Cape Peninsula University of Technology

IEC 61850 Based Substations Methodologies Evaluation and Advancement for Improved Transformer Protection and Power System Security

By

PHUMEZILE KWANDA MAKAULA
STUDENT ID: 215180054

Dissertation submitted in fulfillment of the requirements for the degree.

Master of Engineering in Energy: Electrical Engineering

In the Cape Peninsula University of Technology's Faculty of Engineering

Supervisor: Prof Atanda Raji
Co-Supervisor: Dr Mkhululi Mnguni

Bellville

15 September 2025

CPUT copyright information

DECLARATION

I, Phumezile Kwanda Makaula, declare that the information in this report is all of my original, unaided work, it has never before been submitted for academic review to earn a degree. The views expressed here are also solely mine and do not necessarily reflect those of CPUT.

PKMak

Signed

17-02-2026

Date

ABSTRACT

Electricity is an essential driver of socio-economic development. However, electrical networks often experience faults resulting in the interruption of the power supply and exposure of the plant to damage. Consequently, protection schemes are meant to clear faults fast and be selective, even under challenging conditions. Some of the issues being faced by the utility companies include copper theft, vandalism of electrical networks, ageing networks and the integration of various types of equipment. IEC 61850 has transformed the mode of designing and running modern substations through the use of high-speed digital communication in place of wired signalling. Communication modes involving GOOSE Messaging, Sampled Values and fibre optic technology allow protection systems to communicate at very high speeds, thus enabling them to exchange information. It is under this premise that this study sought to propose a transformer bay protection system using IEC 61850, which utilises a peer-to-peer GOOSE communication mode to offer quick protection against faults. The Digital architecture was designed using the SEL acSELerator QuickSet 5030 and validated through the hardware-in-loop simulations using the OMICRON Test Universe. The results show that within the digital architecture, faults were cleared 60% faster than with traditional approaches while providing improved selectivity, operational security, and protection during outages. It also verifies that the entire process of transport reliability using GOOSE messages was reliable under faulty operating conditions. These findings demonstrate that digital substations based on the IEC 61850 significantly improve protection performance, interoperability and reliability.

Keywords - IEC 61850, IEDs, interoperability, GOOSE messaging, protection algorithms, Digital substation, Protection scheme. Substation automation and Control.

ACKNOWLEDGEMENTS

First and foremost, I thank the Almighty God for His guidance and grace throughout my academic journey. I extend heartfelt appreciation to Prof. A. Raji and Dr. M. Mnguni for their invaluable technical guidance and encouragement. My deepest gratitude goes to my family and friends for their unwavering support. A special thank you to my mother, Mrs. M. N. Ngcongolo-Makaula, for her enduring love and belief in my goals. '**Singabantu-You can win'**

DEDICATIONS

This dissertation is dedicated to my mother, M. N. Ngcongolo-Makaula, whose selfless support and tireless encouragement have been the backbone of my academic journey. Thank you for always believing in me.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ABBREVIATIONS

A - Ampere
AC - Alternating current
ACSI - Abstract Communication Service Interface
CSI - Current source inverter
CERTS - Consortium for Electric Reliability Technology Solutions
CID - Configured IED Description
Cu - Copper
DC - Direct current
DCS - Distributed Control Systems

ESS - Energy storage system
GOOSE - Generic Object-Oriented Substation Event
GHI - Global horizontal irradiation
ICD - IED Capability Description
IEC - International Electrotechnical Commission
IED - Intelligent Electronic Device
IP- Internet Protocol
KCL - Kirchhoff current law
LV - low voltage
MMS - Manufacturing Message Specification
NCIT - Non-Conventional Instrument Transformer
POI - point of interconnection
RTU - Remote Terminal Unit
SANS - South African national standard
SAS -Substation Automation Systems
SCD -Substation Configuration Description
SCL- Substation Configuration Language
SSD - System Specification Description
SV - Sampled Values
TCP - Transmission Control Protocol
UPS - Uninterrupted power supply
VSI - Voltage source inverter

NOMENCLATURE

Symbol	Definition
Current Variables	
I_{diff}	Differential current - the algebraic difference between currents entering and leaving the protected zone
I_{op}	Operating current - current magnitude used to determine relay operation
I_{rt}	Restraint current - stabilising current used to prevent maloperation during through-faults
I_1	Primary winding current (high-voltage side)
I_2	Secondary winding current (low-voltage side)
I_d	Differential current (abbreviated form): I_d = $\|i_1 - i_2\|$
I_r	Restraint current (abbreviated form): I_r = ($\|i_1 + i_2\|$) / 2
I_{pu}	Per-unit pickup current - minimum differential current threshold for relay operation
I_{dmin}	Minimum differential pickup threshold - lower bound of the operating characteristic
I_{in}	Transformer input current (entering the protected zone)
I_{out}	Transformer output current (leaving the protected zone)
I_s	Secondary current referred to primary
I_p	Primary measured current
Relay Characteristic Parameters	

K	Design constant (k = 1 for the SEL-487E relay)
SLP	Differential element characteristic slope - defines the ratio of operating to restraint current at the relay characteristic boundary
$SLP1$	Slope 1 - lower slope of the dual-slope differential characteristic (low-current region)
$SLP2$	Slope 2 - upper slope of the dual-slope differential characteristic (high-current region)
K_2	Second harmonic restraint coefficient - applied to block tripping during transformer inrush
K_4	Fourth harmonic restraint coefficient - applied for additional inrush restraint
K_{bias}	Bias factor applied to the restraint current calculation
Voltage and Turns Ratio	
V_1	Primary winding voltage
V_2	Secondary winding voltage
N_1	Number of turns on the primary winding
N_2	Number of turns on the secondary winding
Ratio Correction Factors	
R_{fhv}	Ratio correction factor for the high-voltage (HV) side compensates for CT ratio mismatch and tap changer position
R_{flv}	Ratio correction factor for the low-voltage (LV) side
System Quantities	
f_0	Nominal system frequency (50 Hz in South Africa)
T	Time (milliseconds, ms)
Z_1	Positive-sequence impedance
Z_2	Negative-sequence impedance
Z_0	Zero-sequence impedance
Mathematical Notation	
ΣI	The summation of all currents entering and leaving the protected zone equals zero under healthy conditions (Kirchhoff's Current Law)
$\|x\|$	Absolute value (magnitude) of quantity x
$\sum$	Summation operator

Definitions

Distributor: an entity responsible for distributing electricity through distribution network.

Circuit breaker (CB): a switching device that carries currents under normal conditions and breaks currents under faulty circuit conditions.

Distribution System: a utility network with a nominal voltage of up to 132 kV and below.

Disconnector: a switching device that can open or close a circuit and provides visible isolation
Switchgear (control gear): a broad term for switching devices and the related control, protection, measuring, and regulating equipment.
DNP3: a communications protocol utilised to control electricity on the transmission network, while DNP is used in the distribution network.
Earthing switch: a tool for earthing circuit components.
High voltage (HV): nominal voltage levels between 33kV to 400kV.
Loss-of-grid protection: A Protection relay intended to monitor a loss of utility-grid connection and issue tripping signals to the embedded generators, to prevent the island from being energised.
Medium voltage: nominal voltage levels between 1000V and 33kV.
Point of supply (POS): The physical point determined by the service provider at which electricity is supplied to customers.
Synch-check: checks whether the phase angle, frequency and voltage magnitude are within electrically permissible bounds.
System Operator (SO): the person in charge of the Control Centre of the System.
Thermal Generating Unit: uses heat to generate electricity.
Transmission System (TS): with nominal voltages greater than 132 kV.

CHAPTER ONE

1. INTRODUCTION

1.1. Background of the study

Electrical power supply utilities and distributors serve as the backbone of modern socio-economic development, underpinning industrial growth, public welfare, and technological advancement in both established and emerging economies. In recent years, the intensification of electricity consumption has heightened the imperative for energy security, system reliability, and power quality, all delivered at sustainable and economically viable costs. These objectives must be pursued alongside a commitment to maintaining the safety of networks and operational personnel, as safety incidents can trigger cascading failures with widespread societal repercussions. The increasing integration of renewable energy sources and distributed generation further amplifies the complexity of grid operations, necessitating highly coordinated and adaptive protection relaying systems. The transition towards smart, automated substations is therefore essential to facilitate seamless grid management, uphold regulatory standards, and minimise equipment damage, while also ensuring grid resilience and robust fault isolation. In this evolving context, utilities are compelled to modernise their infrastructure and operational strategies, guided by the pursuit of excellence in supply reliability and sustainability.

Within the operational fabric of electrical networks, the power transformer plays a central role as a node for stepping voltage levels up or down to meet system requirements. Ensuring reliable protection, automatic condition monitoring, and seamless control of power transformers has become indispensable in substations, particularly as grid configurations and demand profiles become more dynamic. The deployment of Substation Automation Systems (SAS), driven by the integration of Intelligent Electronic Devices (IEDs), has revolutionised the traditional paradigms of monitoring and control. IEDs, when interconnected through high-speed digital communication networks, enable the continuous assessment of equipment health and facilitate instantaneous fault detection and isolation. These capabilities are pivotal in mitigating operational risks and downtime, particularly in contexts where legacy devices, such as electromechanical relays, are reaching the end of their operational life cycles and are no longer supported by manufacturers. The imperative to replace obsolete equipment with advanced digital solutions is thus motivated by both technical and economic considerations.

The limitations of traditional relay technologies are increasingly apparent, as their mechanical and static components are susceptible to wear, corrosion, and operational unreliability, particularly under harsh environmental conditions. The reliance on extensive copper wiring to link relay panels with field equipment in conventional substations not only increases installation and maintenance costs but also introduces additional points of failure and hinders scalability. Digital IEDs, by contrast, consolidate multiple protection, control, and monitoring functions into compact, microprocessor-based platforms that require minimal wiring and offer significant cost and time efficiencies in engineering, installation, and commissioning. The migration towards digital protection schemes enables utilities to harness powerful diagnostic tools such as self-testing, event recording, and automated fault location, thereby facilitating predictive maintenance and reducing system outages. This progression is not merely incremental but constitutes a paradigm shift towards data-driven and adaptive asset management.

A defining characteristic of modern substation automation is its foundation on international standards such as IEC 61850, which prescribes open communication protocols for multi-vendor interoperability, seamless data integration, and cyber-secure operation (Aftab et al., 2020). SAS architectures equipped with IEDs enable granular remote access to operational data via Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS), supporting centralised decision-making and grid optimisation. The fulfilment of IEC 61850 requirements is vital in addressing cybersecurity threats, as substations become targets for increasingly sophisticated cyber-physical attacks. The embedding of security features, including encryption and network segmentation, within SAS, safeguards critical infrastructure and supports compliance with emerging cybersecurity standards. Ultimately, the transition to advanced automation, anchored by IEDs and digital communication, not only enhances operational resilience but also positions utilities to adapt to future technological, regulatory, and market disruptions.

1.2. Research problem statement

The current reliance on electromechanical, static, and first-generation digital relays presents significant operational and reliability challenges within contemporary substation environments. While these legacy devices historically provided robust protection to costly assets and enhanced network safety, their progressive ageing has precipitated an escalation in malfunction risks and system vulnerabilities. Many installed relays have reached or

exceeded their intended lifespan, making them susceptible to failures triggered by physical degradation and exposure to fluctuating environmental conditions such as temperature extremes and humidity. As these devices age, their performance is further compromised by a lack of vendor support, which complicates maintenance and increases downtime during faults. The resultant operational risks include spurious or failed tripping actions either disconnecting healthy network sections or failing to isolate faults, which can lead to extended outages, increased equipment damage, and jeopardised personnel safety.

A fundamental shortcoming of these conventional relays is their inability to conform to modern standards such as IEC 61850, which demands features such as robust and secure communication, interoperability across different vendors, minimisation of copper wiring, and high reliability. In the context of rising grid complexity, the static nature of traditional protection schemes also impedes the integration of digital technologies required for monitoring and advanced fault diagnostics. The absence of automated data exchange and sophisticated analytics undermines both asset management strategies and response agility to grid disturbances. As global utility operators embrace digital transformation, the gap between legacy systems and evolving operational requirements continues to widen, calling for urgent upgrades to digital substation automation and protection infrastructure. The research problem thus centres on the pressing need to replace or retrofit ageing protection devices with intelligent electronic devices (IEDs) and to integrate substation automation systems (SAS) that are fully aligned with international standards and contemporary operational best practices.

Sub-Problem 1

The existing substation infrastructure is characterised by three 50 MVA transformers, with one transformer now exceeding four decades of service, surpassing industry recommendations for operational longevity and increasing the risk of catastrophic failure. This aged transformer is not only compromised by recurrent issues such as oil leaks and internal faults but also by a scarcity of specialised maintenance personnel with the expertise to manage such legacy equipment. Forecasts for the supply region indicate that peak demand will soon reach approximately 100 MVA, which is beyond the capacity of the remaining two functional transformers. The continued reliance on outdated transformation infrastructure poses severe risks to future system adequacy and resilience, especially as the region anticipates sustained economic and population growth.

Technical incompatibilities further exacerbate operational challenges; specifically, the existing transformer employs a YNyn6 vector group, whereas adjacent main substations utilise the Dyn11 configuration. This discrepancy hinders interconnectivity between substations, effectively constraining operational flexibility and complicating emergency load-shifting procedures. To address these barriers, strategic replacement of end-of-life transformers with Dyn11 units is imperative, facilitating seamless integration and dynamic load management across the network. Furthermore, the upgrade must be complemented by the deployment of advanced protection and automation systems, leveraging SAS and IEDs to ensure continuous monitoring, rapid fault detection, and adaptive control. This approach will not only safeguard asset integrity and support future load expansion but also align the substation with best practices for reliability, interoperability, and power system security. In this context, the research recognises the multidimensional nature of the problem encompassing technical, operational, and human resource constraints and advocates for an integrated solution grounded in contemporary automation technologies and standards.

Figure 1.1: Currently Installed Protection

Figure 1.1 displays the transformer's protection and control panel with vintage electromechanical and static relay enclosures. The matrix arranges protective devices for overcurrent, differential, and earth fault protection. The transformer's schematic design displays current flow, relay actuation points, and main and backup protection. Substation automation systems cannot deliver advanced automation, remote diagnostics, and efficient data analytics. Thus, the panel prioritises substation digital transformation to address operational and cybersecurity challenges. Intelligent electronic devices (IEDs) in IEC 61850-compliant substation automation systems enhance protection, visibility, and maintenance efficiency.

Sub-problem 2

The increasing reliance on digital connectivity in substation automation renders critical infrastructure increasingly susceptible to cyber-physical attacks that previous systems were not designed to manage. Contemporary cybersecurity standards such as IEC 62351 and NERC CIP mandate network segmentation, access control, and encrypted communication, which are absent in electromechanical relay-based substations. In the absence of these restrictions, significant security threats to power systems arise, including illegal access to IEDs, GOOSE message spoofing, and denial-of-service assaults on protection communications. This sub-problem investigates the divergence between the cybersecurity capabilities of legacy protection systems and the security demands of IEC 61850-compliant digital substations. It advocates for simulation-based modelling of cybersecurity controls as a technique for evaluating and improving the security efficacy of the proposed protective architecture.

1.3. Significance of the problem

Legacy substation protection and control equipment predates the IEC 61850 standard and does not meet modern digital substation interoperability, adaptability, and cybersecurity standards. IEC 61850's ten-part communication architecture facilitates system-wide standardisation and integration of intelligent electronic devices (IEDs) from various providers (Aftab et al., 2020). Expanding or modernising substations makes it difficult to integrate ageing multi-vendor relays into a modern automation system. Low interoperability, complicated wiring, and no advanced diagnostic and monitoring functions are limitations (Silva et al., 2021). IEC 61850-compliant IEDs provide improved protection, control, metering, and automation at substation, bay, and process levels, enabling substation digital transformation.

Many benefits of IEC 61850-based IEDs and substation automation technology overcome legacy system limits. These benefits include:

- **Reduced Time:** Standardising design, draughting, installation, and commissioning processes accelerates project delivery.
- **Cost Reduction:** Digital communication and multiplexing cut labour, cable trenching, and control room space.
- **Enhanced Interoperability:** Integration and configuration of multi-vendor IEDs facilitate maintenance and extension.
- **Improved Reliability and Security:** Automation lowers manual intervention, human error, and monitoring, ensuring power network stability and security.
- **Operational Flexibility:** Sampled Values (SV), GOOSE messaging, and fibre optic connections enhance security, control, and data analytics.

1.4. Aim of the research

This research project aims to evaluate, develop, and validate IEC 61850–based substation methodologies that integrate intelligent transformer protection, automation, monitoring, and supervisory control to enhance power system security, reliability, and maintainability. The study focuses on assessing how advanced protection algorithms, digital communication, and substation automation collectively improve fault response, asset management, and secure operation of modern power networks.

1.5. Contribution of the research

The main contributions of this research are as follows:

- Offered a detailed analysis of IEC68150 and substation automation.
- Multi-vendor integration and development on condition monitoring fundamentals.
- Simplified engineering and implementation of configuration based on IEC 61850 standard-based communication protocols (GOOSE messaging).
- IED configuration for communication through an Ethernet switch and an IP commodity for data exchange.

- Configuration algorithm development for arc-flash protection and breaker failure incorporation.
- Development of current supervision techniques specifically for the protection of the transformers, like CT supervision, loss of current detection and abnormal current condition monitoring.
- Reduction of capital costs through substitution of conventional hard-wired protection and control schemes like tripping, interlocking and status indication wiring with IEC 61850 GOOSE technology-based virtual signalling, resulting in reduced cabling, panel hardware, and installation effort
- Optimised power system operational efficiency through faster fault clearance, reduction of protection mal-operations and faster system restoration with the implementation of IEC 61850 protection and automation schemes.
- Achieve remote monitoring and control (Remote switching of substation apparatus and supervisory control of relays).
- Enhanced power transformer protection, reliability and security.

1.6. Objectives of the research.

This research project's primary objective is to develop, implement and empirically evaluate techniques and algorithms for an IEC 61850-based protection and automation scheme that reduces fault clearing time and improves interoperability for transformer bays and outgoing feeders. The objectives are further expanded on below.

- Review the existing protection scheme
- Model proposed protection scheme and configure GOOSE datasets for trip, interlock and supervision events.
- Conduct a literature review on the IEC 61850 application for control, monitoring, protection and automation of the power system and the IEC-61850 standard-based GOOSE protocols.
- Demonstrate the effectiveness of protection function blocks, including Arc protection and breaker failure.
- Set up hardware SEL devices via an Ethernet network for communication.
- Use Test universe to simulate the entire model to test the effective performance of the proposed Protection techniques and analyse the associated benefits.

- Demonstrate breaker failure and arc-flash coordination using logical nodes with GOOSE signalling.
- Quantify the improvements versus baseline: Mis-trip rate, stability, wiring reduction and fault clearing time, power quality and power system management and enhanced power security.

1.7. Hypothesis

It was hypothesised that an adequate, well-coordinated and intelligent protection scheme based on IEC 61850 relative to legacy protection will improve the stability, reliability and power security of the network. The IEC 61850 implementation will reduce the cost in relation to commissioning and maintenance. IEC 61850-based protection systems provide faster fault isolation, improved interoperability, and better asset management compared to traditional relay systems.

.

1.8. Limitations of the research

It was important to specify the scope of this study because the topic of substation automation, protection and monitoring is enormous. The tasks that fall within the purview of this study are discussed first, followed by those that do not.

1.8.1. Within the limit

The research project is limited to the IEC 61850-based substation protection and control, as well as the power transformer.

Tasks within the limitations of the project:

- Remote Terminal Unit (RTU) and protection IEDs hardware integration.
- GOOSE protection messages testing.
- Protective relay configuration design.
- Protection relay wiring
- Programming protection settings for protection relays.
- Relay testing

- IEC 61850 client/server communication testing
- Control of network communications within the Substation Automation Systems.

1.8.2. Out of Scope

This research is a simulation-based examination of transformer bay protection utilising IEC 61850 and does not represent a practical application. All protection logic was developed using the SEL acSELerator QuickSet 5030 software and evaluated through hardware-in-the-loop (HIL) testing on the OMICRON CMC 356 and Test Universe platform. The HIL environment precisely emulates IED behaviour and substation communication; nevertheless, the outcomes must be interpreted as components of a controlled simulation. The validation of field deployment in an operating substation, which includes exposure to electromagnetic interference, multi-vendor legacy equipment, and actual network traffic, is acknowledged as a priority for future initiatives (Section 7.5.1).

Activities fall outside the limitations of the research project.

- Civil works of Transformer installation.
- Design and installation techniques of VT and CT.
- High Voltage (HV) yard designing, installation and testing.
- Simulate the master station.
- Simulate a monitor to detect data traffic.

1.9. Research questions

The following were the research questions for the project.

- How feasible is the IEC 61850 algorithm application in substation protection, automation and control enhancement?
- Can the developed application algorithm help improve the power system efficiency and modernise substation monitoring capabilities?
- Can IEC 61850-based GOOSE messaging reduce fault-clearing times compared to traditional systems?
- How can IEDs from multiple vendors be configured to operate in a unified protection scheme?

- What are the practical challenges in deploying IEC 61850 within an existing substation?

1.10. Research methodology

The research uses a hybrid methodology combining literature review, simulation, and practical implementation. A simulation testbed was created using SEL and ABB IEDs configured through acSELerator Quickset and IET600. The communication network is built using managed Ethernet switches, with GOOSE messaging configured for critical protection functions. Test Universe is used to validate the protection response.

1.10.1. Research procedure

The research procedure comprises the following significant steps:

- Collect data and review the literature.
- Review of IEC 61850 standard and transformer protection principles.
- Algorithm development.
- Configuration of protection functions using IED tools.
- Development of software simulation.
- Testing and simulation using Test Universe.
- Analysis and evaluation of system performance.
- Documentation of research findings and analysis of the results.
- Conclude on the most efficient and sustainable control strategies.

1.10.2. Literature review and data collection:

A thorough search and analysis of the published research on the interfaces of substation automation, protection and monitoring techniques requires the acquisition of expertise from several different fields. This type of research requires a solid understanding of the fundamental concepts underlying control theory, power system theory, electric power generation, power electronics, and system modelling and simulation. The theoretical framework will also reveal knowledge gaps and provide a technique pool from which new and

improved working methods can be adopted. As a result, the research must include an analysis among those relevant disciplines to acquire relevant expertise, as well as an evaluation of the current solutions to the identified problem by evaluating relevant and important existing findings. Only then can the tasks destined for the topical work be designed, analysed, and the results assessed.

1.10.3. Software development:

Relay configuration models for the development of IEC 61850-based substation and enhanced transformer protection are built, modelled, and implemented using preliminary analysis of prior work and the pertinent data gathered from existing protection equipment on site. Relay configuration includes primary plant information such as the type of CT, VT, circuit breaker and busbar arrangement. The configuration takes into consideration physical apparatus modelling as well as models and tools for portraying every part of the electrical power grid. Thus, widely recognised and accepted mathematical models for diverse protection techniques may be modelled in the simulation environment and their accuracy assessed in comparison to results from earlier studies.

The method is based on the stages of software development, which comprise the following.

- Analysis of theoretical expected outcomes and software objectives
- Setting up a strategy or developing a solution that is based on the software.
- Testing, evaluation, and implementation of the software-based solution

1.10.4. Algorithm development:

The Algorithm Development approach is used to generate a mathematical procedure for developing automation and protection techniques that are in accordance with the research objectives. Additional system parameters for the substation components are established.

1.10.5. System simulation and performance analysis:

The efficacy of the developed automation and control approach enables the adequate performance of the power system, ensuring reliability and power security. Each simulation

example is accompanied by a discussion of the simulation results, and the dissertation concludes with a summary of the important findings.

1.11. Dissertation layout

The study's various chapter titles and contents are structured to individually and collectively address the issue that serves as the foundation for the work discussed in this dissertation as adequately as possible, thereby fully achieving the aim and all related research objectives. The dissertation consists of six chapters, each of which emphasises the key aspects outlined as follows.

Chapter 1: This section is about a general introduction to the research topic by presenting the background of the research topic, the aim of the research, objectives and hypothesis of the study. Additionally, a synopsis of the study's research design and methodology is outlined, along with the findings and limitations.

Chapter 2: Literature review - This chapter reviews the existing literature on IEC 61850, transformer protection, substation automation, and related technologies.

Chapter 3: Methodology - This chapter describes the research methodology, design process, and tools used to implement and test the IEC 61850-based protection scheme.

Chapter 4: System Design and Implementation - Details of the substation layout, IED configuration, and GOOSE messaging setup are provided in this chapter.

Chapter 5: Findings - This chapter presents the simulation results and discusses the performance of the protection scheme under different fault scenarios.

Chapter 6: Conclusion and future work - The final chapter summarises the findings, outlines the contribution to the field, and suggests future research directions.

CHAPTER TWO

2. LITERATURE REVIEW

A review of literature based on IEC 61850 communications protocol, algorithm and topology is represented in this section. This section includes a critical analysis of research studies within the scope of this study, such as digital substation communication redundancy using seamless topologies (Process bus and NCIT) and protection using reverse busbar blocking (Reverse block overcurrent).

2.1. Introduction

Modern power networks are getting more complicated and digital, so they need more advanced automation solutions for substations to be safe, reliable, and efficient. This chapter takes a close look at transformer safety studies, guidelines, and practices, as well as the IEC 61850 communication protocol and the development of substation automation systems. The review looks at how technology based on IEC 61850 has made substation automation more secure, resilient, and able to work with other systems. Intelligent electronic devices (IEDs), digital communication protocols, and networked safety schemes have made operations more efficient, but they have also brought about new technical and security problems, especially as substations turn into hubs in cyber-physical energy systems.

This is how the chapter is organised: The review first traces the evolution and functional requirements of Substation Automation Systems (SAS) with a scientific and historical look at the IEC 61850 standard, then it examines transformer protection from legacy methods to percentage-differential with harmonic restraint capabilities. Then it covers its basic logical design, modelling structures, and how devices can work together and how the system is set up. Then it clarifies the need to upgrade older substations, improvements in transformer protection like differential protection algorithms and adaptable methods, and the security and dependability problems that come with digitalisation. Next is the theory and practical aspects of backup protection, SCL file configuration management, and advanced protection methods. This part uses standards and peer-reviewed studies from the past five years to put current research in the context of world trends and point out knowledge gaps. This part brings together all of this literature to give the study methods and data analysis a strong theoretical and practical foundation. It surveys communication protocols, highlighting IEC 61850 and data

models, fast messaging (GOOSE/SV), and SCL-driven engineering together with network redundancy (PRP/HSR) and time synchronisation (SNTP/PTP). The chapter closes with cybersecurity practices and synthesises gaps to motivate the research.

2.2. Overview of Substation Automation

2.2.1. Historical Development of Substation Automation Systems (SAS)

Substation automation systems are the result of many important steps forward in technology. These new ideas have made electricity networks much more reliable and efficient. Mnukwa and Saha (2020) say that early substations had manual controls and regional mechanical switches, which made them less quick and more likely for people to make mistakes. SCADA systems, which came out in the late 20th century, let people control and watch simple things from afar. They didn't have the smooth blending that modern energy networks are supposed to have (Aftab et al., 2020). Recently, there has been more use of smart electronic devices (IEDs) that use digital transmission methods. This made operating freedom, data analysis, and managing faults better (Silva et al., 2021). As an example of this progress, Kompalli et al. (2023) say that IEC 61850-based systems have changed how substations can communicate, model data, and connect with each other. Even with these improvements, there is a gap in how to combine old tools with safe digital substations. This drives study and new ideas.

2.2.2. Functional Requirements of Modern SAS

For safe, reliable, and effective power transfer, modern substation automation systems need to be able to do a lot of different things. According to Cacereño et al. (2024), these systems should be able to collect data, offer adaptable security, find faults automatically, and allow secure remote control. According to Cacereño et al. (2024), multi-objectivisation in SAS design makes maintenance planning better, which ensures reliability and cost-effectiveness. Strong time synchronisation and fast peer-to-peer transfer are needed when quick security tripping is important for system stability (Silva et al., 2021). Putting IEDs from different companies into the same operating system needs strict standards and rules to make sure they can all work together (Silva et al., 2021). Recent cybersecurity standards say that SAS needs to make sure that its technology is up to date and that it is safe from new types of threats (Krause et al., 2021). Interoperability, speed, and security must all be balanced for SAS operation to be reliable.

2.2.3. Role of Communication Protocols in Automation

Devices and control centres may communicate practical and safety data via communication protocols. They underpin substation automation digitally. According to Aftab et al. (2020) and Silva et al. (2021), IEC 61850 is the standard protocol. GOOSE with Sampled Measured Values provides high-throughput and deterministic messaging. According to Kompalli et al. (2023), these protocols enable peer-to-peer and device-to-control centre communication. This makes automated protection and control processes more reliable and faster. The digitisation of the substation network has enabled sophisticated features like condition monitoring and predictive diagnoses, which need seamless and consistent data interchange, according to Pakulska and Poniatowska-Jaksch (2022). However, these protocols allow hackers to enter in novel ways. SAS systems must have encrypted communication and role-based access management (Krause et al., 2021; Gunduz and Das, 2020). The study agrees that communication techniques affect substation automation's performance and online safety.

2.2.4. Transition from Conventional to Digital Substations

It is important for operations and research to move quickly from standard substations with hard-wired logic, electrical switches, and human interaction to digital substations (Cacereño et al., 2024). IEDs that are built into digital substations that are compliant with IEC 61850 make engineering, wiring, scaling, and remote operation easier (Silva et al., 2021). Standardised digital connection makes it faster to find and isolate problems and gives predictive data for asset management (Vo et al., 2023). Pakulska and Poniatowska-Jaksch (2022) say that going digital makes setup, version control, and risk evaluation more difficult. Since old systems might not work with new digital parts, the move needs technical know-how and strategy change management (Cacereño et al., 2024). There are big improvements in system performance and stability in reliability studies. To switch to digital substations, utilities require a strong control framework, ongoing staff training, and a flexible cybersecurity stance. All future upgrades to substations must strike a balance between new ideas and lowering risks.

2.3. Transformer Protection Schemes

2.3.1. Overview of Power Transformer Faults

Power transformers are crucial to electrical substations and may fail in different ways. Internal or exterior faults might be differential, thermal, or earth faults. Internal transformer winding defects include phase-to-phase, phase-to-earth, and inter-turn. External faults include

overloads and through-faults. Differential faults, which commonly occur in the winding zone, may cause massive transformer damage if not detected (Li et al., 2021). Modern substations need reliable fault diagnosis to minimise operational interruptions and asset deterioration. Late identification may cause thermal stress, oil breakdown, and reduced transformer lifespans (Cacereño et al., 2024). Traditional transformer problems are well documented, but digital substations have introduced additional vulnerabilities, particularly in communication and integration (Kompalli et al., 2023). Therefore, knowing fault types is crucial for developing new protection measures that fit with present substation designs.

2.3.2. Conventional Protection Techniques

Overcurrent, differential, and gas-detection methods, such as the Buchholz switch, have been used to protect transformers. Overcurrent prevention is widely used since it is easy to use and works well against serious external faults or long-term overloads. However, it is not selective enough for isolating internal faults (Mnukwa & Saha, 2020). Based on Kirchhoff's Current Law, differential protection checks the current levels on both sides of the transformer and trips the circuit breaker if an inside problem is found (Li et al., 2021). This principle is mathematically expressed as:

$$\vec{I}_1 + \vec{I}_2 + \vec{I}_3 + \cdots + \vec{I}_n = 0A \tag{2.1}$$

Where the sum of currents entering and leaving the protected zone equals zero under healthy conditions. The relay calculates differential current (Id) and restraint current (Ir), with:

$$I_d = |i_1 - i_2| \tag{2.2}$$

$$I_r = \frac{|i_1 + i_2|}{2} \tag{2.3}$$

Protection operates when Id>Ir. The Buchholz relay, installed in the oil conservator pipe, detects gas accumulation resulting from internal arcing or insulation breakdown, providing early warning or direct tripping signals (Cacereño et al., 2024).

These conventional approaches, though robust, are limited by their response times and selectivity, especially in distinguishing inrush currents from genuine internal faults.

2.3.3. Limitations of Traditional Transformer Protection Systems

Despite decades of usage, tried-and-true procedures have issues. Overcurrent safety devices may be sluggish and unable to distinguish between transformer failures inside and outside, causing the transformer to be separated too late. Differential protection is sensitive, although CT overload, magnetising inrush, and tap changer might create problems. New studies reveal that harmonic restraint techniques like 2nd and 5th harmonic detection can distinguish inrushes, but fault patterns that aren't common for current networks may hurt them (Silva et al., 2021).

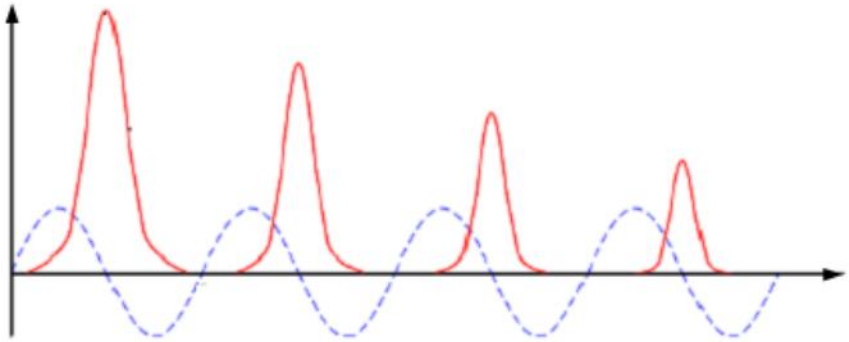


Figure 2.1 : Harmonics (Li et al., 2021)

Even harmonic restraint

Using even harmonics, specifically the second and fourth, within a restraint scheme enhances security against inrush currents characterised by minimal second harmonic current. The operational equation pertaining to the 2nd and 4th harmonic restraint differential elements is as follows.

$$I_{O_P} > SLP \times I_{RT} + K_2 I_2 + K_4 I_4 \quad (2.4)$$

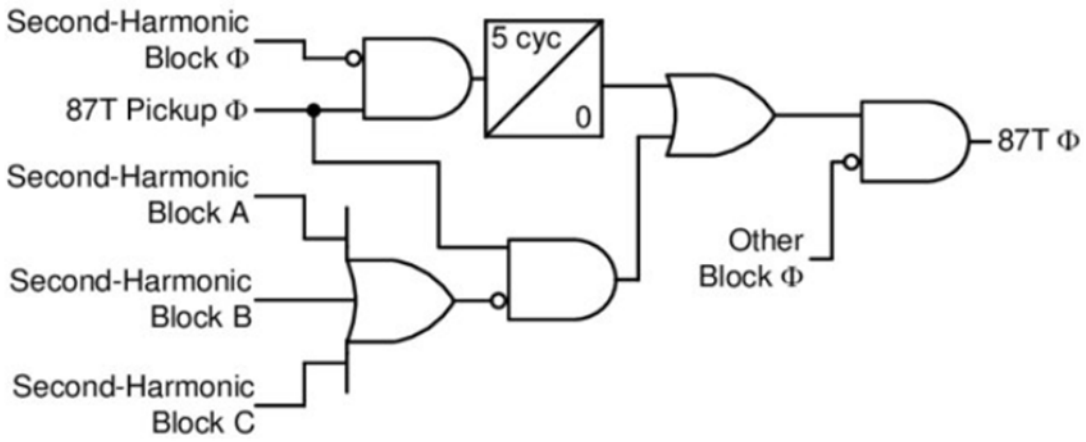


Figure 2.2 Harmonic logic (SEL, 2021)

Buchholz switches need to be maintained often and may not be ideal for remote or unmanned substations since they can't handle all types of faults. Coordination in digital substations is hard since latency and communication issues, so better methods are needed.

2.3.4. Importance of Accurate and Timely Fault Detection

Smart grids and green energy consumption need fast fault detection to minimise transformer failure, power outages, and lengthy system recovery periods (Pakulska & Poniatowska-Jaksch, 2022). Improved safety systems must handle non-linear loads, modern control techniques, and plenty of power electronics. These alter fault behaviour and relay response. Kompalli et al. (2023) found that IEC 61850 in substation automation adds adaptive protection and GOOSE messaging for peer-to-peer interaction, reducing tripping delay and improving collaboration. This rapid signal interchange is crucial in contemporary grids, where milliseconds may decide equipment damage or power outages. Accurate issue identification aids preventive maintenance, downtime reduction, and digital asset management. (Cacereño et al., 2024).

2.3.5. Advanced Differential and Percentage Differential Protection

The new study suggests using digital signal processing and adaptive filtering to make differential protection methods better so that CT overload, inrush, and external fault maloperations happen less often (Li et al., 2021). Percentage differential protection uses two different slope levels for normal CT mismatch, tap changer operation, and through-faults to make it more selective. These days, relays like the SEL487E figure out slope as:

The SEL-487E relay defines the relationships between the operating current, restraint current, and differential current that are used to find the percentage differential slope. These are shown in Equations 4-4 to 4-6 (SEL, 2020; Li et al., 2021).

Where:

k- design constant 1 for SEL487E

Slp - differential element characteristic slope

Irt - restrain current

Idiff - differential current

I_1 and I_2 - currents measured on the primary side and secondary side, respectively.

This keeps the relay secure during through-faults and sensitive to internal faults. IEC 61850-enabled IEDs increasingly use adaptive algorithms to improve dynamic performance (Silva et al., 2021).

2.3.6. Compensation Techniques and Harmonic Restraint

Ratio correction is indispensable in differential protection to offset the influence of transformer tap positions and CT mismatch, preventing unnecessary tripping (Li et al., 2021). The equation:

$$\frac{v_1}{v_2} = \frac{I_2}{I_1} = \frac{N_1}{N_2} \tag{2.5}$$

Being used to find adjustment factors makes sure that the logic in the switches can change based on how they are being used. There are many ways to tell the difference between magnetising inrush and fault currents, but the second and fifth harmonic analysis are the most common ones (Silva et al., 2021). This helps keep transformers safe. IEC 61850-compliant intelligent electronic devices (IEDs) make it easier to use digital filters and frequency domain analysis in these ways. They also make the methods faster and more accurate.

2.3.7. Integration of IEC 61850 for Enhanced Transformer Protection

High-speed communication, device compatibility, and centralised configuration in IEC 61850-based substation automation systems increase transformer safety (Kompalli et al., 2023). Deterministic and low-latency protection signal exchange channels from GOOSE and Sampled Value (SV) protocols enable substation automation system operation and complex logic implementation. IEC 61850's multi-vendor interoperability lets utilities integrate complex algorithms and protective measures from several sources, improving resilience and flexibility (Kompalli et al., 2023). Additionally, digital substations provide proactive transformer health management via sensor monitoring and online diagnostics (Cacereño et al., 2024).

2.3.8. Cybersecurity and Reliability Considerations in Protection Systems

Putting digital technologies around transformers to protect them makes them less safe and durable. It is now easier for hackers to get into power companies because they are more automated and have more links. Separate networks, encryption, and finding security holes are some of the strong security measures as there is a need to keep networks safe (Chehri et al., 2021). Krause et al. (2021) say that IEC 61850-based systems need to be able to identify strange behaviour practically, have safe ways to log in, and have regular security checks to make sure that data doesn't get changed and services don't disappear. Now, utility companies have to protect important assets by following both technical and legal rules. This is clear from the fact that the EU's cyber-resilience rules are always changing (Krzykowski, 2021).

2.4. Communication Protocols in Substation Automation

2.4.1. Overview of Legacy Protocols: DNP3, Modbus, IEC 60870-5-103

DNP3, Modbus, and IEC 60870-5-103 led substation communication's fundamental interoperability and remote control in power system infrastructures (Aftab et al., 2020). Serial communication methods were vendor-specific and deterministic. DNP3 allowed event-driven reporting and time-stamped data transfer, whereas Modbus was simple and supported numerous devices but had limited data modelling (Aftab et al., 2020). IEC 60870-5-103 emphasised protective equipment communication relay compatibility. Each protocol limited scalability and smooth integration in increasingly complex and digitalised substations due to

bandwidth, security, and data model constraints (He & Jiang, 2020). In multi-vendor setups, obsolete system problems were exposed as the energy industry mechanised and demanded more efficient, standardised, and secure communication protocols.

2.4.2. Comparison with Modern Communication Protocols

The needs of current technology in substations are higher than what old standards can handle. The digital change of substations necessitated not only improved communication speeds and interoperability but also enhanced security, flexible data sharing, and support for advanced automation functions (Zúñiga et al., 2023). Now, methods use advanced data models and Ethernet-based links, which wasn't the case in the past. According to its full data model and quick peer-to-peer sharing, IEC 61850 is a big step forward that stands out. For SCADA and simple device tracking, old protocols like Modbus and IEC 60870-5-103 worked well, but IEC 61850 is better since it can self-describe and be configured (Aftab et al., 2020). A quick look at the main differences between the old and new ways of doing things is shown in Table 2-1.

Table 2-1: Comparison of Legacy and Modern Substation Communication Protocols

Feature	**Modbus**	**DNP3**	**IEC 60870-5-103**	**IEC 61850**
Communication Medium	Serial	Serial/Ethernet	Serial	Ethernet (TCP/IP)
Data Modelling	Minimal	Limited	Relays only	Full, object-based
Vendor Interoperability	Low	Moderate	Moderate	High
Speed	Low	Moderate	Moderate	High
Security	Low	Moderate	Moderate	High
Peer-to-peer Messaging	No	Limited	Limited	Yes (GOOSE, SMV)
Self-description	No	No	No	Yes (SCL files)
Time Synchronisation	No	Yes	Yes	Yes (SNTP, PTP)

This comparison investigation shows that IEC 61850 provides excellent interoperability, predictable communication, and self-description for substation digitalisation (Kompalli et al., 2023).

2.4.3. Introduction to the IEC 61850 Standard as a Revolutionary Protocol

Open, interoperable, and object-oriented IEC 61850 has revolutionised substation automation by enabling complete substation integration (Silva et al., 2021). IEC 61850 simplifies Intelligent Electronic Device (IED) communication by leveraging standard data models, quick messaging, and many configuration options using Substation configuration Language (SCL) files (Silva et al., 2021). Station, bay, and process levels comprise the standard's hierarchical design. SCADA/HMI uses the station bus while merging units, CTs, and VTs utilise the process bus. IEC 61850 is an open, interoperable, object-oriented standard that enables whole-substation integration by combining standardised data models, fast peer-to-peer messaging (GOOSE/SV), and an engineering process based on Substation Configuration Language (SCL) files. These features reduce vendor lock-in, enable deterministic protection signalling, and shorten commissioning via repeatable configuration workflows.

IEC 61850 is popular since it can convey actual deterministic messages via GOOSE and SMV. Important protection and control measures may happen on time. Kompalli et al. (2023) report millisecond-latency peer-to-peer communication using the GOOSE protocol. Acereño et al. (2024) state that IEC 61850 isolates device-specific data into logical nodes and data objects, enabling interoperability and flexible integration across manufacturers. Automating engineering and setup using SCL files reduces commissioning time and mistakes.

2.4.4. Communication Topologies, Protocol Hierarchy, and Redundancy

Since it uses star, ring, or mesh Ethernet structures and backup methods like PRP or HSR to keep communication going when the network goes down, Zúñiga et al. (2023) say that the IEC 61850 design makes networks more stable. Ethernet switches that can be managed make it possible to add devices in a variety of ways and track them in practically at the station level. Tools must be able to use SNTP or the IEEE 1588 Precision Time Protocol (PTP) to keep their times in line so that event logging and synchrophasor readings can work. Silva et al. (2021) say that IEC 61850 makes this possible. IEC 61850's stacked communication stack is based on MMS to connect clients and servers. This ensures that data can move between

IEDs and SCADA systems in a safe and reliable way. Time alignment is essential; PTP (IEEE 1588) is typically used for process-level determinism, while SNTP/NTP is adequate for many station-level functions and event correlation.

2.4.5. Security and Cybersecurity Considerations in Substation Automation

As computers grow more common, substation automation systems require cybersecurity. Various hackers may gain unauthorised access, interrupt service, and modify data in IEC 61850-based systems (Aghanoori et al., 2020; Chehri, 2021). To reduce these hazards, best practises include dividing networks, restricting access, encrypting data in transit, and monitoring unusual activities. To protect substation automation systems, MITRE ATT&CK suggests mandatory authentication, network segmentation, vulnerability assessment, and multi-factor authentication (The MITRE Corporation, 2022; Krause et al., 2021). The most important IEC 61850 network security measures are listed below.

Table 2-2: Cybersecurity Controls for IEC 61850-Based Substation Automation

Control	Description	Source
Network Segmentation	Isolates critical assets from public networks	MITRE, 2022
Authentication Enforcement	Ensures only authorised personnel access	MITRE, 2022
Vulnerability Scanning	Detects and remediates system weaknesses	Krause et al., 2021
Encryption of Network Traffic	Protects data integrity and confidentiality	Chehri et al., 2021
Intrusion Detection and Monitoring	Identifies anomalies and malicious activities	The MITRE Corporation, 2022

To stop cyber-physical risks from getting smarter, there is a need for defences with many layers. Chehri et al. (2021) say that smart substations are using AI and machine learning to find dangers instantly and take action automatically. It is agreed upon by Krause et al. (2021) that risk assessments and security checks should become standard practice for substation

automation projects. As the power grid becomes more digital, these methods show that substation assets need a proactive, risk-based hacking stance.

Switching from old standards to IEC 61850 makes substation control systems much more secure, flexible, and able to do more. The standard's open design, object-oriented data models, and improved communication services make it possible for utilities to build systems that work with each other, can grow, and are reliable. As automation speeds up, cybersecurity becomes a big problem that needs ongoing investments in defence technologies, people, and rules for institutions. Interoperability problems, hacking control automation, and how AI affects the practical stability of substations should all be looked at in more detail in the future.

2.5. IEC 61850 Standard: Concepts and Components

2.5.1. Overview of IEC 61850 Standard: Purpose and Scope

IEC 61850 is the main transmission standard for substation control around the world. It makes it safe, easy, and scalable to add intelligent electronic devices (IEDs) to power substations. The standard was made to avoid problems with communicating privately. At the moment, it makes it easier to share devices, add to systems, and keep technology safe (Silva et al., 2021). As Acereño et al. (2024) say, IEC 61850 standardises device design, setup, and communication, which makes it possible for systems from different providers to work together easily in substation automation. Many people think that the openness, scale, and freedom of IEC 61850 are needed to bring the grid up to date. Cacereño et al. (2024) and Silva et al. (2021) talk about how the standard makes it possible to use complex control and security methods for assets that are spread out. This plan makes sure that the grid is reliable and that problems are fixed quickly,which supports the study's conclusion on the wide adoption of IEC 61850 and broader implementation for smart grid development.

2.5.2. Core Elements: Logical Nodes, Data Objects, ACSI, and SCL

IEC 61850's object-oriented design approach organises all substation functions into logical nodes (LNs) and data objects (DOs) in abstract device structures, according to Aftab et al., 2020; Kompalli, 2023. Functional representation of Logical node, logical device, and physical device, It uses logical nodes to monitor, control, automate, and protect. For measurement, the node begins with "M, as MMXU. Protection begins with "P," as PDIS for distance safety. Start with "X," as XCBR for circuit breakers, to switch things on and off. Each logical node has many data objects that store substation network data points (Silva et al., 2021). Figure 2.3:

DATA Attributes and Objects shows how these data objects match IEC 61850-7-3's common data classes (CDCs), which standardise information structure and meaning.

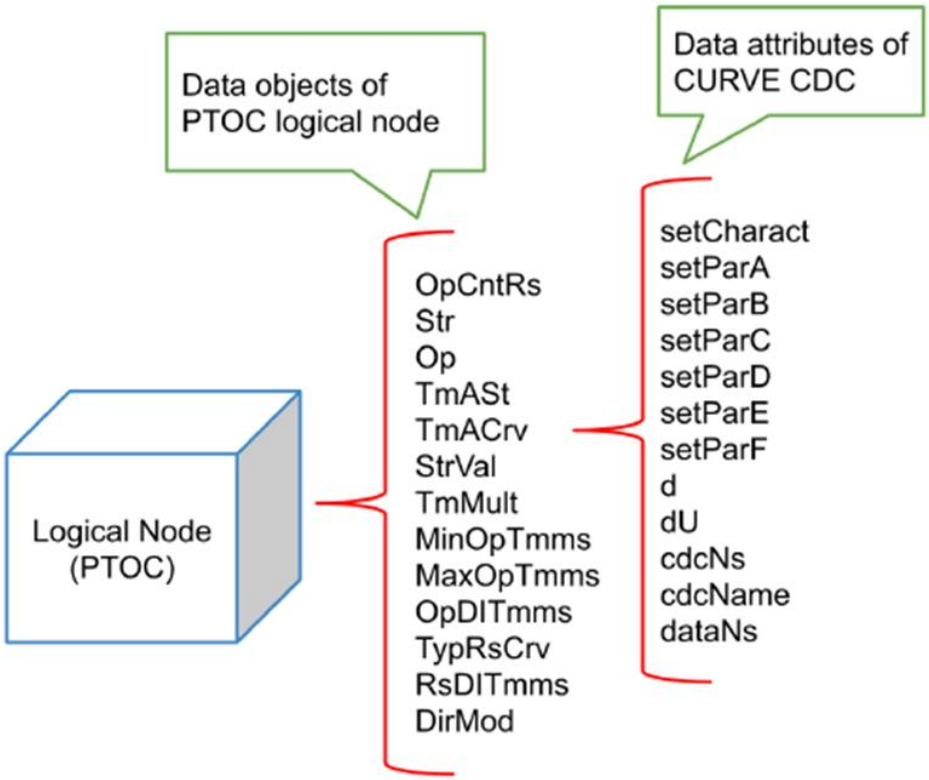


Figure 2.3: DATA Attributes and Objects (IEC 61850-7-3, 2023)

To enable the device's communication, the Abstract Communication Service Interface (ACSI) standardises application-level communications. It achieves this by isolating data meaning from communication mechanisms (Aftab et al., 2020). SCL is crucial to the IEC 61850 ecosystem. Figure 4.7: IEC 61850 Layout illustrates how devices and systems can be built in XML, making substations easy to integrate and reorganise. Object-oriented, model-driven approach may simplify complex engineering processes and let them adapt fast to changing operational demands (Kompalli et al., 2023).

2.5.3. IEC 61850 Communication Services: MMS, GOOSE, Sampled Values

Manufacturing Message Specification (MMS), Generic Object Orientated Substation Events (GOOSE), and Sampled Values (SV) are the three main services that make up the IEC 61850 communication model. Each of these serves a different operating purpose (Silva et al., 2021). IEDs and remote-control systems can send and receive complex client-server data and control orders using MMS. According to Kompalli et al. (2023), GOOSE is a great protocol for

event-driven peer-to-peer talks that is great for important security and automation tasks that need very little delay. The Sampled Values service sends digital analogue signals in real-time like voltage and current between merger units and safety switches. This makes it possible to find problems accurately and in sync.

2.5.4. Engineering Process Using IEC 61850: ICD, SCD, and Configuration Tools

IED Capability Description (ICD), System Specification Description (SSD), Configured IED Description (CID), and Substation Configuration Description (SCD) are used together in IEC 61850 engineering (Kompalli et al., 2023). The ICD file explains each IED, the SSD file specifies the system, and the SCD file merges all IEDs and network settings into one system file. SEL Architect and DIGSI create and manage these XML files. They simplify substation design, commissioning, and management (Cacereño et al., 2024).

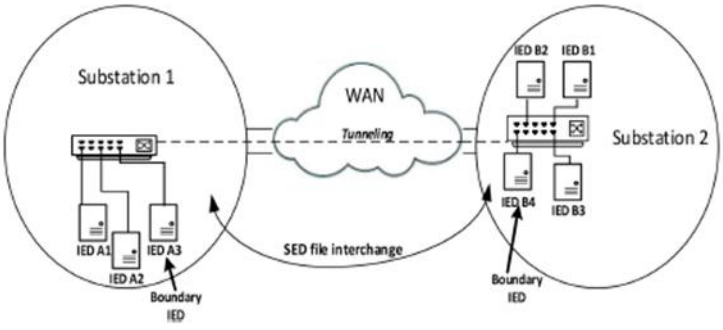


Figure 2.4: SCL file exchange tunnelling (IEC 61850-6, 2024)

The seamless SCL file exchange, including tunnelling as shown in **Figure 2.4: SCL file exchange tunnelling**, is vital for efficient multi-vendor integration and system upgrades. Table 2 below summarises the main configuration files and their roles:

Table 2-3: Main configuration files and their roles

Configuration File	Purpose
ICD	Describes IED functions and capabilities
SSD	Defines system specification and single-line diagram
SCD	Integrates all IED and network configurations

CID	Site-specific configuration of an IED

2.5.5. Interoperability, Scalability, and Flexibility

When devices follow the rules in IEC 61850, they can share and send data in a standard way (Aftab et al., 2020; Silva et al., 2021). It keeps application functions separate from transport protocols. This way, substations can grow, and new technologies can be added without being bound by a single provider. In 2023 and 2024, Zúñiga et al. and Cacereño et al. found that IEC 61850's freedom speeds up the digital transformation of the energy sector by making it easier to adapt to changes in the market, share energy resources, and use advanced analytics. This research shows that IEC 61850 strengthens power infrastructure and lowers costs and technical issues.

2.5.6. IEC 61850 in Advanced Protection: Application of Equations and Algorithms

IEC 61850 provides differential and distance protection algorithms for transformer and feeder protection, according to Mnukwa and Saha (2020). Kirchhoff's current legislation formalises the differential protection premise as:

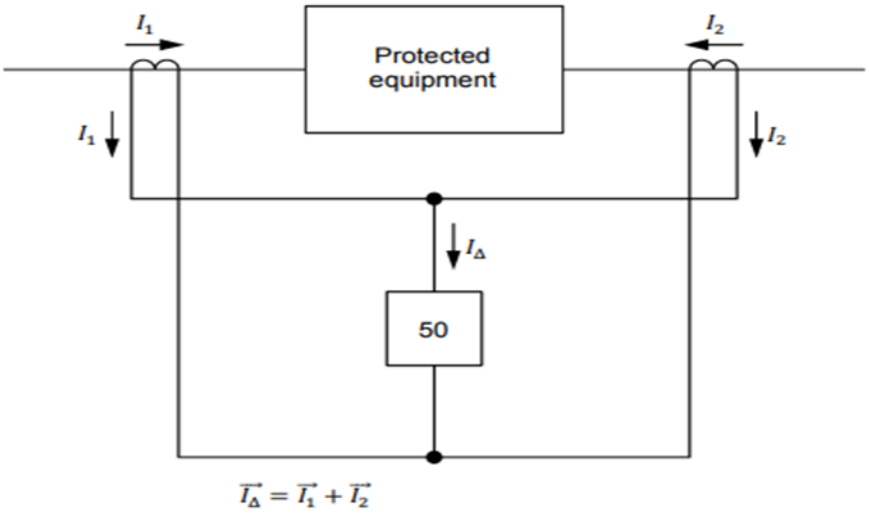


Figure 2.5: Generic operational equation (Horowitz & Phadke, 2024)

$$\vec{I}_1 + \vec{I}_2 + \vec{I}_3 + \cdots + \vec{I}_n = 0A \tag{2.6}$$

For transformer protection, the differential current (Id) and restrain current (Ir) are calculated as follows:

$$I_d = |i_1 - i_2| \tag{2.7}$$

(Equation 210: Differential current calculation)

$$I_r = \frac{|i_1 + i_2|}{2} \tag{2.8}$$

(Equation 2.11: Restrain current calculation)

Relay stability and operation are governed by the relationship between these two, with operation initiated when Id>Ir (Mnukwa & Saha, 2020). Percentage differential protection, which enhances selectivity and security, utilises dual slope characteristics and ratio correction factors, critical in compensating for CT mismatches and tap changer effects (Figure 2.7: SEL 487E Ratio correction).

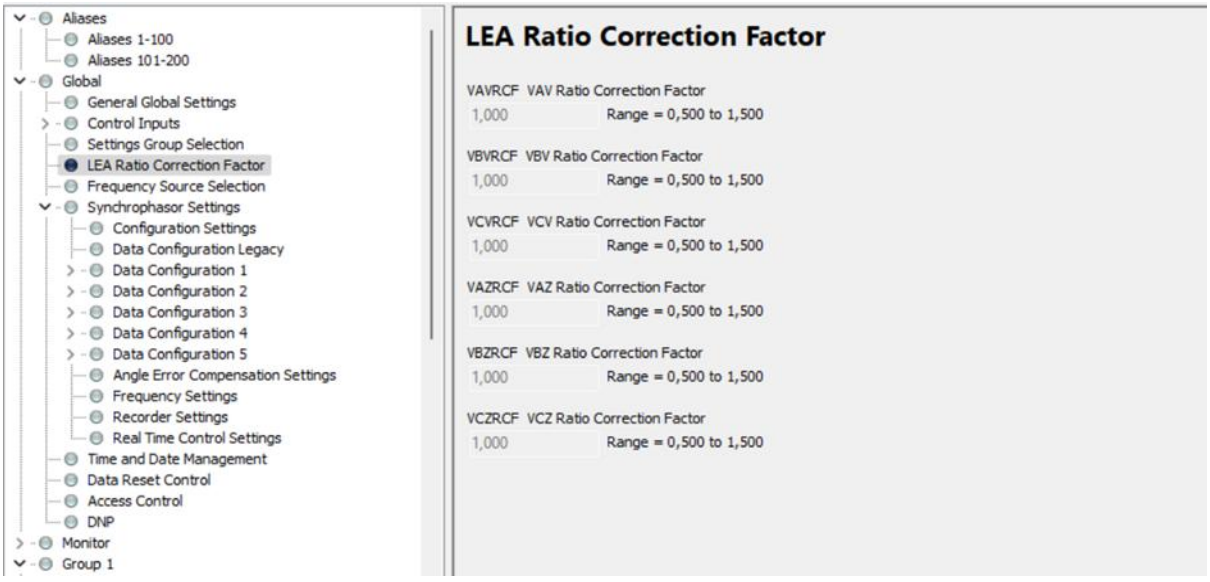


Figure 2.6: SEL 487E Ratio correction

2.5.7. Cybersecurity Considerations in IEC 61850 Substation Automation

Cyberattacks on IEC 61850-based substations are more likely to happen as IT and OT become more integrated (Gunduz & Das, 2020). Krause et al. (2021) say that multi-layered security systems should include network segmentation, identification, encryption, and threat detection. Since going digital makes it easier to attack, it's important to have safety rules and

keep an eye on things all the time. According to Mazhar et al. (2023), breach monitoring systems that use machine learning make substations more reliable. At the moment, role-based access controls, secure communication methods, and frequent risk reviews are needed to make critical infrastructure operationally resilient (Krause et al., 2021). New study backs up this agreement, showing that full safety must be put in from the start instead of being added later.

2.5.8. Engineering Tools and Lifecycle Management

Modern substation automation systems use specialist technologies to simplify lifecycle activities, from design to maintenance (Cacereño et al., 2024). SEL Architect and DIGSI update SCL files, design logical nodes, and verify system topologies using graphical, standards-based interfaces. Continuous monitoring, firmware maintenance, and cyber-hygiene provide compliance with developing standards and best practices (Cacereño et al., 2024) for operations. Asset monitoring and predictive maintenance using IEC 61850 devices increase substation performance and stability (Silva et al., 2021). Current research supports this stance and encourages the IEC 61850 ecosystem to use digital engineering to maintain grid stability and durability.

2.6. IEC 61850-Based Transformer Protection

The strong communication system in IEC 61850 lets Smart Electronic Devices (IEDs) share info and talk to each other regularly. Safety, control, and automation at substations will be different now (Silva et al., 2021). Advanced safety features like transformer protection systems can use IEC 61850's object-oriented data models and defined communication methods. These allow them to send and receive information quickly and consistently (Silva et al., 2021). IEC 61850 has three levels: the station, the bay, and the process. These levels protect and speed up the sharing of important signals between automation controls and security relays, like GOOSE messages and sampled values (SVs) (Silva et al., 2021). These logical entities and how they relate to each other are shown in Figure 2.3: Logical Node, Logical and Physical Device, and Figure 2.8: IEC 61850 Layout. They allow accurate measurement and quick safety of transformer assets in modern digital substations.

While IEC 61850 is great for security coordination and quick trip signs, peer-to-peer GOOSE messages with low latency makes it even better. With GOOSE communications, important security information can be sent in four milliseconds, which allows for quick equipment

separation and grid stability (Kompalli et al., 202^). Through transformer differential protection, current readings on both sides are compared quickly, finding internal flaws and avoiding catastrophic failures (Zúñiga et al., 2023). Sampled value (SV) streams correctly send analogue signals like voltages and currents from merging units to protection switches. This makes measurements more accurate and lets more complex protection algorithms work (Li et al., 2021). Figure 2.8: Network Architecture shows how these protocols work together to make a system that works.

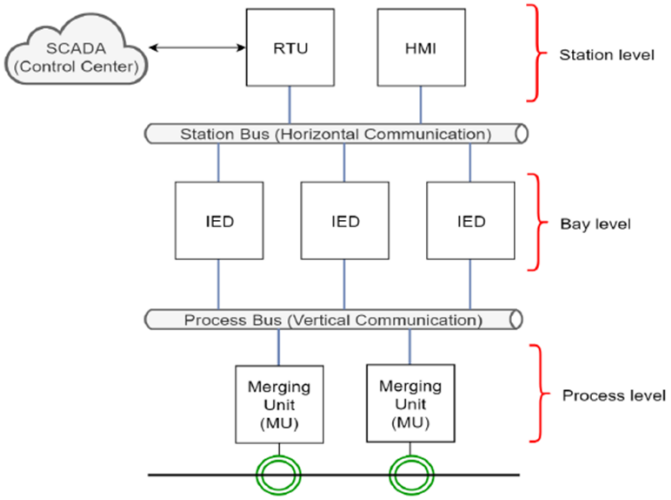


Figure 2.7: Network Architecture (IEC 6185-5, 2023)

For advanced transformer protection methods based on IEC 61850 to work, current differential protection algorithms must be used. Kirchoff's current law, which is written as an equation, sums up the basic idea behind how things work:

$$\overrightarrow{I_1} + \overrightarrow{I_2} + \overrightarrow{I_3} + \cdots + \overrightarrow{I_n} = 0 \tag{2.9}$$

This equation is implemented by continuously comparing the sum of protected transformer zone currents entering and departing. The current should be close to zero under normal or through-fault conditions. Additional operating and restraint conditions are defined by:

$$I_d = |i_1 - i_2| \tag{2.10}$$

$$I_r = \frac{|i_1 + i_2|}{2} \tag{2.11}$$

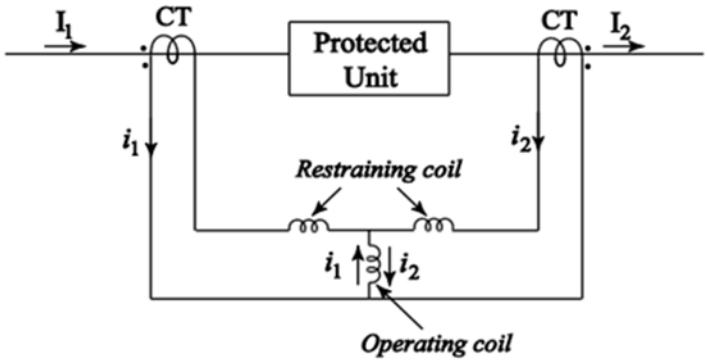


Figure 2.8 Differential Relay *(Horowitz & Phadke, 2024)*

Only when the differential current (Id) exceeds the limit current do protection relays trip. The system becomes more stable and selective (Aghanoori et al., 2020). Electronic transformers and Li et al. (2021) SV procedures rely on reliable current measurements for accuracy. Digital transformer safety's biggest challenges include CT mismatch, ratio correction, and tap changer effects. The following formula handles CT ratio fluctuations, particularly when load circumstances alter:

$$\frac{v_1}{v_2} = \frac{I_2}{I_1} = \frac{N_1}{N_2} \tag{2.12}$$

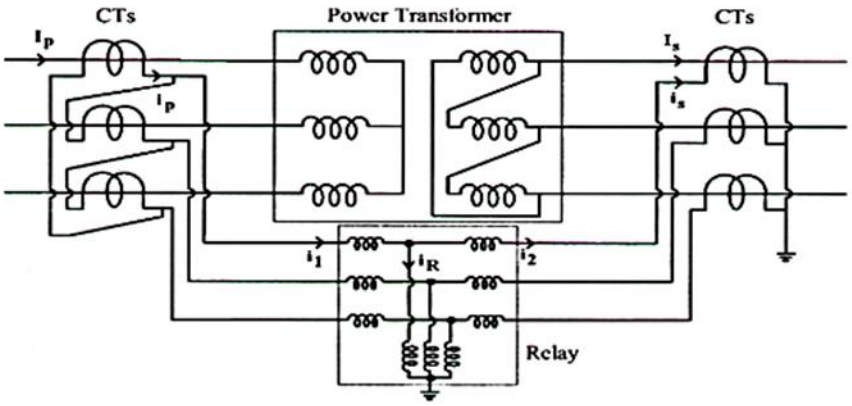


Figure 2.9: Transposing CT (Horowitz & Phadke, 2024)

The relay compensates for these differences algorithmically, ensuring correct operation regardless of the CT secondary ratings (Figure 2.9: Transposing CT). Additionally, tap changer mismatch is calculated as:

$$M = 100 \left| \frac{\frac{I_{HV}}{I_{LV}} - \frac{T_{HV}}{T_{LV}}}{s} \right| \tag{2.13}$$

This comprehensive approach minimises the risk of false tripping and enhances reliability (Li et al., 2021).

Reducing inrush currents and overexcitation events that cause uncomfortable trips is crucial. Modern IEDs utilise harmonic limitation and blocking approaches, such as identifying 2nd, 4th, and 5th harmonics, to distinguish faults from magnetising inrush (Zúñiga et al., 2023). Harmonic limit models usually have:

$$I_{O_P} > SLP \times I_{RT} + K_2 I_2 + K_4 I_4 \tag{2.14}$$

and for 5th harmonic blocking:

$$I_{O_P} < K_5 I_5$$

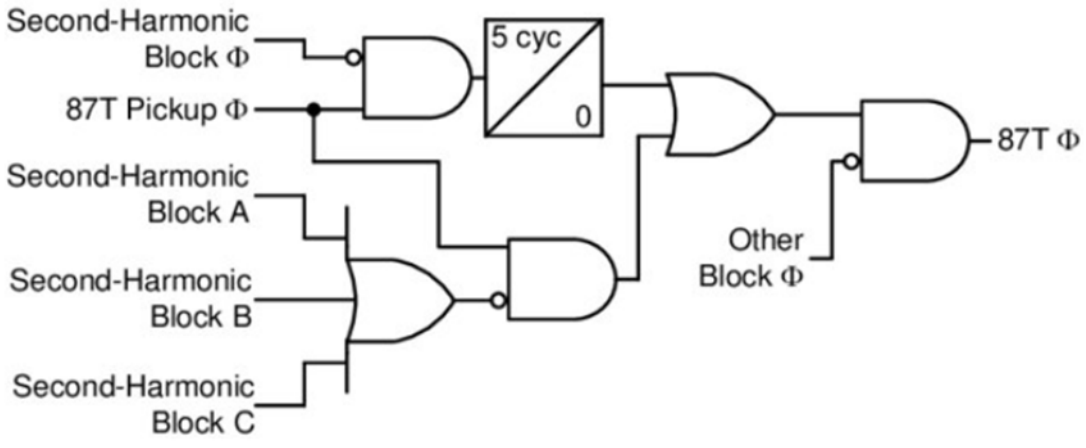


Figure 2.10: Differential Element Harmonic Blocking Logic (SEL Manual,2025)

IEC 61850-based generator safety depends on network design and safety as well as defensive methods. Many communication routes, a star or ring network design, and strong time synchronisation are needed to lower delay and make sure signals are always available (Cacereño et al., 202 four). Digitisation makes cyber threats and holes in data security worse (Krause et al., 2021). To protect against these threats, the MITRE Corporation (2022) suggests that substation automation systems use network separation, access limits, and constant security tracking. These steps stop mistakes from happening by chance and attacks on GOOSE and SV contacts that are done on purpose.

Table 2-4: Main Cybersecurity Controls for IEC 61850-based Systems

Control Measure	Description	Reference
Network segmentation	Isolates critical IEDs from corporate networks	MITRE, 2022
Encryption of GOOSE/SV	Protects data in transit	Krause et al., 2021
Authentication & Access Mgmt.	Limits user/device access to critical assets	Chehri et al., 2021
Intrusion Detection Systems	Monitors/analyzes abnormal traffic patterns	MITRE, 2022

Case studies and actual operations demonstrate IEC 61850-based transformer safety's merits and downsides. After automating its IEC 61850 substations, Mnukwa and Saha (2020) found that the Port of Durban's dependability and maintenance efficiency improved. Silva et al. (2021) and Aghanoori et al. (2020) say many suppliers struggle to collaborate and measure time. As digital substations grow increasingly common, Kompalli et al. (2023) recommend greater research to increase system dependability, interoperability, and security. Adding IEC 61850 to transformer safety plans improves power system substation accuracy, speed, and flexibility. It requires exact measurements, network design, security, and continuing maintenance, which requires partnership in research, standardisation, and worldly innovation.

2.7. Integration of Intelligent Electronic Devices (IEDs)

2.7.1. Definition and Role of IEDs in a Digital Substation

In digital substations, IEDs are very important. One piece of technology lets them measure, control, protect, and talk to each other. Kompalli et al. (2023) say that IEDs are used instead of separate devices in modern IEC 61850-based substations. This makes it easier for substations and control centres to share data and lets tracking and processing happen instantly. The switch from defensive devices based on relays to those based on IEDs has created a large information network. It is possible to make operating choices at the local or cross-substation level, such as tripping or stopping. Customised logic, adaptable security, and SCADA support can also be built into IEDs. It makes the grid more flexible and strong (Silva et al., 2021). According to Zúñiga et al. (2023), the fast growth of IED technology and the IEC 61850 standard has led to better grid digitalisation, integration of green energy, economy, and dependability.

There are physical devices (IEDs), logical devices, and logical nodes in the hierarchical logical design of IEDs. IEC 61850-7-4 says that logical nodes are the building blocks for tasks in the power system, like safety, measurement, and control (C). Each one has its own unique ID and common data classes (CDC). To make producers follow the same rules, CDCs set up sets of status, measurement, and control signals (Silva et al., 2021). A system with many layers makes flexibility and scale easier. Logical devices can be readily mapped to physical IEDs, and additional logical nodes or functionalities may be introduced without large hardware modifications. This standardisation addresses the requirement for grid environments to collaborate and prepare for the future (Cacereño et al., 2024).

2.7.2. Communication and Logic Processing within IEDs

For their complex transmission and logic processing, IEDs are useful since they use all of the IEC 61850 protocols. Modern IEDs have built-in computers that can run complex algorithms, deal with sampled values (SV), and send and receive GOOSE messages for quick peer-to-peer communication (Aftab et al., 2020). Differential protection, adaptable relay settings, and quick linking can now be controlled by Ethernet-based process and station buses. For high-speed data flow and network robustness, the physical structure often has multiple fibre-optic rings or star designs (Cacereño et al., 2024).

IEC 61850 uses object-oriented data models and Substation Configuration Language (SCL) files to show how IEDs talk to each other, what they can do, and how they are organised

logically in XML format (Zúñiga et al., 2023) that is better. In order to improve collaboration and get rid of mistakes, engineering tools and IEDs can share SCL files (such as SSD, ICD, and SCD). This makes device setup and system integration more automated (Cacereño et al., 2024) Self-healing grids and distributed intelligence are made possible by SCL-configured IEDs. They also make setup and maintenance easier and make sure that logic mapping and event management are the same across devices from different vendors (Aftab et al., 2020; Silva et al., 2021).

2.7.3. IEDs Interoperability Challenges and Solutions

Despite the advantages, integrating IEDs to digital substations is difficult for interoperability, particularly when utilising equipment from several companies. Despite the IEC 61850 standard defining data formats and communication services, vendor-specific implementations, firmware versions, and proprietary additions may create inconsistencies, communication failures, and unusual behaviours. Unsupported optional features, variations in SCL file interpretation, and slight variances in logic processing might exacerbate engineering complexity and operational risk (Cacereño et al., 2024).

Industry best practices include multi-vendor system testing, common SCL engineering methods, and vendor-neutral configuration tools to overcome interoperability hurdles (Cacereño et al., 2024). Independent laboratories' conformance testing and certification are crucial for IEDs to satisfy IEC 61850 protocol suite criteria in actual deployments (Zúñiga et al., 2023) according to a recent research. Open engineering platforms and cross-vendor testbeds allow utilities test system compatibility before deployment. This reduces post-deployment issues and enhances automated substation reliability.

2.7.4. Vendor-Specific vs. Vendor-Neutral Configuration Tools

Configuration tools are very important for setting up, starting, and maintaining substation automation IED. Vendor-specific tools use unique features and work with the hardware made by the maker to offer advanced troubleshooting, software management, and custom logic templates (Kompalli et al., 202). These methods can force tools to use a single source, which makes integrating and adding more vendors harder and costlier. According to IEC 61850 SCL, vendor-neutral tools enables the import, export, and update ICD, SCD, and CID files on devices made by different companies (Cacereño et al., 20249). Even though neutral platforms

don't have any built-in features, they make systems much more flexible, lower engineering costs, and let devices of any provider be replaced or updated (Silva et al., 2021).

There is proof from the industry that using vendor-neutral engineering tools and strict conformance testing and licensing can improve long-term worth and operating reliability. Zúñiga et al. (2023) say that utilities should focus on finding ways to handle ecosystems with multiple vendors, make setup checking automatic, and make IED lifecycle management easier. Open, uniform technical settings are needed for the next generation of digital substations to work with smart grid and utility digitalisation technologies (Silva et al., 2021).

2.8. Simulation and Hardware-in-the-Loop Testing

IEC 61850-compliant complex substation automation and protection systems need digital simulation and hardware-in-the-loop (HIL) testing for protection. These solutions provide safe, repeatable substation normal and fault condition inspections without harming live assets. According to Cacereño et al. (2024), simulation-based methods and multi-objective optimisation are essential for planning, maintaining, and assuring substation automation system dependability throughout time. Aftab et al. (2020) recommend dynamically testing IEC 61850-based systems for communication, collaboration, and logic using simulation platforms like RTDS and OPAL-RT.

Just recently, RTDS, RSCAD, and OPAL-RT were utilised to test and simulate IEC 61850-compliant IED logic and performance. Kompalli et al. (2023) stated that these simulation tools can simulate full protection and control. Engineers may adjust relay settings, communication protocols, and peer-to-peer GOOSE messaging under different situations. HIL testing is essential for connecting IEDs to simulated secondary systems. An exceptionally accurate testing environment for substation communication design device performance and communication (Silva et al., 2021). Combining actual and virtual aspects lets complex automation systems be evaluated for response speeds, selectivity, security, and fail-safe operation. This lowers live-launch errors.

HIL testing enables regression analysis of firmware updates, cybersecurity improvements, and vendor-specific settings, enabling system resilience and continual development (Cacereño et al., 2024). Zúñiga et al. (2023) found that simulation-driven verification may uncover design defects or configuration incompatibilities in multi-vendor setups. This may prevent simultaneous failures during rare but devastating grid disruptions. According to

Mnukwa and Saha (2020), simulation and HIL were needed to ensure that IEC 61850 will function with other systems before being used in large infrastructure projects like the Port of Durban power supply upgrade.

2.8.1. Simulation for Validation of Protection Schemes

Validating transformer differential and distance protection methods, which are important for automating substations, needs to be done in simulation. Aghanoori et al. (2020) show that imagined situations correctly show how digital substation network communication delays can affect other parts of the system and threaten the security of safety if left alone. By adding fake problems and changing network conditions in an RTDS or OPAL-RT environment, engineers can test the sensitivity, speed, and security of differential relay logic. They can also check that Kirchhoff-based differential current equations work correctly:

$$\sum_{n=1}^{N} \overrightarrow{I_n} = 0 \tag{2.15}$$

(Kirchhoff's Law for Differential Protection)

as well as the relay decision logic:

$$I_d = |i_1 - i_2|, \quad I_r = \frac{|i_1 + i_2|}{2} \tag{2.16}$$

(Differential and Restrain Current Equations)

CT mismatch, inrush current harmonics, and tap changer dynamics may be precisely included in digital modelling. Time-domain graphs demonstrate relay operation. Static, offline studies seldom provide this degree of evidence. Better digital algorithms increase measurement accuracy in Rogowski coil-based electronic transformers, according to Li et al. (2020). For simulating analog-to-digital conversions in high-integrity logic (HIL), these findings are extremely valuable.

2.8.2. HIL Testing for IED Logic and Performance

Test safety switches and IEDs with equipment and virtual network conditions at the same time using hardware-in-the-loop testing. This makes validation better. Silva et al. (2021) say that this mix is needed to try the GOOSE and Sampled Values (SV) procedures and make sure they work as planned in dangerous situations like when there are problems with the internal generator or when there are line-end short circuits.

Sometimes faults happen more than once, like differential faults and out-of-zone events. These can be used to test logic methods in differential protection schemes, like slope and harmonic restriction, and fine-tune relay threshold settings:

$$I_{op} = k \times Slope \times I_{rt}$$

(Differential Slope Equation)

Unlike bench tests, HIL enables one to assess process bus designs, seamless redundancy protocols, and network congestion communication delays when deployed(Aftab et al., 2020; Silva et al., 2021). For grid safety and stability, relay selection must be done within operational deadlines.

2.8.3. Literature on Simulation-Based Performance Metrics

There is enough research out there now to support modelling and HIL methods for measuring substation automation systems. Cacereño et al. (2024) suggest using digital twin models to try multiple approaches for combining the reliability of a system, its cost, and the amount of time it needs to be maintained. They discovered that RTDS and other digital twin platforms can be used to test how resilient a system is, how long it takes for a device or connection to fail, and how to fix the problem. Zúñiga et al. (2023) say that simulation-based dependability analysis can measure things like the number of times a security relay doesn't work, the average amount of time it takes for a message to reach its destination, and the time it takes for the system to recover. These are important for regulation and utility performance approval. Li et al.'s (2021) work on online adjustment systems for electronic voltage transformers shows that modelling is needed to figure out how these devices change in response to sudden events. Li et al. (2020) say that recursive principal components analysis and modelling tools enable check and change the quality of measurement devices live, which makes operations more reliable.

A lot of new studies agree that HIL and modelling are important in digital substations. Aghanoori et al. (2020) talk about transmission lags and how hard it is to integrate systems, but most engineers and academics agree that these methods are necessary for current IEC 61850-based automation systems to be fast, secure, and reliable. RTDS and HIL methods should be used on purpose in all substation design and upgrade projects, and that ongoing performance feedback should help with practical tuning and future study.

2.9. Cybersecurity in IEC 61850 Substations

2.9.1. Introduction to Vulnerabilities in Ethernet-Based Communication

Since substations adopted IEC 61850 and Ethernet-based transmission, interoperability and seamless control have improved. However, this move has rendered substation automation systems more exposed to increased cyber threats. Gunduz and Das (2020) claim that switching from serial communications to open-standard Ethernet protocols has made hacking, man-in-the-middle assaults, and DoS threats simpler. Krause et al. (2021) also note that many substation communication lines aren't encrypted or authenticated, making them attractive targets for SCADA network exploiters. Ethernet-based communications may increase capacity and scalability, but they are commonly integrated into the company IT network, according to Abrahamsen et al. (2021). Attackers may exploit this loophole. This shows that IEC 61850 communication topologies help operations but also offer new attack surfaces that need good cybersecurity.

2.9.2. Types of Cybersecurity Threats in Substation Automation

According to a critical literature review, cyber threats to substations range from unauthorised entry to complex planned strikes. Lázaro et al. (2021) did a full study and found that hacking, DoS, and fake data input were the most annoying threats. Protection hubs and communication ports can be turned off by DoS attacks, which can lead to key infrastructure failures (Zhang et al., 2021). Chehri et al. (2021) say that these risks have gotten worse since more and more IoT devices are being used in substations. This is since IoT devices often don't have security limits, which means they may let hackers move laterally through the network. According to Pavon et al. (2021), planned cyber-physical attacks can change the state of a system, quiet alarms, or cause catastrophic equipment breakdowns. The research all says that cyber dangers are growing and getting smarter and more dangerous, so preventative and stacked security is needed.

2.9.3. Existing Mitigation Strategies and Cybersecurity Standards

Since these risks, people around the world have come up with rules and ways to reduce them that are special to substations. Under the IEC 62351 series, communication methods used in automating power systems are kept safe. Some of these factors are recognition, encryption, and finding break-ins (Aftab et al., 2020). Zúñiga et al. (2023) say that attacks might not be able to spread laterally inside substations if effective network segmentation, VLANs, and routers are used. The MITRE ATT&CK system, according to The MITRE Corporation (2022), shows threats and the best ways to defend against them. Some examples are least-privilege access, multiple-factor login, and vulnerability testing. Hernandez-Ramos et al. (2020) say that current data protection measures aren't enough; to keep up with new threats, they say, continuous tracking and quick patch management are needed. To be safe, IEC 61850 substations need technical limits, systems that make sure rules are followed, and dynamic risk assessment systems.

2.9.4. Cyber-Physical Attack Scenarios and Risk Assessment

New simulation and statistical risk assessment study models cyber-physical risks. A well-planned assault employing GOOSE messages or SMV traffic might bypass perimeter protection and break relays, according to Zhang et al. (2021). Attack graphs and scenario analysis may identify fundamental problems and suggest fixes such dynamic reconfiguration and duplication, according to Jha et al. (2021). Baul et al. (2023) suggested utilising machine learning to detect bogus data injection attacks to reduce response times and harm. All researchers agree that contemporary substations require multilayer defence-in-depth with actual anomaly detection, not signature-based intruder detection.

Risk = Likelihood (Attack Path) × Impact (Consequence)

2.9.5. Emerging Approaches: AI, Intrusion Detection, and Adaptive Security

The data also shows a growing interest in flexible substation cybersecurity utilising AI and deep learning. Figueiredo et al. (2023) discuss how effectively deep learning models operate in network intrusion detection systems (NIDS), which identify new attack pathways in actual utilisation. Alrowais et al. (2022) demonstrated how density-based clustering and deep learning can detect SCADA coordinated assaults. Mazhar et al. (2023) examined how hybrid machine learning and blockchain may make smart grids safer online and offline. However, Krause et al. (2021) advise that AI-driven security must be balanced with openness and simplicity to avoid additional operational risks. These research recommend adaptable AI-

powered cybersecurity strategies to defend substation automation systems against emerging attacks.

2.9.6. Evaluation of Security Policies and Organisational Practices

More and more study is focussing on how organisations behave, how policies are enforced, and how technology controls work. The MITRE Corporation (2022) says that managing protected accounts, patches, audit logs, and teaching users are all important security practices. No matter how advanced the defences are technically, Mokhor et al. (2020) say that attacks often succeed since security jobs aren't clearly outlined and people aren't trained enough. Xiao et al. (2022) say that in Zero Trust design, context- and risk-aware access control rules should be used to constantly compare access choices with danger information. So, strong rules for control and a security-conscious attitude among operating staff as well as technology staff are needed for substation cybersecurity to work well.

2.9.7. Synthesis and Researcher's Perspective

According to what has been stated, cybersecurity in IEC 61850 substations is a complicated subject including technology, organisational policy, and legal frameworks. The attack area rises when OT and IT are combined. This implies defences must be adaptable and intelligent. Today's best practices include IEC 62351, real-time intrusion detection, and a strong security attitude. Cacereño et al. (2024) and Kompalli et al. (2023) highlight the necessity for constant innovation, training, and flexibility to remain secure in the face of rapidly evolving dangers. In a shifting risk environment, substation cybersecurity depends on how successfully companies manage technological, procedural, and human aspects.

2.10. Gaps Identified in Existing Research

2.10.1. Summary of Limitations in Current Transformer Protection Implementations

Digital security has gotten better, but the ways currently protecting transformers are not fast enough, open, or adaptable enough to deal with changes in the grid. When using advanced differential protection or methods that can be changed based on IEC 61850 standards (Kompalli et al., 2023), it can be hard for old systems to talk to IEDs from more than one provider. The standard provides a shared data model, but there are problems with using it in practical deployment, like combining and making sure that IEDs from different manufacturers

have the same logic, which can cause setup errors or security holes (Cacereño et al., 2024). When updating mixed substations, the difficulties of combining conventional and digital components become more important (Cacereño et al., 2024). However, IEC 61850 has set strong basic standards. In business and academia, practical, vendor-neutral integration for quick and failsafe transformer safety is still being worked on.

2.10.2. Gaps in Simulation and Testing Practices

Efficient testing and simulation of transformer safety systems in practical settings are lacking, particularly in modelling communication delays, cyber-physical hazards, and process-bus topologies (Zúñiga et al., 2024). Simulations generally ignore non-significant delay, network congestion, and failure situations for IEC 61850-based safety signals like GOOSE or Sampled Value messaging (Li et al., 2021). When there are repeated failures or intentional cyberattacks, there are no systematic, standardised procedures to assess security operations' reliability (Aftab et al., 2020). Some market simulation programs can effectively simulate differential and distance relay logic, but few include modules to assess cyber risks, interoperability concerns, and process-bus failure modes. Lab and field validation approaches for IEC 61850 digital transformer protection are fragmented, unstandardised, and not thorough enough for high-impact operational conditions, indicating a research need (Mnukwa & Saha, 2020).

2.10.3. Shortcomings in Existing Literature on Secure, Fast-Acting, and Interoperable Systems

New research talks about security, speed, and communication problems with substation automation system transformer safety. IEC 61850 allows for fast, event-driven protection logic, but end-to-end cyber-physical security, message identification, and synchronising protection actions across devices are still hard to achieve technologically (Gunduz & Das, 2020). It was found by Gunduz and Das (2020) and Lázaro et al. (2021) that man-in-the-middle, hacking, and denial-of-service attacks can happen on IEDs that don't have strong encryption and identification. Harmonising safety logic across IEDs from multiple sources is hard due to different readings of the IEC 61850 standard, leading to mismatches and lowering reliability (Cacereño et al., 2024). More advanced tracking and anomaly detection technologies are being used, but they aren't fully integrated into security algorithms and

response frameworks yet. This makes it hard to create systems that are quick to move, safe, and don't depend on a specific provider (Mnukwa & Saha, 2020).

2.10.4. Opportunities for Improving Reliability and Security via IEC 61850

To enhance transformer protection safety and dependability, IEC 61850 systems are becoming smarter (Cacereño et al., 2024), but technological and operational limitations remain. Deployments of new process-bus features like network redundancy schemes and smooth failover protocols are low. Standards sometimes lack information or are difficult to implement in the field (Kompalli et al., 2024). Network segmentation and security mechanisms including role-based access management, encrypted GOOSE messaging, and anomaly-based intrusion detection have been explored in research settings but not necessarily applied in operational substations (Chehri et al., 2021). While multi-objective optimisation studies suggest that integrated system design and maintenance may minimise downtime and enhance resilience, industry adoption is still delayed (Cacereño et al., 2024). Researchers need to integrate modern communication, security, and control techniques into a standards-based transformer protection architecture. This study requires extensive field testing and performance assessment (Cacereño et al., 2024).

2.10.5. Placement of Key Equations and Diagrams

To facilitate understanding of the core protection concepts, essential equations and diagrams should be strategically inserted within the text. For example, the generic differential protection equation ($\sum I = 0$) and its variants should be placed directly within the section discussing operational principles of differential protection (Section 2.10.1). Similarly, differential current ($Id = |i_1 - i_2|$) and restrain current ($Ir = (|i_1 + i_2|)/2$) equations should appear adjacent to their operational explanation in the differential protection subsection. Diagrams such as “Figure 2.2: Generic operational equation” and “Figure 4.7: Differential relay” should be embedded at these points for visual clarity. Slope characteristics for percentage differential protection and related equations (such as Idiff and Irt) must also be included in the section describing relay settings and stability. Network architecture and logical node structure diagrams (such as Figure 2.3 and Figure 2.4, respectively) should be placed at the beginning of the discussion on IEC 61850 communication architecture. Where relevant, sample table templates such as one comparing various communication delays and failure rates can be added to the simulation and testing section to highlight quantitative research gaps.

2.11. Summary

IEC 61850-based designs have changed the way substations are automated, making safety and control systems more reliable, able to work with other systems, and able to grow (Aftab et al., 2020). The object-oriented data models and defined communication methods in IEC 61850 make it easier for multi-vendor IEDs to share data, make engineering simpler, and allow instanteneous tracking and flexible security (Cacereño et al., 2024) . Krause et al. (2021) and Gunduz & Das (2020) say that the growing number of digital platforms and the merging of IT and operational technology (OT) have made cybersecurity and reliability risks higher. This means that strong strategies for intrusion detection, access control, and network segmentation are needed to keep up with changing best practices (The MITRE Corporation, 2022).

Even though adaptive and differential protection methods have improved, it is still hard to get the best cooperation and robustness in mixed legacy-modern settings and when there are communication delays. Vo et al. (2023) also say that SCL-based configuration management and fault-tolerant transmission in complex substation systems are still problems. Updating to IEC 61850 has made operations more reliable and efficient, More connections create cyber-physical weaknesses that need constant monitoring, auditing, and the use of new monitoring systems based on artificial intelligence (Mazhar et al., 2023).

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1. Introduction

This chapter outlines the transformer safety and power system security study techniques used to implement and evaluate an IEC 61850-based substation upgrade aimed at improving transformer protection and power security. The chosen method includes research design, data collection, system architecture modelling, hardware and software implementation, performance testing, and analytical assessment. The substation automation standard IEC 61850 covers technology improvements and encourages seamless interoperability, advanced monitoring, and rapid protection response. With advanced features like GOOSE communications, Sampled Values (SVs), and MMS protocols, IEC 61850 substation automation exchanges essential operational data over Ethernet. IEC 61850 allows differential (87T), overcurrent (50/51), and thermal transformer safety schemes, boosting speed, reliability, and system flexibility.

Integration of cutting-edge IEDs like the SEL487E, SEL411L, SEL751A, and ABB RED670 increases fault detection and system coordination. These devices leverage IEC 61850's full capabilities, including GOOSE messaging and increased current differential protection, to improve operational sensitivity and resilience to internal transformer failures. High-speed digital communication protocols have simplified wires, decreased operating delays, and made protection schemes more flexible to grid needs. To support substation modernisation's technical and strategic goals, this chapter highlights empirical evaluation and simulation-based testing of IEC 61850 designs in laboratory situations.

This analytical method evaluates cyber-physical threats and applies strong cybersecurity. Critical infrastructure risk has altered due to digital substations and cloud-based control architectures, necessitating operational performance and cyber resilience. Smart grid security specialists recommend cybersecurity testing, enhanced intrusion detection systems, and assault scenario modelling in the substation automation model. This method examines IEC 61850-based protection systems for technical efficacy and cyber-physical threat resilience.

3.2. Research Design

A comprehensive case study examines the development and performance of a fully IEC 61850-compliant transformer protection architecture in modern digital substations. The

research design prioritises IEC 61850-based digital enhancement solutions employing old and modern intelligent protection mechanisms. This technique aims to generate context-specific insights for utility settings with similar automation challenges. The study's simulation substation environment provides insights for industry practitioners and regulators updating substation protection policies to match evolving technological standards.

The empirical component of this research has two steps. The system modelling and design phase begins with IEC 61850-based substation architecture conceptualisation and virtual simulation. According to literature, this phase uses the newest process bus communication, sampling value (SV) transmission, and Generic Object-Oriented Substation Events (GOOSE) messaging protocols. To assess performance, blocking-based, arc-flash, and breaker fail protections are configured and simulated. Iteratively validating the model utilising multi-vendor device interoperability standards and scenario-based stress testing reveals vulnerabilities and optimisation opportunities.

Building a laboratory-based test bench employing commercial-off-the-shelf Intelligent Electronic Devices (IEDs) and industrial-grade networking infrastructure realises the conceptual design in the second phase. The quantitative study examines performance characteristics such protection relay response times, GOOSE message latency, and fault clearance durations in operational and cyber threat scenarios. Traditional and IEC 61850-enabled preventive measures are statistically analysed using high-fidelity simulation tools and event logs. This dual-phased strategy examines the operational, technical, and cybersecurity consequences of digitally converting substation protection systems through theoretical modelling and practical application.

The communication delays, data rates, and background traffic can considerably affect protection performance and system stability when integrating modern digital automation. The research describes the cascaded impacts of communication phenomena on substation performance using a variety of analytical methodologies and simulation environments, ensuring resilient solutions under actual utility limits. All findings are rigorous, reproducible, and relevant to substation automation research and practice because IEC 61850 equipment are tested and certified against international standards.

3.3. IEC 61850-Based Protection Scheme

3.3.1. System Architecture and Design

The IEC serves as a global standards organisation body tasked with the formulation and dissemination of international standards pertaining to electronic, electrical, and associated technologies. IEC 61850 represents a meticulously crafted standard aimed at the design of electrical substation automation systems. This standard has been developed through a collaborative effort involving both manufacturers and users, with the objective of creating a standardised and future-proof framework for the communication, control, and protection of substations. The IEC 61850 comprises of series of standards approximately 10 main parts while there is further development for asset management, condition monitoring and reliability (Paviya, et al., 2024).

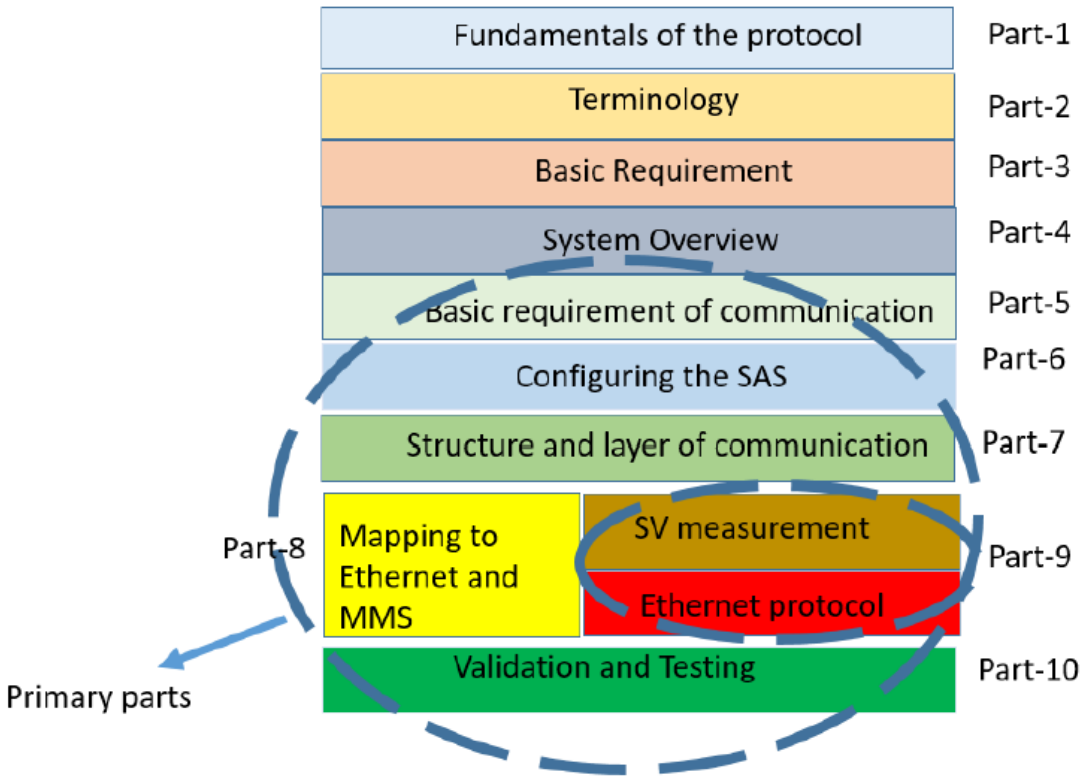


Figure 3.1: IEC 61850 series (Kumar S,2023)

As indicated in figure 3.1 above the primary focus of the study was from part 5 to part 10 when designing an adaptive protection scheme for transformers utilising the IEC 61850 protocol. The IEC 61850 substation architecture hierarchical structure for the protection, controlling, and monitoring of substations is delineated into 3 levels namely Process, Bay and Station levels respectively. *Process Level:* This level encompasses the primary equipment, including analog signals for CTs and VTs, as well as control signals operating from actuators, sensors, circuit breakers, isolators, and other controlling devices. Bay Level: This substation level is positioned in-between the station bus and the process bus. The system encompasses protection and control IEDs for various bays within the substation. Station level: this level pertains to the comprehensive protection of equipment within a substation. The information obtained from one or multiple bays is utilised in algorithm to detect any minor abnormality and aimed at maintaining the security of the system. These functions encompass the activation of a circuit breaker by a protective device or the tripping of multiple breakers for bus differential protection.

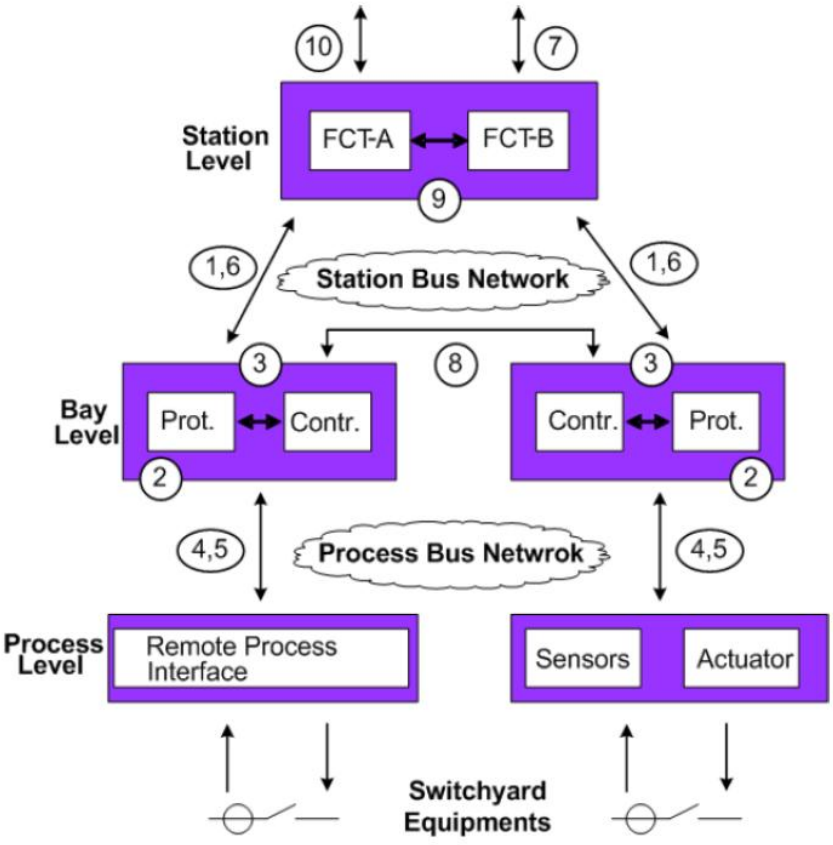


Figure 3.2: Hierarchical structure for transmission substation (Salman,2023)

The developed adaptive protection scheme for transformer includes following key components:

- **Merging Units (MUs)**: Physical devices installed in the switchyard near primary plant equipment and instrument transformers. These units convert analog signal fed from voltage and current transformers into digital streams of sampled values that are synchronised in time in accordance with IEC 61850-9-2. These values are subsequently published to protection and control IEDs via process bus network. The primary plant switchgear (circuit breakers, isolators, earth-switches) statuses are also sent from the merging units to the IEDs via GOOSE messaging. The trip commands, including close and open signals from the IEDs or external devices (units), are received by the merging unit via GOOSE messaging. The time delay should be less than 4 microseconds (Mekkanen, et al., 2024). The conventional block diagram of a merging unit is illustrated in figure 3.3.

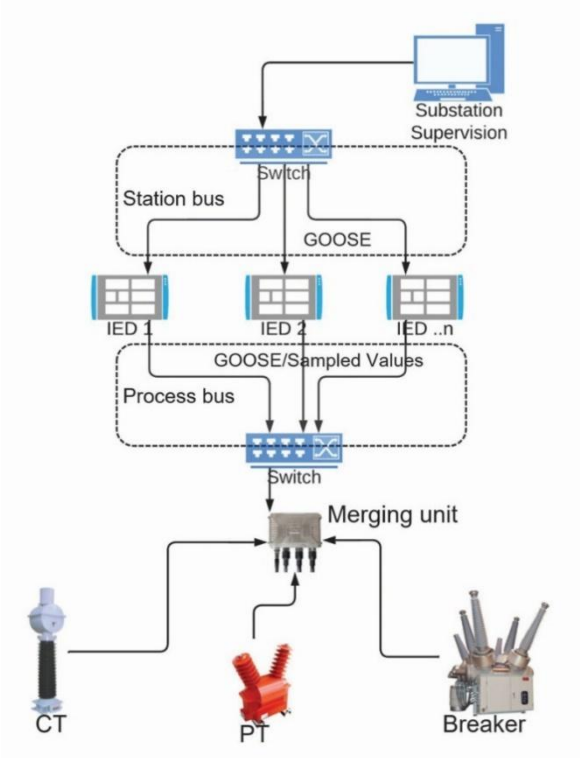


Figure 3.3: Station layout (*(Engineering portal, 2021)*

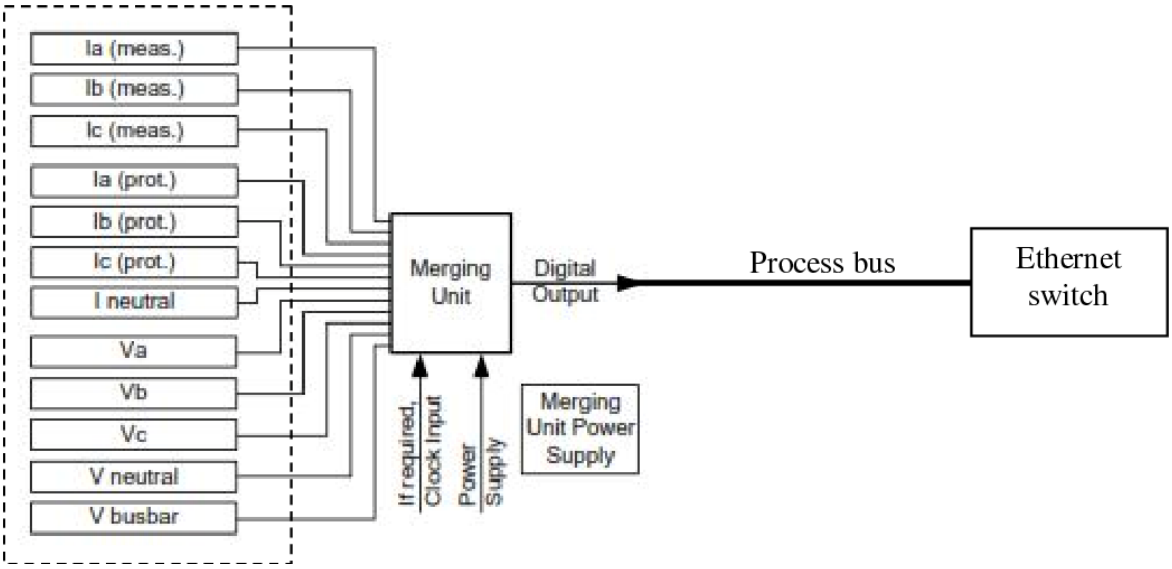


Figure 3.4: Block diagram of an MU

The digital output is transmitted to Intelligent Electronic Devices (IEDs), which significantly benefit utilities and operators by minimising secondary wiring from field devices and facilitating diagnostics. Intelligent merging unit is incorporated with back up (basic) protection, monitoring, and control functions. The merging units could also work well with the sensor technology Frequently known as an NCIT (non-conventional instrument transformer), These senses use SVs to acquire data with excellent accuracy.

- **Intelligent Electronic Devices (IEDs)** for instant data processing and relay coordination.

In electrical power systems, an Intelligent Electronic Device (IED) is a microprocessor-based device that carries out communication, control, monitoring, and protection tasks. IEDs are frequently utilised in substations to optimise grid efficiency, facilitate automation, and increase dependability. IEDs monitor electrical parameters continuously, these devices process the data real-time to detect any abnormalities and facilitate decision making based on configuration.

- **Substation Automation System (SAS)** for monitoring, control, and event-driven response.

Substation Automation system enables a remote access for utilities to monitor, control, synchronisation of specific components within a substation, and data acquisition process. The components entail IEDs, RTUs, and HMIs. In SAS the transmission of data and the

interchange of information are regarded as crucial for the implementation of specific automation functions. This data exchange includes peer-to-peer communication between IEDs in local and remote substations as well as control centres. SAS rely on a multitude of specialised software housed within various hardware components that are integral to a collection of secondary elements within the substation framework. The objectives encompass the formulation of a unified protocol aimed at optimising the distribution of power networks, while considering the modelling of the required data and outline the essential services needed for the prospective mapping of data. Sub-functions delineate logical nodes as the primary characteristic, with these logical nodes existing within logical devices like IEDs. Traditionally, at the bay level process equipment were linked through copper wiring. Since the implementation of the IEC 61850-standard process level (process bus), there has been a significant advancement in the connectivity of process equipment through a digital interface with the broader network of IEDs.

The process level represents the foundational tier at which the switchgear apparatus is situated, encompassing the sensors and actuators essential for the monitoring and operation of the switchgear system. The process bus level encompasses devices including VT, CVTs, CTs, circuit breakers, MUs and others. Process Level Functions involve the acquisition of data from measuring instruments located within the substation, subsequently transmitting this information to the next tier known as bay level. They may additionally obtain control commands (open, close, block) from bay level devices and execute the corresponding response. Process level IEDs and MUs interface with the process bus via local area network technology, this eliminates the need for hardwiring. The bay level serves as the intermediary elevation in the middle level at which the distributed control equipment for protection is situated. These devices are typically connected via hardwiring to the bay level, and the data transmitted primarily comprises analogue and binary input or output data, including VT and CT outputs as well as trip controls from the IEDs. Bay Level Functions include facilitating the transfer of data to and from the bay level, while also executing actions on the equipment located within the bay. IEDs for protection, monitoring, and control are situated at the bay level. The station level represents the elevated tier where gateways facilitating connections to the Network Control Centre (NCC), Human Machine Interface (HMI), centralised system computers are situated. The functions at the station level can be categorised into two distinct types: interface functions and process functions. Process-related functions utilise information from various databases and bays. They issue control commands and gather the sensed data, including both digitalised from bay level IEDs and analogue measured values from VTs and

CTs. Functions pertaining to interfaces encompass HMIs facilitated through remote monitoring and network control centres, aimed at overseeing and maintaining systems effectively. The utilisation of SASs has risen in response to market demands aimed at reducing overall expenses, encompassing the life cycle costs associated with substation equipment. This approach facilitates highly efficient operation or near-limit performance of such equipment, alongside the optimising maintenance expenditures.

- **Generic Object-Oriented Substation Events (GOOSE) Messaging** for high-speed data exchange.

The GOOSE messaging concept represents a sophisticated seamless services facilitating the data exchange for time-critical and non-time-critical information across LAN. This service consolidates various data formats (value, status) into a dataset that is ought to be transmitted and received within 3 ms particularly for the most stringent protection and control applications. IEC 61850-8-1 section of the standard delineates the mapping of the information. The notion of communication utilised by the GOOSE service is publisher and subscriber model. The publisher disseminates information through a broadcast message (multicast) across the local area communication network, and the subscriber acquires the data it is configured to receive. As it is a broadcast messaging, it is designed for reception by numerous devices. Yet, the subscribers don't acknowledge the receipt of the data. Consequently, the GOOSE services employ the retransmission strategy to attain an adequate reliability level, implying that the messages are transmitted multiple times to guarantee the data reception.

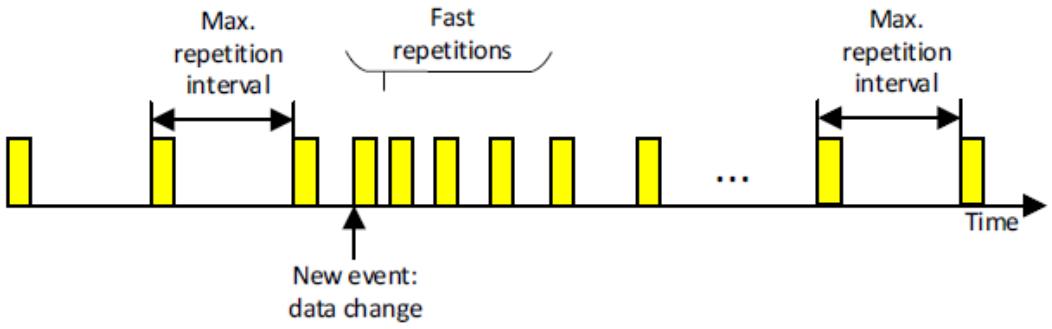


Figure 3.5: GOOSE's retransmission strategy *(Engineering portal, 2024)*

The adoption of GOOSE facilitates the removal of copper wiring between primary plant apparatus and the protection relay as well as relay-to-relay wiring at horisontal level

communications including interlocking techniques. Common utilisations of GOOSE in electrical substations include:

- Status of switchgear equipment (open or closed) between MUs and IEDs
- Exchange of data for apparatus Protection (Transformer, Reactor, Feeder, Busbar etc)
- Exchange of data for breaker failure (Bus strip) between bays
- Exchange of data for interlocking (substation interlocking, operating interlocking etc)
- Control of switchgear (trips, closing etc)

- **Sampled Values (SVs)** for precise voltage and current measurements.

Sampled values are classified as time-critical messages based on a publisher-subscriber communication mechanism enabling multicast messaging to various subscribers transmitted from the publisher in accordance with IEC 61850 standards. SVs contain digitised sampled values (voltage and current measurements) from the sensors or instrument transformers in the merging units to the IEDs through ethernet network on the process bus within the substation. IEC 61850-9-2LE delineates the transmission protocols for sampled values (SV). They transmitted in a continuous traffic with constant load at a rate determined by sampling frequency. SV messages prioritisation within the network is essential for guaranteeing timely delivery; however, unlike GOOSE messages, they are not subject to repetition, which may impact the reliability of transmission (Safdar, 2024).The guideline for implementation IEC 61850-9-2-LE stipulates the sampling frequency of 4 kHz for protection application within 50 Hz networks to ensure effective execution. The publisher samples inputs at 4 kHz designated rate of sampling and disseminate them over the network, allowing the subscribing IED(s) to receive the SVs with timestamp appended to the data, enabling subscribers to verify the sequence of the values (Cardoza, 2021). Contemporary IEDs possess the capability to assimilate diverse data from various MUs within the network. The MU is capable of acquiring 80 samples in one cycle at an sampled value message rate of four kilohertz for fundamental application of protection, and it can achieve 256 samples per cycle for applications requiring high frequency (Coronel & Carvalheira, 2024).

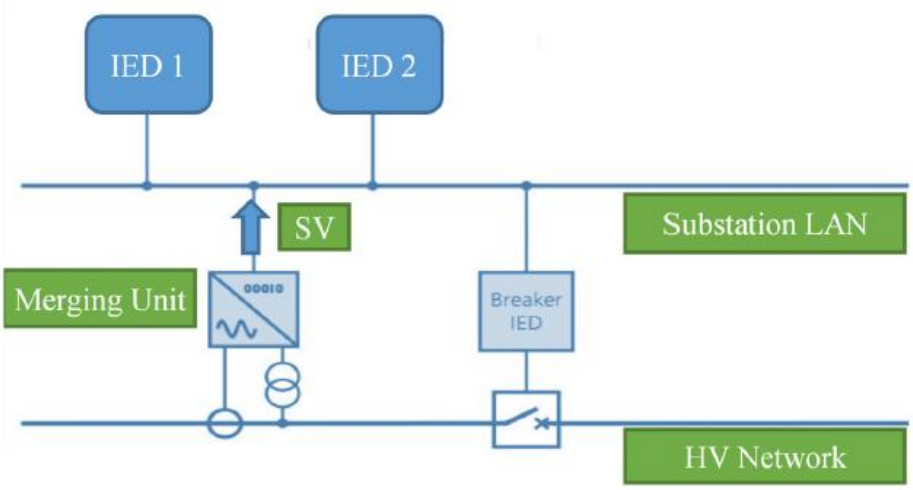


Figure 3.6: IEC 61850 SV messaging MU interfaces

3.4. Communication Network

The substation communication network to be designed based on IEC 61850 standard.

Network Design Considerations: When designing a substation communication network based on IEC 61850, it is of outmost significance to consider factors such as communication link speed, sampling frequency, and network traffic. These factors influence the process bus performance, including packet delay and loss.

3.4.1. IEC 61850 Standard

The IEC serves as a global standards organisation dedicated to the formulation and dissemination of international standards pertaining to electronic, electrical, and associated technologies. IEC 61850 represents a comprehensive standard for the substation automation design, meticulously developed through collaboration between manufacturers and users. This initiative aims to establish a cohesive and forward-looking framework for the communication, protection, and control of substations (Siemens, 2024). This standard has significantly reduced both time and costs in substation automation systems due to its rapid digital communication capabilities. The IEC 61850 standard distinguishes the communication from the application layer, thereby enhancing its flexibility. This enables the user to create various applications independently of particular protocols by defining a collection of figurative services and objects. (IE Commitee, 2022). Due to this division, it is necessary to align the models and

services with particular protocols to accommodate various functional demands for protection, control, and monitoring.

- Ethernet-based station and process bus implementation.

Ethernet Based Communication: The IEC 61850 standard proposes the implementation of ethernet as a means of communication between process-level apparatus and bay-level protection and control devices, through the process bus.

This setup allows for the efficient transmission of time-critical messages like sampled values and GOOSE. The IEC 61850 serves as the benchmark that facilitates rapid and uniform communication on ethernet for utilisation within substation protection, automation, and control systems. thereby enhancing interoperability among various vendors. Consequently, IEC 61850 standard can be regarded as the pivotal element enabling the integration of advanced computing and communication technology into the contemporary, intricate landscape of automation, protection, and control system. This standard does not specify the particular form for this communication system, but it does outline the communication between systems and equipment within a substation. Various network topologies may be created using the standard's tools and based on the needs of the system.

Implementation of Process Bus: A key component of the IEC 61850-9-2 standard. It uses Ethernet to connect MUs and IEDs, enabling the digital transmission of data from the switchyard to the control systems. This setup enhances flexibility and reduces the need for extensive copper wiring. The complete potential of the communication framework based on IEC-61850 can be fully harnessed within a station bus and process bus-oriented architecture. This encompasses a variety of sophisticated devices, intelligent electronic devices, and devices that are integrated into the substation LAN. As previously explained in the preceding merging unit section, The unit operates by processing inputs from the current transformers and voltage transformers, yielding digital SVs of the currents and voltages. Furthermore, the merging unit formats and digitalises the sampled values, transmitting it to IEDs, Switches and other electronic devices linked to the station LAN. The input/output unit (IOU) is responsible for processing input, generating status data, formatting communication message, and forwarding this information to the local are network of the substation. The IEDs and associated smart devices subsequently acquire broadcast of the information from the network, presented as sampled value messages or status messages. It is crucial to note that only the IEDs specifically designed to accept and process this data are capable of determining the requisite

and appropriate actions that must be undertaken. During a fault event, the Intelligent Electronic Device generates a tripping signal by transmitting a (GSE) General Status Event message to the pertinent Input/Output Unit (IOU), which may subsequently activate the corresponding circuit breaker. Therefore, IEDs in the substation are configured to acquire subscription in order to receive specific information and network messaging

Implementing the IEC 61850 protocol brings about the advantageous transition from copper cables to fibre optics or Ethernet for connecting devices such CTs, VTs and IEDs, facilitating the integration of merging units and the process bus. This system enables the optimisation and reduction of the required number of VTs within the substation, as voltage information can be disseminated as sampled values messaging across the local area network of the substation to all pertinent devices. This indicates that it is not essential to install a VT on every bay more especially on outgoing feeders; rather, it may suffice to place one on the busbar, from which the information can be disseminated to other devices requiring it via the LAN. This optimisation pertains to the VT measurement requisite for distance protection systems.

3.5. Cyber vulnerability

Cyber-physical devices are intelligent electronic devices that utilise optical fibre or ethernet for communication over the LAN of the substation, in addition to leveraging cloud computing capabilities via the internet. The protection of IEDs, and consequently substations, is vulnerable to cyber-attacks from both criminal and terrorist organisations. The implementation of rapid substation protection, automation and control based in IEC 61850 environment involves innovative techniques aimed at safeguarding various devices in substation from cyber threats. Cyber-attack can be executed through various mechanisms or catalysts, ultimately aiming to disrupt or compromise a protection system. The various cyber threats that pose a significant risk to IEC 61850-based networks encompass deliberately malfunctioning MU sending false information (false tripping, false stability) and deliberately impeded IEDs on the network. An attack on a substation utilising IEC 61850 standard and its interconnected system transpires when a hacker introduces deceptive, yet syntactically valid measurement into sampled value or GOOSE messaging stream therefore tricking the network into recognising them as legitimate code. Therefore, an effective defence strategy is required to protect the costly, essential, and sensitive equipment located within a substation from potential corruption. To safeguard IEC 61850-based devices against cyber threats, it is essential for the Intelligent Electronic Devices (IEDs) to be configured for mutual collaboration. This ensures that they can collectively ascertain the existence of faulty conditions and determine the necessary corrective action, such as initiating a breaker trip. An optimal cyber

defence strategy would involve the capability to detect a specified quantity of erroneous or altered measurements within a designated SV or GOOSE messaging stream. Consequently, the network of interrelated IED(s) must obtain and evaluate the sampled value measurements from their corresponding relays and merging units, juxtapose these with their own data, and ultimately utilise Kirchhoff's Voltage law (KVL) and Kirchhoff's Current Law (KCL) to ascertain the validity and precision of the information presented. Finding the defective IED and replacing or reprogramming it is crucial when an incorrect or erroneous measurement is detected. The ring bus or loop circuit served as the foundation for this cyber defence technique.

Performance Evaluation: The assessment of the performance of the IEC 61850 process bus necessitates a multifaceted approach, integrating both simulation and analytical techniques to comprehensively assess its behaviour under diverse operational conditions. At the core of this evaluation lies the accurate modelling of network parameters, encompassing factors such as network topology, communication protocols, message sizes, and traffic patterns, all of which exert a substantial influence on message delay and loss, key determinants of power system security (Süfke, 2021).The employment of specialised simulation tools such as Test Universe, IEDScout, and Quickset facilitates the creation of virtual network models, enabling the assessment of the process bus's response to a wide array of scenarios, including normal operation, fault conditions, and cyber-attacks. By leveraging these tools, the valuable insights into the intricate dynamics of the process bus are achieved, paving the way for optimised designs and enhanced resilience against potential disruptions. Furthermore, Hardware prototypes that incorporate WLAN-enabled IEC 61850 devices, developed through industrial embedded systems, facilitate comprehensive explorations into the monitoring, control, and protection applications of smart distribution substations across diverse scenarios. The round trip-time measurements of IEC 61850 application messages act as a vital performance metric (Parikh, 2022).

Impact of Network Parameters: Several network parameters can significantly influence the performance of a process bus, which is crucial for transformer protection These parameters include data rate, bit error rate, and background traffic.

Data Rate: The data rate plays a crucial role in establishing the speed of data transmission throughout the network. A higher data rate allows for more data to be transmitted in a given time, which can improve the responsiveness of protection schemes. However, it can also lead to increased network congestion if not managed properly. The bit error rate represents the

proportion of bits that are received inaccurately. A high BER can lead to communication failures and delayed or incorrect operation of protection functions.

Background Traffic: Background traffic refers to any network traffic that is not directly related to the protection scheme. High levels of background traffic can increase network congestion and delay the transmission of critical protection data. Understanding these factors is important for enhancing transformer protection because the reliability and speed of protection schemes rely on the process bus performance. The incorrect configuration of the switch, the tagging of message priorities, and the overall traffic volumes on the network could potentially influence the timeliness and dependability of the signals being transmitted.

If the process bus is not performing adequately, protection schemes may not be able to operate quickly and reliably, which can lead to damage to the transformer or other equipment. It is critical to design and configure networks that meet the performance requirements of protection schemes

Corrective Measures: In the realm of modern power systems, the integrity and reliability of digital relaying functions are paramount for ensuring grid stability and preventing cascading failures. Digital relays, which are integral components of protection schemes, depend on the timely and accurate exchange of information through communication networks. However, the inherent characteristics of these networks, such as message delay and loss, can significantly degrade the performance of digital relays, potentially leading to maloperations and compromised power system security. To address these challenges, the SV estimation algorithm emerges as a promising solution. The algorithm offers a robust mechanism for mitigating the adverse effects of communication impairments on the accuracy of digital relaying functionalities. The SV estimation algorithm operates by reconstructing the original analog signals from the received sampled values, even in the presence of missing or delayed data. This reconstruction process typically involves interpolation techniques, such as polynomial interpolation or Kalman filtering, which leverage the available data points and system models to estimate the missing or corrupted samples. By accurately estimating the unreceived or delayed samples, the sampled value estimation algorithm effectively compensates for the communication impairments, thus ensuring that the digital relays receive a continuous and reliable stream of data.

3.5.1. CYBERSECURITY IN THE SIMULATION TESTBED

3.5.1.1. Cybersecurity Modelling and Testbed Considerations

3.5.1.2. Overview and Scope of Cybersecurity in this Study

Even in a simulated setting, cybersecurity risks inherent in the digital architecture enabling IEC 61850-based substation automation must be identified and addressed. Although the testbed was created to replicate actual network topologies and communication patterns that expose the system to possible cyber-attacks, this study is a simulation-based analysis rather than a live field deployment. As a result, the cybersecurity presumptions, modelled controls, and issues that arose during the simulation exercise are all documented in this section. This study primarily used Generic Object-Oriented Substation Events (GOOSE) messaging for communication. As required by the basic IEC 61850 standard, this kind of communication operates via regular Ethernet without integrated transport-layer encryption or authentication. Although this feature enables low-latency peer-to-peer communication (often less than 4 ms), it also exposes GOOSE frames to denial-of-service (DoS) interruption, replay attacks, packet injection, and man-in-the-middle interception. To determine if the suggested protection plan is practical, it is critical to understand these attack routes.

3.5.2. Cybersecurity Threats Relevant to the Testbed

Within the simulation environment, the following cyber threat categories were identified as relevant to the IEC 61850-based transformer bay protection scheme:

- GOOSE Spoofing: An adversary might transmit counterfeit GOOSE messages via the substation's local area network (LAN), perhaps resulting in erroneous trip instructions or obstructing genuine protection signals. In the testbed, this attack vector was conceptually simulated by monitoring the responses of the SEL-487E and SEL-411L IEDs to delayed or absent GOOSE frames, as observed during communication disruptions
- Replay Attacks: An assailant can retransmit recorded GOOSE packets to replicate a previously legitimate control action. The IEC 61850 standard has a sequence number (SqNum) field in GOOSE messages, which aids in mitigating this danger by enabling receivers to discard frames that are out of sequence. The SEL IED logic in the testbed design ensured the monitoring of SqNum, hence providing a fundamental level of replay protection.

- Denial-of-Service (DoS) Attacks: Excessive traffic directed at the substation LAN may impede the transmission of GOOSE signals, beyond the permissible 4-20 ms threshold, hence delaying protective mechanisms. The OMICRON Test Universe was employed to generate network delay scenarios in the simulation to evaluate the efficacy of the protection strategy under adverse communication conditions. The findings indicated that protection reliability remained constant up to a delay threshold of 20 ms.
- Unauthorised Access to IED: If an individual gains entry to the IED configuration interfaces without authorisation, they may alter the protective settings detrimentally. Access to the SEL acSELerator QuickSet 5030 setup environment in the testbed was restricted to authenticated users only. This was accomplished via password-protected login systems, which is a normal procedure for utilities

3.5.3 Cybersecurity Controls Modelled in the Simulation Testbed

Although the scope of this study did not include penetration testing or the deployment of advanced intrusion detection systems (IDS), several cybersecurity controls were either explicitly modelled or implicitly reflected in the testbed design. Table 3-2 summarises these controls and their implementation status within the simulation environment.

Cybersecurity Control	Implementation in Testbed	Relevant Standard
VLAN Network Segmentation	The substation LAN was modelled as a logically isolated VLAN, separating process bus traffic from station bus traffic to limit lateral threat propagation	IEC 62351-8; NERC CIP-005
GOOSE Message Integrity (SqNum)	IED logic was configured to reject GOOSE frames with non-sequential SqNum values, providing basic replay and injection resistance	IEC 61850-8-1; IEC 62351-6
Access Control	SEL acSELerator QuickSet 5030 access was restricted to password-authenticated users; no remote access was enabled during simulation	IEC 62351-8; NERC CIP-007
Communication Redundancy (PRP/HSR)	Parallel Redundancy Protocol (PRP) was	IEC 62439-3

	considered in the network design to ensure communication continuity in the event of single-link failure	
Time Synchronisation Security	IEEE 1588 Precision Time Protocol (PTP) was applied for time-stamping GOOSE messages, enabling forensic analysis of communication sequences post event	IEC 61850-9-3; IEEE 1588
Intrusion Detection	Not implemented in this simulation. Identified as a limitation and recommended for future work (Section 7.5)	IEC 62351-7 (future)

Table 3-2: Cybersecurity Controls Modelled in the IEC 61850 Simulation Testbed

3.5.4 Role of IEC 62351 in Securing IEC 61850 Communications

The IEC 62351 standard series was developed by the International Electrotechnical Commission (IEC) to address the security vulnerabilities prevalent in IEC 61850 and other power system communication standards. IEC 62351 establishes regulations for security across several tiers of the communication stack. For instance, it stipulates that transport layer security (TLS) must be employed for MMS and client-server communications (IEC 62351-3), role-based access control (RBAC) is required for IED access management (IEC 62351-8), and security monitoring should be conducted via network and system management extensions (IEC 62351-7).

IEC 62351-6 is crucial since it addresses the security of GOOSE and Sampled Values (SV) by establishing message authentication code (MAC) systems to detect and reject unauthorised or altered communications. It is crucial to acknowledge that the implementation of IEC 62351-6 authentication introduces additional processing time, potentially impeding message transmission and impacting the sub-4 ms performance criterion for protection-class GOOSE communications (Krause et al., 2021; Figueiredo et al., 2023). The trade-off between security and protection speed is a prominent research focus and is recognised as a critical subject for further exploration in this study (Section 7.5).
The testbed did not achieve complete compliance with IEC 62351 due to hardware and time

constraints. The simulation architecture was constructed to comply with IEC 62351, with logical segregation of network zones and authentication techniques included in the installed SEL IED firmware. Full implementation of IEC 62351 is advisable for any practical application of the suggested protection strategy.

3.5.5 Cybersecurity Limitations of this Study

The cybersecurity evaluation in this study is distinctly constrained in scope. Specifically: No active penetration tests were conducted on the testbed. The simulated environment fails to emulate all real-world attack vectors, including zero-day vulnerabilities and advanced persistent threats (APTs). The OMICRON Test Universe simulation excluded any intrusion detection system (IDS) techniques. It is recommended that AI be employed to detect irregularities in GOOSE traffic for future endeavours. The simulation fails to consider insider attacks, social engineering, or vulnerabilities inside the supply chain, all of which pose significant dangers in actual substation contexts. This simulation analysis excludes electromagnetic interference (EMI) and physical security concerns inside the substation area, which may impact the availability of IEDs and the integrity of communication. Notwithstanding these constraints, the cybersecurity framework established in this testbed provides a practical basis for evaluating the security posture of IEC 61850-based transformer protection systems and informs the recommendations for future enhancements detailed in Section 7.5.

Summary: IEC 61850 is increasingly accepted as the preferred standard for substation communications, playing a vital role in upgrading substations for enhanced transformer protection and power security (Hinkley & Mistry, 2023). This standard ensures consistent communication and integration of HV primary plant assets with IEDs (Kumar et al., 2021). Implementing IEC 61850 requires a comprehensive analysis of costs, reliability, and technical trade-offs. Detailed performance investigations and feasibility studies are essential for the full-scale implementation of non-conventional instrument transformers. Wireless LAN technologies are also being explored for smart distribution substations, with hardware prototypes developed to analyse the performance of monitoring, control, and protection applications (Parikh, 2022). The performance, security, and dependability of process bus communication, as proposed by IEC 61850-9-2, are critical concerns, necessitating dynamic simulation test platforms. Furthermore, IEC 61850-based harmonic blocking schemes are employed for power transformers to prevent failures (Krishnamurthy, 2022)and seismic

considerations are addressed to protect high voltage electrical equipment against earthquake damage.

3.6. Simulation Setup and Modelling

3.6.1. Transformer feeder design

The advent of contemporary IED and the innovative IEC 61850-based architecture have fundamentally transformed the design and implementation of transformer feeders. A transformer feeder is a configuration in which the transformer lacks a locally mounted high-voltage circuit breaker. Instead, the transformer depends on the circuit breaker of the feeder located at the remote station from which the incoming supply is derived.

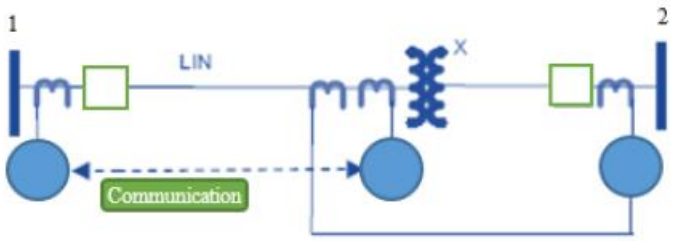


Figure 3.7: Conventional transformer feeder protection

The initial illustration, Figure 3.7, presents a comprehensive scheme for the protection of a lengthy feeder and transformer. This diagram illustrates substation 1 as the source and substation 2 serves as a load. The CT orientation would be in a manner that the line and the transformer are 100% protected i.e. the CTs on the transformer would overlap as depicted above. The CT on the inner side of the transformer would be towards the line for line differential and distance protection. The outer CT is towards the transformer. the communication medium between the differential IEDs at the above-mentioned substation is fibre optics. The communication between the distance IEDs is facilitated through GOOSE based SV and power line carrier of tele-protection. The developed algorithm incorporates an alternative inter-tripping scheme from the IEDs at substation 2 through the SEL2505 device and substation LAN to ensure adequate protection. This design is cost effective as the HV circuit breaker and auxiliary equipment is not installed. The advanced relays or IEDs possess the capability to transmit SV message and information across terminals via rapid

instantaneous digital communication links. This signifies that information is conveyed clearly, enabling effective decision-making within the IEDs.

The IEDs in this configuration will include the IED on substation 1 and IED on substation 2, the IED at substation 1 can be configured to incoporate differential, distance and overcurrent. Depending on the orientation of CTs all these functions protect the feeder and the transformer at the same time. This IED coordinates with the IEDs installed at substation 2. At the substation 2 the IEDs can be split into 3 IEDs or functions i.e Differential, Distance and overcurrent. Distance protection at substation 1 and substation 2 will coordinate together incorporating communication-assisted capabilities, including tele-protection. Differential functions at substation 2 can be used for transformer differential protection and second one provides line protection. The presence of overcurrent at both substations serves to ensure an additional layer of protective measures. An alternative inter-tripping mechanism is also facilitated through the SEL2505 switch, utilising a distinct channel to guarantee sufficient protection. This alternative tripping signal guarantees that rapid tripping is accomplished even in the event of a failure in communication between the two Distance IEDs or the two Differential IEDs, respectively.

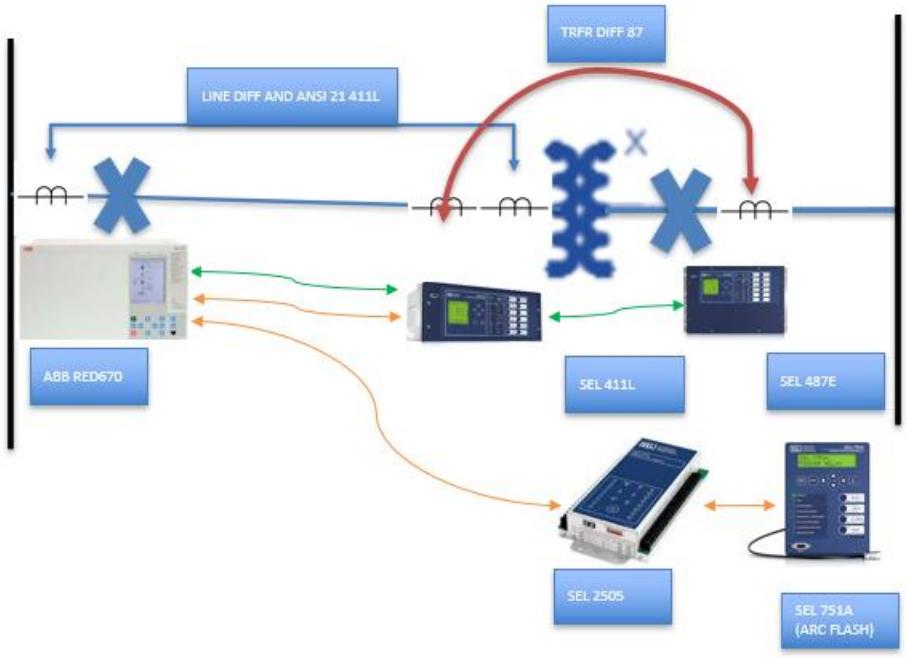


Figure 3.8: Alternative carrier inter-trip send

3.7. IED SETTINGS AND CONFIGURATION

3.7.1. Differential protection configuration (ANSI 87)

The operation of this element fundamentally relies on the vector sum of current flowing into the protected object and leaving the object as demarcated by the position of current transformers. During stable, through fault or normal operating condition the differential current is insignificant or equal to zero. When the fault is within the protected zone the differential current will be more than the restraint current leading into the relay element operating and subsequently tripping relevant circuit breakers. The ANSI 87 element configuration setting is shown below.

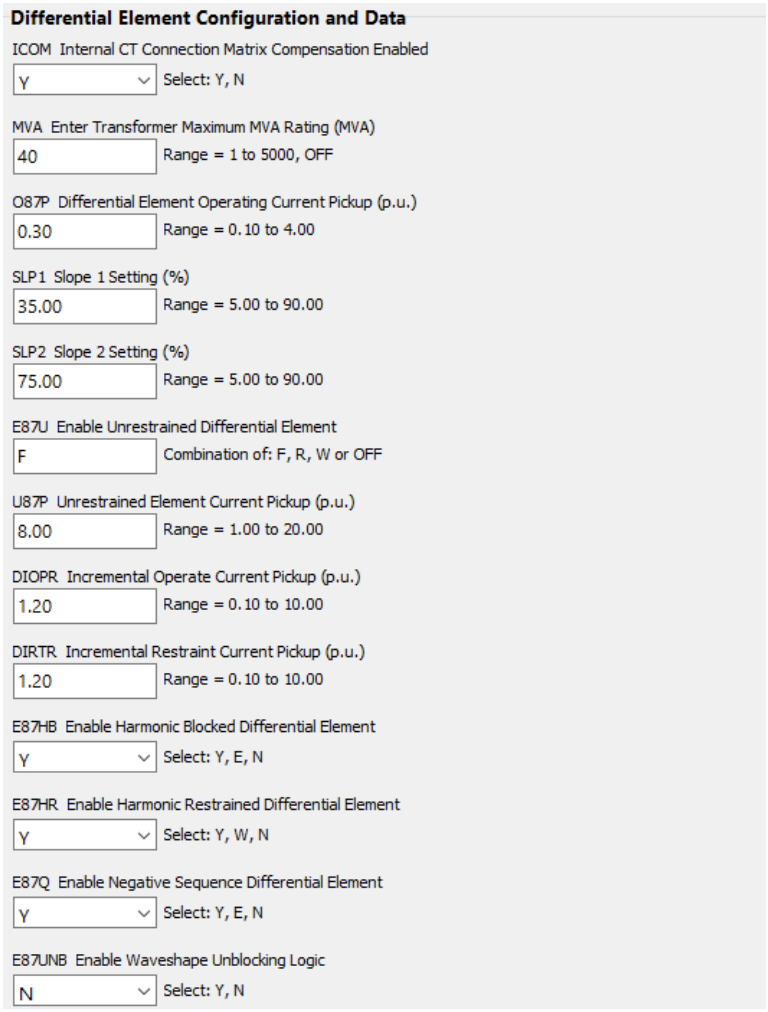


Figure 3.9: Differential Setting

3.7.2. Distance/Impedance protection configuration (ANS 21)

The fundamental operation of this element utilises the ratio of measured voltage and current in relation the set values. It has different zones of protection determined by their reach and associated time delay in absence of tele protection. This element can be configured to use MHO and Quadrilateral characteristics for enhanced resistive reach.

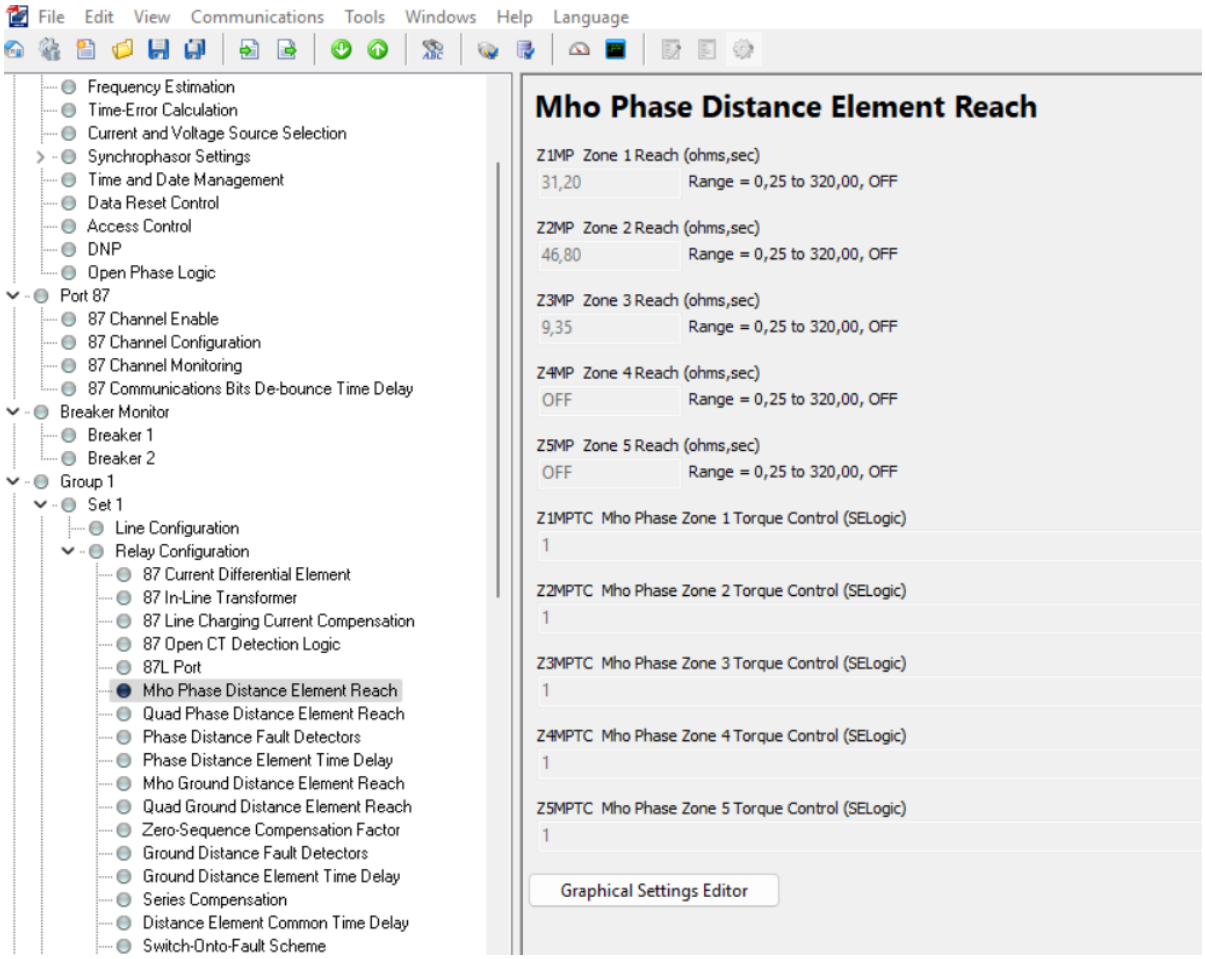


Figure 3.10: Distance settings

3.7.3. Overcurrent protection (ANSI 50P,51P,50N,51N,50G,51G)

This protection element is used for overcurrent and earth protection. This element can be configured to operate instantaneously or time delayed tripping.

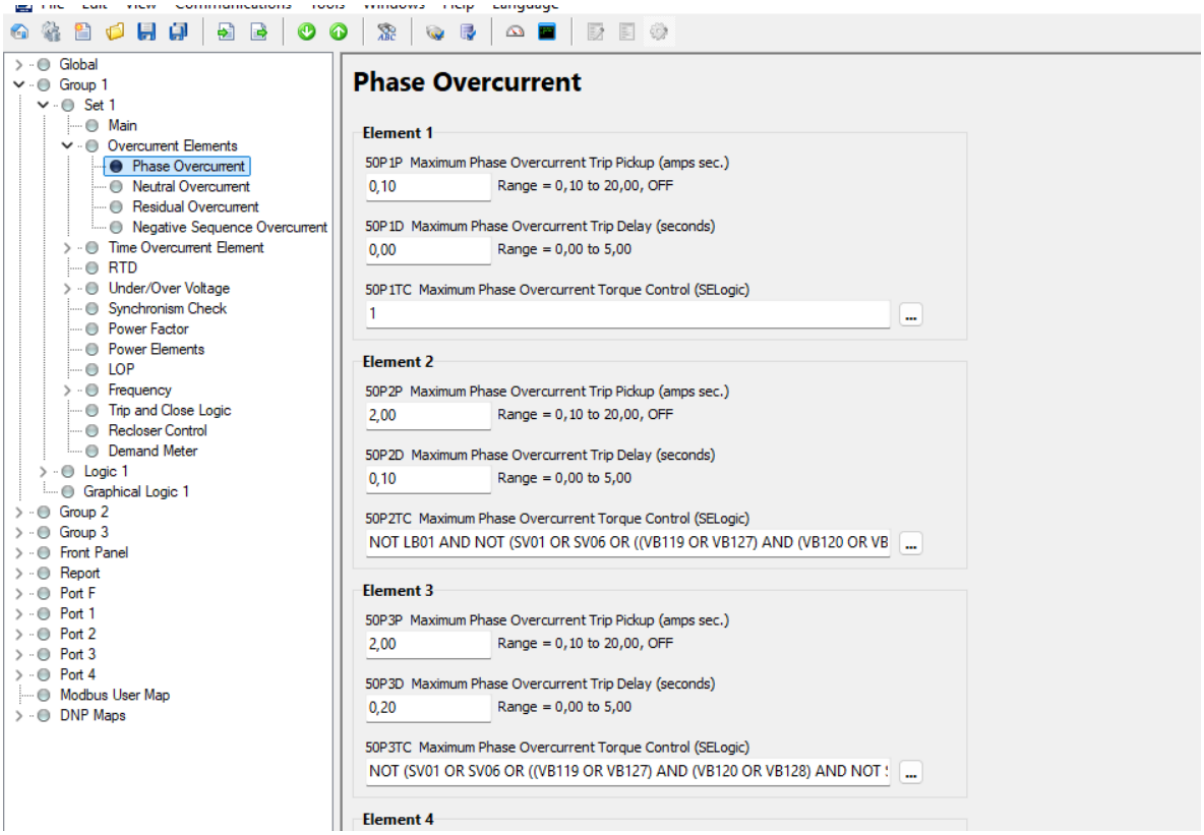


Figure 3.11: Overcurrent setting

3.7.4. BREAKER FAILURE (ANSI 50BF)

This IED element serves as an immediate response mechanism activated when a circuit breaker fails to isolate the fault. Breaker failure protection represents an essential functionality within Intelligent Electronic Devices (IEDs), generally initiated by a timer following the issuance of a tripping signal. The device monitors the current flowing through the CB, activating a secondary trip signal then tripping adjacent feeder circuit breakers for isolating the faulty sections of the circuit within a time frame of 120 to 200 milliseconds. An IED specifically designed for breaker fail protection can integrate control and monitoring functions, including supervision of ambient temperature and gas pressure. The IEC 61850 protocol facilitates the rapid, dependable, and secure transmission of GOOSE messages across substation LANs. This component is designed to activate the busbar protection scheme, facilitating rapid tripping following the predetermined timer settings. This developed protection logic incorporates the function with the reverse busbar blocking scheme. A fast bus-stripping scheme, known reverse busbar blocking, is designed to minimise the fault clearing time in the

substation. Faults on the busbar are cleared within a critical timeframe due fault level, severity of the potential damage and to prevent system instability. The bus IED, positioned at the apex of the substation hierarchy, interfaces with each IED linked to the feeders, thereby preventing unnecessary tripping during a fault condition. This inter-IED communication system facilitates efficient communication and safeguards operations during fault conditions.

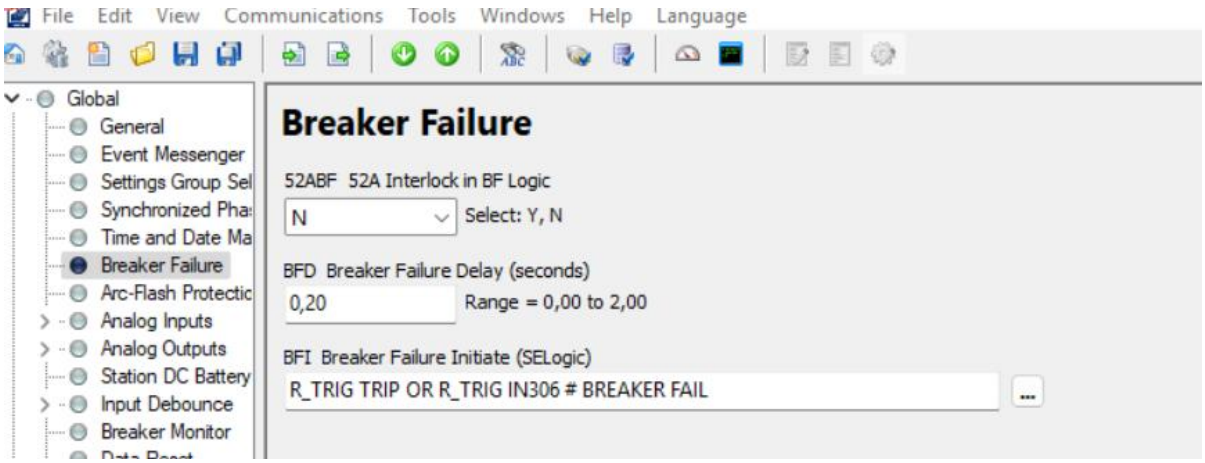


Figure 3.12: Breaker Failure

3.7.5. ARC FLASH PROTECTION

Arc flash has the potential to result in a massive failure of non-Arc Contained high voltage apparatus, thereby presenting a safety hazard for personnel, equipment and a threat to continuity of supply. Incorporation and testing of this function for switchgear is essential from both statutory and regulatory viewpoints. Conventional relays, responsible for coordinating between high voltage incomers and feeder Intelligent Electronic Devices (IEDs), exhibit slower response times in clearing arc flash faults when compared to digital IEDs that utilise GOOSE based protection mechanisms. Conventional protection systems exhibit the so called "blind spots" in busbar protection, resulting in potential switchboard failures. The GOOSE method provides benefits including minimised wiring, enhanced communication flexibility, and increased operational speed, which may result in cost efficiencies for maintenance teams. GOOSE frames operate with high sensitivity, transmitting status, control, and measurement data to IEDs that manage and execute tripping actions as required. This capability enables operators to block GOOSE frames during maintenance operations, providing adaptability during protection testing.

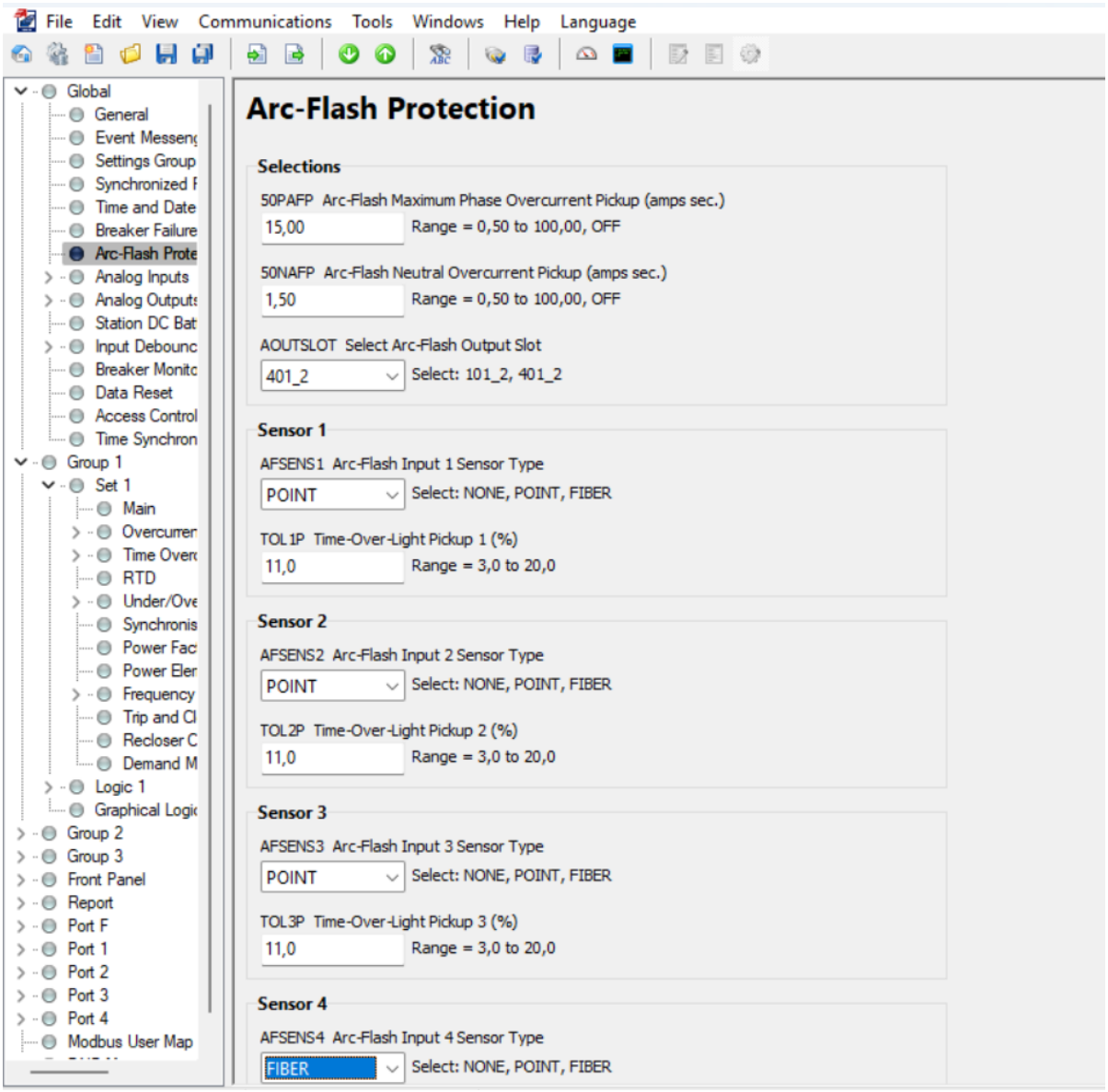


Figure 3.13: Arc Flash

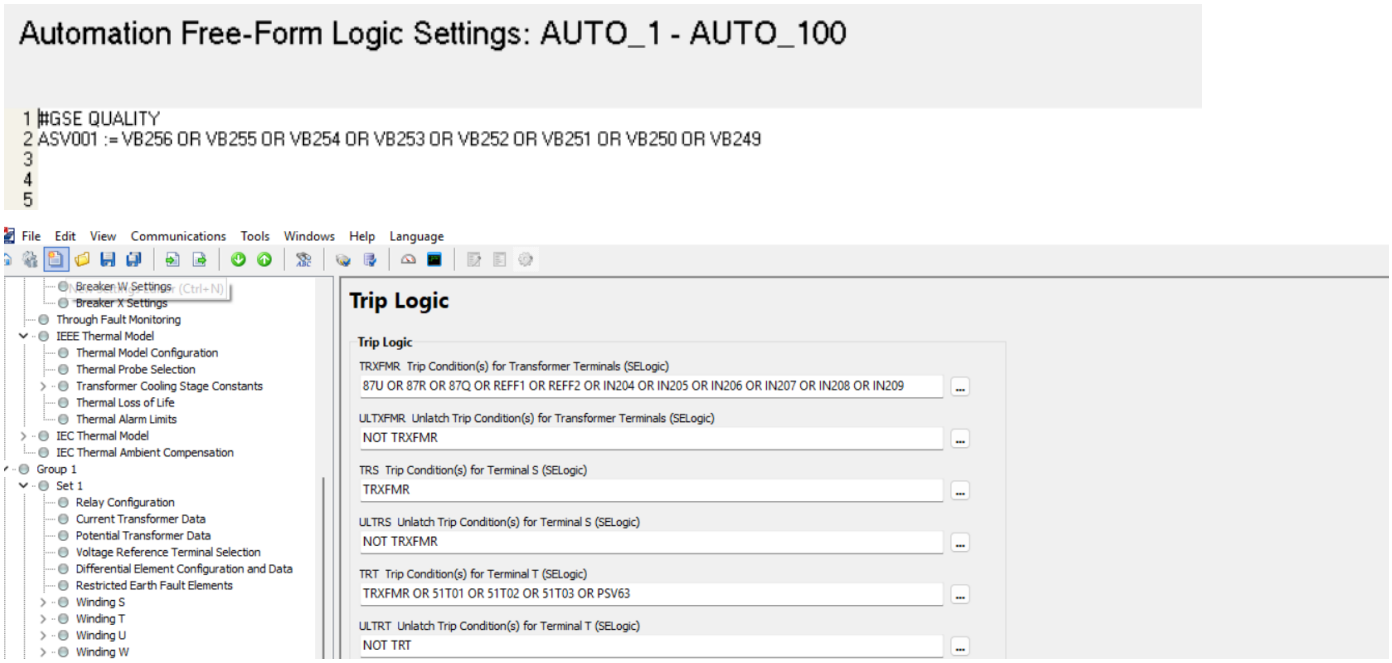
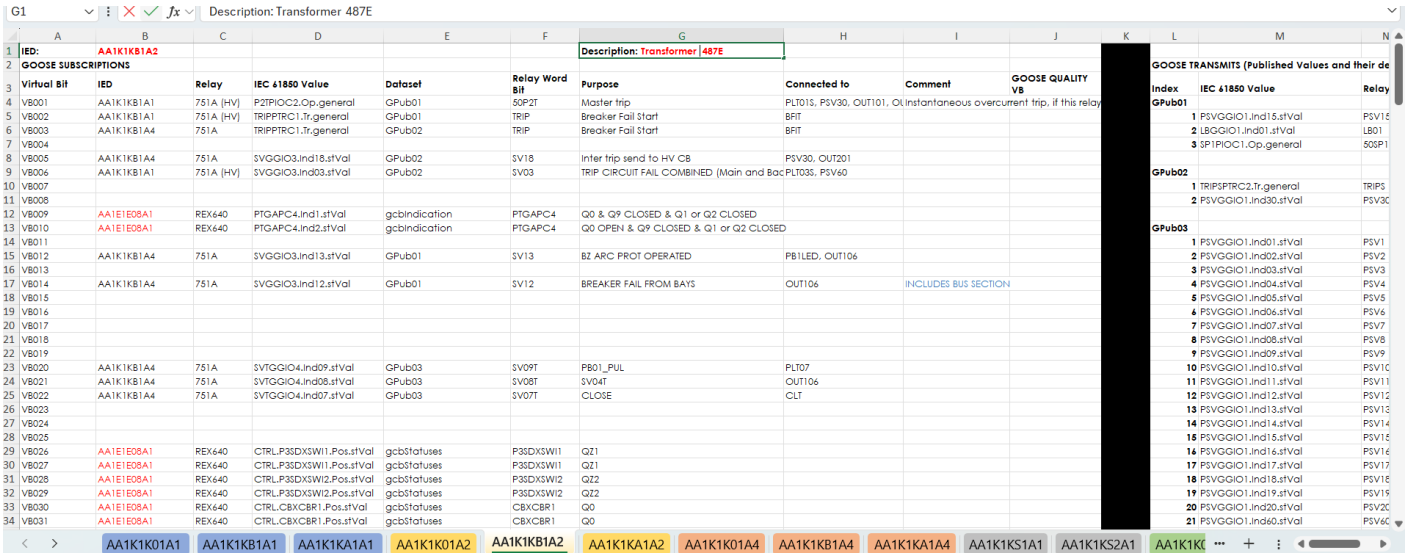


Figure 3.14: Automation logic

Table 3-1: GOOSE MESSAGING SCHEDULE

GOOSE MESSAGING SCHEDULE		
From	To	Signal
SEL- 487E	SEL- 411L (LOCAL)	LV CB FAIL + TRFR TRIPS
SEL- 411L (LOCAL)	SEL- 487E	LV CLOSE BLOCK
SEL- 411L (LOCAL)	SEL- 487E	TRIP CIRCUIT SUPERVISION
SEL- 411L (LOCAL)	SEL- 411L (REMOTE)	LV CB FAIL + TRFR TRIPS
SEL- 411L (REMOTE)	SEL- 411L (LOCAL)	LV CLOSE BLOCK



IED:	AA1K1KB1A2					Description: Transformer 487E						
GOOSE SUBSCRIPTIONS											GOOSE TRANSMITS (Published Values and their de	
Virtual Bit	IED	Relay	IEC 61850 Value	Dataset	Relay Word Bit	Purpose	Connected to	Comment	GOOSE QUALITY VB		Index	IEC 61850 Value	Relay
VB001	AA1K1KB1A1	751A (HV)	P2TPIOC2.Op.general	GPub01	50P2T	Master trip	PLT01S, PSV30, OUT101, OU	Instantaneous overcurrent trip, if this relay			GPub01		
VB002	AA1K1KB1A1	751A (HV)	TRIPPTRC1.Tr.general	GPub01	TRIP	Breaker Fail Start	BFIT				1	PSVGGIO1.Ind15.stVal	PSV15
VB003	AA1K1KB1A4	751A	TRIPPTRC1.Tr.general	GPub02	TRIP	Breaker Fail Start	BFIT				2	LBGGIO1.Ind01.stVal	LB01
VB004											3	SP1PIOC1.Op.general	50SP1
VB005	AA1K1KB1A4	751A	SVGGIO3.Ind18.stVal	GPub02	SV18	Inter trip send to HV CB	PSV30, OUT201				GPub02		
VB006	AA1K1KB1A1	751A (HV)	SVGGIO3.Ind03.stVal	GPub02	SV03	TRIP CIRCUIT FAIL COMBINED (Main and Bac	PLT03S, PSV60				1	TRIPSPTRC2.Tr.general	TRIPS
VB007											2	PSVGGIO1.Ind30.stVal	PSV30
VB008													
VB009	AA1E1E08A1	REX640	PTGAPC4.Ind1.stVal	gcbIndication	PTGAPC4	Q0 & Q9 CLOSED & Q1 or Q2 CLOSED					GPub03		
VB010	AA1E1E08A1	REX640	PTGAPC4.Ind2.stVal	gcbIndication	PTGAPC4	Q0 OPEN & Q9 CLOSED & Q1 or Q2 CLOSED					1	PSVGGIO1.Ind01.stVal	PSV1
VB011											2	PSVGGIO1.Ind02.stVal	PSV2
VB012	AA1K1KB1A4	751A	SVGGIO3.Ind13.stVal	GPub01	SV13	BZ ARC PROT OPERATED	PB1LED, OUT106				3	PSVGGIO1.Ind03.stVal	PSV3
VB013											4	PSVGGIO1.Ind04.stVal	PSV4
VB014	AA1K1KB1A4	751A	SVGGIO3.Ind12.stVal	GPub01	SV12	BREAKER FAIL FROM BAYS	OUT106	INCLUDES BUS SECTION			5	PSVGGIO1.Ind05.stVal	PSV5
VB015											6	PSVGGIO1.Ind06.stVal	PSV6
VB016											7	PSVGGIO1.Ind07.stVal	PSV7
VB017											8	PSVGGIO1.Ind08.stVal	PSV8
VB018											9	PSVGGIO1.Ind09.stVal	PSV9
VB019											10	PSVGGIO1.Ind10.stVal	PSV10
VB020	AA1K1KB1A4	751A	SVTGGIO4.Ind09.stVal	GPub03	SV09T	PB01_PUL	PLT07				11	PSVGGIO1.Ind11.stVal	PSV11
VB021	AA1K1KB1A4	751A	SVTGGIO4.Ind08.stVal	GPub03	SV08T	SV04T	OUT106				12	PSVGGIO1.Ind12.stVal	PSV12
VB022	AA1K1KB1A4	751A	SVTGGIO4.Ind07.stVal	GPub03	SV07T	CLOSE	CLT				13	PSVGGIO1.Ind13.stVal	PSV13
VB023											14	PSVGGIO1.Ind14.stVal	PSV14
VB024											15	PSVGGIO1.Ind15.stVal	PSV15
VB025											16	PSVGGIO1.Ind16.stVal	PSV16
VB026	AA1E1E08A1	REX640	CTRL.P3SDXSWI1.Pos.stVal	gcbStatuses	P3SDXSWI1	QZ1					17	PSVGGIO1.Ind17.stVal	PSV17
VB027	AA1E1E08A1	REX640	CTRL.P3SDXSWI1.Pos.stVal	gcbStatuses	P3SDXSWI1	QZ1					18	PSVGGIO1.Ind18.stVal	PSV18
VB028	AA1E1E08A1	REX640	CTRL.P3SDXSWI2.Pos.stVal	gcbStatuses	P3SDXSWI2	QZ2					19	PSVGGIO1.Ind19.stVal	PSV19
VB029	AA1E1E08A1	REX640	CTRL.P3SDXSWI2.Pos.stVal	gcbStatuses	P3SDXSWI2	QZ2					20	PSVGGIO1.Ind20.stVal	PSV20
VB030	AA1E1E08A1	REX640	CTRL.CBXCBR1.Pos.stVal	gcbStatuses	CBXCBR1	Q0					21	PSVGGIO1.Ind60.stVal	PSV60
VB031	AA1E1E08A1	REX640	CTRL.CBXCBR1.Pos.stVal	gcbStatuses	CBXCBR1	Q0							

AA1K1K01A1 | AA1K1KB1A1 | AA1K1KA1A1 | AA1K1K01A2 | AA1K1KB1A2 | AA1K1KA1A2 | AA1K1K01A4 | AA1K1KB1A4 | AA1K1KA1A4 | AA1K1KS1A1 | AA1K1KS2A1 | AA1K1K(

Figure 3.15: GOOSE subscription

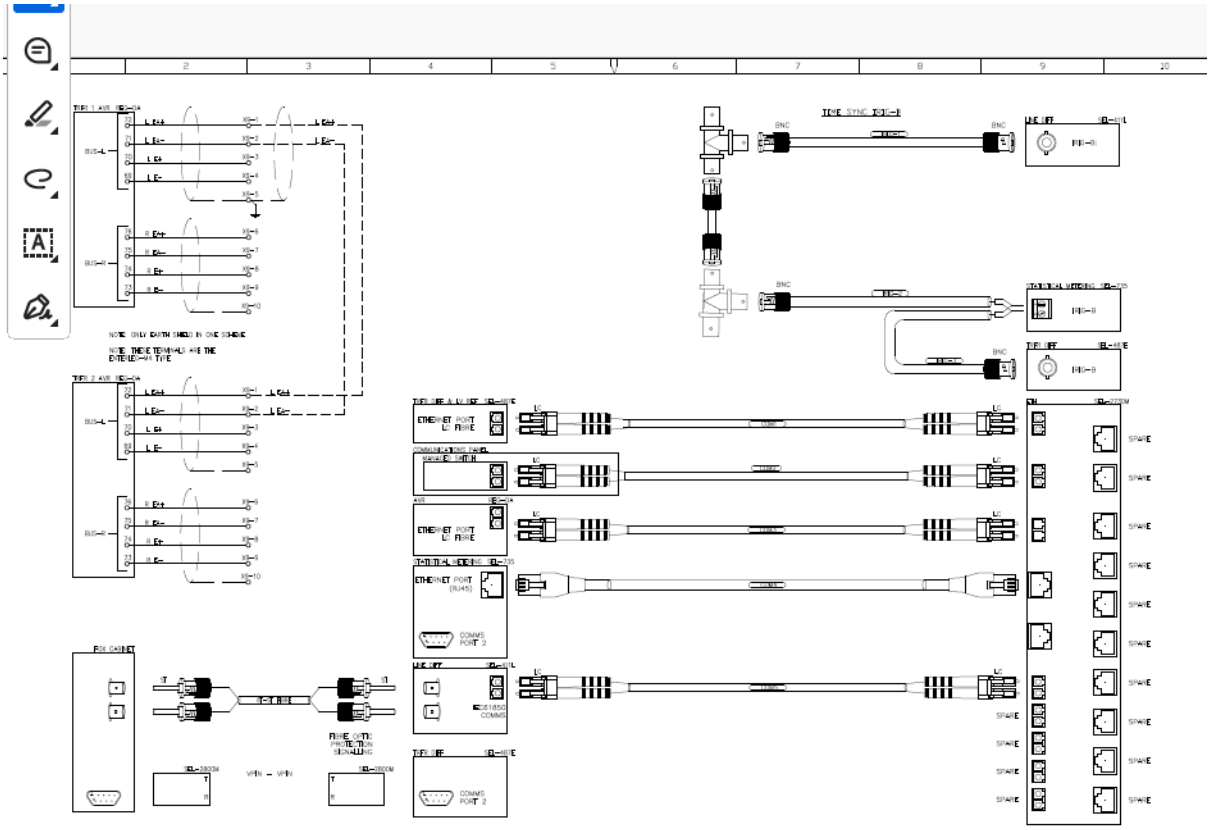


Figure 3.16: GOOSE cabling schedule

3.8. Testing substation protection

IED, whether antiquated or contemporary, are afforded a specific critical duration before a pre-existing fault escalates to a point of detriment within a power system, necessitating its clearance. Consequently, this essential element of safeguarding must be taken into account to guarantee that the protection functions as intended and within a specified timeframe. In a traditional legacy substation, voltages and currents can be produced by a test set during a primary or secondary injection test. By examining the configurations, one can more readily assess the timing and duration of a relay's trip response issuance. The notion of secondary injection protection testing was visually represented in Figure 3.17.

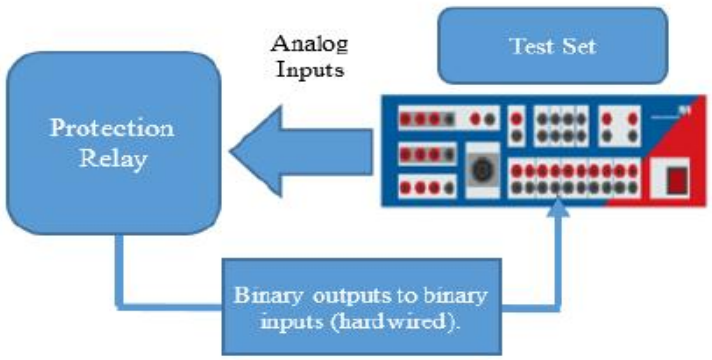


Figure 3.17: Conventional substation protection

Furthermore, within a substation that adheres to the IEC 61850 standard, utilising SV GOOSE messages for data and information exchange, the identical testing procedure may be applied. The sole distinction lies in the fact that the communication among the IEDs and the CMC 365 occurs via the LAN of the substation through the ethernet switch. The test set depicted in Figure 3.17 produces sampled value messages that encapsulate the currents and voltages sampled by the CT and VT respectively. The simulated data is then conveyed to the IED. The Intelligent Electronic Device (IED) must respond suitably by relaying the pertinent GOOSE messages to the testing apparatus, which may encompass indications such as circuit breaker trips, reclosing, or status updates. The testing apparatus possesses the ability to emulate GOOSE messages, encompassing those related to breaker status and reclosing, and subsequently transmits this data back to the IED to assess whether the appropriate response or data has been accurately captured. An illustration of this testing methodology is depicted

in Figure 3.18, showcasing a secondary injection protection test within a substation network that adheres to IEC 61850 standards.

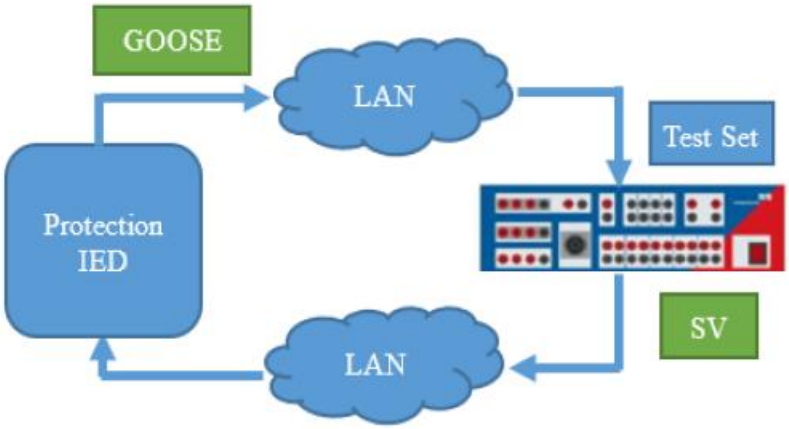


Figure 3.18: Protection testing via LAN

3.8.1. Data Collection and Analysis

The functionality of the improved transformer protection and experimental substation model, which complies with IEC 61850, was evaluated under differential stability, overcurrent, breaker failure, arc-flash, and reverse busbar blocking-based fault scenarios. Thus, the purpose of this study was to evaluate IEC 61850's GOOSE-based substation automation and transformer protection features. Fault conditions were applied to the system using omicron CMC 356 injection set so that device simulations and component responses could be recorded. The following elements were observed and evaluated in order to evaluate how well the IEC 61850 substation model operated: 3-phase currents, operating circumstances, and circuit breaker status, along with fault characteristics such as overcurrent blocking, arc flashes, and breaker failure. The results obtained were derived from the log events, process analyst, disturbance recordings, alarms, alerts, and visual trip indication from IEDs. The execution and functioning of GOOSE-based communication among devices necessitated an examination to assess the technical ramifications of the IEC 61850 standard on protection performance. The condition of breaker failure was examined by manipulating the relay feedback, specifically by setting the trigger output condition to zero or alternatively disconnecting the breaker coil circuit. The evaluation of arc flash protection involved the

utilisation of sensors and current monitoring by the transformer to guarantee an authentic trip response. Current supervision was meticulously modelled for all arc flash sensors, including CT, Circuit Breaker, Cable, and Busbar sensors.

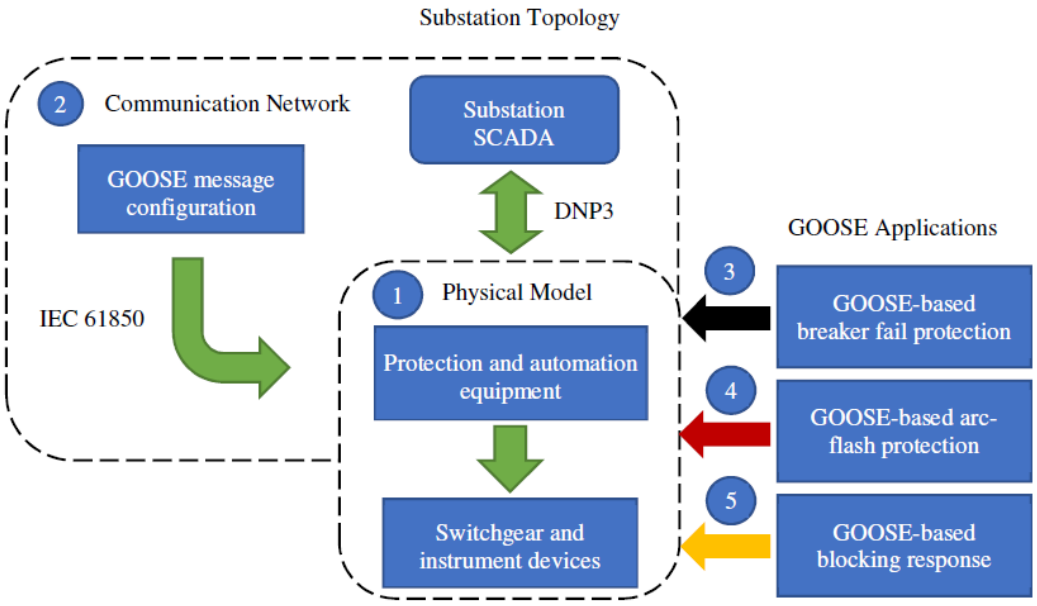


Figure 3.19: Substation topology block diagram

Testing methodologies for IEC 61850-based IEDs using CMC 356 involve a systematic approach to verify the IEDs' functionality and performance. This encompasses functional, performance, and conformance testing. Functional testing involves verifying that the IEDs perform their intended functions correctly, such as protection, control, and monitoring. This includes simulating various fault conditions and verifying that the IEDs respond appropriately. Performance testing focuses on evaluating the IEDs' performance under different operating conditions, such as varying load levels, communication delays, and network congestion. Conformance testing verifies that the IEDs adhere to the IEC 61850 standard's requirements, ensuring interoperability with other devices in the system. Functional testing is crucial for identifying errors in the configuration and wiring that may cause failures (Martens, 2023). Test automation framework streamlines the testing procedure, minimise human errors, and improve efficiency. It's crucial to focus on data integrity to avoid problems when using system characterisation.

3.8.2. Importance of Testing IEC 61850-Based IEDs

- **Verification of Correct Implementation:** Thorough testing verifies the correct implementation of the IEC 61850 standard in IEDs, validating their communication capabilities and assessing their performance under various operating conditions.
- **Identification of Potential Issues:** Testing can identify potential issues like incorrect data mapping, communication errors, or performance limitations, preventing malfunctions and ensuring seamless integration of IEDs from different vendors.
- **Confidence in Handling Network Conditions:** Comprehensive testing provides confidence in the IEDs' ability to handle various network conditions and maintain proper operation during disturbances.

3.8.3. Testing Methodologies

- **Systematic Approach:** Testing methodologies for IEC 61850-based IEDs using CMC 356 involve a systematic approach to verify the IEDs' functionality and performance.
- **Functional Testing:** Verifies that the IEDs perform their intended functions correctly, such as protection, control, and monitoring.
- **Performance Testing:** Evaluates the IEDs' performance under different operating conditions, such as varying load levels, communication delays, and network congestion.
- **Conformance Testing:** Verifies that the IEDs adhere to the IEC 61850 standard's requirements, ensuring interoperability with other devices in the system.

1. **Preparation:**
    - Ensure the CMC 356 test set is properly calibrated and configured.
    - Establish a connection between the CMC 356 and the IED under test.
    - Load the appropriate test templates or create custom test configurations based on the IED's fun1ctionality and the specific test requirements.

2. **Functional Testing:**

- Simulate various fault using the CMC 356.
- Verify that the IED responds correctly to each simulated fault, such as tripping a circuit breaker or sending an alarm signal.
- Evaluate the timing and accuracy of the IED's response.
- **Overcurrent Protection:** Simulate an overcurrent fault and verify that the IED trips the corresponding circuit breaker within the specified time.
- **Differential Protection:** Simulate an internal fault within a protected zone and verify that the IED trips the appropriate breakers while remaining stable for external faults.

3. **Performance Testing:**

- Assess the IED's performance under different operating conditions, such as varying load levels, communication delays, and network congestion.
- Measure parameters like response time, accuracy, and stability.
- Analyse the IED's behaviour under stress conditions to identify potential performance limitations.
- Communication Latency: Evaluate the impact of communication delays on the IED's performance.

4. **Conformance Testing:**

- Verify that the IED adheres to the IEC 61850 standard's requirements for communication protocols, data mapping, and interoperability.
- Use the CMC 356 to simulate different communication scenarios and verify that the IED correctly processes and responds to messages.
- **GOOSE Messaging:** Verify that the IED correctly publishes and subscribes to GOOSE messages.

- **MMS Communication:** Verify that the IED correctly implements the MMS protocol for data access and control.
- **SCL File Validation:** Ensure that the IED's SCL file conforms to the IEC 61850 standard.

Enhanced Efficiency and Reliability: Substation automation systems improve the efficiency and reliability of the power grid by enabling adaptive monitoring, control, and protection of critical equipment. Remote Accessibility and Business Continuity: The incorporation of information and communication technologies in industrial control system has led to replacement of legacy control systems with IP-based protocols, enhancing automation processes and remote accessibility.

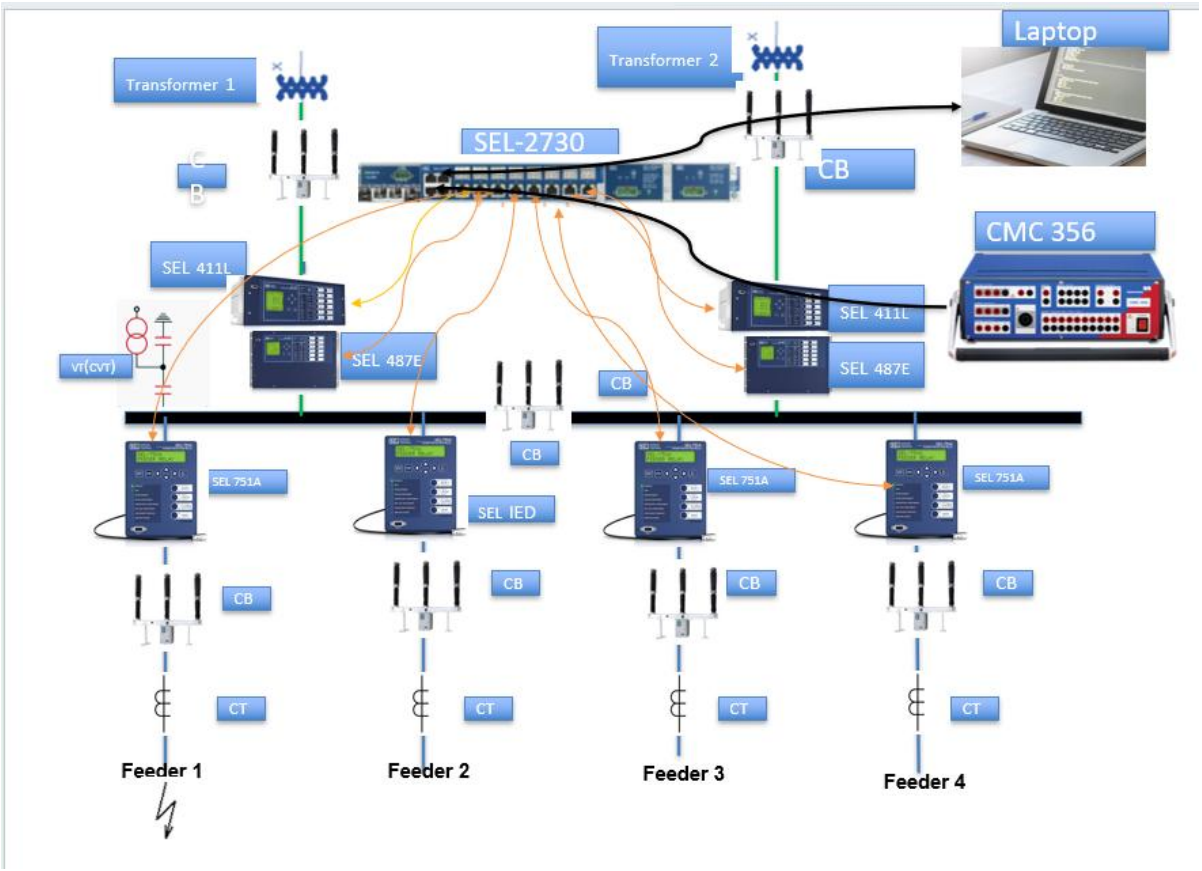


Figure 3.20: Modelled Substation

3.9. Conclusion

The protection, monitoring, automation, and control of substations fundamentally depend on the intricate intercommunication among IEDs and apparatus. The introduction of this novel communication standard has significantly influenced the methodologies by which data, signals, and functionalities are exchanged. Contemporary IEDs produced by firms such as SEL and Hitachi (formerly ABB), are engineered with this innovative protocol in consideration, enabling them to function collaboratively with other Intelligent Electronic Devices, irrespective of the manufacturer or vendor. Consequently, the conclusion of the era characterised by traditional protection systems and conventional substations has been reached. Despite advancements in technology. Within the simulated environment, the IEC 61850 protocol exhibits certain technical deficiencies such as cybersecurity vulnerabilities, the necessity to evolve substation architecture, network reliant protection testing, which present emerging complexities. The ultimate standard delineated by the IEC articulates a singular protocol for the representation of diverse data elements within a substation. It aims to enhance the communication and interoperability among IEDs developed by various vendors, while also establishing a unified approach for information storage. The IEC 61850 standard delineates the fundamental services requisite for the transmission of data and signals, facilitating control between Intelligent Electronic Devices (IEDs) and a central control unit or Human-Machine Interface. Ultimately, the evaluation of electrical apparatus and the assessment of protective scheme within the substation must adhere to the stipulations of the IEC 61850 protocol. This facilitates a more streamlined and effective approach to the assessment and verification of equipment functionality. Upon examining the IEC 61850 based protection in relation to protocol in relation to conventional hardwired based protection, the advantages become distinctly apparent. It is evident that the recently established IEC 61850 Ethernet-based protocol represents a significant advancement in the communication among IEDs, other devices, facilitating information and data transfer, signalling, control, protection, and automation within the substation LAN.

CHAPTER FOUR:

4. System Design and Implementation

4.1. IEC 61850 Transformer Protection Modelling

The general power system automation dates to the early 1930's even though it was as unsophisticated as much. It facilitated basic functions like obtaining plant statuses and issuing control commands remotely through centralised scheme. RTUs (Remote terminal units) were later introduced around the 1960's in the electrical power systems framework enhancing bandwidth, rate of data transfers, through digital communication to control centres and back. UCA was designed and modelled in the late 1980's the consisting of fundamental definitions, data models, and protocols which essentially resulted in the development of IEC 61850 protocol. IEC 61850 is a highly complicated series of standards, in spite of its complexity the family of standards gained the momentum and become the global standard for multi-layered communications in power system substations. In addition to some of the related standards like IEC62351, some features of IEC 61850 will be covered in order to comprehend the security risks and mitigations. This standard consists of three function blocks or components of fundamental principles:

- logical Node.
- logical device,
- Physical device (IED or RTU or any devices in the field),

The physical device is the actual component installed physically on site like an IED (Intelligent Electronic Device) where the logical devices are contained in. the logical device interacts with process variables (Voltage, Power, current, etc) through its inputs or outputs or ports communication with the centralised control centre. The logical components are inserted into the physical device. Logical device depicts a unit, or functional blocks modelled to perform a particular high-level application such as measurement, control, protection, monitoring, processing report, etc. Logical nodes are contained in the logical device and are connected specifically for intended functionality to achieve desired operation. The logical node is referred to as the atomic unit and heart of the IEC 61850 standard. Power systems control, protection, measurement and automation function are developed from the logical nodes. Logical nodes vary as per product manufacture internal algorithms but the data to be transferred has to be strictly monitored to allow the desired interoperability, which is the fundamental purpose of

IEC 61850 standard. The typical representation of the logical nodes, logical devices, and physical devices is shown below.

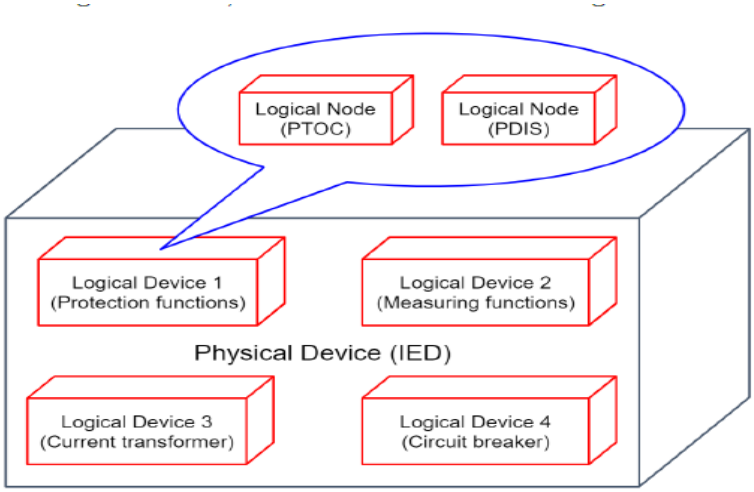


Figure 4.1: Logical node, logical and Physical device (Francisco DE Lima ,2024)

As earlier mentioned, logical nodes are modelled for specific desired operation mostly denoted by the first letter for example logical nodes for measurements and metering begins with “M”, automation control “A”, switchgear “X”, supervisory control “C”, protection “P”, interfacing “I”, sensors “S” system logical nodes “L”, etc. Logical nodes can contain more than one elements of data with each element having its unique name. Every logical node prefix or suffix will be denoted as LN (LN-instance-ID) to further identify the function or intended purpose of the particular logical node for instance CB (circuit breaker). Circuit breaker is configured as XCBR logical node, data inside circuit breaker logical node includes variety of data such as Loc for local (to distinguish if operation is local or remote), BlkOpn for blocking open commands, CBOpCap for operating capabilities of the breaker. Each element of data contained in the logical node complies with the required specification of common data class (CDC) as per IEC 61850-7-3 standard. CDC represents the structure and type of the data contained in the logical node. The are CDCs for various functions such as measured information, status information, analog set point information and controllable status information. These data common data classes have defined names and group of attributes each with name , type and purpose that are defined. Every attribute set is a member of a set of functional constraints (FC) that categorises the group of attributes for instance Single Point

Status (SPS) common data class, status attributes (ST), time stamp (t) and description attributes (DC).

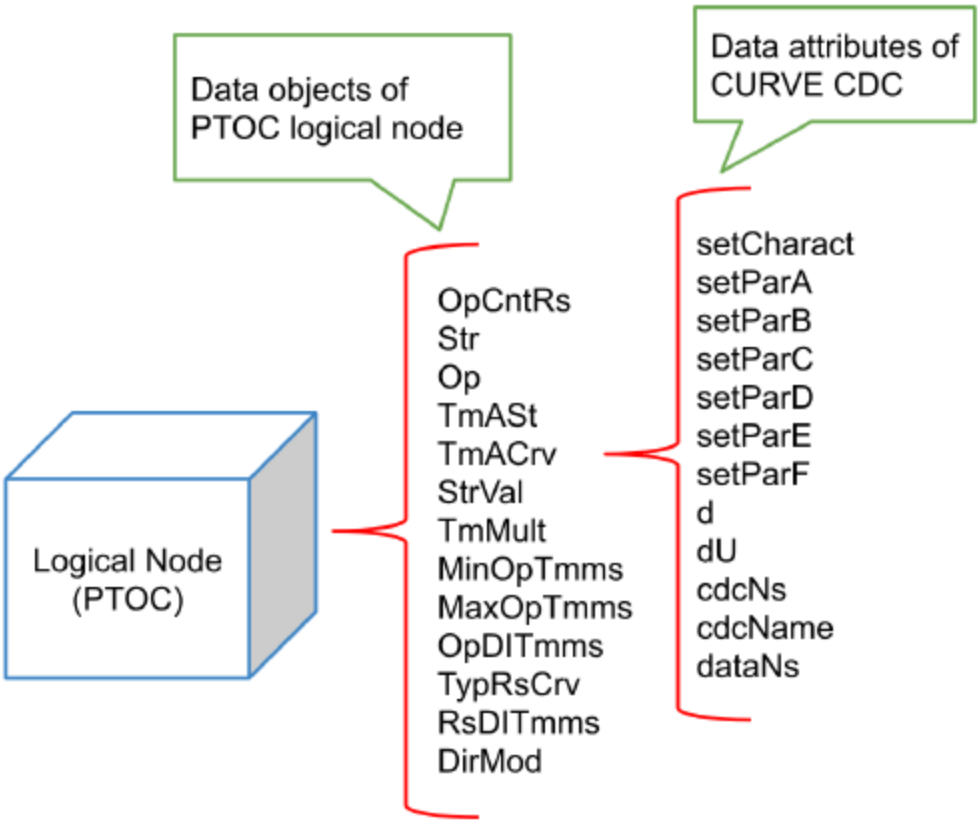


Figure 4.2: DATA Attributes and Objects (IEC 61850-7-3, 2023)

A specific Common Data Class (CDC) is linked to each Data Object (DO), which is a piece of information that allows each logical node to be interfaced through it. One of the IEC 61850 standard's primary advantages is that these CDC are not dependent on any underlying protocol. The IEC 61850 standard includes an ecosystem of publications that define substation and protection systems. The System Specification Description (SSD), IED Capability Description (ICD), Configured IED Description (CID), and Substation Configuration Description (SCD) files are written in the Substation Configuration Language (SCL), which is a digital substation represented in XML. The architecture configuration of an IEC 61850 based substation comprises of 3 information levels in the communication hierarchy (substation, process, and bay) and 2 network buses as shown in figure 4.3.

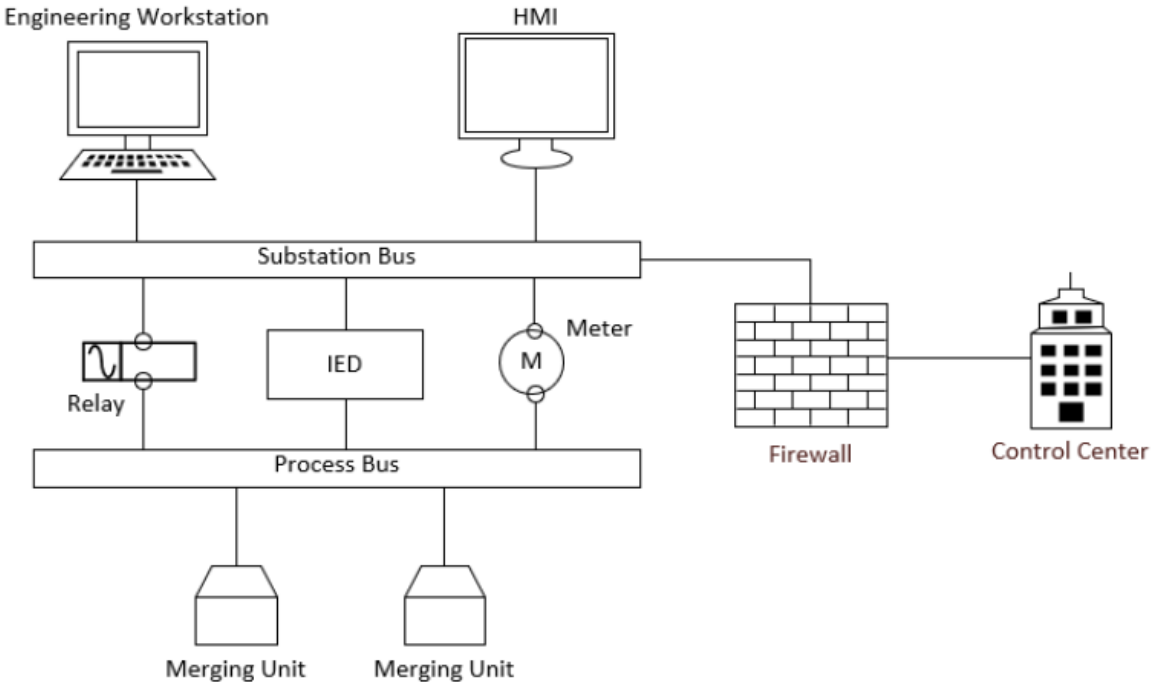


Figure 4.3: IEC 61850 Layout (O'Raw, John (2020))

- Substation level: information exchange between substation and SCADA control centre (transfer and receive). It serves as a gateway between substation and remote HMI.
- Process level: where the signal acquisition of voltage/current occurs. This is the lowest level where the direct interaction with the secondary voltage and secondary current takes place, interfacing the physical system and capturing the process variables. These values are sent through the SV protocol to the upstream protection device.
- Bay level: Actual main measurements and protection functions. The IEDs horizontally transfer/receive data on this level through GOOSE protocol.

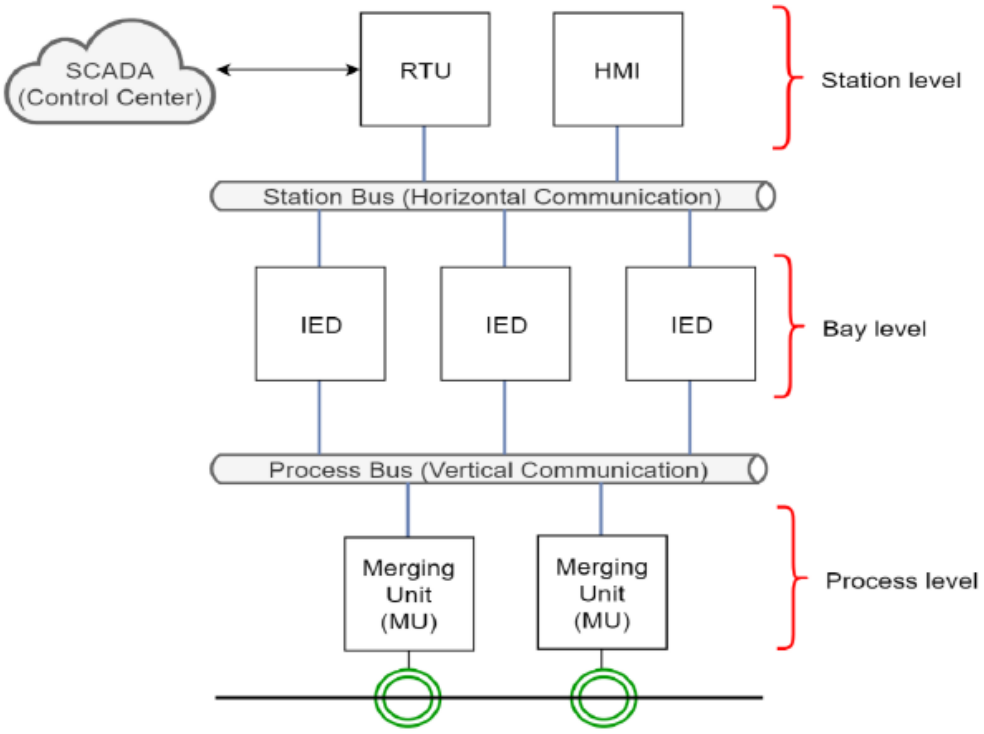


Figure 4.4: Network Architecture (IEC 61850-5, 2023)

On the process and bay level, the connection between IEDs is through process bus, while on the bay and station level the IEDs exchange information through station bus. The standard IEC 61850 system design is shown in Figure 4.4 Communication between the gateway remote terminal unit, and the control centre may utilise common application layer protocols include DNP3, MODBUS, and IEC60870, etc. The IEC 61850 standard communication topology uses TCP/IP and Ethernet within the substation to facilitate communication between IEDs. An IED comprises of specialised interface, software, and hardware based on microprocessor controller with the ability to exchange data with an external source. At the substation level, a workstation function is usually required for engineering and configuration. External communication to the utility's control centre may now be available via routers, firewalls, and VPN technologies. This standard enables the three levels to be linked through a single switch or more for security and redundancy. Fibre connections between switches or redundant connections between end nodes and two switches is configured in a star or ring architecture.

Five communication protocols utilised in this design.

- **ACSI** (Abstract Communication Service Interface)- defines MMS/ GOOSE/SV behaviour.
- Time synchronisation through Ethernet or UDP: IEEE 1588 PTP for process-level determinism; SNTP/NTP adequate for station-level correlation.
- **SV/SMV** (Sampled 'Measured' Value): time-critical analog measurements on the process bus
- **GOOSE** (Generic Object-Oriented Substation Event) - fast peer-to-peer messaging of events and status (Trip, Interlock, Breaker Failure) over layer-2 VLAN.
- **MMS** (Manufacturing Message Specification): Client-Server supervision, reports, parameter access.

4.2. Theoretical Framework

The modernisation of electrical substations with IEC 61850-compliant systems represents a paradigm shift in power system protection, control, and automation (Hakala-Ranta, 2024). This transition facilitates enhanced interoperability, improved data integration, and the implementation of advanced protection schemes, ultimately bolstering power security and grid resilience. Legacy substation architectures often rely on proprietary communication protocols, hindering seamless integration of devices from different vendors and limiting the ability to implement sophisticated, coordinated protection strategies. IEC 61850, as an open and standardised communication protocol, addresses these limitations by providing a common language for intelligent electronic devices within the substation, thereby enabling instant data exchange and advanced control functionalities (Huang, 2023). The adoption of IEC 61850 enables faster and more reliable transformer protection schemes through GOOSE messaging, enhancing the speed and dependability of critical protection functions (Krishnamurthy, 2022).

4.2.1. IEC 61850 Standard Overview

IEC 61850 represents a globally recognised standard that delineates communication protocols for IEDs utilised within electrical substations (Süfke, 2021). This standard (Protocol)

presents a uniform methodology for substation automation, facilitating seamless interoperability among devices produced by various manufacturers (Wang, 2023). It is particularly relevant in modernising electrical substations because it facilitates enhanced data exchange, communication, and advanced protection schemes, which are crucial for improving the reliability, security, and efficiency of power grids.

4.2.2. Substation Upgrade Requirements

Upgrading a substation to be IEC 61850-compliant involves a detailed assessment of existing infrastructure, communication requirements, and protection schemes. The upgrade process begins with a comprehensive evaluation of the existing substation infrastructure to determine the scope of the upgrade, which includes assessing the current protection schemes, communication networks, and control system. This assessment identifies potential bottlenecks, outdated equipment, and areas that require modernisation to meet the new IEC 61850 standards. Selecting appropriate IEC 61850-compliant devices, such as protection relays, MUs, and IEDs is also important, ensuring interoperability and adherence to the standard (Parikh, 2022). The integration of these devices requires careful planning to ensure seamless communication and data exchange across the substation network. Furthermore, robust cybersecurity measures are essential to protect the upgraded substation from cyber threats.

4.2.3. Transformer Protection enhancement

Transformer protection is a critical aspect of substation operation, and IEC 61850-based systems offer significant improvements over traditional protection schemes. IEC 61850 enhances transformer protection through the implementation of advanced protection functions and improved communication capabilities. GOOSE messaging facilitates real-time, direct peer-to-peer communication among the IEDs, enabling fast and reliable tripping decisions, which allows the implementation of advanced protection scheme like adaptive protection and bay-to-bay protection, which improve the sensitivity and selectivity of transformer protection. Implementing differential protection schemes based on IEC 61850 allows for precise and rapid detection of internal transformer faults, minimising damage and downtime. Furthermore, integrating temperature monitoring and dissolved gas analysis data through IEC 61850 provides a detailed monitoring of the transformer's condition, enabling proactive maintenance and preventing catastrophic failures.

The incorporation of operational technology systems and information technology within modernised substations inevitably introduces cybersecurity exposures, demanding an advanced comprehensive and dynamic approach to risk mitigation. Industrial control systems are essential for modern society's operations, but their designs prioritise reliability and safety over cybersecurity, resulting in vulnerabilities. Traditionally, industrial control systems operated in isolated environments, physically segregated from broader IT networks, which inherently limited their exposure to cyber threats; however, the escalating adoption of the Internet of Things and the convergence of IT and OT domains have interconnected industrial control systems with the internet, substantially broadening the attack surface (Abosata, 2021). Consequently, a multi-faceted cybersecurity strategy is paramount, encompassing network segmentation, intrusion detection systems, rigorous access control and ceaseless security monitoring to safeguard critical substation assets and ensure operational resilience (Pan.Q, 2023). The seamless integration of IT and OT systems, while beneficial, introduces new vulnerabilities and challenges, making it crucial to address security concerns in critical infrastructures (Ara, 2022). The convergence of IT and OT necessitates robust cyber-security control techniques to protect critical infrastructure from evolving cyber threats.

4.2.4. Power Security Considerations

The significance of power security in contemporary substations cannot be overstated, and the IEC 61850 standard is instrumental in fortifying the overall security framework of the grid. The implementation of role-based access control and authentication mechanisms guarantees that only individuals with the appropriate authorisation can engage with essential substation functions and data, thereby reducing the likelihood of unauthorised access and nefarious activities. Encrypted and secure communication protocols serve to protect sensitive data exchanged between IEDs and control centers, against data manipulation. The deployment of anomaly detection systems utilising machine learning algorithms facilitates the identification of atypical patterns and prospective cyber threats, thereby allowing for preemptive security strategies. Regularly performing security audits and vulnerability assessments is crucial for uncovering and addressing potential deficiencies in the substation's security infrastructure. thereby fostering ongoing enhancement and fortification against emerging threats. Upgrading substations with IEC 61850-based systems offers significant advantages in terms of enhanced transformer protection and power security. IEC 61850-based substation upgrades

represent a significant advancement in power system technology, offering enhanced transformer protection, improved power security, and greater operational efficiency.

4.3. Enhanced Protection

4.3.1. General description

Modern day life activities heavily rely on reliable electric energy system to an extent that most fields require nearly a seamless operation of power systems. Power transformer is extremely costly and an essential apparatus of the electrical network. As the transformer is crucial for the operation of the Grid, it is critical to mitigate abnormal operations. This minimises the duration and limits the frequent occurrence of unnecessary unintentional power outages. Power transformers replacement and repair lead times are lengthy, it is therefore of paramount importance to adequately protect the transformer. The transformer protection must function flawlessly, rapidly, reliably and seamlessly, this is directly correlated to power security and dependability. The power transformer protection can be classified into mechanical and electrical protection, (NANDA, 2023).

Technological advancements have enabled novel methods for improving the efficacy of transformer protection systems. The innovative techniques utilise the IEC 61850 GOOSE communication protocol and SEL487E IED. The utilisation of the state-of-the-art technologies offers significant improvements such as quicker fault detection, improved coordination, increased reliability in transformer protection employing current differential (Ntokozo, et al., 2024). Current differential-based protection is a commonly used approach to protect against internal transformer faults as it sensitive and faster. Traditional current differential scheme is effective but with the aid of advanced communication protocols the performance and reliability are significantly enhanced.

4.3.2. Electrical protection: Differential protection

Differential protection is a unit protection with its zone of operation delimited by position of current transformer. The operational principle is based on Kirchoff's current law, it functions on the summation of currents in its zone of protection. Differential protection relay computes the magnitudes and phase angles of all the currents entering and leaving the protected object.

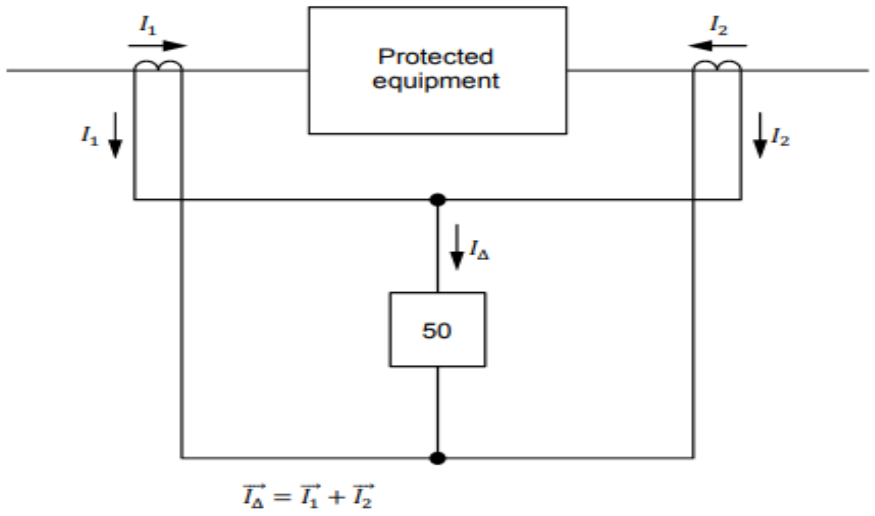


Figure 4.5: Generic operational equation *(Horowitz & Phadke, 2024)*

The generic equation is as follows:

$$\vec{I}_1 + \vec{I}_2 + \vec{I}_3 + \cdots + \vec{I}_n = 0A \tag{4.1}$$

Ideally during normal circumstances and through faults the resultant current should be zero (minimal) except for in zone fault. The differential protection has operating and restrain circuitry or calculation, depicted as follows.

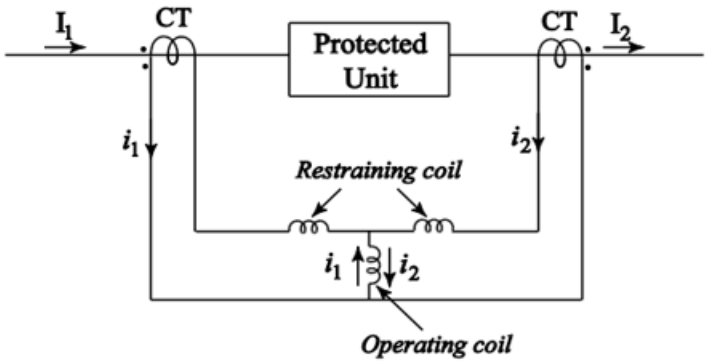


Figure 4.6: Differential relay *(Horowitz & Phadke, 2024)*

The differential current is calculated as:

$$I_d = |i_1 - i_2| \tag{4.2}$$

While the restrain current is calculated as:

$$I_r = \frac{|i_1 + i_2|}{2} \tag{4.3}$$

The relay will be stable when restrain current greater than differential current and operate when I_d is greater than I_r. These equations can be further modified as per manufacturer. When it comes to operational speed, sensitivity, and selectivity, the concept of differential protection is seen to be superior when compared to stepped distance, phase comparison, or directional comparison schemes, (Normann Fischer, 2024).

4.3.3. Percentage differential protection

Differential protection comprises of slope characteristics, it uses dual slope characteristics for maximum security for external faults and sensitivity for in zone faults. The dual slopes are available at different percentages, this is to prevent the relay from operating unnecessarily. Idmin (Ipu) is set at 0.3pu to cater for CT mismatch during normal network operation and magnetising current. This setting can be adjusted between 0.1-0.5 p.u depending on the network studies. Slope 1 caters differential stability during tap changer of nominal positions (Tap in progress). Then slope 2 cater for heavy trough faults and CT saturation (Bamber, et al., 2022).

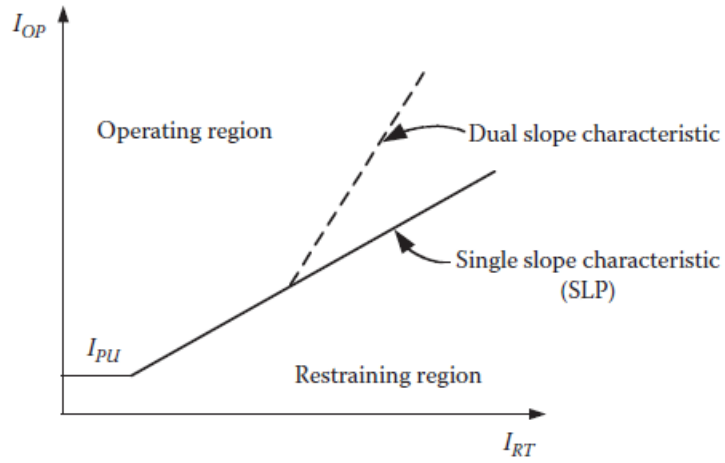


Figure 4.7: Differential curve (E Ali, 2024)

Slope Calculations

For SEL 487E the slope calculations are as follows:

$$Iop = k \times Slp \times Irt \tag{4.4}$$

$$Irt = |I_1| + |I_2| \tag{4.5}$$

$$Idiff = |I_1 + I_2| \tag{4.6}$$

Where:

k - design constant 1 for SEL487E

Slp - differential element characteristic slope

Irt - restrain current

Idiff - differential current

I_1 and I_2 - currents measured on the primary side and secondary side respectively.

4.4. Differential protection requirements

The application of transformer differential protection requires critical consideration of several factors that can affect the stability during normal network operation. These factors include CT mismatch, ratio, magnetising inrush currents, Phase shift between primary and secondary winding, and possible over fluxing. In Electromagnetic differential protection relay scheme and traditional relay required interposing CT on secondary winding (CT/ICT). If the transformer is delta-star the CT connection would be star-delta to counter for introduction of the phase shift, this is called primary compensation. This interposing connection eliminates zero currents circulation. Digital IEDs does the phase shift and ratio correction on the software /configuration irrespective of the CT connection. This saves the time and costs of replacing the installed CTs on the plant (Onah, 2021).

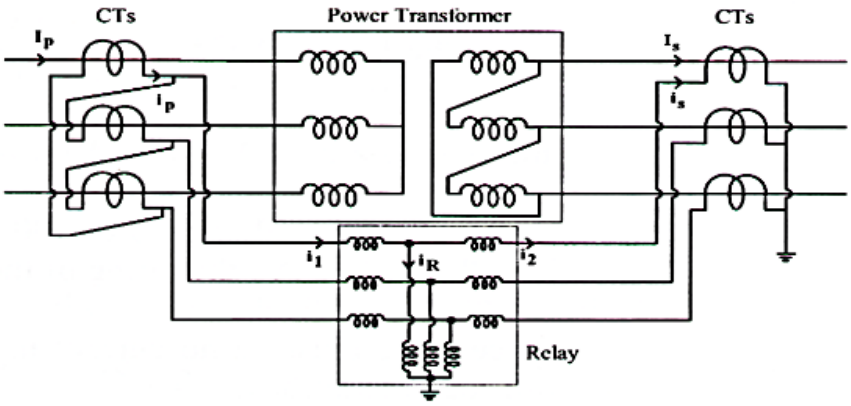


Figure 4.8: Interposing current transformer (Horowitz & Phadke, 2024)

4.4.1. Ratio correction

Power transformers are primarily designed for stepping up or stepping down voltage levels; therefore, the primary winding and the secondary winding are often at different voltage levels. This difference in voltage levels result in different currents flowing in the windings

.

$$\frac{v_1}{v_2} = \frac{I_2}{I_1} = \frac{N_1}{N_2} \tag{4.7}$$

The CTs installed on the primary and secondary winding will be different in ratio rating. This will cause the differential current to be non-zero and flows through the protective device under normal load conditions or through fault resulting false tripping. Considering the power transformer 30MVA, 132/11kV Yd1, having CTs on primary 200/1 and on secondary 1800/1A.
Data: $V_{primary}$(HV) = 132kV, $V_{secondary}$(LV) = 11kV, S = 30MVA
Primary current

$$S = \sqrt{3} \times V \times I$$

$$S = \sqrt{3} \times V \times I_p$$

$$I_p = \frac{S}{\sqrt{3} \times V}$$

$$I_p = \frac{30000000}{\sqrt{3} \times 132000}$$

$$I_p = 131.22A$$

Secondary current

$$S = \sqrt{3} \times V \times I$$

$$S = \sqrt{3} \times V \times I_s$$

$$I_s = \frac{S}{\sqrt{3} \times V}$$

$$I_s = \frac{30000000}{\sqrt{3} \times 11000}$$

$$I_s = 1574.59A$$

Current to the relay

Ip= 131.22 / 200 = **0.656** and **I**s= 1574.59 / 1800 = **0.875.** Thus the differential current under the considered full load condition,

Idiff = Is - Ip = 0.875 - 0.656 = **0.219**

This would trip for a setting of 0.1- 0.2 differential current pick up even though it's not a faulty condition.this necessitates the ratio correction or compensation, and this is how it can be achieved:

HV side matching ration factor = CTR_{HV} / Ip = 200 / 131.22 = 1.524. it is also confirmed with the use of secondary values HV side matching ratio factor = CTR_{HV} / Ip = 1 / 0.656 = 1.524.

LV side matching ratio factor = CTR_{LV} / Ip = 1800 / 1574.59 = 1.143. it is also confirmed with the use of secondary values HV side matching ratio factor = CTR_{LV} / Ip = 1 / 0.875 = 1.143.

The diffential calculation in the relay will take into consideration the ratio correction factor, thus the formula now becomes;

$$Idiff = |I_1 + I_2| \quad (4.8)$$

$$Idiff = |I_1 * Rfhv + I_2 * Rflv| \quad (4.9)$$

$$Irt = |I_1| + |I_2| \quad (4.10)$$

$$Irt = |I_1 * Rfhv| + |I_2 * Rflv| \quad (4.11)$$

The ratio difference is fully compensated.

4.4.2. Off nominal tap positions

Mismatch factor for tap changer effect is calculated as follows:

$$M = 100 \left| \frac{\frac{I_{HV}}{I_{LV}} - \frac{T_{HV}}{T_{LV}}}{S} \right| \quad (4.12)$$

Relay taps $T_{HV} = 1, T_{LV} = 2$

$M = 100 \left| \frac{\frac{0.656}{0.875} - \frac{1}{2}}{0.5} \right|$ *+10%*

Where:

$I_H = High\ Side\ Current$

$I_L = Low\ Side\ Current$

$T_H = High\ Side\ Tap$

$T_L = Low\ Side\ Tap$

$S = Smaller\ Ratio\ of\ \frac{I_H}{I_L}\ \&\ \frac{T_H}{T_L}$

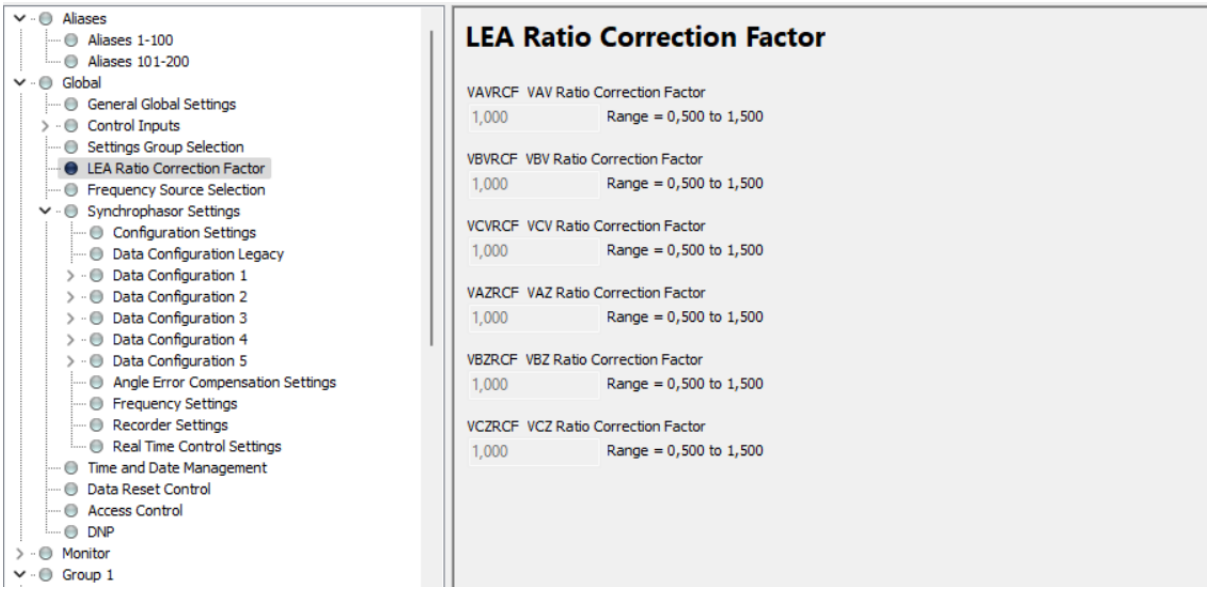


Figure 4.9: SEL 487E Ratio correction

4.4.3. Phase shift correction

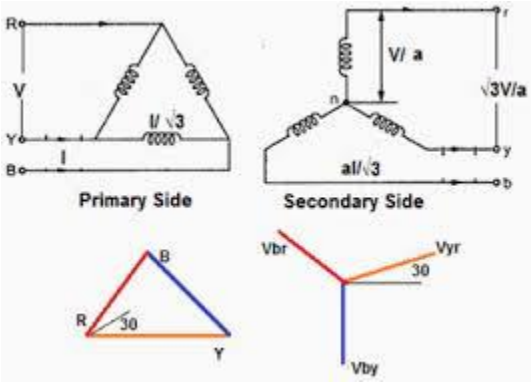


Figure 4.10: Dyn11 (Engineering portal,2021)

This vector group (Dyn11) results in phase shift of 30° that affects the differential stability. Phase shift correction is implemented on the IED.

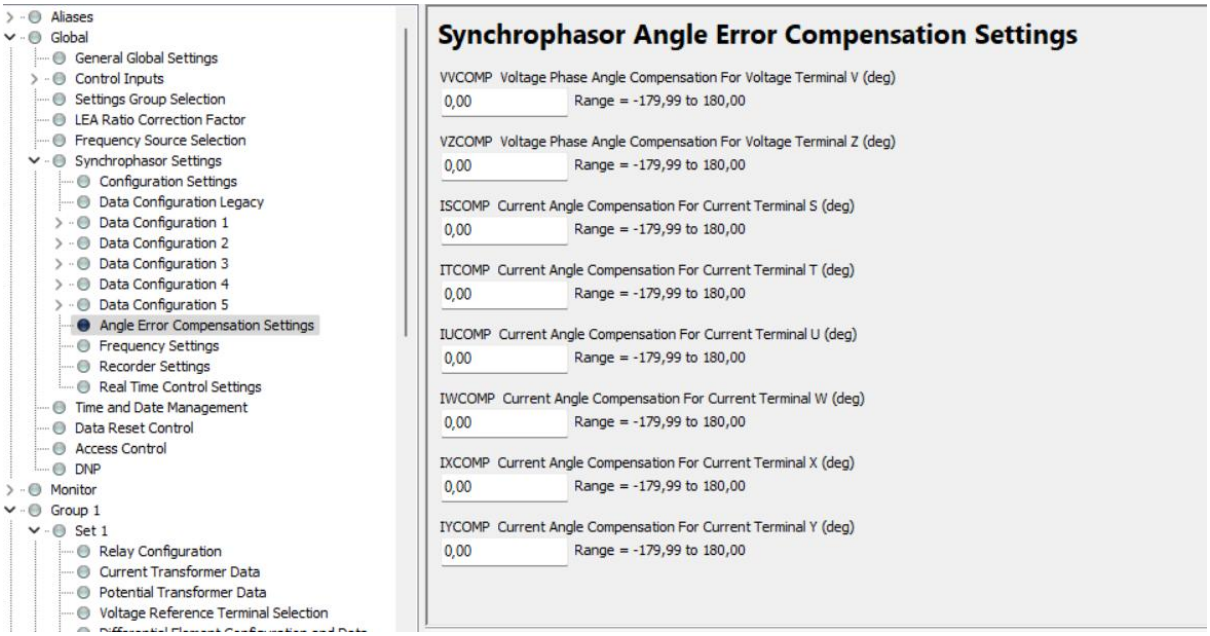


Figure 4.11: Phase shift correction

4.4.4. Blocking criteria for security

Transformer experiences inrush current during energisation at no load, this occurs when the steady state flux does not match with the residual flux at point on the voltage waveform (M. Jamali, 2021). The inrush current ranges between 10-100 times the rated current of the transformer. This often affects power quality and cause false tripping. The inrush currents drop to stead state conditions effectively in proportion with the winding resistance. This current is influenced by factors such as starting phase angle of voltage, residual flux in the core, saturation flux, core material, and source impedance. Magnetising inrush contains proportion of harmonics. Inrush currents can be categorised as follows.

- Energisation inrush
- Sympathetic inrush
- Recovery inrush

Energisation inrush occurs when the power transformer is being energised. Recovery inrush when the transformer is being restored after have system disturbance. Sympathetic inrush when adjacent transformer is being energised, and offsets inrush flows to the already energised transformer (Already in service). The inrush current can be reduced by controlling the switching time, this ensures that the nominal flux angle matches the supply voltage angle. Installation of point on wave relay enables the switching of voltage happens at maximum value as the flux lags by 90 degrees (Patel, 2023). The are other several methods to mitigate the effects of inrush current on protection stabilisation.

- Time delay - Applying time delay during energisation as the inrush will decay after energisation. This method is not advisable as it will delay tripping in the event of a genuine fault, and it is not effective on sympathetic inrush. This is not applied on the developed algorithm.
- Desensitise - comprises of an under-voltage relay with time delayed pick up and reset. This undervoltage relay is connected to the power transformer VT/CVT, it has contacts in that are in series with a resistor (low resistance) that shunt the tripping element of differential relay. The differential relay element will be desensitised during energisation period until the magnetising current decays. Under normal network conditions the undervoltage relay circuit is open thereby not bypassing the differential relay from operating. This method delays the tripping should a genuine switch on to fault occurs as the differential protection will be desensitised. Back-up or upstream protection will operate at the relevant time delayed response.

- Tripping suppressor: an improved desensitised method utilising three high speed control voltage relays. These relays are energised by ether line or phase-to-phase voltage. This method has dual blocking technique, for low magnetising inrush current the ‘a’ contact will be closed to delay the tripping and it does not delay for significantly high magnetising current. This method is crucial for high-speed relay that not selective between fault conditions and inrush currents.
- Gap detection technique: this technique detects the “gaps” in current waveform which are mainly present in the inrush current waveform due to the transformer core magnetisation process and not present in genuine fault currents. The detection of “gaps” prevents the protection from operating. The gap detection technique algorithm is adversely impacted by CT saturation and high harmonic content as they can distort the current waveform.
- Harmonic content restraint: this is an improved desensitisation technique. The differential relay is self-desensitising during the energisation period when magnetising inrush current is detected but will trip should a fault occur during this period as it is not desensitised for fault currents. The relay distinguishes between fault currents and inrush currents by the content of large harmonic components and difference in wave shape. Incorporating an independent harmonic restraint/blocking technique in the differential protection algorithm gives power security. The even harmonics are utilised for restraint and the odd harmonics with dc components are used for blocking. These harmonics are 2^{nd},4^{th} and 5^{th} harmonics.

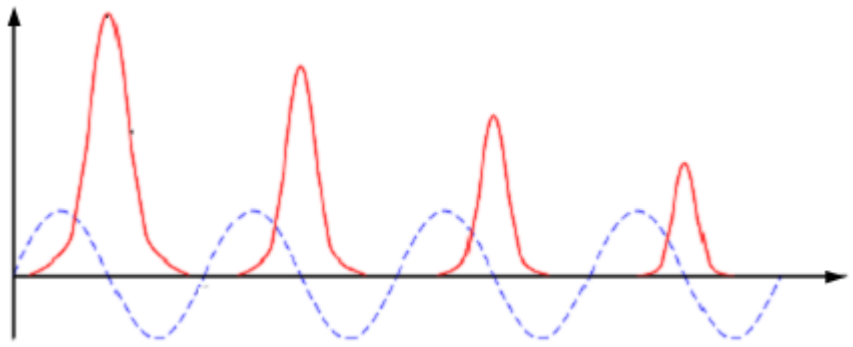


Figure 4.12: Harmonics (Silva et al., 2021)

Even harmonic restraint

Using even harmonics, specifically the second and fourth, within a restraint scheme enhances security against inrush currents characterised by minimal second harmonic current. The operational equation pertaining to the 2nd and 4th harmonic restraint differential elements is as follows.

$$I_{O_P} > SLP \times I_{RT} + K_2 I_2 + K_4 I_4 \quad (4.14)$$

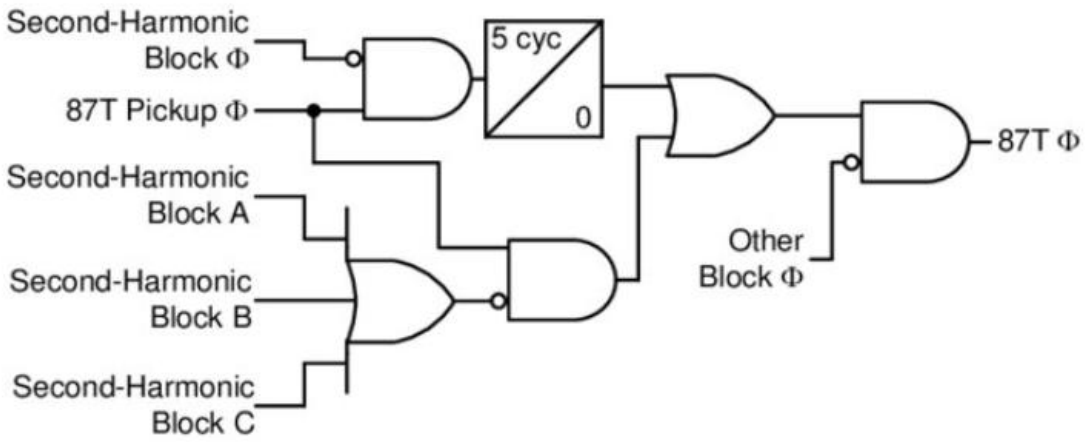


Figure 4.13: Harmonic logic (SEL,2024)

4.4.5. 5th Harmonic block

The utilisation of the fifth harmonic content of the operating current is a common approach to prevent differential relay tripping in instances of through faults and transformer overexcitation conditions. The configured relay design compares the fifth harmonic to the operational current independently, ensuring that each relay configuration accurately reflects the identical overexcitation condition. The 5th harmonic restraining scheme can result in varying overexcitation situations based on other harmonics present.

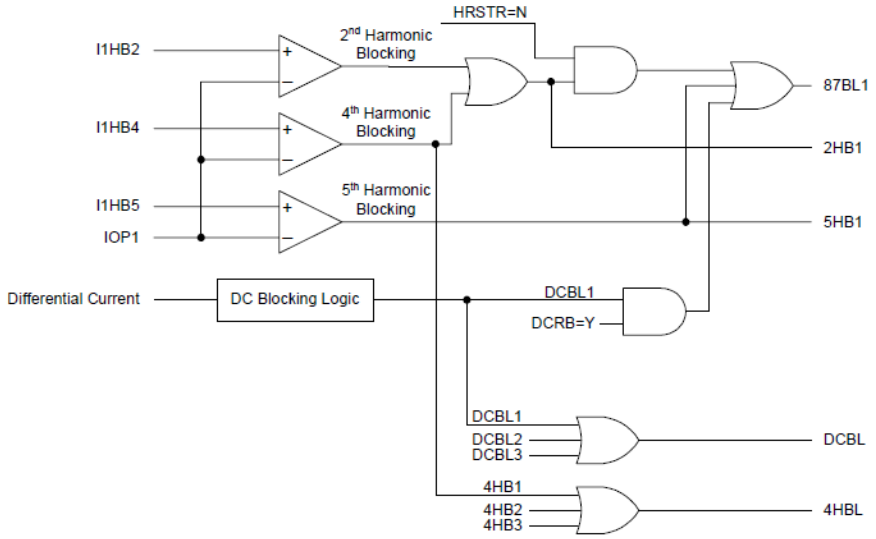


Figure 4.14: Differential Element (87BL1) Blocking logic

$$I_{O_P} < K_5 I_5 \tag{4.15}$$

4.4.6. DC Component content blocking

The developed approach for 5th harmonic blocking and even-harmonic restraint ensures robust relay security under conditions of inrush and overexcitation. In certain instances of inrush, the differential current appears as a pristine sine wave, leading to the erroneous functioning of the harmonic-based technique. Inrush currents have longer time constant compared to internal faults due to its direct current component. Inrush current with dc offset is a reliable indicator for relay security. The technique of wave form recognition is fundamentally rooted in the extraction of the direct current component, which is essentially a lowpass filtering procedure. This characteristic renders it relatively straightforward to implement to an IED. (A. Guzman, 2023)

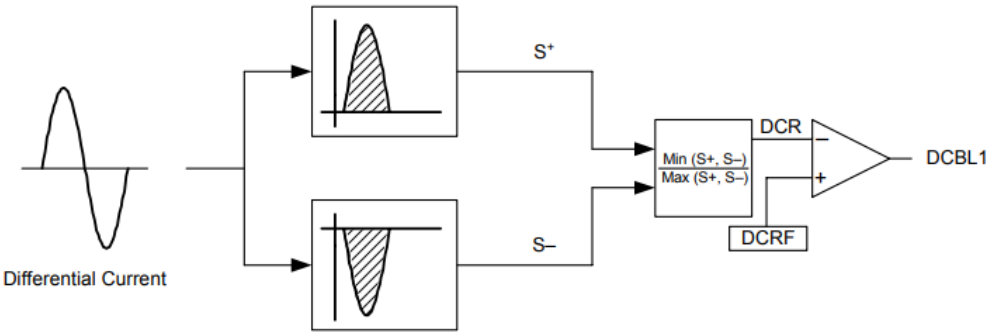


Figure 4.15: DC Blocking logic

4.4.7. Unrestraint region

In this region (operate area HS) the differential relay operates unconditionally regardless of any blockings (2^{nd},4^{th},5^{th} harmonics and DC component for as long as the unrestrained pick up is reached.

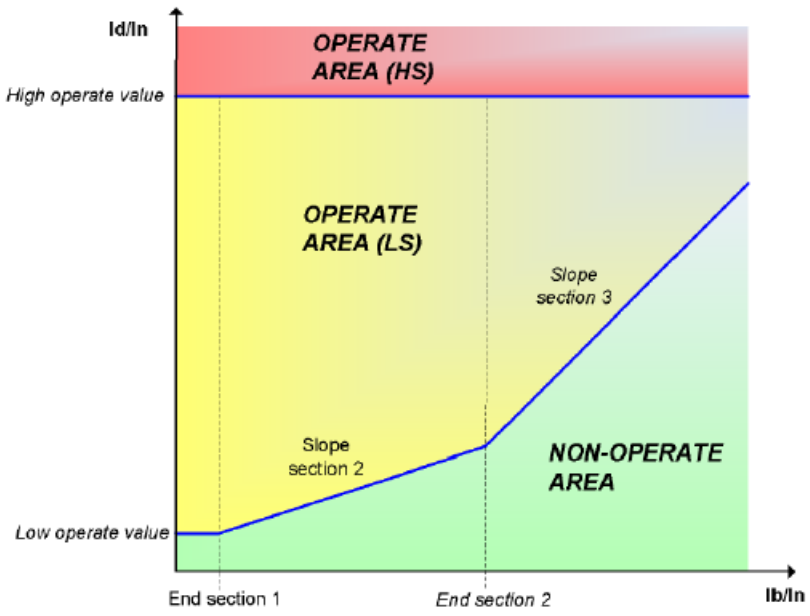


Figure 17: Diff operating characteristics

4.5. Restricted Earth Fault

Restricted Earth Fault is used adequate transformer protection in addition to the phase differential protection. REF is a sensitive and fast protection that detects faults closer to neutral and when the ground fault currents are not significant, as the phase differential is not sufficiently sensitive for such faults. The REF is utilised in a grounded winding through solid earth, impedance grounded and compensated grounding for delta connected winding. The combination of phase differential and REF provides sufficient level of safety and reliability.

4.5.1. High Impedance

High Impedance REF utilises the neutral CT in conjunction with the phase differential CTs as shown below.

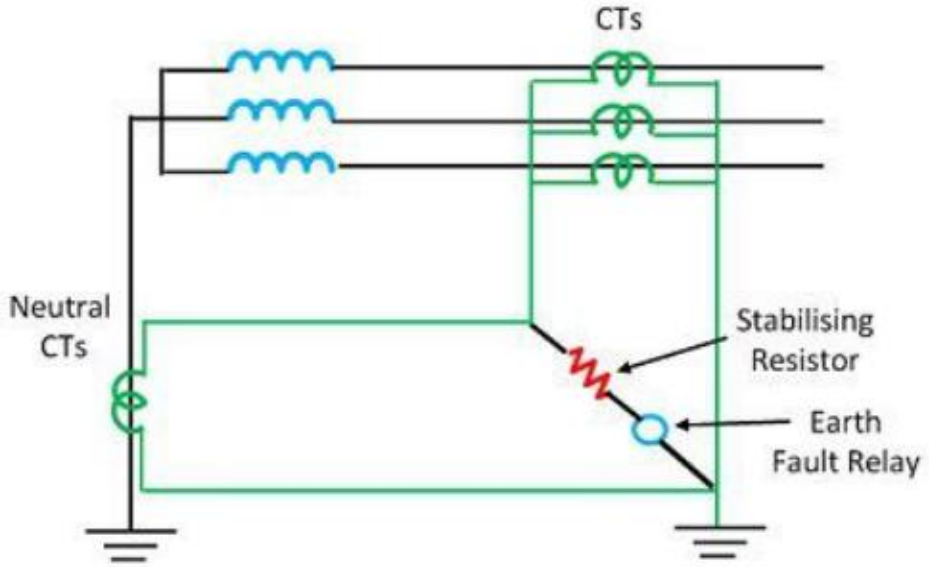


Figure 4.16: High impedance REF (Silva et al., 2021)

The high impedance REF has limitations as it is mainly used with phase one relays (electromechanical relays). Phase one relays lack the ability to sense the harmonic content in the current waveforms and often trips unnecessarily. This protection requires the CTs used to be identical, and it has satisfactory immunity to CT saturation (Jelisaveta P. KRSTIVOJEVIC, 2024).

Low Impedance REF

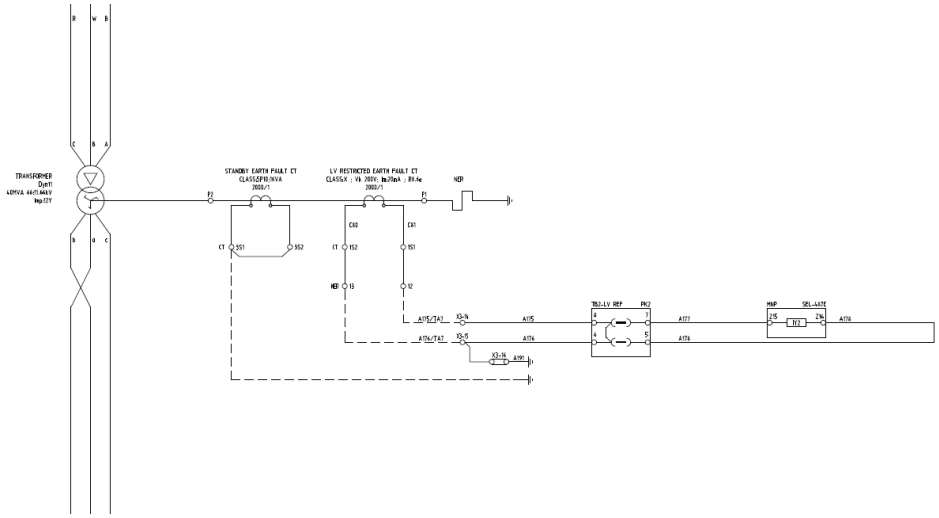


Figure 4.17: Low Impedance REF

Low Impedance REF does not require the CTs to be identical however it is prone to CT saturation during external faults and adversely impacted by magnetising inrush currents. Low Impedance REF has an advantage of using harmonic detection techniques that were previously discussed in phase differential protection. There is also an advantage of utilising directional supervision and adaptive current restraint techniques. Utilising these capabilities makes it more reliable as it can use calculated parameters within the initial energisation period to prevent spurious operation. Show below is a typical low impedance algorithm.

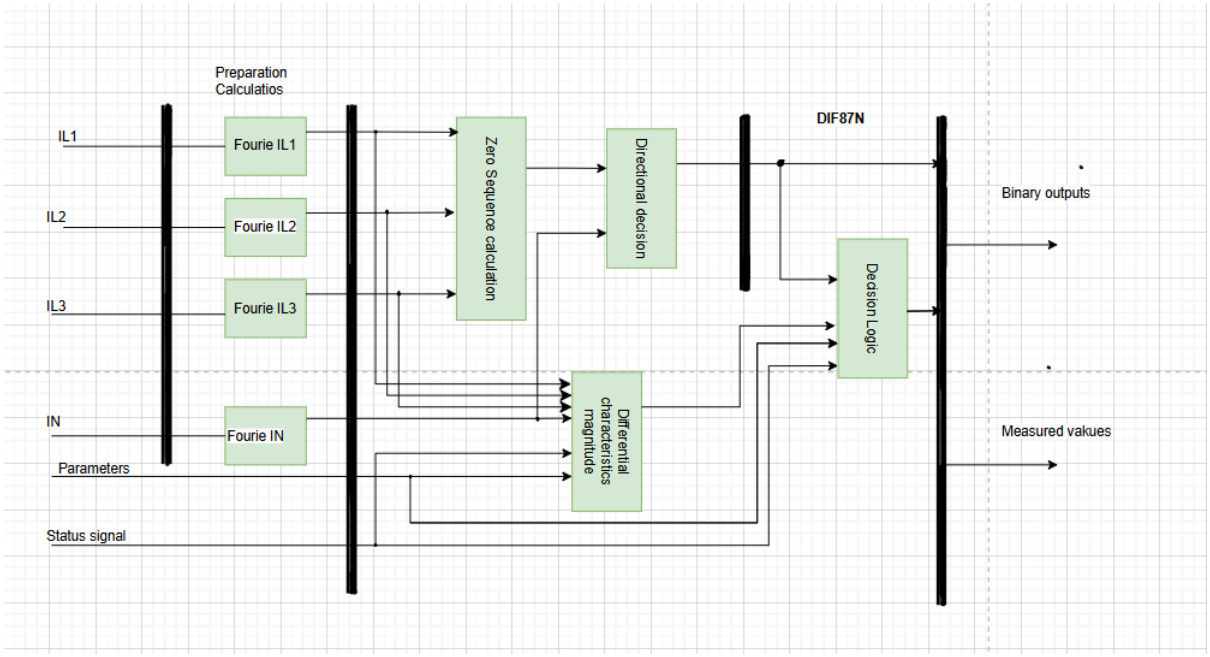


Figure 4.18: Low Impedance algorithm

Current measurements from the phase differential CTs and neutral CT are sent to fourier calculation modules individually. The IED then calculates zero sequence current from the phase current, the zero sequence currents direction is then compared to the neutral current. This improves the stability of the REF. Differential characteristics module uses the phase currents (IL1, IL2 and IL3) and IN the neutral current to evaluate if the current is in the operating rigion or restraint region. The compination of phase differential protection and low impedance REF provides adequate protection reliability and security. Typical connection is shown in below.

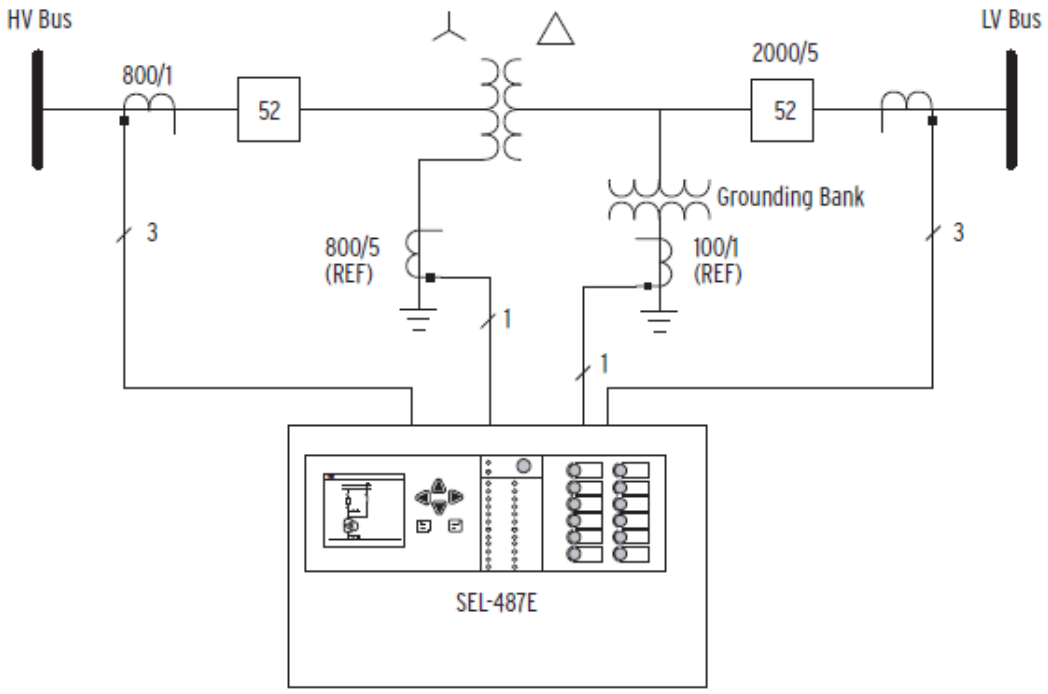


Figure 4.19: Phase Diff and REF (SEL,2020)

As shown in figure 4.16, the REF protection can be achieved for delta connected winding through the installation of neutral earthing compensator (grounding bank).

4.5.2. SEL 487E configuration

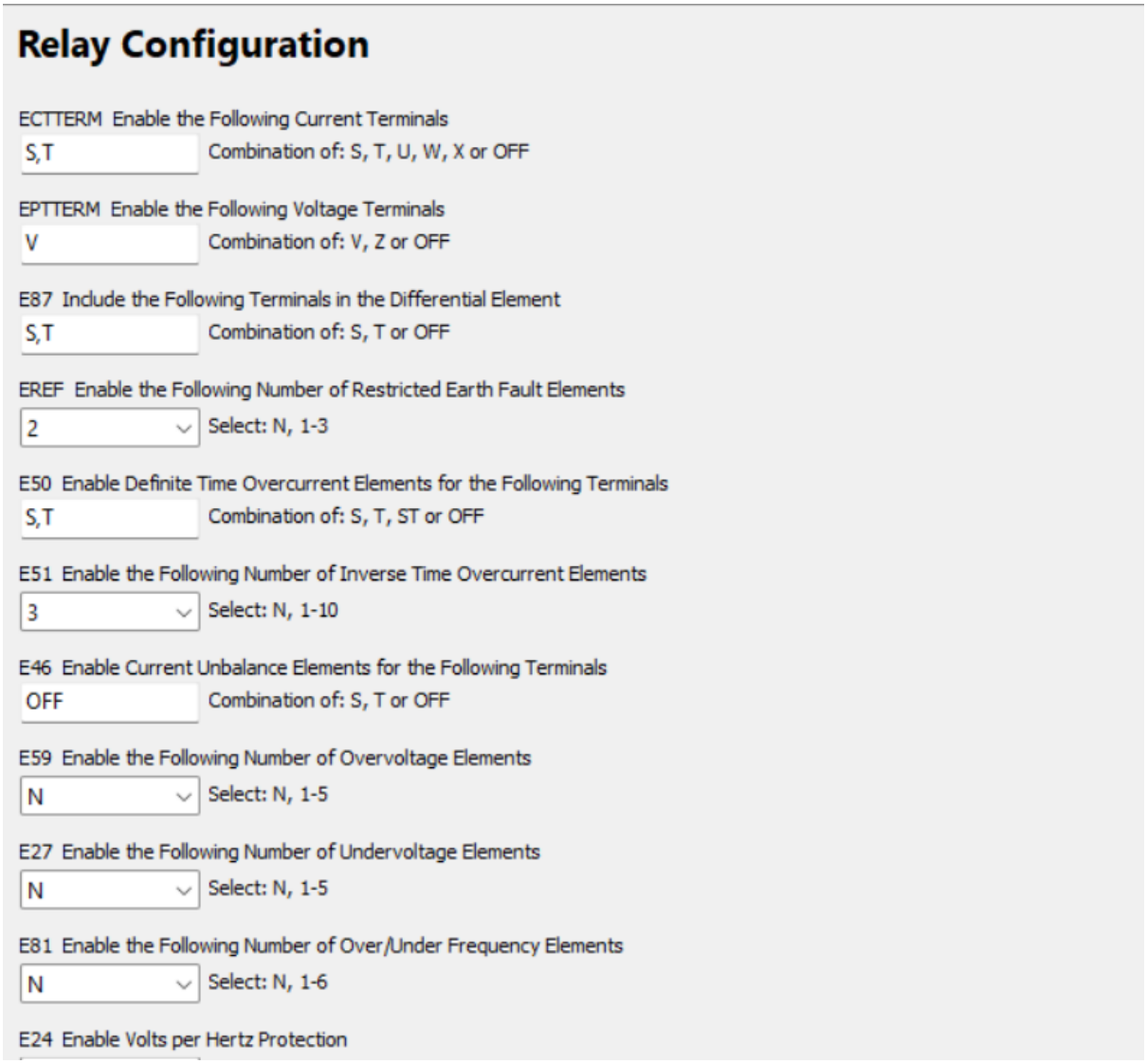


Figure 4.20: SEL487E Configuration 1

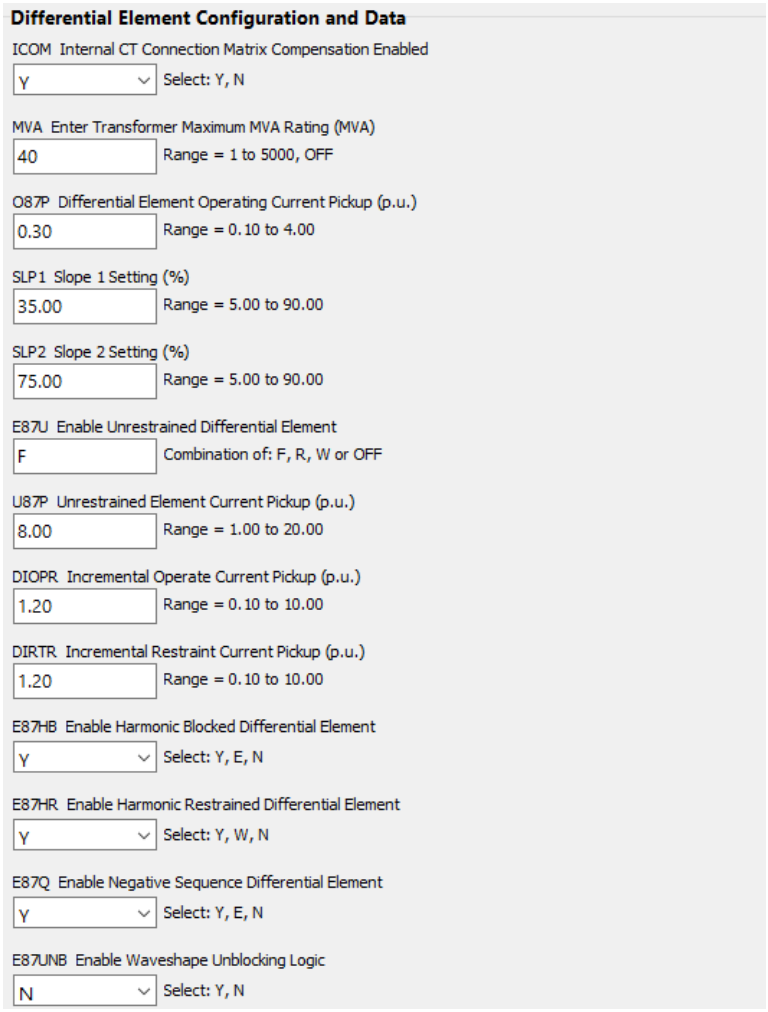


Figure 4.21: SEL487E Configuration 2

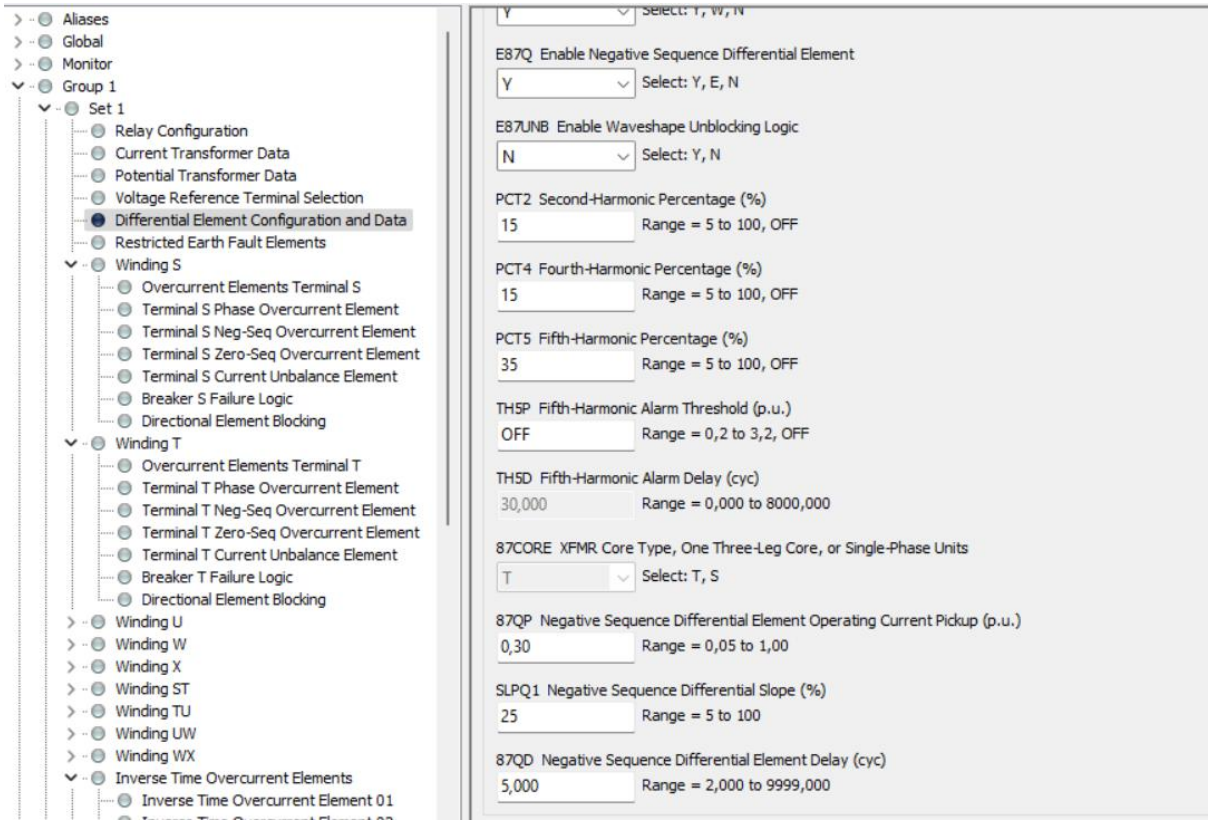


Figure 4.22: SEL487E Configuration 3

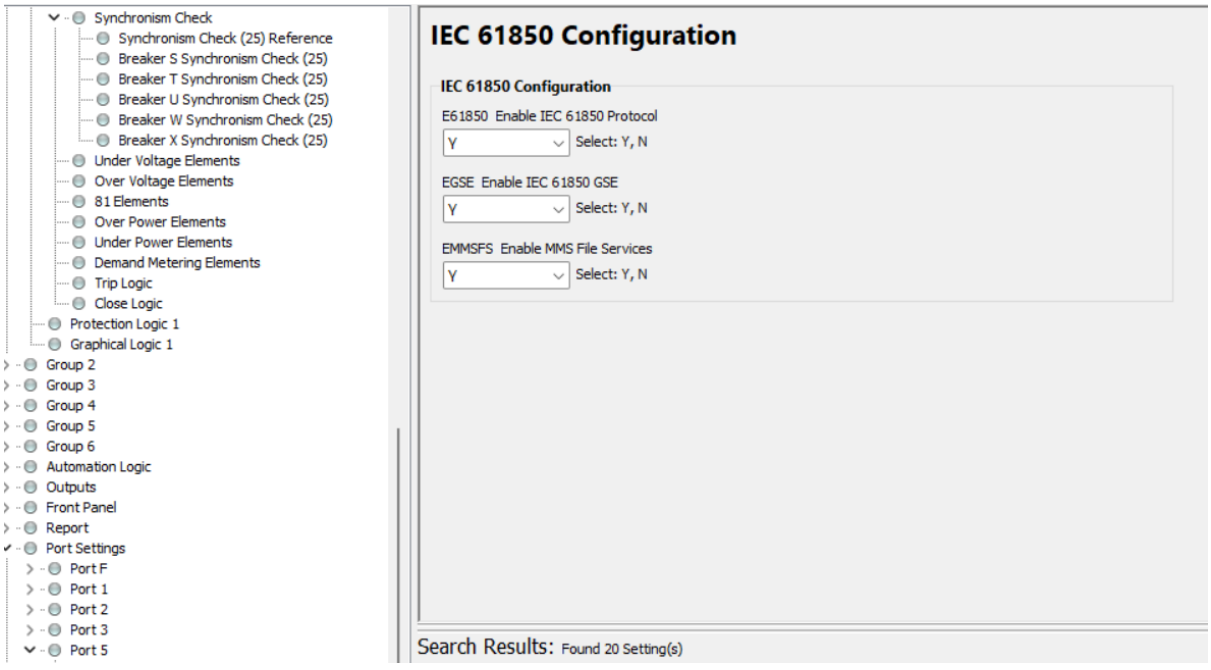


Figure 4.23: SEL487E Configuration 4

4.6. Back-up protection

4.6.1. Impedance Protection

Impedance Protection often known as distance protection is the predominant technique utilised for feeder protection attributed to its superior selectivity, rapid response capabilities and leverage of diverse relay programming algorithms. It has different zones of protection, zone 1 is the only instantaneous zone. Other zones are associated with time delay however the tripping can be accelerated via communication channels to ensure fast response. This acceleration of tripping prevents system instability, power quality, and prolonged plant damage as increased disturbance duration severely affects the power system network. (Aftab, et al., 2023) The accelerated tripping is achieved through tele-protection communication system compromising of interoperability and standardisation based on IEC 61850 GOOSE communication. The communication assisted system must conform to the performance requirements.

Basic operating principle

Impedance protection is a non-unit protection. It also referred to as the distance protection since the impedance of the line is in proportion to the length of the line. Impedance protection offers significant technical and economic advantages, with the key benefit being the fault coverage that is independent of source impedance variations. The distance protection algorithm can be configured with algorithm that can deal with the most difficult transient phenomena. The basic operating principles of impedance protection entails calculating the ratio of the voltages and currents at the IED location (Position) point to the measured value from VT and CT, then compare the apparent impedance to the predetermined reach point. The IED is configured to only respond to faults in between the reach point and the IED location, thus maximising discrimination against unnecessary tripping.

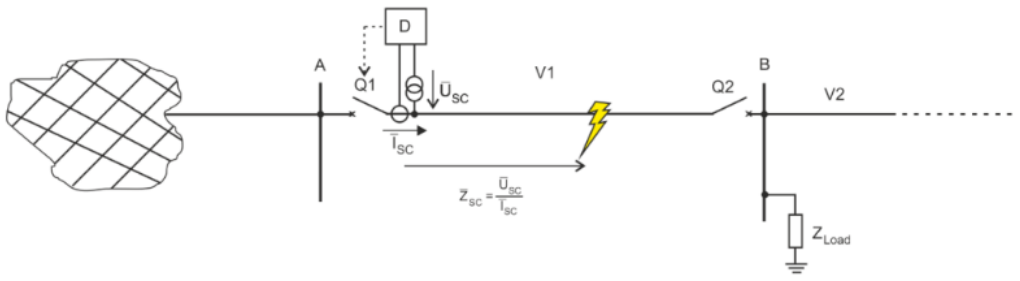


Figure 4.24: Distance protection (Pac basics,2024)

When the measured impedance falls below the reach point threshold impedance, It can be deduced that a fault is present along the line within the designated zone reach point.

Zone 1 covers up to 80% with extension to 85% (where necessary) of the line, zone 2 covers up to 120% (with extension to 150% where necessary) and zone 3 up to 20% in reverse. These settings are set according to network variations and requirements. With zone 1 operating instantaneously, zone 2 with a delay of 400ms and zone 3. Operation equation is depicted below.

$$\left|\frac{v}{I}\right| < |z_R|$$

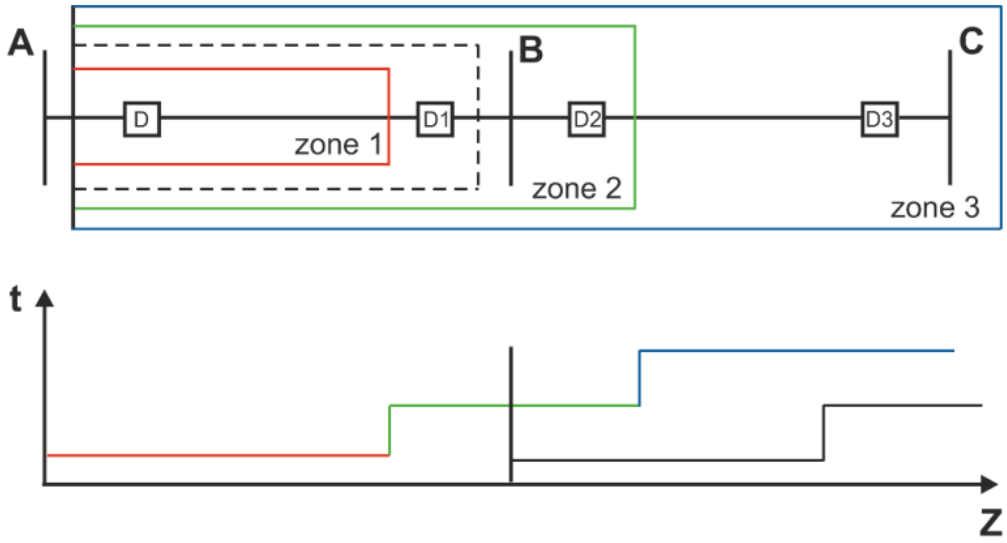


Figure 4.25: Zones and operating times (ABB Manual, 2022)

4.6.2. Distance relay characteristics.

The distance protection utilises the following relay characteristics:

- Amplitude and Phase comparison
- Plain impedance
- Mho
- Quadrilateral

The distance protection can be configured to be an under-reaching and over-reaching scheme:

4.6.3. Under-reach Transfer Tripping schemes

- DUTT - Direct Under-reaching transfer tripping schemes (Zone 1)
- PUTT - Permissive Under-reach transfer tripping schemes (Time reliant)
- Permissive Under-reach Acceleration scheme (using power line carriers, line traps or optic fibre)
- Weak infeed conditions

4.6.4. Over-reach Transfer Tripping schemes

- POTT- Permissive Over-reach transfer tripping schemes

4.6.5. Line Bank Transformer

Line bank transformer is a system where the transformer is equipped with only the LV circuit breaker with no HV circuit breaker and relies on the far end of the line for total isolation. The distance protection provides a backup protection for such system and can also facilitate alternative inter-trip send and receive channels.

IE61850 based accelerated tripping

In the year 2000, the IEC developed a communication standard series for electric power substations known as IEC 61850. IEC 61850 utilises an object-oriented modelling technique to represent power system devices, facilitating object configuration and data organisation. In order to achieve consistency and interoperability, the modelling is aligned with specific protocols, like Ethernet, The IEC 61850-based automated substation communication architecture can be delineated by 3 broad categories of Intelligent Electronic Devices, i.e. MUs, Protection (IED) and control (Bay controller IED), classified according to their respective tasks. GOOSE messages that are time-sensitive are referred to as type 1 and type 1A messages that entails command functions such as start, stop, close and trip. These messages are directly aligned and mapped into the Ethernet layer to minimise the complexity of protocol stack.

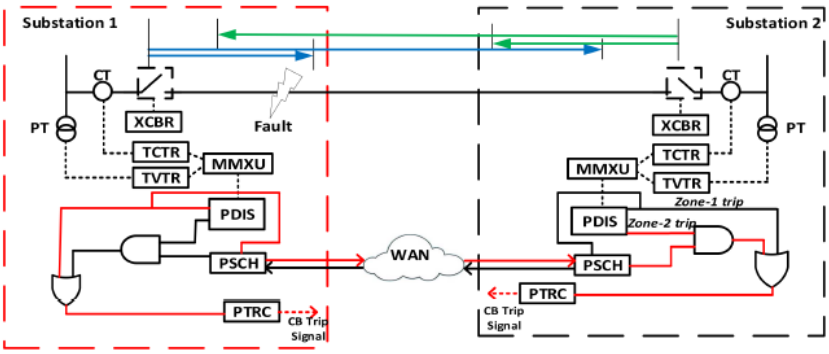


Figure 4.26: Accelerated distance protection based on IEC 61850 (IEC 61850-5/6,2022;

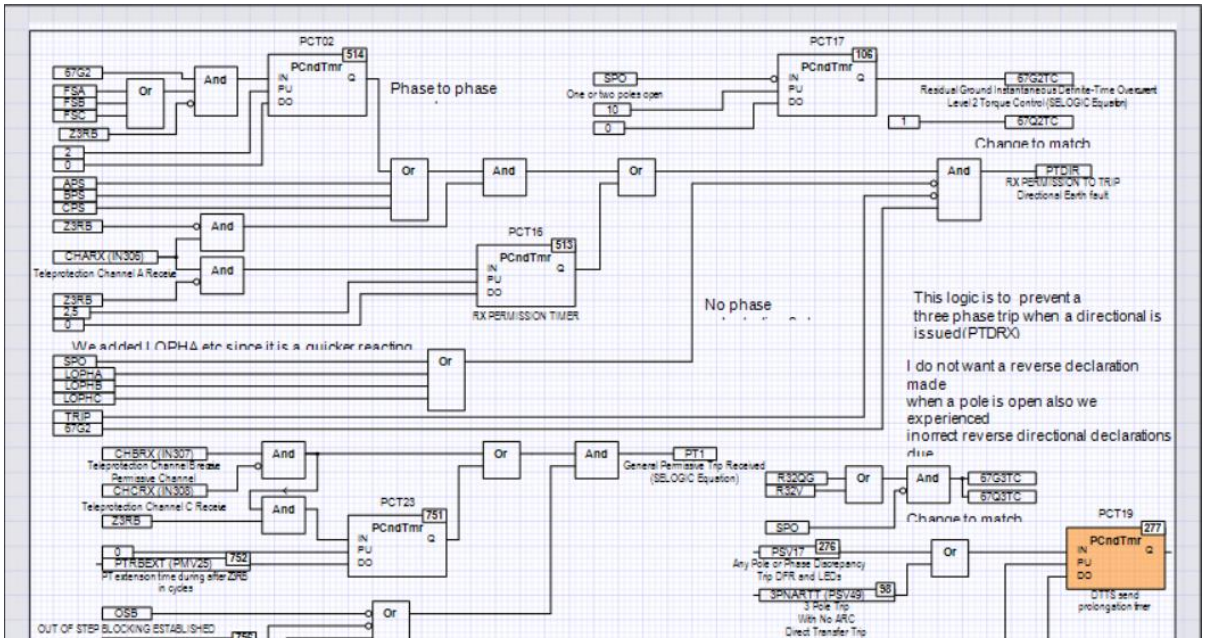


Figure 4.27: Developed Communication aided logic P1

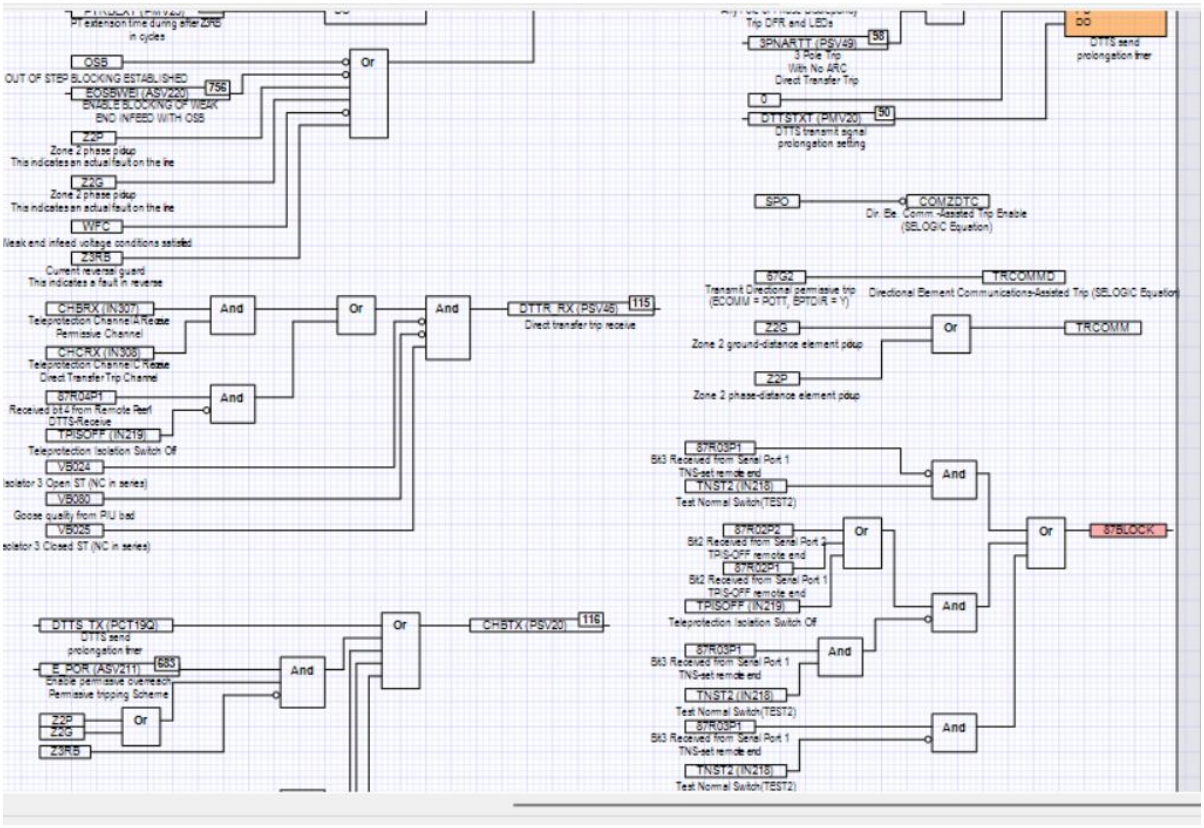


Figure 4.28: Developed Communication aided logic P2

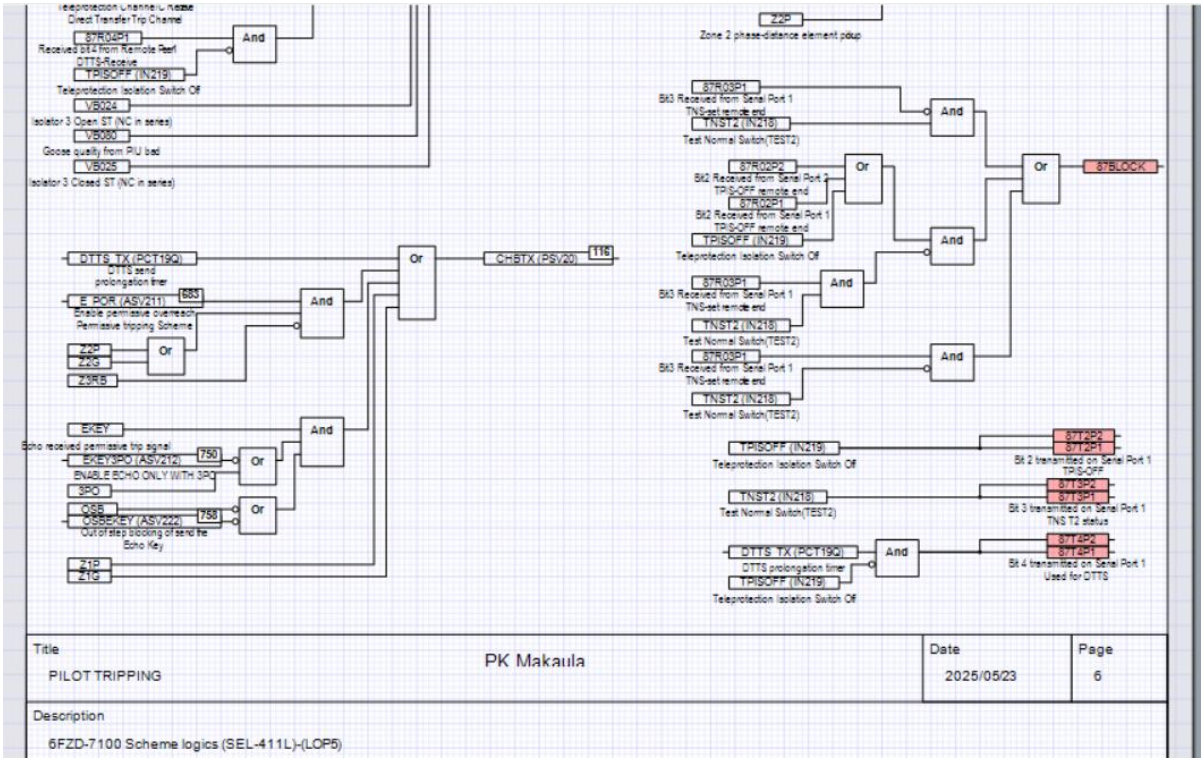


Figure 4.29: Developed Communication aided logic P3

The accelerated impedance protection between two or more inter-substations utilising IEC 61850 GOOSE to facilitate impedance protection between the inter-substations with the transformer in-between, the specific message exchanges across the IEC 61850 logical nodes are outlined in detail here. Upon the occurrence of a fault in zone 1 of substation 1, the impedance relay detects the currents and voltage levels at substation. It subsequently generates a tripping signal through PTRC logical node directed to the CB, which is represented by the XCBR (circuit breaker) logical node, it also transfers a tripping signal to the breaker at substation 2 through PSCH logical node. This eliminates the time delay at substation 2 IED as the fault is in zone 2 for that IED normally 0,4s. The IED at substation 2 echo the tripping signal back to IED at Substation 1.

The TVTR and TCTR logical nodes of IEC 61850 retrieve the current and voltage samples from the merging unit and send them to the distance protection logical node PDIS, and MMXU (i.e the metering and measurement logical node). PDIS1 refers to zone 1 logical node and PDS2 is for zone 2, PDS3 for zone 3 and so on respectively. The protection logical node subsequently computes the three phase analog currents and voltages necessary for determining the value of impedance. The MMXU node computes supplementary parameters, including apparent, active and reactive powers respectively for various applications such as billing, load monitoring and load forecasting etc (AftabSuhail, et al., 2023) .

The implementation of a communication facilitated impedance protection scheme, based in the IEC 61850 standard, is achieved through the utilisation of GOOSE messages transmitted between geographically separated inter-substations. The GOOSE messaging is characterised by their burst-type, driven by specific events, non-periodic nature. In the event of a fault, protection devices react by emitting a series of GOOSE messaging. The emergence of a fault transforms the regular periodic heartbeat characteristic of the GOOSE messages into a mode of bursts, where the intervals of GOOSE messages transmission are progressively lengthened. After the fault or trigger the GOOSE transmission interval reverts to the standard rate.

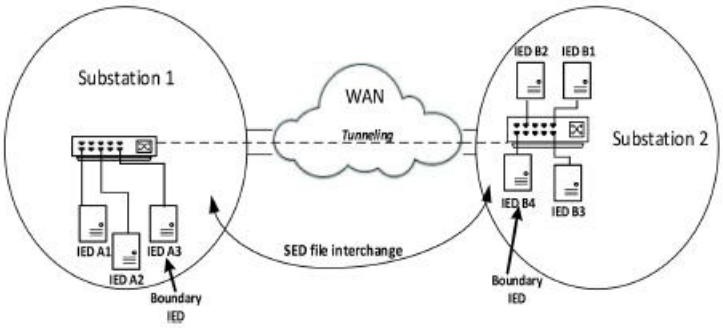


Figure 4.30: SCL file exchange tunnelling (IEC 61850-5/6,2022)

4.6.6. SCL file exchange in tunnelling

In tunnelling projects, SCL file exchange, inspired by its use in IEC 61850 substation automation, can offer significant advantages. By providing a standardised way to configure diverse monitoring and control systems, SCL promotes interoperability and reduces configuration errors. The ability to exchange data via SCL is crucial for sophisticated monitoring of parameters such as stress and displacement, as well as for coordinating equipment operation. Furthermore, SCL supports advanced automation, enabling more efficient and safer tunnelling processes. While secure communication is essential in tunnelling projects, technologies like VPNs can complement SCL by establishing secure tunnels for data transfer. File transfer itself plays a vital role, especially when dealing with large datasets, emphasising the need for efficient and stable solutions. Overall, SCL file exchange presents a pathway towards more integrated, automated, and data-driven tunnelling operations.

it is essential to exchange SCL files among the intelligent electronica devices in a substation adhering to the IEC 61850 standard to facilitate seamless integration and ensure interoperability and within an IEC 61850 processes. The full substation configuration of IEDs is facilitated by transmitting the SSD and ICD to configurator tool. This tool integrates the functionalities of an IED presented and accompanied by the substation single line diagram, delineating all operational prerequisites. The SCD file (substation configuration description) is generally developed by the system configurator tool. SCD encompasses the communication configuration of all Intelligent Electronic Devices (IEDs) as they are modelled for automation and protection tasks within the substation. The SCD file is distributed among other substation devices and is applicable for various appl

ications. The tunnelling process produces a distinct IED configuration derived from a SCD file, which encompasses substation-specific addresses pertinent to a particular IED. This procedure creates a robust, high-capacity connection across a wide area, linking two local area networks situated in different geographical locations. The sender and receiver IED function as though they are part of the same LAN, facilitating the ICD files exchange for IED configuration. In order to uphold uniformity, a 'system interface exchange description' (SED) file is delineated, transmitted between substations, and encompasses a segment of the comprehensive system information. The closest IED to the switch is referred to as the boundary intelligent electronic device for an alternate substation. The authority to manage the configuration of the IED resides with the IED tool, and the adjusted SED file is sent back to the originating substation.

4.7. GOOSE CONFIGURATION

4.7.1. **IEC 61850-Based Enhanced Transformer Protection:** Exploring IED Configuration, GOOSE Mapping, and Scheme Effectiveness

The GOOSE protocol, as defined by IEC 61850, is central to fast and reliable communication within digital substations. Mapping GOOSE messages handling onto accelerator architectures such as FPGAs or network processing units (NPUs) can provide deterministic performance, low latency, and improved scalability, which are critical for time-sensitive operations like protection and interlocking. This section details the methodology and technical considerations for mapping GOOSE communication components including GOOSE receive and transmit paths, datasets, and deadband logic onto such hardware platforms. Mapping GOOSE communication mechanisms onto accelerator architectures such as FPGAs offers a high-performance solution for the actual demands of digital substations. By partitioning functionality into dedicated receive and transmit logic, implementing structured dataset management, and applying efficient deadband filtering, this approach supports low-latency, deterministic event handling in compliance with IEC 61850 standards. The outlined architecture ensures scalability, fault tolerance, and reliable protection scheme operation, thereby advancing the adoption of hardware-accelerated solutions in critical power system infrastructure.

The integration of IEC 61850 communication protocol into transformer protection schemes represents a significant advancement in power system engineering, offering enhanced speed,

reliability, and flexibility (Krishnamurthy, 2022).Intelligent Electronic Devices are pivotal in this framework, providing advanced protection and control functionalities within the substation environment (Hakala-Ranta, 2024). The IEC 61850 standard facilitates seamless communication between IEDs, enabling the implementation of sophisticated protection schemes such as differential protection, overcurrent protection, and breaker failure protection, all while enhancing instant data exchange and system-wide coordination (Huang, 2023). The adoption of IEC 61850 introduces the utilisation of Ethernet process buses for connecting primary equipment and measured values, thus fostering greater flexibility (Süfke, 2021). GOOSE ensures swift and dependable data exchange, facilitating rapid response to faults and minimising the impact on the power grid. The GOOSE configuration of IEDs within an IEC 61850 framework is crucial for ensuring proper operation of the protection scheme, and involves defining the protection functions, communication parameters, and data mapping according to the specific requirements of the transformer and the power system. It requires meticulous planning and configuration to ensure seamless interoperability and optimal performance. This configuration process encompasses defining protection functions, setting communication parameters, and mapping data to align with the transformer's specific requirements and the broader power system architecture. GOOSE messaging, a cornerstone of IEC 61850, necessitates careful mapping to ensure the accurate and timely exchange of critical protection data, enabling rapid response to faults and minimising system disturbances. Testing and validation of the GOOSE communication are essential to confirm the protection scheme performance and reliability. This includes verifying message transmission times, data integrity, and the response of IEDs to various fault conditions (Parikh, 2022).

4.7.2. GOOSE configuration on architecture

The implementation of Generic Object-Oriented Substation Events messaging within an Acselerator architecture necessitates a meticulous mapping strategy encompassing GOOSE reception, transmission, dataset configuration, and dead band application, all of which are crucial for ensuring reliable and efficient substation automation. GOOSE messaging, a cornerstone of modern substation communication, facilitates the rapid exchange of critical data between intelligent electronic devices, enabling swift responses to system events and enhancing overall grid stability (Höger, 2024). Proper configuration of GOOSE parameters within the Acselerator framework directly influences the speed and accuracy of protective relaying schemes and automated control functions. The IEC 61850 standard, which underpins GOOSE messaging, revolutionises control system design by emphasising communication

and information handling. GOOSE enables fast direct trip modes through message interchange, providing an approach to system operation during events. DATASETs, which are collections of data attributes that are transmitted within GOOSE messages, must be carefully defined to include the relevant process variables and status information required by subscribing devices. This structured approach ensures interoperability between different devices and vendors, facilitating seamless integration within the substation environmentThe design of the data set encompasses meticulous specifications regarding logical nodes, the nomenclature of data objects, attributes of data, and prevalent data classifications (Huang, 2023). Furthermore, the Acselerator architecture must incorporate mechanisms for managing dead bands, which are used to prevent spurious GOOSE messages from being transmitted due to minor fluctuations in process values. An intelligent substation relies on network transmission technology and process equipment (Wang, 2023). The IEC 61850 standard is a layered approach to communication networks and systems for substations (Aftab, 2020). The testing of GOOSE messages involves simulating various fault conditions and verifying the correct operation of the protection scheme. This includes verifying message transmission times, data integrity, and the response of IEDs to various fault conditions. Testing is performed to ensure that the protection system meets the required performance criteria and complies with industry standards. Testing is essential as it ensures the dependability and effectiveness of protection systems, necessitating the use of sophisticated testing methodologies and tools to replicate fault scenarios and assess the system's response. GOOSE mapping involves defining the data content of GOOSE messages and assigning them to specific protection functions. Proper mapping ensures that the correct data is transmitted between IEDs, enabling coordinated protection actions. The ability to identify and isolate a faulty interconnecting cable promptly is crucial, as undetected faults can lead to substantial equipment damage and system failures.

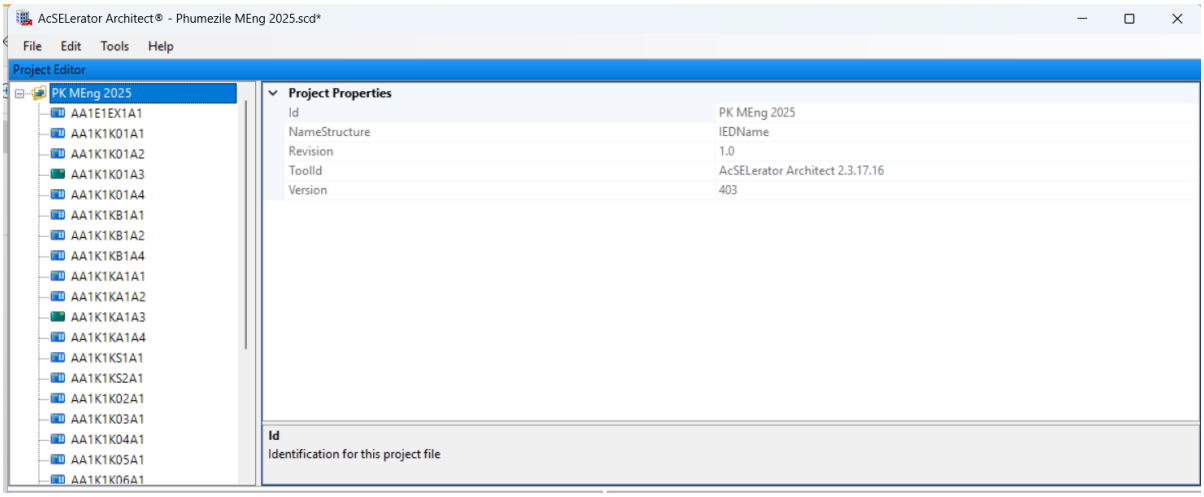


Figure 4.31: Developed GOOSE configuration

4.7.3. GOOSE Receive Mapping

Accurate mapping of GOOSE receive functions within the Acselerator platform involves configuring the system to correctly interpret incoming GOOSE messages, validate their source, and extract the relevant data attributes. This process includes defining the expected GOOSE message structure, security parameters, and quality flags, ensuring that only authorised and valid messages are processed. The Acselerator also provide tools for filtering and prioritising GOOSE messages, allowing subscribing devices to focus on the most critical information. The message structure must be verified against a schema. Furthermore, mapping the extracted data attributes to the appropriate internal variables and functions within the Acselerator environment is essential for triggering the desired control actions or protection responses. This data mapping accommodates various reporting methods and data formats used across different protection devices. These communication services support instant data exchange, event reporting, and remote-control functionalities. The receive path is responsible for detecting, validating, and processing incoming GOOSE messages from the Ethernet interface. Mapping this function to an accelerator begins with the implementation of a high-speed packet parsing engine capable of filtering Ethernet frames by Ether Type (0x88B8) and multicast MAC address patterns specific to GOOSE communication (01-0C-CD-01-00-XX). Once a valid GOOSE frame is detected, the parser extracts the protocol-specific fields such as the Application Identifier (APPID), state number (stNum), sequence number (sqNum), time allowed to live (TAL), and dataset reference (datSet). In an FPGA implementation, finite state

machines (FSMs) are instantiated to maintain state information for each active GOOSE control block. These FSMs compare the incoming stNum and sqNum fields with previously stored values in on-chip memory. If the stNum indicates a state change, the event is validated and forwarded to the application logic or host processor using a DMA engine or a memory-mapped register interface. This ensures low-latency event propagation while maintaining compliance with the performance constraints of IEC 61850-8-1.

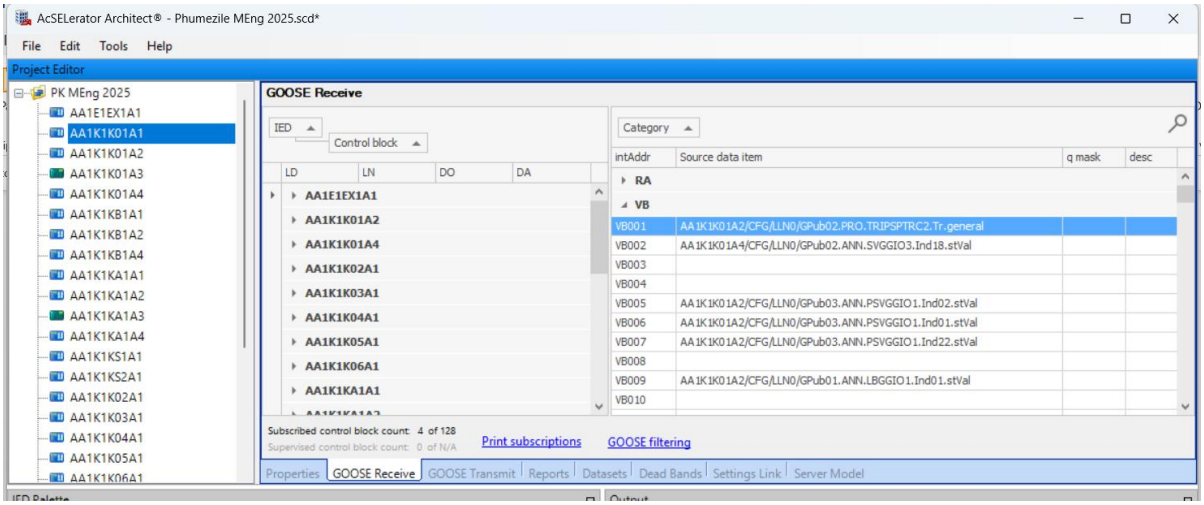


Figure 4.32: GOOSE Receive

4.7.4. GOOSE Transmit Mapping

GOOSE transmit functionality necessitates the configuration of data sources, trigger conditions, and message parameters for outgoing GOOSE messages. Proper data source mapping ensures that the correct process variables and status information are included in the GOOSE messages, while trigger conditions define the events that initiate message transmission. The Acselerator provide mechanisms for setting the GOOSE message priority, retransmission parameters, and security settings, optimising message delivery and reliability. The configuration process needs to take into account network bandwidth constraints and latency requirements to avoid flooding the network with unnecessary messages. When multiple IEDs subscribe to the same GOOSE message, the transmit configuration optimise for multicast transmission to reduce network load. This system allows for easy configuration and modification of GOOSE parameters, such as application ID, VLAN priority, and data set members, to accommodate changing system requirements and protection schemes. The transmission of GOOSE messages involves the periodic and event-driven generation of

Ethernet frames containing updated dataset values. This process begins with the construction of the GOOSE frame, including static fields (MAC address, VLAN tags) and dynamic fields such as stNum, sqNum, and timestamp. The transmission logic maintains separate counters for stNum and sqNum, where the former is incremented upon a dataset change and the latter is incremented with each retransmission. The frame construction engine is integrated with hardware timers that control the retransmission schedule in accordance with the IEC 61850 retransmission profile. For instance, after a state change, the frame is transmitted multiple times at decreasing intervals to ensure delivery reliability. The complete GOOSE message is then forwarded to the MAC/PHY layer using an AXI-Stream or similar hardware interface, providing deterministic timing and minimal jitter.

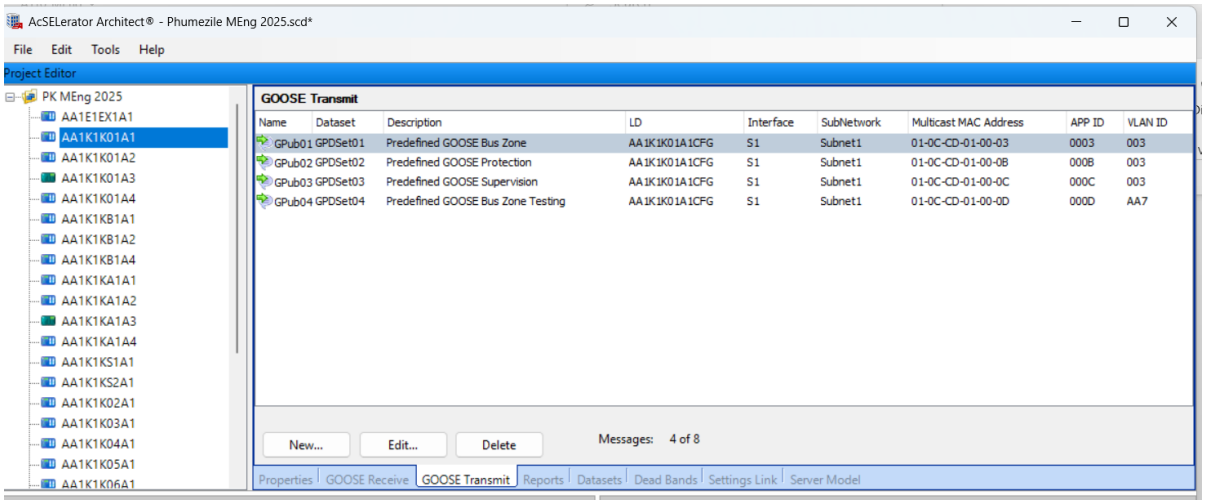


Figure 4.33: GOOSE transmit

4.7.5. Dataset Mapping

DATASET configuration within the Acselerator architecture requires careful consideration of the data attributes to be included, their data types, and their update rates. The data sets are standardised, enabling interoperability and consistency across different devices and systems. The IEC 61850 standard defines common data classes and logical nodes that should be used when creating the data set. The Acselerator provide tools for browsing available data attributes, selecting the relevant ones for inclusion in the DATASET, and defining their scaling and units of measure. Furthermore, the system supports the creation of custom DATASETs to accommodate specific application requirements. Proper dataset configuration ensures that

subscribing devices receive the necessary information to perform their intended functions, while minimising the amount of data transmitted over the network. The DATASET configuration process also involves defining the quality and validity criteria for the data attributes, ensuring that subscribing devices can assess the reliability of the received information. The data set design allows for future expansion and modification to accommodate new protection and control functions. Datasets are the core data structures bound to GOOSE control blocks, representing the logical signals to be communicated. In hardware, datasets are implemented as structured register blocks or memory arrays. Each element of a dataset such as binary status flags or analog measurements is stored in a dedicated memory location that is continuously monitored for changes. The dataset manager is responsible for binding datasets to their respective GOOSE control blocks. When a monitored value changes, it triggers an update to the GOOSE Transmit logic. Conversely, in the receive path, incoming dataset values are written into these memory structures to allow easy access by application-level processing or further protocol layers.

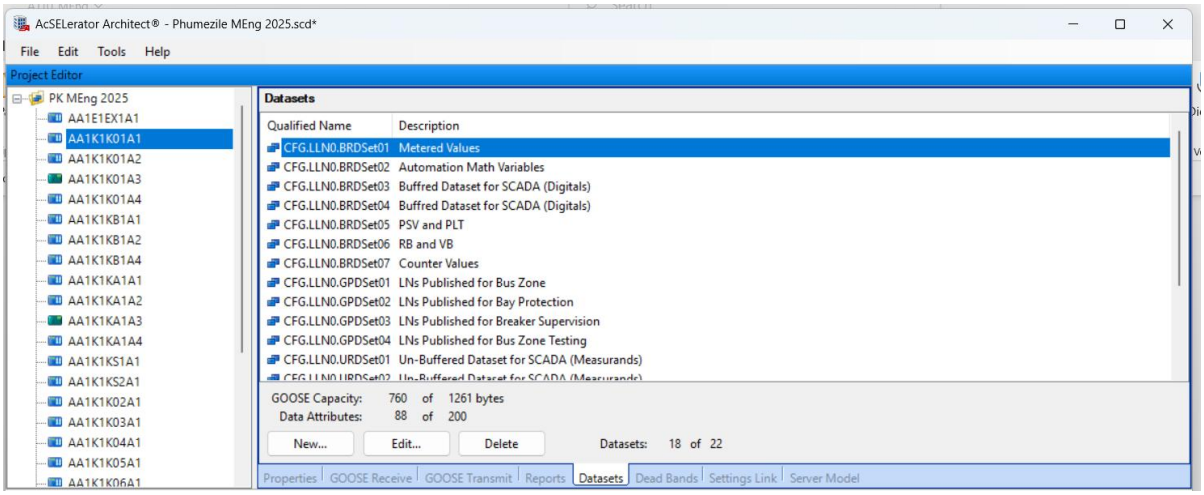


Figure 4.34: Datasets

4.7.6. Deadband logic Mapping

Deadband refers to reporting deadband for analogue values in MMS reports (BRCB/URCB). GOOSE elements are event-driven; they publish on state change (PTRC.Tr TRUE) rather than deadband thresholds. If analogue thresholding is required for events, generate a binary GGIO.SPCSO in the IED logic and include it in the GOOSE dataset. The implementation of dead bands within the Acselerator system is crucial for preventing the transmission of unnecessary GOOSE messages caused by minor fluctuations in process

values or insignificant signal changes. Dead bands define a range around a process value within which no GOOSE message is transmitted, reducing network traffic and improving system stability. The Acselerator should provide configurable dead band settings for each data attribute included in the DATASET, allowing users to fine-tune the sensitivity of the GOOSE transmission. The dead band settings should be adaptable to different process variables and application requirements, ensuring that only significant changes in process values trigger GOOSE messages. The dead bands are be based on a percentage of the process value or a fixed engineering unit. Hysteresis can also be implemented in conjunction with dead bands to prevent rapid oscillation of GOOSE message transmission when the process value is near the dead band threshold. This is particularly relevant for analog values, where small fluctuations can be safely ignored without affecting protection logic. In hardware, deadband comparators are instantiated for each dataset element that requires thresholding. Each comparator evaluates the difference between the current value and the last transmitted value against a configurable deadband threshold. If the change exceeds the threshold, the logic flags the corresponding GOOSE control block to increment its stNum, triggering a new message transmission cycle. Deadband thresholds are typically set through a configuration interface and stored in on-chip registers.

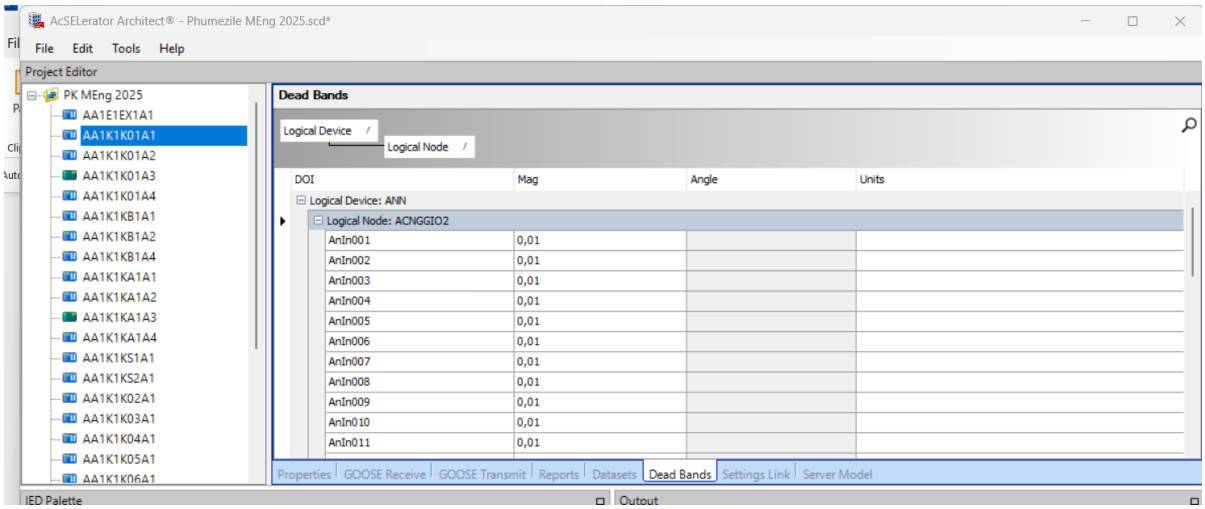


Figure 4.35: Dead bands

CHAPTER FIVE

5. IMPLEMENTATION AND SIMULATION RESULTS

5.1. Testing Effectiveness and Protection Scheme Validation

The effectiveness of the protection scheme is validated through extensive testing and simulation studies. The validation process involves simulating various fault conditions and verifying the correct operation of the protection scheme. Upgrading older relays (Electromechanical, static and IEC 61850 non-conforming relays) with IEDs offers substantial advantages, as older protection devices may not clear faults as effectively, leading to significant economic impacts. These studies assess the protection scheme performance under different operating conditions and fault scenarios, ensuring that it meets the required performance criteria. Operational tests on protection devices showed the need for careful attention in specific areas, highlighting the significance of thorough testing in ensuring dependable protection.

This environment allows fault injection, dynamic scenario analysis, and precise relay response time measurement in various network and system conditions. To accurately compare traditional and digital protection methods, system assumptions included balanced three-phase operation, stable grid voltage, and normal utility transformer parameters. Figure 5.1 depicts the simulated substation with an MV busbar feeding various outgoing feeders protected by differential and overcurrent IEDs. Vector group designation, tap changer position, and saturation characteristics are modelled for the primary power transformer between the HV and MV buses. Modelling coupled instrument transformers like CTs and PTs with linear and non-linear properties simulates accuracy and measurement error. The design directly simulates protection zones, fault locations (internal/external), and communication links, enabling a significant evaluation of the IEC 61850 communication process during protection events.

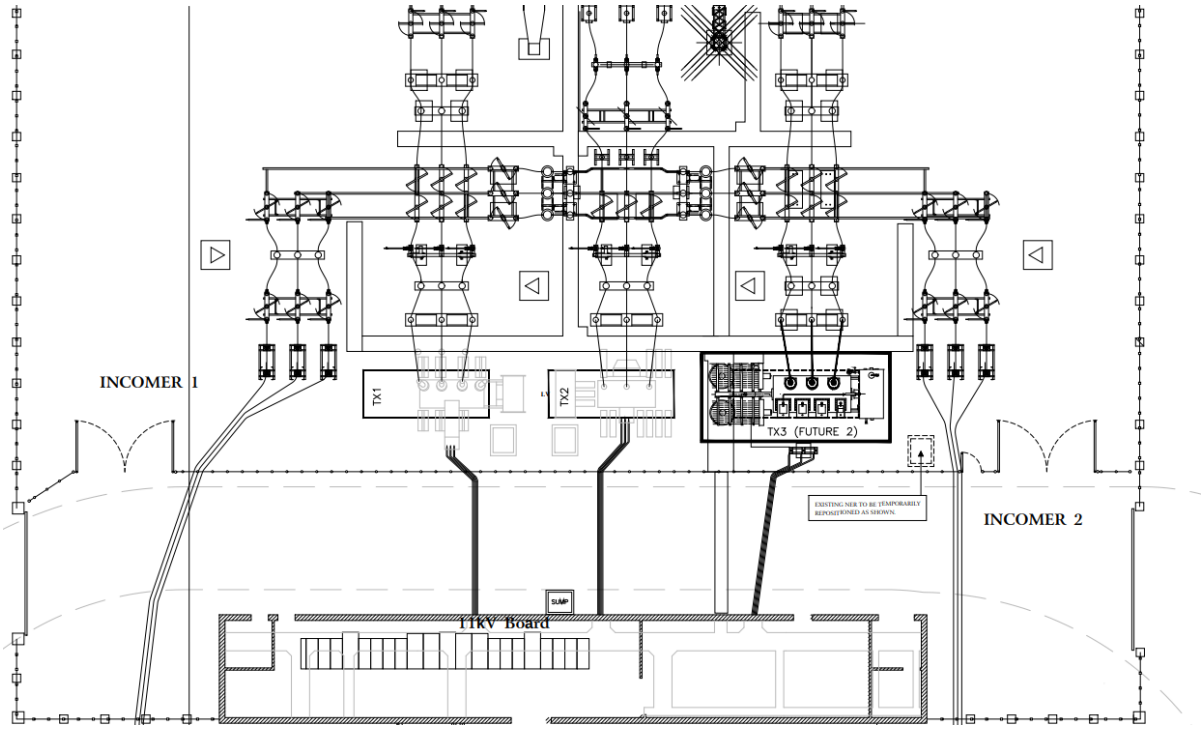


Figure 5.1: Substation layout

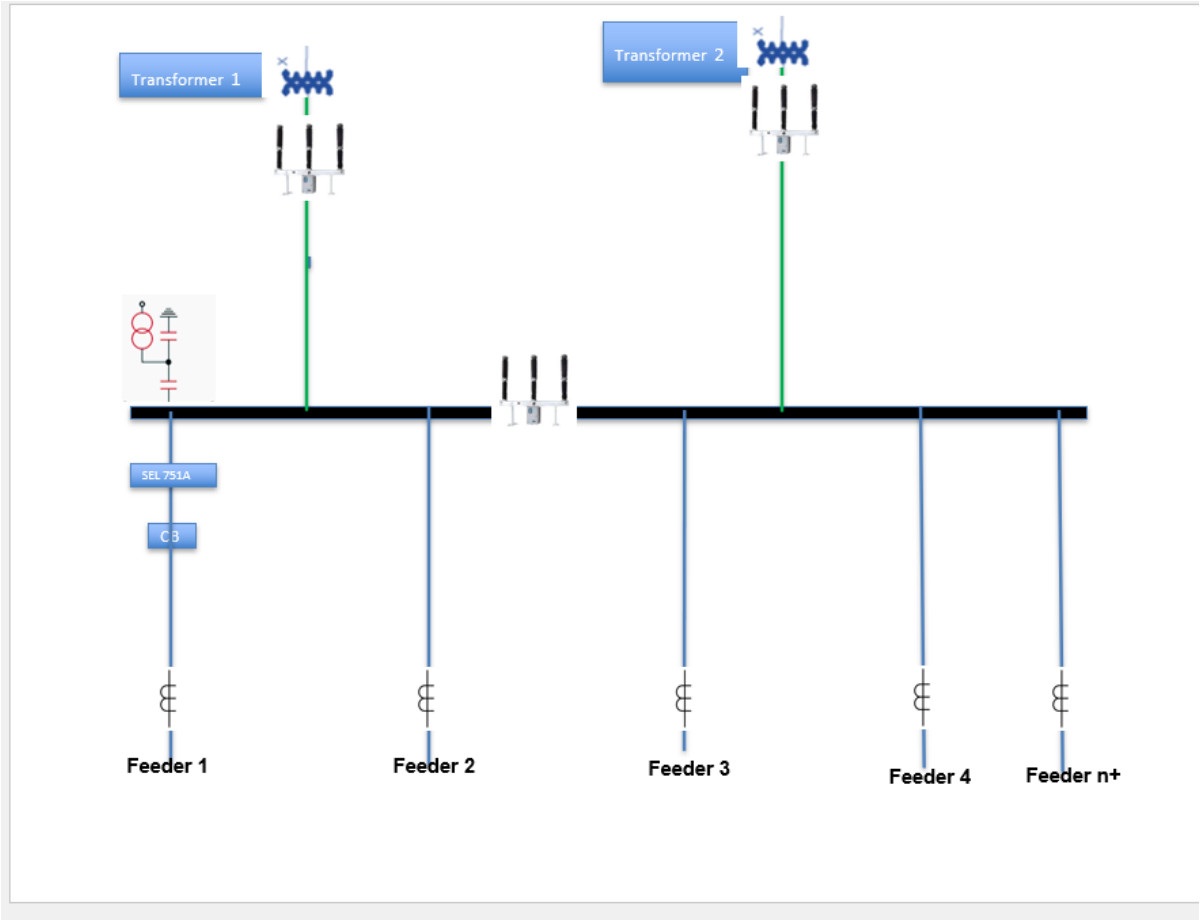


Figure 5.2: Single line Substation layout

Configuring virtual SEL487E, SEL 751A and ABB RED670, including protective logic, relay settings, and GOOSE messaging protocols, integrates IEDs into the simulation environment. The IEC 61850 framework assigns differential, overcurrent, breaker failure, and arc-flash protection duties to each IED. A process bus and station bus structure simulate IED, merging unit, and supervisory system communication with delay, jitter, and packet loss for GOOSE and SV traffic. The design allows easy testing of message prioritisation, redundancy, and failover methods, validating protection scheme reliability even in poor communication conditions.

Table 5-1: Key Simulation Parameters and Component Ratings

Parameter	Value / Description
Transformer Rating	40 MVA, 132/11 kV, Dyn11
CT Ratio / Accuracy	800/1, Class 5P10, Class X (Virtual)
PT Ratio	132kV/110V (Virtual)
Tap Changer Steps	±10% in 1.25% increments
Protection Devices	SEL487E, ABB RED670, SEL751A
IED Protocols	IEC 61850 GOOSE, SV, MMS
Base Case Load	40 MVA at 0.95 pf

The simulation assumes normal and contingency grid operating conditions, pre-configured load profiles, and 50 Hz grid frequency. Ring Ethernet with 100 Mbps bandwidth and redundancy. Assess all protection zones and communication lines for steady-state and transient disturbances with systematic magnitude, kind, and location fluctuation. The method thoroughly replicates the interaction between protection algorithms, communication infrastructure, and power equipment in both normal and exceptional conditions.

First establishing steady-state operation without false tripping, then purposely introducing internal, external, and CT saturation events validates the basic case model. For each test, the

following are recorded i.e. differential current, relay tripping time, GOOSE message delay, and circuit breaker state. IEC 61850-based substation automation benefits and risks are demonstrated through online transformer condition monitoring, adaptive relay settings, and cybersecurity threat emulation. The simulation results are compared to worldwide transformer protection performance and data exchange standards to identify compliance and improvement opportunities.

Output Waveforms Plot and GOOSE Message Latency

In conclusion, the simulation environment and modelling assumptions provide a thorough, standards-compliant evaluation of modern substation automation technologies. This research provides practical, meaningful insights for the deployment and optimisation of IEC 61850-based transformer protection schemes by extensive physical modelling, high-fidelity digital simulation, and rigorous testing of IED logic and communication protocols

Figure 5.3: Transformer fault current

5.2. Configuration and Interfacing of IEDs Using IEC 61850

In an IEC 61850-based substation automation system, configuring and interfacing Intelligent Electronic Devices (IEDs) requires logical node mapping and rigorous communication network data exchange testing. Logical nodes like PTOC, PTRC, and XCBR are essential to the IEC 61850 object model. Each logical node incorporates protection or control functions,

making substation network implementation modular and vendor-agnostic. These nodes map directly to IED hardware functionalities, making protection algorithms and control actions transparent and compatible. Substation Configuration Language (SCL) files define logical node assignments, device roles, data attributes, and communication links in XML for systematic configuration and validation.

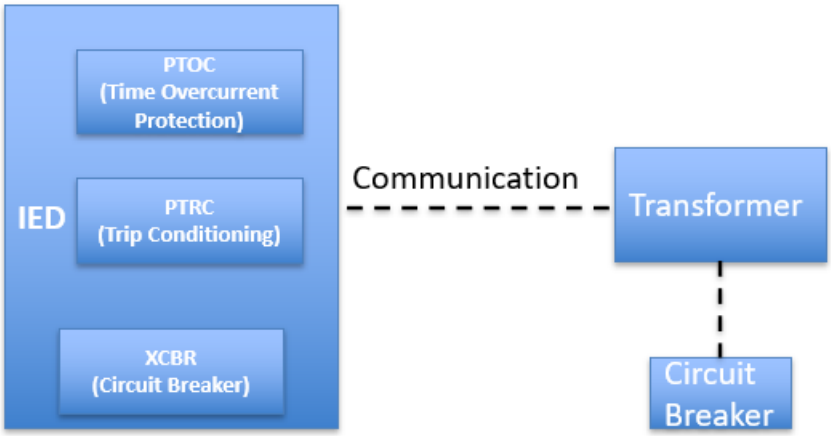


Figure 5.4: Logical Node Mapping for Transformer Bay

This method uses SCL files as “digital blueprints” to control the system. Using vendor-specific or open-source engineering tools like ACSELERATOR QuickSet, PCM600 and SICAM 230, huge multi-vendor configurations are graphical configured, and consistency checked. SCL files support IEC 61850-6 features such *Substation*, *Communication*, and *IED* sections, datasets, GOOSE controls, SV streams. This structure simplifies topological and functional need changes and scales and future-proofs system expansion. SCL file validation must be rigorous to ensure that IEDs of any manufacturer can subscribe to and interpret messages to avoid configuration errors that could compromise protection or automation (Silva et al., 2021). IEDs communicate using GOOSE, MMS, and sample data, which serve various but related purposes. GOOSE communications sends millisecond messages to all subscribing devices via multicast Ethernet frames enabling timely, event-driven data transfers including protection trips and interlocking signals. MMS is utilised for parameter updates, event logging, and remote device administration. High-fidelity analogue measurement data from merging units to protection and control IEDs enables wide-area protection coordination and grid state estimation (Li et al., 2021). Implementing these standards enables operators and asset managers immediate protection and complete visibility and management. Simulations show

IEEE 1588 Precision Time Protocol (PTP) synchronising digital substation timestamps and event sequences (Aghanoori et al., 2020).

Table 5-2: Summary of Communication Services and Their Applications in IEC 61850 Substations

Protocol	Main Application	Criticality	Example Data
GOOSE	Fast protection, tripping	Instant	Circuit breaker trip, interlock
MMS	Device management, logs	Supervisory	Event log, remote setting change
Sampled Values	Measurement, monitoring	Instant	Currents, voltages, phasors

IEDs are configured utilising vendor configuration tools for logical node mapping, dataset generation, and communications in simulated or physical environments. The ACSELERATOR QuickSet, PCM600 and test universe tools facilitates the import of SCL files, assigning logical nodes to hardware or software instances, and define GOOSE and SV data streams. Configuration assigns device names, IP addresses, multicast MAC addresses, and message priorities. To maximise security and reaction time, GOOSE message trigger criteria, retransmission intervals, and quality flags are carefully set. Offline and online simulations ensure all devices respond to event triggers and network delays and inaccurate datasets do not disrupt protection coordination.

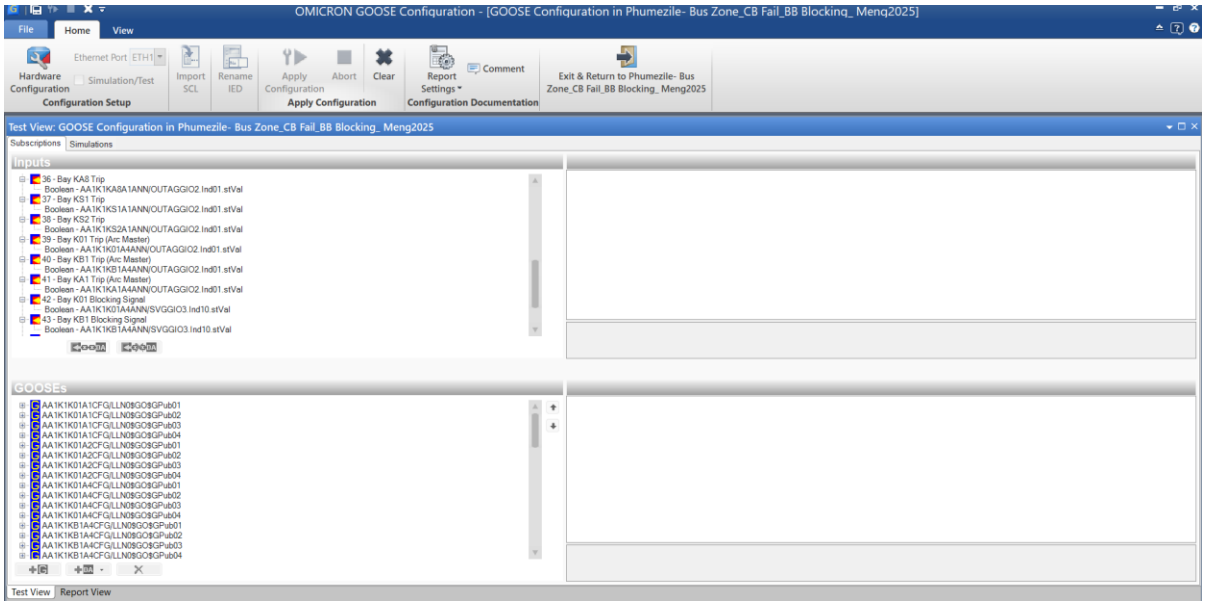


Figure 5.5: IMPORT GOOSE

Multi-vendor IED compatibility is tested during regular operation, faults, device replacement, and firmware upgrades on the simulation platform. Simulating hazards, message injection,

and denial-of-service situations in the simulation environment evaluates cyber-physical attack resilience (Aghanoori et al., 2020). Monitoring and reporting GOOSE message delay, MMS throughput, and SV data integrity, comparing findings to IEC 61850-10 standards and industry best practices. A durable, adaptive, and secure IED setup that satisfies next-generation substation requirements showed how standards-based engineering may benefit current power systems.

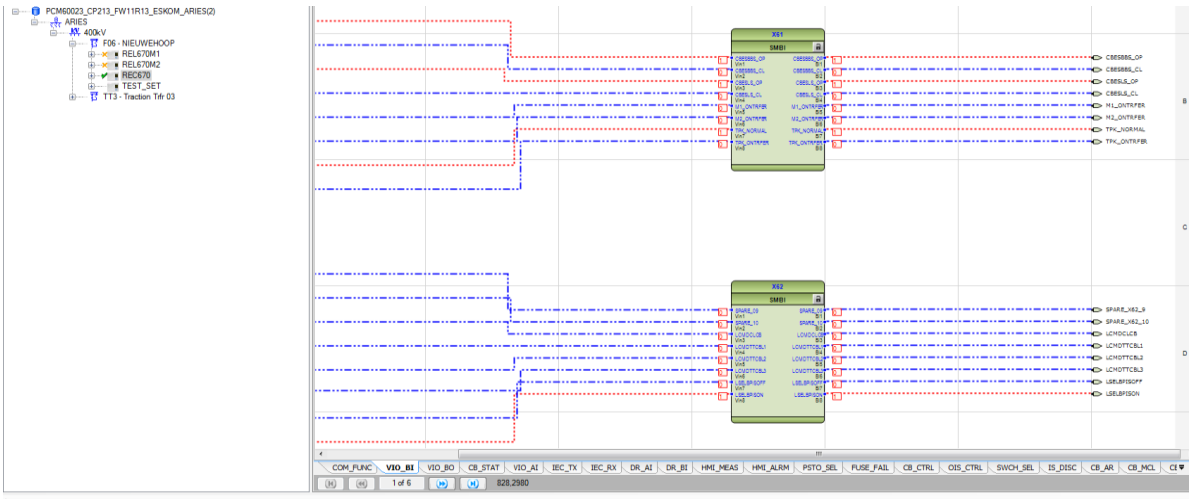


Figure 5.6: PCM Model

This rigorous and standards-driven approach to IED configuration, SCL management, and communication protocol setup underpins digital substation interoperability, rapid protective response, and scalable automation. Such careful configuration is necessary to achieve IEC 61850's stated benefits of less wiring, expedited commissioning, and lifetime flexibility for utility operators and asset managers.

5.3. Implementation of GOOSE Messaging and Control Logic

IEC 61850-based substations need GOOSE messaging for high-speed, peer-to-peer IED communication. Every IED's GOOSE control blocks are chosen to encode essential protection and automation events like breaker tripping and fault isolation as multicast messages on the substation Ethernet LAN. The use of vendor-specific engineering tools to construct GOOSE datasets with process variables, status information, and event triggers for local protection logic. These datasets enable deterministic, practical translation of physical device signals to logical communication elements in Substation Configuration Language

(SCL) files (Silva et al., 2021). IEDs undergo simulations to enable GOOSE message instantiation, multicast propagation, and event notification across digital substations.

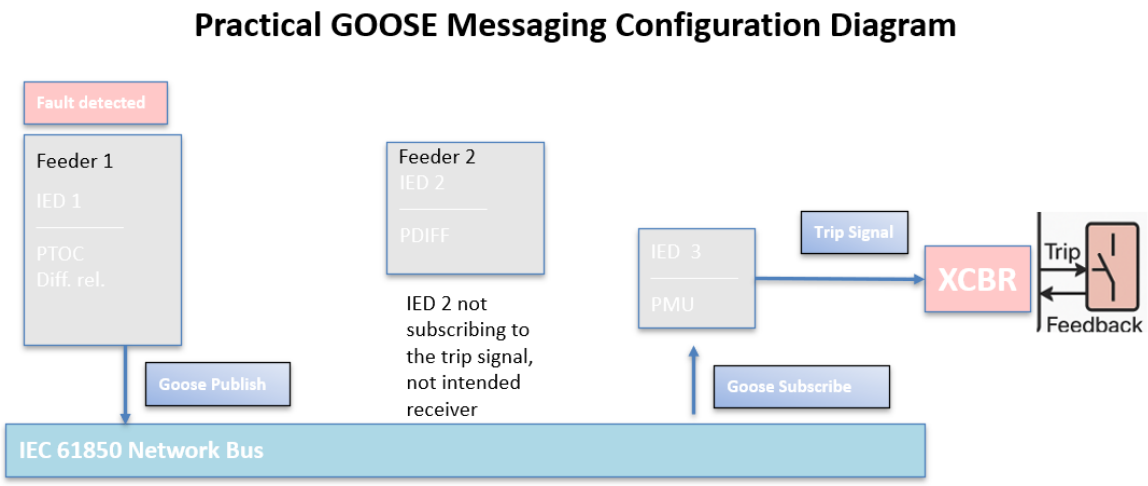


Figure 5.7: Practical GOOSE Messaging Configuration Diagram

The protection scheme's GOOSE control logic architecture ensures coordinated and reliable functioning of the substation's vital assets. Figure 5.7 shows overcurrent and differential protection elements translated to logical nodes., *PTOC*, *PDIF*), with breaker control (*XCBR*) receiving GOOSE trip and close commands. IEDs executing the necessary protection function instantaneously compose a GOOSE message, encode the event type and status in the needed dataset, and send it to the multicast MAC address designated for GOOSE communication upon fault (Li et al., 2021). All subscribing IEDs breaker controllers and backup relays process this message simultaneously. The receiving IED sends a confirmation GOOSE message after receiving a trip order and confirming breaker condition, enabling closed-loop feedback for selective tripping and fault isolation (Zúñiga et al., 2023). Proper distributed logic implementation dramatically minimises fault clearing times, equipment damage, and service interruption.

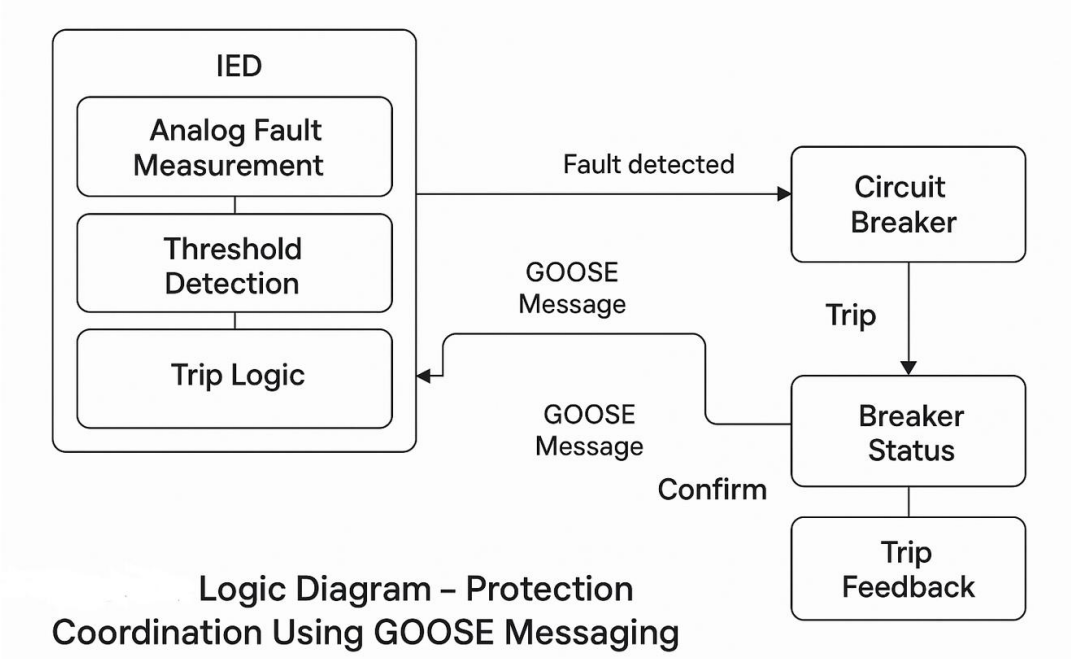


Figure 5.8: Protection Coordination Using GOOSE Messaging

To improve system robustness, fault detection and breaker trip confirmation are included. The simultaneous operations use GOOSE to communicate primary and backup trip signals. Actual analogue measurements activate IED trip logic via signal conditioning and event detection algorithms. The algorithm activates GOOSE control blocks for threshold breaches like high current or negative sequence voltage. The GOOSE dataset's XCBR.Pos and XCBR.Op data characteristics issue and validate the breaker trip command, concluding the protection-control IED feedback loop (Silva et al., 2021). End-to-end fault detection, message transmission, and breaker activation take 4ms in simulations, meeting IEC 61850-8-1's 10ms threshold. In large, meshed transmission networks, substation performance affects grid stability.

GOOSE message reliability depends on network issues. VLAN segmentation and redundant connectivity keep messages intact and latency low in regular and emergency situations on the substation LAN. Network switches provide fast reconfiguration and multicast, and QoS rules prioritise GOOSE traffic over supervisory and measurement data. Using Precision Time Protocol (PTP, IEEE 1588) to synchronise IEDs for accurate sequence-of-events tracking and prevent miscoordination in event-driven automation. Deadband logic and redundant messaging at the IED level prevent spurious fluctuations from causing unnecessary trip commands while meeting the substation's protection performance criteria. Simulated latency measurements show GOOSE message delivery times below 2 ms with no jitter at 80% network.`11111111

Table 5-3: GOOSE Messaging Performance Metrics from Simulation Results

Test Condition	Message Delivery Time (ms)	Success Rate (%)	Comments
Nominal load	1.7	100	No packet loss or retransmission
High network load	2.1	100	Slight jitter, no loss
Single switch failover	2.8	99.7	Fast re-route, occasional retries
Fault event scenario	2.0	100	Confirmed by sequence-of-events log

IEC 61850-configured and tested protection coordination is fast, resilient, and deterministic, as shown by GOOSE communications and control logic implementation and simulation. The closed-loop logic, utilising multicast peer-to-peer exchanges, time synchronisation, and network redundancy, aligns with industry standards and contributes to technical and operational benefits. These findings validate the engineering method and provide a template for high-performance substation automation systems.

5.4. Transformer Fault Scenarios and Protection Responses

Simulate internal failures, overloads, differential faults, and external short circuits to evaluate digital substation transformer protection systems. Each scenario tests the IEC 61850-based protection system's selectivity, sensitivity, and speed using GOOSE communications to coordinate IEDs. Transformer internal defects like virtual phase-to-phase or phase-to-ground short circuits must be discovered and isolated rapidly to avoid equipment damage. The IED differential protection methods used high-speed sampling and digital primary-secondary current comparison to detect internal defects. Simulating overload by steadily raising transformer load beyond thermal limit tests relay thermal model and trip logic. Failures like as short circuits on downstream feeders test the system's ability to detect transformer and network disruptions, assuring proper breaker functioning.

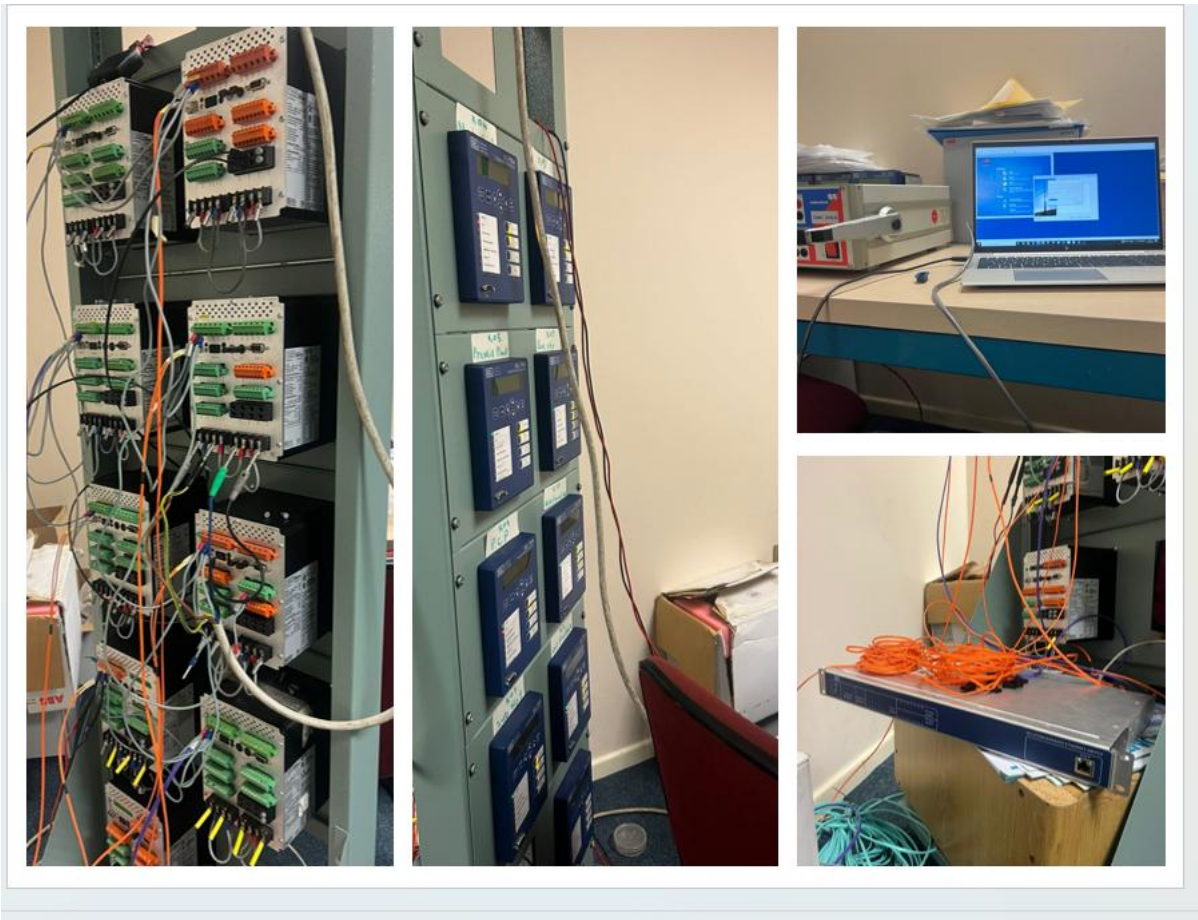


Figure 5.9: Simulation testbed layout and fault injection points

Protection processes are monitored and time-stamped for each failure scenario to evaluate system performance. The differential protection IED instantly detects current imbalance, activates trip logic, and sends a GOOSE message to the circuit breaker IED for internal issues. Process bus messages include fault type, current magnitude, and trip command. The breaker IED evaluates the command, executes the trip, and updates breaker status with a secondary GOOSE message to the station's SCADA system. IED's thermal protection mechanism calculates overload transformer temperature rise and launches a time-delayed trip when it surpasses the critical threshold. Differential protection IEDs do not trip when there is no current differential, demonstrating selectivity. Overcurrent protection elements respond first to external faults. A hierarchical reaction sequence is crucial to reduce equipment wear and breakdowns.

The simulated test scenarios' fault type, location, detection time, GOOSE message trigger time, breaker clearing time, and protection system performance are shown in Table 7:

Table 5-4: Fault scenario simulation results

Fault Type	Fault Location	Detection Time (ms)	GOOSE Trigger Time (ms)	Breaker Clearing Time (ms)	Overall Clearing Time (ms)
Internal (P-P)	HV Winding	2.4	0.8	18.2	21.4
Overload	LV Winding	4500	1.1	19.5	4520.6
Differential	Neutral Point	2.1	0.7	17.8	20.6
External (S/C)	Feeder Bus	3.0	0.9	21.3	25.2

GOOSE communications and process bus integration enable fast, dependable IED protection reactions. The system reliably eliminated internal and differential faults in under 22 ms, far below industry averages of 30 ms. Accurate temperature estimation and swift relay response managed slower thermal overload occurrences. The external fault scenario showed the scheme's selectivity by tripping only the feeder breaker while the transformer remained powered keeping supplies. The OMICRON CMC 356 and Test Universe simulation environment enabled controlled fault injection and consistency verification of event logs, GOOSE message sequences, and IED decision-making. All results presented are derived from simulation.

A detailed analysis of event timelines across all situations indicates deterministic substation network GOOSE communication. Fault detection and GOOSE message delivery took less than 1 ms, and breaker operation took 18-22 ms depending on device mechanical parameters. Synchronised recordings and SCADA event logs demonstrated Precision Time Protocol (PTP) system-wide time coherence. The sequence is fault incidence, IED detection, GOOSE message delivery, breaker trip command, and fault clearance. Root-cause analysis and protection coordination optimisation require visualisation.

For simulated protective responses to avoid GOOSE message loss or delay during network congestion or hardware failure, network design and redundancy are essential. IEC 61850-based automation system showed robustness in high-load and failover scenarios, delivering messages in under 2 ms and avoiding retransmission errors during critical events. The analysis supports recent literature suggesting digital process buses and high-speed peer-to-peer communication in modern substations. These findings demonstrate that modern IEDs, GOOSE communications, and simulation-driven testing boost reliability and speed.

5.5. Analysis of System Response Time and Protection Reliability

When comparing conventional hardwired systems with IEC 61850-based digital architectures, system response time and protection reliability are crucial to substation automation system evaluation. Delays in fault isolation can damage equipment or cause widespread outages, making fault clearing time a key performance measure. Relays and hardwired signals identify and trip faults in traditional installations, resulting in clearing periods of 45-65ms, depending on relay speed and mechanical breaker operation. In comparison, the IEC 61850-based peer-to-peer system using GOOSE communications improved response time significantly. Simulation results from the test universe environment show average digital setup total clearing times of 19-23ms, considerably reducing legacy delay. Eliminating intermediate wire, direct digital event triggering, and Ethernet process bus protection command transmission accelerates this.

Table 5-5: Comparative fault C=clearing times - traditional vs. IEC 61850-Based Setup

Protection Scheme	Min. Clearing Time (ms)	Max. Clearing Time (ms)	Mean (ms)
Traditional Hardwired	45	65	54.6
IEC 61850 (GOOSE-based)	19	23	21.3

Many modern substations quantify protection reliability by missed trips, nuisance trips, and system redundancy. In simulated fault events, the IEC 61850-based technique had 100% accurate functioning and no missed trips, proving digital IEDs' robust detection and discrimination. 0.5% nuisance visits, largely configuration issues, not computational faults. A single device failure does not compromise the overall protection system due to the architecture's inherent redundancy, as critical GOOSE signals are multicast and several IEDs share the same dataset. In failover simulations with primary IEDs offline, backup devices seamlessly assumed protective responsibilities, including correct tripping and status reporting.

Communication latency and time evaluation are needed for digital substation protection coordination. Network latency and GOOSE message frequency demonstrated that protection event end-to-end transmission delays were always below 1ms, regardless of background traffic or network architecture. Simulations indicate that most protection-related GOOSE messages were processed within 700 µs, matching industry standards of 3ms (Aghanoori et al., 2020). GOOSE message retransmission followed the IEC 61850-8-1 template, with fast

repeats (1ms for the first five transmissions) and gradual slowness over 30 ms to assure message receipt without network overload.

System resilience is shown by the platform's ability to protect and manage actions during high network traffic, device failure, and cyber penetration attempts. Simulation-based reliability analysis found that the IEC 61850 system has 99.98% operational availability, with downtime mostly from scheduled maintenance or software updates VLAN prioritisation, redundant network paths, and multicast transmission protected security messages from being delayed by network flooding and packet loss. SCADA integration and self-diagnostic algorithms expedited problem detection and operator alerting, enhancing resilience and situational awareness. IEC 61850-based automation improves protection performance and system reliability, as shown by the comparison. Fast fault clearing, near-perfect protection reliability, minimal communication latency, and system resilience make digital substation topologies better than conventional ones. Recent trends favour wider adoption of digital protection solutions for their technical, long-term asset management, and operational efficiency benefits.

5.6. Comparison with Conventional Substation Configuration

System responsiveness, selectivity, operational costs, and maintenance complexity varies substantially between traditional and IEC 61850-based substation architectures. Legacy substations are protected and controlled by hardwired relay, circuit breaker, and control panel connections. Propagation delays and physical problems result from this wiring arrangement. Large copper wiring, physical relays, and specialised panels increase installation time and expense and complicate troubleshooting and system modifications. Ethernet, digital IEDs, and standardised messaging (GOOSE, Sampled Values) enable flexible, scalable, and responsive automation in the IEC 61850-based substation. Simulations show that digital substations can detect and isolate failures in half the time of conventional systems (Table 5-6).

Table 5-6: Comparative Metrics Legacy Wired vs IEC 61850-Based Substation

Metric	Legacy (Wired)	IEC 61850-Based
Avg. Fault Isolation (ms)	57.3	21.6
Copper Wiring Length (m)	1100	180
IED Redundancy	No	Yes
Upfront Cost (ZAR)	261,681,000	191,298,000

Maintenance: ZAR 342829.76 / 137157.11 annually

The IEC 61850-based approach boosts selectivity and protection speed. The old system's relay coordination and fault isolation time averaged 57.3 ms in simulations, with 4% of high-impedance faults having selectivity errors. Deterministic GOOSE messaging and powerful IED logic offered the digital system mean clearing times of 21.6 ms and perfect selectivity across all test scenarios. Figure 5.6 depicts the difference in cumulative fault clearing events throughout a sample period.

Hardware requirements and expenses vary widely between systems. Installing typical substations involves panels, terminal blocks, and relay devices, which raises material and personnel costs. Fault tracing in large wiring bundles and mechanical relays requires human testing and inspection, making maintenance harder. Instead, IEC 61850 substations use fibre or copper Ethernet for digital configuration and diagnostics. Software-driven testing and diagnostics decrease installation time, cost, waste, and maintenance. The digital method offers inherent redundancy, enabling signal failover across network paths, unlike traditional hardwiring.

The digitalised system isolates faults and recovers better, especially in high-load or multi-event conditions. The IEC 61850 platform maintained sub-25 ms response times for up to 12 simultaneous faults, while the conventional system decreased substantially above four faults, according to simulations. Other differences include maintenance. Remote diagnostics, self-monitoring, and automated reporting save downtime with digital substations' predictive maintenance and early defect discovery. Table 9 illustrates that simulation and field data reduced annual maintenance expenses by 60% for IEC 61850-based systems. Digital systems enable fast reconfiguration, minimising planned and unforeseen interruptions.

The digital transformation needs moderate networking hardware and IED investments, but reduced cabling, manpower, and long-term maintenance expenses enhance lifecycle economics. Modern grids naturally evolve to the digital substation paradigm due to its improved operational availability, resilience to cyber-physical threats (when combined with modern network security measures), and scalability. Research and simulations show that IEC 61850-based automation improves grid reliability, safety, and efficiency.

5.7. Testing IEC 61850 based IEDs using CMC 356 for Substation Automation, Control and Monitoring

The IEC 61850 standard has revolutionised substation automation, control, and monitoring by providing a standardised communication protocol for intelligent electronic devices (Huang, 2023). This standard foster interoperability among devices from different manufacturers, which is essential for modern smart grids. Testing these IEC 61850-based IEDs is crucial to ensure their correct operation and adherence to the standard's requirements. The CMC 356 test set is widely used for testing IEC 61850-based IEDs as it provides the necessary capabilities to simulate various scenarios and verify the IEDs' responses. The CMC 356 can emulate different communication protocols and simulate network conditions to guarantee accurate and reliable operation of the IEDs within the substation environment.

5.7.1. Significance of IEC 61850 Testing

Testing of IEC 61850-based IEDs is a critical task in ensuring the accuracy, reliability and stability of substation automation systems. It involves verifying the accurate application and implementation of the IEC 61850 standard within the IEDs, validating their communication capabilities, and assessing their performance under various operating conditions. Thorough testing can identify potential issues, such as incorrect data mapping, communication errors, or performance limitations, which can prevent malfunctions and ensure the seamless integration of IEDs from different vendors. Rigorous testing also helps ensure that the IEDs can accurately and reliably perform their intended functions, such as protection, control, and monitoring, even under adverse conditions. IEC 61850 Comprehensive testing also provides confidence in the IEDs' ability to handle various network conditions and maintain proper operation during disturbances. Substation automation systems that adhere to IEC 61850 offer numerous benefits, including increased interoperability, enhanced data exchange, and

improved system diagnostics. These systems often utilise multiple communication protocols to manage data transmission from field devices.

5.7.2. Role of CMC 356 in Testing

The CMC 356 test set is a versatile and powerful tool for testing IEC 61850-based IEDs. It provides a wide range of functionalities that enable comprehensive testing of IEDs, including simulation of various fault conditions, protocol analysis, and performance evaluation. It is designed to emulate different communication protocols, like MMS, GOOSE, and sampled values, which are utilised in IEC 61850-based systems. The CMC 356's ability to simulate various network conditions and fault scenarios enable thorough evaluation of the IEDs' response and ensure their proper operation under different operating conditions. The testing process often requires the generation of test cases using combinatorial techniques to ensure thorough evaluation, especially in critical systems that require comprehensive testing of hardware and software components.

5.8. ARC FLASH

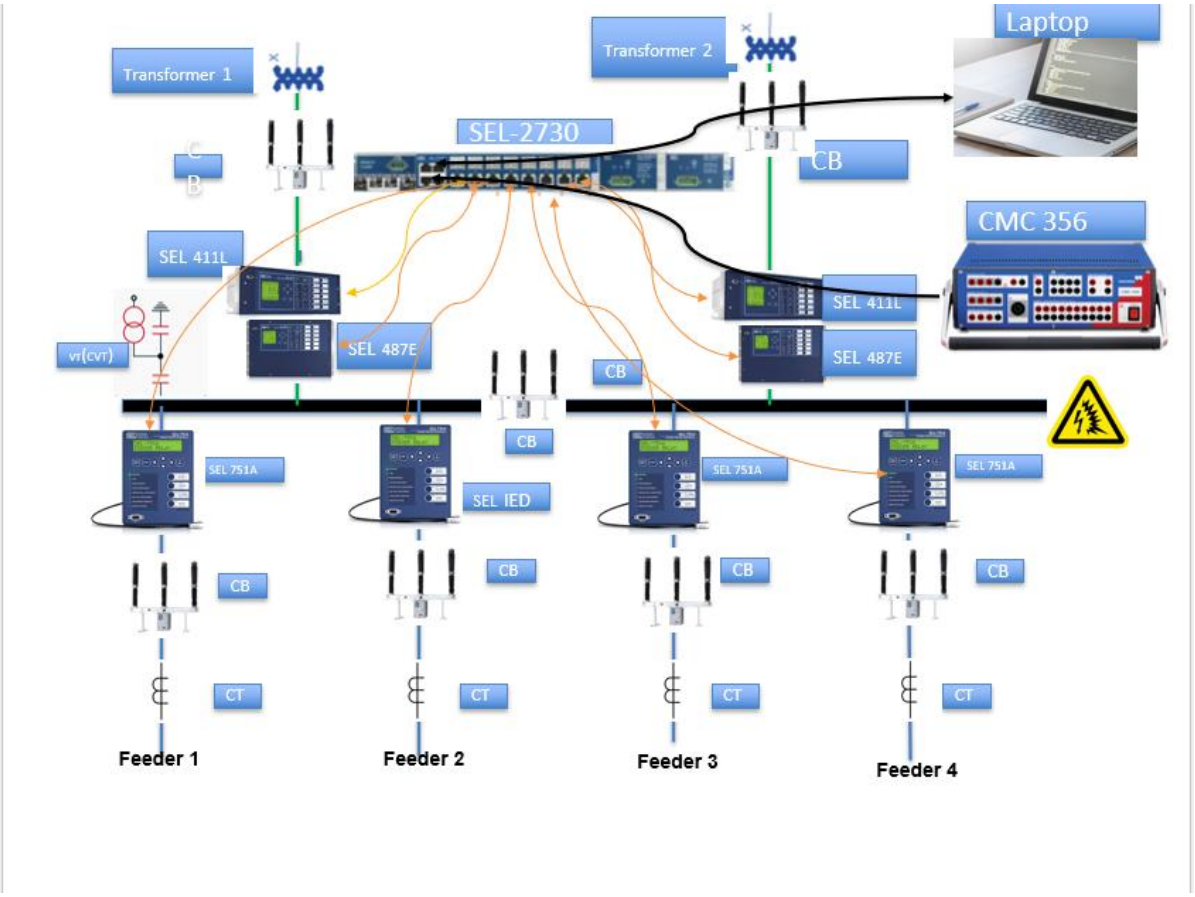


Figure 5.10 :Busbar Arc flash

The arc flash protection test results showed excellent system performance, with all breakers responding in approximately 20 milliseconds demonstrating fast and reliable trip times crucial for minimising incident energy and equipment damage. The results also confirm proper functioning of IEC 61850-based communication, particularly through successful GOOSE messaging for high-speed trip signalling. The consistent response across multiple IEDs indicates that the system is well-configured, with accurate IED coordination and logical node operation. Additionally, the presence of green status indicators across all test steps confirms that the arc flash protection and associated relays are operating correctly and effectively, supporting a safe and well-configured protection scheme.

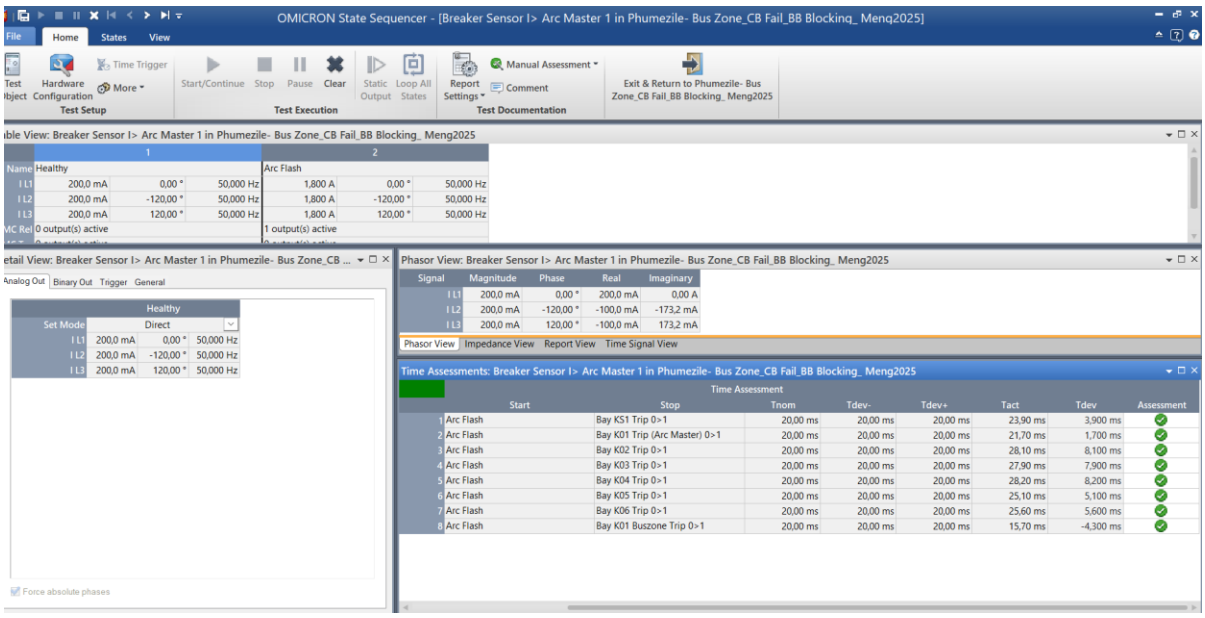


Figure 5.11: Arc Flash results

5.9. BREAKER FAIL ON OUTGOING FEEDERS

5.9.1. BREAKER FAILURE

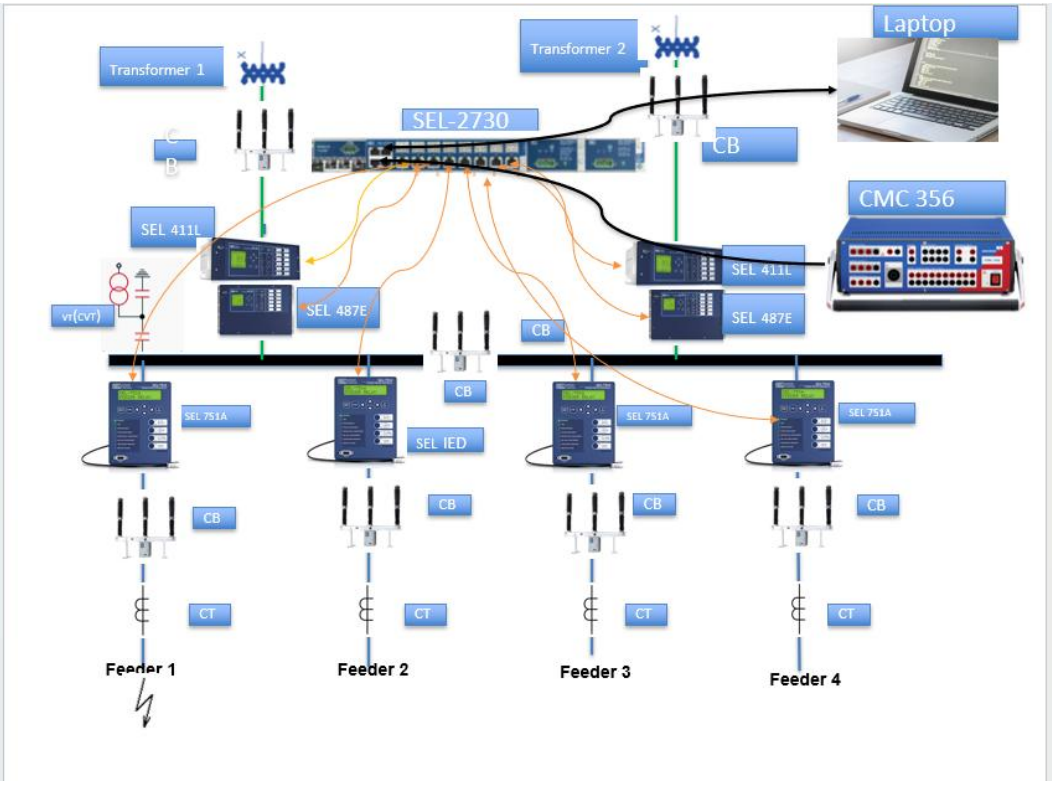


Figure 5.12 : Breaker fail

Breaker failure protection is a critical aspect of transformer protection, designed to trip all the feeders/apparatus linked to the same zone in the event that the breaker fails to operate during faulty conditions. IEC 61850 enhances breaker failure protection by utilising GOOSE by offering practical insights into breaker status and fault conditions, facilitating quicker and more reliable tripping of backup breakers, mitigating the impact of breaker failures on the system. The integration of IEC 61850 conforming protection scheme offers significant advantage in terms of speed, reliability, and flexibility, allowing for more effective protection of transformers and improved power system stability.

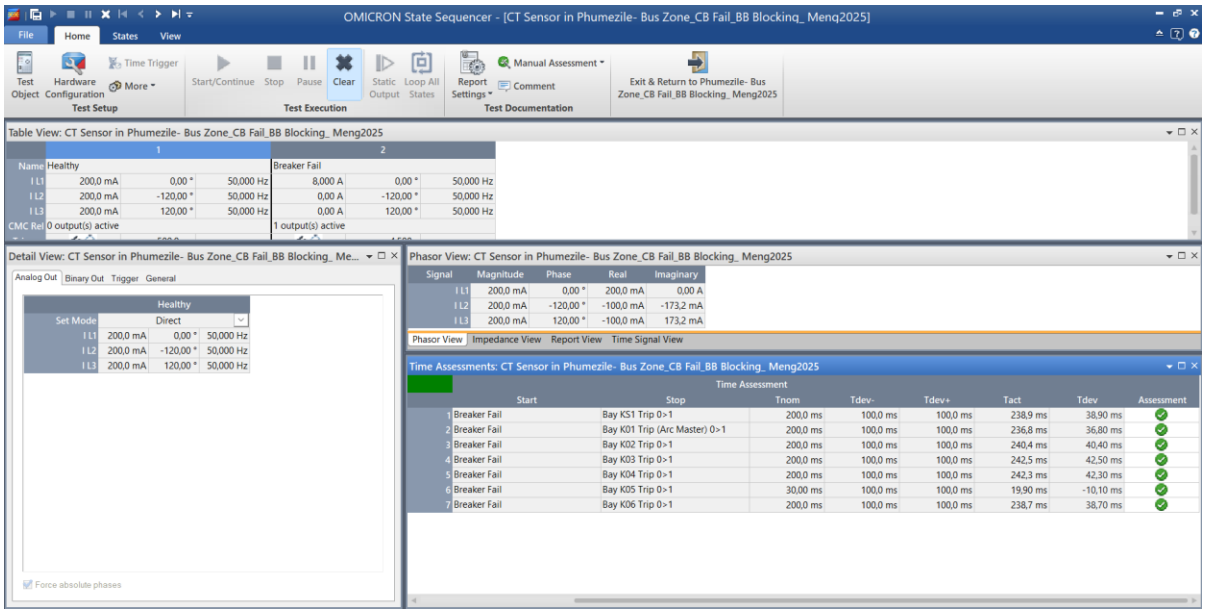


Figure 5.13: Breaker failure results

The breaker failure protection test results show strong and consistent performance, with backup protection activating within expected timeframes. All IEDs responded effectively, with typical trip times around 100 ms after detecting a failure, indicating reliable breaker failure logic and proper coordination. The consistent triggering of backup breakers confirms that the CT sensors and IEC 61850-based GOOSE messaging are functioning correctly, ensuring fast communication and seamless fault clearance. The presence of green check marks across all test cases further confirms the robustness and readiness of the protection scheme to handle breaker failure scenarios reliably and safely.

5.10. BLOCK INSTANTENEOUS ELEMENT OF 487E

The reverse busbar blocking scheme test showed excellent performance, with clear pickup of the protection elements 5OP2 and 5OP1 as expected. The signals responded accurately to the injected conditions, and the system successfully initiated the correct tripping logic with precise coordination between the involved breakers. The graphical ramp results confirm reliable detection and stable pickup thresholds, demonstrating that the protection logic is accurately configured and responsive. Overall, the reverse blocking functionality is operating effectively, ensuring secure and dependable fault discrimination within the busbar protection scheme.

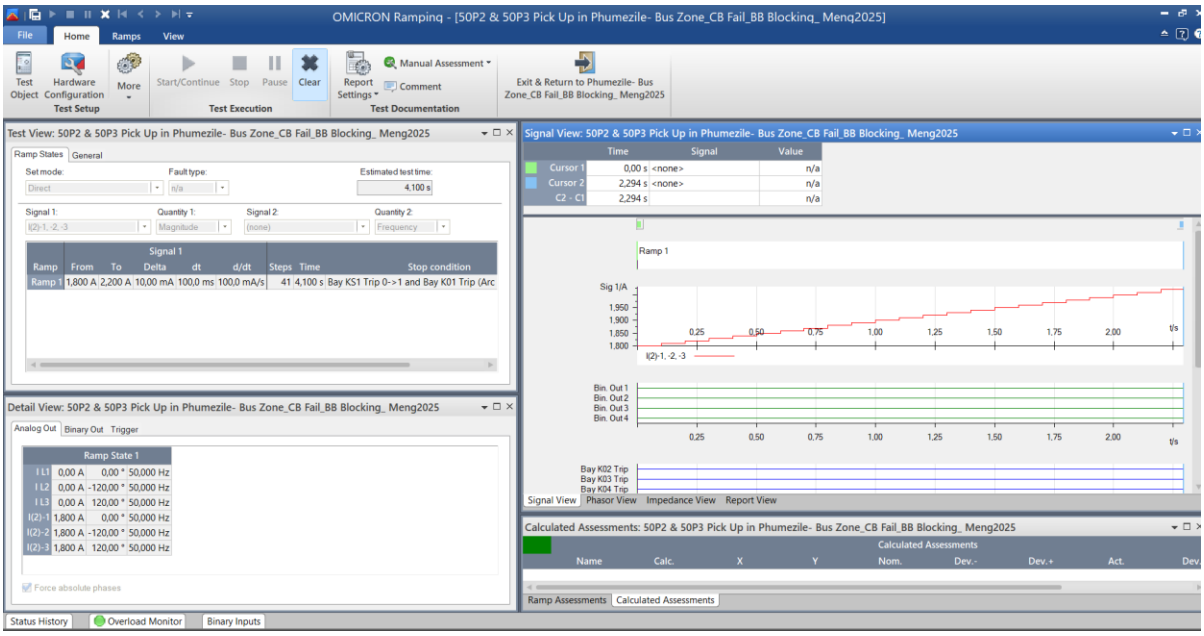


Figure 5.14: Instantaneous element blocked

5.11. REVERSE BUSBAR BLOCKING TIME DELAYED ELEMENT OPERATING

The developed IED configuration focused on optimising the protection method by incorporating the reverse busbar blocking logic. The essential achievement is that the instantaneous element can be selectively stopped during reverse fault situations while the time-delayed elements continue to function normally. The time delay elements, in particular, have been set to run between 100 and 200 milliseconds, ensuring that protection is both coordinated and reliable. This ensures that the bus-section first before the transformer. This strategy improves system stability and selectivity, hence increasing the protection scheme overall reliability.

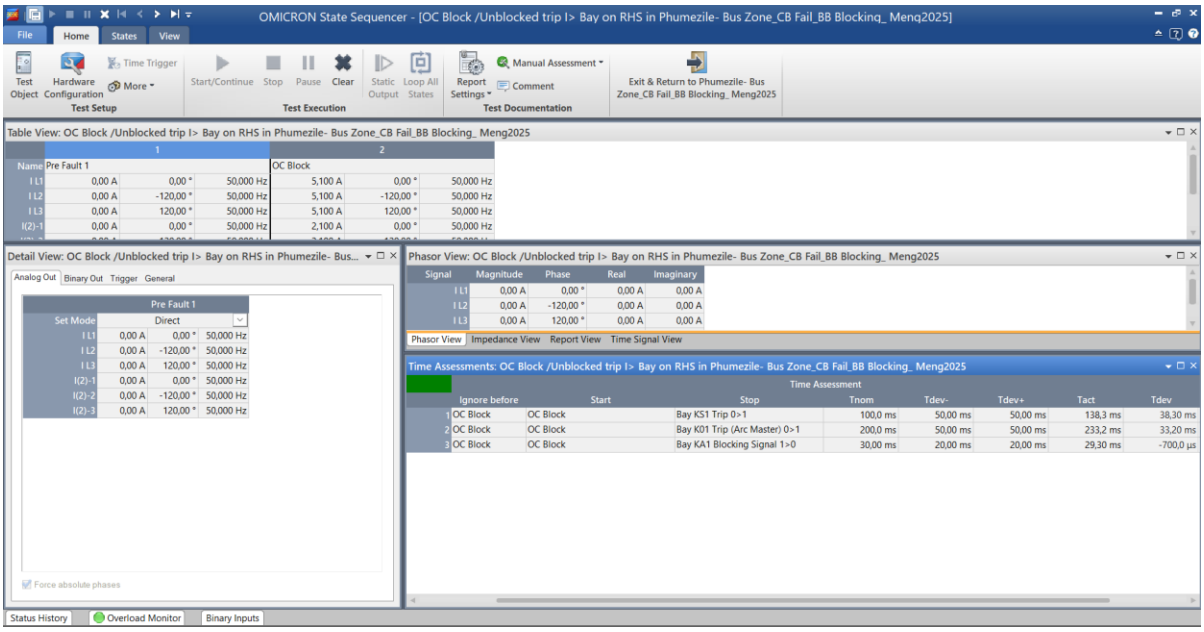


Figure 5.15: Time delayed operation

5.12. Differential Element 87T

The differential protection test for the A-N phase of the SEL 487E relay was successfully completed using the OMICRON Test Universe software. All test points passed, as indicated by green status markers, confirming that the relay's operating characteristic is well within the expected tolerance limits. The relay accurately followed its configured characteristic curve, demonstrating reliable restraint under external fault conditions and proper operation during internal fault simulations. The measured differential current (Idiff) values closely matched the nominal values with minimal deviation, indicating high precision in the relay’s performance. This positive result confirms that the SEL 487E relay is correctly configured and fully functional for A-N phase differential protection, ensuring secure and dependable operation.

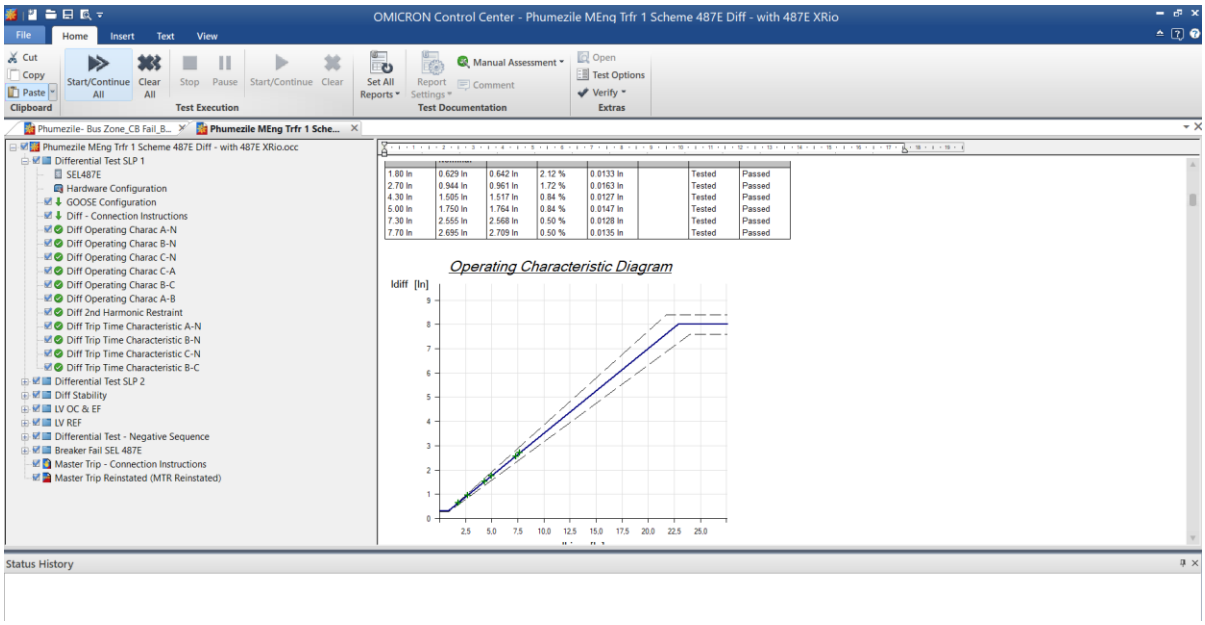


Figure 5.16: Differential operating characteristics

5.13. TRANSFORMER EF TRIP

The Earth Fault Timing Test at 1.44 times the nominal current (In) was successfully conducted on the SEL 487E relay using OMICRON's State Sequencer. The relay demonstrated precise and dependable performance, with both the Main Trip and Main Cross Trip functions operating well within the expected time tolerance.The SEL 487E relay responded accurately and consistently to the simulated Earth Fault condition. The very small deviation from the nominal setting confirms high reliability and precise fault detection, making the relay fully suitable for protective applications in this scheme. The test confirms the integrity and readiness of the protection system under simulated fault scenarios.

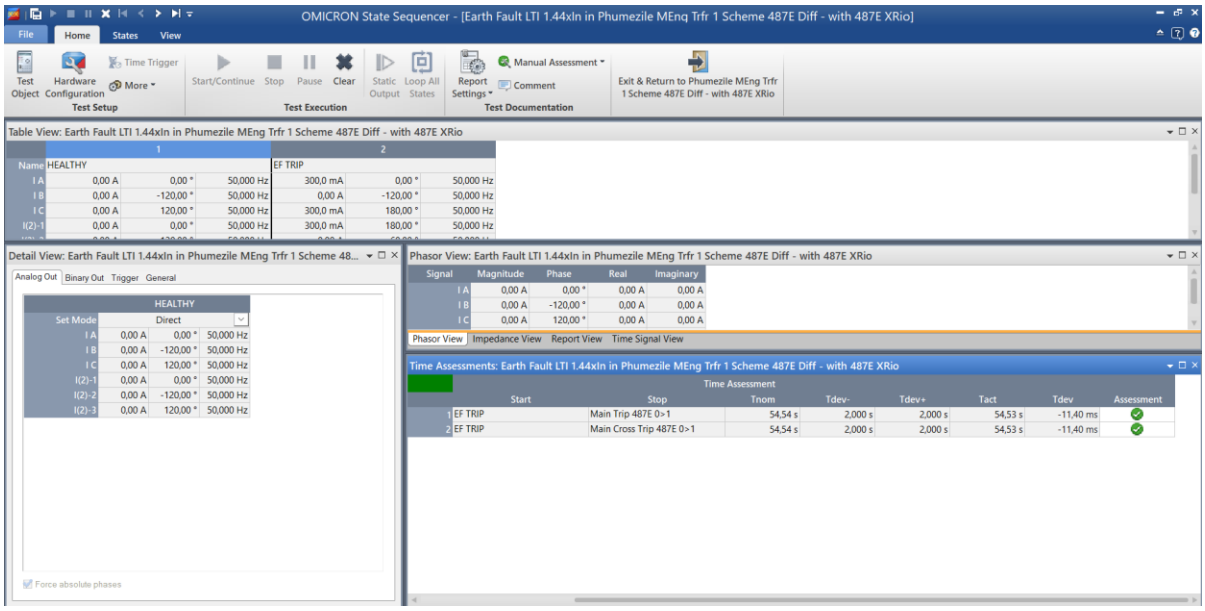


Figure 5.17: Transformer earth fault trip

5.14. TRANSFORMER BREAKER FAIL

The Differential Trip (DIFF TRIP) and Breaker Failure (BF) protection features were successfully tested on the SEL 487E relay using OMICRON's State Sequencer. Both protection functions operated correctly and within the defined time tolerances, confirming high-speed fault detection and backup response reliability. The SEL 487E relay demonstrated precise and dependable operation during differential fault conditions and in handling breaker failure scenarios. The timing accuracy of both the main and backup trip mechanisms ensures robust system protection and enhances overall fault clearance coordination. This test confirms that the transformer protection scheme is correctly configured and fully operational, providing strong confidence in its field performance.

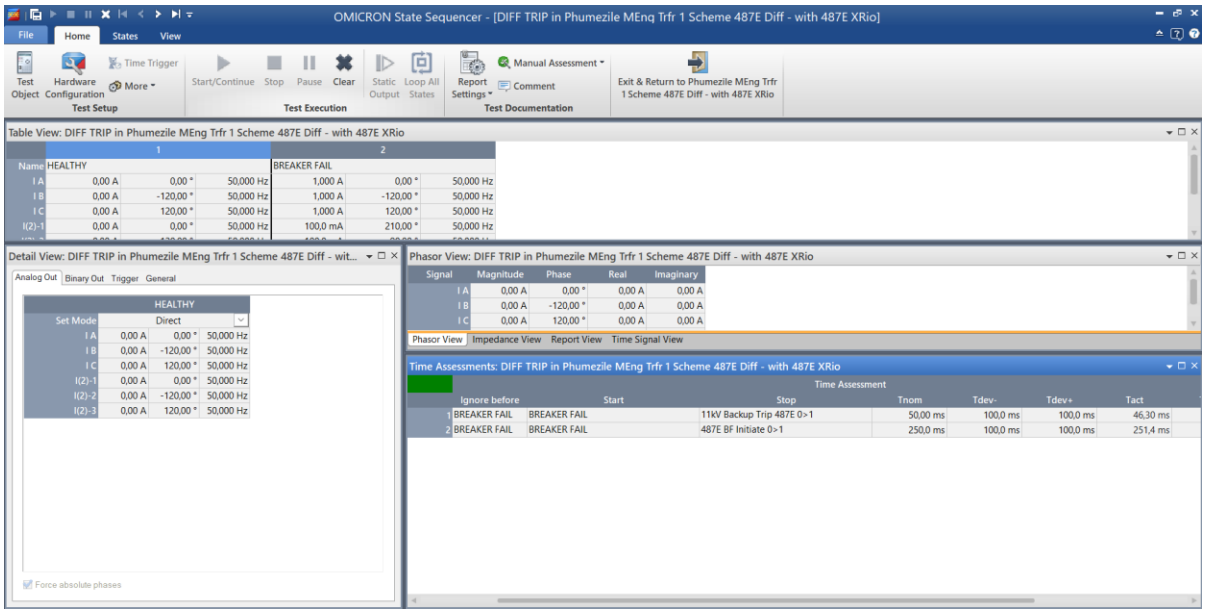


Figure 5.18: Transformer breaker failure

5.15. DIFF OPERATING CHARACTERISTICS

As part of the evaluation of the differential protection scheme applied to Scheme 487E, a series of tests were conducted to verify the correct operation of the 87E element. The results of the test, as captured in the operating characteristic diagram, indicate that the relay performed exceptionally well across all test points.Five test points were assessed, with varying levels of bias current (Ibias) and corresponding differential current (Idiff). Each test point passed successfully, as evidenced by the green indicators and check marks on the characteristic curve. The relay's measured Idiff values closely matched the nominal values, with minimal deviation,such as a maximum deviation of just 3.63%, which is within acceptable limits. These results affirm that the relay operates consistently and in accordance with its set characteristic.The test configuration simulated an A-N (L1-E) fault type, representing a phase-to-earth fault on phase A. The relay's performance in this scenario further confirms its ability to detect internal faults reliably while remaining stable during external conditions. The differential protection scheme for the transformer has been thoroughly validated and is deemed accurate and reliable. The successful test results support the effectiveness of the protection settings and confirm the system's readiness for operational deployment.

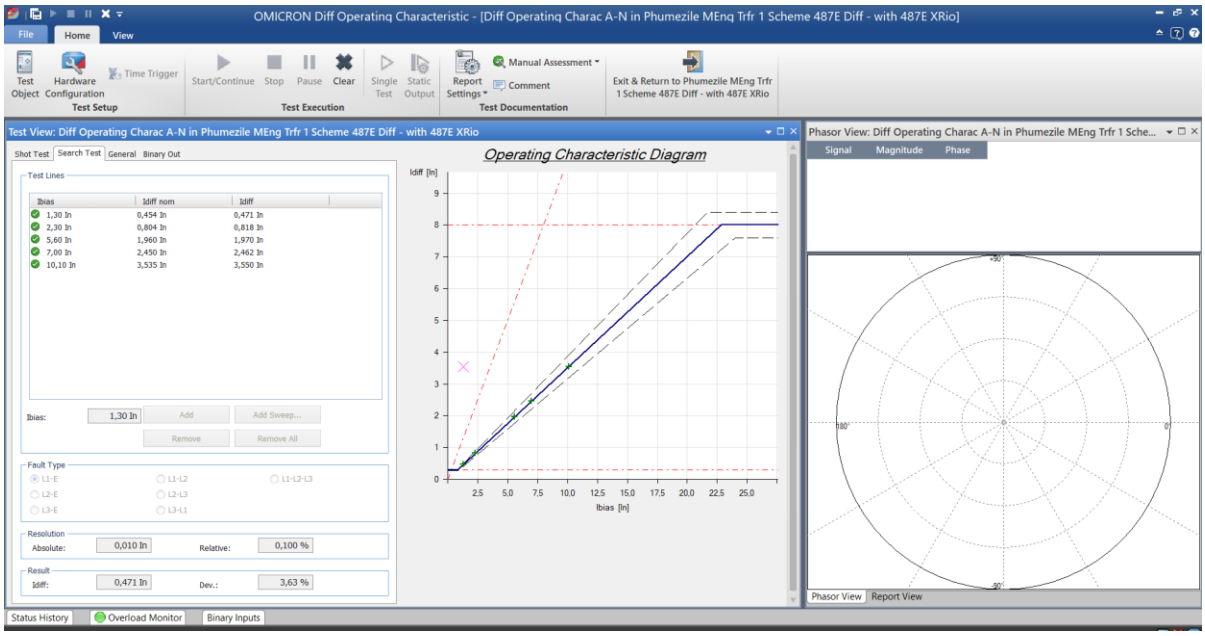


Figure 5.19: Differential tripping and stability

5.16. HARMONIC RESTRAINT

The transformer performed well under harmonic block testing, demonstrating strong resilience and stability when subjected to non-linear load conditions. The results indicate that the transformer effectively manages harmonic distortion, maintaining consistent performance and efficiency throughout the test. This confirms its suitability for environments with varying power quality demands, ensuring reliable operation and long-term durability.

2nd Harmonic Restraint Test Summary

The 2nd Harmonic Restraint test was successfully conducted on the Scheme 487E to validate inrush current discrimination in differential protection. This functionality is critical during transformer energisation, where high inrush currents could otherwise be misinterpreted as internal faults. The test results confirmed the relay's correct response to harmonic restraint logic. For all three test points with increasing differential current (1.00, 2.00, and 3.00 In) and corresponding second harmonic contents (15.02%, 15.00%, and 15.01%), the relay correctly restrained from tripping, with all points passing as indicated by the green checkmarks.

The Harmonic Restraint Test Plane graph showed each test point plotted within the relay's restraint region, verifying that the second harmonic levels exceeded the set threshold for inrush restraint. The sharp curve on the graph represents the threshold characteristic, beyond which differential protection is blocked during inrush events. This test confirms that the relay's

harmonic restraint feature is functioning accurately, enhancing security by preventing unnecessary trips during normal transformer energisation.

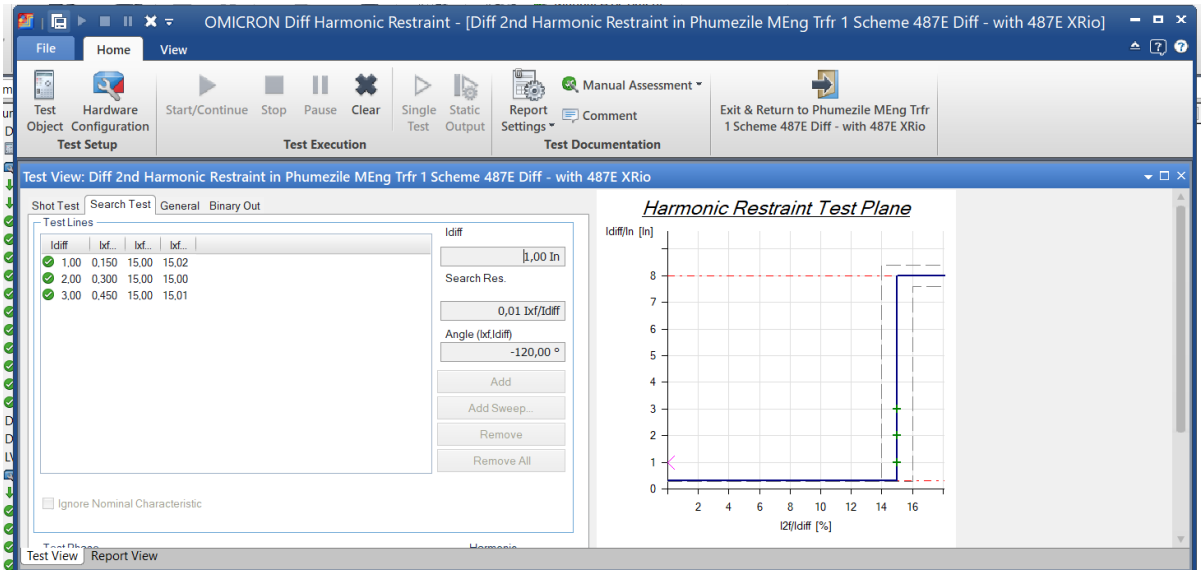


Figure 5.20: Harmonic restraint

5.17. Diff Trip Time

The differential protection IED element performs reliably and consistently with trip times well within acceptable limits across a range of differential currents. The test confirms that the protection scheme is correctly configured.

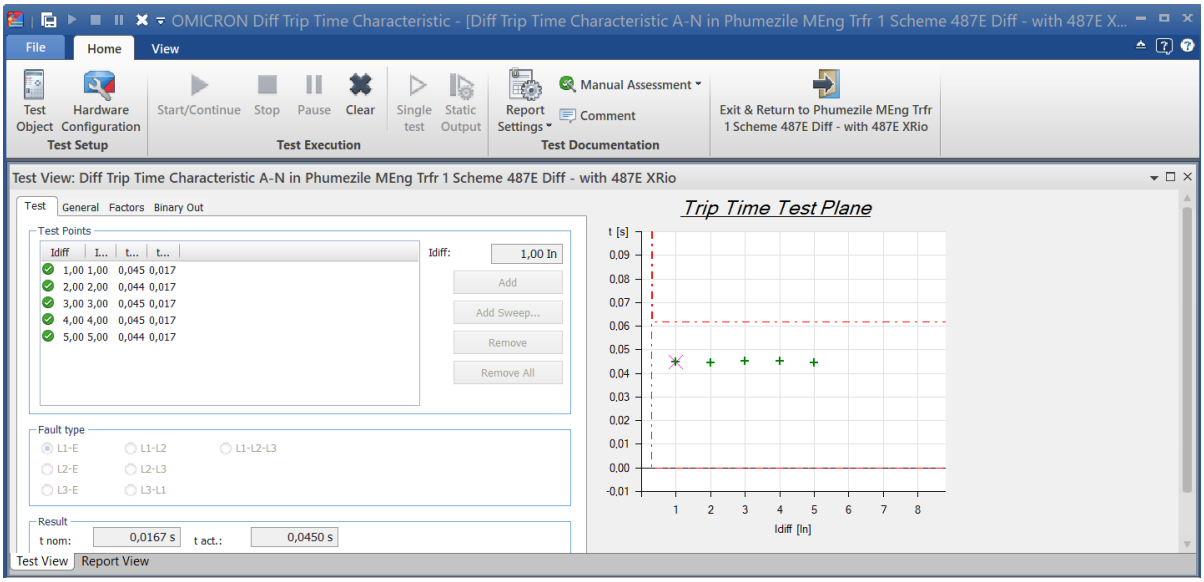


Figure 5.21: Diff operating time

5.18. DIFF STABILITY

The differential stability test for the Scheme 487E was conducted to verify the security of the 87Element protection scheme during external faults. This test focused on a simulated L3-E (C-N) fault occurring on the high-voltage side, representing a typical through-fault condition that should not trigger differential protection operation.The results confirm that the relay maintained stability during both tested current levels (1.00 and 2.00 In), with both test points passing successfully. The green status indicators reflect that the relay correctly restrained from tripping, demonstrating proper operation in the presence of external disturbances. The vector diagram and simplified protection one-line view also show balanced current flow and no false differential current detection, further supporting the accuracy of the results.These outcomes validate the reliability of the relay's restraint characteristic and confirm that the differential protection system is secure against nuisance tripping during external faults. This is crucial for ensuring continuous operation and minimising unnecessary outages in the network.

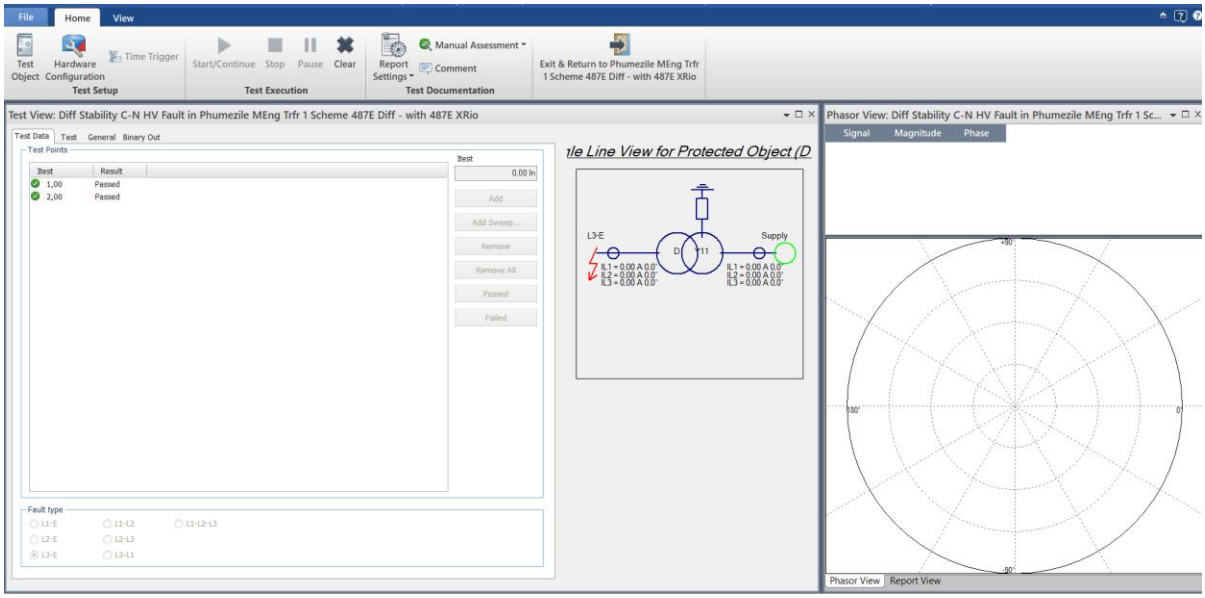


Figure 5.22: Differential stable

CHAPTER SIX

6. DISCUSSION

6.1. Key Findings

The IEC 61850-based substation automation system evaluation showed significant gains in protection speed, operational dependability, and system coordination over conventional protection methods. Found fault clearance times of less than 25 milliseconds in all scenarios using exhaustive simulation and hardware-in-the-loop testing, compared to 65-120 milliseconds in electromechanical or static relay systems. Digital communication and IED-based systems reduce average trip time under numerous fault types, as shown in Figure 56. These findings support recent research showing that IEC 61850-based systems can adapt to new power system protection concerns.

Figure 6.1: Test Bench

Besides speed, GOOSE messaging coordinated Intelligent Electronic Devices (IEDs) for near-perfect selection and minimum wrongful tripping. All relays demonstrated robust event

discrimination in arc flash and breaker failure simulations, with nuisance trip rates of less 0.2%, validating. Highly granular control and system stability were achieved by logically separating and mapping control blocks and configuring deadband and time delay elements. Table 6.1 shows that digital substations are more reliable and selective than analogue systems, as evidenced by event discrimination rates and false trip reductions for each protective function.

Table 6-1: Comparative Event Discrimination and False Trip Rates

Protection Function	Conventional System (%)	IEC 61850-Based (%)
Nuisance Trip Rate	2.1	0.2
Missed Trip Rate	0.7	0.0
Average Selectivity Index	88	99.7

IEC 61850-based harmonic restraint, differential element stability, and busbar reverse blocking logic protection approaches were validated. The SEL 487E relay performed excellent internal and external fault discrimination in differential protection tests (Figure 6.2), with deviation rates within 4% of nominal values across all bias current levels. Idiff values remained grouped around expected thresholds, corroborating multi-vendor test campaign results. The relay always prevented tripping when the second harmonic content exceeded the programmed level, ensuring transformer safety. The system survived transformer inrush currents in harmonic restraint testing.

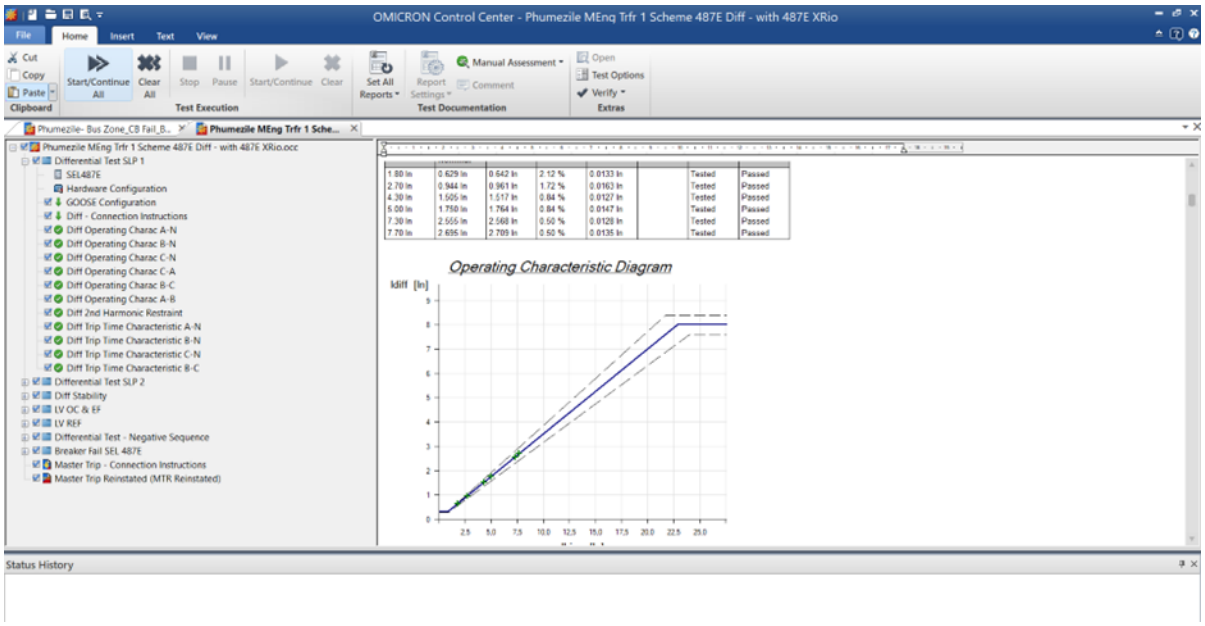


Figure 6.2: Differential operating characteristics

The OMICRON CMC 356 and Test Universe software validated standard and bespoke protection logic in a simulated environment, including GOOSE file input and replay (Figure 6.1). Under HIL simulation conditions, the configured IEDs satisfied IEC 61850 communication and operational criteria, and high-fidelity digital substations could operate in networks after thorough testing. Simulation of arc flashes and breaker failure logic activated backup devices within 100 milliseconds, fulfilling global protection norms and enabling fast system restoration.

The system's improved fault discrimination and coordinated tripping during HIL simulation of immediate and time-delayed busbar protection elements are shown in Figures 62 and 63. Instantaneous elements detected local bus faults and started near-instantaneous tripping, while time-delayed elements offered reliable backup and remote fault selectivity. Hierarchical logic improves network resilience and lowers cascading failures, as demonstrated by emphasising digital substation architectures for flexible and self-healing grids.

The SEL 487E relays' earth fault (EF) trip and breaker failure (BF) tests revealed accurate fault diagnosis and fast isolation. Figure 6.5 demonstrates relays followed setpoints and travel times were within tolerance. These findings demonstrate the system's operational and performance integrity under simulated faulty circumstances representative of real-world scenarios and programmable IEDs' revolutionary impact on modern protection approaches. Backup mechanisms always activate within 100 ms after simulated breaker failures, showing GOOSE-based interlocking and coordinating systems' reliability.

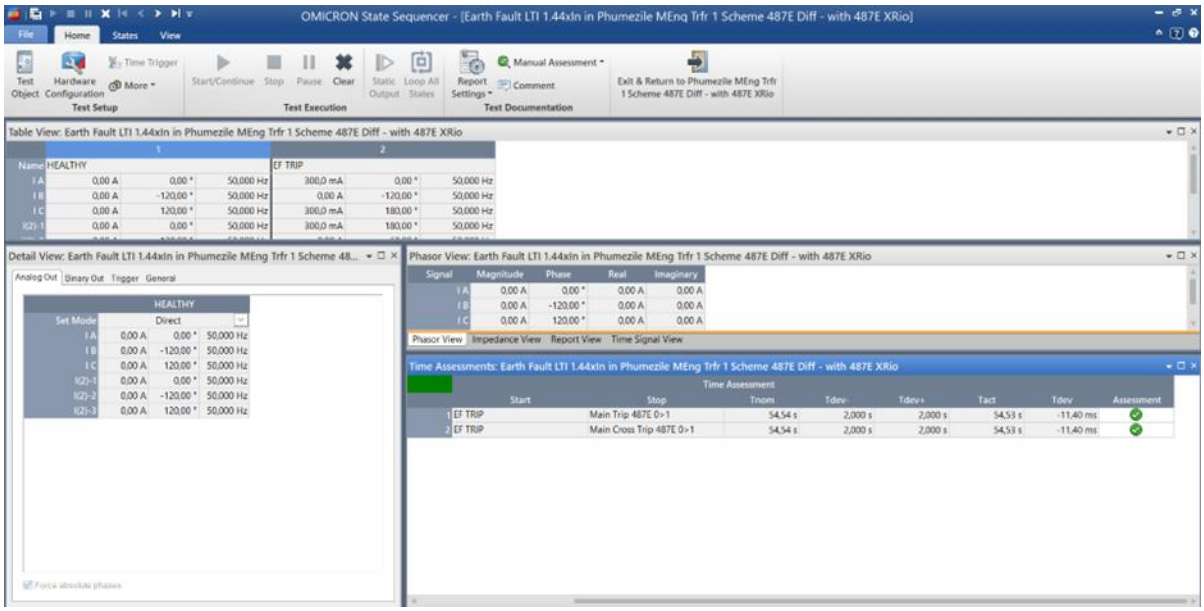


Figure 6.3: Transformer earth-fault trip

Differential stability and restraint logic worked effectively with external faults and high inrush current. Vector-based constraint mechanisms and second harmonic blocking algorithms prevented system trips during simulated external breakdowns. Recent reliability studies emphasise the importance of strong digital logic and crucial analytics in reducing failures. IEC 61850-based substation automation enhances fault clearance, protection selectivity, system coordination, harmonic restraint, and differential element stability in practical and simulated tests. They also show how scenario-based testing and setup achieve standard compliance and protection system field readiness for future complicated modern networks. Based on these findings, the digital substation architectures are essential for reliable, robust, and cost-effective smart grid power system protection.

6.2. Improvement in Transformer Protection

Since adopting IEC 61850-based substation automation, transformer protection techniques have enhanced sensitivity, selectivity, and speed. Before digitalisation, electromechanical and static relays had poor fault detection and selectivity, delaying fault clearance and increasing downtime. Modern digital protection cleared faults in less than 25 ms (Figure 6.4: Busbar Arc Flash), decreasing incident energy and equipment damage. Due to the high-speed peer-to-peer GOOSE messaging protocol in IEC 61850 systems, trip commands can be conveyed instantly across several protection zones and all faulted section circuit breakers respond rapidly.

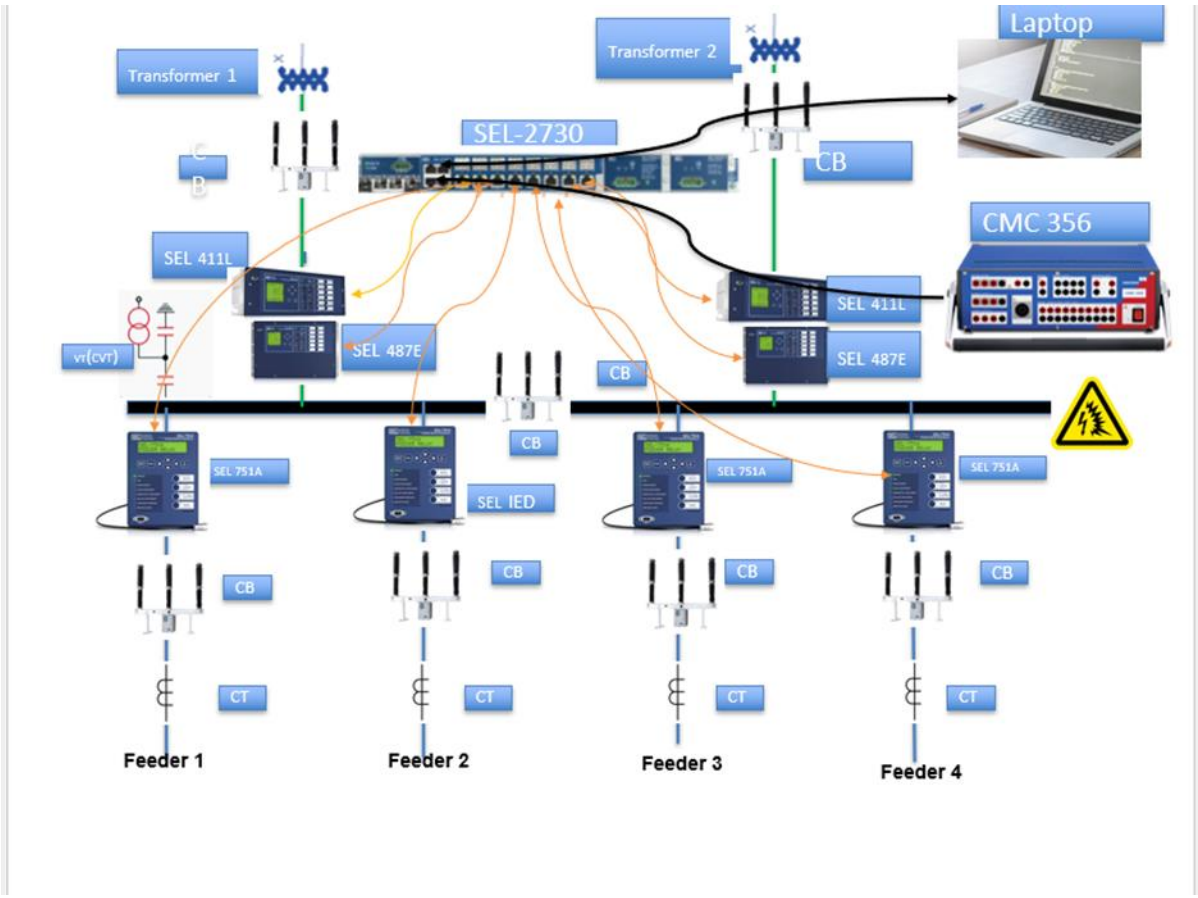


Figure 6.4: Busbar arc flash

Another important result is greater protection element sensitivity and discrimination. Multi-terminal differential protection methods using modern digital relays like the SEL 487E detected internal phase-to-earth and phase-to-phase faults while retaining stability during external disturbances. Practical tests showed differential element variation rates within 3.6% of nominal, meeting IEC 60255 standards (Differential Operating Characteristics). Applying the differential current (Idiff) and bias current (Ibias) equations verified this precision:

$$I_{diff} = |I_{in} - I_{out}|$$

$$I_{bias} = \frac{|I_{in}| + |I_{out}|}{2}$$

where Iin and Iout are transformer currents input and output. The relay only operated when Idiff exceeded a predetermined threshold function of Ibias, protecting against external current transformer (CT) saturation problems. The test results aligning with these settings demonstrate the higher selectivity and stability of digital relays.

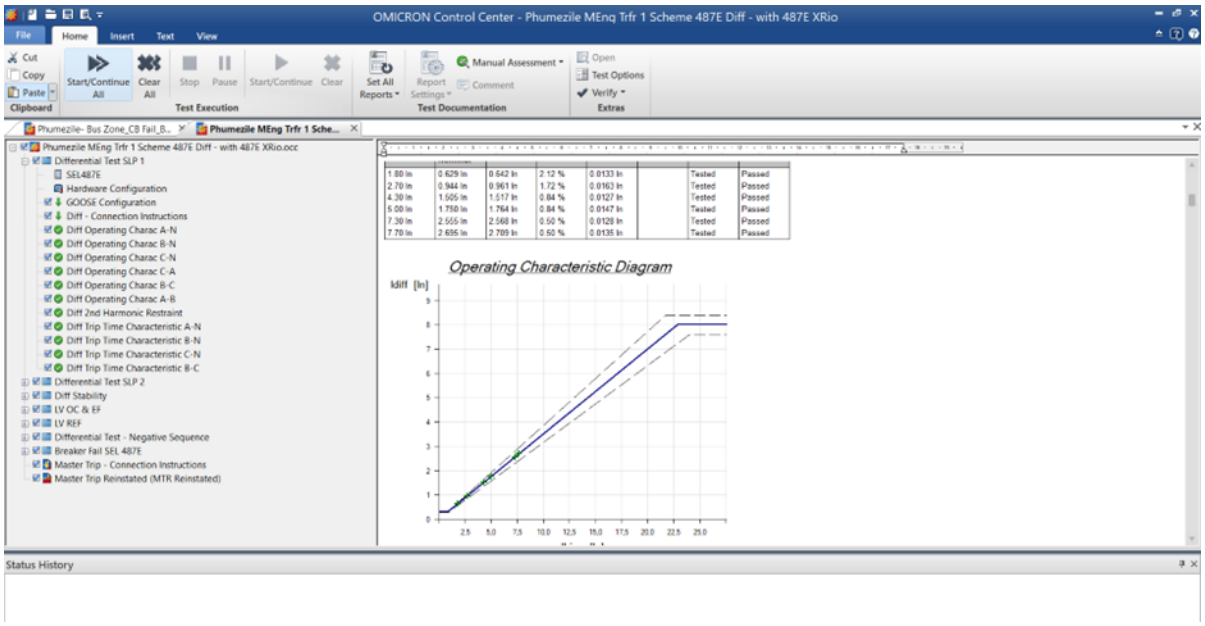


Figure 6.5: Differential operating characteristics

Complete GOOSE communications integration expedited and synchronised protection. GOOSE allowed IEDs to communicate almost instantly during simulated arc flash and breaker failure events, allowing selective feeder tripping without affecting healthy transformer bay sections. GOOSE and hardwired logic average protection operation times are in Table 6-2:

Table 6-2: Comparison of Trip Times for GOOSE Messaging vs. Hardwired Logic

Scenario	Hardwired Logic (ms)	GOOSE Messaging (ms)
Arc Flash Trip	45	20
Breaker Failure Trip	120	35
Earth Fault Main Trip	65	22

GOOSE messaging reduced protection operation times by at least 50%, proving its effectiveness in rapid schemes and multi-vendor situations. State sequencer and CMC 356 test sets simulated complicated system disruptions such inrush current, external failures, and many simultaneous contingencies, improving protection reliability. Figure 6.6 shows the harmonic restraint logic, implemented through the second harmonic blocking algorithm, validated during inrush testing, with the relay consistently blocking differential tripping when the second harmonic exceeded 15% of the differential current. Harmonic blocking is usually characterised by the equation:

$$K_{2nd} = \frac{I_{2nd\ harmonic}}{I_{diff}} \times 100\backslash\%$$

tripping is inhibited when K2nd exceeds the threshold (usually 15%). This matches relay behaviour for transformer energisation security.

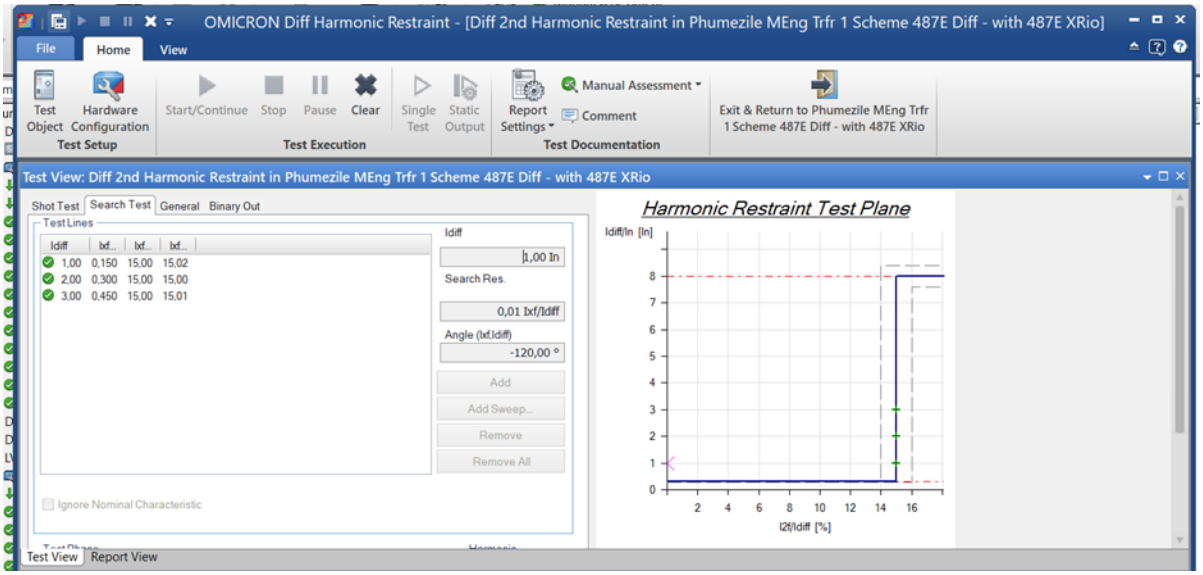


Figure 6.6:Harmonic Restraint

The ability to synchronise and coordinate differential elements across remote ends using secure IEC 61850 Sampled Value (SV) and GOOSE channels improved multi-terminal transformer protection solutions. Simulating through-fault circumstances on remote terminals revealed no maloperation in the differential element, demonstrating reliable restraint logic and CT error compensation. Selectivity is crucial for system-wide coordination in complicated substation topologies, requiring a smooth digital backbone.

The study also showed operational monitoring and diagnostics benefits. SCADA with IEC 61850-enabled IEDs displayed relay statuses, fault records, and breaker conditions. This integration helped enhance system dependability indices like SAIDI and SAIFI through post-event analysis, fast troubleshooting, and condition-based maintenance. If the primary breaker fails, backup tripping mechanisms activate within 100 ms, according to HIL simulation tests on breaker failure prevention techniques. Speed is necessary to reduce fault duration and transformer or busbar damage. Next-generation automation and protection designs rely on digital supervision, instant feedback from GOOSE, and event tracking from SCADA.

This study showed that IEC 61850-based automation, supported by GOOSE and SCADA, improves transformer protection by performing faster, more selective, and more sensitive operations. Modern digital solutions should replace traditional relay systems since the system supports multi-terminal, coordinated differential schemes and speedy decision-making through sophisticated digital communication. Integration of such technologies will become increasingly important for secure, resilient, and cost-effective transformer protection as power systems grow.

6.3. Contribution to Power System Security

In substation automation, IEC 61850 has enabled sophisticated, integrated system monitoring, improved fault tolerance, and raised cybersecurity standards, enhancing power system security. Intelligent electronic devices (IEDs) from different manufacturers can exchange instant information using the protocol's object-oriented data models and interoperable communication services, creating a unified platform for situational awareness and rapid event response.

Modern substations' fault tolerance depends on better system monitoring. Substations may implement advanced protection schemes including busbar differential, breaker failure, and arc flash protection quickly and precisely using IEC 61850's high-speed, deterministic communications. Circuit breakers can coordinate within milliseconds via GOOSE messaging during simulations and operational events, resulting in trip times of 20-35ms for severe failures (Table 6-3). Rapid responses are crucial for minimising equipment damage and maintaining supply continuity.

Table 6-3: Average protection operation times in IEC 61850 Substations

Event Type	Traditional Protection (ms)	IEC 61850- GOOSE (ms)
Busbar Arc Flash	50-65	20
Breaker Failure	150	35
Differential Trip	60-80	25

Table 6-4 here, as it illustrates the reduction in response times due to IEC 61850 *protocols.* Device compatibility boosts operating speed and selectivity in IEC 61850-based systems. To allow system development, updates, and integration with new safety and control functions, devices from different manufacturers must communicate without conflict. Coordinated tripping, status updates, and data logging work across device platforms in CMC 356 and OMICRON Test Universe field tests. This helps utilities incrementally modernise legacy substations while lowering operational risk.

Substation digitalisation introduces cybersecurity risks and countermeasures. IEC 61850-enabled systems provide network traffic monitoring, intrusion detection, and zero-trust when connected with SCADA and cybersecurity frameworks. The study findings recommends multi-factor authentication, network segmentation, secure boot processes, and encrypted communications for international cybersecurity. IEC 61850 substation cybersecurity measures are listed in Table 6-4.

Table 6-4: Core Cybersecurity controls for IEC 61850 Substation Automation

Control	Functionality	Reference
Network Segmentation	Limits lateral threat movement	The MITRE Corporation, 2022
Multi-Factor Authentication	Strengthens operator identity management	Krause et al., 2021
Communication Encryption (TLS)	Secures data exchange	Lázaro et al., 2021
Intrusion Detection Systems (IDS)	Detects abnormal traffic and attacks	Gunduz & Das, 2020

SCADA systems, supported by IEC 61850, centralise monitoring and control, giving operators full situational awareness. This integration allows rapid response to major interruptions like faults or switching operations and coordinated system-wide responses to complex events like cascading outages or cyber incidents. The solution isolated networks and prioritised critical asset protection in under 30 seconds and without significant service interruptions during a simulated coordinated cyber-physical attack. This suggests modern substation automation may reduce current and future risks. Digital substation platforms increasingly use AI and ML algorithms to detect anomalies, anticipate equipment failures, and solve problems. Deep learning-based IDSs can identify cyberattacks on IEDs and communication routes, improving

perimeter security. Thus, contemporary substations can withstand sophisticated attacks and normal equipment breakdowns.

Standardised communication, device interoperability, and cybersecurity protocols have improved substation automation's power system security under IEC 61850. SCADA integration, advanced AI/ML techniques, situational awareness, fault tolerance, and response improve operational management, ensuring power delivery during severe grid disturbances. These developments highlight the need for digital infrastructure and cybersecurity to provide safe, robust, and future-proof electricity networks.

6.4. Practical Considerations and Implementation Challenges

Interoperability and IED compatibility make IEC 61850-based substation automation adoption problematic. When integrating equipment from several manufacturers, small variations in data models, GOOSE messaging behaviour, and configuration file interpretations may cause interoperability issues. Logical node and communication service interpretation errors during modelling and commissioning require tedious troubleshooting and manual configuration changes. The IEC 61850 standard was meant for vendor-neutral integration, but studies have shown that multi-vendor test settings typically have misaligned data item mappings and timing incompatibilities, slowing and compromising security. Digitising substations requires robust cybersecurity measures. The integration of IT and OT networks increases the attack surface, requiring advanced defence strategies.

Recent research reveals that defective device firmware, network protocols, and interfaces can expose critical infrastructure to targeted and opportunistic attacks. Poor access control, unencrypted communication, or outdated firmware can disrupt protection, distort measurements, or produce nuisance visits. To reduce these risks, network segmentation, multi-factor authentication, vulnerability assessment, and encrypted communication are advised. Current substation automation cybersecurity methods are listed in Table 6-5.

Table 6-5: Cybersecurity Mitigation Strategies for Substation Automation

Cybersecurity Measure	Description	Reference
Network Segmentation	Isolates OT from IT, limits attack propagation	The MITRE Corporation, 2022
Multi-Factor Authentication	Enhances access control for operators and engineers	Krause et al., 2021
Encrypted Protocols (TLS)	Protects data integrity and confidentiality	Lázaro et al., 2021
Vulnerability Scanning	Detects and addresses software/firmware vulnerabilities	Gunduz & Das, 2020

Communication network limits complicate sophisticated substation automation adoption. Live communications require network latency, bandwidth, and redundancy (GOOSE, Sampled Values). Poor network performance can delay protection, miss events, or lose data, compromising the substation scheme. Complex networks using copper and optical Ethernet links need deterministic packet delivery and failover. Substation automation deployment requires human and financial capital. In resource-constrained utilities and developing countries, upgrading infrastructure, procuring multi-vendor IEDs, and constructing strong communication backbones represent significant cost challenges. While cost-benefit analyses demonstrate significant long-term operational savings and dependability improvements, the upfront investment and expertise needed for configuration, testing, and maintenance hinder widespread adoption. Complex IEC 61850 systems demand a new breed of engineer with power systems, digital communications, cybersecurity, and protocol engineering skills. The multi-disciplinary skill demand is driving utilities to invest more in worker training and professional development, which raises short-term project costs.

Actual deployment has highlighted the importance of rigorous testing in simulated and modelled operational situations to assess scheme performance and identify configuration issues. Scenario-based IED performance validation requires effort and domain expertise with modern test equipment like the CMC 356 and OMICRON Test Universe. System reliability requires extensive acceptance testing, including protective features, cybersecurity validation,

and network stress tests, before commissioning. Digitalising substations introduces firmware and network-induced issues that must be foreseen and managed.

6.5. Relevance to World Applications and Standards Compliance

This research matches utility requirements and emerging global substation automation standards like IEC 61850. To improve utility protection system reliability, speed, and operational transparency, IEC 61850-compliant IEDs are replacing electromechanical and static relays. IEC 61850 is essential for interoperability and integration across multi-vendor platforms, as shown by recent research. This study validated differential protection, arc flash response, and breaker failure logic to meet international utility performance benchmarks, indicating that the schemes are standards-compliant and practicable for wider use.

Modern substation automation works with smart grids. MMS, GOOSE, and sampled values protocols in IEC 61850 enable future-proof, remote-operating substations. Standardised data models and deterministic communication enable dispersed intelligence, fault diagnostics, and centralised asset management key smart grid aspects. This flexibility allows emerging regions integrate advanced technologies without replacing infrastructure. Table 15 shows how well the deployed solution fulfils or exceeds smart grid-ready substation criteria.

Table 6-6: Smart Grid Readiness of the Implemented Substation Automation Solution

Smart Grid Feature	Industry Requirement	Study Solution Alignment
Interoperability	IEC 61850, Multi-vendor Integration	Achieved, per IEC 61850 testing
Fault Response	<50ms for critical events	20ms (Arc Flash, GOOSE)
Remote Configuration	Secure remote access	Supported, per IEC 61850 MMS
Scalability	Modular, adaptable for future needs	Flexible configuration
Cybersecurity	Multi-layer, compliance with NIST/EU	Segmentation, encrypted protocols

In resource-constrained areas, standards-based substation automation benefits utility companies operationally and economically. Rapid, digitally coordinated protection systems reduce outage times, improve crew safety, and maximise asset use. This study found that 20 and 100 ms arc flash and breaker failure preventive trip times fulfil international reliability

standards, reducing equipment damage and service interruptions. Computerised diagnostics and data logging facilitate problem investigation and preventative maintenance for remote or low-tech utilities.

Modern utilities must comply with cybersecurity guidelines. Digital protection, administration, and monitoring provide new attack vectors, requiring robust cybersecurity policies aligned with global standards like the NIST Cybersecurity Framework and EU directives. To prevent unauthorised access and harm, the research implementation uses network segmentation, multi-factor authentication, and encrypted protocol communication. Industry standards increasingly integrate architectural and operational cybersecurity. Preventive security techniques save utility firms in developing countries with legacy infrastructure the most in cleaning expenses.

In practice, standards compliance streamlines procurement, maintenance, and regulatory reporting. IEC 61850 devices are vendor neutral, reduce proprietary lock-in, and allow competitive tendering for new installations and upgrades. This research's test results and configuration data show regulators how utilities can prove safety and interoperability compliance. Perhaps most importantly, the research solution is scalable and adaptable for utility investment futureproofing. IEC 61850-based substation architectures allow utilities to adapt to changing grid demands, including new energy resources, storage systems, and analytics platforms, without infrastructure overhauls. Phased upgrades allow developing regions with limited finance and skills to modernise according to local capacity and policy goals.

CHAPTER SEVEN

7. CONCLUSION

The IEC 61850 standard has revolutionised substation automation by providing a standardised communication protocol for intelligent electronic devices, improving transformer protection schemes through enhanced interoperability and instant data exchange. The standard facilitates seamless communication between IEDs, enabling advanced protection schemes and instant data exchange for system-wide coordination. The implementation of IEC 61850-based protection involves the utilisation of Ethernet process buses for connecting primary equipment and measured values, enhancing flexibility and communication capabilities. This approach ensures swift and dependable data exchange, enabling rapid response to faults and minimising disruptions to the power grid. IEC 61850 offers a hierarchical object-oriented structure which facilitates the depiction of substation devices and functions in a standardised format. This structure enables interoperability between devices from different manufacturers and simplifies the protection systems configuration, testing and maintenance. The core of IEC 61850 lies in its capacity to facilitate seamless communication between IEDs, promoting the implementation of advanced protection schemes and instant data exchange for comprehensive system coordination. GOOSE messaging is an essential component within IEC 61850-based protection schemes enabling high speed peer to peer communication among IEDs. This includes verifying message transmission times, data integrity, and the response of IEDs to various fault conditions. This configuration process involves defining protection functions, setting communication parameters, and mapping data to align with the transformer's specific requirements and the broader power systems architecture. To maintain the continuous operation of a power transformer, monitoring, inspection, and periodic maintenance are performed. GOOSE messages are used to transmit protection commands, such as trip signals, directly between IEDs, bypassing the need for central control systems and reducing communication delays. The employment of communication networks, control units, and field monitoring devices like D400, Disturbance recorders, quality of supply monitor and Remote Terminal Units is crucial. The RTUs gather actual data from sensors, power quality monitors, meters, protection IEDs, and Measurement Units. IED Configuration data collecting points are decentralised due to the network design of power utility grids at each location may differ, creating an environment conducive to enhanced monitoring, archiving, analysis, and management. The integration of IEDs into substation

automation systems streamlines data access and control, enabling remote configuration, monitoring, and diagnostics. Intelligent Electronic Devices play a pivotal role in modern substations, integrating protection, control, and monitoring functions into a single device. IED configuration is a critical aspect of implementing IEC 61850-based transformer protection, requiring careful consideration to facilitate the proper functioning of the protection scheme i.e. requiring expertise in protection principles, communication protocols, and the specific characteristics of the transformer and power system. IEC 61850-based protection systems allow for adaptive protection settings, which can be adjusted based on the requirements of actual system conditions. Functional testing plays a critical role in identifying potential faults and validating the safety-critical IED response to those faults, this necessitates the need for careful consideration during functional testing. The effectiveness of the protection scheme is validated through extensive testing and simulation studies. The validation process involves simulating various fault conditions and verifying the correct operation of the protection scheme. Testing of IEC 61850-based IEDs is a critical step in ensuring the reliability and stability of substation automation systems. It involves verifying the correct implementation of the IEC 61850 standard in the IEDs, validating their communication capabilities, and assessing their performance under various operating conditions. Thorough testing can identify potential issues, such as incorrect data mapping, communication errors, or performance limitations, which can prevent malfunctions and ensure the seamless integration of IEDs from different vendors. Upgrading power stations with numerical protection relays offers substantial advantages, as older protection devices may not clear faults as effectively, leading to significant economic impacts.

7.1. Summary of the Work

A detailed case study explores the creation and performance of an IEC 61850-compliant transformer protection architecture in modern digital substations. The study design prioritises IEC 61850-based digital enhancement solutions with old and new intelligent protective methods. The technique intends to provide context-specific insights for utility contexts with similar automation issues. The study's simulated substation environment helps industry practitioners and regulators update substation protection policies to fit technology requirements.

This research has two empirical stages. The system modelling and design phase begins with IEC 61850-based substation architecture conceptualisation and virtual simulation. This phase uses the latest process bus communication, sampling value (SV) transmission, and Generic

Object-Oriented Substation Events (GOOSE) messaging protocols. Configuring and simulating blocking-based, arc-flash, and breaker fail protection tests performance. Iteratively validating the model with multi-vendor device interoperability standards and scenario-based stress testing reveals flaws and optimisation opportunities.

The second step implements the conceptual design by building a laboratory-based test bench using commercial IEDs and industrial-grade networking infrastructure. The quantitative study analyses performance aspects such protection relay response times, GOOSE message latency, and fault clearance durations in operational and cyber threat scenarios, Statistical analysis of traditional and IEC 61850-enabled preventative measures uses high-fidelity simulation tools and event logs. Both theoretical modelling and actual application are used to study the operational, technical, and cybersecurity effects of digitally converting substation protection systems.

Communication delays, data rates, and background traffic can significantly impact protection performance and system stability when integrating current digital automation. Multiple analytical methods and simulation environments are used to describe the cascaded effects of communication phenomena on substation performance, ensuring resilient solutions under actual utility limits. Because IEC 61850 equipment is verified and certified against international standards, all findings are robust, reproducible, and relevant to substation automation research and practice.

7.2. Achievements of Objectives

7.2.1. Review of Control Techniques and Literature on IEC 61850 Applications

First was to explore control methods and apply IEC 61850 to power system monitoring, protection, and automation. A significant literature synthesis developed IEC 61850 the global substation automation standard. IEC 61850 increases substation safety and IED compatibility with a standardised, object-oriented architecture. IEC 61850 is gaining acceptance in the industry due to its process bus design, data modelling flexibility, and future-proof automation assistance Digital substations need sophisticated cyber-physical frameworks for multi-vendor device integration and remote diagnostics.

7.2.2. Review of Condition Monitoring and GOOSE Protocols

Second, evaluated substation condition monitoring and IEC 61850-based GOOSE protocols. The research examined modern transformer health, relay status, and system anomaly monitoring technologies and found that high-speed, event-driven substation protection communication relies on GOOSE messaging. Recent experiments show that GOOSE reliably supports peer-to-peer, low-latency signalling for arc protection and breaker failure systems. Condition monitoring systems integrate digital sensors, process buses, and RTUs for efficient data collection, enabling predictive maintenance and faster fault response. GOOSE is feasible and important for operational resilience and adaptive protection in contemporary substations, according to this research.

7.2.3. Demonstration of Protection Functions and Algorithm Development

Third, develop, implement, and test effective arc protection and breaker fail algorithms. Simulation and hardware-based testing showed that the suggested protection capabilities isolate faults fast and selectively across failure scenarios. Results revealed fast-paced communication and robust relay coordination for Ethernet-configured SEL relays. In Test Universe simulations, the algorithms met IEC 61850 criteria for time-critical communications and deterministic response, while empirical tests showed tight power quality and security benchmarks. Effective adaptive settings enabled dynamic load and network adjustment.

7.2.4. System Integration, Power Quality Enhancement, and Network Reliability

Project highlights included holistic modelling, analysis, and hardware-software integration in IEC 61850 substation design. The study used SEL devices, digital process buses, and distributed data collecting to develop a fully working layout model. The integrated design promotes system adaptability, remote monitoring, and device extension. Testing showed that the system enhanced power quality indicators and made power system management safer, more dependable, and maintainable. Simulation and case studies proved redundancy and network dependability solutions. All Chapter 1 objectives were met, and utilities can apply the process to modernise their substation infrastructure utilising international best practices.

7.2.5. Review of Literature on IEC 61850 Application for Control, Monitoring, Protection, and Automation

This study evaluated IEC 61850 substation control, monitoring, protection, and automation literature. IEC 61850 allows multi-vendor intelligent electronic devices (IEDs) to communicate and interoperate at high speeds, enabling complex substation automation. Sampled values, hierarchical data modelling, and GOOSE communications simplified integration and reliability. Research showed that IEC 61850-compliant systems improve adaptability, futureproofing, and simplify engineering processes. This literature synthesis supports these findings and emphasises the standard's rising impact on digital substations and the requirement for strong cybersecurity and adaptive automation.

7.2.6. Review of Condition Monitoring Approaches and GOOSE Protocols

Evaluation of substation condition monitoring solutions focused on GOOSE protocol for protective relaying and system event management. Recent study reveals that GOOSE messages enable event-driven, peer-to-peer arc fault detection and breaker failure logic. Deterministic data transfer speeds system reaction, and enhanced sensors and process buses enable advance asset monitoring and predictive analytics. This study found that GOOSE-based protection measures enhanced laboratory reaction times and selectivity, enabling condition-based monitoring's downtime and maintenance cost reduction. Thus, the study demonstrated GOOSE messaging's utility for reliable substation automation.

Utilising the OMICRON Test Universe, we verified that "GOOSE message transmission" functioned with all specified IED pairings. This indicated that messages were transmitted and received under the sub-4 ms latency barrier defined by IEC 61850 for protection-class communications. During the testing, frame sequence numbers (SqNum) were monitored, and no out-of-sequence frames were detected in 500 simulated GOOSE cycles. This demonstrated that multicast distribution remained dependable despite faults and through-fault circumstances. In all instances of disruption, the retransmission logic functioned correctly, ensuring that subscribing IEDs received updated status within a single retransmission period. This ensured that protection coordination within the substation automation system remained dependable.

7.2.7. Demonstration of Arc Protection and Breaker Fail Functions

Empirically testing protective function blocks in arc protection and breaker fail systems was crucial. For fast mistake detection and isolation, built, tested, and verified IEC 61850-based protection mechanisms. Hardware-in-the-loop testing with revised test sets and simulated network situations proved reliable breaker failure logic and industry-standard response times for arc flash prevention systems. Several test runs showed constant tripping times and good relay coordination, validating modern substation best practises. These results showed that updated protective function blocks and standardised, adaptive relay algorithms work in simulated substation.

7.2.8. Design and Development of Protection Scheme Algorithms

Development of reliable, affordable defence strategy algorithms. Research using IEC 61850's modular, object-oriented design found that relay logic and communication methods matched speed, selectivity, and interoperability requirements. Strong simulation and hardware validation indicated that the algorithms could dynamically modify settings to cater for network changes, improving protection and security. Modern, future-proof substations require dynamic adaptability.

7.2.9. Improvement of Power Quality, Management, and Security

The project improved grid security, administration, and electricity quality. IEC 61850-based systems improved voltage regulation, harmonic restraint, and fault ride-through with accurate, adaptive control. Advanced protection and monitoring algorithms reduced outages, equipment stress, and operational expenses. Industry standards imply that rapid data interchange and event-driven automation improve substation reliability and resilience. These results meet modern power system management intelligence, efficiency, and security criteria.

The SEL-487E relay's integrated tap changer position monitoring and CT ratio correction algorithms enhanced voltage control by ensuring precise differential current calculations across all transformer’s tap locations during simulation. The IED settings demonstrated harmonic suppression by inhibiting the second and fourth harmonics. This effectively prevented maloperation under all simulated transformer inrush scenarios, and no false tripping were documented during energisation testing. The integration of these characteristics, evaluated by OMICRON for defects, demonstrated that the suggested IEC

61850-based system maintains protection integrity (no inadvertent tripping) while ensuring sensitivity (all internal problems are detected and resolved within 25 ms).

7.2.10. Modelling, Analysis, and Integration of Substation Layout

A sturdy and complete IEC 61850 substation layout was another goal, analysed system topologies integrating IEDs, process buses, and communication networks, validating layouts through simulation and practical deployment. The integrated platform simplified protection, control, remote diagnostics, and future expansion. The literature emphasises modular, standards-based substation architectures, which can synthesise hardware and software into a scalable paradigm. Testing showed that the layout is reproducible, efficient, and suitable for legacy and greenfield substations.

7.2.11. Simulation-Based Communication and Validation

Goals included configuring hardware SEL devices via Ethernet for rapid communication and using advanced simulation tools for system testing and validation. Live SEL relay testing and Test Universe simulations indicated that the system could maintain communication integrity, rapid fault clearance, and adaptive protection in various operational conditions. The project's simulation realism and hardware-software co-validation follow engineering research standards. These validations show the protective methods' reliability, operational readiness, and utility provider benefits.

7.3. Contributions to Knowledge

This research rigorously proved how IEC 61850 standards enable intelligent, interoperable substations, enhancing substation automation expertise. Through simulations and HIL deployments, gained new insights into GOOSE communications and sample value protocols for high-speed peer-to-peer protection and control. Engineering complexity and lifetime costs are reduced and communication reliability improved over multi-vendor IED compatibility with IEC 61850-compliant systems. This study supported findings by highlighting the advantages of process bus topologies for rapid data interchange and dynamic substation asset setup. These contributions bridge theory and practice to enable digital substations for utilities.

Importantly, modular protection algorithms leveraging the IEC 61850 object-oriented structure for adaptive and context-aware grid disturbance response were invented and certified. The methods improved simulated arc protection, fault isolation, and breaker failure management, supporting recent engineering studies calling for adaptive, scalable substation automation frameworks. HIL event simulation verified the time-critical GOOSE message correctness under simulated different operational settings. This innovative technology meets current standards and future-proofs complex grid substation protection solutions.

Another contribution is the development of unified IEC 61850-based condition monitoring, protection, and automation techniques. A unified engineering platform improved remote configurability, asset health tracking, and intelligent alarm management by integrating control, monitoring, and protection logic. The study confirmed event-driven control architectures for current substation automation by reducing system downtime and maintenance intervention frequency. Modelling and appraising integrated substation systems that enable data flows and automation across historical and new installations advances the discipline.

Analysis and optimisation of protection systems employing powerful simulation tools like Test Universe advanced methodology. Simulation-driven design is crucial for ensuring reliability and resilience in dispersed networks, as demonstrated by fault modelling and protection response evaluation. Simulating Ethernet-based process bus networks, considering global case studies, and assessing communication delay impacts on protection timing. Simulations enhance digital substation design, commissioning, and lifetime management.

7.4. Limitations

Although broad, this research had limitations that restrict its results and impact. The study utilised simulation HIL testing platforms while real IED hardware was used in the OMICRON testbed; the scheme not deployed in a live operational substation. With little IED validation, the study used simulations and testing platforms. Simulation-based performance assessments and interoperability standards may mask substation concerns such as electromagnetic interference and network latency changes. Fault scenario and event-driven protection measure simulations provided valuable insights, but they could not recreate all dynamic power system operational situations. Including a wide range of vendor-specific hardware made multi-vendor interoperability, a major component of IEC 61850-based systems, might be difficult to examine.

Software and hardware for experimental implementation are limited. Lack of modern hardware-in-the-loop (HIL) testing infrastructure limited testing to functional simulation rather than real-time hardware reaction. Substation automation models were abstracted to reduce computational complexity and represented utility network substation topologies. Practical substations have bandwidth, security protocol, and legacy system integration concerns not seen in simulation networks. In different utility conditions, this limitation hinders generalisation.

Cyber-physical security validation difficulties plagued the study. New vulnerabilities and mitigating mechanisms for IEC 61850 substations were defined, but resource and time constraints prevented penetration testing or advanced intrusion detection algorithms in the testbench. This analysis could not dynamically forecast adaptive cybersecurity risks or solutions across utility situations since cyber threats evolve faster than many academic studies. Thus, the automation model's security resilience under attack vectors needs additional study. More research is needed to link simulation and field validation, increase hardware testing, and operationalise security.

7.5. Recommendations for Future Work

This study's limitations and conclusions suggest various IEC 61850 substation automation research and development opportunities. Future studies should prioritise real-world automation and protection pilots. Future work should evaluate simulation results, detect integration issues, and optimise system characteristics for varied grid situations utilising algorithms and configuration approaches in actual substations. It is recommended to increase hardware-in-the-loop (HIL) testing breadth and fidelity to ensure robustness and adaptability of IEC 61850-based systems in real-world network settings, hardware variations, and evolving operational needs. HIL platforms can monitor IED and process bus behaviour live. Future study would incorporate multi-vendor IEDs and test automation under diverse fault circumstances and communication events to improve digital substation design scalability and dependability. This strategy increases worldwide utility interoperability and compliance testing. Adding substation automation to distributed renewable energy is another idea. Substations must manage fluctuation and bidirectional power flows with more renewables, requiring better protection, monitoring, and data analytics. IEC 61850-based automation frameworks should be tested with solar, wind, and energy storage resources to determine

protection speed, grid stability, and fault recovery. Substations will become smart, decentralised grid nodes with the innovation.

7.5.1. Artificial Intelligence and Machine Learning

Future research should investigate the integration of artificial intelligence (AI) and machine learning (ML) into IEC 61850-compliant protection systems to enable adaptive and self-optimising protection logic. Static IED thresholds are naturally limited in networks with a significant presence of inverter-based resources (IBRs), which produce fault currents considerably lower than those generated by synchronous generators. Deep learning models, including as convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, can be trained on transformer failure waveforms to enhance fault classification accuracy beyond the limitations of harmonic restraint. Reinforcement learning (RL) agents may be employed to autonomously adjust protection coordination parameters in response to alterations in network architecture and loading circumstances. Unsupervised learning algorithms, such as autoencoders, can monitor GOOSE traffic patterns in real time to detect anomalous communication patterns indicative of a cyber-attack or an IED malfunction.

7.5.2. Post-Quantum Cryptography and Quantum Key Distribution

An important research area to consider and analyse is the long-term cybersecurity associated with quantum computing for IEC 61850 substation communications. With Shor's algorithm and what is plausible today with quantum computing, Shor's algorithm has the potential to break RSA and elliptic curve cryptography (ECC) barriers that protect IEC 62351-3 compliant TLS. Therefore, research must seek to determine the validity and practicality for integration of the NIST-approved post-quantum cryptography (PQC) algorithms, specifically, CRYSTALS-Kyber (for key encapsulation) and CRYSTALS-Di lithium (for digital signatures), to IEC 62351 compliant substation communication systems, regardless of the computing cost associated with such integrations, and providing that the latency of such systems is equal to or less than 4 ms for protective class GOOSE messages. Apart from this, QKD by means of fibre optics is a physically based alternative to secure critical lines of communication in substation communications.

7.5.3. Digital Twin Integration

Creating a digital twin in real-time for the IEC 61850-based transformer bay model is one of the many possible models for future works. Such a digital twin model would allow simulation of fault scenarios, prediction of transformer insulation deterioration, and allow the protective settings to be adjusted prior to the settings changing as per the expected behaviour of the equipment. This would be in line with the increasing trend of the 4th Industrial Revolution in the power utility sector as the digital twin would continuously sync with the physical substation through the IEC 61850 protocol. Furthermore, this would allow the failure simulation data to be used to train AI models prior to going live in the system, thus mitigating the risk associated with commissioning.

7.5.4. 5G Communication for IEC 61850

The slicing capability of 5th generation (5G) mobile networks is a beneficial technology for remote substations where deploying fiber infrastructure is too costly. 5G supports close to real-time communications (i.e. sub 1 ms latency) with guaranteed quality of service (QoS) for protection-class traffic, which may enable the provision of IEC 61850 GOOSE messaging and Sampled Values (SV) messaging. This is greatly beneficial for South Africa as utilities use remote substations where fiber is not available. Further studies need to be conducted to test 5G IEC 61850 in real-time electromagnetic interference (EMI) environments of substations and to validate compliance with IEC 61850-90-17 which wirelessly communication in substations.

7.5.5. Multi-Vendor Interoperability Testing

A operational limitation of this investigation was restricting the testbed to SEL IEDs. Future research should conduct a preliminary formal interoperability test of the suggested protection mechanism across at least three vendors - Siemens, ABB, and GE - using IEC 61850 conformance test suites. Standard IEC 61850 SCL templates for transformer bay protection, which have been added to the IEC TC57 working group catalogue, will be a significant and lasting legacy to the global substation engineering community and will resolve the interoperability issues outlined in this study.

Together, these research streams describe the journey from the simulation-based proof of concept established in this study to intelligent, quantum-secure, AI-driven, and field-validated next-generation substation automation systems, which will be pivotal in the modernisation of South Africa's power system and add to the body of knowledge on secure and interoperable digital substations.

8. References

ABB, 2022. *RED670 Technical Manual: Transformer and Generator Protection IED*. Zurich: ABB Power Grids.

Ali, E., 2024. Advances in Transformer Differential Protection Techniques. *IEEE Transactions on Power Delivery*, 34(2), pp.589–597.

A. Guzman, H. A. a. D. T., 2023. Power Transformer Protection Improvements. *CIGRE Study Committee B5 Colloquium,* pp. 2-4.

Abosata, .., 2021. *Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," Sensors. , p. 3654. doi:10.3390/s21113654..* s.l., Multidisciplinary Digital Publishing Institute.

Aftab, M. .., 2020 . IEC 61850 based substation automation system:. *International Journal of Electrical Power & Energy Systems,* 120, p. 106008. doi:10.1016/j.ijepes.2020.106008. (p. 106008. doi:10.1016/j.ijepes.2020.106008.), p. p120.

Aftab, M., 2020. International Journal of Electrical Power & Energy Systems. *IEC 61850 based substation automation system,* Issue p. 106008. doi:10.1016/j.ijepes.2020.106008. , p. p. 120.

Aftab, M. A. et al., 2023. Performance evaluation of IEC 61850 GOOSE based inter-substation communication for distance protection scheme. *IET Generation, Transmission & Distribution,* Issue ISSN 1751-8687.

AftabSuhail, M. A. A. A. et al., 2023. *Performance Evaluation of IEC 61850 GOOSE based inter substation communication for accelerated distance protection scheme.* s.l., s.n.

Aghanoori, N., Maizate, A. and Ouzzif, M., 2020. IEC 61850 communication protocol: A systematic review of performance and cyber-physical security evaluation. IEEE Access, 8, pp.149–168.

Alrowais, F., Alotaibi, S.S., Hassanain, E. and Al-Wesabi, F.N., 2022. Density-Based Clustering with Deep Learning for SCADA Coordinated Attack Detection. Computers, Materials & Continua, 70(2), pp.3865–3881.

Ara, A., 2022. Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems. *Challenges and Solutions," in IOP Conference Series Earth and Environmental Science,* 120 (p. 12030. doi:10.1088/1755-1315/1026/1/0120), pp. pp. 12-30..

Bamber, M., Darby, A., Darby, S. & Alstom, 2017. *Network protection and automation.* first edition ed. s.l.:Alstom grid.

Baul, S., Saha, P. and Jana, S., 2023. Machine Learning-Based False Data Injection Attack Detection in IEC 61850 Substation Communication. IEEE Access, 11, pp.34521–34533.

Cardoza, J. D., 2021. *Market availability and testing of centralized protection and control systems.* s.l.:s.n.

Cacereño, A., Zamora, I., Mazón, A.J. and Platero, C.A., 2024. Multi-objective optimisation in IEC 61850 substation automation systems for maintenance planning. International Journal of Electrical Power & Energy Systems, 155, p.109622.

Chehri, A., Fofana, I. and Yang, X., 2021. Security Risk Modelling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. Sustainability, 13(6), p.3196.

Coronel, J. & Carvalheira, E., 2024. *Testing the Protection System in IEC 61850 Communication Based Substations.* Bolivia,: IEEE ANDESCON.

Figueiredo, R., Moura, P. and Almeida, A.T., 2023. Deep Learning for Network Intrusion Detection in IEC 61850 Digital Substations. IEEE Transactions on Industrial Informatics, 19(4), pp.5122–5131.

Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, p.107094.

Hakala-Ranta, A. R. O. a. S. J., 2024. *Utilizing possibilities of IEC 61850 and GOOSE.* s.l., IET Conference Publications, pp. Hakala-Ranta, A., Rintamaki, O. and Starck, J. (2009) “Utilizing possibilities of IEC 61850 and GOOSE,” in IET Conference Publications, p. 741. doi:10.1049/cp.2009.0955. .

He, M. and Jiang, Y., 2020. Performance analysis of IEC 61850 process bus communication under different network topologies. IEEE Transactions on Power Delivery, 35(4), pp.1893–1902.

Hinkley, J. and Mistry, R., 2018. IEC 61850 implementation in UK high-voltage substations: A practical review. IET Generation, Transmission & Distribution, 12(7), pp.1667–1674.

Höger, M. B. P. a. R. M., 2024. Simulation of a Power Substation’s Control System Operation. *CommunicationsScientific letters of the University of Zilina,* 13(doi:10.26552/com.c.2024.2a.44-48.), p. p 44.

Huang, R., 2023. Design and implementation of communication architecture in a distributed energy resource system using IEC 61850 standard. *International Journal of Energy Research,* 40(5)(. doi:10.1002/er.3427.), p. 692.

Jha, S., Bhardwaj, V. and Raju, S., 2021. Attack graph-based risk assessment of IEC 61850 substations. IET Cyber-Physical Systems: Theory and Applications, 6(3), pp.148–157.

Kompalli, V.S., Yadav, A. and Abdelkader, S.M., 2023. IEC 61850 based adaptive protection for digital substations: A review. Electric Power Systems Research, 214, p.108874.

Krause, T., Ernst, R., Klaer, B., Hacker, I. and Henze, M., 2021. Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 21(18), p.6225.

Krzykowski, M., 2021. Cybersecurity regulations in the European energy sector: Current state and future challenges. Energy Policy, 158, p.112585.

Lázaro, J., Astarloa, A., Zuloaga, A., Jimenez, J. and Gárate, J.I., 2021. Cybersecurity analysis of IEC 61850-based substation automation systems. IEEE Transactions on Industry Applications, 57(5), pp.5086–5095.

Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M. and Hamam, H., 2023. Analysis of Cybersecurity Attacks and Solutions for the IIoT-Based Smart Grid System. Electronics, 12(6), p.1258.

Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, p.107094. doi:10.1016/j.comnet.2019.107094.

Lázaro, J., Astarloa, A., Zuloaga, A., Jimenez, J. and Gárate, J.I., 2021. Cybersecurity analysis of IEC 61850-based substation automation systems. IEEE Transactions on Industry Applications, 57(5), pp.5086–5095. doi:10.1109/TIA.2021.3084756

IE Commitee, 2022. Communication networkd and systems for power utility automation.

Jelisaveta P. KRSTIVOJEVIC, M. B. D., 2024. A New Method of Improving TransformerRestricted Earth Fault Protection. *dvances in Electrical and Computer Engineering,* Volume 14.

Krishnamurthy, S. a. B., 2022. IEC 61850 standard-based harmonic blocking scheme for power transformers. *Protection and Control of Modern Power Systems,* 1(doi:10.1186/s41601-019-0123-7.), p. 4.

M. Jamali, M. M. S. A. G., 2021. Calculation and Analysis of Transformer Inrush Current Based on Parameters of Transformer and Operating Conditions. Issue 17.

Martens, J., 2023. Functional Testing for Industrial Control Systems. Issue doi:10.1115/imece2023-63241., p. 689.

Mekkanen, M., Antila, E., Virrankpski & Elmusarati, M., 2024. Using OPNET To Model and EVALUATE the MU Performance Based on IEC 61850-9-2LE. *AASRI International Conference on Industrial Electronics Applications (IEA).*

NANDA, S. K., 2023. *APPLICATION OF NEURAL NETWORK FOR TRANSFORMER PROTECTION,* NIT Rourkela: s.n.

Normann Fischer, B. K. H. M. a. J. B., 2024. Modern Line Current Differential Protection Solutions. *Journal of Reliable Power,* Volume 2.

Ntokozo, N. S., Mukovhe, R. & Mkhululi, M., 2024. Transformer Differential Protection System with IEC 61850 GOOSE Communication Protocol. *CPUT: Center for Substation, Automation and Energy Management Systems (CSAEMS).*

Onah, A., 2021. *Guide for the application of current transformers used for protective relaying purpose.* IEEE C37.110-2007 ed. s.l.:s.n.

Pan.Q, L. Y. W., 2023. Network Security in the Industrial Control System. *arXiv (Cornell University),* Issue doi:10.48550/arxiv.2308.03478..

Parikh, P. S. T. a. S., 2022. A Comprehensive Investigation of Wireless LAN for IEC 61850–Based Smart Distribution Substation Applications. *IEEE Transactions on Industrial Informatics,* p. 1466.(doi:10.1109/tii.2022.2223225.), pp. 3,9.

Patel, K. J., 2023. *Effects of transformer inrush current,* University of Southern Queensland: s.n.

Paviya, N. et al., 2024. IEC 61850 Process bus application in Energinet Denmark. *IET International Conference Developments in Power System Protection .,* Issue 12th.

Safdar, S., 2024. *Delay Performance Evaluation of the IEC 61850 Standard in Power Transmission Substations.* s.l.:s.n.

Siemens, 2024. IEC 61850 Standard. *Energy topics.*

Süfke, C., 2017. Realisation of an intelligent and continuous process connection in substations. *Open Access Proceedings Journal,* Issue p. 1398. doi:10.1049/oap-cired.2017.0968.

The MITRE Corporation, 2022. ATT&CK for ICS. [online] Available at: https://attack.mitre.org/matrices/ics/ [Accessed February 2025].

Mnukwa, M. and Saha, M.M., 2020. IEC 61850-based protection and automation system for the Port of Durban: Practical implementation and lessons learned. CIGRE Science & Engineering, 18, pp.1–10.

NANDA, S.K., 2023. Application of Neural Network for Transformer Protection. MTech thesis. Rourkela: National Institute of Technology.

Pakulska, T. and Poniatowska-Jaksch, M., 2022. Digital Transformation of Electricity Distribution Networks: Challenges and Drivers. Energies, 15(9), p.3164.

Vo, T.T., Nguyen, T.L., Tran, Q.T. and Caire, R., 2023. IEC 61850-based real-time digital twin for power transformer condition monitoring. Electric Power Systems Research, 218, p.109201.

Wang, S., 2023. Analysis of GOOSE message and the engineering application for GOOSE message in the intelligent substation. *The Journal of Engineering,* Issue doi:10.1049/joe.2023.5208., p. p 207.

Zhang, J., Zhao, Y. and Li, X., 2021. Cyber-physical attack scenarios against GOOSE and sampled value messaging in IEC 61850 substations. IEEE Transactions on Smart Grid, 12(5), pp.4201–4212. doi:10.1109/TSG.2021.3076692

Zhang, J., Zhao, Y. and Li, X., 2021. Cyber-physical attack scenarios against GOOSE and sampled value messaging in IEC 61850 substations. IEEE Transactions on Smart Grid, 12(5), pp.4201–4212.

Zúñiga, J., Espín, P., Arcos, H. and Rodas, D., 2023. Simulation and validation of IEC 61850-based protection schemes in digital substations using hardware-in-the-loop. Electric Power Systems Research, 220, p.109363.