UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE TELECOMUNICAÇÕES

MATHEUS FELIPE AYELLO LEITE

A New Proposal for Line Differential Protection Schemes using Sampled Values to Enhance Protection Performance

NITERÓI

2023

UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE TELECOMUNICAÇÕES

MATHEUS FELIPE AYELLO LEITE

A New Proposal for Line Differential Protection Schemes using Sampled Values to Enhance Protection Performance

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Mestre em Engenharia Elétrica e de Telecomunicações. Área de concentração: Sistemas de Energia Elétrica.

Orientadora:
YONA LOPES

NITERÓI

2023

Ficha catalográfica elaborada pelo Sistema de Bibliotecas da UFF - SDC/UFF
com os dados fornecidos pelo(a) autor(a)

S586t Silva Junior, José Lins da
Título do Trabalho: subtítulo do trabalho / José Lins da Silva Junior; Orientador Sobrenome, orientador; Coorientador Sobrenome, co-orientador. Niterói, 2017.
120 f.

Monografia (Especialização em Engenharia de Produção)-Universidade Federal Fluminense, Laboratório de Tecnologia, Gestão de Negócios e Meio Ambiente, Niterói, 2017.

1. Primeiro assunto. 2. Produção intelectual. I. Título II. Sobrenome,Orientador, orientador. III. Sobrenome, Coorientador, co-orientador. IV. Universidade Federal Fluminense. Laboratório de Tecnologia, Gestão de Negócios e Meio Ambiente.

CDD -

Matheus Felipe Ayello Leite

A New Proposal for Line Differential Protection Schemes using Sample Values to Enhance Protection Performance

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Mestre em Engenharia Elétrica e de Telecomunicações. Área de concentração: Sistemas de Energia Elétrica.

Aprovada em 5 de abril de 2023.

BANCA EXAMINADORA

Prof$^{\underline{a}}$. Yona Lopes, D.Sc. – Orientadora, UFF

Prof$^{\underline{a}}$. Natalia Castro Fernandes, D.Sc. – UFF

Prof$^{\underline{a}}$. Maria Cristina Dias Tavares, D.Sc. – UNICAMP

Niterói
2023

À familia

Agradecimentos

Agradeço profundamente a minha família pelo apoio incondicional, a meu pai Amauri, minha mãe Alaíde, minhas irmãs Ana Clara e Maria Beatriz e aos meus irmãos Pedro Henrique e João Gabriel. Também aos meus sobrinhos Antônia e Gabriel que conseguem trazer alegria ao meu dia todas as vezes que converso com eles.

A minha querida orientadora Yona Lopes pelo carinho, cuidado e exemplo de profissionalismo. A todos a equipe e companheiros de faculdade que fizeram parte dessa minha jornada de mestrado. A nossa querida Universidade Federal Fluminense.

Aos meus grandes amigos que fazem todo esse esforço valer a pena com os momentos que construímos em nossas reuniões.

Por fim, um obrigado a todos que, embora não estejam citados aqui, me incentivaram, contribuindo de forma direta ou indireta, para o desenvolvimento deste trabalho.

Resumo

A proteção diferencial de linha apresenta grande seletividade para isolar equipamentos em condições de falta. No entanto, o uso dessa técnica tem sido limitada por fatores como o comprimento da linha de transmissão, atrasos na rede de comunicação, o uso de protocolos proprietários e vulnerabilidades relacionadas a falhas na rede de comunicação. Em relação ao comprimento da linha, algumas técnicas apresentam limitações para linhas com comprimento inferior a 120 km e são restritas a fabricantes específicos por serem proprietárias. A técnica de ondas viajantes, as tradicionais fasoriais e as soluções de envio de dados digitalizados proprietárias de fabricantes são exemplos de soluções para o esquema. As técnicas proprietárias geralmente são dependentes da rede de comunicação para sincronização mútua através da rotação do fasor, fazendo com que qualquer atraso na rede gere imprecisão e prejudique o desempenho da proteção. Com a crescente digitalização dos sistemas elétricos, as subestações digitais têm sido adotadas, possibilitando a criação de soluções mais robustas para as redes de comunicação. A norma IEC 61850 é o pilar que fundamenta e viabiliza a implantação de subestações digitais, as quais têm se mostrado uma boa opção para a melhoria da confiabilidade e eficiência do sistema elétrico. Isso ocorre pois novas soluções podem ser exploradas para o aumento do desempenho de esquemas de proteção. Contudo, com a chegada da norma IEC 61850 e a utilização de transformadores de instrumentação não convencionais torna-se necessário conduzir estudos direcionados também à avaliação da rede de comunicação nestas novas propostas, uma vez que esta rede é responsável pelo envio dos valores amostrados de tensão e corrente dentro e entre as subestações. As soluções adotadas para as subestações digitais passam a estar intrinsecamente ligadas às redes de comunicação, o que demanda estudos mais efetivos sobre o impacto da comunicação no desempenho das soluções de proteção. Nesse sentido, é proposto um novo esquema para proteção diferencial de linhas de transmissão, utilizando mensagens SV em conformidade com a norma IEC 61850. Essa nova abordagem permite a redução de custos e da complexidade do sistema, além de aumentar a robustez da rede de comunicação. Isso é possível graças à possibilidade de utilização de equipamentos de diferentes fornecedores e a resiliência proporcionada pelo uso de caminhos redundantes na comunicação e ao método utilizado para cálculo análogo ao da proteção diferencial que não é dependente do conhecimento do atraso na rede de comunicação para rotação do fasor. Além disso, foi realizado um estudo de viabilidade para proteção diferencial em duas linhas de transmissão de 500 kV do sistema interligado brasileiro por meio do software Aspen Oneliner. Nesse estudo de viabilidade foram realizados quatro faltas de alta impedância em diferentes posições em ambas as linhas, vale ressaltar que esse tipo de falta é desafiador para esquemas de proteção diferencial de linhas. A proposta foi avaliada e testada em laboratório, onde a solução foi simulada em dois relés de proteção da SEL modelo 421-7 com envio e recebimento de mensagens SV, uma mala de testes Omicron CMC 356, um dispositivo distribuidor de sinais de sincronismo SEL-2488, uma antena GPS SEL-9524, switches para a devida formação dos barramentos de comunicação e hardwares para emulação do comprimento do canal de comunicação da linha de transmissão, injeção de tráfego concorrente e geração de perda de pacotes. Os resultados mostraram a viabilidade de implementação da função de proteção diferencial nas duas linhas de transmissão estudadas. Para os testes, foi utilizado um esquema de proteção similar à proteção diferencial de linha a ser implementada nos IEDs, onde utilizou-se uma função de sobrecorrente com um arranjo de barramento em disjuntor e meio. Os testes de rede indicam a viablidade do esquema para linhas de até 300 km de extensão, além disso o esquema manteve-se atuante para uma taxa de perda de pacotes até 50% e uma injeção de tráfego concorrente até 200 Mbps. Outras avaliações especificamente de redes foram avaliados como o efeito do tráfego concorrente na latência e na perda de pacotes. Os resultados são promissores e indicam a viabilidade da proposta.

Palavras-chave: IEC 61850, Linhas de Transmissão, Sampled Values, Proteção Diferencial de Linha.

Abstract

Line differential protection features great selectivity to isolate equipment under fault conditions. However, this technique has been limited by factors such as transmission line length, communication network delay, use of proprietary protocols, or vulnerability to network failures. Regarding the line length, some techniques have limitations for lines less than 120 km long and are restricted to specific manufacturers because they are proprietary. The traveling waves technique, the traditional phasor-based ones, and the proprietary digital solutions from manufacturers are examples of solutions that use the communication network. Proprietary methods usually depend on the communication network to synchronize through the phasor rotation, causing any delay in the network to generate inaccuracy and impair protection performance. With the growing digitization of electrical systems, digital substations have been adopted, enabling more robust solutions for communication networks. The IEC 61850 standard is the pillar that supports and enables the implementation of digital substations, which have proven to be a good option for improving the reliability and efficiency of the electrical system. This occurs because new solutions can be explored to increase the performance of protection schemes. However, with the arrival of the IEC 61850 standard and the use of non-conventional instrumentation transformers, it becomes necessary to con duct studies also aimed at evaluating the communication network in these new proposals since this network is responsible for sending the sampled voltage values and current within and between substations. The solutions adopted for digital substations are now intrinsically linked to communication networks, which demands more effective studies on the impact of communication on the performance of protection solutions. In this sense, a new scheme for differential protection in transmission lines is proposed, using SV messages by the IEC 61850 Standard. This new approach allows the reduction of costs and system complexity, in addition to increasing the network robustness of communication. This is possible thanks to the possibility of using equipment from different suppliers, the resilience provided by the use of redundant communication paths, and the method used to calculate that is similar to differential protection and that is not dependent on knowing the delay in the communication network for phasor rotation. In addition, a feasibility study was carried out for differential protection in two 500 kV transmission lines of the Brazilian interconnected system using the Aspen Oneliner software. In this feasibility study, four high-impedance shorts were performed in different positions on both lines. It is worth noting that this type of short circuit is challenging for line differential protection schemes. The proposal was evaluated and tested in the laboratory, where the solution was simulated in two SEL model 421-7 protection relays with sending and receiving SV messages, an Omicron CMC 356 test case, a signal distributor device of SEL-2488 synchronism, an SEL-9524/GPS antenna, switches for proper formation of communication buses, and hardware for emulating the length of the transmission line communication channel, concurrent traffic injection, and generation of loss of packages. The results showed the feasibility of implementing the differential protection function in the two studied transmission lines. For the tests, a protection scheme similar to the line differential protection to be implemented in the

IEDs was used, where an overcurrent function was used with a breaker and a half busbar arrangement. Network tests indicate the scheme's viability for lines of up to 300 km in length. The scheme remained active for a packet loss rate of up to 50% and a concurrent traffic injection of up to 200 Mbps. Other network-specific evaluations have looked at the effect of concurrent traffic on latency and packet loss. The results are promising and indicate the viability of the proposal.

Keywords: IEC 61850, Transmission lines, Sampled Values, Line differential protection.

List of Figures

List of Tables

List of Abbreviations and Acronyms

ASDU	Application Specific Data Unit	23
CTR	Current Transformer Ratio	10
CT	Current Transformer	viii
GNSS	Global Navigation Satellite System	4
GOOSE	Generic Object Oriented Substation Event	23
GPS	Global Positioning System	35
HMI	Human Machine Interface	22
HVDC	High Voltage Direct Current	36
IEC	International Electrotechnical Commission	2
IED	Intelligent Electronic Device	2
IEEE	Institute of Electrical and Electronic Engineers	25
IFG	Inter Frame Gap	66
ISO	International Organization for Standardization	19
LAN	Local Area Network	31
MMS	Manufacturing Message Specification	22
MU	Merging Unit	2
NCIT	Non-conventional Instrument Transformer	2
NTP	Network Time Protocol	26
PDV	Packet Delay Variation	32
PSN	Packet Switching Network	31
PTP	Precision Time Protocol	4
PT	Potential Transformer	23
RTDS	Real Time Digital Simulator	35
SCADA	Supervisory Control and Data Acquisition	22

SCN	Substation Communication Network	40
SCSM	Specific Communication Service Mapping	19
SV	Sampled Values	2
TDM	Time Division Multiplexing	31
UDP	User Datagram Protocol	29
VLAN	Virtual Local Area Network	69
WAN	Wide Area Network	4

Contents

Chapter 1

Introduction

Due to the constant expansion of electrical systems, system stability requirements become increasingly demanding. Faster and highly selective protection schemes are paramount in this scenario. According to Liu et al, differential protection is superior from the stability, speed, and selectivity point of view compared to overcurrent, distance, and directional comparison schemes [11]. Thus, it is widely used to protect power transformers, generators, substation busbars, and transmission lines. Although all the aforementioned advantages, differential protection presents some drawbacks. First, the available protection schemes are implemented through proprietary protocols, which may increase the costs and creates incompatibility issues among different vendors as detailed in Ayello and Lopes [12]. Furthermore, traditional differential protection techniques depend on the rotation of phasors from the other line terminal to be processed with the local phasor value. This rotation, however, depend on prior knowledge of the communication time, disregards communication delays, which impact the performance of the protection scheme and lead to a length limitation for short transmission lines (up to 120 km) as stated in Ziegler [13]. Alongside, traditional CTs carries the risk of saturation. This occurs because the CTs are based on electromagnetic principles, in which a magnetic flow through the CT magnetic core transmits the line current information on the primary coil to the secondary coil. That magnetic core has a limitation of the magnetic force that flows through him. Hargrave et al explains that when that threshold is reached, the current value measured on the secondary side is no longer reliable since it is no longer directly associated with the primary value, which can lead to unwanted protection actuation or to the protection relay not detecting the fault [3].

The more devices are attached to the secondary coil of the CT, the bigger the load is, the load is directly related to the CT saturation limits, and therefore, it is no desired to have many devices attached to a single CT. The use of Merging Unit (MU) allows reducing this risk since it represents a single load to the CT, and every other device will receive the current information through the digitalized Sampled Values (SV) messages. It is worth mentioning that, according to Hargrave et al, the Non-conventional Instrument Transformer (NCIT) is based on light deviation principles and, therefore, does not have the risk of saturation [3].

The power systems environment is composed of many devices, such as power transformers, instrument transformers, control, and switching. Among the primary devices present in automation environments are the protection relays, which are responsible for protecting the system against disturbances, ensuring the system's integrity and safeness of human life. With the digitalization of protection relays and the advent of International Electrotechnical Commission (IEC) 61850 standard, these relays are now named Intelligent Electronic Device (IED) due to integrating other functionalities such as control and supervision, which are now included in the equipment.

Interoperability between equipment developed by different vendors or even between the same vendor allows a more innovative and competitive scenario in power systems. Initially, there was no such a feature because all equipment that uses digital information has communication protocols and they were proprietary developed by each vendor to their own devices. As Sharma and Rudolph states, this situation makes electrical systems, especially substations, dependent on the vendor that originally supplied the equipment [14]. In this sense, the international standard IEC 61850 was developed to standardize the information models to be implemented in digital devices and requirements to be achieved by the power systems applications.

1.1 Motivation

Ensuring the electrical supply is a critical role of power systems. The world energy demand grows each year, and maintaining the safety of power systems equipment through a reliable protection scheme is mandatory. A failure in the protection actuation can be very costly, and the faster the fault clearance, the better for equipment and human safety.

Transmission lines can have hundreds of kilometers of extension and are regularly subjected to short circuits. The are several protection functions, and a protection engineer will use a combination of them to offer a better solution for protecting the transmission lines. A differential protection scheme is considered to have better selectivity and fault clearance performance in comparison with other functions. Thus, expanding its use in power systems applications results in a more reliable energy supply.

Another motivator is the study comprising the IEC 61850 standard. The SV protocol, standardized by IEC 61850, enables the digitalization of analog voltage and current values obtained in the field, allowing for more selective and faster differential protection functions. Increasing the use of this technique in transmission lines can significantly enhance the reliability of power systems.

The use of the IEC 61850 standard also brings operational benefits, such as reducing the risk of CT saturation, lowering costs for copper cables, and increasing the redundancy of protection schemes through the network's topology. These advantages are not achievable when using proprietary protocols from different vendors. Furthermore, the existing traditional analog differential protection schemes were restricted to smaller transmission lines (up to 120 km) and relied on dedicated communication channels between line ends, limiting the use of excess bandwidth for other services [13].

Solutions that contribute to the far-reaching implications for the power industry, contributing to improved efficiency, reliability, and cost-effectiveness are highly motivating.

1.2 General goals

This work aims to expand the use of line differential protection scheme through the use of IEC 61850 standard to allow open and more flexible solutions for substations communications and also promote the expansion of the IEC 61850 standard on power systems applications. To achieve these goals, we propose a new line differential protection scheme based on the SV protocol. We present the scheme's architecture describing each feature in detail, also highlighting the advantages. Using the SV protocol allows interoperability between different vendors.

1.3 Specific goals

Considering using SV in line differential protection, this work aims to:

- Allow the use of optic CTs for line differential protection and eliminate the risk of CT saturation;
- Allow interoperability with different vendors in 87L schemes;

- Provide commercial use for the exceeded bandwidth on Wide Area Network (WAN) in 87L schemes;
- The reliability increase of the transmission of sampled current values through the network topology;
- Exclude dependence on time synchronization by the communication network.

1.4 Proposal and Main contributions

To address the limitations mentioned of the current differential protection scheme and to align with the ongoing trend towards the digitalization of power systems, which brings about the benefits afforded by the IEC 61850 Standard, we present a novel approach using the SV protocol established by the standard IEC 61850. Our proposal is based on an open and standardized communication protocol available on most of IED vendors. Also, in our proposal, we solve the impact caused by communication network delay on synchronizing the phasors of the proprietary protocols by using message timestamps and the Precision Time Protocol (PTP) for synchronizing the devices. The main economic advantage of the IEC 61850 standard is the reduction of costs with copper cables, mainly responsible for sending analog signals, and with the implementation time. Alongside, with MUs being the only load at the CT, the risk of saturation is reduced since the information can be sent to any device through the communication network without adding extra load at the CT.

Also, we evaluate the impact of the communications network over the proposed protection scheme under communication network stress conditions. Evaluating the impact of communication network issues on the protection performance is crucial in assessing the feasibility of the proposed scheme, also we can evaluate how much concurrent traffic can flow alongside the SV messages without compromising the scheme. It is assembled a testbed with one SV publisher SEL IED, one SV subscriber SEL IED, an Omicron CMC 356 device, a Global Navigation Satellite System (GNSS) antenna, a PTP distribution device, a hardware for analysis and network stress, and an HP 1820 gigabit switch. We carried out four simulation scenarios: a standard case without any stress condition; an SV transmission delay increase with NETEM software to simulate the line length through hardware; an increase in background traffic with the injection of packets in the network through the Pypacker library; and a package loss scenario with the software NETEM to concludes the network simulations. The automatization of the process allowed the performance of several simulations. There was a total of forty-nine cases, and each of them was tested in 30 rounds. We also evaluated the performance of the SV message delays at the same network stress scenarios in the SEL 421 SV subscriber through an automated method with 1000 times repetitions. This automatization allows to obtain the average results with a 95% confidence interval. The results indicate possible thresholds for the three assessed network conditions that can further help engineers to plan their communication network.

Therefore, the main contributions are summarized as follows:

- A new methodology for line differential protection using the IEC 61850 SV protocol;
- Demonstration of the benefits of using the IEC 61850 standard, including improved operational efficiency, reduced risk of CT saturation, and increased reliability through redundancy in the network topology. Also, we demonstrate the benefits of having a non-dedicated communication network for performing line differential protection;
- Improvement by bringing interoperability between different vendors in line differential protection schemes;
- Reduction of costs associated with copper cables and equipment maintenance through increased reliability and efficiency of the digital protection scheme;
- The impact of communication network stress scenarios on line differential protection schemes;
- A solid theoretical foundation in line differential protection schemes and its comparison with other common line protection functions.

1.5 Work structure

The rest of the work is structured in five chapters, with Chapter 2 establishing the theoretical foundation for adequately comprehending the work by presenting the line differential protection scheme and the ways of performing it (percentage differential protection, alpha plane R-X diagram, and charge comparison relays), introducing challenging scenarios for applying line differential protection schemes and presenting the line differential protection logical node. Discusses high impedance faults and CT operational principles with an explanation of why it saturates. It also shows all the main features of the IEC 61850 Standard, including the data structure, the division into sections, and the protocols. Also, we explained the PTP with many details, comparing it with the other available protocols, his profile options, and variations. We also explained how the internal time synchronization among differential protection schemes works. Finally, the chapter concludes by presenting the network evaluation metrics that will be used in the network case study: delay; bandwidth; throughput; and packet loss.

Chapter 3 discusses the related work in the literature where as Chapter 4 details our new proposal by presenting our main motivations towards its conception, the proposal architecture with all features discussed in detail, its main advantages, an example of its functioning, and a comparison whit other available methods.

Chapter 5 presents the evaluation of the new proposal. A percentage line differential case study is carried out by simulation of four high impedance (fault resistance of 120 Ω) short circuits throughout two 500 kV transmission lines. Also, a network performance test is done by assembling a testbed with an SEL-421 SV publisher, an SEL-421 SV subscriber, an Omicron CMC 356 device for relay testing, a GNSS antenna SEL-9524, an SEL-2488 time synchronization device, and two hardware that generates the desired network stress scenarios through the software NETEM and Pypacker.

Finally, Chapter 6 concludes the work by summarizing the results, the proposal's main characteristics and enhancement, and also presents the future works.

1.6 Publications

Throughout the master's degree course, the following publications were submitted and accepted:

- AYELLO, MATHEUS; Lopes, Yona. Interoperability based on IEC 61850 standard: Systematic literature review, certification method proposal, and case study. ELECTRIC POWER SYSTEMS RESEARCH. , v.220, p.109355 - , 2023;

- AYELLO, MATHEUS; LOPES, Y.; Cruz, Arthur Augusto Pereira; LOPES, T. T. E. PROTEÇÃO DIFERENCIAL DE LINHAS BASEADA EM SAMPLED VALUES: AVALIAÇÃO DA VIABILIDADE DE IMPLEMENTAÇÃO E IMPACTOS CAUSADOS PELO COMPORTAMENTO DA REDE DE COMUNICAÇÃO, XXVI SNPTEE, 2022.

- AYELLO, MATHEUS; Azevedo, Amanda Ferreira; Azevedo, João Henrique Paulino; Filho, João Teles de Pontes; Gonçalves, Felipe da Silva Fernandes. Análise da Operação Frente à Inserção de Usinas Eólicas e Usinas Híbridas Eólico-Fotovoltaicas no Submercado Sudeste/Centro-Oeste, Brazil Wind Power, 2022.

- LEITE, MATHEUS FELIPE AYELLO; Cruz, Arthur Augusto Pereira; Colombini, Angelo Cesar; Fortes, Márcio Zamboti; Lopes, Yona PROTEÇÃO DIFERENCIAL DE LINHAS - UMA ABORDAGEM USANDO SAMPLED VALUES In: Engenharia Elétrica: Desenvolvimento e Inovação Tecnológica.1ª ed.: Atena Editora, 2021, p. 54-70.

- SANTOS, MAYARA HELENA NOGUEIRA DOS; Ayello, Matheus Felipe; Pinheiro, Paulo Henrique Barbosa de Souza; Pinho, André da Costa; Colombini, Angelo Cesar; Fortes, Márcio Zamboti; Lopes, Yona. LATÊNCIA NA COMUNICAÇÃO PARA ESQUEMAS DE TELEPROTEÇÃO: REQUISITOS, AVALIAÇÕES E MEIOS DE TRANSMISSÃO In: Engenharia Elétrica: Desenvolvimento e Inovação Tecnológica.1 ed.Ponta Grossa, PR: Atena Editora, 2021, p. 325-342.

Chapter 2

Theoretical Foundation

To properly understand line differential protection using SV, we must understand the protection function proposed in our scheme with its operational principle, its advantages compared to other protection functions, and challenging implementation scenarios. The IEC 61850 standard, with its features, requirements, and protocols (extra attention will be directed towards SV protocol since it is plays critical role in our proposal). Also, it is essential we comprehend the time synchronization mechanisms since it is mandatory for the line differential protection function success. Understanding CT saturation is also crucial to understanding why reducing the risk of CT saturation plays a vital role in our proposal. We will also discuss high-impedance can be challenging for line differential protection scheme implementations along with the network metrics that we will evaluate in the net stress scenarios.

2.1 Transmission line differential protection

As shown in Figure 2.1, differential protection in transmission lines compares current magnitudes that enter and leave the protected circuit, according to Kirchhoff law. The currents at the two ends of the transmission line are compared by sending magnitudes and phases through a transmission medium, traditionally though a point-to-point communication link between substations.

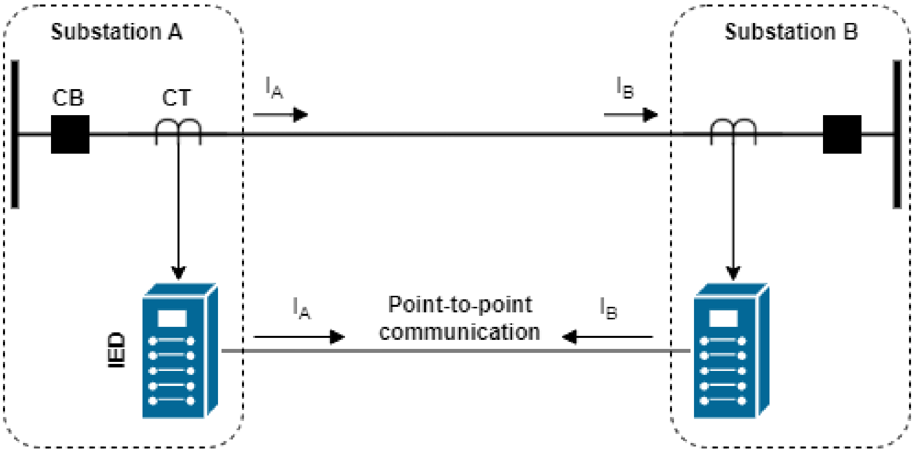


Figure 2.1: Typical scheme of line differential protection. (Prepared by the authors)

When very large currents flow through the protected zone for faults external to the zone, an erroneous differential current can appear due to the errors from different ratios and saturation of the CTs, channel delay measurement, and finite sampling frequency. If this erroneous differential current exceeds the operation threshold, it will result in incorrect operation of the current differential protection. Such an unwanted operation is avoided by means of stabilization. This technique traditionally uses a bias or restraint current, which is proportional to the sum of the absolute values of the currents measured at each protection terminal, i.e., $|I_A| + |I_B|$, to reduce the sensitivity of the protection for higher through currents. This stabilization technique is also called percentage restraint. Other implementations may use restraining quantities based on the maximum value of the measured currents, or the average value of the measured currents, or other methods. It is worth mentioning that our proposal can reduce the risk of CT saturation.

The usual communication mediums for differential protection are pilot wire or optical fiber. Major manufacturers of protective relays, such as ABB [15] and Siemens [16], use point-to-point communication with proprietary information protocols. That proprietary protocol does not allow interoperability among vendors.

There are different methods to implement the differential protection algorithm in protection relays. In practice, each manufacturer has its own method. We discuss one application found in protective relays from Siemens [16], and SEL [1] vendors for illustration. Although charge comparison relays are outdated, their operational principle will also be discussed in the following subsections.

2.1.1 Percentage differential protection

This algorithm provides sensitive protection for short circuits inside the protected area and good stability for external short circuits. The restraint current is the sum of the magnitudes of the currents measured at the local and remote terminals, and the operating current is the magnitude of the vector sum of both terminal currents. Figure 2.2 represents the operating characteristic of this principle.

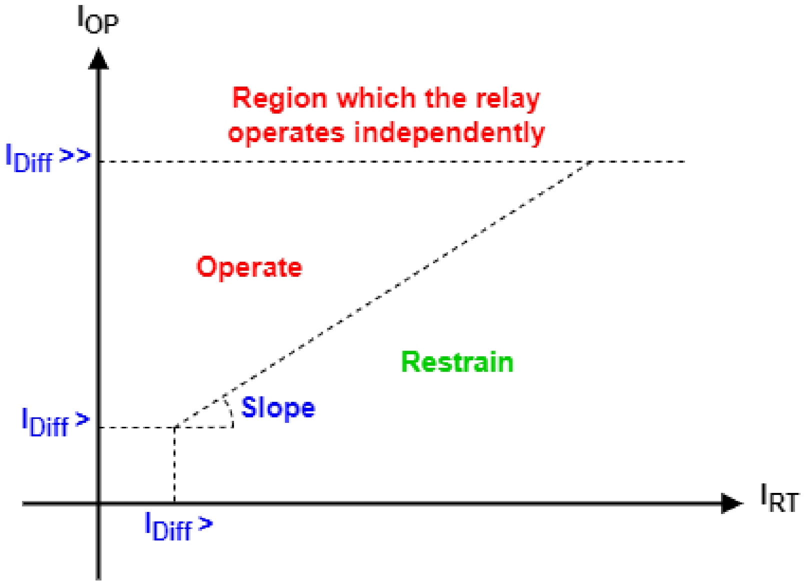


Figure 2.2: Percentage differential operation principle. (Prepared by the authors)

As shown in Figure 2.2, below a minimum current threshold ($I_{\text{Dif}} >$) there is no protection action. There is also another region for very high currents ($I_{\text{Dif}} >>$), where actuation occurs independently of the restraining current. The parameters to adjust the operating curve of a percentage differential relay are:

- $I_{\text{Dif}} >$ – sets the minimum threshold current of the function. The value goes both to I_{OP} and I_{RT} currents;
- *Slope* – defines the slope of the line;
- $I_{\text{Dif}} >>$ – it is a protection stage whose algorithm allows a faster action.

The $I_{\text{Dif}} >$ is determined from intrinsic errors of the measuring equipment. By default, it is equivalent to 10% Current Transformer Ratio (CTR) [17]. As recommended by manufacturers, the Slope is set to 0.3 to allow stability against external faults. For

$I_{\text{Dif}} >>$, it is necessary to evaluate switch on to fault scenarios, which makes the parameter determination more complex. Siemens specifies the method of parameterization of this variable for IED Sisprotec 7SD87 [16].

2.1.2 Alpha plane R-X diagram

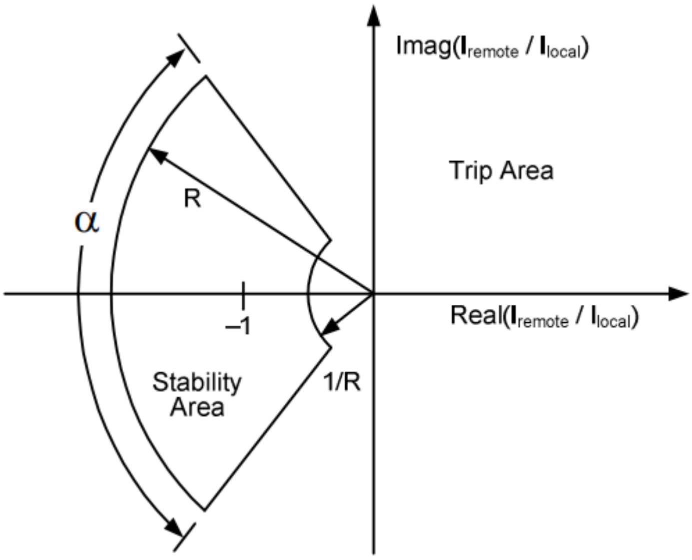

Imag(I_{remote} / I_{local})
Trip Area
α
R
−1
Real(I_{remote} / I_{local})
Stability Area
1/R

Figure 2.3: R-X plane characteristics [1].

Another way to perform differential protection is to use the angle between the current at the remote terminal and the current at the local terminal. The division between the two currents is performed, and its outcome is inserted into an R-X impedance plane. If the vector resulting from this division is located at the "Trip Area", as shown in Figure 2.3, the protection will act. The ratio would be close to the minus one point (–1,0) in a no-fault situation. There are two settings for this characteristic:

- **Radius - R:** the greater arc, typically between 5 and 10;
- **Alpha angle:** angle of the area, typically betwwen 160 and 210 degrees.

The complex variable representing the remote ($\mathrm{I_R}$) and local ($\mathrm{I_R}$) currents are established by the following equation $\frac{I_{\mathrm{R}}}{I_{\mathrm{L}}} = \mathrm{a} + \mathrm{bi} = \vec{r} = \mathrm{re}^{\mathrm{j}\theta}$.

In which:

- $\mathrm{a} = \frac{\vec{I}_{\mathrm{R}}}{\vec{I}_{\mathrm{L}}} \cos\theta$

- b = $\frac{\vec{I}_{\mathrm{R}}}{\vec{I}_{\mathrm{L}}}$sen θ
- r = $\sqrt{a^2 + b^2}$
- θ = arctan$\frac{b}{a}$

The above mentioned variables are the basis for the current ratio plane's both on the cartesian or polar coordinates versions. The alpha plane depicts the complex ratio of $\frac{I_{\mathrm{R}}}{I_{\mathrm{L}}}$ which is exposed in Figure 2.4.

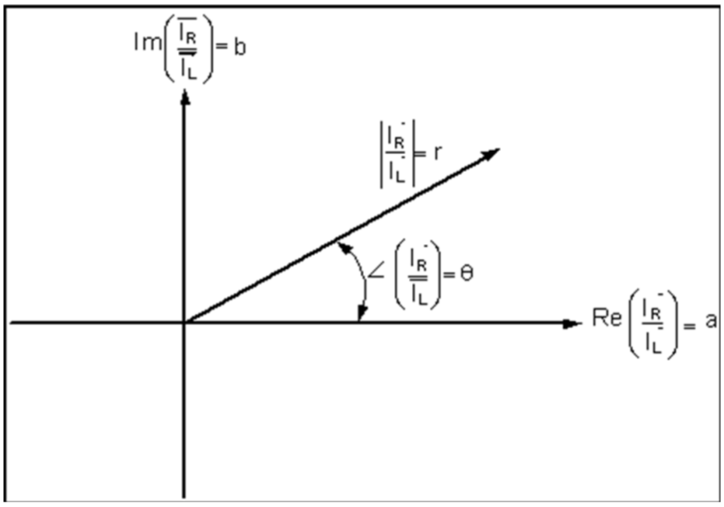

$\mathrm{Im}\left(\frac{\overline{I_R}}{\overline{I_L}}\right) = b$
$\left|\frac{\dot{I}_R}{\dot{I}_L}\right| = r$
$\angle\left(\frac{\dot{I}_R}{\dot{I}_L}\right) = \theta$
$\mathrm{Re}\left(\frac{\dot{I}_R}{\dot{I}_L}\right) = a$

Figure 2.4: Cartesian or polar coordinate being represented in the alpha plane. [2]

The alpha plane is useful for visualizing various power system load and fault conditions and sources of instrumentation error. Neglecting line charging current, through-load plots one unit to the left of the alpha plane origin at a = -1, regardless of the size or angle of the load current. Under ideal conditions, the current ratio for external faults is the same as for load conditions. Figure 2.5 shows the alpha plane region areas along the real axis of the alpha plane for ideal fault and load conditions. Internal faults with infeed from both line terminals have a > 0. Internal faults with outfeed at one terminal have a < 0 [2].

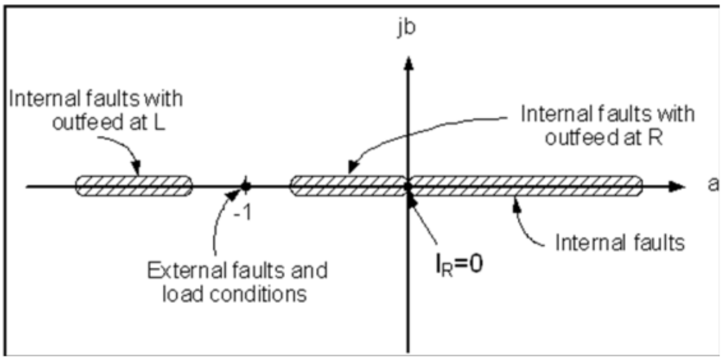

jb
Internal faults with outfeed at L
Internal faults with outfeed at R
a
-1
External faults and load conditions
I_R=0
Internal faults

Figure 2.5: Alpha plane regions only among the real plane - X. [2]

The corresponding source impedance angles and the angles of the impedances from the corresponding source to the fault site determine the angles of the local and remote fault currents. For an internal fault, the currents at both line endpoints are typically not perfectly in phase. When a CT reaches saturation, the primary waveform's basic component is smaller and is angled away from the reference value. The magnitude and phase angle of the alpha plane ratio increase, and an error with substantial magnitude and angle components results if the local CT saturates while the CT at the other end of the protected line does not. The transmission channel delay also produces an apparent phase shift between the local current and the received remote current as shown in Figure 2.6.

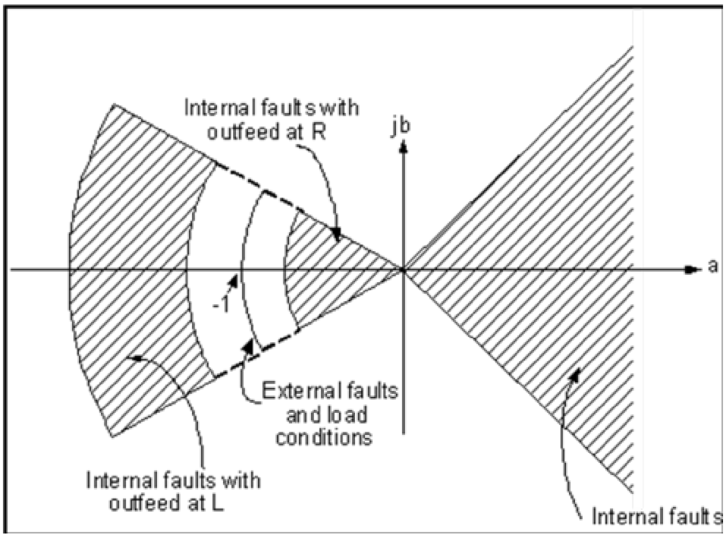

Internal faults with outfeed at R
jb
a
-1
External faults and load conditions
Internal faults with outfeed at L
Internal faults

Figure 2.6: Effect of channel delay compensation and system non-homogeneity in alpha plane. [2]

To avoid the apparent phase shift corrupting the current ratio computation or generating too much current difference, the line current differential relay must account for the channel delay. Measuring the roundtrip channel delay is a typical step in the ping-pong technique, a method for channel delay correction. The relay divides the return delay in half to determine the one-way channel delay. This calculation is correct if the delays in the transmit and receive directions are identical. In some channels, the propagation delay for the send and receive paths are dissimilar.

Delay asymmetry produces an error in channel-delay compensation. The effect of the error is to rotate the current ratio around the origin on the α-plane. A 1 ms error rotates the current ratio phasor by 21.6 degrees when the system frequency is 60 Hz while the magnitude ratio remains unchanged.

2.1.3 Charge comparison relays

The operating principles of charge comparison are similar to those of the more common percentage restraint current differential type of protective relay. Current differential relays compare the total currents entering and leaving the primary protection zone. They will trip if the difference between these currents exceeds some pre-defined restraint limit. For this comparison to be made, the current differential relay at the local station has to know the identical phase current recorded at the remote station(s) for the same interval being considered at the local station. This requires precise communications delay measurement and compensation. With current differential relays that compare instantaneous values, any error in compensation causes an error in the comparison and results in a variation of pickup point. In addition, many samples per cycle are sent to the remote station, burdening the communications channel.

Charge comparison relaying addresses this problem by comparing local and remote station readings on a half-cycle basis. The total charge is added for a half cycle upon a zero crossing and transmitted to the remote end. For a proper comparison to be made at the remote station, all that is required is that the proper half cycles be compared. This allows a much greater error in time delay compensation with no impact on the pickup point. The transmission of only one value per phase per half cycle dramatically reduces the throughput requirements of the communications channel [2].

Data synchronization is typically done automatically with ping-pong round trip time measurements where the resultant measurement is divided by two to get the one-way delay. This method can result in minor errors for asymmetrical communications networks, but due to the tolerance for errors in a charge comparison relay, this is rarely an issue. Assuming a perfect alignment between local and remote currents, there is approximately 4 ms of error tolerance in the compensation. Given that line capacitance will cause a slight misalignment of the currents and that any compensation will have some resolution, it is practical to use approximately 3 ms to limit how much the communications channel delay can vary during regular operation without affecting the relaying. This is well within the normal operational limits of most communications channels in a dedicated fiber or T1(E1)/SONET(SDH) environment, even under adverse conditions [2].

2.1.4 Challenging line differential protection implementation scenarios

The following implementations with specific types of power systems configuration challenges traditional line differential protection schemes [2]. The highlighted ones will be further detailed in Chapter 4. It is worth mentioning that all the solutions for those challenges that are not directly handled by the use of SV on the scheme can be incorporated into the internal line differential protection algorithm to be implemented.

1. **Multi-terminal line protection;**
2. **Dual breaker applications;**
3. Setting considerations;
4. Open-CT conditions;
5. **CT ratio compensation;**
6. Mutually coupled lines;
7. Charging current compensation;
8. Switch-onto fault;
9. Weak infeed issues;
10. Out-of-step;
11. **CT saturation detection/compensation;**
12. Stub bus;
13. Single phase tripping;
14. Multi-phase auto-reclosing;
15. Series compensated lines;
16. Shunt reactors;
17. In-zone transformers and tapped loads;
18. Backup protection considerations;
19. Communication channel cutout switch.

2.2 High impedance faults

High-impedance faults majority occurs in electric distribution systems, but they can also occur in transmission systems. A conductor contacting a tree with a high impedance or when a broken conductor touches the ground are examples of high-impedance faults. Some of the typical features of high impedance faults are:

- **Non-linearity:** Voltage-current characteristics are highly non- linear due to changes in current conducting path [18];
- **Asymmetric nature of its current:** Peak values of current are different in the positive and negative half cycles due to the presence of varying breakdown voltage [18];
- **Intermittent nature:** High-impedance faults current is not steady due to intermittent nature of arc [18];
- **Build up:** Current magnitude progressively increases till it reaches its maximum value [18];
- **Randomness:** The magnitude of their current and its shape changes with time due change in impedance of conducting path [18];
- **Low and high-frequency components:** High-impedance faults current includes low-frequency components due to their non-linearity nature. Additionally, its current also contains high-frequency components due to intermittent nature of arc [18].

Since high-impedance faults can lead to small short-circuit currents, their detection can be challenging because their values can be in the same range as some of the line operational conditions. A transmission line overload is expected in some cases, so power systems engineers must guarantee that the protection functions will not operate in those cases unless they were previously predicted to occur or actuate after a long time of overload.

2.3 CT operational principles

A CT basically consists of two sets of wire windings around an iron core, as shown in Figure 2.7. The concept is the same for a window or bushing CT, which consists of a secondary winding around a core, with the primary winding being the primary conductor that passes through it. An alternating magnetic flux in the presence of a wire loop induces a voltage across that loop. Magnetic flux is the amount of magnetic field passing through the transformer core.

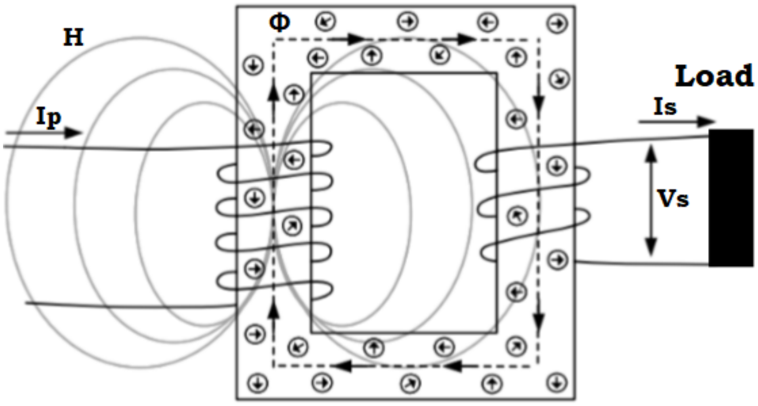


Figure 2.7: Current transformer operational principle. [3]

When alternating current I_P flows in the primary winding of a transformer, it generates an alternating magnetic field H, which corresponds to an alternating magnetic flux Φ, around the transformer core. This alternating magnetic flux passes through the secondary winding.

When the secondary coil is connected to a burden, the alternating magnetic flux in the core induces an alternating voltage V_S across the secondary winding. This causes a corresponding alternating current I_S to flow in the secondary winding. The alternating current in the secondary creates its own alternating magnetic field and alternating magnetic flux that opposes those created by the primary winding. These primary and secondary fluxes cancel, leaving a negligible net flux in the core.

The secondary current leaving the CT (I_S) is a replica of the primary current (I_P) divided by the ratio of the number of turns in each winding. This occurs until the core becomes saturated [3].

2.3.1 CT saturation

The material of the magnetic core of the CT has limitations regarding the amount of magnetic flux it can withstand. The secondary voltage induced from the primary side directly relate to the amount of magnetic flux that flows through the core. In other words, the bigger the load attached to the secondary coil, the bigger is the risk of saturation [3]. Figure 2.8 illustrates the effect of increasing the load attached at the secondary winding.

The core will need to withstand more flow to maintain the secondary voltage, increasing the saturation risk.

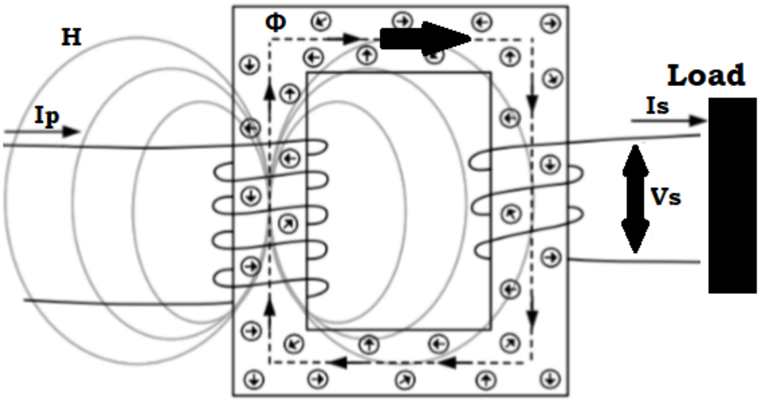


Figure 2.8: Load increase on the secondary winding. [3]

When a CT saturates, I_S does not accurately replicate I_P. That situation can lead to the non-functioning of protection functions or unwanted trip operations. It is worth mentioning that NCIT does not function under the same electromagnetic principle and has no risk of saturation.

With many devices requiring the CT current information, they must all be connected to the secondary winding which will increase the secondary load and, therefore, the risk of saturation.

MU helps mitigating this situation since it does not matter how many devices are connected, the information will be sent in digital communication networks through SV protocol. This occurs because the MU will be the only load connected to the CT. Since we propose the use of SV protocol on line differential protection schemes, the risk of CT saturation is either mitigated with MUs or eliminated through the NCIT.

The NCITs operational principle is based on light deviation principles, where the polarized light will deviate accordingly to the magnetic field force generated by the primary current. Figure 2.9 shows the device's functioning.

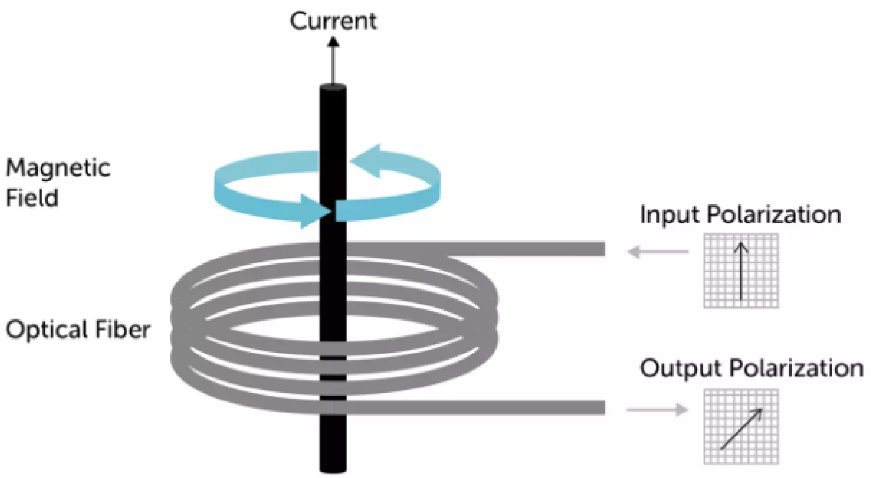


Figure 2.9: Optic CT operational principle. [4]

2.4 IEC 61850 standard

The Standard is divided into parts that establish specific points to be addressed in each of them, the segments that are relevant to the work are described as follows:

- **Part 1:** Introduction and overview [19];
- **Part 2:** Glossary [20];
- **Part 3:** General requirements [21];
- **Part 4:** System and project management [22];
- **Part 5:** Communication requirements for functions and device models [23];
- **Part 6:** Configuration description language for communication in electrical substations related to IEDs [24];
- **Part 7-4:** Basic communication structure for substation and feeder equipment - Compatible logical node classes and data classes [6];
- **Part 9-2:** Communication networks and systems for power utility automation - Specific Communication Service Mapping (SCSM) - SV over International Organization for Standardization (ISO)/IEC 8802-3 [25];
- **Part 90-1:** Communication networks and systems for power utility automation - Use of IEC 61850 for the communication between substations [26];

- **Part 90-2:** Communication networks and systems for power utility automation - Using IEC 61850 for communication between substations and control centres [27];
- **Part 90-3:** Communication networks and systems for power utility automation - Using IEC 61850 for condition monitoring diagnosis and analysis [28];
- **Part 90-4:** Communication networks and systems for power utility automation - Network engineering guidelines [29];
- **Part 90-12:** Communication networks and systems for power utility automation - Wide area network engineering guidelines [10];

Equipment's based on the Standard has the functional structure as shown in Figure 2.10 in which the exposed levels are defined as follows:

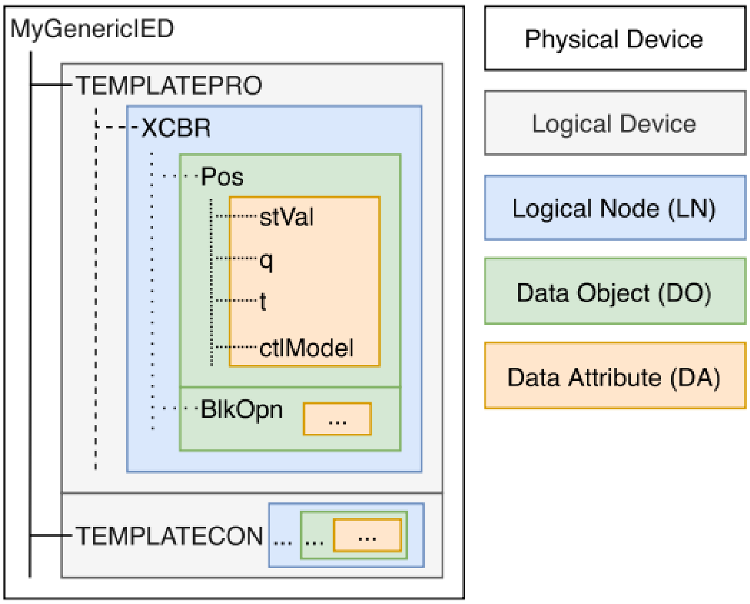


Figure 2.10: Functional structure of IEC 61850 based equipments. [5]

1. **Physical Device:** The IED itself, being identified by the name of the equipment or its IP (Internet Protocol) address;
2. **Logical Device:** Organizational role, the devices' common logical nodes are grouped according to a chosen rule, such as their functionality. Examples of established logic devices include protection, automation, measurement, control, and configuration logical devices. However, the Standard does not standardize the terminology of logical devices and leaves them up to the users, being one of the challenges for interoperability;

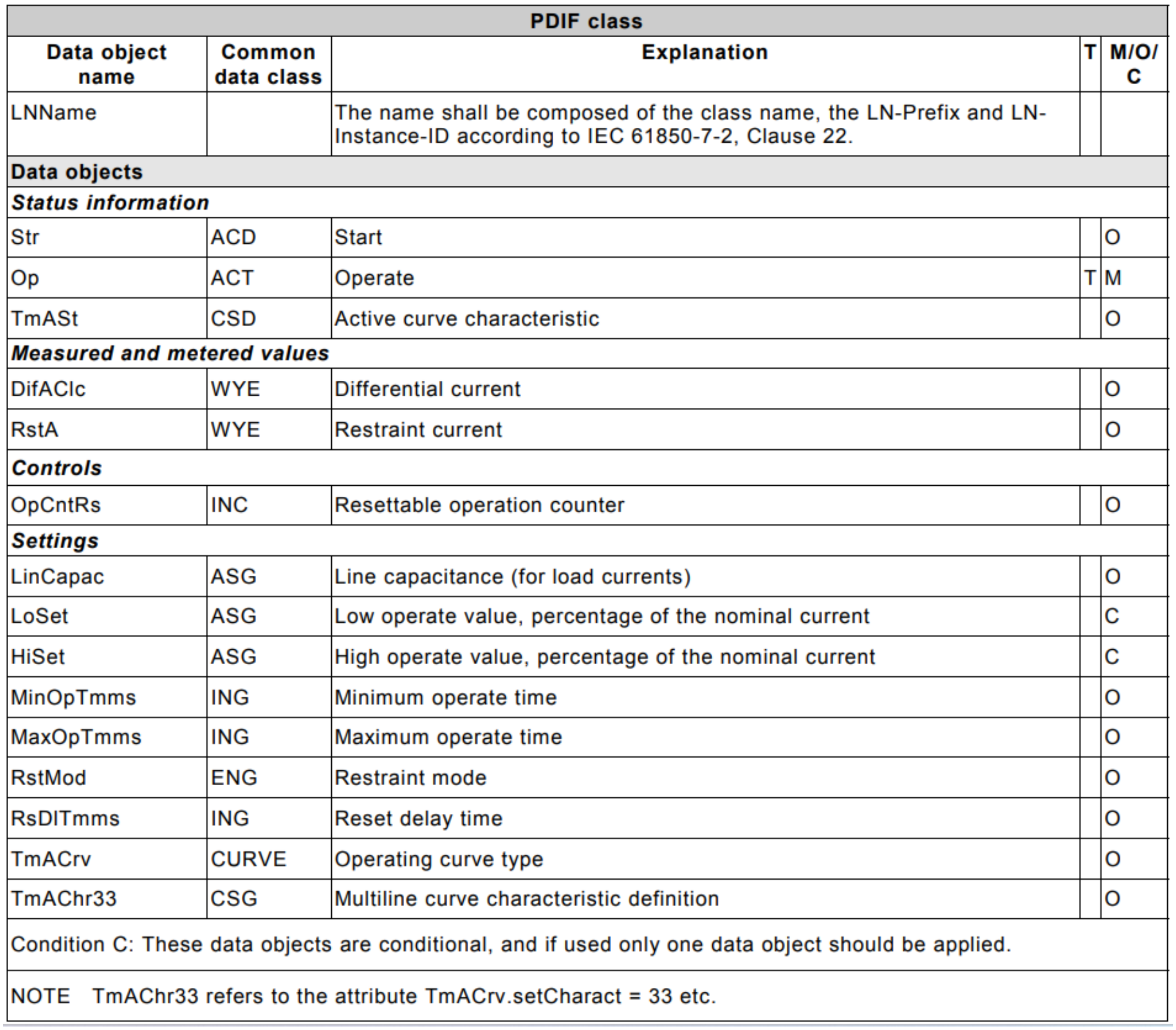
3. **Logical node:** These are the functionalities, equipment or actions modeled in conformance with the Standard. The model is made with three to six characters as a prefix, while the functionality of the logical node itself is defined by four standardized characters according to its class (e.g., XCBR - Circuit breaker). Finally, there is a suffix to be used with the feature's instance number. An example would be the logical node **FrqPTOF2**, where it would be a way of naming the second stage over-frequency protection. The class **PTOF** is standarised for over-frequency protection, the three-character prefix **Frq** and the suffix **2** indicates second stage. It is important to note that both the prefix and the suffix are user-oriented, with only the maximum number of characters being standardized, which makes it an important field to be checked for interoperability;

4. **Data object:** This item presents greater detail in the hierarchy, and the available types are standardized according to data class, established in IEC 61850-7-3 [30], of the chosen logical node;

5. **Data Attribute:** The actual data to be sent by the dataset. It can take the form of measurement attributes, equipment binary state, integrity descriptions, etc. For instance, the attribute **stVal** of the data object **Pos** of the logical node **XCBR**, indicates the breaker state.

2.4.1 Logical node for differential protection - PDIF

This logical node is used for all kinds of current differential protection. Proper current samples for the dedicated application shall be subscribed. On master-slave current differential protection schemes, the master IED can signalize to the slave's line terminals the protection actuation through the PDIF logical node. Figure 2.11 exposes the PDIF class on section 7-4 of the IEC 61850 Standard [6]. When signalizing the actuation of the differential protection function, the data object "Op" is used.



PDIF class				
Data object name	**Common data class**	**Explanation**	**T**	**M/O/C**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22.		
Data objects				
Status information				
Str	ACD	Start		O
Op	ACT	Operate	T	M
TmASt	CSD	Active curve characteristic		O
Measured and metered values				
DifAClc	WYE	Differential current		O
RstA	WYE	Restraint current		O
Controls				
OpCntRs	INC	Resettable operation counter		O
Settings				
LinCapac	ASG	Line capacitance (for load currents)		O
LoSet	ASG	Low operate value, percentage of the nominal current		C
HiSet	ASG	High operate value, percentage of the nominal current		C
MinOpTmms	ING	Minimum operate time		O
MaxOpTmms	ING	Maximum operate time		O
RstMod	ENG	Restraint mode		O
RsDlTmms	ING	Reset delay time		O
TmACrv	CURVE	Operating curve type		O
TmAChr33	CSG	Multiline curve characteristic definition		O
Condition C: These data objects are conditional, and if used only one data object should be applied.				
NOTE TmAChr33 refers to the attribute TmACrv.setCharact = 33 etc.				

Figure 2.11: PDIF class. [6]

2.4.2 MMS

The Manufacturing Message Specification (MMS) protocol incorporated in the 8-1 section [31] of the Standard, previously defined by ISO 9606 [32], designed for communication between programmable devices with monitoring and control interfaces, following a client-server model. Its application is mainly associated with Supervisory Control and Data Acquisition (SCADA) and Human Machine Interface (HMI), carrying out monitoring, control, and commands directly in the IED. Usually, the IED works as a server that will provide information and reports to client users that requested those services.

2.4.3 GOOSE

The Generic Object Oriented Substation Event (GOOSE) messages, defined in the 8-1 section [31] of the Standard, are designed to send datasets through the network based on event changes or periodically. These messages are exchanged between the network IEDs informing the status of variables contained in the datasets and can be used for protection or control schemes. Its use is mainly associated with protection interfaces, breaker trip commands, among other applications. The protocol works asynchronously, following a publisher-subscriber model.

2.4.4 SV

The SV messages, defined in section 9-2 [25] of the Standard, are the digitalization of the acquired voltage and current values and are sent to devices configured to receive them. Such conversion and sending can be performed by NCIT, being the optical CTs and Potential Transformers (PTs), or through the MUs, being these intermediate conversion equipment, which acquires analog values of voltage and current through conventional measurement and, later, sends the digitized information using the SV protocol. The 9-2 Light Edition [33] reduces the complexity and difficulty of implementing an interoperable process bus based on IEC 61850-9-2. This is achieved by restricting the transmitted data sets and specifying the sampling rates, time synchronization requirements, and the physical interfaces to be used.

The protocol overhead for IEC 61850-9-2-based sampled value transfer is substantial. Twelve bytes of frame wrapping, twelve bytes of address data, four bytes of 802.1Q tag, two bytes of Ethertype, and twelve bytes of payload make up a typical 802.1Q marked Ethernet frame. The ASN.1 encoding, additional fields that indicate the source of the sampled data and a time-stamp are the overhead for the sampled value payload specified in IEC 61850-9-2. Figure 2.12 depicts a 126-byte long 9-2LE frame for protection applications, but only 32 of those bytes actually hold the sampled values. (eight 32-bit integers). The Application Specific Data Unit (ASDU) would be replicated seven more times in the 9-2LE [33] power quality application. The no ADSU attribute at offset 0x1E in this instance would be eight.

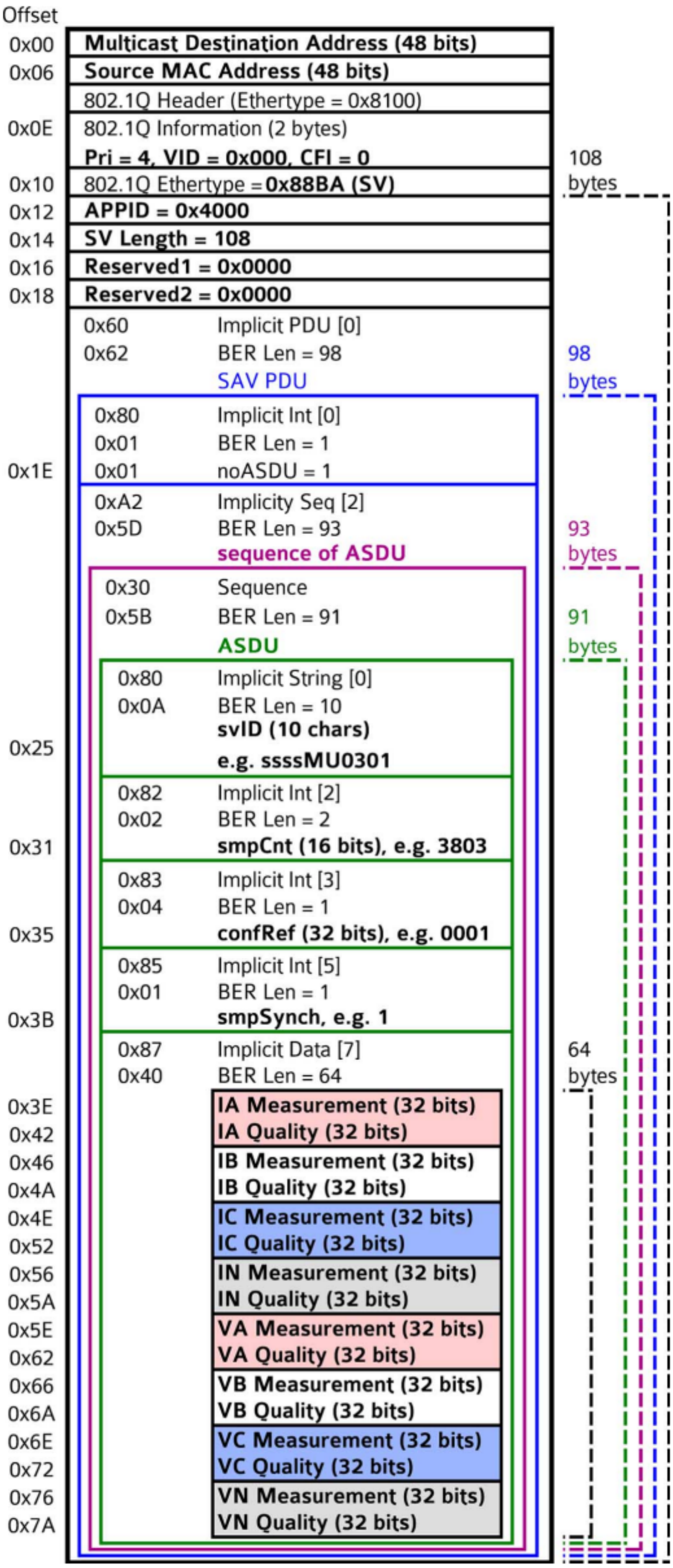

Offset
0x00 Multicast Destination Address (48 bits)
0x06 Source MAC Address (48 bits)
802.1Q Header (Ethertype = 0x8100)
0x0E 802.1Q Information (2 bytes)
Pri = 4, VID = 0x000, CFI = 0
0x10 802.1Q Ethertype = 0x88BA (SV)
0x12 APPID = 0x4000
0x14 SV Length = 108
0x16 Reserved1 = 0x0000
0x18 Reserved2 = 0x0000
0x60 Implicit PDU [0]
0x62 BER Len = 98
SAV PDU
0x80 Implicit Int [0]
0x01 BER Len = 1
0x1E 0x01 noASDU = 1
0xA2 Implicity Seq [2]
0x5D BER Len = 93
sequence of ASDU
0x30 Sequence
0x5B BER Len = 91
ASDU
0x80 Implicit String [0]
0x0A BER Len = 10
svID (10 chars)
0x25 e.g. ssssMU0301
0x82 Implicit Int [2]
0x02 BER Len = 2
0x31 smpCnt (16 bits), e.g. 3803
0x83 Implicit Int [3]
0x04 BER Len = 1
0x35 confRef (32 bits), e.g. 0001
0x85 Implicit Int [5]
0x01 BER Len = 1
0x3B smpSynch, e.g. 1
0x87 Implicit Data [7]
0x40 BER Len = 64
0x3E IA Measurement (32 bits)
0x42 IA Quality (32 bits)
0x46 IB Measurement (32 bits)
0x4A IB Quality (32 bits)
0x4E IC Measurement (32 bits)
0x52 IC Quality (32 bits)
0x56 IN Measurement (32 bits)
0x5A IN Quality (32 bits)
0x5E VA Measurement (32 bits)
0x62 VA Quality (32 bits)
0x66 VB Measurement (32 bits)
0x6A VB Quality (32 bits)
0x6E VC Measurement (32 bits)
0x72 VC Quality (32 bits)
0x76 VN Measurement (32 bits)
0x7A VN Quality (32 bits)
108 bytes
98 bytes
93 bytes
91 bytes
64 bytes

Figure 2.12: Dissection of a 9-2LE sampled value frame, with key items in bold. [7]

SV messages can follow a multicast or unicast profile, depending on the application.

Unicast communication is from one device on the network to exclusively another device on the network. In contrast, multicast communication is from one device on the network to many, but not necessarily all devices on the network.

For this multicast communication to occur, the messages need to be configured with the multicast address through which they will propagate. Regarding the recommendation of the standard for the structure of this address, its informative annexes B of part 8-1 [31] and part 9-2 [25] describe the multicast address structure as follows:

- The first three octets are assigned by the Institute of Electrical and Electronic Engineers (IEEE) to be 01-0C-CD;
- The fourth octet must be 01 for GOOSE and 04 for SV;
- The value 00-00-00-00-00-00 should be used to indicate that the multicast address was not set;
- The last two octets are to be used as assigned individual addresses by the interval defined in Table 2.1.

Table 2.1: Range of recommended multicast addresses. [9]

Service	**Initial address (hexadecimal)**	**Final address (hexadecimal)**
GOOSE	01-0C-CD-01-00-00	01-0C-CD-01-01-FF
Multicast SV	01-0C-CD-04-00-00	01-0C-CD-04-01-FF

The information transfer rate follows the system frequency, being 4000 samples per second for 50 Hz systems and 4800 samples per second for 60 Hz systems. The SV messages have a label indicating which type of synchronism the device is using [25]. This feature is important in assuring time synchronization when a device receives SV frames from multiple devices. There are three options for time source label:

- 0 - indicates that the current and voltage samples are not synchronized with any time source;
- 1 - indicates that the samples are synchronized with a local time source;
- 2 - informs that the samples are synchronized with a global time source.

To perform line differential protection, both of the IEDs must have a mutual synchronization. Considering that in such a technique, the devices are at two different substations, it is mandatory that the devices are synchronized with a global time source.

2.5 Time synchronization

In time-critical applications, reliable and precise synchronism among the devices is mandatory. In line differential protection, the IED must process current values measured simultaneously, or unwanted trips might occur. There are two forms of providing this synchronism: It can be incorporated into the differential protection scheme or by an external time source for the equipment. The majority of power system devices allow three different types of external synchronization mechanisms. Table 2.2 qualitatively analyzes the methods.

The dominant protocol in power systems is IRIG-B, which requires a separate cable in addition to the Ethernet or serial cable used to communicate with the device. Although Network Time Protocol (NTP) is the most widely used time synchronization protocol in the world, it lacks the accuracy to be used in power systems. Watt et al observes that IEEE 1588 PTP distributes precise time with better than 1-microsecond accuracy over Ethernet, which is becoming the standard technology for IED communication [8].

Table 2.2: Time syncrhonization protocols comparison [8].

Time distribution methods	IRIG-B	NTP	PTP (IEEE 1588 and IEEE C37.238)
Physical Layer	Coaxial cable	Ethernet	Ethernet
Model	Master-slave	Client-server	Master-slave
Syncrhonization accuracy	=∼100 ns to 1 μ s	=∼1 to 100 ms	=∼100 ns to 1 μ s
Compensation for latency	Yes, using cable lenght as user input	Yes	Yes
Update interval	Once per second, pulse per second (pps)	Minutes	Configurable, typically once per second
Hardware requirements	Special hardware required at master and slave	Master only	Hardware support required for high accuracy
Relative cost	Medium	Low	Medium to high

It is worth mentioning that for SV applications, some manufacturers require the mandatory use of PTP on their devices as can be seen in Watt et al [8]. Therefore, only this option will be discussed in more detail.

2.5.1 PTP

IEEE 1588 PTP is a message-based time transfer protocol that enables synchronization accuracy and precision in the sub-microsecond range for packet-based networked systems [34]. The PTP was first released in 2002 as Version 1 and then revised in 2008 as Version 2. The two versions are incompatible; therefore, having a mix of Version 1 and Version 2 devices in the same network is not possible. This work focuses entirely on Version 2 because it is the most widely deployed version.

We must understand all the variables to configure PTP devices properly. In Figure 2.13 we see a usual PTP network topology, where the devices are described below:

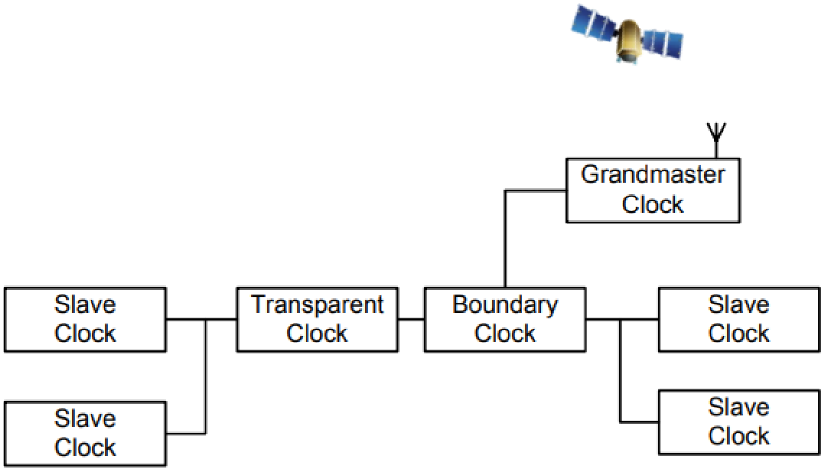


Figure 2.13: Example of PTP network topology. [8]

- **Grandmaster clock:** serves as the ultimate source of time for all other devices in the network [8];
- **Slave clock:** synchronizes to another clock serving time [8];
- **Boundary clock:** is a multiport network device that synchronizes to the reference time on one port and serves time on one or more ports. One of the ports is a slave port, and the rest are master ports. In essence, boundary clocks terminate and then start the time distribution. This functionality is usually built into PTP-aware network components like switches, bridges, and routers. Boundary clocks can be used to scale up a PTP network by servicing requests from slave clocks that would otherwise be serviced by the grandmaster clock [8];

The **transparent clocks** can be either end-to-end or peer-to-peer, and Figure 2.14 demonstrates the difference between the two approaches. Their definitions are explained as follows:

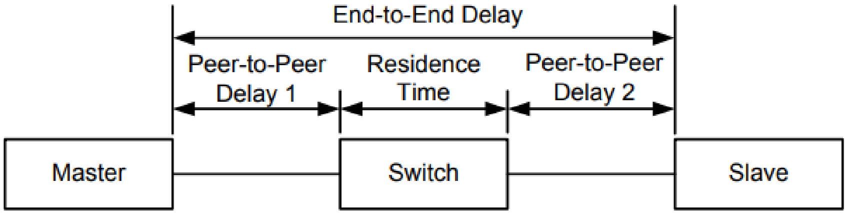


Figure 2.14: Example of PTP network topology. [8]

- **End-to-end:** a multiport network device that measures the length of time a PTP message spends within the device as it is routed from the ingress port to the egress port and then adds that information to a correction field in the message. This is intended to eliminate any variations in message delays and asymmetry that the device may introduce in the transfer of PTP messages. The end-to-end transparent clock functionality is typically performed by PTP-aware switches [35].

- **Peer-to-peer:** a multiport network device that measures the link delay of each port and adds that information and the residence time to PTP messages traversing the device. Like the end-to-end transparent clock, the peer-to-peer transparent clock eliminates asymmetry and packet delay variations in the device. Additionally, it allows for scaling because slave devices do not have to send requests to the grandmaster clock to measure the end-to-end delay. Instead, each device measures the delay to its peer [35].

A non-transparent switch is a device that does not support PTP and does not account for the residence time for the traffic going through it. Those devices can reduce the accuracy of the time synchronization mechanism.

More than one PTP profile is available to be configured on the grandmaster clock device. The concept of PTP profiles allows organizations or industry groups to specify a subset of options and features and default values for protocol attributes that will meet the performance requirements of applications in the domain and eliminate or minimize device settings. The most popular profiles are the default profile, telecom profile, and power system profile. The default and power system profiles are the most common profile for power systems applications. Their difference is mainly due to attribute options (e.g., transport over IEEE 802.3 Ethernet or User Datagram Protocol (UDP) over IPv4) and optional features (e.g., unicast message negotiation) [8].

With the SV protocol, the IED can sort the current values according to their message time stamps inside the SV frame. The mechanism to guarantee time synchronization is on the time source label. This attribute on the SV frames will be further detailed in the following Section. Once the values are sorted based on their timestamps in a global time source, the IED can use multiples SV messages from various devices without causing misoperations.

2.5.2 Time synchronism inherited to the scheme - 87L

To incorporate the device synchronism in the line differential protection scheme, the communication channel among the line terminals must be a deterministic and symmetric network. The latency of the communication network is then provided to the devices to compensate properly for the sending delay of the remote terminal.

Once both devices know the communication latency, the IEDs can compensate for the current value to be processed by shifting it accordingly with the remote current value, as shown in Figure 2.15.

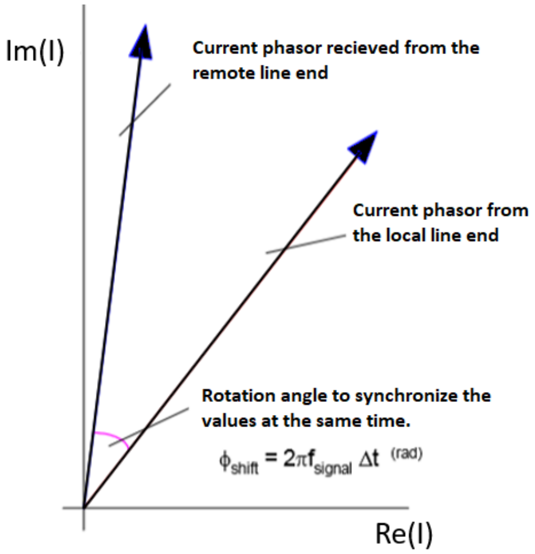

Im(I)
Current phasor recieved from the remote line end
Current phasor from the local line end
Rotation angle to synchronize the values at the same time.
$\phi_{shift} = 2\pi f_{signal} \Delta t$ (rad)
Re(I)

Figure 2.15: Rotation angle to synchronize both of the values. (Prepared by the authors.)

2.6 Network evaluation metrics

Network performance consists of several metrics to be considered when implementing a communication network. Section 90-12 of IEC 61850 Standard [10] establishes several performance requirements to be followed in WAN power systems applications. Following those guidelines is crucial for ensuring a reliable power system.

Although there are other metrics to be considered on Ethernet communication networks, this work will only bring more detail into the delay, bandwidth, throughput, and packet loss since the network case study will only perform scenarios under those variables.

2.6.1 Delay or latency

Network latency is the time it takes for messages to travel from one network component to another. Latency on a radial network path is cumulative, so proper network engineering can mitigate latency issues by preventing excessive buildup of latencies.

Section 5 of Standard IEC 61850 [23] specifies the latency classes for internal communication within the substation, while section 90-1 [26] for external traffic to substation. However, they do not directly contextualize the case of WANs. In this sense, a new class of latencies specifically for WAN networks is defined in [10] according to Table 2.3.

Table 2.3: WAN latency classes. [10]

WAN latency class	**Latency (ms)**	**Application**
TL1000	$\leqslant 1000ms$	Every other application
TL300	$\leqslant 300ms$	Operator commands
TL100	$\leqslant 100ms$	Slow automated interactions
TL30	$\leqslant 30ms$	Fast automated interactions
TL10	$\leqslant 10ms$	Teleprotection
TL3	$\leqslant 3ms$	Differential Protection

The delay can be subdivided into two main classes:

2.6.1.1 Propagation time

This time is mainly related to the physical means of transmission of the message. In [10], a common parameter of 5 μs/km for optical fibers or copper cables and 3 μs/km for radio waves is defined. It is worth mentioning that there are other considerations for the physical environment, such as signal attenuation and maximum distance associated with technologies, among others. In Local Area Network (LAN) networks, this propagation time is more relevant for time synchronization protocols, with little impact on other applications. As for applications on WAN networks, this time is significant for network analysis.

2.6.1.2 Message residence time on network components

This time is related to the message hopping along network components such as switches, routers, gateways, and connection interfaces. In Time Division Multiplexing (TDM) networks, the waiting time is constant. Since the operation is cyclical, only a short buffer time is needed to synchronize the cycles. On Packet Switching Network (PSN), the residence time may vary, taking into account the following factors:

- Processing time, including the integrity, checks time, and cybersecurity associated with the message;

- Waiting time in message queue;
- Waiting time for data grouping before definitive sending;
- Jitter buffering, waiting time to compensate for the jitter introduced in non-deterministic networks;
- Actual message transmission time.

The average latency value is insufficient for the proper temporal evaluation of network packets. The jitter or Packet Delay Variation (PDV) expresses the packet latency variation on the network. Some methodologies for mitigating network jitter, such as de-jitter buffer, can be found in [10]. Jjitter and the associated challenges are a common reality in non-deterministic networks. In this sense, Table 2.4 presents the classes for WAN networks defined in section 90-12 [10].

Table 2.4: WAN jitter classes. [10]

Jitter class	**Jitter (ms)**	**Application**
TJ00	Non specified	Every other
TJ10	10	External signal synchronization
TJ0,3	0,3	Mutual synchronization

2.6.2 Bandwidth

Bandwidth is the maximum possible data transfer rate of a network. When sharing multiple services under the same communication network, we must consider if our system has enough bandwidth to withhold all those applications. A poorly planned network can compromise its applications and lead to a surpass of the allowed latency or the non-retrieval of critical messages. Also, there are cyber attacks that lead to network flooding. Throughput is the actual data transferred successfully in a network. Measuring network bandwidth does not consider whether a test data transfer results in successful or unsuccessful data transmission. It simply calculates the amount of data transferred in the network.

2.6.3 Throughput

The throughput or transmission rate of a network is a critical performance metric that informs the rate at which information is transmitted over a link and is defined by the number of bits the link can transmit in a given time interval, being measured in some multiplicative quantity of bits/s.

Depending on the size of the link, the throughput may be heterogeneous in some of its sections due to the different capacities of the interfaces of each piece of equipment. When two-channel interfaces communicate with each other with two different transmission rates, it is intuitive to understand that the channel throughput will be given by the lowest rate between the two interfaces. However, the higher rate can support all data the inferior receives, but the opposite is not valid. The network section where the lowest throughput link is located is defined as the network bottleneck [36].

Although trivial in the case of two interfaces, the problem of identifying the bottleneck link in a larger network can become more complex. It can cause high packet loss values and even lead to network unavailability when not properly considered.

2.6.4 Packet loss

Packet loss is a metric generally expressing the percentage of the total number of packets transmitted over a link that the destination host did not receive. The impact of the number of lost packets can vary from service to service, so some solutions such as redundancy, interpolations and retransmissions can be used to mitigate the loss of information. Packet losses can also occur due to cyberattacks and misconfigured equipment. However, its leading causes in switched networks come from physical failures, such as cable breakage and hardware burnout; and spikes in network congestion.

Congestion in non-deterministic networks is mostly caused by random bursts of a high volume of packets, which causes the rate of packets processed by network nodes to be higher than their transmission rate. This situation causes buffer to enter the condition of overflow, in which the transmission queue of the equipment reaches its maximum value and, due to lack of space, new processed packets end up being discarded and consequently lost. In deterministic networks, network congestion is controllable due to the absence of traffic variation, and its occurrence is more linked to link sizing errors. The causes can be summirized in the following items:

- An overload on the network switch, the amount of data being processed surpasses his capacity;
- Signal attenuation (interferences, degraded communication channel, defective connector, etc).

- Routing errors;
- Cyber attacks.

Chapter 3

Releated Work

Since early 2000, Gao et al was pointed out the need for using Global Positioning System (GPS) clocks in line differential protection schemes [37]. Apostolov and Ingram et al explores the use of SV messages in bus differential protection and power transformers [38, 39]. However, there are few works for transmission lines, and their focus has been on time synchronization without performing feasibility studies.

Liu et al discuss the line differential protection based on IEC 61850. The authors perform a theoretical analysis emphasizing time synchronization and conclude that its use is feasible [11]. However, no simulations were carried out to validate the analysis. Blumschein et al. discuss interoperable line differential protection schemes with devices from the same vendor but with older device versions [40], and their proposal focuses on the protection algorithm, not the communication network dynamics. One of the main contributions is detailing how both studied devices process their line differential protection algorithm and how interoperability can be performed.

Ingram et al uses an Real Time Digital Simulator (RTDS) and equipment's from digital substations to evaluate SV in transformer differential protection [39]. An important contribution of the paper is the evaluation of the performance of the scheme by purposeful increasing the time lag between the MUs. The authors observed that 1 ms of difference is enough to cause several unwanted trips close to the constraint curve of the differential function. Pereira et al proposes a new tool for testing protection systems providing a closed loop test with IEC 61850 functionalities incorporated in the device [41]. The authors perform a case study comparing legacy analog injections with SV. Melo et al carry out a similar test in [42].

The Cigré Joint Working Group 34/35.11 stablishes a maximum time asymmetry of

0.1 ms to guarantee reliability in any differential protection schemes [43]. Bächli et al raise the symmetry requirement to 0.2 ms. The authors also point that, for systems operating at a frequency of 60 Hz, an asymmetry of 0.4 ms means an angular discrepancy of 3.6^{o} between the currents, which can lead to problems in the protection's sensitivity [44].

Barron et al discuss the performance of differential protection in feeders using GPS synchronization and show results from its use in the UK electrical transmission system. They also present a network architecture with backup routes for differential protection [45].

Different papers indicate the need for evaluation of the communication network and the analysis of the synchronization requirements for SV messages. An et al make a general analysis of possible architectures and network requirements for digital substations [46]. Oliveira and Yona carries out a case study in the company Braskem, in Brazil, with a SONET network to evaluate the network latency from messages according to IEC 61850 standard protocols [47]. The authors found times of up to 4.14 ms, including IED processing at source and destination. However, the architecture consisted of a ring between five substations ranging from 2 km to 5 km. Santos et al carries a reliability assessment of communication assisted line protection schemes is done. Both works apply a statistical approach considering the device's repair times and system failure probabilities [48], [49]. Zheng et al. present an interesting study regarding the use of line differential protection schemes on High Voltage Direct Current (HVDC) transmission lines [50].

In the present work, we propose and evaluate the use of SV messages for line differential protection. Alongside the proposal, we conduct a case study to investigate the protection performance by doing high impedance short-circuit simulations in two 500 kV transmission lines. Another significant contribution is the network performance test under stress conditions (delay increase, concurrent traffic, and packet loss) to verify communication impact on the protection's overall performance. Table 3.1 compares the contributions of the present work with some of the debated along Section 3.

Table 3.1: Qualitative comparison between the current work and those discussed in the Section.

Papers	Discusses 87L with SV	Presents a new 87L scheme with SV	Propses the use of external synchronization in 87L	Carries out case studies to verify the feasibility of 87L with SV	Perform case studies on communication metrics that influence the use of SV in differential protection schemes	Proposes or discusses the use of SV in differential protection schemes for generators, busbars, feeders, and transformers
Current work	✓	✓	✓	✓	✓	
[11]	✓	✓	✓			
[37]			✓		✓	
[38]			✓			✓
[39]			✓		✓	✓
[40]	✓		✓		✓	
[41]	✓		✓	✓	✓	
[42]	✓		✓		✓	
[43]	✓		✓		✓	✓
[44]	✓		✓	✓	✓	✓
[45]	✓		✓			✓
[47]					✓	
[46]	✓	✓	✓		✓	

Chapter 4

The use of Sampled Values in Line Differential Protection

As stated in Chapter 1, the traditional use of differential protection on transmission lines has the following issues:

- Limited to short transmission lines (up to 120 km);
- Requires a dedicated deterministic communication channel between the devices. This represents an economic disadvantage since utilities cannot offer possible extra bandwidth to other services;
- Since it relies on proprietary communication protocol with dedicated point-to-point communication channels, it requires the addition of extra communication cards on the IED in other to obtain more reliability on the communication network;
- Increases the risk of CT saturation in comparison with the use of MU and SV messages;
- Does not incorporate a modern and more accurate time synchronization mechanism - PTP;
- Does not allow interoperability among vendors.

To surpass those issues, a line differential protection scheme based on SV protocol is proposed. The main goal of this new method is to enhance the line differential protection and expand its use since it is currently the more selective and fast protection function for transmission lines [11]. The use of standardized communication protocols and non-point-to-point communication channles allows to increase the network reliability through the network topology. Also, we intend to further expand the IEC 61850 standard applications since it represents economic and operational advantages.

4.1 Proposal scheme architecture

The new proposal is represented in Figure 4.1 consisting of a transmission line interconnecting two substations and its communication network. It represents the implementation of SV in line differential protection schemes, and its main elements are the substation communication network, the IEDs in compliance with IEC 61850 standard with SV publishing and subscribing, the line differential protection function (87L), the MU that could be NCIT as well, the GNSS antenna with the time synchronization device, and the Ethernet communication network. Those features will be discussed in detail in Sections 4.1.1 to 4.1.6:

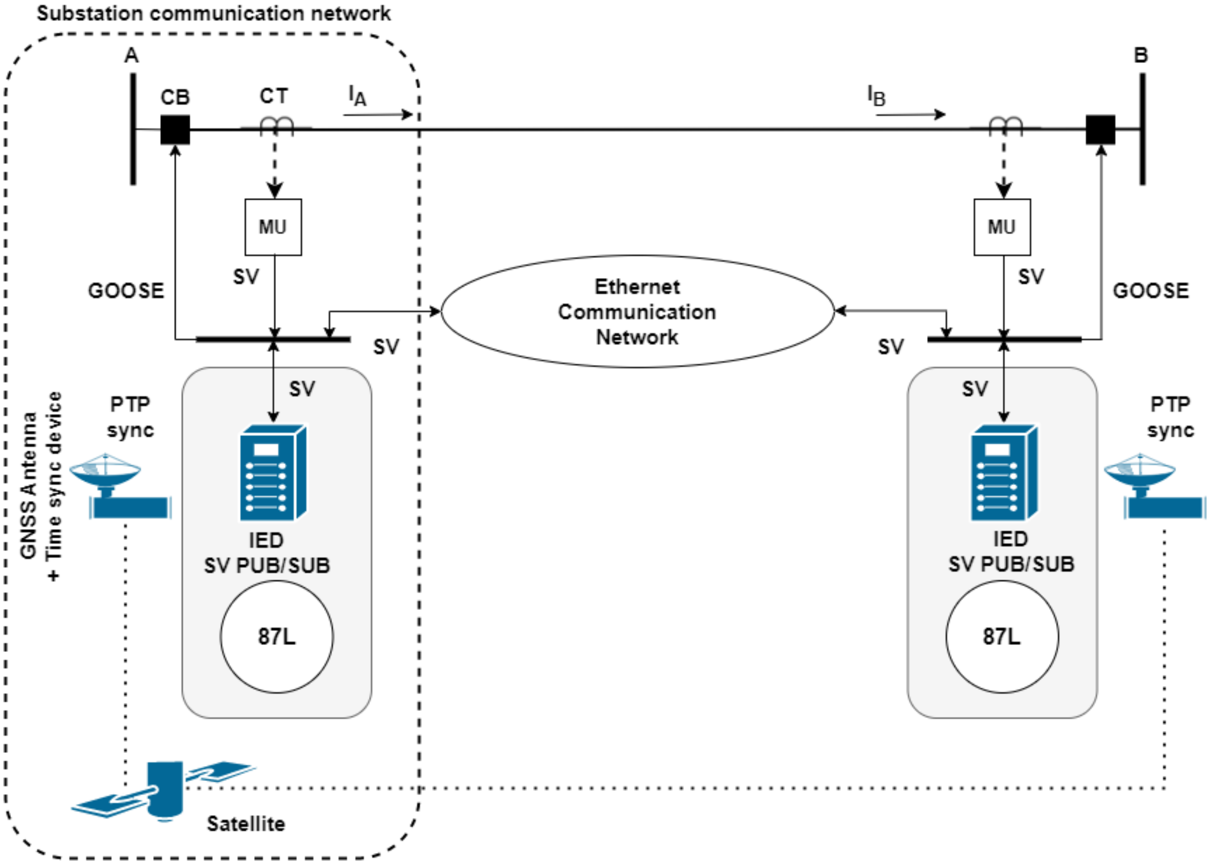


Figure 4.1: The proposal of using SV for line differential protection (Prepared by the authors).

4.1.1 Substation communication network

Substation Communication Network (SCN) consist of the entire internal substation communication network infrastructure and its interface with the external Ethernet communication network. SCNs need to be robust, reliable, and resilient, being able to properly attend their desired applications in compliance with the IEC 61850 communication modeling, data structure, and service requirements.

As stated in Chapter 2, the Standard follows functional levels linked to functional interfaces to be implemented among the levels, and communication buses types. It is important to consider that those functional levels are an abstraction of the Standard functionalities and not an network architecture impose by IEC 61850. The various possible solutions for SCN must be tested and discussed for redundancy, performance, disturbance, and network security due to the fact that Ethernet provides a flexible base for the bus and the IEC 61850 series does not require a particular type of solution.

4.1.2 IED with SV publishing and subscription

IED are microprocessor-based power system devices that can incorporate several functionalities such as protection, control, automation, supervision, measurement, monitoring, and cyber security functions. The IED must have the line differential protection function among its applications and to be able to both publish and subscribe SV messages in compliance with Section 9-2 of IEC 61850 Standard [25].

The device must support the PTP synchronization mechanism in other to properly sort the remote and local current in other to process its line differential protection algorithm. The IED that receives the SV message uses the SmpCnt to align the samples in time and thus reconstitute the waveform, becoming independent of any frame transmission delay through the Ethernet network that works with statistical switching.

Interoperability must be assured in case of using different vendors among the line terminals. The SV messages must interoperate by having the same sample rate and the same desired numerical base for some identification tags (some manufacturers use hexadecimal and others the decimal one, as stated by Junior et al [51]).

4.1.3 87L

It consists of the line differential protection function algorithm that will be implemented on the IEDs. The 87L protection function is not tied to any vendors specific methodologies.

As stated in Chapter 2 there are several line differential protection types, with each of them having its own advantages and preferences among vendors. The 87L must be fast, selective, and reliable to protect the transmission line properly.

Using SV messages in line differential protection only interferes with the mutual synchronization of the remote and local values by sorting it accordingly with its time stamps and has no impact on the protection function detection algorithm. It is worth reminding that for the line differential protection function, the SV time source label must be 2, an indication that the SV message has a global time source reference.

4.1.4 MU or NCIT

The sampling of current line current measurements can be done either with MU or NCIT. In the first case, the analog CT hardwire is connected to the MU that digitalizes and encapsulates the current values and sends them to the IEDs via SV protocol. NCIT are next-generation instrument transformers that do not rely on the use of coils and magnetic principles for measuring primary values. The line current induces a light deviation inside the device that directly associates the light deviation to current values, which sends the measurements to the other devices using the SV protocol.

4.1.5 GNSS antenna alongside a time synchronization device

The devices must be synchronized with global time reference source. This feature is mandatory so that the line differential protection algorithm can be processed using remote and local current values measured at the same time.

The GNSS antenna captures that GPS or GLONASS satellites signals and provides a global time reference source for the time synchronization device. The device needs to comply with the PTP protocol that reaches accuracy in the nanosecond range. It is suitable for applications where timing is critical for the measurement system. The high accuracy of the protocol is obtained by compensating for the propagation delay of the information between the synchronization source and the destination.

4.1.6 Ethernet communication network

The WAN that connects the substations is the Ethernet communication network. The process values of currents from both the local-end and remote-end MU IEDs are required to implement differential protection. As a result, the protection IED in the local substation must receive process value information in the form of SV from the MU of the remote end substation. A WAN is required for the transmission of SV messages between substations that are far apart. The typical SV message, on the other hand, only has a data link layer and does not include transport or network layers. As a result, two communication methods are recommended by IEC 61850-9-1 [26] for transmitting SV messages over a wide area network for inter-substation communication: 1) tunneling; and 2) the proxy gateway method, which makes use of specific telecom equipment.

4.2 Advantages

As stated in several chapters in this work, the implementation of SV protocol in line differential protection provides multiple benefits regarding operational advantages, innovative solutions for the communication network, more reliability to the scheme performance, and innovative commercial solutions for the non-dedicated architecture. Sections 4.2.1 to 4.2.4 detail further those advantages, whereas Section 4.2.5 summarizes the comparison with other methods.

4.2.1 Communication Reliability Through Network Topology

The use of standardized communication protocols, in contrast with proprietary communication protocols that requires dedicated point-to-point communication networks, brings several advantages regarding the innovation possibilities among the communication network topology and network recovery times.The increase of backup paths between devices drastically increases the network reliability and, therefore, will enhance the transmission line communication network. As demonstrated in Figure 4.2, a backup path can be established between the IEDs. With proprietary communication protocols, this would only be possible with the addition of extra communication cards on the devices, which will increase the IED cost. Another economic advantage is that with standardized communication protocols and non-dedicated networks, any extra bandwidth can be sold for commercial purposes as long as they do not interfere with the performance of the scheme. This feature will be tested in Chapter 5.

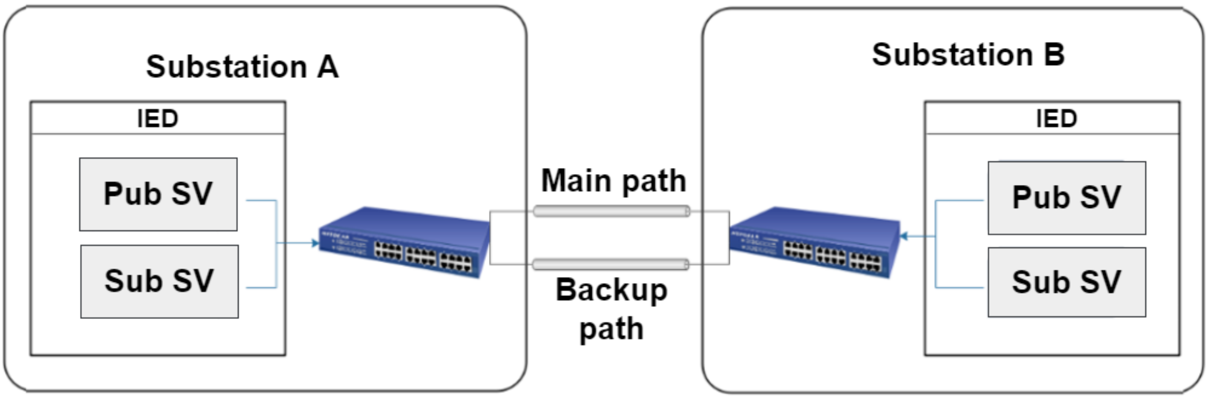


Figure 4.2: Example of communication redundancy through the network topology (Prepared by the authors).

4.2.2 CT Saturation Risk Reduction

As stated in Chapter 2, CT saturation can compromise line differential protection functions and must be considered while implementing the function. This phenomenon is directly related to the number of devices that are attached to the CT. Often the CT must provide the measured current values for many devices among the substation to fulfill the desired applications. With the use of the MU, that situation is minimized since the MU will be the only load connected to the CT. The measured current is sent to the rest of the devices through the communication network with SV messages. Figure 4.3 illustrates this scenario.

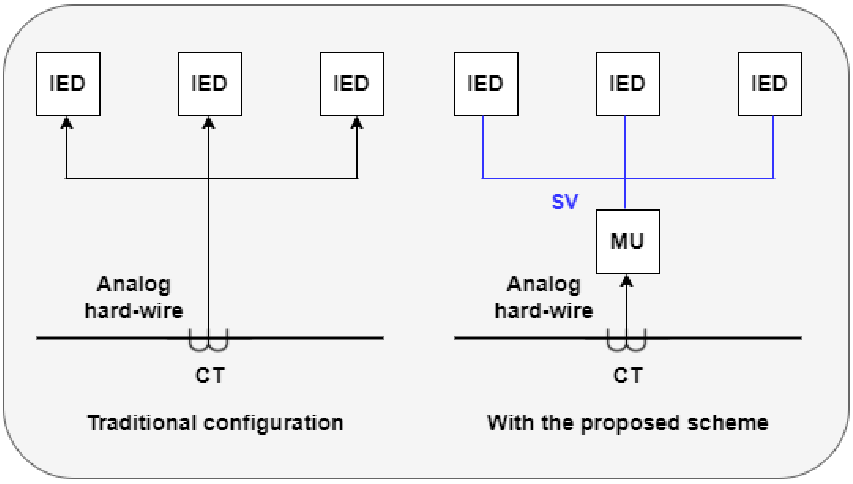


Figure 4.3: Comparison between the conventional CT hard wire to the IED and the use of MU (Prepared by the authors).

4.2.3 Specific Power Systems Implementation Advantages

As shown in Chapter 2, there are specific power systems implementation cases that directly impact the line differential protection scheme performance. The following cases can be directly solved or minimized through our proposal.

1. **Multi-terminal line protection:** Since the most common power system transmission lines have two or three terminals, the typical digital line current differential relay has been designed to accommodate these two applications and cover the case of operating radially. Most vendors offer options for at least two communications ports on the relays for exchanging the current differential data as well as any corresponding restraint data between relays. Having two ports permits either a single or redundant/backup channel link between the relays of a two-terminal line or a single channel communicating with two remote relays for three-terminal applications operating without redundant channels. If the traditional relay-to-relay dedicated communication mode is considered, each relay will require N-1 communications ports for exchanging its current data with the other relays. An eight-terminal application, for example, would require seven ports. The number of channels required, just for non-redundant coverage, will also greatly expand with increased N. Obtaining simultaneous data for channel-based schemes could also present difficulties, especially in establishing the synchronization of many sampling clocks.
   Our new proposal can effectively handle that situation. The use of standardized communication protocols alongside with non-point-to-point communication channels allows the increase of reliability through the communication network, and the time-synchronization is performed isolated at each terminal, so synchronizing the devices will not be an issue.

2. **Dual breaker applications:** Line protection in breaker-and-a-half configurations requires main protection functions to respond to the sum of the two currents. This concerns many protection functions, mainly when sensitive settings are applied and/or significant CT saturation occurs. If the remote system is relatively weak, the current supplied through the line towards a close-in reverse fault on the breaker-and-a-half terminal may be overridden with a spurious current produced by saturated CTs. In addition to the usual difficulties associated with CT errors, this arrangement introduces an additional aspect when only one of the two CTs goes into heavy saturation during an external close-in fault. Because the relay does not respond to the individual currents but to their sum, a combination of restrained

and unrestrained differential principles is effectively applied and may face stability problems. The combination of the small restraining current and the relatively large erroneous differential current could cause unwanted operation in the worst case.
The use of SV protocol through MU or NCIT will either reduce or eliminate the CT saturation. So our proposal can help mitigate the described issue.

3. **CT ratio compensations:** Comparing currents between stations requires identical scaling of currents at both ends. In an ideal world, current differential relaying would always be installed with exactly matched CTs to help ensure that not only are the steady state measurements identical, but reactions to transients are similar at both ends. Unfortunately, this is often not the case. Due to various factors, existing CTs may be used, and they are often very different in ratio and characteristic behavior. A difference in ratio can often be corrected for by the relay. The ratio between line current and secondary current is entered into the settings, and the difference is compensated for in the analog gain section of the current input or in the software itself. There are a couple of factors to consider when unequal CTs are used. All relays are optimized for a known full load line current, either 1A or 5A typically. This allows the measurement and processing design of the relay to work with a given range of values. For example, assume the two CTs are 600:5 and 2400:5. One end will have four times the secondary current. The lower ratio CT may saturate and should be selected so that maximum currents remain within the dynamic range of the CT and relay input circuitry.
The use of SV protocol through MU or NCIT will either reduce or eliminate the CT saturation. So our proposal can help mitigate the described issue.

4. **CT saturation detection/compensation:** One source of CT measuring errors is CT saturation. CT saturation is less of a problem for internal faults, and the main concern is external faults with an unequal degree of saturation in the two line ends. When one of the CTs saturate and not the other, the secondary currents presented to the relays will cause a differential current to be measured. Generally, CT errors due to saturation can be compensated by decreasing the relay sensitivity. Some percentage restraint current differential relays include a CT saturation detector that increases the bias in the presence of saturated current waveforms.
The use of SV protocol through MU or NCIT will either reduce or eliminate the CT saturation. So our proposal can help mitigate the described issue.

4.2.4 Commercial Advantages - Exceeded Bandwidth

As can be seen in Figure 4.4, utilizing non-dedicated communication networks allows for selling exceeded bandwidth for other applications. This feature can provide extra income for utilities and incentives for more innovative solutions with open architecture. This feature was one the motivations for evaluating the performance of the protection with the concurrent traffic injection.

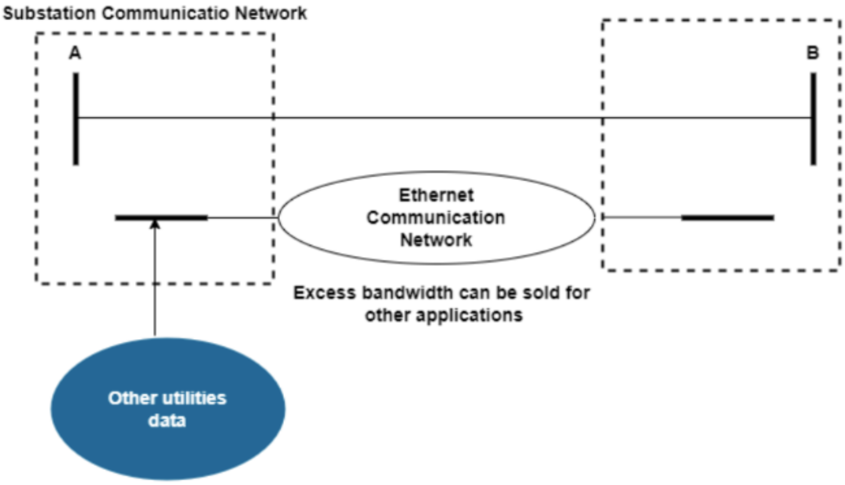

Substation Communicatio Network
A
B
Ethernet Communication Network
Excess bandwidth can be sold for other applications
Other utilities data

Figure 4.4: Using exceeded bandwidth for other commercial purposes. (Prepared by the authors)

4.2.5 Comparison with Other Methods

In traditional transmission line differential protection, the communication channel transfers in every execution loop at least three current values and may transfer status and control digital messages. However, the sampled values (three voltages and three currents) is a digital message along the previous status and control messages. Therefore, resulting in similar data rates and bandwidth requirements from traditional line differential protection schemes.

When compared to the other available methodologies, Table 4.1 shows the main advantages of performing differential protection with the SV protocol.

4.3 Functioning of the proposal

To properly understand the functioning of the proposal, we must consider the behavior under a short circuit case. As can be seen in Figure 4.5, a short circuit was applied at

Table 4.1: Comparison between the proposed scheme and the others found in the literature.

Methods	**Feasible for line lengths above 120 km or 74,6 miles**	**Fast fault clearence**	**No risk from CT saturation**	**Exceeded bandwidth for commercial purposes**	**External time synchronization**	**Communication resiliance through network topology**	**Interoperability**
87L-SV proposed scheme	✓	✓	✓	✓	✓	✓	✓
Traditional analog hard wired		✓					
Proprietary communication protocols	✓	✓			✓		
Equivalent travelling wave	✓	✓	✓		✓		

the transmission line. In that case, the following steps will occur to eliminate the fault:

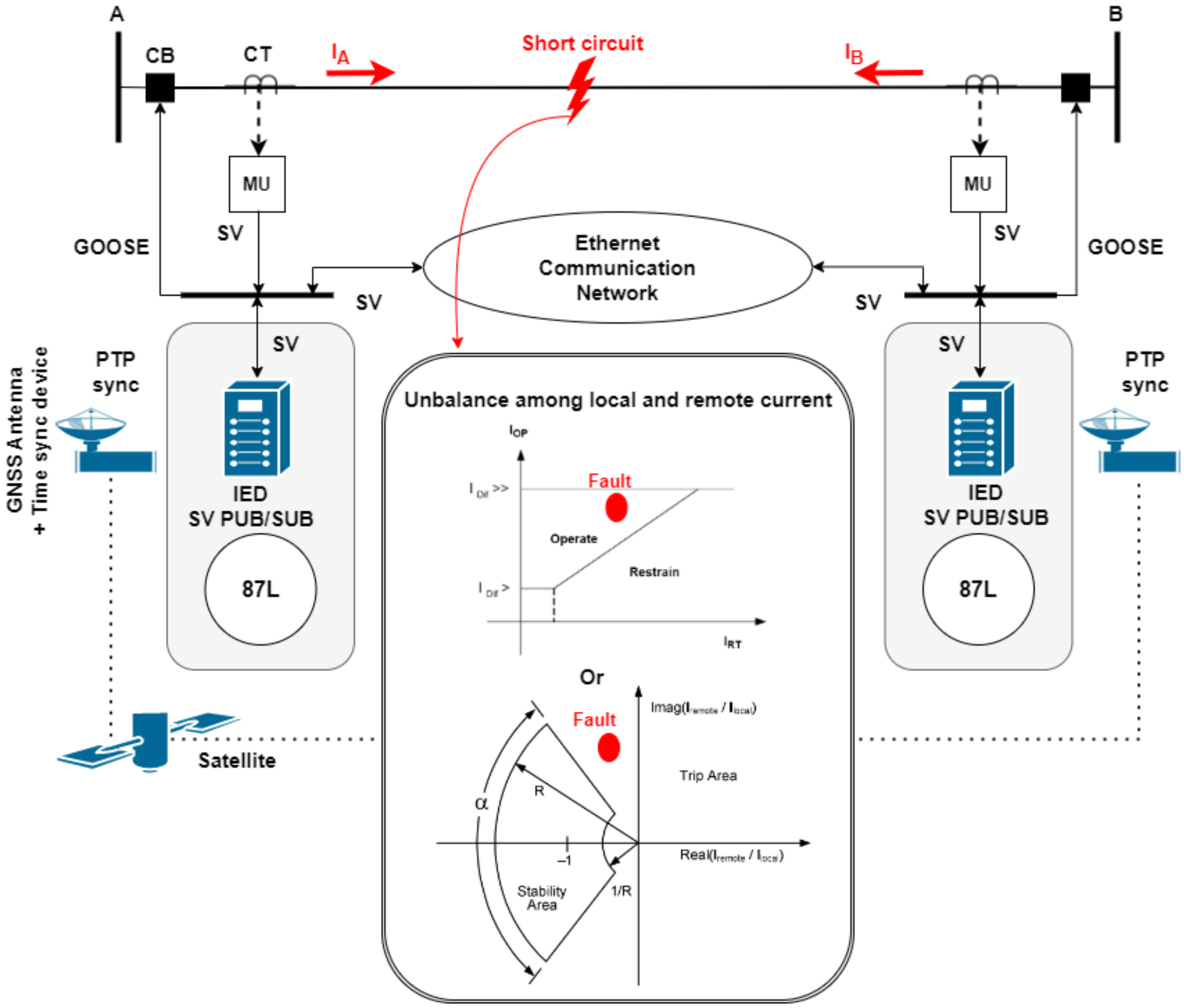


Figure 4.5: Demonstration of the functioning of the proposal.

1. Both of the currents (I_A and I_B) will flow towards the short circuit;
2. The current values measured by the CTs will drastically increase in comparison with the line current nominal value;
3. The MUs will digitalize the analog current measurements through the SV protocol;
4. The measured current strings at the local terminal are constantly being sent to the adjacent remote terminal through the Ethernet communication network;
5. The IEDs are receiving the local and remote current measurements and sorting it accordingly with the message time stamps;
6. Once the IED receives a remote fault current and processes with its local fault current, the line differential protection function will detect the unbalance between the current values. It is important to mention that the line differential protection

algorithm is not imposed and can be either the alpha plane R-X diagram or the line percentage differential protection;

7. With the detection of the fault condition, the IEDs will command the opening of its circuit breaker to eliminate the fault;

8. With both of the circuit breakers opened, the transmission line is no longer under a short circuit;

9. In a master-slave mode, only the master IED will be subscribing both of the SV messages and will command the opening of the slave terminal circuit breaker through a GOOSE message in the Ethernet communication network.

Chapter 5

Line Differential Protection Scheme Proposal Evaluation

Line differential protection is fast and selective, and its use enhances transmission line protection. Transmission lines can have a wide range of lengths, and each case will have its particularities. Due to their enormous extensions, they are susceptible to many faulty conditions. One of the more challenging is the high-impedance short circuit that, as stated in Chapter 2, can be difficult to detect. In this sense, we carry out a case study using percentage line differential protection on two 500 kV transmission lines. The transmission lines have different lengths, and we will apply four high-impedance short circuits throughout the lines. The test aims to verify the scheme's feasibility in the two studied lines.

The WAN that represents the Ethernet communication network that interconnects the substations is a critical part of our new proposal. The SV messages are transmitted through the WAN, and it must fulfill the performance requirements for differential protection established by IEC 61850 Standard (such requirements can be found in Chapter 2). We will assess the impact of network stress scenarios on line differential protection schemes. The following tests will be proceeded in Section 5.2: Delay increase test (emulating the line length); a heavy traffic scenario with concurrent traffic throughout the same WAN; and packet loss scenario. In each test, we will injected a short circuit in the IED, and we will assess the trip time. We repeated each scenario thirty times to ensure average results within the 95% confidence interval. The net stress scenarios impact among the network metrics is also evaluated, and intent to evaluate the impact of common communication network issues on the line differential protection scheme. The concurrent traffic scenario can also assess how much traffic can be transmitted alongside the SV messages, this scenario can help commercial decisions of selling excessive bandwidth to other applications. We will also measure the impact of the packet loss and additional traffic net stress scenarios on SV messages delays. The testing methodologies will be described at Sections 5.2.

5.1 Percentage line differential protection case study*

To evaluate the feasibility of the line differential protection algorithm on transmission lines, it will be performed a short-circuit case study considering high impedance faults (with 120 Ω of fault resistance) at two 500 kV transmission lines in four different locations among the lines. We chose two transmission lines with different lengths to cover the scheme feasibility in a short and long transmission line. The four fault locations serve a similar purpose in verifying the scheme's performance covering the entire line length.

The study data were taken from case 1912PB[1] present in the short-circuit database provided by ONS - The National Electric System Operator in Brazil - and the short-circuit simulations were performed in the Aspen Oneliner software.

As can be seen in Figure 5.1 from the Aspen Onliner software, two 500 kV transmission lines were chosen to evaluate proposal feasibility to verify if the percentage differential relay in those lines is feasible. In any of the chosen transmission lines, it would be possible to implement the new methodology proposed in Section 4. In that case, the "S.MESA 500" would be the substation represented in busbar A, and "S. MESA 2 500" and "SAMAMB. 500" would be positioned in busbar B.

*The results were published at XXVI SNPTEE 2022."Uso de Sampled Values da IEC 61850 na Proteção Diferencial de Linhas" Ayello. M, Pereira. A, Collombini. A and Lopes. Y

[1] https://sintegre.ons.org.br/sites/8/32/85/paginas/servicos/produtospasta.aspx?RootFolder=/sites/8/32/85/Produtos/167/03-06-2020_192602 - Private base. Access available upon registration.

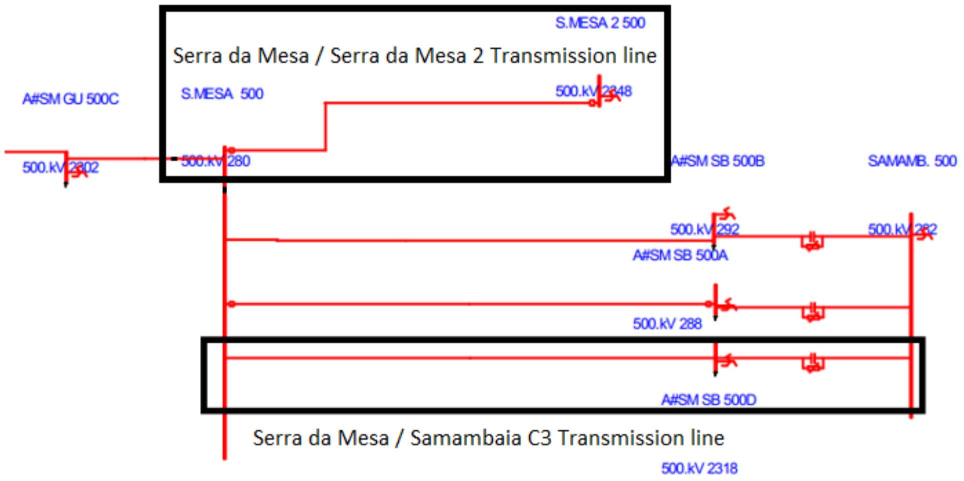


Figure 5.1: Capture highlighting both transmission lines in Aspen Onliner software.

The lines have the following length:

1. Serra da Mesa – Serra da Mesa 2: line length - 42 km;
2. Serra da mesa – Samambaia C3: line length - 248 km.

The lines were chosen to assess the difference in behavior for different lengths. According to the CT ratio in Table 5.1, the parameter $I_{\mathrm{Dif}} >$ of Serra da Mesa – Serra da Mesa 2 and Serra da Mesa – Samambaia transmission lines are 200 A and 300 A, values that are equivalent to 10% of the transformation ratio of the lines current transformers. As can be seen in Chapter 2, this is a standard parameterization while using percentage-type differential schemes.

Table 5.1: Transmission lines data

Transmission line	**Line length (km)**	**CT Transformation ratio**
Serra da Mesa - Samambaia C3	248,56	3000
Serra da Mesa - Serra da Mesa 2	42,68	2000

We evaluate the feasibility of differential protection in four different scenarios of short circuits with high impedance faults 120 Ω. We create short circuits for both transmission lines with a fault distance in relation to the Serra da Mesa terminal equivalent to 25%, 50%, 75%, and 99% of the total line length, Figure 5.2 ilustrate the scenario.

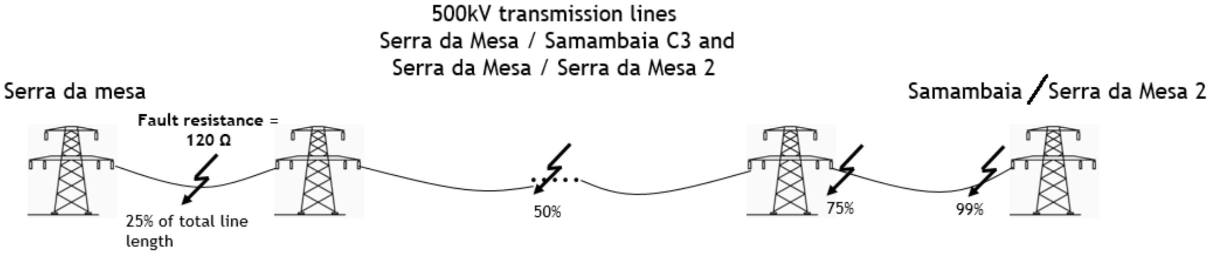


Figure 5.2: Four high-impedance short circuits throughout the the two transmission lines.

With this, it is possible to evaluate the current measured in the four reported situations. The results are in Tables 5.2 and 5.3. The slope of the curves present in Figures 5.3 and 5.4 follow the recommendation of Section 2 of 0,3. To evaluate the results, we generated restrain curves of line differential protection for the two transmission lines following the $I_{Diff >}$ equivalent with 10% of the CT ratio, and the curve slope equivalent of 0,3. After generating the graph, the results from Tables 5.2 and 5.3 were placed on the curve to verify it the faults would be positioned among the operating region of the restrain curve.

Table 5.2: Fault simulation Serra da Mesa - Samambaia transmission line

Distance (%)	**I_{OP}(A)**	**I_{RT}(A)**
25	**545,90**	**1255,08**
50	**549,04**	**1240,21**
75	**1713,94**	**1738,12**
99	**2695,13**	**2269,75**

Table 5.3: Fault simulation Serra da Mesa - Serra da Mesa 2 transmission line

Distance (%)	**I_{OP}(A)**	**I_{RT}(A)**
25	**371,01**	**1330,86**
50	**693,42**	**1368,40**
75	**1026,16**	**1461,84**
99	**1337,81**	**1580,70**

In Figure 5.3, we observe that for Serra da Mesa – Samambaia, any faults along the line enter the relay's operating region.

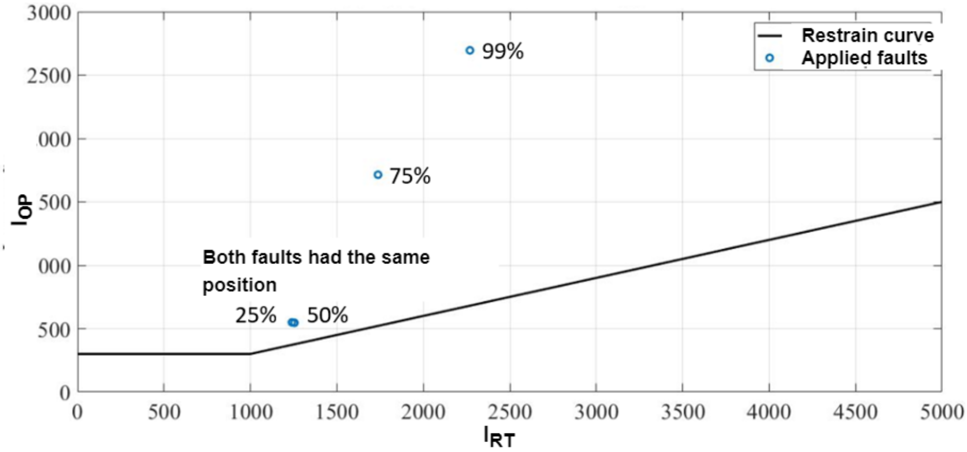


Figure 5.3: Simulation results - Serra da Mesa - Samambaia.

For the transmission line Serra da Mesa – Serra da Mesa 2 case, shown in Figure 5.4, only the 25% case was in a more critical situation, but it is worth mentioning that at the threshold adjustment, the relay is sensitized. Therefore, the protection presented satisfactory results for all simulated cases.

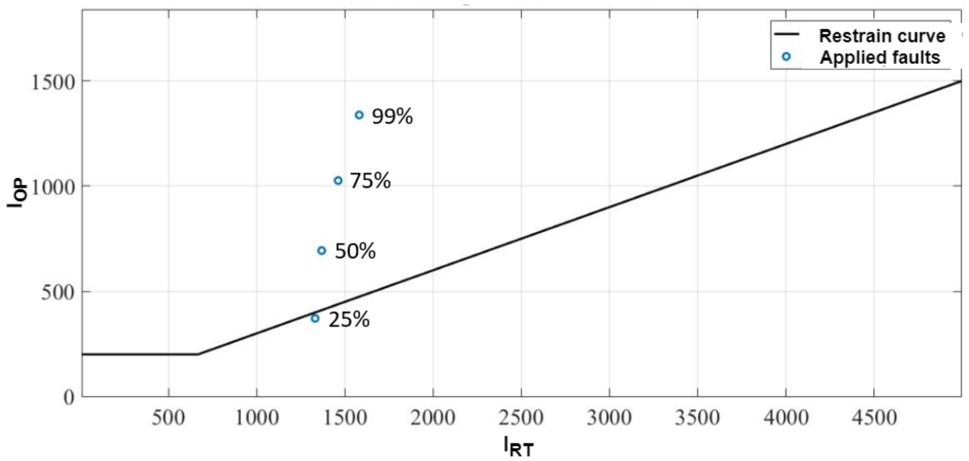


Figure 5.4: Simulation results Serra da Mesa – Serra da Mesa 2.

Although we usually see the short transmission lines as more suited to line differential protection schemes, we observed that the short transmission line performed worse for the 25% case. It occurs because it is a short line, and 25% represents a small fault distance to the "Serra da Mesa" terminal, which has a more potent energy source and contributes more to the short circuit. Also, in the long transmission line, the behavior of the short-circuit current value varies more because of the bigger distances between the fault locations.

5.2 Network performance tests**

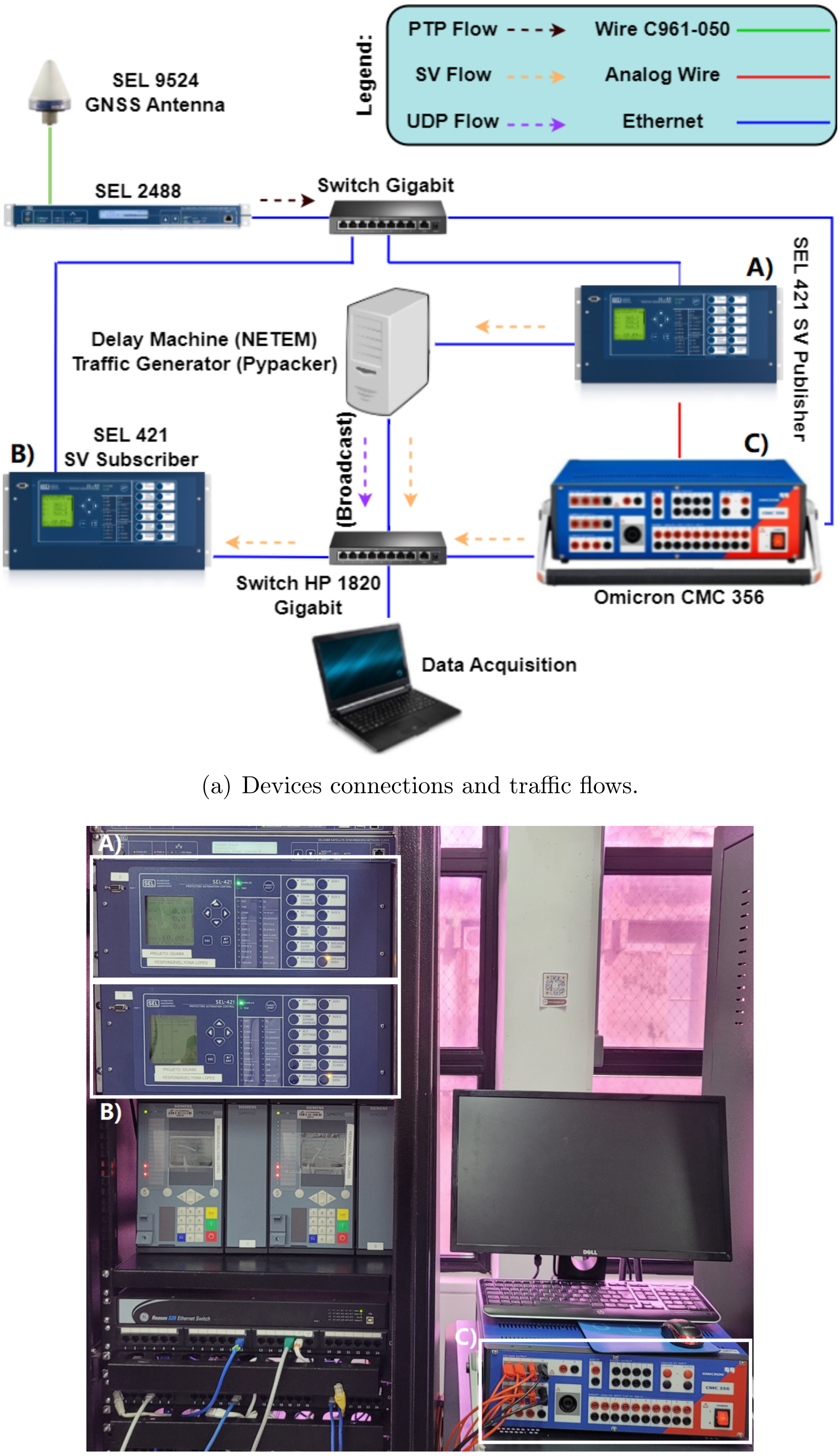
The protection system operation with the SV messages over an Ethernet network makes it susceptible to the traditional digital packet network problems, which are: delay, packet loss, and bandwidth [36].

As exposed in Section 2.6 delay expresses the total time that a message sent by an IED takes to reach the destination, with a strong component of the distance between those. Packet loss gives a percent quantification of the number of messages that weren't delivered to the destination, causing a loss of information. Finally, bandwidth informs the total amount of information transmitted over a communication link that has a physical limit, which after being reached affects directly the other two metrics.

To reproduce the differential protection system behaviour in our testbed, we created the scenario described in Figure 5.5. We use two SEL IEDs through a single star topology, each IED representing a distinct substation. Omicron CMC 356 [52] implemented the local metering. This device is a commissioning relay test solution able to generate up to six current and/or voltage sources, and can work like a MUs publishing SV streams from the generated sources on the communication network. CMC 356 collects the trip time, by registering the beginning of the fault applied by the relay test set and the receipt of a GOOSE trip message issued by the subscriber IED after the fault detection. We run trip events tests with thirty rounds for each network configuration and average results are presented with 95% confidence interval.

To survey the impact of each metric in line differential protection system, we implement a testbed. Table 5.4 shows the test parameters, in which delay tests are defined in terms of distance. We adopt this methodology to determine the distance threshold for differential protection using our scheme. We established the test limits based on hardware limitations and empirical and theoretical analysis. The max line length of 300 km is due to the lack of long lines modeling evaluation in Section 5.1. We would need to update the fault modeling to fully simulate the long transmission lines' behavior. The 200 Mpbs additional traffic is a hardware limitation of the testbed. We did not have other hardware to inject more concurrent traffic. The packet loss threshold is an empirical analysis of the results we were obtaining, so we established the limitation accordingly with the packet loss value that made the scheme unfeasible.

**The results obtained are in submission at the Electric Power System Research journal."The use of Sampled Values in Line Differential Protection" Ayello. M, Fulli. N, Fernandes. N and Lopes. Y



(a) Devices connections and traffic flows.

(b) Physical arrangement main components.

Figure 5.5: Testbed topology devices.

Table 5.4: Methods and range of evaluation for the testing of each metric.

Test Goal	Method	Distance (km)	Additional Traffic (Mbps)	Packet Loss (%)
Evaluate the effect of distance in the differential protection	Emulate on the relay publisher's transmission link a network delay proportional to the propagation delay of the distance	0, 50, 100, 150, 200, 250, 300	0	0
Evaluate the effect of concurrent traffic in the differential protection	Insert in the lab-mounted protection network a UDP traffic concurrent with the SV message flow	0	5, 10, 15, 20, 50, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 100 ,125 , 200	0
Evaluate the effect of packet loss in the differential protection	Emulate on the relay publisher's transmission link a percentage loss of the packets sent	0	0	1, 3, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50

Since it does not exist a line differential protection relay that uses SV messages to send current measurements to the other terminal, we designed a similar mechanism for the network test using a phase-instantaneous overcurrent function. As seen in Figure 5.6, the relay operates with a breaker-and-a-half arrangement, in which its line current equals the sum of both of the CT currents. The injected fault will only sensitize the overcurrent function if both data streams are received by the IED. If any of the imposed network critical scenarios compromise the remote data stream, the function will not properly operate. The "SEL 421 Subscriber" was configured accordingly with the described mechanism.

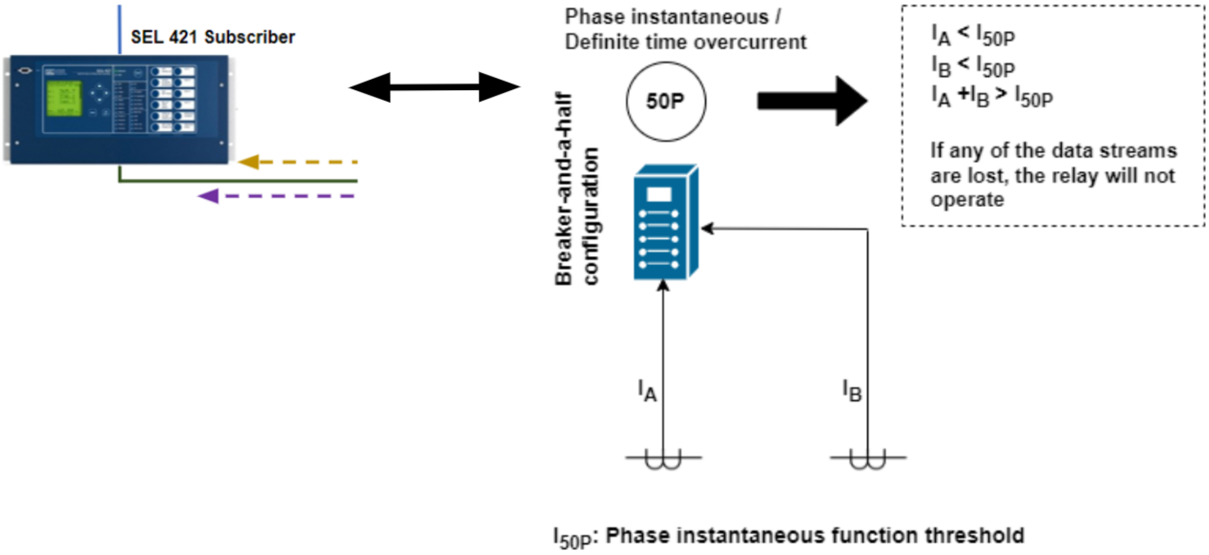

SEL 421 Subscriber
Phase instantaneous / Definite time overcurrent
50P
Breaker-and-a-half configuration
$I_A < I_{50P}$
$I_B < I_{50P}$
$I_A + I_B > I_{50P}$
If any of the data streams are lost, the relay will not operate
I_A
I_B
I_{50P}: Phase instantaneous function threshold

Figure 5.6: Breaker-and-a-half configuration with phase instantaneous function.

As can be seen in Figure 5.5, to emulate the distance between the two IEDs, a desktop computer with a network bridge interface was inserted between the publisher IED and the network switch, where the Linux software NETEM [53] was responsible for the delay and packet loss injection.

For the UDP broadcast generation, we use the Pypacker [54], a python library for multi-layer packet creation and manipulation. We use Wireshark wrapper for Python, called Pyshark [55], as the network sniffer, used for packet capture and loss estimation.

NETEM also generated the packet loss effects, which were configured with a 25% correlation in the probability of loss of a packet against the loss of the previous packet. This method has been used such that the losses had a characteristic closer to the real network scenario.

SVs messages were configured without priority over competing UDP messages. Besides, all message flow and performance metrics were collected by a data acquisition notebook, with a network interface capacity equivalent to that of the IEDs, of 100 Mbps.

We divided the tests into two methodologies. Section 5.2.1 will assess the influence of network stress on the trip time of the IED. Section 5.2.2 will evaluate the impact of packet loss and additional traffic at the SV message delay.

5.2.1 Network stress scenarios impact on trip time

The Omicron CMC 356 will inject fault currents through the analog wire at the SEL 421 Publisher, which will publish those values by the SV protocol to the SEL 421 Subscriber, and the CMC 356 will also publish those fault currents through to the SEL 421 Subscriber. In this case, the SEL 421 Publisher is the remote line terminal, and the Omicron CMC 356 is the local line terminal.

We semi-automated the procedure to perform thirty test rounds in each network configuration and ensure the 95% confidence interval. In Figure 5.7, we can see the automation schematic.

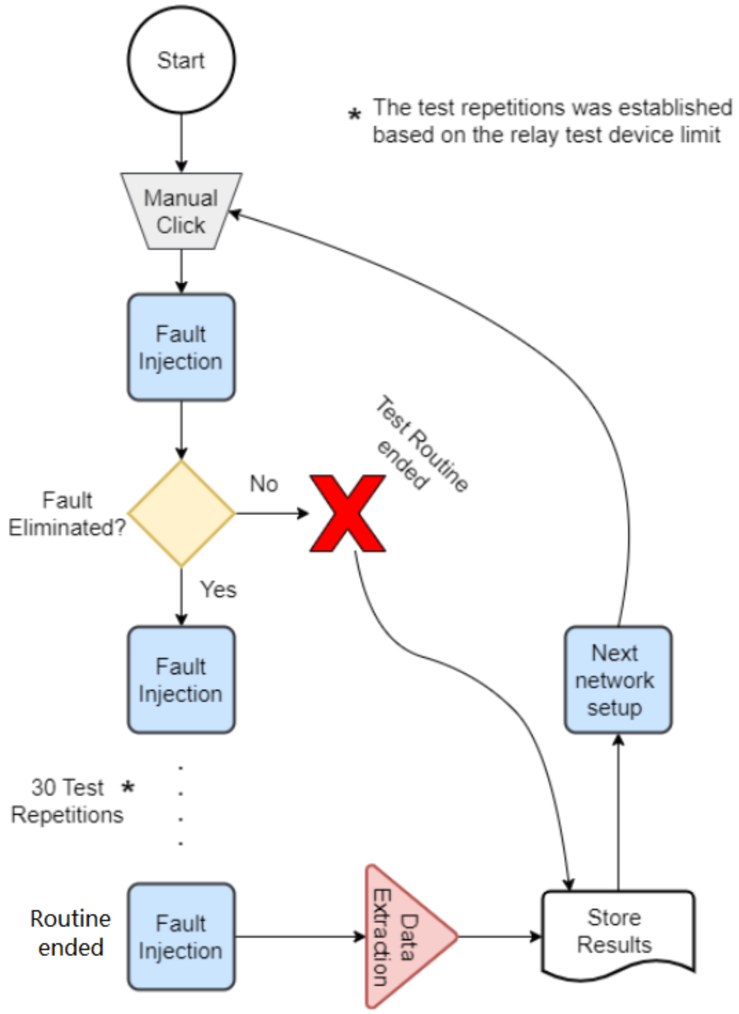
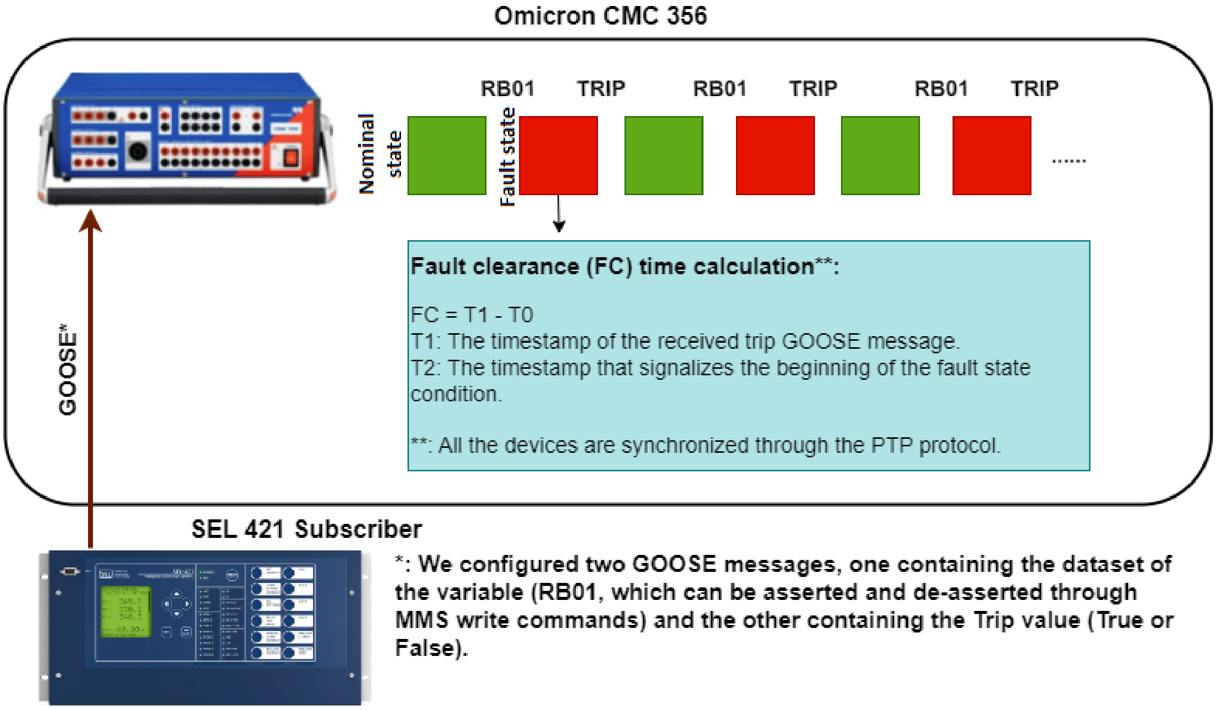


Figure 5.7: Semi-automated test routine for fault clearance time evaluation.

The Omicron CMC 356 has a software module “State Sequencer” that we configure current and voltage values states and inject from the analog wire connection and the SV messages. We configured a nominal state and a fault state in the module and replicated this combination thirty times in a row, and we navigated through those states using a GOOSE messages. Asserting the GOOSE containing the dataset with the RB01 - Remote Bit 1 - to true starts the fault state condition, and Asserting the GOOSE containing the dataset with the Trip value to true ends the fault state condition. Figure 5.8 illustrates the method.



Fault clearance (FC) time calculation**:

FC = T1 - T0
T1: The timestamp of the received trip GOOSE message.
T2: The timestamp that signalizes the beginning of the fault state condition.

**: All the devices are synchronized through the PTP protocol.

*: We configured two GOOSE messages, one containing the dataset of the variable (RB01, which can be asserted and de-asserted through MMS write commands) and the other containing the Trip value (True or False).

Figure 5.8: Navigation through the states with GOOSE messages.

We configured a set of network stress conditions through NETEM or Pypacker. The navigation along the stress conditions is done by a Python code. We developed the semi-automation procedure in Python, and we divided it into the following steps:

1. Manual click to start the fault injection from the CMC 356, and the nominal state starts;
2. The program flips the RB01 variable from false to true, and the fault state is asserted;
3. The SEL 421 Subscriber clears the fault, and the trip finishes the fault state condition;
4. This process of flipping the RB01 variable to navigate through the thirty established repetitions;
5. We store the time calculation of the trip timestamp minus the fault state initiation timestamps of each round in a file for further processing;
6. The code configures the next network stress scenario;
7. The code keeps repeating the routine until we have all our desired network conditions.

Sections 5.2.1.1 to 5.2.1.3 show the results for each evaluated metric.

5.2.1.1 Delay tests

During the transmission delay test, the delay machine was configured to gradually increase the delay of the publisher IED link, in order to simulate the path delay generated by the length of a network link in an actual environment.

Figure 5.9 show the distance increment generates an almost linear behavior in the network delay, as expected. This validates the methodology to simulate the distance in our testbed.

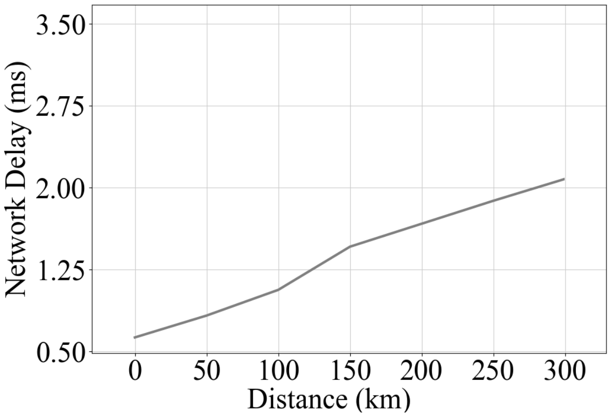


Figure 5.9: Network delay measurements converted to line lengths.

The result of the trip time test under these conditions is shown in the graph in Figure 5.10, where we see that the 87-L protection did not have its performance affected by the increase of the distance since it was under a link length of less than approximately 300 km. Another interesting aspect that can be noticed from the generated graph is that the trip time does not increase proportionally to the distance, as would be expected. This behavior is justified by the processing time of the IEDs, which for SEL devices is approximately 4 ms. Because this interval is greater than the delay values generated by a distance of 300 km, the trip time was not affected.

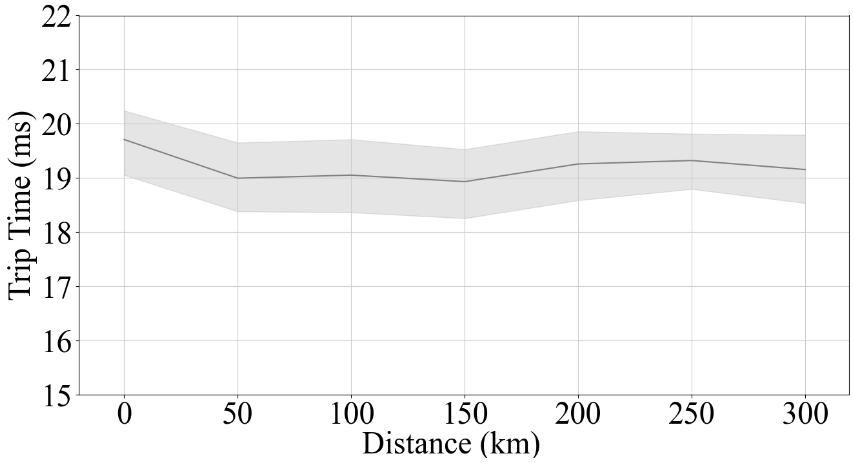


Figure 5.10: Trip time measurements according to the distance increase, where the shaded area represents a 95% confidence interval.

5.2.1.2 Concurrent traffic tests

In this test, the traffic generator machine of Figure 5.5 inserts a concurrent traffic into the network by assembling UDP packets with Pypacker, configuring their destination addresses as broadcast. Since the packets are relayed over all the hosts, the network is flooded with these packets. The size of the additional load is controlled by changing the size of the packet payload. The operational conditions of the network were measured, obtaining a load of 4.6 Mbps per SV flow, generating a total of 9.2 Mbps due to the two flows in the architecture.

Figure 5.11 shows the result of the trip time test under these conditions, showing an absence of influence of the additional traffic on the protection actuation time.

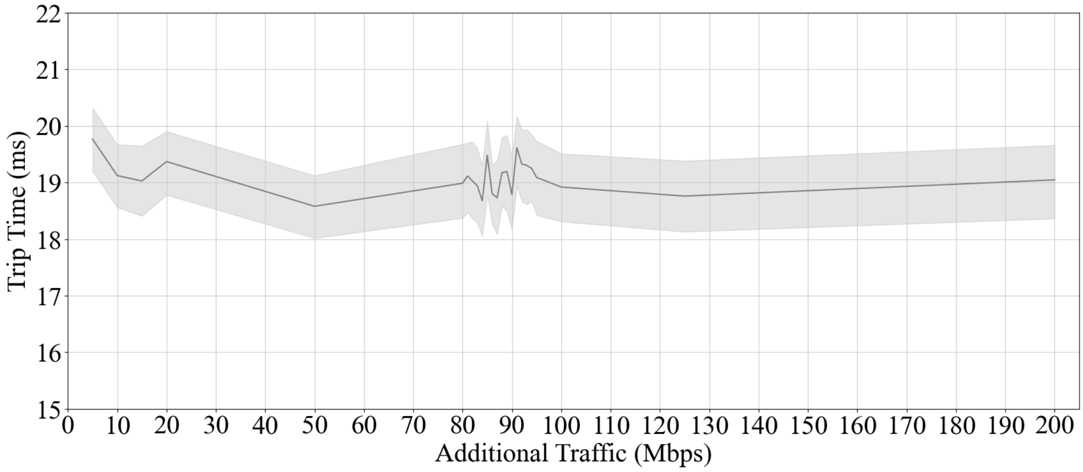


Figure 5.11: Trip time measurements according to the additional traffic increase, where the shaded area represents a 95% confidence interval.

It is worth noting that the threshold of 200 Mbps is due to the hardware limit. We could not inject more than 200 Mbps, and we expect in future works to increase this injection and evaluate the performance.

5.2.1.3 Packet loss tests

The last test performed was packet loss, implemented by changing the SV flow of the publisher by the NETEM software on the delay machine. The flow was changed to simulate a burst traffic, assigning a correlation of 25% to the probability of consecutive packet loss. The burst behavior is closer to that of real communication networks.

Relating the obtained statuses with the trip time results exposed in Figure 5.12, no influence of packet loss on the protection activation time was detected until a value of 50% was reached, after which there was a jump caused by the delay in receiving sample messages due to network losses. Table 5.5 shows the statistical breakdown of the trip times obtained in the test, and it is possible to verify the magnitude of the values acquired. Except for the loss of 50% remained similar in all other tests.

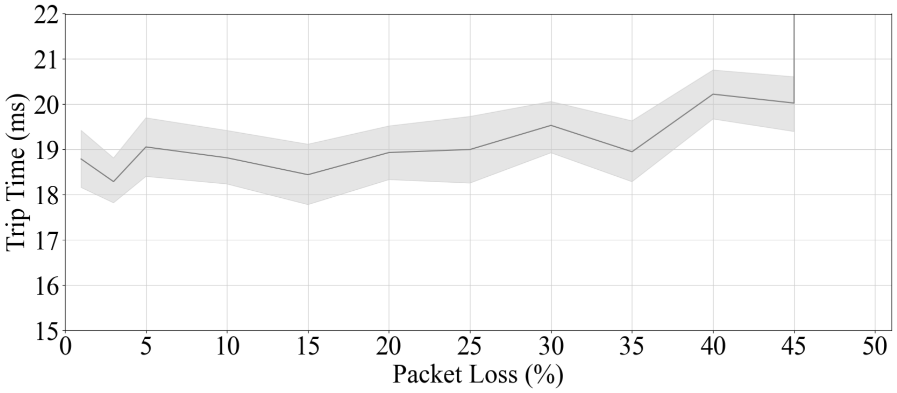


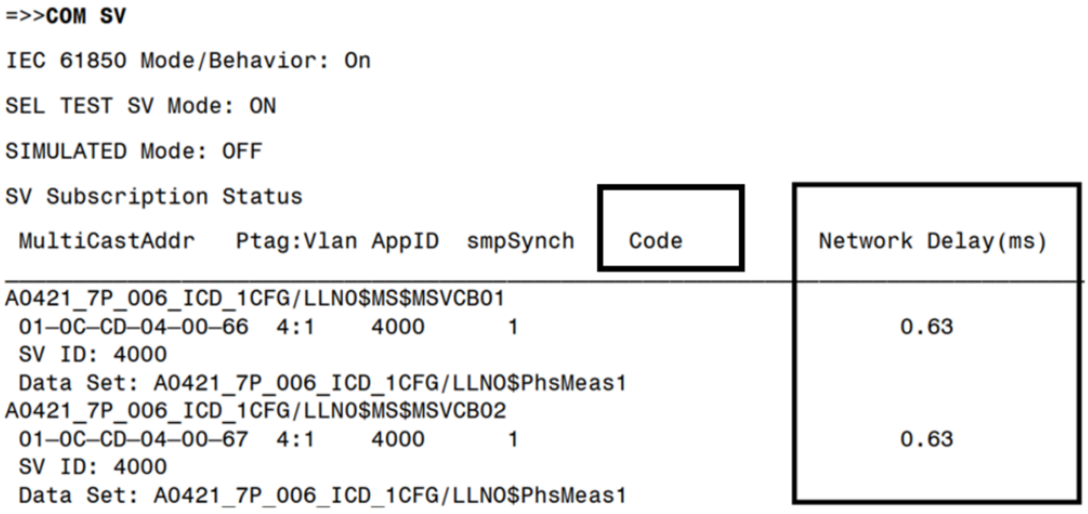
Figure 5.12: Trip time measurements according to the percentual loss increase, where the shaded area represents a 95% confidence interval.

Table 5.5: Statistical information of the acquired trip time by applied percentage loss.

Loss (%)	Mean (ms)	Std. (ms)	Min. (ms)	Max. (ms)
1	18.79	1.79	16.4	21.1
3	18.29	1.44	16.4	20.9
5	19.06	1.89	16.3	21.2
10	18.82	1.80	16.5	21.2
15	18.44	1.88	16.5	21.1
20	18.93	1.76	16.5	21.2
25	19.00	2.02	16.5	23.1
30	19.53	1.60	16.4	21.2
35	18.95	1.86	16.5	23.1
40	20.22	1.58	16.5	23.0
45	20.03	1.69	16.6	23.1
50	4983.97	7146.50	16.5	26110.0

5.2.2 Network stress scenarios impact on SV messages delay

To continue testing the impact of stress scenarios at the SV performance, we evaluate the influence of the scenarios at the SV message delays. The ***COM SV*** command at SEL IEDs command terminal returns a series of status information for the SV flow in the communication channel. Figure 5.13 shows the information display, and the highlights expose the diagnostic codes and the SV message delay.



```
=>>COM SV
IEC 61850 Mode/Behavior: On
SEL TEST SV Mode: ON
SIMULATED Mode: OFF
SV Subscription Status
 MultiCastAddr   Ptag:Vlan AppID  smpSynch    Code        Network Delay(ms)
--------------------------------------------------------------------------------
A0421_7P_006_ICD_1CFG/LLN0$MS$MSVCB01
 01-0C-CD-04-00-66  4:1    4000      1                          0.63
 SV ID: 4000
 Data Set: A0421_7P_006_ICD_1CFG/LLN0$PhsMeas1
A0421_7P_006_ICD_1CFG/LLN0$MS$MSVCB02
 01-0C-CD-04-00-67  4:1    4000      1                          0.63
 SV ID: 4000
 Data Set: A0421_7P_006_ICD_1CFG/LLN0$PhsMeas1
```

Figure 5.13: COM SV command return at SEL 421 Subscriber terminal.

The message delays are exposed in milliseconds, and the code field can have multiple responses. The following ones appear in this work:

- **OK:** When nothing appears in the code field, the SV messages are functioning without errors;
- **INTERPOLATED:** Displayed after the loss of 1-3 consecutive SV messages when the SEL SV subscriber relay starts to interpolate the lost SV message;
- **SV STREAM LOST:** Displayed after the SEL SV subscriber relay has not received four or more consecutive SV messages.

To automatize the procedure, we developed a Python code to establish the network conditions automatically and then carry out the ***COM SV*** command 1000 times in each scenario and store the result for further processing to evaluate each result. Figure 5.14 exposes the methodology in a schematic procedure.

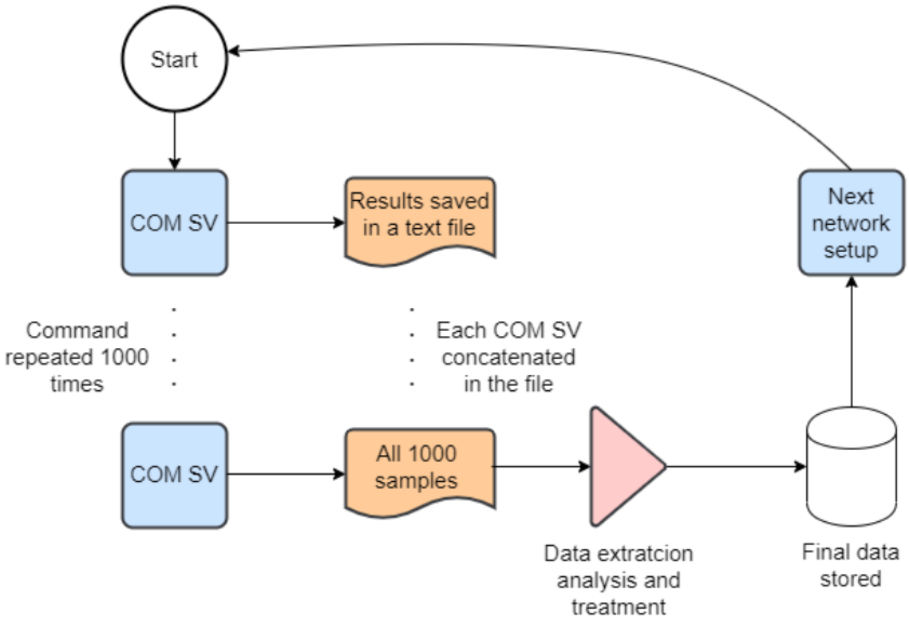

Start
COM SV
Results saved in a text file
Next network setup
Command repeated 1000 times
Each COM SV concatenated in the file
COM SV
All 1000 samples
Data extratcion analysis and treatment
Final data stored

Figure 5.14: Automated routine for COM SV command processing and data storage.

5.2.2.1 Concurrent traffic tests

Figure 5.15 demonstrates the effects of additional traffic on the average delay of the communication network for the SV messages, in which it is possible to verify an influence starting at 87 Mbps of additional traffic. This UDP traffic added to the operational traffic configures a total flow of approximately 96.2 Mbps on the network interfaces. It is also worth noting that the delay values obtained for the concurrent traffic tests at 86 and 89 Mbps were not included in the graph. These tests generated highly disparate delay values and were not included in the analysis of the results.

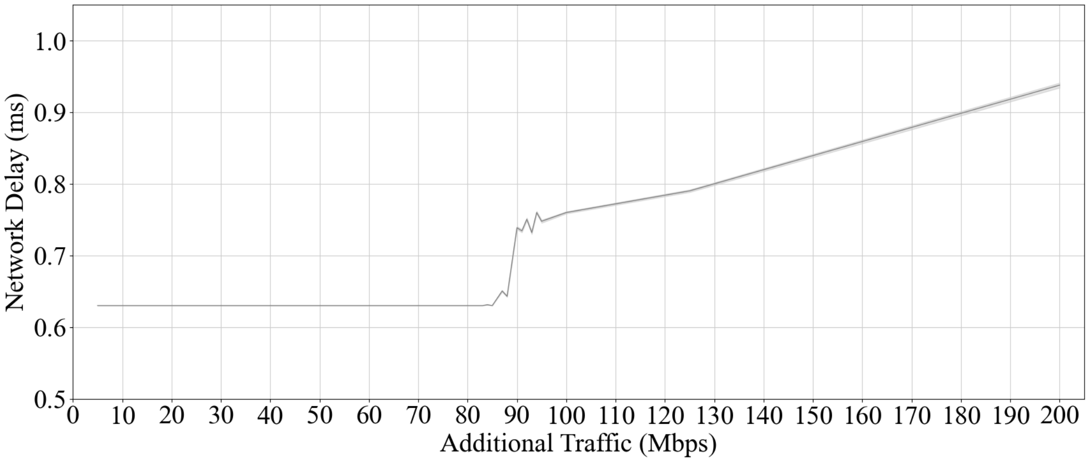


Figure 5.15: Network delay measurements according to the additional traffic increase, where the shaded area represents a 95% confidence interval.

The increase in network time evidenced from this value of total traffic is justified by the beginning of queue formation on the network interfaces of the hosts. Although the interfaces have a capacity of 100 Mbps the formation of queues starts below this value because the Ethernet standard defines a transmission interval between the frames, called Inter Frame Gap (IFG) [56]. This difference at the Fast Ethernet rate of 100 Mbps is equivalent to the transmission time of 20 bytes, which results in a maximum interface efficiency of 98.695 Mbps. Although the influence of delay has been identified at values close to but before the maximum efficiency value, it is from this threshold that the impact of queue formation becomes more significant. The gradual increase in network delay from this point due to the increase in traffic is consistent with what is expected.

5.2.2.2 Packet loss tests

According to the graph in Figure 5.16, it is possible to verify that besides isolated peaks, there was no direct relationship between the increase in loss with the increase in additional traffic up to 200 Mpbs. The occurrence of peaks is justified by the magnitude of the identified loss, in which the loss of one additional packet has a significant scale relevance. Furthermore, the stability in the loss values with the addition of additional traffic can be justified by the storage capacity of the used switch.

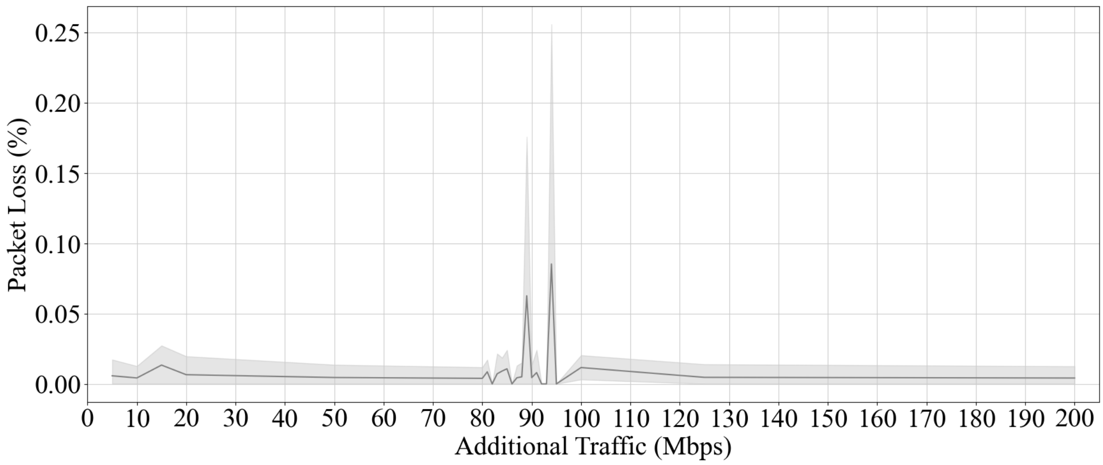


Figure 5.16: Packet loss measurements according to the additional traffic increase, where the shaded area represents a 95% confidence interval.

We also verified the ***COM SV*** command response to the packet loss scenarios. Figure 5.17 shows the results, in which changes in the status of the SV stream can be verified as its losses increase. Note that a small network loss causes some events of the status ***INTERPOLATED***, which indicates that up to three consecutive messages were lost and their values were interpolated by the equipment. With 20% we see the beginning of a new ***SV STREAM LOST*** status, which indicates that more than three consecutive messages have been lost.

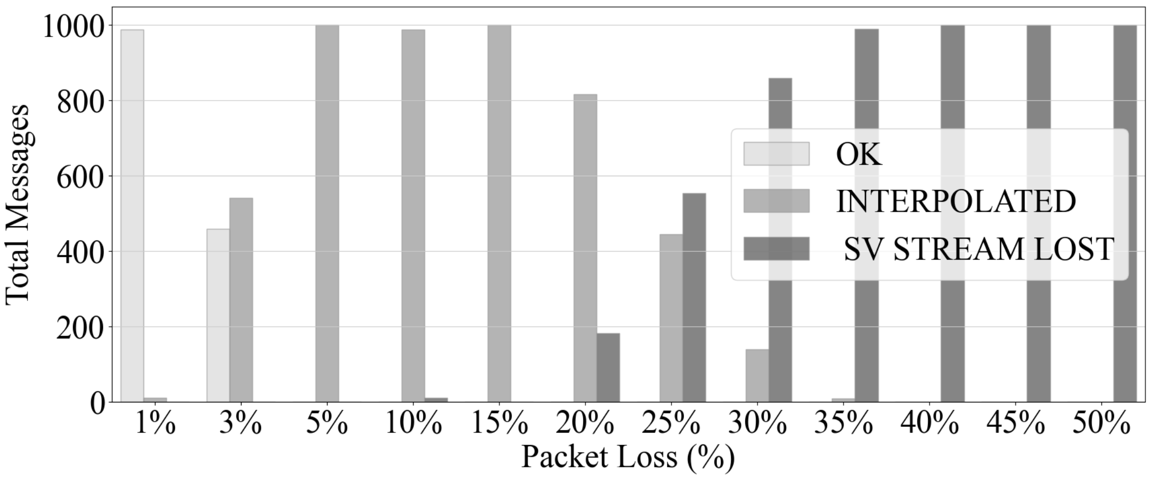


Figure 5.17: COM SV command's obtained channel status codes by percentual loss.

Chapter 6

Conclusion

The IEC 61850 standard brings new possibilities using standardized protocols, common information modeling, a well-defined data structure, and application performance requirements. Its use holds great value for power systems by reducing structural costs, bringing more efficiency, and allowing innovative ways of automatizing with the interoperability feature. The line differential protection scheme is fast and selective, and its use enhances transmission line protection. However, it has yet to adopt IEC 61850 standard on transmitting between the line ends. The traditional analog hardwired line differential protection had many limitations by being restricted to 120 km of line lengths, mutually synchronizing through the line length compensation, and relying on proprietary solutions that do not allow the reliability to increase through the communication network topology. With the digitalization of devices, the introduction of digital communication networks on power systems, and advances in microprocessor-based IED, some of those limitations have already been surpassed.

However, as shown in Chapter 4, the up-to-date schemes still have not achieved interoperability and rely on proprietary communication protocol to transfer the data between the line ends.

This work has proposed a new line differential protection scheme that uses SV messages to transfer the current measurements to the adjacent IED. The new approach is based on a standardized communication protocol that allows interoperability between different vendors and innovative ways to increase the reliability of the communication network through its topology. To evaluate the proposal, a percentage line differential protection scheme was done using the Aspen OneLiner software.

In the case study, the percentage line differential protection scheme was evaluated with a high-impedance short circuit, and although it is a challenging scenario for the protection function, the results indicate that the scheme is feasible for the two transmission lines. The parameterization of the function followed the recommended settings exposed in Chapter 2.

Also, the network test results indicate possible thresholds for the evaluated conditions. The message delay test, through the hardware emulating the line length, shows that the scheme will be feasible for up to 300 km transmission lines.

The background traffic test can help to assess the amount of traffic that can simultaneously be sent with the SV messages through the network without compromising the differential protection. This is a very important test since it can assess the amount of concurrent traffic that can be transmitted with the SV messages and represents an economic advantage since the remaining bandwidth can be sold to otter applications.

Finally, the packet loss scenario demonstrated a possible threshold for this metric in other to not compromise the scheme. With that result, we can evaluate the network metrics and establish an acceptable operational value for the communication network.

Using a non-point-to-point communication channel increases message reliability through the network topology without adding extra communication cards into the IEDs. This feature, combined with the interoperability between manufacturers and the effectiveness of line differential protection, makes the proposed solution a reliable option in digital substations.

6.1 Future works

For future work, it is intended to test further the proposal with new features, devices, and data analysis. The percentage line differential protection scheme can be evaluated more assertively, with IEDs that has the protection function and injecting the fault with the same Omicron CMC 356 device.

Alongside, our simple arrangement that simulated line differential protection on the SEL IEDs can be carried out in different vendors to make a performance comparison.

The same network tests will be carried out with other vendors to compare the network threshold levels, as well as evaluate the tests in a scenario with more robust switches, using features to increase the reliability of the messages such as Virtual Local Area Networks (VLANs), priority tagging, the physical segregation of process and station in the devices to enhance the PTP time synchronization.

More stable and potent traffic generation methods will also be implemented, along with a comparative analysis of packet loss of UDP traffic versus SV traffic. Also, devices specifically designed to simulate line lengths can be used to have more assertive results.

References

[1] BENMOUYAL, G. The trajectories of line current differential faults in the alpha plane. In: *proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA*. [S.l.: s.n.], 2005. p. 19.

[2] IEEE. Ieee guide for application of digital line current differential relays using digital communication. *IEEE Std C37.243-2015*, p. 1–72.

[3] HARGRAVE, A.; THOMPSON, M. J.; HEILMAN, B. Beyond the knee point: A practical guide to ct saturation. In: *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*. [S.l.: s.n.], 2018. p. 1–23.

[4] FIBER Optic Current Sensors Optical Current Transformers. `https://fibercore.humaneticsgroup.com/perspectives/fiber-optic-current-sensors-and-optical-current-transformers`. Accessed: 2023-05-23.

[5] SOARES, A. A. Z.; SOARES, L. F.; MATTOS, D. P.; PINHEIRO, P. H. B. S.; QUINCOZES, S. E.; FERREIRA, V. C.; APOSTOLO, G. H.; CARRARA, G. R.; MORAES, I. M.; ALBUQUERQUE, C.; LOPES, Y.; FERNANDES, N. C.; MUCHALUAT-SAADE, D. C. Enabling emulation and evaluation of iec 61850 networks with titan. *IEEE Access*, v. 9, p. 49788–49805, 2021. ISSN 2169-3536.

[6] International Electrotechnical Commission. *IEC 61850-7-4 Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*. [S.l.: s.n.], 2010.

[7] INGRAM, D. M.; SCHAUB, P.; TAYLOR, R. R.; CAMPBELL, D. A. Performance analysis of iec 61850 sampled value process bus networks. *IEEE Transactions on Industrial Informatics*, v. 9, p. 1445–1454, 2013. ISSN 15513203.

[8] WATT, S. T.; ACHANTA, S.; ABUBAKARI, H.; SAGEN, E.; KORKMAZ, Z.; AHMED, H. Understanding and applying precision time protocol. In: *2015 Saudi Arabia Smart Grid (SASG)*. [S.l.: s.n.], 2015. p. 1–7.

[9] LOPES, Y. *"SMARTFlow: Sitema Autoconfigur´avel para Redes de Telecomunica¸c˜oes IEC 61850 com arcabou¸co OpenFlow*. [S.l.: s.n.], 2013.

[10] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 90-12: Wide area network engineering guidelines*. [S.l.: s.n.], 2020.

[11] LIU, Y.; GAO, H.; GAO, W.; LI, N.; XIANG, M. A design scheme of line current differential protection based on iec61850. v. 2, p. 520–523, 2011.

[12] AYELLO, M.; LOPES, Y. Interoperability based on iec 61850 standard: Systematic literature review, certification method proposal, and case study. *Electric Power Systems Research*, v. 220, p. 109355, 2023. ISSN 0378-7796.

[13] ZIEGLER, G. *Numerical differential protection: principles and applications*. 4. ed. [S.l.]: John Wiley & Sons, 2012.

[14] SHARMA, M.; RUDOLPH, T. *A Rule Driven Architecture to Address Interoperability in an IEC 61850 Series Based Power Utility Automation System*. [S.l.]: Springer Singapore, 2018. 93–101 p. ISBN 9789811082498.

[15] ABB. *615 series ANSI Technical Manual*. [S.l.], 2019.

[16] SIEMENS. *SIPROTEC 5 Distanc Protection, Line Differential Protection, and Breaker Management for 1-Pole and 3-Pole Tripping 7SA87, 7SD87, 7SL87, 7VK87*. [S.l.], 2022.

[17] RED670, M. A. *Line differential protection RED670 Version 2.2 ANSI Technical manual*. [S.l.], 2017.

[18] SARWAR, M.; MEHMOOD, F.; ABID, M.; KHAN, A. Q.; GUL, S. T.; KHAN, A. S. High impedance fault detection and isolation in power distribution networks using support vector machines. *Journal of King Saud University - Engineering Sciences*, v. 32, n. 8, p. 524–535, 2020. ISSN 1018-3639.

[19] International Electrotechnical Commission. *Communication Networks And Systems For Power Utility Automation - Part 1: Introduction And Overview*. 2. ed. [S.l.: s.n.], 2013.

[20] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 2: Glossary*. [S.l.: s.n.], 2019.

[21] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 3: General requirements*. [S.l.: s.n.], 2013.

[22] International Electrotechnical Commission. *IEC 61850-4 Communication networks and systems for power utility automation – Part 4: System and project management*. [S.l.: s.n.], 2011.

[23] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models*. [S.l.: s.n.], 2013.

[24] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs*. [S.l.: s.n.], 2009.

[25] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3*. [S.l.: s.n.], 2011.

[26] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations.* [S.l.: s.n.], 2010.

[27] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 90-2: Using IEC 61850 for communication between substations and control centres.* [S.l.: s.n.], 2016.

[28] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 90-3: Using IEC 61850 for condition monitoring diagnosis and analysis.* [S.l.: s.n.], 2016.

[29] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines.* [S.l.: s.n.], 2020.

[30] International Electrotechnical Commission. *IEC 61850-7-3 Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes.* [S.l.: s.n.], 2010.

[31] International Electrotechnical Commission. *Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.* [S.l.: s.n.], 2011.

[32] International Organization for Standardization. *ISO 9506-2 Industrial automation systems — Manufacturing Message Specification — Part 2: Protocol specification.* [S.l.: s.n.], 2003.

[33] GROUP, U. I. U. *Implementation Guideline for Digital Interfaces to Instrument Transforming Using IEC 61850-9-2.* [S.l.: s.n.], 2004.

[34] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, p. 1–269, 2008.

[35] INGRAM, D. M.; SCHAUB, P.; CAMPBELL, D. A.; TAYLOR, R. R. Performance analysis of ptp components for iec 61850 process bus applications. *IEEE Transactions on Instrumentation and Measurement*, v. 62, p. 710–719, 2013. ISSN 00189456.

[36] KUROSE, K. W. R. J. F. *Computer Nertworking: A TopDown Approach.* 7. ed. [S.l.]: Pearson Education Limited, 2009. 26-34 p.

[37] GAO, H.; HE, J.; JIANG, S. Gps synchronized digital current differential protection for transmission lines. *Electric Power Systems Research*, v. 62, n. 1, p. 29–36, 2002. ISSN 0378-7796.

[38] APOSTOLOV, A. Iec 61850 based bus protection — principles and benefits. p. 1–6, 2009.

[39] INGRAM, D. M. E.; SCHAUB, P.; TAYLOR, R. R.; CAMPBELL, D. A. System-level tests of transformer differential protection using an iec 61850 process bus. *IEEE Transactions on Power Delivery*, v. 29, n. 3, p. 1382–1389, 2014.

[40] BLUMSCHEIN, J.; KERGER, T.; MATUSSEK, R. Interoperability of line differential protection. In: *2021 74th Conference for Protective Relay Engineers (CPRE)*. [S.l.: s.n.], 2021. p. 1–6.

[41] Pereira Jr, P. S.; BERNARDINO, R. C.; SALGE, G. S.; MARTINS, C. M.; PEREIRA, P. S.; LOURENçO, G. E. Performance assessment of a line protection implemented with process bus and goose through transient closed loop tests. *Electric Power Systems Research*, v. 197, p. 107221, 2021. ISSN 0378-7796.

[42] Silva Melo, A. F.; NETTO, U. C.; da Silva, J. C. C.; DREYER, U. J. Influence of process bus on performance of power system protection. *Electric Power Systems Research*, v. 200, p. 107491, 2021. ISSN 0378-7796.

[43] Cigré Joint Working Group 34/35.11. *Protection Using Telecommunications*. [S.l.], 2001. 1–173 p. Disponível em: <https://e-cigre.org/publication/192-protection-using-telecommunications>.

[44] BäCHLI, R.; HäUSLER, M.; KRANICH, M. Teleprotection solutions with guaranteed performance using packet switched wide area communication networks. p. 1–6, 2017.

[45] An, W.; Tart, N.; Barron, D.; Bingham, M.; Hackett, A. A transmission utility's experience to date with feeder unit protection systems. In: *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*. [S.l.: s.n.], 2012. p. 1–6. ISSN null.

[46] ALI, I.; HUSSAIN, S. M. S.; TAK, A.; USTUN, T. S. Communication modeling for differential protection in iec-61850-based substations. *IEEE Transactions on Industry Applications*, v. 54, n. 1, p. 135–142, 2018.

[47] OLIVEIRA, W.; LOPES, Y. Teleprotection over sonet based on iec 61850. In: . [S.l.]: IEEE, 2018. p. 1–6. ISBN 978-1-5386-3363-2.

[48] dos Santos, A.; Correia de Barros, M.; CORREIA, P. Transmission line protection systems with aided communication channels—part i: Performance analysis methodology. *Electric Power Systems Research*, v. 127, p. 332–338, 2015. ISSN 0378-7796.

[49] dos Santos, A.; BARROS, M. C. de; CORREIA, P. Transmission line protection systems with aided communication channels—part ii: Comparative performance analysis. *Electric Power Systems Research*, v. 127, p. 339–346, 2015. ISSN 0378-7796.

[50] ZHENG, J.; WEN, M.; CHEN, Y.; SHAO, X. A novel differential protection scheme for hvdc transmission lines. *International Journal of Electrical Power Energy Systems*, v. 94, p. 171–178, 2018.

[51] ESHPETER, A.; ENG, P. Resolving the Challenges of Multiple Vendor 61850 Implementations. 2016.

[52] L3194, O. *CMC 356: The Universal Relay Test Set and Commissioning Tool*. 2021. Brochure.

[53] LINUX. *The Linux Foundation Wiki - NETEM*. 2010. Disponível em: <https://wiki.linuxfoundation.org/networking/netem>.

[54] STAHN, M. *Pypacker: The fastest and simplest low-level packet manipulation library for Python.* 12 2022.

[55] GREEN, K. D. *Pyshark: Python wrapper for tshark, allowing python packet parsing using wireshark dissectors.* 7 2022. Disponível em: <https://github.com/KimiNewt/pyshark>.

[56] SOCIETY, I. C. IEEE Standards for Local and Metropolitan Area Networks: Supplement – Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100Mb/s Operation, Type 100BASE-T (Clauses 21-30). *ANSI/IEEE Std 802.3-1985*, 1995.