UNIVERSITY OF ™
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

CONSIDERATION OF THE IEC 61850 PROTOCOL AND IMPLICATIONS FOR SUBSTATION ENGINEERING

Nathan Barry Sparks

In fulfilment of the degree of Masters in Electrical Engineering, College of Agriculture, Engineering and Science, University of KwaZulu-Natal

17/03/2018

Supervisor:

Dr Akshay Kumar Saha

FINAL COPY

COLLEGE OF AGRICULTURE, ENGINEERING AND SCIENCE

As the candidate's Supervisor I agree/do not agree to the submission of this thesis.

Signed:

……………………………………………………………………………………

DECLARATION 1 - PLAGIARISM

I, ………………………………………….………………………., declare that

1. The research reported in this thesis, except where otherwise indicated, is my original research.

2. This thesis has not been submitted for any degree or examination at any other university.

3. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

4. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a. Their words have been re-written but the general information attributed to them has been referenced

b. Where their exact words have been used, then their writing has been placed in italics and inside quotation marks, and referenced.

5. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed:

……………………………………………………………………………………

COLLEGE OF AGRICULTURE, ENGINEERING AND SCIENCE

DECLARATION 2 – PUBLICATIONS

DETAILS OF CONTRIBUTION TO PUBLICATIONS that form part and/or include research presented in this thesis (include publications in preparation, submitted, *in press* and published and give details of the contributions of each author to the experimental work and writing of each publication)

Publication 1

Title: "A Review of the IEC 61850 Protocol and its Implications for Substation Communication"
Authors: N. B. Sparks and A. K. Saha

Accepted for final publication in the peer reviewed Journal of Engineering and Applied Science (JAES), published by the Faculty of Engineering at Cairo University.

Database: Scopus, EMBASE, Compendex, GEOBASE, EMbiology, Elsevier BIOBASE, FLUIDEX, World Textiles and IIIumin 8.

Publication 2

Title: "A Review of the IEC 61850 Protocol and its Implications for Protection and Design"
Authors: N. B. Sparks and A. K. Saha

Accepted for final publication in the peer reviewed Journal of Engineering and Applied Science (JAES), published by the Faculty of Engineering at Cairo University.

Database: Scopus, EMBASE, Compendex, GEOBASE, EMbiology, Elsevier BIOBASE, FLUIDEX, World Textiles and IIIumin 8.

Publication 3

Title: "Implementation of a Multi-Protocol Substation Communication and Automation Network"
Authors: N. B. Sparks and A. K. Saha

Pending final publication with the South African Universities Power Engineering Conference (SAUPEC), January 24th -26th 2018, hosted by the University of the Witwatersrand (Wits).

Publication 4

Title: "Applications of GOOSE Messaging for Breaker Fail Protection"
Authors: N. B. Sparks and A. K. Saha

Pending final publication with the South African Universities Power Engineering Conference (SAUPEC), January 24th -26th 2018, hosted by the University of the Witwatersrand (Wits).

Signed:

………………………………………………………………………………

ACKNOWLEDGEMENTS

The author of this paper would like to acknowledge the contributors of the studied engineering works, texts and literatures for developing and maintaining the IEC 61850 protocol which was investigated during the course of this dissertation. The author must also thank Dr Akshay Kumar Saha for his supervision of this research as well as for his hard work and invaluable contribution to the final works. Additionally, gratitude must be expressed to Mr Flip Helberg and to those from Actom (Pty) Ltd who kindly helped with the donation and configuration of important equipment. Final acknowledgement must be given to the University of KwaZulu-Natal in Durban, South Africa whose facilities, knowledge and infrastructure were used to compile this dissertation.

ABSTRACT

This dissertation presented a study on the future-proof IEC 61850 communication protocol and its implications for substation engineering. The advent of contemporary technologies has resulted in the decentralization of substation architecture. Over the last 15 years the IEC 61850 protocol has been contributing to the refurbishment and upgrade of conventional substations. As the aging infrastructure of these centres has been slowly replaced, the hybrid substation has begun to emerge. These substations have been known to contain tedious combinations of different proprietary protocols all attempting to operate within the same substation network. Therefore, the introduction of IEC 61850 to old substations can have an effect on automation, protection and communication within the substations local environment. In this dissertation a multi-protocol substation communication network and SCADA was established using DNP3, Modbus RTU and IEC 61850. A communication network was developed between a physical nexus of connected IEDs and end equipment. It was from this model that the operation of a typical substation automation system was analysed. This critical assessment focussed on the workings of the remote-control points as well as the response of end equipment under fault conditions such as breaker fail, overcurrent and earth fault. In addition to the operation of the multi-protocol model, individual inferences could be drawn from the implementation of the aforementioned protocols themselves. These deductions related to the significance of time stamped data, the reduction of cross-wired copper cables within substations, the obvious limitations of serial RS 485 Modbus RTU and the convenient benefits of 'virtual' networks.

It was during the main research phase of this study that the principal benefits of the IEC 61850 standard were readily enforced and interpreted. Furthermore, special consideration was given to the implications of the GOOSE message class on substation protection. It was here that GOOSE-based breaker fail protection, arc-flash protection and blocking response were investigated. As a result of the implementation of these protection schemes it was determined that GOOSE messaging and by extension the IEC 61850 standard provides optimisation, economic benefits as well as revolutionary advancements in protection and automation to substations. The IEC 61850 substation standard is current, universal, promotes the interoperability between devices and is a leading contributor in the development of smart grids. Therefore, IEC 61850 is a standard of the present and of the future.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

THE electrical engineering principles that govern the way modern substations are designed and define the way protection and automation equipment communicates have evolved substantially in the early 21st century. The term 'protection', within the context of this dissertation, refers to the ability of a device to detect a potentially dangerous electrical anomaly, such as fault current, and immediately or otherwise isolate the vulnerable constituents of a power system [1], [2]. The failure of a piece of protective equipment, such as a relay, to operate under fault conditions can cause instability, system outages, damage to expensive equipment as well as danger to human life [1], [2].

The design of protection for power systems and substations worldwide has continued to change, develop and evolve as technology has improved [2]–[4]. In times past, the numerous media, mechanisms and methods of communication between equipment within substations have presented an economic and technical obstacle to engineers, vendors and utilities on a global scale [3], [4]. Over time substation equipment like relays and Remote Terminal Units (RTUs) have become even more technically advanced, smart and complex with many different functions incorporated onto one physical device [5]. As a result of this innovation, countless communication protocols have been developed by vendors to help transfer pieces of information between their own devices and products [4], [6]. Therefore, it is common that a variety of different proprietary protocols exist on a particular substation network to serve many different functions [4], [6]. However, complex combinations of these protocols can make designing a substation automation system (SAS) and integrating devices from different manufacturers a tedious task [4], [6]–[7]. A new standard of communication from the International Electrotechnical Commission (IEC) was needed to make the design, protection, control and automation of a substation more efficient and generic within its local environment. It was in this dissertation that the relatively young IEC 61850 substation communication protocol was practically and theoretically researched. Thus, in doing so it was used as a technical benchmark for both past and present standards in industry.

Modern relays are typically intelligent microprocessor-based devices that are, in the most basic sense, used to control and trip electrical circuit breakers upon sensing, for example, a fault current at a particular point on a system [1]–[3]. In addition, these intelligent relays have different levels of time-response that enable them to clear abnormalities like under- and over- current, under- and over- voltage and fluctuations in the grid frequency before any damage is incurred on a system [2]. Hence, when a fault occurs and an abnormal electrical quantity is sensed, a trip logic is created by the relay and sent to a circuit breaker which interrupts the flow of power to the connected equipment preventing any damage and or other related consequences within the appropriate timeframe [2]. These newer, faster and more intelligent relays have now begun to use TCP/IP

Ethernet-based protocols such as the IEC 61850 substation communication standard. This new protocol is henceforth replacing the older Ethernet and serial-based legacy protection schemes that use Modbus RTU and DNP3 to transfer data between devices and their peers [2], [5].

Today's relays are often referred to as cyber-physical devices since their design is both digital and programmable in nature [2], [5]. They have been developed to perform many advanced peripheral functions that act to improve the coordination, security and reliability of a power system [1], [4]. These functions may include metering, automation, protection, fault finding and recording as well as control and monitoring [2], [4]–[6]. Hence, such relays are commonly referred to as Intelligent Electronic Devices (IEDs) [2]. It was before the advent of the IEC 61850 standard that IEDs communicated using their very own proprietary TCP/IP, serial or hardwire-based communication techniques [4], [6]–[7]. Substations became plagued with complicated combinations of both alike and dissimilar communication standards. This posed a technical barrier to both utilities and engineers alike. However, the IEC 61850 protocol allows existing relays to communicate with their neighbouring IED's or to a master control unit within the substation regardless of the manufacturer or vendor [2], [4].

The IEC 61850 standard defines the layer, method and protocol for communication between relays and other IEDs [5]. This allows them to interoperate with other IEC 61850 compliant pieces of equipment, tools and systems. It also introduces new data objects and formats as well as a Substation Configuration Language, commonly referred to as SCL [2], [4]. This protocol has been instrumental in the development of 'smarter grids' which is resulting in the subsequent and swift death of legacy, serial and other less favourable TCP/IP protocol-based protection schemes [2], [5]. The IEC 61850 standard has allowed engineers to consider innovative designs for smarter substations and to repurpose old equipment within the confines of this new protocol [2], [3]. Furthermore, the manufacturers of IEC 61850-compliant IEDs now begun to offer gateways or communication shells that allow the modern IEDs of today to interface and connect to present and or older legacy-based systems [3]. This has resulted in the proliferation of 'hybrid' substations.

Historically, each of the protection, control and monitoring devices within a substation have required different proprietary communication links in order to transfer important data and commands [4], [6]–[7]. This means that communication systems relied on networks of relays using links with EIA-232 point to point and EIA-485 multi-drop communication ports [4]. The speed of data transfer and information exchange over these links was around 38.4 kilobits per second [4]. Two of the legacy communication protocols that were used included DNP3 and Modbus RTU which over time also migrated to the TCP/IP ethernet-based communication medium [4], [6].

Alternatively, the new IEC 61850 standard defines several different interfaces that can be used to communicate between equipment within the substation using the shared physical connections, Ethernet links and the substation Local Area Network (LAN) [5], [6]. The Ethernet communication architectures on which the IEC 61850 protocol is based can be either 10 or 100 Mbit/second for the low to high speed processing or transfer of information [3], [4]. This makes IEC 61850 much faster than EIA-232 or EIA-485 based serial protection schemes [3], [4]. Henceforth, the interconnection of IEDs is now standardized regardless of the manufacturer or vendor. This has had significant cost and maintenance advantages over older legacy protection systems that require mostly hardwire-based techniques to connect and interface between different relays based on a physical response from fuse elements and induction disks [2]. Therefore, the IEC 61850 communication standard defines the future of substation automation, monitoring, control and protection.

1.1 Research proposal

This study aimed to experimentally investigate the relatively new IEC 61850 substation protocol and conduct research into the implications of this protocol on substation engineering. The important aspects of this study included the effects of communication protocols like Modbus RTU, DNP3 and IEC 61850 on the design, protection, automation and interaction of devices within a typical substation. One of the most important benefits of the IEC 61850 standard lies in its ability to allow relays of different vendors to react in a collaborative fashion in response to an electrical anomaly like fault current [1]. This new protocol also allows the IED's, that sense fault current and trip electrical circuit breakers, to inform their peers of the protective actions that were undertaken [1]. Hence, this refers to the publisher-subscriber concept of the IEC 61850 standard.

An important consideration within the context of substation protection refers to how the IEC 61850 standard can affect sympathetic trip protection and the blocking principle. This particular principle seeks to prevent the tripping of unfaulted feeders or incomers on the bus in question [2]. In a station bus-based architecture certain advantages can be exploited when making the transition from legacy to IEC 61850. A conventional or "old-fashioned" protection scheme requires a large number of cross-wired binary inputs between devices and equipment. In some substations, one may encounter a large number of feeders connected to the same medium voltage bus [2]. This means that the number of available relay inputs and outputs of the IEDs could present a limitation to the designer and to the protection scheme's application [2]. An example of this limitation can be seen in an analysis of the overcurrent blocking principle.

In a typical legacy-based substation, the relay that senses a fault current and issues a trip signal will need to apply a blocking signal on the inputs of the other relays on all the adjacent feeders for a certain period of time to ensure that they do not needlessly trip [2]. This means that the number of connections between all the feeder relays and the number of relay inputs and outputs can be very large if there are, for example, 16 feeders connected to a particular medium voltage bus. The same blocking principle (also called sympathetic trip protection) is relatively straight forward to implement using the IEC 61850 protocol. In this case the relay that detects the feeder fault can send a GOOSE (Generic Object Orientated Substation Event) message (over the station bus) to all the other relays that are connected to the distribution bus [2]. This message would indicate that the relay had tripped and had cleared the fault i.e. the blocking signal has been sent to all the other affected relays [2]. This was only one of the many applications of the IEC 61850 communication protocol and the powerful GOOSE message class. The aforementioned concept as well as other additional aspects of GOOSE messaging and IEC 61850 were investigated in greater detail during the course of this study.

1.1.1 Research questions

The further progression of this dissertation as well as the evolution of the research model itself relied upon a number of vital study questions which defined the author's overall approach to this investigation. In summary, these research questions were defined as, but not limited to, the following:

What is the IEC 61850 protocol, what are its requirements and specifications, how is it implemented and what does it offer to aging, present-day and future substations?

What are the advantages and or disadvantages of upgrading legacy-based protocols such as Modbus RTU and DNP3 to the IEC 61850 substation standard using smart protocol-compliant protection IEDs?

What were the performance benefits, protection and automation implications as well as the design and communication considerations of the IEC 61850 protocol for both smart and hybrid substations?

What is the GOOSE message class, what are its applications and implications, and how can it be used to improve the efficiency, effectiveness and economy of protection schemes within substations?

How are the blocking principle, arc-flash protection and breaker fail protection implemented using an IEC 61850-based protection scheme and what are the associated benefits of these implementations in relation to how these protections were typically achieved in legacy-based substations?

1.2 Motivation

The means by which data, information, commands and signals have been transported throughout electrical substations has for years been regarded as a subject of contention between engineers, utilities and vendors alike. Over time, a wide variety of substation protocols, standards, proprietary systems and physical communication methods have emerged for the consideration of engineers when developing and designing electrical networks. It is because of this that complex combinations of different transport mechanisms may exist within a single substation. It was within the last 15 years that a universal substation communication standard had presented itself in the form of the IEC 61850 protocol. In a by-gone era signals and information were transmitted physically via traditional copper hardwire links between relays and their associated legacy equipment. As technology has developed a moved to an Ethernet-based architecture was proposed and now data and information can be transmitted virtually over a substation LAN. Thus, the ease, efficiency and reliability with which this communication can be achieved has become a critical consideration in substation engineering.

In general, under graduate studies at university don't specifically cover the basics of communication within substations, therefore, real world problems, considerations and limitations such as this can only be faced within an industry environment – in the real world. Hence, it was within the author's interest to further his knowledge in the field of substation communication and gain practical and theoretical experience on this topic. This was the field in which the author wished to specialize and work within industry. Thus, this vital opportunity to learn through design, implementation, research and simulation could not be missed. This topic is current, it is developing and it represents a shift of the communication mechanisms within substations for the future. Thus, it was found to be an exceptional real-world topic for a young engineer moving into industry where these concepts will be faced in the coming years.

1.3 Background

The IEC 61850 communication protocol allows IEDs that have been manufactured by different vendors to communicate with each other as well as with related devices within the automated substation architecture. It achieves this by using a generic, beneficial and commonly understood method of communication. This protocol was developed in part by the IECs Technical Committee 57 (TC57) which exists to address the reference architecture for power systems [4], [6]–[7]. The current and developing communication media on which this protocol is grounded include web and internet-based services as well as data, information and signal communication over an Ethernet or optical fiber-based substation local area network [6], [7]. The message classes that this protocol continues to offer include databases like: client-server messaging, Manufacturing

Message Specification (MMS), Generic Object Oriented Substation Event messaging (GOOSE) and Sampled Measured Values (SMV or SV) [2]–[4], [7]. Therefore, the IEC 61850 standard and its associated communication networks can run over TCP/IP Ethernet-based networks using high speed ethernet communication links which deliver acceptable response times of less than 4 ms [2], [4]. This makes the IEC 61850 protocol ideally suited for the fast form of communication and data transport that is required during protective relaying [2], [4].

1.3.1 A brief history

The very first microprocessor-based distance relays, with fault location detection, appeared in the early 1980s [4], [7]. Over the years many different protocols, like Modbus RTU and DNP3, have been developed for substation control, protection and automation; some of which have their very own unique communication links and proprietary systems [4], [6]. The IEC 61850 standard offers benefits which include the interoperation and intercommunication of information between IEDs from different manufacturers. This is of significant advantage to engineers that specialise in substation automation, protection and design [2]. An IEC task team of around 60 group members from various nations around the world developed three IEC working committees in the year 1995 [6], [7]. These working groups responded to and identified all the concerns of power utilities, engineers and vendors alike and created the IEC 61850 protocol which made its first formal appearance in early 2003 [6], [7]. Today, the standard is still enjoying rapid development, growth and implementation worldwide. The aims and objectives that were set by the commission were to [4], [6]–[7]:

- Develop a single universal protocol for transporting information, data, commands and signals.
- Define the services required to transfer data, signals and information between different and similar devices.
- Promote the interoperability between IEDs of different manufacturers within an electrical utility.
- Develop a common format for storing information.
- Define and specify the types and methods of protection, control and automation testing for the new IEC 61850 protocol.

1.3.2 Applications and benefits

A conventional substation is a hardwire-based environment which uses mostly copper based media to connect tools, hardware and equipment [8]. Therefore, converting this type of infrastructure into an IEC 61850-based TCP/IP architecture can be considered tedious. If protection equipment and or other devices were to be installed in a conventional substation it then becomes very difficult and costly to move them [8]. So, functions that are practically impossible for legacy-based substations become far easier and more achievable in an IEC 61850 Ethernet-based environment where the operation and maintenance of IEDs is more 'virtual' [2], [4], [8]. One of the major advantages of this protocol includes the use of functions. All of the functions in a substation are modelled using constructs called logical nodes (LN) [3], [7]–[8]. Therefore, the functions specific to an IED are communicated using LNs which ensures that the communication and exchange of data, signals and information happens in a format that other IEDs can understand [3], [7]–[8]. Since the IEC 61850 standard is so convenient, effective and efficient in its approach to substation automation, protection and control the advantages of this protocol are boundless. A few of the benefits of the IEC 61850 standard are listed as follows but not limited to [7], [9]:

- Reduced hardwire connection within substations.
- Installation of IEDs is not as labour intensive.
- Lower maintenance and cheaper commissioning costs.
- Facilitates the optimisation of substation architecture.
- Functions and capabilities that help to eliminate current transformer saturation and open circuit.
- Intercommunication between devices from different vendors.
- The inception of a single unified substation protocol.

The IEC 61850 standard is a relatively new protocol that is already enjoying widespread popularity within substations for protection and automation due to its advances in communication, configuration, interoperability and topology [2], [3]. However, one of the major disadvantages of this protocol is that its infrastructure is vulnerable to cyber-attacks simply because it is an Ethernet-based architecture [2]. IEC 61850-based substation IEDs are programmable, computerized and connected to a substation local area network and even to the internet. This means that IEDs rely on these virtual systems for the transfer of cyber information. Therefore, IEC 61850 systems are susceptible to cyber-attacks since they are defined as a "hackable" TCP/IP-based infrastructure [2]. Since this protocol is reasonably young, the applications and potential of the standard are still developing at the hands of the IEC, engineers and utilities alike. The present focus of this protocol is to effectively communicate items such as [2], [6]–[7]:

- SVs for current and voltage transformers (CT and VT).
- Input/output information and data for control, monitoring and protection.
- Trip signals and GOOSE messages.
- Configuration information and setup files.

- Transfer data to control hubs.
- As well as system metering.

1.4 Feasibility

This brief section aimed to discussed the feasibility of the proposed undertaking by defining the scope of the research, requirements, approach to the study as well as an analysis of the merits of the research that was to be investigated during the course of this dissertation.

1.4.1 Scope

The scope of this dissertation seeks to cover the exploration and assessment of a new substation communication protocol that has been put forward by the IEC. The IEC 61850 substation standard affects and influences substations in various ways. This influence may extend to equipment, design, protection, automation as well as the different media and methods of communication. The definition of the research statement is thus to: compile a scientific, engineering research analysis, comparison and implementation of this standard in order to shed light on the outlined influences.

1.4.2 Current analysis

The present understanding of the IEC 61850 protocol is that it is current, developing, smart and considered a convenient, effective and universal way to establish communication between substation devices of different vendors. It is because of this that it is becoming more popular and widespread as substations are upgraded and as technology improves. However, the extent to which this protocol is implemented varies from substation to substation based on the views, expertise and budget of the utilities that implement it. Being a relatively new standard, it has received both praise and resistance from engineers and utilities alike. Therefore, by the end of this study the merits of the IEC 61850 protocol should hopefully be established giving credit to either those who praise it or to those who shun it.

1.4.3 Requirements

The requirements for the progression of this research included the acquisition of IEC 61850 and legacy compliant hardware such as relays, remote terminal units, Ethernet switches, input/output units as well as SCADA host software. Furthermore, this research topic would make use of the RSCAD software package and a Real Time Digital Simulator (RTDS), both of which are available at the university, for the simulation of experimental tasks. The author may also use some of the protection relays and other hardware which is already available at the school of engineering at the University of KwaZulu Natal as well as those kindly provided by Actom. In addition, research into the IEC 61850 standard itself was conducted using IEEE journal papers, Science Direct and industry documents that can be accessed within the UKZN libraries or on the internet.

1.4.4 Approach

In order to assess the effectiveness of substation protocols like Modbus RTU, DNP3 and the IEC 61850 standard it was important to establish a typical multi-protocol substation network with all the associated automation systems. This involved designing an interactive SCADA model of the substation architecture as well as implementing a network of compliant modern and legacy IEDs along with the associated switchgear. Once a fully-fledged substation communication network had been established with a variety of alike and dissimilar industry protocols a comparison, analysis and conclusion about the communication methods could be obtained along with the electrical operation, automation and protection results of the substation itself.

1.4.5 Evaluation

Since the IEC 61850 standard will be implemented in conjunction with present and aging legacy standards like Modbus RTU and DNP3 it became possible to critically compare it to the legacy protocols and obtain a benchmark from which to draw certain conclusions, inferences and technical deductions.

The cost of this multi-protocol implementation as well as of the equipment to be used was to be borne by the university and by donations from industry partners alike. The infrastructure that was needed to conduct this study was already in place, thus experimentation and implementation could proceed.

1.4.6 Review

The thoroughness and accuracy of the approach that was required to proceed with this research has been deemed satisfactory in this brief assessment of the topics feasibility. The IEC 61850 protocol is a current standard, it is of interest, it is developing and it is a partner to the technological advancement of substation design, communication, protection and automation worldwide. Thus, based on these criteria this topic was adjudged to be appropriate, the study relevant and therefore the undertaking could proceed.

1.5 Aims and objectives

This research aimed to investigate the IEC 61850 substation protocol for the intercommunication of substation IEDs and associated devices. In addition, this study also strives to determine the extent of the influence of alike and dissimilar communication protocols on the design, protection and automation of a substation. Hence, this research involved an analysis of the benefits, pitfalls and associated implications of upgrading legacy protection schemes as well as the impact of IEC 61850-based protection on substation architecture. The advent of modern cyber-physical IEDs has resulted in broadening the applications of 21st century protection systems. These systems have become more intelligent, interconnected, interoperable and generic using the new IEC 61850 substation protocol. Therefore, this research aimed to:

- Consider the implications of the IEC 61850 standard on substation protection, design, automation and communication using the following means:
    - Design a multi-protocol communication network using standards like Modbus RTU, DNP3 and the IEC 61850 protocol.
    - Compare the IEC 61850 standard to present and past protocols such as Modbus RTU and DNP3 commenting on their technical effectiveness.
    - Development of smart substation SCADA for remote control, monitoring and data capture in multi-protocol and IEC 61850-based environments.
    - Design, simulate and implement fast substation protection in IEC 61850-based environments.
    - Implement and analyse the GOOSE message class studying its technical applications, perceived advantages and possible short-comings.
    - Assess the benefits of using the IEC 61850 standard for items like blocking response (sympathetic trip protection), breaker fail, disturbance recording and arc protection.
    - Determine the impact of modern IEC 61850 compliant IEDs on the old and aging infrastructure of the legacy era.
- Analyse the electrical operation of a typical multi-protocol and IEC 61850 compliant substation automation system with different protection functions.

Here follows the list of project objectives that were followed when proceeding with this research in order to compile a comprehensive investigation into the basics of protocol-based substation communication:

- Background research and pilot study on the chosen topic.
- Literature survey to be conducted on any relevant issues and topics using standard references, texts, IEEE journal papers, scientific literatures, industry documentation and alike.
- Formulation of research goals, specifications and methodology.
- Development of a preliminary system model based on the literature survey and background research.

- Development of the main research model for an industry application of the IEC 61850 standard with basic protection functions in a substation.
- Simulation of the developed models.
- Hardware testing and capture of results.
- Performance evaluation of the simulation and hardware solutions.
- A critical analysis of the results that were obtained and the research conducted along with relevant critical comparisons, provisions for future works and conclusions.

1.6 Dissertation structure

The succeeding chapters of this thesis aimed to explore the basic design, protection, automation and communication aspects of the IEC 61850 and alike substation protocols. In chapter 2 the author offered a critical literature study of the IEC 61850 standard which reviewed published works, scientific text and technical documentation from the champions of industry. This survey sought to investigate the inception of the IEC 61850 protocol, discover the objectives for which it was developed, determine how it functions as well as its implications for both modern and aging substations. The authors discussed a few acute details of the standard such as message classes, communication functions, SCL, the impact of this protocol on protection and substation design, substation automation, cyber vulnerability, backup protection as well as testing. Additionally, once a better technical understanding of the research topic was achieved, the methodology of the proposed experimental study could be outlined as was demonstrated in chapter 3. This section presented the procedures, materials and methods for the investigative works that were conducted in the subsequent chapters.

The principal body of research for this dissertation occurred within the stage 1 and stage 2, preliminary and main studies which were concluded in the chapters 4 and 5 respectively. Chapter 4 sought to deliver a basic induction into the preliminary undertaking by including the results and analyses which were determined from the early stage of experimentation by using both practical and simulation studies. It was in this chapter that a multiprotocol substation communication network was established using Modbus RTU, DNP3 and the IEC 61850 standard. Finally, the foremost focus of the research for this dissertation was firmly established during the course of chapter 5. It was here that the primary and basic functionalities of the IEC 61850 protocol were investigated, with special consideration given to the applications and implications of the GOOSE message class. Items such as sympathetic trip protection (blocking response), breaker fail, disturbance recording and arc protection were explored in greater detail. Furthermore, chapter 6 offered a comparative study of the IEC 61850 protocol in relation to legacy standards like Modbus RTU and DNP3. This analysis used the results and conclusions drawn from the experimental study conducted in this thesis as well as the researched literature on all three standards to discuss the associated, perceived and technical benefits and short-comings of the aforementioned protocols. Lastly, chapter 7 offered a definitive conclusion of the topics researched and experimented upon during the course of this dissertation. Therefore, it was as a result of this study that certain inferences, deductions and interpretations of the communication protocols could be drawn.

2. LITERATURE REVIEW

2.1 Introduction

This chapter presents a detailed review of the IEC 61850 substation protocol and its implications for both modern and legacy-based protection schemes, inter-IED communication and substation design. The intelligent electronic devices of today have the ability to communicate, interface and interoperate using Ethernet-based protocols like the IEC 61850 standard. This has promoted an industry shift from the outdated serial and legacy protection schemes to a universal Ethernet-based architecture. These aging infrastructures use communication protocols like Modbus RTU and DNP which may rely on serial RS 232 and RS 485 binary hardwire connections between devices in order to transport data, commands and vital control signals. Therefore, the new IEC 61850 protocol affects the way present-day substations are designed, how IEDs are interfaced, the manner in which devices communicate and the overall effectiveness and efficiency of a substation. However, this contemporary standard also presents a fresh set of problems to engineers and utilities alike such as cyber vulnerability, a new set of standards in protection testing, smart IED back-up prior to failure, IED file configuration as well as the communication of information between IEDs using a new peer to peer message system. Thus, the continued collaboration of the International Electrotechnical Commission (IEC) has resulted in the development of a communication standard that allows IEDs of different manufacturers to interact within the local substation environment and transfer data and signals quickly over a ‘virtual’ Ethernet-based local area network (LAN).

2.2 Communication classes

The IEC 61850 protocol provides a standardized means of communication for IEDs within a substation. Not only does this standard specify the medium of communication, whether optical fibre or Ethernet, but it delivers a set of functions, formats and layers that define how information or signals are transferred between devices [2]–[4]. In addition to Client-server messages, there are two common classes of communication for protection, control and automation, namely: the GOOSE and SV message classes respectively [2]–[4]. Firstly, Client-server integration deals with the services that are needed or used by the Client in order to receive and store information from devices as well as send control signals to the IED servers [2]–[4]. Therefore, a typical Client-server system may refer to the Supervisory Control and Data Acquisition (SCADA) or Human Machine Interface (HMI) of the broader substation. Importantly, Client-server messages are sent through the TCP/IP stack where no specific time constraints are implied [4]. On the other hand, the GOOSE and SV message classes are exclusively used as packets for sending signals and data between IEDs. These are both real time messages that bypass the TCP/IP stack and interface onto the Ethernet link layer [4]. The GOOSE and SV message classes are both vital aspects of the IEC 61850 protocol and were discussed further, as follows, in this section of the paper [4], [10]–[16]. The diagrammatic illustration in Figure 2-1 provides a framework that shows how these message classes map directly onto the Ethernet link layer [12].

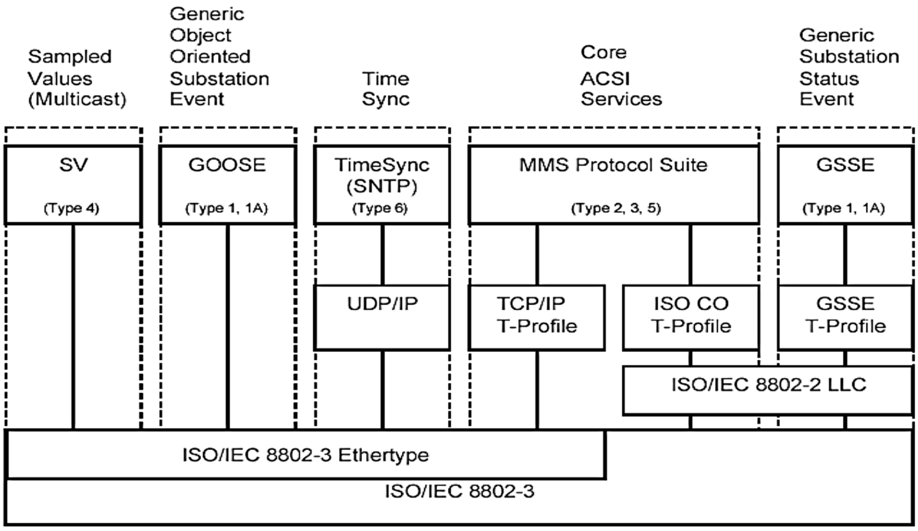


Figure 2-1. IEC 61850 message class data mapping [12]

2.2.1 Generic substation events

The two most commonly used horizontal message classes in IEC 61850-based substations are the GSSE and GOOSE message classes respectively [2]–[4]. The major difference between them is that GOOSE can transfer data formats like analog, binary and integer information whereas GSSE is constrained mainly to binary event status data [11]–[14]. These classes are both referred to as peer to peer communication mechanisms that transfer information in a 2-layer message between the bay and process levels [11]–[14]. GOOSE messages allow for the transfer of a vast range of common data that is organized by a DATA-SET [13]. Hence, this message system is favoured, widely understood and enjoys greater popularity within IEC 61850-based environments due to its greater flexibility. GOOSE messages are typically used by IEDs to report status events to other IEDs within and between feeders. It was developed to operate on TCP/IP Ethernet or optical fibre networks to replace the old hardwire or serial communication links between IEDs and legacy relays on the station bus [2]–[4]. To setup an IEC 61850 communication network is a fairly simple procedure. Each IED within a network will have an IP address which will specify which GOOSE messages the device has access to [16]–[18]. This makes the GOOSE message system and by extension IEC 61850 more efficient than legacy-based architectures.

In addition to its flexible transfer of data, the GOOSE message class is also configurable and can send information like circuit breaker status and analogue measurements. This means that a particular IED could issue a GOOSE message to its peer devices notifying them if it had issued a trip signal [4]. The applications of this allow the IED closest to the fault (the downstream IED) to issue a trip and at the same time ensure that the other upstream IEDs do not trip needlessly, thus reducing the size of the outage [4], [11]. This is called a blocking response or sympathetic trip protection [4]. Therefore, IEDs connected to the substation LAN are aware of the currents and voltages at the points that they measure directly as well as from the GOOSE messages that are received from the other IEDs [2], [4], [11].

Table 2-1. Time performance and message types [4]

Type	Application	Performance Class	Transmission Time
1A	Fast Messages (Trip)	P1	10 ms
		P2/P3	3 ms
1B	Fast Messages (Other)	P1	100 ms
		P2/P3	20 ms
2	Medium Speed		100 ms
3	Low Speed		500 ms
4	Raw Data	P1	10 ms
		P2/P3	3 ms
5	File Transfer		≥1000 ms
6	Time Sync.		(Accuracy)

Typically, a number of relays may be used to take readings on a particular line or bus section with GOOSE messages being exchanged between those devices who have subscribed to the information stream [4]. Importantly, GOOSE messages include items like trip, interlocking and inter-trip messages [2], [4], [13]. These messages are time critical and must be transmitted at speeds of between 10 and 3 ms as illustrated in Table 2-1 [15], [16]. This means that GOOSE is referred to as a 'fast' messages system and is used to decrease the clearing time of faults. Usually, no more than 4 ms is allowed to elapse from the time a particular event in the system is detected until the point at which the message is transmitted [4], [15].

As previously mentioned, GOOSE messages are multi-cast to the substation LAN and are only accepted by those IEDs that have been configured to subscribe to that particular data stream [4]. Importantly, these messages are broadcast multiple times using a 3 ms back-to-back retransmission mechanism that transmits regardless of whether a change has occurred [4]. This improves the reliability of the system and ensures that the event has been received by the appropriate IED [2]–[4], [14]. Therefore, GOOSE messages are an example of multicast/broadcast messages i.e. a single device will send out a message to several devices in the multicast case and all the devices on the network in the broadcast case [4]. This has huge benefits over the point-to-point message systems of old. When the Ethernet switch receives a particular message, it forwards it to all other ports on the network apart from the port where the message was received [2]–[4]. The IED must then analyse this message and decide whether or not it has been configured to receive it. This constricts the bandwidth of the network and can increase network traffic affecting the speed of the messages that are transmitted. Two methods exist to alleviate this problem. One is to develop a system of several virtual LANs that divide the traffic between them [3], [4], [11], [14]. The other solution is to use the fact that GOOSE messages may be assigned a priority so that the switch knows which messages to send first. The time duration and speed of transfer of messages in the IEC 61850 standard are shown in Table 2-1 [4]. The table specifies that GOOSE messages are a 1 or 1A fast message system [4].

2.2.2 Sampled values

The GOOSE and SV message classes are both referred to as priority real-time messaging that can interface directly over the substation LAN. The SV message class is used to send digitized voltage and current measurements to the IEDs within the substation on the process bus [2]–[4], [13]–[16]. SV messages are also multicast which means that the data obtained from a measurement taken at one location may be sent to any number of devices connected to the Ethernet network. This measured information is typically obtained from the secondary analog outputs of the instrument CTs and VTs respectively [4]. Furthermore, the analog data from the instrument transformers must be sent to a device called a merging unit (MUs) whose function is to digitize the sensed information and finally deliver it to the IEDs using logical interfaces ‘4’ and ‘5’ [8]. Modern IEDs can input different data from multiple MUs on the network.

The MU can take 80 samples per cycle with an SV message rate of 4.8 kHz for basic protection and 256 samples per cycle for high frequency applications; other SV message rates may also include 1.5 kHz, 4 kHz and 12 kHz respectively [2]–[4]. Therefore, a merging unit is a device that provides the interface between the CTs/VTs and the IEDs within a substation and they can receive multiple binary and analog inputs [2], [4], [14]. Figure 2-2 shows a basic implementation of this concept [11].

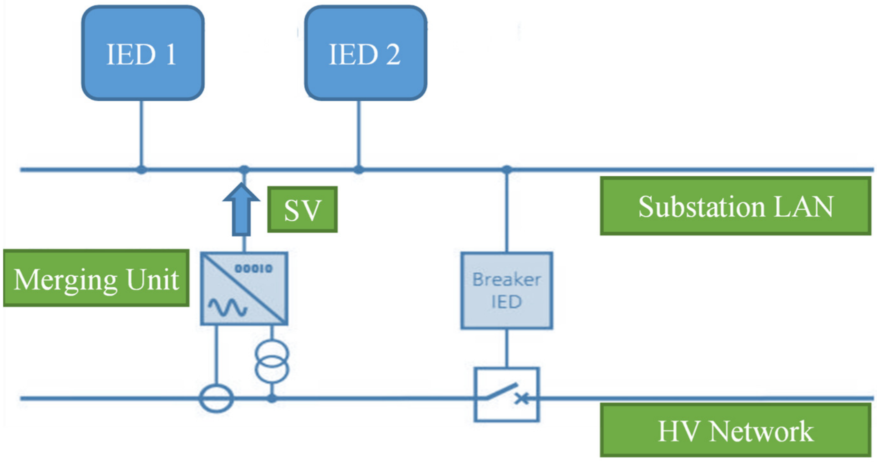


Figure 2-2. IEC 61850 SV messaging and MU interfaces [11]

Additionally, the IEC 61850 protocol also allows relays to send messages via the MU to other devices on the station bus. Hence, the MU may arbitrate the interaction between a certain number of IEDs and communicate with other MU's connected to the substation LAN [2], [4]. An IED must however, be configured to subscribe to the SV stream from its associated MU and can then also receive GOOSE messages and phasor information from its surrounding IED's provided it is configured to do so. It is common that several merging units interface with one another over the substation LAN which can transfer information at speeds of up to 100 Mb/s [3], [4]. Numerous devices can be interconnected using this system as well as a central supervisory computer which may receive current and voltage samples in the form of SV messages from the MU [3]. This means that substation protection, control and monitoring can be implemented in a very coherent fashion. Hence, the IEC 61850-based communication architecture may have an impact on the design of substations and on the layout of switchgear as compared to legacy-based protection schemes [2], [4]. In summary, MU's carry the following functionalities as described [2]:

- Signal processing of sensors and transducers;
- Synchronisation of three-phase voltage and current measurements;
- Analog interfacing;
- Reduction in CT saturation;
- Digital interfacing (IEC 61850-9-2).

2.2.3 Logical interfaces

One of the most important benefits of the IEC 61850 protocol lies in the ability of relays or IEDs to react in a collaborative fashion when dealing with an electrical anomaly like fault current [6], [7]. The IEC 61850 standard allows the IEDs, that sense items like fault current and trip electrical circuit breakers, to inform their peer relays of the protective actions that were undertaken or needed using the shared physical communication links between physical devices [6]. Thus, a function used by a particular IED may be specific to that device such as an IED on a particular feeder or distributed to two or more IED's over the Ethernet communication network if they subscribe to that particular information stream [7]. Thus, the allocation of functions between IEDs in a substation defines the requirements of the aforementioned physical interfaces.

All known functions within a substation may be modelled using Logical Nodes (LNs) [6]. There are logical nodes for automatic control whose names begin with 'A' as well as logical nodes for protection (P) and monitoring (M) as well as nodes for all other necessary function within the substation. Each node has an Instance-ID as a suffix to delineate between nodes as they are transferred thus ensuring that LNs are not received by the incorrect IED [8]. These nodes communicate with each other and transfer information using logical interfaces.

The logical interfaces within a substation distribute functions (logical nodes) between IEDs on different levels of the substation hierarchy (station, bay and process buses) from IF1 to IF10 as shown in Figure 2-3 [6]–[8]. Therefore, IF 1-10 are referred to as logical function interfaces and represent the different hierarchies over which specific information like trips, inter-trip and interlocks can be transferred between various IEDs in a substation. The authors of paper [8] define the IF4 and IF5 functional levels, shown in Figure 2-3, as interfaces for the transfer of data from the CTs and VTs between the process level and the bay level respectively [8]. Alternatively, the IF8 functional level refers to the direct transfer of data between bays for fast information processes like interlocking [8]. IF 4 and 5 are typically used for process bus applications whereas IF 8 has applications for station bus communications. The supplementary logical function interfaces that link devices and IEDs within a substation, from IF1 to IF10, were illustrated in Figure 2-3 [8].

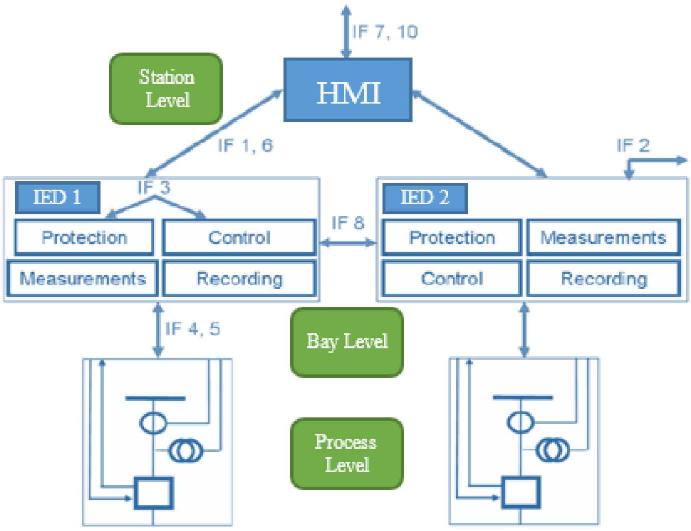


Figure 2-3. IEC 61850 logical interfaces [8]

2.3 Substation configuration language

The IEC 61850 protocol specifies that engineers and vendors use a Substation Configuration Language (SCL) which was developed to configure the settings and format the functions within a particular IED [2], [3]. Manufacturer specific IED configuration tools are used to convert the functionality, communication mechanisms and the parameters of an entire IED into a hierarchy of SCL system files [3], [4]. This is one of the major differences between IEC 61850-based IEDs and other protocol-based substation automation systems. SCL is a description configuration vernacular that is based on eXtensible Markup Language (XML) [4].

The authors of papers [3], [4] and [5] describe in detail the various aspects of SCL engineering and the associated file transfer and configuration techniques of IEDs. SCL specifies a file format that describes IED communication, switch yard structure and any relations that take place between them. It ensures that the IED capability descriptions (ICDs) and the substation descriptions are transferred between the IED engineering tools and the system engineering tools of different vendors or manufacturers [4]. Upon setup, the IED configurator tool converts functionality, data communication, events and alarms into SCL [3], [5]. This simplifies substation configuration and communication between IEDs. Therefore, the generation of data, reading of data and data structure is less ambivalent [3], [5].

In addition, SCL specifies file formats that describe the configuration, parameters and the relationship between IEDs. Furthermore, SCL engineering results in the creation of a substation configuration description file (SCD) which contains all the necessary information about a substation [3], [5]. As previously mentioned, SCL allows the easy and simple exchange of information between IEDs of different manufacturers. Hence, when a new IED is installed within a substation the configuration of the previous IED is available in SCL format and can simply be imported onto the new device. This concept is similar to changing a SIM card in a new phone [5]. So, the functionality and communication of the existing protection, automation and control schemes can be effectively maintained. Therefore, SCL engineering has major advantages over older legacy-based systems which are not programmable and must be replaced rather than reconfigured [5].

In protection systems, the time-current response of a particular IED can be configured using SCL. The response logic within a particular IED may call for an instantaneous trip when the current exceeds a particular value or a delayed trip where the IED integrates the value of the fault current over time and waits for it to exceed a second threshold value [3]. Hence, over current protection may be implemented, using SCL, in stages.

2.3.1 SCL-based protection

The initialisation and setup of an SCL-based protection IED involves the use of three files, namely: the ‘startup.cfg’, ‘datamap.cfg’ and CID files. The function of the first file, called the ‘startup.cfg’ file, is simply to store logical device data [5]. In addition, mapping information is stored in the ‘datamap.cfg’ file and lastly, the CID file stores the function and role of the IED [3], [5]. Furthermore, the protection IED parses a CID file that stores the data which defines the roles that are specific to a particular IED [5]. The IED not only parses these three files but is also initialized via data object generation, information mapping, network setting, logical node setting and the subscription that allows it to broadcast and receive SV data from the instrument transformers and MUs [3], [5]. Thus, this means that the protection type, function and configuration of the IED is determined by parsing the CID file [5].

In order to configure an IEC 61850 relay certain SCL-based communication files are required [5]. In summary, these files may include but are not limited to the [3], [5]:

- System Specification Description file (SSD): which stores information like, logical nodes, physical connections and single-line diagrams of the substation.
- System Exchange Description file (SED): stores the information specific to communicating with other configurators.
- IED Capability Description file (ICD): which identifies the logical nodes that are available to the IED
- Substation Configuration and Description file (SCD): which describes data exchange and transfer structures and hence, the interaction between IEDs in the system or project
- Configured IED Description file (CID): which enables and configures the IED according to its functions.

2.3.2 IED setup using SCL

The first and most fundamental aspect of setting up an IED using SCL is to select a suitable IED for the intended function and or role within the substation and configure it using the IEDs configuration tool [4]. An IED Capability Description (ICD) is produced for each relay based on the IED specific description file. This file describes the logical devices and nodes, GOOSE and SV information, communication services and addresses for data [3], [5]. In the second step, all the ICD files are transferred to the IED configuration tool. This configures the system functions and allocates functions to the IEDs within the substation [3], [5]. The system configurator then creates a Substation Configuration and Description file (SCD) after it has received the ICDs, SSD and SED files [4]. The SCD file defines the interaction between different IEDs and holds all the information that describes the substation. Finally, based on this SCD file an IED engineering tool is used to build the CID file for each device [5]. The system configurator then sends the IEDs their specific CID files. The IEDs parse these files during the initial start-up and the configuration is complete [3]–[5]. The file transfer and configuration system that was described above was shown in Figure 2-4.

2.3.3 Benefits of SCL

SCL engineering is used by engineers and utilities to best suit the user’s requirements and by extension the requirements of the substation [3]–[5], [7]. SCL allows offline configurator tools to produce the necessary files needed for the configuration of IEDs automatically, purely based on the specifications of the designed power system [5], [7]. This means that there need not be a connection to the IED network for IED client configuration. This has significant cost advantages and eliminates the manual labour required for manual IED configuration tasks. In addition to setup, SCL also allows the distribution of IED configurations among vendors which makes this language somewhat generic [3]–[5], [7].

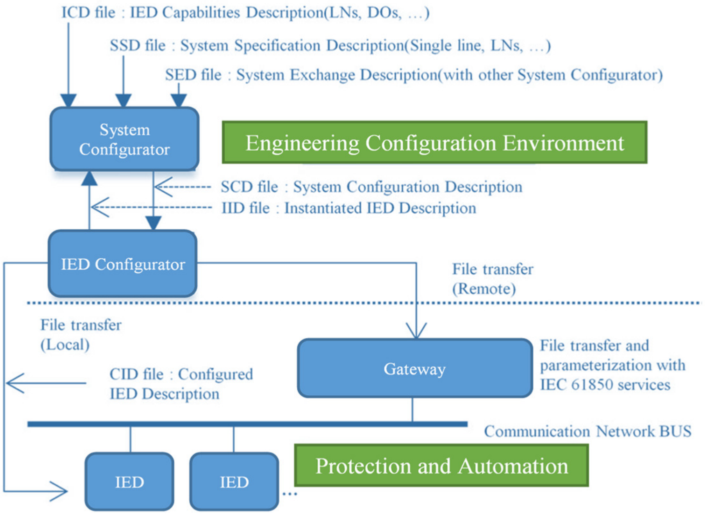

ICD file : IED Capabilities Description(LNs, DOs, …)
SSD file : System Specification Description(Single line, LNs, …)
SED file : System Exchange Description(with other System Configurator)
System Configurator
Engineering Configuration Environment
SCD file : System Configuration Description
IID file : Instantiated IED Description
IED Configurator
File transfer (Remote)
File transfer (Local)
CID file : Configured IED Description
Gateway
File transfer and parameterization with IEC 61850 services
Communication Network BUS
IED
IED
…
Protection and Automation

Figure 2-4. SCL file configuration [5]

2.4 The impact of IEC 61850 on protection and substation design

In this section of the review paper the authors divide substations into three categories, namely: conventional, station bus as well as station and process bus-based architectures. The literature reviewed in papers [2] and [8] discussed the design and simulation of fast substation protection in IEC 61850 environments as well as the architectures on which this protection is based. The IEC 61850 standard affects not only the design of a substation but almost every component and system in it [8]. Hence, this standard has been implemented slowly by adding IEC 61850 station bus and process bus-based communication solutions gradually over time.

2.4.1 Conventional substation design

The conventional legacy-based approach for designing substations involves the inefficient, costly and labour-intensive use of copper as a medium for serial communication between primary and secondary equipment [2], [8]. The substation networks that rely on this copper hardwire interconnection of equipment include analog communication links between relays and instrument transformers, binary inputs and outputs (which denote protection and control signals) as well as power supply circuits for both AC and DC components [2], [8].

In the 1960s Data Acquisition Systems (DAS) were installed as digital communication architectures began to develop [7]. This type of communication was bandwidth limited and was designed to operate on low-bandwidth communication paths to minimize the amount of data that was transferred whilst still providing the necessary functions to the substation automation system [7]. In summary, legacy-based protection and control systems within a substation have mostly determined how bytes of information and data can be transmitted on a copper wire [2], [7]–[8]. This method of sending data was hence referred to as a serial link technology [7], [8]. Thus, the cost to optimize, install and maintain these primitive substation models was and is great. The diagram illustrated in Figure 2-5 denotes the conventional layout for a typical legacy-based substation architecture.

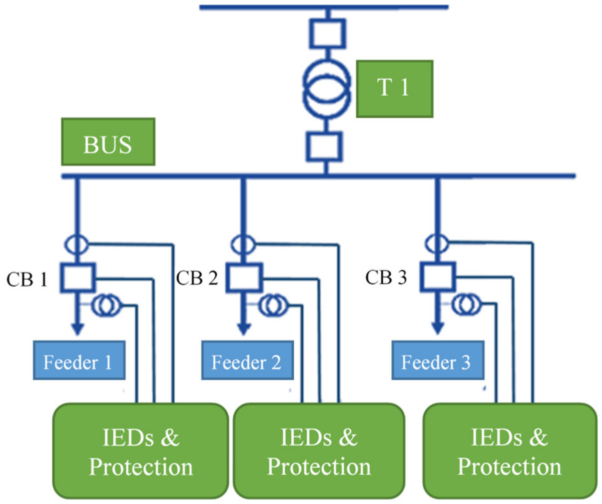


Figure 2-5. Conventional substation architecture [8]

In the design of a conventional substation, such as that shown in Figure 2-5, there is a large number of copper cables of various diameters and spans, regardless of the size of the substation [8]. This means that the maintenance, installation and testing of these cables is considered a nightmare. A conventional substation may have a considerable number of measurement transformers and breakers which are paired with other control, protection and monitoring devices housed in the switchgear panels in the control room [8]. Therefore, the copper cables and other hardwire connections must run from the equipment in the outdoor yard through cable trenches to the control room. These cables are usually bundled together according to their function and sectioned to the required length [8]. Hence, this procedure is considered to be very labour intensive and is especially tedious when there is a fault and a particular cable needs to be replaced or maintained [8]. Hence, there are certain risks and concerns that arise from copper hardwire connections between primary and secondary equipment within a conventional substation, these concerns include but are not limited to [8]:

- The impact of electromagnetic transients that occur as a result of the distance the copper cables cover.
- The damage of cables due to equipment failure.

- The damage of cables or insulation due to construction and or other related works.
- Copper cable theft.
- Lastly, the resistance of the chosen copper cables must also be taken into consideration when selecting the appropriate instrument transformers and the relevant protection equipment.

2.4.2 Station bus-based architecture

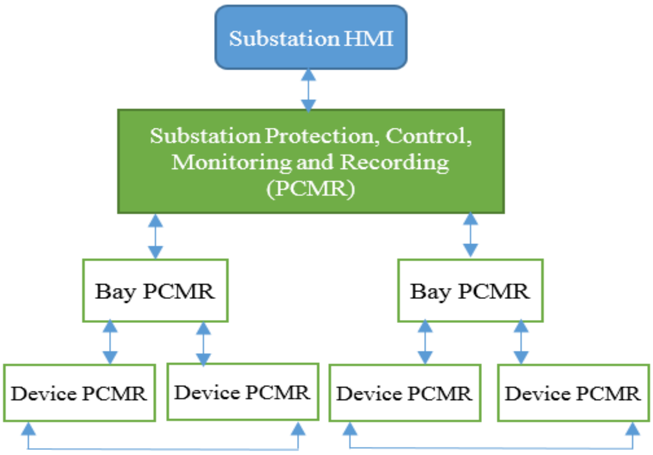


Figure 2-6. Station bus-based architecture [8]

The station bus-based architecture demonstrated in Figure 2-6 only represents a partial implementation of the IEC 61850 protocol. In this case the PCMR (protection, control, monitoring and recording), that occurs at the bottom of the substation functional hierarchy, is conventionally hardwired using copper cables [8]. However, the system in Figure 2-6 still offers certain advantages over conventional substations in making a partial transition to IEC 61850.

A conventional substation requires a large number of cross-wired binary inputs. In some substations, one may encounter a large number of feeders connected to the same medium voltage bus [8]. This means that the number of available relay inputs and outputs of the IEDs could present a limitation to the designer and to the flexibility of the protection scheme. An example of this can be explained when one considers the overcurrent blocking principle [4], [8]. This principle seeks to prevent the needless, callus and problematic tripping of unfaulted feeders [4], [8], [10], [19].

In typical legacy-based substations the overcurrent relays are configured in such a manner that the circuit breaker closest to the fault trips first which minimizes the extent of the affected area i.e. a smaller portion of the circuit experiences an outage [8], [4], [10]. This is achieved by correctly setting the time response logic of the relays/IEDs. In a conventional substation that uses hardwire interfaces the relay or IED that senses the fault current and issues the trip signal will have to apply a signal on the inputs of the relays on all the other adjacent feeders for a certain period of time to ensure that they do not needlessly trip [8]. This means that the number of interconnections between all the feeder relays as well as the number of relay inputs and outputs can be very large. This is especially true if there are for example 16 feeders connected to a particular bus [4], [10], [19].

The same blocking principle, also referred to as sympathetic trip protection, is relatively straight forward to implement using the IEC 61850 protocol [3], [4], [10]. In this case the IED that detects the feeder fault can send a Generic Substation Event (GSE) message over the substation local area network to all the other IEDs that are connected to the distribution bus, provided that these relays subscribe to the message stream and can then receive the appropriate information [4], 19]. This GSE message would indicate that a particular IED had tripped, cleared the fault and would act as a blocking response to all the other affected relays [4], [10]. The GSE message is sent continuously using a repetition mechanism until a new change of state occurs requiring a different message [4]. The transmission time of data between two functions in an IEC 61850 Ethernet-based architecture is also much faster than in a conventional substation taking only 0.25 cycles as opposed to 0.75 cycles for legacy-based systems [4]. Thus, equipment can be protected faster and more efficiently.

The major advantage of the IEC 61850 standard lies in the user's ability to make easy changes whether this means changing the IEDs themselves or downloading software updates [2], [3]–[6]. In legacy protection systems replacing and maintaining cables can be very time consuming and costly, whereas in an IEC 61850 Ethernet-based environment the IEDs can be reconfigured very easily using SCL-based engineering tools for the configuration of settings and peer to peer communication between devices on the virtual substation LAN [2], [3]–[6].

2.4.3 Station and process bus architecture

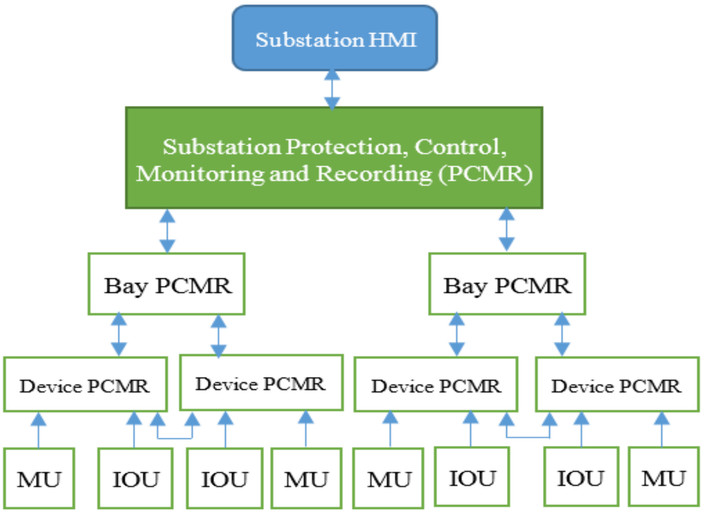


Figure 2-7. Station and process bus architecture [8]

The full advantage of the IEC 61850-based communication mechanism may be realized, in a station and process bus-based architecture as was shown in Figure 2-7. This involves several different smart devices, IEDs and pieces of equipment that are connected to the substations local area network [8]. In the figure illustrated on the previous page the MU processes the inputs from the instrument transformers and produces sampled values of the incoming three-phase currents and voltages [2], [4]–[8]. In addition, the MU formats and digitizes this sampled information and sends it to the other electronic devices that are connected to the substations LAN [8]. Another device called the input/output unit (IOU) processes the status inputs, generates status data, formats communication messages and forwards this information onto the substation LAN [3], [4]–[8]. The IEDs and related smart devices then receive the multicast information on the network in the form of sampled value messages or status messages. Importantly, only the IEDs that have been configured to accept and receive this data can then decide upon the appropriate and necessary actions that are required [8]. In the case of a fault, an IED will issue a trip signal by sending a GSE message to the relevant IOU which may then trip the appropriate circuit breaker [2], [3]–[8]. Hence, relays and IEDs within the substation must subscribe to receive certain messages and information from the network. The system demonstrated in Figure 2-8 shows a simple example of an IEC 61850-based architecture as was described above.

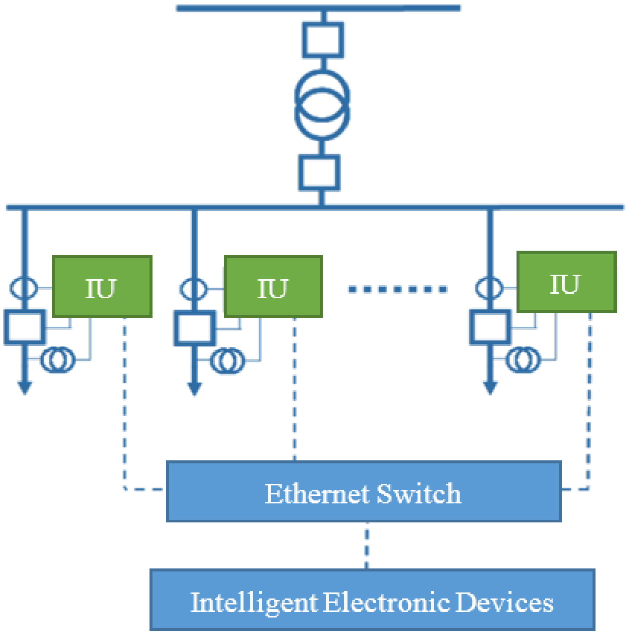


Figure 2-8. Complete Implementation of IEC 61850 [8]

The benefit of the implementation of the IEC 61850 protocol ensures that all the copper cables that are used to connect devices like instrument transformers and IEDs are replaced by fibre optics or Ethernet, merging units and the process bus [4]. It is also possible to optimize and reduce the number of voltage transformers needed within the substation using this system since voltage information can be broadcast as SV messages on the substation LAN to all the electronic devices that need it [4], [8]. This means that it is not necessary to have a voltage transformer on each outgoing feeder, but perhaps just on the busbar from where the information can be distributed to the other IEDs that need it over the local area network [8]. This optimisation applies to the voltage measurements that are needed by distance protections [8].

2.5 Substation automation

Substation Automation (SA) allows a utility to remotely control, switch, monitor and coordinate certain elements of a substation. These elements include: IEDs, Remote Terminal Units (RTUs), human machine interfaces and related devices or systems which protect equipment as well as monitor and control the flow of power within a substation [6]–[7], [9]. The authors of papers [6], [7] and [9], discussed the implications of the IEC 61850 standard on substation automation. The reviewed literature studied the architectures that defined how IEDs and other devices were arranged in a substation for the collection of data and the automatic protection of substation equipment.

In a substation automation system, the communication of data and the exchange of information is considered very important in order to realize certain automation functions. This communication refers to that between different IEDs as well as to and from a control centre and the remote substation. The current and aging protocols for this data communication include Modbus, Modbus Plus, DNP 3.0 and IEC 60870 as well as Utility Communication Architecture 2.0 (UCA) [6], [7]. These communication standards have their own technical short falls; the biggest of which that none of them fully deliver interoperability between IEDs of different manufacturers. For example, Modbus and Modbus Plus were originally developed for serial RS485 and RS232 and were never fully optimized for TCP/IP Ethernet communication [4], [6], [7]. Thus, the internationally accepted IEC 61850 communication standard was developed by the IEC based on the inputs, objectives and goals of utilities, engineers and manufacturers alike.

Substation automation exists to achieve switch control, data monitoring and protection [6]. The IEC 61850 standard segments these areas into sub-functions which are performed by an IED from within the substation. This set of sub-functions conglomerate to form the overall substation automation function where communication exists over the substation LAN and by extension, over the internet [7], [9].

2.5.1 Automation architecture

As was discussed in section III, the sub-functions that reside within an IED are referred to as logical nodes. IEDs or logical devices can typically hold multiple logical nodes, each of which has an object class which is commonly referred to as the logical node class [6]–[8]. A typical example of this is the “XCBR” logical node class which is for monitoring and controlling the operation of a circuit breaker [6]–[8], [17], [18]. In addition, these logical node classes each contain supplementary data classes that have their very own attributes. Therefore, these data class attributes can be used to determine, monitor and control the position of a particular breaker within the substation [17], [18]. Importantly, the functions or logical nodes like “XCBR” are assigned and exist at three different levels in a substation, namely: process level, bay level and station level which are graphically represented in Figure 2-9 [6].

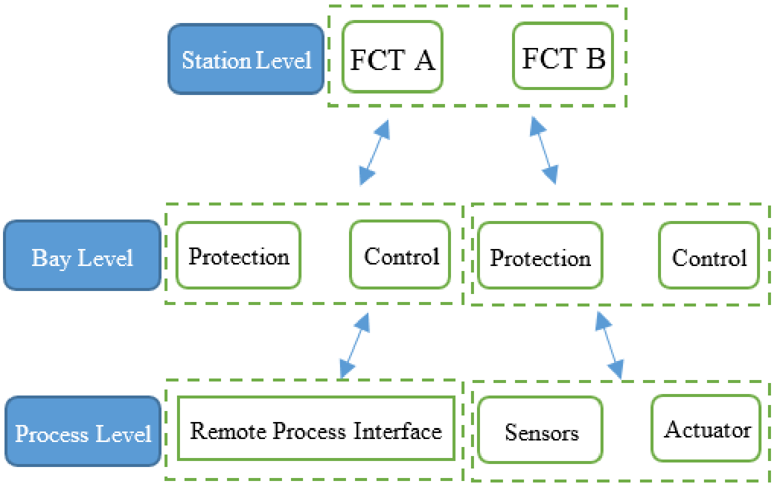


Figure 2-9. IEC 61850 substation levels [6]

The following bullet points refer to the three formal definitions of the process, bay and station level functions that were graphically described in Figure 2-9 [6]-[8], [17], [18]:

- Process Level Functions: take data from sensors or transducers within the substation and send them to bay level devices. They may also receive control commands from bay level devices and carry out the appropriate actions. Devices that occur on the process level may include instrument transformers, circuit breakers and merging units.

- Bay Level Functions: take data from and to the bay level and act on the equipment within the bay itself. The concept of bay levels is shown in Figure 2-10. Here each grouping of related equipment between two voltage levels or between different substation functions is called a bay. Control, monitoring and protection IEDs are devices that occur on the bay level.

- Station Level functions: these can be broken down into two types, namely: process functions and interface functions. Process related functions use data from many bays or databases. They submit control commands and collect the sensed data, such as analog or digital voltage and current values from bay level devices (IEDs). Interface related functions include human machine interfaces via remote monitoring and control centres for monitoring and maintenance. Therefore, interface related functions refer to the relationship between the substation and the user.

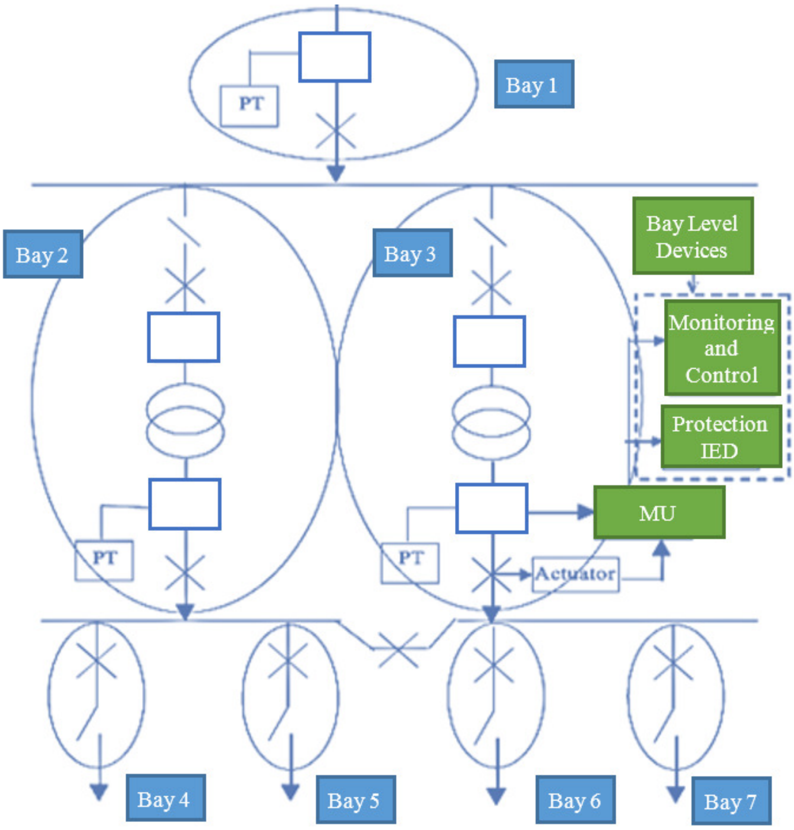


Figure 2-10. Conventional substation bays [6]

In the IEC 61850 standard and across the three aforementioned functional levels there exists over 90 logical nodes or sub-functions [7]–[9]. The communication between these 90 logical nodes takes place using the shared physical connection that is provided by the 'virtual' Ethernet or optical fibre-based substation LAN. In a substation, each network switch on the LAN forms part of a network node [7]–[9].

2.5.2 Automation equipment and automation systems

There are two main categories of equipment within a substation, namely primary equipment which includes transformers and switchgear as well as secondary equipment like protection, control and communication devices [8]. In the IEC 61850 protocol, secondary equipment is broken down into equipment for the station, bay and process levels respectively. Human Machine Interfaces (HMI) and Communication Units (ComU) which link to the Master Control Centre (MCC) occur at the station level and are connected to bay level devices via the station bus [6]. A few examples of station level equipment may include the station computer and database, the operator workspace and remote communication interfaces. Bay Level equipment, on the other hand, consists of control, monitoring and protection equipment whereas process level equipment includes sensors, actuators and remote inputs and outputs [6]. Naturally, bay level devices communicate with process level equipment via the process bus and station level devices communicate with bay level devices using the station bus [6]. This communication via station and process buses is realized via Ethernet or optical fibre communication links which eliminate traditional hardwire connections between equipment [6]. In addition, the process bus ensures that there is an expedient exchange of tripping commands between IEDs and switchgear as well as the swift transmission of SVs via the MU that occurs over the LAN [6].

The station bus is created using a mutli-port Ethernet switch which prioritizes and forwards packets of information between nodes [6], [8], [17]. Typically, the HMI and the substation router, which enables remote communication with the MCC, are connected to the switch at station level [6]. If a station level device needs to send a message to a bay level device it will send a message through the Ethernet switch [6], [8], [17]. The bay level device then completes its function based on the received message and forwards the necessary information to the process level via an MU [6]. Hence, the final action is performed by the process level device.

2.5.3 Communication architecture

Communication services within and between station, process and bay levels may be referred to as horizontal or vertical communication mechanisms [6], [9], [17]. This type of communication seeks to decentralize the substation communication system and reduce the tedious copper wire communication links that plague legacy systems. These concepts are shown graphically in Figure 2-11 and 2-12 respectively. Vertical communication typically takes place between station level and bay level devices where information is directed vertically [6]. In addition, Vertical communication is related to the human interaction and operation of the substation and is hence a Client-server based system [9], [17]. This type of communication includes any instructions from the operator (human interface) as well as measurements from CTs and VTs and isolator or breaker positions. It therefore involves [6], [9]:

- Establishing dialogue with the substation SCADA
- Reporting of information between bay level and station level elements
- Sending of commands, control and signals
- File transfer and data acquisition
- Dealing with events and alarms
- Operation of the substation switchgear and high voltage equipment

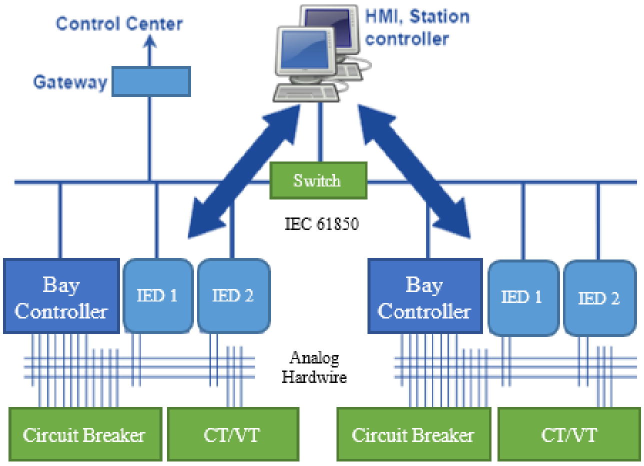


Figure 2-11. Vertical communication architecture [6], [9]

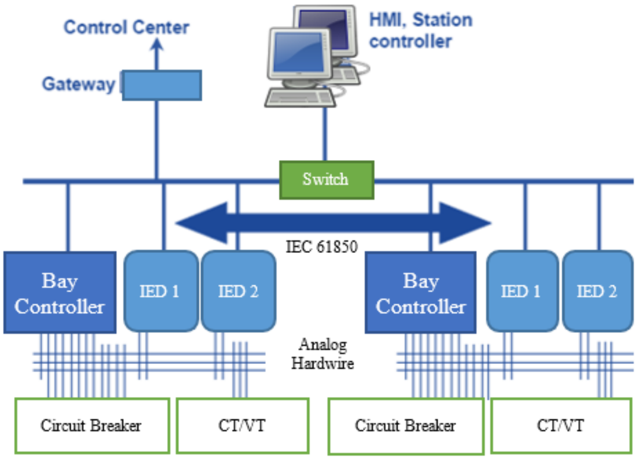


Figure 2-12. Horizontal communication architecture [6], [9]

Horizontal communication may be achieved using copper hardwiring or serial communication between devices based on the requirements or preferences of the designer [6], [9], [17], [18]. However, today an Ethernet-based interface is used in IEC 61850 and other TCP/IP protocol-based substations. The horizontal architecture shown in Figure 2-12 deals with the transfer of information and data between bays and with the exchange of information or data between certain elements or functions at the bay level [9], [17]. The horizontal communication architecture used within a substation, as described in Figure 2-12, is used for but not limited to [6], [9], [17]:

- Interlocking
- Data/information exchange between the line protection and the recloser

In addition to IEC 61850 compliance on the station and bay levels, process level devices, such as switch gear and instrument transformers, may also satisfy the requirements of an IEC 61850 architecture. A design of this nature seeks to replace the analog hardwire connections between the IEDs on the bay level and the CTs, VTs and circuit breakers on the process level respectively. The hardwire method for connecting process and bay level devices was shown in Figure 2-11 and in Figure 2-12. In this model, the conventional process level CTs and VTs communicate via serial point to point communication links to the IEDs as well as with the bay controller on the bay level [17], [18]. Figure 2-13 shows how modern switchgear can be installed in the place of legacy equipment, allowing process level devices to communicate with the bay and station level devices over IEC 61850 communication links further reducing the analog hardwire connections within the substation [6], [9]. Therefore Figure 2-13 shows an example of how a substation can use the full functionality of the IEC 61850 protocol. However, typically utilities will pick and choose the stages of the protocol that they wish to implement within a hybrid substation. A similar network to that shown by figure 2-11 and 2-12 was developed during the course of this study in chapters 4 and 5. IEC 61850 communication was achieved both horizontally and vertically between IEDs.

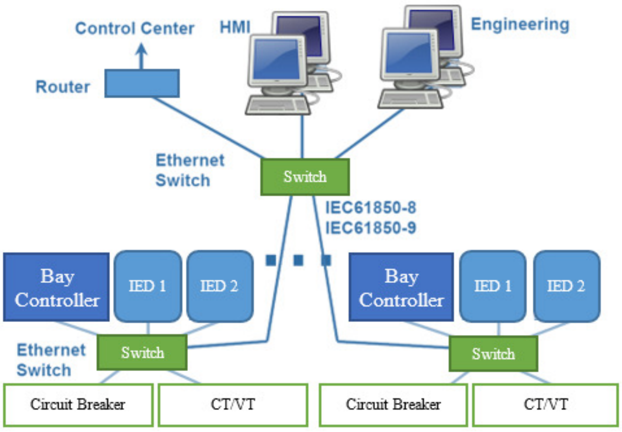


Figure 2-13. IEC 61850 Communication Network [17], [18]

2.6 The impact of the IEC 61850 protocol on protection systems

The following chapter describes fast bus tripping, reclosing and breaker fail protection and how these concepts relate to control, protection, monitoring and automation within a substation. Hence, this section of the paper seeks to describe how the IEC 61850 protocol uses an Ethernet-based communication system to accomplish and improve traditional protection schemes. In the following sub-sections, the authors discover how the GOOSE message class is typically used over the substation LAN and between the station and process buses to replace the copper hardwire connections between IEDs within a substation. Therefore, the authors present a short discussion on what the IEC 61850 protocol can and cannot offer to traditional protection schemes.

Furthermore, the aforementioned schemes can be grouped into two main categories, namely: protection and automation that requires inter-IED message exchange within the internal environment of a particular substation and protection schemes that require inter-substation (external) communication. The authors discussed the first concept in more detail in the following subsections.

2.6.1 Fast bus tripping

A fast bus tripping scheme is also typically referred to as reverse interlocking [4]. The purpose of this scheme is to decrease the clearing time of different bus faults on radial distribution systems [4]. Hence, a fault on a particular bus must be cleared within a certain critical amount of time before the system goes unstable or equipment is badly damaged by a sharp current or voltage disturbance. An example of a fast bus tripping scheme by GOOSE was demonstrated below in Figure 2-14.

In Figure 2-14. the bus IED that is at the top of the substation hierarchy communicates with each of the IEDs connected on the three feeders below [4]. This means that if a fault or disturbance occurs on a particular feeder then the IED on that feeder will issue a GOOSE blocking response to ensure that the bus IED does not needlessly trip [4]. This GOOSE message can be retransmitted to ensure that the relevant IEDs have received the required information. Additionally, only those IEDs that have subscribed to the message stream may interpret the relevant data. Alternatively, if a fault occurs on a bus section then the feeder IEDs are not aware of it and therefore, do not prevent the bus IED from tripping [4]. Hence, the bus IED may trip as and when is required using its fast trip protection elements and the GOOSE message class to clear the fault within the appropriate time frame [4]. Thus, a typical fast bus trip protection scheme was shown in Figure 2-14. This diagram represents an example of an inter-IED communication system by utilizing the IEDs physical inputs and outputs or the process and station buses to transfer fault information within the substation.

During the course of the study conducted in Chapter 4 and 5 of this study fast bus tripping was implemented during GOOSE for blocking-based protection as well as for traditional protections under fault conditions. The subscribing devices could communicate and administer protection effectively by accessing the control functional blocks of the required IEDs in the protection zone.

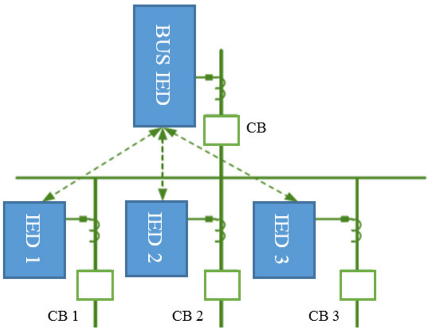


Figure 2-14. Radial feeder and fast bus tripping scheme [4]

2.6.2 Reclosing

Newly developed IEC 61850-based IEDs have become commercially available from companies like ABB, Schneider and SEL. These manufacturers will commonly include many protection, monitoring, automation and control functions such as reclosing and breaker fail protection within their IEDs [4], [20]. Typically, these IEDs possess sophisticated control structures for up to two circuit breakers. Hence, the aforementioned structures can be utilized to control and monitor equipment in breaker-and-a-half and ring bus protection schemes respectively [4], [20]. However, in most cases a power utility or design engineer will choose to use a single exclusive IED to perform the reclosing function or for breaker fail protection within a substation [4], [20]. This means that a particular IED is assigned only one job. An example of line reclosing is shown in Figure 2-15.

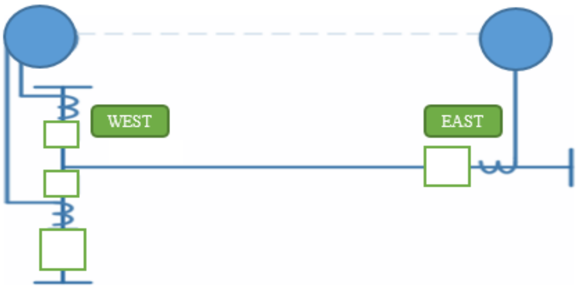


Figure 2-15. Line Reclosing [20]

Challenges on transmission systems and within substations are not only limited to clearing faults, but include the restoration of services after the circuit breakers have opened [4], [20]. How a particular circuit breaker is restored can have a significant impact on the circuit breaker itself as well as the on the associated power system to which it is connected. The process of restoring a circuit breaker to its close position is referred to as reclosing [4], [20]. Current differential relays are equipped with autoreclosers for each circuit breaker and binary information can be communicated between the relays [4], [20]. An example of line reclosing is shown in Figure 2-15. Here the relays communicate between remote ends which allows each breaker to reclose safely. If breaker 1 closes first a signal is send to the west remote end specifying a successful reclose [4]. Breaker 2 and 3 can then close one at a time, after a certain time delay, provided a successful reclose occurs in each instance [4], [20]. This method of reclosing reduces the stresses on the breakers if the fault resurfaces.

Reclosing takes place when a signal from a traditional protection IED activates an exclusive reclosing IED via a hardwire link or physical inputs and outputs in a conventional substation [4], [20]. However, the communication for reclosing within modern substations takes place over the LAN using IEC 61850 GOOSE messaging or other related protocols. Apart from simply replacing the hardwire communication links between devices, the IEC 61850 GOOSE message system also monitors the health of the 'virtual' wiring [4]. This helps to avoid a situation where a failed device is not noticed until it is called upon to protect a particular piece of equipment [4], [20].

2.6.3 Breaker fail protection

Breaker fail protection is commonly required in combination with reclosing and most IEDs will typically have an inbuilt breaker fail protection function. This protection works using a timer that activates once an IED has issued a trip signal. In addition, as the timer ticks the IED monitors the current through the circuit breaker [4], [19]. This means that if the breaker current is not completely interrupted the relay will issue a second trip signal or alternatively trip the neighbouring breakers to isolate the faulted circuit [4], [19]. Alternatively, a separate dedicated IED may be used for breaker fail protection of a particular bay. This enables the system to incorporate monitoring and control functions like gas pressure and ambient temperature supervision when using a dedicated breaker fail protection IED [4], [19]. The control and trip signals may be exchanged using the IEDs physical inputs/outputs and traditional hardwire interconnections. However, once again, the IEC 61850 protocol allows for the fast, reliable and secure exchange of GOOSE messages over the substation LAN. This allows breaker fail protection to be carried out 'virtually' over an Ethernet or optical fibre local area network and for trip signals to be retransmitted as and when is needed by the IEDs. Breaker fail protection was effectively implemented in this study in the network shown in Chapter 5.

2.6.4 Protection schemes requiring inter-substation communication

The present scope of the IEC 61850 protocol is limited to the protection, control and monitoring of equipment that takes place exclusively within a substation [4]. However, the IEC is currently working on developing their protocol further such that inter-substation IEC 61850 communication can be realized. There are a number of protection schemes that require information from surrounding substations and could benefit from an IEC 61850 architecture in the future [4]. These protection schemes include but are not limited to: directional comparison schemes and line current differential schemes [4].

Until such a time that the IEC 61850 standard has developed to allow for the transmission of GOOSE messages over a public wireless area network (WAN), the aforementioned protection schemes will remain relatively unchanged [4]. Currently, one of the known methods for establishing a secure channel through WAN is to use Ethernet tunnelling using a virtual private network (VPN) [4]. However, even with Ethernet tunnelling the existing GOOSE message system is still not good enough for current differential protection which relies on a constant stream of current values [4]. Therefore, the future development of inter-substation communication using the SV message class would be required to expedite this type of protection using the IEC 61850 protocol [4].

2.7 Cyber vulnerability

Cyber-physical devices are Ethernet or optical fibre-based IEDs that communicate over the substation local area network as well as using cloud computing on the internet. This makes protection IEDs, and by extension substations themselves, susceptible to cyber-attacks by both criminals and terrorists alike. The authors of paper [2], which discussed the design and implementation of fast substation protection in IEC 61850 environments, proposed an innovative solution that sought to protect different IEDs within a substation against cyber criminals. An attack on an IEC 61850-based substation and its associated systems occurs when the hacker injects false, but syntactically accurate measurements in the GOOSE or SV message streams which tricks the network into accepting them as friendly code [2]. Thus, a cunning defence is needed to ensure that the expensive, vital and vulnerable equipment within a substation is not corrupted.

2.7.1 Cyber attacks

Cyber-attacks may be carried out using different mechanisms and or catalysts to ultimately damage or impede a protection system. The different cyber-attacks that are of concern to IEC 61850-based networks include, but are not limited to, the following items [2]:

- A deliberately malfunctioning MU can be forced to deliver a false SV message that tells an IED that a fault current is present when in fact none exists. This means that the relay could needlessly issue a trip signal if it has subscribed to that particular SV message stream.
- Additionally, a deliberately malfunctioning MU can deliver a SV message that hides the presence of fault current when it is in fact present. This means that the power system/substation could operate in a potentially dangerous state causing damage to equipment, outages or danger to human life. The time-current logic of an upstream relay would eventually trip and clear the fault. However, the damage to the system would be minimized if the primary protection had operated within the necessary time frame.

The faults that occur within a substation may arise as a result of hackers tampering with sensitively calibrated equipment, messages and code, or intentionally introduced by mechanical and or other related means [2]. Hence, a system fault and the damage caused to equipment within a substation may be opportunistic if the cyber-digital attack is the primary mechanism [2].

Alternatively, the hacker may intentionally introduce a fault by mechanical or physical means and then finally he/she may deliberately impede an IEDs ability to clear the induced fault [2].

2.7.2 Preventing attacks

In order to protect IEC 61850 Ethernet-based devices from cyber-attacks the IEDs must be configured to collaborate with one another so that they are all able to agree on the presence of a fault condition and whether or what the appropriate corrective actions (breaker trip) should be [2]. An ideal cyber defence would be for the protection to identify a certain number of incorrect or tampered measurements within a particular GOOSE or SV message stream [2]. Hence, the conglomerate of interconnected IEDs would be required to receive and analyse the SV measurements from their peer relays and MUs, compare these to their own measurements and then lastly apply Kirchhoff's Voltage and Current Laws (KVL and KCL) to determine whether or not this information is valid and accurate [2]. Upon the detection of an invalid or false measurement is it imperative to identify the malfunctioning IED so that it can be replaced or reprogrammed [2]. This method of cyber defence was based on a ring bus or loop circuit as was shown in Figure 2-16.

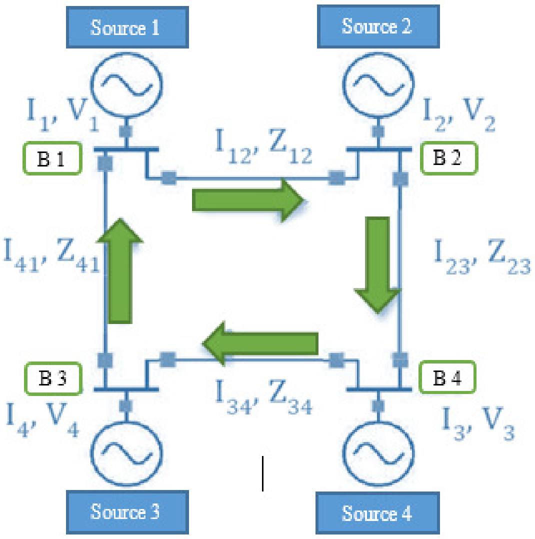


Figure 2-16. 4-generator, 4-bus loop [2]

In Figure 2-16 the current and voltage at and between each of the buses, as well as the complex impedance between the busses, was denoted according to the bus number as was shown. Therefore, the above system could be solved mathematically by an IED using the KCL and KVL rules in order to check that the sensed and received SV or GOOSE information is indeed correct [2]. As a result of the technological advancements of Ethernet-based cyber-physical IEDs as well as the implementation of the IEC 61850 protocol the threat of a serious and damaging cyber-attack on substations is ever growing [2].

2.8 Backup IEDs for IEC 61850-based protection

IEDs fulfil an integral, vital and fundamental aspect of IEC 61850-based communication, monitoring, control and protection within a substation. In conventional legacy-based protection schemes the consideration and implementation of backup devices for IEDs has been infrequent [5], [19]. However, the authors of paper [5], which investigated the design of backup IEDs for IEC 61850-based environments, realized that —in modern substations— the need for backup IEDs has grown exponentially and become a prerequisite for many utilities. Backup protection for older legacy-based IEDs was not widely considered due to the fact that these devices only used data local to the relay itself [5], [19]. Additionally, there were certain limiting factors within conventional substations that emerged as a result of their hardwired point to point communication links between legacy-based relays. Hence, and furthermore, because of the IEC 61850 protocol the removal of copper hardwire connections within substations has become a reality. This is providing a better medium for backup IED protection simply because of the introduction of virtual Ethernet or optical fibre-based communication channels like the substation LAN.

2.8.1 Methods of backup protection

The current and preferred method for backing up IEDs that operate within IEC 61850-based environments uses a technique that activates an identical backup IED in the case of a malfunction or misoperation [5], [19]. This method of backup protection requires a very large number of IEDs (essentially double) because each and every IED within a substation needs to have an identical backup device [5], [19]. A disadvantage of this strategy arises when both the backup IED and the protection IED fail at the same time [5]. This means that there is no protection until both or either of the IEDs is restored [5].

Primary protection equipment and backup IEDs also require a rebooted if any of the IEDs configuration settings or protection parameters have been changed [5]. Hence, the system is without backup or primary protection for this initial start-up period [5]. The reboot time of a typical IEC 61850 IED is roughly 12 s, this period increases to 45 s if a file replacement or file update is required [5]. Hence, if an engineer or a substation technician makes a change to a particular IED the equipment may remain unprotected for up to 45 s [5].

The authors of paper [5] propose a method of protection that uses a single or fewer number of backup IEDs which contain every protection element within a substation. This means that a large number of IEDs can be covered or backed up by a single unit which waits for a particular IED to fail [5]. This reduces the number of backup IEDs that are required within a substation which naturally has various economic and technical advantages. In addition, the backup protection for one IED can be activated by the operator and can even be used as a second redundancy safeguard for another backup IED [5].

The IED that was proposed by paper [5] can be deployed to provide backup protection for any primary IED but not necessarily every single IED within a substation. Therefore, this method optimises the use of IEDs in a substation to a certain point. An additional benefit of this recommended method is that the suggested backup IED shortens the unprotected time of the system since it does not require any reboot or file update [5]. Hence, backup protection is virtually instantaneous. This means that the operation, reliability, security and efficiency of a substations protection can be improved and maintained [5].

The design specifications for the backup IED that was conceptualized in paper [5] consist of the following items:

- SCL-based activation using an SCD file.
- Continuous operation without reboot.
- Storage of all information, functions and logical nodes of every IED within a substation.

However, in contrast to the proposed backup IED in paper [5], the IEC 61850 protocol prescribes that a protection IED use a CID file for backup protection. Therefore, the protection IED in question should receive the CID file from the IED configurator and parse this file to obtain the information about the particular IED that it backs up. The reason the recommended IED in paper [5] uses an SCD file is because here the authors are attempting to back up more than one IED using a single device. This means that an SCD file is required because the backup IED needs access to all the information describing every device that it covers within a substation [5], [19]. The backup IED can therefore change its protection settings as well as its configuration characteristics without a reboot [5].

2.8.2 Applications of backup IEDs

The first method of backup protection, as was previously mentioned, ensures that any IED in an IEC 61850-based environment uses an identical backup IED as a potential safeguard. This can be described as having one primary and one backup device [5]. The, aforementioned, IEDs would then operate according to the same protection target and thus have the same protection settings. However, in the second proposed method for backup protection, one or more IEDs can be used to back up a much larger number of devices [5]. Hence, the backup device is loaded with all the protection elements of every device that it seeks to cover. Naturally, a particular backup IED is applied until the malfunctioning IED has been restored or replaced. The recommended method in paper [5] states that a conventional system of fourteen IEDs can be optimized to use only seven primary IEDs with as few as two devices required for backup (instead of the same number of primary IEDs) [3], [5]. Hence, this system has a significant economic advantage over other more traditional IED backup protection methods due to its efficient redundancy measures.

2.9 Implications of modern relays on protection design

Modern microprocessor-based relays have changed the way substations are designed and the manner in which IEDs communicate with their peers in order to operate, monitor and control circuit breakers, reclosers and related equipment. The need for high speed communication links between these new intelligent devices has given birth to Ethernet-based protocols like the IEC 61850 standard. Naturally, protocols such as this have different implications, benefits and advantages for the way in which protection schemes can be devised and implemented.

A number of the following modern protection mechanisms use the new IEC 61850-based communication standard as is shown in the included diagrams, Figs. 2-17 to 2-23. The subsequent sections of research were based on paper [20] which discussed certain perspectives of substation design whilst at the same time considering the impact of modern relays. The authors explored various power systems, protection structures and the associated communication links that are used to connect the IEDs that control circuit breakers, reclosers and other electrical equipment [20]. These design systems include line protection, impedance protection, bus protection and protection on transformers as well as feeder design — to name but a few.

2.9.1 Line protection

In electrical transmission systems, the section of infrastructure on which most faults occur is on a powerline [20]. Traditionally, powerlines span great distances which makes them susceptible to many physical dangers and vulnerabilities, like falling trees or lightning. Therefore, these dangers can cause or induce different fault conditions which may extensively damage equipment on a power system. The lengthy spans that electrical powerlines traverse also makes it difficult to detect faults along a long transmission line and open the relevant circuit breakers [20]. Conventional distance protections seek to provide instantaneous protection to a portion of a transmission line without relying too much on direct communication links along the length of the line itself [4], [20]. Alternatively, distance protection along the whole length of the line may rely on the singular exchange of digital information between IEDs so that they can clear or isolate any prolonged faults by activating the appropriate breakers [1], [20]. On the other hand, differential protection relies on the transmission of an analog signal from one end of a transmission line to the other [1], [20]. Essentially it uses Kirchhoff's Laws, to analyse current and voltage information at the sending and receiving ends, and decides whether or not a particular fault is present [20]. In general, the IEC 61850 protocol seeks to replace this transmission of analog data with digital SV messages over Ethernet communication links. Modern IEDs can issue trip signals and blocking responses using the GOOSE message class over these virtual communication channels [4], [20].

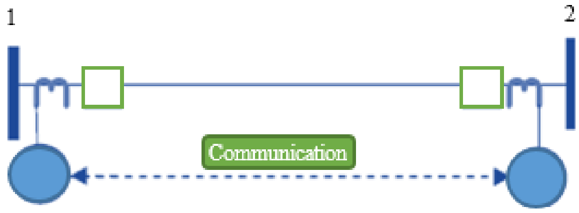


Figure 2-17. Two terminal line differential protection [20]

Figure 2-17 shows a typical line differential protection scheme with communication links for a two-terminal system. The IEC 61850 protocol could theoretically be used to implement the necessary communication links and facilitate the exchange of data between functions linking the line protection and the auto reclosers from two substations [4], [20]. Hence, the future development of the IEC 61850-based communication of data between IEDs, circuit breakers, reclosers and between substations at each end of the line can help to provide distance protection to powerlines. In a conventional system shown in Figure 2-17 pilot wire is used to transmit analog current information between either ends of the powerline [1], [20]. Line protection is not only limited to systems of two terminals but systems of, for example, five terminals may also exist as shown in Figure 2-18.

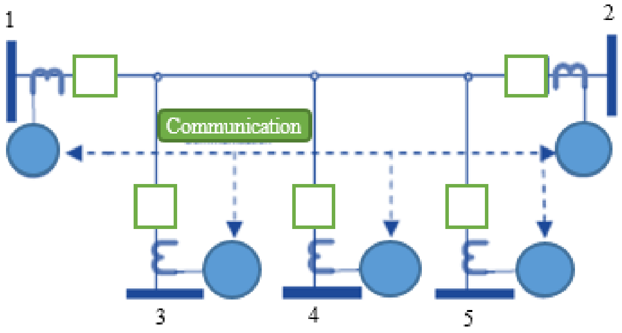


Figure 2-18. Five terminal line with differential protection [20]

In the theoretical system depicted in Figure 2-18, it is possible to trip all the breakers selectively for a fault that is internal to the system. There is a communication link between each of the terminals or buses from A to E [20]. This represents an intercommunication between substations where the IEC 61850-based architectures have been implemented. Here the IEDs local to the substations themselves received SV messages from instrument transformers and MUs and decide whether or not to trip certain circuit breakers and protect or isolate the transmission line [1], [20]. Inter-substation IEC 61850 communication is still being researched and developed by the IEC.

Digital communication over long distances is costly so analog to digital conversion may be employed at either ends of long lines giving way to optical fibre/Ethernet IEC 61850-based communication links within a substation itself.

2.9.2 Bus protection and current transformers

High impedance protection is commonly considered a very simple protection scheme since the feeder's CTs are wired in parallel and then connected directly to the relays in the control room [1], [20]. The first image, Figure 2-19, in the diagram below shows a high voltage substation bus that is protected using a form of high impedance protection. In this design, each of the feeders CTs has an identical CT ratio as well as a very low magnetizing current [1], [20].

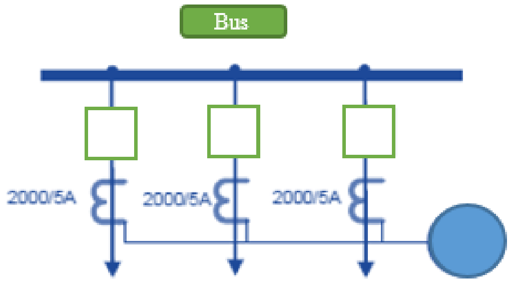


Figure 2-19. High impedance bus protection [20]

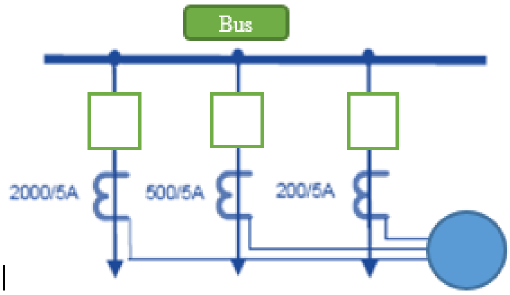


Figure 2-20. Low impedance bus protection [20]

In more advanced substations, which use intelligent electronic relays, it is common to use low impedance protection as is shown in Figure 2-20. This type of protection is more expensive, but can read the individual circuit current from each bay and implement the desired action [4], [20]. The benefits of this system may include fault recording, the generation of current waveforms, event sequencing as well as the different communication capabilities [4], [20]. One of the disadvantages of low impedance protection is that both the CTs and the CT arrangement of this type of protection is considered to be costly and presents more of an economic barrier to clients and engineers [1], [20]. In an IEC 61850 architecture the analog signals from the CTs are delivered to MUs which digitize the sensed information and forward it to the IEDs in the control room using SV messaging [4].

2.9.3 Transformer protection

A breaker-and -a-half scheme, also referred to as a ring bus system, requires that the CT ratio be decided by the measured value of the breaker's load current as opposed to the load current drawn by the transformer [1], [20]. This is an important consideration when protecting transformers. In Figure 2-21 the breaker CTs are 3000/5A as opposed to a load current of 500 A through the transformer [20]. The CT currents from the secondary winding act as inputs to the differential relays or merging units and the associated IEDs in an IEC 61850 environment. The relays then decide whether or not to issue trip signals to either or all of the circuit breakers connected to the protection zone [20].

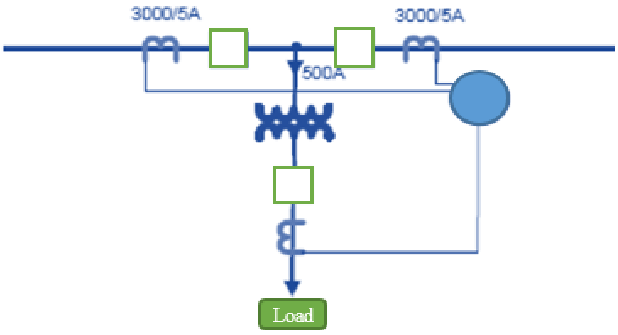


Figure 2-21. Dual breaker transformer protection [20]

2.9.4 Transformer feeder design

Modern IEDs and the new IEC 61850-based architectures have modified the way in which transformer feeders are designed and implemented. The diagrams in Figures 2-22 and 2-23 illustrate this concept visually.

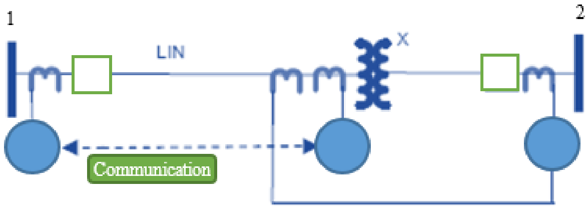


Figure 2-22. Conventional transformers feeder protection [20]

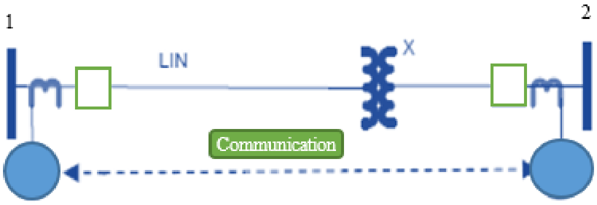


Figure 2-23. Modern transformers feeder protection [20]

The first diagram, Figure 2-22, shows a long feeder and transformer protection scheme. In this diagram, the buses 1 and 2 represent the source and load respectively. In addition, a CT is usually connected on the HV side of the transformer as is shown to avoid allowing the transformer and line to be protected by a single IED [1], [20]. This CT is then connected to line protection on one end of the line and the transformer protection at the other end [1], [20]. The line protection is typically either distance or differential protection with certain legacy-based communication links. In modern networks as shown in the second image, Figure 2-23, the intelligent relays or IEDs can send instantaneous information and SV messages across terminals using fast instantaneous digital communication links [4], [20]. This means that information is available in a transparent way and decision making for the IEDs is easy and simple. Additionally, in this system transformers need not be included in the zone of protection [1], [20]. Medium length lines can now be terminated on transformers with LV side breakers which saves cost and makes the design and implementation of such systems economically appealing [20].

2.9.5 Breaker-and-a-half schemes

In a breaker-and-a-half or ring bus scheme the CT currents are summed together by numerical means before the information is given to the distance or differential line protection element within a substation.

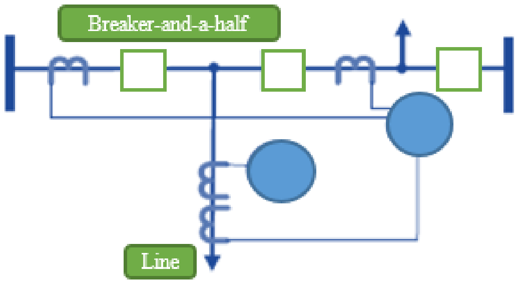


Figure 2-24. Conventional line protection [20]

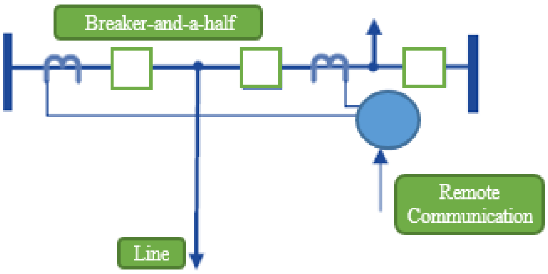


Figure 2-25. Modern line protection [20]

In line distance protection schemes the CTs are sized not to saturate. However, CTs may saturate due to a through fault across two breakers in a breaker-and-a-half scheme [1], [20]. Thus, as a result of this CT saturation, the summation of currents from the two CTs which is delivered to the protection is no longer accurate [1], [20]. Hence, an error in the operation of the system may occur. One solution to this was shown in Figure 2-24. Here an additional CT was included in the protected line [1], [20]. However, the latest IEC 61850-based numerical protection systems negate the inclusion of this CT and prefer to make use of saturation detectors in the case of differential protection. Alternatively, directional detection is used in each of the breakers for distance protection schemes [1], [20]. These concepts are captured in the Figures 2-24 and 2-25.

2.9.6 Transformer tap-off

Primary line protection is often compromised as a result of the presence of tap-off transformers along the transmission line [20]. This compromise is caused by the sensitivity issues and protection speed constraints that such devices pose. Most transformers are designed with a delta HV winding which provides zero sequence isolation for earth faults [1], [20]. This ensures good sensitivity and fast earth fault currents. The more modern Ethernet-based protection systems allow for multiple tap-offs along the power-line since they measure the current on the LV side of the transformer in a substation using the SV message class and can then communicate this information with both ends of the line [4], [20]. The concepts of conventional and modern transformer tap-off and line protections are captured graphically in Figures 2-26 and 2-27 respectively.

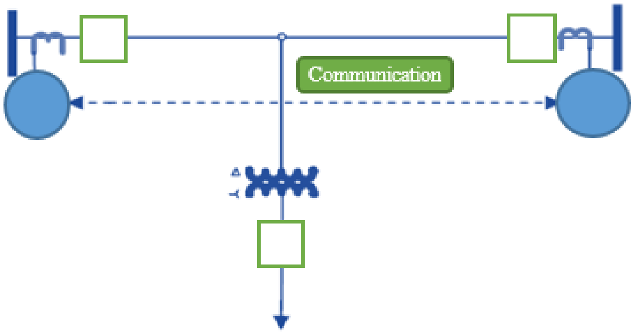


Figure 2-26. Tap-off transformer conventional protection [20]

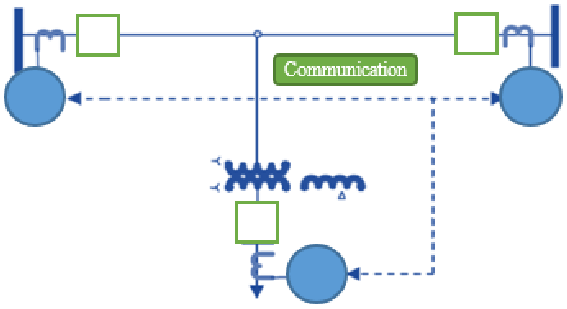


Figure 2-27. Tap-off transformer modern protection [20]

The communication links for the conventional tap-off protection schemes only occur between either ends of the powerline, however, in modern protection systems the IEDs communicate with either end of the line as well as with the instrument transformers connected at the tapping point [20]. This makes protection more reliable, secure and efficient.

2.10 Testing of protection schemes in IEC 61850-based substations

Protection engineers are required to check, test and commission IEDs, equipment and other related devices within a substation. This forms part of the installation and maintenance of instruments in order to ensure that they are functional and adequate. The unfamiliar and unaccustomed task of testing IEC 61850-based IEDs and their associated automation systems can be considered quite a new and abstract duty for engineers. Test equipment, in conventional legacy-based protection schemes, uses the analog, serial and binary inputs/outputs of IEDs to test associated protection functions. However, more advanced tools and test apparatus is needed for the technologically advanced virtual environments of today [11]. In the IEEE paper compiled by Omicron, the authors discuss the testing of protection systems in IEC 61850-based substations and highlighted a few of the specialized Ethernet-based testing techniques using Omicron test equipment [11].

A number of the substations that exist today are referred to as hybrids and have a mixture of modern and conventional protection equipment. In a hybrid substation IEC 61850-based IEDs can connect to and communicate with legacy-based devices through a communication gateway. The use of the IEC 61850 protocol and the extent to which this protocol is implemented within a substation depends on the particular municipality that has requested and implemented it [2], [7], [11]. Some utilities only use Client-server communication for SCADA systems and tend to ignore the GOOSE and SV message benefits of the protocol. Others utilities prefer GOOSE messaging and use it for items like breaker tripping and status information since the use of copper hardwire connections is minimized by introducing Ethernet-based communication links [2], [7], [11]. Therefore, protection engineers must often deal with substations that have a complex variety of different protocols and IEDs operating on the same network [11]. Hence, these hybrid substations combine both conventional protection architecture with virtual networks and digitized communication systems.

A few examples of the tests that engineers and manufacturers must carry out on different equipment within a particular substation may include but are not limited to: the type test of an IED, factory acceptance testing as well as commissioning and or maintenance. One of the methods for testing IEC 61850-based IEDs uses specialized test equipment to mimic either GOOSE, GSSE and SV messages [10]. An example of this technique was shown in Figure 2-28 which was illustrated below.

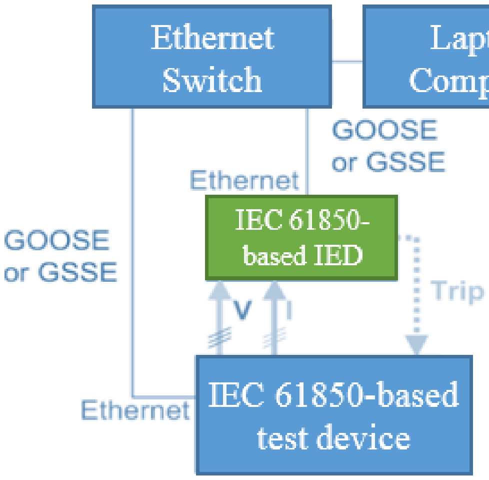


Figure 2-28. IEC 61850 GOOSE and GSSE message testing [10]

2.10.1 Testing wiring, continuity and connections

In a conventional substation —as part of the substations acceptance test— it is important for engineers to check that the cables that exchange information or signals between different IEDs are correctly wired [11]. This verification can be achieved using a simple multi-meter to check the continuity of the connected cables [11]. These checks ensure that the binary inputs of one relay are correctly wired to the binary outputs of another relay [11]. However, in an IEC 61850-based substation, where information is transferred through GOOSE and SV messages, a software approach must be taken to check that the "virtual" wiring between IEDs is adequate. Here the software monitors and may even broadcast GOOSE messages over the substation LAN and ensures that they have been received by the IED which has correctly subscribed to that particular message stream [11]. The tested IED should then react accordingly by enacting the appropriate function based on the received information.

2.10.2 Testing substation protection

IEDs, both old and new, are allowed a certain critical amount of time before an existing fault becomes detrimental to a power system and must be cleared. Therefore, this fundamental aspect of protection must be considered by engineers to ensure that the protection is operating as it should and within a certain amount of time [11]. In a conventional legacy-based substation analog currents and voltages may be generated by a test set in a primary or secondary injection test [11]. Engineers or technicians can then analyse if, when and how long a relay takes to issue a trip response. The concept of secondary injection protection testing was graphically illustrated in Figure 2-29.

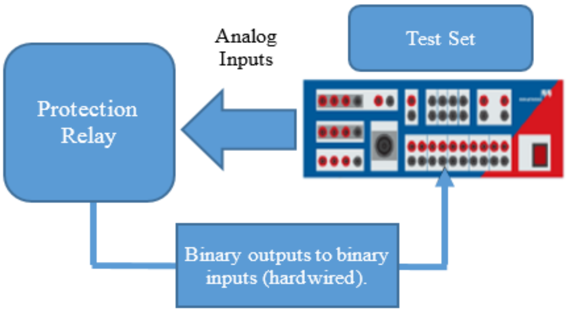


Figure 2-29. Conventional substation protection test [11]

Additionally, in an IEC 61850-based substation, where GOOSE and SV messages are used for the communication of data and information, the same test procedure can be utilised [11]. In this case, the only difference is that the communication between the IED and the test set takes place over the substation LAN [11]. The test set shown in Figure 2-30 will produce SV messages that quantify the current and voltage that was sampled by the instrument transformers. This simulated data is delivered to the protection IED. The IED must then react accordingly and send the appropriate GOOSE messages back to the test set i.e. breaker trip, reclosing or status information [11]. On the other hand, the test set may also simulate GOOSE messages such as breaker status and reclosing and then send this information back to the IED and analyse whether or not the appropriate response/data has been captured [11]. An example of this test procedure was shown in Figure 2-30. This represents a secondary injection protection test in an IEC 61850-based substation network.

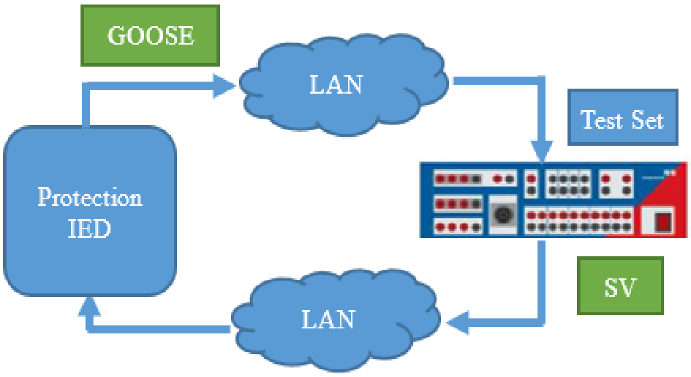


Figure 2-30. IEC 61850 protection test over the substation LAN [11]

2.10.3 Testing merging units using primary injection

A Stand Alone Merging Unit (SAMU) seeks to convert the analog signals or sampled information from the instrument CTs and VTs into digital data that can be sent to the IEDs that require it [2],

[7], [11]. Usually MUs are tested by the manufacturer before delivery since this process requires highly sensitive pieces of test equipment that produce time synchronised analog signals which are required to test the MUs operational functionality [11]. In addition, directly testing an MU from the network is referred to as secondary injection testing since the MU is tested exclusively from the test set. However, on the other hand, primary injection and testing of devices like an MU involves a direct analog current or voltage injection on the instrument CTs or VTs primary coil [11]. This means that the entire voltage or current path can be checked [11]. Hence, this infers that the sampled information from the CT or VT can be validated and analysed by a test set after or before it has passed to the MU. This method of testing was shown in Figure 2-31.

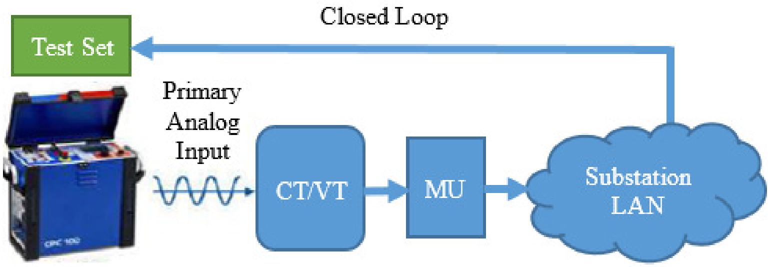


Figure 2-31. SV testing and primary injection [11]

During the course of the studies conducted in both Chapters 4 and 5 of this dissertation, testing was conducted using an Omicron current amplifier to mimic the nominal and fault effects of system currents and a real time digital simulator communicated with an RSCAD test model. This created a closed loop/feedback test system for the developed substation model. Testing of the aforementioned nature allowed the authors to test the operational nature of the proposed substation protection and automation network. This included the technical assessment of the benefits of certain communication protocols such as: the new and preferred IEC 61850 standard, serial Modbus RTU and legacy DNP 3, based on the configuration, connections and responses of the implemented system.

2.10.4 Conformance testing

The IEDs that are designed and built by a particular manufacturer must undergo system tests, routine tests and type tests in accordance with IEC 61850 standard regardless of the final design applications [3], [18]. These devices must also go through traditional Factory Acceptance Tests (FATs), site commissioning and Ste Acceptance Tests (SATs) to ensure that the equipment is functioning as was intended [3]. In addition to the aforementioned tests conformance testing is carried out to ensure that the vendors and their devices have complied with the IEC 61850 communication protocol [3], [18]. Typically, conformance testing covers items like: document verification, configuration, data models and mapping [3]. Conformance testing may be carried out by private test labs that have been accredited by the UCA International Users Group [3], [18].

2.11 Conclusion

Substation protection, monitoring, automation and control collectively rely on the intercommunication of intelligent devices and equipment. This literature review presented a comprehensive review of the IEC 61850-based communication architecture and its associated implications for the protection of various electrical devices within a substations local environment. This new communication standard has had a marked effect on the way in which data, signals and functions can be shared between IEDs, control centres and other electronic and electrical elements within a substation. Modern relays from companies like SEL, ABB and Schneider are being developed with this new protocol in mind and can interoperate with other IEDs regardless of the manufacturer or vendor. Therefore, the age of legacy protection systems and conventional substations is at an end.

Although technology has moved on, the IEC 61850 protocol is not without its technical short-comings. Cyber-attacks, back-up IED protection, a need to develop and change substation architecture, network-based protection testing and inter-IED data transfer are all new and developing complications that must be tackled by engineers, manufacturers and utilities alike. The final standard as specified by the IEC defines a single protocol for modelling various pieces of data within a substation. It seeks to promote the interoperability and communication between IEDs that were developed by different vendors as well as synthesize a common method for storing information. The IEC 61850 standard also provides the basic services needed to transfer data, signals and enable control between IEDs and a central control unit or HMI. Lastly, the testing of electrical devices and the testing of protection schemes within the substation must also conform to the constraints of the IEC 61850 protocol. This makes checking and testing the operation of equipment easier and more efficient.

When the IEC 61850 protocol is compared against traditional SCADA protocols like DNP 3 and simpler serial methods of data transmission like Modbus RTU then the benefits become obvious. During the course of this study (chapter 4 and 5) it was clear that as a result of the hardwired nature of Modbus, its lack of time stamped data, the serial aspects of its communication and the loss of data during a break in communications; that both DNP 3 and especially IEC 61850 offered far more significant advantages.

Therefore, from the thorough investigation conducted in this chapter and indeed throughout this dissertation, it can be concluded that the newly developed IEC 61850 Ethernet-based protocol is at the forefront of the intercommunication between devices for information and data transfer, signaling, control, protection and automation over the substation LAN. Hardwired electromechanical legacy-based systems are the past, IEC 61850 is the present and the future.

3. Methodology

The IEDs of both past and present substations have the ability to transmit data, commands and signals for the purposes of substation protection and automation. They can achieve this by applying one or more of the numerous alike and dissimilar serial- or Ethernet-based communication protocols. The goal of this dissertation was to assess the technical benefits and implications of the IEC 61850 standard on substation engineering. Therefore, it was necessary to implement the protocol independently as well as alongside standards like Modbus RTU and DNP3 on a communication network. Thus, a multi-protocol substation network was established during the preliminary experimental phase. This model then moved towards an almost exclusively IEC 61850 architecture during the course of the main research. The design process allowed the author to make deductions about the new IEC 61850 standard, identify the advantages and pitfalls, outline notable functions and features as well as critically and experimentally compared it to legacy protocols such as Modbus RTU and DNP3. This research gave the author insight into the effects of protocol-based communication on the important aspects of substation design, protection and automation. In the subsequent chapter the materials and methods of the experimental procedure were explored for both the preliminary and the main research models. The following subsections offered an explanation of the design process, how and why the study was conducted as well as why this form of practical experimentation was chosen.

3.1 Preliminary research

This section formed part of the initial stage of research, experimentation and concept development and contributed to the foundation of the principal study. It was during the preliminary developmental stage in chapter 4 that the basis for the main experimental procedure was formalized.

3.1.1 Research design

The basic research design that was explored in chapter 4 of this dissertation consisted of a station level SCADA model which was developed using the CitectSCADA software platform. This structured system monitored a physical network of connected protection equipment and related substation devices. The typical topology of a substation was used to define the feeders, incomers, buses, bays and the switchgear over which the SCADA model observed. Furthermore, the communication of information, commands and signals from and to different devices, equipment and the station computer was achieved using the IEC 61850 protocol, Modbus RTU and DNP3 respectively. It was during this early experimental stage that the obvious advantages and disadvantages of IEC 61850, DNP3 and Modbus RTU were evaluated and discussed.

3.1.2 Equipment and software

The preliminary design stage of this study required that a number of different protection, monitoring and supervisory devices and switchgear be obtained in order to effectively develop a typical substation model. Protocols including the IEC 61850 standard, DNP 3 and Modbus RTU should be supported by the substations protection hardware. The equipment that was obtained included primary and secondary devices to be connected on the station, bay and process levels respectively. The following list briefly describes the three fundamental component elements of substation engineering that were needed to develop the communication network that was investigated during the early experimental stage of chapter 4.

1) Station computer, SCADA platform and IED software configurators
2) Substation automation, monitoring and protection IEDs supporting multiple protocols
3) Test devices and test software

The type, manufacturer and model of the protection IEDs that were used in the early part of this study (including a detailed equipment list) could be viewed in the Appendix (Annex A and B).

3.1.3 Procedure

Here follows an outline of the experimental method, that was used in order to develop the research model for stage 1 of the study which was discussed in chapter 4. This process involved:

1) Definition of an architecture which represented that of a typical electrical substation;

The topology of the substation should consist of two 11kV buses, a connecting bus section as well as two incomers and up to three feeders on each bus. Standard switchgear such as an isolator, circuit breaker and earth switch should be present on each incomer and feeder respectively. The substation switchgear would be controlled by a network of process level automation and protection IEDs. This topology would form the physical layer over which a SCADA model could provide monitoring and control at the station level.

2) Development of a station level SCADA model based on the chosen substation topology;

i) CitectSCADA

Schneider's CitectSCADA software was used to create an automatic and interactive SCADA model of the physical system. This model should provide remote control points for the operation of circuit breakers and isolators, visual indications of the status of switchgear, modes of operation of devices, current readings as well as alerts, alarms and warnings under fault conditions.

3) Implementation of a network of connected hardware at station, process and bay level;

   i) SCADA

   The SCADA should exist on a host PC and should be connected to the RTU via an Ethernet switch i.e. over the substation LAN.

   ii) Ethernet switch

   Mediates data flow and traffic on the network and can be used to prioritize real time messages which are sent from one IED to another.

   iii) RTU

   Stores the information, variables, commands and databases which describe the overall electrical and graphical topology of the entire substation.

   iv) IEDs

   A network of interconnected IEDs was implemented to control the operation, automation and deliver protection to the equipment and switchgear of the substation model. The model code and manufacturer of these IEDs were those mentioned in the list of equipment in section 3.1.2 and shown in the appendix.

   v) Switchgear

   The switchgear used to interrupt the flow of power to the network were Omron relays. These contactors were used as an alternative to large industrial vacuum or oil circuit breakers which were not available, nor essential to this study.

4) Establishing communication between IEDs, related equipment and the SCADA;

   i) DNP3

   DNP3 should be implemented on the telecontrol bus between the MiCOM C264 RTU and the host PC where the SCADA was located. DNP3 is traditionally used as a SCADA protocol and was ideally suited to this application.

   ii) Modbus RTU

   Modbus RTU was implemented on the legacy bus between the RTU and the MiCOM P122 IED.

   iii) IEC 61850

   The IEC 61850 protocol was implemented on the station bus between the RTU and the VAMP 255 and VAMP 259 IEDs.

5) Testing the substation, the equipment and the practical functions of the model;

    i) Steady state conditions

    Steady state conditions were used to assess the operational effectiveness of the experimental model and capture graphical, numerical and visual results of the workings of the system under operating conditions considered to be normal and stable. This was to be achieved using a test that involved the injection of secondary 3-phase current, an RSCAD test model and a real time digital simulator (RTDS).

    ii) Fault Conditions

    Fault conditions were used to assess the operational effectiveness of the experimental model and capture graphical, numerical and visual results of the workings of the system. This was to be achieved using a test that involved the injection of secondary 3-phase current, an RSCAD test model and RTDS.

6) Assess and compare the technical benefits, disadvantages, implications, functions and features of the communication protocols that were implemented;

    i) Comparative study

    A comparative study was conducted in chapter 6 to critical analyse the benefits, ramifications, features and functions of the three protocols implemented in this study.

7) Discuss recommendations and future works;

8) Analyse, conclude and finalize the preliminary study.

9) Move to the main research (chapter 5).

3.1.4 Analysis

Once the experimental model had been established its functionality was tested under steady state and fault conditions. In order to test the substations protection and automation functions secondary current was injected into the IEDs analog inputs using a current amplifier to mimic normal and over current conditions. Additional fault conditions were applied via the RTDS and the RSCAD test model. In order to assess the workings of the model the following aspects were monitored and tested: 3-phase currents, breaker status, isolator status, earth switch status as well as fault conditions like earth fault, breaker fail and overcurrent characteristics.

The results captured were those taken from the process analyst, alerts, alarms and visual aids of the SCADA model as well as from the HMI of the IEDs on the physical network. As a result of the implementation and operation of protocol-based communication between devices making up the substation network and based on the features and functions that each protocol possessed or failed to possess an analysis was established which evaluated the technical implications of the IEC 61850 standard on substation engineering. In addition, resemblance, likeness and contrast was also drawn between the new standard and the legacy protocols DNP3 and Modbus RTU. The reason for this experimental approach was such that the author could describe the ramifications of the IEC 61850 substation protocol on a variety of substation criteria such as design, automation, communication and protection and compare this to that of the older legacy standards. A comparative study was included in chapter 6 which sought to compare the literature from each of the three protocols as well as the deductions made during the course of this research.

3.1.5 Summary

Stage 1 of experimentation sought to broadly define the main concepts of the study, gain a high-level understanding of the research problem and formulate ideas about how to achieved the more acute goals of this research. In order to accomplish these aims and objectives the author completed a substation model, illustrated in Figure 3-1, consisting of switchgear, protection and automation equipment as well as a SCADA model. This network of connected equipment and IEDs used DNP3, Modbus RTU and the IEC 61850 protocol to transfer commands and data to and from their peers. This gave rise to a multi-protocol communication nexus that linked the SCADA host to an I/O device, the I/O device to the IEDs and the IEDs to the switchgear. Hence, using this basic approach, it was possible to assess the implementation, features, functions, implications, benefits and short-comings of protocols like Modbus RTU and DNP3 as compared to IEC 61850. This gave the author insight into the consequences of both modern and legacy-based engineering. The preliminary works which were conducted and included in chapter 4 provided the groundwork for the broader study which was explored in chapter 5.

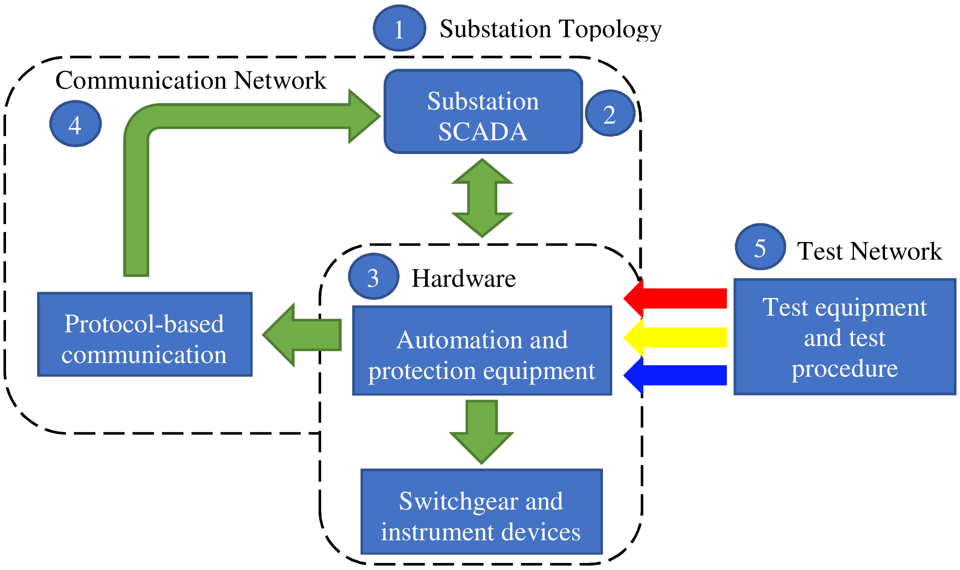

1
Substation Topology
Communication Network
4
Substation SCADA
2
5
Test Network
3
Hardware
Protocol-based communication
Automation and protection equipment
Test equipment and test procedure
Switchgear and instrument devices

Figure 3-1. High-level experimental block diagram

3.2 Main research

The main research, which was conducted in chapter 5, sought to accomplish the principal goals of this dissertation. It was here that the final works and concluding analysis of the undertaking were fulfilled. The purpose of the primary study was to build on the principles that were outlined during the course of chapter 4. Therefore, this component represented the stage 2 experimental development of the final research.

3.2.1 Research design

The principal research that was explored during the course of chapter 5 employed a station level SCADA model and a network of substation protection equipment that was developed as a direct result of stage 1 experimentation. The foremost purpose of this component of the study was to practically configure a fully IEC 61850-compliant protection architecture and assess the ramifications thereof on modern substation protection and design. The applications of the GOOSE message class were investigated and used to provide breaker fail, arc-flash and blocking-based protection to the substation model. Hence, it was during this final stage of the study that the implementation, benefits and shortcomings of the IEC 61850 standard and by extension the implications of the contemporary GOOSE message class, were examined.

3.2.2 Equipment

In order to develop a quintessential substation model which focused predominantly on the technical assessment of the IEC 61850 protocol; compliant protection, monitoring, supervisory devices and switchgear were required. Secondary investigations of Modbus RTU and DNP 3 were also conducted accordingly, such that the chosen protection devices still required compliance with these protocols. However, it remained that the most important characteristic of the specified equipment relied upon the communication compliance of the IEDs with the IEC 61850 standard.

3.2.3 Procedure

Here follows an outline of the experimental method that was used to fulfil the objectives of the research model for stage 2 of the study which was discussed in chapter 5. The following components discussed the configuration and implementation of an IEC 61850-compliant substation model. This process involved:

1) Substation model

   The self-same typical substation model and SCADA that was developed and implemented during the preliminary experimental stage (chapter 4) was used during the course of chapter 5. Minor modifications were made to the device configurations in order to investigate further applications of the IEC 61850 protocol and the GOOSE message class. However, the physical topology of the substation remained consistent.

2) GOOSE message configuration

   i) Compliant protection devices and systems

   Multiple VAMP 259 and VAMP 255 IEC 61850-compliant protection IEDs and a MiCOM C264 RTU were connected over the substation LAN to provide relaying and automation to the substation model. A legacy-based MiCOM P122 was connected outside the IEC 61850 protection zone and communicated over serial RS 485 using Modbus RTU. Information, commands and signals were communicated via the RTU to a CitectSCADA PC model using DNP3 on the telecontrol bus.

   ii) GOOSE message configuration

   The configuration procedure for GOOSE messaging for applications in breaker fail protection, arc-flash and blocking-based protection was followed using VAMPSET. Here the logical nodes, virtual outputs, control block logic, output matrix as well as publisher and subscriber information could be defined specific to each case.

3) GOOSE-based breaker fail protection

   i) Protection architecture

   The GOOSE-based breaker fail protection characteristics of the experimental substation model were investigated simply by disconnecting the trip coil of a particular breaker. Thereafter, fault conditions or remote operation was applied to the breakers protection IED. A trip command would then be issued by the relay output to its respective breaker after which it should fail. Hence, the faulted circuit breaker was then to be isolated using GOOSE-based breaker fail protection.

4) GOOSE-based arc-flash protection

   i) Protection architecture

   The GOOSE-based arc-flash protection characteristics of the substation model were studied using two arc sensors which were connected on the appropriate input of a particular IED. The purpose of this would be to detect cable and busbar arcing. Each arc sensor was tested by simply applying a flash close to the detection element which activated the device. Therefore, in order to isolate the arc-fault GOOSE-based arc-flash protection was implemented to the appropriate protection zone in order to extinguish the arc.

5) GOOSE-based blocking response

   i) Protection architecture

   The GOOSE-based blocking response or sympathetic trip protection characteristics of the experimental system were explored. In this instance the GOOSE message class of a particular IED was configured to issue blocking signals to other neighbouring devices in order to prevent the operation of healthy circuit breakers and ensure that the appropriate protection zone had tripped. This helped to ensure proper protective coordination, grading and selectivity on the network.

3.2.4 Analysis

Once the IEC 61850-compliant experimental substation model of chapter 5 had been established its functionality was tested under breaker fail, arc-flash and blocking-based fault conditions. Therefore, this investigation sought to test the GOOSE-based substation protection and automation functions of IEC 61850. VAMPSET was used to apply fault conditions to the system such that the response of components and devices could be captured. In order to assess the workings of the IEC 61850 substation model the following aspects were monitored and tested: 3-phase currents, circuit breaker status and operating conditions as well as fault parameters like breaker fail, cable arc, busbar arc and overcurrent blocking.

The results captured were those taken from the process analyst, alerts, alarms and visual aids of the SCADA model as well as from the HMI of the IEDs on the physical network. As a result of the implementation and operation of GOOSE-based communication between devices an analysis was established to assess the technical implications of the IEC 61850 standard on substation protection. The reason for this experimental approach was such that the author could describe the ramifications of the IEC 61850 substation protocol on a variety of substation criteria such as design, automation, communication and protection and compare this to that of the older legacy protocols. A comparative study was included in chapter 6 which sought to compare the literature as well as the experimental deductions made during the course of this study.

3.2.5 Summary

Stage 2 of experimentation sought to definitively establish the main concepts of the study, gain an understanding of the research problem and conduct experimental investigation into the IEC 61850 protocol and its intelligent GOOSE message class. In order to accomplish these aims and objectives the author completed an analysis of the applications of GOOSE on breaker fail protection, arc-flash protection and blocking response. Figure 3-2 shows the high-level functional block diagram which explained the procedure of the research conducted in chapter 5.

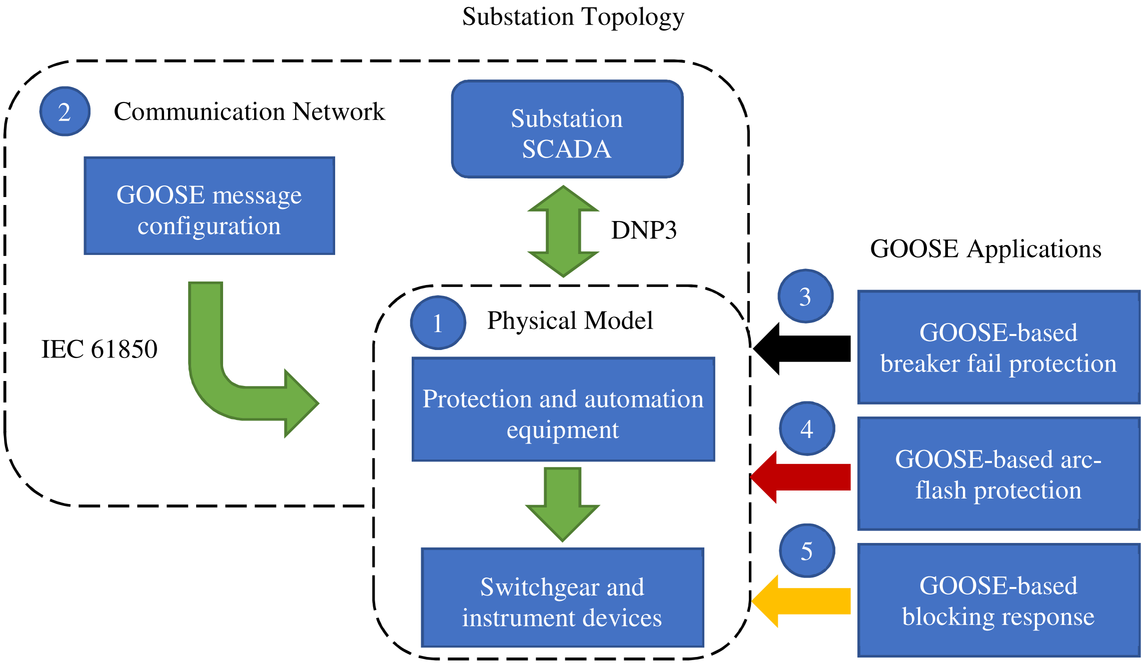

Substation Topology
2
Communication Network
Substation SCADA
GOOSE message configuration
DNP3
IEC 61850
1
Physical Model
Protection and automation equipment
Switchgear and instrument devices
GOOSE Applications
3
GOOSE-based breaker fail protection
4
GOOSE-based arc-flash protection
5
GOOSE-based blocking response

Figure 3-2. High-level experimental block diagram

4. Substation Network

The consideration, differentiation and implementation of substation communication protocols formed the basis for this dissertation. These communication standards included: DNP3, Modbus RTU and mostly importantly, the new IEC 61850 substation protocol. Therefore, the aim of this chapter was to understand the technical applications, implications, perceived benefits and pitfalls of a multi-protocol protection and automation system. Chapter 4 saw the development of a typical substation model as well as the rudimentary implementation of protocol-based data dissemination. Hence, this component of the dissertation presented a brief explanation of the first experimental stage which included: the development of a working network, practical results as well as an analysis, discussion and a definitive conclusion.

The point of departure, from which a working prototypical substation would evolve, focused on the development of an interactive substation SCADA which was designed on the CitectSCADA host platform. This SCADA model was equipped to communicate, transfer, control and monitor data from a network of physically connected substation hardware. The design of a typical protection and automation system provided a means to analyse the various alike and dissimilar methods of communication between substation devices. In addition, it was also possible to assess the operational effectiveness of the model itself. The electrical network of a substation was implemented to achieve the basic research outcomes and provide a spring board from which to further this study in the following chapter. The subsequent model consisted of a communication network that linked the SCADA host to an I/O device (RTU) which was connected to both legacy and IEC 61850-compliant IEDs. Hence, a multi-protocol substation communication network was established. In summary, the purpose of chapter 4 was to develop the foundation of the main research model. Hence, it demonstrated the primary conceptual development of the broader undertaking as well as the initial set of results that were captured during the early experimental stage. Lastly, the results obtained were those relating to both practical and simulation studies.

4.1 Development of SCADA

CitectSCADA software is a fast, reliable SCADA package that is commonly utilized for a variety of industrial applications [21]. SCADA software platforms such as this, provide functions for control, data acquisition, monitoring, graphical displays, event capturing, alarming, trending as well as the storage of data [21]. A quintessential substation SCADA system occurs at the station level and requires information from the physical hardware processes which the SCADA seeks to monitor and control [22]. Corrective control and monitoring actions can be performed by the SCADA host based on the information that has been acquired from the physical network [22]. This allows the SCADA to provide overall control remotely from a host platform [22]. The substation network that was developed using Citect in Figure 4-2, provided remote control for the physical model ensuring that devices turned on and off at the appropriate time as well as monitoring system parameters and the response of automatic actions. There are four distinct levels of SCADA; these include: hardware instrumentation, RTUs, communication networks and SCADA host platforms [23]. The interactive hierarchy of these respective levels was illustrated in Figure 4-1. In the context of this undertaking, hardware instrumentation refers to the instrument devices and IEDs that measure, transmit and act upon the sensed information within the physical network. On the other hand, RTUs store and ferry the sensed electrical parameters and other commands or data over a particular communication medium to a station computer where the SCADA host then captures, interprets and monitors the received data.

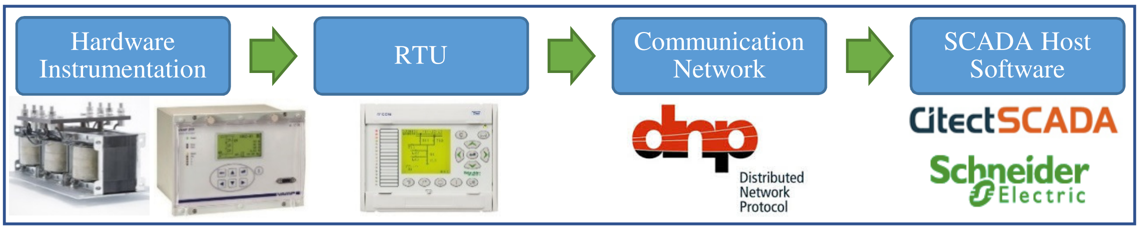
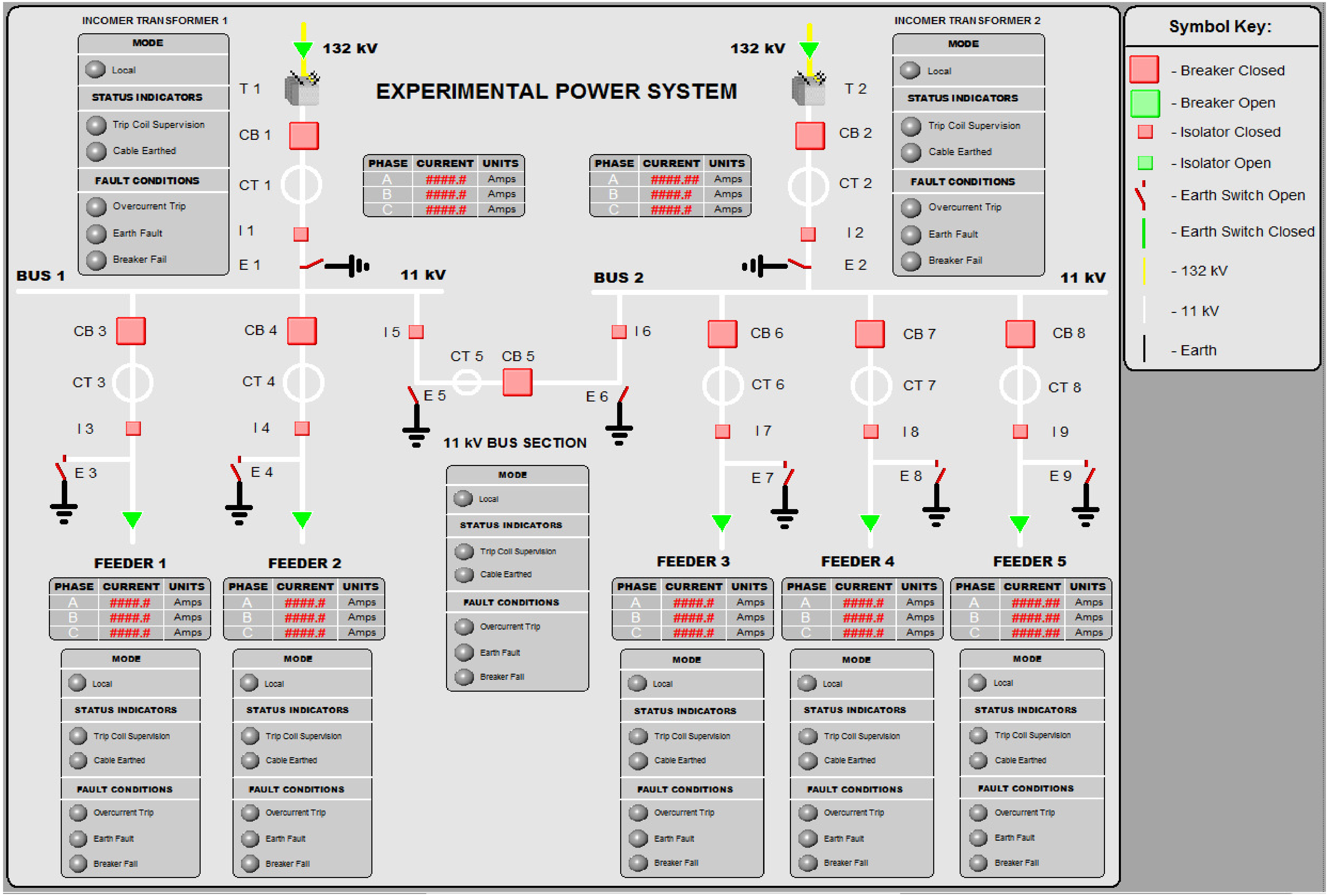


Figure 4-1. Four distinct levels of SCADA

The interactive substation model illustrated in Figure 4-2 was configured to communicate with an intelligent I/O device or RTU. RTUs are microcomputers that can interface with a wide variety of equipment such as IEDs, HMIs, transducers and end equipment [24]. In addition, they can transfer information, data and commands from these components to a PC on which the SCADA host is located [24]. The SCADA can then identify, processes, distribute, analyse and display the relevant information [25], [26]. This helps the observer to interpret data from the greater network and make important decisions based on the alarms, readings and visual alerts of the model.

4.1.1 Substation model

The development of a typical substation was initially realized via the implementation of a station level SCADA as well as the associated physical hardware model on the bay and process levels respectively. This illustrative and interactive smart SCADA, which was demonstrated in Figure 4-2, presided over a nexus of authentic hardware including a number of modern and legacy IEDs. The characteristic electrical network that was described in the layout on the following page consisted of three basic sub-architectures. Therefore, the substations graphical topology was comprised of two incomers, five outgoing feeders on bus 1 and 2 and lastly, a bus section which connected the two respective buses. Furthermore, each feeder, incomer and bus section had a framework of basic switchgear which included: a circuit breaker, an isolator and an earth switch on each bay. Hence, the aforementioned description was that of a quintessential substation.



Incomer Transformer 1:

PHASE	CURRENT	UNITS
A	####.#	Amps
B	####.#	Amps
C	####.#	Amps

Incomer Transformer 2:

PHASE	CURRENT	UNITS
A	####.##	Amps
B	####.#	Amps
C	####.#	Amps

FEEDER 1

PHASE	CURRENT	UNITS
A	####.#	Amps
B	####.#	Amps
C	####.#	Amps

FEEDER 2

PHASE	CURRENT	UNITS
A	####.#	Amps
B	####.#	Amps
C	####.#	Amps

FEEDER 3

PHASE	CURRENT	UNITS
A	####.#	Amps
B	####.#	Amps
C	####.#	Amps

FEEDER 4

PHASE	CURRENT	UNITS
A	####.#	Amps
B	####.#	Amps
C	####.#	Amps

FEEDER 5

PHASE	CURRENT	UNITS
A	####.##	Amps
B	####.##	Amps
C	####.##	Amps

Figure 4-2. Substation SCADA model

The SCADA model in Figure 4-2 had a variety of supervisory features and visual alerts that interactively illustrated network activity to the observer. These display functions included status indicators for the isolator, breaker, local mode, trip coil supervision, cable earth, overcurrent trip, earth fault, breaker fail and 3-phase currents respectively. Furthermore, in order to open and close the switchgear in Figure 4-2, the SCADA model had two interactive control panels for the corresponding isolator or breaker. Hence, a pop-up window appeared upon clicking on each of these symbols. This allowed the user to remotely open or close the breaker or isolator in question, provided that the appropriate rules for interlocking had been observed. Interlocking prevented arcing across a particular isolator by ensuring that the contacts were not live during switching.

4.1.2 Variable tags

In order to communicate, control, monitor and capture data and signals from a physical network or an I/O device (RTU), SCADA models require descriptive tags that define the data and commands which it seeks to supervise. Table 4-1 showed an example of how the tags were catalogued for one of the incomers in the substation model depicted in Figure 4-2. A number of the descriptive tags in Table 4-1 had an attached time stamped alarm or an associated interactive trend. The alarms and alerts allowed certain critical events including: breaker fail, different fault conditions as well as isolator and breaker status to be captured and identified. On the other hand, the attached graphs acted as an analysis tool that provided a visual description of how certain system parameters within the SCADA model; like phase currents, breaker status, trip commands and fault conditions, were trending. In addition, the trends for each parameter could be viewed on the SCADAs trend page or alternatively within the process analyst.

Table 4-1. Variable tags, alarms and trends

Network Parameter	Variable Tag Description	Time Stamped Alarm	Trend
Circuit Breaker 1	Transformer breaker 1 closed	Yes	Yes
	Transformer breaker 1 opened		
	Transformer breaker 1 open/close command	No	No
Isolator 1	Isolator 1 closed	Yes	Yes
	Isolator 1 opened		
Earth Switch 1	Cable incomer 1 earthed	Yes	No
Phase A Current I1	Current incomer 1 IA	No	Yes
Phase B Current I1	Current incomer 1 IB	No	Yes
Phase C Current I1	Current incomer 1 IC	No	Yes
Local Mode CB 1	Local/Remote mode CB1	Yes	No
Earth Fault I1	Transformer 1 earth fault	Yes	Yes
Overcurrent CB 1	Over current trip CB1	Yes	Yes
Breaker Fault CB 1	Breaker 1 failure	Yes	Yes
Trip Coil Supervision CB 1	Breaker 1 trip coil supervision	No	No

4.1.3 I/O device configuration

CitectSCADA offers a number of different ways to configure an I\O device with the user's software model. Firstly, the convenient express communication wizard can be recruited to automatically setup a particular device as well as to identify the external device database. Alternatively, an I/O device can be manually configured using the Boards, Ports and I/O devices forms in the CitectSCADA project editor. Therefore, using the aforementioned methods, an I/O device like an RTU could be used to link the tags, which were populated in Table 4-1, to the data stored in the external data source of the RTU itself.

RTUs are typically programmed independently of a SCADA model using a different proprietary configuration software [21], [26]. Hence, using its own configurator, the RTU for the model in Figure 4-2 was programmed with the necessary plant variables, parameters, functions and elements that were required by the graphical and electrical topology of the substation. Thus, this allowed the RTU to exchange data, information and control commands with the station computer and populate the tags within the SCADA model. Therefore, for the purposes of this dissertation, the aforementioned and described configuration techniques allowed the author to establish communications with the RTU using the Boards, Ports and I\O devices forms of CitectSCADA. This configuration procedure also defined the protocol over which the RTU and the SCADA host communicated.

4.1.4 Citect system configuration overview

The logical system configuration was graphically depicted in Figure 4-3. This diagram represented a brief overview of the symbiotic relationship between the SCADAs configuration parameters and the runtime components. The functional block diagram outlined a structure that required that the engineer: define an I/O server, define the transport type in the Boards form (TCP/IP), define the communication port in the Ports form and lastly, define the protocol-based driver (DNPR) [21].

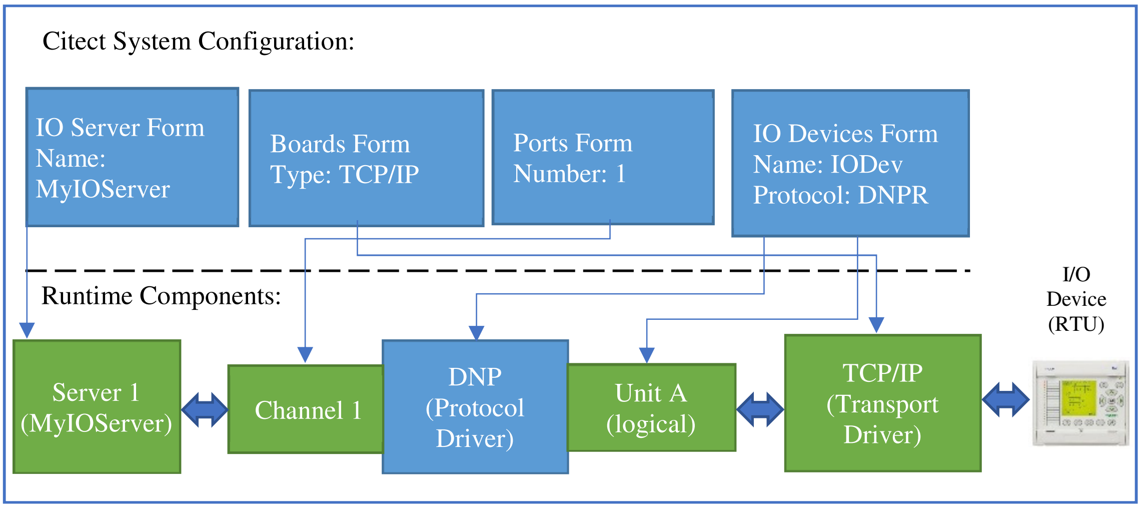


Figure 4-3. Citect system configuration and runtime components [21]

4.1.5 Legacy SCADA and I/O device interface

In this chapter the DNP3 protocol was used over an Ethernet communication link to connect the SCADA host to the RTU. DNP3 has been known to play a crucial role in electrical networks, where it is commonly utilized as a communication mechanism to link master control stations to substation RTUs [25]. In contrast to DNP3, basic serial protocols like Modbus RTU are byte-orientated and can only exchange a single byte of information in order to communicate [25]. However, such protocols have evolved to become packet-orientated, with each packet containing a particular number of bytes structured in a certain way (header, data and checksum) [25]. In the packet structure for DNP3 a master (control PC on which the SCADA is active) will initiate and transmit a read request for an object or multiple objects from the slave [25]. The remote device or slave will then respond with the desired or requested data [25]. Furthermore, the master can also send an operate command which generates the output actions of the specific object reference [25], [26]. In addition, the remote device can send an automated message to the SCADA host when a particular event has occurred enabling it to send messages of alarm in the case of a fault, failure or trip [25], [26]. This concept was graphically illustrated in Figure 4-4 which showed the interaction between master and slave.

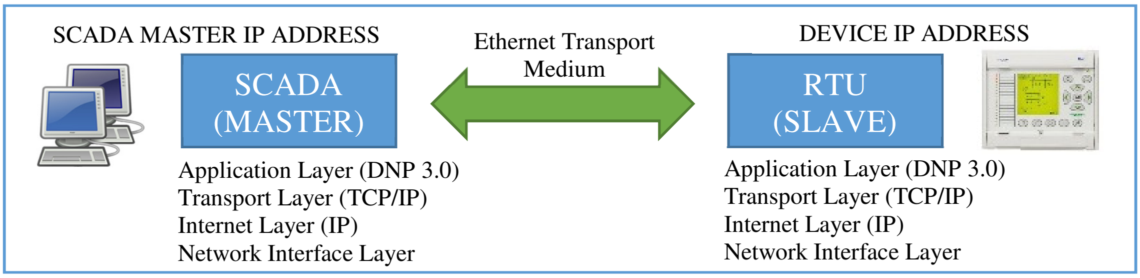


Figure 4-4. SCADA master and RTU slave communication interface [25]

4.2 Development of a substation communication network

Typically, modern substations will employ a smart SCADA model that acts as a watchdog for the substations network of physical hardware. This network refers to the complex combination of IEDs, CTs/VTs, switchgear and related devices, cables and communication links that make up a substations fundamental architecture. The development of the aforementioned SCADA model was explored in the previous section. Thereupon, it was necessary to consider the implementation of the virtual and physical communication between devices over which the SCADA monitored and on which the SCADA acted. The quintessential electrical substation, which is illustrated in Figure 4-2, incorporated a variety of typical substation components. These items included: an I/O device or RTU, an Ethernet switch, a network of modern and legacy IEDs as well as switchgear that was used to mimic the operational functionality of circuit breakers, isolators and earth switches alike. The following segments discussed how such a network of interconnected components was established and configured as well as the communication mechanisms that allowed protocol-based data transport, over IEC 61850, DNP3 and Modbus RTU to take place.

4.2.1 Configuration and structure

The basic primary structure of the communication network that was established in chapter 4, is illustrated in Figure 4-5. This high-level overview depicts only the essential functional blocks of the system which identified the type of equipment used as well as the protocol-based method of communication between each element over the TCP/IP Ethernet-based LAN and serial RS 485. For the purposes of chapter 4, protocols like DNP3, the IEC 61850 standard and Modbus RTU were implemented between the SCADA and the RTU (Figure 4-4) as well as between the RTU and the IEDs (Figure 4-5) respectively. Hence, certain configurations and requirements for each device were statutory in order to setup the aforementioned protocol-based transport media. Importantly, since this dissertation focussed on the different communication mechanisms themselves rather than on the detailed functionality and setup of the protection hardware, the following discussion may omit certain details about the operational theory of such devices. Protocol-based communication between the SCADA host and related devices as well the peer to peer interoperability of the IEDs, illustrated in Figures 4-4 and 4-5, formed the basis for this analysis and discussion.

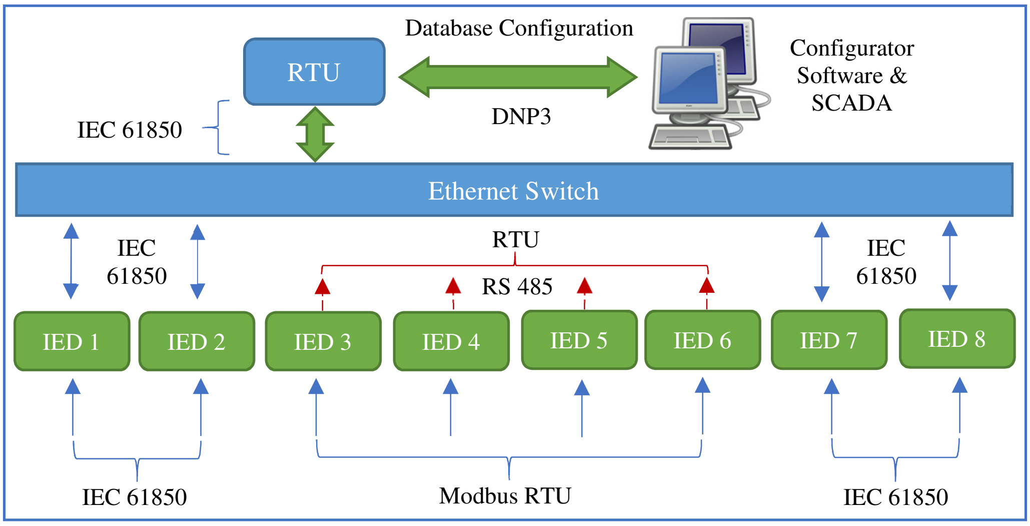


Figure 4-5. Communication network

4.2.2 Configuration and interconnection of an intelligent I/O device

The MiCOM C264 RTU is a modular bay computer that records information as well as monitors and controls the status and behaviour of components/bays within a substation such as that shown in Figure 4-2 [27], [28]. An RTU such as that described was implemented and configured during the development of chapter 4 to establish the topology of the network model and provide a variable, functional and technical description of the physical model. This allowed the IEDs, SCADA and the RTU to transfer relevant pieces of data, information and commands that were configured within the database. The aforementioned RTU can also be configured to provide sample value measurements of associated substation systems at regular intervals [27], [28]. These sampled values are delivered to the SCADA, which enables the user to achieve remote monitoring and control. The data facilities of the bay computer were designed for controlling and monitoring a substation's switchgear which is subsequently governed by the IEDs to which the RTU is connected. A System Configurator Editor, called PACiS SCE, allowed the user to adjustment information, parameters and the overall description of the electrical network within the RTUs database [27], [28]. The following numbered segments describe some of the basic principles that were used to setup and configure the RTU that was used in the network of equipment that was established in chapter 4.

(i) Communication

This I/O device or bay computer has different communication levels which define the architecture or the particular substation component to which the RTU was connected [27], [28]. These levels, which were graphically illustrated in Figure 4-6, are referred to as the: telecontrol bus (TBUS), legacy bus (LBUS) and the station bus (SBUS) respectively.

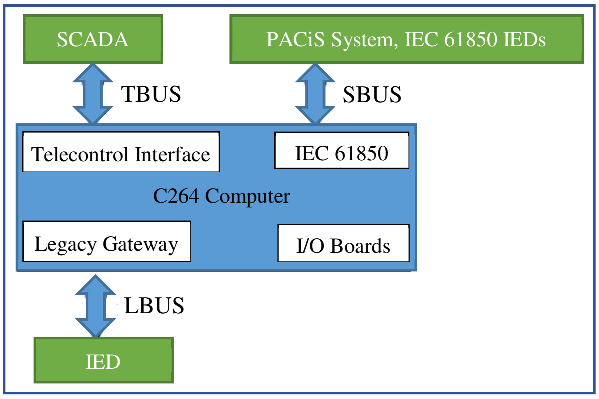


Figure 4-6. MiCOM C264 communication block diagram [27]

The telecontrol bus is typically used to connect the intelligent RTU to the SCADA host platform. Hence, this bus was employed in combination with DNP3 over TCP/IP to link the associated SCADA model to the RTU. This concept was graphically illustrated in Figure 4-4. When the RTU was connected to the station computer over the TBUS, it behaved as a slave using DNP3 as the master/slave protocol [27], [28]. The I/O device can also connect to the SCADA directly via the DNP3 physical communication layer or by using a modem. Interestingly, the RTU can facilitate as many as 2 different serial telecontrol protocols on the TBUS. However, for the purposes of this chapter TCP/IP Ethernet-based communication transport mechanisms were implemented [27], [28].

Alternatively, over the LBUS the RTU behaves as a master using legacy protocols like Modbus, DNP3 and IEC 60870 to transfer data, information and commands [27], [28]. Therefore, the LBUS could be used to connect devices such as the MiCOM P122 which uses legacy-based protocols such as those already mentioned. Hence, via the LBUS the RTU can communicate with other devices and relays using the RS 232 or RS 485 physical transport layers as well as via optical fibre [27], [28]. Lastly, SBUS protocols may be used for PACiS subsystems but are, however, also available for other applications such as data transport between the RTU and the IEDs. In this instance, the bay computer typically behaves as a server; however, it can also be used as a client for IEC 61850-based IEDs [27], [28]. On the SBUS the link layer is Ethernet-based with 10 to 100 Mb/s speed data transfer. The physical layer uses copper twisted pair (J45) or optical fibre connections [27], [28]. Therefore, for the purposes of chapter 4 and 5 the SBUS was used to interface and communicate information between the IEDs and the RTU using IEC 61850 as well as directly between the IEDs themselves.

(ii) Data exchange

Since the bay computer is IEC 61850 compliant over the SBUS, it can obtain and transfer data over an IEC 61850 network using the REPORT/ GOOSE message mechanisms [27], [28]. The REPORT class allows for the specific exchange of information between the IED server and a particular client [27], [28]. Hence, REPORT messaging provides:

- a data value;
- data status or an equivalent quality attribute;
- a time stamp of the last data value change;
- and a time stamp quality attribute.

The term ‘data quality’ defines if certain data is valid or not and is able to specify several different types of invalidity, including: an unknown state when a device is disconnected, saturated states as well as an undefined state [27], [28]. REPORT or GOOSE messages are sent/received periodically by devices along with the reason for inclusion (RFI) which specifies a state/value change or a means of control [27], [28]. In addition to REPORT, the GOOSE message class is a short message system which includes the data value and quality. Importantly, it is multicast to all the SBUS equipment that have subscribed to the message stream [27], [28]. GOOSE is typically much quicker than REPORT messaging, thus, it was employed between the IEC 61850 IEDs in chapter 4 and 5.

(iii) Transmission

The RTU uses binary inputs to transfer data and messages. As a result of different configurations, a binary input can be distributed on a client/server basis or via the SBUS using two of the following modes:

- Report based mode: a change of status is transferred to all the subscribers along with the associated time stamp and the reason for the aforementioned status change (RFI). Report modes are typically used if certain data is needed for displaying, printing or archiving between the RTU and the SCADA platform [27], [28].
- GOOSE based mode: a change of status is multicast to the devices that have subscribed to receive it. On an IEC 61850 network every binary value can be transferred using GOOSE messaging. In addition, the GOOSE message mode is commonly used to transmit vital packets of data as soon as it can be sent (immediately after acquisition). This ensures the that essential equipment is protected in an expedient manner [27], [28].

(iv) An overview of PACiS system configuration

In order to define the RTUs substation variable data source using the PACiS system configurator; three fundamental aspects were considered. The first of these referred to the topology of the system which dealt with the composition of the device whose role it was to manage the client's electrical process [27], [28]. The second aspect referred to the electrical topology of the proposed model and directly dealt with the definition of the client's electrical process – in this case that of the substation SCADA model as was illustrated in Figure 4-2. Furthermore, this included the definition of electrical devices such as: earth switches, disconnectors and circuit breakers respectively [27], [28]. The third and final aspect to be considered was that of graphical topology. This topology referred to the layout of the model itself as well as the relevant graphical animations and descriptions which occurred on the substation control points and bay control points (HMI) respectively [27], [28].

(v) Defining the addressing mapping of a station-bus network

IEC 61850 address mapping refers to the conglomeration of logical devices that are composed of elements called bricks [27], [28]. Typically, the term 'brick' refers to a particular electrical device or an associated function. The brick seeks to provide its own real-time status data, measurements, controls and configurations by grouping data into these different categories. These are called functional components and they group data objects that are seen as real-time equivalents of PACiS data points. When the IEC 61850 client needs the real-time value of a data point managed by another IEC 61850 server, the server transmits the information via a data object of its own IEC 61850 mapping [27], [28]. Using PACiS and the SCE the operator, could define the IEC 61850 clients and the IEC 61850 servers from and to which the clients transmit and retrieve information [27], [28]. Generally, IEC 61850 data objects have common class categories. The structures of these class stereotypes must be known by all the PACiS IEC 61850 compliant sub-systems. These common classes are referred to as the terminal description of the IEC 61850 data modelling system [27], [28]. The communication that took place on the station bus between the RTU and the IEDs was graphically depicted in Figure 4-5 and 4-7 respectively.

(vi) Control points

An electrical substation, such as that depicted in Figure 4-2, can be supervised and controlled using PACiS user interfaces called substation control points or bay control points as well as remotely via the SCADA host [27], [28]. Typically, the remote-control point of a substation is achieved using a legacy communication network. A variety of different legacy networks can be connected to a PACiS system, using a PC or alternatively a telecontrol gateway [27], [28]. As was previously stipulated, DNP3 was used as the legacy transport mechanism between the SCADA master and the RTU slave. This concept was diagrammatically illustrated on the TBUS of Figure 4-5 and 4-7.

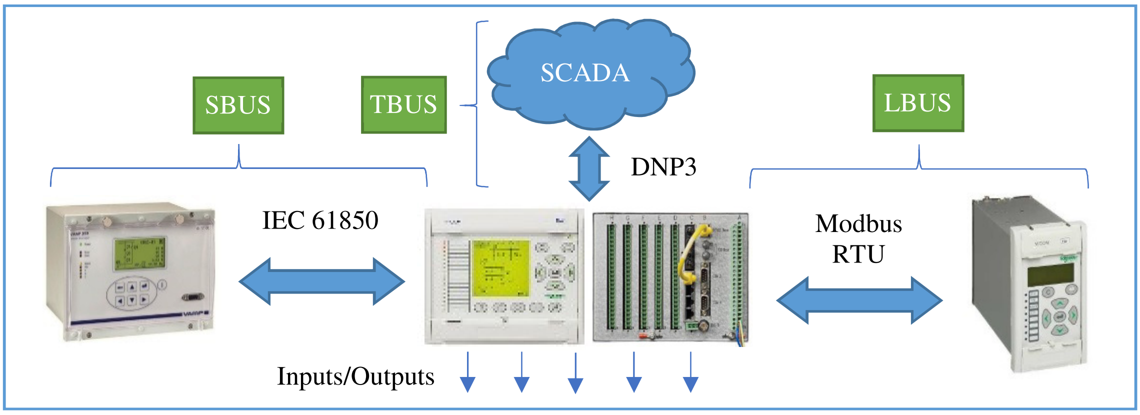


Figure 4-7. TBUS, SBUS and LBUS communication interfaces

4.2.3 Ethernet switch

The Moxa PowerTrans PT-7728 series IEC 61850 Ethernet switch was used for the purposes of the communication network that was implemented in chapter 4 [9]. This Ethernet switch has many advanced functions including: noise guard technology and EMC resistance [9]. The device also features a packet prioritization feature that is used for both GOOSE and SV messages, an MMS server base for SCADA as well as a configuration wizard designed specifically for substation automation [9]. The prioritization feature of the Ethernet switch allows messages of the highest importance to be sent first which regulates data traffic on the network. In chapter 4 the advanced functions of the switch were not readily established and the device was used simply as an Ethernet switch to ferry data/information on the station bus to which the IEDs and RTU were connected.

4.2.4 Configuration and interconnection of modern IEDs

The VAMP 259/255 numerical line protection devices and feeder managers have a full protection scheme with distance and line differential functions as well as several standard protection functions that are typically needed for the protection of medium voltage transmission lines, cables, substation equipment, power plants and offshore applications [29]. These two devices have a wide variety of protection functions including, over- and undercurrent, over- and undervoltage, over- and under frequency, auto reclosing, earth fault as well as circuit breaker failure protection; to name but a few. Two VAMP 259 feeder managers and one VAMP 255 were employed during the development of the physical network for chapter 4. This allowed the author to implement, observe and analyse IEC 61850 communications between these IEDs and the RTU. Hence, the purpose of this dissertation was to focus on the communication capabilities, configuration and implementation of dissimilar and alike devices. Therefore, although a few protection functions like overcurrent, circuit breaker failure and earth fault protection were implemented in the network shown in Figure 4-2 the main focus was on inter-IED and SCADA communication. Hence, the protection functions themselves were not discussed in great detail.

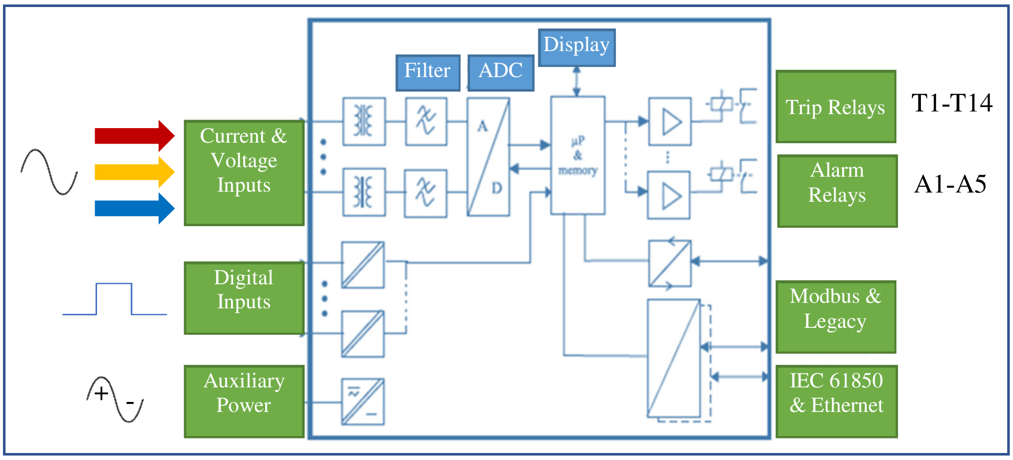


Figure 4-8. Principle block diagram of the VAMP hardware [29]

Figure 4-8 illustrates the principle block diagram of the VAMP 259/255 feeder managers. The main components of these devices consist of the energizing inputs, digital inputs, output relays, A/D converter as well as the advanced microcontroller [29]. The devices also contain a power supply and an interactive LCD (HMI). The current and voltage inputs of the IEDs take the analog response of the incoming signal and convert it into a digital value that can be interpreted by the device themselves, using the ADC (Analog to Digital Converter) [29]. In terms of the electrical network shown in Figure 4-2, a 3-phase test current was injected into a particular IED using a RSCAD test model along with a Real Time Digital Simulator (RTDS) and a current amplifier to test certain desired functionalities. This test procedure was demonstrated by Figure 4-9. Thus, the monitoring capabilities of the SCADA, intercommunication of devices as well as the overcurrent characteristics of the intelligent relays could be validated. The numerous components, connections, configurations and communications of the IEDs were discussed in the numbered segments that follow:

(i) Digital inputs

There are 32 digital inputs (DIs) available on the IEDs rear panel for input control. As expected, the DIs required an external AC or DC control voltage, from the connected equipment, in order to be activated [29]. These DIs were ideal for transferring the status information of switching devices like the circuit breakers, isolators and earth switches into the IED for the purposes of the network model shown in Figure 4-2 as well as the diagram in Figure 4-9. The label name and virtual description texts of the defined DIs could be edited within the IEDs VAMPSET software on a PC, according to the application of the input in question [29]. Therefore, the user defined what each digital input was used for by manipulating the configuration software [29]. This package also allowed the user to set and define the IEDs protection and configuration parameters.

(ii) Digital outputs

The outputs of the different protection stages, digital inputs, logic outputs and other internal signals can be connected to output relays, front panel indicators and virtual outputs using the IEDs output matrix [29]. Output relays are also referred to as digital outputs; to which any internal signal of the relay can be connected. [29]. The output relays on the IED were used to send trip commands to the circuit breaker, in the network shown in Figure 4-9; as a result of a disturbance or automatic trip request. The digital outputs can be configured on the IEDs output pins as follows in Table 4-2 [29].

Table 4-2. Digital output relays

Parameter	**Value**	**Description**
T1 – T14	0 or 1	Status of trip output relay.
A1-A5	0 or 1	Status of alarm output relay.
Remote Pulses		
A1-A5	0.00 – 99.98 or 99.99	Pulse length for direct relay output control using communication protocols. 99.99 = infinite. Released by writing 0 to the direct control parameter (SET).

(iii) Controllable objects

These IEDs allow control for up to six objects, which include: circuit breakers, isolators and earth switches such as those in the substation network of Figure 4-2. The control of such objects can be achieved by using the ‘select-execute’ or ‘direct control’ principles [29]. Importantly, only the objects 1 – 6 are controllable while the objects 7 – 8 are only able to show the status of the devices such as those mentioned [29]. These control principles may be employed using the local HMI, through a remote communication and SCADA or using a digital input. The interconnection of an object to a particular output relay was achieved using the output matrix as previously mentioned (object 1 – 6 open output, object 1 – 6 close output) [29]. The signal “Object failed” may be activated if the control of a particular object was not completed [29]. This has implications for object parameters such as ‘breaker fail.’ Therefore, objects are said to have the following states as was shown in Table 4-3.

Table 4-3. Controllable object states

Setting	Value	Description
Object state	Undefined (00)	State of the object.
	Open	
	Closed	
	Undefined (11)	

Table 4-4. Object control signals

Output Signal	Description
Object x Open	Open control signal for the object
Object x Close	Close control signal for the object

Every control object, like the earth switch, circuit breaker and isolator of the substation network in Figure 4-2 has two associated controls in the control matrix. The control signals depicted in Table 4-4 use control pulses to send activation commands when an object is controlled by a digital input [29]. Hence, when a control command such as ‘circuit breaker close’ is sent from the SCADA via the RTU a control pulse is sent to the respective virtual input of the IED which singles that the IED should trip the relevant circuit breaker. Importantly, objects can be controlled using digital inputs, virtual inputs as well as virtual outputs [29]. If the IED is set to local control state, the remote-control inputs are ignored. Object control is activated when a rising edge is detected by the input in question [29]. The length of this control pulse must be at least 60 ms [29]. Hence, there are four settings for each controllable object as follows in Table 4-5.

Table 4-5. Controllable object settings

Setting	Active
DI for remote open/close control	In remote state
DI for local open/close control	In local state

(iv) Local and remote mode

When a device was in local mode the output relays could be controlled using the local HMI on the device itself, but they could not be controlled using the remote ethernet-based communication interface to the SCADA [29]. In remote mode, on the other hand, the output relays could not be controlled using the local HMI on the device. They could only be controlled using the remote Ethernet-based communication interface to the SCADA [29]. The selection of the Local/Remote mode could be achieved using the local HMI on the device, or by using one of the selectable digital inputs [29]. Hence, a digital input was implemented to change the device from local to remote mode and vice versa [29]. This digital input for remote and local mode was set and defined in the VAMPSET software. Hence, the operation of local/remote mode could be achieved by using a simple switch on the relevant digital input of the IED.

(v) Communication ports

The feeder managers have a number of different communication ports that can be used to communicate with other IEDs over various transport media. These communication means include: RS 232, RS 485 as well as Ethernet [29]. In the physical model developed for this chapter the IEDs were setup for TCP/IP Ethernet-based communication using the IEC 61850 protocol in VAMPSET. Hence, this allowed the IEDs to communicate with the RTU using IEC 61850 over their Ethernet ports on the station bus. TCP port 1st INST and TCP port 2nd INST are the ports on the IEDs that are used for and by ethernet-based communication protocols like IEC 61850 [29]. The associated parameters of the aforementioned ports can be set using the HMI local to the device or using the appropriate menus in the VAMPSET software.

(vi) Communication protocols

The IEC 61850 protocol achieved the transfer of data and information between the IEDs and the RTU. This information included: events, status information, measurements and control commands. Hence, the VAMP 259 supported communication using the IEC 61850 standard. This protocol was available for implementation when using the optional inbuilt Ethernet port on the relays themselves. This communication standard can be used to read /write data from the relays as well as to receive events and to receive/send GOOSE messages to other IEDs [29]. In addition, the IEC 61850 server interface is capable of items such as [29]:

- Selection of logical nodes for certain application functions;
- Configurable pre-defined data sets;
- Dynamic data sets defined by clients;
- Reporting functions;

4.2.5 Configuration and interconnection of legacy IEDs

The MiCOM P122 universal overcurrent relay developed by Schneider was implemented on the legacy bus using Modbus RTU and serial RS 485. This was in addition to DNP3 and the IEC 61850 standard which were implemented in conjunction with the VAMP 259/255 IEDs on the telecontrol and station buses respectively [30]. The MiCOM P12X series relays are designed to control, protect and monitor substations, distribution networks and other industrial processes [30]. Furthermore, these devices can be used for back-up protection of high voltage (HV) transmission networks [30]. The following numbered segments briefly described how the MiCOM P122 was connected on the legacy bus of the experimental model that was shown in Figure 4-2.

(i) Communication

This legacy protocol-based IED has twin serial RS485 communication ports that allow the device to read, reinitialize and change its own software settings from a local or remote PC with the MiCOM S1 software package [30]. The physical transport medium for serial RS 485 is copper twisted pair that passes a particular potential difference between the two cables in order to communicate. This IED has a rear mounted RS485 communication port with dedicated terminals 29, 30, 31 and 32 that are typically used to communicate with other IEDs on the legacy bus [30]. In addition to RS485 the relay also has a front mounted 9-pin RS232 communication port that is dedicated to the setting software and enables configuration by connecting the relay and a PC [30].

(ii) Protocols and standards

The P122 IED can communicate using four standard protocol databases namely: Modbus RTU, Courier, DNP3 and IEC 608750-5-103 [30]. For the purposes of chapter 4 Modbus RTU was implemented between the IED and the RTU in addition to DNP3 which had already been established on the TBUS between the RTU and the SCADA host. The rear panel of the device provided a two-point RS 485 serial connection [30]. The speed of transmission could be adjusted by the user by selecting the appropriate baud rate from 300-38400 on the front panel of the relay [30]. In addition, there were different transmission modes that define the start bits, data, parity and stop bits. This defined the total number of bits in a message and was checked by a CRC [30]. Lastly, the frame sent and received by the relay consisted of the slave number, the function code, the data (information) and the CRC [30].

Therefore, by employing the IEDs aforementioned configuration features and communication mechanisms, it was possible to establish dialogue between the legacy-based IED and the RTU on bus 2, feeder 5 of the substation illustrated in Figure 4-2. Since, the MiCOM P122 overcurrent relay only has three digital inputs it could only be utilized to control the operation of a single circuit breaker on feeder 5. The three inputs were subsequently used for the open and closed statuses of the circuit breaker as well as for the open/close command itself. Lastly, the breaker fail, overcurrent trip and earth fault alert functions were implemented as before.

4.2.6 Test network

In order to test the developed substation electrical network and by extension the SCADA model as well as the IEDs, RTU and associated connected devices; a test model was established using RSCAD, RTDS as well as a current amplifier. The test network depicted in Figure 4-9 shows how the RTDS and amplifier were used in conjunction with the RSCAD model to inject 3-phase analog test current into the IEDs. Hence in this way, the overcurrent trip characteristics of the relay could be tested. Additionally, using the same equipment, ground faults could also be applied to the conceptual network and the associated response of the IEDs and the SCADA could be assessed.

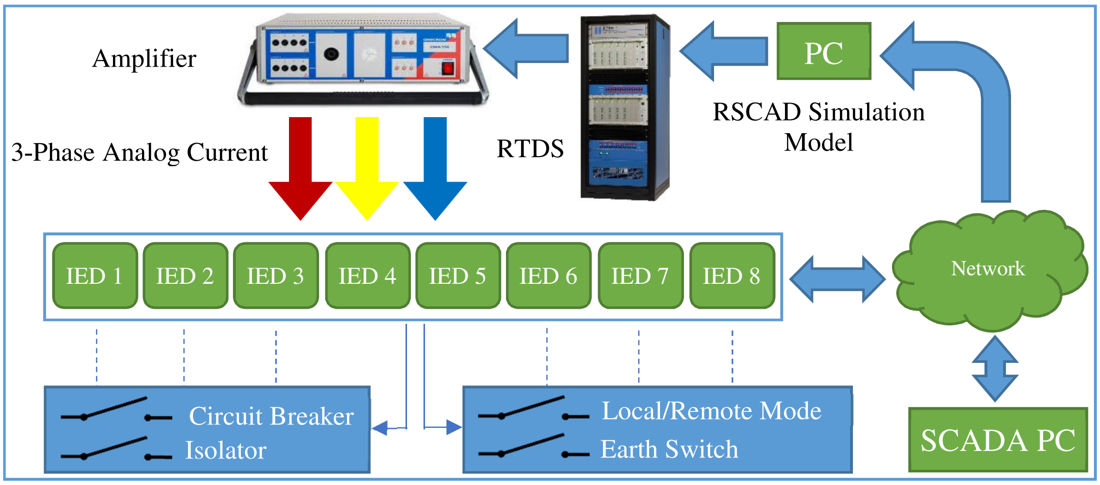


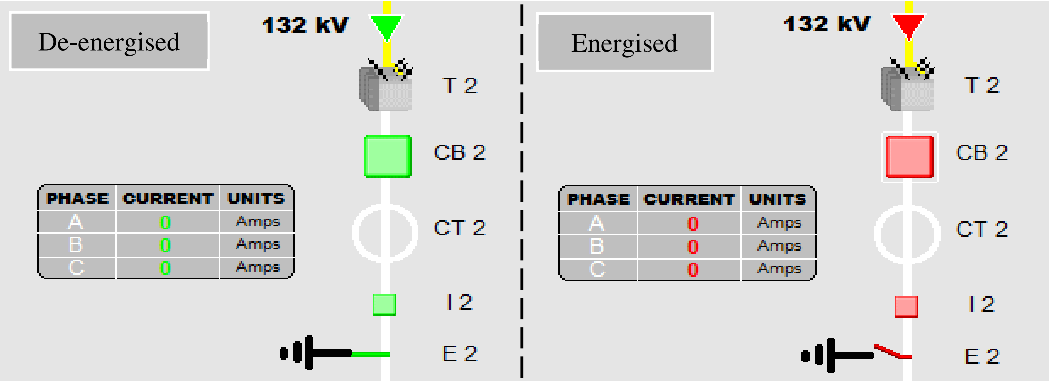
Figure 4-9. Test network and hardware layout

4.3 Preliminary results

The following subsection of chapter 4 outlined a brief demonstration of the preliminary results that were recorded from the experimental substation model. The communication network that was established in this chapter transferred data and commands between the SCADA host and the RTU using DNP3 as well as between the RTU and the IEDs using the IEC 61850 substation protocol and Modbus RTU. The operation and functionality of the physical model itself was then tested and evaluated. Hence, the behaviour of the SCADA as well as the performance of the associated equipment on the network were simultaneously reviewed using the practical results captured from each unique aspect of the substation. Lastly, as a redundancy measure, the experimental tests were not repeated for each and every feeder or incomer of the model that was illustrated in Figure 4-2.

4.3.1 General operation of SCADA model and associated physical equipment

(i) Circuit breaker, isolator, earth switch and basic system operation

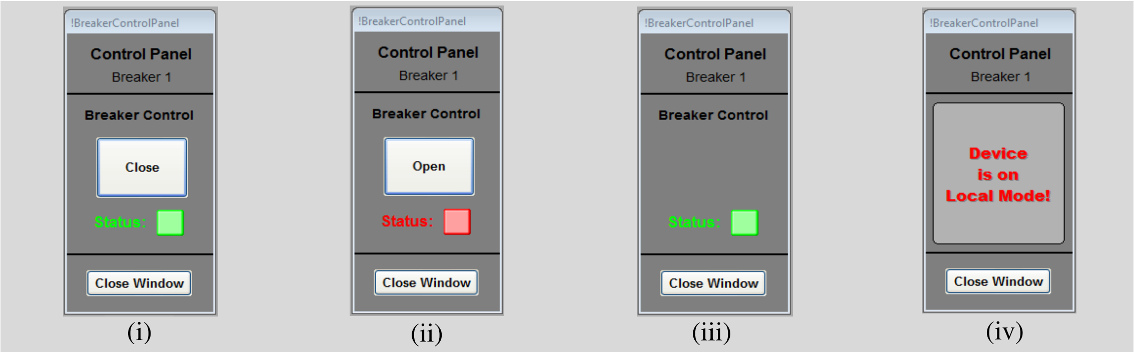


PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 4-10. Energised and de-energised states of incomer

The remote operation of the circuit breaker, isolator and earth switch for an incomer in the substation electrical network was graphically illustrated in Figure 4-10. In this figure the interactive status alerts of the breaker, isolator and earth switch were diagrammatically demonstrated. In addition, a table of the incomers 3-phase current as well as an animated display of the directional energised states of the incomer were visually depicted. When the incomer was de-energised the directional indicator, circuit breaker symbol, isolator symbol, earth switch and current numerals changed to green. Alternatively, when the incomer was in the energized state the directional indicator, circuit breaker symbol, isolator symbol, earth switch and current numerals changed to red. In the table of results depicted in Figure 4-10 a numerical reading of 0 A was captured for the incomer whist in the energized state. This reading was as a result of the de-energized status of the associated feeder and bus section, hence, the resulting load current in this instance was 0 A. The energized state of the incomer with full load current was shown on the SCADA at a later stage under steady state conditions in Figure 4-15 as well as on the IEDs HMI in Figure 4-16.



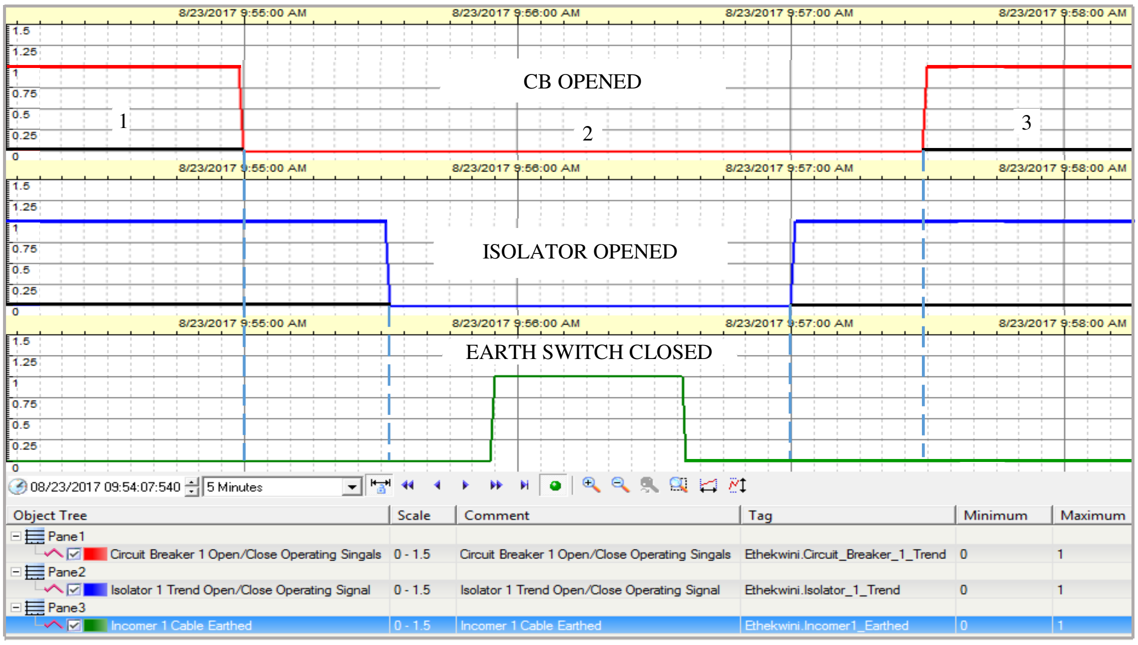
Device is on Local Mode!

(i) (ii) (iii) (iv)

Figure 4-11. Circuit breaker control panel

In order to remotely open and close the substations switchgear, as was demonstrated in Figure 4-10, an interactive control facility was developed using the intelligent templates of the CitectSCADA software model. Hence, by applying these facilities, the circuit breaker and isolator control panels were constructed as was illustrated in Figure 4-11. These windows, labelled: (i) to (iv), are pop-up windows and appeared when the operator clicked on either the circuit breaker or isolator symbols respectively. Once open, the operator could remotely open or close the particular circuit breaker or isolator in question. In addition, the status indicator in the pop-up window glowed green when the breaker was open and red when the breaker was closed i.e. green for safe and red for danger. The segments (i) and (ii) of Figure 4-11 visually demonstrated this concept.

An important consideration of the switchgear model shown in Figure 4-10 was that of interlocking. This feature ensured that if the circuit breaker and isolator were both closed then the circuit breaker should be opened first. Alternatively, if the circuit breaker and isolator were both open then it followed that the isolator be closed first. Hence, segment (iii) of Figure 4-11 prohibited the user from closing the breaker if the isolator was initially open. Lastly, if the mode of the IEDs controlling the switchgear was changed to 'local mode' then the circuit breaker or isolator in question could only be directly operated from the IED on the switchgear panel itself. This concept was illustrated in segment (iv) of Figure 4-11 where the window indicated that the device was in 'local mode'. Thus, remote operation of the switchgear from the SCADA model was disabled.



Object Tree	Scale	Comment	Tag	Minimum	Maximum
⊟ Pane1					
☑ 🟥 Circuit Breaker 1 Open/Close Operating Singals	0 - 1.5	Circuit Breaker 1 Open/Close Operating Singals	Ethekwini.Circuit_Breaker_1_Trend	0	1
⊟ Pane2					
☑ 🟦 Isolator 1 Trend Open/Close Operating Signal	0 - 1.5	Isolator 1 Trend Open/Close Operating Signal	Ethekwini.Isolator_1_Trend	0	1
⊟ Pane3					
☑ 🟩 Incomer 1 Cable Earthed	0 - 1.5	Incomer 1 Cable Earthed	Ethekwini.Incomer1_Earthed	0	1

Figure 4-12. Interlocking of switchgear

The interlocking of the switchgear on one of the incomers was graphically illustrated in the graph of Figure 4-12. In stage 1 the circuit breaker and isolator and were closed with the earth switch open. The circuit breaker was opened first in stage 2 followed by the isolator and then the earth switch closed. This order of operation ensured that the mechanical components of the isolator were not live during the interlocking process. Thereafter, the earth switch was opened followed by the closing of the isolator and finally, the circuit breaker. Hence, this type of interlocking prevented arcing across the contacts of the isolator when it was opened or closed. Additionally, the earth switch could only be operated when both the isolator and breaker were in the open positions and the incomer was de-energised.

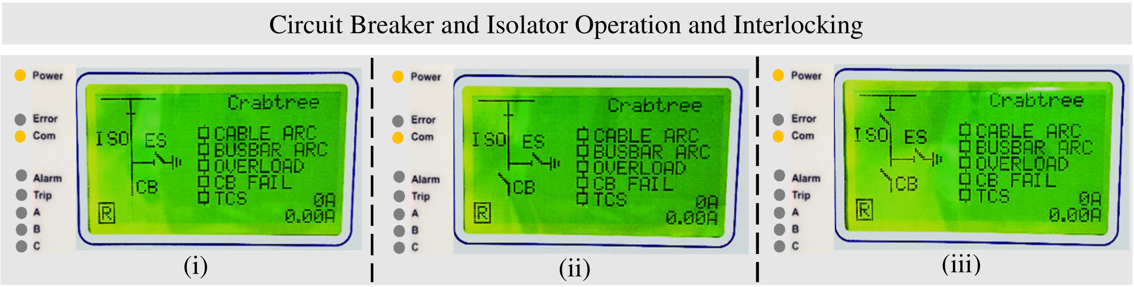
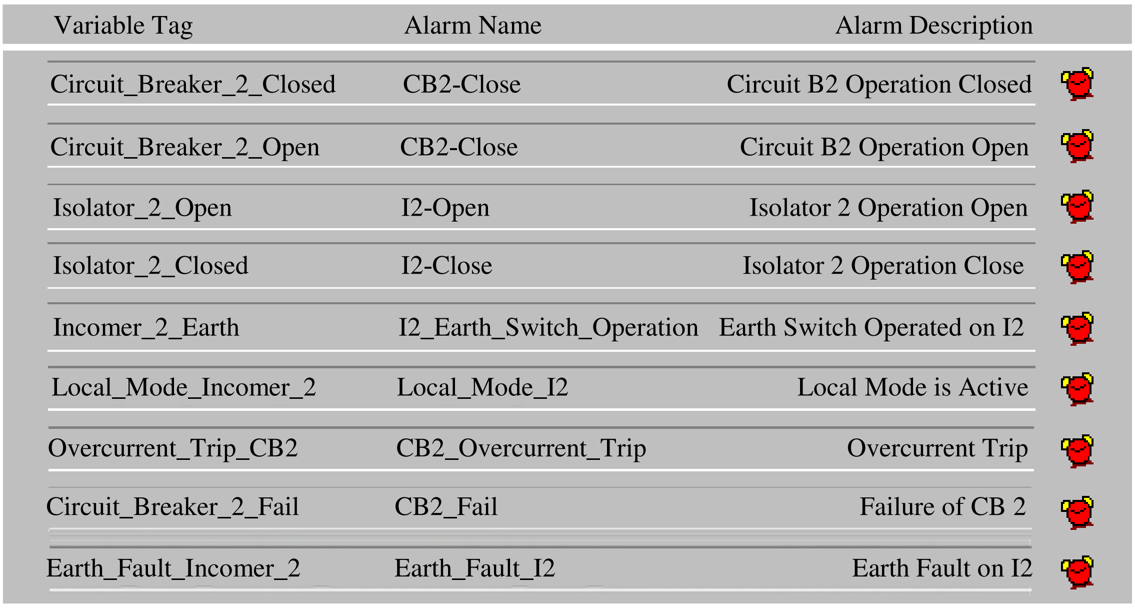


Figure 4-13. Switchgear operation and states of local HMI

The figures labelled (i) to (iii) in Figure 4-13 depicted the various stages of interlocking of the circuit breaker, isolator and earth switch on the IEDs HMI. This image showed both the isolator and circuit breaker as closed in segment (i) whilst the earth switch remained open. The circuit breaker was subsequently opened in (ii) followed by the isolator in segment (iii) which follows the appropriate rules of safe interlocking. The further operation of the earth switch could now be considered. Thereafter, this procedure was followed in reverse during reclosing from (iii) to (i).

(ii) Alarms

Table 4-6. Time stamped digital alarms



Variable Tag	Alarm Name	Alarm Description	
Circuit_Breaker_2_Closed	CB2-Close	Circuit B2 Operation Closed	⏰
Circuit_Breaker_2_Open	CB2-Close	Circuit B2 Operation Open	⏰
Isolator_2_Open	I2-Open	Isolator 2 Operation Open	⏰
Isolator_2_Closed	I2-Close	Isolator 2 Operation Close	⏰
Incomer_2_Earth	I2_Earth_Switch_Operation	Earth Switch Operated on I2	⏰
Local_Mode_Incomer_2	Local_Mode_I2	Local Mode is Active	⏰
Overcurrent_Trip_CB2	CB2_Overcurrent_Trip	Overcurrent Trip	⏰
Circuit_Breaker_2_Fail	CB2_Fail	Failure of CB 2	⏰
Earth_Fault_Incomer_2	Earth_Fault_I2	Earth Fault on I2	⏰

When a particular operation, fault or mode change was affected on the substations physical network, the SCADA model sent an alarm to the operator informing him/her of a particular event. The associated alarms for the incomer were populated in Table 4-6. These alarms alerted the user to operated equipment such as the circuit breaker, isolator and earth switch respectively. The alarms could also warn the user about hazardous fault conditions including: overcurrent, circuit breaker fail and earth faults as shown. Additionally, these digital alarms were time stamped, and thus informed the operator of the exact moment in time in which certain events had occurred. As a result, a comprehensive record of the networks operational activity could be established. Lastly, these alarms could be acknowledged by the operator on the SCADAs alarm page in order to be deactivated or cleared.

(iii) Status indicators

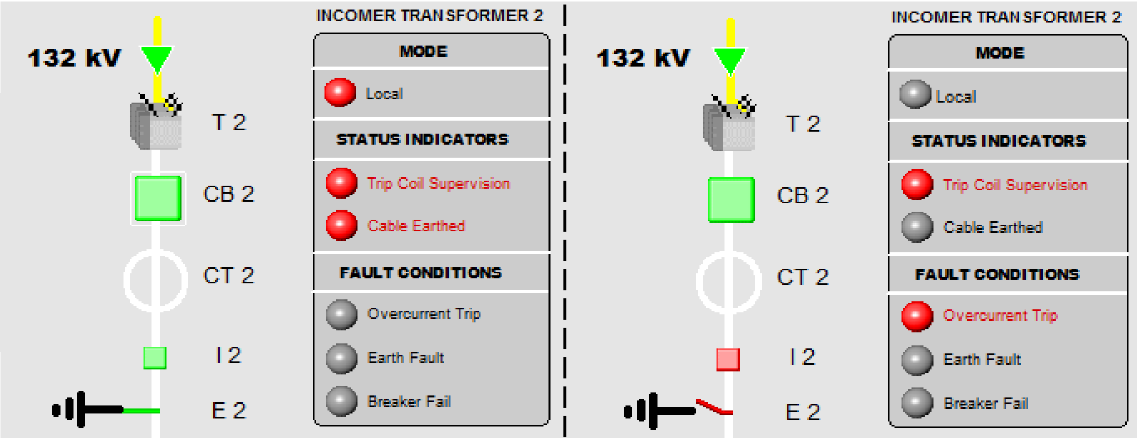
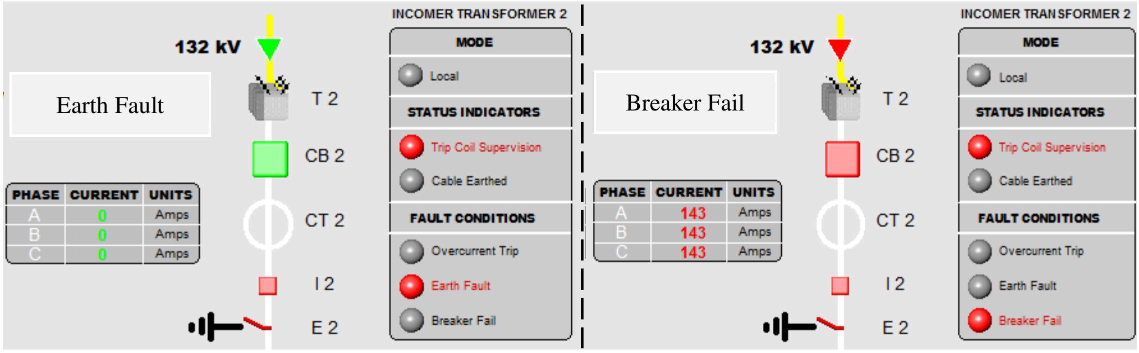


Figure 4-14. Local/remote, trip coil supervision, cable earthed and overcurrent status indicators



PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	143	Amps
B	143	Amps
C	143	Amps

Figure 4-15. Earth fault and breaker fail status indicators

The red and grey status indictors of Figure 4-14 and 4-15 illustrated items such as local mode, trip coil supervision, cable earth, overcurrent trip, earth fault and breaker fail conditions respectively. The indicators glowed red as shown when a particular feature or event was active and grey when inactive. In addition, when an overcurrent or earth fault had been applied to the system the circuit breakers in Figure 4-14 and 4-15 could be seen to have tripped and the current had fallen to 0 A. Alternatively, when the circuit breaker had failed it did not trip or clear the fault and the associated 3-phase current persisted. When a fault occurred, then an automatic trip signal would be created by the IED under normal operating conditions. Alternatively, an open command could be issued at any time by the remote end and delivered from the SCADA via the RTU to the IED. The IED may then issue a trip command and deliver it to the appropriate breaker. If the breaker did not trip within the appropriate time frame then it was said to have failed. Hence, when this occurred the breaker fail status indicator was activated. The result of this concept was illustrated in Figure 4-15.

In addition to the alerts, alarms and status indicators of the SCADA model; the HMI of the IED may also display informative and relevant information to the operator. In Figure 4-16 the results of local mode, trip coil supervision, circuit breaker, isolator and earth switch status as well as the 3-phase test currents were observed under steady state conditions. In addition, the IEDs HMI was also able to confirm the functionality of the circuit breaker fail indicator under fault conditions as and when an open command was delivered from the remote SCADA model to the IED. In Figure 4-16 a numerical reading of 0 A was captured on the HMI for the incomer under breaker fail conditions. This reading was as a result of the de-energized state of the associated feeder and bus section, hence, the resultant load current was 0 A.

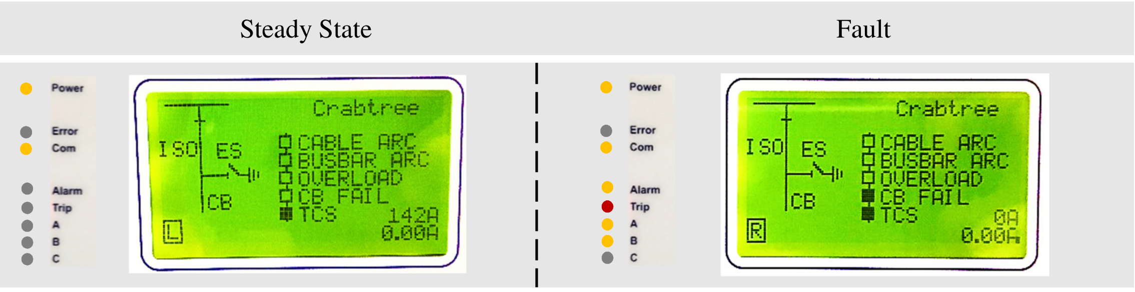
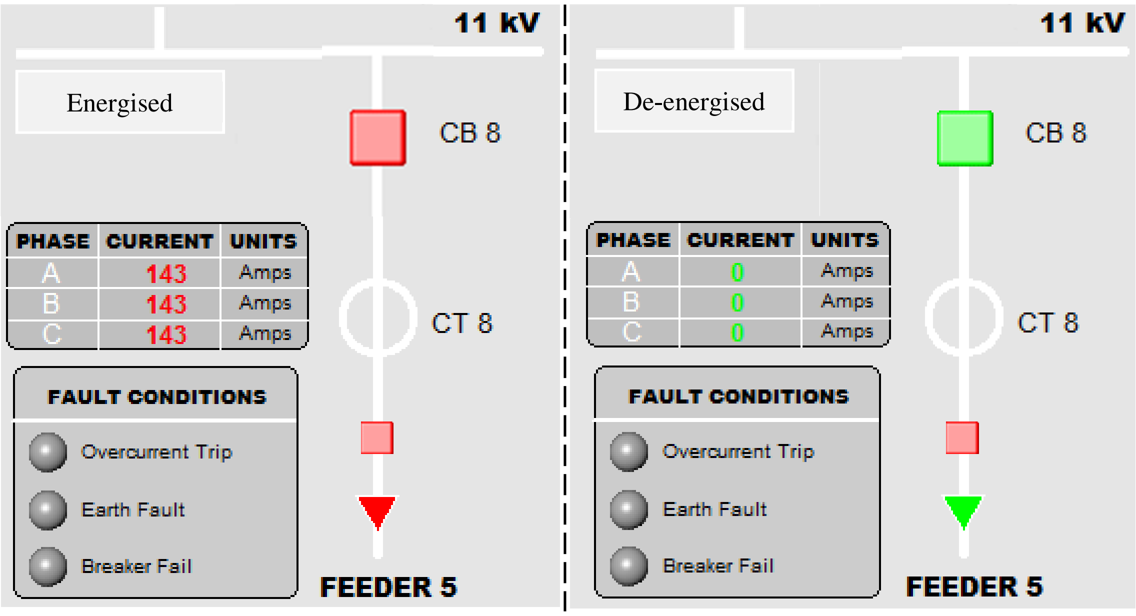


Figure 4-16. VAMP 259 HMI under steady state and fault conditions

(iv) Legacy relaying

The SCADA and HMI results from the interconnection of the MiCOM P122 legacy IED on feeder 5 of bus 2 were illustrated in Figures 4-17, 4-18 and 4-19 respectively. This relay communicated over the LBUS via serial RS 485 with the RTU. In Figure 4-16 the energised and de-energised states of feeder 5 were represented. In the energised state a steady state three-phase current of 143 A flowed through circuit breaker 8 and as a consequence the fault indicators remained inactive. In the de-energised state circuit breaker 8 was opened by the remote end cutting off the flow of current to the feeder as was shown by both Figure 4-17 and 4-18. Due to the limited number of digital inputs on the MiCOM P122 relay local mode, trip coil supervision, cable earth and the control of the operation and status of the isolator could not be implemented with only one IED. Therefore, the MiCOM P122 protection IED was only used to control the operation of circuit breaker 8 as well as monitor the currents, earth fault and breaker fail conditions over serial RS 485 using legacy Modbus RTU.

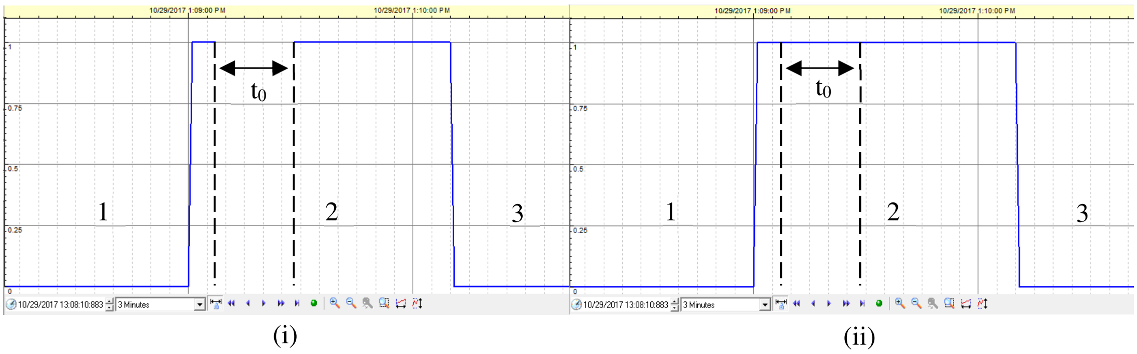


PHASE	CURRENT	UNITS
A	143	Amps
B	143	Amps
C	143	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 4-17. Energised and de-energized states of MiCOM P122 feeder

The two blue graphs, which shown by Figure 4-18, demonstrated the operation of the circuit breaker on feeder 5 of the substation model. Initially in stage 1 the circuit breaker was open; a close comment was then delivered from the IED to the breaker in stage 2 and finally in segment 3 the breaker was again opened. The first graph of Figure 4-18, labelled (i), showed the consequences of an interruption in communications between the MiCOM P122 relay and the RTU. This is characteristic of serial RS 485 and Modbus RTU since the lack of time stamped data means that information is lost during a communication outage. However, the component labelled (ii) is characteristic of what can be achieved in a DNP3 or in an IEC 61850-based environment where after a communication loss the time stamped data can be restored or updated to the system.



(i) (ii)

Figure 4-18. Graph of MiCOM P122 circuit breaker operation on feeder 5

The two components of Figure 4-19, labelled (i) and (ii), demonstrated the HMI of the energised (steady state) and de-energized operation of the MiCOM P122 IED which was connected on feeder 5 to control circuit breaker 8. In this figure the HMI of the IED was illustrated with a steady state current of 142 A in the energized state and 0 A when circuit breaker 8 was opened via the IED by a command from the remote end. Both of the images, labelled (i) and (ii), supported the SCADA results that were shown in Figures 4-17 and 4-18 showing the state change of switchgear.

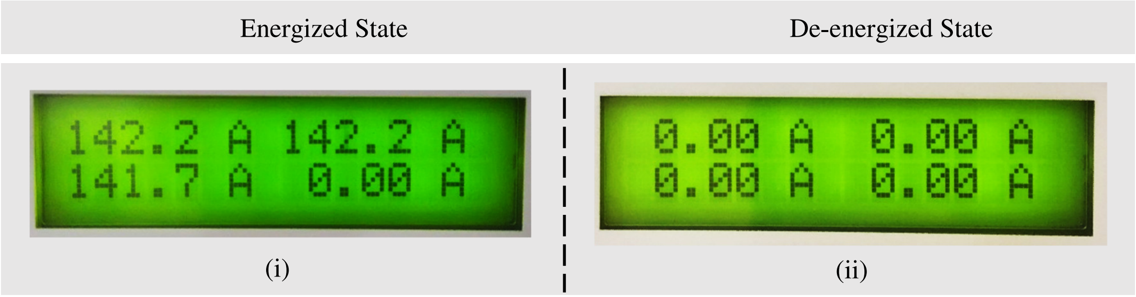
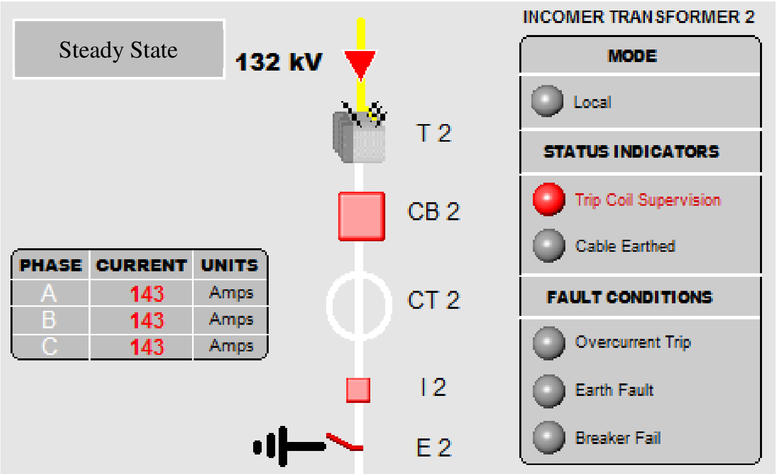


Figure 4-19. HMI of the MiCOM P122 IED on feeder 5

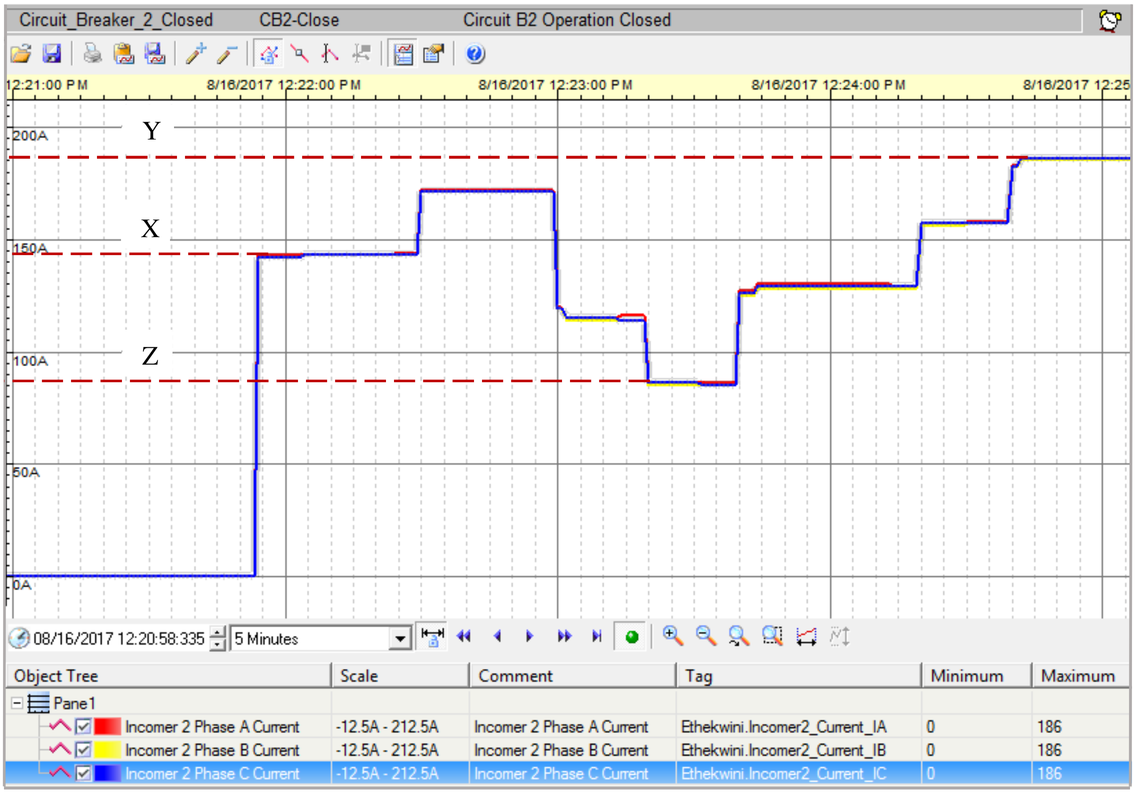
4.3.2 Steady state operation



PHASE	CURRENT	UNITS
A	143	Amps
B	143	Amps
C	143	Amps

Figure 4-20. Steady state operation on incomer 2

The steady state operation of the substations physical protection and automation network was simulated under normal operating conditions i.e. the injected current was below the pickup setting of the IEDs and there were no intentionally induced system faults. Therefore, as could be observed in Figure 4-20, the incomer was energized with a steady state load current of 143 A. In addition, there were no faults registered by the interactive status indicators. The injected load current was then changed using the test model from 143 A to a maximum of 186 A and a minimum of 86 A which was shown in Figure 4-21. This was done to simulate real-life changes in the load on bus 2 of the substation model. The system remained under steady state conditions during this time since the load current still fluctuated below the pickup setting of the protection IEDs, hence the stability of the network was maintained.



Circuit_Breaker_2_Closed CB2-Close Circuit B2 Operation Closed

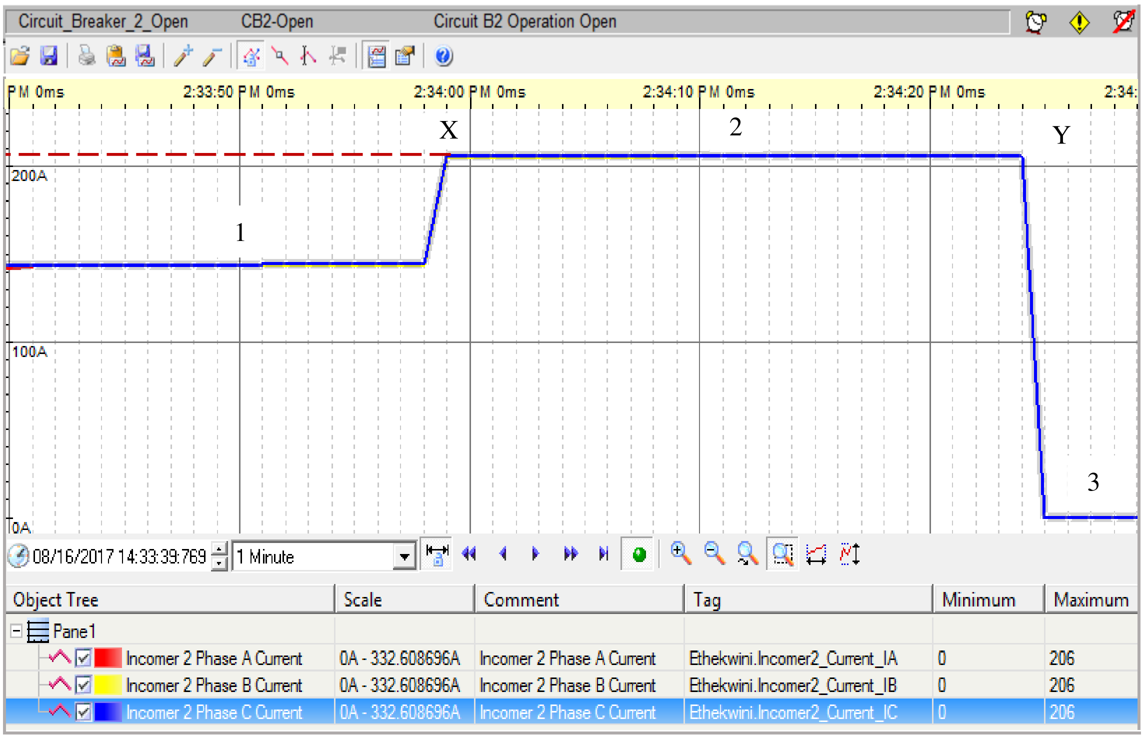
Object Tree	Scale	Comment	Tag	Minimum	Maximum
Pane1					
☑ 🟥 Incomer 2 Phase A Current	-12.5A - 212.5A	Incomer 2 Phase A Current	Ethekwini.Incomer2_Current_IA	0	186
☑ 🟨 Incomer 2 Phase B Current	-12.5A - 212.5A	Incomer 2 Phase B Current	Ethekwini.Incomer2_Current_IB	0	186
☑ 🟦 Incomer 2 Phase C Current	-12.5A - 212.5A	Incomer 2 Phase C Current	Ethekwini.Incomer2_Current_IC	0	186

Figure 4-21. Steady state operation and changes in load current

4.3.3 Fault Conditions

(i) Overcurrent

In this section of the results the 3-phase overcurrent characteristics of the substation model were tested in order to record the response of the protection equipment using the SCADA. A 3-phase test current was injected into one of the protection IEDs controlling a particular incomer. Therefore, in addition to the steady state conditions, by raising the injected 3-phase current the overcurrent protection of a particular IED could be tested. The graph shown in Figure 4-22 illustrated 3 zones of operation for an incomer. The first zone dealt with steady state conditions, the second with overcurrent and the third respective zone represented the post trip stage. In Figure 4-22 the incoming current was initially set at 143 A in stage 1, which was below the pickup setting of the IED, thereafter an overcurrent of 206 A was applied at point ‘X’. This overcurrent persisted according to the inverse time characteristics of the IED in question. After a time delay, the IED then finally issued a trip signal to the circuit breaker which opened at point ‘Y’. Hence, the 3-phase circuit on the incomer was interrupted and the current had fallen to 0 A. This concept was illustrated in stage 3 of Figure 4-22.



Circuit_Breaker_2_Open CB2-Open Circuit B2 Operation Open

08/16/2017 14:33:39:769 1 Minute

Object Tree	Scale	Comment	Tag	Minimum	Maximum
⊟ Pane1					
☑ 🟥 Incomer 2 Phase A Current	0A - 332.608696A	Incomer 2 Phase A Current	Ethekwini.Incomer2_Current_IA	0	206
☑ 🟨 Incomer 2 Phase B Current	0A - 332.608696A	Incomer 2 Phase B Current	Ethekwini.Incomer2_Current_IB	0	206
☑ 🟦 Incomer 2 Phase C Current	0A - 332.608696A	Incomer 2 Phase C Current	Ethekwini.Incomer2_Current_IC	0	206

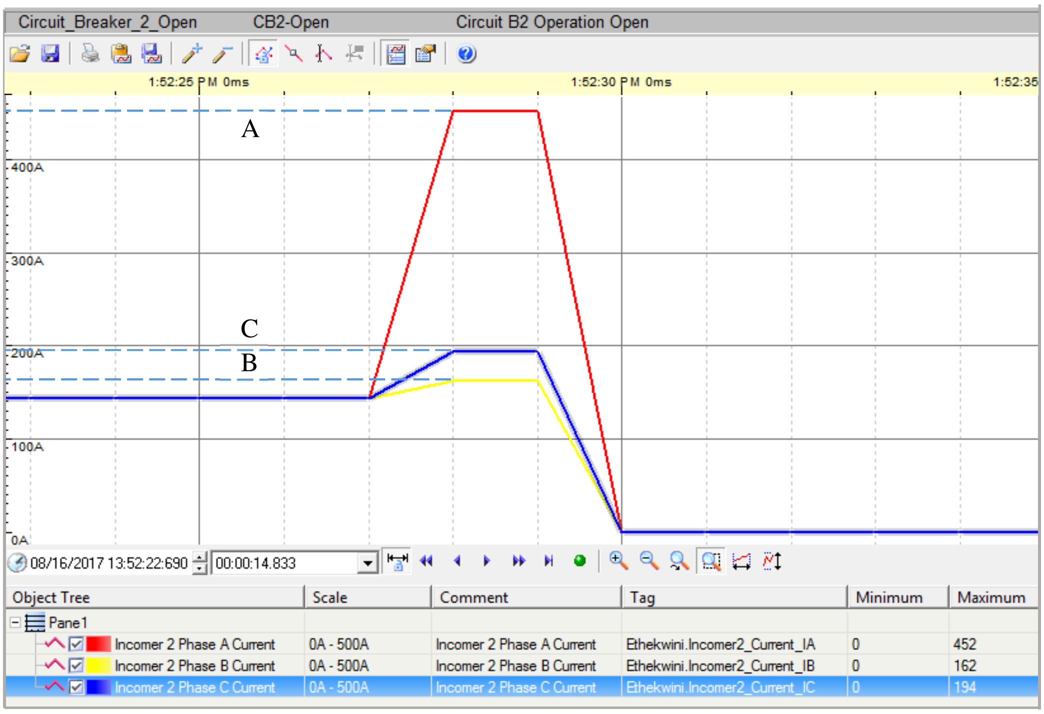
Figure 4-22. Overcurrent trend

(ii) Earth fault

In this section of the results three separate earth faults were applied to the incomer to test and observe the earth fault response of the physical network. The results of each scenario were recorded using the SCADA model. For the purposes of display, the earth faults that were applied on the incomer were designed to persist for a longer period of time then would be practically expected under normal fault conditions. This procedure was adopted so that the spike in fault current could be registered by the process analyst of the SCADA host. The faster fault currents could not be monitored by the process analyst on the SCADA model as its fastest sampling rates were insufficient with regard to capturing the entire response.

A. Single phase to ground

A single phase to ground fault was the first earth fault to be applied on phase A of one of the incomers in the substation electrical network. As a result of this earth fault, there was an associated induced fault current on phase A as well as an unbalanced increase of the currents on the phases B and C respectively. The RMS value of the fault current of the single phase to ground fault was illustrated in Figure 4-23. This graph showed when the fault was applied as well as the associated tripping of the circuit breaker on the incomer which occurred after the appropriate time delay. The incomer current reduced to 0 A and when the circuit breaker opened and the fault was cleared.

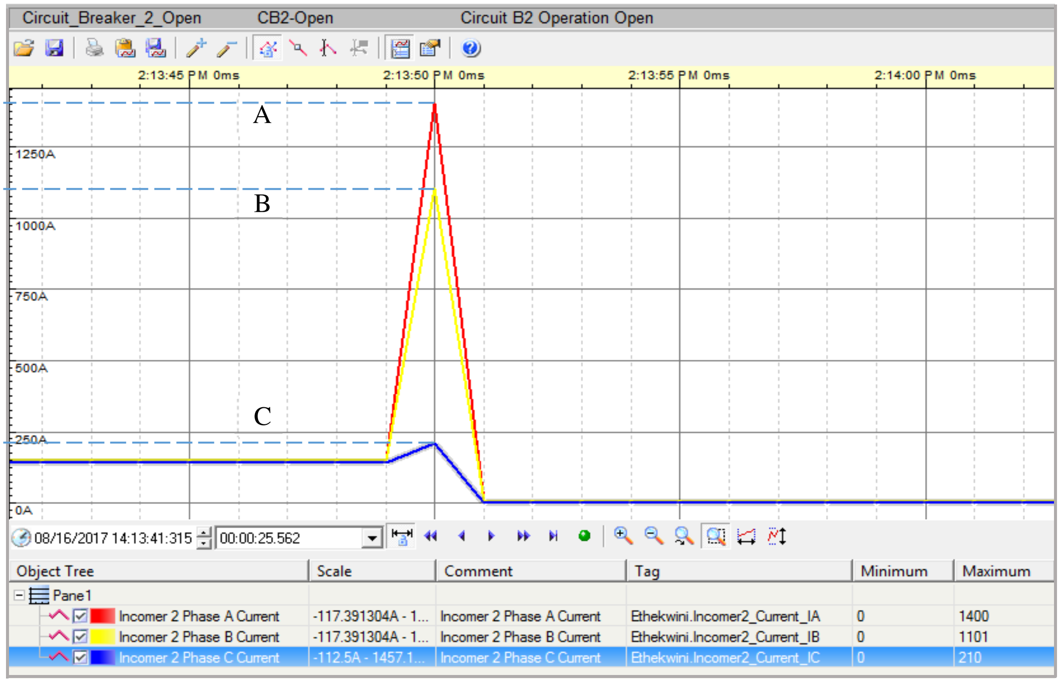


Object Tree	Scale	Comment	Tag	Minimum	Maximum
⊟ Pane1					
☑ 🟥 Incomer 2 Phase A Current	0A - 500A	Incomer 2 Phase A Current	Ethekwini.Incomer2_Current_IA	0	452
☑ 🟨 Incomer 2 Phase B Current	0A - 500A	Incomer 2 Phase B Current	Ethekwini.Incomer2_Current_IB	0	162
☑ 🟦 Incomer 2 Phase C Current	0A - 500A	Incomer 2 Phase C Current	Ethekwini.Incomer2_Current_IC	0	194

Figure 4-23. Single phase to ground fault on red phase

B. Double phase to ground

A double phase to ground fault was applied on the phases A and B respectively. The resulting trend, illustrated in Figure 4-24, depicted the response of the unbalanced fault currents on each of the three phases. The circuit breaker tripped and the currents fell to 0 A when the fault was cleared.

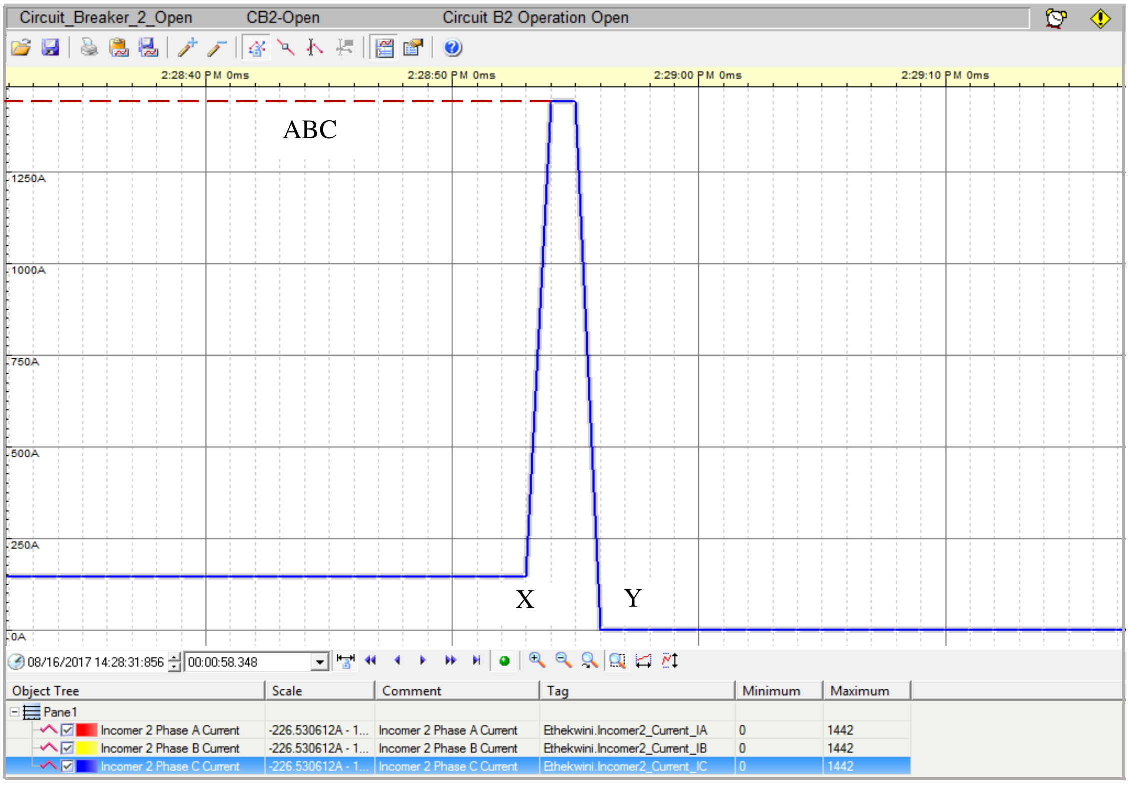


Object Tree	Scale	Comment	Tag	Minimum	Maximum
⊟ Pane1					
☑ 🟥 Incomer 2 Phase A Current	-117.391304A - 1...	Incomer 2 Phase A Current	Ethekwini.Incomer2_Current_IA	0	1400
☑ 🟨 Incomer 2 Phase B Current	-117.391304A - 1...	Incomer 2 Phase B Current	Ethekwini.Incomer2_Current_IB	0	1101
☑ 🟦 Incomer 2 Phase C Current	-112.5A - 1457.1...	Incomer 2 Phase C Current	Ethekwini.Incomer2_Current_IC	0	210

Figure 4-24. Double phase to ground fault on red and yellow phase

C. 3-phase to ground

Lastly, a three phase to ground fault was applied on all the phases of the incomer at point X, as was demonstrated in Figure 4-25. Hence, there was an associated balanced fault current on each of the respective phases as was shown. As in the previous cases, the circuit breaker cleared the fault when it tripped and the currents reduced to 0 A. The operation of the circuit breaker during the three earth fault conditions was illustrated on the SCADA in Figure 4-14.



08/16/2017 14:28:31:856 | 00:00:58.348

Object Tree	Scale	Comment	Tag	Minimum	Maximum
Pane1					
☑ 🟥 Incomer 2 Phase A Current	-226.530612A - 1...	Incomer 2 Phase A Current	Ethekwini.Incomer2_Current_IA	0	1442
☑ 🟨 Incomer 2 Phase B Current	-226.530612A - 1...	Incomer 2 Phase B Current	Ethekwini.Incomer2_Current_IB	0	1442
☑ 🟦 Incomer 2 Phase C Current	-226.530612A - 1...	Incomer 2 Phase C Current	Ethekwini.Incomer2_Current_IC	0	1442

Figure 4-25. 3-phase to ground fault on all phases

D. Fault currents

Ground faults can result in very high fault currents that flow in a three-phase system posing a possibility of damage to expensive equipment like transformers, underground cables, transmission lines, terminations, instrument devices and many other components of a power system. One such example is common with regard to the use of bundle conductor which is utilized over large transmission lines as well as within substations. When large fault current flows down a conductor bundle there is a resultant force that draws the individual cables together. This force can cause the bundle spacers to bend and deform under short circuit fault conditions.

Hence, for our power systems, it is imperative that fast, reliable, secure and efficient communications be employed to ensure that fault currents are extinguished or isolated within the appropriate amount of time before lasting damage is incurred on a particular system. It is because of the efficiencies, convenience and speed of communication (via GOOSE) which can be administered using the IEC 61850 substation protocol that protection IEDs located at different points on the network can coordinate effectively to clear such currents. In addition, if fault currents persist and conditions of breaker fail occur the intelligent IEC 61850 protocol with its GOOSE message class can be used to administer back-up protection to a system. This may be achieved much faster and in a more convenient and effective manner than was possible using traditional legacy back-up or overcurrent protection. This has all been made possible by the fast Ethernet-based communication networks, intelligent switches, advanced Gateways and compliant modern IEDs on which the technology of the IEC 61850 standard is based.

4.4 Analysis and discussion

In order to assess the perceived, preferred and technical benefits or downsides of different substation communication protocols, an experimental network was established. This involved designing a SCADA blueprint as was outlined in section 4.2 as well as a physical communication model consisting of an RTU, IEDs as well as the associated switchgear which was discussed in section 4.4. Therefore, in this chapter an analysis of the developed network as well as the implementation of protocols like the IEC 61850 standard, Modbus RTU and DNP3 was undertaken. In subsection 4.5 the preliminary results that were recorded from the elementary communication network were validated. The substation model comprised two incomers, five feeders, two buses and an associated bus section. In chapter 4, the performance of the substation and by extension its equipment was tested and the distinct functional outcomes of the model itself were captured.

The SCADA that was demonstrated in Figure 4-2 and whose results were captured in the previous section, achieved remote operation and monitoring over the IEDs and switchgear that were connected on the physical network. The interactive alerts, alarms, displays and trends were illustrated under different fault conditions as well as under steady state. Therefore, it was demonstrated that information, data and commands could be transferred from a remote CitectSCADA host over an Ethernet link, using the telecontrol bus and DNP3 directly to an RTU which mediated the transfer of signals and the exchange of state variables on its database. Once, actionable variables within the RTU were changed or commands received this information was sent to the subscribing IEDs on the SBUS using the IEC 61850 substation protocol or to legacy relays using Modbus RTU over the LBUS. When information was sent and received by the IEDs the actionable outcomes of the commands or the change of state changes could be managed. The results of commands sent from the SCADA to the RTU and from the RTU to the IEDs and vice versa were demonstrated by the trends, pictures and screen grabs of the open/close requests, fault conditions, trip responses, interlocking as well as mode and status changes demonstrated in the Figures 4-10 to 4-25.

The results of chapter 4, illustrated in subsection 4.5, revealed and validated both the sound and effective operation of a quintessential substation physical network, SCADA and associated communications. The benefits of the chosen communication media, transport mechanisms and the implementation thereof were assessed as follows in the conclusion.

4.5 Conclusion

The primary objective of chapter 4 was to demonstrate the foundation of the broader research model. In order to achieve this, a typical electrical network was used to illustrate the functionality of substation equipment; specifically, the interfaces and transport links between IEDs that rely on protocols like DNP3, Modbus RTU and the IEC 61850 standard to communicate.

The communication network that was established during the course of this chapter used a common protocol like DNP3 over the telecontrol bus between the SCADA host and the RTU as well as the new IEC 61850 standard and older Modbus RTU protocol between the RTU and IEDs on the station and legacy buses respectively. DNP3 is typically used as a SCADA protocol between the substation and the control centre due to the fact that it stores all the system changes and includes the time and date stamp of a particular event at the point at which the change had occurred [31]. The alarms and event capturing capabilities of the CitectSCADA model relied of this capacity of DNP3 so that time stamped digital alarms could be configured. When the RTU communicated with the SCADA it sent all the necessary information as and when it was required, therefore if there was a break in communications DNP3 ensured that the system updated all the missing time stamped data [31]. Additionally, DNP3 may be configured such that it only updates when a variable state toggles. This ensured that there were notifications for immediate problems whilst at the same time not clogging up the bandwidth of the network [31]. DNP3 also allowed the use of acknowledgements from the SCADA model which ensured that the data had been sent and received by the host [31]. Thus, DNP3 has advantages over protocols like Modbus RTU which does not store state changes or have any time stamping of its messages. This means that Modbus RTU, being a two wire RS485 serial communication mechanism, can only tell the user that a variable has changed, not when and how many times it has done so [31]. In addition, if communication is lost between the Modbus RTU slave and the master data that elapses during the outage is and cannot be updated. Hence, the DNP3 protocol was an obvious choice for the telecontrol bus in the network that was established in chapter 4. Alternatively, Modbus was implemented on the legacy bus between the RTU and a compliant IED.

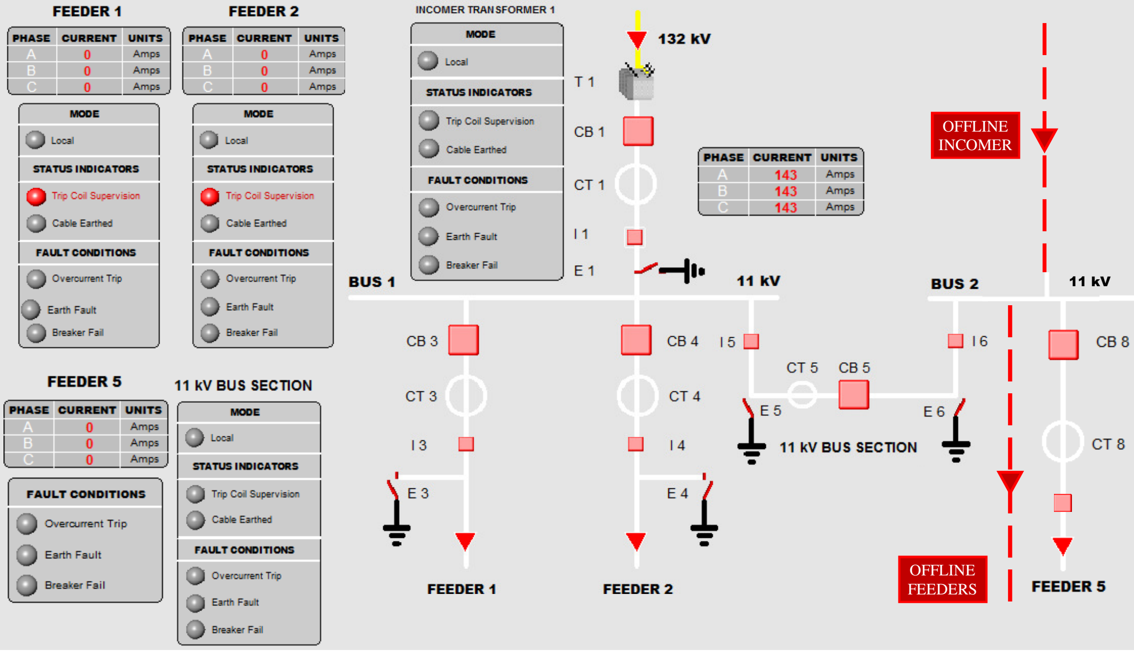
The main focus of this dissertation was on the IEC 61850 protocol. Hence, not being a remote protocol, this standard was implemented within the substation itself between the RTU and the IEDs in chapter 4 as well as directly between the IEDs themselves in chapter 5. REPORT messaging was used between the RTU and the IEDs in order to report the changes in the status of components like circuit breakers, isolators and earth switches as well as fault conditions and modes of operation. Lastly, the GOOSE message class, which can be used between the IEDs in order to achieve fault clearing under breaker fail conditions, was investigated in the following chapter. The advantages of the IEC 61850 protocol ensured that each IED on the station bus was interoperable and aware of the state of operation of adjacent IEDs and could effectively interoperate as and when was required. In addition, both the IEC 61850 standard and DNP3 are "virtual" protocols that operate over a LAN. Hence, this works to reduce the number of cross-wired binary copper connections between IEDs and related devices saving cost, labour and increasing efficiency.

The introduction of protocols like DNP3 and the IEC 61850 standard in chapter 4 assisted the electrical network in Figure 4-2 during its operation and function as a typical substation. The results of this functionality were illustrated in subsection 4.5 which discussed the results of SCADA, general operation, interlocking, steady state, alarming, over current, earth fault and breaker fail conditions. This model formed the basis for the primary research objective. In the subsequent chapter further expansion of the IEC 61850 protocol as well as the assessment of rival protocols were explored.

5. Protection-Based Applications of IEC 61850 and GOOSE

The practice of implementing modern microprocessor-based relays, which show compliance with the IEC 61850 substation protocol, at distribution points has become more frequent. This has resulted in the optimization of protection schemes that were previously too complicated, too labour intensive or far too expensive to be justified [1]. Three such examples of these protection schemes include: breaker fail protection, arc-flash protection and blocking response which is also referred to as sympathetic trip protection [1]. Therefore, smart microprocessor-based relays, the IEC 61850 standard and its intelligent GOOSE message class have changed the way protection is administer to devices and equipment. This has ensured that relative simplicity, assured reliability and nominal security exists when applying the aforementioned methods of relaying to equipment at distribution points or substations [1].

It was in chapter 5 that the main body of research for this dissertation was demonstrated and discussed. The following section of this study was based on first principles, intensive background research as well as on the groundwork which was prepared during the course of the preliminary works in chapter 4. The subsections of chapter 5 sought to investigate the breaker fail, arc-flash protection and blocking applications of the IEC 61850-based GOOSE message class. The steady state operation of the substation model for chapter 5 (before disturbance) was illustrated in Figure 5-1 as was shown. It is important to note that in Figure 5-1 there was an injected test current on the analog inputs of incomer 1 IED (unseen by the other relays) and that incomer 2 and feeder 3 and 5 from chapter 4 were offline and played no part in further investigations.



FEEDER 1

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 2

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

INCOMER TRANSFORMER 1

PHASE	CURRENT	UNITS
A	143	Amps
B	143	Amps
C	143	Amps

FEEDER 5

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-1. Unfaulted state of substation model for chapter 5 study

5.1 Breaker fail protection

Today's progressive developments in modern technology have seen the inception of new and innovative IEC 61850-compliant IEDs. Devices such as these have become commercially available from many different vendors including: ABB, Schneider, SEL, Siemens and Arcteq to name but a few. These manufacturers will typically incorporate numerous protection, monitoring, automation and control functions such as reclosing as well as breaker fail protection within their new products [4], [19]. Commonly, IEDs such as those mentioned, would possess sophisticated control structures that are capable of controlling up to two circuit breakers. Therefore, as a result of this dual control, the aforementioned protection structures can be implemented to manage substation equipment in breaker-and-a-half and ring bus protection schemes respectively [4], [19]. However, in some cases a power utility or design engineer could choose to use a single exclusive IED to perform the reclosing function or to initiate breaker fail protection within a particular substation [4], [19].

Breaker fail protection is a function that traditionally occurs in combination with reclosing and most IEDs will typically have inbuilt breaker fail protection and other functions for a certain bay. It is often initiated by a trip command that is within or external to the protection terminal [32]. In conventional substations, breaker fail protection works using a timer that activates once an IED has issued a trip signal to a particular breaker [4], [19]. Furthermore, as the timer ticks the relevant IED will monitor the three-phase current through the circuit breaker to check whether or not it has been extinguished [4], [19]. Therefore, with no or a very brief time delay, the relay will issue a second trip signal or consequently trip the neighbouring breakers to isolate the faulted circuit if the breaker current was not initially completely interrupted [32], [4], [19].

Alternatively, a separate dedicated IED may be used for breaker fail protection of a particular bay. The use of an extra IED enables the protection scheme to incorporate additional monitoring and control functions like gas pressure and ambient temperature supervision [4], [19]. In traditional substations, the control and trip signals may be exchanged using the IEDs physical inputs/outputs as well as using the serial copper hardwire connections of the legacy era. In the past, breaker fail relaying has been sparsely established at the distribution level because of the expense and the complications that were typically involved with the old electromechanical protection schemes [32]. However, the IEC 61850 protocol has allowed for the fast, reliable and secure exchange of GOOSE messages over the substation LAN. Hence, breaker fail protection can be achieved using this intelligent message mechanism making it far simpler and more efficient to implement. Therefore, protection can now be carried out 'virtually' over an Ethernet-based local area network using GOOSE and trip signals can be retransmitted as and when is required by the IEDs.

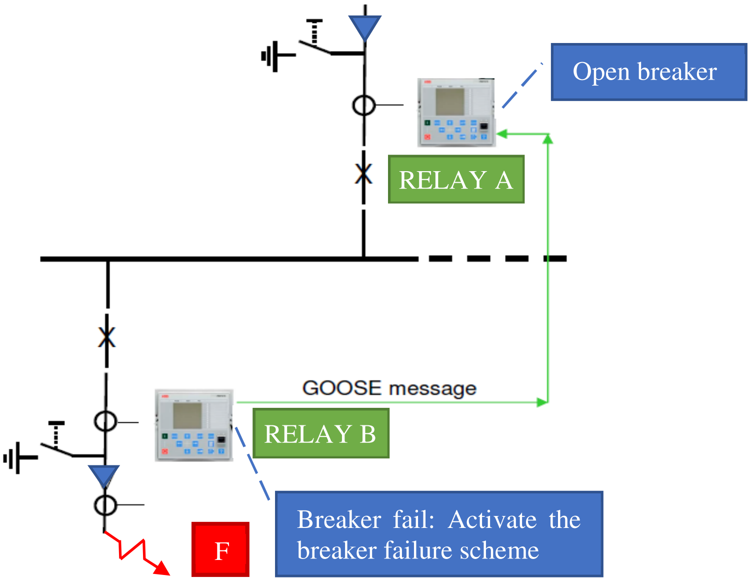


Figure 5-2. Intercommunication of feeder and incomer IEDs during breaker fail [22]

An elementary example of breaker fail protection was diagrammatically illustrated in Figure 5-2. In the above schematic there was a ground fault which occurred on the outgoing feeder (labelled "F") resulting in an overcurrent condition. This fault was seen by both the feeder IED (Relay B) and the incomer IED (Relay A) as a result of a rapid increase in current through both of the circuit breakers. Relay B on the outgoing feeder would detect the fault first, issue an open command to its circuit breaker and start the breaker fail protection procedure [22]. If the protection failed on the feeder and the circuit breaker managed by Relay B did not open then the fault must be cleared by other means. Therefore, after a certain amount of time the IED at Relay B would send out a backup message, in the form of a GOOSE request, to the incomer IED asking it to trip its circuit breaker [22]. Upon receipt of this GOOSE message from Relay B, Relay A would issue a trip command to its circuit breaker which would then operate and cleared the fault [22]. An example of this inter-IED GOOSE communication between Relay A and Relay B in the case of breaker fail during an outgoing feeder fault was shown in Figure 5-2.

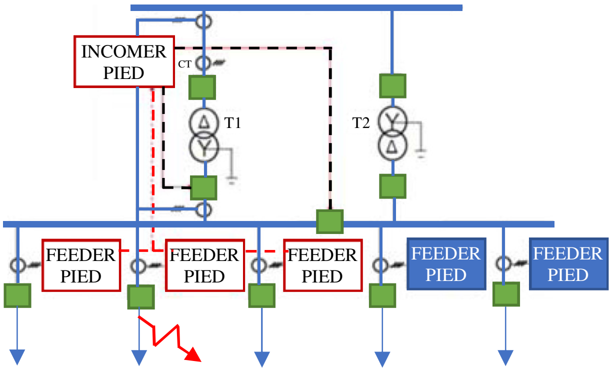


Figure 5-3. Breaker fail protection on a typical distribution bus scheme [19]

A slightly more complex example of breaker fail protection was shown by Figure 5-3 using a typical distribution bus scheme. Breaker fail protection is usually implemented at the distribution level of a network to prevent the occurrence of instability on the grid in the case of a breaker misoperation during a fault [19]. As previously mentioned, many IEDs have inbuilt protection functions that can achieve this outcome. Furthermore, IEC 61850-compliant IEDs make protection even more convenient using the GOOSE message class. Being a fast message system, GOOSE subscribes to the requirements of present day protection which calls for the decrease in the time duration of faults [19].

There are two predominant GOOSE-based methods of breaker fail protection which are defined by the location of the breaker fail protection element. In the first method the breaker fail protection element resides within the multifunctional transformer protection relay situated on the incomer [19]. When the distribution feeder IED operates it will send a GOOSE message to all the adjacent subscribing relays which indicates the change of state of its functional elements like switchgear [19]. The incomer IED will receive this information and perform the appropriate actions. If the feeder relay has failed to trip its circuit breaker, the fault will ensure that the system current remains above the pickup setting of the breaker fail detection element and after a particular delay in time the incomer IED will trip the appropriate circuit breakers [19].

The second method of breaker fail protection relies on the inbuilt protection elements of each of the feeder relays. When the feeder IED sends a trip command it automatically initiates the breaker fail protection function. If the feeder IED fails to trip its circuit breaker the breaker fail protection function will activate and it will send a GOOSE message to all of the neighbouring IEDs informing them that they must act to extinguish the fault [19]. Once the neighbouring relays have sent trip commands to their respective breakers the fault can be cleared. Hence, this concept was visually depicted in Figure 5-3 on the previous page.

5.1.1 GOOSE configuration

In order to investigate the IEC 61850 GOOSE-based implications of breaker fail protection the substation communication network of chapter 4 was modified to study these outcomes. The station level SCADA model which was established on CitectSCADA was used to monitor the results of breaker fail and supervise the status of a network of interconnected substation hardware. The VAMP 259, VAMP 255, MiCOM C264 and MICOM P122 protection and automation devices were used. In addition, the configuration of inter-IED GOOSE messaging between the VAMP relays and the RTU was established using VAMPSET. Hence, this software configurator allowed the operator to setup communications between the IEDs themselves. The MiCOM P122 communicated using serial Modbus RTU on the legacy bus and played no direct part in the

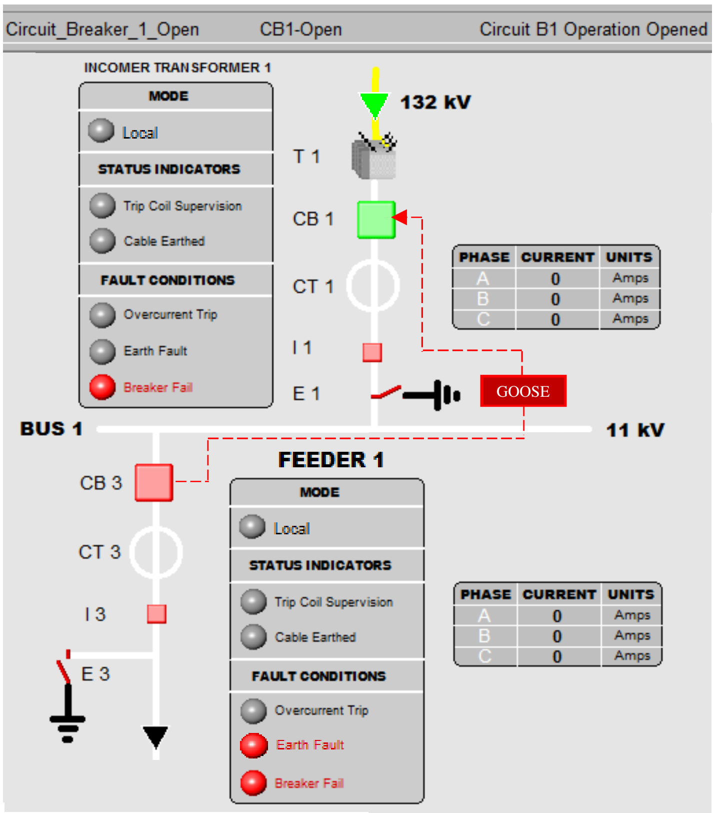
GOOSE investigation. The following VAMPSET menus were used to organise the IEDs GOOSE characteristics and setup the publisher and subscriber IED parameters:

a. Publisher Configuration: this menu accessed the GOOSE control blocks and set parameters such as the GOOSE ID and application ID.
b. Subscriber Configuration: defined the devices or IEDs that subscribed to receive information from a particular message stream.
c. GOOSE Control Block Data Points: which selected which control signals were being configured as GOOSE.
d. Subscriber Data Points: defined which IEDs can access information from other IEC 61850 devices as well as to which message stream the current IED is subscribing.
e. GOOSE Matrix: defined the signal name as well as the type of input. Network inputs are signals received by an IED via GOOSE over an Ethernet link whereas virtual inputs are those inputs that are internal to the device.
f. Logic: here the logical outcome of the GOOSE message may be defined using gates to generate a virtual output.
g. IED Output Matrix: the generated virtual output can be connected to one of the IEDs output relays such as T1 to trip a circuit breaker as well as to the alarms and LED indicators of the IED.

5.1.2 Results of breaker fail protection

(i) Elementary breaker fail protection

On an IEC 61850-based network the protection IEDs can send critical information or control commands to their peers using the GOOSE message class. In the following subsection this concept was investigated under breaker fail conditions. When a circuit breaker of a particular feeder failed to operate, the IEDs on both the feeder and the associated incomer could communicate this failure using the GOOSE message class. Thus, the proper use of the breaker fail protection element and GOOSE can enable IEDs to trip the affected protection zone, isolate malfunctioning equipment and clear the fault. This concept was diagrammatically illustrated in Figure 5-4 of the experimental substation model which was represented in Figure 4-2 in chapter 4. This schematic showed the associated states of the feeder and incomer circuit breakers under the simulated fault conditions. In Figure 5-4 a trip command was automatically sent from the outgoing feeder IED to the circuit breaker (CB3) on feeder 1 as a result of a double-phase to earth fault. The ‘breaker fail’ status indicator of feeder 1 became active since the circuit breaker (CB3) had failed to open within the appropriate timeframe (or did not operate at all). Thereafter, using the breaker fail protection element, the feeder IED delivered a GOOSE message to the incomer IED which tripped the circuit breaker (CB1) on the incomer and the earth fault was extinguished.

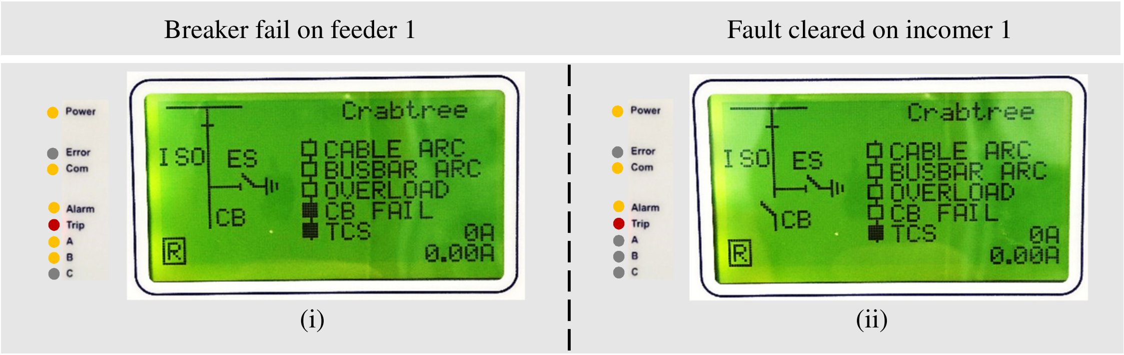


Circuit_Breaker_1_Open CB1-Open Circuit B1 Operation Opened

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-4. Circuit breaker fail on feeder 1 and GOOSE message response



Breaker fail on feeder 1

Fault cleared on incomer 1

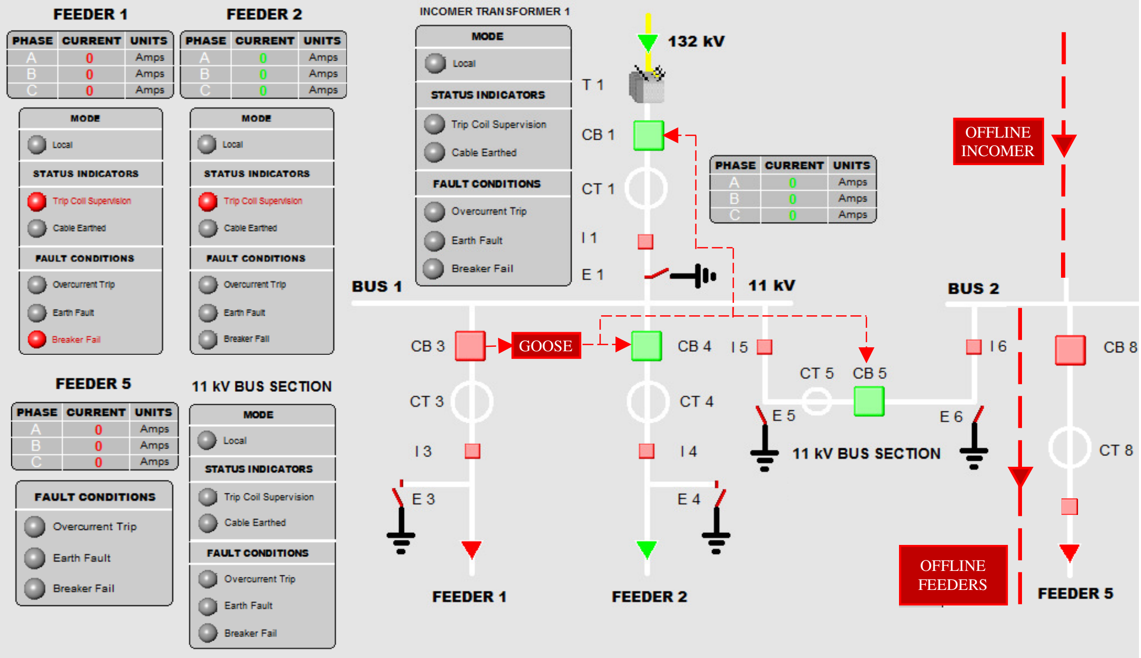
(i)

(ii)

Figure 5-5. Breaker fail on feeder 1 and fault clearing using grading on incomer 1

The pictures of the HMI from the feeder and incomer IEDs under breaker fail conditions were illustrated in Figure 5-5. These images demonstrated the failed operation of the feeder circuit breaker which remained in the closed position (i) as well as the associated operation of the incomer circuit breaker which opened in response to the GOOSE message that was sent from the feeder IED (ii). In addition, the “CB Fail” indictor of the feeder IED was active as was shown in segment (i). The items, labelled (i) and (ii), depicted in Figure 5-5 related to the substation model given by Figure 5-4. In addition, the red LED trip indicators of both IEDs were active to illustrate the issuing of trip commands to the respective breakers and the yellow LEDs of phases A and B were in the latched state in segment (i). This indicated a double-phase to earth fault on the phases A and B of feeder 1 respectively.

(ii) Breaker fail on a distribution bus scheme


FEEDER 1

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 2

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 5

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-6. Breaker fail on CB3 of feeder 1 and inter-IED GOOSE message response

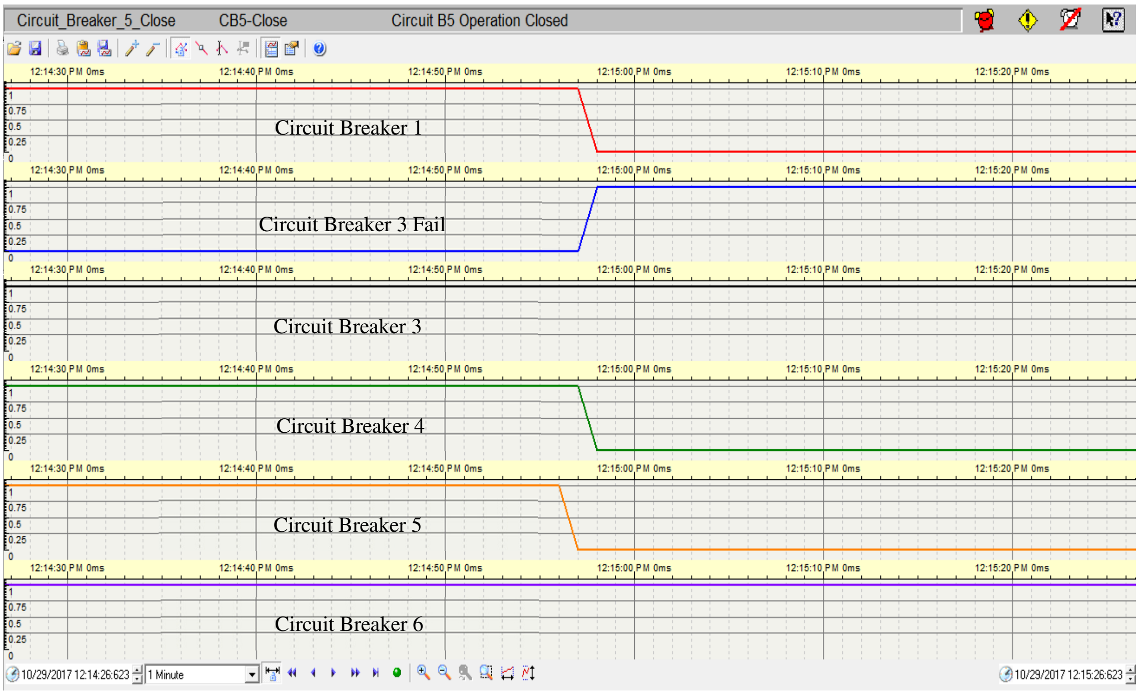
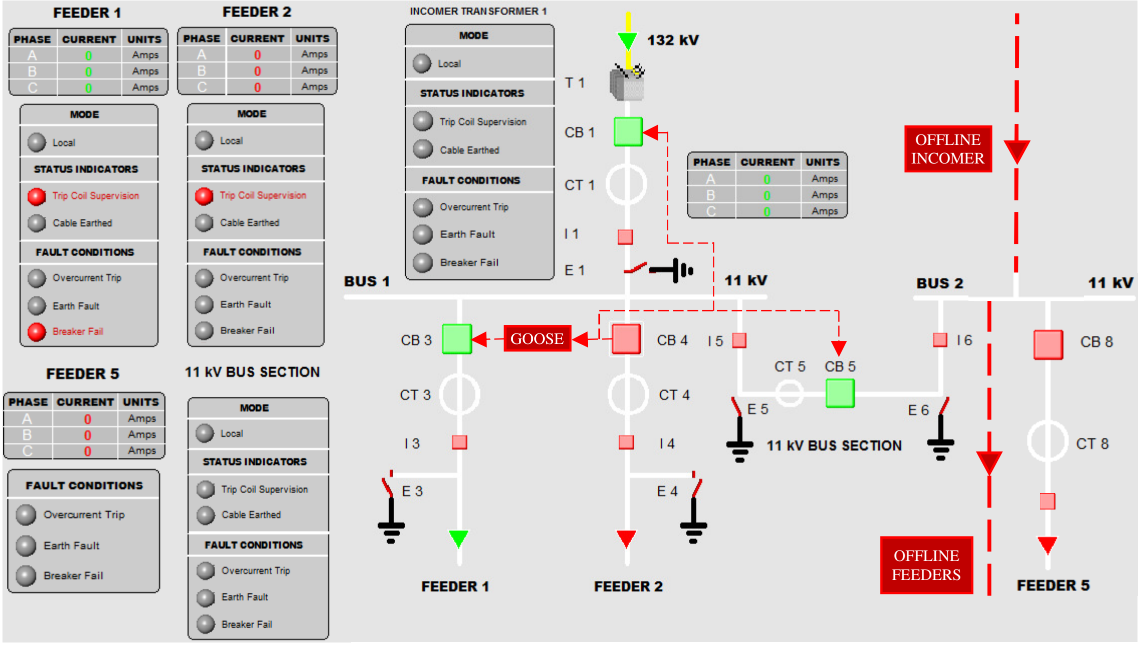

Circuit_Breaker_5_Close CB5-Close Circuit B5 Operation Closed

Figure 5-7. Graph of the operation of substation switchgear and breaker fail on CB 3



FEEDER 1

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 2

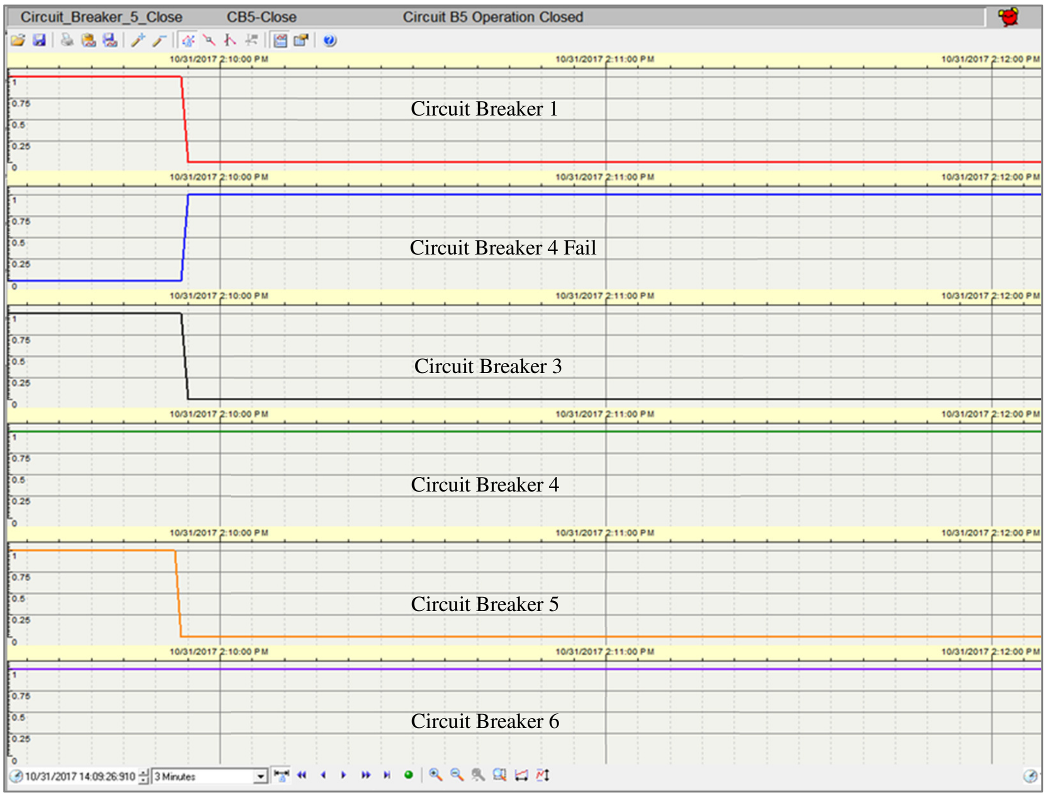
PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 5

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-8. Breaker fail on CB 4 of feeder 2 and inter-IED GOOSE message response

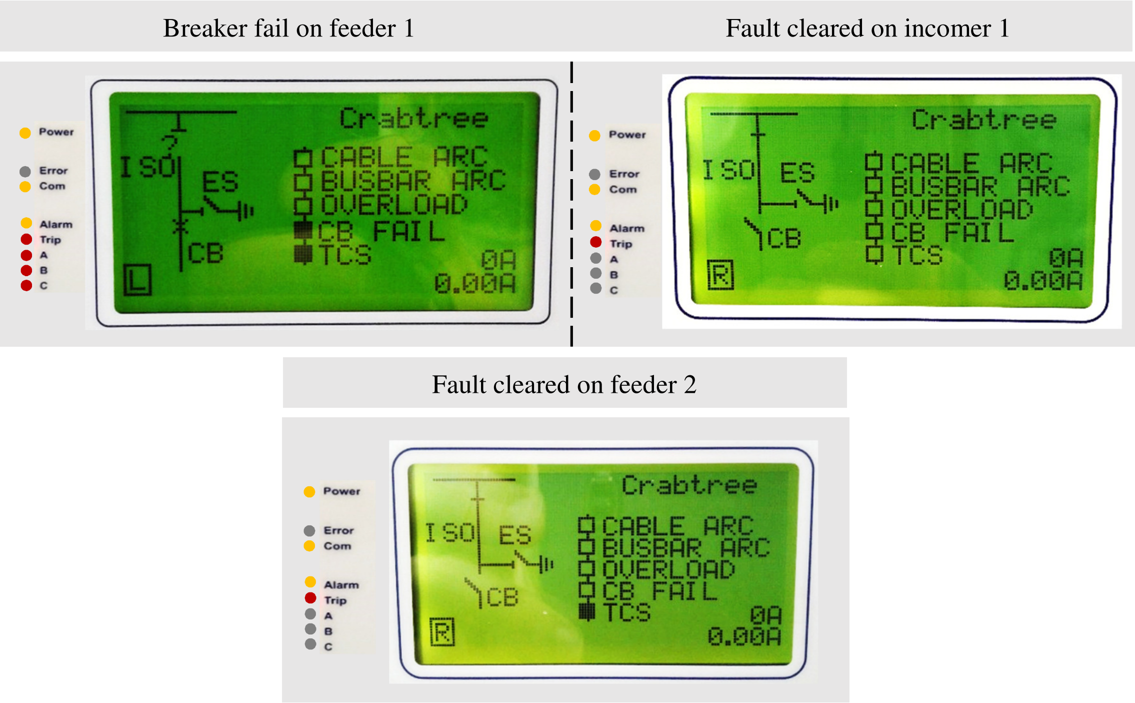


Circuit_Breaker_5_Close CB5-Close Circuit B5 Operation Closed

Figure 5-9. Graph of the operation of substation switchgear and breaker fail on CB 4

The concept of breaker fail protection, which was initially illustrated in Figure 5-4, was expanded upon as was demonstrated by the diagrams in Figure 5-6 and Figure 5-8. In these two protection schemes breaker fail conditions were simulated on the circuit breakers of either feeder 1 (CB 3) or on feeder 2 (CB 4). This was achieved by simply disconnecting the trip coil (TC) of the respective breaker and then sending a remote end open command using the SCADA model. Once the breaker on either of these two feeders had failed to open the breaker fail protection element within the feeder IED became active and a GOOSE message was sent from the feeder IED to the adjacent subscribing IEDs on bus 1. These relays then tripped their associated breakers in order to ensure that the failed feeder, and hence the fault, was completely isolated.

Alternatively, the publisher IED controlling the failed breaker could issue a GOOSE message to the subscribing IED on the upstream incomer which then tripped the appropriate protection zone. In Figure 5-6 breaker fail was simulated on feeder 1 (CB 3) whereas in Figure 5-9 breaker fail had occurred on feeder 2 (CB 4). In each case the failed circuit breaker was isolated by tripping the bus section breaker, the incomer and the adjacent feeder. Noticeably, the breaker on feeder 3 of bus 2 was unaffected and remained in the closed position since it played no role in the isolation of the failed protection zone. Additionally, the graphs shown by Figure 5-7 and Figure 5-9 illustrated the operation or nonoperation of each of the circuit breakers in the substation models demonstrated in Figure 5-6 and Figure 5-8 respectively. Furthermore, the point at which the breaker fail protection element became active was also demonstrated on the aforementioned trends.


Breaker fail on feeder 1

Fault cleared on incomer 1

Fault cleared on feeder 2

Figure 5-10. HMI illustrating breaker fail on feeder 1 and fault clearing on feeder 2 and incomer 1

The HMI of the two feeder and incomer IEDs under breaker fail conditions was demonstrated in Figure 5-10. This image depicted the status of the circuit breaker, labelled CB 3 on feeder 1, which remained in the closed position after failing to operate. In addition, the HMI showed the associated operation of the circuit breaker (CB 1) on incomer 1 as well as the breaker on feeder 2 (CB 4) which opened in response to the GOOSE message that was sent from the IED on feeder 1. The HMI depicted in Figure 5-10 related to the substation model given by Figure 5-6. The very same results were recorded for the substation model illustrated in Figure 5-8 with the exception that breaker fail conditions occurred on CB 4 of feeder 2. In addition, the red LED trip indicators of both IEDs were active to illustrate the issuing of trip commands and the red breaker fail LEDs of all the phases A, B and C were in the latched state. Note that the bus section breaker was controlled by the same IED as that on the incomer. Hence, there was no HMI representing the status of the circuit breaker on the bus section (CB 5).

5.2 Arc-flash protection

Conventional arc-flash protection schemes commonly rely on and occur in combination with overcurrent protection. Here the arcing time is predominantly affected by the time taken for both the protection IED to operate and for the circuit breaker to extinguish the arc [33]. Traditional arc-flash protection techniques are typically hardwire-based and use the relays output contacts to connect to devices and switchgear [33]. Conventional approaches such as that described, may increase the cost and complexity of a particular project whilst at the same time being less effective at quenching arc-flash incidents [34].

Importantly, the amount of energy that is released during an arc-flash incident is proportional to the duration of the arc itself [34]. Therefore, time is a critical consideration when it comes to detecting and reducing the impact of arcing on cables and busbars within substations [34]. If left unattended, arc faults that persist for up to and longer than 500 ms can result in major damage to substation equipment as well as danger to technical personnel [34]. However, if the time period of the arc-flash is reduced to less than 100 ms the potential for system damage decreases greatly [34]. Furthermore, if the arc-flash is quenched within a time of less than 35 ms the impact of the arc is considered to be almost negligible [34]. Unfortunately, the operating time of traditional overcurrent relays may be greater than the minimum arc protection time of 35 ms. This is usually because of the selectivity, coordination and grading settings between relays on the substation network [34]. Thus, conventional overcurrent relays may not be quick enough to clear the high currents associated with arc faults safely [34]. Therefore, by adopting an IEC 61850-compliant IED with built in arc protection, the fast GOOSE message class can be used to apply effective arc-flash protection in an expedient manner well below 35 ms. Hence, the IEC 61850 standard has important applications for arc-flash protection, ensuring that the security of the network is maintained and that its expensive equipment is safeguarded in the event of an arc fault.

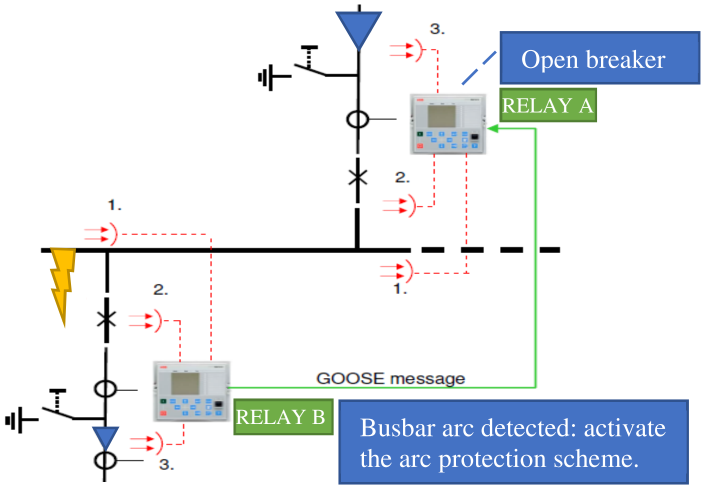


Figure 5-11. Arc protection scheme using GOOSE [22]

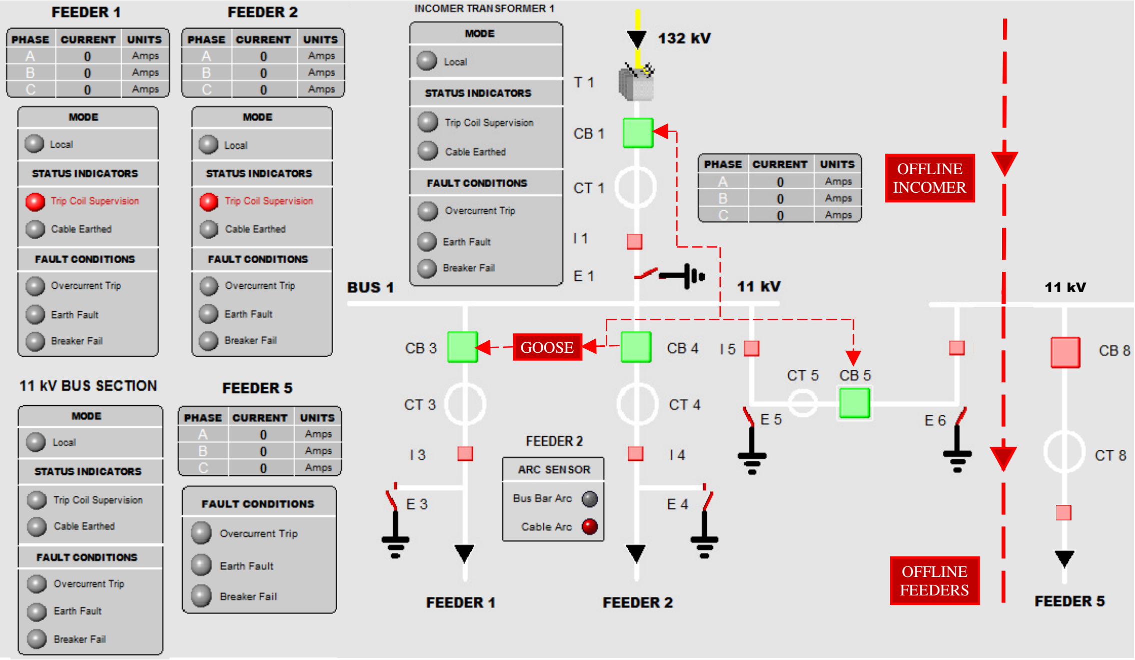
In Figure 5-11 the rudimentary concepts of busbar, circuit breaker and cable arc protection were diagrammatically demonstrated. This figure showed how Relay A (on the incoming line) and Relay B (on the outgoing feeder) were equipped with three arc-flash sensors [22]. When sensor 1 of Relay B detected a busbar arc, Relay B sent a GOOSE message to Relay A on the incomer informing it that there was an arcing busbar [22]. Upon receiving this GOOSE message from Relay B, the IED on the incomer then checked the current level and issued a trip command to breaker A [22]. The same principle could be applied to protection in the case of cable arc or circuit breaker arc as was demonstrated by arc sensors 2 and 3 of Figure 5-11. Thus, the GOOSE message class enables fast protection in response to arc faults [22]. Therefore, using the IEC 61850 protocol protection can be achieved in less than 23 ms whereas with traditional hardwire techniques protection may only be administered in under 37 ms [22]. Therefore, these outcomes ensure that the IEC 61850 substation communication protocol and the GOOSE message class subscribe to the standards of efficient, fast, effective and reliable protection.

5.2.1 Configuration

The same substation model that was used for breaker fail protection in 5.1 was also employed to test arc-flash protection in the following subsection. Additionally, the same GOOSE configuration procedure that was adopted in section 5.1.1 was used to configure the inter-IED communication between bays. In this study two arc sensors were used to test the impacts of cable arc and busbar arc. The arc sensors were tested using a simple flash to trigger each device.

5.2.2 Results of arc-flash protection

The upcoming subcomponents of chapter 5 presented the experimental results of arc-flash protection which was performed based on cable arc and busbar arc conditions that were simulated on feeder 2. In this section GOOSE-based arc protection was used to extinguish fault conditions in each case.



FEEDER 1

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 2

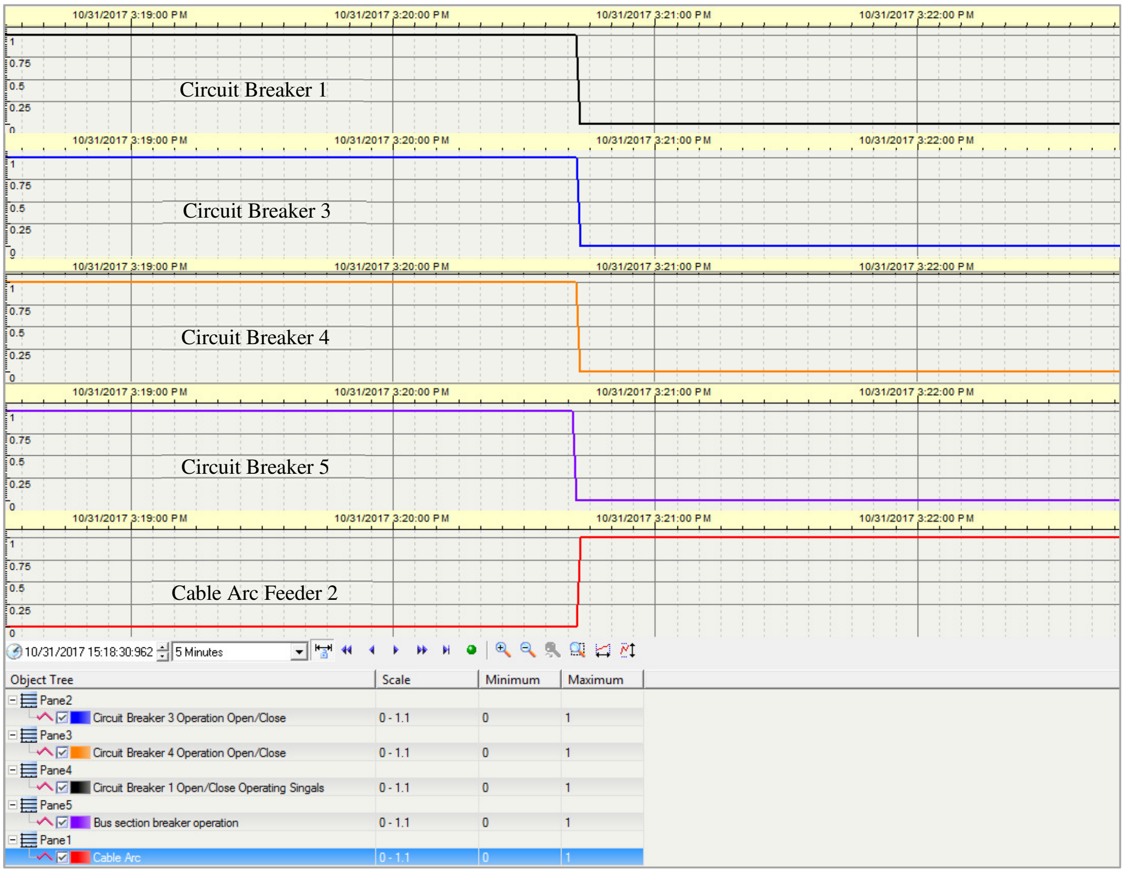
PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 5

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

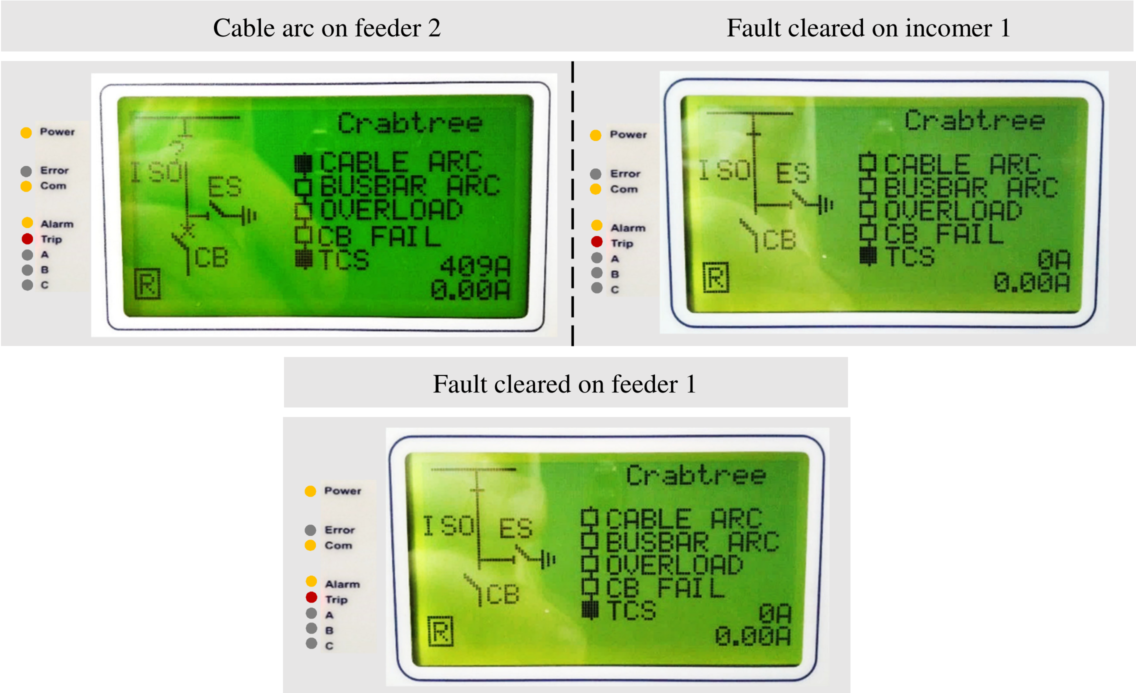
PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-12. Cable arc on feeder 2 and GOOSE message response



Object Tree	Scale	Minimum	Maximum
Pane2			
Circuit Breaker 3 Operation Open/Close	0 - 1.1	0	1
Pane3			
Circuit Breaker 4 Operation Open/Close	0 - 1.1	0	1
Pane4			
Circuit Breaker 1 Open/Close Operating Singals	0 - 1.1	0	1
Pane5			
Bus section breaker operation	0 - 1.1	0	1
Pane1			
Cable Arc	0 - 1.1	0	1

Figure 5-13. Graph of circuit breaker operation and cable arc on feeder 2



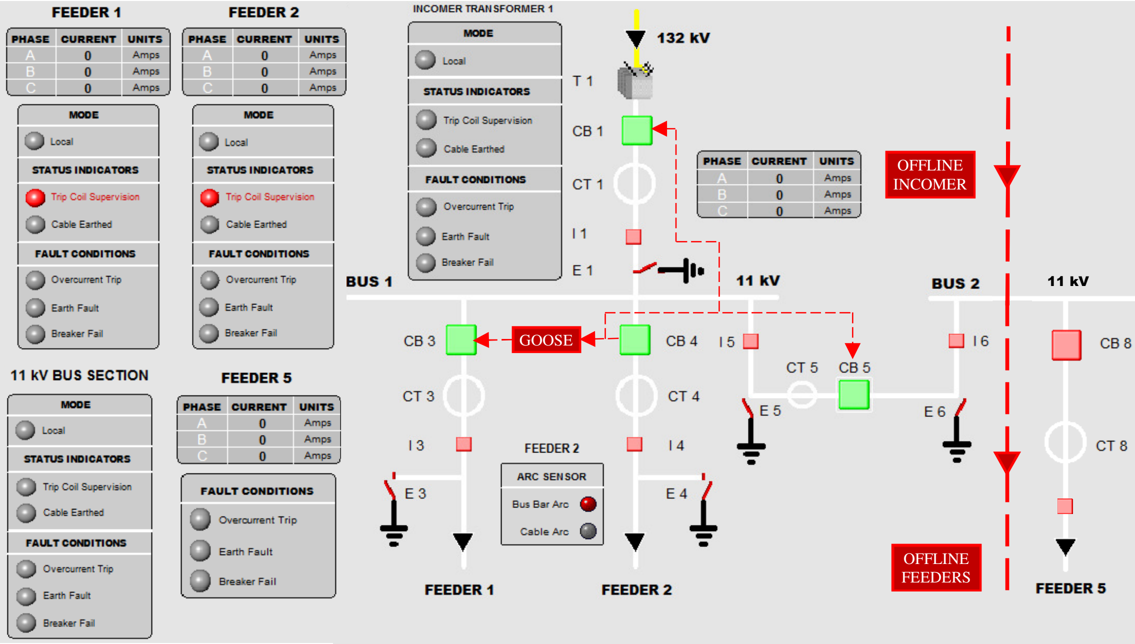
Cable arc on feeder 2

Fault cleared on incomer 1

Fault cleared on feeder 1

Figure 5-14. HMI of cable arc on feeder 2 and fault clearing on feeder 1 and incomer 1

The concept of arc-flash protection (specifically cable arc) which was initially illustrated in Figure 5-11, was expanded upon in this study as was demonstrated in Figure 5-12. In this scheme, arc protection was simulated using a cable arc sensor that was connected on the appropriate input of the IED on feeder 2. The cable arc sensor was tested simply by applying a flash close to the detection element which activated the device. Once the arc had been detected by the sensor on the IED of feeder 2, the arc protection element become active. Thereafter, the relay published a GOOSE message on the substation LAN. This multicast GOOSE transmission was received by the subscribing IEDs which were controlling the incomer (CB 1), bus section (CB 5) as well as the first outgoing feeder (CB 3) respectively. The IEDs then issued trip commands to their associated breakers in order to ensure that the cable arc was completely isolated. Alternatively, the IED controlling the circuit breaker (CB 4) on the arcing feeder could have also issued an exclusive GOOSE message to the primary relay on the upstream incomer which would deliver the trip commands for the appropriate protection zone. In Figure 5-12 the cable arc alert indicator of the substation SCADA was illuminated on feeder 2. Additionally, Figure 5-13 demonstrated a trend of the trip signals of each of the subscribing IEDs as well as indicating the point at which the cable arc protection element became active. Noticeably, the breaker on feeder 3 of bus 2 was unaffected and remained in the closed position since it was located outside the protection zone and played no role in the isolation of the faulted area. Figure 5-14 depicted the HMI of each of the IEC 61850-compliant IEDs on the incomer and feeders respectively. This HMI showed the open status of each of the breakers of the model in Figure 5-12 as well as the cable arc indication on the HMI panel of feeder 2. Note that the bus section breaker was controlled by the same IED as that on the incomer. Hence, there was no direct HMI representing the status of the bus section breaker (CB 5).



FEEDER 1

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 2

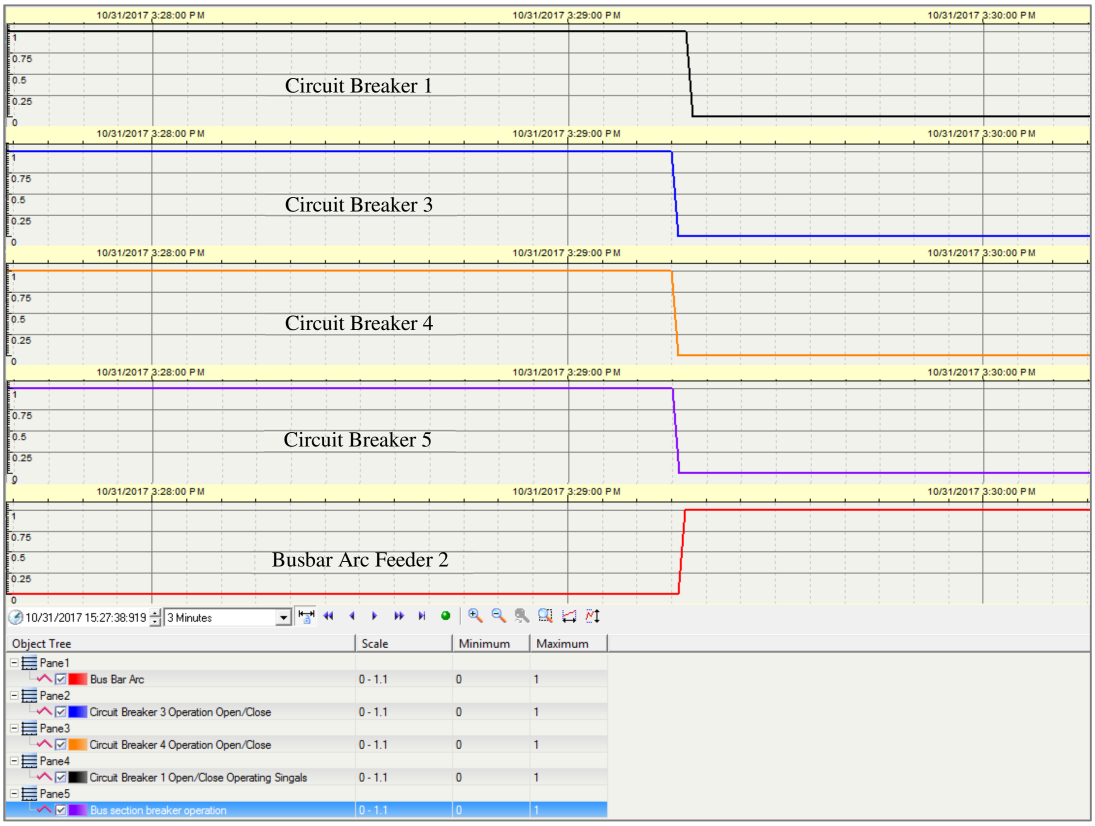
PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

FEEDER 5

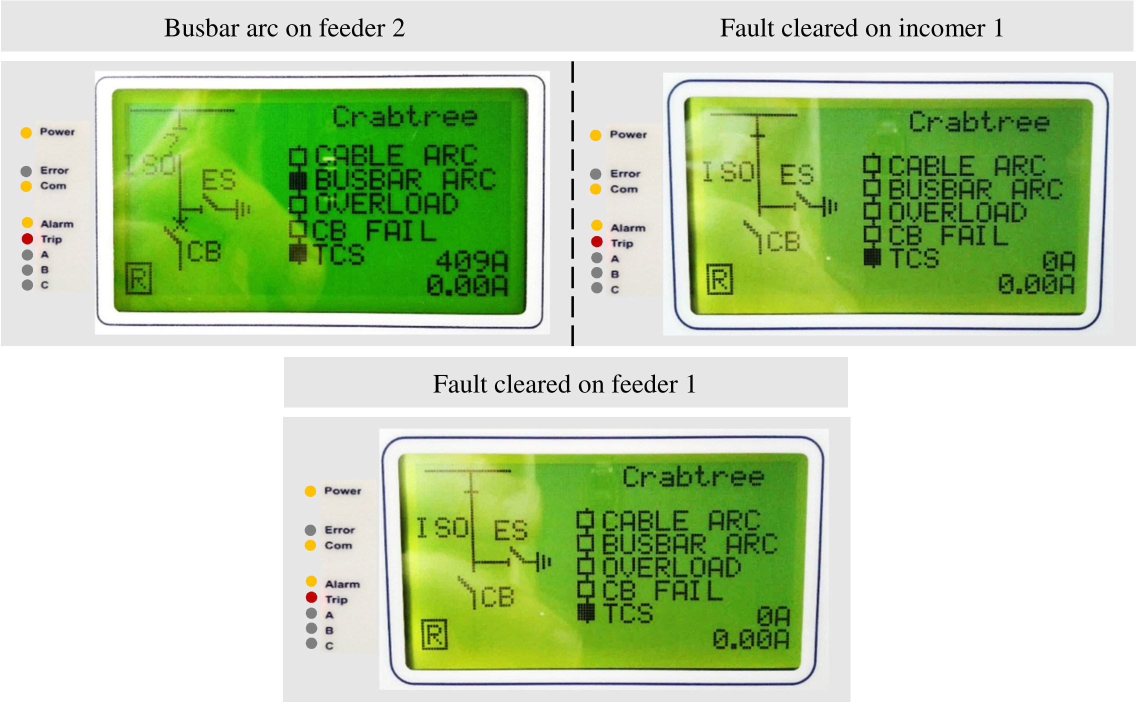
PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-15. Busbar arc on feeder 2 and GOOSE message response



Object Tree	Scale	Minimum	Maximum
Pane1			
☑ 🟥 Bus Bar Arc	0 - 1.1	0	1
Pane2			
☑ 🟦 Circuit Breaker 3 Operation Open/Close	0 - 1.1	0	1
Pane3			
☑ 🟧 Circuit Breaker 4 Operation Open/Close	0 - 1.1	0	1
Pane4			
☑ ⬛ Circuit Breaker 1 Open/Close Operating Singals	0 - 1.1	0	1
Pane5			
☑ 🟪 Bus section breaker operation	0 - 1.1	0	1

Figure 5-16. Graph of circuit breaker operation and busbar arc on feeder 2



Busbar arc on feeder 2

Fault cleared on incomer 1

Fault cleared on feeder 1

Figure 5-17. HMI of busbar arc on feeder 2 and fault clearing on feeder 1 and incomer 1

A similar test approach to that performed during the simulation of a cable arc was carried out to capture the results of a busbar arc on bus 1 of the substation model. Hence, the busbar arc sensor was connected to the IED on feeder 2 using the appropriate input. Once a flash was detected, the busbar arc protection element of the IED was activated. A GOOSE message was published and delivered from the feeder IED to the subscribing relays located within the protection zone. Thereafter, trip commands were issued and delivered from the relevant IEDs to the incomer breaker (CB 1), bus section breaker (CB 5) and feeder breakers (CB 3) in order to isolate the arc fault on the busbar of bus 1. This concept was illustrated in the substation model of Figure 5-15. In addition, the trend in Figure 5-16 depicted a graph of the operating states of the respective switchgear as well as showing the point at which the busbar arc was detected. The HMI of the respective IEDs was illustrated in Figure 5-17 showing the persistence of the busbar arc on bus 1 as well as the associated tripping of circuit breakers 1, 3, 4 and 5 respectively. Circuit breaker 8 on bus 2 remained in the closed position since it was located outside the protection zone and played no role in extinguishing the arc.

5.3 Blocking response and sympathetic trip protection

As a result of the new IEC 61850 protocol and the smart GOOSE message class better protective coordination, selectivity and grading can be achieved between the IEDs within a substation [22]. This has become evident when one considers the concepts of blocking-based busbar protection and the overcurrent blocking principle. Multiple IEC 61850-compliant IEDs can be connected to the substation LAN in distribution bus protection schemes [8], [10]. If a fault occurs on one of the substations feeders the feeder protection IED will detect the fault current and try to clear the disturbance. Furthermore, the same fault current will be detected by the protection IED located at the transformer of the incomer [8], [10]. When the overcurrent protection element of the feeder relay becomes active the IED will deliver a GOOSE message to indicate that the fault has been captured and that it has issued a trip signal to its breaker to clear the disturbance [8], [10]. The IEDs on the unfaulted feeders and incomer subscribe to this GOOSE message. Thereafter, the relays situated on the healthy protection zones can be blocked by adapting their overcurrent settings for a period of time during the inrush condition [8], [10]. Inrush conditions may be caused as a result of a voltage sag at the busbar which exists as a direct result of the fault itself or from fault clearing. In addition, an outcome of this condition could see the tripping of the circuit breakers on healthy feeders [8], [10].

Alternatively, the faulted feeder IED can block the sensitive overcurrent stages (high set stage, low set stage and instantaneous stage) of the other IEDs using a GOOSE message as and when is required. The traditional approach to delay setting with instantaneous overcurrent protection achieves effective relaying within 100 ms [22]. However, using the IEC 61850 protocol the same principle can be achieved within 70 ms [22]. Figure 5-18 demonstrates how the instantaneous overcurrent stage of a particular IED can be blocked using IEC 61850 and GOOSE messaging.

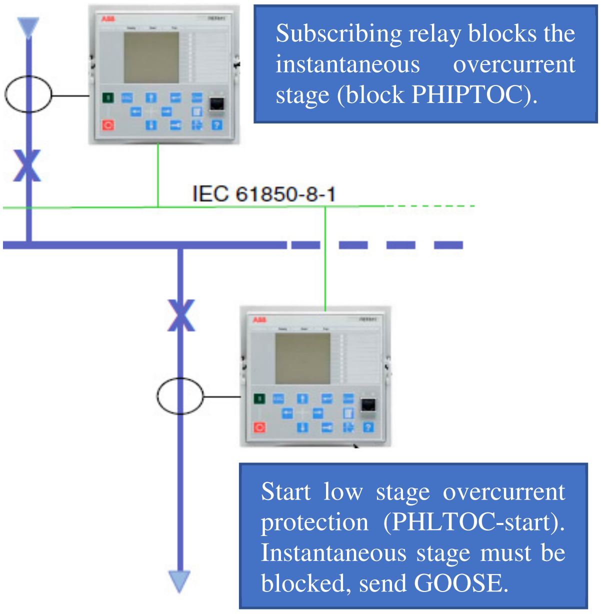

Subscribing relay blocks the instantaneous overcurrent stage (block PHIPTOC).
IEC 61850-8-1
Start low stage overcurrent protection (PHLTOC-start). Instantaneous stage must be blocked, send GOOSE.

Figure 5-18. Blocking-based busbar protection [22]

The benefit of this form of protection lies in the ease with which blocking signals can be transmitted between devices. Traditionally, in legacy substations there would be a large number of wires connecting the binary inputs and relay outputs of the IEDs [8], [10]. However, with IEC

61850, messages can be published and subscribed to easily over the substation LAN [8], [10]. Figure 5-19 shows an example of the inter-IED GOOSE blocking signals that can be sent between feeder IEDs during sympathetic trip protection on a distribution bus scheme.

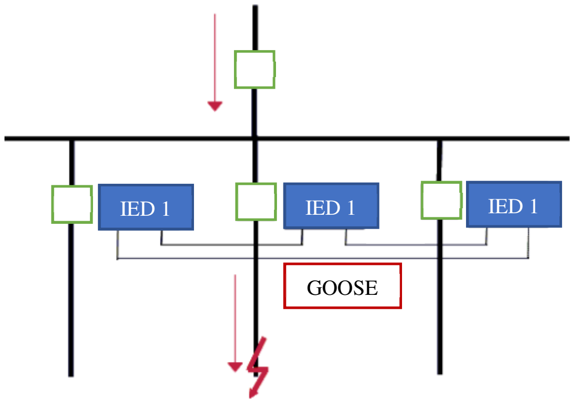


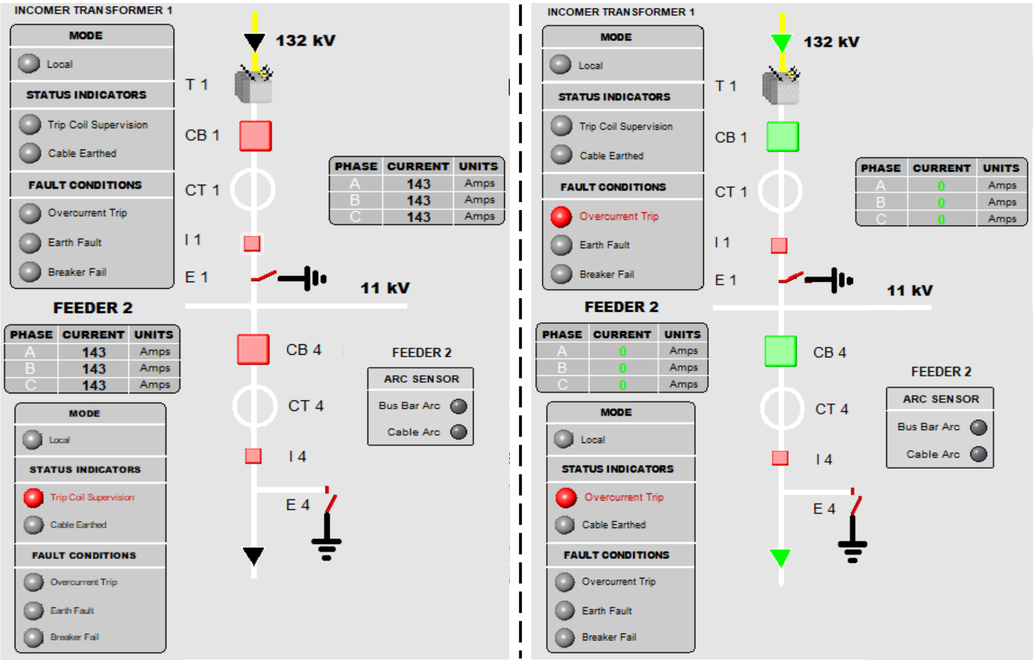
Figure 5-19. Inter-IED GOOSE blocking [8]

5.3.1 Configuration

The same substation model that was used for breaker fail protection in 5.1 was also employed to test blocking response in the following subsection. Additionally, the same GOOSE configuration procedure that was adopted in section 5.1.1 was used to configure the inter-IED communication between bays. Here blocking-based protection using GOOSE was implemented to block the overcurrent stages of a particular incomer to ensure that only the appropriate stage of the feeder protection operated when it was required.

5.3.2 Results of blocking-based protection

The subsequent component of chapter 5 demonstrated the results of blocking-based overcurrent protection using the GOOSE message class. In this section sympathetic trip protection (blocking response) was applied to a busbar with a single incomer and a single feeder which were both in simultaneous operation. This sub-model was taken from the substation in Figure 4-2 from chapter 4. The IED located on the outgoing feeder used GOOSE to block the overcurrent stages of the IED on the incoming line. Here the IEDs were of the same family, with the same overcurrent protection settings (pick-up) and were both IEC 61850-compliant. A fault, located on the feeder, was applied to the system thus creating an overcurrent condition so that the associated responses could be recorded. In Figure 5-20 the energized and de-energized states of the single incomer-feeder model were illustrated. Firstly, a steady state current of 143 A was passed to incomer 1 of the substation model as shown in the figure. The circuit breakers on both incomer and feeder remained closed since the system was under steady state and devoid of faults. However, once an overcurrent was applied to the model both circuit breakers (CB1 and CB4) tripped as a result. The IEDs on both the incomer and feeder saw the same fault current and hence issued trip signals to their respective circuit breakers. This dual trip occurred due to that fact that these IEDs were both of the same family with identical overcurrent protection settings. The tripping of both breakers represented a non-ideal operation of switchgear especially since the fault was located downstream of the feeder breaker. Therefore, the circuit breaker on the incoming line needlessly tripped.



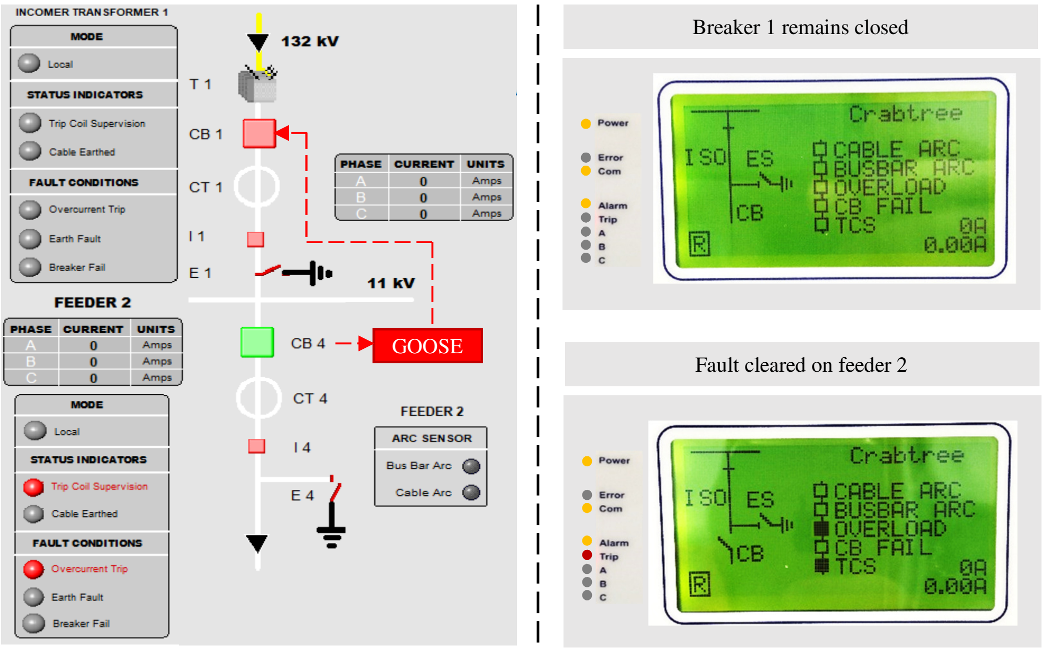
PHASE	CURRENT	UNITS
A	143	Amps
B	143	Amps
C	143	Amps

PHASE	CURRENT	UNITS
A	143	Amps
B	143	Amps
C	143	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-20. Energized and de-energized states of the single incomer-feeder model

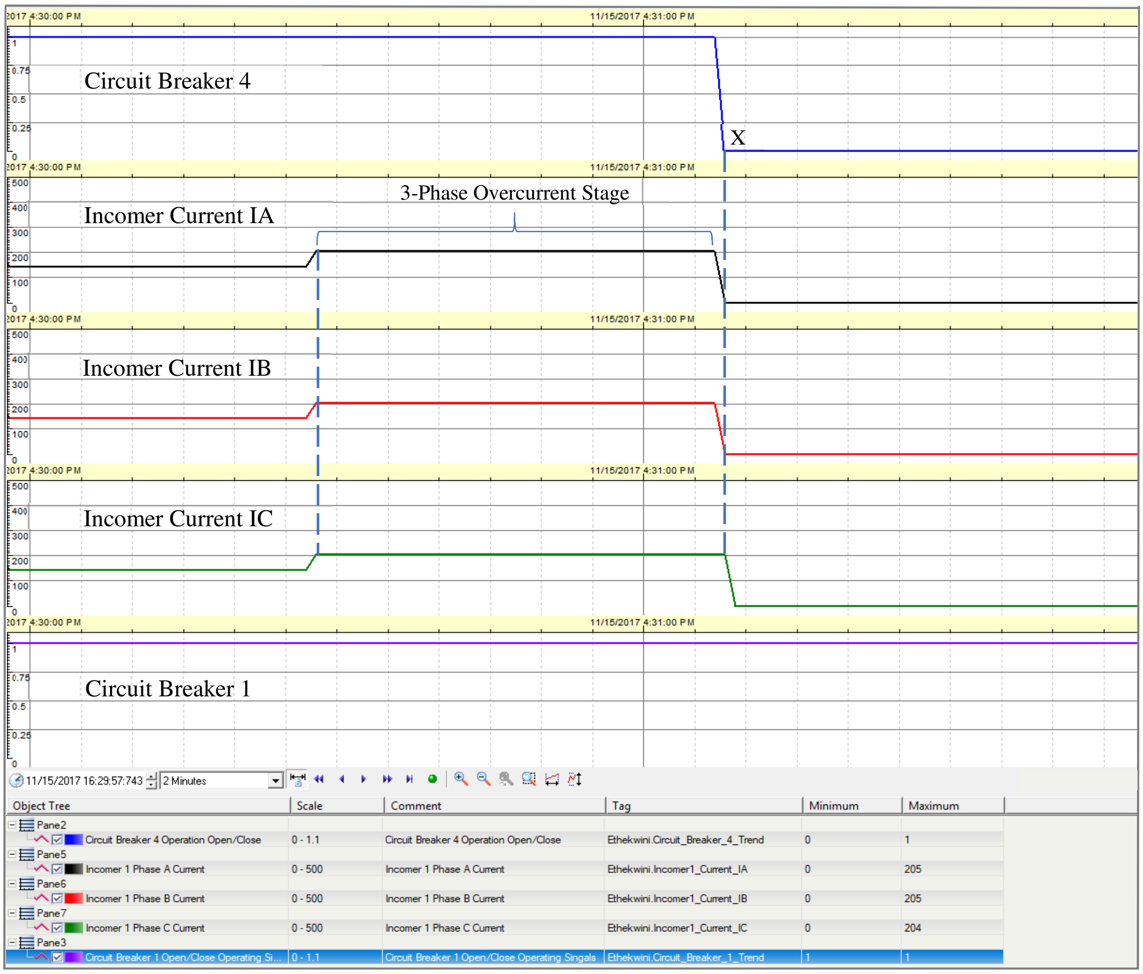


PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

PHASE	CURRENT	UNITS
A	0	Amps
B	0	Amps
C	0	Amps

Figure 5-21. Blocking-based protection using GOOSE

In order to prevent the unnecessary tripping of unfaulted lines, such as incomer 1 in Figure 5-20, a blocking response could be issued by a particular IED to suppress the overcurrent protection element of another relay. This concept was illustrated in Figure 5-21. Here a fault occurred on the outgoing feeder which affected the overcurrent characteristics of both the IED controlling CB 4 as well as that controlling CB 1. Since the fault occurred downstream of CB 4 it makes sense that this circuit breaker should trip in order to isolate the fault. Hence, the IED controlling CB 1 sent a blocking response to the incomer IED which blocked the overcurrent element of this relay (I>, I>>, I>>>). Thus, only CB 4 opened and cleared the overcurrent fault condition. These concepts were illustrated in the HMI of the IEDs in Figure 5-21. The HMIs showed that the incomers circuit breaker remained closed and the feeder circuit breaker opened to extinguish the fault.



Object Tree	Scale	Comment	Tag	Minimum	Maximum
⊟ Pane2					
☑ Circuit Breaker 4 Operation Open/Close	0 - 1.1	Circuit Breaker 4 Operation Open/Close	Ethekwini.Circuit_Breaker_4_Trend	0	1
⊟ Pane5					
☑ Incomer 1 Phase A Current	0 - 500	Incomer 1 Phase A Current	Ethekwini.Incomer1_Current_IA	0	205
⊟ Pane6					
☑ Incomer 1 Phase B Current	0 - 500	Incomer 1 Phase B Current	Ethekwini.Incomer1_Current_IB	0	205
⊟ Pane7					
☑ Incomer 1 Phase C Current	0 - 500	Incomer 1 Phase C Current	Ethekwini.Incomer1_Current_IC	0	204
⊟ Pane3					
☑ Circuit Breaker 1 Open/Close Operating Si...	0 - 1.1	Circuit Breaker 1 Open/Close Operating Singals	Ethekwini.Circuit_Breaker_1_Trend	1	1

Figure 5-22. Graph of the operation of switchgear and the 3-phase incomer current

Figure 5-22 demonstrated the graphical characteristics of the blocking-based protection model illustrated by Figure 5-21. This graph showed the associated operation and non-operation of CB 4 and CB 1 respectively. The circuit breaker on feeder 2 (CB 4) opened to clear the downstream overcurrent fault, whilst the upstream breaker on incomer 1 remained closed after receiving the blocking signal. The black, red and green pens of the graph in Figure 5-22 depicted the 3-phase current of the incomer and feeder. Initially the current remained under steady state at 143 A; it was then increased to 205 A and after a time delay (according to inverse time characteristic of the relay) the fault current was cleared by CB 4 and immediately dropped to 0 A.

5.4 Provision for future works

In addition to the IEC 61850 GOOSE-based applications of breaker fail protection, arc-flash protection and blocking response, the standard also has implications for busbar earthing and disturbance recording. Thus, during the course of future works it may be necessary to investigate these two additional protection applications of the GOOSE message class. The following subsection briefly outlined the underlying principles of each of the aforementioned protection schemes.

5.4.1 Busbar earthing

In this protection scheme a busbar may be grounded by closing an earth switch on a particular bus. If the busbar earth switch is in the closed position then there must be a blocking signal that is sent from the upstream IED on the incomer (Relay A) to ensure that none of the other IEDs (Relays B and C) close their breakers [22]. The circuit breaker positions of all the breakers connected to that particular busbar must be published. The subscribing IEDs receive this information and deliver it to the blocking input of the control functional block within the relay [22]. Hence, this process prevents the closing of the relevant circuit breakers [22]. Alternatively, this protection scheme can be configured in reverse where the circuit breaker positions on the feeders and incomer can block the operation of the earth switch on the busbar [22]. Figure 5-23 illustrated the concept of GOOSE-based busbar earth protection.

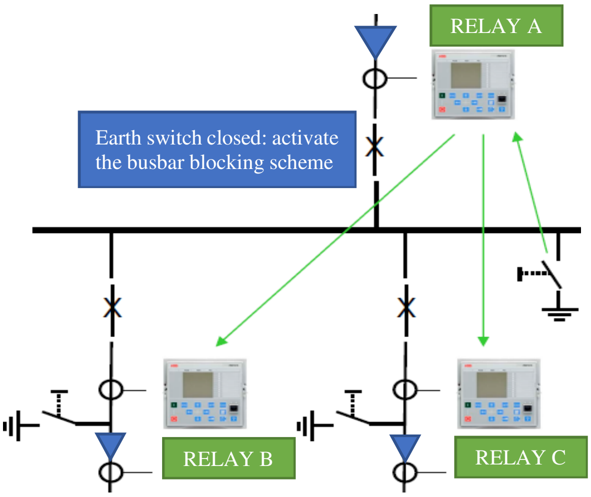


Figure 5-23. GOOSE-based busbar earth blocking principle [22]

5.4.2 Disturbance Recording

The IEC 61850 protocol can also be used to initiate the disturbance recording function within IEDs. In this case a GOOSE message from one IED may be used to activate the disturbance recorder of a different relay one an adjacent bay [22]. If a fault is detected on one of the feeders (Relay B or C) or on an incomer (Relay A) of the substation model illustrated by Figure 5-24, then a GOOSE message can be used to trigger the disturbance recorders of the IEDs on the adjacent feeders [22]. This facility could be used to create trends and monitor the substations system parameters like power, currents and voltage levels during fault conditions. Beneficially, disturbance recorders can be triggered almost instantaneously without any considerable time delays. Figure 5-24 demonstrated the concept of disturbance recording using GOOSE-based techniques.

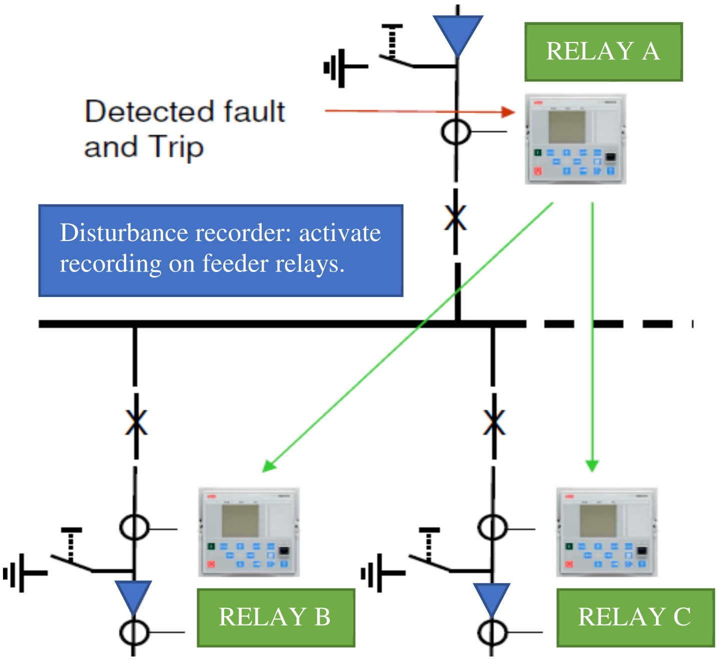


Figure 5-24. GOOSE-based disturbance recording [22]

5.4.3 1 of N blocking

In this protection scheme (Figure 5-25) the operator may send a ‘select breaker before operate’ command from the substation control system (SCS) to a feeder on which a particular IED is located [22]. A GOOSE-based blocking signal is then sent from the users remotely chosen feeder IED to all other feeders and incomers of the protection zone [22]. Importantly, no other control commands of any kind are permitted during the course of this ‘select before operate’ timeout period [22]. The selected IED (publisher) sends out the circuit breaker control selection using the GOOSE message class to all of the subscribing IEDs on the network [22]. The receiving IEDs connect this signal to the blocking input of the control functional block [22]. Lastly, when the 1 of N blocking control sequence is terminated, the publisher IED delivers the new value change to all of its subscribers which frees the control function block situated within those IEDs [22]. The aforementioned concepts were diagrammatically demonstrated by Figure 5-25.

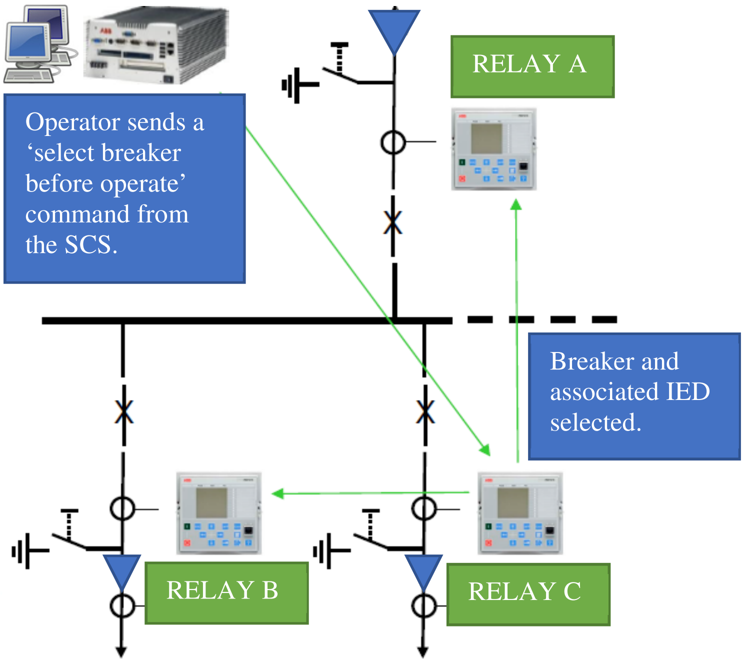

RELAY A
Operator sends a 'select breaker before operate' command from the SCS.
Breaker and associated IED selected.
RELAY B
RELAY C

Figure 5-25. 1 of N blocking using GOOSE [22]

5.4.4 Selective backup tripping

Typically, a single protection IED is used on a particular substation feeder or incomer [19]. However, if this protection IED fails to clear a fault then it must be extinguished by the backup overcurrent protection of the incoming line (transformer protection) which trips its breaker and the bus section [19]. The disadvantage of this approach is that protective relaying may not be administered quickly enough [19]. The IEC 61850 GOOSE message class delivers a repetitive retransmission mechanism that ensures expedient protection, health of communication and eliminates hardwiring [19]. A better method of relaying for backup protection uses selective backup tripping which monitors the normally closed contacts of the feeder relays that close when a relay has failed [19]. The backup IED can make its own decision if it sees a fault and does not receive a blocking signal from the feeder relays [19]. There are two possible cases that the backup protection must consider. Firstly, the fault could be on the feeder with the failed relay or secondly, the fault might be on the busbar [19]. The probability of a feeder fault is much higher than a bus fault, therefore, the backup overcurrent protection IED on the incomer tries to trip the feeder breaker [19]. If the fault persists the source breakers (on the incomer and the bus section) are then also issued trip commands [19].

The incomer IED (transformer IED) subscribes to all the GOOSE messages of the feeder protection IEDs [19]. Thus, if one of the IEDs on the feeders stops transmitting its GOOSE messages then the relay on the incomer knows that it has failed [19]. This will then activate the selective backup trip element of the transformer protection on the incoming line [19]. The concepts of selective backup tripping were illustrated in Figure 5-26.

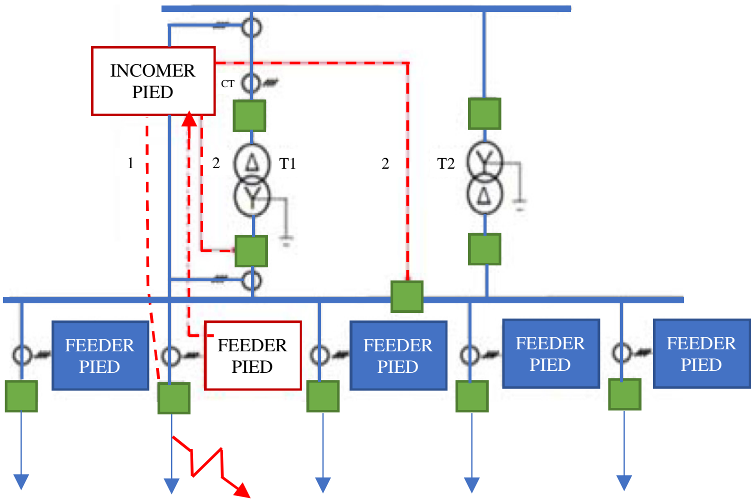


Figure 5-26. Selective backup tripping using GOOSE [19]

5.4.5 Priority Tagging/ VLAN

The IEC 61850-based GOOSE message class is considered to be a multicast or broadcast Ethernet compliant message system [4]. Thus, these terms suggest that protection IEDs can use GOOSE to send messages to a particular group of devices (multicast) or to every device that is connected to a substation network (broadcast) [4]. Hence, broadcast and multicast messages can greatly increase the data traffic on a particular LAN [4]. When an Ethernet switch receives a GOOSE message from a publisher it will forward it to all of the other network ports on the LAN; except to that from which it was sent [4]. Unfortunately, a large number of published messages on the substation network can quickly use up all of the available bandwidth [4]. However, there are two convenient engineering methods that can be used to elevate this problem. The first uses VLANs which divide the network up into serval virtual local area networks (Figure 5-27) [4]. This solution helps to segregate network traffic from different areas of the substation and adds a number of new Ethernet switches to the network in order to effectively handle the increase in traffic [4]. The second solution to the problem of bandwidth saturation uses the concept of priority tagging. During this approach the Ethernet switch will monitor or decipher the priority segment of the information frame and then transmit the highest-level priority GOOSE messages first [4]. Therefore, it is by using either of these basic techniques that the network traffic of a substation can be efficiently managed and that commands, messages and information can be reliably distributed for expedient protection and automation. The diagram that was illustrated by Figure 5-27 sought to demonstrate the concept of VLANs.

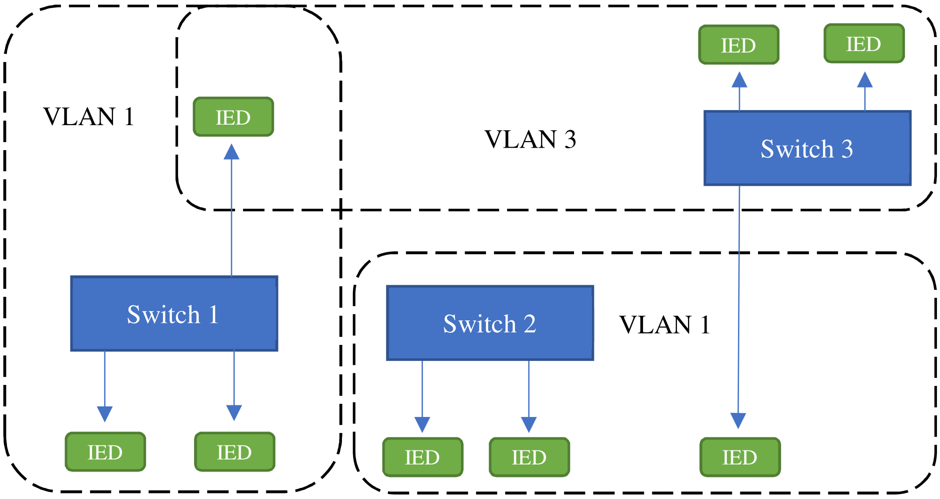


Figure 5-27. Concept of VLANs for bandwidth efficiency

5.5 Conclusion

The applications of the GOOSE-message class in substation protection and automation have benefitted substation design and simplified physical protection architecture. It is because of the IEC 61850 standard that messages can be periodically multi-cast from publisher devices to subscriber IEDs which promotes coordination, reliability and system security. Not only is GOOSE reliable but it is fast; achieving message speeds of up to 3 ms which allows it to be used for protective relaying. By using this smart message system for breaker fail, arc-flash and blocking-based protection it is possible to reduce the clearing time of faults, decrease lengthy and expensive copper wiring within the substation, reduce cable resistance and eliminate CT saturation using cleverly positioned MUs as well as efficiently broadcast information to the 'virtual' substation LAN.

In a conventional substation the protection techniques that were discussed in chapter 5 would have been implemented using hardwire-based techniques and the many digital inputs, digital outputs and output relays of the IEDs to perform substation protection, monitoring and automation. Not only is traditional hardwiring slower than IEC 61850, it is labour intensive, expensive and especially tedious, complicated and time consuming to implement. The GOOSE message class is the most powerful and flexible tool of the IEC 61850 protocol.

6. Comparative Study

The foregoing chapters of this dissertation considered the design, implementation and experimental evaluation of a prototypical substation and its corresponding communication structures. The substation protocols including: Modbus RTU, DNP3 and the IEC 61850 standard were utilized between intelligent equipment on a physical network. Therefore, this chapter sought to establish a research consensus regarding the benefits and drawbacks of the aforementioned communication protocols as well as offer a critical analysis and comparison between the researched literature on Modbus RTU, Modbus TCP, DNP3 and the IEC 61850 protocol, as well as between the findings that were observed during the experimental procedure. The subsequent components of chapter 6 included a critical literary survey of Modbus RTU, Modbus TCP and DNP3 in addition to the review on the IEC 61850 standard that was compiled in chapter 2. The author discussed the technical inferences that could be drawn from both the practical studies and researched literatures that were discussed in this thesis.

6.1 Modbus

Modbus is an application layer, legacy communication protocol that can be used for transmitting data over serial links between electronic devices like programmable logic controllers (PLCs) [35], [36], [44]. In addition, Modbus is based on the 'master/slave principle' whereby the master station delivers a request to the slave and the addressed slave sends back the appropriate response [35]. Therefore, the control device that sends a request for the data is referred to as the master (traditionally only one, especially in RS485 networks) and the device that transmits the data is called the slave (there can be up to 247 slaves) [35], [36]. Each slave has an address from 1 - 247 to which the masters may write or read different information [36]. Since serial Modbus is a protocol that is independent of the physical network layer, it can be easily integrated into Ethernet-based TCP networks, using gateway devices such as smart RTUs [35]. Modbus has been widely used within industry as a free protocol for manufactures and vendors alike. Therefore, users are allowed to implement Modbus and use it within their industry products as they see fit [35]. This protocol is typically used to communicate data or signals between instrumentation devices and control devices such as relays, RTUs and data acquisition systems (SCADA), within an electrical substation [35], [36]. In a SCADA network Modbus is typically used to connect a supervisory computer to a remote terminal unit (RTU) for data supervision, monitoring, control and information capture [35]. In the context of this dissertation Modbus RTU was used to connect a compliant IED of a particular feeder to the substation RTU. Here Modbus was used to deliver control commands like breaker trips and send alerts for items like breaker fail, earth fault and overcurrent conditions as they appear on the relay.

6.1.1 Operation and integration

As previously mentioned, Modbus is a protocol that allows information to be transmitted serially over different hardwire links. Modbus can communicate using serial RS485 or serial RS232. RS232 uses approximately three wires; a transmit wire, a receive wire and a common wire in a point to point communication system between two devices [35], [36]. Since the transmit (T_X) and Receive (R_X) functions occur on different circuits data is able to flow both ways at the same time. RS232 sends data in the form of a timed-series of bits. An example of an RS232 based serial communication cable was shown in Figure 6-1. This cable can be used to connect a master device to a slave. In Modbus, the data is sent in binary as ones and zeros [37]. Each bit represents a voltage so that the one's correspond to + 5 V and zeros to – 5 V. The information is transferred at rates of up to and exceeding 9600 bits per second [35], [37]. RS485, on the other hand, is a differential system. In this case, there are only two wires and the difference in the potential (voltage level) between the two wires determines what the bits or binary values of the data packet are; Modbus RTU is essentially a RS485 protocol [35], [36]. Modbus RTU (RS485) is multi-dropped which means that there can be one master with a large number of slaves, however data can only be sent in one direction along a communication link at a time [35], [36].

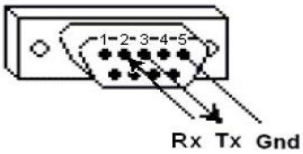


Figure 6-1. Serial Communication Cable [35]

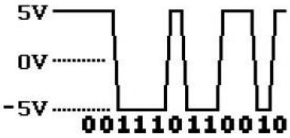


Figure 6-2. Binary Sequence of Bits [35]

A large string of ones and zeros in a complex binary sequence, shown in Figure 6-2, can be quite difficult to read and translate so Modbus requires that each block of four bits be divided into the hexadecimal number from 0 to F as shown in Table 6-1 [35]. Each byte of data, which consists of 8 bits, can be described using one of the 256-character representations from 00 to FF [35].

Table 6-1. Hexadecimal system [35]

0000 = 0	0100 = 4	1000 = 8	1100 = C
0001 = 1	0101 = 5	1001 = 9	1101 = D
0010 = 2	0110 = 6	1010 = A	1110 = E
0011 = 3	0111 = 7	1011 = B	1111 = F

6.1.2 Data storage

In Modbus data and information is stored in the slave device in four different tables [35]. Discrete values (such as those representing on/off states) are stored in two tables called coils. However, the other two tables which are referred to as registers, store numerical values. Each pair of tables that make up the coils and registers have a read-only table and a read-write table respectively. These tables each have 9999 values [35]. In addition, each individual coil is represented by 1 bit and has a data address from 0000 to 270E. On the other hand, the registers are each comprised of 1 word which is 16 bits long or two bytes. Here the data is also addressed in hexadecimal from 0000 to 270E as was demonstrated by table 6-2 [35].

Table 6-2. Coils and registers [35]

Coil/Register Number	Address	Type	Table Name
1-9999	0000-270E	Read-write	Discrete Output Coils
10001-19999	0000-270E	Read-only	Discrete Input Contacts
30001-39999	0000-270E	Read-write	Analog Input Registers
40001-49999	0000-270E	Read-only	Analog Output Holding Registers

The coil or register numbers are also referred to as location names and do not appear within the frame of the transmitted message; only the data address is used in the message to ensure that the appropriate information is stored correctly [35]. The primary difference between the data address and the register or coil number is the offset. Hence, table 6-2 showed how each of the coil and register tables had a numerical offset as follows: 1, 10001, 30001, 40001 [35], [36].

6.1.3 Slave ID

The many slave devices that may exist within a physical substation network are individually assigned a specific slave ID which is defined from 0 to 247 [35], [36]. Therefore, Modbus is constrained to one master with up to 247 slaves. Importantly, when the Modbus master requires data or information from a particular slave IED the first byte it sends in a message is the slave address or slave ID. This ensures that the message is delivered to the correct device and that the other slaves ignore the message if the slave ID or address is not theirs [35], [36].

6.1.4 Function code

The second byte of information that the master sends to a slave device is called the function code. This byte of data tells the slave IED, such as an RTU, which table it needs to use (coils or registers) and if it is going to read or write data to the particular table in question [35], [36]. The various Modbus function codes, their table names and actions were populated in Table 6-3 on the following page.

Table 6-3. Modbus function codes [35]

Function Code	Action	Table Name
01 (01 hex)	Read	Discrete Output Coils
05 (05 hex)	Write Single	Discrete Output Coils
15 (0F hex)	Write Multiple	Discrete Output Coils
02 (02 hex)	Read	Discrete Input Contacts
04 (04 hex)	Read	Analog Input Registers
03 (03 hex)	Read	Analog Output Holding Registers
06 (06 hex)	Write Single	Analog Output Holding Register
16 (10 hex)	Write Multiple	Analog Output Holding Registers

Therefore, based on the past few subsections, the Modbus data package that the master device sends to the slave consists of four specific items, namely: device/slave ID (addressed from 1 to 247), the function code (FC), data address (of the coils/registers) and lastly, the data packet itself [35], [37]. In addition to these four items, a cyclic redundancy check (CRC) could be included at the end of each message package so that the receiving IED can check for any errors in the sent data [35], [37].

6.1.5 Cyclic redundancy check

A CRC refers to the two bytes that should be added to the end of any Modbus message in order to perform a specific type of error detection. Each byte of information that exists within a particular message frame can be used to determine or calculate the CRC [35], [37]. The slave device that receives the Modbus message also determines the CRC and attempts to compare this calculated value with that of the CRC of the sending master. If even a single bit in the sent message is received incorrectly the CRCs of the master and slave will not be the same and an error will have occurred [35], [37].

6.1.6 Modbus RTU

Modbus RTU is a serial RS232 or RS485 communication protocol that communicates data between a single master and multiple slaves [37]. The Modbus RTU packets can only send the data itself whereas items like point name, resolution and units can only be send using other protocols such as Modbus TCP/IP [37]. In Modbus RTU the packets are send with the least important bit first and devices must decipher each byte of information with this procedure in mind [37]. A transmitted byte of data is coded as was shown in Figure 6-3 and in the top half of Figure 6-4 as an 8-bit binary value. The Modbus RTU memory map was populated in Table 6-4 on the following page.

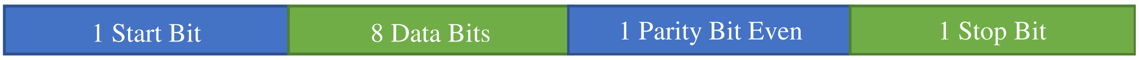


Figure 6-3. Data packet (1 byte) [37]

Table 6-4. Modbus RTU memory map [37]

Modbus RTU Data Type	**Common name**	**Starting address**
Modbus Coils	Bits, binary values, flags	00001
Digital Inputs	Binary inputs	10001
Analog Inputs	Binary inputs	30001
Modbus Registers	Analog values, variables	40001

6.1.7 Modbus TCP/IP

In addition to Modbus RTU, which is a serial protocol, Modbus was also developed to operate over Ethernet using a separate communication standard called Modbus TCP/IP. The acronym TCP stands for Transmission Control Protocol and IP stands for Internet Protocol, hence, these two protocols can be used together to transport data over the internet [38]. When a message is sent the required data is first delivered to the TCP layer where certain transmission specific information is attached to the package [38]. Thereafter the IP layer transfers the data into a packet and transmits it to the requested location. This is achieved by the Modbus TCP master which establishes a communication link with the slave server. In contrast to Modbus RTU, the slave device does not have a slave ID; instead it has an IP address [38]. In addition, one of the major differences between Modbus RTU and Modbus TCP is the 7-bit MBAP Header (Modbus Application Header) that is added to the Modbus RTU data packet [38]. This header includes a 2-byte transaction identifier which is set by the client in order to identify the request. In addition to the MPAB, there is a 2-byte protocol identifier which is also set by the Client, a 2-byte length which specifies the number of bytes in the data message and lastly, a 1-byte unit identifier which identifies the connection of the slave device [38]. This structure was illustrated in Figure 6-4 and offered a comparison between the frames of Modbus RTU and Modbus TCP/IP.

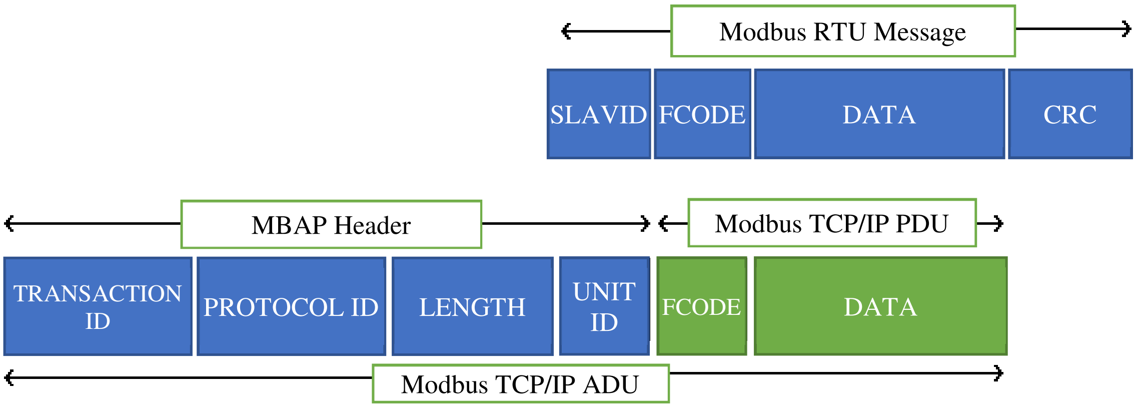


Figure 6-4. Modbus RTU versus Modbus TCP/IP [38]

The construction of a typical TCP/IP packet which can be transmitted using an Ethernet-based substation network connection using Modbus TCP/IP was illustrated in Figure 6-5 on the next page [38].

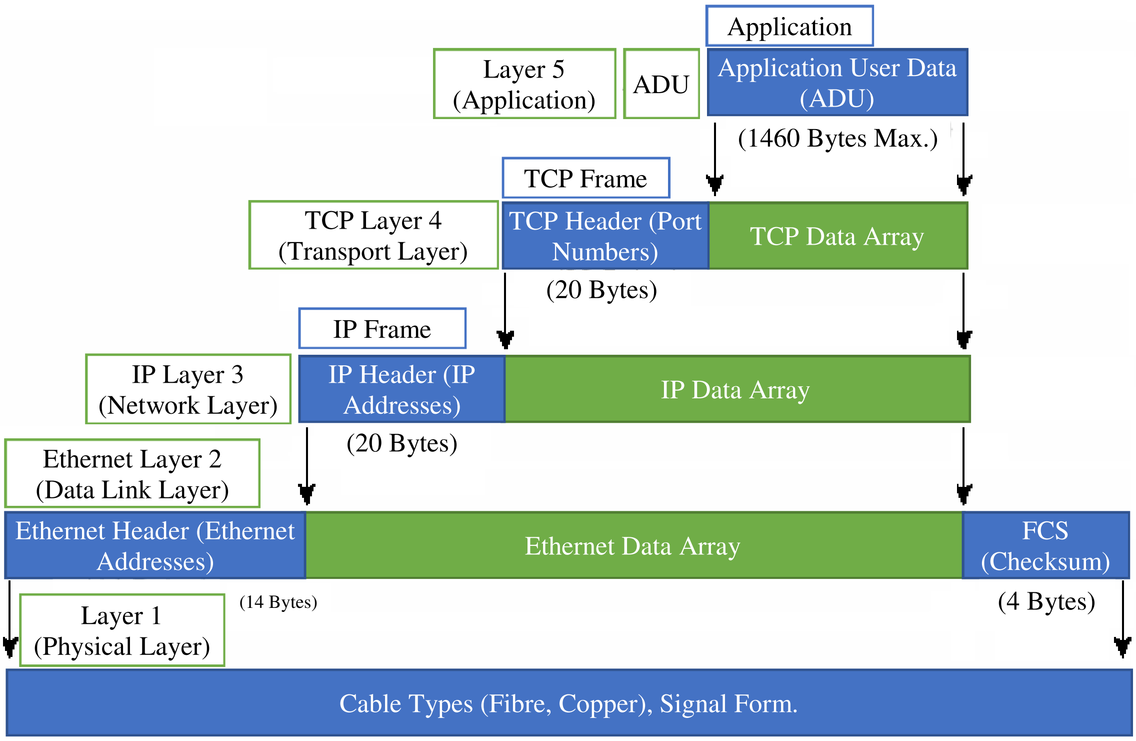

Application
Layer 5 (Application)
ADU
Application User Data (ADU)
(1460 Bytes Max.)
TCP Frame
TCP Layer 4 (Transport Layer)
TCP Header (Port Numbers)
TCP Data Array
(20 Bytes)
IP Frame
IP Layer 3 (Network Layer)
IP Header (IP Addresses)
IP Data Array
(20 Bytes)
Ethernet Layer 2 (Data Link Layer)
Ethernet Header (Ethernet Addresses)
Ethernet Data Array
FCS (Checksum)
(14 Bytes)
(4 Bytes)
Layer 1 (Physical Layer)
Cable Types (Fibre, Copper), Signal Form.

Figure 6-5. Construction of a TCP/IP Ethernet data packet [38]

6.2 DNP3

Distributed Network Protocol 3 (DNP3) was primarily designed as an open source substation protocol that was developed to provide a standard means of communication between the IEDs, instrumentation devices, RTUs and station computers that exist within and external to an electrical substation [39]. This protocol can be defined as a set of serial and TCP/IP-based communication rules that conform to the stringent standards of Working Group 3 of the IEC Technical Committee 57 [39], [43]. DNP3 is exclusively available to all and can be easily accessed for free by vendors and utilities alike [39]. Importantly, all DNP3-based devices communicate using the same language allowing them to easily interoperate with peer equipment [40]. In times past, different IEDs from foreign vendors communicated using proprietary protocols known only to the devices developed by the same manufacturer [40]. Therefore, with the advent of DNP3 the integration of equipment from different companies and the communication between devices within a substation has become a far simpler, easier to implement, efficient and cost-effective reality [40].

DNP3 can communicate via range of different means such as by high speed Ethernet and via low speed radio links; thus, making it robust and versatile for engineers [40]. It also allows many devices to communicate and interact on the same network, which increases the efficiency of the interactions between equipment and limits the number of physical hardwire connections between IEDs and related technologies [40]. Hence, the installation and maintenance of the network is less labour intensive and it saves copper and therefore money. Figure 6-6 shows a high-level diagram which depicts how DNP3 communicates from one point to another.

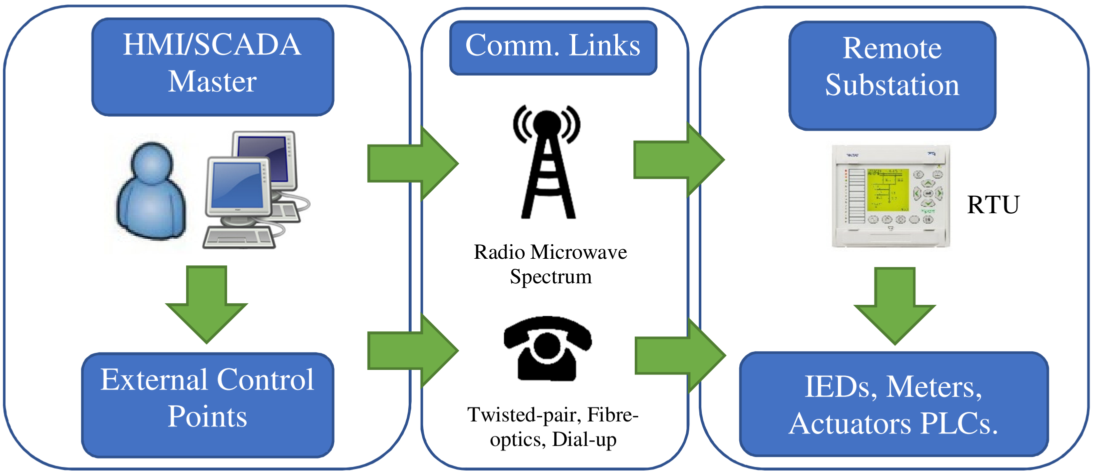


Figure 6-6. High-level DNP3 communication diagram [41]

Commonly considered as a SCADA protocol between RTUs and PCs, DNP3 employs the definition ‘outstation’ to refer to remote computers (like intelligent RTUs) which are located within substations [43]. Furthermore, the term ‘master’ is used to refer to the station level computers located at central control points [43]. Hence, DNP3 defines the set of rules for master and outstation (slave) devices in order to transfer information, data and control commands [43]. Outstation or slave devices are used to gather information that can be transmitted to the station level master, this data includes [43]:

- Binary data that is used to monitor dual-state equipment such as a circuit breaker which can be either in the closed or open positions;
- Analog data that denotes voltage levels, currents and electrical power;
- Counter data that monitors energy consumption in kWh;
- Files with configuration information.

The master station, on the other hand, is used to issue control signals such as [43]:

- Open or close commands for a particular circuit breaker;
- Analog output values to set a required voltage level.

The mater and outstation also communicate items and perform functions such as: synchronizing the time and date, sending recorded or logged data, waveforms and disturbances [43]. DNP3 was primarily intended for SCADA applications and was developed to simplify the transmission of information, acquisition of data as well as the delivery of control commands from one station computer to the next [43]. The conceptual organisation of arrays at the top of the outstation in Figure 6-7 illustrates the location in which different data is stored within the outstations database [43]. Firstly, the array of binary inputs on the left depicts the state of logical devices, whereas the values in the analog input array depict variables that the outstation has measured or calculated. Furthermore, the array of counters illustrates count values that monitor items like power and increase until a maximum is reached before resetting to zero [43]. Additionally, the control outputs exist in an array that denotes logical on-off and, lastly, the array of analog outputs illustrates logical analog variables respectively [43]. The DNP3 master also has a similar database for the arrays already mentioned. Typically, the master utilizes variables in its database to display system states, control outputs and alarms [43]. The master database constantly updates and it achieves this by requesting information from the other outstations asking them to return the desired values in their databases; this is referred to as polling [43].

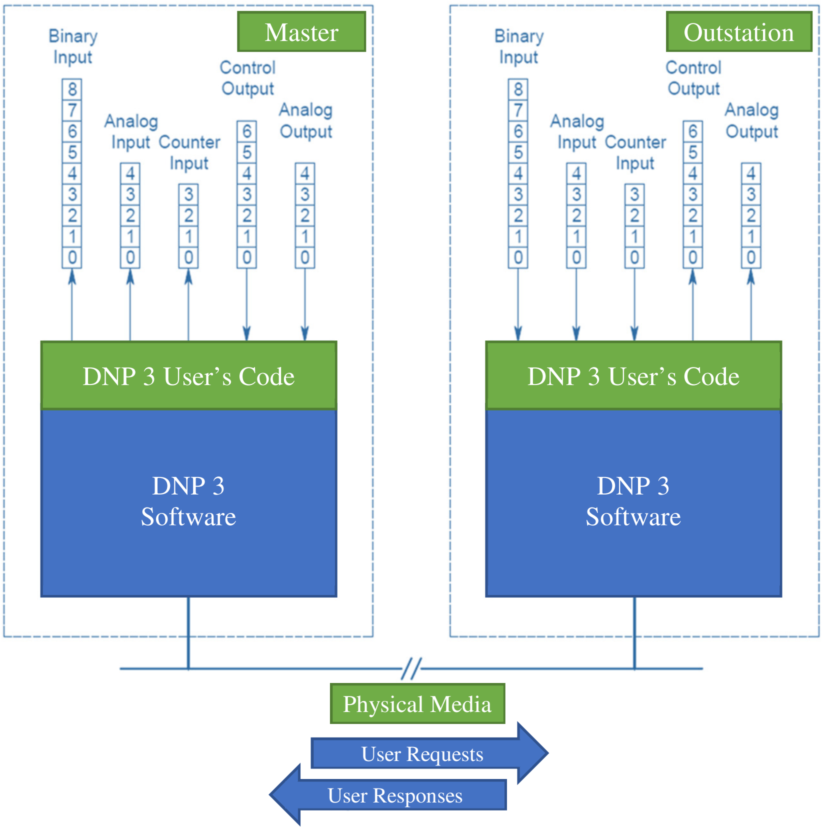


Figure 6-7. Master and outstation communication [43]

6.2.1 DNP3 communication

DNP3 may incorporate one-to-one communication between one master and a slave, or multidrop between a mater and multiple outstations gathering different data and information from each [43]. DNP3 uses 27 generic function codes that are used to transfer packets of information between a master and a remote [42]. These functions include items that allow the master to request and accept status data from a remote device or a remote centre [42]. Other uses of the function codes are to configure and adjust a remote, control the remote or its associated equipment and to allow automated message responses to certain events which enables outstations to report alarms [42].

6.2.2 DNP3 object library

DNP3 has a library of objects that are commonly used for applications that involve SCADA. The objects that occur in this library may include items like binary inputs which deal with discrete instances such as on/off states and breaker open/closed [42]. Alternatively, the analog inputs allow the protocol to communicate characteristics that have a variety or a range of parameters [42]. Objects allow remote centres to communicate information with upstream masters enabling them to capture data from outstations for decision making processes [42].

6.2.3 Message structure

Basic protocols like Modbus RTU are byte-orientated and can exchange a single byte of information in order to communicate [42]. Modbus can also be organized into a packet-orientated structure, with each packet containing a certain number of bytes structured in a particular way (header, data and checksum). DNP3 can also be used as packet-orientated protocol with a structure as was shown in the DNP3 frame in Figure 6-8 as well as in the application layers illustrated in Figure 6-9 [42].

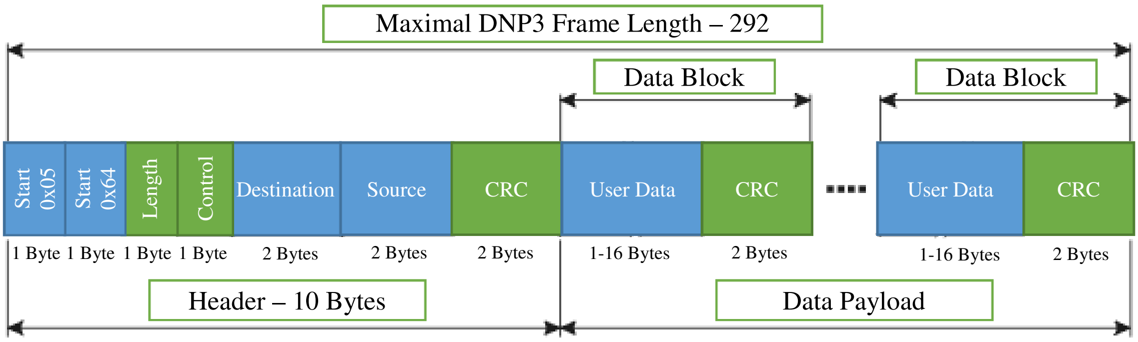


Figure 6-8. DNP3 frame and data payload [42]

The DNP3 frame is comprised primarily of a header and the user data [43]. The header section defines the size of the frame, has data link control information and identifies the source and destination addresses [43]. The user data is typically referred to as the payload and includes the data that has been passed down from the transport and application layers [43]. Additionally, each frame starts with two bytes called the magic that allow the receiver to determine where the frame begins [43]. Furthermore, the length segment of the packet defines the number of bytes in the rest of the frame [43]. The data payload of the link layer contains the CRC pair for every 16 data octets. This means that communication errors can be detected by analysing the checksum. The maximum number of octets in the payload is 250 whereas the maximum length of the link frame is 292 octets if the CRC and the header are included [43]. Using the illustrated packet structure in Figure 6-8 and Figure 6-9 a master will initiate and transmit a read request for an object or multiple objects [43]. The remote will then respond/reply with the desired or requested data [42]. The master can also send an operate command which generates the output actions of the specific object reference [42]. In addition, the remote device can also send an automatic message when a particular event has occurred enabling it to send alarms in the case of a fault [42].

6.2.4 Layered communication

The master and the outstation illustrated in Figure 6-7 both have two different software layers [43]. The top most layer is referred to as the DNP3 user layer. In the case of the master, it interacts with the database and requests outstation data [43]. In the outstation, it fetches the requested data from the outstation database in response to the master request. The second layer which is the DNP3 user code layer, uses the DNP3 software to transmit master requests to the associated DNP3 outstation user code [43]. The DNP3 software layer can be further layered into 3 additional segments.

The application layer of DNP3 includes an Application Service Data Unit (ASDU) which is a packed object as well as an Application Protocol Control Info (APCI) block which makes up the Application Protocol Data Unit (APDU) [42]. Importantly, messages from the application layer are segmented into fragments with the normal size range from 2048 to 4096 bytes [42]. The transport layer seeks to break down the APDU into smaller modules which are of a size of no more than 16 bytes [42]. Thus, the transport layer is given the job of dismembering long application layer messages into much smaller packets that are suitable for the link layer to transmit [43]. This layer also reassembles frames into longer application layer messages when receiving messages. In DNP3 the transport layer is incorporated into the application layer [43]. The transport package consists of an 8-bit transport control header as well as a 16-bit module which contains the CRC. This creates the transport frame. The link layer attaches a header to the control and address data which ensures the entire packet is ready to be transmitted to a particular destination [42]. The link layer ensures that the physical link is reliable. It achieves this using error detection as well as duplicate frame detection to avoid redundant frames [43]. The link layer sends and receives packets called frames, as was illustrated in Figure 6-2 and Figure 6-9. In some cases, the transmission of more than one frame may be necessary to transport all of the information from one point to the next [43].

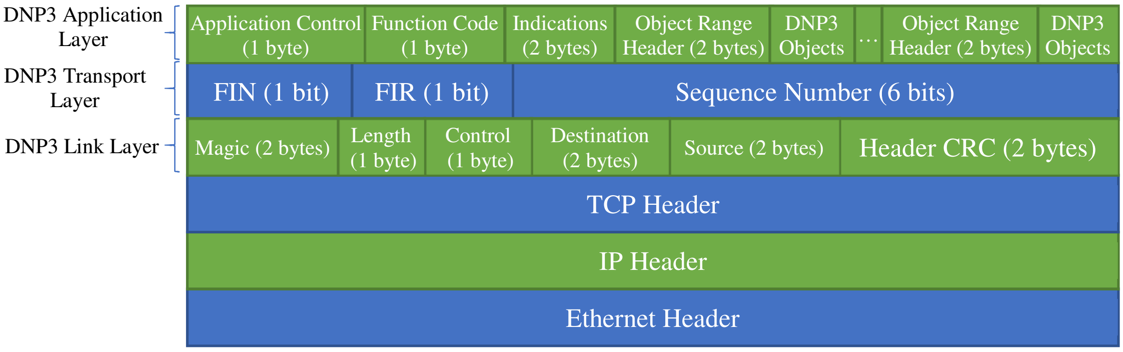


Figure 6-9. DNP3 application layers [42]

In addition, the aforementioned layers can be mapped onto a four-layer model depending on how the information and data is being sent [42]. If the packet is sent via a LAN then the three previously mentioned DNP3 layers can be packaged into a single application layer [42]. This packet is then enclosed in a TCP by the transport layer which is additionally wrapped in a IP by the internet layer [42]. The fourth and final layer to be mentioned in this instance is the network interface layer [42]. This stage is where the wrapped and layered packet of data is interfaced via a method or medium of transportation such as a co-axial or fibre optic cable [42]. This aforementioned process of layer communication can be seen by the graphical representation in Figure 6-10.

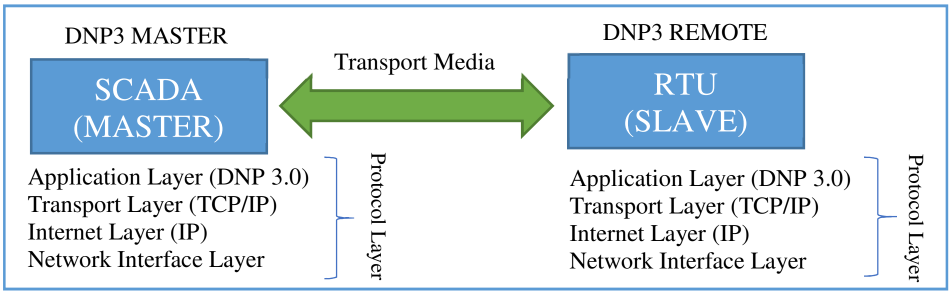


Figure 6-10. Layer communication model [42]

6.2.5 Navigating the layers

If one was to consider an example of a Master which submits a read request over a LAN since it wants to know the status of the Remotes power then the communication of data can be intricately described as is to follow [42]. The Master must first prepare a read request message for the object that is concerned. This read message passes through the three DNP3 layers and finally arrives at the TCP/UDP transport layer [42]. This transport layer must add a block to the packet that identifies the port on the Master from which this request message was initially sent [42]. The transport layer then finds the particular port on the Remote device to which the message should be transmitted. After this process, the packet passes to an IP layer where the data segment is included [42]. This contains the IP addresses of both the Remote and Master devices. Finally, the completed packet is transferred to the network interface layer which places the packet on a particular medium, like fibre optics, for it to be transmitted to the Remote [42].

When the sent package is received by the Remote device it must pass through the exact same four layers but in the opposite order as it did in the Master [42]. It is firstly pulled off the transportation medium (cable) by the network interface layer where it passes to the IP layer [42]. The IP verifies the addresses and passes the packet to the TCP/UDP layer [42]. If an application is listening at the target point then the packet passes to the application layer [42]. However, if the application listening is the Remote DNP3 process then the packet is passed to the three DNP3 layers to identify the request and send the appropriate information back to the Master [42]. When the message/data is send from the Remote device it follows the identical process in the reverse direction back to the Master.

The user layer in the master station generates its appeal for data from the outstation by informing the application layer of the functions that it needs to execute (like reading) and it also defines the data types that it requires [43]. Additionally, this request can specify the number of objects it wants [43]. The application layer then delivers the request through the transport layer to the link layer, which sends the message to the outstation [43]. The link layer checks the frame for any errors and then delivers it to the transport layer where the message is constructed in the outstation application layer [43]. The application layer then informs its user layer which groups and format variations were requested. Variations and groups define the format and type of data whether it be static or analog, integer of floating point [43].

Responses are similar since the outstation user layer retrieves the desired data and delivers it to the application layer which uses the group and variation numbers to format user layer data into objects [43]. Data is then sent across the communication medium to the master's application layer. The data objects are then finally given to the master user layer [43].

6.2.6 Data and Addressing

(i) Addressing

The destination address identifies which DNP3 device must process the data, whereas the source address identifies which device sent the message [43]. Hence, the receiver knows where to direct its responses. There are 65520 individual addresses available [43]. Naturally, each DNP3 device must have its own distinct address within the network of substation devices that all send and receive messages [43].

(ii) Static and Event Data

In DNP3, the term 'static' is utilized to define the present value of data. Therefore, static binary data may refer to the on/off state of a dual-state device [43]. Static analog data contains the instantaneous value of an analog signal [43]. The term 'event' is associated with state changes, values exceeding certain thresholds, varying data, transient data and new information. An event may occur when a particular binary value changes from an on state to an off state. DNP3 can report events with or without time stamps if required [43]. The master user layer can request events and may be updated quickly if it polls for events from the outstation and only occasionally requests for static data. This is because reason the number of events generated is small and, thus, less data must be returned to the master [43]. DNP3 may also classify events into three classes [43]. Class 1 events are considered to have highest priority, class 2 events have medium priority, and lastly, class 2 events have the lowest priority [43]. The user layer can request the application layer to poll for combinations of class 1, 2 or 3 events [43].

6.2.7 DNP3 in SCADA systems

This section discusses an important list of considerations that need to be kept in mind when using DNP3 within a SCADA system and the associated controls, actions, roles and functions of the Master as well as the Remote [42].

- Masters should be able to deliver concise alarm information/messages.
- Masters should be able to recognize and identify alarms that have been cleared.
- Masters should be able to capture a concise history of the active and cleared alarms.
- Remote devices should support emergency power and power back-up.
- Remote devices should provide on-site SCADA so that units can be browsed on site.
- Master devices should be able to sort through and sift through alarms
- Masters should support automatic/manual notifications, monitoring and status events.
- Lastly, Masters should not only be limited to DNP3 communication protocols but should also support other standards like Modbus.

6.3 Comparative analysis

6.3.1 Literary analysis

(i) DNP3

The DNP3 protocol, because of its many features listed below, helps enormously in implementing a complex system [45]. This in turn helps to decrease the operational and maintenance costs of the system which benefits the client as well as the end-user [45]. The advantages of DNP3 are as follows:

- Open protocol allowing the end-user to install equipment from different vendors while maintaining a single top end SCADA (or DNP3 master). DNP3 and Modbus are both open protocols, Modbus being the mostly commonly used due to its compatibility with a variety of devices and simplicity to implement [45]. IEC 61850 on the other hand is not exclusively open source although some free implementations available.
- DNP3 allows the user to categorize field data, thus allowing for efficient communications and data transfer between a master and outstation. DNP has common classes 0, 1, 2, and 3 to group data. Classes 1, 2 and 3 are used for objects that require time stamped information. The class also has a variation parameter associated with it that allows the user to select the data type, time and diagnostic information to be recorded [45]. Modbus RTU on the other hand offers no way of representing object classes whereas the IEC 61850 standard takes this idea to new heights.
- Unsolicited reporting – allows events to be reported from the outstation as and when they occur rather than only when they are polled by the master; something Modbus RTU is incapable of doing [45].
- DNP3 and IEC 61850 both have the ability to log an event with a time and date stamp as and when it occurs. There are two primary advantages of this: firstly, if an event occurs at a different instant in time to which the outstation is being polled then the time of the event is not lost or misjudged. Secondly, if there is a communication failure between the outstation and the master the outstation can still record the event and time stamp and restore this information to the master when communication is restored [45].
- Time Synchronisation – accurate and reliable time-based scheduling.
- Secure authentication with dynamic key management between a DNP3 master and outstation. This allows the slave and master to determine whether or not they are communicating with the appropriate master or slave. This may be achieved using the 'select-before-execute' principle where the master sends a 'selects' signal to an outstation and awaits its response, the outstation will only execute the control action if the 'operate' command has been received from the master within a given amount of time [45].
- Communication to multiple DNP3 Masters, thus making the same data available at multiple locations. Data is made available to system-wide top-end masters. This is important if systems are spread out over a large area and many operators require access to the local data [45]. The IEC 61850 standard also achieves this to great effect within the confines of the substation.

(ii) Modbus

The primary advantage of Modbus is its simplicity for small devices and the very large range of devices that have some sort of Modbus interface. It is widely used in process control and SCADA systems [44]. However, when one compares Modbus to protocols like the IEC 61850 standard and DNP3 it has many disadvantages in this new technologically advanced era. These include:

- The Modbus protocol standard does not specify how the 16-bit register values are sent. They may be sent high-byte first or low-byte first, signed or unsigned [44]. Successive registers may even be combined to create floating point numbers. [44] Many Modbus device manufacturers add custom extensions to their devices to extend the functionality beyond that provided by standard Modbus [44]. This and the common use of outputs as inputs sometimes makes it quite difficult to make even simple Modbus devices inter-operate [44]. Since the data types are not strictly defined, knowledge of how the device sends data is required in order to interpret the value that is sent. This adds an additional step of complexity to the Master station setup [44].
- No standard way exists for a node to find the description of a data object, for example, to determine if a register value represents a temperature between 30 and 175 degrees. [37]
- Since Modbus is a master/slave protocol, there is no way for a field device to “report by exception” (except over Modbus TCP/IP) [37].
- No time stamps or time synchronization. Modbus treats all data as "present value". Standard Modbus does not have a concept of events or time. Any data that is not collected by reading it is lost when new field data updates it [44].
- Modbus is restricted to addressing 247 devices on one data link, which limits the number of field devices that may be connected to a master station (once again Modbus TCP/IP the exception) [37].
- Modbus data transmissions must be continuous which limits the type of remote communication devices to those IEDs that can buffer data to avoid gaps in the transmission. [37]

(iii) IEC 61850

The advantages of the IEC 61850 substation protocol are boundless; it vastly out matches the capabilities of Modbus RTU and Modbus TCP as well as building substantially from the foundations set by DNP3. For example, the use of virtual LANs and priority flags for GOOSE and SV messages allow for the intelligent use of Ethernet switches which was not previously possible [46], [7]. This on its own can deliver significant benefits to users in terms of optimizing bandwidth traffic which is not possible using other approaches [46], [7]. For the sake of economy, the author lists some of the more typical features that provide tremendous benefits to users who employ the IEC 61850 standard [46], [7]:

- Virtualized Model: The virtual model which consists of logical devices, logical nodes and Common Data Classes (CDCs) allows for the definition of the information, commands as well as the behavior of devices. The protocol itself is used to define how the data is transmitted over the network.
- Names for data: Each and every component of the IEC 61850 data model is given a name using descriptive strings to describe the information or command. Legacy protocols like Modbus tend to identify data by items like storage location, index numbers and register numbers respectively.
- Standard Object Names: The names and descriptions of the information or commands used by an IEC 61850 device are not defined by the device vendor or by the user. They are determined in the standard itself and are provided within the context of a power system. This allows an engineer to quickly identify the meaning of data without having to look at protocol message class mappings or match index numbers, register locations or addresses to power system data.
- Self-describing devices: IEC 61850 clients that communicate with IEC 61850 compliant devices have access to the descriptions of all the data of the device without any prior configuration of data objects or names.
- High Level Services: The GOOSE, GSSE and SV classes are just a few of the special message capabilities of the IEC 61850 protocol that allow generic and efficient communication.
- Standard Configuration Language: SCL allows devices to be configured and precisely defines the role of devices within the power system using XML files. When a new device is added the SCL configuration files of the previous devices are simple added.
- Economic Viability: The IEC 61850 standard offers lower installation cost to substations, lower commissioning costs, cheaper maintenance and lower transducer costs to name but a few of the economic advantages of this standard.

6.4 Evaluation of experimental observations

6.4.1 Preliminary work

The study that was conducted during the course of chapter 4 sought to achieve the implementation of a multi-protocol substation communication network and SCADA. This section saw the execution of DNP3, Modbus RTU and IEC 61850 on the substation network. Once the preliminary model was developed the engineering features, functions and facilities of the experimental substation could be tested. Chapter 4 formed a basis for future work and laid the groundwork for the main research which was accomplished at a later stage in chapter 5.

One of the main observations made during the course of the preliminary work was based on the technical and economic obstacles that multi-protocol communication networks pose to engineers. Convoluted amalgamations of different substation protocols which exist on the same substation network require expensive gateway devices, knowledge of a wide variety of communication standards, different physical transport layers over copper or fibre (RS232/RS485 serial or Ethernet), IEDs with an extensive range of protocol compliance, complicated labour-intensive installation and maintenance as well as different device configuration and setup procedures. These numerous aspects lead to the inception of ‘hybrid’ substations which, in comparison to a solely IEC 61850 substation architecture, are less efficient both technically and economically in their approach to design, automation and protection.

Secondly, during the establishment of both modern (IEC 61850) and legacy (Modbus RTU and DNP3) communication standards on a multi-protocol network it became evident that there were certain limitations to the latter. Modbus RTU in particular was considerably more constrained in its approach to communication between devices. This means that certain functions and features of modern substation automation and protection could not be achieved using Modbus RTU. The most prominent among these was the absence of time stamped data; because of this Modbus RTU was unable to give exact information about the time of events or the number of events (like breaker operation) that had occurred. This means that if there was a break in communications between Modbus RTU devices then information could be missing or lost since it could not be updated after communication was restored. This left gaps in captured trends and missing data upon loss of signal. In addition, certain protection features like blocking response (sympathetic trip protection) are far more tedious to implement in legacy schemes using Modbus RTU since they rely on a huge number of cross wired binary inputs between all the appropriate relays connected on the network. Therefore, the use and expense of copper hardwire related connections between devices on the network could be large and inefficient.

DNP3 over Ethernet was much more effective in its approach to the transfer of data, commands and signals between substation devices and SCADA. Here data is time stamped which means that engineers could be informed of the exact moment in time in which certain events (like breaker operation) had occurred. In addition, if there was a break in communication then graphical and numerical data could be restored along with the associated time stamps. As a result, DNP3 could be used to enable alarms and alerts on the substation SCADA model as well as for time related trending and graphs.

Finally, the IEC 61850 substation protocol allows for a huge variety of automation, protection and communication features and functions. During the course of the preliminary study the IEC 61850 standard was only implemented on the station bus between the RTU and the IEDs. Here only messaging directly between the RTU and the IEDs (GOOSE and Report) was used to deliver the status of equipment and commands from the remote end. Further investigation of the automation and protection applications of inter-IED communication using GOOSE was implemented during the course of chapter 5. However, just based on the basic implementation of the IEC 61850 standard during stage 1 experimentation a number of advantages were revealed. The most obvious of which related to the 'virtual' Ethernet-based architectures on which the protocol was based. IEC 61850 allows for communication over a local TCP/IP-based network which reduced the number of complex physical copper hardwire connections within the substation. In addition, the IEC 61850 protocol used functions called logical nodes to transfer commands and properties between the RTU and the IEDs. These logical nodes could be used to define breaker operation and status as well as isolator, earth switch and the mode of operation of the IED. This was both an efficient and effective way of controlling smart devices.

6.4.2 Main research

The final segment of the study (chapter 5) which was concluded prior to this chapter sought to discover and appraise the IEC 61850 and GOOSE-based implications on substation protection and design. This section saw the configuration of breaker fail, arc-flash and blocking-based protection techniques using the descriptive attributes of the GOOSE message class.

Modbus RTU is considered to be a rather simple and primitive form of communication relying on the potential difference between two wires to transfer data over serial RS 485. The interconnection of devices using a copper hardwired-based physical layer such as this is complicated, confusing, expensive as well as labour intensive and time consuming. Therefore, legacy-based breaker fail, arc-flash and blocking protection is far to inconvenient and inefficient to be using serial protocol techniques. Hence, Modbus RTU was implemented outside the IEC 61850 protection zone of the model in chapter 5. Making the migration to "virtual" Ethernet networks using DNP3 is a step in the correct direction. This standard includes valuable features like time stamping and priority messages that can be communicated using TCP/IP-based means. Often used as a telecontrol protocol, DNP3 was implemented between the SCADA and the PC during the course of the final research.

The IEC 61850 substation standard, on the other hand, seeks to build on the more convenient foundations left by DNP3. It did so by providing an intelligent, descriptive and expedient message class using GOOSE. Chapter 5 saw the implementation of GOOSE for breaker fail, arc-flash and blocking-based protection. Therefore, this protection used the logical nodes, attached parameters and corresponding objects of GOOSE to configure an appropriate message in each case. This allowed the IEDs of adjacent feeders, incomers and systems to share status, position, operation and fault conditions of associated switchgear and cables with subscribing devices. This gives devices a much larger understanding of the actionable outcomes and ongoing of many different functions of different IEDs throughout the protection zone. Therefore, using the GOOSE message class many different types of protections, including those mentioned, can be carried out quickly and effectively improving coordination, grading and selectivity on the grid. GOOSE and by extension the IEC 61850 standard is forcing legacy substations to convert to a “virtual” ethernet-based SAS environment relying on compliant protection IEDs, IOUs, MUs, priority switches and modern gateways. Hence, the design of substations has been greatly impacted and transformed as a direct result of the IEC 61850 protocol.

6.5 Discussion, recommendations and conclusion

The experimental and literary-based inferences that were drawn from this comparative study concluded that the IEC 61850 substation protocol was both intelligent and powerful in its approach to substation communication. Hence, this standard was considered to be advantageous, convenient and favourable when compared to legacy protocols such as Modbus RTU and DNP3. The IEC 61850 protocol is a standard for substations of the future and should be implemented more frequently as old and aging infrastructure is replaced or upgraded. This universal specification for substation communication owes its success and innovation to the advanced GOOSE message class, the implications of GOOSE messaging on various methods of protection and automation, its interoperability between vendors as well as its ‘virtual’ Ethernet-based architectures. Legacy standards, including Modbus RTU and DNP3, lag substantially behind the IEC 61850 protocol in all aspects and applications. This is a gap which should only broaden with development and future progress in substation engineering.

7. CONCLUSION

7.1 Final discussion

The future-proof IEC 61850 substation communication protocol is both universal and unique in its approach to substation engineering. The strongest merits of this standard arise from its sturdy design philosophies which promote interoperability, reliability, coordination and system security. IEC 61850 is both resilient and flexible which makes it capable of adapting to future developments in communication technology. Therefore, as a result of this robustness, it is unlikely that it will become redundant or obsolete in the coming years [47]. The IEC 61850 standard achieves this longevity as a result of its design architecture which separates substation-specific applications from innovative communication technologies [47]. The slow growing aspects of substation engineering and the expedient and explosive growth of 'virtual' communication systems have called for this basic design approach [47]. Hence, the IEC 61850 protocol has been referred to as future-looking as well as long-term since it seeks to safeguard the investments of current infrastructure, technology and systems [47].

The *raison d'etre* of this dissertation was the consideration of the IEC 61850 substation protocol and its implications for protection, automation and substation design. The principal goals of this study were prosecuted by a literature review in chapter 2, an initial experimental phase in chapter 3, a main research component in chapter 5 as well as a comprehensive comparative assessment in chapter 6. In was within these four segments that the key justifications of this dissertation were defended. Firstly, the literature study comprised a fact-finding investigation which critically reviewed scientific texts, published works as well as the standards of industry. The aims of this review were to garner a technical understanding of IEC 61850, its methods of communication, structures, applications as well as its impact on substation engineering. In addition to the literary investigation, the inceptive design component of this dissertation was introduced during the course of chapter 4 where a multi-protocol communication model was created based on a typical substation architecture. It was here that DNP3, Modbus RTU and the IEC 61850 protocol were implemented between both modern and legacy IEDs, an RTU and the station computer. Furthermore, a substation SCADA was developed to monitor and control equipment as well as administer interactive dialogue with the operator whilst being interfaced with the physical hardware model. Finally, the terminus of the main study was reached during the course of chapter 5. This concluding stage of research explored the GOOSE-based aspects of IEC 61850 and assessed the implications of the GOOSE message class on breaker fail, arc-flash and blocking-based protection that took place within the substation model. Ultimately a detailed comparative assessment of each of the substation communication protocols that was explored in this study was presented in chapter 6. It was at the end of this chapter that the merits of the IEC 61850 communication standard were discussed and evaluated.

The development of a multi-protocol communication network highlighted the limitations of legacy protocols as well as the disadvantages of complicated multi-protocol substations. These concepts were tackled during the preliminary research phase that was conducted in chapter 4. An intricate marriage of proprietary communication protocols existing between the IEDs within a substation can present both technological and economic barriers to engineers and utilities alike. By having different communication standards such as Modbus RTU, DNP3 and IEC 61850 the system can become constrained by a variety of different limitations that each protocol may present. In particular Modbus RTU lacks the ability to time stamp data, is hardwire-based, relies on continuous communication, is a 'present value' system, and does not allow for time synchronisation between IEDs. DNP3 on the other hand expands on the lack of Modbus functionality by adding time stamping, classed data for priority messages, and is based on a 'virtual' Ethernet architecture. Furthermore, the configuration, connection and maintenance of a multi-protocol network can become incredibly labour intensive, complex and therefore expensive to implement. In addition, technologies like smart gateways must be added to the network in order to interface different protocols. Chapter 4 works achieved a functional substation hardware model, communication network and SCADA using DNP3, Modbus RTU and IEC 61850. The breaker fail, earth fault, overcurrent, local mode and steady state conditions for the model were tested, trended and interactively represented using the substation SCADA, RTDS, a current amplifier and an RSCAD test model. These results validated the sound operation of the model itself and drew attention to the disadvantages of legacy-based Modbus RTU in comparison to the further advanced standards such as DNP3 and especially IEC 61850.

The kingpin of the IEC 61850 protocol must be the convenient yet powerful GOOSE message class. This fundamental playmaker of IEC 61850 is famous for its intelligent retransmission mechanism that transfers commands, switchgear status and data periodically after an exponential decay in time (4 ms, 8 ms, 16 ms etc) [48]. In chapter 5 this approach ensured that messages which were multi-cast to the substation LAN by a publisher IED were received by the appropriate subscribing devices [48]. A primary process object as well as a protection or control function could be modelled into a standard logical node with common classed data that was grouped under a particular logical device [48]. Using this model, an IED could be configured to transfer a GOOSE message that had been grouped into a data set which contained value and status information along with certain attributes, parameters and instances [48].

A more detailed consideration of the IEC 61850 standard was implemented during the course of the main research component which was demonstrated in chapter 5. It was here that the GOOSE message class was used to provide breaker fail, arc-flash and blocking-based protection to the substation model. The results, analysis and evaluation of each of the aforementioned protection schemes was presented in the aforementioned chapter. In order to setup GOOSE-based communications between the respective IEDs within the substation model the VAMPSET software configurator was used. VAMPSET allowed the user to prepare the GOOSE data set, setup the GOOSE control block parameters to specify how data was sent as well as define the subscribing IEDs. In breaker fail protection GOOSE provided a quick yet effective way to automatically isolate a fault that was present as a result of the loss of a particular circuit breaker. In addition, arc-flash protection using GOOSE sought to quench an arcing busbar or cable by opening all the circuit breakers that were connected to the affected bus. Sympathetic trip protection or blocking logic, on the other hand, used GOOSE messaging to help decreased fault clearing time and increased system performance. Hence, a protection scheme by GOOSE can provide improved reliability, greater security, easy relay interoperability, simple expansion as well as large cost savings to both a substation and its utility [48].

An IEC 61850-based architecture greatly differs from the topology of a conventional substation. Therefore, the upgrade of aging infrastructure is creating a shift from legacy and hybrid substations to an almost completely ‘virtual’ IEC 61850 environment [49]. This has greatly reduced the demand for copper hardwire connections within substations, decreasing the need for deep cable trenches to the control room, expensive terminations and lengthy wiring. Furthermore, IEC 61850-compliant equipment such as MUs can be placed at or near the switchgear adjacent to the CTs which can help to reduce the length of copper cables from the CTs to the control room. This process shortens the conductor and therefore can drastically drop the total resistance of a particular cable which is a contributing factor towards the elimination of CT saturation. Therefore, from just one example, it has been revealed that substation design is and must change to suit the requirements of IEC 61850 and its associated systems.

The future-proof IEC 61850 standard has defined the way substation-specific information, commands and data can be transferred quickly between similar or vendor-diverse devices over an Ethernet-based local area network [49], [50]. This protocol has represented a leap in convenience, application, efficiency, reliability and security of communications [49], [50]. Legacy-based protocols such as Modbus RTU and DNP3 represent the past. The IEC 61850 protocol is a sovereign standard of tomorrow and is changing the design, automation and protection of substations for the better.

7.2 Future works and development

This careful study considered a functional multi-protocol substation communication network, formed comparisons between standards like Modbus RTU, DNP3 and IEC 61850 as well as implemented the GOOSE message class for breaker fail, arc-flash and blocking-based protection schemes. Despite this, the IEC 61850 protocol and the smart GOOSE message class have yet further applications for substation engineering. The following items, which were discussed in greater detail at the end of chapter 5, could be examined during the course of later works.

- Busbar earthing using GOOSE
- Disturbance recording
- GOOSE-based 1 of N blocking
- Selective backup tripping
- Priority tagging/VLANs

It must be noted, during the course of this conclusion, that the equipment (IEDs, Gateway/RTU and other devices) which was used during the course of this study was not necessarily preferred in this context. The author could not advocate for a particular device by a certain manufacturer since only those from Schneider Electric were utilized during this investigation. Unfortunately, the study was limited by the equipment which was donated and available to the university at the time. Therefore, a benchmark was obtained, however, since the IEDs of rival vendors were not worked on the author could not adequately say that one device/manufacturer should be preferred over the other. Alternatively, it could be concluded that the VAMP 259/255 IEDs were user friendly, both in the operation of the HMI as well as in the ease of their configuration using VAMPSET. In addition, the VAMPs were also compliant with a variety of different serial and Ethernet based communication protocols, including the IEC 61850 standard. The MiCOM P122 IED on the other hand, was a legacy relay with drawbacks in terms of the limited serial protocols which it supported, however it provided simple and reliable relaying to the system over Modbus RTU. Lastly, the MiCOM C264 was found to be an intelligent, convenient and advanced gateway/bay computer which was configured with the graphical, electrical and communication topology of the developed substation. This allowed for the ease of interface of devices operating over different protocols as well as for the development and interaction of a SCADA model on CitectSCADA. Finally, part of the future expansion of this study could be to obtain a wider variety of protection, automation and monitoring equipment in order to gain a better understanding of which devices and vendors are preferred over others as well as to show how protocol-based communication differs between various manufacturers.

The IEC 61850 protocol has thus far been limited to protection schemes and engineering applications that form part of the internal abstract components of a substation [51], [52]. Protections that require inter-substation (external) communication have yet to properly benefit from the IEC 61850 substation standard. However, this type of external communication has already begun to develop and the first inter-substation IEC 61850 communications have now started their early implementation phase [51], [52]. As this protocol becomes more widely implemented the future growth, technical development, expansion and longevity of the future-proof IEC 61850 standard is assured.

8. APPENDICES

ANNEX A – PROTECTION IEDS

A. IEC 61850-Compliant IEDs

VAMP 259

Line Manager

Publication version: V259/en M/A010

User Manual

Schneider Electric

VAMP 255 and 230

Feeder and Motor Manager

User manual

63230-218-205
04/2015

Retain for future use.

Schneider Electric

B. Legacy IEDs

MiCOM
P120/P121/P122/P123

Overcurrent Relays

1.1 USER INTERFACE

1.1.1 Relay Overview

The next figures show the P120, P121, P122 and P123 relays.

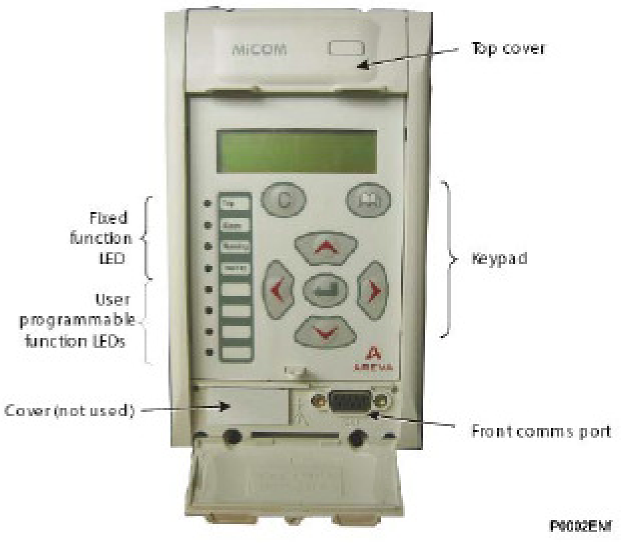
The table shows the case size for the relays.

Height	Depth	Width
4U (177mm)	226mm	20 TE

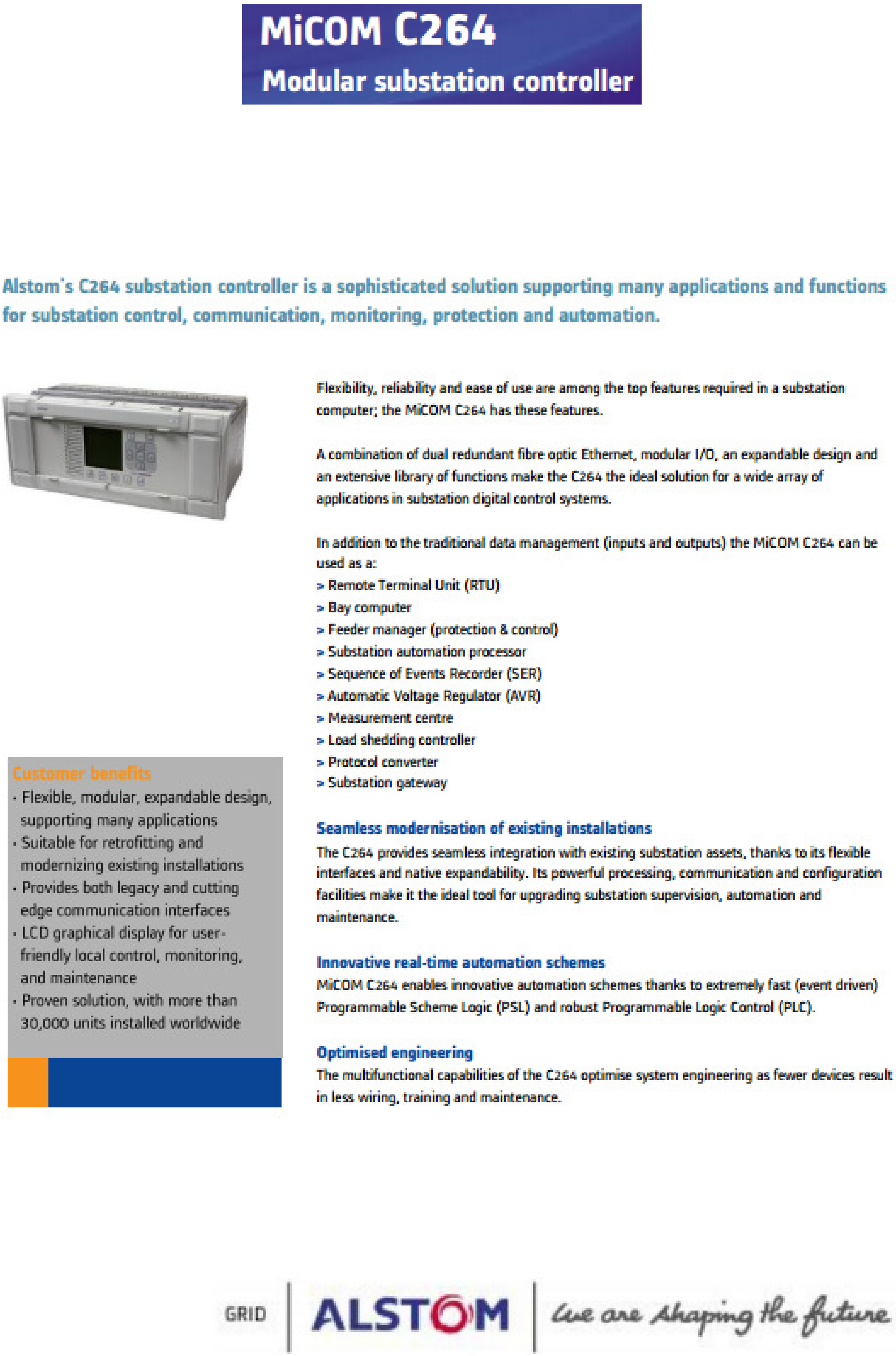
The hinged covers at the top and bottom of the relay are shown closed. Extra physical protection for the front panel can be provided by an optional transparent front cover; this allows read only access to the relays settings and data but does not affect the relays IP rating. When full access to the relay keypad is required to edit the settings, the transparent cover can be unclipped and removed when the top and bottom hinged covers are open.

1.1.2 Front panel description

MiCOM P120, P121, P122 and **P123** relay front panel allows the user to easily enter relay settings, display measured values and alarms and to clearly display the status of the relay.



C. Remote terminal unit



MiCOM C264
Modular substation controller

Alstom's C264 substation controller is a sophisticated solution supporting many applications and functions for substation control, communication, monitoring, protection and automation.

Flexibility, reliability and ease of use are among the top features required in a substation computer; the MiCOM C264 has these features.

A combination of dual redundant fibre optic Ethernet, modular I/O, an expandable design and an extensive library of functions make the C264 the ideal solution for a wide array of applications in substation digital control systems.

In addition to the traditional data management (inputs and outputs) the MiCOM C264 can be used as a:
> Remote Terminal Unit (RTU)
> Bay computer
> Feeder manager (protection & control)
> Substation automation processor
> Sequence of Events Recorder (SER)
> Automatic Voltage Regulator (AVR)
> Measurement centre
> Load shedding controller
> Protocol converter
> Substation gateway

Customer benefits

- Flexible, modular, expandable design, supporting many applications
- Suitable for retrofitting and modernizing existing installations
- Provides both legacy and cutting edge communication interfaces
- LCD graphical display for user-friendly local control, monitoring, and maintenance
- Proven solution, with more than 30,000 units installed worldwide

Seamless modernisation of existing installations

The C264 provides seamless integration with existing substation assets, thanks to its flexible interfaces and native expandability. Its powerful processing, communication and configuration facilities make it the ideal tool for upgrading substation supervision, automation and maintenance.

Innovative real-time automation schemes

MiCOM C264 enables innovative automation schemes thanks to extremely fast (event driven) Programmable Scheme Logic (PSL) and robust Programmable Logic Control (PLC).

Optimised engineering

The multifunctional capabilities of the C264 optimise system engineering as fewer devices result in less wiring, training and maintenance.

GRID | ALSTOM | we are shaping the future

ANNEX B – DETAILED EQUIPMENT LIST

A. List of software and equipment

1) Station computer and configurators
    - i) Equipment
        - (1) Station Computer (PC)
    - ii) Software
        - (1) CitectSCADA
        - (2) PACiS System Configurator
        - (3) VAMPSET
        - (4) MiCOM S1
2) Substation network, monitoring and protection hardware
    - i) IEC 61850 compliant IEDs
        - (1) VAMP 259
        - (2) VAMP 255
    - ii) Legacy IED
        - (1) MiCOM P122
    - iii) Remote terminal unit
        - (1) MiCOM C264
    - iv) Ethernet switch
        - (1) Moxa PowerTrans PT-7728 series
    - v) Circuit breaker
        - (1) Omron MK2KP
3) Test devices
    - i) Equipment
        - (1) PC
        - (2) Real Time Digital Simulator (RTDS)
        - (3) Omicron current amplifier
        - (4) Arc sensors
    - ii) Software
        - (1) RSCAD simulator

9. REFERENCES

[1] J.L. Blackburn, T.J. Domin, “Introduction to General Philosophies,” in *Protective Relaying: Principles and Applications*, 3rd ed., New York: Taylor and Francis Group, 2006, pp. 31 – 58.

[2] A. Valdes, C Hang, P. Panumpabi, N. Vaidya and C. Drew, “Design and Simulation of Fast Substation Protection in IEC 61850 Environments,” presented at the *Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Seattle, WA, USA, 2015, pp. 1-5.

[3] B. Lundqvist, B. Bjorklund and T. Einarsson, “A user friendly implementation of IEC 61850 in a new generation of protection and control devices,” ABB Power Technologies, Sweden, Rep. SA2007-000062, vol. 1, 2007. [Online]. Available: http://fs1.gongyeku.com/data/default/201212a/20121215232059843.pdf, Accessed on: 17th March 2017.

[4] D. Hou and D. Dolezilek, “IEC 61850 – What It Can and Cannot Offer to Traditional Protection Schemes,” *Sel J. of R. Pwr*, vol. 1. pp. 1-11, 2010.

[5] H. H. Lim and T. S. Sidhu, “Design of Backup IED for IEC 61850-Based Substation,” IEEE Transactions on Power Delivery, vol. 28, pp. 2048 – 2055, 2013.

[6] R. P. Gupta, “Substation Automation using IEC61850 Standard,” presented at the *National Power Systems Conference (NPSC)*, Bombay, India, 2004, pp. 300-304.

[7] R. Mickiewicz, “Technical Overview and Benefits of the IEC 61850 Standard for Substation Automation,” presented at the *IEEE PES Power Systems Conference and Exposition*, Atlanta, USA, 2006, pp. 1-8.

[8] M. C. Janssen and A. Apostolov, “IEC 61850 Impact on Substation Design,” presented at the *IEEE/PES Transmission and Distribution Conference and Exposition*, Bogota, Colombia, 13-15 August 2008, pp. 3-8.

[9] I. Mesmaeker, P. Rietmann, K. P. Brand and P. Reinhardt, “Substation Automation based on IEC 61850,” presented at the *Regional Conference for National Committees of CIGRE*, Cairo, Egypt, 2005, pp. 1-10.

[10] P. K. Naik, N. K. Nair and V. Vyatkin, “Sympathetic Trip Protection Scenario in IEC 61850,” University of Auckland, Auckland, New Zealand. [Online]. Available: https://www.researchgate.net/publication/228437784_Sympathetic_Trip_Protection_Scenario_in_IEC_61850, Accessed on: March 17th 2017.

[11] J. Coronel and E. Carvalheira, “Testing the Protection System in IEC 61850 Communication Based Substations” presented at *IEEE ANDESCON*, Bolivia, 2014, pp. 1-4.

[12] D. Baigent, M. Adamiak and R. Mackiewicz, “IEC 61850 Communication Networks and Systems in Substations: An Overview of for Users,” [Online]. Available: http://www.gegridsolutions.com/multilin/journals/issues/spring09/iec61850.pdf, Accessed on: March 20th 2017.

[13] C. Kriger, S. Behardien, J. Retonda-Modiya, “A Detailed Analysis of the GOOSE Message Structure in an IEC 61850 Standard-Based Substation Automation System,” Centre for Substation Automation and Energy Management Systems, Cape Peninsula University of Technology, Bellville, Cape Town, South Africa. [Online]. Available: http://univagora.ro/jour/index.php/ijccc/article/viewFile/329/pdf_66, Accessed on: 23rd March 2017.

[14] “IEC 61850 Substation Overview and Smart Grids,” Moxa Inc., Germany. [Online]. Available: https://www.moxa.com/support/request_catalog_detail.aspx?id=1425, Accessed on: March 5th 2017.

[15] “Substation Technical Guidebook – IEC 61850 and IEEE 1588 in Smart Substations,” Moxa Inc., Germany, 2011. [Online]. Available: https://www.moxa.com/Solutions/Substation/eBook/index.htm, Accessed on: March 8th 2017.

[16] A. Hakala-Ranta, “Enhanced protection functionality with IEC 61850 and GOOSE,” Singapore, September 22-23, 2008, [Online]. Available: http://www02.abb.com/global/sgabb/sgabb005.nsf/bf177942f19f4a98c1257148003b7a0a/e81bb489e5ae0b68482574d70020bf42/$FILE/B5_G2_Enhanced+protection+functionality+with+IEC+61850+and+GOOSE.pdf, Accessed on: 2nd July 2017.

[17] L. Anderson, C. Brummer and F. Engler, “Substation Automation based on IEC 61850 with new process-close Technologies,” presented at the *IEEE Bologna Power Tech Conference Proceedings*, Bologna, Italy, 2003, pp. 1-6.

[18] I. Mesmaeker, C. Brunner and K. P. Brand, “How to use IEC61850 in Protection and Automation,” SC B5 Electra, Switzerland, vol. 1, 2005. [Online]. Available: https://library.e.abb.com/public/fed26a71538479c3c12570d50034fbe4/Rapport.pdf, Accessed on: March 3rd 2017.

[19] A. Apostlov, B. Vandiver, “IEC 61850 GOOSE Applications to Distribution Protection Schemes,” Omicron Electronics, USA. [Online]. Available: www.ee.co.za/wp- content/uploads/legacy/Energize%20.../06TT01_IEC.pdf, Accessed on: March 3rd 2017.

[20] R. A. Hedding, S. Ganessan, “Perspectives on Substation Design Based on Functionality of Modern Relays,” presented at the *61st Annual Conference for Protective Relay Engineers*, TX, USA, 2008, pp. 367 – 373.

[21] Schneider-electric.co.za, “CitectSCADA Supervisory Control and Data Acquisition (SCADA) software solution,” Schneider Electric, France, 2012. [Online]. Available: http://software.schneider-electric.com/products/citect-scada/, Accessed on: August 1st 2017.

[22] W. Bin, “Substation Automation Solution with IEC 61850,” ABB Singapore, 24th March 2010. [Online]. Available: http://www02.abb.com/global/seitp/seitp202.nsf/0/9276485464e7953cc125770300133d9a/$file/ABB+Substation+Automation+Solution.pdf, Accessed on: August 2nd 2017.

[23] Scheider-electric.co.za, “SCADA Systems,” Schneider Electric, France, March 2012. [Online]. Available: http://www.schneider-electric.com/solutions/ww/EN/med/20340568/application/pdf/1485_se-whitepaper-letter-scadaoverview-v005.pdf, Accessed on: August 3rd 2017.

[24] Inductiveautomation.com, “What is SCADA? – SCADA Explained,” Inductive Automation, USA, [Online]. Available: https://inductiveautomation.com/what-is-scada, Accessed on: August 5th 2017.

[25] Dpstele.com, “Important Considerations Scada Systems,” DPS Telecom, USA, [Online]. Available: http://www.dpstele.com/dnp3/tutorial-important-considerations-scada-systems.php, Accessed on: August 5th 2017.

[26] Controsys.hu, “CitectSCADA Technical Overview – An in-depth guide to our high-performance operations management solution,” Schneider Electric, France, 2012. [Online]. Available: http://www.controsys.hu/download/Citect/CitectSCADATechnical-Overview-v710.pdf, Accessed on: August 6th 2017.

[27] Scheider-electric.co.za, “MiCOM C264/C264C Bay Controller – Operation Guide,” Schneider Electric, France, 2012. [Online]. Available: www.schneider-electric.com/en/download/document/C264_EN_C80/, Accessed on: August 7th 2017.

[28] Scheider-electric.co.za, “MiCOM C264 Modular Substation Controller,” Schneider Electric, France, 2012. [Online]. Available: www.ase.cz/sites/default/files/upload/files/MiCOM/C264_brochure.pdf. Accessed on: August 7th 2017.

[29] Schneider-electric.co.za, “VAMP 259 Line Manager User Manual,” Schneider Electric, France, 2012. [Online]. Available: https://m.VAMP.fi/dmsdocument/17. Accessed on: August 8th 2017.

[30] Schneider-electric.co.za, “MiCOM P120/P121/P122/P123 Overcurrent Relays: Technical Guidebook,” Version 12, Schneider Electric, France. [Online]. Available: ms.schneider-electric.be/OP_MAIN/Micom/P12x_EN_Da6.pdf. Accessed on: August 28th 2017.

[31] Multitrode.com, “Benefits of a modern SCADA protocol: DNP3 vs Modbus,” Multitrode, November 2007. [Online]. Available: http://www.multitrode.com/assets/assets/benefits-of-a-modern-scada-protocol-.pdf. Accessed on: August 29th 2017.

[32] Library.e.abb.com, “ABB: Breaker failure protection,” 2002. [Online]. Available: https://library.e.abb.com/public/c1256d32004634bac1256e28005f594b/1MRK580139-BEN_en_REO_517_2.4_Breaker_failure_protection.pdf, Accessed on: November 5th 2017.

[33] H. Nikolajenko, A. Bajracharya, “IEC 61850 GOOSE Based Arc Flash Protection Scheme,” EECON, Melbourne, Australia, 22-23 November 2017. [Online]. Available: http://eecon.com.au/wp-content/uploads/2017/08/BAJRACHARYA-Aman-EECON-2017Abstract.pdf, Accessed on: November 6th 2017.

[34] ABB.com, “IEC 61850 relays: now with integrated arc flash protection,” 2017. [Online]. Available: http://www.abb.com/cawp/seitp202/17dcf2998d43c787c1257e1200355004.aspx, Accessed on: November 7th 2017.

[35] Schneider-electric.co.za, “What is Modbus and How does it work?” 2017. [Online]. Available: www.schneider-electric.co.za/en/faqs/FA168406/, Accessed on: September 15th 2017.

[36] Dpstele.com, “Understanding Modbus RS-232 and Modbus RS-485”, 2017. [Online]. Available: http://www.dpstele.com/modbus/rs485-rs232-protocol-data-flow.php, Accessed on: September 15th 2017.

[37] J. Rinaldi, “Modbus RTU,” 2016. [Online]. Available: www.rtaautomation.com/technologies/modbus-rtu/, Accessed on: September 16th 2017.

[38] Simplymodbus.ca, “Modbus TCP and Modbus RTU,” 2017. [Online]. Available: http://www.simplymodbus.ca/TCP.htm, Accessed on: September 17th 2017.

[39] Dnp.org, “Overview of the DNP3 Protocol,” 2011. [Online]. Available: https://www.dnp.org/pages/aboutdefault.aspx, Accessed on: September 20th 2017.

[40] Automationgroup.com.au, “What is DNP3?” 2017. [Online]. Available: http://automationgroup.com.au/what-is-dnp3/, Accessed on: September 22nd 2017.

[41] G. Lee, “Power System Automation,” 2016. [Online]. Available: https://www.slideshare.net/guiderlee/power-system-automation-57314758, Accessed on: September 23rd 2017

[42] Dpstele.com, “8 Important Considerations in DNP3 SCADA System,” 2017. [Online]. Available: http://www.dpstele.com/dnp3/tutorial-important-considerations-scada-systems.php, Accessed on: September 23rd 2017.

[43] Dnp.org, “A DNP3 Protocol Primer,” DNP Users Group, Revision A, 20th March 2005. [Online]. Available: https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf, Accessed on: September 23rd 2017.

[44] Scadahacker.com, “Modbus and DNP3 Communication Protocols,” Raleigh, North Carolina. [Online]. Available: https://scadahacker.com/library/Documents/ICS_Protocols/Triangle%20Microworks%20-%20Modbus-DNP3%20Comparison.pdf, Accessed on: September 24th 2017.

[45] Ioselect.com, “Advantages of the DNP3 Communications Protocol,” USA, 2015. [Online]. Available: http://www.ioselect.com/application%20notes/remote-telemetry/ioselect-dnp3-communications-protocol.pdf Accessed on: September 25th 2017.

[46] S. Edvard, “Advantages of IEC 61850,” 2010. [Online]. Available: http://electrical-engineering-portal.com/advantages-of-iec-61850, Accessed on: September 25th 2017.

[47] Abb.com, “IEC 61850 – The Basic Approach,” 2017. [Online]. Available: http://www.abb.com/cawp/seitp202/c1256a8c00499292c1256d41003803b4.aspx, Accessed on: 9th November 2017.

[48] W. Huang, “A Practical Guide of Troubleshooting IEC 61850 GOOSE Communication,” ABB Inc. Lake Mary, USA, 2016. [Online]. Available: http://prorelay.tamu.edu/wp-content/uploads/sites/3/2017/04/A-Pratical-Guide-of-Troubleshooting-IEC-61850-GOOSE-communicaiton-Wei-Huang.pdf, Accessed on: 7th November 2017.

[49] Y. Pradeep, P. Seshuraju, S. A. Khaparde, Vinoo S. Warrier, Sushil Cherian, "CIM and IEC 61850 integration issues: Application to power systems", *Power & Energy Society General Meeting 2009. PES '09. IEEE*, pp. 1-6, 2009, ISSN 1944-9925.

[50] C. M. Adrah, S. Bjørnstad, Ø. Kure, "Fusion networking technology for IEC 61850 inter substation communication", *Smart Grid and Smart Cities (ICSGSC) 2017 IEEE International Conference on*, pp. 152-156, 2017.

[51] V. Dehalwar, A. Kalam, M. Lal Kolhe, A. Zayegh, "Review of IEEE 802.22 and IEC 61850 for real-time communication in Smart Grid", *Computing and Network Communications (CoCoNet) 2015 International Conference on*, pp. 571-575, 2015.

[52] C. Brunner, “IEC 61850 for power system communication,” *Transmission and Distribution Conference and Exposition, 2008 IEEE/PES,* pp. 367 – 373, 2008.