Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

Kristoffer Ballantine Øverby

Addressing Reliability Challenges in Digital Substation Automation Systems

A Comparative Analysis of Digital versus Conventional Substations and an Examination of the IEC 61850 Redundancy Protocols

Master's thesis in Electric Power Engineering
Supervisor: Hans Kristian Høidalen
Co-supervisor: Rizwan Rafique Syed

June 2023

NTNU
Norwegian University of
Science and Technology

Kristoffer Ballantine Øverby

Addressing Reliability Challenges in Digital Substation Automation Systems

A Comparative Analysis of Digital versus Conventional Substations and an Examination of the IEC 61850 Redundancy Protocols

Master's thesis in Electric Power Engineering
Supervisor: Hans Kristian Høidalen
Co-supervisor: Rizwan Rafique Syed
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

NTNU
Norwegian University of
Science and Technology

Kristoffer Ballantine Øverby

Addressing Reliability Challenges in Digital Substation Automation Systems

A Comparative Analysis of Digital versus Conventional Substations and an Examination of the IEC 61850 Redundancy Protocols

Master's thesis in Energy and Environmental Engineering
Supervisor: Hans Kristian Høidalen
Co-supervisor: Rizwan Rafique Syed
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

NTNU

Abstract

This master's thesis investigates the reliability of digital substations utilizing the IEC 61850 process bus. The digital substation, characterized by enhanced interoperability and real-time performance, relies heavily on this process bus for effective communication and information exchange within the system. However, the transition from conventional to digital substations raises concerns about the reliability of power systems. This study investigates the reliability attributes of digital compared to a conventional substation along with an analysis of how different process bus architectures impact the system's reliability, with an examination of the High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) protocols. The study employs reliability block diagrams to conduct this reliability analysis and to also evaluate maintenance times, and resilience of non-repairable versus repairable systems. The research also identifies and analyzes potential failure modes in digital substations.

Findings from the study indicate that the reliability of a conventional substation surpasses that of a digital one due to fewer points of failure. Yet, the research reveals potential enhancement of the digital system's reliability where it was found that the incorporation of duplicate components, star Ethernet topology, and the PRP protocol is a good option. The failure modes analysis revealed that the Ethernet communication network introduced with the process bus is the greatest vulnerability in the digital substation. Although, an efficient network topology integrated with robust redundancy protocols could improve reliability. This study, therefore, suggests that a combination of PRP protocol with a star Ethernet topology could be a promising solution for enhancing the reliability of digital substations.

Preface

This thesis is an important milestone in my life, signifying the completion of my Master's degree. The experiences and knowledge gained during this process have been rewarding and will undoubtedly serve me well in my future endeavors. Without the support, patience, and guidance of the following people, this study would not have been possible.

I would like to express my deepest gratitude to my supervisor, Professor Hans Kristian Høidalen. His expertise and insightful advice have been invaluable. Professor Høidalen's critical questions during our discussions have greatly enriched this work. I am particularly grateful for the trust he has given me throughout this process. His approach of providing me the space to independently explore this research, without excessive interference, gave me the opportunity to use the working process I wanted to complete this thesis.

I am also immensely grateful to my co-supervisor, Rizwan Rafique Syed, for his patience and invaluable advice. His insightful comments have been of great assistance in shaping this research. The quality of this thesis would have been significantly diminished without his help.

To all those who have been part of this, I hope this work reflects your positive impact. To the reader, I hope this study provides valuable insights into the reliability of digital substations and the IEC 61850 process bus.

Table of Contents

List of Figures

List of Tables

Glossary

CB Circuit Breaker.

CBM Condition-Based Maintenance.

CT Current Transformer.

DSAS Digital Substation Automation System.

ES Ethernet Switch.

HSR High-availability Seamless Redundancy.

LAN Local Area Network.

MTTF Mean Time To Failure.

MTTR Mean Time To Repair.

MU Merging Unit.

NCIT Non-Conventional Instrument Transformer.

PRP Parallel Redundancy Protocol.

RBD Reliability Block Diagram.

RSTP Rapid Spanning Tree Protocol.

SAMU Stand-Alone Merging Unit.

SAS Substation Automation System.

SV Sampled Values.

VLAN Virtual Local Area Network.

VT Voltage Transformer.

1 INTRODUCTION

The rapid evolution of technology has significantly influenced the power sector, leading to the development of new technologies that further enhance interoperability and real-time performance. With these new technologies, there is an increased emphasis on communication and information exchange within the power systems. One technology that stands out in this realm is the digital substation and its use of the IEC 61850 process bus.

The IEC 61850 process bus presents a new approach to substation communication, altering the components, monitoring, control, and protection systems employed in substations [1]. Along with these alterations comes a set of challenges as the process bus needs to be able to handle large amounts of data quickly, work in real-time, be reliable and available, and be cost-effective. It can be difficult to achieve all of these goals at the same time because they sometimes conflict with each other [2]. The implementation of new components and given the process bus's key role in substation systems raises questions regarding the impact of this standard on the reliability of power systems.

1.1 Assignment

This thesis aims to investigate these reliability uncertainties by addressing the following assignments:

- Develop reliability models for digital substations and compare this with the conventional substation. Will a digital substation result in reduced or increased reliability? And how will this depend on the reliability of the individual components involved?
- Reliability analysis and evaluation of different communication infrastructures and IEDs with different architectures of process bus.
- Identification of the failure modes in a digital substation.

1.2 Scope

This project explores the reliability of digital substations in comparison with conventional substations, focusing on the importance of process bus architecture and other related elements. It acknowledges that conducting a reliability analysis of a digital substation reflecting real-world conditions would be extremely complex due to the intricate interactions of various elements within the substation. Instead, this study aims to identify reliability tendencies that may reflect real-world scenarios. The scope of the research covers several aspects as detailed below:

To address the assignment of performing a reliability analysis and evaluation of different communication infrastructures and process bus architectures the following method will be employed:

The research will examine the dynamic interaction between High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) protocols in the context of different process bus architectures. The influence of these protocols on the reliability of the process bus is a central consideration.

Given the distinct architectural designs of the PRP and HSR systems — with PRP systems designed around a star topology and HSR systems based on a ring architecture — a comparative analysis will be performed. The goal is to understand how these different topologies and their corresponding protocols impact the reliability of the process bus.

In order to answer the assignment: Does a digital substation result in reduced or increased reliability compared to a conventional substation? Two distinct substation designs will be developed: one employing an IEC 61850 process bus to represent the digital substation, and another representing a conventional substation. These protection systems will be structured similarly to make the comparison of their reliability attributes straightforward. The two systems are compared by giving them the same protection coordination and then seeing which coordination system is the most reliable. By applying this method, the research aims to reveal distinctions in reliability between the two types of substations.

Additionally, this research also includes a comparative analysis of the maintenance times and the resilience of non-repairable versus repairable systems. By comparing maintenance times between digital and conventional substations, it may be possible to determine the effects of the new monitoring systems in the digital substation. Simultaneously, by incorporating an analysis of non-repairable and repairable systems, the study aims to provide a broader perspective on the reliability of digital substations under varied architectures.

Finally, identification and analysis of potential failure modes in digital substations will be undertaken to better understand the vulnerabilities of these systems. The research aims to compile a list of failure modes that may appear in digital substations. This list will be based on the literature review and will be revealed in the ”Reliability Theory” chapter. This is because it was felt that this was better from a structural point of view.

The research does not extend to other aspects of digital substation design or operation beyond those specified above. The focus remains on digital substation reliability.

2 BACKGROUND

2.1 Literature Review

This literature review is structured into two distinct sections, each focusing on a fundamental aspect of process bus functionality - reliability and failure modes. The division into two sections is required because of the different methodological approaches applied in the investigation. The first section delves into the reliability of the process bus, explaining the findings and methods applied in recently published papers on the subject. The second section delves into failure modes, investigating papers to identify the potential failure modes for a process bus.

2.1.1 Literature Review on Reliability In The IEC 61850 Process Bus

This review summarizes the key findings from several relevant studies and evaluates their methodologies with the goal of establishing the method for this research objective.

Many research papers, including [1], [2], [3],[4], [5], and [6], has examined the reliability of various process bus architectures. Notably, these studies have consistently used reliability block diagrams as a methodological approach, confirming the usefulness of this method.

The study by [3] is of particular relevance as it calculates the mean time to failure (MTTF) and availability of different process bus architectures, namely cascade, ring, and star, using reliability block diagrams. The star architecture was found to have the highest MTTF and availability, which suggests that the chosen architecture could significantly influence process bus reliability.

This notion is supported by [1], which evaluated the reliability of a digital substation considering different topologies. Utilizing reliability block diagrams combined with Monte Carlo simulation, the study found that the ring architecture process bus is a reliable and cost-effective topology. Furthermore, they proposed the use of parallel redundancy protocol (PRP) based architectures as a solution for meeting the reliability and performance requirements of substations.

Reliability evaluations have also considered component redundancy and communication. [4] proposed a redundant process bus architecture and found that the failure of any component, communication link, or even an entire protection system does not impact the reliability of the protection system.

Various studies have compared the reliability of different architectures. [5] used a reliability block diagram to examine the reliability of various Ethernet architectures for process buses. They found that the star-ring and redundant ring architectures provided higher reliability and availability compared to the cascaded and ring architectures.

These studies collectively highlight the importance of the architecture decision for enhancing the reliability and efficiency of the process bus. However, a significant gap appears to be present in the existing literature. Notably, no studies were identified that directly compared the reliability of a digital substation with a conventional substation. The existing research largely focuses on optimizing digital substations, with [6] providing the only indirect comparison. This research gap underlines the necessity for direct comparison studies, which could provide vital insights into the advantages and disadvantages of digital and conventional substations.

2.1.2 Literature Review on Failure Modes In The IEC 61850 Process Bus

Investigating the reliability of digital substations by identifying the possible failure modes is a recurring theme in many of the reviewed papers. For instance, the paper "Testing Reliability Performance of IEC 61850-Based Digital Substations" [7] offers a method for assessing digital substation reliability through simulated failure scenarios. The study considers two significant cases - heavy network load and packet loss (SV) - and their impacts on substation functionality. Its findings suggest that the failure likelihood increases with data load, highlighting the need for efficient network traffic control with Virtual Local Area Network (VLAN) use and priority tagging for time-sensitive information [7]. This idea is supported by the paper "Reliability evaluation of centralized protection system in smart substation considering the impact of communication message" [8], which emphasizes the importance of optimizing network traffic flow to enhance the reliability of substations.

A deep dive into specific failure modes in digital substations is provided by the paper "Failure Modes in IEC 61850-Enabled Substation Automation Systems" [9]. It categorizes failures into four types: physical, logical, software, and operational revealing that network structure and data communications are the most vulnerable areas of a Substation Automation System (SAS) [9]. This conclusion is shared by the "Reliability Investigation Of Digital Substation Networks Design Using FMEA Technique" [10], which used the Failure Modes and Effects Analysis (FMEA) to identify the communication network as the most vulnerable area for critical failure modes.

The implications of latency on substation automation systems are explored in "Latency Considerations in IEC 61850-Enabled Substation Automation Systems" [11]. The paper underscores that latency can lead to serious consequences, including incorrect readings, missed events, and an adverse impact on the performance of protective IEDs. This research underscores the urgency of addressing latency, proposing strategies such as improving network infrastructure, adopting real-time communication mechanisms, and utilizing data compression techniques to reduce data transfer volumes [11].

The paper "A methodology for the evaluation of the message transmission delay over IEC 61850 communication network — a real-time HV/MV substation case study" [12] further delves into latency issues, providing a methodology to evaluate message transmission delay and underscoring the effectiveness of tools like Wireshark in examining network traffic and identifying delay causes.

Moreover, the "Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying" [13] study highlights how data link speed and network background traffic can influence packet loss and delays. It reveals that the maximum sampled value delay could reach up to 26 ms and an average of 6 consecutive sampled values could be lost per second in a 345 kV/230 kV substation [13].

Packet loss and its effects on the performance of IEC 61850-based digital substations are further discussed in "Testing Reliability Performance of IEC 61850-Based Digital Substations" [14]. This research emphasizes that packet loss can lead to delayed and inaccurate data delivery, compromising the reliability and safety of the substation. It is also pointed out that multiple consecutive packet losses can cause a maximum operation delay of 20ms, and a cyclic suppression after each message could significantly mitigate this issue [14].

The evaluated papers emphasize the importance of implementing reliable hardware and software, optimizing network design, and effectively managing network traffic. The key to this analysis is identifying failure types and their possible effects. These contributions are certainly valuable, yet they are scattered across several different publications. The scattered nature can make it more difficult to comprehend all potential failure scenarios in digital substations.

2.2 Motivation

The importance of process bus architecture in enhancing the reliability and efficiency of a digital substation is evident in the reviewed literature. An examination of these works reveals a gap in the existing literature; there is an apparent lack of direct comparison between the reliability of a digital substation and a conventional one. To address this knowledge gap, this study aims to offer a comparative reliability assessment between digital and conventional substations. This, it is hoped, will shed light on the vulnerabilities and limitations of digital substations, contributing to the broader literature on substation reliability.

Moreover, the literature review revealed that the use of HSR and PRP has been thoroughly evaluated. These protocols have proven their effectiveness in enhancing the reliability of digital substations. However, an area that remains relatively less explored is how varying process bus architecture and Ethernet topology impact the reliability of these protocols and the overall reliability of the process bus. Such an analysis might improve the understanding of how these protocols adapted to various architectural environments and how that affects system reliability.

The digital substations also involve the integration of new monitoring functions, which directly affect the maintenance and reliability of the substation. Therefore, a comparison of the maintenance times between a conventional substation and a digital substation is a vital component of understanding the overall reliability of these new systems. In addition, to provide a broader perspective on the reliability of digital substations a comparison between non-repairable and repairable systems is necessary.

Lastly, the literature review makes clear how crucial it is to recognize different failure types and their potential effects in order to maintain the reliability of digital substations. However, the fact that these observations are scattered among several publications makes it difficult to have a complete grasp of potential failure scenarios. In order to address this dispersion, this research intends to centralize the information and create a list of failure modes in digital substations. This will create a centralized archive where failure modes in digital substations can be located, making the existing literature more easily accessible.

2.3 Hypothesis

Three related hypotheses form the basis of the investigation. First, it is anticipated that the incorporation of the process bus introduces additional complexity and potential points of failure to the substation automation system, thereby affecting its reliability when compared to conventional substations. The hypothesis also speculates that the Ethernet communication network, a core element of the process bus, may represent a significant vulnerability in the digital substation setup. It is also proposed that the architecture of the process bus may have a large impact on the overall reliability of the substation and on the performance of the HSR and PRP protocols.

3 THEORY ON SUBSTATIONS

This chapter will shed light on the conception and functionality of digital substations, contrasting them with their conventional counterparts to highlight their characteristics and advantages. The primary source of the content in this chapter is the specialization project titled "Theoretical Framework and Methodology Assessment for Calculating Reliability in an IEC 61850 Process Bus" [15]. Chapter 3.2 and 3.8.2 are new, while section 3.8.2.1 is from the specialization report but has been greatly changed. As well as structural improvements have been made.

These sections are included in this thesis to provide completeness, as understanding digital substation reliability demands an understanding of how digital substations work. As written in [16], "Probability theory is simply a tool that enables the analyst to transform knowledge of the system into a prediction of its likely future behavior."

3.1 Substations in General

A substation is a crucial part of the electrical grid, as it is responsible for stepping down high-voltage transmission lines to lower-voltage distribution lines. As the substation is such a critical component in the power system, there is a lot of use of protective equipment, such as [17]:

Circuit breakers: These are used to protect the substation equipment from damage caused by electrical faults or overloads.

Protective relays: These are used to monitor the substation equipment for any abnormalities and to automatically disconnect the equipment in the event of a problem.

Instrument transformers (CT/VT): They convert current and voltage to a lower magnitude so that relays and meters are able to measure the values.

Busbars: These are conductive metal bars that are used to distribute power to different parts of the substation.

Disconnect switches: These are used to isolate sections of the substation for maintenance or repair work.

Earthing switches: are a type of electrical switch that is used to connect a conductor to the earth. This is typically done for safety reasons, as it provides a low-resistance path for electrical currents to follow in the event of a fault, such as a short circuit.

Lightning arrester: Diverts the electrical energy from a lightning strike away from the equipment and to the ground.

Substations can have many different architectures as different voltage levels require different designs [18].

In figure 8 a two-busbar substation system can be seen. The purpose of connecting a substation to multiple busbars is to provide multiple paths for electricity to flow through the substation. This allows the substation to distribute power more efficiently, and it can also increase the reliability of the electrical grid by providing backup paths for electricity to flow in the event of a failure on one of the busbars. Additionally, connecting a substation to multiple busbars can make it easier to manage the flow of electricity through the substation, which can help to prevent overloads [17].

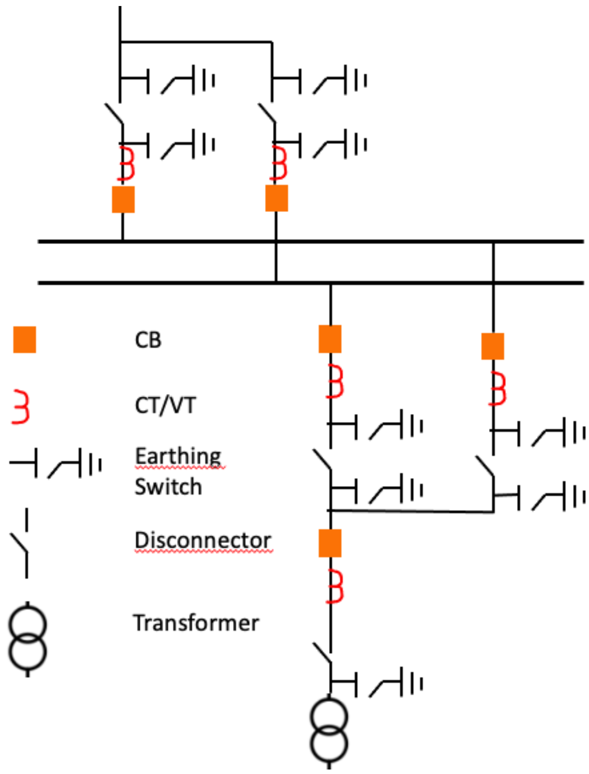


Figure 1: Line diagram of a substation [5], [6].

3.2 Power System Protection

A power system protection scheme is a coordinated set of protective devices, such as relays, sensors, and circuit breakers, designed to detect, identify, and isolate faults in an electrical network. The main objective of a protection scheme is to keep the power system stable by isolating only the components that are under fault, whilst leaving as much of the network as possible in operation [19].

Relays are essential components in power system protection, designed to detect and isolate faults to maintain the stability, safety, and reliability of the electrical grid. Once a fault is detected, protective relays analyze the changes in electrical parameters and determine the type and location of the fault. After identifying the fault, the relay sends a trip signal to the corresponding circuit breaker. The circuit breaker then opens, disconnecting the faulty section from the rest of the power system. This process minimizes damage to equipment and prevents the fault from spreading to other parts of the network [19].

3.2.1 Protection Coordination

Protection coordination in a power system refers to a strategic arrangement of protective devices such as circuit breakers, fuses, and relays/IEDs to ensure a sequence of operations that minimizes the effect of faults within the system [19].

In a power system, Protection is set up in zones to reduce the area of the electrical system that is disconnected when a malfunction occurs. This principle is displayed in Figure 2. Each zone is protected by dedicated protection devices, such as relays and circuit breakers, that are specifically designed and coordinated to respond to faults within that zone. To ensure comprehensive protection, the protection zones often overlap. Overlapping zones help avoid any unprotected areas within the power system and provide backup protection. If a fault occurs in the overlapping region, protective devices from both zones can detect and isolate the fault [19].

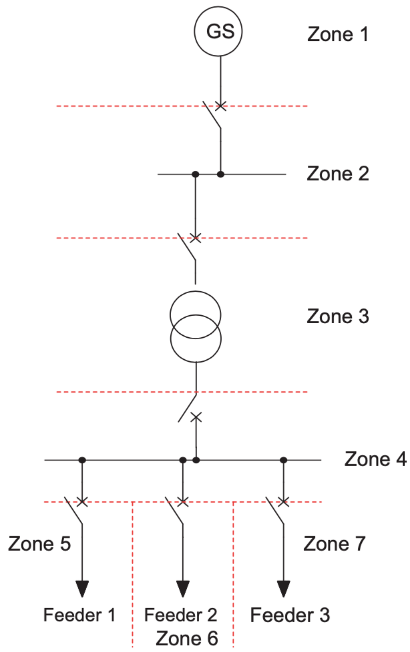


Figure 2: Zones of protection in a power system [19]

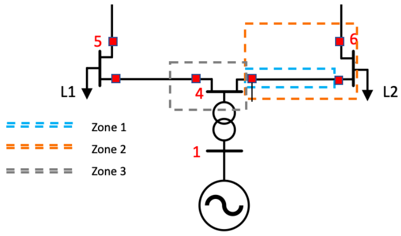
3.2.2 Backup Protection

Backup protection is a secondary system designed to operate if the primary relay protection fails or is unable to isolate the fault. It provides an additional safety measure to ensure the stability of the power system. There are two types of backup protection: local backup protection and remote backup protection [19].

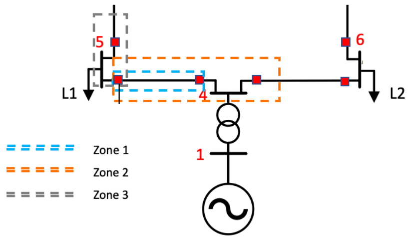
Local backup protection: Local backup protection is installed within the same protection zone as the primary protection. It is designed to act if the primary protection fails to operate or does not isolate the fault within the required time. Local backup protection usually involves time-delayed relays or relays with less sensitivity than the primary protection, giving the primary protection a chance to operate first [19].

Remote backup protection: Remote backup protection relies on neighboring protection zones to provide backup protection. If both primary and local backup protections fail to operate, remote backup protection detects the fault and sends a trip signal to the circuit breakers in the neighboring zones [19].

Each protective relay must have a minimum of two protection zones. The first zone covers 80% of the length of the power path, while the second zone covers 120%. Apart from these two zones, a third zone serves as a backup, which extends backward and acts as a safeguard for the bus bar located behind the relay [19]. These protection zones are illustrated in figure 3 and 4



(a)



(b)

Figure 3: The three zones of distance relays

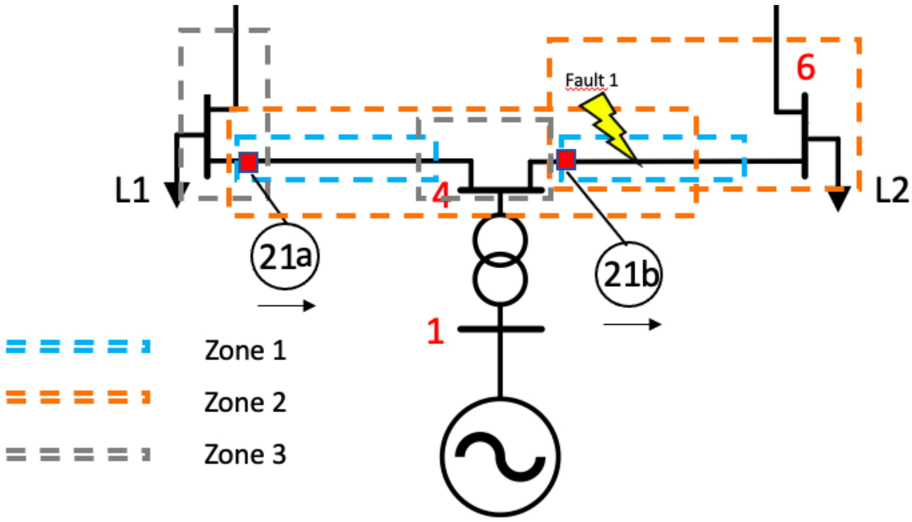


Figure 4: Overlapping zones

The scenario in figure 4 illustrates how backup protection can enhance the reliability and security of a power system. Consider the case where fault 1 occurs as depicted in figure 4. In this situation, relay 21b is responsible for tripping to isolate the fault. However, if relay 21b fails to do so, the backup protection mechanism comes into play, and relay 21a will trip to clear the fault.

3.3 Substation Automation System (SAS)

This chapter is highly based on information from [20]. Initially, electric power substations were operated manually by operators who monitored and controlled the electrical equipment using mechanical and electromechanical devices. The substation automation system (SAS) is a system that helps operate and maintain the electric power transmission and distribution system safely and reliably by automating certain tasks. One way it does this is by replacing the traditional mechanical relays with intelligent electronic devices (IEDs). IEDs can do many tasks at the same time, such as monitoring, protection, control, and communication.

The substation automation system (SAS) is organized into three hierarchical levels: the station level, the bay level, and the process level. The three levels are illustrated in figure 5.

3.3.1 The station level

of the substation automation system is responsible for the supervision, monitoring, and other tasks. It is usually located in a special room where authorized engineers, technicians, and operators can work and perform tasks such as inspecting the primary equipment and configuring devices and equipment through engineering software. The station staff uses human-machine interfaces (HMIs) to monitor the substation and send commands to its devices and equipment, and they can also use computers to access log databases with records of events that have occurred at all levels of the substation.

3.3.2 The bay level

of the substation automation system contains protection and control IEDs. These devices can work independently to clear faults at the process level as well as receive data at the station level. The devices at the bay level usually have local human-machine interfaces that can be accessed by technicians for maintenance purposes.

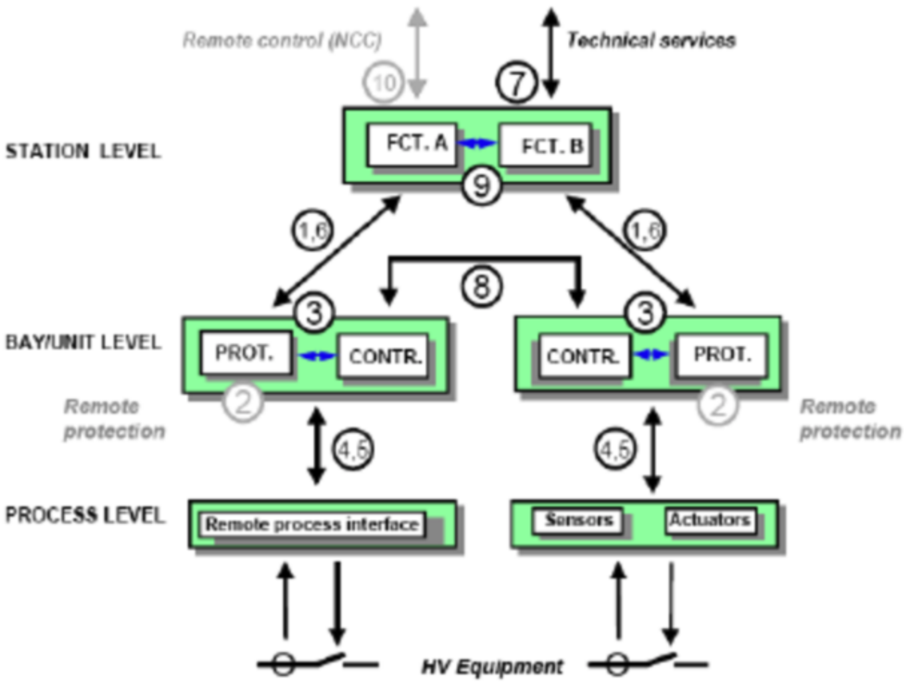


Figure 5: The three levels of the substation automation system [21].

3.3.3 The process level

The process level is part of the substation that contains the primary equipment, such as switchgear and transformers. This equipment is responsible for the main functions of the substation. The size and functionality of the substation automation system depend on the size, function, and technology of the process level.

3.4 Conventional Substation

The type of SAS depends on the level of automation and the technology used for communication and data exchange [20]. In figure 6 one can see how the levels of automation have evolved through the years. In this report, a conventional substation is defined as a substation that utilizes a station bus for automation but not a process bus, as can be seen in the 1995 column in figure 6. In such a system, the instrument transformers and circuit breakers are connected directly to the relays using cobber wires, and it operates on analog signals.

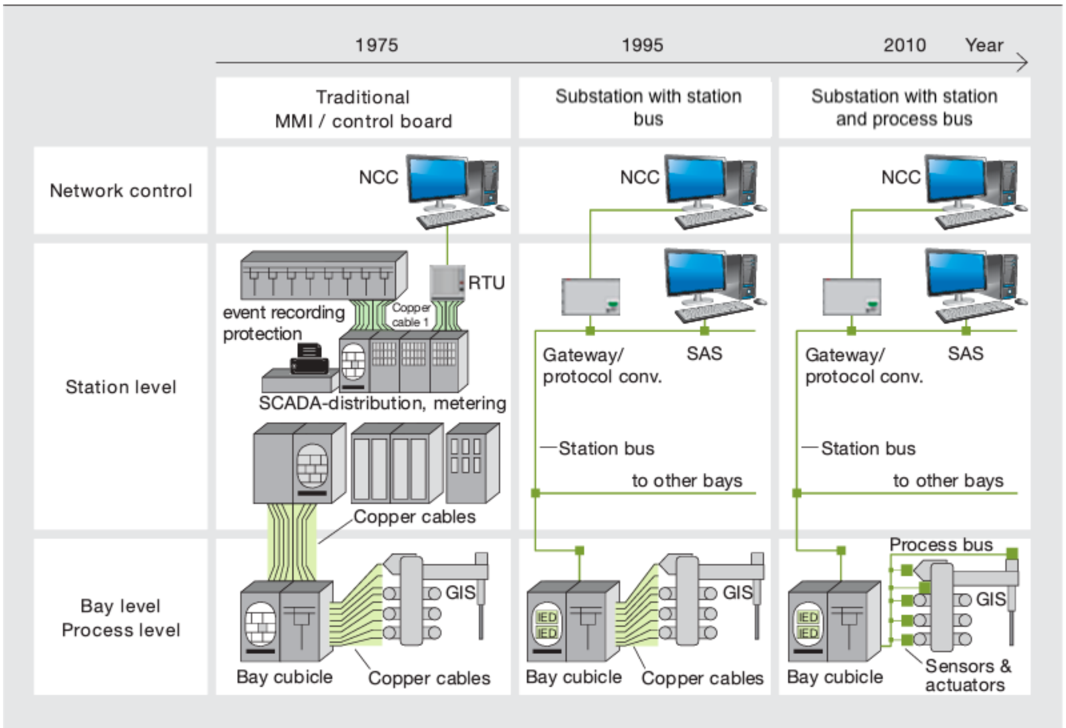


Figure 6: The evolution of the substation [22]

In a conventional substation, instrument transformers are typically based on electromagnetic principles. A CT works by wrapping a conductor carrying the current to be measured around a core, which creates a magnetic field. This magnetic field is then used to induce a current in a secondary winding that is proportional to the current in the primary winding [23]. The secondary winding is connected to a meter or other device, which can then measure the induced current and calculate the magnitude of the primary current [19].

A VT works by stepping down the voltage to a safer and more manageable level, which can then be measured by a meter or other device [23]. The voltage transformer consists of a primary winding, which is connected to the high-voltage circuit, and a secondary winding, which is connected to the measuring device [19].

In figure 7 a conventional substation system is presented. Here, intelligent electronic devices (IEDs) are microprocessor-based and have many features, but they are connected using copper wires. Digital communication between the IEDs is possible using the station bus but the communication protocols differ between manufacturers [3] making it difficult to connect devices from different suppliers. In this architecture, the IEDs send data about substation events and equipment status to the station level and exchange events and status with other IEDs at the same level via the station bus. Conventional instrument transformers are still used in the switchyard.

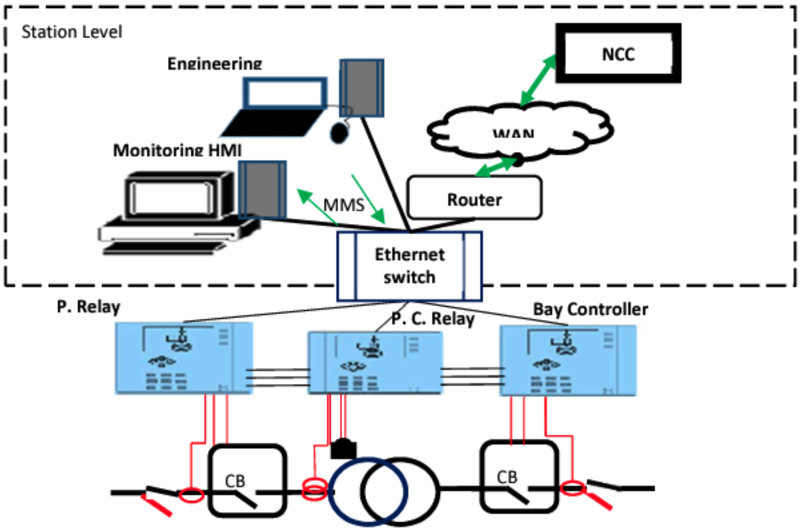


Figure 7: Conventional cabling system [20]

The differences between a conventional and digital substation will be discussed in chapter 3.6, but first, it is necessary to introduce the digital substation.

3.5 Digital Substation

A digital substation refers to a substation that utilizes the IEC 61850 standard for communication processes, interoperability, and automated engineering processes. In a digital substation, the copper wires are replaced by fiber optic cables, which enable the use of the process bus and devices such as merging units and Ethernet switches. The fiber-optic-based system enables high-speed communication within the substation devices. Optical fibers are tiny glass strands that act as light waveguides. The ability to transmit light over long distances can be exploited to create optical communication links that have a huge capacity for information transfer and built-in immunity to electromagnetic interference [20].

An illustration of a digital substation is presented in figure 8. In a digital substation, merging units (MUs) and breaker IEDs are connected to the instrument transformers (preferably NCITs) and switchgear and are responsible for converting the analog voltage and current signals to digital format and controlling the circuit breakers.

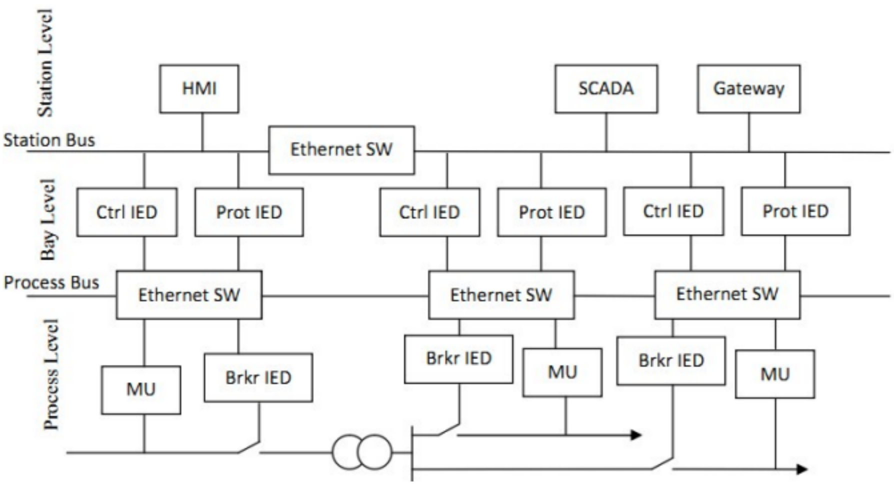


Figure 8: IEC 61850 digital substation topology [24]

The three levels of the digital substation are connected with each other using two local area networks (LANs). The first LAN, called the process bus, connects the process level to the bay level. The second LAN is called the station bus and connects the bay level to the station level. These LANs are communication networks that enable the connection between the major switchyard equipment—voltage transformers, current transformers, circuit breakers, disconnectors, etc.—and the protection, measurement, and control IEDs.

The three levels of the digital substation are connected with each other using two local area networks (LANs). The first LAN, called the process bus, connects the process level to the bay level. The second LAN is called the station bus and connects the bay level to the station level. These LANs are communication networks that enable the connection between the major switchyard equipment—voltage transformers, current transformers, circuit breakers, disconnectors, etc.—and the protection, measurement, and control IEDs.

3.6 Comparison Between Digital and Conventional Substations

Compared to a digital system, a conventional substation has no ability to convert signals from analog to digital. This means that a conventional substation operates without the use of merging units, Ethernet switches, or time synchronization sources. Instead, the conventional substation connects the circuit breakers and current transformers directly to protective relays using copper wiring. A conventional substation wiring network is therefore composed of extensive copper wiring networks, which makes diagnostic procedures for fault scenarios time-consuming. The number of copper wires increases depending on the function of the devices and can be much more expensive to implement than a fiber optic network [22], as the networks are larger. The difference in the cabling systems can be seen in figure 10. More than 30 tons of material can be saved in a digital substation [25]. This facilitates less travel. The fiber optic installation reduces the cabling by 90% and by the adoption of NCITs rather than conventional CTs, reduces the weight of CTs by 80% [26]. IEC 61850-compatible devices don't need as much manual configuration, which results in lower installation costs.

The fiber optic LAN in a digital substation reduces infrastructure and installation costs as the process bus eliminates the need to connect unique cables for every IED. Thus, there is less need for trenching during installation and they are much lighter than copper wires[19]. An existing IEC 61850-based network can be expanded without significantly affecting the equipment already in place [19]. Fiber optic cables have much higher bandwidth, meaning they can transmit data at much higher speeds. Also, fiber optic cables are considered more reliable as they are not affected by electromagnetic interference which can cause data loss in copper cables. They are also much safer to use as there is little chance of them overheating since they are non-conductive.

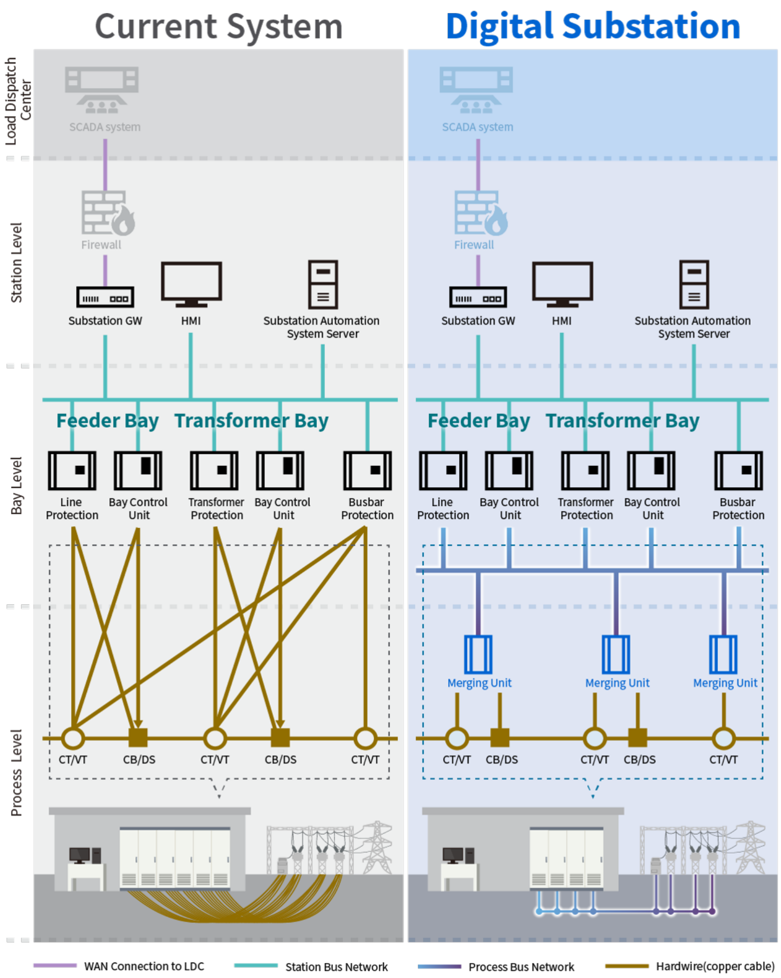
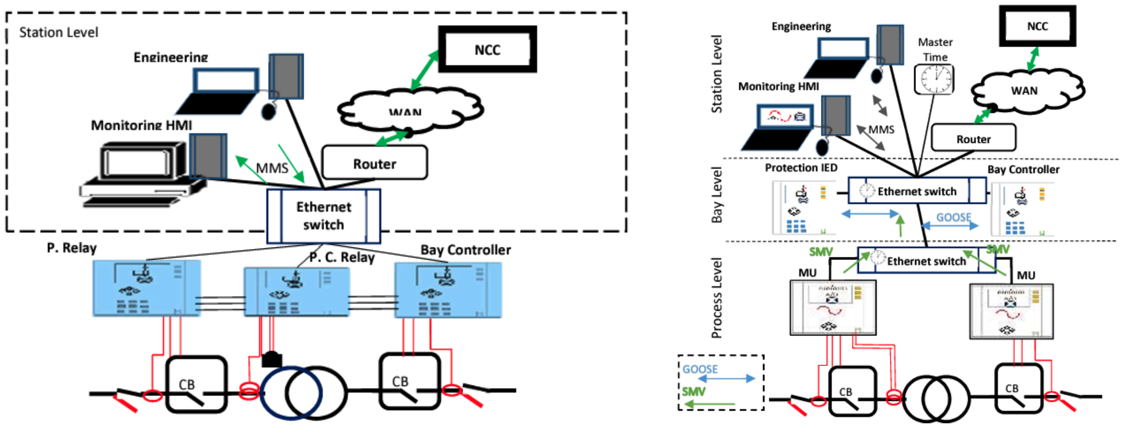


Figure 9: Conventional vs. digital substation [27]

The communication language implemented by the IEC 61850 standard allows for interoperability between devices from different manufacturers. In a conventional system, there was no common communication language, thus devices were only able to communicate with other devices that were produced by the same manufacturer. This lack of sufficient communication infrastructure means that the conventional substation has limited access to real-time data regarding changes in load and system operating conditions. Messages between devices could get lost due to interference or a fault. As a result of this lack of situational awareness, the substation is more vulnerable to frequent disruptions that might cause blackouts [28].

Device names are not predetermined by either the user or the device manufacturer. They are presented in a power system context and stated in the standard, enabling the engineer to understand the significance of the data right away.

As mentioned, in a conventional substation the CTs, VTs, and CBs are connected directly to the IEDs using cobber wiring. The IEDs in a digital substation are connected to the circuit breakers and instrument transformers using a process bus, which enables them to communicate with each other and with other components within the substation. This enables the IEDs to provide a coordinated and integrated protection and control system for the digital substation [20]. The difference in the wiring systems can be seen in figure 10



(a) conventional cabling system

(b) Digital cabling system

Figure 10: Conventional vs digital cabling system [20]

3.6.1 Analog Vs. Digital Signals

A conventional substation operates using analog signals while a digital substation uses digital signals. Figure 11 illustrates the difference between the two signals. The distinction between these two is that digital signals are discontinued and operate using binary format (zeros and ones), they can only be represented with fixed values. In contrast, analog signals are continuously changing and have a sinusoidal shape.

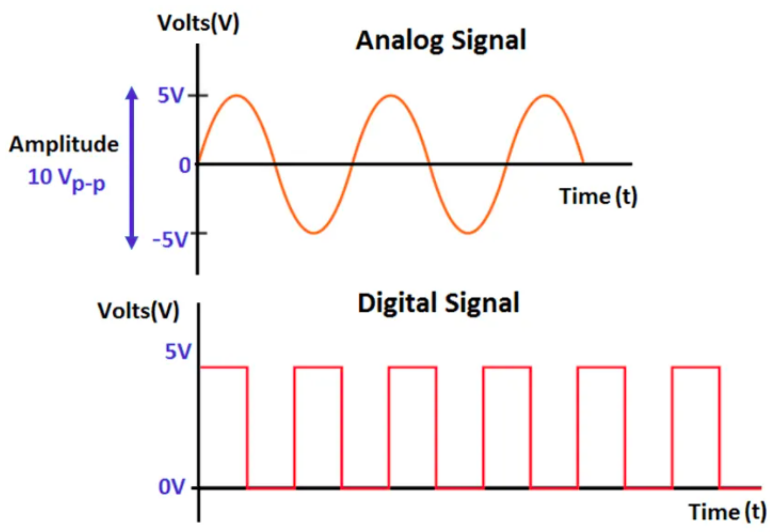


Figure 11: Difference between analog and digital signal [29]

Using digital signals in a substation offers several advantages over analog signals. Digital signals are more accurate and precise and are less prone to error or degradation over distance or time. They can be easily transmitted and processed using computers, which allows for greater flexibility in the design and operation of substations [30].

Another advantage of digital signals is their ability to prevent data loss. Analog signals can be lost or distorted during transmission because they are prone to electromagnetic interference. Digital signals, on the other hand, use error-correction techniques to ensure the integrity of the data and reduce the risk of data loss [31].

Digital signals are also more secure than analog signals. They can be encrypted to protect against unauthorized access, making them well-suited for use in substations where sensitive data may be transmitted [30].

3.6.2 Electromechanical Vs. Non-Conventional Instrument Transformer

In a conventional substation instrument transformers are based on electromechanical principles which have some disadvantages as it is necessary to have a large iron core in order to avoid saturation during faults [19]. The core is also a source of inaccurate measurements during normal operation due to eddy currents and flux reminiscence [19]. The wiring systems within the transformers can also overheat and degrade the measurement performance [19]. Conventional instrument transformers are typically designed to perform a single function, such as current or voltage measurement. The basic concept of an electromechanical current transformer is illustrated in figure 12

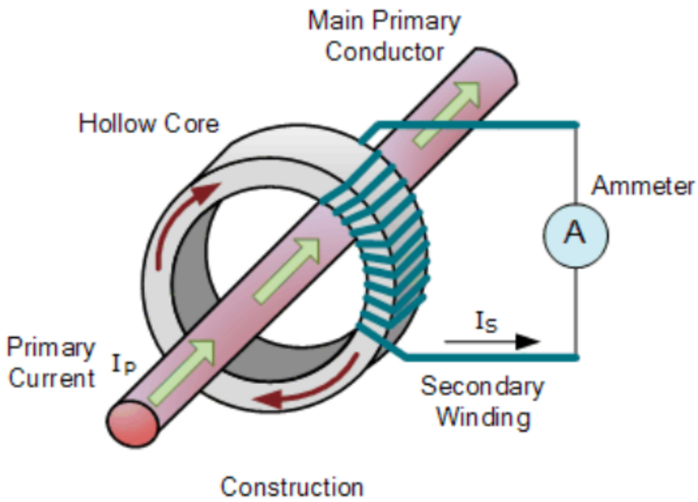


Figure 12: Electromechanical current transformer [19]

Digital substations can use non-conventional instrument transformers (NCITs). The IEC 61869-9 [32] is an international standard that specifies the requirements for instrument transformers used in metering and protection applications for the IEC 61850 standard. The goal of the standard is stated as "To provide a product standard for instrument transformers with a digital interface according to the IEC 61850 series" and "To reduce the engineering amount required to achieve interoperability for the digital interface between instrument transformers and equipment that uses the digital signals"[32]. The basic concept of the NCIT is illustrated in figure 24. Here, the NCIT is connected to multiple phases and uses an internal merging unit to convert to digital signals.

Non-conventional instrument transformers (NCIT) are based on digital technologies, such as microprocessors and software algorithms, and require no iron core. Thus, it can overcome the limitations of the conventional instrument transformer [19]. NCITs are typically able to provide higher accuracy and stability, as they are based on digital technologies and can be calibrated and compensated for environmental factors [22]. NCITs are typically able to perform multiple functions, such as protection, control, and measurement. This enables NCITs to provide a more versatile and flexible measurement system compared to conventional instrument transformers [19]. NCITs are connected to the process bus in a digital substation, which enables them to communicate with other substation components and provide a coordinated and integrated measurement system.

Since NCITs can replace conventional measuring transformers, the footprint of primary switchgear can be lowered. Traditional VTs are large, heavy components, however new sensor technology for voltage measuring allows for significantly smaller equipment [22]. Additionally, since all NCIT adjustments may be completed with software and their hardware can be standardized, a shorter overall delivery time can be achieved [22].

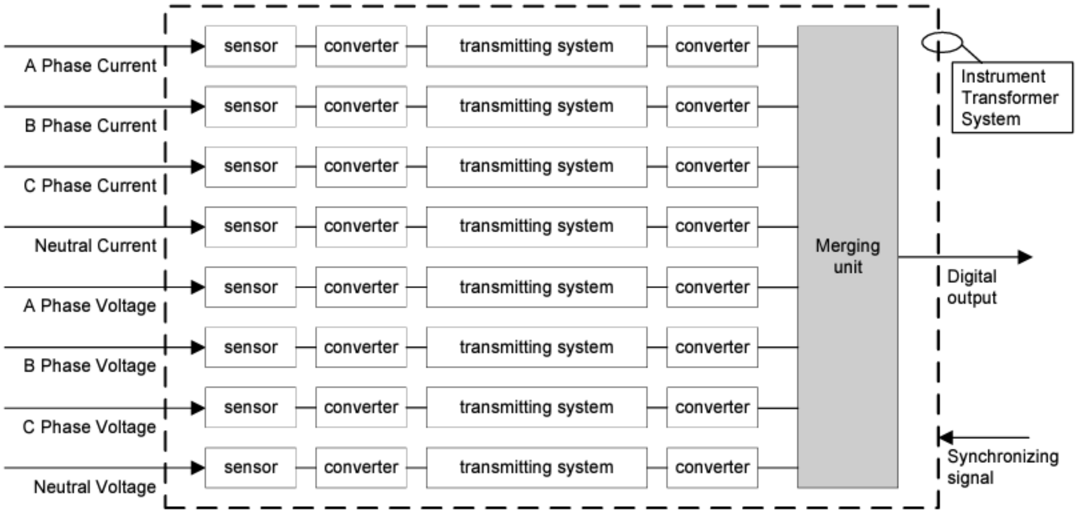


Figure 13: Concept of a NCIT [32]

3.7 IEC 61850

The IEC 61850 standard [33] was developed to secure high-speed communication between digital substation equipment by defining communication protocols, data models, and communication requirements between IEDs [3]. The standard, titled "Communication Networks and Systems in Substation," was issued by IEC Working Group TC57 and presented in 2003. Before this standard, there was no common communication protocol, therefore different manufacturers created their own protocols, which prevented devices from different manufacturers from communicating with one another [3]. The standard's development was guided by three main objectives [33]; facilitate communication between IEDs made by various manufacturers. Technology advancements shouldn't cause the standard to become obsolete, and the standard should allow for the independent implementation of needed features.

IEC 61850 offers a detailed model for how data organization for power system devices should be similar across all types and brands of equipment. This enables the next level of substation automation systems as the devices can configure themselves, eliminating a lot of the laborious non-power system configuration work [19]. For instance, if a CT/VT is connected to an IEC 61850 relay, the relay can recognize this module and, without human input, assign it to a measurement unit [34]. The standard consists of multiple parts, each covering an individual aspect of the digital substation system. The mapping of these parts is shown in figure 14.

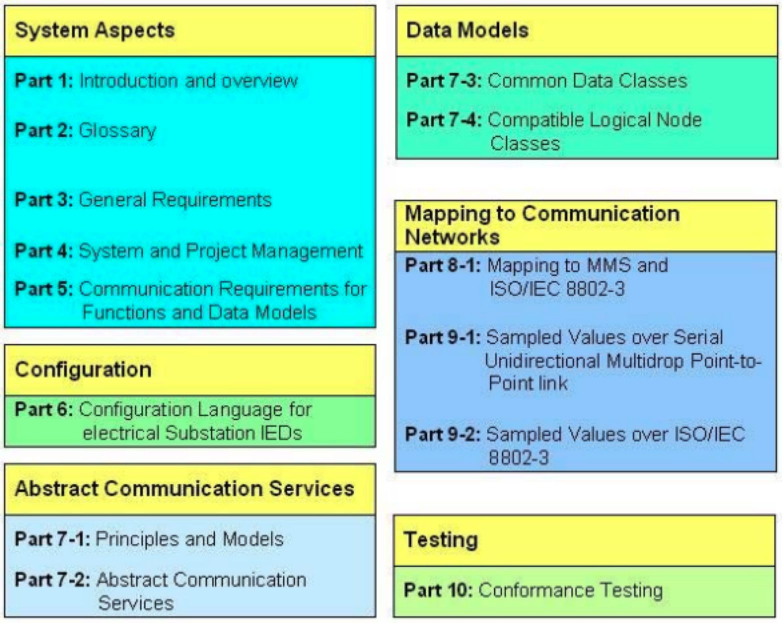


Figure 14: Structure of the IEC 61850 Standard [35].

3.7.1 Data Model

The data model is defined in the IEC 61850-7-3 and 61850-7-4. It defines the structure and organization of the data exchanged between devices in the digital substation, as well as the rules and protocols for exchanging and processing the data [19]. All IEDs must adhere to this shared communication language, which provides consistency across the substation and creates interoperability between devices from different manufacturers [19].

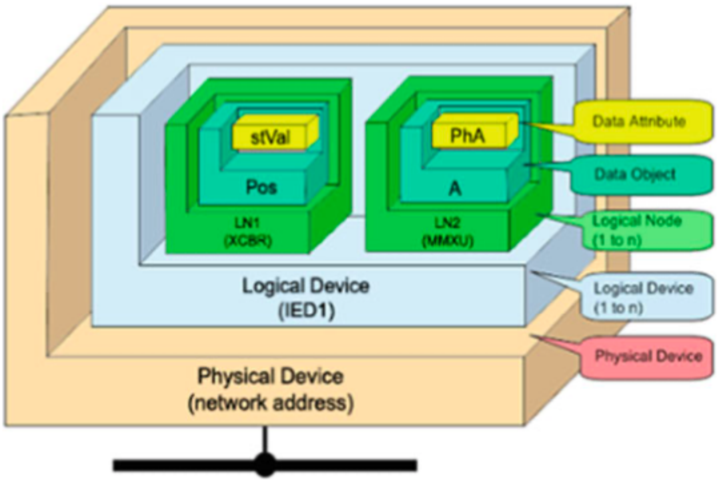


Figure 15: Data model levels of hierarchy 15.

In figure 15 the hierarchical level of the data model is presented. This explanation of the data model is based on information from [19]. The data model starts with a physical device, which is typically an IED and is defined by its IP address. Within a physical device, there are one or more logical devices, which again contain logical nodes. A logical node consists of four prefixed characters that specify what task the IED must complete. The first letter represents the group indicator. The next three letters represent what purpose the logical node has. For instance, if an IED receives a logical node containing the letters PTOC, the "P" means that it has something to do with protection, and "TOC" stands for time over-current. Thus, PTOC means that there are required protective functions for over-current. Data objects are stored within the logical nodes and can contain multiple elements of data, such as measured values, system information, physical device information, status information, and more. In table 1 the group designator for logical node categories is tabulated.

Table 1: Logical node categorisation [19]

Logical node groups	Group designator
System logical nodes	L
Protection functions	P
Protection related functions	R
Supervisory control	C
Generic function references	G
Interfacing and archiving	I
Automatic control	A
Metering and measurement	M
Switchgear	X
Instrument transformer	T
Power transformer and related functions	Y
Further power system equipment	Z

3.7.2 OSI Model for Communication

Within a digital substation, transferring messages from one device to another is the definition of communication [19]. The communication procedure might take place between two devices or over larger networks. Time synchronization and language issues could come up during this communication procedure [19].

In order to deal with these issues, the International Standards Organization (ISO) introduced the open system interconnection model (OSI) in 1984 [19]. This model is the foundation of the IEC 61850 communication protocol. In table 2, the seven layers of the communication process are listed. Each of these layers specifies how data is processed along the various transmission phases [19].

Table 2: The 7 layers of the OSI model [19]

Layer	Name	Function
7	Application layer	Communication application
6	Presentation layer	Encryption and data representation
5	Session layer	Inter-host communication
4	Transport layer	End-to-end connections and reliability
3	Network layer	Logical addressing
2	Link layer	Physical addressing
1	Physical layer	Media, signal, and binary transmission

The seven layers of the model are [19]: The physical layer, which deals with the physical connection between devices, such as cables and connectors. In the case of a process bus, it is fiber optic cable. The data link layer ensures that data is transmitted reliably between devices on the same network [36]. The network layer routes data between different networks; this is normally done using an IP address [19]. The transport layer is responsible for sorting and managing the data packets when they arrive and presenting the data in the correct sequence to the correct destination [19]. The session layer ensures that the connections are operating correctly [19]. The presentation layer translates data into a format that can be understood by the application layer. The application layer provides services to the user, such as email and web browsing [19].

3.7.3 Communication Services

In order to identify between applications and manage traffic flow, the IEC 61850 standard specifies five different types of communication services [28].

- Manufacturing Message Specification (MMS)
- Generic Object Oriented Substation Event (GOOSE)
- Generic Substation Status Event (GSSE)
- Sampled Values (SV)
- Time Synchronization (TS)

The ISO 9506 standard covers the MMS protocol. The MMS messages serve as a communication service between the bay level and the station level devices and can be used for a variety of applications, such as human-machine interfaces, supervisory control, data acquisition, and configuring devices [20]. MMS is carried through the transmission control protocol (TCP), which is a communication protocol used to transmit data over a network in a reliable manner by establishing an end-to-end connection and ensuring that data is delivered in the proper sequence [37].

Event and status data are exchanged using the GOOSE and GSSE services. Together, they are called generic substation events (GSE). GOOSE messages can carry multiple data types, including digital, analog, binary, and integer values. While GSSE only includes binary state messages [20]. The GOOSE messages take advantage of multicast services, which enable the delivery of the same message to numerous IEDs at once [37]. IEDs can publish and subscribe to GOOSE and GSSE messages to exchange data and make decisions based on the received data [20]. When an event occurs, the messages are immediately transmitted, and they are then repeated with a growing time interval from T_{min} to T_{max}. The T_max repetition continues indefinitely until a new event occurs, at which point the repetition rate is reset to T_min [28]. Consequently, high-speed communication for locking switchgear is possible with GOOSE messages [37]. This process is defined in the IEC 61850 standard and ensures a highly dependable GOOSE delivery system.

Sampled values are a digital representation of the measured current, voltage, and frequency [20]. The process bus is used to transfer sampled values from the merging units to the protection and control IEDs. The unidirectional multicast communication method is used to send sampled values. When a merging unit employs this technique, it can send data simultaneously across the process bus to numerous recipient IEDs by using a multicast address [20]. Instead of sending separate messages to each IED separately, this enables the merging unit to send a single message to a number of IEDs at once.

In substation automation applications, many time-sensitive messages have a Time-To-Live (TTL) field, which denotes that the message will lose its significance if it is not delivered within a given timeframe [28]. For instance, the trip/close commands must be sent to the appropriate IEDs within 5 ms for 50Hz systems to carry out the necessary operations [28]. Consequently, as shown in table 9, the IEC 61850 standard establishes transfer time standards for SAS applications.

Table 3: IEC 61850 transfer time requirements [28]

Services	**Transfer Time (ms)**
SV	3-10
GOOSE, GSSE	3-100
MMS	20-100

GOOSE and SV messages are used for time-sensitive tasks, including protection trip commands and analog measurements. Because of this, GOOSE and SVs are highly prioritized, and the transmission control protocol (TCP) doesn't meet the requirements for protection applications [20].

Therefore, GOOSE and SV messages skip some of the layers within the ISO communication model, which results in low-latency, high-speed data transportation with no requirements for confirmation [28]. This makes GOOSE and sampled value message transmission much faster than the other communication services within the IEC 61850 standard, as is depicted in figure 16. The MMS communication service goes through all 7 layers of the ISO model.

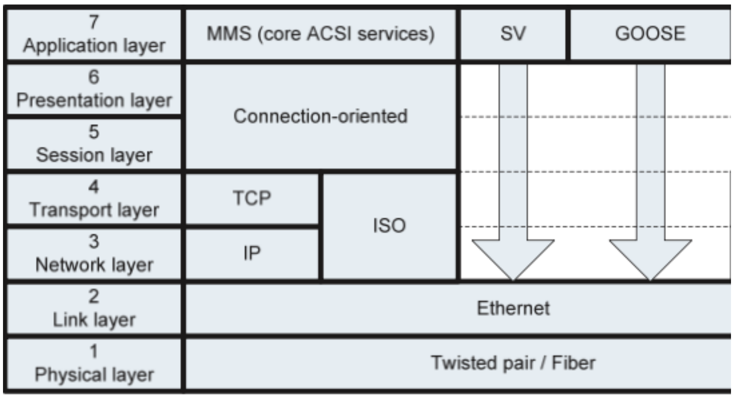


Figure 16: IEC 61850 protocol stack [19]

3.7.4 Time Synchronization Source

A typical IEC 61850-based substation measures parameters at several physical locations. To achieve proper application performance, these measured parameters must be precisely time-synchronized to a shared time reference. A digital substation needs appropriate time synchronization to correctly analyze faults and incidents and to operate correctly [28]. If time synchronization fails, the performance of the merging units may be affected. When global synchronization is restored after synchronization drift, the time sequence of SV data may become disorganized. This could block protection functions until the time sequence is recovered or lead to unwanted protection function activities. Local time servers or clocks may be synchronized by using timing signals from a GNSS (global navigation satellite system) [28]. In figure 17 the concept of time synchronization is presented. The common standard for all devices is the external global primary reference. The master clock/local primary reference) is a clock that is located in the substation and is synchronized to the global primary reference. The end devices can be synchronized with the master clock by using several distribution architectures. [38] defines the accuracy of time synchronizations as "the difference in time between the global primary reference and the end device".

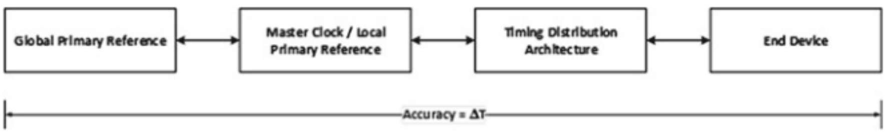


Figure 17: Time synchronisation block diagram [38]

In substation automation, the two most utilized protocols for time synchronization are the global positioning system (GPS) and the Precision Time Protocol (PTP) [28]. When utilizing GPS, devices are equipped with GPS, which means that they are able to communicate with satellites that are synchronized at the same time. This time is used as the reference clock for all the devices and ensures that the process bus is properly synchronized [39]. PTP is designed to be utilized in a ping-pong manner, where data frames are sent and received between the master clock and end devices [38]. In addition, PTP allows for the use of several master clocks to provide redundancy and enables end devices to choose the best master clock for synchronization [38].

3.8 The IEC 61850 Process bus

The process bus is a high-speed communication Ethernet network defined in the IEC 61850-9-2 standard. The term "process bus" refers to the fiber-optic LAN that connects the process-level devices to the bay-level devices. The process bus exchanges old copper wires with a fiber optic network which greatly reduces cost while at the same time enhancing the communication flexibility within the network [3]. The messages transmitted over the process bus are termed GOOSE and Sampled Values (SV) [3]. The five most vital devices of the process bus are depicted in green in figure 18. These devices include the time synchronization source, merging unit, breaker IED, protection IED, and control IED.

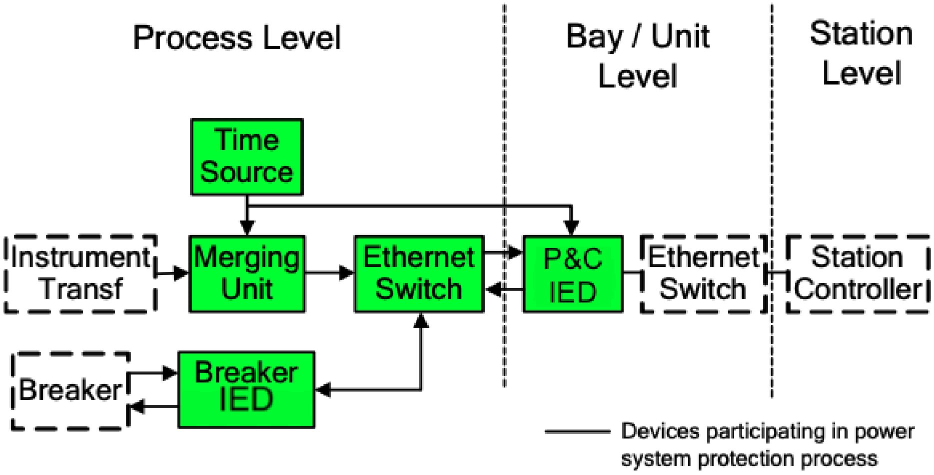


Figure 18: Block diagram indicating vital devices of the process bus [40]

In the process bus, merging units and breaker IEDs collect information about the status of switchgear and instrument transformers and send it to protection and control IEDs at the bay level using the IEC 61850 communication protocol [41]. The protection and control IEDs use this data to identify issues and manage the power system. They also send information to a human-machine interface (HMI) at the station level using IEC 61850 [41]. A time synchronization server keeps all of the devices in sync. The following chapters will provide an explanation of the most vital devices in the process bus excluding the time synchronization source as it has already been explained in chapter 3.7.4.

3.8.1 Ethernet Switches

In the case of a process bus, Ethernet switches (ES) are devices that are used to connect IEDs to the local area network (LAN). The switches receive data from IEDs and forward the data to the correct destination using MAC addresses. [42]

3.8.2 Ethernet LAN

The process bus uses a Layer 2 Ethernet network. Layer 2 Ethernet refers to the second layer of the OSI (Open Systems Interconnection) networking model, which is responsible for providing a reliable communication service between devices on the same local network. In the context of a process bus, Layer 2 Ethernet is a networking technology used to connect IEDs within a substation, allowing them to exchange data and communicate with each other [43].

Layer 2 Ethernet uses a variety of protocols and technologies, including Ethernet, MAC (Media Access Control) addresses, and VLANs (Virtual Local Area Networks), among others, to ensure that data is transmitted efficiently and securely between devices.

According to [14], using a Virtual LAN (VLAN) may be a way to improve reliability in digital substations. A VLAN divides a physical network into numerous separate sub-networks. Data traffic and time-sensitive data, such as trip commands, can be prioritized using VLANs. This enables relevant messages to be forwarded first and reduces the likelihood of delay or congestion caused by non-critical traffic.

3.8.2.1 Ethernet Network Architecture

The way in which the devices in a network are connected to each other is referred to as its topology. For an Ethernet network, there are numerous potential network topologies, and each of these has a unique effect on the network's reliability [44]. In general, a network with a redundant topology, where there are multiple paths between devices, is more reliable than a network with a non-redundant topology, where there is only one path between devices. According to the findings in the literature review, there are three main Ethernet architectures that can be used in a process bus: cascade, star, and ring.

In cascade architecture, all Ethernet switches are connected in a chain, as shown in figure 19. This architecture is relatively cheap compared to a ring or star system, but consequently, it will result in a higher time delay. [5].

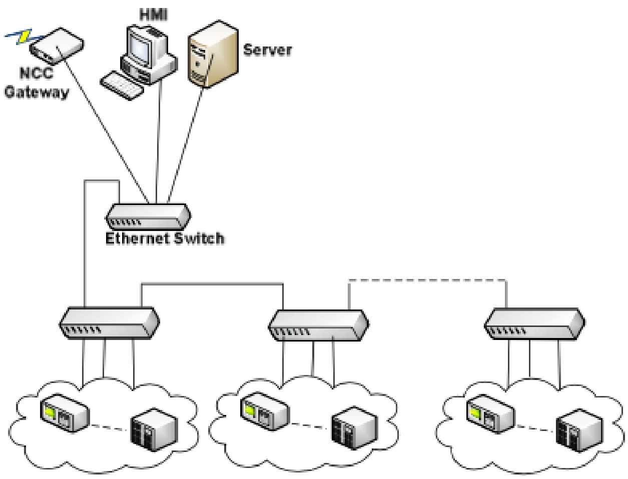


Figure 19: Cascade [3]

In a star architecture, all components are individually connected to one central Ethernet switch. This switch acts as a central point of communication, routing data from one device to another[5]. The advantage of a star topology is that it is relatively easy to set up and manage, and it allows for easy expansion of the network [3]. Using this typology creates a weak point in the scheme, which is that message transmission is dependent on only one switch. If this switch fails, the entire network will be disrupted [4].

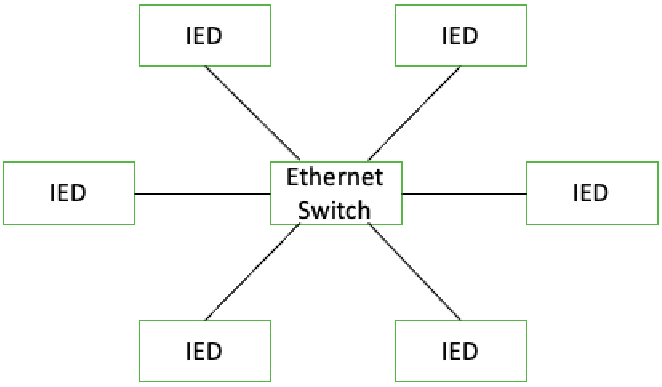


Figure 20: Star topology

Ring architecture creates a closed-loop LAN. Loops are not supported by Ethernet switches because messages could continue to cycle indefinitely [4]. Consequently, IEEE 802.1W introduced the use of Rapid Spanning Tree Protocol (RSTP) [45]. This protocol enables switches to identify loops and stop the circulation of messages. During this protocol, the Ethernet switches temporarily disable some of the redundant devices, putting them in a backup state, and thus breaking any loops in the system. This means that in the event of a communication cable failure, the LAN can be reconfigured with the aid of RSTP[4]. As a result, even after the failure, the fault system will continue to work. Consequently, a single communication cable failure won't have an impact on the protection mechanism. [3].

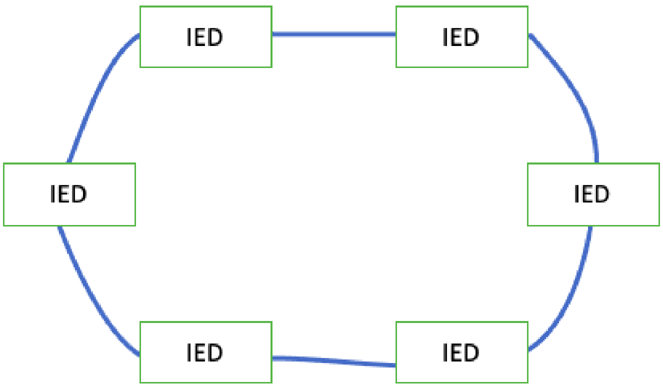


Figure 21: Ring topology

In a ring architecture, the Ethernet switches are connected in a loop, and managed switches with Rapid Spanning Tree Protocol (RSTP) are used to ensure network reliability and fault tolerance.

This incorporates n-1 redundancy to the system, the "n" refers to the total number of components in the system (in this case, Ethernet switches). "n-1" means that the system can continue to operate even if one of the components fails. This level of redundancy is achieved in the ring architecture because of the looped structure and the RSTP [5].

To illustrate this, consider a scenario where there are four Ethernet switches; A, B, C, and D connected in a ring. In normal operation, the data flows in the following order: A $\rightarrow$ B $\rightarrow$ C $\rightarrow$ D $\rightarrow$ A. If one of the switches fails (e.g., switch B), RSTP will detect this failure and reconfigure the network so that the communication path bypasses the failed switch. The new communication path will be A $\rightarrow$ C $\rightarrow$ D $\rightarrow$ A and only 3 out of the 4 Ethernet switches are now required for inter-bay communication [46].

This n-1 redundancy in ring architecture ensures that the system remains operational even in the event of a single switch or connection failure. However, it's essential to note that this level of redundancy is limited to a single failure; if multiple failures occur, the system may not be able to maintain its functionality [46].

3.8.3 IEDs

An IED is a general term for relays that use digital technology. An "intelligent electronic device" (IED) may monitor processes and execute electrical protection or control tasks in power systems. Sensors and power sources feed data to IEDs. IEDs can send control commands, such as tripping circuit breakers if they detect voltage, current, or frequency abnormalities. They can also raise or lower voltage levels in order to maintain the desired level. IEDs used in the IEC 61850 standard and their functions are listed in table 4.

Table 4: Different types of IEDs

IED Type	**Function**
Merging Unit	Converts analog signals to digital form
Protection IEDs (Prot. IED)	Perform protection functions
Control IEDs (Ctrl. IED)	Monitoring and metering functions
Breaker IEDs (Brkr. IED)	Operate and trip the breakers

The sampling rate refers to the rate at which a system or device measures or captures data. In the context of a process bus, the sampling rate refers to the frequency at which IEDs measure and capture data from sensors and other devices connected to the electrical equipment in the substation [47]. IEC 61850-9-2 specifies two different sampling rates for IEDs in process buses [40]: one of 80 samples per frequency cycle which is used for simple protection and control applications, and another of 256 samples per frequency cycle for high-frequency applications like power quality monitoring and high-resolution oscillography. The frequency in Europe is 50 Hz, which means that the sampling rate of the process bus is either 4000 Hz or 12 500 Hz [40].

Figure 22 illustrates the various communication services that the IEDs in the process bus employ. The protection and control IEDs can communicate with both GOOSE and sampled value services, unlike the merging unit, which is only concerned with sampled values, and the breaker IED, which only uses GOOSE messages.

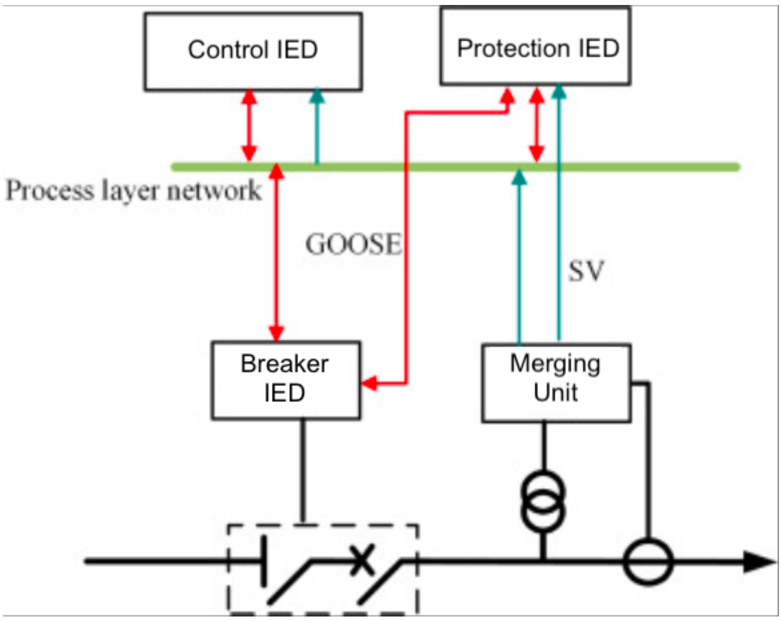


Figure 22: What communication services the IEDs use [48].

3.8.3.1 Merging Unit

The merging units (MUs) transmit sampled values (SV) of phase currents and phase voltages to the protection and control IEDs. This concept can be seen in figure 23. They are what connect the instrument transformers to the process bus. A MU can also receive data from several instrument transformers originating from a single bay [38]. A MU may be a component of a non-conventional instrument transformer (NCIT), which directly transforms optical signals into digital form, or it may be a distinct stand-alone merging unit (SAMU), which is used to convert analog signals from conventional instrument transformers [32].

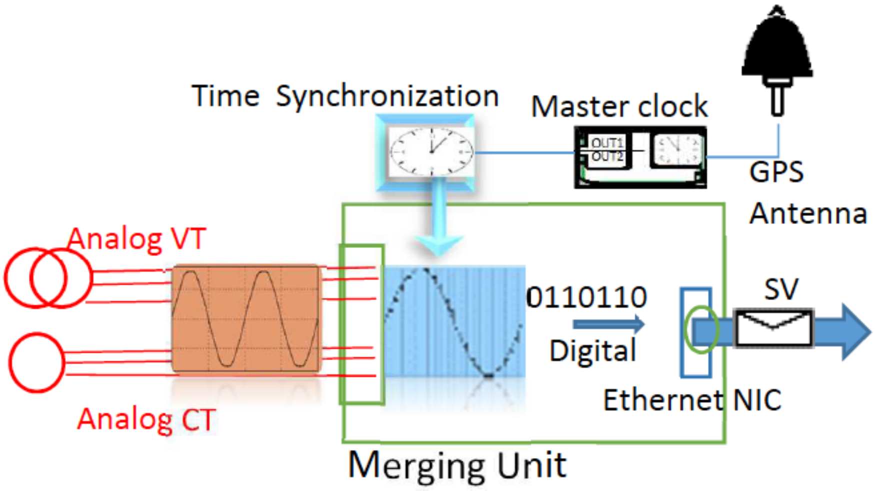


Figure 23: The concept of a merging unit [20]

Figure 24, shows various scenarios for digital protection, where the primary differences between conventional and modern protection designs can be seen. At the top of figure 24 a conventional protection design is shown. Here, currents and voltages are measured using conventional instrument transformers. The analog signal is converted to digital form inside the IED [38]. A MU is introduced in the next section of the figure, which demonstrates how much less burden the new IED has in comparison to the IED based on conventional principles. The NCITs are introduced at the bottom of the figure; with these devices, the MU simply functions to adjust digital signals and has much less responsibility [38].

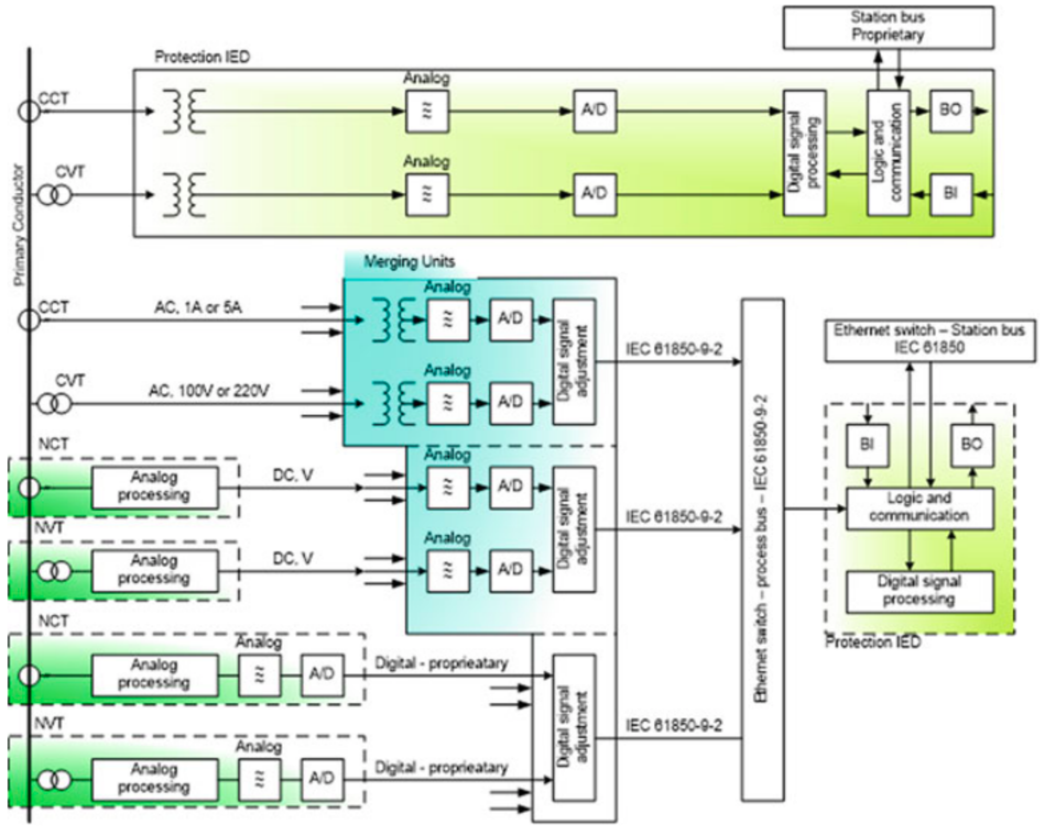


Figure 24: Different possibilities of digital protection [38]

Because of its weight and size, NCIT has a significant impact on the substation yard because it can be fixed directly to other major equipment or placed on considerably lighter foundations [22].

3.8.3.2 Breaker IED

By transmitting IEC 61850 trip commands to primary switchgear and returning position status to the protection and control IEDs, a breaker IED serves as an actuator and sensor gateway [2]. A breaker IED is also referred to as an intelligent breaker controller (IBC). The breaker IED will convert the commands from IEC 61850-9-2 format to binary contact signals that can be used to trip the coils in the primary equipment like the circuit breaker, disconnector, and earthing switch [49].

The circuit breaker IED's functions include receiving trip messages, determining end-to-end (ETE) delays, and sending multicast GOOSE/GSSE events to other protection IEDs and station PCs [50]. ETE delay is the period of time between the creation of the message at the transmitting IED's application layer and its arrival at the receiving IED's application layer [50].

When a circuit breaker IED receives a GOOSE message, it can use the information contained in the message to update its internal state and take appropriate action [49]. For example, if a circuit breaker IED receives a GOOSE message indicating that the current flowing through a power line has exceeded a certain threshold, the IED can automatically trip the circuit breaker to interrupt the flow of current and prevent damage to the power system [49].

Protection IEDs will identify a power system fault when it happens and send a trip command to the breaker IED. The associated circuit breakers are tripped by the breaker IED. The appropriate control IEDs will also receive the new circuit breaker status once the circuit breaker trips. [49]

The breaker IED may act as both a subscriber and a publisher simultaneously for GOOSE communication, allowing it to simultaneously receive and transmit GOOSE signals [49]. As a publisher, the breaker IED continuously distributes the status data gathered from the circuit breakers to all other IEDs on the process bus, allowing all subscriber IEDs to receive these messages and obtain real-time information about circuit breaker position status and some other information. The breaker IED, as a subscriber, receives GOOSE control commands from connected publishers and uses these commands to determine its appropriate response. [49]

3.8.3.3 Control and Protection IEDs

In a process bus, both control and protection IEDs play important roles in ensuring the reliability and performance of the power system. The protection IED can use the process bus to communicate with other devices in the system and respond to electrical faults, while the control IED can use the process bus to monitor and adjust the flow of electricity to ensure that the power system is operating safely and efficiently. [40]

Protection IEDs receive SVs from the MUs, and they send/receive data to other IEDs to perform protective functions. For example, if a protection IED detects a short circuit on the power system, it may automatically send GOOSE messages to the breaker IED, which disconnects the affected circuit to prevent damage to the equipment. [40]

A control IED, on the other hand, is primarily focused on monitoring and controlling the flow of electricity through the power system [51]. They use the information to make decisions about how to manage the flow of electricity. For example, a control IED might monitor the load on the power system and adjust the flow of electricity to prevent overloads or other issues.

4 THEORY ON RELIABILITY

This chapter will explain the critical aspect of reliability within power systems, starting with an exploration of the general concept of reliability. Then, it delves into its specific role and importance within the power systems context. Then an explanation of measures that can be taken in order to improve reliability, such as maintenance and monitoring, redundancy, and cybersecurity. Then, there is an explanation of the methodologies for calculating reliability. After this, the chapter introduces a software called Relyence, a tool used specifically for reliability analysis. The chapter concludes with a failure mode analysis.

For system design and operation management, reliability evaluation is crucial. The management of system operation and maintenance can greatly benefit from an accurate reliability prediction. In some situations, such as military situations, reliability is measured because lives are at risk. In other instances, reliability has a more commercial application where it is used for cost analysis. [52]

4.1 Power System Reliability

This chapter is from the specialization project titled "Theoretical Framework and Methodology Assessment for Calculating Reliability in an IEC 61850 Process Bus" [15].

The book "Electric Power Grid: Reliability Evaluation" [52] defines the reliability of an electric power system as "the probability that an electric power system can perform a required function under given conditions for a given time interval." Power system reliability is subdivided into two groups, namely, adequacy and security [53]. The ability of a system to meet operational costs or consumer load demands is referred to as adequacy. Security is related to the system's capacity to react to dynamic or transient disturbances that may arise [53]. Most reliability evaluation techniques are in the system adequacy domain. When calculating reliability in a power system, it is mostly done in the steady state domain, meaning that the investigating system is showing average behavior over a long period of time [52]. In reliability analysis, there are two categories for classifying system states: success states and failure states. In a successful state, the system is capable of doing its intended task, in contrast to a failed state, where it is not. Reliability evaluation is mainly concerned with the system's behavior in a failure condition. The book [52], states that a thorough reliability assessment is indicated by finding the following fundamental indices: the probability of failure, frequency of failure, mean cycle time, mean down time, and mean up time.

The probability of failure is the probability that the system will fail. The frequency of failure is the number of times the system is expected to be in the failure state per year. The system's mean cycle time measures the average time between failures. The mean downtime is the average time spent in the failed state. The mean up time is the average amount of time the system remains in a successful state. [52]

4.1.1 Assessing Reliability in a Process Bus

This chapter is from the specialization project titled "Theoretical Framework and Methodology Assessment for Calculating Reliability in an IEC 61850 Process Bus" [15].

There are various factors that can affect the reliability of a SAS, such as the reliability of the individual components and how they are arranged in the system. According to [54], there are several ways to measure the reliability of a SAS, including mean time to first failure, mean time to failure (MTTF), failure rate, and availability. In the literature review it was also discovered that there were several practical analytical methods for calculating reliability in an Ethernet communication architecture including reliability block diagrams [3] and the reliability function [6].

According to the IEC 61850 standard, "there shall not be a single point of failure that will render the substation inoperable" [33]. However, as the standard does not specify a requirement for redundancy applications, it is up to the substation engineers to choose the ideal level of redundancy. As a result, reliability is one of the most challenging aspects of the digital substation design [55]. Data can be collected to assess past performance or to predict future performance. In general, to predict a system's future behavior, it is necessary to look at past experiences and use data with appropriate reliability models, techniques, and equations. Thus, the quality of a reliability assessment heavily depends on the data available for the investigated system. The idea that the objective of reliability evaluation is to identify the system that offers the highest reliability is a frequent misconception. It's crucial to keep in mind that the objective is to identify the system with the ideal or required reliability, not the system with the highest reliability [52]. One can think of reliability as a restriction within which other parameters can be altered or improved. For instance, a generally acknowledged benchmark for power generation reliability is a loss of load of one day per ten years [52]. Also, reliability can be used for cost optimization. Figure 25 represents the relationship between cost and reliability. The cost of the investment and the cost of failure combine to make up the total cost. The investment cost often increases as more reliability is required. On the other hand, the cost of failures to the consumer typically decreases with more reliable systems. The lowest total cost results in the optimal level of reliability [52].

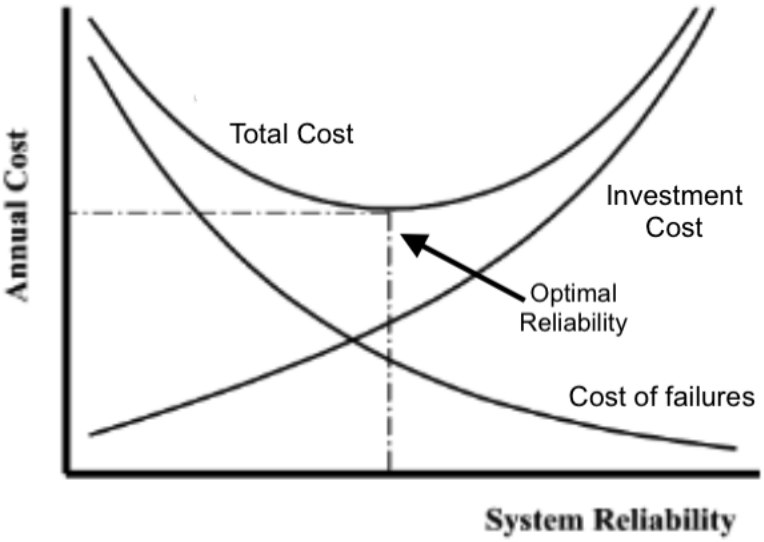


Figure 25: Relationship between cost and reliability [56]

4.2 Improving Reliability

Improving reliability is a continuous effort to minimize the probability of failures and reduce their impact. This chapter will explore various strategies and techniques that can be used to enhance the reliability of a process bus. Generally, there are several standard ways to improve the reliability of a system. For a process bus, these measures may include:

- Redundancy: This can be achieved by having multiple systems or components that can take over in case of failure.
- Maintenance and Monitoring: Regular maintenance and testing of equipment can help identify and address potential issues before they become serious problems. And monitoring systems can help identify and diagnose problems in real-time, allowing for quick response and repair.
- Cyber-security: Implementing strong cybersecurity systems to protect against cyber threats is important to ensure the reliability of the digital substation.

4.2.1 Redundancy

This chapter is from the specialization project titled "Theoretical Framework and Methodology Assessment for Calculating Reliability in an IEC 61850 Process Bus" [15].

The duplication of essential elements or functions within a network is referred to as redundancy [57]. Substation devices must continuously publish important data, and any form of data loss is unacceptable [19]. As the Cigre report "Experience Concerning Availability and Reliability of DSAS" states, "Redundancy for protection devices has been selected by utilities as the key factor to achieving a high level of DSAS reliability" [18]. Generally, there are two ways of improving the reliability of a power system: using more reliable components and adding redundancy. Components are often off-the-shelf devices and may not have the desired reliability requirements, thus, redundancy is more effective [19]. A fully redundant system can continue operating in the event of failure. This lessens network downtime while preventing data loss and potential threats to people's safety and property. The possibility of carrying out maintenance while the network is active is an added benefit [58].

This section is about the different redundancy methods that are optional for the optical fiber network in a process bus. A digital substation is a very time-critical system, which means that the recovery time and frame loss during faults are critical elements since the devices within the system are heavily dependent on correct time synchronization [19]. The IEC 62439-3 standard [55] introduces a redundancy mechanism for Ethernet networks. In table 5, one can see the frame loss and recovery time of the redundancy protocols discussed in the IEC 62439-4 standard [19]. As one can see, the PRP and HSR protocols are of special interest as they offer no frame loss and zero recovery time during faults.

Table 5: Typical recovery times for redundancy protocols [19]

Protocol	Description	Frame Loss	Recovery Time
IP	IP routing	Yes	30 seconds
STP	Spanning Tree Protocol	Yes	20 seconds
RSTP	Rapid Spanning Tree Protocol	Yes	2 seconds
CRP	Cross-network Redundancy Protocol	Yes	1 second
MRP	Media Redundancy Protocol	Yes	200 milliseconds
BRP	Beacon Redundancy Protocol	Yes	8 milliseconds
PRP	Parallel Redundancy Protocol	Yes	0 seconds
HSR	High-availability Seamless Ring	Yes	0 seconds

4.2.1.1 Parallel Redundancy Protocol (PRP)

This chapter is from the specialization project titled "Theoretical Framework and Methodology Assessment for Calculating Reliability in an IEC 61850 Process Bus." [15]

The parallel redundancy protocol is the reference standard for star-topology networks and offers network reliability by simultaneously publishing the identical message to two LANs [4]. The first message is accepted by the receiving device, while the second message is discarded [38]. In PRP networks, the dual-port IEDs are always active and transmitting data packets, ensuring that there is always a redundant communication path available in case of a fault. This eliminates the need for a switch-over and results in zero recovery time delay and no loss of frame rate [4].

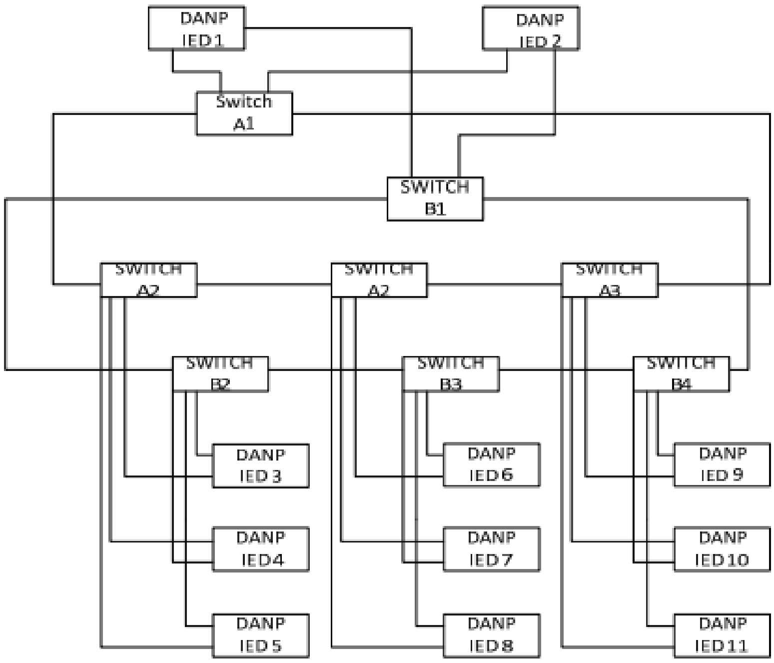


Figure 26: Typical typology of a PRP system [59]

In a PRP network, each node is connected to two independent LAN networks via Doubly Attached Nodes with PRP (DANP) [44]. A DANP is connected to two independent, parallel-operating local area networks (LANs) called LAN A and LAN B, which have the same topology. The same frame is sent over both LANs by the source DANP, and over a certain amount of time, the destination DANP receives it from both LANs consumes the first frame and discards the duplicate. The two LANs are taken to be fail-independent and have no connectivity to one another. In a PRP network, one of the two packets is always available, even during a fault, and there is zero recovery time [4]. Single points of failure, such as a shared power source or a direct connection that fails and brings both networks to a halt, can defeat redundancy [55]. Nodes with a single port can also be connected to PRP networks by using a ”redundancy box” that connects the node to both LANs. Additionally, a PRP network can utilize HSR within the two individual LANs [4]. In figure 27 a process bus utilizing PRP is depicted. In this figure, there are no single points of failure, leading to the assumption that the reliability of this system would be very high.

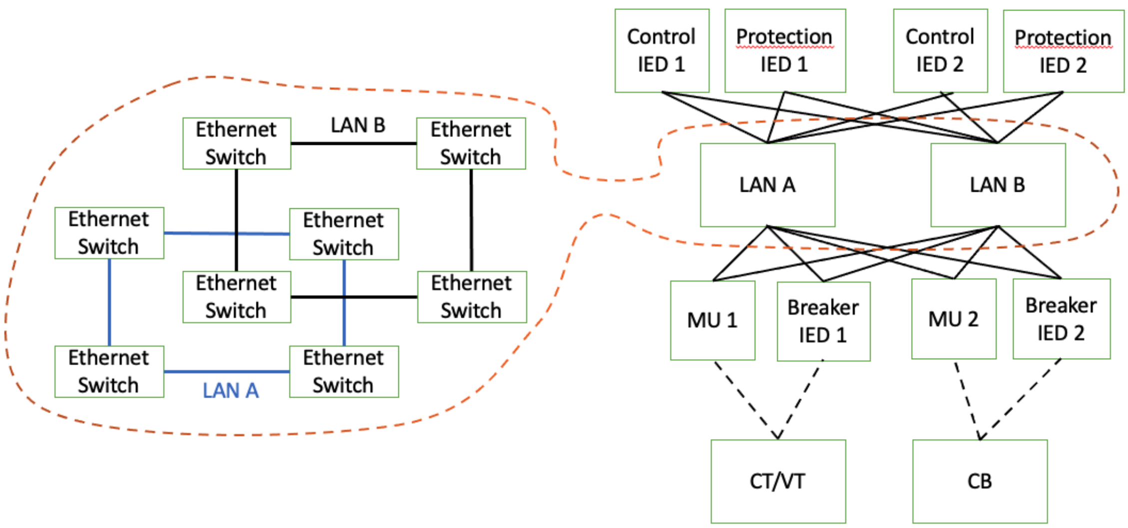


Figure 27: Process bus with PRP

4.2.1.2 High-Availability Seamless Redundancy (HSR)

Devices connected to HSR networks form a ring network. In this ring, devices will transmit information in both directions using Doubly Attached Nodes with HSR (DANH) [44]. After receiving the first transmission, a receiving DANH will discard the second message [38]. HSR protocol requires fewer Ethernet switches, however, according to [4] in HSR, the amount of traffic processed at every node is much greater than in PRP resulting in latency delays. This is because every IED must process every piece of data twice, even if it isn't intended for that specific IED [60]. The larger the size of the HSR network, the greater the delay, as the number of nodes in the network grows [19]. The network's available bandwidth is reduced as a result. Singly attached nodes (SAN), such as maintenance laptops or printers, cannot be added straight into the ring. Since they only have one port and are unable to support DANH, they must be paired with redundancy boxes (RedBoxes) in order to transport message packets in both directions within the ring network. Additionally, a Redbox is required for communication between the HSR process bus and the station bus [61].

Figure 28 shows a typical HSR ring typology. Here, a MU transmits two messages, each carrying the destination MAC address (address for one specific device). When a destination DANH receives two identical messages, it distinguishes one from the other by its sequence number. The destination IED will pass the first message to its upper layers and ignore the second. Appropriate redundancy protocols can automatically rearrange the ring in the event of a break at one point, ensuring that the data will still reach its destination by sending it back in the opposite direction. [19]

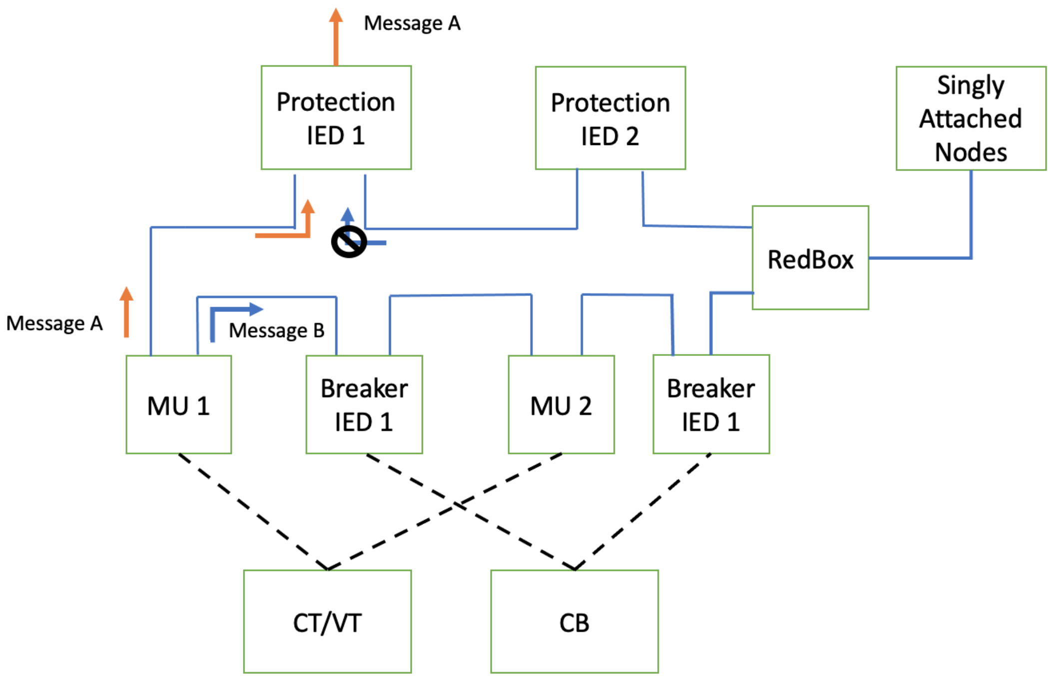


Figure 28: Typical typology of a HSR process bus [59]

4.2.1.3 Partially Redundant Systems and Binomial Distribution

In partially redundant systems, the overall functionality of the system is maintained even if some components fail [62]. An example of this is a ring network topology incorporating HSR. In this case, each switch is connected to two other switches, creating a circular path for data transmission. When all four switches are working correctly, the system operates at its full capacity. However, in the event of a single switch failure, the ring system can still maintain data flow between the remaining three switches because of the duplicated message in the opposite direction.

The binomial distribution is used in the context of partially redundant systems to calculate the probability of the system working under different scenarios, such as when at least a certain number of components has to be operational [62]. It is a probability distribution that models the number of successes (in this case, working components) in a fixed number of trials (total components), given the probability of success for each trial (probability that a component works) [62].

The binomial probability formula is used to calculate the probability of exactly k successes (working components) in n trials (total components), given the probability of success for each trial (probability that a component works). The formula is as follows [46]:

$$P(X = k) = C(n, k) * p^k * q^{(n-k)} \tag{1}$$

Table 6: Probability notation and terms

Symbol	**Definition**
P(X = k)	The probability of obtaining exactly k successes in n trials.
n	The total number of trials (total components).
k	The number of successes (component working) we are interested in.
p	The probability of success in a single trial.
(1-p)	The probability of failure in a single trial.
C(n, k)	The number of combinations of choosing k successes from n trials.

$$C(n, k) = n!/(k! * (n - k)!) \tag{2}$$

4.2.1.4 Comparison Between HSR and PRP

The 2018 IEEE paper "Modeling and Performance Analysis of Data Flow for HSR and PRP under Fault Conditions" [57] compares the advantages and disadvantages between HSR and PRP in a process bus. The paper found that HSR networks can connect to fewer devices than a PRP network and they use more of their available bandwidth. When a single link within the network fails, the HSR network takes longer to transmit data than the PRP network. Overall, the PRP network performs better in terms of device connection and data transmission speed.

4.2.2 Maintenance and Monitoring

The performance and reliability of a substation hinge largely on the effectiveness of its maintenance strategies. Several key factors influence the duration and effectiveness of maintenance and repair activities in a substation system, which include the monitoring system, service agreement, availability of replacement components, and the readiness of skilled personnel.

The industry generally agrees that maintenance strategies for digital substations cannot be the same as those used for conventional substations and must be adjusted to meet their specific requirements [63]. The maintenance strategies depend on various characteristics of the substation, such as the substation's type, size, complexity, reliability, and performance [63].

According to [63], there are three main types of maintenance:

- Preventive maintenance
- Corrective maintenance
- Condition-based maintenance

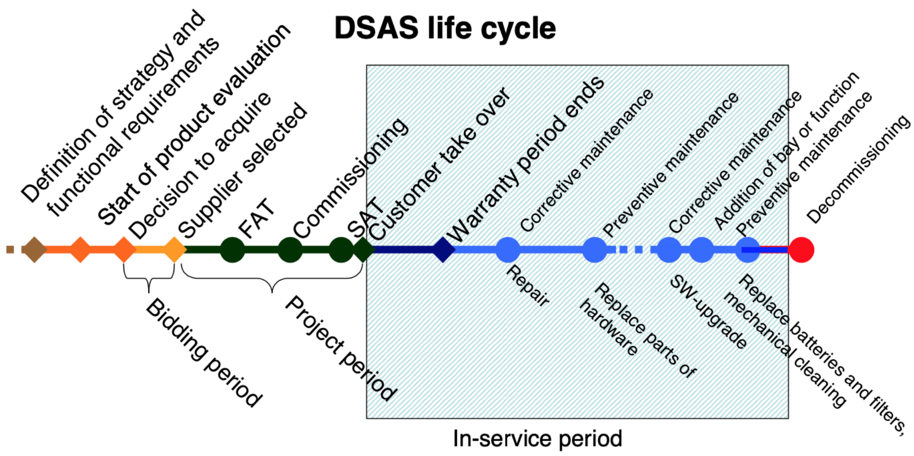


Figure 29: Life cycle of a DSAS [63].

In figure 29 the life cycle of a DSAS is depicted. Once it enters its in-service period, it will be in operation for approximately 20 years [63]. During this phase, the utility may perform maintenance activities such as preventive maintenance (to prevent equipment failure) and corrective maintenance (to repair any equipment that has failed).

Preventive maintenance is done within defined time periods or based on the advice of a manufacturer to verify that equipment is working correctly and within given tolerances. Digital substations rely heavily on solid-state components (non-rotating parts). Due to this, preventive maintenance is often limited to visual inspections and checks of memory buffers. Utilities also program periodic testing of IEDs based on their strategies and vendor recommendations [63]. The frequency of maintenance varies from one year to 12 years, depending on utility strategy or fault statistics.

Corrective maintenance is event-driven and must be done after a malfunction or the detection of a failure of a system or device. Corrective maintenance is often initiated by the substation's self-supervision after detecting a failure or malfunction. Corrective maintenance requires verifying spare part availability and accessibility, maintenance staff skill and training, vendor support if needed, updated documentation and procedures, and tool and software availability [63].

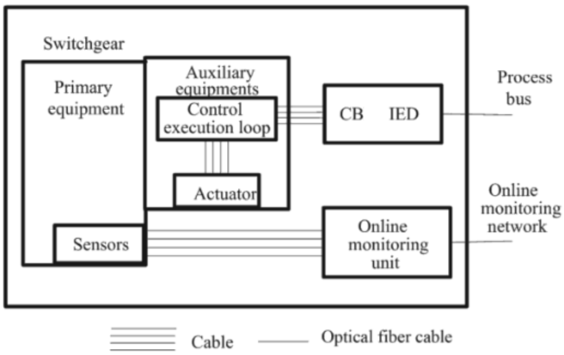
Corrective maintenance, which only takes action after a component fault or breakdown occurs, and preventive maintenance, which is performed at predetermined intervals without considering the real-time condition of the equipment, have both been found to be expensive and inefficient strategies [64]. To address these limitations, the concept of condition-based maintenance (CBM) has emerged, which relies on continuous monitoring of equipment to assess its condition and initiate maintenance actions accordingly.

Condition-based maintenance is done by the digital substation's self-supervision features, which offer the chance to eliminate or minimize breakdowns and extend preventive maintenance intervals. By monitoring equipment conditions and initiating maintenance based on its actual needs, CBM can increase equipment and power availability [64]. This indicates that compared to conventional substations, where faults may go unnoticed for a long time, the mean time to repair is considerably shorter [63].

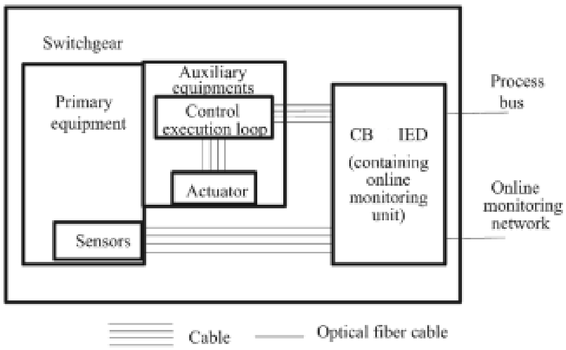
CBM relies on monitoring selected parameters of the equipment to continuously assess its ongoing condition. Maintenance actions are then initiated based on the present needs of the equipment's condition. The self-supervision system expands its monitoring beyond the IEDs, enabling protection and control equipment to evaluate the network's state and guide event-driven targeted maintenance. It ensures the integrity and accuracy of instrument transformers and merging units. [65] It verifies on-load direction and calculates load impedance for availability while also monitoring the performance of the process bus communication channels and all internal and external communication infrastructure. Additionally, self-supervision checks the integrity of the circuit breakers and provides diagnostic functionalities for IEDs, station computers, and gateways. This extensive monitoring can optimize the trade-off between preventive and corrective maintenance, leading to potential cost savings and improved reliability compared to conventional time-based management [65].

Monitoring: Monitoring in digital substations can be referred to as ”online monitoring” because it involves real-time, continuous observation and analysis of the operating conditions of electrical equipment without the need to shut down the system or interrupt the power supply [65]. This is achieved by utilizing IEDs and advanced sensors that continuously collect and process data. Thus, the monitoring of digital substations involves the strategic installation of sensors and IEDs to gather real-time data from both primary and secondary equipment, such as circuit breakers and transformers, allowing for quick response and repair.

As the circuit breaker IED serves as a bridge between the circuit breakers and the secondary equipment, such as protection and control IEDs, the online monitoring unit is often incorporated into the circuit breaker IED, or it can be a separate unit [65]. This is depicted in figure 30.



(a) Separate online monitoring



(b) Integrated online monitoring

Figure 30: Circuit breaker IED online monitoring [65]

Online monitoring is achieved through a variety of advanced functions like one-touch sequence control, source-end maintenance, intelligent alarm and fault comprehensive analysis, and load optimization control. These functions automate various tasks, reduce workload, and ensure the reliable operation of the substation [65]:

One-Touch Sequence Control [65]: This is a standard function of digital substations that automates various operation tasks according to a predefined sequence of operations. This means that multiple control steps can be executed at once with just one command, improving efficiency and reducing the chance of human error. Before each step, the sequence control system automatically checks against anti-misoperation lockout logic to ensure the operations are safe and correct.

Source-End Maintenance [65]: This involves providing a variety of self-describing configuration parameters from the substation, which serve as the data source for a centralized control system. Standard configuration files, including those detailing the main wiring diagram and network topology, can be generated at the substation. This approach reduces the maintenance workload and ensures consistent system models and data across all substations and main stations.

Intelligent Alarm and Fault Comprehensive Analysis [65]: This system analyzes alarm data and combines it with a knowledge base for fault processing. To give a thorough study of errors, it merges multiple data sources, including alarm data, fault reports, and waveform recordings. This provides a wide range of failure analysis functions, from fault diagnosis and location to equipment operation monitoring.

Optimization Control of Intelligent Load [65]: A Voltage Quality Control (VQC) module that is built into the substation controller software is used for this. VQC ensures that the voltage levels in the substation stay within a specified range to maintain high-quality, stable, and efficient power delivery. The VQC module can adjust the voltage levels by controlling various equipment in the substation based on real-time data and setting target values.

4.2.3 Cybersecurity

This chapter is based on information from the article "Cyber-security in Substation Automation Systems" [66].

The use of IEC 61850 standard networks reduces costs but also introduces new digital vulnerabilities, as information packets can be easily intercepted, altered, or even replaced. Cyber-security intrusions could disrupt the normal functioning of a digital substation, causing outages or malfunctions that would negatively impact its reliability. For example, unauthorized access, manipulation of data, or malicious software could cause malfunctions in the control equipment, resulting in incorrect measurements, miscommunication, or even system shutdown.

In recognition of these challenges, the IEC TC57 Working Group 15 has been developing cybersecurity standards for power system communications. The IEC 62351-6 standard specifies security mechanisms for IEC 61850 communications, recommending the use of cryptography algorithms for device protection. The challenge lies in implementing these algorithms on substation devices with limited memory and processing power. The standard recommends a combined approach for message authentication and integrity in power system communications. This approach involves the use of Message Authentication Codes (MACs), which are computed using the Secure Hash Algorithm (SHA) to ensure the integrity of the message. MACs are short pieces of information that confirm the message's authenticity and integrity, as they are derived from both the message and a shared secret key. SHA is a family of cryptographic hash functions. These functions take an input (in this case, the message) and return a fixed-size string of bytes, with even a minor change in input producing a significantly different output. To further enhance security, the computed MAC is digitally signed using the RSA (Rivest, Shamir, and Adleman) public key. This digital signature process provides an additional layer of authentication, confirming that the message was created by a known sender and has not been altered during transmission.

However, this security method has some limitations, primarily due to its use of RSA (Rivest, Shamir, and Adleman) digital signatures. RSA is a public-key cryptosystem used for data encryption and digital signatures. However, it requires significant computational resources, especially for key lengths considered secure in modern systems. The text mentions that even with high-end processors in substation equipment, some RSA signatures can't be computed and verified within the strict time constraints required by the GOOSE protocol. This is because RSA operations involve large mathematical computations, which are resource-intensive and thus slow.

The time taken to compute and verify RSA digital signatures can therefore become a bottleneck, slowing down communication and making this method suboptimal for scenarios requiring near real-time responses, such as digital substation systems.

The text suggests the implementation of Elliptic Curve Digital Signature Algorithms (ECDSA) in dedicated crypto cores. ECDSA is a public-key cryptography method that offers similar levels of security to RSA but with shorter keys, making computations quicker and less resource-intensive. This could provide the necessary latency times required by IEC 61850 for fast messages.

4.3 Calculating Reliability

In this chapter, methods for calculating reliability metrics will be presented.

4.3.1 Exponential Distribution and Failure Rate

Failure rate (λ), denoted in equation 3 [67], is one of the most widely utilized reliability assessment methods. The failure rate is the frequency at which failures occur, the number of failures per unit time [5]. The exponential distribution is a statistical model that uses independent intervals with constant failure rates to explain the likelihood of an event occurring over a continuous period of time [68]. In reliability analysis, the exponential distribution is a commonly chosen model due to its simplicity and the assumption of a constant failure rate, which is often a reasonable approximation for certain stages of a system's lifecycle. The concept of a constant failure rate arises from the Bathtub Curve, a graphical representation of the failure rates over time for a typical system or product[5].

$$\lambda = \frac{1}{MTBF} \tag{3}$$

Figure 31 shows the typical failure rate of an electrical component. The figure is divided into three distinct regions. Region 1, the start-up phase, is characterized by a higher failure rate due to manufacturing mistakes or improper design. Region 2, the useful life period, is characterized by a constant failure rate. Region 3, the wear-out phase, is characterized by a high failure rate brought on by aging [69]. For many complex systems like digital substations, the majority of their operational life is spent in the useful life period, where the failure rate is approximately constant.

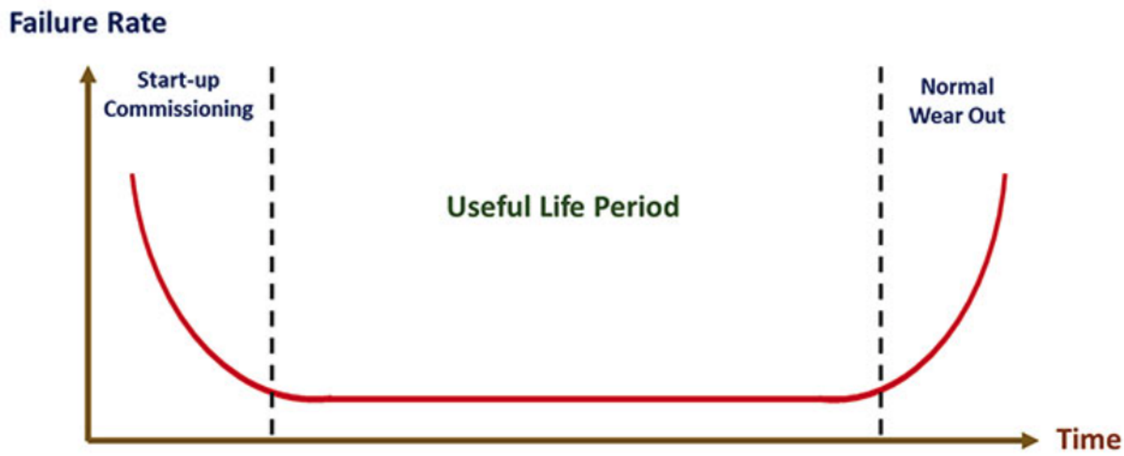


Figure 31: Bathtub Curve [69]

The exponential distribution is therefore a useful model because it provides a good approximation for the behavior of systems in this useful life period. To elaborate further, the exponential distribution assumes that failures occur independently and randomly over time due to its inherent memoryless property. This means that the system does not "remember" when the last event occurred. The chance of failure in the next unit of time is always the same, regardless of how long it has been since the last failure [68]. The constant failure rate assumption simplifies calculations and allows for straightforward reliability predictions. In other words, the chance of a system failure in the next instant does not depend on how long it has already been operating [68].

However, this model and the assumption of a constant failure rate will not accurately represent the system during the start-up phase or wear-out phase, when failure rates are not constant. Hence, while the exponential distribution is a good starting point, it's important to remember its limitations and consider more complex models like the Weibull distribution which will be explained in chapter 4.4.1.

4.3.2 The Hazard Rate Function

The hazard rate provides the rate at which a component or system fails at a specific time t, given that it has survived up to that time. In other words, it represents the instantaneous probability of failure at a specific time, given that the system has survived up to that time. The hazard rate can vary over time, indicating changes in the risk or failure intensity [52]. For example, for a component within a substation, the hazard rate would indicate the likelihood of a fault happening at any given moment, considering the time it has been in operation. In contrast, the failure rate provides an average measure of failure occurrence and assumes a constant failure rate over time. The failure rate would indicate, on average, how many components within the substation would be expected to fail over a certain period.

The hazard rate at time t, denoted by $h(t)$, is calculated as the probability density function, divided by the survival function [52].

$$h(t) = \frac{f(t)}{S(t)} \tag{4}$$

Where:

- $h(t)$ represents the hazard rate at time t.
- f(t) represents the probability density function (PDF) of the event at time t.
- S(t) represents the survival function and gives the probability of a component or system surviving beyond a specific time point [52].

Probability Density Function: The PDF provides a mathematical representation of how failure events are distributed across a time interval. It allows for an understanding of the shape, concentration, and behavior of the failure distribution, providing insights into the likelihood and patterns of failure occurrences [70].

4.3.3 The Reliability Function

The Reliability Function can be defined using the exponential distribution, assuming that the system or component under study has a constant failure rate over time. The reliability function gives the probability of a system not failing over a specified time period t [52].

The reliability function is given in equation 5. The function shows how reliability decreases over time and gives a long-term perspective, illustrating the overall likelihood of a system operating without failure up to a specific time. It depicts the system's survival over time, taking into account the constant failure rate [5].

$$R(t) = e^{-\lambda_i * t} \tag{5}$$

λ	=	Failure rate
t	=	Period under consideration

Equation 5 shows that as time (t) increases, $e^{(-\lambda * t)}$ decreases. In other words, the reliability of the system or the probability that the system will perform without failure up to time t decreases as time progresses. However, the rate at which these failures are expected to occur remains constant.

This is the hallmark of the exponential distribution: while the probability of failure decreases over time, the failure rate remains constant. This constancy is because, under the exponential distribution assumption, the system does not have a "memory" of the past. The chance of failure in the next unit of time is always the same, no matter how long the system has already been running without failure [68].

4.3.4 Reliability Block Diagram

Reliability block diagrams (RBDs) are often used when calculating the reliability of a system because they provide a simple, graphical representation of the components of the system and the ways in which they can fail. This can make it easier to identify potential problem areas and evaluate the overall reliability of the system [52].

Additionally, RBDs can provide more detailed and accurate predictions of system reliability than other methods, such as fault trees. This is because RBDs take into account the dependencies between different components of the system, as well as the likelihood of each component failing. By contrast, fault trees are limited in their ability to consider the interactions between different components and may not provide as accurate a prediction of system reliability [52].

A reliability block diagram demonstrates how a system fails as a result of component failure. Each block represents a single device, the only two states of which are working and failing. By joining blocks in either series or parallel, the system reliability block diagram is created [52]. A single component failure in a series connection will result in system failure. Failure of all components in a parallel connection will result in system failure [52]. According to [5] other reliability evaluation techniques, such as fault trees, cut sets, and path sets, all have different layouts but may produce the same outcome as a reliability block diagram.

4.3.4.1 Series Connection

Two components are in series if the failure of either one will cause the system to fail. An example of a series connection is shown in figure 32

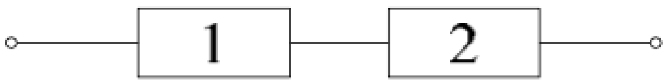


Figure 32: Series connection [5]

The reliability function of a series-connected system is as follows [5]:

$$R_s(t) = R_1(t)R_2(t) = e^{-\lambda_1 t}e^{-\lambda_2 t} = e^{-(\lambda_1+\lambda_2)t} \tag{6}$$

4.3.4.2 Parallel Connection

Two components are in parallel if both must fail for the system to fail. An example of a parallel connection is shown in figure 33

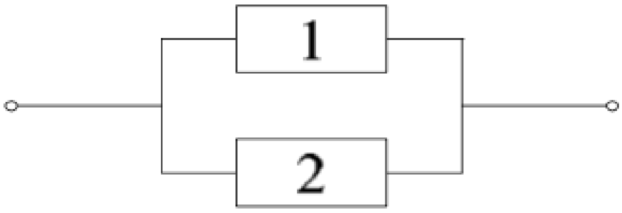


Figure 33: Parallel connection [5].

The reliability function of a parallel-connected system is as follows [5]:

$$\begin{aligned} R_p(t) &= R_1(t) + R_2(t) - R_1(t)R_2(t) \\ &= e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t} \end{aligned} \tag{7}$$

4.3.5 Mean Time To Failure (MTTF)

One of the most commonly used reliability measurement methods is mean time to failure (MTTF). MTTF provides the typical amount of time that an object works without failure [3]. In general, a system with a high MTTF is considered more reliable than one with a low MTTF, as it is expected to operate for a longer period of time before experiencing a failure. Every piece of equipment will eventually break down, but using MTTF one can prepare for this and take action beforehand. Knowing how to calculate MTTF will allow one to replace speculation with trustworthy, actual data for analysis. This will therefore result in better decisions on maintenance, planning, and repairs [71]. The same idea is frequently represented as the mean up time (MUT) in order to avoid confusion. The equations for MTTF are taken from [3].

In relation to the failure rate function, the mean time to failure is given as:

$$\text{MTTF} = \int_0^{+\infty} R(t)dt \tag{8}$$

As the failure rate function is constant during the useful life period, MTTF is given as:

$$\text{MTTF} = \frac{1}{\lambda}. \tag{9}$$

To calculate the MTTF of a series-connected system, such as in figure 32, the following equation can be used:

$$MTTF_s = \frac{1}{\lambda_1 + \lambda_2} = \frac{MTTF_1 \cdot MTTF_2}{MTTF_1 + MTTF_2} \tag{10}$$

In a two-component parallel system, such as that shown in figure 33, MTTF can be calculated using the following equation:

$$\begin{aligned} MTTF_p &= \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} \\ &= MTTF_1 + MTTF_2 - \frac{MTTF_1 \cdot MTTF_2}{MTTF_1 + MTTF_2} \end{aligned} \tag{11}$$

Here, MTBF is the total time available for system operation (MTBF = MTTF + MTTR), and MTTR is the average time taken to repair the system after a failure occurs.

4.3.6 Mean Time Between Failure (MTBF)

Mean Time Between Failures (MTBF) refers to the average amount of time that passes between one system breakdown and the next. The calculation of MTBF is rather straightforward. It is achieved by dividing the total operational hours of an asset by the number of failures experienced during that period. It's essential to note that this calculation only takes into account unplanned maintenance, excluding scheduled maintenance like inspections, recalibrations, or preventive parts replacements [72].

$$MTBF = \frac{\text{Number of operational hours}}{\text{Number of failures}} \tag{12}$$

4.3.7 Mean Time To Repair (MTTR)

Mean Time to Repair (MTTR) represents the average time taken to repair a failed component and restore it to full functionality [3]. Lower MTTR values are generally considered desirable, as they indicate a more efficient and faster repair process, which contributes to higher system reliability. In contrast, higher MTTR values indicate longer periods of downtime, leading to reduced system availability, increased costs, and potential disruptions in operations [3].

To calculate MTTR, one can use the following formula [3]:

$$MTTR = \frac{\text{Total Time Spent on Repairs}}{\text{Number of Repairs}} \tag{13}$$

MTTR provides insights into the expected downtime of the system or component. This helps in predicting the total time a system is expected to be out of service, which can be crucial for planning and optimizing maintenance schedules. MTTR directly impacts the availability of a system. The quicker a system can be repaired and made operational, the higher its availability will be. Including MTTR in your analysis allows you to assess the effectiveness of redundancy and fault tolerance in your system. Identifying components with high MTTR values and significant impacts on system performance can help you design additional redundancy or improve component reliability to reduce the risk of system failure [23].

4.3.8 Availability

In contrast to the reliability function where one measures the frequency of failure, availability is a measurement of the percentage of time a device is operational within a year. For example, if a device has a 90% guaranteed availability, the annual downtime could be as much as 876 hours [73].

In a series-connected system, availability is assessed by the use of equation 14 [5].

$$A_s = A_1 * A_2 \tag{14}$$

In a parallel-connected system, availability is assessed by the use of equation 15 [5].

$$A_P = A_1 + A_2 - A_1 * A_2 \tag{15}$$

Availability can also be expressed using MTBF and MTTR [5]:

$$A = \frac{MTBF}{MTBF + MTTR} \tag{16}$$

4.3.9 Annual Downtime

Annual downtime is a measure of the total amount of time that a system is unable to perform its intended function over the course of a year.

The relationship between availability and annual downtime is inverse. In other words, as availability increases, annual downtime decreases. This is because a system with a higher availability is able to perform its intended function more often, and therefore experiences less downtime [3].

Annual downtime can be calculated using the availability of a system [3].

$$\text{Annual downtime} = (1 - \text{availability}) * 8760 \tag{17}$$

In this equation, annual downtime is expressed in hours, and availability is expressed as a decimal. 8760 is the number of hours in a year.

4.4 Other Reliability Assessment and Probability Distribution Methods

In this chapter, other reliability assessment methods than reliability block diagrams are presented along with a probability distribution alternative to the exponential distribution.

4.4.1 Weibull Distribution

Weibull analysis is a form of probability distribution used to predict failure and reliability trends by analyzing life data such as times of product failures during use. The Weibull analysis allows for the prediction of reliability performance based on data captured during actual use, enabling forecasts of a product's life, failure rate, reliability and mean life. The data needed to perform a Weibull analysis includes life data such as times of product failures during use and associated operating and environmental conditions. From the sample data graphs can be generated, and future performance can be analyzed and predicted. [74]

In Weibull distribution, the scale parameter (represented by the symbol β) and shape parameter (represented by the symbol η) are used to describe the distribution of failure times in a system. The scale parameter determines the time scale of the distribution, while the shape parameter describes the rate at which the failure rate changes over time. [75]

The relationship between the scale and shape parameters and the failure rate can be summarized as follows:

The scale parameter β is related to the average lifetime of the system. A larger value of β indicates a longer average lifetime of the system. The shape parameter η is related to the shape of the failure rate curve. A value of η greater than 1 indicates an increasing failure rate over time, a value of η equal to 1 indicates a constant failure rate over time (i.e., the system has a "memoryless" failure rate), and a value of η less than 1 indicates a decreasing failure rate over time. [75]

Therefore, in general, as the scale parameter β increases, the failure rate of the system will decrease. Meanwhile, the shape parameter η can affect the failure rate in a more complex way, depending on its value relative to 1. [75]

4.4.2 Markov Chain

This section is based on information from the book "Electric Power Grid, Reliability Evaluation" [52]. A Markov chain is a mathematical model that undergoes transitions from one state to another within a finite or countable number of possible states. A Markov chain is a model used to predict a future state based on the current state, without any consideration for how we arrived at the current state. Each transition in a Markov chain is determined by a set of probabilities that depend solely on the current state, not on the history of past states. This property, often referred to as the Markov Property or memorylessness, is a defining characteristic of Markov chains. In reliability analysis, Markov chains can model the reliability of systems by representing the various possible states of a system (such as operational, partially operational, or failed) and the probabilities of transitioning between these states. Markov chains are especially adept at modeling the transition of systems from one state to another. In a substation, the equipment could be in various states, not just fully operational or failed. For example, a component might be in a degraded state where it is operating, but not at full capacity. Markov chains can effectively model these state transitions and give a more accurate picture of the system's reliability.

Markov chains model the transitions between states using probabilities. Each state in the chain has a certain probability of moving to each of the other states. There are two primary ways to represent the states and probabilities of transitioning from one state to another of a system in a Markov chain. These two ways are through a transition probability matrix and a state transition diagram. The transition probability matrix is a square matrix where each entry represents the probability of transitioning from one state to another.

To illustrate an example of the transition probability matrix an example of a substation with three possible states is considered. Here, the substation can be in the following states:

- Fully Operational (FO)
- Partially Operational (PO)
- Non-Operational (NO)

The transition probability matrix for this Markov chain might look something like table 7.

Table 7: Transition probability matrix

	FO	PO	NO
FO	0.9	0.1	0.0
PO	0.2	0.7	0.1
NO	0.0	0.6	0.4

Here, each row represents the current state of the substation, and each column represents the next possible state. The numbers in each cell represent the probability of transitioning from the current state to the next state.

For example, if the substation is fully operational, there is a 90% chance that it will stay fully operational and a 10% chance that it will become partially operational in the next time step. There's a 0% chance it will go directly from fully operational to non-operational in one step.

On the other hand, a state transition diagram is a visual representation of the various states in a system and the probabilities of transitioning from one state to another. The diagram consists of nodes and arrows, where each node represents a state and each edge represents the transition from one state to another. Nodes are the points or dots in the diagram. Each node represents a possible state in the system. Arrows are the lines or paths connecting the nodes. Each arrow represents a possible transition from one state to another. An arrow is accompanied by a number, which represents the probability of that transition. Figure 34 illustrates a state-transition diagram of a three-state system. Here, the probability of going from state 1 to state 2 is 50%, and the probability of the system staying at state 1 is 25%.

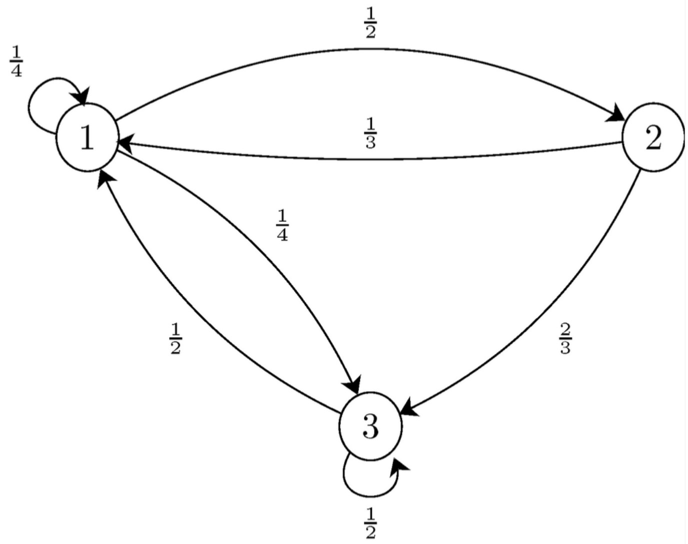


Figure 34: State-transition diagram of a three-state system. [52]

Essentially, Markov chains use probabilities to simulate the transitions between states over time. Each step in the simulation follows the probabilities in the transition probability matrix or the state-transition diagram to decide the next state. By running this simulation over many steps, one can get a sense of the long-term behavior of the system.

4.4.3 Monte Carlo Simulation

Monte Carlo simulation can be applied when the system or model under investigation is deemed too complex to be solved by an analytical approach. In general, Monte Carlo modeling can simulate any system that exhibits any kind of random behavior. When evaluating a system's reliability, Monte Carlo simulation is used to determine how the system's reliability is affected by the unpredictable failures of its components [52].

At the core of a Monte Carlo simulation is the concept of random number generation, which plays a role in simulating system states. The probability distributions of a system, which theoretically reflect the behavior of its individual components, are obtained using these random numbers. In a system with multiple independent components, a system's reliability can be examined by simulating the behavior of each component separately and observing the overall system performance.

The book "Electric Power Grid, Reliability Evaluation" [52] explains the basic principles of Monte Carlo simulation in power systems, using an example of a system with two parallel components. Through Monte Carlo simulation, a mathematical model of this system can generate hypothetical historical data, which in turn can be used to estimate system reliability. This history of component failures and repairs is called a realization of the stochastic process.

At the start of the simulation, component 1 is considered functional. A random number, along with the component's uptime probability distribution, is used to determine when this component will fail. Likewise, a random number helps generate a probable duration for the component's repair time. The process is repeated for component 2. Overlap in failure durations between the two components represents periods of system failure, given that both components are needed for the system to function successfully. This simulation process can be repeated to create multiple realizations of the system's history, from which reliability measures can be derived. This process highlights the essence of Monte Carlo simulation, which involves creating realizations of a system's stochastic process and extracting reliability parameters from these realizations. [52]

4.5 Non-Repairable Vs. Repairable Systems

Non-repairable and repairable systems are two classifications of systems based on how they respond to failures. These classifications have significant implications for system reliability and performance measurements, particularly those related to MTTF and MTBF.

Non-repairable Systems: As the name implies, these are systems that, once they fail, are not repaired but rather replaced. The most common steady-state measure for non-repairable systems is the MTTF, which represents the average time that the system is expected to operate without failure. For non-repairable systems, the MTTF is a critical measure because it helps estimate the expected operational lifetime of the system. After a failure, the system is replaced, and a new operational life begins. The results from a reliability analysis of non-repairable systems will primarily provide an understanding of the system's lifespan under certain conditions. For instance, the analysis might reveal that a specific type of lightbulb, on average, functions for 1,000 hours before failure.

Repairable Systems: These are systems that are repaired and returned to service when they fail. The steady-state measure for repairable systems is the MTBF, which measures the average time between failures. MTBF includes the operational time as well as repair time, reflecting the actual time between failures, regardless of whether the system is operating or under repair. Since these systems are repaired, not replaced, upon failure, their overall operational lifespan can extend significantly beyond the MTBF, assuming repairs are effective. Reliability analysis for repairable systems provides insights not just into the expected operational lifespan of components (like with MTTF), but also into the frequency and duration of downtime for repairs. For example, the analysis might reveal that a specific type of industrial machinery, on average, operates 5,000 hours between failures, with a typical repair time of 10 hours.

Time-Based Metrics Relevant for Non-Repairable and Repairable systems: In non-repairable systems, the hazard rate is equal to the failure rate, and the reliability is equal to the availability, this is due to the absence of repair activities. While in repairable systems, the hazard rate and failure rate will differ because the hazard rate considers both the occurrence of failures and the repair activities, while the failure rate only represents the rate of failures without repair. Typically, the repair process will make the hazard rate fluctuate as it provides an opportunity to restore the system's functionality. Additionally, the presence of repair activities will have the same effect on the availability, as it also considers the time required for repair and restoration. As a result, the reliability and availability differ in repairable systems.

4.6 Relyence Software

Relyence is a computer program that provides reliability analysis tools for complex systems. It offers several different assessment tools such as Reliability Block Diagrams (RBD), reliability prediction, and Failure Mode and Effects Analysis (FMEA). The program costs money and for this study, it has been paid for an analysis using RBD.

There are several advantages to using a computer simulation to calculate the reliability of a digital substation, including accuracy, scalability, and visualization. Relyence can provide a more accurate and detailed prediction of the reliability of a digital substation compared to analytical methods, as it can take into account a wide range of factors and variables that may affect the reliability of the digital substation [76], such as the MTTR. A computer simulation is also more flexible and adaptable than analytical methods, as it can be easily modified or updated to reflect changes in the design or operating conditions of the digital substation.

In addition, a computer simulation can be easily scaled up or down, making it possible for the simulation to provide accurate predictions of the reliability of the digital substation for a variety of operating conditions and configurations [77].

4.6.1 Reliability Block Diagram in Relyence

Relyence's RBD is a powerful tool that combines an intuitive diagramming interface with a robust calculation engine. This software suite provides detailed system modeling and comprehensive reliability and availability metrics, making it a valuable asset for any reliability professional[78].

The software's interface is designed for easy construction and editing of block diagrams, with abilities that automatically organize diagrams for optimal readability and clarity. Users can define the properties of system components, including redundancy configurations and repair distribution models [78].

The calculation engine of Relyence RBD can compute a broad set of reliability and availability metrics. Depending on the complexity of the system model, the software can employ analytical techniques, simulations, or a combination of both to ensure efficient and accurate computation. Results are displayed in both tabular and graphical formats and can be exported to various formats, such as PDF and Excel, for further analysis.

One of the standout features of Relyence RBD is its support for analyzing the impact of redundancy in system configurations. This allows for detailed "What-If?" calculations and the evaluation of various design alternatives, offering invaluable insights for optimizing system reliability.

4.6.1.1 Building and Analyzing RBDs Using Relyence

Relyence RBD software is designed to make the RBD analysis process easier and more efficient. To perform RBD analysis using Relyence, the steps presented in figure 35 are required:

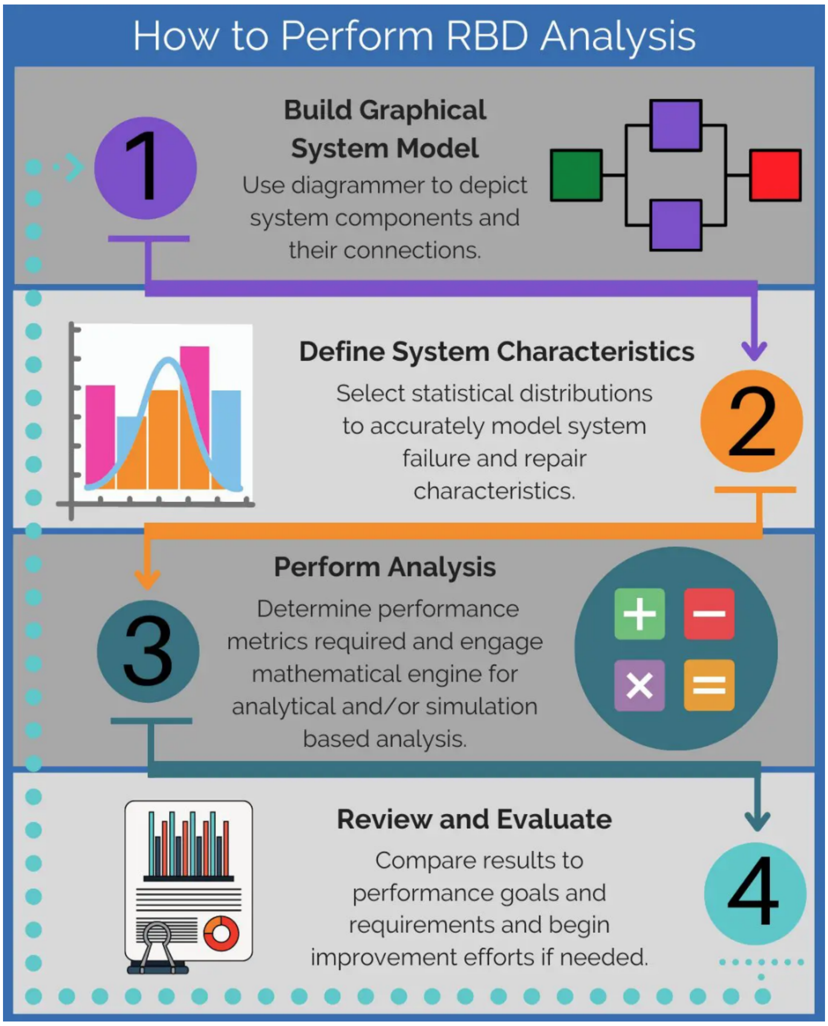


Figure 35: How to perform RBD analysis in Relyence [79]

The first step is building a graphical system model, which involves using the software's diagramming tool to visually represent the components of the process bus and their relationships. An example of this is shown in figure 36.

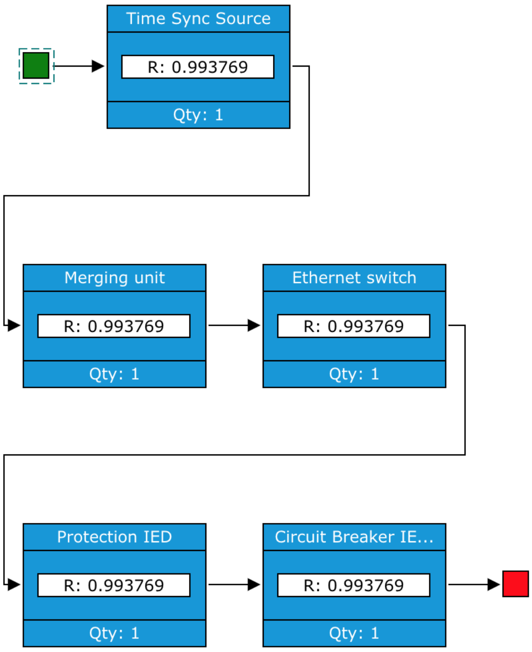


Figure 36: Reliability block diagram in Relyence

The next step is to define system properties: This means defining the failure and repair-related information for each component. This information can be obtained from various sources, like scientific journals.

In figure 37 the properties window in Relyence is shown. This is where one can add the component parameters, such as failure rate and MTTR.

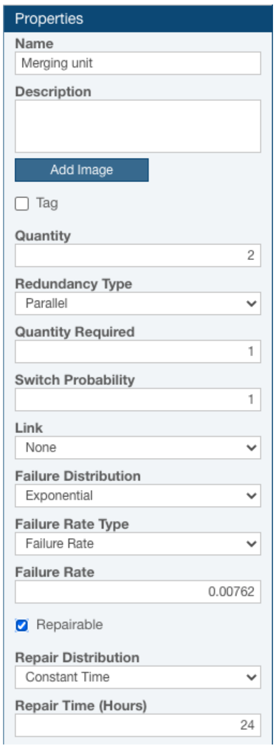


Figure 37: Properties window in Relyence

Next, perform analysis This means that once the calculation inputs are defined, Relyence's cal-

Example

Diagram Name	PRP Test	**MTTF**	309988.258546
Calculation Method	Simulated	**MTBF**	∞
		MTTR	∞
		Steady State Availability	0.000000

TIME-BASED RESULTS

Time	Reliability	Failure Rate	Availability	Total Downtime
0	1.000000	0.040024	1.000000	0.000000
3504	0.986900	0.038108	0.986900	23.559371
7008	0.974100	0.035103	0.974100	92.283272
10512	0.963200	0.017764	0.963200	204.297898
14016	0.952700	0.028721	0.952700	352.005943
17520	0.942000	0.033881	0.942000	535.254399
21024	0.931900	0.025695	0.931900	758.336754
24528	0.921800	0.028448	0.921800	1015.059307
28032	0.912400	0.028740	0.912400	1305.650524
31536	0.903100	0.039118	0.903100	1627.790262
35040	0.892300	0.039591	0.892300	1985.681257
38544	0.880500	0.033659	0.880500	2384.990529
42048	0.870400	0.020965	0.870400	2822.999178
45552	0.860100	0.027838	0.860100	3296.304660
49056	0.850600	0.026810	0.850600	3803.446011
52560	0.842100	0.028432	0.842100	4342.523014
56064	0.832700	0.028753	0.832700	4913.118306
59568	0.824100	0.024907	0.824100	5514.618552
63072	0.813900	0.048985	0.813900	6146.400713
66576	0.803100	0.029811	0.803100	6818.955785
70080	0.794700	0.032991	0.794700	7521.905189
73584	0.785200	0.031940	0.785200	8258.627110
77088	0.775500	0.044075	0.775500	9026.900568
80592	0.767300	0.031200	0.767300	9827.846591
84096	0.759500	0.031520	0.759500	10655.510774
87600	0.748700	0.035015	0.748700	11518.298349
91104	0.742600	0.023035	0.742600	12409.322126
94608	0.734000	0.034164	0.734000	13326.885729
98112	0.727200	0.026655	0.727200	14271.043961

Figure 38: Relyence example report

culation engine is used to compute the reliability and availability metrics. Depending on the complexity of the system model, RBDs may be analyzed using analytical techniques, simulation, or a combination of the two.

Lastly, the results are shown in a report, which automatically appears after the calculations are done. A sample of such a report is shown in figure 38. This report can also be converted to an Excel file, which will make it easier to review and evaluate using graphs.

4.6.2 Steady-State Vs. Time-Based Analysis

In Relyence, both steady-state metrics and time-based metrics are used, but they offer different perspectives on the system's reliability.

A steady-state reliability analysis assumes that the system is in a constant, unchanging state. It provides a snapshot of the system's reliability at a specific point in time, ignoring any changes that may occur over time. This assumes that the system has been operating for a sufficiently long period of time such that its transient behavior (short-term effects of initial conditions) has decayed and the system is operating in a stable manner. Steady-state metrics include in Relyence are MTBF, MTTF, and steady-state availability.

While on the other hand, time-based reliability analysis considers how the reliability of a system changes over time, taking into account events such as aging, usage, and maintenance that can affect the system's performance. These metrics consider the reliability of a system over a specific period of time, from the moment it starts operating ($t = 0$) until a certain end time ($t = T$). The time-based metrics included in Relyence are as follows:

- Reliability

- Unreliability
- Failure rate
- Equivalent failure rate
- Availability
- Unavailability
- Mean availability
- Mean unavailability
- Hazard rate
- Failure frequency
- Total downtime
- Expected number of failures

Put simply, steady-state metrics give a long-term average view of system reliability, while time-based metrics provide a more dynamic picture, reflecting the system's reliability over specific time intervals. Both types are important and complementary for a complete reliability assessment.

4.7 Failure Modes in Digital Substations

A failure mode analysis is fundamental to this thesis, providing insights into potential system vulnerabilities. Given the fact that the identification of these failure modes is primarily based on an extensive literature review, this analysis will be presented entirely within this "Theory on Reliability" chapter. This approach was chosen to maintain the structural integrity of the thesis, ensuring a smooth and logical flow of information. Encapsulating the entire failure modes analysis within this section also allows for a more focused and coherent explanation of the topic.

The process bus architecture offers several advantages over the conventional substation design, such as improved interoperability. However, it also introduces some unique failure modes that are not present in conventional substations. Because the process bus relies on digital communication, it is vulnerable to failures in the communication network, which may cause delays, packet loss, and network congestion. These failure effects can lead to inaccurate measurements, delays in protection operations, and loss of control signals, which can affect the reliability and safety of the substation. This study will focus on issues related to the process bus, such as communication failures and failures in the components of the process bus. The failure modes are divided into the following categories: component failures and communication failures. But before mentioning any specific failure modes there is a need for an overview of digital substation failures.

4.7.1 Understanding Component Failures in Digital Substations: An Overview

Component failure in the process bus refers to any malfunction or breakdown in the individual hardware or software components that make up the bus. Hardware failures include problems with physical components such as the merging unit, Ethernet switch, protection IED, control IED, circuit breaker IED, and fiber optic wires. Software failures refer to the errors, bugs, or malfunctions that occur in computer software programs of the IEDs, resulting in the software not functioning as intended.

The survey in the Cigre paper "Experience concerning availability and reliability of DSAS" [80] revealed that digital substations generally have high availability, with the majority of respondents reporting availability rates above 99%. However, a significant number of respondents also reported reliability issues, with the devices suffering most of the faults being protection IEDs, control IEDs, and fiber optic wires. Table 8 displays the results from the survey conducted in the report on the most common failures in digital substations.

Table 8: Most common component failures in DSAS [80].

Component	Percentage of failures
Control IED	26.9%
Fiber optic wires	22.6%
Protection IED	14.4%
Ethernet switch	14.1%

4.7.1.1 IED Failures

IEDs are responsible for collecting data, running commands, and controlling the circuit breaker. Due to this, failures in any of these components can have severe impacts on the operation of the substation. According to [9], there are two types of failures that can occur in IEDs: revealed failures and hidden failures. Revealed failures occur when an IED fails to collect data from the electrical switchgear or to transfer commands received from HMIs to the interface devices. With multi-functional IEDs, a single failure can cause all functions provided to the system to become disabled. Hidden failures, on the other hand, remain hidden during normal operation of the power system and are only exposed when failures occur. These failures can cause the substation to either not perform its intended operation when it is needed or to perform an operation when it is not needed.

Protection IED failures are mostly hidden failures, meaning that a failure in the power system can occur, but the IED either cannot detect it or cannot respond to it [9]. To prevent hidden failures, IEDs usually integrate self-testing and diagnostics to help with preventive failure detection.

The merging unit gathers multiple analog inputs from switchgear equipment and produces time-synchronized digital outputs that transmit data to the process bus through the Ethernet network. Interruptions in data transmission from the MUs to the receiving IEDs can cause malfunctions in control and protection. A faulty merging unit might produce inaccurate or out-of-sync data, leading to incorrect decisions by protection IEDs. This not only affects the performance of the substation but also potentially increases wear and tear on equipment, thereby increasing maintenance costs and decreasing equipment lifespan.

4.7.1.2 Fiber Optic Cables and Ethernet Switches

Fiber optic cables connect all components in the process bus together. If a cable between two nodes becomes disconnected or unplugged, a portion of the network becomes separated from the rest and loses communication. A solution to this problem is to implement redundant paths in the Ethernet network so that the data communication systems can use other paths in case of failure. Some transmission companies stated that rodents are the main cause of the fiber optic cable problem, but bad quality in the installation of the network could also be a cause of the high failure rate for physical communication links [80].

Regarding performance, the optical fibers and the Ethernet switches impose a small delay. Ethernet switches process every message received or transmitted by each IED. It takes time for a switch to process messages, and this introduces a short but unavoidable processing delay. A message may need to go through several switches in a network to reach its destination. So the more switches there are in the system, the greater the delay in data transmission.

4.7.2 Component Failures Modes

This chapter will mention the common component failures that may occur in an IEC 61850 process bus found in the literature review. According to [9], the component failures that may occur in a digital substation can be divided into the following categories:

- Ethernet network failure.
- Operational failure.
- Software failures.
- External Failures.

4.7.2.1 Cable Failures

Faulty Cables Cables can fail due to damage, wear and tear, manufacturing defects, or errors in the installation or maintenance of the communication cabling.

Inappropriate Physical Network Design To ensure optimal network performance, several limits must be considered in the communications network design. If these limits are not taken into account, the network's performance will be considerably lower than expected. The Ethernet network detects collisions using carrier-sense multiple access with collision detection (CSMA/CD) technology. When the length of a segment or network exceeds the IEEE standard maximum, the probability of collision increases. Collisions within the Ethernet network can result in runts (packets smaller than the minimum packet size) and giants (packets exceeding the maximum packet size). Choosing the appropriate cable lengths for a DSAS minimizes the risk of these failures. For example, the IEEE limits the 100BASE-TX segment in the Ethernet network to 80 meters. Adding a switch reduces cable length and therefore the collision risk, but the additional device also has its own failure rate and reduces overall system reliability. [9]

4.7.2.2 Operational Failures

Operational failures in a power system can result from the incorrect design of the DSAS, leading to unintended operations.

Misconfigured Settings Each device within a substation requires specific configuration software with specific parameters, known as configurations and settings, to function properly. If these values are incorrect or missing, the device may not work or malfunction. IEDs require a large amount of data to be transmitted for their configurations. While creating basic specifications for IEDs is relatively straightforward, the process is time-consuming and requires significant input data. A reliable tracking system is necessary to ensure proper settings are applied to the IEDs and to assist with troubleshooting in the event of issues. [9]

Commissioning Issues Commissioning refers to the process of ensuring that the device has been installed correctly and is operating as intended. The objectives for commissioning IEDs are to test the interlocking, control, and protection logic. This requires validation and verification of all controls, inputs and outputs, indications, and switches. This testing is necessary to verify the correct operation of the IEDs. The most common issue encountered during this process is uncertainty. This uncertainty can stem from the intricate complexity of the IEDs, which include advanced software and hardware components that may behave unpredictably during testing. Variability in device configuration, due to a multitude of customizable settings and parameters, can also contribute to unpredictable outcomes. Furthermore, IEDs' interactions with other networked devices might yield unexpected behavior, adding to the uncertainty. [9]

4.7.2.3 Software Failures

In digital substations, software plays a crucial role but also poses a risk of failure that traditional hardwired systems do not face. This section covers the two main types of software failures in digital substations:

Code Faults Each IED has specialized software to implement its logic, and a deep understanding of programming is required to take advantage of the many features and flexibility of modern IEDs. The risk of failure is linked to various factors, such as the number of variables, inputs and outputs, operation codes, operands, subroutines, and keywords. More complex software designs increase the likelihood of failure. [9]

Database Failures Each piece of software has a database designed to store large amounts of data, which grows as new data from the power system is collected. To ensure reliability and safety, this data needs to be stored on a secure and spacious drive. Any disruption or mismatch in the database can directly impact software performance, and crashes can result in significant data loss. To maintain cybersecurity, database connections must be secure to prevent unauthorized access. [9]

4.7.2.4 External Faults

The operation of digital devices and networks can be impacted by non-technical failures due to certain conditions.

Loss of Power One of the main external failures is a loss of power, which can be caused by issues in the power distribution system, switchovers, surges, or intolerably high voltages. Even a momentary loss of power can reset devices, leading to system failure. The failure is more destructive with IEDs and network switches, as these devices not only provide protection but also control and data acquisition. To mitigate the impact of power loss, a backup battery or redundant power source, such as a battery station, may be necessary. [9]

Aging Other factors that can induce environmental failures involve the accelerated aging of equipment, which is increased by ambient conditions such as temperature and moisture. Over time, these conditions can speed up the wear and tear process, leading to the gradual deterioration of communications equipment, wiring, and switches. Additionally, the accumulation of dirt and dust can compromise the performance of electronic components. This could result in overheating and, in extreme cases, even cause a fire. Hence, environmental factors like temperature and moisture significantly contribute to the life expectancy and functionality of digital substation equipment. [81]

4.7.3 Communication Failure Modes

The process bus relies on an Ethernet network to enable communication between IEDs and switchgear instruments. This means that a process bus consists of vast networks of switches and fiber-optic cables. Like any communication network, Ethernet networks can experience failures that can impact the performance and reliability of the process bus. Communication failures refer to any issues with the communication network, including issues with the communication protocols used to transmit data between devices. Communication failures can disrupt the flow of information between devices, causing data errors, delays, or the loss of communication altogether. This chapter is about what consequences failures in the communication process between the components of the process bus may cause. From the literature review, it has been found that common communication failures in an Ethernet network can be placed in the following categories:

- Data transfer failure.
- Loss of synchronization.
- Heavy network loads

4.7.3.1 Data Transfer Failures

Data delivery in a digital network is not automatically ensured by just connecting two points; specific conditions must be met to ensure proper communication. Data communication failures are different from network structure failures in that there is no tool to identify them. As a result, logical connectivity issues tend to be more complex and challenging to diagnose, isolate, and solve than network structure problems. The following sections describe a few data communication challenges in digital substations.

Defective Network Interface Cards (NICs) Most problems that affect data communication in a digital substation occur at the physical layer of the Open System Interconnection (OSI) model, which includes NICs (a hardware component that provides the interface between an IED and the process bus). One common network failure is "jabbering". This is typically caused by faulty NICs. Although Ethernet networks are generally considered reliable and fast, they can still be susceptible to jabbering. This occurs when a device re-transmits a packet that other devices do not understand, leading to network congestion and a loss of performance [9].

Uncalibrated instruments Instruments that have not been correctly calibrated can lead to inaccurate measurements. The effects of these errors might appear in a number of ways, such as inaccurate data being communicated or devices breaking down and causing messages to be repeated, a condition known as repetition. Incorrect calibration may also result in extra data being unintentionally added during transmission, corrupting the data. In some cases, data could be received in the wrong sequence which can lead to mistakes in the interpretation of the data [82].

Cyberattack Unauthorized access to the communication network can result in security breaches or data theft. Attackers may attempt to alter data as it is being transmitted, this can result in miscommunication and incorrect decision-making. Additionally, bit errors within the message frame have the potential to corrupt data, compromising the reliability of the entire communication system. Lastly, incorrect addressing brought on by unauthorized network access might result in message frames reaching the wrong recipients, creating more disruption and potential harm [9].

Upgrade and Compatibility Issues Even if the configurations of two components match, they may still not receive the same responses when communicating with a single node. Compatibility problems can occur due to upgrades in hardware, software, or firmware, such as in IEDs, switches, or servers. Upgrading firmware can be a time-consuming task that stops substation operation for several hours, and there's a possibility that the IED will not be able to effectively communicate with existing IEDs after upgrading [9].

4.7.3.2 Loss of Synchronization

IEC 61850 mandates that sampled value data must be synchronized at the process level. If the synchronization source fails or malfunctions, the devices in the substation will no longer be synchronized with each other, rendering the collected data useless for wide-area monitoring and control purposes. There are numerous circumstances under which time synchronization can encounter problems, and these largely hinge on the type of time synchronization protocol utilized. If Precision Time Protocol (PTP) is employed, there's a risk that the master clock might malfunction, delivering incorrect time readings to the merging unit [9].

4.7.3.3 Heavy Network Loads

Oversubscription of bandwidth This situation arises when the bandwidth demand exceeds the available capacity. Consequently, congestion ensues, leading to the potential dropping of some data packets. The consequences are substantial, as it not only disrupts smooth data transfer but can also lead to significant loss of crucial data, affecting the overall operations of the substation [14].

Broadcast storms Occur when a broadcast packet is continually forwarded by a network switch or router, flooding the network with excessive traffic. This overflow can slow down the network significantly and even result in packet loss, impairing communication, and operations within the digital substation [14].

4.7.4 Ending Effects of Communication Failures

This section covers packet loss, latency, and network congestion, three common symptoms of network failures. Although these events are sometimes seen as failures in and of themselves, it is more accurate to view them as effects of underlying network failure.

4.7.4.1 Packet Loss

One of the most common communication issues in Ethernet networks is packet loss. Packet loss occurs when one or more packets of data sent between devices fail to reach their intended destination. In an IEC 61850 process bus, packet loss can lead to data corruption, delay, and disruption of the communication flow between the IEDs and the switchgear instruments [83]. Packet loss can happen due to network congestion, device failure, or faulty cabling.

In a process bus, the SV messages may not always reach their destination due to packet loss. SV messages contain a sample counter that indicates the number of samples taken within a one-second window. This counter increments from 0000 to 3999 and resets at the top of every second, depending on the system frequency and publication rate (e.g. 50Hz and 80 samples/cycle) [14]. The merging units use the sample counter to detect packet loss. When an SV message is lost, analog data is lost at the merging unit, potentially leading to delayed protection actions. The tolerance for consecutive missing or invalid samples varies between IEDs and different functions.

4.7.4.2 Latency

Another common communication failure in Ethernet networks is latency. Latency is the delay that occurs between the time a packet is sent and the time it is received. In an IEC 61850 process bus, latency can cause a delay in the transmission of data, leading to synchronization errors and miscommunication between the IEDs and switchgear instruments [84]. There are two types of latency in the network: constant latency and variable latency. Constant latency is related to inherent delays in nodes and connections and depends on the physical structure of the network and bandwidth. It is calculable and predictable. Variable latency depends on traffic and network loading and can significantly degrade throughput and increase latency during simultaneous communications or network failures. In time-critical tasks, such as power system protection, latency is a crucial issue, and protective devices must operate quickly, reliably, and with deterministic timing. Latency increases even further in the event of a failure in an intermediary device or connector, which requires data to travel a less optimal alternate path and increases hop counts and traffic delays [9].

In a process bus, the smallest unit for data exchange is a logical node (LN), which represents a virtual description of device functions. The IEC 61850 standard outlines performance requirements for data exchange between LNs, specifying transfer time in terms of the transmission data. These transmission time requirements are shown in table 9. This means that network delay is not only dependent on the local and remote IEDs but also on the processing times of active components such as routers and switches. These components can significantly contribute to network transfer time delays, limiting functional performance due to the availability and latency imposed by the communication network and its configuration. Two critical networks are identified: the Ethernet-based substation LAN and the time synchronization network. Both networks must remain operational at all times and are often not segregated, making them vulnerable to common failures. [14].

Table 9: IEC 61850 transfer time requirements [28]

Services	**Transfer Time (ms)**
SV	3-10
GOOSE, GSSE	3-100
MMS	20-100

Messages that are critical for protecting the power system have strict requirements for how quickly they need to be transmitted. These messages are divided into different types and performance classes, with faster transmission times for the most important messages. If different types of messages are sent over the same network, the network must be designed to meet the requirements of the most sensitive message. The messages that require the quickest transmission times are for tripping, blocking, and sampling. These messages are classified as types 1A, 1B, and 4 and are sorted into different performance classes. Performance classes P1 and P7 require transmission times of less than 3 milliseconds, while classes P2 and P3 require 10 or 20 milliseconds [14].

4.7.4.3 Network congestion

Network congestion is another communication failure that can occur in Ethernet networks. Network congestion happens when the amount of traffic on the network exceeds its capacity, causing communication failures that can lead to system instability, data corruption, and equipment failure [85]. The maximum amount of data that can be transferred over a given network is known as the "bandwidth." In a digital substation, a 100 Mbps process bus is usually sufficient [86]. According to the work done in [14], failure is low when network traffic is below 50 Mbps. As more data occupies the bandwidth, the probability of failure increases exponentially. However, SV messages typically occupy the majority of the bandwidth. A single SV stream message consists of 160 bytes at 80 samples per cycle, which takes up approximately 5% of the total bandwidth. The remaining bandwidth is affected by the size and publication rate of GOOSE messages published by IEDs.

5 METHOD

This chapter describes the approaches used to investigate the reliability differences between Ethernet typologies, HSR and PRP protocols, and conventional and digital substations. The entire process is conducted using the Relyence software. The exponential distribution is assumed on all failure rates.

The methodology chapter begins with an explanation of why the controller IED was disregarded from the analysis and then an explanation of the use of Relyence. Following this, the chapter presents the data utilized for the analyses, detailing the specifics and the source of the information. The chapter then shifts to a comparison of HSR and PRP, additionally, it will present a method for comparing two different HSR networks. Next, an approach is outlined for comparing digital and conventional substations. The method includes an analysis of two line diagrams, focusing on their design.

5.1 Disregarding The Controller IED

The essential protective and breaker control functions are carried out by protection and circuit breaker IEDs. The controller IED might serve additional roles not specific to the immediate process bus operation. This could be why you might disregard the controller IED when analyzing the core operation of an IEC 61850 process bus. Despite being a vital part of the overall substation automation system, its importance was downplayed in this research, which focused on the immediate operation of the process bus, the interaction of protective devices, and the activation of circuit breakers. Therefore, in the context of this investigation, the controller IED can be ignored.

5.2 The Use of Relyence

Relyence is used to make all reliability block diagrams as well as to calculate all reliability results in this report. The process of creating an RBD in Relyence is explained in chapter 4.6.1.1. Figure 39 illustrates the calculation window in Relyence. Here, one can select the simulation time as well as the output results one wants from the software. The simulation time for this research is 250.000 hours. The metrics selected for calculation are shown in table 10 and 11:

Table 10: Selected time-based metrics

Metric	Description
Reliability	The probability of a system running without failure for a specific time period.
Failure rate	The probability of system failure at a particular time.
Availability	The probability of the system working at a given time.
Total Downtime	The total expected downtime over a predetermined period.
Expected number of failures	Predicted system failures within a specific timeframe.
Hazard rate	The probability that failure occurs at a specific time.

Table 11: Selected steady-state metrics

Metric	Description
MTTF	Mean time to first failure
MTTR	Mean time to repair
MTBF	Mean time between failure
Availability	The likelihood of the system being operational

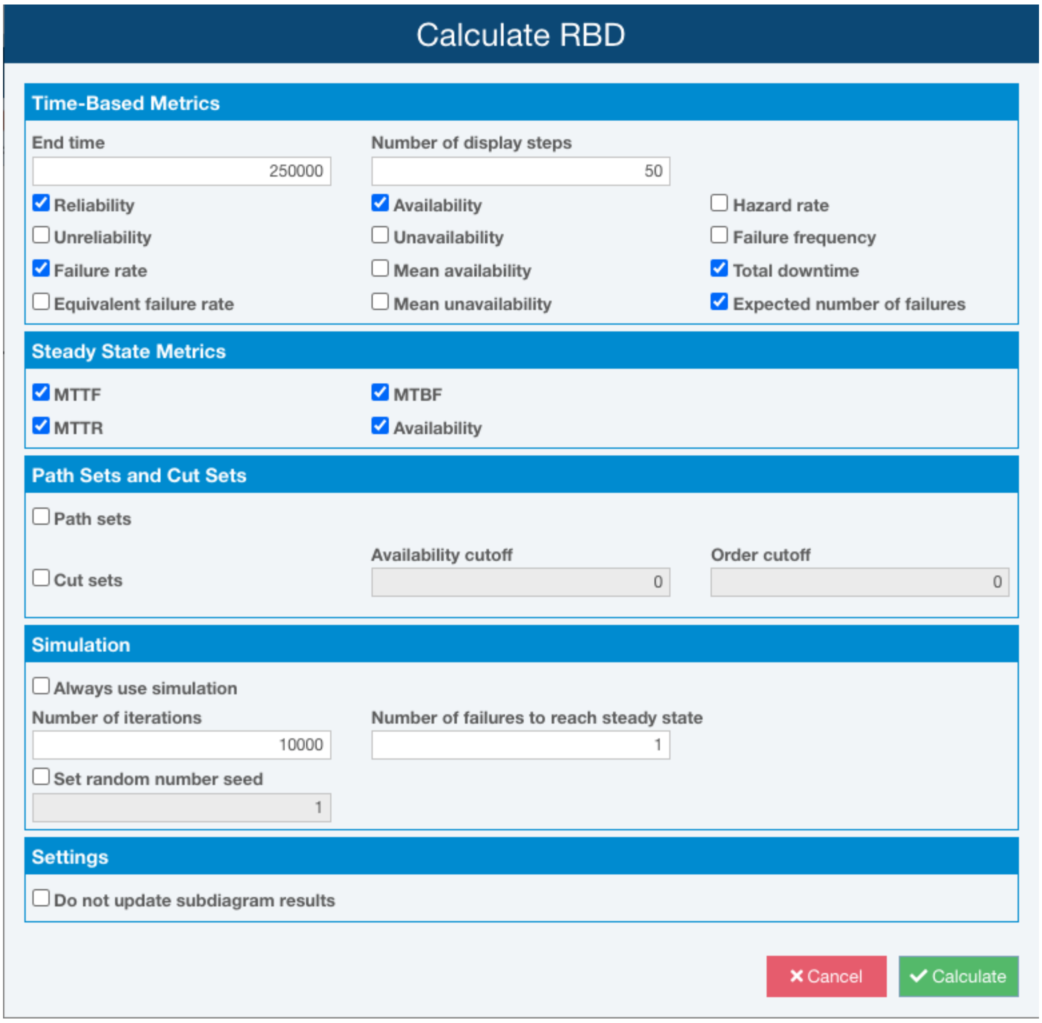


Figure 39: Calculating reliability block diagram in Relyence

5.3 Data

In this research, a distinctive approach is applied to the data utilized for digital and conventional substations due to the significant technological differences between the two. Two separate data sets are employed, each representing the unique parameters and characteristics of the respective station types and derived from different sources. The differences in cable systems make this especially relevant. While fiber optic wires are used in digital substations, copper wires are mostly used in conventional substations. As a result, IEDs in conventional substations are thought to be less reliable. By taking this into account, the study will not neglect the cable systems of the two substations.

The digital substation reliability parameters are retrieved from the scientific articles "Estimation of Digital Substation Reliability Indices" [6] and "Switchgear Optimization Using IEC 61850-9-2" [87]. The parameters can be found in table 12. The article [87] gives NCITs an MTBF of 2 628 000 hours (300 years), a 31.39% increase from a conventional instrument transformer as given in table 14. Although the article does not provide a detailed justification for the specific MTBF values, it emphasizes that the main purpose is to illustrate the potential improvements in availability when using NCITs and IEC 61850 communication.

Table 12: Digital substation reliability parameters

Component	Failure Rate	MTBF (hours)	MTTR (hours)
Protection IED	0.07	125,000	48
Merging Unit	0.07	125,000	48
Ethernet Switch	0.025	344,827	48
Time Synchronization	0.07	125,000	48
Breaker IED	0.07	125,000	48
NCIT	0.0038	2,628,000	48

Multiple HSR networks are used in these analyses. Given that all IEDs have the same failure rate of 0.07, the probability of at least 5 out of 6 switches working in the system depicted in figure 45b can be calculated using equations 1 and 2. The probability that one IED works is 0.93. The method on how to calculate the reliability parameters of these networks is as follows:

Exactly 5 out of 6 switches are working:
$P(X = 5) = C(6, 5) * p^5 * (1 - p)^{(6-5)} = 6 * (0.93)^5 * (0.07)^1$

All 6 switches are working:
$P(X = 6) = C(6, 6) * p^6 * (1 - p)^{(6-6)} = 1 * (0.93)^6 * (0.07)^0$

Now, the probabilities of the two scenarios are summarized to get the probability of at least 5 out of 6 switches working:

P(at least 5 working) = P(X = 5) + P(X = 6)

Calculate the probabilities:
$P(X = 5) = 6 * (0.93)^5 * (0.07)^1 = 0.2922$ $P(X = 6) = 1 * (0.93)^6 * (0.07)^0 = 0.6471$

Summarize the probabilities:
P(at least 5 working) = 0.2922 + 0.6471 = 0.94

Thus, the probability of at least 5 out of 6 switches working is 0.94. Then the failure rate is 0.06 and the MTBF is 146 000 hours or 16.67 years. The reliability parameters of the HSR networks used in this research are listed in table 13.

Table 13: Reliability parameters for the HSR loops

Component	Failure Rate	MTBF (hours)	MTTR (hours)
2/3 IEDs must function	0.014	625,089	48
5/6 IEDs must function	0.06	146,000	48
3/4 Ethernet switches must function	0.0038	2,308,804	48

The conventional substation reliability parameters are retrieved from [87], [88] and [89] and can be seen in table 14.

From a reliability point of view, IEDs in conventional and digital systems have the same reliability if wiring systems are neglected (assuming that cables are 100% reliable). The article "Switchgear Optimization Using IEC 61850-9-2" [87] mentions the expected differences in MTBF between IEDs that are connected to a conventional substation and a digital substation. Since the IEDs in a conventional station are connected using a wide net of copper cables, the expected failure rate will be higher than that in an IEC 61850-enabled substation. According to [87] the MTBF of a digital substation has a 70.45% increase compared to a conventional substation. Siemens has calculated that their SONO 3000 conventional current transformer has an MTBF of 2 000 000 hours (228.31 years) which equals a failure rate of 0.005 [89]. For simplicity, it is assumed that a voltage transformer has the same MTBF as a current transformer.

Table 14: Conventional substation reliability parameters

Component	Failure Rate	MTBF (hours)	MTTR (hours)
IED	0.1	88 062	96
Current Transformer	0.0050	2 000 000	96
Voltage transformer	0.0050	2 000 000	96
Circuit breaker	0.013317	750 944	96

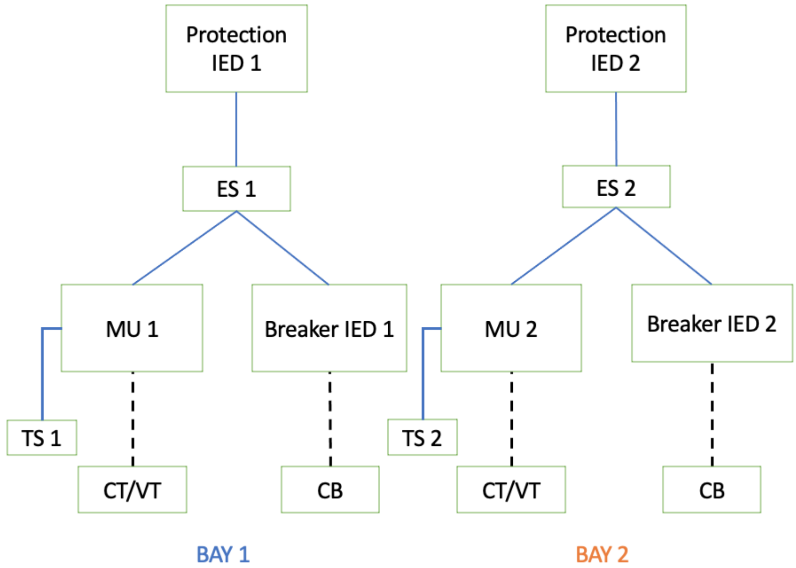
5.4 Comparing the Redundancy Protocols

In this chapter, a comparative analysis of the reliability differences between a no-redundancy, HSR, and PRP process bus systems is presented. To achieve this, process bus systems with no redundancy protocol as well as process bus systems based on HSR and PRP principles were designed, with two systems for each. Reliability block diagrams for each system were created, serving as the basis for calculations and evaluation of the system's performance. By utilizing Relyence software, reliability calculations were conducted to thoroughly assess and compare the dependability of both HSR and PRP process bus systems. PRP systems are designed with a star topology, whereas HSR systems adopt a ring architecture. Consequently, a comparative analysis of how the different topologies affect the reliability of the process bus may be established. This analysis also contain an analysis comparing non-repairable with repairable systems. Meaning, each system is analysed twice, one where the components are repairable with an MTTR of 48 hours and one where they are non-repairable.

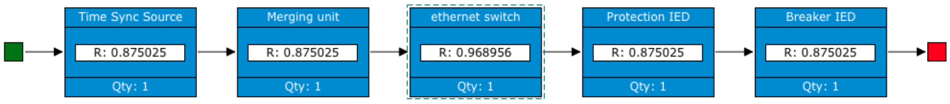
The systems under investigation are assessed in their steady-state conditions, meaning that the systems are not experiencing any significant disturbances or changes in their operating conditions. Importantly, this steady-state analysis assumes an absence of faults, focusing strictly on the operational state where the systems are functioning as designed. It does not indicate that these systems are inherently faultless, but rather constrains the scope of the study to normal, fault-free operational conditions.

5.4.1 The No Redundancy Protocol Process Buses

Figure 41 shows a basic process bus system with its corresponding reliability block diagram, this system has no redundancy. In this configuration, there are two bays. The primary objective is to evaluate the efficiency and reliability of this simplified design in comparison to more complex process bus systems which utilize PRP and HSR protocols.

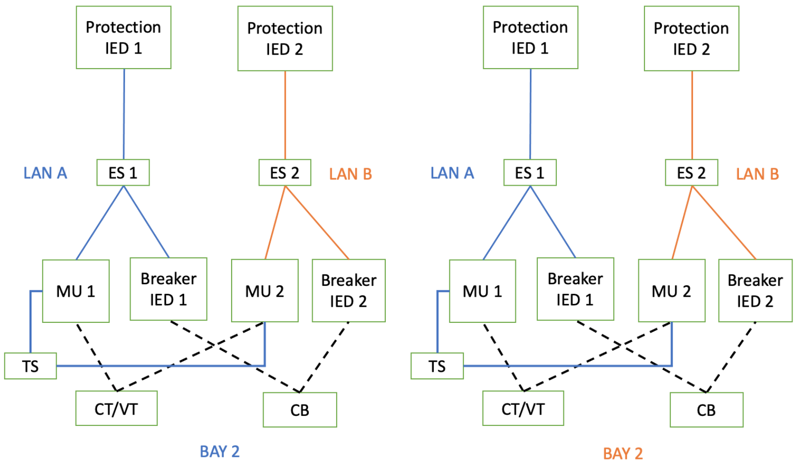


(a) No redundancy process bus

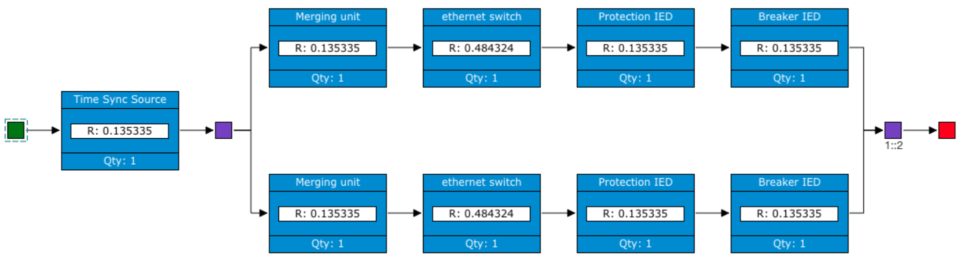


(b) RBD of no redundancy process bus

Figure 40: Design and reliability block diagram of no protocol process bus



(a) No redundancy protocol with component redundancy process bus



(b) RBD of no redundancy protocol with component redundancy process bus

Figure 41: Design and reliability block diagram of no redundancy protocol with component redundancy.

5.4.2 The PRP and HSR Process Buses

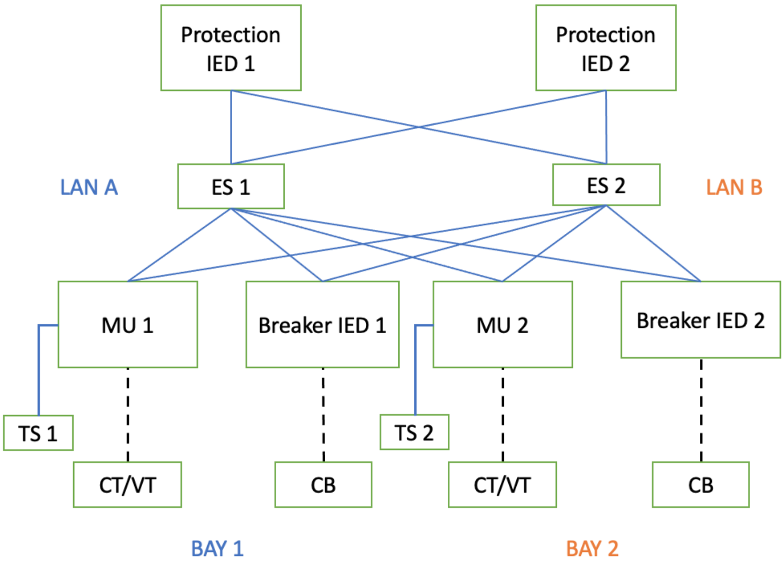
This study involves the design of four systems to investigate the reliability of PRP and HSR protocols within an IEC 61850 process bus. Each system has been designed with two bays for consistency and ease of comparison. Two of these systems employ PRP protocols - one designed with component redundancy and the other without, while the remaining two systems implement HSR protocols, likewise distinguished by the presence or absence of component redundancy. In this context, component redundancy means that there is a duplicate for every component within the system.

5.4.2.1 PRP Process Buses

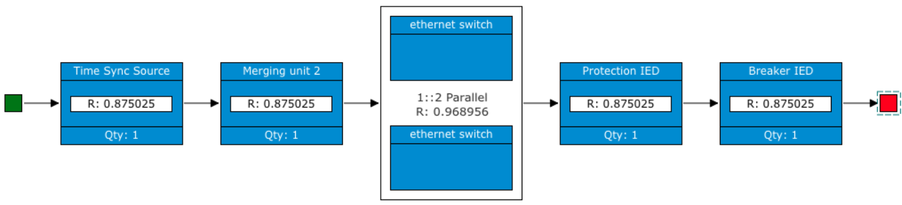
In the PRP systems illustrated in figures 42a and 43a, both configurations ensure that all IEDs are connected to two separate Ethernet LANs, providing independent communication paths.

Figure 43a demonstrates the first PRP system, which comprises two bays and no component redundancy. Within this configuration, the merging units, breaker IEDs, and protection IEDs establish dual connections to the switches using star architecture. Each merging unit is connected to its own individual time sync source.

In contrast, the second PRP system, depicted in Figure 42a, incorporates component redundancy. The inclusion of component redundancy introduces a new layer of complexity to the communication infrastructure. Nevertheless, the dual connections for the merging unit, breaker IED, and protection IEDs are retained by introducing two new Ethernet switches. Here, each bay consists of two switches connected in a star formation, guaranteeing consistent redundancy and fault tolerance in both systems. Now, the merging units in the same bay share a time sync source.

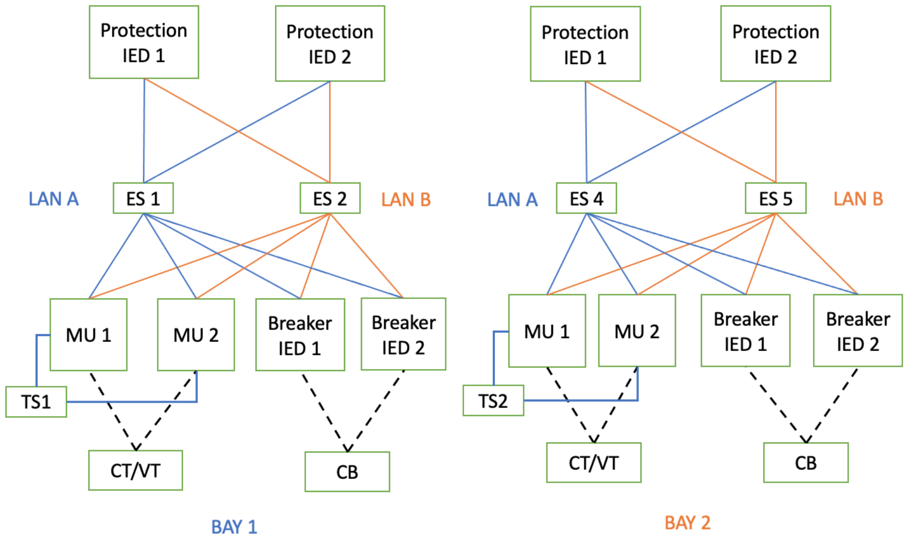


(a) PRP process bus with no component redundancy

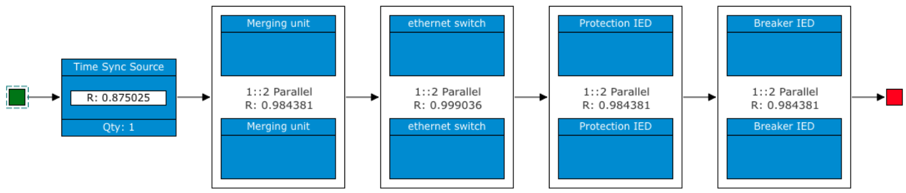


(b) RBD of PRP process bus with no component redundancy

Figure 42: Design and reliability block diagram of PRP process bus with no component redundancy



(a) PRP process bus with component redundancy



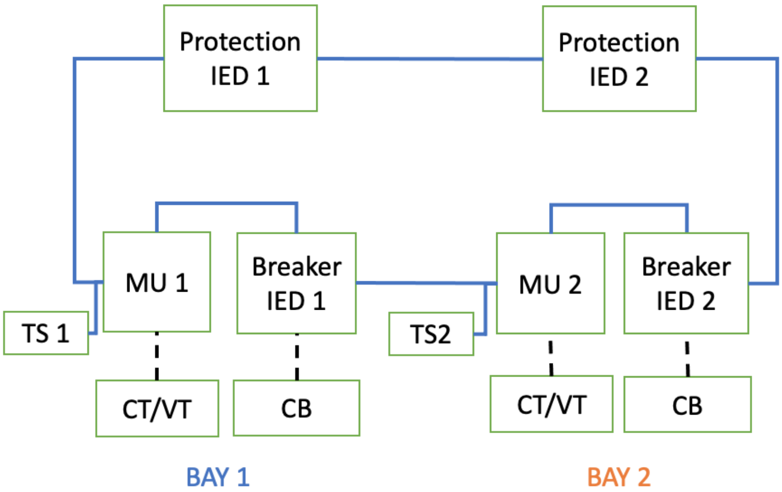
(b) RBD of PRP process bus with component redundancy

Figure 43: Design and reliability block diagram of PRP process bus with component redundancy

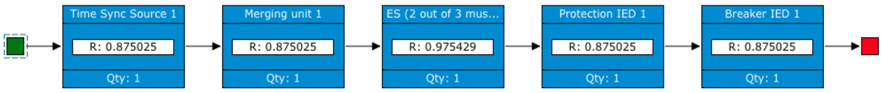
5.4.2.2 HSR Process Buses

The systems depicted in figures 44a and 45a employ the HSR protocol to ensure continuous and uninterrupted communication between the IEDs in a loop topology.

Both systems consist of two bays, but in the system shown in figure 44a there is no component redundancy thus, there the system only contains 6 IEDs connected in a loop, in addition time sync sources are connected to each merging unit. In contrast, the second HSR system, illustrated in figure 45a, utilizes component redundancy meaning that there are 12 IEDs connected in a loop, potentially affecting its reliability compared to the no component redundancy system.

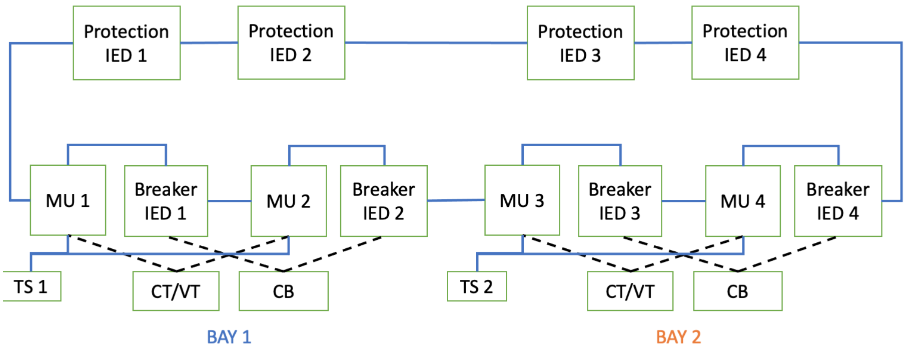


(a) HSR process bus with no component redundancy

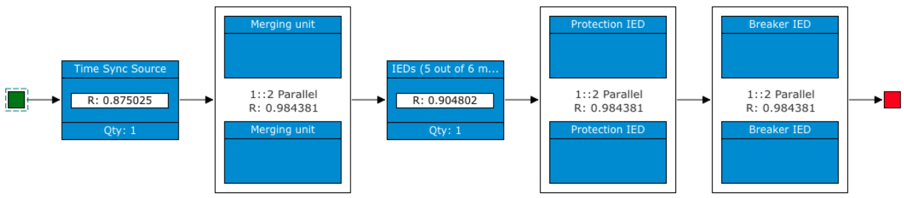


(b) RBD of HSR process bus with no component redundancy

Figure 44: Design and reliability block diagram of HSR process bus with no component redundancy



(a) HSR process bus with component redundancy



(b) RBD of HSR process bus with component redundancy

Figure 45: Design and reliability block diagram of HSR process bus with component redundancy

5.4.3 Comparing HSR networks

Additionally, there will also be a reliability analysis performed on the two HSR networks. This is to see what effect network complexity and additional components will have on the reliability of the HSR protocol. The analysis will be done on the two HSR networks in the process buses in figures 44 and 45. The analysis is done in Relyence which has already calculated the reliability metrics of the two HSR loops.

5.4.4 Reliability Block Diagrams for the Redundancy Protocol Analysis

The reliability block diagrams serve to illustrate an understanding of each system's architecture and its impact on the overall reliability of the process bus network. The reliability block diagrams for all systems focus on the reliability of bay 2, which serves as a representative example for other bays, as they consist of identical components and have the same reliability characteristics. All RBDs are made in Relyence as well as all calculations.

5.4.4.1 The PRP RBDs

In the RBD in figure 42b all IEDs are connected in series but the merging unit sends two messages to the two separate Ethernet switches creating parallel connections.

The second PRP system features the merging units sending messages to two separate Ethernet switches, and providing independent communication paths. If one switch fails or a communication path is interrupted, the other switch can continue to facilitate communication between the IEDs. This is why all IEDs are connected in parallel in the second PRP system, in figure 44b.

5.4.4.2 The HSR RBDs

RBD for the HSR systems is shown in figure 44b and 45b. In the first figure all IEDs are connected in series and at least 2 out of the 3 of the remaining IEDs in the loop must function for the system to work. In contrast, for the system in figure 45b, all components have a parallel connection and at least 5 out of the 6 remaining IEDs in the loop must function. This is because the loop topology ensures that even if one IED fails, the other two can still maintain communication and data transmission through the alternative path.

5.5 Comparing Conventional and Digital Substation

To assess the reliability of both the digital and conventional substations two different substations have been designed: One is connected to an IEC 61850 process bus for the digital substation and the second is a conventional substation. The digital substation is illustrated in figure 46, while the conventional is in figure 47. The two protection systems are designed in a similar way to facilitate the comparison of their reliability attributes. By comparing these two substations, it may become possible to reveal the reliability differences between the IEC 61850-based digital substation and its conventional counterpart. This analysis is done on only repairable systems.

In both substations, there are a total of three bays. Bay one is a transformer bay and consists of one merging unit and one circuit breaker IED which are connected to two circuit breakers and NCITs on opposite sides of the transformer. The connection of these IEDs incorporates differential protection for the power transformer, which ensures effective protection coordination. In the digital configuration, the IEDs in bay A only subscribe to Ethernet switches A1 and A2, which implies that protection IED A sends GOOSE signals to both circuit breakers A and B. Bays two and three are line bays. In the digital substation, each of these bays is equipped with two Ethernet switches. One Ethernet switch connects to the merging unit and breaker IED, while the other corresponding switch links to the protection IED.

The digital substation utilizes HSR in its process bus for communication purposes. Comprising a total of 6 Ethernet switches, the HSR loop enhances the reliability of communication and control within the system. Furthermore, the digital substation incorporates the use of NCITs to achieve improved accuracy and performance.

The conventional system is a much simpler system as it does not consist of a process bus, here, the IEDs are simply connected to VTs, CTs, and circuit breakers using copper cables. Bay one consists of one IED connected to switchgear on opposing sides of the power transformer. The line bays consists of one IED connected to CTs, VTs, and CBs. The IEDs are further connected to the station bus using copper cables. The IEDs are also here interconnected with each other using copper cables, meaning they can subscribe to each other.

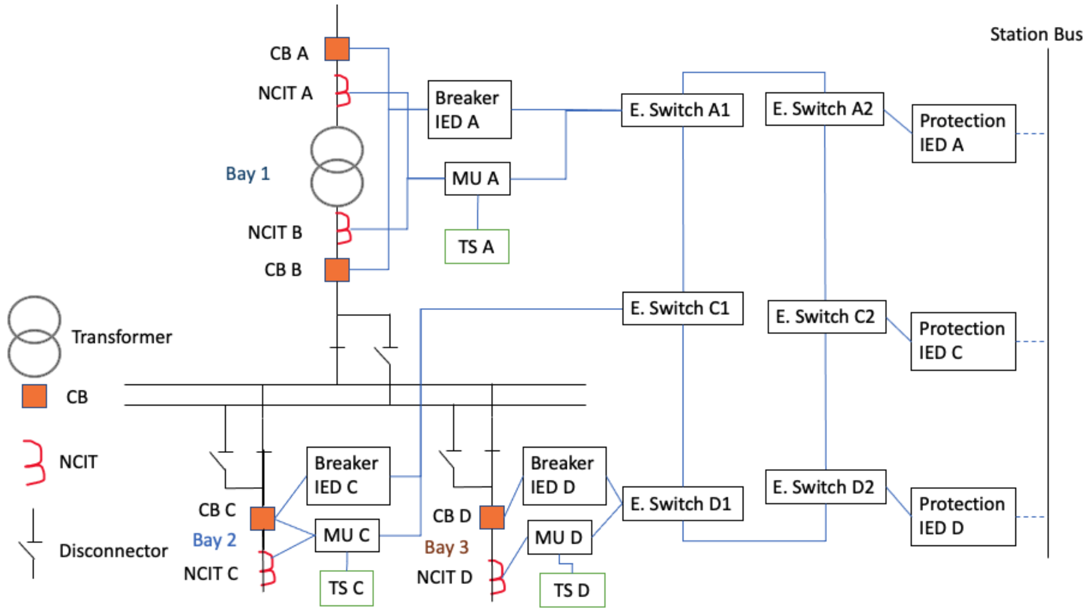


Figure 46: Digital protection system

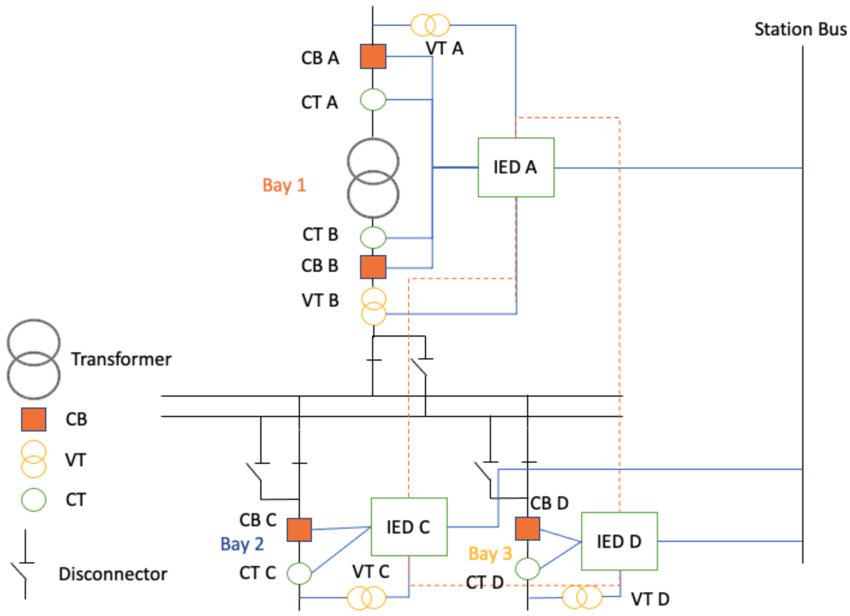


Figure 47: Conventional protection system

5.5.1 Defining Protection Coordination Within the Systems

Remote backup protection is explained in chapter 3.2.2. Essentially, if a fault were to occur in one of the distribution lines, the associated circuit breaker should trip. If the breaker in the distribution line fails to operate due to a malfunction, the next breaker in the hierarchy should then operate as a backup. This strategy prevents unnecessary widespread outages and ensures optimal continuity of service.

In figure 48 the protection zones of the two stations are established. In this figure, each bay has its own individual zone while zone 4 illustrates remote backup protection.

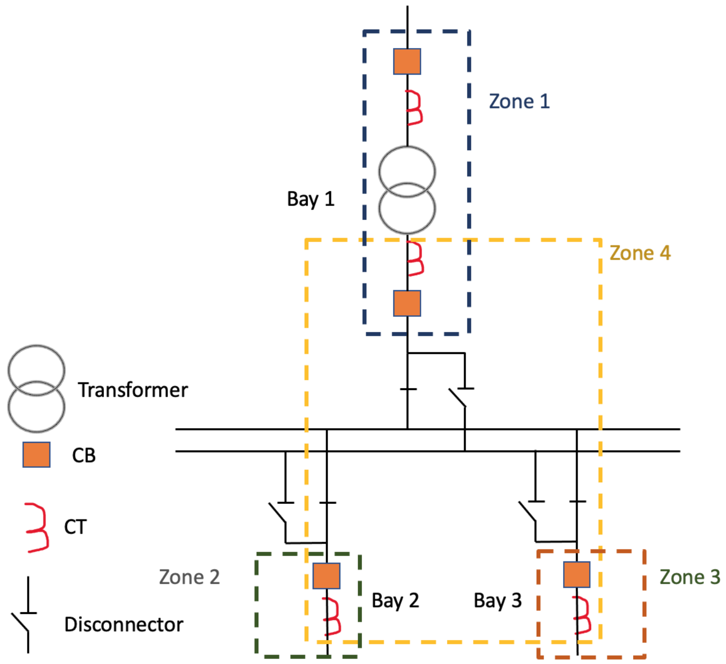


Figure 48: Protective zones in the power system

In these power system designs, communication is achieved between the IEDs installed across different bays. This communication ensures that when one IED malfunctions, another IED from a neighboring bay can step in to mitigate the issue. The neighboring IED will take the appropriate action based on the nature of the fault or the specific equipment involved.

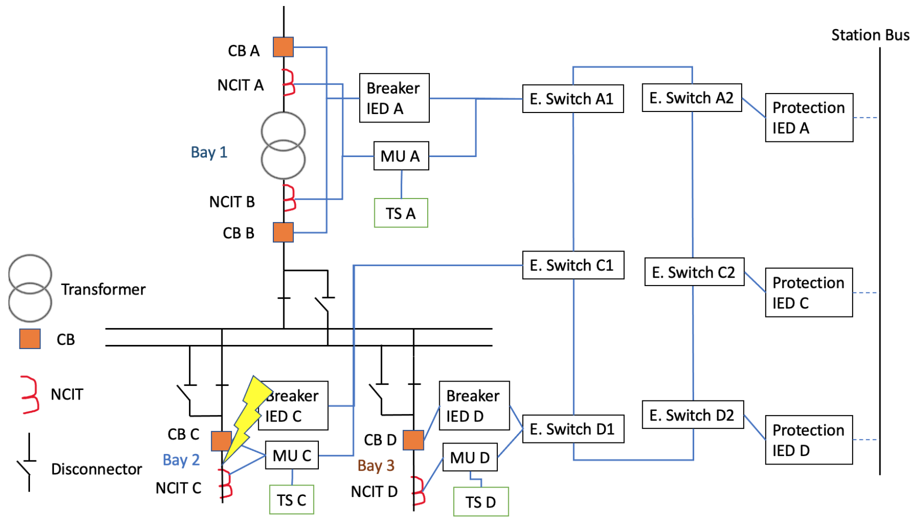
To address a malfunction, the neighboring IED may either operate the circuit breaker within the bay where the faulty IED is located, or it may operate the circuit breaker within its own zone depending on the type of malfunctioning. This coordinated response helps maintain the stability and reliability of the power system while minimizing the impact of faults on the overall network.

Consider an example to illustrate the protection coordination of these substations. In this example, the IEC 61850 process bus in figure 46 is in focus:

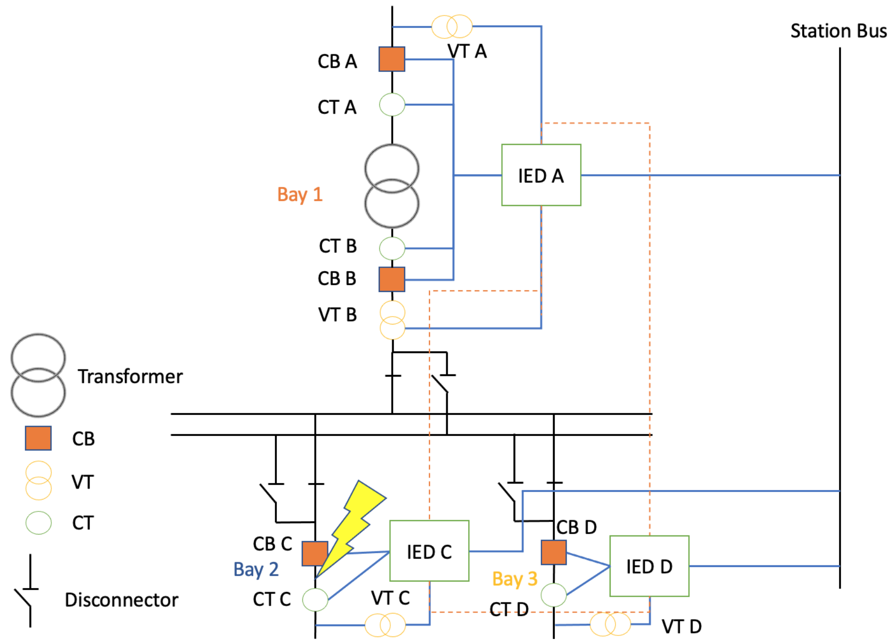
Suppose a fault occurs in Bay 2 and protection IED C fails to function properly. In this scenario, the SV message from MU C can be rerouted to protection IED B as an alternative. Upon receiving the SV message, protection IED B takes action by sending a GOOSE message to Breaker IED C, which consequently triggers the opening of the corresponding circuit breaker.

5.5.2 Equipment Malfunction Scenarios

To investigate the difference in reliability between the two systems, they are looked at during different equipment malfunction scenarios. Reliability block diagrams are then created to look at how the protection coordination within the systems would respond to these failures. The protection coordination in the two systems is designed in a similar manner in order to accurately compare the reliability of the two systems.



(a) Overcurrent fault digital



(b) Overcurrent fault conventional

Figure 49: Overcurrent fault in bay 2

One such scenario involves a circuit breaker malfunction during an overcurrent fault in bay 2 illustrated in figure 49. In both the conventional and digital systems, when this fault occurs it should trip circuit breaker C, but as it malfunctions the protection coordination has to step in. For the digital station, the GOOSE message has to be rerouted through the HSR process bus to Ethernet switch B. Subsequently, it reaches breaker IED B, which then opens circuit breaker B as an alternative. This protective coordination is illustrated with RBD in figure 50.

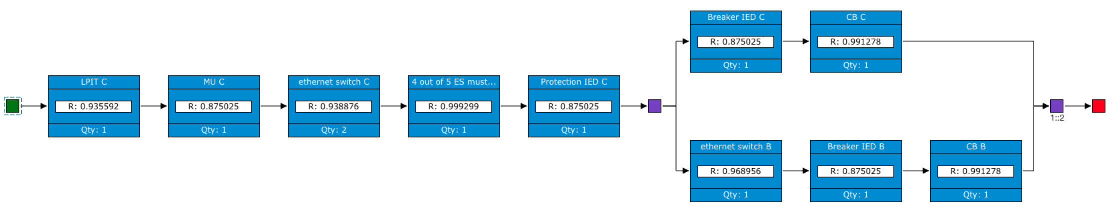


Figure 50: CB failure, digital

On the other hand, in the conventional substation, if circuit breaker C fails, IED C sends a message to IED B, instructing it to close circuit breaker B as a backup measure. This protective coordination is illustrated with RBD in figure 51.

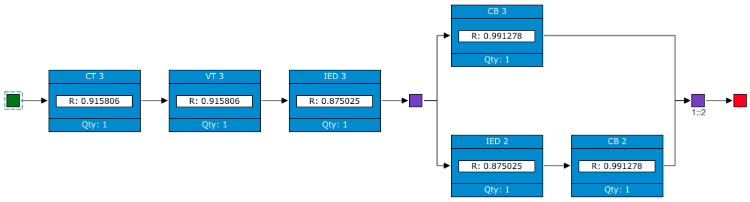


Figure 51: CB failure conventional

Another scenario is the malfunction of an IED. Consider the overcurrent fault scenario in figure 49 happens again. In this situation, IED C in the conventional station experiences a malfunction. As a result of the malfunction, it is assumed that IED C is unable to send a signal to IED A to intervene. Consequently, the instrument transformers in Bay 1 are required to detect the overcurrent in Bay 2. Upon receiving the overcurrent measurements from the instrument transformers, IED A responds by opening the circuit breaker in bay 1. This process is illustrated with RBD in figure 52

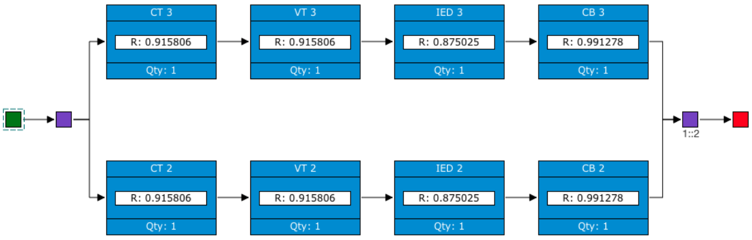


Figure 52: IED failure conventional

For the digital system, IED C malfunctions and fails to close its corresponding circuit breaker during a fault in bay 2. Then, breaker IED A must come into play and close its circuit breaker. The GOOSE message sent to breaker IED C must be rerouted to bay 1 and breaker IED A. Breaker IED A then will open its associated circuit breaker to mitigate the fault and maintain the power system's stability.

However, this comes with a drawback: breaker IED A's activation also results in disconnecting bay 3, where there is no fault. This consequence negatively impacts the system's overall performance and availability.

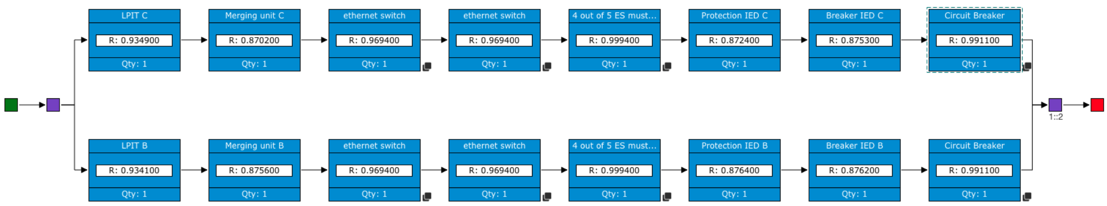


Figure 53: Merging unit failure

6 RESULTS

This chapter presents the findings of the analysis conducted to compare the redundancy protocols PRP and HSR as well as with the no-redundancy protocol systems along with the results from the digital versus conventional substation comparison. The graphs plotting the reliability of the systems denote the reliability function, while the graphs plotting the hazard rate denote the hazard rate function.

6.1 Results From The Redundancy Protocol Comparison Analysis

For the redundancy protocol analysis, the results are structured into sections covering repairable and non-repairable systems separately as different metrics are relevant for each. For repairable systems, the steady-state results of interest include MTBF, MTTR, and steady-state availability, while time-based results include availability, expected number of failures, total downtime, and hazard rate. Conversely, for non-repairable systems, the steady-state focus lies on MTTF, while time-based results include total downtime, reliability, and failure rate. This is explained in chapter 4.5. These sections are further divided into subsections dedicated to "Results for systems without component redundancy" and "Results for systems with component redundancy" in each.

Steady-state results are presented in tables, whereas time-based results are depicted using graphs. The complete set of time-based results can be found in the appendix.

6.1.1 Repairable Systems

6.1.1.1 Steady-State Results for Repairable Systems Without Component Redundancy

Table 15: Steady-State Results for Repairable Systems Without Component Redundancy

Metric	**Value**
MTBF	287867.004735
MTTR	48.099817
Steady State Availability	0.998100

(a) Steady state results for the no redundancy protocol system

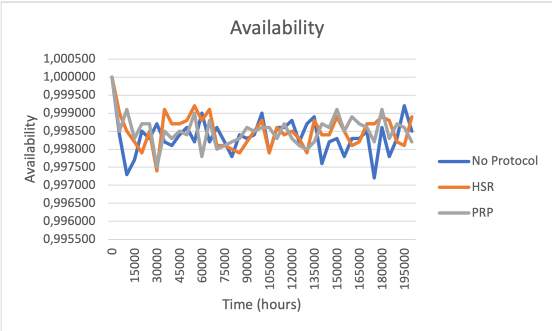
Metric	**Value**
MTBF	313211.520173
MTTR	47.895211
Steady State Availability	0.997900

(b) Steady state results for PRP with no component redundancy, repairable

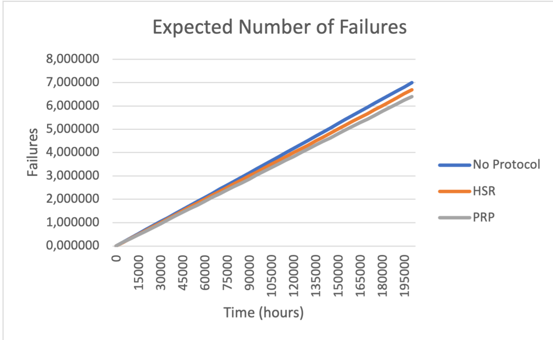
Metric	**Value**
MTBF	298340.294628
MTTR	47.895211
Steady State Availability	0.997900

(c) Steady state results for HSR no component redundancy, repairable

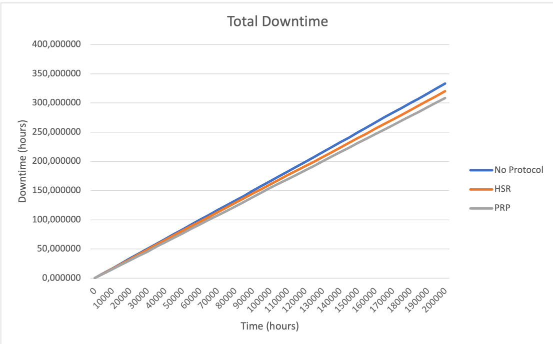
6.1.1.2 Time-Based Results for Repairable Systems Without Component Redundancy



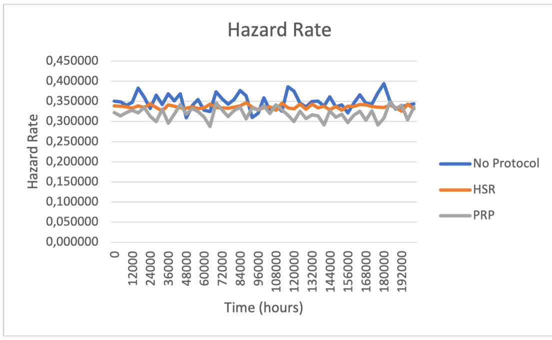
(a) Availability for repairable systems without component redundancy



(b) Expected number of failures for repairable systems with no component redundancy



(c) Total downtime for repairable systems with no component redundancy.



(d) Hazard rate for repairable systems with no component redundancy.

Figure 54: Time-Based Results for Repairable Systems Without Component Redundancy

6.1.1.3 Steady-State Results Repairable Systems With Component Redundancy

Table 16: Steady-state results for repairable systems with component redundancy.

Metric	Value
MTBF	120388.648598
MTTR	47.978860
Steady State Availability	0.999767

(a) Steady state results for no protocol repairable systems with component redundancy.

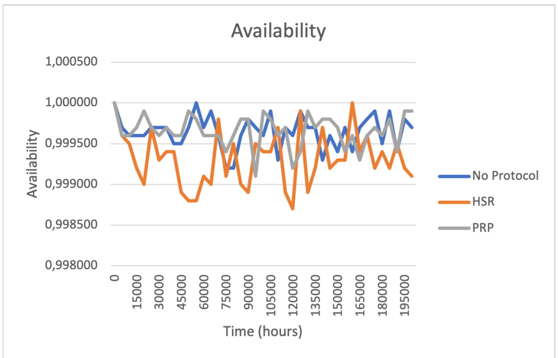
Metric	Value
MTBF	123422.518338
MTTR	48.317526
Steady State Availability	0.999700

(b) Steady state results for repairable PRP component redundancy.

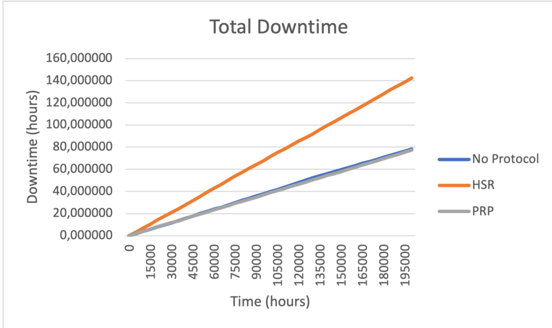
Metric	Value
MTBF	67600.921141
MTTR	48.407558
Steady State Availability	0.999167

(c) Steady state results for HSR with component redundancy repairable.

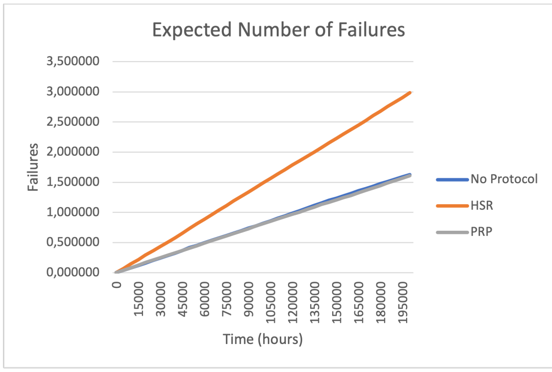
6.1.1.4 Time-Based Results for Repairable Systems With Component Redundancy



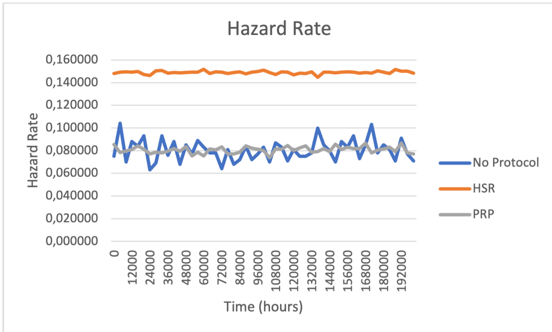
(a) Availability of repairable systems with component redundancy



(b) Total downtime for repairable systems with component redundancy



(c) Expected number of failures for repairable systems with component redundancy



(d) Hazard Rate for repairable systems with component redundancy

Figure 55: Time-Based Results for Repairable Systems With Component Redundancy

6.1.2 Non-Repairable Systems

As mentioned in chapter 4.5, the time-based metrics reliability and availability are equal to each other as well as the hazard rate and the failure rate. Therefore, in this section, the results for the hazard rate and the availability is not directly shown but they are assumed to be the same as the failure rate and reliability.

6.1.2.1 Steady-State Results for Non-Repairable Systems Without Component Redundancy

Table 17: Steady-State Results for Non-Repairable Systems Without Component Redundancy

(a) Steady state results for no redundancy protocol system without component redundancy

Metric	**Value**
MTTF	28653,249064

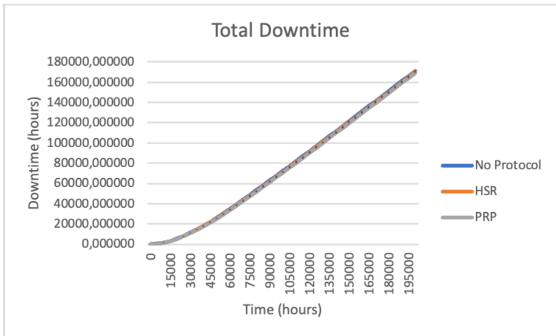
(b) Steady state results for PRP without component redundancy

Metric	**Value**
MTTF	30851,519654

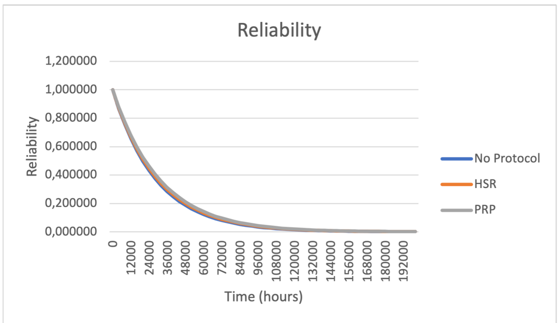
(c) Steady state results for HSR no component redundancy

Metric	**Value**
MTTF	29762,062905

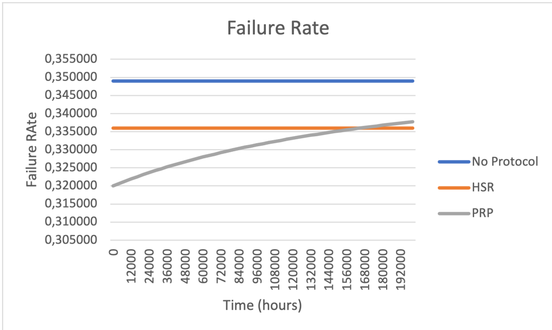
6.1.2.2 Time-Based Results for Non-Repairable Systems Without Component Redundancy



(a) Total Downtime for non-repairable systems without component redundancy



(b) Reliability for non-repairable systems without component redundancy



(c) Failure rate for non-repairable systems without component redundancy

Figure 56: Time-Based Results for Non-Repairable Systems Without Component Redundancy

6.1.2.3 Steady-State Results for Non-Repairable Systems With Component Redundancy

Table 18: Steady-State Results for Non-Repairable Systems With Component Redundancy

Metric	Value
MTTF	41125,311872

(a) Steady state results for no redundancy protocol system with component Redundancy

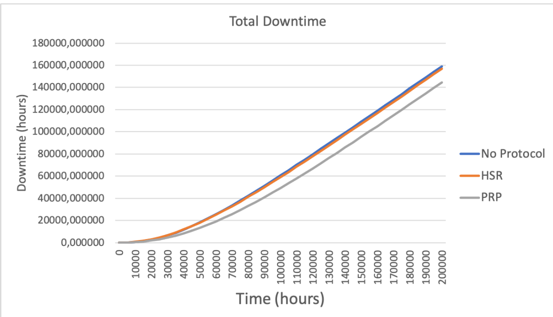
Metric	Value
MTTF	55838,229047

(b) Steady state results for PRP component redundancy with component redundancy

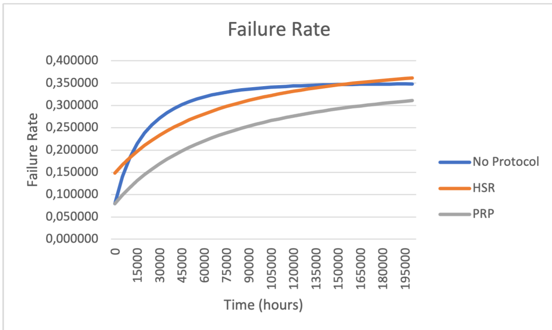
Metric	Value
MTTF	43262,982394

(c) Steady state results for HSR with component redundancy

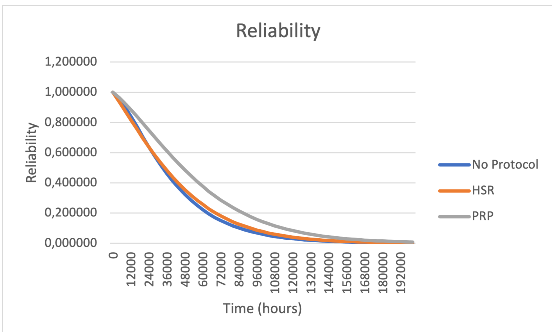
6.1.2.4 Time-Based Results for Non-Repairable Systems With Component Redundancy



(a) Total Downtime of non-repairable systems with component redundancy



(b) Failure rate for non-repairable systems with component redundancy

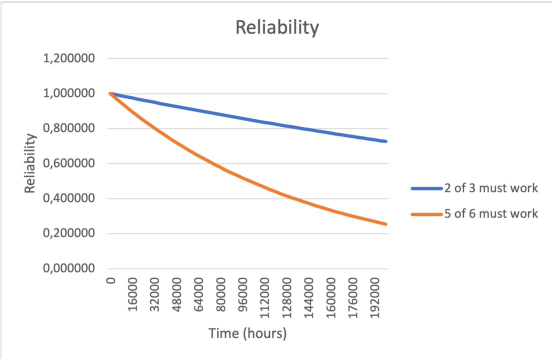


(c) Reliability for non-repairable systems with component redundancy

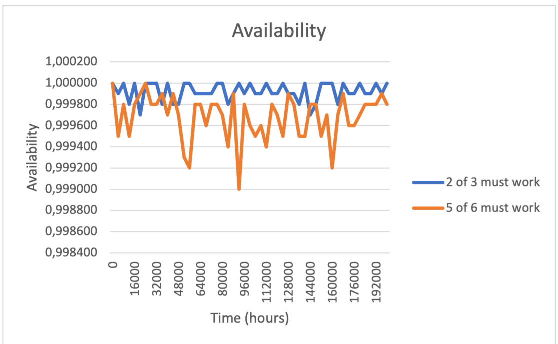
Figure 57: Time-Based Results for Non-Repairable Systems With Component Redundancy

6.2 Results From the HSR Network Comparison Analysis

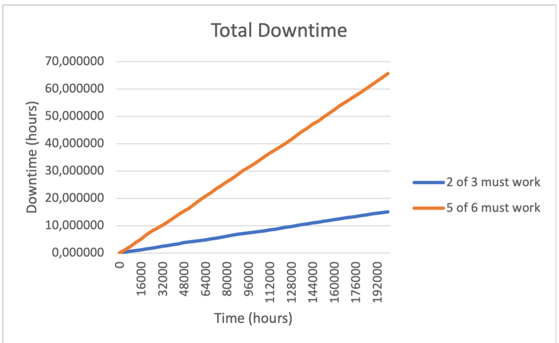
This section unveils the findings of the analysis conducted on the two HSR loops, one consisting of 6 IEDs and the other comprising 12 IEDs. The objective is to investigate how increased components and complexity impact the reliability of the HSR protocol. In Relyence, only time-based results were accessible for this analysis, which are presented in the form of graphs. Notably, the HSR loop with 6 IEDs represents a network where 2 out of 3 must function properly, while the HSR loop with 12 IEDs constitutes a network where 5 out of 6 IEDs must work.



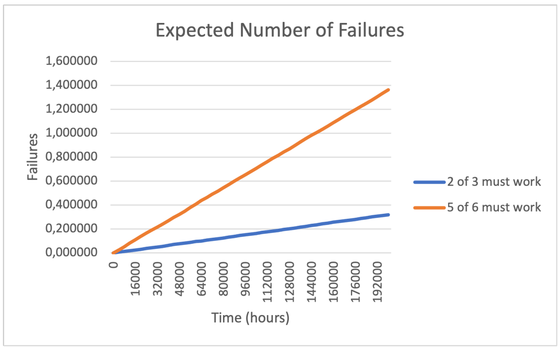
(a) Reliability comparison of the two HSR loops



(b) Availability comparison of the two HSR loops



(c) Total downtime comparison of the two HSR loops



(d) Expected number of failures comparison of the two HSR loops

Figure 58: Time-based results from the two HSR loops, one where 2 out of 3 IEDs must function, the other where 5 out of 6 must function.

6.3 Results From the Substation Comparison Analysis

For the substation comparison analysis, only repairable systems are analyzed. Thus, the results are structured into sections covering results from the two malfunction analyses and then into the subsections of steady-state results and time-based results. Here, maintenance is in focus, the digital systems were given an MTTR of 48 hours, while the conventional systems were given an MTTR of 96 hours.

Steady-state results are presented in tables, whereas time-based results are depicted using graphs. The complete set of time-based results can be found in the appendix.

6.3.1 Circuit Breaker C Malfunction

6.3.1.1 Steady-state results

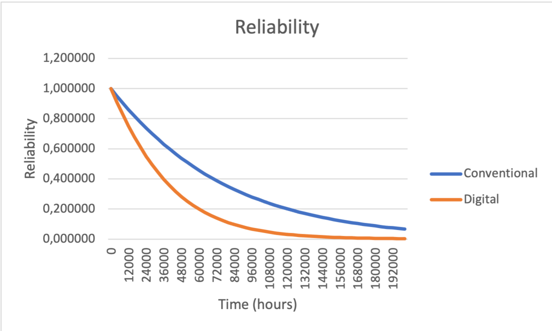
Table 19: Steady state results for circuit breaker C malfunction in conventional substation

Metric	**Value**
MTTF	75076,508503
MTBF	81850.733
MTTR	95,164993
Steady State Availability	0.998600

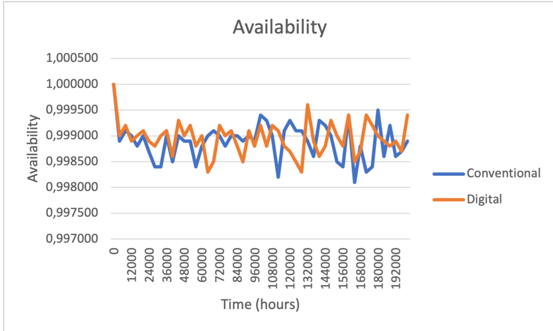
Table 20: Steady state results for Circuit Breaker C malfunction in digital substation

Metric	**Value**
MTTF	37365,489749
MTBF	44317,038924
MTTR	47,988550
Steady State Availability	0.998930

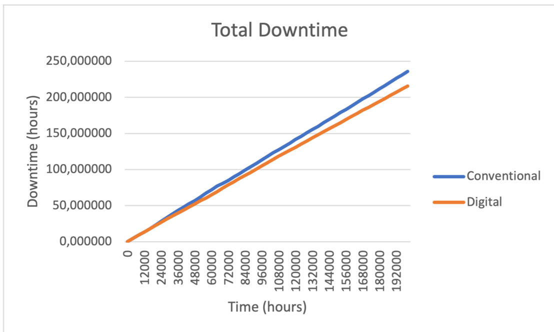
6.3.1.2 Time-based Results



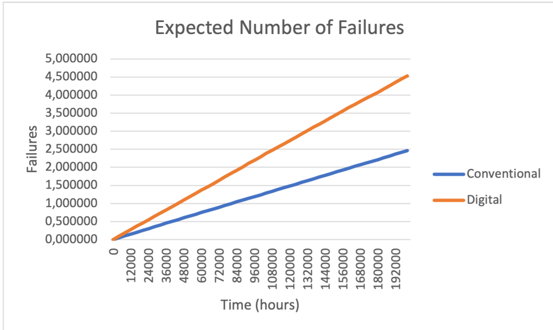
(a) Reliability comparison between digital and conventional station



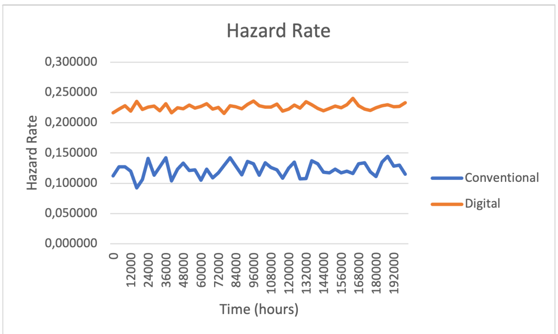
(b) Availability comparison between digital and conventional station



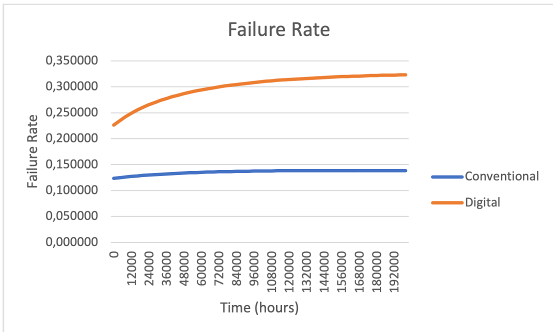
(c) Total downtime comparison between digital and conventional station



(d) Expected number of failures comparison between digital and conventional station



(e) Hazard rate comparison between digital and conventional station



(f) Failure rate comparison between digital and conventional station

Figure 59: Time-based results for circuit breaker 3 malfunction

6.3.2 IED C Malfunction in Conventional Substation and Merging Unit C Malfunction in Digital Substation

6.3.2.1 Steady-state Results

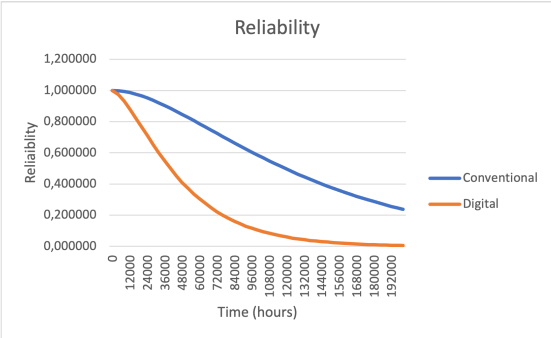
Table 21: Steady state results for IED C malfunction conventional

Metric	**Value**
MTTF	145184,694026
MTBF	Unable to Calculate
MTTR	Unable to Calculate
Steady State Availability	1

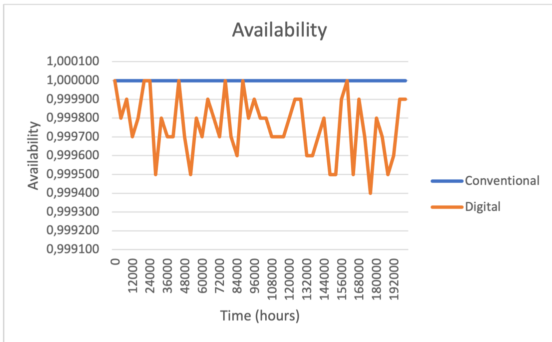
Table 22: Steady state results for merging unit C malfunction digital

Metric	**Value**
MTTF	50359,670096
MTBF	211696,201663
MTTR	47,795562
Steady State Availability	0,999773

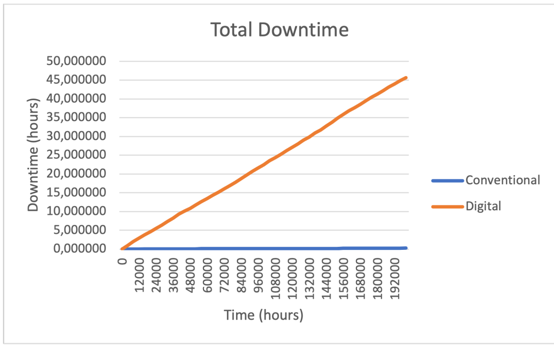
6.3.2.2 Time-based Results



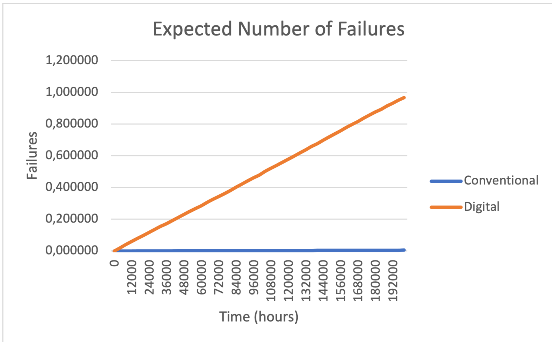
(a) Reliability comparison between digital and conventional station



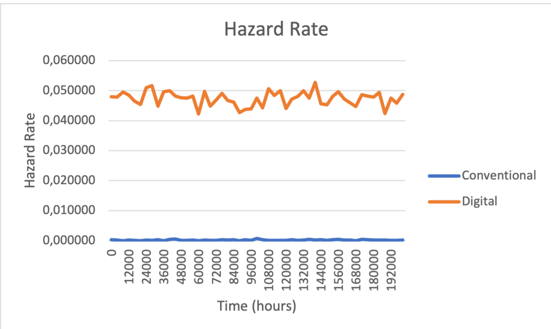
(b) Availability comparison between digital and conventional station



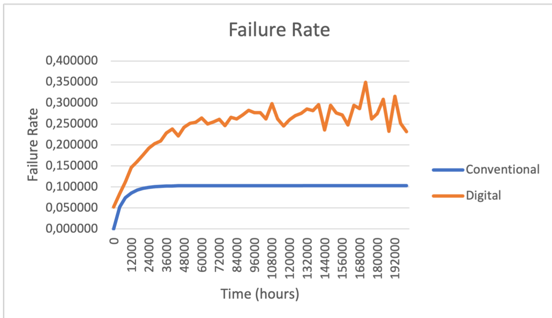
(c) Total downtime comparison between digital and conventional station



(d) Expected number of failures comparison between digital and conventional station



(e) Hazard rate comparison between digital and conventional station



(f) Failure rate comparison between digital and conventional station

Figure 60: Time-based results from merging unit C malfunction in digital and IED C malfunction in conventional

7 DISCUSSION

This discussion chapter delves into the findings of the study, analyzing the results and discussing the limitations of the analysis. The chapter is organized into multiple sections, each focusing on a specific area.

The chapter begins by discussing the challenges of acquiring data on process bus components, highlighting the lack of historical data. Then, there is an explanation of why reliability block diagrams were chosen as the methodology. The discussion then delves into the redundancy protocol comparison analysis, summarizing the results and further discussing the findings. Then, the comparison of digital and conventional substation systems is presented, evaluating the results and a discussion of the impact of maintenance time. Potential vulnerabilities that are found from the results are then given. Finally, the chapter discusses the limitations of the method used, thereby pointing out possible inaccuracies in system reliability estimation due to simplifications.

7.1 Obtaining Data

Obtaining data on the components of a process bus can be challenging. Neither IEC 61850 nor IEEE provides specific failure rates, MTBFs, or availability for the devices and systems it covers. The 2017 Cigre report "Experience Concerning Availability and Reliability of DSAS" [18] states that "The use of process bus is at the top of the list of features not yet exploited enough by vendors and utilities, at the moment the process bus implementations are mostly limited to some pilot substations." Thus, the process bus is a fairly new concept, and historical data on equipment is hard to find. The source of data on MTBF, availability, and failure rate for process bus components used in this research is scientific and technical articles published in academic journals. The data used for calculations are not based on any analysis of the specific equipment and are not applicable for real use.

The absence of real-world data could introduce a significant level of uncertainty in the results. The failure rates, MTBF, and availability derived from these data may not accurately represent the actual behavior of the equipment under study. This could then lead to overestimations or underestimations of the reliability metrics, thereby leading to less accurate results.

While the data does not directly reflect specific equipment or real-world use, it is important to note that the results can still contribute valuable insights into the reliability tendencies of digital substations. This information can aid in identifying potential patterns, trends, and behaviors of these systems. Therefore, while interpreting these findings requires careful consideration, they can still provide valuable insights into the reliability of these redundancy protocols.

7.1.1 The High IED Failure Rate

The failure rate used on IEDs and time synchronization source (TS) in digital substations was retrieved from [6]. This failure rate is high in relation to the other components in the substation system. The reason for this is that IEDs and the time synchronization source are thought to be relatively unstable. This is so because IEDs have a lot of hardware and software operations [90]. Additionally, they are relatively new equipment types. Furthermore, there is a chance that the TS's global time reference will experience interference, be jammed, or be blocked [1]. These high failure rates suggest that these components represent weak links in the system, potentially compromising overall reliability. As a result, the reliability analysis might project a less optimistic outcome.

7.2 Why Reliability Block Diagrams Was Chosen

Reliability block diagrams were chosen as the method for analyzing reliability in this research. This is due to a multitude of reasons. These reasons stem from the complex nature of digital substations and the insights gained from the literature review.

Firstly, the structure of RBDs provides an uncomplicated graphical and mathematical model, outlining how individual components contribute to the success or failure of an entire system. This makes them particularly suitable for representing complex systems like substations, thereby providing clarity and simplicity to the reliability assessment. Furthermore, RBDs can handle a variety of system setups, demonstrating flexibility. This flexibility makes them a good tool for analyzing a variety of architectural circumstances. From the articles [1], [4] and [2] for instance, it was found that RBDs have been used successfully to analyze the reliability of various process bus topologies. This successful application of RBDs in prior research underscores their usefulness in analyzing the reliability of the process bus in digital substations.

7.3 Examining the Results from the Redundancy Protocol Comparison

This chapter examines the results of the analysis comparing the reliability of the no redundancy protocol, HSR, and PRP used in the IEC 61850 process bus. The chapter starts with a summary of the results. These summaries are organized based on whether the systems are repairable or non-repairable, and subsequently by the level of redundancy, beginning with repairable systems that lack component redundancy.

In the analysis, every system has two bays and there are two systems designed for every redundancy protocol, one without component redundancy and the other with it. This method is used to assess how the implementation of more components affects the functionality and resilience of the redundancy protocols. By utilizing these designs, the study aims to identify any potential advantages and disadvantages that may be present in each system. A better knowledge of how redundancy mechanisms handle system complexity and potential weak points may result from this comparison.

The reason behind designing four systems is that it allows for a consideration of a broader range of potential configurations. While there are numerous architectural configurations for implementing PRP and HSR in a process bus, this study aims to examine some representative architectures that can serve as a basis for understanding the overall reliability of these two protocols.

7.3.1 Summary of Results from Repairable Systems

7.3.1.1 Without Component Redundancy

The results for the systems without component redundancy can be seen in table 15 and figure 54. The results show similar trends for all systems, but there are some small differences. The no redundancy protocol system exhibits high availability (mostly 0.99) but varies more than the other two protocols with an average of 0,998356 over the 200 000 hours. It also has the highest downtime (333 hours) and it anticipates more frequent system failures approximately once every 3.3 years. The HSR protocol shows more stable availability with an average of 0,998505 and a similar trend in the hazard rate (0.32-0.35) to the previous system. This accumulates to a lower total downtime (320 hours), and it expects fewer failures - once every 3.4 years. Meanwhile, the PRP protocol stands out, the availability is about the same as for the HSR, but it has a lower hazard rate (0.29-0.35) indicating reliable system stability. It also has the lowest downtime (308 hours), and the least frequent failures, occurring approximately once every 3.57 years. For the MTBF the PRP exhibits an 8.80% increase, while the HSR system only produces a 3.64% increase from the no redundancy protocol system.

7.3.1.2 With Component Redundancy

The results for the repairable systems with component redundancy can be viewed in figure 55 and table 16. Figure 57a shows that the no redundancy protocol system exhibits a high availability with an average of 0,999649. Its hazard rate ranges between 0.063 and 0.104. Over time, both total downtime and expected failures increase linearly. The figure also shows that the HSR protocol doesn't improve availability which now has an average of 0,999305 and fluctuates more than in the previous system. The hazard rate and the total downtime increase as well. Possibly due to added complexities with the protocol. The system grows more complex with all 12 IEDs interconnected, leading to higher downtime and expected failures. According to the results, PRP offers marginally higher availability of 0,999616 and a more compact hazard rate (0.0737-0.0867), suggesting that redundancy aids in maintaining a lower, more consistent risk of failure. Total downtime is lower compared to the HSR system but similar to the no redundancy system, with no significant impact on the total number of failures over time. Looking at the MTBF, the PRP system offers a slight improvement from the no redundancy protocol system being at 123 422 hours (2.52% increase) while the HSR system is much lower than the two other systems being at 67 600 hours which is a 43.87% decrease.

7.3.2 Summary of Results from Non-Repairable systems

7.3.2.1 Without Component Redundancy

The results for the non-repairable systems without component redundancy can be viewed in table 17 and figure 56. These results show only a slight difference between the three systems. Figure 56b reveals that the reliability of the no redundancy protocol system experiences a decline in reliability over time, decreasing to 0.13% after 200,000 hours while figure 56c shows that it has a constant failure rate of 0.349. The HSR system shows similar deterioration but with slightly better performance, reducing reliability to 0.12% and a failure rate of 0.336 failures. The PRP system's reliability decrease is slower, reaching 0.11%, and has an increasing failure rate, starting at 0.320 failures and rising to 0.338 failures. The steady-state results show that there is a minimal increase in MTTF for the two protocols with an increase of 7.68% for the HSR system and a 3.86% increase for the PRP system.

7.3.2.2 With Component Redundancy

The results for the non-repairable systems without component redundancy can be viewed in table 18 and figure 57. The no redundancy protocol system sees a decrease in reliability to 0.1856% after 200,000 hours of operation. Its failure rate, beginning at 0.08, escalates until stabilizing at around 0.34. The HSR system displays marginally better reliability, reaching around 0.2048% after 200,000 hours. Its failure rate increases slightly more to approximately 0.361545. Conversely, the PRP system maintains higher reliability, at approximately 0.7789% after 200,000 hours, with a slower increase in failure rate, peaking at around 0.310777. The Steady-state results show a marginal improvement for the HSR system with only a 5.18% increase in MTTF, while the PRP system shows a 35.79% increase in MTTF from the no redundancy protocol system.

7.3.3 Evaluating the Results from the Redundancy Protocol Comparison

Based on the results presented, there are several elements that can be further discussed regarding the different protocols' performances and the impact of added system complexity.

Among the three protocols, the PRP protocol generally demonstrates superior performance. The PRP systems consistently maintain the highest availability, the lowest hazard rate, the least downtime, and the least frequent failures. It also shows significant improvement in MTBF and MTTF compared to the no-redundancy system, especially when component redundancy is applied.

The HSR protocol shows improvement over the no redundancy protocol in terms of availability and fewer failures, but it is typically surpassed by PRP. This is particularly evident in the repairable system with component redundancy in figure 55, here, the system seems to struggle with the increased complexity. The reliability is greatly reduced, and its hazard rate and downtime increase. This is due to the complexity of the HSR network. The HSR system with component redundancy is interconnected between the two bays, meaning that the reliability block diagram consists of more IEDs than the equivalent PRP and no redundancy protocol RBDs. With this increase in components, there is an increase in the total number of points that could potentially fail. This means there are more opportunities for something to go wrong.

The PRP system is designed in such a way that there is no interconnection between the bays, which results in a more reliable system, mainly because the PRP system's reliability block diagram consists of fewer IEDs than the HSR. This simplicity reduces potential points of failure and complexity. Due to the PRP system's absence of interconnected bays, it is probable that the comparison between HSR and PRP may be skewed, it's important to consider that each system's design aligns with its underlying principles. The PRP system was designed to provide redundant paths for every component in the process bus which was possible without interconnecting the two bays, which makes it inherently less complex than the HSR system resulting in a more reliable system.

7.3.3.1 About the Constant Failure rate

In figure 56c one can see that the failure rate of the no redundancy protocol and HSR process bus are constant while the failure rate of the PRP system increases with time. The explanation for this is that in a system with only series connections, all components need to function for the system to function. A failure in any component leads to a failure of the entire system. The overall system failure rate is essentially the sum of the individual component failure rates. If all components have a constant failure rate, the system failure rate will also be constant. The failure rate of a system with components arranged in series doesn't change with time because the failure of one component doesn't affect the failure rate of the others. Keep in mind that this is only true for systems using constant failure rates like exponential distribution.

On the other hand, in parallel configurations, the system will continue to function as long as at least one component is functioning. When one component fails, the others must bear the full load, and their failure rates increase. Over time, as more and more components fail, the surviving components are increasingly likely to fail, and the system failure rate increases.

7.3.3.2 Discussing the High Availability

A significant factor in the overall system availability is the MTTR. The longer the MTTR, the more downtime the system would experience, and hence the lower the availability would be. The availability in all systems is always above 0.99, which is high and does not accurately depict the real world. This is because the MTBF for these systems is considerably higher than the MTTR. Specifically, in order to achieve an availability of at least 0.99, the MTBF would need to be at least 99 times the MTTR.

The availability equation (16) further clarifies the relationship between MTBF, MTTR, and system availability. By dividing the MTBF by the sum of MTBF and MTTR, the equation determines the availability. Consequently, a larger difference between the MTBF and MTTR leads to higher availability. The assumed MTTR of 48 hours served as a reference point to demonstrate the significance of a shorter repair time on digital substations. But in this assumption, the calculations fail to accurately simulate real-world scenarios.

Thus, the success of these designed systems in achieving such high availability can be attributed to the substantial difference between the MTBF and MTTR. While a shorter MTTR generally contributes to higher system availability, it is crucial to consider the real-world variability of repair times when evaluating the availability of a system. In reality, the MTTR can vary significantly depending on various factors, including the complexity of the system, availability of spare parts, the skill level of maintenance personnel, and operational constraints. By assuming a fixed MTTR, the analysis overlooks the variability and uncertainty associated with repair times.

This limitation impacts the accuracy of availability calculations and the assessment of system performance. Since the MTTR is a crucial component in determining system availability, an assumed fixed value fails to capture the realistic downtime.

7.3.3.3 Comparing Non-Repairable with Repairable Systems

As explained in chapter 4.5, the main difference between non-repairable and repairable systems lies in how downtime affects the overall system's operation. For non-repairable systems, once a failure occurs, the system cannot be restored to its original operating condition. As a result, MTTF is the key measure of reliability, indicating the expected time to the first failure. In contrast, repairable systems can be restored to full functionality after a failure, meaning the system's uptime can be increased with maintenance and repair, therefore the key measures of reliability for these systems are MTBF. If the MTBF is only slightly higher than the MTTF, that suggests that a significant portion of the system's time is being spent in a state of repair rather than operation. If MTBF is significantly higher than MTTF, that would mean less time is spent in repair relative to operational time, increasing the system's overall availability.

From the results it can be seen that the MTBF is significantly higher than the MTTF for all scenarios, showing that despite failures, the system spends more time being operational than in a failed state. This is especially true when component redundancy is introduced. This is a strong indication that repairable systems, especially those with component redundancy, have better reliability than their non-repairable counterparts. Like the high availability, the superior MTBF for the repairable systems can be attributed to the low MTTR and the quick recovery capabilities of the digital substation. This underscores the value of the advanced monitoring system of the digital substation, which opens the opportunity to facilitate rapid repair processes, ultimately increasing the overall operational time and system reliability.

The availability results provided for the non-repairable and repairable systems allow for a comparison of their respective performance. For the non-repairable system, the availability values range from 1.000000 to 0.001319. As time progresses, the availability decreases. This suggests that the system is more prone to failures as time goes on and eventually becomes less reliable.

In contrast, the repairable systems exhibit consistently high availability values. The availability ranges from 1.000 to 0.991. This indicates that the repairable system maintains a high level of operational readiness throughout the observed time period. The availability remains close to 100% over time, indicating that the system experiences very minimal downtime or failures. This suggests that the repairable system is designed to be more reliable and resilient, as it can undergo repairs and restore functionality when failures occur.

7.3.4 Comparing the HSR Networks

Figure 58 provides a comparative view of the HSR loops for systems with component redundancy and those without component redundancy. The first system requires at least 2 out of 3 IEDs to function, while the second system needs at least 5 out of 6 IEDs to work.

Here's the examination of the results from each system:

For the first system (2 of 3 IEDs must work): The reliability gradually decreases to 0.726182 at the end of the study period, which indicates the probability that the system has not failed in the time range. The availability generally remains very close to 1, indicating a high level of system availability throughout the period. This suggests that the system is highly available, typically returning to a functional state relatively quickly after any failures. The total downtime reaches a maximum of 15,087746 hours at the end of the period. The expected number of failures also gradually increases over time, reaching 0.318100 by the end of the period, implying that we expect around 0.318100 failures to occur over the 200,000 hours.

For the second system (5 of 6 IEDs must work): The reliability declines to 0.254142 at the end of the study period, much lower than the first system. This suggests that this system is less reliable than the first one over the long term. The availability also here remains close to 1, but it experiences more dips compared to the first system. This suggests that while the system is highly available, it may experience brief periods of unavailability more frequently than the first system. The total downtime is significantly higher than for the first system reaching 65.67 hours after 200 000 hours of operation. The expected number of failures reaches 1.363100 at the end of the period, again much higher than the first system, suggesting that more failures are expected in this system over the same time period.

When comparing the systems, it appears that the first system (2 out of 3 IEDs must work) is more reliable than the second system (5 out of 6 IEDs must work) over the studied time period. This might seem counterintuitive, as systems with more components, like the second system, are often thought to be more reliable. However, in this case, the reliability of the second system is lower due to its higher threshold for functioning; it needs 5 of 6 IEDs, whereas the first system only needs 2 of 3 IEDs. The increased number of components in the second system does not lead to more redundancy but instead results in more potential points of failure.

If it is assumed that all components have the same failure rate, as the number of components increases, the likelihood of at least one component failing also increases. In the first system, where 2 out of 3 IEDs must work, the system can tolerate a failure rate of up to 33% at any given time and still be functional. However, in the second system, where 5 out of 6 IEDs must work, the system can only tolerate a failure rate of 16.7%. Therefore, the second system is more susceptible to failure due to its lower tolerance for component failure.

From this, it can be drawn that having more components in an HSR loop can decrease the reliability of the network due to the increased possibility of at least one component failing, especially when a significant number of these components must function for the system to work. Therefore, while the HSR protocol's redundancy principle supports high reliability, it's essential to manage the number of components within the network carefully. There should be a balance between adding redundancy and maintaining a level of simplicity to ensure high reliability.

7.4 Examining the Results from the Substation Comparison

This chapter delves into the findings derived from the comparative analysis of digital and conventional substation systems. The discussion starts with a systematic comparison of the results, beginning with outcomes from the circuit breaker malfunction analysis, followed by the comparison of the IED and merging unit malfunction results. Subsequently, the influence of the maintenance time on the two systems is examined. The chapter then explores the vulnerabilities revealed by the results.

As a methodological refresher: The two systems are compared by giving them the same protection coordination and then seeing which coordination system is the most reliable.

This chapter examines the results of the analysis from the substation comparison analysis. The chapter starts with a systematic comparison of the results. Starting with the results from the circuit breaker malfunction and then the results from the IED and merging unit malfunction. After this, it will be looked at what effect the maintenance time of the two systems had. and then a discussion on the vulnerabilities that the results present. A reminder of the method is: The two systems are compared by giving them the same protection coordination and then seeing which coordination system is the most reliable.

Additionally, it should be mentioned that in both digital and conventional systems IEDs are present. However, the MTBF and failure rate assigned to these components differs between the two systems. This differentiation is intentional and was done to illustrate the availability differences between these system setups and to underscore the benefits of employing NCITs, fiber optic cables, and IEC 61850 communication protocols.

7.4.1 Comparing the Results from the Circuit Breaker Malfunction Analysis

Steady-State Results: The steady-state results from the Circuit Breaker C Malfunction Analysis can be viewed in table 19 and 20. The conventional substation's steady-state results exhibit an MTTF of 75 076.51 hours, an MTBF of 81 850.73 hours, an MTTR of 95.16 hours, and a steady-state availability of 99.86%. Conversely, the digital substation displays an MTTF of 37 365.49 hours, an MTBF of 44 317.04 hours, an MTTR of 47.99 hours, and a steady-state availability of 99.89%. These results demonstrate that the conventional substation tends to operate longer without failure, but when a failure occurs, the digital substation is repaired and restored more quickly. Despite the digital substation's shorter MTTF and MTBF, its efficient repair and maintenance process maintains a high steady-state availability, slightly edging out the conventional substation.

Time-Based Results: The time-based results from the Circuit Breaker Malfunction Analysis can be viewed in figure 59. The conventional substation showcases better long-term reliability with a terminal reliability of 0.07 at 200 000 hours, versus 0.002475 for the digital substation. It also has a slower increase in failure rate (0.123 to 0.138) than the digital substation (0.226 to 0.323). Despite this, both systems maintain a high availability of around 0.999 due to efficient repairs. Interestingly, the digital substation, despite its higher failure rate, experiences less total downtime (217.3 hours) than the conventional substation (236.2 hours) by 200 000 hours, hinting at more efficient repairs. The conventional substation also presents fewer expected failures (2.47 vs 4.52) and a lower hazard rate. Thus, despite quicker repair times in digital substations, conventional ones exhibit superior reliability and lower failure rates over the operation time.

7.4.2 Comparing the Results from the IED and Merging Unit Malfunction Analysis

Steady-State Results: The steady-state results from the IED and Merging Unit Malfunction Analysis can be viewed in table 22 and 21. The conventional substation has a higher MTTF of 145 184 hours versus the digital substation's 50 359.67 hours, implying it operates longer before facing a failure. The digital substation, with an MTBF of 211 696.20 hours, suggests a longer interval between failures, whereas the conventional substation's MTBF couldn't be determined, hinting at infrequent failures or limited observation time. Repairs are done faster in the digital substation with an MTTR of 47.80 hours, whereas the conventional substation's MTTR couldn't be assessed. Nevertheless, both systems maintain high steady-state availability - an impeccable 1 for the conventional substation and 99.98% for the digital substation.

Time-Based Results: The time-based results from the IED and Merging Unit Malfunction Analysis can be viewed in figure 60. The conventional substation retains higher reliability, ending at around 23.7% at 200 000 hours versus the digital substation's 0.6%. Despite increased failure rates for both, with the conventional substation ending at 0.096 and the digital substation slightly higher, their availability remains high (perfect 1 for conventional and above 0.9996 for digital), showing effective repair strategies. Downtime increases due to repair needs, with the digital substation showing more because of its higher failure rate. Expected failures rise as components age, being more substantial in the digital substation, indicative of its higher failure rate. The hazard rate follows a similar pattern, suggesting a higher risk for the digital substation due to its increased failure rate.

7.4.3 Evaluating the Results from the Substation Comparison Analysis

It's important to note that the findings do not represent the absolute values of the reliability metrics. Instead, they illustrate the reliability trends, thereby allowing for a comparative analysis between the two types of substations.

According to the results, the conventional substation generally exhibits superior MTTF and MTBF, which implies that they operate longer before encountering a failure and have a longer interval between failures. In the IED and Merging Unit Malfunction Analysis the MTBF was not determinable for the conventional substation, This is due to the perfect availability of the system which will be further discussed in section 7.4.3.2.

When considering the time-based results, conventional substations also consistently show superior reliability over a longer period, with slower increases in failure rates, lower hazard rates, and fewer expected failures over time. This points to fewer malfunction events in conventional systems compared to digital ones over an extended operational timeframe. In contrast, digital substations, while suffering more frequent failures, demonstrate their strengths in MTTR and overall system availability. The shorter MTTR of digital substations implies a more efficient repair and maintenance process, leading to less total downtime over the course of operation in figure 59c. This increased maintenance efficiency is a key attribute of digital systems, where advanced diagnostic tools and automated repair processes can identify and fix issues quickly, thereby minimizing disruption. Even though digital substations show a faster reliability decay over time due to their higher failure rates, the average availability of the digital substation is higher than the conventional in the circuit breaker 3 malfunction analysis. This is also thanks to the digital substations' effective monitoring strategies.

The conventional substation appears to outperform in overall reliability. It displays a greater tendency to operate for longer periods without failure, less frequent failures, and superior reliability in the long term. Therefore, based on the presented results, it can be asserted that the conventional substation is more reliable than the digital substation.

7.4.3.1 Comparing the Maintenance Times

From figure 59b the availability between a conventional and digital substation can be seen. Here, the meaning is to show what effect the difference in maintenance time will have on the availability of the two systems. The conventional system was given an MTTR of 96 hours while the digital system was given half that. Now, the question is how big of an effect this will have on the complete availability of the system.

The conventional system has an average availability of 0.998890, while the digital system, with a shorter MTTR, has an average availability of 0.998939. The difference is minuscule (around 0.005%), and only makes up to 10 more hours of uptime for the digital station over the course of the 200 000 hours. In principle, a shorter MTTR should lead to higher availability because the system is restored to a working state more quickly after a failure. However, this isn't the case according to the results, this is because the system's availability is not only dependent on how quickly a failed system can be repaired but also on how often failures occur (failure rate). As the digital system has a higher failure rate than the conventional one in both investigations the availability is not much greater even though it has half the MTTR. Implying that the added maintenance strategies of the digital system have only a small effect on the availability compared to a conventional system. This is due to the extra components and extra failure points in the digital system.

7.4.3.2 Discussing the Perfect Availability

The analysis of the IED and Merging Unit Malfunction points to an unusual result - the availability of the conventional substation is calculated to be 1. This implies the substation was available 100%

of the time during the analysis period, which is an extraordinarily high level of performance.

This availability figure also impacts the calculation of other significant parameters such as MTBF and MTTR. Due to the perfect availability, the software couldn't derive these values, implying that there might be insufficient failure events to analyze these parameters. Similarly, the total downtime, expected number of failures, and hazard rate are approaching zero, all of which again are highly unusual outcomes in a real-world setting.

The high availability of the conventional substation can be traced back to the components used in the system's Reliability Block Diagram (RBD). As Relyence calculates the availability of the system with equation 16 the reason behind this perfect availability is revealed. These components possess exceptionally high MTBF combined with a relatively low MTTR (only 96 hours). This means that the components in the system rarely fail, and when they do, they are quickly repaired and brought back online. This creates a system that will fail after an extraordinarily long time, as the simulation time for this analysis is only 200 000 hours the availability becomes a perfect 1. Additionally, the decimal points used when calculating availability in Relyence are 6 digits. This should have been sufficient precision.

The perfect availability score of the conventional substation, while remarkable, must be treated with care. While it is possible for a system to have a high MTBF and low MTTR, these results are considered to be near impossible and do not at all reflect the real world

7.5 Unveiling the Vulnerabilities of Digital Substations Revealed by the Results

The transition from conventional to digital substations leads to an increase in system complexity and a shift of potential vulnerabilities and failures. These vulnerabilities are reflected in the results as well as in the failure modes analysis.

7.5.1 The Vulnerability of Added Points of Failure

The data reveals that conventional substations seem to have superior MTTF and MTBF compared to digital substations, indicating they typically operate longer without experiencing a failure. The conventional substation exhibits superior long-term reliability, maintaining significantly higher reliability at 200,000 hours. In addition, despite having faster repair times, the digital substation experiences more total downtime over this period. By looking at these results it is obvious that the conventional substation is a more reliable system. This reveals an important vulnerability of digital substations, namely the addition of multiple components.

Digital substations introduce a higher number of components compared to conventional ones, which inherently increases the potential points of failure. This vulnerability arises from the complex nature of digital systems and the interdependencies among their various components. In contrast, conventional substations have a simpler architecture with fewer components, leading to a reduced likelihood of failures. From this point of view, the analysis suggests that while digital substations offer benefits such as more efficient fault diagnosis processes, their inherent complexity, due to the integration of more components, leads to more frequent and new failure modes.

However, it is crucial to note that this analysis is based on a simple version of the digital substation architecture that lacks component redundancy and employs a ring Ethernet architecture. As a result, this analysis only provides a partial perspective on the reliability of digital substations. The digital substation, as observed in this study, merely adds more components to the system, thus creating more potential points of failure. The reasoning is straightforward: an increase in system components leads to more potential points of failure. Each additional piece of hardware or software amplifies the overall system's failure rate, reducing the MTBF and MTTF. This is what leads to a reduction in reliability compared to conventional substations.

Yet, the reality can differ greatly as there exist multiple strategies to account for this increase in potential points of failure in digital substations. Various redundancy protocols and Ethernet architectures can be employed to manage and mitigate this risk. As the results show, the reliability of the process bus is greatly affected by the redundancy protocol used, and the topology of the system. And the process bus offers many architecture alternatives as well as the HSR or PRP protocols which again can be further enhanced with a hybrid system [5]. So as the digital substation offers great flexibility in the design there might be a potential to compensate for the increased points of failure and enhance the reliability beyond what is seen in this report and perhaps beyond a conventional system.

As such, even though digital substations contain more components and, on the surface, seem to be less reliable, as the articles [3], [1], and [5] show, their flexible design alternatives and extensive use of redundancy protocols can offer high, and potentially superior, reliability.

7.5.2 The Vulnerability of the Communication Network

From the failure modes analysis, it was found that one of the most vulnerable areas in a digital substation is related to digital communication and the communication network. Digital substations bring forth the process bus and a fiber optic communication network, which, in turn, introduce a new set of vulnerabilities due to the increased dependence on a fully operational communication network. Since the functionality of the substation is so tightly linked to digital communication, any instability or inefficiency in the data transmission can have a substantial effect on the overall reliability. In contrast, conventional substations' reliability is more closely tied to the robustness of their physical components.

As a result of this dependence on the communication network, the substation is now susceptible to, among other things, latency, packet loss, and network congestion. According to the findings of the failure modes studies, creating a solid communication architecture that would enable smooth data packet delivery is crucial to addressing these vulnerabilities. This means that the design process for digital substations must now take a broader approach. Incorporating the correct redundancy level, selecting the right Ethernet topology, and implementing monitoring and recovery mechanisms are all essential design considerations for achieving the desired reliability. As well as considering cybersecurity to ensure the security of the station. By carefully planning and implementing a reliable network topology, it is possible to mitigate some of the vulnerabilities introduced by the transition from conventional to digital substations.

In order to design such a network the findings in this research can be helpful. As it is found that a PRP network combined with a star Ethernet architecture will offer a very reliable system topology. The findings also highlight the necessity for a balanced approach in system topology design, where the advantages of additional redundancy are balanced against potential reliability difficulties brought on by increased complexity, as observed in the HSR system where all bays were interconnected.

7.6 Limitations

This chapter attempts to explore the limitations of the reliability analysis employed in this study. The addition of this section became crucial for addressing a crucial issue - the method's clear simplicity.

While simplicity often renders a method user-friendly it will also often provide some shortcomings. In this context, the simplicity of the reliability analysis performed in this study might not fully reflect the intricate realities of the system under consideration. There's a risk that this simplicity might contribute to a wrong estimation of the system's reliability. Therefore, in an effort to provide a more balanced view, this chapter explicitly identifies the limitations of the method employed.

7.6.1 The Limitations of Reliability Block Diagrams

Reliability block diagrams are the foundation of the analysis method used in this study. While these are effective tools in offering a general perspective of a system's reliability, they are not without their drawbacks. RBDs often present an oversimplified view of the system, thereby failing to take into consideration the dynamic nature of system components and their interdependencies. This lack of insight compromises the accuracy of the reliability analysis.

Understanding the dynamics and interdependencies between individual components is crucial for capturing the complete reliability of complex systems like digital substations. Dynamics refer to how the components change and evolve over time. Interdependencies, on the other hand, imply that the functionality or performance of one component could directly affect or be influenced by other components within the same system. Thus, overlooking these factors could lead to an oversimplified analysis, ultimately misrepresenting the true state of the system.

RBDs tend to perform an analysis on a function-by-function basis without considering the potential cascading impact of the loss of one function on subsequent functions. Moreover, RBDs represent a system in only two states; operational (up) and non-operational (down), thereby ignoring the reality that a system can have various degrees of failure. For instance, a partial failure might occur where some functions of a component are malfunctioning, while others remain operational. This diverse range of failure scenarios is not accurately represented in a traditional RBD approach.

For these reasons, researching more complex methods becomes essential. When examining such a complicated system, Markov chains, and Monte Carlo simulations can both offer significant value. Markov chains, for example, can account for the many different states a system can be in and the transitions between these states over time, thus capturing the dynamics of the system. Moreover, the Markov chain can model interdependencies between components, providing a more realistic representation of the system's reliability. The transition probabilities in a Markov chain describe the likelihood of moving from one state to another. These probabilities can be given by the dependencies between components. For example, if the failure of an IED drastically increases the likelihood of circuit breaker failure, this would be reflected in the transition probabilities from states where the IED is operational, to states where it has failed. A state in a Markov chain can also represent various levels of component degradation. This means that the Markov chain can model a component as it degrades from fully operational, through various stages of reduced efficiency, to completely failed.

On the other hand, Monte Carlo simulations stand out for their ability to model a broad array of scenarios, effectively handling the dynamic and interdependent nature of system components. They offer a more accurate depiction of the time-dependent behavior of components, considering factors such as aging, wear and tear, and maintenance activities. Unlike RBDs, these simulations are not restricted to binary 'up' or 'down' states and can thus represent various degrees of functionality and failure states. Additionally, like the Markov chain, they can capture the complex interdependencies within the digital substation, acknowledging the potential cascading impact of a failure in one component on the rest of the system.

Models that fail to consider these interdependencies and dynamics, like reliability block diagrams, can provide a limited and potentially misleading view of system reliability. They treat components independently and ignore the reality that a component's reliability is often interwoven with the functioning of others.

7.6.2 The Limitations of MTTR

MTTR provides a generalized view of maintenance efficiency by calculating the average repair time [3]. Using this provides some drawbacks, primarily because MTTR overlooks the variability of repair times. Since it's an average, it may mask instances where repair times fluctuate significantly. Some failures might require quick fixes, while others may demand prolonged repair periods due to their complexity or the availability of spare parts. A singular average value could obscure such variables, failing to give insights into the failure's severity

It offers an average time value but fails to detail the causes of failures or the exact nature of repairs conducted. It does not reveal the context of the repairs, whether they were complex or simple. This lack of detail can prevent an understanding of the system's reliability and hinder the development of effective preventive maintenance strategies.

Furthermore, MTTR's focus is inherently on corrective maintenance after a failure has occurred, which means it does not account for preventive maintenance efforts [91]. Therefore, in the context of digital versus conventional substations, it fails to capture the real effects of the preventive maintenance done by the digital substations monitoring systems and the improvement in system reliability this offers. Consequently, the benefits of the advanced monitoring system including fewer breakdowns, reduced maintenance costs, and improved system availability, may not be reflected properly when using MTTR. Additionally, a substation may be a system with frequent but quick repairs that may yield a low MTTR, mistakenly implying a high-reliability system. However, the frequent need for repairs might suggest poor system reliability, despite the rapid repair time.

Thus, the MTTR's simplicity may render it unsuitable for complex systems. The single average value fails to capture the complexities of substation reliability, limiting the results of an MTTR analysis.

7.6.3 The Limitations of Exponential Distribution

Exponential distribution was used as the time model for the failure rate in this research. This is a mathematically convenient method and has its limitations, for instance, the assumption of "memorylessness". This means that no matter how long a component has been operating without failure, the failure rate remains the same. Using this assumption the analysis fails to capture the dynamics of the system. Meaning, it fails to capture how the components change over time. For instance, an increased load on the substation might speed up wear and tear on the components. This results in aging and the components become more prone to failures, which is a pattern that the exponential distribution cannot capture. It also fails to capture the start-up phase of a system where the failure rate is at a decreasing phase. Another limitation is that the exponential distribution can't account for any dependency between components. For example, the failure rate of one component might be affected by the state of another component, or by environmental conditions, or maintenance activities. Therefore, while the exponential distribution can be useful for modeling the failure behavior of components in simple systems, it may not capture the full complexity and dynamics of substations.

An alternative to exponential distribution is the Weibull distribution which was discussed in chapter 4.4.1. This probability distribution method can provide a more realistic and accurate failure rate model compared to the exponential distribution. The Weibull distribution, with its shape and scale parameters, can effectively model increasing failure rates to simulate the aging of equipment. Furthermore, the Weibull distribution can capture the effects maintenance activities have on the failure rate, in contrast to the exponential distribution where it always remains constant. But since this analysis only focused on the useful life period it was felt that the exponential distribution was a reasonable assumption.

8 CONCLUSION

To achieve the intended purpose of the study reliability block diagrams of several process bus systems have been built and analyzed. Also, line diagrams of both a digital and conventional substation have been created and analyzed in order to prove the reliability difference between the two systems.

The results clearly show that a conventional substation is more reliable than a digital substation. This is thanks to the implementation of a process bus in a digital substation, which introduces additional potential points of failure, which increases the overall probability of failure for the substation system. However, there is a potential to enhance the reliability of the digital system, as this study shows introducing duplicate components, star Ethernet topology, and the PRP protocol will increase the reliability of the process bus, suggesting a potential way to improve the robustness of the digital system.

In the case of digital communication, it exposes the digital substation to a new set of vulnerabilities. Notably, the failure modes analysis revealed that the Ethernet communication network presents the most significant vulnerability in the digital substation. This necessitates a solid communication architecture that ensures smooth data packet delivery and incorporates proper redundancy levels, and an appropriate Ethernet topology.

In conclusion, the conventional substation seems to have higher reliability, but designing a digital substation that integrates efficient network topology with robust redundancy protocols can enhance reliability. The combination of PRP and star Ethernet topology could be a promising solution to achieve this objective.

8.1 Further Research

Further research could make use of other reliability assessment methods like the Markov chain method to explore the dynamics and interdependencies between the components of the process bus. Also, going further into depth on what effect the communication network and data model have on the reliability of the protection system would be of great interest. This investigation leads to further questions, for instance; Do the IEC 61850 protocol, data model, and the fact that the IEDs operate with binary language create a more responsive and reliable protection system? And how much more reliable do the IEDs become when operating with this protocol? To what level do the fiber optic cables enhance the reliability of the IEDs?

Further research could also take a cost analysis into consideration. As explained in chapter 4.1.1, the investment cost increases as more reliability is required. It would be interesting to find out what the optimal relationship between cost and reliability is. Also, what are the financial benefits of utilizing a digital system in contrast to a conventional one? Are they more expensive to build or are they cheaper to run?

Bibliography

[1] N. Liu, M. Panteli and P. Crossley, 'Reliability evaluation of a substation automation system communication network based on iec 61850', in *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*, IET, 2014, pp. 1–6.

[2] J.-C. Tournier and T. Werner, 'A quantitative evaluation of iec61850 process bus architectures', in *IEEE PES General Meeting*, IEEE, 2010, pp. 1–8.

[3] X. Sun and M. Redfern, 'Process bus configurations for protection schemes in the digital substation: Iec 61850', in *2011 46th International Universities' Power Engineering Conference (UPEC)*, 2011, pp. 1–6.

[4] S. Gupta, A. Gandhar and M. Tiwari, 'Reliability analysis of a novel iec 61850-9-2 process-bus based substation automation system architecture', *Journal of Statistics and Management Systems*, vol. 23, no. 1, pp. 65–75, 2020.

[5] M. G. Kanabar and T. S. Sidhu, 'Reliability and availability analysis of iec 61850 based substation communication architectures', in *2009 IEEE Power & Energy Society General Meeting*, IEEE, 2009, pp. 1–8.

[6] P. Pinchukov and S. Makasheva, 'Estimation of digital substation reliability indices', in *International Scientific Siberian Transport Forum*, Springer, 2019, pp. 3–14.

[7] R. Loenders, D. Van Hertem, J. Beerten, G. Chaffey and L. Yang, 'Testing reliability performance of iec61850-based digital substations', in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, 2020, pp. 1–7. DOI: 10.1049/cp.2020.0126.

[8] S. Xu, J. Ma, L. Cao *et al.*, 'Reliability evaluation of centralized protection system in smart substation considering impact of communication message', in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2018, pp. 1–6. DOI: 10.1109/EI2.2018.8582424.

[9] B. Falahati and E. Chua, 'Failure modes in iec 61850-enabled substation automation systems', in *2016 IEEE/PES Transmission and Distribution Conference and Exposition*, 2016, pp. 1–5. DOI: 10.1109/TDC.2016.7520066.

[10] A. Altaher, H. Madi and A. Khomsi, 'Reliability investigation of digital substation networks design using fmea technique', in *International Conference on Technical Sciences (ICST2019)*, vol. 6, 2019, p. 04.

[11] B. Falahati, M. J. Mousavi and M. Vakilian, 'Latency considerations in iec 61850-enabled substation automation systems', in *2011 IEEE Power and Energy Society General Meeting*, 2011, pp. 1–8. DOI: 10.1109/PES.2011.6039138.

[12] R. Feizimirkhani, A. I. Bratcu, Y. Bésanger, A. Labonne and T. Braconnier, 'A methodology for the evaluation of the message transmission delay over iec 61850 communication network—a real-time hv/mv substation case study', *Sustainable Energy, Grids and Networks*, vol. 28, p. 100 555, 2021.

[13] M. G. Kanabar and T. S. Sidhu, 'Performance of iec 61850-9-2 process bus and corrective measure for digital relaying', *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 725–735, 2010.

[14] R. Loenders, D. Van Hertem, J. Beerten, G. Chaffey and L. Yang, 'Testing reliability performance of iec61850-based digital substations', 2020.

[15] K. B. Øverby, 'Theoretical framework and methodology assessment for calculating reliability in an iec 61850 process bus', vol. 1, p. 60, 2022.

[16] R. Billinton and W. Li, 'Basic concepts of power system reliability evaluation', in *Reliability assessment of electric power systems using Monte Carlo methods*, Springer, 1994, pp. 9–31.

[17] E. Article. 'Equipment used in substation'. (), [Online]. Available: http://electricalarticle.com/equipment-used-in-substation/ (visited on 14th Dec. 2022).

[18] M. PETRINI, R. LØKEN, E. CASALE and A. DARBY, *Experience Concerning Availability and Reliability of DSAS*. Cigre, 2017.

[19] M. Bamber, M. Bergstrom and Darby, 'Protective relays, measurement and control', *Network Protection and Automation Guide*, vol. 4, 2011.

[20] A. Altaher, 'Implementation of a dependability framework for smart substation automation systems: Application to electric energy distribution', Ph.D. dissertation, Université Grenoble Alpes, 2018.

[21] M. Mekkanen, R. Virrankoski, M. Elmusrati and E. Antila, 'Reliability evaluation and comparison for next-generation substation function based on iec 61850 using monte carlo simulation', Feb. 2013, pp. 1–6, ISBN: 978-1-4673-2820-3. DOI: 10.1109/ICCSPA.2013.6487306.

[22] O. HANS-ERIK, W. THOMAS and R. PETER, 'Impact of the process bus', 2022.

[23] H. S. Horowitz, 'Power system relaying', pp. 25–28, 2019.

[24] Y. Zhang, A. Sprintson and C. Singh, 'An integrative approach to reliability analysis of an iec 61850 digital substation', in *2012 IEEE Power and Energy Society General Meeting*, 2012, pp. 1–8. DOI: 10.1109/PESGM.2012.6345699.

[25] V. M. Viswanatham, A. Chari and V. Saritha, 'Region-based group and hierarchical key management for secure smart grid communications', *International Journal of Smart Grid and Green Communications*, vol. 1, no. 1, pp. 50–61, 2016.

[26] A. Waleed, U. S. Virk, M. T. Riaz *et al.*, 'Effectiveness and comparison of digital substations over conventional substations', *Advances in Science, Technology and Engineering Systems Journal*, vol. 4, no. 4, pp. 431–439, 2019.

[27] Toshiba. 'What is digital substation?' (), [Online]. Available: https://www.global.toshiba/ww/products-solutions/transmission/products-technical-services/protection-relay/digital-substation.html (visited on 29th Nov. 2022).

[28] R. H. Khan and J. Y. Khan, 'A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network', *Computer Networks*, vol. 57, no. 3, pp. 825–845, 2013.

[29] I. Tools. 'What are analog and digital signals? differences, examples'. (), [Online]. Available: https://instrumentationtools.com/what-are-analog-and-digital-signals-differences-examples/ (visited on 18th Dec. 2022).

[30] Diffen. 'Analog vs. digital'. (), [Online]. Available: https://www.diffen.com/difference/Analog_vs_Digital (visited on 18th Dec. 2022).

[31] Analog. 'Electromagnetic interference (emi) filtering reduces errors in precision analog applications'. (), [Online]. Available: https://www.analog.com/en/analog-dialogue/articles/how-emi-filtering-reduces-errors.html (visited on 18th Dec. 2022).

[32] I. E. COMMISSION, 'Instrument transformers – part 9: Digital interface for instrument transformers', in *IEC 61869-9*, 2016.

[33] I. communication networks, 'Communication networks and systems for power utility automation', *IEC 61850-1*, 2020.

[34] R. Mackiewicz, 'Overview of iec 61850 and benefits', in *2006 IEEE Power Engineering Society General Meeting*, 2006, 8 pp.-. DOI: 10.1109/PES.2006.1709546.

[35] T. Sidhu and P. Gangadharan, 'Control and automation of power system substation using iec61850 communication', in *Proceedings of 2005 IEEE Conference on Control Applications, 2005. CCA 2005.*, 2005, pp. 1331–1336. DOI: 10.1109/CCA.2005.1507316.

[36] E. E. Portal. 'What is the digital substation and what makes it digital?' (), [Online]. Available: https://electrical-engineering-portal.com/digital-substation#osi-model (visited on 7th Dec. 2022).

[37] N. Ali, B. Mohd Ali, O. Basir, M. L. Othman, F. Hashim and E. Aker, 'Science & technology opportunity for using wlan with iec 61850 and the future of this protocol', *Pertanika Journal of Science and Technology*, vol. 25, pp. 25–38, Jan. 2017.

[38] P. Bishop and N.-K. C. Nair, Eds., *IEC 61850 Principles and Applications to Electric Power Systems* (CIGRE Green Books), en. Cham: Springer International Publishing, 2022, ISBN: 978-3-031-06911-6 978-3-031-06912-3. DOI: 10.1007/978-3-031-06912-3. [Online]. Available: https://link.springer.com/10.1007/978-3-031-06912-3 (visited on 10th Oct. 2022).

[39] Masterclock. 'How does gps network time synchronization work?' (), [Online]. Available: https://www.masterclock.com/support/library/gps-network-time-synchronization (visited on 21st Dec. 2022).

[40] V. Skendzic, I. Ender, G. Zweigle *et al.*, 'Iec 61850-9-2 process bus and its impact on power system protection and control reliability', in *proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA*, 2007.

[41] ISO/IEC, 'Information technology — sensor networks: Sensor network and its interfaces for smart grid system', *ISO/IEC 30101*, vol. 1, Nov. 2014.

[42] E. Notes. 'What is an ethernet switch & how it works'. (), [Online]. Available: https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/what-is-ethernet-switch-how-it-works.php (visited on 22nd Dec. 2022).

[43] G. S. Antonova, S. Sastry and B. Vasudevan, 'Review of digital substation communication technologies', in *2022 75th Annual Conference for Protective Relay Engineers (CPRE)*, 2022, pp. 1–26. DOI: 10.1109/CPRE55809.2022.9776567.

[44] G. S. Antonova, S. Sastry and B. Vasudevan, 'Review of digital substation communication technologies', in *2022 75th Annual Conference for Protective Relay Engineers (CPRE)*, IEEE, 2022, pp. 1–26.

[45] IEEE. '802.1w - rapid reconfiguration of spanning tree'. (), [Online]. Available: https://www.ieee802.org/1/pages/802.1w.html (visited on 21st Dec. 2022).

[46] R. W. Billinton and R. Allan, *Reliability Evaluation of Engineering Systems*. Springer, 1992.

[47] Siemens. 'Siprotec 5 process bus'. (), [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cache.industry.siemens.com/dl/files/460/109742460/att_1029776/v1/SIP5_Processbus_V08.30_Manual_C054-5_en.pdf (visited on 14th Dec. 2022).

[48] S. Chen, Y. Du, L. Song, Q. Shen and L. Zhang, 'Principle and testing technology of process bus in smart substations', in *IEC 61850-Based Smart Substations*, Elsevier, 2019, pp. 91–146.

[49] S. Content. 'Circuit breaker control ied application in high voltage substations'. (), [Online]. Available: https://switchgearcontent.com/2021/04/26/2781/circuit-breaker-control-ied-application-in-high-voltage-substations/ (visited on 12th Dec. 2022).

[50] T. S. Sidhu and Y. Yin, 'Modelling and simulation for performance evaluation of iec61850-based substation communication systems', *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1482–1489, 2007. DOI: 10.1109/TPWRD.2006.886788.

[51] M. A. M. Younis, 'Reliability study for process bus based substation considering various practical process bus architectures', in *2016 Saudi Arabia Smart Grid (SASG)*, 2016, pp. 1–9. DOI: 10.1109/SASG.2016.7849665.

[52] C. Singh, P. Jirututujaroen and J. Mitra, *Electric Power Grid Reliability Evaluation*. IEEE Press Editorial Board, 2019.

[53] R. Billinton, *Power system reliability evaluation*. Taylor & Francis, 1970.

[54] H. Hajian-Hoseinabadi and M. E. H. Golshan, 'Availability, reliability, and component importance evaluation of various repairable substation automation systems', *IEEE Transactions on Power Delivery*, vol. 27, no. 3, pp. 1358–1367, 2012. DOI: 10.1109/TPWRD.2012.2187935.

[55] I. communication networks, 'Industrial communication networks - high availability automation networks - part 3: Parallel redundancy protocol (prp) and high-availability seamless redundancy (hsr)', *IEC 62439-3*, 2021.

[56] R. Billinton and W. Zhang, 'Cost related reliability evaluation of bulk power systems', *International journal of electrical power & energy systems*, vol. 23, no. 2, pp. 99–112, 2001.

[57] L. Xu, H. Li and L. Chen, 'Modeling and performance analysis of data flow for hsr and prp under fault conditions', in *2018 IEEE Power & Energy Society General Meeting (PESGM)*, 2018, pp. 1–5. DOI: 10.1109/PESGM.2018.8586044.

[58] T. Industrial. 'Hsr/prp redundancy protocols for high-availability smart grid networks'. (), [Online]. Available: https://www.tttech-industrial.com/resource-library/blog-posts/hsr-prp/ (visited on 10th Oct. 2022).

[59] S. Kumar, N. Das and S. Islam, 'High performance communication redundancy in a digital substation based on iec 62439-3 with a station bus configuration', in *2015 Australasian Universities Power Engineering Conference (AUPEC)*, 2015, pp. 1–5. DOI: 10.1109/AUPEC.2015.7324838.

[60] M. Goraj and R. Harada, 'Migration paths for iec 61850 substation communication networks towards superb redundancy based on hybrid prp and hsr topologies', in *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*, 2012, pp. 1–6. DOI: 10.1049/cp.2012.0055.

[61] L. Xu, H. Li, L. Chen, C. Patterson and P. Mohapatra, 'Assessment and analysis of different process bus redundancy networks performance for iec61850-based digital substation', *The Journal of Engineering*, vol. 2018, no. 15, pp. 856–860, 2018.

[62] A. Rushdi, 'Partially-redundant systems: Examples, reliability, and life expectancy', *IMACST: International Magazine on Advances in Computer Science and Telecommunications*, vol. 1, pp. 45–47, Jan. 2010.

[63] W. G. B5.06, 'Maintenance strategies for digital substation automation systems', *CIGRE TECHNICAL BROCHURES*, 2011.

[64] P. Lloret, J. L. Velásquez, L. Molas-Balada, R. Villafáfila, A. Sumper and S. Galceran-Arellano, 'Iec 61850 as a flexible tool for electrical systems monitoring', in *2007 9th International Conference on Electrical Power Quality and Utilisation*, IEEE, 2007, pp. 1–6.

[65] A. Apostolov, 'Efficient maintenance testing in digital substations based on iec 61850 edition 2', *Protection and Control of Modern Power Systems*, vol. 2, pp. 1–14, 2017.

[66] N. Moreira, E. Molina, J. Lázaro, E. Jacob and A. Astarloa, 'Cyber-security in substation automation systems', *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1552–1562, 2016.

[67] A. Direct, 'Mtbf and product reliability', vol. 1, p. 3, 2010.

[68] H. F. Martz, 'Reliability theory', in *Encyclopedia of Physical Science and Technology (Third Edition)*, R. A. Meyers, Ed., Third Edition, New York: Academic Press, 2003, pp. 143–159, ISBN: 978-0-12-227410-7. DOI: https://doi.org/10.1016/B0-12-227410-5/00659-1. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B0122274105006591.

[69] P.
bibinitperiod Systems. 'The bathtub curve as applied to pumping systems'. (), [Online]. Available: https://www.pumpsandsystems.com/bathtub-curve-applied-pumping-systems/ (visited on 18th Oct. 2022).

[70] CueMath. 'Probability density funtion'. (), [Online]. Available: https://www.cuemath.com/data/probability-density-function/ (visited on 12th Jun. 2023).

[71] R. King. 'How to calculate mttf'. (), [Online]. Available: https://www.rowse.co.uk/blog/post/how-to-calculate-mttf (visited on 10th Dec. 2022).

[72] R. Automation. 'Mean time between failures'. (), [Online]. Available: https://www.fiixsoftware.com/maintenance-metrics/mean-time-between-fail-maintenance/ (visited on 9th Jun. 2023).

[73] BMC. 'Reliability vs availability: What's the difference?' (), [Online]. Available: https://www.bmc.com/blogs/reliability-vs-availability/ (visited on 30th Nov. 2022).

[74] B. W. Tuinema, J. Rueda Torres, A. Stefanov, F. Gonzalez-Longatt and M. van der Meijden, *Probabilistic Reliability Analysis of Power Systems*. Springer, 2020.

[75] ReliaSoft. 'The weibull distribution'. (), [Online]. Available: https://reliawiki.org/index.php/The_Weibull_Distribution (visited on 7th Jun. 2023).

[76] TWI-Global. 'What is simulation? what does it mean? (definition and examples)'. (), [Online]. Available: https://www.twi-global.com/technical-knowledge/faqs/faq-what-is-simulation (visited on 19th Dec. 2022).

[77] Reliasoft. 'System reliability, availability, and maintainability analysis'. (), [Online]. Available: https://www.reliasoft.com/products/blocksim-system-reliability-availability-maintainability-ram-analysis-software (visited on 12th Dec. 2022).

[78] Relyence. 'Relyence reliability block diagram (rbd): High performance system modeling'. (), [Online]. Available: https://relyence.com/2017/10/12/relyence-reliability-block-diagram-rbd-high-performance-system-modeling/ (visited on 20th May 2023).

[79] Relyence. 'A guide to system modeling using reliability block diagram (rbd) analysis'. (), [Online]. Available: https://relyence.com/2021/06/07/guide-to-rbd-analysis/ (visited on 13th Apr. 2023).

[80] M. PETRINI, R. LØKEN, E. CASALE and A. DARBY, *Experience Concerning Availability and Reliability of DSAS*. Cigre, 2017.

[81] H. Ge and S. Asgarpoor, 'Reliability and maintainability improvement of substations with aging infrastructure', *IEEE Transactions on Power Delivery*, vol. 27, no. 4, pp. 1868–1876, 2012. DOI: 10.1109/TPWRD.2012.2198672.

[82] IEC/TC56, 'Industrial communication networks', *IEC 61784-3-1*, 2010.

[83] Elecricalaxis. 'Iec 61850 communication networks and systems in substations: An overview for users'. (), [Online]. Available: http://www.electricalaxis.com/2021/04/IEC%5C%2061850%5C%20Communication%5C%20Networks%5C%20and%5C%20Systems%5C%20In%5C%20Substations.html (visited on 27th Mar. 2023).

[84] D. Baigent, M. Adamiak, R. Mackiewicz and G. Sisco, 'Iec 61850 communication networks and systems in substations: An overview for users', *SISCO Systems*, 2004.

[85] SGRwin. 'Basic understanding of iec 61850'. (), [Online]. Available: https://www.sgrwin.com/basic-understanding-iec-61850/ (visited on 27th Mar. 2023).

[86] R. Loenders, D. Van Hertem, J. Beerten, G. Chaffey and L. Yang, 'Testing reliability performance of iec61850-based digital substations', in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, 2020, pp. 1–7. DOI: 10.1049/cp.2020.0126.

[87] J. Starck, W. Wimmer and K. Majer, 'Switchgear optimization using iec 61850-9-2', in *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*, 2013, pp. 1–4. DOI: 10.1049/cp.2013.0616.

[88] S. Electric. 'What is the mean time between failures (mtbf) for 140cpu67861 in hours ?g'. (), [Online]. Available: https://www.se.com/us/en/faqs/FA358479/ (visited on 22nd May 2023).

[89] Siemens. 'Mean time between failure best estimate on all instrumentation products'. (), [Online]. Available: https://support.industry.siemens.com/cs/document/21444300/mtbfbe-sitrans-f-us-mean-time-between-failure-best-estimate-on-all-instrumentation-products?dti=0%5C&lc=en-SK (visited on 10th May 2023).

[90] Y. Hu, P. Zhang, Y. Su and Y. Zou, 'An optimal reliability allocation method for digital substation systems', in *PES T&D 2012*, 2012, pp. 1–5. DOI: 10.1109/TDC.2012.6281562.

[91] R. Automation. 'Mean time to repair (mttr)'. (), [Online]. Available: https://www.fiixsoftware.com/maintenance-metrics/mean-time-to-repair-maintenance/ (visited on 9th Jun. 2023).

Appendix

A Repairable Systems

No Redundancy Protocol Results

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,349000	1,000000	0,000000	0,000000
10000	0,705393	0,349000	0,998200	17,139963	0,358000
20000	0,497579	0,349000	0,998100	34,218001	0,707600
30000	0,350989	0,349000	0,998200	51,256810	1,067600
40000	0,247585	0,349000	0,998300	68,287070	1,418800
50000	0,174645	0,349000	0,997900	85,206070	1,770500
60000	0,123193	0,349000	0,997800	102,266601	2,116700
70000	0,086900	0,349000	0,998100	119,383579	2,461700
80000	0,061298	0,349000	0,998100	136,070625	2,811900
90000	0,043240	0,349000	0,998000	153,183734	3,155500
100000	0,030501	0,349000	0,998600	170,593169	3,510500
110000	0,021515	0,349000	0,998100	187,994484	3,864500
120000	0,015177	0,349000	0,998000	204,093167	4,207100
130000	0,010705	0,349000	0,998700	219,844908	4,544600
140000	0,007552	0,349000	0,997800	236,991575	4,900500
150000	0,005327	0,349000	0,998900	253,716882	5,247300
160000	0,003758	0,349000	0,998000	270,149895	5,595400
170000	0,002651	0,349000	0,998400	287,258567	5,945900
180000	0,001870	0,349000	0,998800	304,241521	6,299600
190000	0,001319	0,349000	0,998600	320,811700	6,646600
200000	$9,303023E-004$	0,349000	0,999100	337,801288	6,996000

Table 23: Time-based results for no redundancy protocol, repairable, no component redundancy

PRP without component redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,320000	1,000000	0,000000	0,000000
10000	0,725556	0,321612	0,998800	15,199267	0,319900
20000	0,525618	0,323094	0,998400	30,332743	0,636100
30000	0,380235	0,324461	0,998300	46,124031	0,967200
40000	0,274702	0,325725	0,998800	61,122595	1,284100
50000	0,198218	0,326898	0,998000	77,260833	1,613800
60000	0,142868	0,327987	0,998200	92,442083	1,939800
70000	0,102865	0,329002	0,998700	107,885816	2,260200
80000	0,073991	0,329949	0,998500	123,454930	2,585900
90000	0,053172	0,330835	0,998400	138,385164	2,902900
100000	0,038179	0,331664	0,998900	153,935373	3,232700
110000	0,027391	0,332443	0,998100	169,382449	3,547300
120000	0,019637	0,333174	0,998000	185,523236	3,878000
130000	0,014068	0,333863	0,998300	200,896961	4,197700
140000	0,010071	0,334512	0,998400	216,019319	4,512100
150000	0,007206	0,335124	0,997800	231,858499	4,836300
160000	0,005152	0,335702	0,998300	247,016297	5,151900
170000	0,003682	0,336250	0,999200	262,072092	5,472200
180000	0,002630	0,336768	0,998300	277,615406	5,790200
190000	0,001878	0,337259	0,998100	292,306397	6,099600
200000	0,001340	0,337725	0,998200	307,707838	6,422300

Table 24: Time-based results for PRP with no component redundancy, repairable

HSR with no component redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,335998	1,000000	0,000000	0,000000
10000	0,714625	0,335998	0,999200	16,218450	0,338000
20000	0,510689	0,335998	0,998100	32,427011	0,682500
30000	0,364951	0,335998	0,997500	47,905343	1,012300
40000	0,260803	0,335998	0,997800	64,687701	1,355300
50000	0,186376	0,335998	0,998500	80,443903	1,682100
60000	0,133189	0,335998	0,998600	97,105383	2,021300
70000	0,095180	0,335998	0,998400	113,228114	2,356700
80000	0,068018	0,335998	0,998500	129,879572	2,690900
90000	0,048607	0,335998	0,998800	145,223695	3,015000
100000	0,034736	0,335998	0,998500	161,147769	3,350800
110000	0,024823	0,335998	0,998300	177,124272	3,682400
120000	0,017739	0,335998	0,998400	193,333786	4,018600
130000	0,012677	0,335998	0,997500	210,149354	4,359500
140000	0,009059	0,335998	0,999000	226,449880	4,697500
150000	0,006474	0,335998	0,998200	242,703624	5,040000
160000	0,004626	0,335998	0,998500	259,204521	5,382600
170000	0,003306	0,335998	0,998500	275,386344	5,716900
180000	0,002363	0,335998	0,997900	291,532656	6,050400
190000	0,001688	0,335998	0,998000	307,754870	6,380600
200000	0,001207	0,335998	0,998000	322,990314	6,711400

Table 25: Time-based results for HSR no component redundancy, repairable

A.0.1 Repairable Systems With Component Redundancy

No Redundancy Protocol with component redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,080000	1,000000	0,000000	0,000000
10000	0,871765	0,182674	0,998600	3,823763	0,083100
20000	0,704515	0,233079	0,998300	7,792131	0,167400
30000	0,545369	0,271753	0,999700	11.493518	0,249000
40000	0,410755	0,293717	0,999300	15,104743	0,325000
50000	0,303783	0,308709	0,999500	19,021929	0,407000
60000	0,221850	0,319262	0,999700	22,884945	0,482500
70000	0,160579	0,326854	0,998400	25,652418	0,560200
80000	0,115471	0,332399	0,999600	30,535668	0,641300
90000	0,082638	0,335497	0,999400	34,320357	0,722900
100000	0,053931	0,339549	0,999300	38,453013	0,305100
110000	0,041914	0,341838	0,999400	42,122254	0,835000
120000	0,029752	0,343561	0,999800	46,053544	0,965600
130000	0,021087	0,344864	0,999400	50,177738	1,047500
140000	0,014928	0,345851	0,999800	53,944838	1,128700
150000	0.010559	0,346600	0,999700	57,598111	1,208600
160000	0,007464	0,347170	0,999500	61,691549	1,295300
170000	0,005274	0,347604	0,998600	65,472928	1,379300
180000	0,003725	0,347934	0,999500	69,232544	1,459300
150000	0,002630	0,348187	0,999700	72,832515	1,538300
200000	0,001856	0,348379	0,999500	75,535203	1,517300

Table 26: Time-based results for no redundancy protocol repairable system system with component redundancy.

PRP with component redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,080000	1,000000	0,000000	0,000000
10000	0,906102	0,115881	0,999300	4,332732	0,084800
20000	0,794937	0,144923	0,999800	8,115133	0,165200
30000	0,679256	0,168869	0,999500	12,057434	0,247200
40000	0,567829	0,188915	0,999800	15,893449	0,327500
50000	0,465999	0,205909	0,999600	19,407235	0,404400
60000	0,376461	0,220468	0,999700	23,062897	0,481100
70000	0,300037	0,233054	0,999400	26,872845	0,559100
80000	0,236334	0,244019	0,999600	30,942017	0,646800
90000	0,184254	0,253636	0,999700	34,983626	0,727700
100000	0,142359	0,262121	0,999600	38,829310	0,808700
110000	0,109114	0,269645	0,999800	42,903222	0,891400
120000	0,083041	0,276348	0,999800	46,585432	0,967000
130000	0,062799	0,282343	0,999200	50,659045	1,050400
140000	0,047222	0,287725	0,999800	54,650610	1,128600
150000	0,035327	0,292573	0,999800	58,674107	1,213500
160000	0,026308	0,296951	0,999100	62,536612	1,293000
170000	0,019509	0,300916	0,999900	66,251245	1,371400
180000	0,014413	0,304516	0,999800	70,339584	1,452700
190000	0,010612	0,307791	0,999500	74,357805	1,533700
200000	0,007789	0,310777	0,999700	78,477575	1,615000

Table 27: Time-based results for repairable PRP system with component redundancy.

HSR with component redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,148493	1,000000	0,000000	0,000000
10000	0,846810	0,182763	0,999100	7,293022	0,149400
20000	0,695379	0,210322	0,999100	14,613927	0,302300
30000	0,556956	0,232901	0,999200	22,361713	0,457500
40000	0,436993	0,251683	0,999200	29,054533	0,598100
50000	0,337007	0,267504	0,999200	36,353194	0,750400
60000	0,256131	0,280973	0,999500	43,570418	0,900800
70000	0,192249	0,292545	0,998800	50,675136	1,047200
80000	0,142753	0,302563	0,999200	57,669344	1,189300
90000	0,105014	0,311295	0,999100	64,479737	1,332700
100000	0,076622	0,318950	0,999200	71,770765	1,481200
110000	0,055506	0,325696	0,999200	78,904939	1,633500
120000	0,039955	0,331667	0,998800	86,177932	1,789200
130000	0,028599	0,336974	0,999300	93,593379	1,944300
140000	0,020369	0,341707	0,999600	100,970281	2,095900
150000	0,014442	0,345942	0,999400	108,306727	2,245100
160000	0,010199	0,349741	0,999300	115,465506	2,391600
170000	0,007176	0,353159	0,999200	122,392954	2,538100
180000	0,005033	0,356241	0,999300	129,242980	2,686000
190000	0,003520	0,359025	0,999000	136,146140	2,837000
200000	0,002455	0,361545	0,999500	143,715671	2,987500

Table 28: Time-based results for HSR with component redundancy Repairable

B Non-Repairable Systems

B.0.1 Non-Repairable Systems Without Component Redundancy

No protocol no Component Redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures.
0	1,000000	0,349000	1,000000	0,000000	0,000000
10000	0,705393	0,349000	0,705393	1558,543239	0,294607
20000	0,497579	0,349000	0,497579	5603,997954	0,502421
30000	0,350889	0,349000	0,350889	11403,702375	0,649011
40000	0,247585	0,349000	0,247585	18440,843793	0,752415
50000	0,174545	0,349000	0,174645	26350.853530	0,825355
60000	0,123193	0,349000	0,123193	34876.605957	0,876307
70000	0,065800	0,349000	0,085900	43835,674950	0,913100
80000	0,051298	0,349000	0,051298	53103,114883	0,938702
90000	0,043240	0,349000	0,043240	62s85,655772	0,956760
100000	0,030501	0,349000	0,030501	72220,652543	0,969499
110000	0,021515	0,349000	0,021515	81963,191177	0,973485
120000	0,015177	0,349000	0,015177	91781,572752	0,984823
130000	0,010705	0,349000	0,010705	101653,460467	0,589295
140000	0,007552	0,349000	0,007552	111563,091044	0,992448
150000	0,005327	0,349000	0,005327	121499,345175	0,984573
160000	0,003758	0,348000	0,003758	131454,379378	0,996242
170000	0,002651	0,349000	0,002551	141422,660914	0,997349
180000	0,001870	0,349000	0,001870	151400,287026	0,988130
190000	0,001319	0,349000	0,001319	161384,504738	0,996681
200000	$9,303023E-004$	0,349000	$9,303023E-004$	171373,372119	0,989070

Table 29: Time-based results for No protocol, non-repair, no Component Redundancy

PRP With No Component Redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,320000	1,000000	0,000000	0,000000
10000	0,725556	0,321612	0,725556	1444,320905	0,274444
20000	0,525618	0,323094	0,525618	5241,304753	0,474382
30000	0,380235	0,324461	0,380235	10750,690381	0,619765
40000	0,274702	0,325725	0,274702	17504,206546	0,725298
50000	0,198218	0,326898	0,198218	25160,138834	0,801782
60000	0,142868	0,327987	0,142868	33469,633244	0,857132
70000	0,102865	0,329002	0,102865	42251,797532	0,897135
80000	0,073991	0,329949	0,073991	51375,363968	0,926009
90000	0,053172	0,330835	0,053172	60745,224057	0,946828
100000	0,038179	0,331664	0,038179	70292,566838	0,961821
110000	0,027391	0,332443	0,027391	79967,673512	0,972609
120000	0,019637	0,333174	0,019637	89734,664192	0,980363
130000	0,014068	0,333863	0,014068	99567,675384	0,985932
140000	0,010071	0,334512	0,010071	109448,083494	0,989929
150000	0,007206	0,335124	0,007206	119362,491406	0,992794
160000	0,005152	0,335702	0,005152	129301,270622	0,994848
170000	0,003682	0,336250	0,003682	139257,507108	0,996318
180000	0,002630	0,336768	0,002630	149226,240052	0,997370
190000	0,001878	0,337259	0,001878	159203,912770	0,998122
200000	0,001340	0,337725	0,001340	169187,977103	0,998660

Table 30: Time-based results for PRP with no component redundancy, non-repairable

HSR With No Component Redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,335998	1,000000	0,000000	0,000000
10000	0,714625	0,335998	0,714625	1506,631553	0,285375
20000	0,510689	0,335998	0,510689	5437,060415	0,489311
30000	0,364951	0,335998	0,364951	11099,594805	0,635049
40000	0,260803	0,335998	0,260803	17999,934661	0,739197
50000	0,186376	0,335998	0,186376	25784,840929	0,813624
60000	0,133189	0,335998	0,133189	34201,880240	0,866811
70000	0,095180	0,335998	0,095180	43070,657465	0,904820
80000	0,068018	0,335998	0,068018	52262,257779	0,931982
90000	0,048607	0,335998	0,048607	61684,555460	0,951393
100000	0,034736	0,335998	0,034736	71271,715186	0,965264
110000	0,024823	0,335998	0,024823	80976,689410	0,975177
120000	0,017739	0,335998	0,017739	90765,856788	0,982261
130000	0,012677	0,335998	0,012677	100615,190676	0,987323
140000	0,009059	0,335998	0,009059	110507,521042	0,990941
150000	0,006474	0,335998	0,006474	120430,577753	0,993526
160000	0,004626	0,335998	0,004626	130375,592272	0,995374
170000	0,003306	0,335998	0,003306	140336,298382	0,996694
180000	0,002363	0,335998	0,002363	150308,218092	0,997637
190000	0,001688	0,335998	0,001688	160288,151316	0,998312
200000	0,001207	0,335998	0,001207	170273,811198	0,998793

Table 31: Time-based results for HSR no component redundancy, non-repairable

B.0.2 Non-Repairable Systems With Component Redundancy

No Redundancy Protocol With Component Redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,080000	1,000000	0,000000	0,000000
10000	0,871765	0,182674	0,871765	576,286179	0,128235
20000	0,704615	0,238079	0,704615	2687,863428	0,295385
30000	0,545369	0,271753	0,545369	6454,498951	0,454631
40000	0,410755	0,293717	0,410755	11696,961566	0,589245
50000	0,303788	0,308709	0,303788	18146,675276	0,696212
60000	0,221860	0,319262	0,221860	25537,567856	0,778140
70000	0,160579	0,326854	0,160579	33640,653669	0,839421
80000	0,115471	0,332399	0,115471	42272,146176	0,884529
90000	0,082638	0,336497	0,082638	51290,404118	0,917362
100000	0,058931	0,339549	0,058931	60589,046737	0,941069
110000	0,041914	0,341838	0,041914	70089,547394	0,958086
120000	0,029752	0,343561	0,029752	79734,634706	0,970248
130000	0,021087	0,344864	0,021087	89482,896886	0,978913
140000	0,014928	0,345851	0,014928	99304,576342	0,985072
150000	0,010559	0,346600	0,010559	109178,387971	0,989441
160000	0,007464	0,347170	0,007464	119089,158768	0,992536
170000	0,005274	0,347604	0,005274	129026,100294	0,994726
180000	0,003725	0,347934	0,003725	138981,556364	0,996275
190000	0,002630	0,348187	0,002630	148950,101516	0,997370
200000	0,001856	0,348379	0,001856	158927,895276	0,998144

Table 32: Time-based results for No protocol, non-repair, Component Redundancy

PRP With Component Redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,080000	1,000000	0,000000	0,000000
10000	0,906102	0,115881	0,906102	448,707619	0,093898
20000	0,794937	0,144923	0,794937	1935,066409	0,205063
30000	0,679256	0,168869	0,679256	4564,569036	0,320744
40000	0,567829	0,188915	0,567829	8335,379421	0,432171
50000	0,465999	0,205909	0,465999	13175,702724	0,534001
60000	0,376461	0,220468	0,376461	18974,223544	0,623539
70000	0,300037	0,233054	0,300037	25602,644636	0,699963
80000	0,236334	0,244019	0,236334	32931,011610	0,763666
90000	0,184254	0,253636	0,184254	40837,188732	0,815746
100000	0,142359	0,262121	0,142359	49211,973820	0,857641
110000	0,109114	0,269645	0,109114	57961,186540	0,890886
120000	0,083041	0,276348	0,083041	67005,804906	0,916959
130000	0,062799	0,282343	0,062799	76280,952966	0,937201
140000	0,047222	0,287725	0,047222	85734,303149	0,952778
150000	0,035327	0,292573	0,035327	95324,265230	0,964673
160000	0,026308	0,296951	0,026308	105018,190883	0,973692
170000	0,019509	0,300916	0,019509	114790,721821	0,980491
180000	0,014413	0,304516	0,014413	124622,341916	0,985587
190000	0,010612	0,307791	0,010612	134498,150969	0,989388
200000	0,007789	0,310777	0,007789	144406,852652	0,992211

Table 33: Time-based results for PRP component redundancy, non-repairable

HSR With Component Redundancy

Time	Reliability	Failure Rate	Availability	Total Downtime	Expected Number of Failures
0	1,000000	0,148493	1,000000	0,000000	0,000000
10000	0,846810	0,182763	0,846810	760,841782	0,153190
20000	0,695379	0,210322	0,695379	3057,084787	0,304621
30000	0,556956	0,232901	0,556956	6809,259181	0,443044
40000	0,436993	0,251683	0,436993	11856,002962	0,563007
50000	0,337007	0,267504	0,337007	18002,554967	0,662993
60000	0,256131	0,280973	0,256131	25052,026942	0,743869
70000	0,192249	0,292545	0,192249	32823,234297	0,807751
80000	0,142753	0,302563	0,142753	41159,098011	0,857247
90000	0,105014	0,311295	0,105014	49929,010118	0,894986
100000	0,076622	0,318950	0,076622	59027,701753	0,923378
110000	0,055506	0,325696	0,055506	68372,355402	0,944494
120000	0,039955	0,331667	0,039955	77899,067170	0,960045
130000	0,028599	0,336974	0,028599	87559,304243	0,971401
140000	0,020369	0,341707	0,020369	97316,692535	0,979631
150000	0,014442	0,345942	0,014442	107144,274222	0,985558
160000	0,010199	0,349741	0,010199	117022,260600	0,989801
170000	0,007176	0,353159	0,007176	126936,245170	0,992824
180000	0,005033	0,356241	0,005033	136875,814975	0,994967
190000	0,003520	0,359025	0,003520	146833,490863	0,996480
200000	0,002455	0,361545	0,002455	156803,930650	0,997545

Table 34: Time-based results for HSR with component redundancy non-repairable

NTNU

Norwegian University of
Science and Technology