinsic IEC61850 standard. The IEC61850 data that resides in the IEC61850 default dataset is included in the DNP3 object mapping. Object within DNP3 datasets produce time tagged event. DNP3 event and time stamps are propagated to IEC61850 client when added to the network [55].

3.7.8 Writable data configuration

Writable objects belong to object types (binary outputs) and (analogue outputs). Outputs are controlled through the control relay output block or analog output block commands. From the DNP3 output objects, the commands are propagated further to the native IEC 61850 control objects [55]. Controls are also called pass-through commands in this scenario.

3.8 Data collection architecture

This section represents the architecture of collecting data between two systems that is analyzed and discussed in chapter four. There are two tools that are used: Fieldcom data analyzer for DNP3 and wireshark data analyzer for IEC61850.

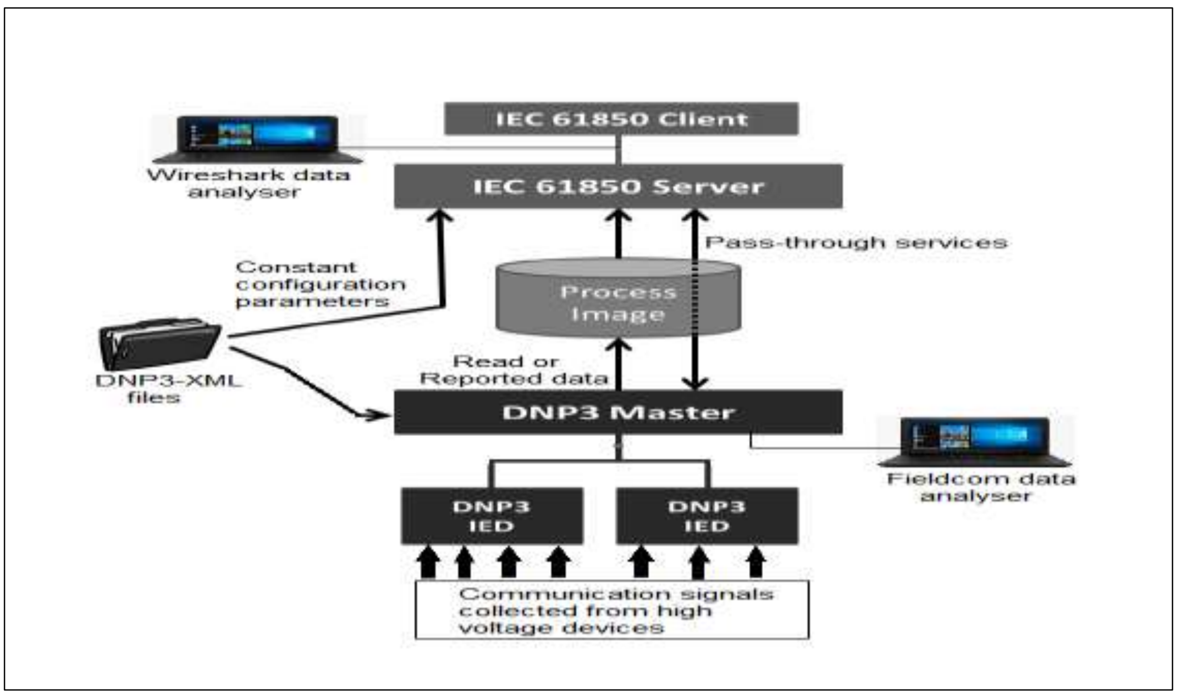


Figure 3.20: Data collection architecture

Figure 3.20 represent the architecture on how the devices are interconnected and how the data is captured between two systems.

3.8 Conclusion

This chapter demonstrated that; the integration of DNP3 data points either Ethernet or serial communication into IEC61850 is possible. However the key aspect discussed in chapter two as interface, real time data networking and device communication must be taken into consideration so devices will share data effectively. This approach maximizes the life span of legacy devices by linking them into modernized digital substation architecture. Integrating DNP3 data points into IEC61850 over Ethernet communication network architecture is a cost saving strategy that improve data and device availability to the host control centres. The availability of data is foremost requirement to achieve real time data networking and communication. This architecture does not only expand the lifespan of legacy devices it further reduce the cost related to the wholesale replacement of DNP3 devices. The configuration of this network will benefit utilities that are planning to use IEC61850 SCADA management or both DNP3 and IEC61850 within substation to reduce full replacement costs. The detailed results and data analysis of this architecture is chapter four.

Chapter Four

Results and Analysis

This chapter comprises the analysis, presentation and interpretation of the findings resulting from this study. The analysis and interpretation of data discussed in this chapter fall within the following classifications. The communication speed performance, network traffic analysis, and data availability and reliability.

4.1 Introduction

The integration of DNP3 data points into IEC61850 data model discussed in chapter three has improve the capabilities of substation devices that are dependent to communication medium and data integration procedure. It has further brought together the standards and technologies that were developed separately. Both DNP3 and IEC61850 were developed to achieve similar goals as to improve the substations automation capabilities. The results of this approach have created the flexible, efficient and reliable substation communication network. Moreover this approach is preferable other than a complete replacement of legacy devices in substations.

4.2 Checking errors for configuration files

The configuration files may contain errors that need to checked and rectified before is uploaded to the devices.

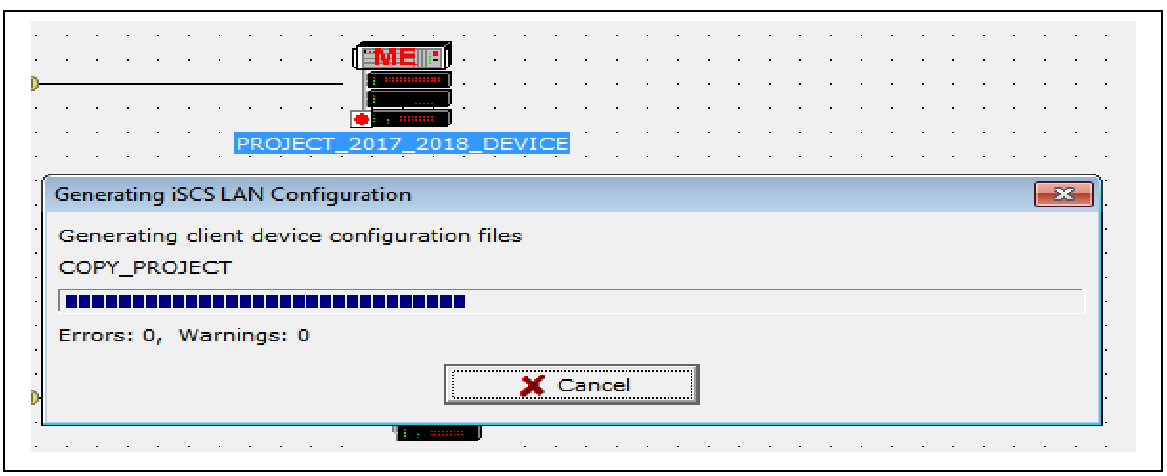


Figure 4.1: Generating files for configurations

Figure 4.1 illustrate the procedure of checking errors and warnings to the configuration files. As the system continues to scan files, it shows that the configuration has got no error and warning, and then it can be uploaded to the devices.

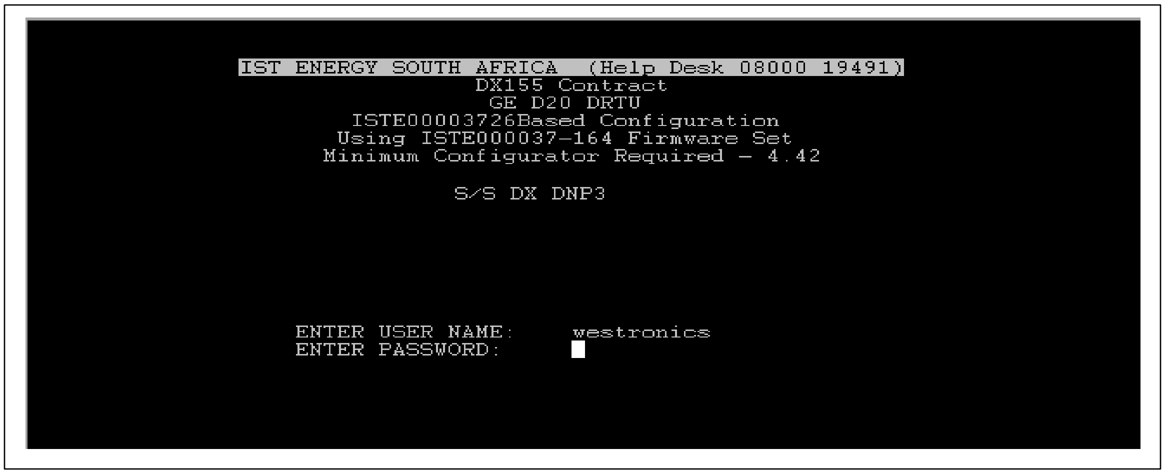


Figure 4.2: Terminal emulator login screen

Figure 4.2 illustrate the procedure that is used to login it to the telemetry unit (D20) to view the statuses of integrated devices once the configuration has been uploaded to the devices. Figure 4.3 below shows the communication transaction between peripheral cards and the central unit.

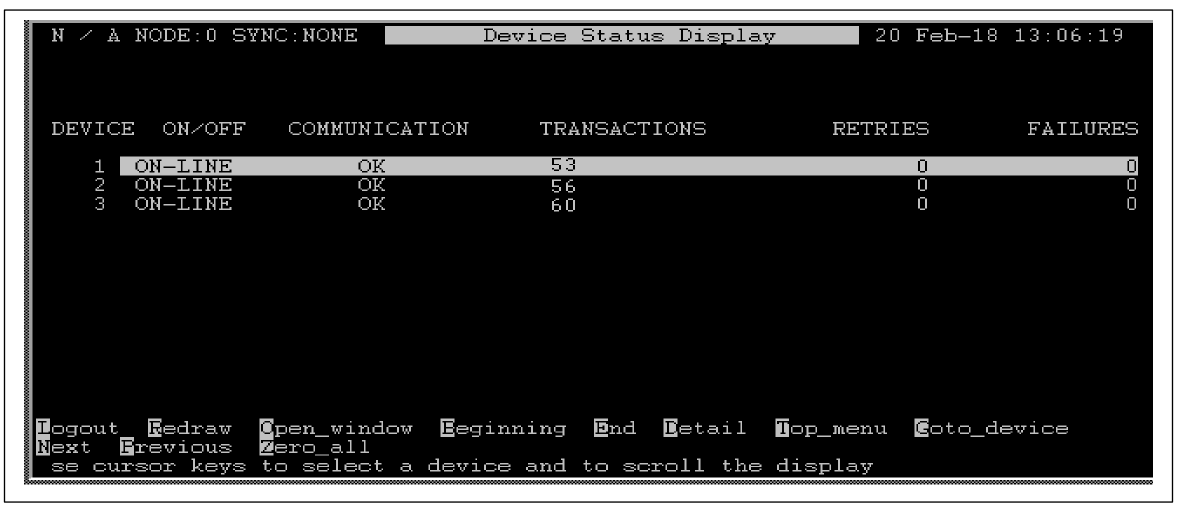


Figure 4.3: Communication transactions for peripheral points

Figure 4.3 conform to figure 3.14 in chapter three; showing only three peripheral cards for status, controls and analogue.

4.3 Communications verification and analysis

After completing the mapping between telemetry unit and protection relays; the communication counts are viewed to see whether the device are online and updating the data to the central unit.

4.3.1 SEL 487E and REF615 communication counts

The integration of substation devices is driven by communication between protection relays and telemetry unit. Figure 4.4 shows that, the SEL 487E device is online and updating data to the telemetry unit.

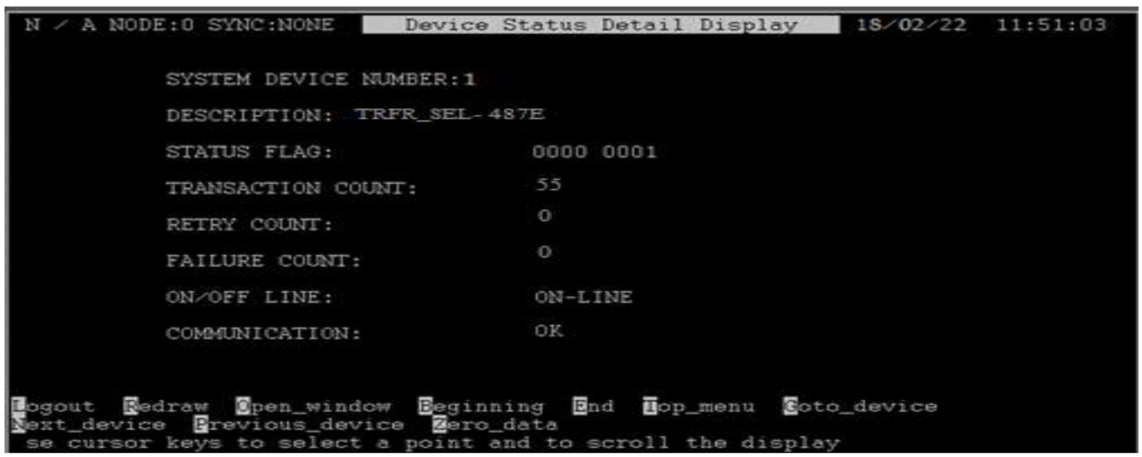


Figure 4.4: SEL 487E communication count

This is just an indication that the communication function is working properly and the device is online. Figure 4.5 below show the communication status for REF616.

Figure 4.5: REF615 communication counts

Figure 4.4 and 4.5 show the communication count of protection relays integrated to the telemetry unit. As shown all devices are online and communication is ok. Following is the verification of digital inputs.

Figure 4.6: Confirmation of mapped digital inputs

Figure 4.6 above shows the first ten digital inputs for the specific substation that is used in this study. These status points are mapped to the telemetry system matching both the points for both protection relays. The telemetry system is configured to scan and process these digital inputs in the interval of one millisecond to ensure that all changes are reported as soon as possible. Below is the screen that shows the controls that are mapped between relays and telemetry unit.

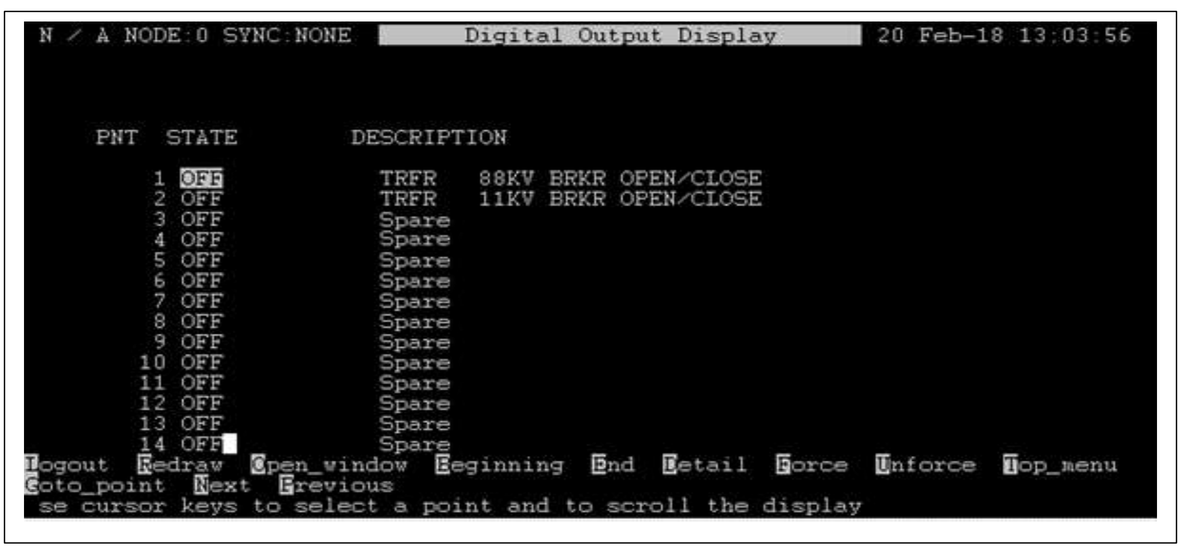


Figure 4.7: Verification of mapped digital outputs

Figure 4.7 shows two controls for 11kV and 88 kV breakers. These controls are open and close. The point's addresses are very important to the IEC61850 server and client when the controls need to be executed. The telemetry system in this case is configured to ensure that, the following control security requirements are met.

a) Select Before Operate
b) Only one control is selected and executed at a time by IEC61850 client
c) The control must be cancelled if not execute within specified time.
d) RTU will not execute any selected control if it shutting down or powering up.

4.3.2 Delay performance analysis

This analysis were done between two communication medium (Ethernet and serial) for the similar protocol (DNP3) to validate that, the introduction of Ethernet in substation automation has improve the efficiency of data exchange between integrated devices. This analysis proved that, the rate at which the data is transferred from device to device strongly depends upon communication medium. Ethernet communication has the following basic settings

a) Dedicated TCP/IP address
b) Subnet mask address
c) 1000Mb speed auto negotiation full duplex

Serial communication has the following settings

d) Baud rate: 9600, speed the rate at which data is transferred across devices, this is known as baud rate or bit rate. The speed of 9600 bit per seconds is used that means every bit will take 104.2 micro seconds to transfer data
e) Data bits : Eight (8)
f) Parity : None

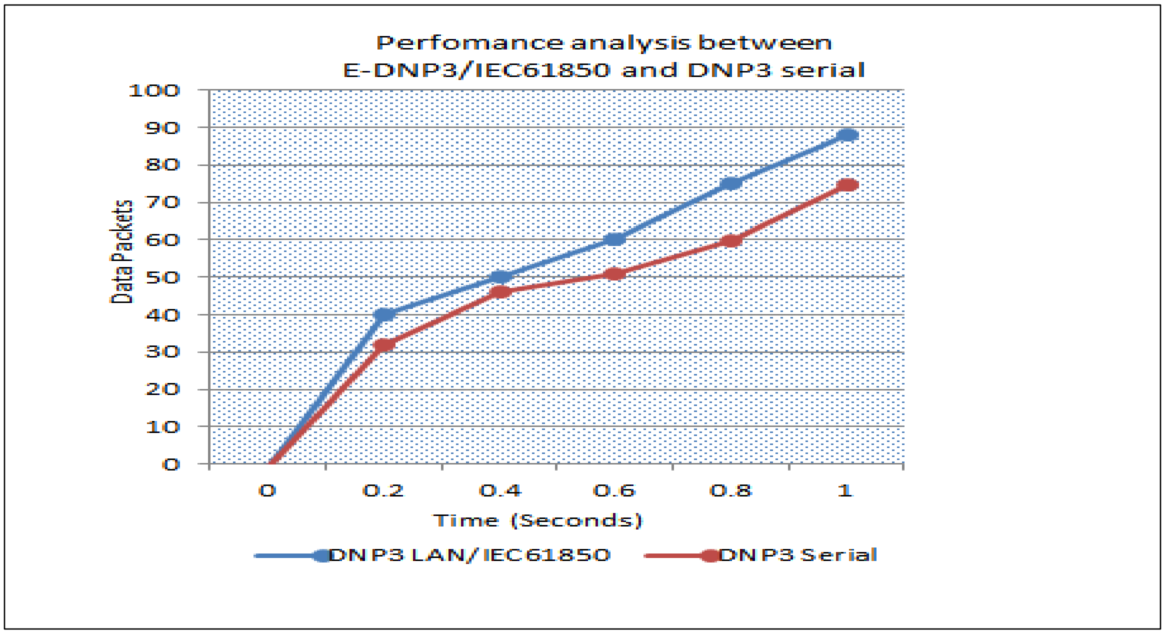


Figure 4.8: Performance analysis of DNP3 serial and Ethernet

Figure 4.8 above illustrate that, the speed at which the devices communicate to each other in Ethernet communication is much higher than those over serial communication network, because the serial communication always send the data sequencially between devices using the principle of Least Significance Bit (LSB) first and Most Significance Bit (MSB) after that cause delay.There is a data distortion that is caused by signal interference if the signal is travelling over the long distances and exposed to sound . If the control pannels are close to each other the effect of signal interference is reduced but the vibration of high voltage apparatus can still cause distortion.This analysis also revealed that Ethernet communication provides auto negotiation mechanism as discussed in chapter three; that enables the network to switch between 10Mbps and 100Mbps. The transmitted message must be coordinated by both sender and receiver of the data to improve the reliability since its send and receive multiply data packets at the time. From the results obtained it was observed that DNP3 TCP interchanges data continuously to the network to ensure that data all data packets reaches its destination, however the data packets are unstructured since its uses advanced data addressing, collussion detection or avoidance, re-transmission function and CRC.

Fast messages are generally binary value data intended for protection scheme and control, and are mapped directly to Ethernet TCP/IP to optimize its decoding and overall transfer time. From the results it was further revealed that, the received data signal over serial communciation will never be the same as transmitted signal, hence the serial communication network requires the installation of additional devices to regenarate the signal. This often complicate the network. The received signal must be always sampled at the right time or else it will result to the signal bit error.It was then concluded that, the adoption of DNP3 ethernet for substation communication have the following advanatages:

a) Reduce the domain for broadcasting, (increase security of the network and reduce the traffic in the network). These advantages are hampered in serial communciation network architecture
b) Reduce the need for bulky hardwiring and the easily expanded
c) Improve the traffic control function over various traffic categories
d) High speed peer-peer communcation

Figure 4.9 illustrate the response of DNP3 serial and E-DNP3 if the data request message is sent to the protection relays.

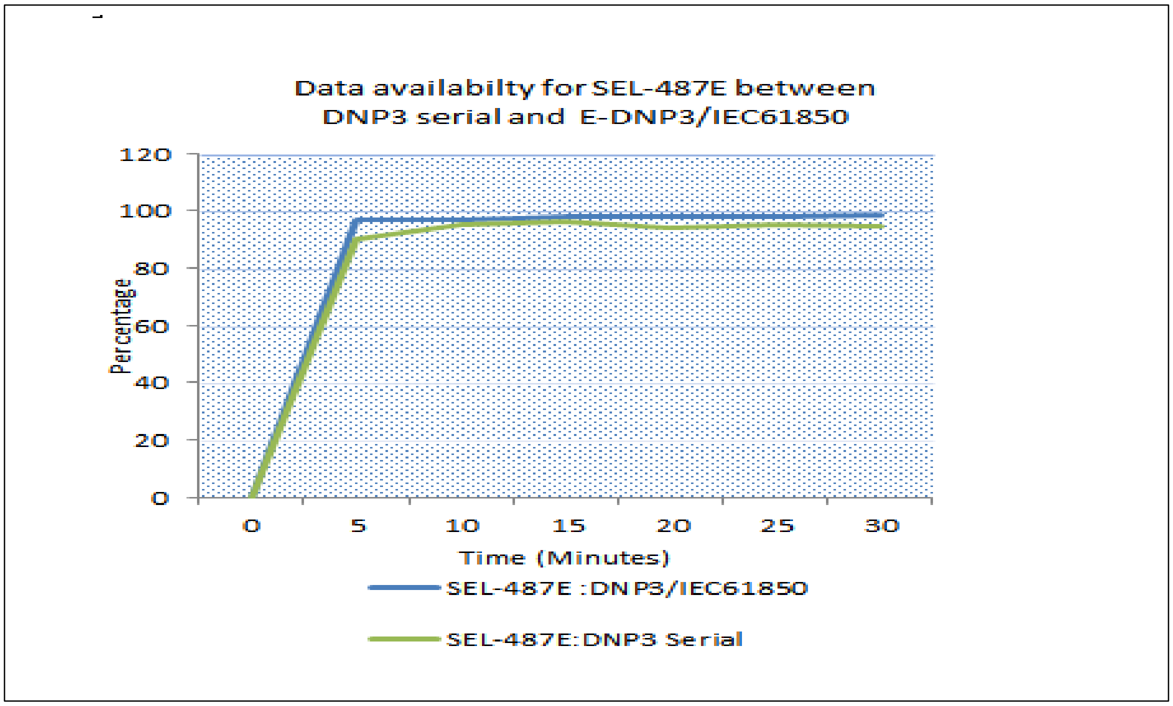


Fig. 4.9: DNP3 data communicated between substation devices.

The first integrity poll was initiated from zero to five minutes and the data availability for DNP3 serial was (90%) whereas the DNP3/IEC61850 was (97%). The second class poll was initiated in twenty minutes and the DNP3 serial data availability was (94%) whereas the DNP3/IEC61850 was at (98%). The last integrity poll was initiated in thirty minutes and, the data availability for DNP3 serial was (94%) and the DNP3/IEC61850 was recorded as (98%). This whole process took thirty minutes. The availability of data is calculated within the server of the network using modified linear equations to generate. From this performance analysis it is inferred that the availability of data in substation is dependent to the software and hardware architecture. Thus, to justify the response of DNP3 devices; the following equations are used.

$$Y = \beta 0 + \sum \beta i X i + \epsilon i \quad (1)$$

Y variable is a response and X_i is a predictor that is used in case the real data is not accessed. β is the linear limit estimates in computing tool and ϵ the error expected. The equation for contiguous exponential graph is:

$$Y = A^{-x} + B \quad (2)$$

This equation is to merge linear and exponential graphs within the server computing tool. A is a constant and B is a base that determine whether the performance grow or decay in terms of the data requested in the system. It must be noted that the percentage of data availability is not dependent to whether the time increase or decrease. However it is dependent to the physical and software integration of devices, the time just represent the intervals of timely polls. The equations are used to shape of the relationship between the systems. From these results it was observed that the integration of DNP3 data into IEC61850 server also improves the data availability for the legacy DNP3 devices that are currently used in substations. The data availability is the one most important requirement of substation automation to ensure that the local or remote control have the clear picture of substation data at all times. The improvement of data availability also increases the availability of integrated devices in the network. It further improves the device visibility.

4.3.3 Evaluation of substation data traffic between devices

When configuring or modelling the substation network and devices it very important to categorize data according to its priority. This is a very complex network that will control the flow of DNP3 and IEC61850 data. This analysis is performed to provide the insight of what is happening at the backstage of these devices. The reliability of time critical messages depends mostly on substation communication network and communication mechanism used in DNP3 and IEC61850 standard. The network data traffic management features offered by Ethernet communication improve the overall performance of integrated devices within substation communication network. Unlike serial hardwired substation automation schemes where the changes of the communication network parameters such as background traffic, data packet size, signal sampling frequency and etc influence the overall performance of integrated devices. Its further divulges the importance of communication network in substation automation applications where numerous multivendor devices need to be integrated. The use of Ethernet communication in substation provided the simplified communication backbone. Ethernet communication is easily expanded. The recent protection relays are also provided with direct Ethernet communication port in addition to serial communication port. The introduction of new the communication protocols such as DNP3 LAN and IEC61850 provided the various options to integrate the substation devices. These innovative contributions will speed up the adoption of Ethernet communication in substation applications. The communication between devices can only take place in the following order: SEL 487E to REF615 and D20 master/61860 server; REF615 to SEL 487E and D20 master/61850 server; D20_61850 server to D400_61850 client.

4.3.4 DNP3 interoperability demonstration

Breaker fail trip signal also known as (50BF) is used to demonstrate the interoperability between DNP3 devices integrated in the network. The simulation was done for both serial and Ethernet communication to compare the time taken for trip signal to reach the upstream relay. The CMC356 is used to inject fault current of 7 A to the SEL 487E protection relay. The main aim of the test is to compare the time taken for the trip signal to reach upstream (REF615) relay for both traditional integrated substation and Ethernet integrated. The block diagram to explain figure 4.10 below is attached in (appendix A-9).

Figure 4.10: Architecture of simulating interoperability using CMC356

Figure 4.10 above show the architecture of injecting fault current to the SEL 487E to demonstrate interoperability between DNP3 devices. Following is the figure that shows the growth of current in the relay contacts with respect to the voltage.

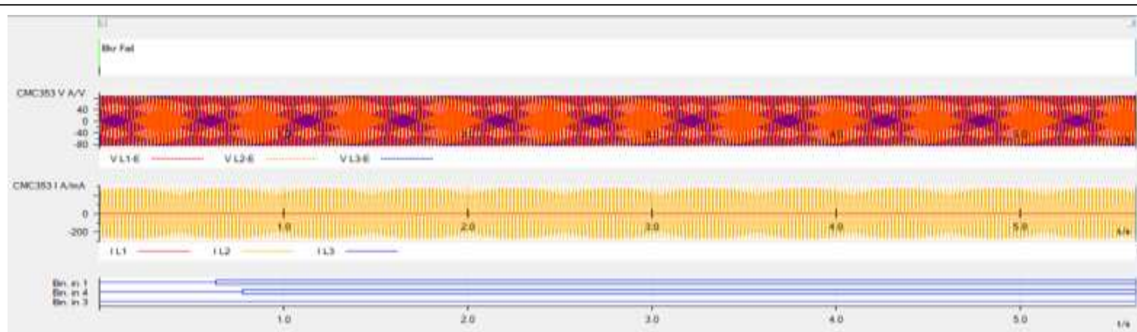


Figure 4.11: Voltage and current signal developing in relay contact

Figure 4.11 show the current and voltage signals that appeared in the relay contact after 7 A faults current was injected to SEL 487E. As the current grow to the pickup value, both relays detected the fault and the trip was blocked in trip terminals of SEL 487E so that; the breaker fail trip signal will be generated and transferred to the upstream relay (REF615).

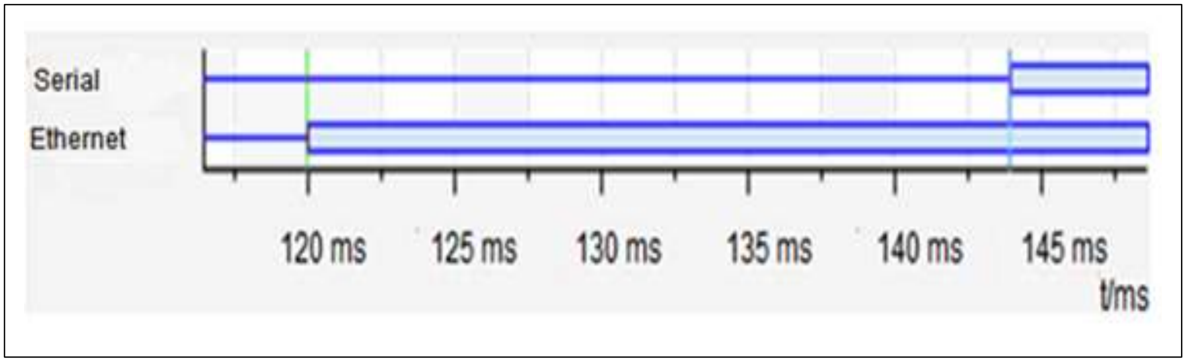


Figure 4 .12: Comparison of serial and Ethernet breaker fail trip signal

Test Results

Time Assessment

Name	Ignore before	Start	Stop	Tnom	Tdev-	Tdev+	Tact	Tdev	Assess
MV Bkr Fail Time	BFail Time	BFail Time	HV Bkr Fail 0>1	150.0 ms	30.00 ms	30.00 ms	120.1 ms	-29.90 ms	+

Assess: + .. Passed x .. Failed o .. Not assessed

Test State:
Test passed

Figure 4 .13: Breaker fails trip signal results

Figure 4.12 and 4.13 demonstrate the time taken for breaker trip signal for both Ethernet signal and serial wired analogue signal coming over the communication wire that is more than two meters. The trip signal was detected in 25 milliseconds faster than serial wired analogue signal. These results validate that Ethernet communication is a better solution for communication substation if the control panels are more than one meters apart. Since the lifetime of substation power plant equipment is generally between 35 and 60 years, the interoperability and interchangeability must be considered for every design to anticipate the replacement of substation devices in case there is a fault. The summary to illustrate the basics of using CMC356 is attached in (appendix A-8 and A-9)

4.3.5 Topology for the control execution

The main objective of this research is to analyse the performance of the legacy substation automation when the DNP3 data points is integrated into IEC61850 data model. Execution of control is an auxiliary test to demonstrate that there is a communication between IEC61850 server and DNP3 relay. The control is extended to the protection relays integrated in the network. Secured control is executed only if the specified condition has been met. The concept of secured control is to ensure that there is no false control that can be executed in power plant equipment through control devices.

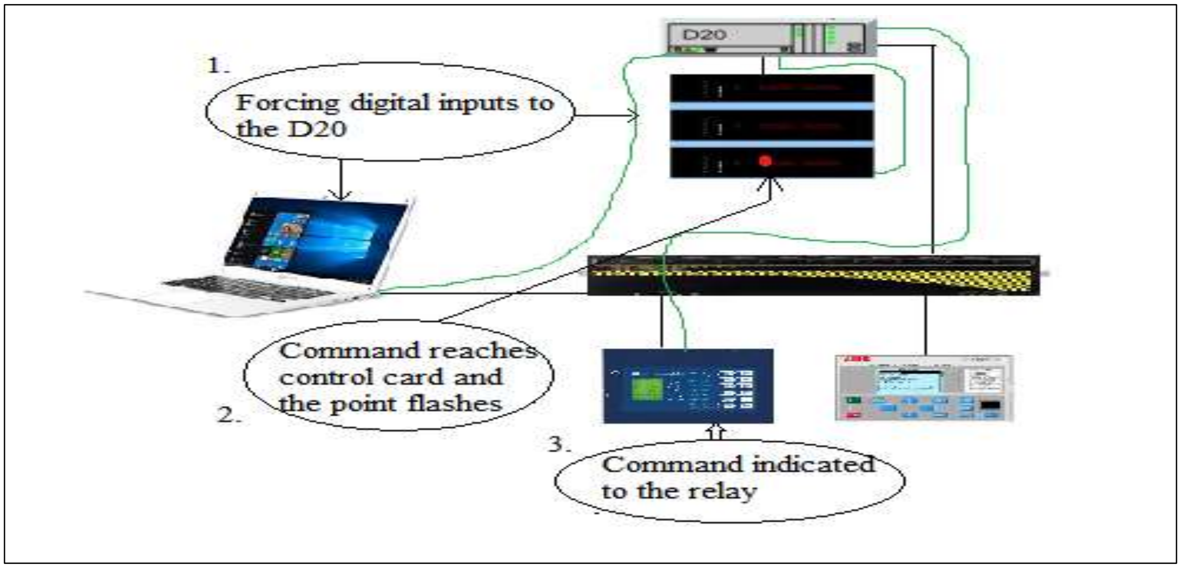


Figure 4.14: Architecture of testing controls locally

Figure 4.14 shows that the connection between D20 and testing laptop is via substation network where telnet is used to establish the communication. For simplicity, this test is extended to the protection relay to ensure that there is a communication between IEC61850 server and DNP3 relays. Before the test was carried out, the data traffic was generated in the network. Despite the traffic being the generated; the results of the test proved the following;

- Control does not joint the data network traffic queue; it always jumps to the front since it is a high priority command.
- Even though there is traffic in the network control must be executed since it is a command to safeguard substation machinery and operating personnel.
- DNP3 Ethernet uses data priority tagging

4.4 Device Visibility

This section provides the analysis of device visibility adhering to the analysis of figure 4.8 and 4.9. The analysis carried out in section 4.3.2 has been expanded to the device level. Figure 4.15 represent the device visibility of DNP3 devices integrated in different paradigm.

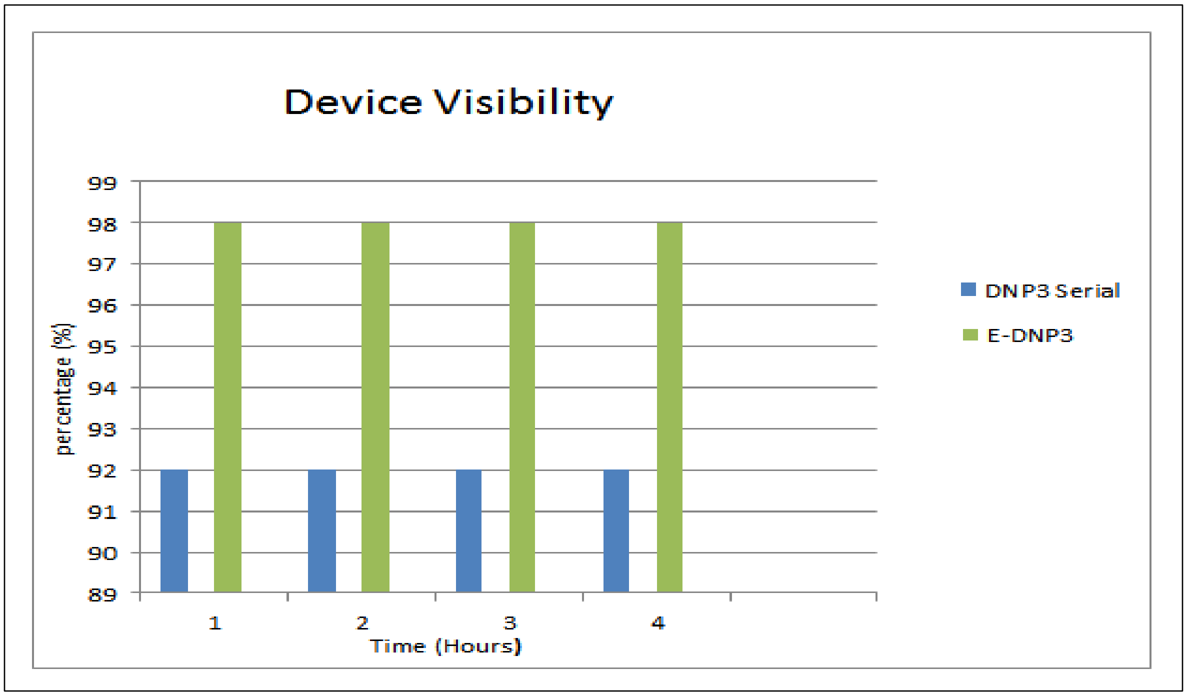


Figure 4.15: DNP3 device visibility.

Figure 4.15 above shows the comparison of protection relays visibility for both DNP3 serial and DNP3 LAN to the substation gateway or telemetry unit. The visibility of serial communication can be improved through hardware and software alteration depending on the convolution of the network architecture and these changes can increase the network strain. The following equation is used to estimate the visibility of devices when numerous devices are integrated in the network. Visibility is an ability of local or remote control centre to view and control the power system network through the picture that is reflected by the integrated devices. There are numerous factors that may contribute to the poor visibility of devices such as: communication medium, data collusion and improper configuration of telemetry unit. In the current practice, the telemetry unit will wait for pre-determined time to fail the relays and then recover it immediately if the bad or no response was received after issuing a command. The utilization of Ethernet has addressed the concern over data collusion. Other changes that were introduced were to change Data Collection Application (DCA) settings from “offline after fail” to “offline after channel fail” that means the DCA will retry on application level before its fails the devices.

4.5 Protection relays to GE D20 data monitoring

The Fieldcom tool is used to monitor the DNP3 data between substation relays and telemetry unit. Fieldcom uses two addresses as where the data come from and where is transmitted to. The data is represented in hexadecimal format.

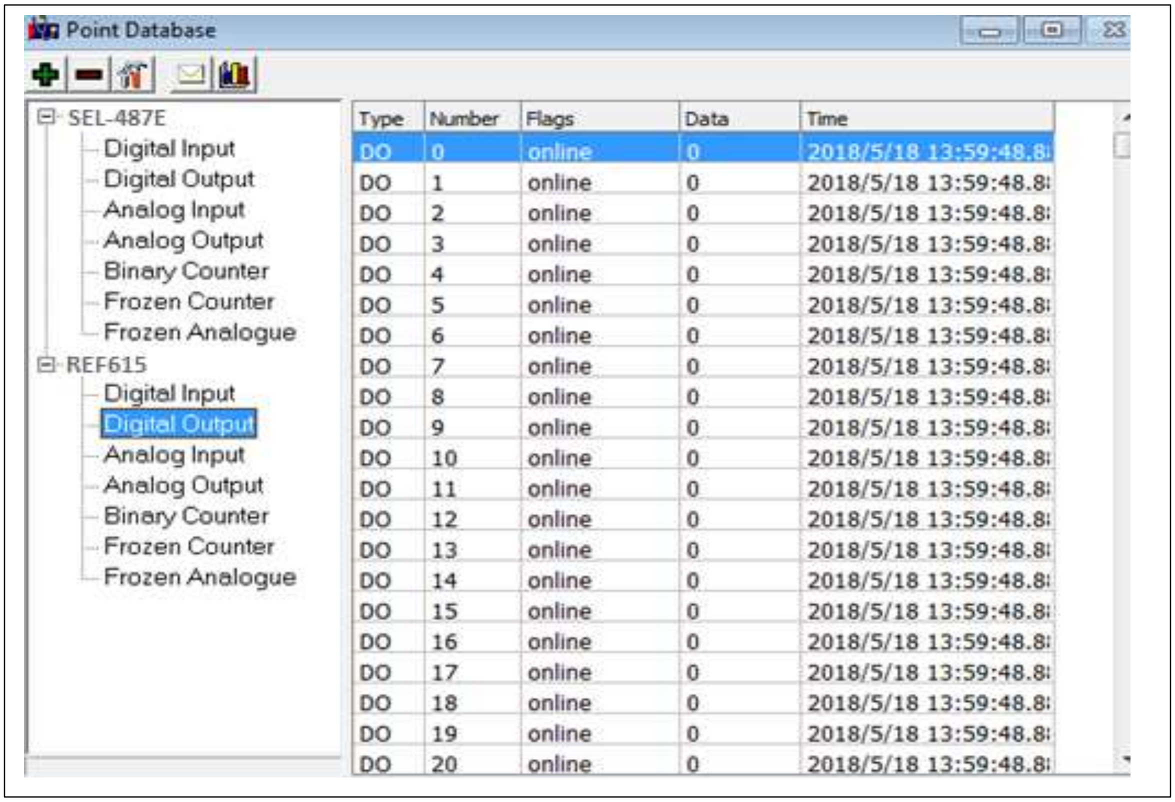


Figure 4.16: DNP3 data monitoring using Fieldcom

Figure 4.16 shows the flags of Digital Outputs (DO) for both protection relays integrated in the network. From figure 4.12 it can be seen that, the all points are online validating that relay points are matching the points configured on telemetry unit.

4.6 IEC61850 client modelling

For the purpose of testing IEC61850 data points GE D400 is added to the network [56]. Only GE D400 uses IEC61850 default settings. D400 is used as IEC61850 client to the D20 that is configured as IEC61850 server. Client application used to collect data from server and write it to the real time system database. Figure 4.17 show the modelling of IEC61850 D400 channel that is used to collect data from D20.

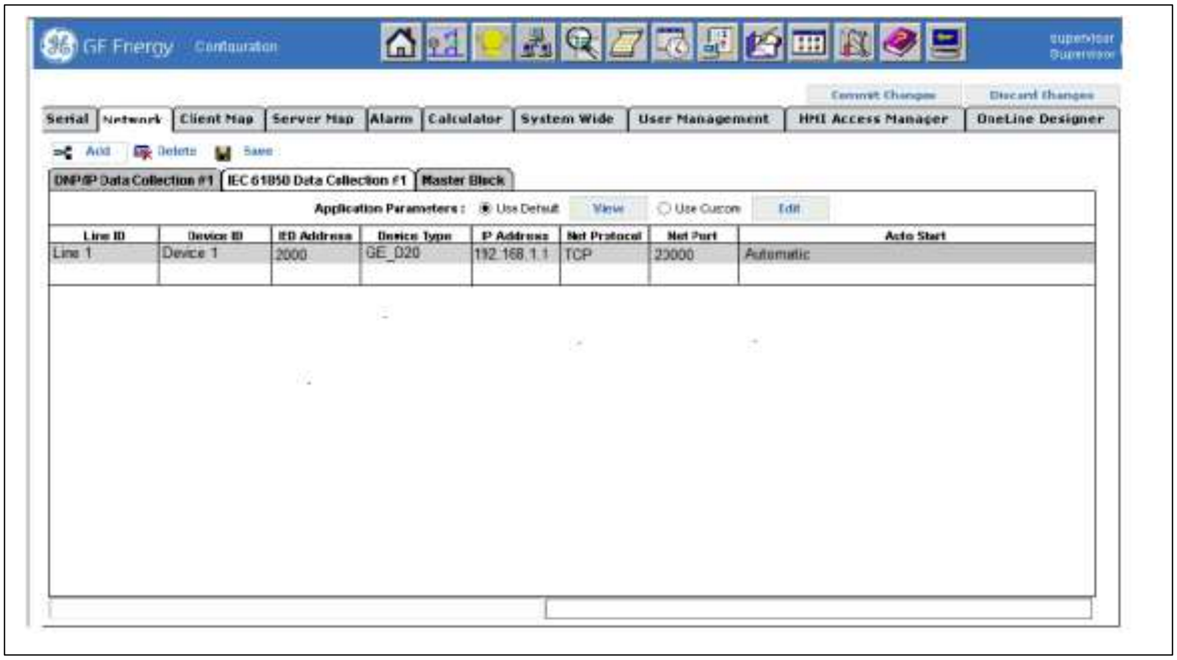


Figure 4.17: Modelling of IEC61850 server (GE D400)

Figure 4.17 above show the modelling of the data collection application for the IEC61850 client. This is a communication link that is used to collect data from IEC61850 server. The modelling of IEC61850 client needed the internet browser.

4.7 Monitoring IEC61850 data

Figure 4.18 illustrate the utilization of wireshark protocol analyser to capture the information in substation LAN. Wireshark is an open and free data analyser used for investigation and data capturing in the network [56]. There are numerous commands and messages that were captured in the network as shown in figure 4.18 and 4.19.

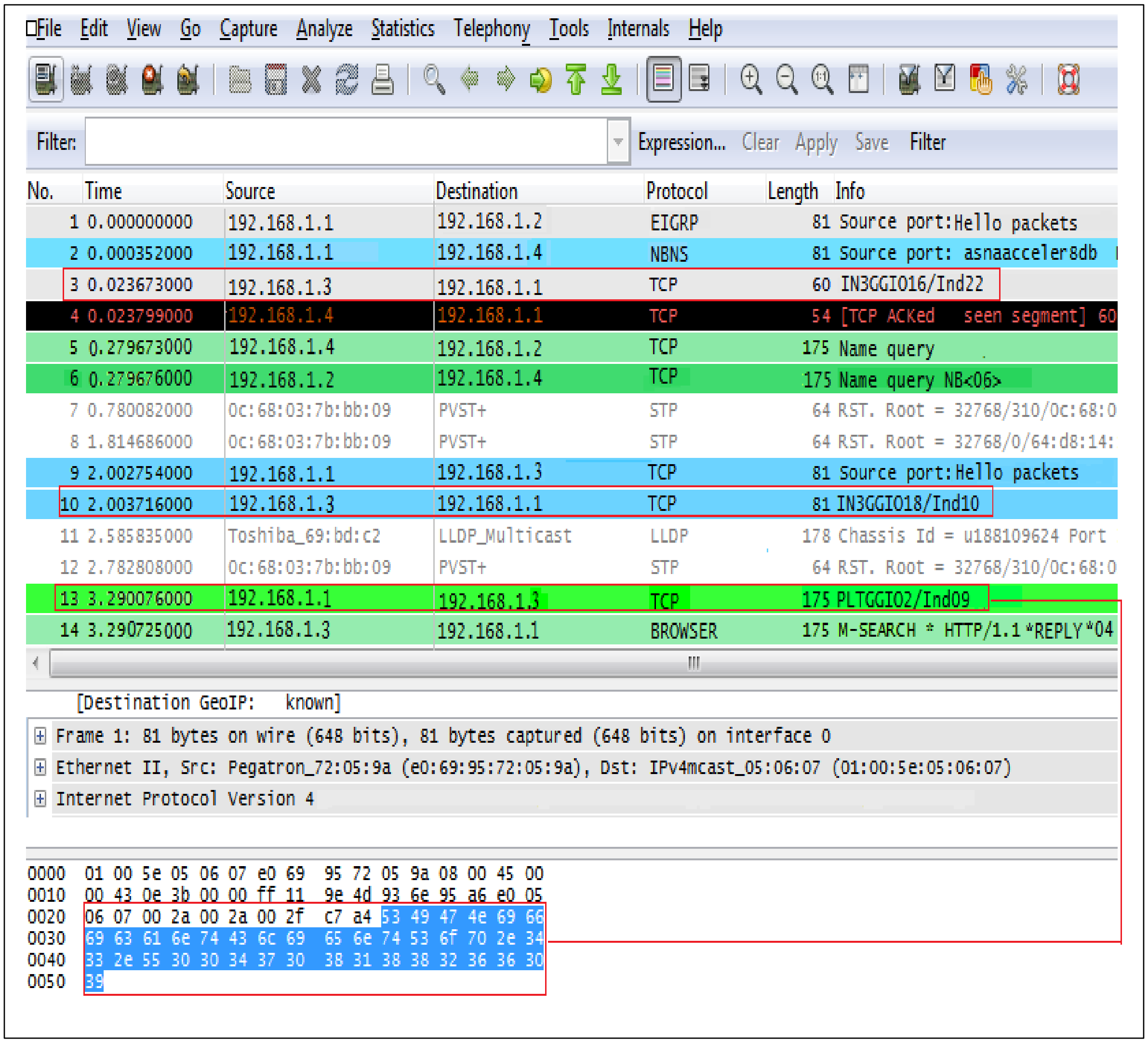
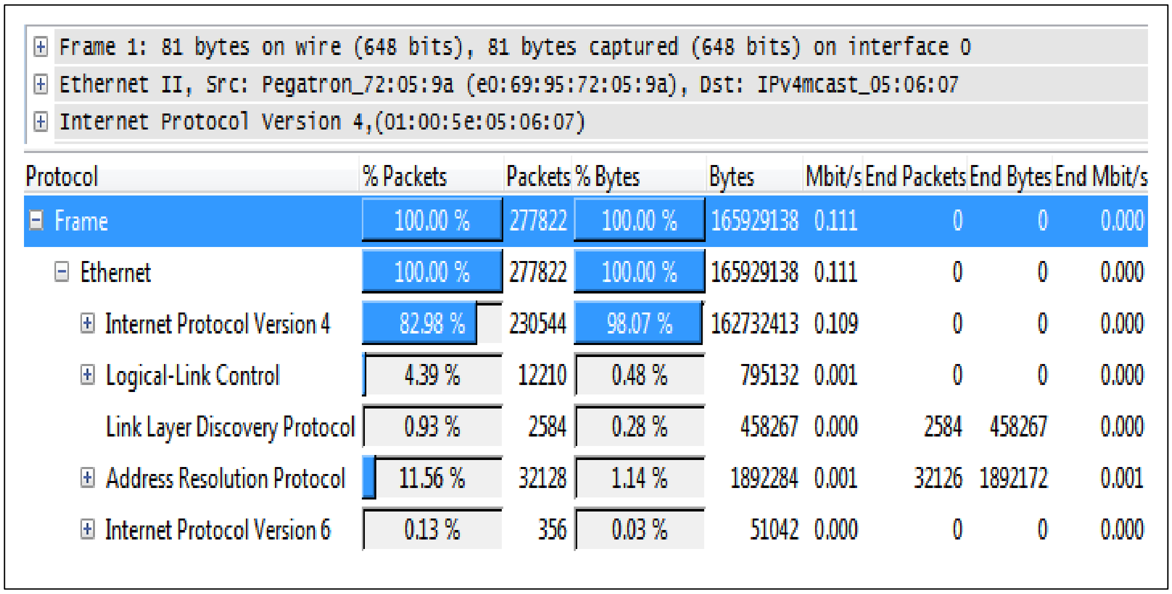


Figure 4.18: Various data packets captured in the substation network using wireshark.

The data represented in figure 4.18 are in hexadecimal format with some IEC61850 commands and alarms marked. The wireshark was not only capturing the data related to IEC61850 and substation automation, instead it's captured even the backstage messages of the IEDs. Figure 4.18 provided the summary of DNP data decoded in IEC61850 to provide the answer to the research question stated in chapter one.



⊞ Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
⊞ Ethernet II, Src: Pegatron_72:05:9a (e0:69:95:72:05:9a), Dst: IPv4mcast_05:06:07
⊞ Internet Protocol Version 4,(01:00:5e:05:06:07)

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100.00 %	277822	100.00 %	165929138	0.111	0	0	0.000
⊟ Ethernet	100.00 %	277822	100.00 %	165929138	0.111	0	0	0.000
⊞ Internet Protocol Version 4	82.98 %	230544	98.07 %	162732413	0.109	0	0	0.000
⊞ Logical-Link Control	4.39 %	12210	0.48 %	795132	0.001	0	0	0.000
Link Layer Discovery Protocol	0.93 %	2584	0.28 %	458267	0.000	2584	458267	0.000
⊞ Address Resolution Protocol	11.56 %	32128	1.14 %	1892284	0.001	32126	1892172	0.001
⊞ Internet Protocol Version 6	0.13 %	356	0.03 %	51042	0.000	0	0	0.000

Figure 4.19: Analysis and scanning of data packets in the substation network

Figure 4.18 and 4.19 illustrates the analysis of IEC61850 data packets over the substation network. It gives the comprehension analysis of the real-time and background traffic. Figure 4.19 shows that, the application of the IEC61850 and DNP3 has been refined to a form that contains data gathering and broadcasting services. The data attributes extracted to a string to simply data model and discard the functional constrains. In order to reduce the complexity of maintaining and analysing the internal data image, the database system have been configured to provide the flexible data tables. The IEC61850 messages captured using Wireshark are represented in two forms: request (from IEC61850 client) and response (from IEC61850 server).

4.8 DNP3 and IEC61850 hexadecimal data interpretation

DNP3 and IEC61850 messages captured using IEC61850 server terminal emulator; Fieldcom software and wireshark are represented in hexadecimal format. Hexadecimal format have the first and second most important bytes as shown in (appendix A-10) and figure 4.18. The first byte of the tag is called identifier octet that uses the following composition: (data class tag), (originality or primitive flag) and the (the number of tags). The second byte is used to explain the length of the encapsulated data followed by data content that can be data integer, data boolen, time stamp and visible string. Supervisory isolated (PLTGGIO2/Ind09) in figure 4.18 have tag header of 53 and data content tag of 49. Tag 53 (binary of 1010011) represent the data class application, data type composition and fieldname. The byte of the header is not necessary consider for this analysis. Tag 49 (binary of 1001001) represent the content of supervisory message with 73 bytes (Decimal).

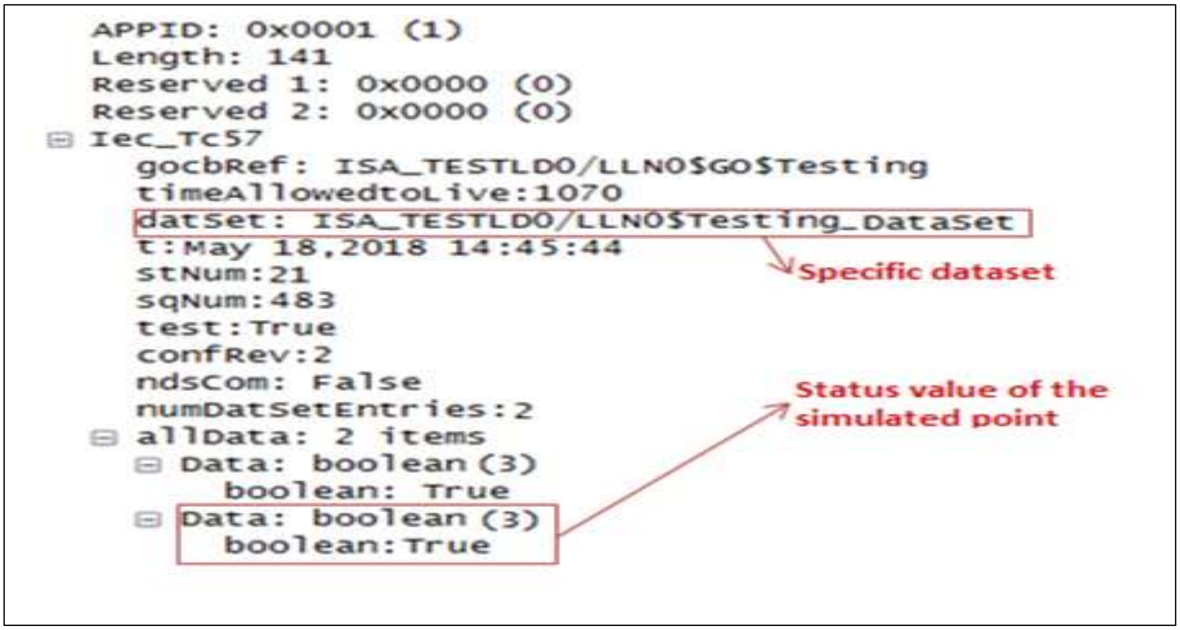


Figure 4.20: Boolean values for the simulated point between IEC61850 server & client

Figure 4.20 above show the detailed analysis of status points and dataset that were created in IEC61850 server application to enable the integration of DNP3 into IEC61850. It was observed that, the gateway is able to provide all information compulsory to represent IEC61850 data that are not available with DNP3 services. Gateway has the capabilities to emulate the optional information. From figure 4.20 it is shown that, logical node zero for both IEC61850 server and client are interconnected to monitor the physical device status that brings the self-monitoring to the devices. Logical node zero contains the information with regard to the logical device. Figure 4.21 represent the sequence of event captured in D400 terminal server, whereas figure 4.22 represents the event trap list of D20.

4.9 GE D20 and D400 historical data

Report Results - Windows Internet Explorer

Alarm Name	Alarm Date/Time	Reset Date/Time
D20_61850/T52AXCBR2	18-May-18 14:30:40	18-May-18 14:31:26
D20_61850/IN3GGIO16/Ind23.stVal[ST]	18-May-18 14:30:40	18-May-18 14:31:26
D20_61850/T52AXCBR1	18-May-18 14:31:25	18-May-18 14:32:22
D20_61850/IN3GGIO16/Ind22.stVal[ST]	18-May-18 14:31:25	18-May-18 14:32:22
D20_61850/PLTGGIO15/Ind09.stVal[ST]	18-May-18 14:32:30	18-May-16 14:34:40
D20_61850/PSVGGIO1/Ind29.stVal[ST]	18-May-18 14:34:46	18-May-18 14:35:20
D20_61850/PSVGGIO1/Ind02.stVal[ST]	18-May-18 14:40:22	18-May-18 14:40:28
D20_61850/IN2GGIO15/Ind24.stVal.[ST]	18-May-18 14:43:21	18-May-18 14:45:10
D20_61850/IN2GGIO15/Ind05.stVal[ST]	18-May-18 14:45:21	18-May-18 14:45:28
D20_61850/IN3GGIO16/Ind23.stVal[ST]	18-May-18 14:46:01	18-May-18 14:46:14
D20_61850/PSVGGIO1/Ind20.stVal.[ST]	18-May-18 14:48:05	18-May-18 14:48:30

Figure 4.21: Historical data of IEC61850 client

The control function of DNP3 devices was cross linked to the IEC61850 control data classes called single point status of a controllable object and double-point control.

N / A NODE:0 SYNC:NONE SOE Buffer Display 18-May-18 14:52:37

SOE#	PNT#	YY/MM/DD	HH:MM:SS:msc	STATE	DESCRIPTION	
26	10	18/05/18	14:30:40:182	ON	Trfr	11 kV MV Brkr Close
27	28	18/05/18	14:30:40:207	ON	Trfr	MV CB Not Healthy
28	28	18/05/18	14:30:47:323	OFF	Trfr	MV CB Not Healthy
29	10	18/05/18	14:31:25:782	OFF	Trfr	88kV HV Brkr Close
30	9	18/05/18	14:31:25:795	ON	Trfr	HV CB Not Healthy
31	8	18/05/18	14:31:32:741	OFF	Trfr	11 kV MV Brkr Close
32	7	18/05/18	14:31:32:754	ON	Trfr	11 kV MV Brkr Open
33	23	18/05/18	14:32:08:854	OFF	Trfr	Supervisory Switch Iso
34	29	18/05/18	14:32:46:034	ON	Trfr	Protection Not Health
35	29	18/05/18	14:32:47:034	OFF	Trfr	Protection Not Health
36	29	18/05/18	14:32:51:033	ON	Trfr	Protection Not Health
37	29	18/05/18	14:32:52:034	OFF	Trfr	Protection Not Health
38	7	18/05/18	14:34:06:388	OFF	Trfr	11 kV MV Brkr Open
39	8	18/05/18	14:34:06:406	ON	Trfr	11 kV MV Brkr Close
40	27	18/05/18	14:34:06:417	ON	Trfr	HV CB Not Healthy
41	29	18/05/18	14:34:10:087	ON	Trfr	Protection Not Health
42	29	18/05/18	14:34:11:859	OFF	Trfr	Protection Not Health
43	27	18/05/18	14:34:18:559	OFF	Trfr	HV CB Not Healthy
44	9	18/05/18	14:34:36:999	OFF	Trfr	11kV MV Brkr Open

Logout Redraw Open_window Beginning End Top_menu Goto_point Next
Previous del_All del_to_cUrsor reFresh
Use cursor keys to select a point and to scroll the display

Figure 4.22: Historical data of IEC61850 server

Figure 4.21 and 4.22 shows the historical data of the event that had occurred. Most of the event browsed from IEC61850 client corresponds to the event captured in IEC61850 server (DNP3 RTU) terminal emulator. Following is an example of winding temperature trip alarm (D20_61850/IN2GGIO15/Ind20) captured in the IEC61850 client; that specifies the IEC61850 server device (D20) and data collection protocol. The DNP3 and IEC61850 data is separated by process image. In this architecture the controls are considered as pass through services. Figure 4.23 shows the IEC61850 data availability between D20 and D400.

RTU Type	Available	Failed	Disabled	Other	Total %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	99.51 %	0.49 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %
D20	100 %	0 %	0.00 %	0 %	100 %

Figure 4.23: Telemetry system monitoring server

Figure 4.23 show the readings of the external monitoring system that monitors the communication, and data availability between D20 and D400. This data was used to plot the graph represented in figure 4.24:D20_IEC61850 data availability. The data from IEC61850 server is 100% available to the IEC61850 client; that means the objectives of this research has been achieved as figure 2.25 proves that; the integration of DNP3 into IEC61850 was successfully.

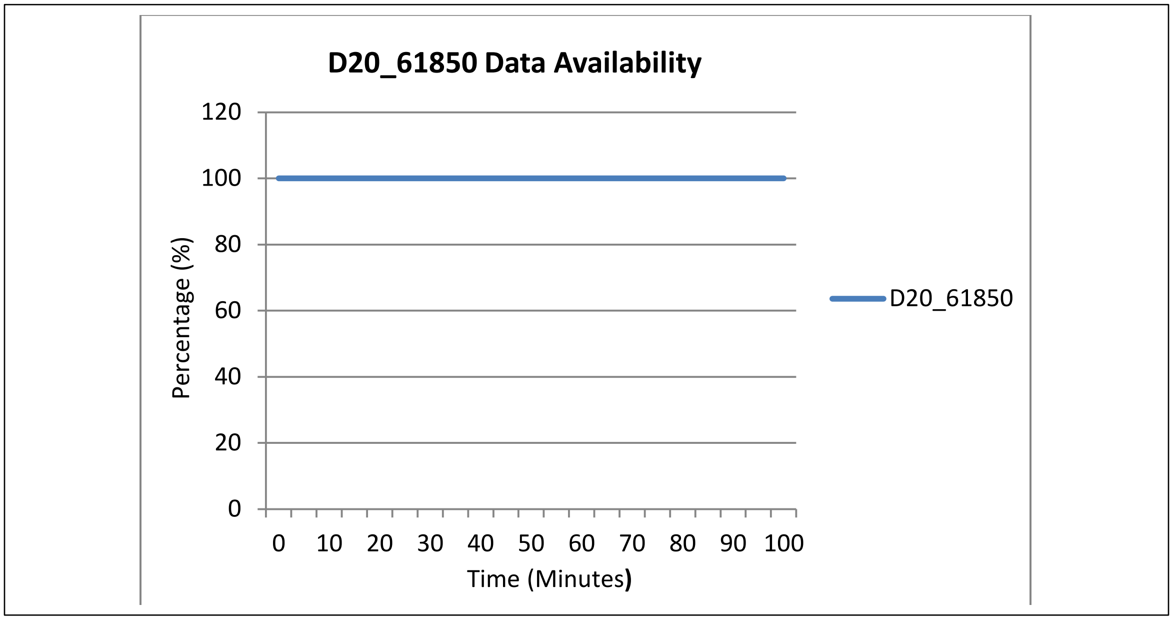


Figure 4.24: Availability of IEC61850 data to IEC61850 client

Figure 4.24 show the availability of IEC61860 data to the IEC61850 client (D400) monitored through IEC61850 data collection application between IEC61850 server and client. The average availability of substation data shown in figure 4.24 proves that even though the integration of DNP3 data into IEC61850 brought some complexity to the network but the device availability and efficiency has improved. There was a slight drop, where the availability was at 99.51%. This drop was deliberately caused to test whether the system will be able pick up small changes.

4.10 Real-time inputs testing

Real-time input testing was conducted to assess the accurateness, and discrimination of the time and priority tagging functions for the system. The results shown in figure 4.21 and 4.22; shows that there is no significant delay of data exchange between IEC61850 server (D20) and IEC61850 client (D400) communicated over IEC61850 Data Collection Application (DCA) link.

4.11 Costs to benefit Investigation

Improving the efficiency of substation devices also improves the utility revenues. Online and advanced monitoring of substation equipment are the most recognized benefits of this work with the purpose of avoiding catastrophic failures in the power system network. The financial benefits accomplished in this research translate to both reduced commissioning and maintenance cost. Advanced monitoring and control of the power system network help the utility to reduce the amount of energy lost and extend power system equipment lifecycle. Furthermore DNP3 is a dominantly used SCADA protocol in transmission and distribution substations in the world, however it lack some of the features required for advanced substation automation systems. The infrastructures of legacy substation automation still hold huge investment that can never be replaced. It is not economical to completely replace the legacy devices currently in service, but rather incorporate DNP3 into IEC61850 systems. The complete replacement will not only have high cost implication but will also interrupt the existing applications and further interrupt the supply that will badly decrease the utility revenues. The integration of DNP3 into IEC61850 will create new control and monitoring capabilities in both transmission and distribution substations.

4.12 Reliability Analysis

The reliability of the substation automation systems is a prime requirement to ensure that, the system will continuously provide the real – time operational and non-operational data to the network operator. The reliability of the system presented in this research is derived from speed performance, data and device availability. This is defined as the trustworthiness of the integrated devices to perform its functions as per configuration uploaded to them. The recent application has adopted the use of Ethernet communication is substation that bring a high degree of flexibility and reliability in terms of its operations. The results obtained from the analysis of data, and device availability and interoperability has proved that, this work offered a high degree of flexibility and reliability. Over serial communication flexibility is compromised by bulky wiring needed to transfer signals between devices, whereas the reliability is compromised when the installation of devices to recover the signal is required.

4.13 Conclusion

The data availability to the authorized user or network operator is a key requirement of substation automation. The advantages of Ethernet communications over serial communications were demonstrated, since the communication between substation devices was achieved through DNP3 Ethernet TCP/IP connection. DNP3 Ethernet TCP/IP communication offered high speed peer to peer communication and the secured data exchange between substation devices. DNP3 TCP/IP is used to encapsulate the data packets to improve security. This chapter concluded by simulating the integration of DNP3 and IEC61850 data, and used Wireshark protocol analyser to monitor IEC61805 data. The results provided in this chapter with regard to the DNP3 and IEC61850 data integration will enable the utilities to operate their existing substations equipment in a reliable and economical mode.DNP3 data is represented in an evocative manner, not just the list of event that had occurred.

Chapter Five

Conclusion and future work

This chapter provides the summary and conclusion of this research work through research deliverables, literature review, results applications, and challenges encountered to achieve the results discussed in chapter four. This chapter further discusses future work to extend this work.

5.1 Introduction

Currently more focus is given to the substation automation designs due to the restructuring that forces the utilities to generate, transmit and distribute reliable and efficient supply to the end user either Large Power User (LPU) or Small Power Users (SPU). Power supply reliability is very crucial since its play a huge role in economic development across the world. Utilities uses electricity to collect it revenues and pay the workforce, hence it must be stable and reliable. Although there are too many protocols and devices for substation automation, the utilities have key the requirements to consider when designing a substation automation network just before is deployed for implementation those are; commissioning costs, operating costs, maintenance costs, interoperability, interchangeability and overall performance of the whole network. Well-designed substation automation will enable the utilities to protect, control and operate power system through dedicated communication channel. It is not feasible to achieve any automation function if communication is failing. This enables the utilities to monitor, control, and operate distribution components in a real-time or non-real-time mode from remote locations. It is the mere fact that not all substations are well automated especially in South Africa due to financial constrains that has led to the investigations of cost effective method of developing advanced substation automation utilizing legacy devices. The tests and simulations that were conducted proved that there are many operational similarities between DNP3 and IEC61850 that will help the utilities to adopt the new standard without a complete replacement of legacy devices. The integration of DNP3 and IEC61850 ensured that, the protocols and standard were developed independently are brought together for one purpose “advanced substation automation” to meet the demanding requirement of smart grid. Smart grid uses the digitized platform for any form of communication. Most of the substation data that is used to monitor and control power system comes from integrated devices ranging from protection relay to remote terminal unit. The availability of data depends upon the communication medium used for devices to exchange the data. Substation devices contain the collective and similar set of functionalities.

The integration of DNP3 into IEC61850 improved the visibility of devices and availability of data to the network operators and it is expected to reduce the overall operating costs. This integration further extend to ease the management of the data linked to monitoring, control, protection, communication and general configurations files. These various functions are incorporated to advance the power system network resilience and capabilities. The fact is IEC61850 is here to stay for long and there is a continuous support of DNP3 software facilitated by DNP3 user group. That means these standards must be used concurrently where there is a need. Therefore the approach of this study will allow the utilities to improve revenues through legacy devices while also provide the necessary training to the workforce.

5.2 Research deliverables

This study have demonstrated that the current technical concerns over the adoption of IEC61850 for substation automation applications can be resolved through an innovative approach of presenting the selected DNP3 data into IEC61850 server and combine its functionalities. The study reveal that some of the IEC61850 functions that are not applicable with DNP3, however IEC61850 application server can add those function to DNP3 data if they are compulsory. The issue with the adoption of IEC61850 is not only technical. Some utilities are facing financial constrains that; they cannot afford a complete replacement of the substation devices. DNP3 devices can never be changed into IEC61850 devices, only the data from DNP3 devices can be changed. The last issue is the lack of skilful workforce. The integration of DNP3 into IEC61850 a brought the solution to this issues collectively. The simulations results proved that DNP3 and IEC61850 can be brought together to build up advanced substation automation. The utilization of DNP3 Ethernet improved the device visibility to the local control and improves data availability. These features help with the prediction of major maintenances and network expansion. The thesis deliverables can be loosely grouped as following:

5.3 Literature review

For better understanding of methodologies and approach being used in substation automation, numerous papers were reviewed and analysed. The literature review described the concept of substation automation. The literature review further examined the chronological review of communication protocols and standard; Modbus, DNP3, UCA and IEC61850. Literature review explained the concept of Ethernet communication in substation automation. DNP3 has emerged as the most predominant protocol globally for SCADA applications originated from electrical power utility from North America. DNP3 have proven high degree of interoperability between devices in a multivendor environment. DNP3 is not just a protocol, it a standard that continue to progress through its universal user group that meets with vendors to improve the interoperability and technical proficiencies. DNP3 can leverage the flow of data locally and remotely, that why is still used in many applications. The global adoption and attraction of the DNP3 is influenced by the methodology it uses for device integration and its continuous growth. DNP3 offer features that are also applicable in IEC61850 such as; high data integrity (no miscalculated and corrupted data that will be communicated), high accuracy of real time data, high level of recording, high level of remembering, no loss of data even if when something goes wrong in the channel and object based definition of data. Every device that is using DNP3 presents the data in the same way. These features strongly influence the utilities to retain their DNP3 devices in substation environment even though there is a new standard that has been published. Literature review provided the insight of the three levels of communication that are used in IEC61850 standard. Those levels are; station, bay and process level. The object model is used to describe description of data accessible from primary equipment and automation devices. The ACSI is used to link the IEC61850 to the relevant protocol that the standard is capable to co-operate with.

5.4 Results Application

The reluctance of the utilities to adopt IEC61850 due to financial issues, lack of knowledge and unresolved issues pertaining to the standard has necessitated the need to investigate the alternatives of implementing the standard in traditional substations, where it is costly to replace the entire communication network. The obtained results can be used in electrical industries, gas and oil applications. The result will also enable the researchers to look at the options of advancing DNP3 substation. The results will be used to demonstrate the capabilities of DNP3 and IEC61850 for student studying toward substation automation field. The work presented in this research is the integration of substation data from legacy protection devices into IEC61850 server using IEC61850 application embedded in DNP3 configuring software. These results could be applied in:

a) DNP3 substation that are currently non- compliant to IEC61850
b) IEC61850 substation currently communicating to DNP3 control centre
c) DNP3 substation interconnected to IEC61850 substation
d) Hybrid substations communicating using both DNP3 and IEC61850

The following benefits were obtained from the study:

a) Lower commissioning cost
b) Lower IEC61850 implementing cost
c) Improved the performance of existing devices
d) Improve the availability of data and visibility of devices
e) High speed peer to peer communications between devices
f) Strongly defined data types including binary, integer, floating point, accumulators, controls, strings, point quality information
g) Configuration file download and upload competencies
h) Confederacy of logged data and event using data models
i) Definition of device profile for device operation
j) Advanced direct data modelling using data set segregation

5.5 Challenges

There are numerous technical challenges that have been encountered during the course of this research project making it more challenging to achieve the stipulated objectives. However the objectives of the research were obtained through hard work and dedication. These challenges include:

a) IEC61850 is explained using lots of tables and diagrams that are difficult to understand.
b) The real functionalities of the both DNP3 and IEC61850 are not corresponding to what is in the markets. Some of the features explained in both standards are not practical tested.
c) Very little comprehensive knowledge available for public and academic use dealing with integration of DNP3 devices into IEC61850 data model. Most of valuable information resides with automation device manufactures and relevant service providers.
d) There are too many ambiguities that have been not defined in IEC61850 standard.
e) The application of DNP3 and IEC61850 require the advanced knowledge in various field such as; data network management, data interpreting and data modelling through software applications embedded to the system.

The encounters mentioned above indicate that this work required a dedication and hard work to achieve the objectives, since it involve the incorporation of two protocols that were developed independently from each other. This research was developed from comprehensive analysis of DNP3 and IEC61850 standards to investigate the similarities between these protocols. The findings clearly indicated that this methodology of adopting the standard to the existing substation is economical. The results provided the utilities with the opportunities to consider the alternatives of adopting the IEC61850 to improve the efficiency and stability of the grid. The methodically investigation of DNP3 and IEC61850 capabilities provided the solid solutions to the challenges that were experienced.

5.6 Future work

Significant achievements have been obtained through this research, with regard to the integration of DNP3 data points into IEC61850 data model. However there are still several ambiguous areas in IEC61850 standard that need more investigation and proper procedure of testing. Although DNP3 is considered as a matured protocol, some issues with regard to interoperability need to be investigated in the future improve the incorporation of these standards. Further investigation is required to improve the synchronisation between power plant switchgears and digital sources that communicate the measured sampled value over substation LAN. While smart grid platform offers wide range of advantages to stabilise power system network and improve the efficiency of the network, but it also provide the access to third party that can hack the system. The damage can be catastrophic since the system is centralised, hence there is an urgent need for further investigations that will address security of substation automation taking care of currently used protocols DNP3 and IEC61850. The future substations are expected to provide the warning alarm to authorized network operators via mobile devices. This will be achieved through series of investigation with regard to IEC61850.The future work can be further summarized as following;

a) Investigate the application of IEC61850 standard in distribution lines auto-recloser.
b) Investigate the application of IEC61850 standard in SCADA application, since it is currently used for communication within substation.
c) Advances the concept of Select-Before-Operate in DNP3 standard.
d) Investigate the reliability and stability of GOOSE protection messages in case substation network fails.
e) Further investigate the re-transmission of GOOSE message in case signal is lost in transit.

References

[1] A. Oy, "ABB review special report: IEC 61850," *The corporate technical journal [cited 3.3. 2011],* 2010.

[2] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," *IEE/PES Power Systems Conference and Exposition, PSCE'09,*March,2009, Seattle, pp. 1-9.

[3] I. E. Davidson, D. McKenzie, and G. Madonsela, "Integration and automation in the electrical telecontrol industry-prospects and problems," *ELEKTRON JOURNAL-SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS,* vol. 18, no. 1, 2001, pp. 11-13.

[4] E. Chikuni, "Power System and Substation Automation," *in Automation*: In Tech, 2012.

[5] M. Shen, F. Chan, R. Laprise, and L. Lu, "A fully integrated substation LAN network for protection, control and data acquisition," *IEEE Power & Energy Society General Meeting, PES'09*, July, 2009, Calgary, pp.1-6.

[6] . McDonald, "Substation Automation Basics-The Next Generation," *Electric Energy T&D Magazine,* 2007.

[7] W. R. Blum, "Distributed supervisory control and data acquisition system," ed: Google Patents, 1995.

[8] F. Li, W. Qiao, H. Sun, H. Wane, J. Wang, Y. Xia, Z. Xu and P. Zhang,, "Smart transmission grid: Vision and framework," *IEEE transactions on Smart Grid*, vol. 1, no. 2, 2010, pp. 168-177.

[9] C. Moreira, A. G. Madureira, and J. P. Lopes, "Defining control strategies for microgrids islanded operation," 2006.

[10] D. Shirmohammadi, W. E. Liu, K. C. Lau, and H. W. Hong, "Distribution automation system with real-time analysis tools," *IEEE Computer Applications in Power,* vol. 9, no. 2, 1996, pp. 31-35.

[11] E. Udren, S. Kunsman, and D. Dolezilek, "Significant substation communication standardization developments,"*2nd Annual Western Power Delivery Automation Conference (WPDAC) Proceedings*,2000, pp.1-12.

[12] A. Elgargouri, "Implementation of IEC 61850 in Solar Applications," 2012.

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

[14] A. Swales, "Open modbus/tcp specification," *Schneider Electric,* vol. 29, 1999.

[15] S. Amjadi, "Managing IEC61850 GOOSE Messaging in Multi-vendor Zone Substations," Victoria University, 2016.

[16] K. Curtis , "DNP Users Group, 2005".

[17] T. Mander, F. Nabhani, L. Wang, and R. Cheung, "Data object based security for DNP3 over TCP/IP for increased utility commercial aspects security," *IEEE Power Engineering Society General Meeting,* June,2007*,* Tampa, pp. 1-8.

[18] W.-q. TAO and Y. YANG, "Implementation of DNP3. 0 Protocol in FTU," *Proceedings of Electric Power System and Automation,* China, vol. 4, April 2004, pp.1- 12.

[19] M. Majdalawieh, *Security Framework for DNP3 and SCADA*. VDM Verlag, 2008.

[20] F. G. Julie, "Development of an IEC 61850 standard-based automation system for a distribution power network," Cape Peninsula University of Technology, 2014.

[21] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," *Advances in Computer, Information, and Systems Sciences, and Engineering*: Springer,2007, pp. 227-234.

[22] K. Curtis, "A DNP3 Protocol Primer. A basic technical overview of the protocol, 2005," ed, 2016.

[23] H. Lou and C. A. Davidow, "Last leg utility grid high-speed data communication network having virtual local area network functionality," ed: Google Patents, 2010.

[24] B. T. P. Morais, "Emerging technologies and future trends in substation automation systems for the protection, monitoring and control of electrical substations," 2013.

[25] T. S. Sidhu, M. G. Kanabar, and P. P. Parikh, "Implementation issues with IEC 61850 based substation automation systems," *15th National Power Systems Conference,* December, 2008, Bombay, pp. 473-478.

[26] G. Antonova, L. Frisk, and J.-C. Tournier, "Communication redundancy for substation automation," *6th Annual Conference for Protective Relay Engineers*, April, 2011,Texas, pp. 344-355.

[27] A. Bakhtar and M. Kooshavar, "Implementation of UCA Based Inter and Intra Substation Communication Architecture." *20th International Power System Conference*, 2005, China,pp.1-9.

[28] J. White, "Implementation of UCA/IEC 61850 for Substation Automation at Grant County Public Utility District," *IEEE/PES Transmission and Distribution Conference and Exhibition,*May, 2006, Texas,pp.1-6.

[29] D. Proudfoot, "UCA and IEC 61850 for dummies," *Siemens Power Transmission & Distribution,* 2002.

[30] J. Zhang and C. A. Gunter, "Iec 61850-communication networks and systems in substations: an overview of computer science," *University of Illinois at Urbana-Champaign,* 2007.

[31] M. Lehtosaari, "Integration testing of protection relays," 2011.

[32] C. Brunner, "IEC 61850 for power system communication," *IEEE/PES Transmission and Distribution Conference and Exposition*, April, 2008, Chicago, pp. 1-6.

[33] IEC TC57, Communication Network and Systems in Substations- Part 5:Communication*Communication Requirements for Functions and Device Model.* , 2003.

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

[35] W. He, C. Tang, X. Zhang, S. Zhu, H. Yuan, and W. Miao, "The design of data structure for IED based on IEC61850," *China International Conference on Electricity Distribution (CICED),*September, 2006,Beijing, pp.1-6.

[36] B. LI, L.-s. MU, J. SU, L.-z. CUI, and Z.-p. LI, "Modeling of IEC61850 SCL Configurator Based on Relational Model Mapping," *Power System Technology,* vol. 10, 2006.

[37] TC57, "IEC 61850: Communication networks and systems for power utility automation," *International Electrotechnical Commission Std,* 2010, vol. 53, p. 54.

[38] TC57, "IEC61850: *Communication Networks and Systems for power utility automation,Part 7.2 Basic communication structure for substation and feeder equipment and Abstract Communication Service Interface (ACSI),* 2003.

[39] R. Hunt and B. Popescu, "SCADA communications for protection engineers," *68th Annual Conference for Protective Relay Engineers,* March/April 2015,Texas, pp. 881-891.

[40] S. Matsuda, Y. Watabe, I. I. Asrizal, S. Katayama, K. Okuno, and K. Kasuga, "Issues overcome in the design and application of IEC 61850-compliant substation automation systems," *International Conference on Advanced Power System Automation and Protection (APAP)*, October, 2011, Beijing, vol. 1, pp. 198-202.

[41] R. Kirkman, "Development in substation automation systems," *3rd International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*, Taiwan, pp. 598-603, April 2008.

[42] O. Kristofersson, L. Cederblad, and M. Adolfsson, "IAIS concept for intelligent substations," *ABB REVIEW,* pp. 4-11,1997.

[43] S. Meliopoulos and A. Bose, "Substation of the future: A feasibility study," *Power System Engineering Research Center Publication,* 2010*,* pp. 10-17.

[44] Y. Jo, K. T. Wan, C. MyeonSonget, L. SeungJae, L. ByeongHo, K. HyusSung and C. ChulHee , "A software engine for HMI of IED based on IEC 61850," *International Conference on Advanced Power System Automation and Protection(APAP),* October, 2011, Beijing, vol. 2, pp. 1312-1316.

[45] L. B. Oliveira, M. Zapella, A. Sarda, and W. Zanatta, "Managed Ethernet switches performance over IEC 61850 networks: applications with high traffic flow," *13th International Conference on Development in Power System Protection 2016 (DPSP),* March, 2016, Edinburgh, pp.1-6.

[46] S. H. Horowitz, "Transmission Line Protection," *by Taylor & Francis Group,* 2006.

[47] B. K. Duncan and B. G. Bailey, "Protection, metering, monitoring, and control of medium-voltage power systems," *IEEE Transactions on Industry Applications,* vol. 40, no. 1,2004, pp. 33-40.

[48] Q. Hong, S. M. Blair, V. M. Catterson, A. Dysko, C. D. Booth, and T. Rahman, "Standardization of power system protection settings using IEC61850 for improved interoperability," *IEEE Power & Energy Society General Meeting (PES)*, July, 2013, Vancouver, pp. 1-5.

[49] P. Zhang, L. Portillo, and M. Kezunovic, "Compatibility and interoperability evaluation for all-digital protection system through automatic application test," *IEEE Power Engineering Society General Meeting*, June, 2006, Canada, p.7.

[50] D. Gutschow and M. O. Kachieng'a, "Making business sense of distribution automation systems: the case of Eskom, South Africa," *IEEE Transactions on Power Systems,* vol. 20, no. 1,2005, pp. 272-278.

[51] Available: RUGGEDCOM. 2100 Rugged Operating System User Guide [Online]. Available: http://inlsystem.se/doc/ManualRSG2100.pdf

[52] Available: SEL. Relay Configuration Tools Manual available at: https://cdn.selinc.com/assets/Literature/Product%20Literature/Data%20Sheets/487E_DS_20120810.pdf?v=20150812-155326

[53] Available: ABB: REF615 Feeder Protection and Control Relay Application Manual[online].Available:https://library.e.abb.com/public/ca0cdd3d79e543e1b5e5227eba428a8d/REF615_appl_756378_ENr.pdf

[54] Available: GE D20 based substation RTU available at. https://ist.co.za/product/d20-based-substation-rtu

[55] *IEEE Standard 1815.1 "Standard for Exchanging Information between networks Implementing IEC 61850 and IEEE Std 1815™ (Distributed Network Protocol - DNP3)"*, 2015.

[56] Available: Multilin D400 Manual - available [Online] at: https://www.gegridsolutions.com/multilin/energy/catalog/d400.htm

APPENDIX A

A-1: High voltage yard substation apparatus

A -1 show the high voltage yard that compromises of power transformer, busbar, transmission lines and dog-box breakers. This picture represents the concept of conventional and non-conventional substations. Power transformer is a normal conventional substation that is coordinated to non-conventional circuit breaker (Dog-box type). No stand-alone CTs and VTs, since all are integrated to the dog-box breaker.

A - 2: Categories of logical nodes

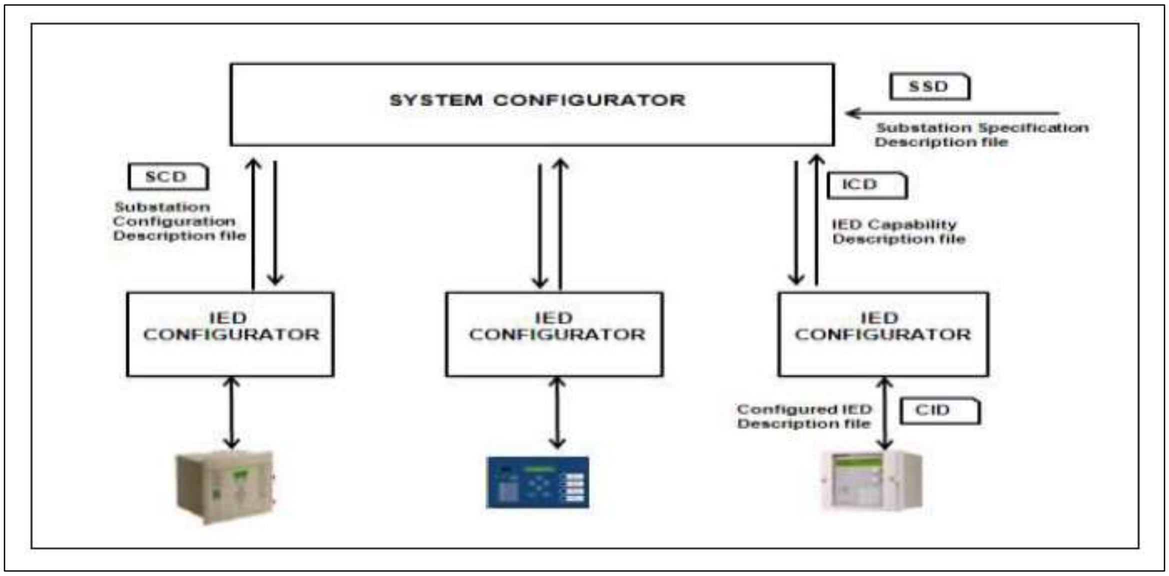
LN Groups	Group Designator	LN Groups	Group Designator
Metering function	M	System LN	L
Switchgear	X	Sensor and monitoring	S
Power system equipment	Z	Protection function	P
Power transformer	Y	Automatic Control	A
Instrument transformer	T	Protection Related	R
Control	C	Generic	G

The standard defines a logical node as the basics of organising data within IEDs. Every specific function within a physical device is defined by a logical node.

A - 3: Substation automation logical node

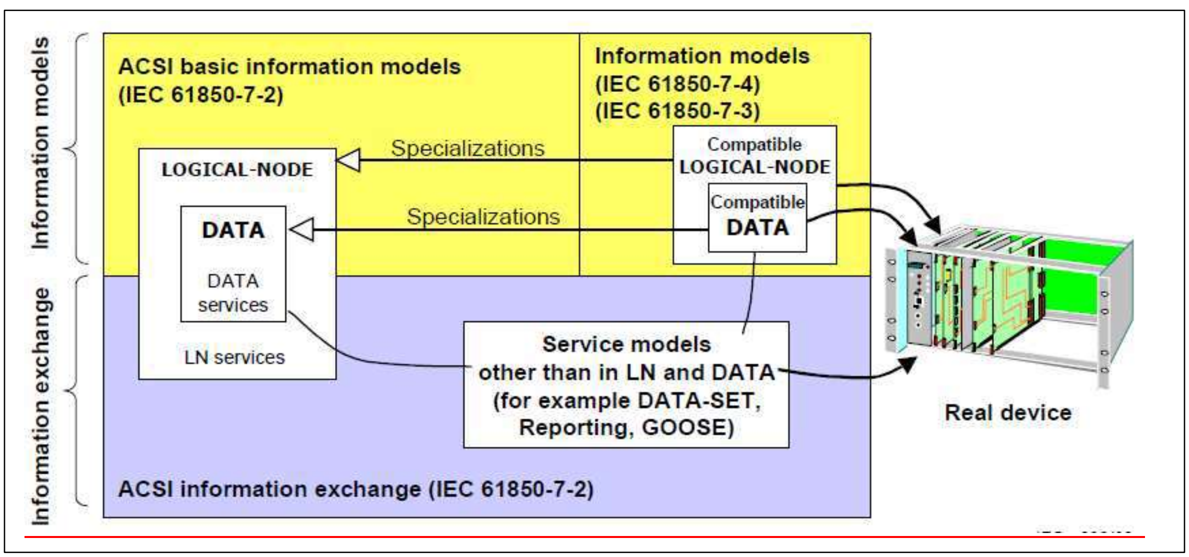
LN Groups	Group Explanation	LN Groups	Group Explanation
XCBR	Circuit breaker	XSWI	Circuit switch
YPTR	Power transformer	MMTR	Metering
MMXU	Measurement unit	RBRF	Breaker fail
PTOC	Time Overcurrent Protection	PDIF	Differential protection
GGIO	Generic logical node	PDIS	Distance protection

A- 4: System configurator



IEC61850 focused in identifying the software tool that can be used to guarantee the interoperability between IEDs. Without XML device profiles it is impossible to achieve interoperability.

B- 5: ACSI information exchange



IEC61850 uses two models to define the relationship of data or information exchange between substation physical devices namely; information exchange and information models. Logical node is used as service that denotes specific functions of substation automation systems other than GOOSE, data set and etc

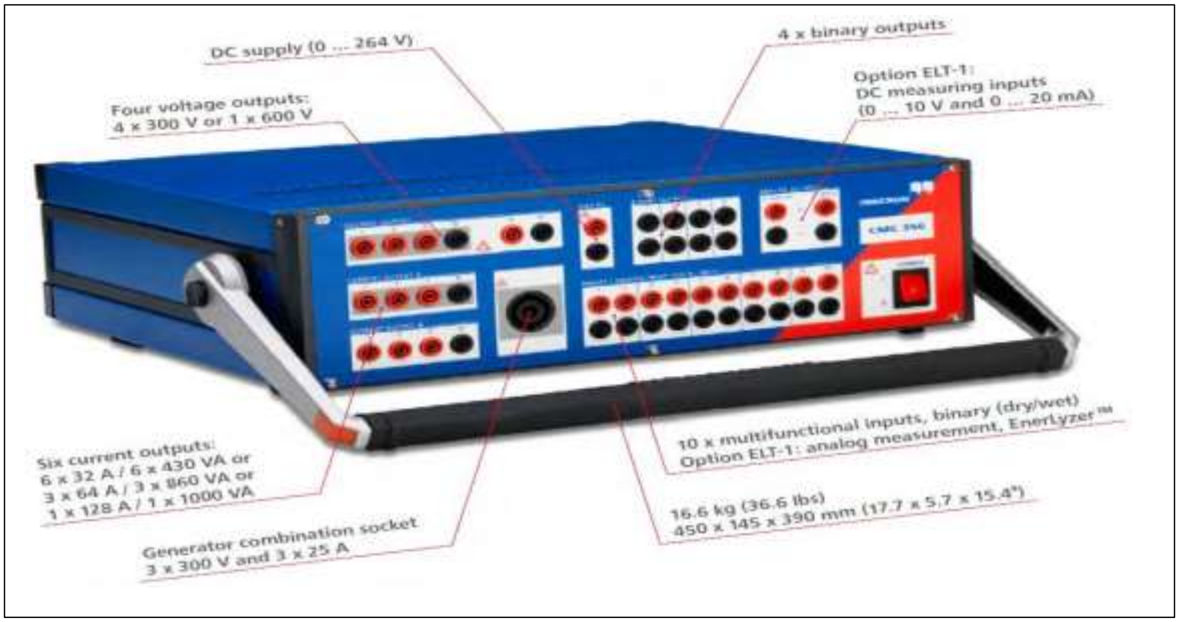
A- 6: Hardwired telemetry unit (D20)

A- 7: Digital inputs points mapped to telemetry unit

Icons Tables

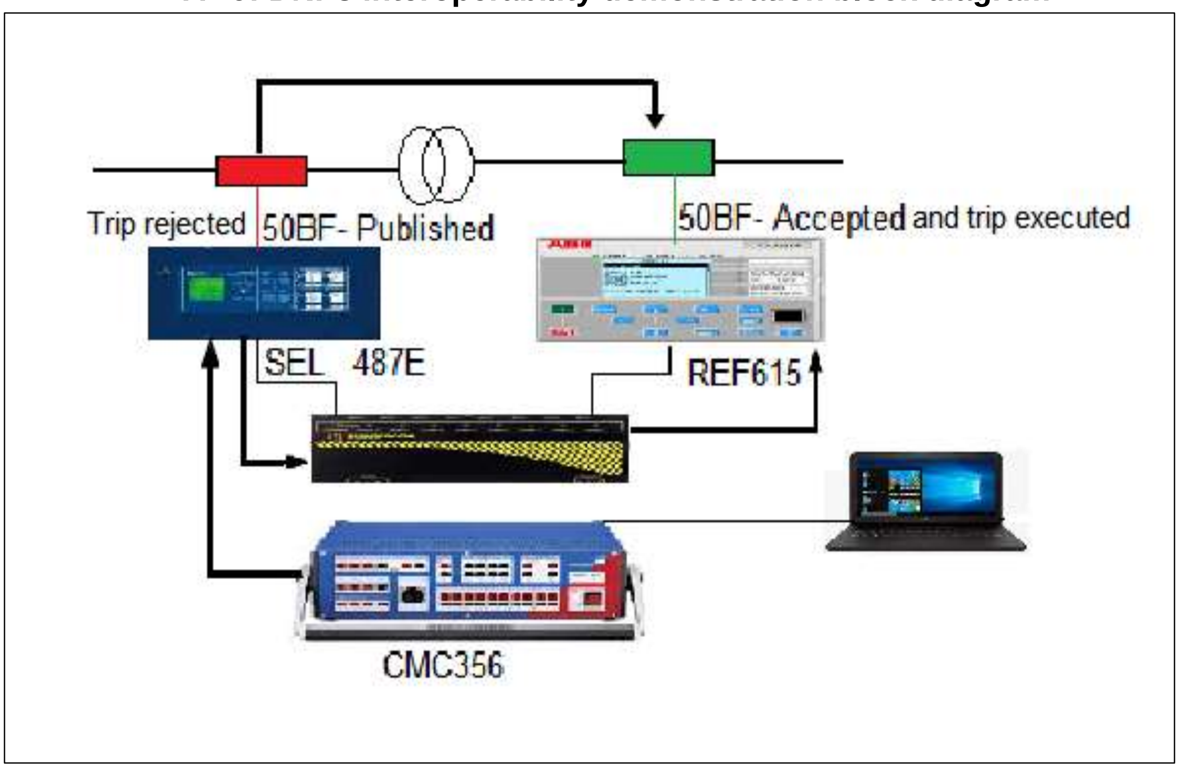
Point	Binary Input Point	Invert Status	COS	SOE	Event Class
2	(000002) Digital Input 002	Disabled	Disabled	Enabled	Class 1
3	(000003) Digital Input 003	Disabled	Disabled	Enabled	Class 1
4	(000004) Digital Input 004	Disabled	Disabled	Enabled	Class 1
5	(000005) Digital Input 005	Disabled	Disabled	Enabled	Class 1
6	(000006) Digital Input 006	Disabled	Disabled	Enabled	Class 1
7	(000007) Digital Input 007	Disabled	Disabled	Enabled	Class 1
8	(000008) Digital Input 008	Disabled	Disabled	Enabled	Class 1
9	(000009) Digital Input 009	Disabled	Disabled	Enabled	Class 1
10	(000010) Digital Input 010	Disabled	Disabled	Enabled	Class 1
11	(000011) Digital Input 011	Disabled	Disabled	Enabled	Class 1
12	(000012) Digital Input 012	Disabled	Disabled	Enabled	Class 1
13	(000013) Digital Input 013	Disabled	Disabled	Enabled	Class 1
14	(000014) Digital Input 014	Disabled	Disabled	Enabled	Class 1
15	(000015) Digital Input 015	Disabled	Disabled	Enabled	Class 1
16	(000016) Digital Input 016	Disabled	Disabled	Enabled	Class 1
17	(000017) Digital Input 017	Disabled	Disabled	Enabled	Class 1
18	(000018) Digital Input 018	Disabled	Disabled	Enabled	Class 1
19	(000019) Digital Input 019	Disabled	Disabled	Enabled	Class 1
20	(000020) Digital Input 020	Disabled	Disabled	Enabled	Class 1
21	(000021) Digital Input 021	Disabled	Disabled	Enabled	Class 1
22	(000022) Digital Input 022	Disabled	Disabled	Enabled	Class 1
23	(000023) Digital Input 023	Disabled	Disabled	Enabled	Class 1
24	(000024) Digital Input 024	Disabled	Disabled	Enabled	Class 1
25	(000025) Digital Input 025	Disabled	Disabled	Enabled	Class 1
26	(000026) Digital Input 026	Disabled	Disabled	Enabled	Class 1
27	(000027) Digital Input 027	Disabled	Disabled	Enabled	Class 1
28	(000028) Digital Input 028	Disabled	Disabled	Enabled	Class 1
29	(000029) Digital Input 029	Disabled	Disabled	Enabled	Class 1
30	(000030) Digital Input 030	Disabled	Disabled	Enabled	Class 1
31	(000031) Digital Input 031	Disabled	Disabled	Enabled	Class 1
32	(000032) Digital Input 032	Disabled	Disabled	Enabled	Class 1
33	(000033) Digital Input 033	Disabled	Disabled	Enabled	Class 1
34	(000034) Digital Input 034	Disabled	Disabled	Enabled	Class 1

A- 8: CMC356 Testing tool



CMC356 shown in B.1 is the test set that is used to test protection relays that uses six current sources operated using omicron test universe software.

A- 9: DNP3 interoperability demonstration block diagram



A- 10: DNP3 data communicated between protection relays and telemetry unit


```
7E 05 64 11 C4 E1 2E 01 00 36 9B E9 C9 01 3C 02 06 3C 03 06 3C 04 06 9A 41 05
64 0A 44 01 00 E1 2E 9E DA C0 C9 81 00 00 5B DF 05 64 11 C4 E2 2E 01 00 77 91
D3 C3 01 3C 02 06 3C 03 06 3C 04 06 79 AE 05 64 0A 44 01 00 E2 2E 35 6A C0 C3
81 00 00 DD E2 05 64 11 C4 C9 32 01 00 F7 10 D5 C4 01 3C 02 06 3C 03 06 3C 04
06 73 3F 05 64 0A 44 01 00 C9 32 B9 D2 F6 C4 81 00 00 6C 4C 05 64 11 C4 CA 32
01 00 B6 1A DB CF 01 3C 02 06 3C 03 06 3C 04 06 1F 88 05 64 0A 44 01 00 CA 32
12 62 D3 CF 81 00 00 41 04 05 64 11 C4 CB 32 01 00 5E D8 EC C8 01 3C 02 06 3C
03 06 3C 04 06 E4 DF 05 64 0A 44 01 00 CB 32 5C C9 EC C8 81 00 00 BF DC 05 64
11 C4 F9 2A 01 00 DE AF DF CE 01 3C 02 06 3C 03 06 3C 04 06 86 FA 05 64 0A 44
01 00 F9 2A 5A B3 D8 CE 81 00 00 EA F6 05 64 11 C4 FA 2A 01 00 9F A5 F0 C3 01
3C 02 06 3C 03 06 3C 04 06 1A 21 05 64 0A 44 01 00 FA 2A F1 03 E3 C3 81 00 00
8A 9F 05 64 11 C4 E1 2E 01 00 36 9B EA CA 01 3C 02 06 3C 03 06 3C 04 06 58 02
05 64 0A 44 01 00 E1 2E 9E DA C0 CA 81 00 00 1A D5 05 64 11 C4 E2 2E 01 00 77
91 D4 C4 01 3C 02 06 3C 03 06 3C 04 06 94 D3 05 64 0A 44 01 00 E2 2E 35 6A C0
C4 81 00 00 B7 34 05 64 11 C4 C9 32 01 00 F7 10 D6 C5 01 3C 02 06 3C 03 06 3C
04 06 AD 51 05 64 0A 44 01 00 C9 32 B9 D2 F7 C5 81 00 00 82 AD 05 64 11 C4 CA
32 01 00 B6 1A DC C0 01 3C 02 06 3C 03 06 3C 04 06 82 41 05 64 0A 44 01 00 CA
32 12 62 D4 C0 81 00 00 16 CE 05 64 11 C4 CB 32 01 00 5E D8 ED C9 01 3C 02 06
3C 03 06 3C 04 06 8D 25 05 64 0A 44 01 00 CB 32 5C C9 ED C9 81 00 00 51 3D 05
64 11 C4 F9 2A 01 00 DE AF E0 CF 01 3C 02 06 3C 03 06 3C 04 06 77 12 05 64 0A
44 01 00 F9 2A 5A B3 D9 CF 81 00 00 04 17 05 64 11 C4 FA 2A 01 00 9F A5 F1 C4
01 3C 02 06 3C 03 06 3C 04 06 57 AC 05 64 0A 44 01 00 FA 2A F1 03 E4 C4 81 00
00 F2 A0 05 64 11 C4 E1 2E 01 00 36 9B EB CB 01 3C 02 06 3C 03 06 3C 04 06 31
F8 05 64 0A 44 01 00 E1 2E 9E DA C0 CB 81 00 00 F2 17
```


These messages are represented in hexadecimal format. The messages over the white background represent the command from the telemetry unit to the protection relay; the messages over the black background represent the response from protection relays. The structure of hexadecimal messages is made up of octet identifier and length of the captured data.