Implementation of a dependability framework for smart substation automation systems : application to electric energy distribution

Ahmed Altaher

Communauté
UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir le grade de
DOCTEUR DE LA COMMUNAUTE UNIVERSITE GRENOBLE ALPES
Spécialité : **Automatique Productique**
Arrêté ministériel : 25 mai 2016

Présentée par
Ahmed ALTAHER

Thèse dirigée par **Jean-Marc THIRIET, Professeur, UNIVERSITE GRENOBLE ALPES**, et
Codirigée par **Stéphane MOCANU, Maitre de conférences, GRENOBLE INP**

Préparée au sein du **Laboratoire GIPSA-lab.**
Dans **l'École Doctorale EEATS**

Mise en œuvre d'un cadre de sûreté de fonctionnement pour les systèmes d'automatisation de sous-stations intelligentes : application à la distribution de l'énergie électrique

Thèse soutenue publiquement le **27/2/2018** , devant le jury composé de :
M Abdelaziz BENSRHAIR
Professeur à l'INSA de Rouen, Président
M Abdessamad KOBI
Professeur à l'Université d'Angers, Rapporteur
M Éric RONDEAU
Professeur à l'Université de Lorraine, Rapporteur
M Stéphane MOCANU
Maitre de conférences à Grenoble INP, Examinateur
M Jean-Marc THIRIET
Professeur à l'Université Grenoble Alpes, Examinateur

Implementation of Dependability Framework for Smart Substation Automation Systems: Application to Electric Energy Distribution

Ahmed ALTAHER

Submitted in fulfillment of the requirements for the Degree of Doctor of Philosophy

Doctoral School of Electrical and Electronic Engineering, Automatic Control and Signal Processing

University Grenoble Alpes

Abstract

Since its invention, Electricity has played a vital role in our everyday life. The appearance of the first power production facilities in the late nineteenth century paved the way for the electrical power system and its subsystems. Consumers of electric power demand dependable service in terms of power grid stability and safety. Since the liberalization of the markets, producers of electric power, utilities and equipment suppliers, as principal players, are following an emerging trend to satisfy consumers' demands. This trend involves improving technologies, innovating and respecting standards requirements and governments' regulations. All these efforts termed as the concept of the Smart Grid that is evolving to meet future demands.

Modern and future digital substations shape essential nodes in the grid, where stability of electric power flow, converting of voltage levels and protecting switchyard equipment are among the primary roles of these nodes. The promising standard IEC 61850 and its parts, bring new features to the substation automation systems. The use of Ethernet based communication within these systems reduces the amount of hardwired connections that results in lowering footprint of substation equipment, devices and their cabling.

Integration of the new IEC 61850 features at the substation levels requires multidiscipline competences. For instance, consider power protection and control tasks from one side and information and communication technologies from the other side. Dependency between substation automation functions and communication networks inside a substation brings new kinds of challenges to designers, integrators and testers. Thus, investigating the dependability of the system functionalities, e.g. the protection schemes, requires new methods of testing where conventional methods are not applicable. The new techniques should provide means to evaluate performance of designed systems and checking their conformance to the standards requirements.

In order to improve the designed system dependability, this work aims to develop methods for testing the IEC 61850 enabled substation automation systems, especially on the process and the bay levels, in a platform dedicated for research tasks. This platform incorporates state-of-art devices and test-set cards that will help to simultaneously observe dynamic interactions of the power transients and communication network perturbations. Data obtained during the experimental tests will be used for diagnosing of failures and classifying their causes in order to remove them and enhance dependability of the designed system.

Résumé

Depuis son invention, l'électricité joue un rôle essentiel dans notre vie quotidienne. L'apparition des premières installations de production d'électricité à la fin du XIX^{ème} siècle a ouvert la voie au système électrique et à ses sous-systèmes. Les consommateurs d'énergie électrique exigent un service fiable en termes de stabilité et de sécurité du réseau électrique. Depuis la libéralisation des marchés, les producteurs d'énergie électrique, les fournisseurs de services publics et d'équipements, en tant qu'acteurs principaux, suivent une tendance émergente pour satisfaire les demandes des consommateurs. Cette tendance implique l'amélioration des technologies, l'innovation et le respect des normes et des réglementations gouvernementales. Tous ces efforts ont été qualifiés de concept de réseaux intelligents (Smart Grid en anglais) qui évolue pour répondre aux demandes futures.

Les sous-stations numériques modernes et futures façonnent des nœuds essentiels dans le réseau électrique, où la stabilité du flux d'énergie électrique, la conversion des niveaux de tension et la protection de l'équipement du poste de commutation figurent parmi les principaux rôles de ces nœuds. La norme prometteuse CEI 61850 et ses composants apportent de nouvelles fonctionnalités aux systèmes d'automatisation des postes. L'utilisation de la communication Ethernet dans ces systèmes réduit la quantité de connexions câblées qui réduit l'encombrement de l'équipement de la sous-station, des dispositifs et de leur câblage.

L'intégration des nouvelles fonctionnalités CEI 61850 au niveau des sous-stations requiert des compétences multidisciplinaires. Par exemple, considérons les tâches de protection et de contrôle de la puissance d'un côté et les technologies de l'information et de la communication de l'autre. La dépendance entre les fonctions d'automatisation des sous-stations et les réseaux de communication à l'intérieur d'une sous-station pose de nouveaux défis aux concepteurs, intégrateurs et testeurs. Ainsi, étudier la fiabilité des fonctionnalités du système, par exemple, les schémas de protection, exige de nouvelles méthodes d'essai où les méthodes conventionnelles ne sont pas applicables. Les nouvelles techniques devraient fournir des moyens d'évaluer les performances des systèmes conçus et de vérifier leur conformité aux exigences des normes.

Afin d'améliorer la fiabilité du système conçu, ce travail vise à développer des méthodes pour tester les systèmes d'automatisation de sous-station CEI 61850, en particulier sur les processus et les niveaux de la baie, dans une plate-forme dédiée aux tâches de recherche. Cette plate-forme incorpore des dispositifs de pointe et des cartes de test qui aideront à observer simultanément les interactions dynamiques des transitoires de puissance et les perturbations du réseau de communication. Les données obtenues lors des tests expérimentaux seront utilisées pour diagnostiquer les défaillances et classer leurs causes afin de les supprimer et d'améliorer la fiabilité du système conçu.

Table of Contents

List of Figures

List of tables

List of Abbreviations

ACSI	Abstract Communication Service Interface
AIS	Air Insulated Substation
BN	Bayesian Network
CB	Circuit Breaker
CDC	Common Data Class
CFC	Continuous Functional Chart
CID	Configured IED Description
CIGRE	Conseil International des Grands Réseaux Électriques
CPF	Conditional Probability Function
CPT	Conditional Probability Table
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSV	Comma Separated Values
CT	Current Transducer
DAG	Direct Acyclic Graph
DBN	Dynamic Bayesian Network
DES	Discrete Event Simulators
DOS	Denial of Service
DUT	Device under test, IED under test
ECMA	European Computer Manufactures Association
EHV	Extra High Voltage
EM	Expectation Maximization
EPA	Enhanced Performance Architecture
EPRI	Electric Power Research Institute
ESW	Ethernet Switch
EUC	Equipment Under Control
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
Gbps	Giga bit per second
GIS	Gas Insulated Substation
GOOSE	Generic Object Oriented Substation Events
GSE	Generic Substation Events
GSSE	Generic Substation State Events
HITL	Hardware In The Loop
HMI	Human Machine Interface
HV	High Voltage
ICD	IED Capability Description
ICMP	Internet Control Message protocol
IEA	International Energy Agency
IEC	*International Electrotechnical Commission*
IED	Intelligent Electronic Device
IEEE	International Institute of Electric and Electronic Engineering
ISO	International Standard Organization
Ktoe	Kiloton of oil equivalent
LAN	Local Area Network
LD	Logical Device
LLN0	Logical Node zero
LN	Logical Node
LPHD	Logical Physical Device
LTPLTC	Load Tap Changer
MAC	Media Access Control
Mbps	Mega bit per second
MMS	Manufacturing Message Specification
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MU	Merging Unit
NCC	Network Control Center
NCIT	Non-Conventional Instrument Transducer
NTP	Network Time Protocol
OMNET++	Objective Modular Network Testbed in C++
OPNET	Optimized Network Engineering Tools
PC	Personal Computer
PHD	Physical Device
PICOM	Piece of Information for COMmunication
PICS	Protocol Implementation Conformance Statement
PSRC	Power System Relaying and Control committee
PTP	Precision Time Protocol
RBD	Reliability Block Diagram
RPN	Ranked Priority Number
RTDS	Real Time Digital Simulator
RTT	Round Trip Time
RTU	Remote Terminal Unit
SAMU	Stand Alone Merging Unit
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description
SCL	Substation Configuration Language
SCSM	Specific Communication Service Mapping
SDN	Software Defined Networks
SIL	Safety Integrity Level
SITL	Software In The Loop
SLD	Single Line Diagram
SMV	Sampled Measured Values
SNTP	Simple Network Time Protocol
SPAN	Switch Ports Analysis Node
SSD	System Specification Description
SV	Sampled Value
TC57	Technical Committee 57
TCP/IP	Transmission Control Protocol/Internet Protocol
TS	Time Source
UCA	Utility Communication Architecture
UDP	User Datagram Protocol
VLAN	Virtual LAN (see LAN)
VT	Voltage Transducer
WAN	Wide Area Network
XML	eXtensible Markup Language

Dedication

To my mother, my wife, my daughter and to those who enlightened me during my life.

Acknowledgement

An enormous work embracing a doctoral study is seldom accomplished without help and support from surrounded people. I would like to express my deepest thanks to all who helped me to undergo this study.

Kind moments with my advisor have inspired me to undergo this unique experience. I am grateful for Mr. Jean-Marc Thiriet, his wisdom valuable guidance throughout all phases of the research project. Grateful thanks for punctual technical and academic support of my supervisor Mr. Stéphane Mocanu.

I sincerely acknowledge reviewers and examiners of my thesis Mr. Kobi, Mr. Rondeau and Mr. Bensrahier. It is a privilege to have you all as part of the examination committee.

Appreciation and thanks for Mr. Serge Germiano for his appropriate logistical aid at the industrial platform.

Remembering moments of useful discussions, I memorize every steps at GIPSA-Lab, starting with an internship, continuing a journey to doctoral study. Special thanks for my office mates and department (DAUTO) colleagues. Thanks for warmhearted friendly environment that is enriched by international human experiences. Thanks for GIPSA-lab football teammates. Thanks for all academic, administrative and technical staff at GIPSA-lab.

With emotions to end up this acknowledgment with appreciation for every word that encourages me to continue. Thanks for my wife for her patience and support.

chapter 1 : Introduction

Since its invention, electricity has played a vital role in our everyday life. The appearance of the first power production facilities in the late nineteenth century paved the way for the electrical power system and its subsystems; generation, transmission and distribution. Consumers of electrical power demand dependable services in terms of power grid stability and safety. Since the liberalization of the markets, producers of electrical power, utilities and equipment suppliers, as principal players, are following an emerging trend to satisfy consumers' demands. This trend involves improving technologies, innovating and respecting evolved standards requirements and governments' regulations.

Standardization bodies and governmental agencies assist emerging technologies by proposing standards and regulations. Hence, several efforts have resulted in proposing standards that are attempting to cover all these emerging technologies by considering demands of consumers, utilities and power suppliers. These efforts have paved the way for involving information technology, power engineering, communication engineering, and related disciplines. All these efforts termed as the concept of the Smart Grid that exists to meet future demands. Power transmission and distribution substations are involved in the efforts of new standardization trends.

Modern and future digital substations shape essential nodes in the grid, where stability of electric power flow, converting of voltage levels and protecting switchyard equipment are among the primary roles of these nodes. The promising standard IEC 61850 and its parts, bring new features to the substation automation systems. Among these features are the use of Ethernet-based communications within these systems that reduce the number of hardwired connections, the attempts to achieve interoperability among devices from different vendors, exploiting of data from devices with the integration of SCADA functionalities, as well as the flexibility of protection and control schemes, etc.

The standard and its parts provide flexibility of measurements, fault events recording, supervision, protection and control functionalities, and other interconnected functions inside the substations. The editions of this standard have evolved to achieve interoperability among protection relays, intelligent electronic devices and equipment manufactured and provided by different suppliers of substation automation systems.

Modern and future digital substations will include IEC 61850 enabled features. Integration of these features at many levels within the substation requires experience that covers

multidiscipline tasks. For instance, consider power protection and control skills from one side and information and communication technology skills from the other side.

Once more, the raising of new technologies and standards' evolvement will increase complexity because new competencies and knowledge are required. Understanding the IEC 61850 standard and related systems requirements is an essential task to face these challenges. The communication network involved in these systems bring new tasks in which designers and integrators should inspect conformity of devices to performance requirements of the standards that generally insist on reliability and safety of protection and control messages. Hence, the network state and behavior, e.g., service quality, may influence the performance.

Designers, integrators and testers should consider these issues. When a service performance no longer agrees with the specifications required, then a failure could occur. One of the purposes of diagnosis is to mitigate and prevent this condition by identifying the root causes of this failure, during testing or operation.

Dependency between substation automation functions and communication networks inside a substation brings new kinds of challenges to designers, integrators and testers. Thus, investigating the dependability of the system functionalities, e.g., the protection schemes, requires new methods of testing where conventional methods are not applicable. The new techniques should provide means to evaluate the performance of designed systems, that include communication networks, and to check their conformance to the standards requirements. Analyses of quality of service (QoS) of a communication network are essential to evaluate the impact on the dependability of the system.

This work aims to develop methods for dynamic testing of the IEC 61850 based protection schemes to assist design and validation of protection functions and data networks inside future substation systems. This study also provides a comprehensive understanding of using of relevant subsystems especially the Ethernet networks for measurements, protection and control communications at process and bay levels. The data that were obtained during performance evaluation and tests were used for evidence-based diagnosis of causes in case malfunctions or failures take place, especially on the quality of service of the communication network. Some issues arise from the specific aims: 1) How devices interactions, i.e. measurement and protection devices, can influence the Ethernet network and what will be consequences on the protection schemes? 2) Will tests involve, evaluate and observe dynamics of both power transients and perturbations, e.g., high traffic, of data networks? Moreover, 3) How data

obtained during these tests can be used for diagnosis of failure causes and predicting dependability of devices, protections schemes or a whole system?. This approach examines whether dependability techniques are suitable and can be applied to Smart Grid technologies.

The QoS is defined and covered network throughput, frames delay, delay variation (jitter), alteration and loss of frames for the device under test. To take into account the complexity of the system and to perform a realistic evaluation, we decided to work on a platform that incorporates several state-of-the-art industrial devices and equipment. This platform includes, but is not limited to; network equipment, computer-based engineering workstations, HMI (Human-Machine Interface) screens, protection and control devices such as PLCs (Programmable Logic Controllers), IEDs (digital protective relays named intelligent electronic devices). Power protection and control IEDs include transformer differential, overcurrent protection, feeder protection, and bay controllers from different suppliers.
We developed real power protection schemes. We also performed some experimentations on the platform to 1) evaluate the performance of the protection messages (IEC 61850 GOOSE frames), 2) to check the limits considering the available bandwidth and several traffic scenarios, and 3) to check if the network perturbations would cause the GOOSE exchanging service to no longer meet the performance requirements. During these experiments, we adjusted a dynamic scenario where both power transients and network high traffic profiles were performed simultaneously.
At the end of this work, we proposed evaluations of reliability, inherent availability, and functional safety. In addition, The IEC 61850 GOOSE frames were investigated according to safety requirements. Diagnosing causes of malfunctions and failures were performed using the data obtained from all experiments. The diagnosis was built into a Bayesian model that was developed according to a proposed architecture.

This PhD thesis is divided into eight chapters. This general introduction introduces the manuscript and presents the problem. The main aims and questions are provided. To contribute to the field of dependability of smart digital substation systems, the work organization and the proposed approach are highlighted.

The second chapter provides background information about the electrical power system and its components, including Smart Grids and the substation and its automation system. Substation communication protocols are provided with detailed information about the IEC 61850 standard and its parts. This chapter ends with motivations of this research work.

The third chapter provides a state-of-the-art literature review of performance evaluation of the IEC 61850 based substation automation systems and related technologies. The reader finds fundamental information about terminologies such as performance levels and standards requirements. From the relevant literature, a comparison of the existing approaches and four categories are identified; analytical, simulation, co-simulation and experimental. Significant work of all categories is comprehensively compared, and we finally conclude to provide a global synthesis. Based on this synthesis, we used the platform to perform experiments.

The fourth chapter introduces the experimental platform and explains purposes of protection schemes, time coordination and safety requirements. Configuration steps are provided for setting the experimental environment. We conclude this chapter by defining the metrics of the communication network inside substations within the context of IEC-61850.

The fifth chapter illustrates the procedure of experimental works. Beginning with validating the measurement setup. In the first experimentation, we compared the feasibility of Ethernet-based signaling to conventional hardwired connections. Secondly, we evaluated the effect of emulated substation traffic scenarios on the functional protection and control messages (GOOSE frames). Then, we evaluated the time precision using an available SNTP server, by achieving acknowledgment of GOOSE reception at the subscriber IED. The fourth experiment is similar to the second one, but it proposes dynamics of the power system by injecting current faults during several traffic profiles. Finally, we proposed a solution to overcome the effects of the traffic profiles by using VLAN-based priority. Overall discussions of the results obtained are discussed at end of this chapter.

The sixth chapter introduces the definition of dependability, dependability attributes, dependability impairments and dependability means. The chapter then presents implementing functional safety to evaluate the SIL level of three proposed architectures. Another aspect related to the second purpose is to check GOOSE frames conformity to functional safety requirements by investigating their contents according to the safety communication requirements.

In the seventh chapter, a Bayesian Network (BN) model is developed depending on the system structure proposed in chapter six, which is related to the platform architecture. In order to reduce the complexity of the model, we use a canonical model (Noisy MAX gate). The BN model uses the data obtained from experiments that are explained in chapter five. This model is used to

diagnose causes of failures and malfunctions of the functions of the substation automation system. The model is flexibly adapted to predict, prognosis, system dependability. Finally, the model is validated by evaluating several diagnosis cases, generating synthetic data and analyzing the sensitivity.

The last chapter concludes this thesis with research findings, contributions, and the significance of this research. Reliant on the practical experiences gained through this research, this chapter suggests some recommendations and highlights current study limitations. Finally, potential future research topics are given.

chapter 2 : From Electrical Power Systems, Through Substations, Toward Smart Grids

2.1. Introduction

This chapter provides a global overview about the electrical power system, where main components that build this system are stated in the section 2.2, and their roles are given. It is advisable that the reader should begin reading by this chapter, regarding it as inevitable prerequisite to understand the following chapters. To provide good example of power grid, a system from Libyan grid is illustrated that demonstrates the power system and its subsystems. The term of smart grid is elucidated in section 2.3 to emphasis its necessity for achieving sustainable and reliable power grid goals in the developed and developing countries. Meanwhile, the section 2.3 also highlights the importance of the substation systems and their automation and communication protocols, ranging from proprietary protocols until reaching the promising standard (IEC 61850). Section 2.4 emphasizes standard communication services and object modeling that promote comprehensive solutions for the interoperability issues. Section 2.5 discusses main parts of this chapter and provide motivation for the research work, whereas section 2.6 concludes this chapter with challenges that meet adoption of new standardized technologies.

2.2. Electrical power system

The power system is an electrical grid that forms most major and critical national infrastructure. Considering its importance for private and public sectors the system has significant importance for daily life economic and social activities. In most countries, political authorities have interest in the system planning, development and follow-up. The system covers large areas that reach both urban, suburban and rural lands. Maintaining this system requires protection and control of its subsystems assets and enforcing use of reliable components and safe measures.

Power generation plants produce electricity to serve as main stable sources for the power grid. These plants produce electrical energy depending on availability of different resources. The ordinary plants typically use fossil fuel including coal, oil and gas, while nuclear plants use uranium [Karady & Short, 2006]. Current trends augmented generation of electrical power from renewable resources such as wind energy, photovoltaic cells energy and hydro energy. According to the nature of the power system, generation plants are first components of the system. Usually large companies, either public or private, are involved in the power generation process. The transmission lines transmit power from generation plants to the rest of the power system network (Fig 2.1). Transmission substations are important nodes that are technically used to transmit electricity from generation plants to distribution substations, and ultimately to

final consumers. These substations are connected nodes that build a network of networks giving the existence of the power grid.

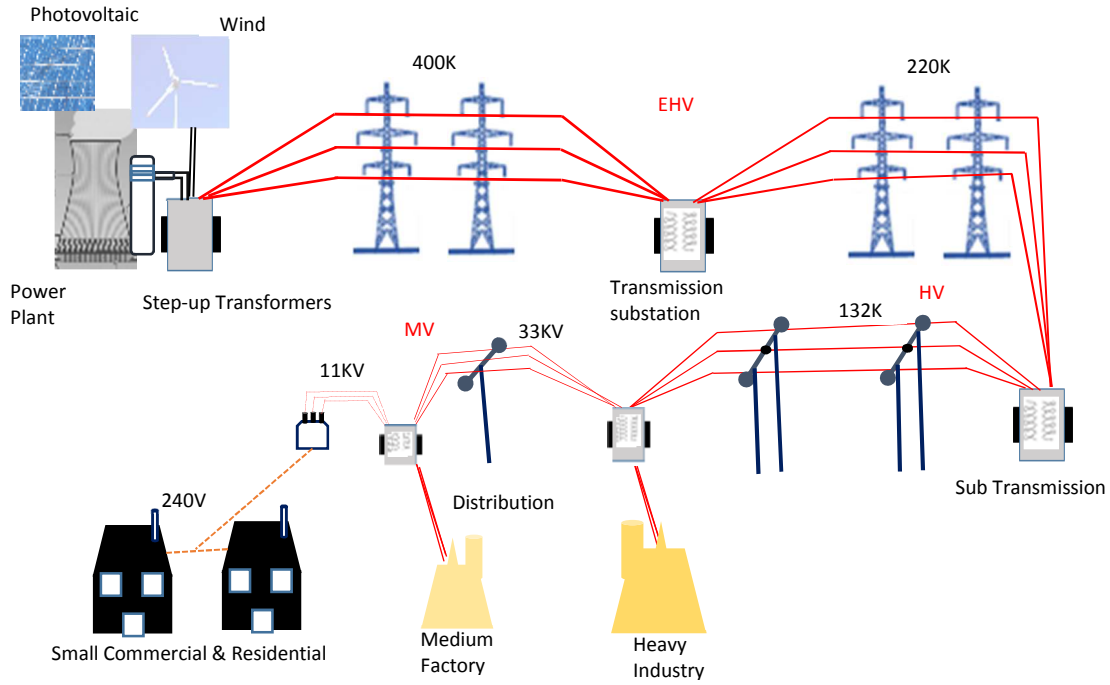


Figure 2.1 : The components of the Electrical Power System Grid

Since 1900s, the power system has followed the increased demand of electricity caused by the population growth and large industrial installations have raised the demand since the era of industrial revolution [Merrill, 2001]. Many innovations are directly targeting the system components: generation plants, transmission and distribution substations and control centers. Development of new technologies, such as power relays, contribute directly to the improvement of the system reliability, but adding complexity to the power grid. Since power demand is increasing constantly, as a result new plants and substations have installed and operated causing enlargement of the topology of the power network. These novel issues impose dividing the power system supervision among generation plants' owners, electric utilities and electricity distributors. Hence, maintaining the power system reliability is the responsibility of many players. The free market regulations launch competition between the key players in the electricity market; this competition enforces more inventions and innovations in the field of electrical power. The main objective of new technologies is to guarantee a higher reliability and safety during supplying electricity, which requires monitoring and control of transmission from generation plants until distribution to the final consumers. One of these technologies is the communication network that extends the protection and control system from communications existing within (intra) a substation, among (inter) substations, and up to remote tele-control centers.

Recently, information and communication technologies provide new means for managing the electric power system by enabling transmission of tele-protection data and control messages. These technologies enable sending commands from the enterprise (control) side, and gathering data from the electric system components [Farhangi, 2010]. At the consumption side, industrial and public consumers (residential) may use this information for planning. The collected data is useful for utilities to perform power system planning and development. In

further, intelligent devices are developed to enable performing many required functions such as monitoring, fault recording, protection and control [Brand et al, 2003]. Microprocessor based devices provide intelligence for the power system, and paved the way for the smart grid. The smart grid (see section 2.3.1) involves power network, information technology, and communication capabilities to enable new operation features such as demand/supply analysis, integration of renewable distributed resources, etc.

Concerning the new operation features and the requirement of the smart grid, the transmission and distribution substations have undergone intensive modernization. Distribution substations are core nodes for delivering electricity to industrial, commercial and housing facilities. These substations follow specific requirements to make electricity affordable for different types of customers. Power utilities adopt standardized steps, driven by international norms, to meet operation availability and scalability requirements [Brand et al, 2003].

2.2.1. Electric Generation plants

Historically, electric power generation for commercial use started with central power plants in 1882 in Manhattan (The United States) [Josephson, 1959]. Consumption is continuously increasing following a high demand of the world industry and commerce. Most of the electrical energy is generated by conventional power plants, which remain the only cost-effective method for generating large quantities of energy [Karady, 2006]. Power plants convert energy stored into the earth to an electrical energy. Around the turn of the 19th century, the first fossil power plants used steam engines as the prime mover. These plants have 8- to 10-MW capacity, but increasing power demands resulted in their replacement by a more efficient steam boiler-turbine arrangement. The first commercial steam turbine was introduced by DeLaval in 1882 [Karady, 2006]. The boilers were developed from heating furnaces. Oil was the preferred and most widely used fuel in the beginning. The oil shortage promoted coal-fired plants, but the adverse environmental effects curtailed their use in the late 1970s. Presently the most acceptable fuel is natural gas, which minimizes pollution and increase efficiency due to its availability in large quantities. The increasing peak load demand led to the development of gas turbine power plants that can be started and stopped within few minutes. The last development is the combined-cycle power plant, which combines a gas turbine and a thermal unit [Karady, 2006].

Nuclear power plants appeared after the Second World War. In the sixties, these plants were gradually developed to increase electrical energy supply [Karady, 2006]. Developed countries such as the United States, France, Japan etc., have a large deployment of nuclear reactors alongside other generation plants to produce electrical energy. For environmental reasons, some countries choose to use alternative power generation plants instead of nuclear energy. Briefly, generation of electrical energy requires availability of primary natural resources such as fossil fuel and gas, or renewable resources such as wind, hydro and solar energy.

Recently, power utilities in many countries encourage using distributed power generation, which harnesses renewable and nonrenewable energy sources. Distributed power technologies depend on process and concepts in which small to medium, i.e. a few kW up to 50 MW or more, power generation facilities, energy storage facilities, i.e. thermal, flywheel, hydro, flow, and regular batteries, and other strategies are located at or near the customers' loads and premises. These technologies operate as grid-connected or islanded resources at the distribution or sub-transmission levels [Enslin et al, 2006], and future trends promise using small power generation facilities that shall depend on the mentioned renewable resources. In the other hand,

electrical power storage will form main issues such as rechargeable batteries in the electrical vehicles and compressed air energy storage (CAES) that contribute to Greenhouse gas (GHG) reduction, stabilization of transmission and distribution that result in optimization of energy supply [Mahlia et al., 2014].

2.2.2. Transmission and distribution

Electrical energy shall be transmitted, via power grid lines from electrical generation plants up to planned destinations, through transmission and distribution networks. This transmission process requires step-up and step-down subsystems. Transmission and distribution substations represent these subsystems [Brand et al, 2003]. Utilities connect ultimate costumers to distribution substations via electrical power lines, or directly to nearest transmission substations, i.e. industrial facilities, where distribution substations exist in large consumer site, e.g. heavy factory, very large commercial center, airports, etc.

At the continental level, planning of transmission and distribution is under the responsibility of agreement between governmental bodies with cooperation of utilities and power generation companies. At the regional levels, electrical companies maintain the stability of the transmission and distribution grid. While at the national level, the state authority supervises coordination and cooperation between regional companies. For example, EDF (Electricité De France) is the largest producer and supplier of electricity in France and worldwide, while Enedis, the former ERDF (Électricité Réseau Distribution France), i.e. subsidiary of EDF, manages and operates the public network of high voltage HV and Extra High Voltage EHV transmission in France. In the United States alone, the power network encompasses both transmission and distribution facilities. It includes some 15000 generators that send power through over 450000 miles of high-voltage (greater than 100KV) transmission network lines, and additionally, there are about 5600 distribution facilities [Amin, 2011].

Generally, power grids consist of transmission and distribution networks, in many countries extra-high voltage networks, owned by bulk electrical utilities, transmit power from power plants to large load centers and distribution networks. The distribution networks, also known as mid/high voltage networks, are used to supply power to ultimate customers [Brand et al, 2003].

Transmission and distribution substations construct switching components in the topology of the power grid, these substations with power lines could be altered during faults or network upgrades causing change of electrical grid, hence that, the electrical power system depends on these components to deliver a reliable service. A telecommunication network is used to exchange important status and information between power stations, transmission and distribution substations and tele-control centers [Mohagheghi et al, 2009]. Another subsystem is the protection and control system that monitors power equipment in substations by gathering configuration and operation data to protect electrical switchgear equipment during the external faults or electrical power system failures. These subsystems are distributed between network control centers and inside the substations, to allow local and remote management of electrical power system components [Mohagheghi et al, 2009].

2.2.3. Consumption

In general, the public housing (residential) consumes large amount of electrical power for many purposes and utilization such as heating, air conditioning, lightening, cooking etc. hence that, electric consumption rate depends on population growth rate and living style. Industrial usage of electricity requires direct connection to the EHV network through a dedicated small distribution substation installed at the industrial facilities. Large manufacturing

and industrial plants could have their own power generation units to guarantee the continuity of electrical service operation. Electrical power demand increases as a natural response for raised industrial consumption. Responding to growing demands requires expanding capacity of the electrical power system either via increasing the amount of the generated electricity or the served area to cover new consumption areas. According to statistical information in 2009, global energy utilization faced a slight decline for the first time since 1981 on any significant scale — because of the financial and economic crisis [IEA 2009]. Globally, energy storage becomes a key part in accomplishing goals in energy sustainability that lead to energy and cost savings. Many efforts have been done to identify and implement the most suitable technology to rectify these issues (Mahlia et al., 2014).

2.2.4. Control centers

To manage the electric grid dependability, control centers monitor the power grid health such as load peaks, faults, etc. These centers assist utilities for keeping balance between power demand and electric load (response) availability, while tracking hourly utilization of electric power in covered areas. Usually these centers, i.e. network control centers (NCCs), have remote connection to supervisory control and data acquisition (SCADA) systems in the transmission and distribution substations via a wide area network either provided by telecommunication operators or proprietary communication networks. In the other hand, NCCs exchange data with power utilities and electric planning departments aiming to deliver up-to-date reports for the grid planning at the corporation level [Brand et al, 2003].

Modern NCCs send protection and control data remotely to the transmission and distribution substations through network gateways and routers. These substations communicate with NCCs either via connected cables or by wireless communication means such as mobile networks [Stanton et al, 2001]. NCCs operators can change substation configurations and process parameters remotely. For instance, they can open a motor-enabled disconnector or circuit breakers during maintenance or upgrade schedules. Furthermore, NCCs receive updatable information about power process equipment (switchgear) such as disconnectors' status and circuit breakers positions, e.g. open or closed. Nowadays, human machine interfaces (HMIs), with touch screens, provide user-friendly interactive access that improves work environment in control rooms [Brand et al, 2003].

2.2.5. Example of a power grid in Libya

GECOL (General Electricity Company of Libya) is the electric utility of the State of Libya. The company alone controls domestic production, transmission and distribution of the electrical power. The grid is accessible for 99% of the population. For 15 years, GECOL has more than doubled its electric power generation to satisfy the faster growth of electric energy demand. All generated power is produced at large central power plants, which are usually built in the coastal areas [Ekhlat et al, 2007]. The company operates more than 30 electric production plants, which use conventional energy resources. Additionally, it implements pilot projects to benefit from renewable energy resources [Ekhlat et al, 2007]. The company planned to run the power grid, from the 400 kV level down to the distribution network, in a highly reliable and efficient way, a state of the art utility communications connected to many local area network (LAN) services were planned and began implementation in 2007. This power grid is connected with neighbored coastal countries (Egypt and Tunisia) [Wadi et al, 2009].

The entire transmission power system contains approximately 75 substations on 220 kV (13,677 km) and 132 kV (1,208km) voltage levels with connections to sub-transmission networks of 66 kV (13,973 km) and distribution systems of 30 kV (8,583 km) and 11 kV.

Connections in the transmission network of Libya are realized as overhead lines (14,747 km) and cables (138 km) [Veleba & Buhawa, 2011]. Figure 2.2 illustrates a geographical location of the existing 400 kV and 220kV systems at West Libyan power grid [Wadi et al, 2009].

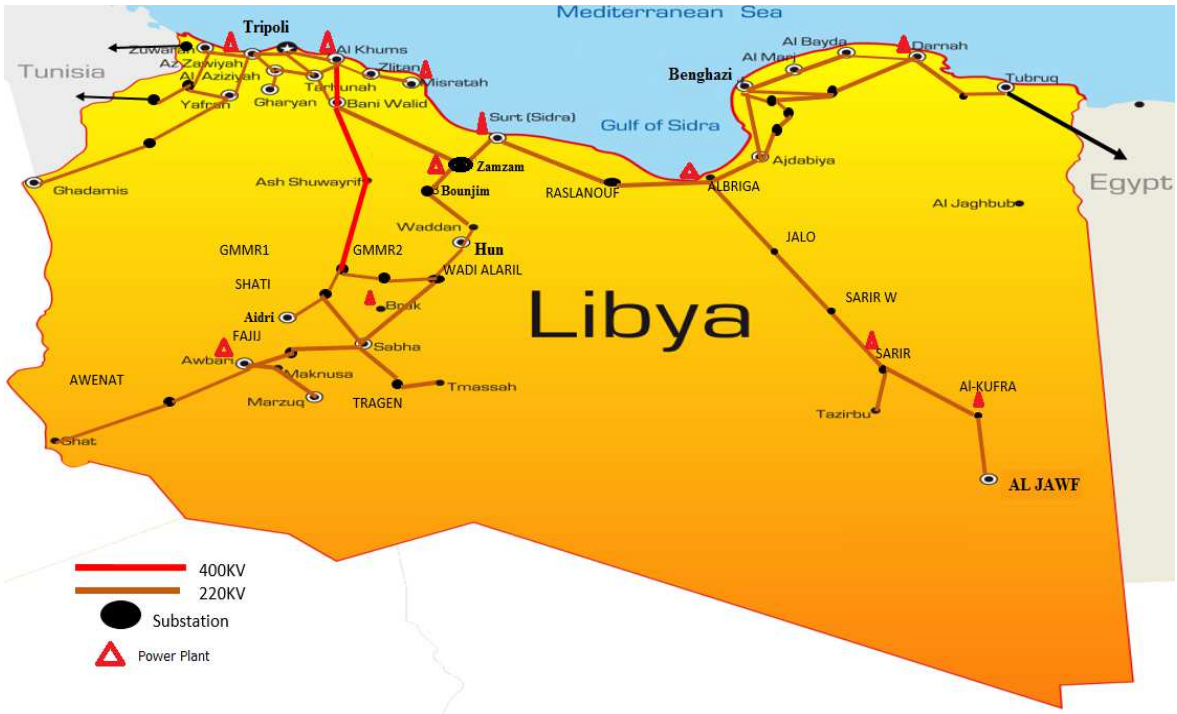


Figure 2.2 : Libya, existing 220kV and 400kV electric network and main transmission substation are shown

In 2011, power plants produced electric power with estimated amount, i.e. about 30962 ktoe (kiloton of oil equivalent), equals almost 360 GWh (Giga Watt hour) [IEA, 2011]. Most of this power is produced from fuel and natural gas facilities, because that Libyan reserve of oil and natural gas is huge. Hence that, the electric power production in Libya depends on crude oil, which makes up almost 79% of the energy production [Bindra & Salih, 2014].

2.3. The substations, active elements of the smart grid

2.3.1. The smart Grid

The smart grid can be considered as a new emerging trend toward a modern electric power grid infrastructure for enhanced efficiency and reliability through automated control, high-power converters, modern communications infrastructure, sensing and metering technologies, and modern energy management techniques based on the optimization of demand, energy and network availability [Gungor et al, 2011]. This term refers to the utilization of computer, communication, sensing and control technology that operates in parallel with an electric power grid, aiming to facilitate the interconnection of new generating sources in addition to aforementioned objectives [Amin, 2011].

[Li et al, 2010] presented the features and functions of new vision for the smart transmission grids, in their vision; a smart transmission grid is regarded as an integrated system

that functionally consists of three interactive smart components, i.e., smart control centers, smart transmission networks, and smart substations. The smart transmission and distribution substations are designed based on existing and emerging substation automation technologies. These technologies should provide efficient monitoring, operation, maintenance, protection and control of installed equipment in the substations. From the operation aspect, a smart substation must rapidly respond and provide increased operator safety. For achieving these goals, smart substations shall propose these functionalities [Li et al, 2010]:

a) Digitalization platforms that enable reliable tasks,
b) Autonomous operation and fast responses under emergency conditions,
c) Coordination with other substations and control centers (see § 2.2.4) to improve the security of the whole power grid, and
d) Self-healing to recover from network component failures, attacks and disasters

The European Commission mentioned that distribution grid management would focus, among eight priorities, on maximizing performance of feeders, transformers, and other components of networked distribution systems and integration with transmission systems and customer operations, which requires intra-substation communication technologies [European Commission, 2006]. The issue of interoperability is critical to the achievement of smart grid priorities at the system and components levels. The GridWise architecture council, i.e. industry leader council, addressed this issue by identifying standardization areas of intelligent and interactive electric systems. The council proposed means to achieve interoperability through covering these areas [GridWise, 2005]:

- Exchange of meaningful information between two or more components of the system,
- A shared understanding of the exchanged information,
- A consistent behavior of the system components complying with system rules, and
- A mandatory quality of service: reliability, time performance, privacy, and security.

2.3.2. Substations

The substations play an important role in the electrical power network, representing connection nodes connecting power lines and cables to power sources in order to transmit and distribute the electric power [Brand et al, 2003]. The transmission substations used to: connect extra high voltage (EHV) lines, controlling the conversion of extra high voltage to specific high voltage (HV) via transformers, as well as delivering various voltage levels to distribution substations [Brand et al, 2003].

From what mentioned earlier, the substations are normally categorized into transmission and distribution substations. Recently, specific substations are used for collecting electric power from distributed energy resources, i.e. conventional power plants and renewable resources based generation plants, in order to achieve higher reliability, lower carbon emissions and comparable economic cost/benefit return on investment.

High voltage substations are normally located near the load centers, e.g. outside a large city. These substations connect electrical transmission networks to the distribution networks aiming to permit load sharing among power plants and to ensure a high level of reliability. In this case, the failure of a line or power plant will not interrupt the energy supply [Karady & Short, 2006].

According to insulation technology, the substations can be classified into two types: gas insulated substations (GIS) and air insulated substations (AIS). The former requires small space for installations and operation control (normally indoor). GIS was first developed in various

countries between 1968 and 1972. After about 5 years of experience, the use rate increased to about 20% of new substations in countries where space is limited [Bolin, 2001]. In the other hand, AIS substations have large footprint that may cover several hectares. From engineering perspectives, several factors affect the reliability of a substation or switchyard (electrical process): one of these factors is the arrangement (topology) of the buses and switching devices. In addition to reliability, arrangement of the buses/switching devices will affect maintenance, protection, initial substation development cost [Bio, 2001]. According to common industrial practices, six types of arrangement topologies are commonly used in air-insulated substations, for more details see Fig. 2.3 [Bio, 2001]:

1. Single bus
2. Double bus, double breaker
3. Main and transfer (inspection) bus
4. Double bus, single breaker
5. Ring bus
6. Breaker and a half

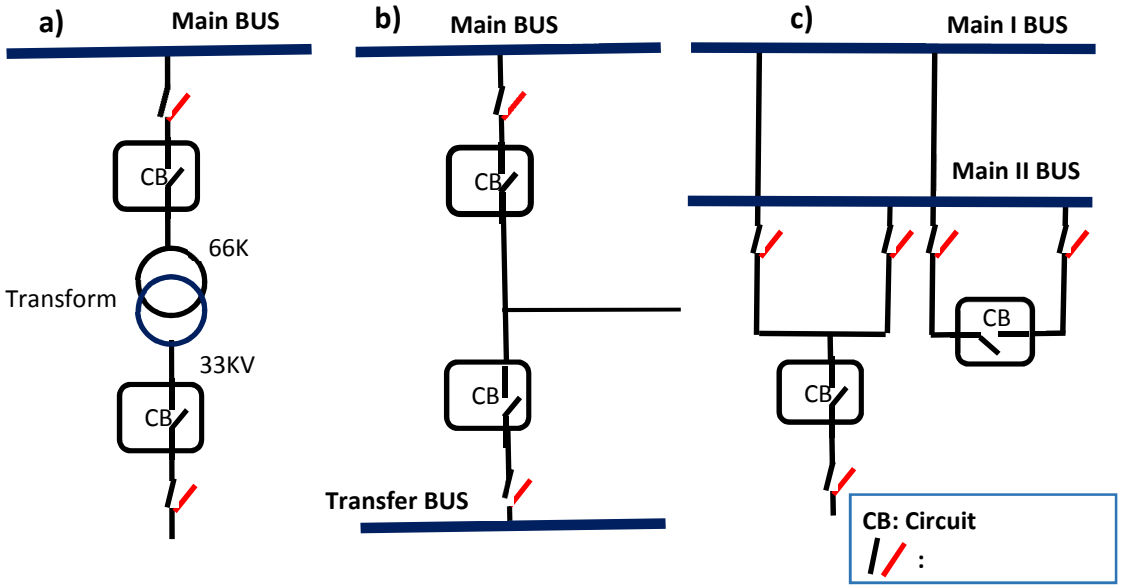


Figure 2.3 : Single Line Diagrams: a) single bus, b) double bus double breaker, c) double bus single breaker

In power engineering, single-line diagrams (SLD) represent the substation topology and illustrate allocation of electrical process equipment, in (fig 2.3 a) a single-bus substation, with their single line diagram, is shown. From this figure, the reader can notice the existence of a single bus (main bus) connected to a main transformer that converts 66 kV into 33 kV. The single bus topology less reliable than the other two topologies, which are shown in parts b and c in Fig 2.3. Later topologies are more reliable which represent double bus bar with double and half breaker respectively. In addition, circuit breakers (CBs) are located near the transformer, these equipment and related switchgear are used to isolate the line as protection requirements, i.e. to interrupt the power flow (trip) into the transformer bay. In this structure, disconnectors (switches) are associated with the circuit breakers, and installed to guarantee the disconnection of electric power during maintenance procedures. Therefore, these disconnectors should operate accompanying the circuit breakers in open position. Moreover, to provide a sufficient level of safety during the maintenance operations, the ground switches, i.e. connected to earth,

are used to keep the required area disconnected, which means without power [Brand et al, 2003].

In early designed substations, voltage and current measurements were obtained through conventional instrumentation, and control of switchgear was performed through operators' commands. The two main functions were performed locally at the substation (not from control centers). These functions were: a) the data acquisition from the power process via instrument transformers, i.e. sensing of volt and ampere values, and b) issue of commands to change switch positions. The need for automated operations are raised to protect the most costly switchgear equipment such as transformers, buses, feeders, etc. Therefore, protection and control require monitoring of equipment and automatic calculating of many electric power parameters such as frequency, active and reactive power values [McDonald, 2001].

2.3.3. The substation automation system

The substation automation system (SAS) can be defined by its functions that replace operators' effort by automated actions as its name reflects. In this manner, performed automatic functions are necessary for maintaining safe and reliable service of the electric power transmission and distribution. These functions would include, but are not limited to, monitoring, data acquisitions, protection, control, and remote access communications.

In the past, for distant surveillance functions, Remote Terminal Units (RTUs) were available only as interfaces between the electric power switchgear at the process level in the substations, and utilities' network management system (fig 2.4). These units have many inputs and outputs as communication interfaces to the remote network control centers (NCCs). In this structure, both RTUs and NCC formed the Supervisory Control and Data Acquisition System (SCADA) as depicted in Fig 2.4 [Brand et al, 2003].

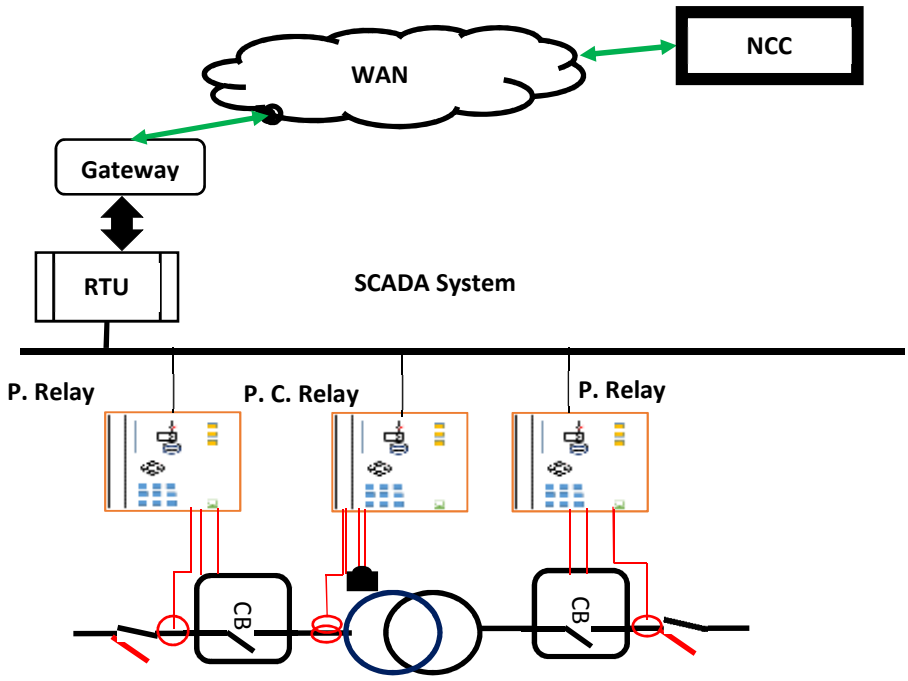


Figure 2.4 : The substation Automation System, an architecture of classical SCADA systems

For instance, the Power Systems Engineering Research Center at Arizona State University [PSERC, 2010] states the following functions of the substation automation system:

a. Control of voltage transformation (Load Tape Changer Control)
b. Protection of buses, lines, feeders, transformers, generators, and other equipment.
c. Automate interlocks and switchgear switching mechanisms,
d. Sending monitoring data to control center,
e. Clearing power system faults locally or remotely,
f. Communications with other substations (intra) and regional control centers.

Obviously, the substation automation system provides important information for the central system at the utility level (enterprise). On the other hand, the SAS receives updated control data from the control centers to keep normal operation of the power system [Stanton, 2001]. For example, many functions in SAS are coordinated for self-healing in case of equipment failure or short-circuit faults. These functions employee several devices and their tasks are distributed at either the primary (i.e. circuit breakers, transformers, instrument transformers, etc.) or the secondary equipment (i.e. protective relays, merging units, intelligent electronic devices). Hence that, cabling and wire connections, between these devices and equipment, become complex and in consequence cost huge efforts and longer time as long as conducting maintenance, repair, extension or modification operations [McDonald, 2001]. Many efforts aimed to decrease the amount of cabling and wiring results in adopting and using serial communication networks in deferent levels of substation hierarchy. These efforts suggested proprietary solutions that are developed by substation equipment providers. Large companies, non-profit consortium of substation equipment suppliers and utility users such as Utility Communication Architecture (UCA) international users group (UCAiug), continue to improve substation communications by contributing to international standards to increase the functional interoperability and to propose architectures that provide higher throughput, i.e. network bandwidth, aiming to increase inter and intra substations communications reliability [Brand et al, 2003].

Today, protective relays become intelligent electronic devices (IEDs), i.e. programmable electronic based protection and control devices with at least one communication interface. An IED is a microprocessor based electronic device that includes input, output, memory, storage media, and communication network interface. This device is capable of doing many functions in the same time benefiting from the processing power. IEDs embed logic programs that perform the electric power functions such as calculating reactive power, monitoring primary equipment, sending protection trip, etc.

Generally, IEDs exchange information that can be gathered and saved locally or remotely for detailed processing and log registration. This information helps utilities to enhance reliability, and to enable asset management programs including predictive maintenance, life extensions and advanced planning [McDonald, 2007].

2.3.4. Communication architecture of Substation Automation Systems

SAS Technological implementations categorize the substation automation hierarchical architecture. The three levels of the substation automation system are the station, the bay and the process levels (Fig 2.5) that can be implemented for different functionalities. Technically, the size of an SAS will be larger in the extra high voltage transmission substations than high

voltage distribution substations. Thereafter, the bay level will exist in most installations of modern substations, while in early days of SAS no bay level can be recognized [Alstom, 2011].

Briefly, the substation automation system follows basics of control system design, where sensors, control logic and actuators are connected to keep the system or equipment under control (EUC) in stable conditions as predefined by setting parameters. Typically, the sensors measure very high current and voltage quantities. Instrumentations such as current and voltage transformers (CTs/VTs) convert very high quantities of current and voltage into rated values that are delivered to relays inputs. These scaled values are normally equals to 5A (1A in Europe) for the current, and 120 Volts for the voltage. Protection relays or modern intelligent electronic devices perform the protective logic. These devices sense electrical current and voltage quantities in order to calculate certain values that are monitored by the protective logic, e.g. electrical current value in two different sides of EHV/HV transformer. When a parameter overpasses a setting value (pickup setting), the protective logic will react according to a logic sequence or programmed control algorithm. In general, a trip signal will be sent to the associated circuit breaker to disconnect a line or bus while a fault exists [Brand et al, 2003].

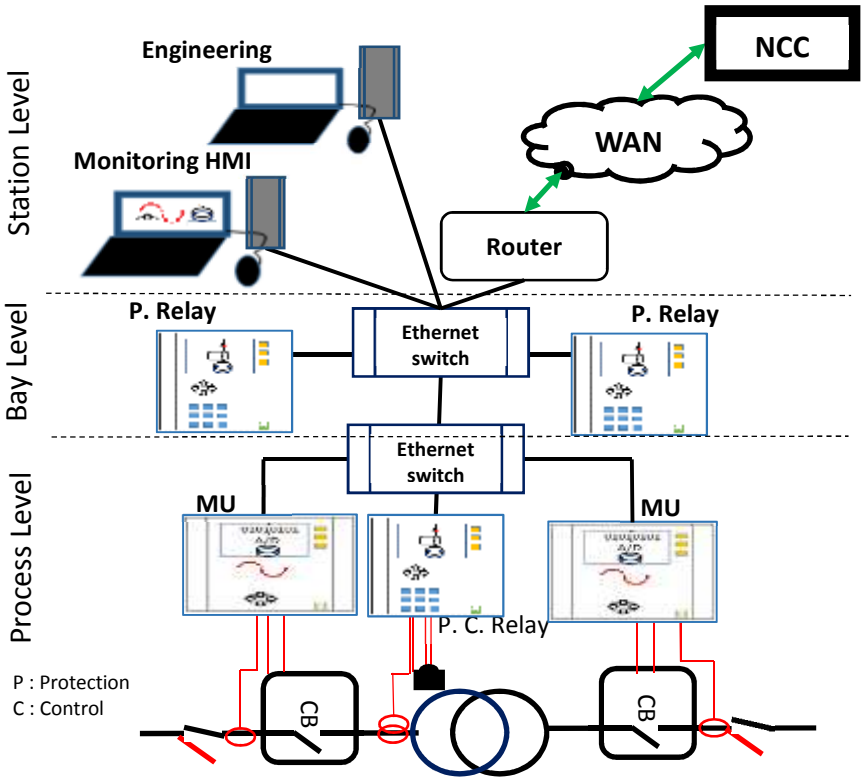


Figure 2.5 : The structure of a Substation Automation System representing station, bay and process levels

A battery or direct current (DC) source will supply power to these devices. Practically, a modern substation architecture includes three levels, which are developed in the following subsections.

2.3.4.1. The station level

The purpose of the station level is to incorporate supervision, monitoring and related tasks. The station level is often located in a special, if necessary shielded room providing an overview across the whole station [Brand et al, 2003]. Authorized power engineers, technicians

and operators to perform engineering and supervision tasks occupy this room. Operators can use engineering workstations (computers) to undertake daily tasks or to perform (remotely) monthly or annually inspections for the primary equipment health and state. For upgrading and retrofitting of existed substations, the early stage of implementation requires configuration and setting of different devices and equipment through engineering software. These applications are installed in station level computers that may have access for corporate data via a wide area connection. The substation system exchanges information with regional control centers through communication gateway existing at the station level. The station staff uses human machine interfaces (HMI) to monitor and/or to send commands to the substation devices and equipment. They use computers to access log databases that contain archival records for daily sequential event records happened at all substation levels.

2.3.4.2. The bay level

The bay level is located near the power process (switchgear). At this level, protection and control devices are allocated for specific functions as planned by the substation requirements and specifications. These devices are protective relays and intelligent electronic devices that are connected to local area network devices such as Ethernet switches [McDonald, 2007]. At this level, devices can perform autonomously power protection and control functions to clear faults in the process level as well as receiving data from the station level. Additionally many bays may exist in one substation, hence devices cooperate with other devices in near bays or other substations, e.g. to clear a fault in a line or to coordinate load shedding from generation plants. Usually, these devices have local human machine interfaces for direct access by substation technicians. For modularity and simplicity of the maintenance tasks, substations are organized into bays, e.g. transformer or generator bay, to allow disconnection of one bay, without affecting other bays, or process equipment during repair or maintenance schedules.

2.3.4.3. The process level

This level represents the primary equipment (switchgear) level; technically, the word switchyard is another nomenclature for the process level. At this level EHV/HV power equipment, such as transformer and bus bars, are installed and connected to provide existence of principal operations of a substation. This level includes connection of feeders, lines, buses, transformers, instrumentation, etc. In fact, the size and the functionality of the substation automation system depends on topology, architecture, size, function and technology of the process level [IEC 61850-3, 2003].

2.3.5. Types of SA systems

SAS systems can be classified into several types according to the technology and implemented levels inside the substations. Integration of protection, control, and data acquisition functions into minimum number of devices is required to reduce capital, operation and maintenance costs. Intelligent electronic devices are key components in substation integration and automation technology. Using IEDs based schemes reduce control room and panel space via minimizing wires and number of devices [Brand et al, 2003]. This design increases the system efficiency by adopting assets management based on available information from digital devices at different substation levels. In this approach, integration, enhancement

of operation and maintenance can be achieved with minimal human intervention [McDonald, 2007]. Therefore, substation automation depends on several distributed functions implemented in many IEDs, and major operational information for the SCADA will come from these IEDs. The IED incorporates network communication interface, hence that there are no conventional remote terminal units (RTUs), in modern digital substations. RTU functionalities are addressed by using IEDs, PLCs and a local network based on state-of-art technologies for data exchanging and reporting of substation state and events. To sum up, SAS type depends on automation integration and communication technology. In the following sections, differences between types of SAS are illustrated.

2.3.5.1. Conventional cabling SAS

In this substation automation system, the devices and equipment are interconnected within hardwired connections; hence, adding new equipment will increase efforts when cabling between protective relays and power equipment devices adds complexity to the SAS structure. In this classical architecture, cabling adds certain costs during installation and maintenance. In addition, repair time will be longer when a connections' failure happened. This structure requires more space for connection of primary equipment to secondary devices, and of secondary devices to the control room at the substation yard. Notably, in this type of SAS analog devices such as electromechanical protective relays and/or solid-state relays use copper hardwires [Alstom, 2011].

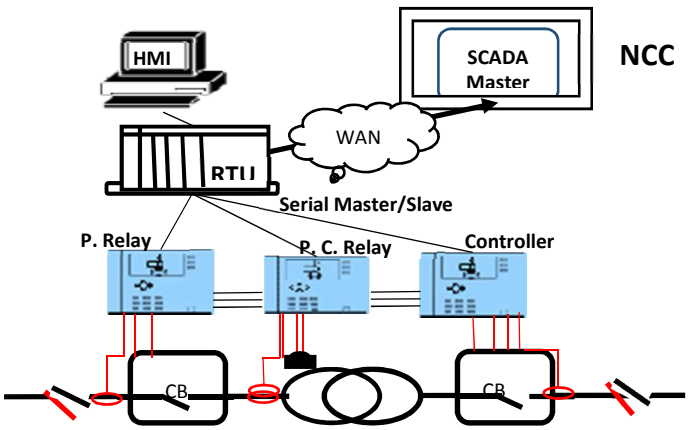


Figure 2.6 : Conventional cabling: inter-relay cabling and process hardwired connection

2.3.5.2. Station Bus within SAS

When computer manufacturers start producing microprocessor-based systems for industrial applications, the small microprocessor-based devices become an emerging solution in the power system industry. In 1970s, advances in hardware technology and software techniques led to the first microprocessor based relays in 1984 [IEEE PSRC, 2005].

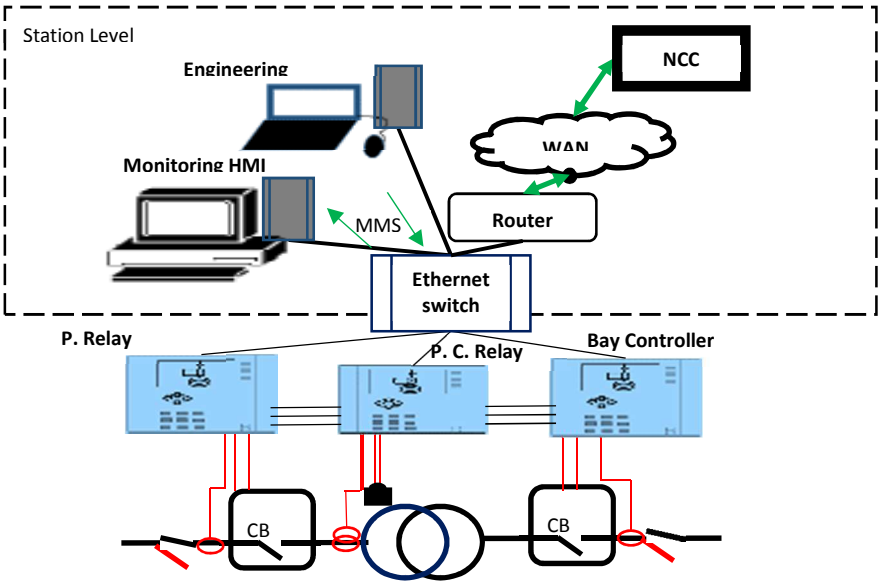


Figure 2.7 : Station bus implementation: station-level LAN to monitor and supervise connected devices

Microprocessor based relays with many features were developed for the protection and control functions. These protective relays incorporate a communication network interface to enable exchanging of data and commands with engineering computers at the station level, i.e. supervisory side. In this architecture, protective relays send reports about substation events and equipment status to the top level as well as exchanging of events and status with other relays at the same level. These devices become smarter and called intelligent electronic devices (IEDs). In this type of SAS, digital relays with communication capabilities allow interfacing with the station level-devices, but still conventional instrumentation used in the switchyard. Modern protective relays embed software logic to enable execution of multi tasks functions within the same device [IEC 61850-3, 2003].

2.3.5.3. Station and Process Buses within SAS

The future trend in substation automation consists in enabling digitalization of the whole substation automation system. In other words, the three levels of substation will adopt digital enabled technologies. For example, in the process level non-conventional instrumentation transducers (NCIT) will transduce and send digital parameters to merging units (MUs), standalone MU or embedded NCIT, which in accordance collect and send these digital parameters via frames of sampled measured values (SMV) through an Ethernet network [IEC 61850-3, 2010].

These SV frames require precise synchronization to encapsulate accurate timestamp data as well as three phase current and voltage parameters. Fig 2.8 helps to distinguish this architecture from other former SAS types (without process bus). This type of SAS is equipped

with: a) IEDs supporting process-bus connections via Ethernet network interfaces, b) devices sending timestamped SV frames which are synchronized within microsecond precision, and 3) Merging Unit (MU) interfacing with process level (primary equipment), to collect physical parameters, with either conventional instrument transformers or NCIT equipment. [Gungor et al, 2011].

Data frames allow transfer of control and data from NCC to primary equipment at a substation switchyard under the assumption that the process level is connected to a communication network. In this approach software based human-machine interface (HMI) devices can send commands via local area network or remotely from the regional control centers, as well as operators can access and configure power process locally by using the embedded HMI within the IEDs [Alstom, 2011].

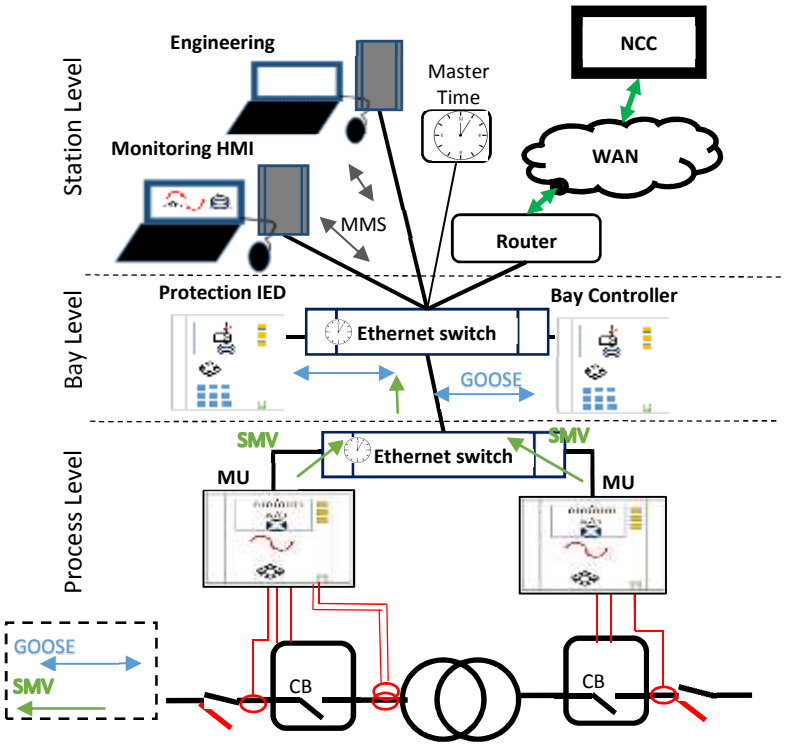


Figure 2.8 : Process and station buss: horizontal from process and vertical inter-IEDs communications

2.3.6. Communications of Power Substation Automation System

As it was reminded previously, in early days of the substation automation systems, substation devices such as protective relays, RTUs and SCADA panels were connected via hardwired cables to power process equipment, e.g. instrument transformers and circuit breakers. Communication network interfaces, such as EIA 232 and EIA 485, were introduced only as developers' debug tools [Alstom, 2011]. Modern communication technology enables replacement of hardwired connections by Ethernet ports. Thereupon, polling of physical parameters will be via the network message frames that utilize communication protocols as a method to encapsulate these parameters and to send them to SCADA equipment, also tripping

commands can be transferred in the same way [Sauter & Lobashov, 2011]. The implementation of network protocols, in the industrial control facilities, opens the door for the development and use of many protocols in the substation automation. This development helps substation manufacturers to integrate several functions in a single IED. As a result, the integration process of protection and control become technically achievable [PSERC, 2010].

2.3.6.1. SAS legacy protocols

The communication protocol identifies how devices can exchange data and understand engagement rules [Tanenbaum & Wetherall, 2011]. Communication protocols achieve and manage data exchanging in a formal way. In other words, devices share common language and specific procedure to determine messages syntax, size, etc. Industrial control systems adopt network protocols that enable communication between sensors, controllers and actuators within predefined operation mechanisms. Networked control systems appeared since that in many manufactory automation lines, and their protocols were different and proprietary [Mohagheghi et al, 2009].

Installing several communication protocols within different substation levels requires conversion gateways, i.e. translation between devices protocols, to allow connection among different devices and equipment. This operation adds cost and efforts during installation and configuration of the substation automation system. The need for plug-and-play connection between devices from different suppliers rises the demand for common standards.

Among the substation communication protocols are Modbus and DNP (fig 2.9) which are well-known protocols in the power industry. Modbus is developed by Modicon (becomes Schneider electric) in 1979. This protocol was originally utilized as a control network protocol for PLC to allow process control communications. The original edition forms a Master/slave environment between control devices. The Master can initiate a request with this protocol, and corresponding slave or slaves will send response with required action/data. The Master station can initiate a broadcast message or address one slave station [Gungor et al, 2011; Mohagheghi et al, 2009].

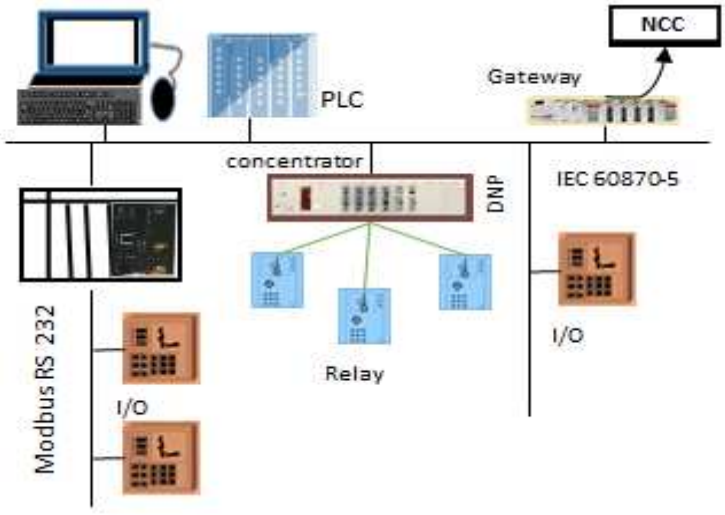


Figure 2.9 : substation Automation system with legacy communication protocols

Schneider makes this protocol open by transferring rights to Modbus organization. The physical layer of this protocol is not defined, which allow manufactures to develop their choice of physical interface. This freedom opens the door for many versions of the protocol, e.g. Modbus RTU, ASCII and TCP. Modbus RTU and ASCII are commonly used with RS 232, RS

422 and RS 485 with maximum baud rate between 19200 bps and 100 Kbps. While Modbus TCP supports client/server communications with different physical layers such as Ethernet unshielded twisted pair (UTP) cables.

The protocol DNP 3.0 was developed by Harris in 1993 to enable communications between Master station level devices, RTUs and protective relays. This protocol has been openly standardized according to the IEC 60870-5 series when it was under development. It is widely used in power, water and gas process control for SCADA connections to RTUs. DNP 3.0 uses RS232 or RS485 as serial physical layer [Mohagheghi et al, 2009].

Table 2.1 provides a comparison between dominated legacy protocols that are used in the substation communications.

Table 2.1 : Comparison between legacy communication protocols of substation automation

Protocol	**Modbus**	**IEC 60870-5-103**	**DNP 3.0**
Release date	1979	1997 (former VDEW6, in late 1980s)	1993
Developed by	Modicon	IEC standards (TC 57 WG 03)	Harris
Standards support	Modbus organization	IEC 60870	IEEE 1815-2012, open specification
Substation use	SCADA Master to RTUs slaves. Also as client/server with IEDs network	Interoperable connection between protection and control devices (RTUs and relays)	SCADA, RTUs and Protective relays
Physical interface	- EIA (RS) 232,422 and 485 for Modbus RTU and ASCII - Exist also Ethernet for Modbus TCP	EIA 485, and optic-fiber	- EIA (RS) 232, 485 - Exist also for Ethernet
Communication type	Master/Slave, peer-to-peer and client/server	Master/Slave	Master/Slave, Peer-to-Peer and Client/Server
Support OSI layer	Application layer	Application Layer and 3 EPA layers (Enhanced Performance Architecture)	2nd Layer and somehow 4th and 7th layers supporting TCP/IP
Baud rate	19200 up to 100 Kbps (EIA), and Ethernet bandwidth for Modbus TCP (up to 10Mbps)	6900 or 19200 bps	38400 bps (some versions up to 112.5 Kbps) depends on hardware
Dominant market	worldwide	Europe	North America

2.3.6.2. SAS modern protocols

Aforementioned sections about the communications inside substations explained the existence and use of different communication and network protocols for data exchanging and management. Therefore, many proprietary protocols have appeared in the field of substation automation systems. Protocol converters and gateways are required to maintain data interoperability when a substation project mix protocols of devices and equipment from different suppliers. Additional tasks are required to install these gateways, which results in increasing of cost, effort and configuration complexity [Dolezilek, 2006].

Since 1986, Electric Power Research Institute (EPRI) has addressed the issue of different protocols in substation installations. EPRI took efforts that resulted in release of the Utility Communication Architecture (UCA 1.0) project by the end of 1991.

In 1990s, the deregulation of power energy market and global competition enforced the need for common efforts to increase integration of substation automation systems. Pilot projects involved experimental technologies were attempting to develop a standardized approach to cover all communications from an IED up to the control center or SCADA master [Apostolov et al, 2003]. These projects resulted in the release of UCA that specifies the use of Manufacturing Message Specification standard (MMS) and Integrated Utility Communication (IUC). Therefore, EPRI established a forum with Northern States Power Company (NSP), about the implementation of MMS across multiple communication media. Demonstrations from the MMS forum projects have resulted in detailed specifications. These specifications addressed interoperable communications in the utility industry covering communication profiles, application services and object models for IEDs [IEEE PSRC, 2005].

In 1999, these works, i.e. substation implementation documents, were released as UCA 2.0, published in the IEEE 1550 technical report, and further used as foundation for the IEC 61850 standard [Skendzic & Guzma, 2004].

A working group worked in the harmonization of certain parts from the UCA that resulted in extension of UCA modeling, data definitions, data types and services. The IEC 61850 adopted these results in respective standardization parts. The IEC 61850 standardization parts are intended to be a superset of UCA.

2.4. The IEC 61850 standard

The International Electrotechnical Committee (IEC) technical committee (TC) 57 was established in 1964 to publish and elaborate international standards in the field of communications between the equipment and systems for the electric power process, including tele-control, tele-protection and all other telecommunications in the electric power systems [Dolezilek, 2006]. The TC 57 developed the international standard IEC 61850: Communication Networks and Systems in Substations. Utilities, suppliers and users noted that the industry should end up with a single standard for substation communication and all of technical issues based on the application of UCA 2.0 are to be resolved in the appropriate parts of IEC 61850 [Apostolov et al, 2003]. The meeting between IEC TC 57 members, in 1997 at Edinburgh, concluded with an agreement that only one standard for substation automation and communication should be developed, and to merge the North American and European approaches [IEEE PSRC, 2005].

TC57 aims to enable interoperability, seamless data communications and standardized information exchange between the overall distribution networks. The standard enables systems integration by allowing interfacing among substation devices and subsystems to improve data collection and real-time situational awareness. This integration empowered by the use of microprocessor based relays (IEDs) and communication networks. For these purposes, i.e. integration and interoperability, the standard separates application data, data transfer services and communication protocols in such a way that enforcing data and services abstraction. TC57 extended the scope of this standard to the completely electric network, and provided its compatibility with Common Information Model (CIM) for monitoring, control and protection applications [Sauter & Lobashov, 2011]. The first release of the standard includes at least 10 parts published in edition series since its appearance. The standard covers not only the

communication protocols, but also standardizes the devices abstraction, their communication service interfaces. It opens a direction for benefiting from information technology capabilities such as object oriented modeling and XML (extended markup language) based configuration language.

2.4.1 The parts of IEC 61850 standard

One of the efforts for integration has undertaken with the framework issued by the Electric Power Research Institute (EPRI) resulted in release of the Utility Communication Architecture 2.0 (UCA 2.0). In 2001, the technical committee 57, responsible of development of IEC 61850 standard, and the UCA group agreed to merge their efforts in one international standard. Since this agreement, UCA2/MMS have been chosen for IEC 61850, in the same time other efforts were taken to release the distributed network protocol (DNP 3.0) in order to achieve open standards based interoperability between substation computers, RTUs, IEDs and other devices. The TC 57 released the first edition of the standard around 2003 with core parts including technical reports (TR), technical specifications (TS) and international standards (IS). These parts cover definitions, general requirements, system and project management in the first four parts. The fifth part explains communication requirements for devices and functions models [IEC 61850-5]. In the sixth part, detailed examples are given to illustrate the description languages such as substation configuration language (SCL) and IED capability description (ICD) with related XML based files. The basic communication structures, abstract communication services, data classes and logical nodes are explained in the subparts of the seventh part. The eighth part introduces the mapping of MMS communication service to the ISO/IEC layers interface, i.e. ISO/IEC 9506-1, ISO/IEC 9506-2 and ISO/IEC 8802-3 (Ethernet), while the ninth part emphasizes the SV mapping to serial unidirectional multi-drop point to point link and ISO/IEC 8802-3.

Table 2.2 : The IEC 61850 standard parts and their aim

Part	Short Title	Type	Aims to	status
IEC 61850-1: 2003	Introduction and overview	TR	Give overview about communications between IEDs and related requirements	Ed. 2.0 (2013)
IEC 61850-2: 2003	Glossary	TS	Define terminologies and give comprehensive glossary	Ed. 2.0 est. 2018
IEC 61850-3: 2002	General requirements	IS	Identify general requirements and quality of communication network	Ed. 2.0 (2013)
IEC 61850-4: 2002	System and project management	IS	Describe the system life cycle and related engineering processes	Ed. 2.0 (2011)
IEC 61850-5: 2003	Requirements for functions and device models	IS	Specify communication requirements of functions performed in substation automation system	Ed. 2.0 (2013)
IEC 61850-6: 2004	Configuration description language	IS	Specify file format for describing communication related IED configurations and parameters	Ed. 2.0 (2009) & est. 2018
IEC 61850-7-1: 2003	Basic communication structure- principles and models	IS	Provide modeling concepts and methods for specific information, device functions and communication service to achieve interoperability	Ed. 2.0 (2011)
IEC 61850-7-2: 2003	Basic communication structure- ASCI	IS	Provide specific communication interface for applications to describe communication.	Ed. 2.0 (2010)

IEC 61850-7-3: 2003	Basic communication structure- CDC	IS	Specify common attribute types and common data classes for substation applications	Ed. 2.0 (2010)
IEC 61850-7-4: 2003	Basic communication structure- compatible LN and data classes	IS	Specify compatible logical node names and data names for communications between IEDs including relationship between data and LNs	Ed. 2.0 (2010)
IEC 61850-8-1: 2004	SCSM to MMS	IS	Specify a method for exchanging time and non-time-critical data	Ed. 2.0 (2011)
IEC 61850-9-1: 2003	SCSM- SV over serial unidirectional link	IS	Specify mapping of communications between process and bay levels	Withdrawn, replaced by 9-2
IEC 61850-9-2: 2004	SCSM-SV over ISO/IEC 8802-3	IS	Specify SV communication mapping to direct Ethernet layers	Ed. 2.0 (2011)
IEC 61850-10: 2005	Conformance testing	IS	Specify standard techniques for implementation conformance testing	Ed. 2.0 (2012)

For conformance testing, i.e. related to the substation project life cycle, a dedicated procedure in the tenth part provides the tester/testing-team with invaluable procedure for conformance testing by starting from IEDs, protection and control functions and ending with full substation automation system.

The first edition of the standard includes the early mentioned parts. Since the release of the standard, the TC 57 publishes many solved problems as improvement for detailed raised technical issues (TISSUES). The TC 57 made huge efforts to improve, add and benefit from new features between 2009 and 2010 resulting in the official release of the second edition entitled communication networks and systems for power utility automation in 2012. The cooperation between IEEE and IEC TC 57 helps the release of documented standards for substation communication technologies particularly for time synchronization mechanism with the precision time protocol profile in 2016 [IEC/IEEE 61850-9-3, 2016].

2.4.2 The IEC 61850 edition 2

The second edition of the standard is released to remove inconsistences and solve technical issues (TISSUES). Since 2010, many parts have witnessed modifications with extensions to other power system applications, such as communications between substations and network control centers, distributed energy resources (DER) and recommendations for redundant architectures. In addition, some parts are withdrawn such as the part 9-1. The IEC 61850 edition 2, clearly states the communication redundancy recommendations for the GOOSE and SV messages services. The redundancy must be bump-less (zero-recovery time). Hence, mission-critical applications in SAS communications can benefit from the standardized redundancy technologies [Khavnekar et al, 2015]. The redundancy with zero-recovery time such as parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR) are mentioned among the other protocols. The second edition of the standard recommends these technologies as means to achieve higher reliability and avoiding single-point-of-failure. Khavnekar et al make a comparative analysis between the first and second editions of the IEC 61850 standard. They conclude that edition 2 provides: seamless redundancy to boost the level of communication reliability, and extends data models to expand the scope of the standard to other power and smart grid domains [Khavnekar et al, 2015].

For testing procedures, the second edition offers the ability to use new features such as test mode and simulation flag within GOOSE and SV messages frames during testing or maintenance procedures. In this approach, software-based testing is feasible for both factory acceptance testing and on-site testing [Carvalheira & Coronel, 2014]. Based on the second

edition, Schossig proposes a systematic approach for combining the new possibilities with the existing testing procedures considering both conventional process-level hardwiring and SV based solutions [Schossig, 2014].

2.4.3 The features of IEC 61850

The standard has several parts that cover many domains in the field of power utility communications. In the SAS applications, the standard aims to enforce interoperability among devices and to integrate subsystems to build the overall SAS system [IEC 61850-1, 2003]. IEC 61850 based SAS shall incorporate several devices that have certain features such as:

1. Data models with logical nodes (LN) and common data classes (CDC)
2. Communication service interfaces
3. Reporting, GOOSE and SV communication services
4. Interoperable protection, control, measurement and monitoring functions
5. Support of XML based IED capability description (ICD) files
6. Substation devices could be configured through SCL language

The standard evolves, but it considers backward compatibility, to afford and improve interoperability in mixed substations, i.e. where the standard edition 1 and 2 devices are used. The standard enables use of emerging technologies in the field of communication networks, smart protective devices and smart instrumentation and metric equipment.
Abstraction of devices and representing real devices with the virtual model based logical nodes enable independency. This approach allows the development of physical devices without changing the communication interfaces.

The aforementioned features provide many benefits for maintenance and operation. For example, operators and technicians can upload and download self-diagnostic data and self-description data from IEDs that use the IEC 61850 models.

2.4.4 The IEC 61850 data models

The IEC 61850 data model incorporates the results of North America UCA project specification and modeling approach. As it was explained before, the standard parts extend and adopt the UCA 2.0 data definition, models, types and services [IEEE PSRC, 2005] (see § 2.4.1). Parts 7-1 to 7-4 of the standard present object oriented and data modeling principles. Therefore, the standard defines not only data exchange and communication, but provides data models approach that represents substation devices and equipment, and extends these definitions to cover other power system devices. The data model, i.e. IEC 61850 based modeling concept, follows a hierarchical structure where physical devices (PHD), e.g. IEDs, contain logical devices (LD) that encapsulate predefined logical nodes (LN). A logical node is the smallest part of a function that exchanges data. A LN is an object defined by its data (i.e. attributes) and methods (i.e. functions) [IEC 61850-7-1, 2003].

The general approach of IEC 61850 is to decompose application functions into small entities. The logical nodes are entities that communicate to exchange power process information, protection status, and control data. Using this approach, protection and control devices are made of several logical nodes. Obviously, one or more logical nodes embedded in different logical devices that are located in different physical devices can cooperate and perform distributed functions. In the case of either losing of one logical node LN or one included

communication link, the result can be losing functionality because of completely blocked function, or showing graceful degradations as applicable [IEC 61850-2, 2003].

The standard defines these data elements providing a given unique name. Hence that, the core of IEC 61850 series is the information model and modelling methods. The information represented by the data models and their attributes are exchanged by the communication services according to the well-defined rules and the requested performance as described in IEC 61850-5.

2.4.4.1 The concept of Logical Node

The logical nodes normally represent power protection tasks and related functions according to ANSI/IEEE formal device function numbers (IEEE std. C37.2, 2008). The standard uses the object-oriented methodology to define the logical nodes and their data regarding both content structure (syntax) and content meaning (semantic). IEDs manufacturers should follow these concepts to guarantee devices interoperability.

The IEC 61850 standard part 7-4 aggregates and groups the logical nodes into high-level LN groups according to their functions. For instance, MMXU logical node starts with M that represents measurements group [IEC 61850-7-4, 2003]. The standard defines 92 different logical nodes classified into 13 groups in which suppliers can develop a new LN under G group (Generic functions). Table 2.3 provides comprehensive examples about common used logical nodes that exist in most modern IEC 61850 enabled devices.

Table 2.3 : Logical Nodes Groups and number of corresponding LNs

LN Groups	Group Indicator	Number of LNs	Examples
System LNs	L	3	LPHD for physical device and LLN0 for common logical node information
Protection Functions	P	28	PDIF for differential and PTOC for time overcurrent protection
Protection Related Functions	R	10	RBRF for breaker failure and RREC for reclose recording
Supervisory Control	C	5	CALH for alarm handling, CILO for interlocking, and CSWI for switch controller
Generic Function References	G	3	GGIO for generic process I/O, GSAL for generic security application
Interfacing and Archiving	I	4	ITCI for tele-control and IHMI for human machine interfaces
Automatic Control	A	4	ATCC for automatic tap changer and AVCO for automatic voltage control
Metering and Measurement	M	8	MMXU for measurement and MMTR for metering
Switchgear	X	2	XCBR for circuit breaker and XSWI for disconnector switch
Instrument Transformer	T	2	TCTR for current and TVTR for voltage transformers
Power Transformer and related functions	Y	4	YLTC for tap changer and YPTR for power transformer
Further power system equipment	Z	15	ZBAT for battery and ZMOT for motor
Supervision and Monitoring	S	4	SCBR for circuit breaker and SLTC for tap changer supervisions
Total number of LNs is 92			

The IED as a physical device encloses a connection interface connected to the communication network. It has at least one network address that identifies its data set. The standard modeling starts with a physical device model that incorporates one or more logical devices. In this manner, the standard allows a single physical device to act as a proxy or a gateway for multiple devices (virtual devices) thus providing standard representation of a data concentrator [Mackiewicz, 2006]. Each logical device contains one or more logical nodes.

These logical nodes contain data objects (DO) that also include data attributes (DA). Figures 2.10 through 2.12 show an example of this data model. The logical node contains one or more data elements based on their functionality. For instance, data elements that represent a power equipment status or position with dedicated data attributes. These data objects have a structure and a defined semantic, i.e. meaning in the context of substation automation systems.

The average number of specific data provided by logical nodes is approximately 20 data objects [IEC 61850-7-4]. Each data, e.g. circuit breaker position, comprises several details (data attributes). For instance, the circuit breaker position (called "**POS**") is defined in the logical node **XCBR,** and the position data (**POS**) is made up of many data attributes. The data attribute **ctlVal** represents controllable information, i.e. can be set to OFF or ON. The data attribute **Pos.stVal** represents the position of the real breaker (could be in intermediate-state, off, on, or bad state). Fig 2.10 ilustrates a protection IED as a physical device that contain a physical device, i.e. PIED 1, which incorporates two logical nodes, PDIS and XCBR. The PDIS logical node has a data object representing operation mode, OP, that has two data attributes, similarly the XCBR logical node has a data object representing position of a circuit breaker that has two data attributes representing control and quality.

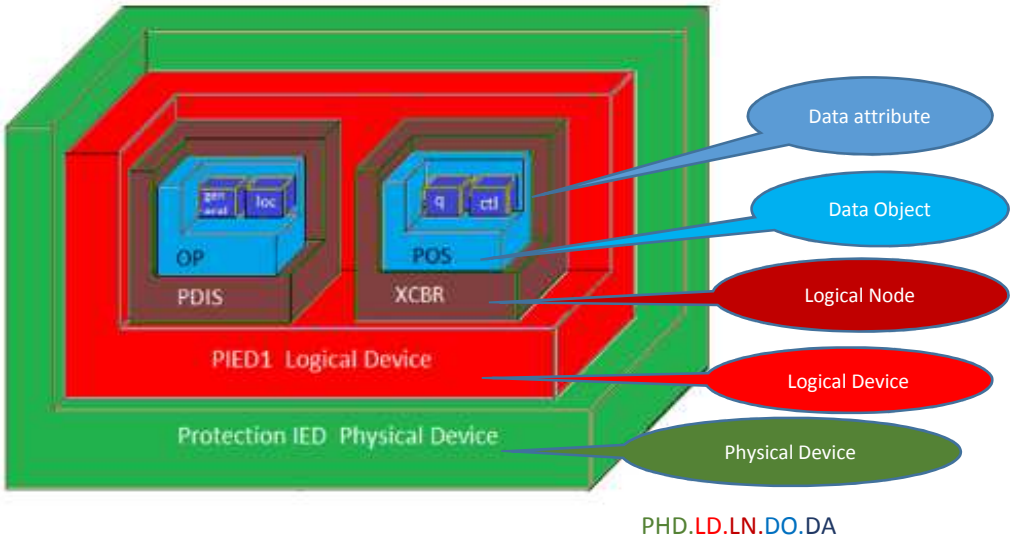


Figure 2.10 : Object modelling, of the IEC 61850 data, illustrates physical device and logical device

Fig 2.11 shows the hierarchy of the IEC 61850 data model with a given example showing the physical device PIED1. The data attribute shall have a value that is important for exchanging the status of an equipment and protection events.

Figure 2.11 : The concept of physical device with path to data attributes of logical nodes

Some data that refer to a physical device itself are needed such as results of device self-supervision. Therefore, the standard introduces a default logical node called as LLN0 [IEC 61850-5]. The logical node LLN0 contains information related to the physical device (IED) data (fig 2.12), independent from all included logical nodes, such as device identification or nameplate, device self-supervision, etc. IEC 61850-5 clauses 9, 11 and 12 provide names and classification of logical nodes according to their functions and logical location at station, bay and process levels.

Figure 2.12 : The default Logical node LLN0 within default logical device LPHD0

The part 7-3 of the standard defines common data classes (CDC), which group LNs data object elements into specific data classes. Each LN can have a few or up to 30 data objects that belong to CDC class. These data object in turns has a few or more than 20 data attributes. Each CDC describes the type and structure of data within the logical node, and each CDC has a defined name and set of CDC attributes with defined name, defined type and specific purpose [Mackiewicz, 2006; Mohagheghi et al, 2009].

2.4.4.2 Piece of Information for COMmunication (PICOM)

Information exchanged via logical connections between logical nodes are organized according to functional requirements. PICOM is a description for information transfer (logical connection) with communication attributes between two logical nodes. It also contains associated attributes such as performance data [IEC 61850-2].
The standard adopted this approach from the working group 34.3 of Conseil International des Grands Réseaux Électriques [CIGRE, 2001]. The PICOM does not represent the actual structure and format for the exchanged data, but IEC 61850-8 and IEC 61850-9 include this information. The components or attributes of a PICOM, as given by the standard, are:

1. Data that contains functions identification as needed by the devices (semantics).
2. Type that describes structures of the data, i.e. an analog or a binary value, a single value or a set of data, etc.
3. Performance that means permissible transmission times (performance class), data integrity and methods or transmission causes, e.g. periodic, event driven or on request.
4. Logical connection that contains logical source (sending logical node) and logical sink (destination logical node).

With these attributes, PICOM information describes exchange data between logical nodes that share status, values or changes (events) [IEC 61850-5]. Thousands of individual PICOMs

may describe communications between LNs, and these PICOMs have common similarities that are useful for classifying purpose, e.g. communication requirements. Classification allows obtaining of comprehensive requirements and supports strong modelling of the requested communication performance. These requirements differ according to the performance class that depends on the application criticality such as the fastest and important messages in the substation, i.e. trip and block messages.

By knowing required functions, designers can identify composed logical nodes and their associated communication requirements. In this way, they can statically estimate performance of substation networks depending on transmission time of logical nodes data (PICOMs). For performance evaluation, TC57 studied different substations and network topologies by using calculations database containing about 100 logical nodes and 1400 PICOMs. The standard uses this approach to calculate the data flow, without considering both message structure and frames overhead data. [Annex I of IEC 61850-5, 2003].

2.4.5 The IEC 61850 communication services

Communications inside substations exist in horizontal and vertical schemes. The horizontal communication inside modern substations takes place between IEDs. These devices exchange data in real-time. The vertical communications exist between operation, engineering and database archives at the station level and IEDs in the bay level. Other communications messages may carry power values such as current, voltage and frequency data from the process level to protection and control IEDs in the bay level.

Therefore, the standard defines data transmission rules in standardized methods of describing power system devices to enable all IEDs exchange data using identical structures related to their functions [Mackiewicz, 2006]. The Abstract Communication Service Interface (ACSI) models, described in the part IEC 61850-7-2, enable IEDs to behave according to specific rules in the network behavior perspectives. These models need to benefit from state-of-art networking technology such as communication protocols. The ACSI is a network independent interface that defines the semantic of service models with their attributes, and identifies what these services provide. Abstraction is necessary to separate SAS specific data models from the communication technology, in other words ACSI makes SAS devices compatible with the fast advances in communication technology [Mohagheghi et al, 2009]. Specific Communication Service Mapping (SCSM) defines messages encoding and syntax, e.g. peer-to-peer services for SV and GOOSE messages transmission.

Network communications between substation devices take the form of either a real-time multicast, i.e. publisher/subscriber without acknowledgment, such as SV and GOOSE, or client/server networking with connection-oriented association such as Manufacturing Message Specification, MMS, over Transmission Control Protocol/ Internet Protocol, TCP/IP (Fig 2.13). Power protection and control applications in substation automation systems require connectionless real-time performance due to time criticality, hence that, Ethernet frames encapsulate these data directly without middle-layers overhead data. While TCP/IP based communication, i.e. client /server MMS data exchange, uses additional layers for reliable delivery of messages.

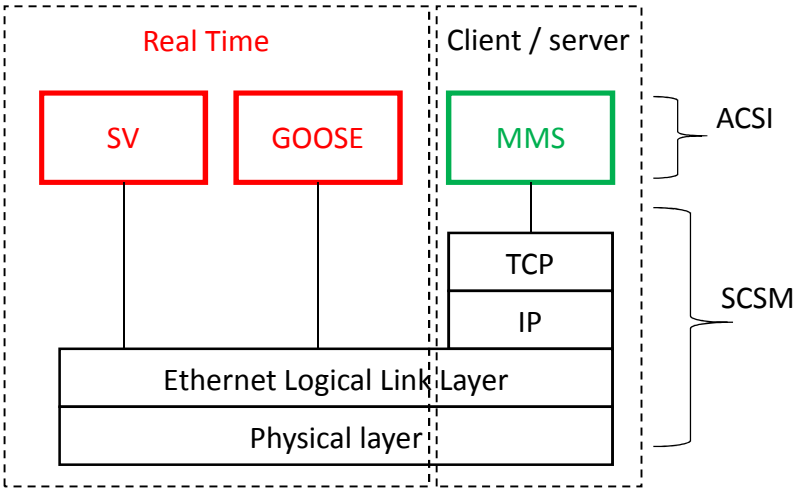


Figure 2.13 : Communication services: Direct mapping of real-time messages to Ethernet layers

2.4.5.1 Mapping to Manufacturing Message Specification (MMS)

The international standard organization (ISO) published the ISO 9506 standard that covers all aspects of MMS protocol, which is a public protocol that has a proven implementation track report in the field of process control. UCA chose MMS protocol in 1991 and that is lastly kept for IEC 61850, because of its rich library of objects and services [IEEE PSRC, 2005].

The IEC 61850 uses MMS objects for mapping of its objects, and MMS protocol easily supports the complex naming and service models of IEC 61850 [Mackiewicz, 2006]. Services mapping can become tedious and complex when choosing such protocols that support limited read/write/report services with simple variables accessed by register or index numbers.

IEC 61850-8-1 is a Specific Communication Service Mapping (SCSM) for mapping of client/server services into MMS protocol suits that has full TCP/IP stack above Ethernet layer, i.e. two bottom layers of the ISO Open System Connection (OSI) [Sidhu & Yin, 2007; Mohagheghi et al, 2009]. Non-critical data uses MMS message services embedded through reliable upper layers protocols starting from the application layer. TCP/IP based MMS data makes Ethernet frames longer with an overhead data, as a result messages transfer passes longer period. The MMS is suitable for communication between bay level IEDs and station level engineering workstations and HMI screens for many purposes such as sending commands, reporting, status polling, etc.

The mapping of ACSI services into MMS is straightforward, e.g. the MMS Service (Write) is used for the ACSI Service (Operate) and (Set Data Values), the MMS Service (Read) is used for the ACSI Service (Get Data Values) and (Select, i.e. the first step in a Select-Before-Operate control sequence). Many applications can use MMS services inside a substation, for example HMI, SCADA, control, and IEDs configurations [IEEE PSRC, 2005].

2.4.5.2 Generic Substation Events GSE

In addition to MMS, IEC 61850-8-1 defines peer-to-peer communication services named Generic Substation Events (GSE) for exchanging data between protection and control applications. These applications transfer defined data objects when their attributes change

[Liang & Campbell, 2008]. The information contained in the hierarchical model of the IEC 61850 models can be communicated using services defined within the standard mapping services [IEC 61850-7-2]. These services have a relation to the IED input from (or output to) the process information. The information models, i.e. logical nodes and data classes, and the service models, e.g. reporting and logging, provide means to retrieve comprehensive information about the data model and the services that operate on the information models (self-description) [IEC 61850-7-1].

GSE includes two kinds of message services, Generic Object Oriented Substation Events (GOOSE), i.e. IEC 61850 GOOSE, and Generic Substation State Events (GSSE) that is backward compatibility for UCA GOOSE. The GSE– GOOSE and GSSE-provides the peer-to-peer information exchange between the input data values of one IED to the output data of many other IEDs via multicast communication pattern [IEC 61850-7-1, 2003].

IEC 61850 GOOSE flexibly carries long datasets, while GSSE is used to carry binary data representing state changes (bit pairs). The IED creates a data set that contains many data with associated attributes, e.g. analogue, binary or integer values. The IEDs publish GOOSE messages containing data values grouped into data sets. Other IEDs subscribe to and receive interested published GOOSE and GSSE messages in order to manage decisions or compute data for internal use such as local interlocking condition processing via comparing received switches positions. Therefore, the IED can play a role of publisher and subscriber at the same time.

IEC 61850 transmission profiles for time-critical applications require real-time performance class such as GOOSE messages (see chapter 3). This constraint enforces directly embedding of GOOSE dataset into an Ethernet frame, instead of using TCP or UDP as transport protocols, thereby avoiding processing of any middle layers, and making shorter frames without overhead data [Mackiewicz, 2006]. The protection and control IEDs can exchange input and output status via multicast GOOSE messages in the substation bay-level. A new connected IED can publish initialized data about its status. Thereafter, the IED receives subscribed data, via a serial communication, from other IEDs to act on the substation according to their programmable logic algorithm. In this approach, IEDs can cooperate without input/output hardwired connections.

In the following page, table 2.4 compares between UCA 2.0 GOOSE, i.e. IEC 61850 GSSE, and IEC 61850 GOOSE [Schwarz, 2004; IEEE PSRC, 2005]:

Table 2.4 : A comparison between UCA GOOSE and IEC 61850 GOOSE

	UCA GOOSE	**IEC 61850 GOOSE**
Standardization	IEEE TR 1550-UCA 2.0 (technical report)	IEC TC 57 (international standard)
Issue date	1999	2003
Mapping to	ISO Ethernet 8802-3	IEEE Ether-type with Ethernet II
Priority support	Not supported	Supports priority tagging (IEEE 802.1p)
VLAN support	Not supported	Supports VLAN (IEEE 802.1q)
Frame content	Fixed size binary data	flexible dataset from any data object embedded into Ethernet data frame
Data types	Binary bit pairs	Supports any type of information (logic bits, characters, bytes, integers, float numbers etc.)
Maximum length	259 bytes / 24 bytes for overhead control data	1518 bytes up to 1522 with priority and VLAN tagging / 22 bytes for frame overhead control data
Reliability	Basic feature depends on a cyclic redundancy check field	Enhanced with retransmission mechanism carrying reliability related fields: sequential counter, status change counter, quality, time to live and timestamp

2.4.5.3 Measured Sampled Values SV

The IEC 61850 extends its scope to include digital communications to: 1) the process switchgear with integrated electronics and to 2) non-conventional current and voltage transformers (acting as sensors) with a digital communication interface [IEC 61850-9-2, 2010]. With these communication interfaces, the standard enables transmission of sampled values representing current, voltage, frequency and other process values.

The transmission of sampled values requires special attention regarding the time constraints [IEC 61850-7-2]. To avoid processing delay of the middle layers, the standard maps the SV application data directly into Ethernet layers (two lower layers of the ISO OSI). The transmission of SV messages uses unidirectional multicast or unicast communication scheme. These messages contain measured values already sampled and digitized at the source, and directly encapsulated into Ethernet frames (Fig 2.14). IEC 61850-9-1 defines mapping of measured sampled value to Unidirectional Multi-drop Point-to-Point link carrying fixed data. While 61850-9-2 identifies the transmission mechanism of SV frames with configurable dataset embedded into multicast Ethernet frames. Nevertheless, both parts do not provide details about the data, sampling rate and size that can define how many frames will be sent during a power cycle, e.g. 20 milliseconds for 50 Hertz. Devices that send streams of sampled values, such as merging units, require high synchronization precision class.

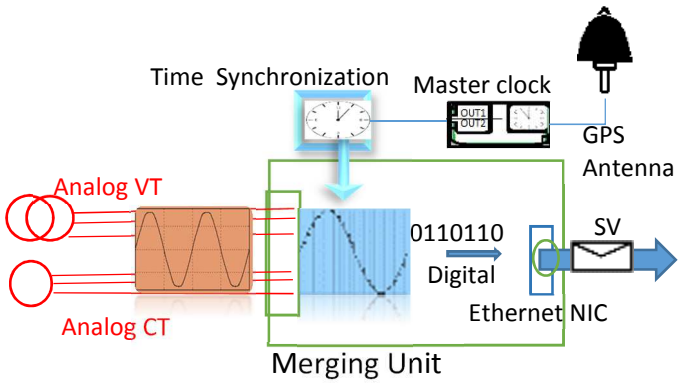


Figure 2.14 : Time source enables synchronization of Merging Unit SV streams

IEC 61850-5 mentioned messages performance requirement, among these messages the time synchronization message that requires time precision expressed in microseconds. This part of the standard also mentioned the raw data performance class [see chapter 2 table 2.2] as transfer time requirement. This time counts from the time the sender puts the data content on top of its transmission stack up to the time the receiver extracts the data from its transmission stack [IEC 61850-5, 2003].

Regarding the transfer time, the standard classified communication between message types into messages and performance classes. The SV messages are classified into raw messages type with three performance classes namely P1, P2 and P3 that have sampling rate of 480, 960 and 1920 samples per second consequently. These messages require sampling rate accuracy down to one microsecond time precision.

2.4.5.4 Time Synchronization

Timing functions support data objects and services that contain timestamp attributes. The standard proposes a time synchronization model that shall use simple network time protocol (SNTP) via LAN communications [IEC 61850-8-1, 2003]. This type of communication service carries timing messages to synchronize devices such as MUs and other IEDs internal clock in the SAS.

Ingram et al, find that Precision Time Protocol version 2 (PTPv2) is a credible option for synchronizing IEC 61850-9-2 based devices such as merging units (MU). They followed a guideline, published by UCA in 2004, about the SV implementation, which is commonly referred to as IEC 61850-9-2 Light Edition (LE). Several suppliers of non-conventional instrument transformers follow the 9-2LE guideline that specifies the data set, sampling rates, time synchronization requirements and physical interfaces [Ingram et al, 2011].

The precision time protocol profile for power utility automation supports highly precise synchronization with IEEE 1588-2008 standard [IEC 61850-9-3, 2016]. Understandably, MUs and related devices that send and receive measured sampled values require high precision time for SV frames synchronization and timestamp data attributes (Fig 2.14). In this case, the protection system may benefit from master time hardware devices such as GPS based timers that use universal time system UTS as a reference for clock synchronization.

2.4.6 The Substation Configuration Language (SCL)

In March 2004, TC 57 committee released the IEC 61850-6. This part specifies the SCL language that is used to describe IED configurations, substation system and communication system according to IEC 61850-5 and all parts of IEC 61850-7. This language identifies file formats based on eXtensible Markup Language XML 1.0 [IEC 61850-6].

Within this part, the standard intends to facilitate the engineering process at the early stages of any substation project. First tasks would include setting project specifications such as documenting SAS design requirements. In other meaning, SCL files must be capable of describing: a) functional specifications, b) IED engineering data, and c) SAS engineering data. This concept helps to describe and automate configurations of the system design that begins with single-line diagrams, protection and control functional units represented by LNs and communication engineering including LNs interactions and description of these communications.

SCL specifies a hierarchy of configuration files that enable multiple levels of a target system to be described in unambiguous and standardized XML files. The standard proposes various SCL files including system specification description (SSD), IED capability description (ICD), substation configuration description (SCD), and configured IED description (CID) files. These files contain different scopes, but follow same methods and formats [Mackiewicz, 2006]. The philosophy behind using SCL is to ease reusing of IED configuration by sharing and importing preconfigured files. SCL enables configuration of functions and related applications without network connection to a client software, i.e. offline. This offline system configuration enables development of software-based tools, to automate generation of required files from power process designs, which reduce the efforts and the cost by avoiding manual configuration tasks in large projects. The resulted files help documenting all the project phases because all configured devices and their role in the SAS can be gathered automatically. The configuration files contribute to the substation design file by importing and exporting these files among several projects. Four types of SCL files provide specific tasks [Mohagheghi et al, 2009] (Fig. 2.15):

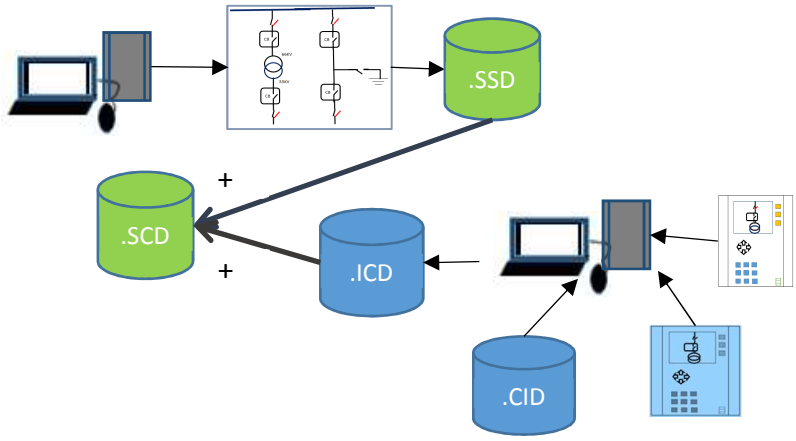


Figure 2.15 : SCL based tools enable creation of several XML based substation-engineering files

1. ICD describes an IED capability, and includes sections for IED data attributes, data type templates, logical node type definition, optional communication and optional substation.
2. SSD describes specifications of related system through an SLD diagram, and includes substation description section, data type templates, and definitions of logical node types.
3. SCD describes a detailed power substation system, and includes description section for each IED with data type templates, full IEDs communications configuration section and substation description section.
4. CID describes a configuration of a particular IED that has a unique communication section, containing a current address for an IED to exchange data and settings with configuration tools.

With these files types, a complete configuration description of a substation project, automation system and all IEDs is available in XML formats instead of traditional documents. With this approach, standardized third party engineering tools, i.e. supplier independent, can support configuration and documentation through the substation-engineering project.

2.5. Discussions and motivations

The emerging economics lead to new challenges considering several technologies. These challenges require comprehensive solutions that need to sustain for short and long terms. The development of Smart Grid opens new dimensions for research in academia and industry. One of these dimensions is scalability, dependability and feasibility of transmission and distribution substations in the electrical power system. These substations play a major role in the grid stability and dependability where emerged functionalities such as protection and control are evolved. The IEC 61850 standard brings advantages such as flexibility of protection schemes, Ethernet based communications, and exchange of substation events.

This research shall investigate various components of the substation automation system based on the IEC 61850 standard and develop methods for testing to assist the design and validation of Ethernet networks inside the bay and process levels. Besides, during these tests evaluation of the standard communication performance shall be performed. The evaluation shall cover the standard protocols regarding the service quality. Dynamics of the protection schemes also shall be observed to identify malfunctions and failures. These works will provide

helpful understanding, which is essential for achieving FAT (Factory Acceptance Testing), and SAT (Site Acceptance Testing) procedures.

The gathered data during the dynamic tests and evaluations will be exploited in order to classify root causes of malfunctions and failures (or errors). The aim here is to investigate the dependability of the proposed techniques, by the IEC 61850 standard, for the substation automation and communication in terms of dynamic behavior of the protection schemes.

To undertake these tasks, relevant literature will be reviewed considering the standard several parts and their releases. This review will include searching and studying research works involve performance evaluation and fundamentals of the IEC 61850 communication protocols by focusing on the GOOSE and the related protection and control functionalities.

2.6. Conclusion

The transmission and distribution substations play vital roles in the electrical power grid. In this chapter, background information about these substations and automation systems and functions are provided. The reader can understand the communication architectures inside substations. Legacy and modern communication protocols are briefly illustrated and compared.

In conjunction with its engineering series, the IEC 61850 is a core standard that offers promising technical solutions. The standard brings to power utilities adopted communication services that utilize Ethernet based protection and control communications, object modeling concepts and digital substation automation systems. These communications exist in modern digital substations at many levels to provide many advantages such as reducing costs, efforts and space of wired connections. Tangible advantage is the avoiding of possible voltage contact at the control rooms.

The standards press on compulsory specifications such as performance and time requirements concerning exchange of substation events and switchyard related status. Dynamic testing is required in a real-time environment to evaluate and assess the performance of the protection and control functions in this circumstance. Performance evaluation, functional testing and dependability studies of IEC 61850-based architectures require detailed understanding of dynamics (interactions) between the protection and control functions from one side, and the communication services and the data objects from the other side.

chapter 3 : The Evaluation and Testing of IEC 61850 Based Protection and Communication Services

3.1. Introduction

Substation communications that involve IEC 61850 enabled devices become part of the utilities retrofit and renovating plans. In spite of its novelty, many trials were endeavored to evaluate the interoperability among different suppliers' devices. For instance, the UCA international users' group[1] organizes interoperability tests every two years.

Due to the critical role of substations in the power grid, design of substation automation systems must guarantee dependable operation and conformance to the standards. This conformance requires specific procedures to test and validate the protection and control IEDs. Alternative approaches are proposed to tackle these tasks because testing of in-service high voltage substation is not possible during operation modes. The part IEC 61850-10 suggests testing techniques for implementations conformance, as well as specific measurement techniques to be followed during evaluation of performance parameters. The industry and academia witnessed numerous efforts to tackle these concerns.

This chapter presents a review of past and current efforts that cover topics related to the testing, assessment and performance evaluation of the IEC 61850 standard based communication services, and protection functions. The review focuses on the process and bay level communication services where devices interact to accomplish certain missions. The referred sources arrange among international standards, academic resources, professional magazines, suppliers' product specifications with conjunction of industrial reports.

Sections from 3.2 until 3.3 afford fundamental materials related to the IEC 61850 communication services. Section 3.4 provides definition of time requirements and several constraints about transfer time obligations. Section 3.5 reviews related studies and helps to distinguish between several approaches of testing and evaluation of the standard services, while section 3.6 compares between these approaches. Section 3.7 concludes this chapter showing some challenged issues.

3.2. The Data Communication Networks inside IEC 61850 Substations

Communication networks in substations are necessary at many project phases, i.e. installation and configuration as well as operation phase. Data networks allow exchanging of operation data such as protection response messages and control commands to clear fault events. While the control system typically acts slowly, perhaps on the scale of seconds, the protection system acts at a much higher speed, i.e. one fourth of a cycle (~ 4 to 16ms for 60 Hz) [IEEE PSRC, 2015]. Therefore, digital networks currently exist in hierarchical architectures to support high-speed protection and control applications. Sending commands from control room devices to switchyard equipment in early days design require physical hardwired connections. In contrast, these days' vertical communications exist as MMS client/server (fig. 3.1, interface 1 and 6) network connections [Mohagheghi et al, 2009].

Data networks also take a horizontally place between protective relays (IEDs) at bay and process levels. With this hierarchy operators and technicians can operate commands either locally at a substation control room or remotely at control centers that are connected via wide area networks (see § 2.3.4)

1. http://iec61850.ucaiug.org/2017IOP-NOrleans/default.aspx

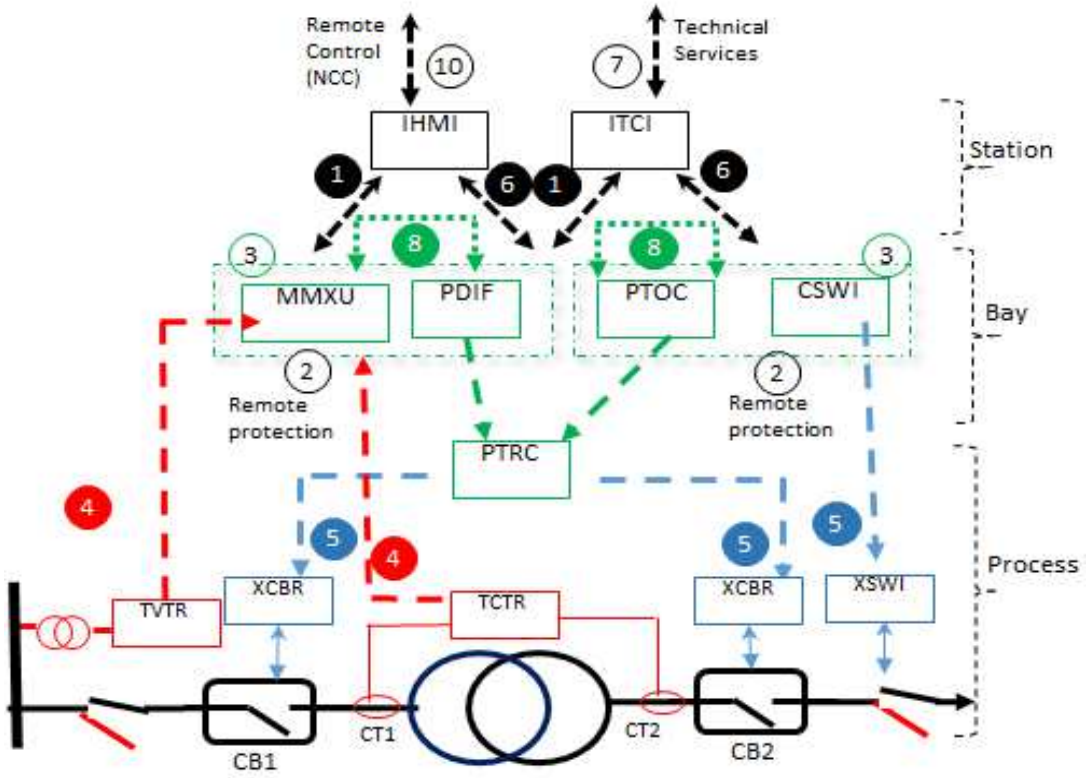


Figure 3.2 : Representation of logical communications in IEC 61850 based SAS

Fig. 3.1 shows several communication interfaces (small circle with numbers inside), for instance interface 1 represents exchanging of protection data between station and bay level, interface 2 represents protection data exchange between bay level and remote protection system, i.e. in another substation, which is beyond IEC 61850 scope. Interface 3 represents data exchange within bay level, while interface 4 represents data transfer, e.g. current measurements, from process to bay level. Interface 5 and 6 represent exchanging of control data from bay to process and from station to bay respectively. Interface 8 represents data exchange between several bays within a substation, while interfaces 7 and 10 represent data exchange between a substation and remote engineering and remote control center respectively, i.e. both are beyond the standard scope. Time-critical distributed protection functions use horizontal GOOSE (Fig 3.1, interface 8). The peer-to-peer publisher/subscriber GOOSE communication pattern uses Ethernet multicasting without acknowledgement hence this behavior is analogous to applying a voltage on wire , i.e. hardwired signals between protection relays to exchange status and events[Ali, 2012]. The communication using GOOSE protocol allows high-speed communication over Ethernet technology [Fernandes et al, 2014]. An IED can publish GOOSE messages to a nearby subscriber (IED), or many subscribers simultaneously. Another communication service is a unidirectional multicasting (interfaces 4 Fig. 3.1) from process switchgear to bay level devices, e.g. multicast sampled value (SV) frames used to transfer digital power parameters. The logical nodes (rectangular shapes in fig 3.1) can be incorporated into a single device, e.g. trip conditioning (PTRC), protection through differential and time overcurrent (see table 2.3 for logical nodes initials).

3.3. The Ethernet based SAS Communications

The DIX (Digital Equipment Corporation, Intel and Xerox) consortium introduced the Ethernet technology in the late 1970ˢ. Both IEEE and ECMA (European Computer Manufactures Association) made efforts to standardize this technology. In 1983, The IEEE 802 committee (formed in February 1980) released the first draft of the standard 802.3 that includes CSMA/CD (carrier sense multiple access/collision detection) mechanism. Commercial use of Ethernet technologies became popular in the late 80ˢ [Pujolle, 2008].

In the early days of Ethernet LANs, bus topology with coax cables were widespread implementations, and data rate was around one Mbps. Network nodes shared the same bus segment to transmit and receive Ethernet frames across a broadcasting domain. The sharing of physical media limits the data rate and network length. To extend the length of network segments a device called repeater retransmits automatically all received data signals, which in return causes broadcasting of noise into the entire network. Hence, number of segments and repeaters are limited in an Ethernet network. In contrast, to connect two segments a device called bridge passes data frames within the same segment, via knowing their addresses, to extend the network length and to decrease the broadcasting domains.

Ethernet originally is a LAN (Local Area Network) technology for computer networks, which has evolved since its appearance to offer several improvements for data rate performance and network applications. These improvements enthused manufactures to adopt the Ethernet technology for industrial applications.

3.3.1. Shared vs switched Ethernet

A hub is a device with many ports, which connects network terminals and establishes a star topology. It acts like a repeater broadcasting ingress frames to all egress ports. An Ethernet switch is an intelligent device that inspects data frames to determine destination addresses that help delivering frames to their exact destination [Tanenbaum & Wetherall, 2011].

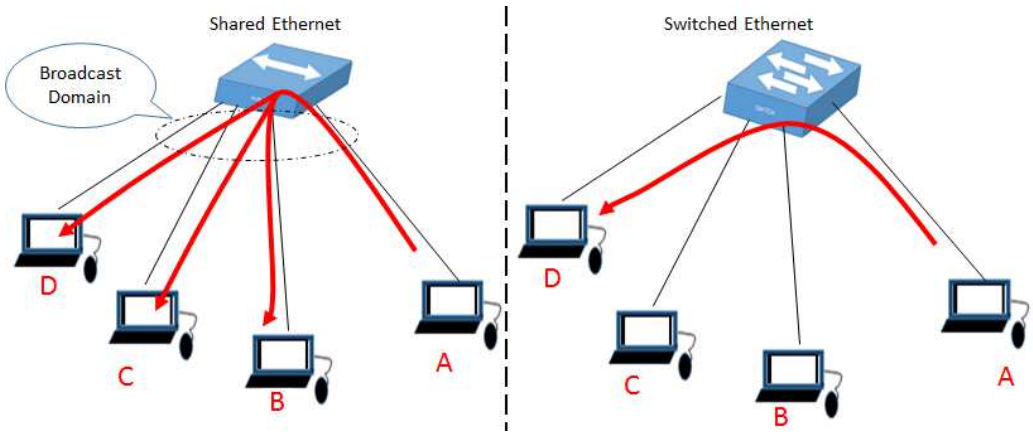


Figure 3.2: Shared vs. Switched Ethernet: switches eliminate broadcast domains

Bus and hub-centric networks have a common physical interface for a group of terminals. These networks support shared access to a physical medium. Therefore, data transmission at nodes should be controlled to avoid frames collision. Network nodes use CSMA/CD to control frames transmission. Collisions happen when two nodes send frames at the same time. A network node listens to the shared communication channel before transmission. When a shared

channel is busy, a network node will enable back-off algorithm that identifies delay period for retransmission, then the node will transmit when the channel become free [Pujolle, 2008].

Ethernet devices work in two bottom layers, i.e. physical and data link layers, of the ISO OSI (Open System Interconnection) model. These devices have MAC (Media Access Control) addresses that are unique identifiers for each network interface. This address has six bytes long representing manufacturer and serial numbers.

In 1990s, switched Ethernet is introduced, when devices called switches are used to connect personal computers, printers and other Ethernet enabled devices. It is important to note that, while they are both referred to as Ethernet, they are quite different. Classic Ethernet is the original form and ran at rates from three to ten Mbps. Switched Ethernet is what Ethernet has become and runs at 100, 1000, and 10,000 Mbps, in forms called fast Ethernet, gigabit Ethernet, and 10 gigabit Ethernet respectively. In practice, switched Ethernet is mostly used nowadays [Tanenbaum & Wetherall, 2011].

The switch is an intelligent device that learn and save MAC addresses in order to determine destinations of Ethernet frames. This mechanism avoids collisions between transmitted frames, especially when full-duplex technology enables transmission and receiving of frames between nodes and switches at the same instances. Data rates are increased with the introduction of network switches that have additional features such as full-duplex transmission, auto negotiation of transmission speed, and fast switching. The switching mechanisms could be one of the following methods [Pujolle, 2008]:

a) Store-and-forward: switches save all ingress frame data into the switch memory, and check error before retransmission
b) Cut-through: retransmission begin toward egress port when destination address is known from frame header fields.
c) Adaptive error free: adoption of both above mechanisms, which means a switch starts retransmission using cut-through and changes its mechanism into store-and-forward when errors happened.

3.3.2. Priority and Virtual LANs

When a network administrator wants to manage departments and build *n* separated LANs, he can buy *n* switches and assign each department a switch that results in a large LAN consisting of these separated switches. Nevertheless, in such situation, putting all computers on a single LAN adds initial costs, increases network load and worsens security. In addition, building a physical topology to reflect the organizational structure can add maintenance work and cost, even with centralized wiring and switches. Three issues will face the network administrator in this situation; the first issue is a security matter because all devices can access the network, the second issue is increased network loads, and the third issue is broadcast traffic domains [Tanenbaum & Wetherall, 2011].

Switches broadcast (increased traffic) when destinations are unknown. Another problem related to broadcasts: occasionally a network interface collapses and begins generating an endless stream of frames leading to additional traffic. The result of this broadcast storm is that (1) these frames occupy the entire LAN capacity, and (2) all the devices process and discard all the frames being broadcast [Tanenbaum & Wetherall, 2011]. To overcome these issues a tag field is added to each Ethernet frame that enabled multi-tree bridge. This tag is what is known as the VLAN tag, i.e. in 2003 technically becomes IEEE 802.1Q header [IEEE, 2003]. Network suppliers began working on a way to rewire departments entirely in a software based LAN

resulting in a concept of VLAN (Virtual LAN). Virtual network is a separated broadcast domain [Pujolle, 2008].

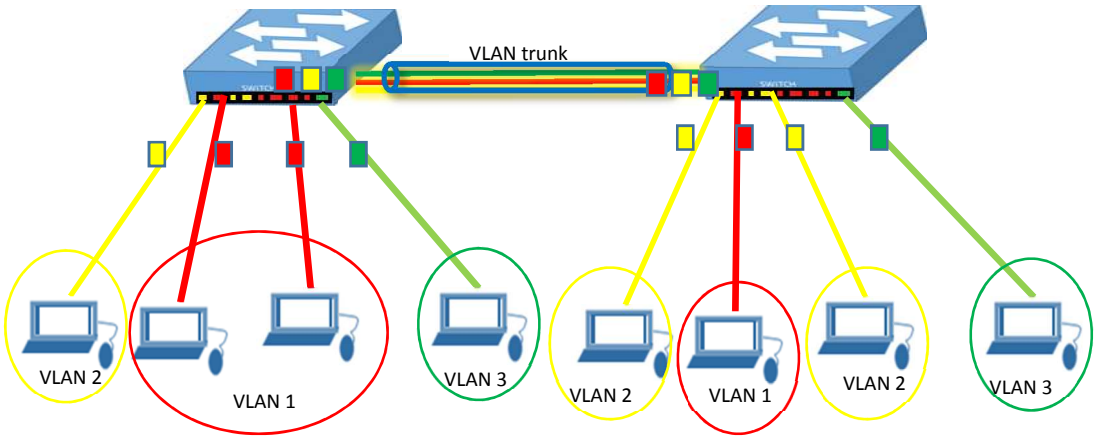


Figure 3.3: Virtual LANs, two switches reduce broadcast domains via three VLANs

Managed switches with VLAN implementations help splitting the Ethernet network into virtual segments (Fig 3.3). The IEEE 802.1Q standard introduces additional fields, into Ethernet frames, to support this implementation. Three-bits exist to implement priority for specific traffic in order to provide better quality of service over Ethernet [Pujolle, 2008]. Additional benefit is that VLANs increase security, e.g.: a) limiting broadcasting domains, multicast or unicast traffic with same VLANs. b) Hosts at VLAN 1 will not receive data frames not belonging to their VLAN and they cannot see other VLAN traffics, c) devices can be forced to communicate with the same VLAN devices only.

The quality of service (QoS) for specific applications data can be achieved via prioritizing the data frames belonging to these applications. Frames marked with high priority levels, in this case, are always sent before any low priority frames that are buffered in the switches memory. For example, priority scheduling is needed for real-time applications when network loads can affect time-critical functions [Pujolle, 2008]. A study proposes a method to identify the relation between traffic scheduling and regulating mechanisms and their effects on QoS values. This method is based on fuzzy logic to dynamically control QoS [Bombardier et al, 2018].

3.4. Teleprotection and IEC 61850 communications performance parameters

3.4.1. Definitions of propagation, transfer and transmission time

As early mentioned in the previous chapter, protection and control functions are distributed among several IEDs (cf. section 2.3.3). These devices cooperate through a LAN network to perform real-time functionalities. For example, one of the functionalities that requires coordination is the interlocking scheme when modern network-enabled IEDs intercommunicate by means of peer-to-peer network connection to exchange relevant switchyard status. The IEC 61850 GOOSE messages are used for exchanging system status and events. By nature, these messages are not commands, in contrast they include datasets that represent status of equipment such as circuit breaker position, protection function pickup, etc. These messages enable changing a position of circuit breakers via modifying a position field

(data attribute) for a specific circuit breaker object (XCBR) at the connected IED dataset [Mackiewicz, 2006].

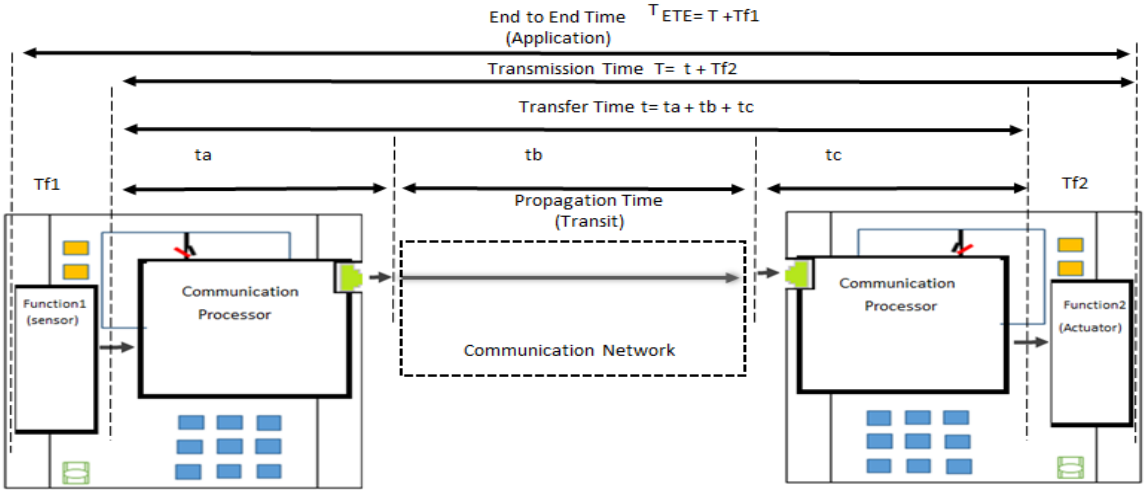


Figure 3.4: Transfer, Transmission and Application time

Figure 3.4 shows propagation, transfer, and transmission time schemes. Additionally, an End-To-End time also is shown as a communication period between two functions inside two IEDs. Most important time in this figure is the propagation time of event messages, i.e. GOOSE carrying events and status data.

3.4.2. Performance classes and time requirements

The standard classified time-critical messages of protection functions and other messages into performance classes and types. There are two independent groups of performance classes, one for control and protection (P class), and another one for metering and power quality applications (M class). Table 3.1 provides description of the performance classes. Process data such as sampled values require accurate time tagging (timestamp) with high precision constraints. Time synchronization needs two subtasks: 1) setting of absolute time in the distributed nodes and 2) continuous synchronization of the clocks in the distributed nodes [IEC 61850-5].

Table 3.1: description of the performance classes

Class	Applies typically to
P1	Distribution bay or where low performance requirements can be accepted
P2	Transmission bay or if the customer does not specify.
P3	Transmission bay with top performance synchronizing or differential requirements.
M1	Revenue metering with accuracy up to the 5th harmonic.
M2	Revenue metering with accuracy up to the 13th harmonic
M2	Quality metering up to the 40th harmonic

Table 3.2 shows message types with the correlated performance classes. It is clear that synchronization at the process level requires precise timing and accurate synchronization, because real-time protection depends on many calculated power parameters and fast protection response.

Table 3.2: Messages types and performance classes according to IEC 61850-5

Type		Application	Performance class	Time requirement
1	1A	Time-critical, e.g. trip.	P1 P2/P3	T <= 10 ms T<= 3 ms
	1B	Other fast message but not critical	P1 P2/P3	T <= 100 ms T <= 20 ms
2		Medium speed messages		T <= 100 ms
3		Low speed messages, e.g. settings parameters		T <= 500 ms
4		Raw data, e.g. synchronized sampled values	P1 P2/P3	T <= 10 ms T<= 3 ms
5		File transfer		T >= 1000 ms
6		Time synchronization for IEDs and SV metric devices, e.g. MUs	T1,T2,T3,T4,T5	High precision accuracy (±): 1ms, 0.1ms, 25µs, 4µs, 1µs

- T: total transmission time
- T1 to T5: time performance classes
- T3 to T5 are required for supporting type 4 messages and where process data transferred

Table 3.2 illustrates performance requirements for message communication. These requirements set a constraint for delay time, i.e. transmission time, between publishers and subscribers in case GOOSE messages are used. It is obvious that station level communication requires low speed where users perform slow tasks, while message transfer at the bay and process levels requires fast speed for fast protection and automatic control. For instance, a P2/P3 class of performance is assigned to GOOSE trip messages [IEC 61850-5]. The transmission of process measurement, i.e. SV, and timestamping of substation events needs a T4 class of performance with four microseconds as precise synchronization of time messages with P2/P3 as transmission class of performance (transfer time in terms of three milliseconds).

To summarize the requirements of IEC 61850: this standard sets performance levels P2/P3 for transmission substation (voltage more than or equal to 100 kV), and assigns type 1A for trip GOOSE and type 4 for SV measurement streams where transfer time must not exceed 3 ms [IEC 61850-5]. The standard allocates 20% of this time to network transmission and 80% divided between publisher and subscriber nodes, which means 600 µs for the communication channel and 1.2 ms for two communicated nodes (sender and receiver IEDs) according to [IEC 61850-10]. Ethernet communications should respect the standards requirements, especially time constraints and performance levels. The GOOSE based event exchanging normally faster than hardwired based signaling [IEC 61850-8] due to transfer of digital dataset within the GOOSE frames instead of classical hardwired analog signals. Similarly, SV based measurements according to [IEC 61850-9-2] reduce wiring complexity and increase speed and flexibility of installations compared to traditional CT/VT instrumentation.

3.4.3. Teleprotection schemes performance requirements

The IEC 61850 standard refers to other norms for performance requirements. Nevertheless, it does not refer to methodologies for assessment of security and dependability of digital communications for the teleprotection functions. The standard IEC 60834-1 identifies

these issues, i.e. this standard terminology is not similar to the dependability community nomenclature. Section 3.3 of this standard defines performance requirements (table 3.3) and testing approaches for teleprotection communications (for details about protection schemes see chap 4 § 4.3.3). The standard states that a nominal transmission delay is a transmission of GOOSE message in a noise-free channel, while the actual transmission time (T_{ac}) is the transmission delay of a protection message (GOOSE) in a noisy communication channel. Furthermore, it defines the probability of unwanted commands (P_{uc}) which is related to the safety considering the dependability community, (see chap 6 § 6.2), i.e. the ability to prevent interference from issuing a command state at the receiver, which is given by:

$$P_{uc} = \frac{N_{uc}}{N_B} \qquad (3.1)$$

Where N_{uc} is the number of unwanted commands, N_B is the bit error rate bursts, whereas the dependability is the ability to issue a valid command during interference and noisy conditions, which is signified by low probability of missing commands (P_{mc}) [IEC 60834-1, 1999].

$$P_{mc} = \frac{N_T - N_R}{N_T} = 1 - \frac{N_R}{N_T} \qquad (3.2)$$

Where N_T and N_R represent the number of transmitted and received commands respectively. The test procedure shall use noisy-type fault injections. These injections imply bit error rates correlated to equivalent traffic impairments [Scheer & Woodward, 2001]. Table 3.3 represents the requirements for both missed and unwanted commands within varied channel quality and noise duration if digital communications are used as means for teleprotection signaling.

Table 3.3: Time constraints and performance requirements of digital teleprotection communications [IEC 60834-1, 1999]

Protection scheme	**Maximum actual transmission time T_{ac} (ms)**	**Channel quality (BER)**	**Noise duration T_B (ms)**	**Security P_{uc}**	**Dependability P_{mc}**
Blocking	10	10^{-6}	continuous	N/A	$< 10^{-3}$
Blocking	10	Worst case	200	$< 10^{-4}$	N/A
Intertripping	10	$< 10^{-6}$	Continuous or pulsed	N/A	$< 10^{-4}$
Intertripping	10	Worst case	200	$< 10^{-8}$	N/A
N/A means not applicable					

Noticeably, with blocking and intertripping schemes (see § 4.3.3) Table 3.3 depicts that actual transmission time, i.e. transmission where impairments such as traffic load and noise do exist, must be within a range of 10 ms with pulsed and continuous noise. However, specific requirements differ according to the protection scheme: a) security that must be reported with worst case during 200 ms of noise duration and b) dependability that should be checked with continuous and pulsed noise and 10^{-6} rate of bit errors. As I insist here that, the used terminologies from this standard, i.e. security and dependability, are not similar to the academia point of view in which security and dependability in this context shall be safety and reliability with the academia terminology (see chap 6 § 6.2).

3.5. Testing and benchmarking Ethernet network services

As it was reminded in the previous parts, communication networks have entered many sectors, which are not limited to the information technology field. Many electric utilities use Ethernet based networks to deploy protection and control applications that evolved significantly with the use of Ethernet in substation automation networks. In this section, available benchmarking techniques are given. The communities of the information and communication technology have developed specific techniques that can be used for evaluating the Ethernet based services.

3.5.1. The internet engineering task force (IETF) methods

Initially, the request for comments (RFCs) issued by the internet engineering task force (IETF) and the internet society have been used to offer benchmarking methodologies that can be used to evaluate Ethernet services performance. Generally, the RFC 1242 (Benchmarking Terminology for Network Interconnection Devices) provides benchmarking terminology and definitions for interconnection devices, while the RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) was published particularly as a benchmarking methodology for internetworking devices in the lab. RFC 2285 (Benchmarking Terminology for LAN Switching Devices) and 2889 (Benchmarking Methodology for LAN Switching Devices) are commonly used for benchmarking of network switching devices.

RFC 2544 recommends generating traffic that overloads network devices' resources in order to assess their capacity [Morton et al, 2012]. Industry and academia introduced many modifications to the RFC 2544 methodologies and guidelines to describe specific issues in production environments. Bonica and Bryant suggested an approved method adapted to the production service activation [Bonica & Bryant, 2012]. In result, these methodologies are not appropriate for inclusion in wider specifications, which limit testing of telecommunication service due to some artifacts such as:

1. Validation of service configuration, e.g. the committed information rate (CIR).
2. Validation of performance metrics in a service level agreement (SLA), e.g. frame loss and latency.
3. Service activation testing, where traffic that shares network resources with the test could be adversely affected [RFC 6815].

3.5.2. The international telecommunication union (ITU) approach

To overcome limitations of the RFC 2544 methodologies, which are mentioned previously, in 2011 a leading standardized body, the international telecommunication union (ITU), released systematic methods that develop testing and benchmarking metrics for Ethernet services. The ITU-T Y.1564 specifies a standardized methodology to measure the performance parameters, which covers assessment of information rate, service level agreement and service activation test. In fact, ITU-T Y.1564 is more comprehensive and applicable than RFC 2544, e.g. inter frame delay variation is not part of RFC 2544 legacy test standards. The ITU-T Y.1563 and ITU-T Y.1564 standards involve extra definitions for vital metrics covering Ethernet service such as throughput, bandwidth, frame loss, delay and frame delay variation [ITU-T Y.1564, 2011 & 2016]. The recommendation of ITU-T Y.1564 fills the methodological gap for measurement of operational Ethernet network services. It covers new benchmarking metrics applicable to Ethernet service activation that include:

1. Multiple time durations for tests, as often performed in operational networks with time-varying impairments.

2. Measuring committed information rate (CIR) and excess information rate (EIR) with several frame rates and several type of loads.
3. Identifies bandwidth components profile with color mode representing CIR and EIR.
4. Measuring latency and frame delay variation within several traffic load profiles.

The bandwidth profile is a concept, related to the expected frame service rate, which defines four traffic parameters: a) committed information rate (CIR), b) committed burst size (CBS), c) excess information rate (EIR) and d) excess burst size (EBS) [ITU-T G.8011, 2015]. The CIR can be defined as the maximum sustained information rate (IR) the network is committed to transfer while meeting the performance level guaranteed in the service level agreement (SLA).

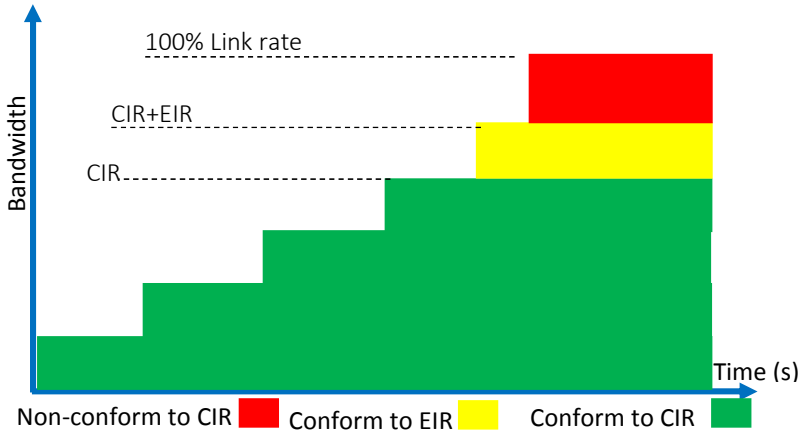


Figure 3.5: classify frames according to bandwidth profile

Performance metrics in terms of frame delay, frame delay variation and frame loss are applicable only to those frames that are transmitted at or below the CIR [ITU-T Y.1564, 2016]. EIR can be interpreted as the maximum sustained IR by which a user can exceed its CIR with some expectations that the excess traffic might be carried though the network. Figure 3.5 explains the relation between CIR, EIR and color-coding of the traffic. In addition, the recommendation defines two tests namely service configuration test that aims to validate service configurations, and service performance test to validate the quality of service over time. During these tests, the frame size can be constant, or a distribution of multiple frame sizes. Also user-defined frame sizes can be used during the configuration and performance tests. The test duration should be 15 minutes, 2 hours or 24 hours. For detailed procedures of these two tests, refer to ITU-T Y.1564, released in early 2016.

3.6. Approaches of performance evaluation and testing of IEC 61850 based communication services

Many studies were done to evaluate the performance of communication networks inside IEC 61850-based substation architectures. Several research works, that follow different approaches, assess communication functions and data models inside the IEDs. Some researches evaluate interactions of station-bay or process-bay functions related to services offered by the standard based communication network. Further researches focus on modeling and simulation to analyze and evaluate proposed devices and techniques.

Botza et al, at The University of North Carolina Charlotte, applied the IEC 61850 standard to a substation integration project that was firstly designed using traditional serial communications methods. They compared between serial communications and hardwired contacts based protective relays from one side. In the other side, results compared to IEC 61850 protection schemes using GOOSE messages communicating via Ethernet LAN. In this research project, ten IEDs were implemented, configured and networked to provide protection, monitoring, metering and control of two 138 kV lines, a 138 kV ring bus, a 12.47 kV feeder, and a transformer. They found that hardwired input/output are the slowest of the three schemes connections at a data transfer rate of 38400 bps, while serial peer-to-peer communication and GOOSE IEC 61850 protocol have about the same transmission time [Botza et al, 2008]. The authors said that, in these tests IEC 61850 protection schemes never lost command messages that were transferred via the network. They reported that the switch is still a single point of failure, and Ethernet based IEC 61850 GOOSE does not provide any acknowledgement mechanism because a relay will multicast fast GOOSE at first, and then gradually slowing to reach a heartbeat update time. The repetition after changes will invoke new messages. They concluded that "In low-voltage distribution substations, it may be feasible to only use a single, individual IEC 61850 system. However, in high-voltage transmission systems, the nondeterministic nature of IEC 61850 protocols suggest it may still be prudent to use two parallel forms of protection communications" [Botza et al, 2008].

Figure 3.6: IEDs interconnection: a) Hardwired I/O and b) Ethernet communications [Botza et al, 2008]

Ali and Thomas studied the availability of several network topologies such as star, redundant star, ring and double ring. They specified that double ring topology is the best choice for reliable communication in IEC 61850 implementations. They simulated performance of a double ring containing eight protection bays. The authors followed two scenarios: a) changing network bit rate (i.e. 10 Mbps, 100 Mbps and 1 Gbps) and b) augmenting the flow rate of transmitted data. The results obtained stated that the performance in 10 Mbps network does not comply with the requirements when the sampling rate surmounted 4800 samples/second, i.e. 80 samples per 60 Hz nominal frequency. Nevertheless, the authors reported that double ring

topology needs redundant network equipment and double network interfaces at end nodes which in result costs more than other topologies [Ali & Thomas, 2008].

Choi et al implemented a test-set to simulate IEC 61850 communications between two connected personal computers where the first PC receives sampled values, processes and measures the delay time, while the second PC includes ten logic nodes to simulate switchgear measurements. They used two logic nodes, LPHD and LLN0, and four current transformers and four logical nodes representing voltage transformers [Choi et al, 2012]. Results obtained in their work reported delay from 1.9 ms to 2.9 ms distributed over thirty messages that conforms to performance requirements as depicted by table 3.2.

Generally, the previously mentioned studies can be organized into four categories that include analytical approach, simulation approach, co-simulation approach and experimental approach. The following sections cover these approaches.

3.6.1. Analytical Approach

This approach intends to analyze communication systems and networks through mathematical models such as using probability, queueing theory or analytical algebra. In one of efforts in the analytical technique, mathematical formulas with stochastic (probabilistic) expressions were proposed to evaluate modern SAS network performance [Falahati et al, 2012]. The authors calculated the stochastic network latencies between bay control units and a remote substation switch in anti-islanding case study. They conclude that a failure in the communications network can compromise the required performance of the protection function due to loss of messages, i.e. network frames that carry equipment state or power fault event.

The classical queuing concept relies on stochastic processes and probabilistic distributions, and does not model well the periodic traffic such as sampled values in the substation automation communications [Georges et al, 2002; Skeie et al, 2006]. Cruz introduced a calculus for network delay to analyze the delay bounds and obtain buffer requirements using the maximum traffic burst size and the long-term average traffic rate [Cruz, 1991a; 1991b]. George et al conducted an analytical approach on basis of Network Calculus to identify worst-case boundaries for intra-substation communications. The basic idea of Network Calculus is to determine upper and lower traffic output bounds on both node and network level [George et al, 2013]. In addition, they built a model for two bay-level network scenarios. They developed an IEC 61850-based SAS model with OPNET modeler (i.e. event based simulation software) to examine generation of sampled raw values and event messages. In this work a hybrid approach is done aiming to compare results from simulative and analytical modelling, and to evaluate overall real-time performance of the bay LAN.

[Zhang et al, 2015] developed a traffic-flow model, including sub-models: port connections, a traffic-flow source, and a traffic-flow service of a substation communication network. They designed a traffic-flow calculation algorithm based on Network Calculus to obtain the stochastic distribution of traffic load and maximum message delay. Calculated results were compared to laboratory based substation network results measured by a network analyzer.

The mentioned studies proposed different assumptions regarding the traffic type and pattern. Nodes and network switches were modeled according to service, traffic arrival and departure rate. Table 3.4 depicts a comparison between these analytical studies. The table shows that analytical studies do not capture the influence of the network traffic rates on the operation of the protection schemes. In the other side these studies are supported by additional techniques such as simulations and laboratory setups to report the messages delay.

Table 3.4: Comparison between analytical studies of performance assessment

Comparison aspect	George et al, 2013	Zhang et al, 2015	Falahati et al, 2012
Used technique	Network Calculus	Network Calculus	Stochastic expressions
Additional technique	simulation	laboratory setup	None
The system	Two bay level networks	Substation network	Bay control unit and remote substation switch
Aim	Identify worst-case boundaries	Determine amount of traffic flow and message delay	Evaluate performance of SAS network
Node models	Yes	Yes	No
Traffic flow model	SV and events	Yes	No
Frame size and rate	Assumed	Assumed	Assumed
Additional Traffic type	SV and GOOSE without background traffic	Per port background traffic is assumed	Switches background traffic
Protection scheme behavior	No	No	No

These analytical studies provide fundamental base for understanding the IEC 61850 based communication LANs, but in a real-world scenario, additional delays will occur due to protocol stack processing, network throughput and topology changes, frames loss and processing capability of hardware devices. Even real-time communication interactions and behavior of substation protection and control events during fault events differ from human oriented application interactions.

Skeie et al focused on simulation technique and mentioned challenges regarding application of the analytical methods Network Calculus theorem and worst-case scheduling analysis for Ethernet based SAS networks. They state advantages of simulation regarding the limitations of the analytical approach as a system or protocol becomes larger or more complex. They therefore used the simulation as full-scale experiments to analyze a substation automation system in steady state delay and during transient behaviors [Skeie et al, 2006].

3.6.2. Simulation Approach

Simulation techniques are largely used for evaluating performance of computer networks, which also approved by studies involved in the industrial automation fields of research [Lee & Lee, 2002]. Many studies employed well-known software based simulation packages, e.g. event based systems simulators, to study and evaluate the performance of IEC 61850 communication services and protection and control devices behavior. Relevant simulation approaches had been performed that could be grouped into two categories:

a) Event based simulation tools such as OPNET [Xin & Duan, 2005; Sidhu & Yin, 2007; Thomas and Ali, 2010; Haffar et al, 2010], and OMNeT++ [Juarez et al, 2012], and
b) Simulation and programming language packages such as J-sim [Liang & Campbell, 2008] and Matlab with Simulink [Peirelinck et al, 2016].

3.6.2.1. Event based simulation

Many research platforms combine both event based simulation approach and programming applications. A number of these studies concentrate on IEC 61850-9-2 sampled value at process-level networks, while others studied the communication networks of intra-bay, inter-bay or station-to-bay, i.e. protection and control interactions.

Firstly, Xin and Duan designed and applied star topology with one central 100 Mbps Ethernet switch in a real time simulation environment. During this study, they simulate a file transfer, substation events and sampled values message frames, with implementation of OPNET

software libraries [Xin & Duan, 2005]. They classified the data flow into four categories according to the standard constraints (see Table 3.2) and the IEEE 802.1p. In addition, they proposed a priority-based mechanism at end-nodes (network interfaces) based on the IEC 61850 information model. The authors validated results and analyzed a case study by implementing a thin software layer with VxWorks in real-time operating system (RTOS) platform. In this work, the authors aim to classify data messages and to detect the effect of different data transmissions at the process-level; nonetheless, they omitted full implementation of the standard based message frames and modeling of the protection and control IEDs.

Skeie et al performed a full-scale detailed simulation analysis of switched Ethernet enabled substation automation system. They showed via simulation experiments almost 90% of the message latency happens within the end nodes. They proposed a priority algorithm to overcome this issue, which is implemented in a protocol stack of end station nodes [Skeie et al, 2006].

In another study, Ozansoy et al identified design constraints of a suitable real-time publisher/subscriber middleware, i.e. a layer to map networking protocols to applications in the network interface, for SAS communications [Ozansoy et al, 2007]. They added a detailed model of CORBA middleware with architectural components and discussed the processes of message registering, subscription, binding and filtering. In their paper they evaluates the proposed publisher/subscriber priority model with several simulation results using OPNET simulator, although no details are given about how the simulation has been performed or how object models have been implemented.

Sidhu and Yin [Sidhu & Yin, 2007] proposed a simplified modeling technique of several IEDs such as models of merging unit (MU), circuit breaker (CB), protection and control IEDs. They used OPNET software package to implement these models aiming to prove that Ethernet is sufficient for critical-time applications regarding SAS priority requirements. The study compares between Ethernet with and without priority tagging in a simulation environment. A case study is given in order to evaluate performance and behavior of an IEC 61850-based protection and control communications. In this work, two topologies (Star and Ring) were simulated with two bandwidth scenarios (10 Mbps and 100 Mbps). However, in their simulation platform they simplified the standard message frames, i.e. type two and four messages, providing simple implementation in order to determine End-To-End delays via estimating frame lengths and number of exchanged messages.

Thomas and Ali [Thomas and Ali, 2010] modeled network nodes with OPNET modeler according to [Sidhu & Yin, 2007], and proposed an Ethernet based topology for IEC 61850 protection and control communication networks. They concluded that Ethernet based SAS can fit time-critical performance requirement and satisfies reliability measures with fast and deterministic features.

Kanabar and Sidhu used OPNET modeler tool to continue their performance study to evaluate IEC 61850-9-2 process bus for distribution substation with a 345/230 kV transformer bay [Kanabar & Sidhu, 2011]. In this work, the authors developed algorithm to predict and compensate sampled values loss as a correction measure for delayed or missed stream of data. They simulated the substation power parameters with the help of PSCAD/EMTDC and developed MATLAB tools embedding scenarios of delayed streams obtained from OPNET simulations.

Combining both real and virtual devices is a feasible approach when some devices are not available. [Haffar et al, 2010] built a hardware in the loop (HITL) platform with OPNET Modeler. To pursue their simulation approach, they connect real network devices to simulated devices. They connect IEDScout analyzer system to the IED models using real and simulated devices with several scenarios to undertake tasks of a conformance test. In their methodology, they aim to verify conformity of an IED object model to the IEC 61850 standard object oriented

models. Hence, they tested the connection between an IED device and the simulated device's frames without reporting the metrics of the IED performance.

[Chen et al, 2013] and [Ali et al, 2014] used OPNET modeler to simulate protection and control network backups, and process-to-bay communications correspondingly. In [Chen et al, 2013], a real-time performance is studied based on theoretical analysis and OPNET simulation. In this study, IEC 61850 based node models were built for sending SV and GOOSE messages without providing details about the frames structures. Their objective was to simulate Ethernet performance with and without VLAN implementations. They reported that the real-time performance without VLAN could satisfy the communication demand. Further, they studied the effects of VLAN technology implementation and they found that the total time-delay would drop dramatically due to the decrease of the data queuing delay.

[Ali et al, 2014], used the same concept of OPNET modeler, their study is distinguished by adding a wireless LAN (WLAN) scenario with IEEE 802.11b peer-to-peer performance for the process-to-bay level network, which is based on an AP (access point) device. In their paper, they suggested several frame sizes, and reported that sampling rate or GOOSE messages generation from the instruments or IEDs must not be varied which is not the case in real protection and control applications. Furthermore, they did not consider electromagnetic interference (EMI), which is a normal case in the power systems, in their simulation scenarios.

As aforementioned, it is obvious that OPNET is the dominant simulator that has been used by many research platforms. It has the largest protocol model library among the existing simulation tools [Juárez et al, 2012]. However, other researchers developed other simulation platform based on OMNET++ being completely open-source.

Table 3.5: Comparison between some of previous studies created by event based simulation tools

Comparison aspect	**Haffar et al, 2010**	**Juárez et al, 2012**	**Kanabar & Sidhu, 2011**
Used tool	OPNET Modeler	OMNeT++ package	OPNET Modeler
Additional technique	HITL	HITL	Matlab and power simulation
The application	IED devices	Distribution substation	Transmission substation
Aim	Conformance testing of IED object models	Evaluate algorithms before implementation and performance evaluation	Performance evaluation of process bus, and algorithm for SV estimation
Node models	Protection IED	MU and Protection and Control IED	MU, protection, control and transformer IEDs
Traffic flow model	Simulated network	SV and GOOSE	SV and process bus
Frame size and rate	No	Small frames (16 to 98 bytes)	Only bit rate of SV
Additional Traffic type	No	No	Process background traffic from 250 to 350 KB/s
Protection scheme behavior	No	No	No

Finally, [Juárez et al, 2012] performed a HITL simulation accompanied by OMNeT++ modeling technique. The overall aim was to evaluate algorithms before implementing them into a real device. They purposed a simulation core that uses two processes working in a parallel manner, i.e. consisting of two elements: an event list, where the events are stored; and a scheduler that selects the next event in the event list to be executed. Their implementation also covers a real IEC 61850-communication protocol stack integrated into the simulation tool libraries.

Table 3.5 represents a comparison among some of these event based simulation efforts. These simulations did not incorporate any details about the behavior protection schemes and related functions. Kanabar and Sidhu only reported use of process level periodic traffic with rates from 250 to 350 Kbps, which is optimistic comparing with high traffic rates in modern digital process level measurements [Kanabar & Sidhu, 2011]

3.6.2.2. Simulations with programming packages

Liang and Campbell present their understanding of the IEC 61850 standard through programming of a simulation tool, and they provide suggestions on the implementation of the IEC 61850 standard based on the J-Sim as development simulator. In their research, the goal is to inspect possible security vulnerabilities in implementation of the standard protocol, and they only set related ACSI services and reporting services without strict implementation of the standard functional constraints and object models.

[Peirelinck et al, 2016] presented an SITL co-simulation platform with MATLAB/Simulink models representing two renewable sources in interaction with a communication network. Communicated devices are modeled according to the IEC 61850 GOOSE protocol. Simevents blocks and Sim Power Systems blocks are used respectively. They analyzed the effect of data communication perturbation on the decentralized reactive power control functions. Three test cases are performed in their study; starting a scenario of communications without disturbances. After that, disturbed power reference transfer, and at the end, high disturbances on the whole network and their effects on the electrical grid. This implementation omitted some GOOSE transmission details aiming to simplify the simulation, in which additional modeling effort is required to enrich the results.

Table 3.6 provides a comparison between these programming based simulation studies. Same as previous simulation studies, there are no details about behavior of protection schemes and background traffic data.

Table 3.6: Comparison between some simulation studies created by programming language packages

Comparison aspect	Liang & Campbell, 2008	Peirelinck et al, 2016
Used tool	J-Sim based on Java	Matlab
Additional tool	None	Simulink and Simevents
The application	Network topology and logical nodes	Renewable generation station
Aim	Inspect possible security vulnerabilities	Analysis the effect of data network perturbations
Node models	MMS services	Switch
Traffic flow model	Simple client/server	No
Frame size and rate	No	Not reported
Additional Traffic type	No	Assumed packet loss
Protection scheme behavior	No	Reactive power control

The traffic load of real SAS applications is not constant because of non-deterministic substation events, but in contrast to synchronized and fixed sampling value streams. Generally, the simulation approach supports substation design and testing phases. When some equipment and components are not available, this approach could replace these components by developing simulation platforms. Combining real physical devices with simulated ones would add advantages such as avoiding risks, of high voltage equipment, by simulating input and output signals and additionally the communication network.

The programming and event based simulation approach depends on the level of modelling and related assumptions. Some of these models have neglected many constraints and standardized details. For this reason, many researchers combine simulation and real hardware devices to understand the nature of protection and control events while evaluating performance of SAS communication networks.

3.6.3. Co-simulation Approach

The co-simulation approach could represent hardware-in-the-loop (HITL) or software-in-the-loop (SITL) platforms where some devices or software applications do not exist. This approach also can be adopted to test devices with simulated signals where safety of personnel could face risks of potential high voltage equipment in power process switchyard. From another point of view, it is not feasible to test devices at factory or assembly workshop without simulating real signals or communication messages. Open-source Discrete Event Simulators (DES), such as OMNET++, can be adapted for this approach, not only to enable analysis scenario of network performance, but also to design and handle HITL simulations [Juárez et al, 2012].

3.6.3.1. Hardware and software in the loop simulations

Many simulation platforms used a HITL technique in order to understand the IEC 61850 protocols and related communication services [Haffar et al, 2010; Juárez et al, 2012; Sichwart et al, 2013; Jamborsalamati et al, 2016]. In special arrangements, SITL/HITL based platforms use real hardware with simulated network to exploit powerful experimental setup with the ability to handle different simulation scenarios. In this approach, design of experiments and parameters setting could be achieved with limited availability of hardware equipment and devices. [Haffar et al, 2010] designed a test setup including a real protection IED as publisher. In this setup, they simulate a subscriber IED (controller) to receive substation events via a virtual network model designed by OPNET simulation tool.

Ingram et al. arranged a test and evaluation system that incorporates process level

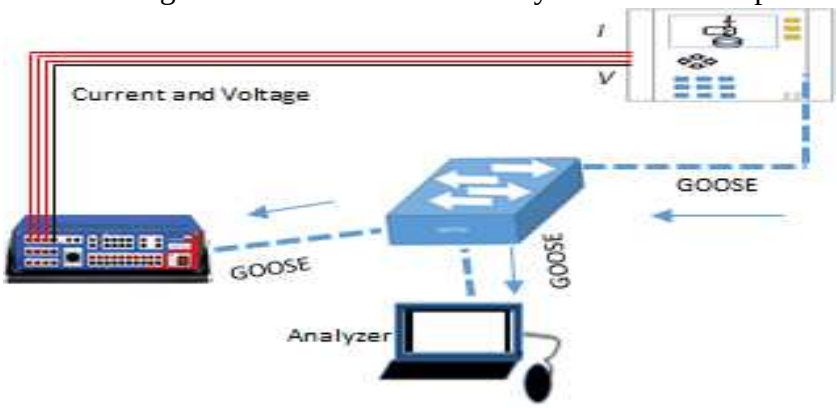


Figure 3.7: Hardware in the Loop implementation with test set (CMC 365) [adapted from Sichwart et al, 2013]

interactions with live protection relays in an HITL environment. In this work, they proposed a testbed used to validate new designs of precision time protocol (PTPv2) based protection schemes. The system application integrates a co-simulation of power transients via real time digital simulator (RTDS) and master/slave time clocks. According to the authors, accurate tests were performed to evaluate effect of SV data streams on PTP performance [Ingram et al, 2011].

In HITL setup, [Sichwart et al, 2013] implemented process level platform via adjusting a load tap changer (LTC) to control a transformer tap using the IEC 61850 standard in a

laboratory environment. They used one IED device as an LTC controller, second device as Merging Unit, and other test set (see Fig. 3.7, Omicron CMC) to supply three-phase voltage.

Two experiments were achieved, one to test tap raise and one for tap-lower in order to change the voltage level by controlling the LTC motor, i.e. located on the high voltage side. Results showed acceptable operation delays and concluded that IEC 61850 GOOSE is reliable for LTC operation.

Finally, a study incorporated real time digital simulator (RTDS), i.e. real-time hardware based simulation equipment dedicated for electric power simulations, is implemented to simulate real-time power system fault scenarios [Jamborsalamati et al, 2016]. A complete setup of the HITL platform is given. The protection scheme implements a Distributed Fault Location Isolation and Service Restoration (D-FLISR). Both GOOSE and MMS are used in this implementation. Fault such one and three phase-to-ground are simulated, and related breakers are tripped to isolate the fault based on GOOSE messages. In this research, the authors do not report any performance results considering time latency for the implementation that incorporates GOOSE-enabled algorithm.

To compare between these co-simulation works that incorporate HITL or/and SITL, table 3.7 list some of their features. The table shows that protection schemes were evaluated, but without mentioning the dynamics of current faults.

Table 3.7: Comparison between some of previous studies that incorporate co-simulation works

Comparison aspect	**Ingram et al, 2011**	**Sichwart et al, 2013**	**Jamborsalamati et al, 2016**
Power simulator	RTDS	Omicron CMC 256-6	RTDS
Communication Network	Real network	Real network	Real network
The application	Process level	Transformer controller	Distributed fault location isolation and service restoration
Aim	Evaluate PTP time precision and frame delays	Evaluate GOOSE based LTC control	Evaluate GOOSE enabled fault isolation and service restoration
Devices	Real devices	Real MU and IEDs	Real IED and cards to emulate GOOSE
Traffic flow model	Real devices and emulated bit error rates	Real devices	8 GOOSE messages
Frame size and rate	Not reported	Not reported	Flexible
Additional Traffic type	High traffic	No	No
Protection scheme behavior	Not reported	Load tap changer delay	Phase-to-ground fault (breaker tripping)

3.6.3.2. Emulation to enrich co-simulations

Emulation of substation communication protocols frames with computers, such as emulating GOOSE or SV frames by using software tools, is a useful approach to test devices response or to monitor traffic load effects. Background traffic and impairments can be handled by using the emulation technique, e.g. generating high load network traffic while testing time delay protection and control schemes. Baranov et al developed an emulation tool to generate and transmit SV messages at 80 or 256 samples per nominal power cycle, and they used a feasible approach through employing LabVIEW graphical programming environment [Baranov et al, 2013]. The authors used the commercial software SVScout to verify conformity of the generated SV frames, while Lopes et al. developed an emulation package to generate GOOSE messages. They developed this software tool (called Geese) with the open source tool (Scapy).

The authors intended to use this tool for evaluation of performance and reliability of IEC 61850 networks [Lopes et al, 2015]. In this testbed, they send parallel GOOSE frames with three virtual machines, each machine with one virtual CPU, 1024 MB of memory, and running Ubuntu 11.10 operating system. In addition, their research studied different communication topologies by using software-defined networks (SDN) accompanied by different design scenarios, i.e. different number of devices and communication switches [Lopes et al, 2015].

3.6.4. Experimental Approach

In the research and development environments, this approach often incorporates SITL and HITL platforms and testbeds. To distinguish this approach from the other mentioned approaches, real communication network or real devices construct the experimental setup. In this manner, previous works vary between using real communication network and modeled devices and equipment, simulated communication network and real devices, and both real communication network and real devices. In fact, most of these experiments target interaction between substation process and bay level devices such as protective relays (IEDs) and merging units. The previous and current works can be organized into: a) LAN based protection when intra-substation communication inside the process and /or the bay levels and b) inter-substation where WAN means used to connect devices and equipment between two substations to achieve the protection scheme such as coordination of distance and differential protection functions.

3.6.4.1. Experiments on local area network (LAN) settings

Choi et al. used two personal computers to simulate the IEC 61850 communication process and controller response. In their research platform, the intention is to measure application-to-application delivery delay requirement that should not exceed three milliseconds. This delay encounters processing latency of communicating devices, including not only delays on wire but also protocol stack processing at the application layer. Hence, they simulate a substation behavior by sending simultaneous IEC 61850-message frames from the first computer representing transformers status. The Controller on other computer receives these frames. This computer uses the C-language library WinPcap to capture data coming from the other computer. They reported that time delay is determined for thirty messages, which conforms to the standard with varied latency values (from 1.9 ms to 2.9 ms) [Choi et al, 2012].

Ali published an article about testing a protection scheme in a laboratory setup, in his work he configured three real protection IEDs. These devices are Siemens SIPROTEC 4 devices that are used in an experimental platform. The platform also incorporates the test set CMC 256 from OMICRON. The purposes are implementation and testing of IEC 61850 GOOSE based substation automation schemes. The three IEC 61850 enabled devices, i.e. having GOOSE capability and Ethernet communication port, are multifunction protection relay with synchronization, differential protection relay and distance protection relay [Ali, 2012]. He concludes that observations prove that the GOOSE affords flexible and reliable means for the reporting of substation events among protective relays for interlocking and protection schemes.

Blair et al. proposes an open source platform for prototyping objective. This platform produces the data model required for an IED to implement GOOSE and SV messaging services. The open source Eclipse Modeling Framework was used to manage the complexity of the IEC 61850 standard. The authors validated substation configuration description (SCD) files and automatically generated the required code for communication implementations. Their implementation demonstrated a case study of prototyping of a real-time, fast-acting load-shedding scheme for a low-voltage micro grid network [Blair et al, 2013].

Table 3.8: Comparison between certain previous experimental studies incorporating LAN settings

Comparison aspect	**Choi et al, 2012**	**Ali, 2012**	**Blair et al, 2013**
Power simulator	No	256 + NET-1	RTDS
Communication Network	Small switched Ethernet	Small switched Ethernet	switched Ethernet
The application	Bay controller	Distance protection	Low voltage Micro-grid system
Aim	Evaluate end-to-end delay	Evaluate end-to-end delay	Automatic generation of data models
Devices	2 controllers	3 IEDs	Embedded microcontroller
Protection scheme behavior	Not reported	Not reported	Load shedding

Table 3.8 underlines particulars facts about these studies that do not inform any details about frames rates of protection messages. Hence, no traffic flow pattern or additional background load are given, and delay times were testified according to steady state condition of the protection system and the related communications. Although these experiments provide a good details about the design of a test-setup. We will use several protection schemes within our experimental platform with real traffic and background traffic loads to evaluate performance of these schemes and to test and observe dynamics of a substation automation system (see chap 4 § 4.3).

3.6.4.2. Towards wide area network (WAN) implementations

Recently, IEC 61850 WAN applications attract researchers. These implementations concern protection schemes and interacted communication networks such as inter-substation communications to transfer GOOSE and SV message frames [Blair et al, 2014; Čelebić et al, 2016].

Blair et al, demonstrates the use of commercial off-the shelf IP/MPLS and protection IEDs to support protection functions of a power system using multiple protocols--IEEE C37.94, IEC 61850-9-2 SV, and IEC 61850-8-1 GOOSE. In this experiment, IP/MPLS routers were connected in chain topology, i.e. topology implemented without redundancy of communication, or ring topology, i.e. assuming redundant ring, as tradeoff design for the WAN communication system. The results, about delay of SV and GOOSE messages in this implementation, reported that trip times take between 23.4 ms and 24.9 ms with bandwidth utilization equals 5.4 Mbps [Blair et al, 2014].

In addition, [Čelebić et al, 2016] used alternative solutions for WAN communications (inter-substation) such as E12 channel, TDM (Time Division Multiplexing) and focused on synchronous digital hierarchy (SDH) network, hence they conclude that SDH network is the best solution. Čelebić et al implemented these WAN technologies to carry Ethernet based frames for protection, e.g. GOOSE. Moreover, they reported in their conclusion that satisfied security and dependability results are achieved in their tests. Specifically, they found that the transmission of the tele-protection commands was significantly below the limit of 10 ms constraint, and that the probability of 5 ms transmission time was less than 10^{-5} for dedicated messages, and less than 10^{-6} for GOOSE messages. Čelebić et al. do not use any power faults or protection schemes during testing of their setup.

To summarize and understand differences between these two studies table 3.9 illustrates main facts where traffic of power data into a network is not detailed; in addition, no details about protection schemes are given. Advantages of these studies that use of real communication equipment provide tangible results about propagation delays of GOOSE messages, furthermore

Blair et al determine SV delay and IEEE C37.94 teleprotection over optical fibers additionally [Blair et al, 2014].

Table 3.9: Comparison between certain previous experimental studies incorporate WAN settings

Comparison aspect	**Blair et al, 2014**	**Čelebić et al, 2016**
Power simulator	RTDS	None
WAN technology	IP/MPLS	E12 and SDH
Protection application	Differential protection over a distance	Only redundant path for GOOSE and other messages
Aim	Evaluate propagation delay of SV and GOOSE frames	Assess redundant path delay for substation WAN communications
Protocols of protection communication	SV, GOOSE and IEEE C37.94	GOOSE and dedicated protection messages
Devices	2 differential protection IEDs	2 Computers emulating IEDs
Behavior of protection scheme	Not reported	Not reported

3.7. Discussions

Several studies have followed the mentioned approaches (see § 3.6) that were used to investigate and to evaluate the performance of IEC 61850-enabled protection and control functionalities. Many of these approaches have made assumptions about networks traffic, communication protocols behavior and messages frames size and contents.

Table 3.10: A comparison between the approaches of testing and performance evaluation of IEC 61850

Comparison aspects	**Analytical**	**Simulation**	**Co-simulation**	**Experimental**
Used and additional Technique	Analysis formulas. Simulation and laboratory setup	Simulation tools. SITL and HITL co-simulation	SITL and HITL co-simulation. Real network and devices	Real devices, network and equipment. SITL and HITL co-simulation
Evaluating developed modules, e.g. IEDs	Non applicable	Partly applicable	Partly applicable	Applicable with real devices
Observing traffic flows and inspecting message frames and added background traffic	Assumed traffic flows and message frames	Simulated traffic flow and limited representation of SV and GOOSE contents and size	If real devices exist. Flexible for SV and GOOSE contents, and traffic flow	Real network traffic, detailed contents of SV, GOOSE and other protocols
Observing behavior of protection schemes	none	Assumed modules	If real devices or modules exist.	Applicability to report behavior with details
Learning efforts	Less effort	More effort	More and most	Most effort
Dynamic testing within performance evaluation	Not applicable	Partly applicable	Partly applicable	Applicable with real devices
Network behavior	Not applicable	Partly applicable	if real network exist it is applicable	Applicable with real devices

These approaches provide helpful understanding for the IEC 61850 standard parts and related technologies. However, for testing devices in order to validate a design of protection schemes and communication network in substations designers and testers shall use real or at least co-simulated equipment and devices in order to check conformity of the developed design

to the standards requirements (see § 3.4). The table (table 3.10) provide a comparison between the mentioned approaches considering the dynamic testing and performance evaluation.

3.8. Summary of operation technology requirements

IEC 61850 and teleprotection standards (early mentioned § 3.4) set constraints on protection schemes that use GOOSE messages for time-critical applications. Performance requirements are covered in the following table.

Table 3.11: A summary of performance classes according to IEC 61850

Requirements	Specification	Comments
Messages type & Performance class	1A - P2/P3	time-critical (e.g. GOOSE for tripping & intertripping)
Time constraints	Transfer time T<= 3 ms End-To-End delay <= 4 ms	ETE delay consists transfer time and fault sensing function at source relay and output acting at destination relay
ETE delay shares	Processing at source 40%, transfer message 20%, at destination 40%	From source relay, through GOOSE transfer, then destination relay
Time synchronization	SV T4 class	Synchronization accuracy is 4 µs
Ethernet Bandwidth	Fast Ethernet	10/100 Mbps (switched) due to relays network interfaces
Dependability	$P_{mc} < 10^{-3}$	Probability of missed commands
Security	$P_{uc} < 10^{-4}$	Probability of unwanted commands

3.9. Conclusion

The IEC 61850 standard combines between emerging smart grid engineering disciplines namely power protection and communication networks. These disciplines cover the substation project life cycle from requirement identification until conformance and site acceptance testing. The modern digital process and bay levels incorporated digital interfaces where Ethernet based communication networks are suggested for exchanging of measurement, status and event messages. As the standard become an industrial trend in the field of substation automation with Ethernet communications, traditional testing procedures such as point-to-point testing and electromagnetic noise injection are not applicable, hence new methodologies for exhaustive testing are required. These tests shall inspect dynamics of distributed protection functions in IEC 61850-based substation protection schemes where Ethernet based GOOSE messages are used for coordination between functions and collaborated devices.

The process and bay level communications have been modelled using simulation tools; although these models endeavored to include the real behavior of protection communication protocols that shall exist in the substation automation systems. Some assumptions were made in the previous studies suggesting fixed size of frames, limited traffic load scenarios and steady-state protection schemes. Dynamic testing is required in order to evaluate the effect of communication interaction on the coordination between logical nodes. The later are distributed among cooperated devices.

An empirical study, that uses an experimental platform to test dynamically, and to evaluate the performance of protection and control bay-level communication network, is appreciated. This platform architecture shall consist ideally of protection IEDs from different suppliers, programmable logic devices, Ethernet switches and simulated secondary power

process interfaces with flexibly adoptable parameters. In addition, the platform shall incorporate features that shall enable fault currents insertions, real protection messages, protection and control interactions, fault recording, capturing the network traffic, and analyzing it for detailed investigation of data.

To sum up, evaluating the performance of IEC 61850 communication services shall employ using designed equipment to simulate power system dynamics, and network analyzers that can capture and save the functional data flow into files for specific periods, i.e. in normal and during fault transients. This approach helps to calculate the transmission delay and other metrics. Furthermore, to verify conformity of devices and transmitted data to the IEC 61850 data services and communication protocols. In addition, inspecting time synchronization shall be used to verify precision of devices' time coordination. Moreover, assessing and using of network time protocol such as the simple network time protocol (SNTP) is important to allow precise timestamping of log events (inside the devices log files) from one side and to timestamp events within protection message (frames) from the other side.

chapter 4 : An Experimental Platform for an IEC 61850-Based Protection and Control: Safety Oriented Design

4.1. Introduction

The previous chapter highlights many research studies that evaluate the performance of the IEC 61850 based communications. Most of these studies are simulation-based that make many assumptions to determine certain performance metrics. From the behavioral viewpoint of the protection and control devices, we consider that these devices behave differently in the real substation applications regarding many predefined assumptions.

In this chapter, an experimental platform is illustrated to evaluate the process and bay levels communication interactions aiming to determine the network quality of service, and its effects on the protection and control. This platform shall satisfy time constraints and coordination to achieve safety requirements. The chapter is organized with introductory sections; section 4.2 emphasizes the work environment such as the GICS platform, and section 4.3 proposes an industrial substation (under study) with its automation system functionalities, i.e. protection schemes. Further, section 4.3 illuminates the main research tasks and objectives that incorporate analyzing the risk and proposing integrated solutions, as an overall mitigation measure, through coordination of protection schemes.

Section 4.4 presents the communication network of the substation (under study), while section 4.5 identifies the network performance metrics via describing Ethernet performance metrics and effecting factors, e.g. sources of delay. Finally, section 4.6 concludes this chapter by highlighting some parts of this chapter to help the reader identify main aims within the designed experimental work.

4.2. The GICS platform

The GICS (GreEn-ER Industrial Control Systems) platform is a part of the teaching and research activities at the GreEnER campus (Grenoble Energie Enseignement Et Recherche), i.e. academic campus belongs to the Grenoble Institute of Technology (Grenoble-INP). This industrial platform was installed in the late of 2014 for research and experimental purposes. A large part of this platform is allocated for research activities covering: substation automation, interoperability, functional safety and cybersecurity. This platform facilitates studying wide range of industrial communication protocols and networks such as PROFINET, Modbus, DNP 3.0 and IEC 61850 based communications and systems for power utility automation. The platform consists of several industrial devices and equipment (fig 4.1) including but not limited to: network equipment, computer based engineering workstations, HMI screens, protection and control devices such as PLCs, IEDs, etc. This platform involves power protection and control IEDs including transformer differential, overcurrent protection, feeder protection, and bay controllers from different suppliers, e.g. WAGO, Siemens, ABB and Schneider (fig 4.1). These devices are connected to an Ethernet LAN through network interfaces existing within embedded modules. Monitoring and configuring of these devices shall be performed via

networked applications (engineering tools). Engineering workstations are used to configure IEDs within specific tools supplied by the suppliers.

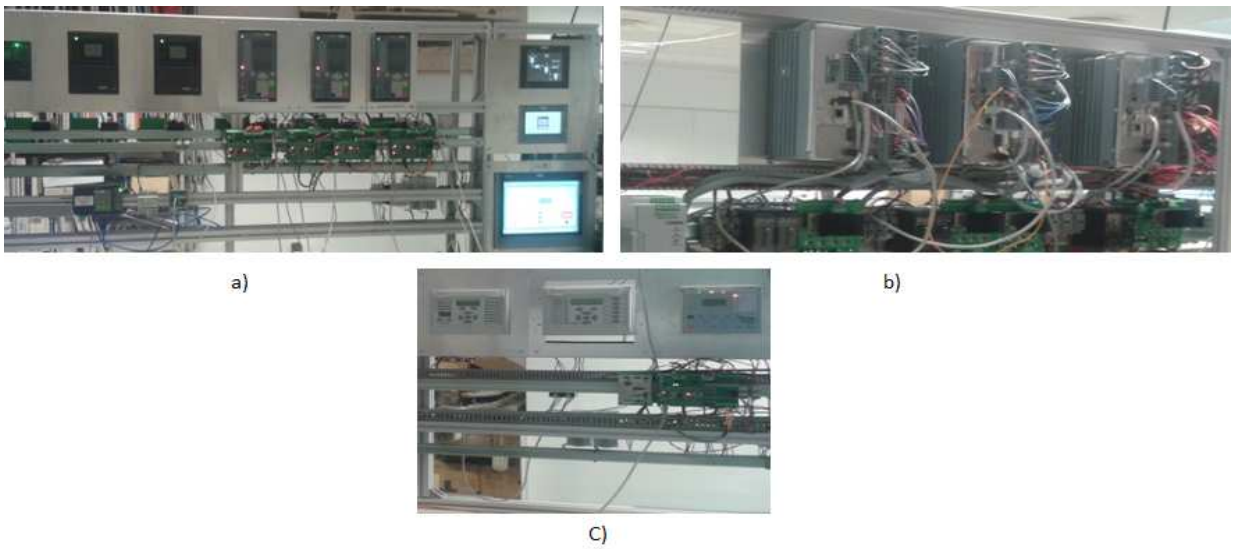


Figure 4.1: The substation automation systems: a) front panel view for IEDs and HMIs from specific supplier, b) same supplier rear view of IEDs and c) front view for IEDs from another supplier

Aiming to design a flexible research oriented test set with hardware-in-the-loop (HITL) capabilities, a developed card (see § 4.5) simulates the electrical power process current, voltage and switchyard equipment. This card feeds power measurements as secondary current transformers at the process level (switchyard). With this approach, the electrical power grid is simulated as HITL apparatus that incorporates adjacent advantages such as real-time reaction and safely alteration of power parameters. An STM32 embedded card developed with collaboration of the GIPSA-lab reproduces the grid parameters and other related signals. Indeed, this card gives real-time measurements and interacts with the corresponding IED. Additionally, software based tool developed to control this signals from networked computers, i.e. via UDP packets, to allow remote, flexible and automatic experimenting and testing.

In this research, we used the GICS platform to evaluate the effects of communication services quality on protection and control functions in an industrial substation setup. In details, our experimental setup consists in a 10/100 Mbps Ethernet LAN deployed with COTS (Component on the Shelf) switches. Engineering PCs incorporates Intel® networked interfaces that are connected to the network with twisted pair cupper cables.

4.3. The Industrial Substation and the Protection Schemes

We aim to empirically evaluate several protection schemes using the IEC 61850 based communications instead of the hardwired protection schemes, as well as understanding the interactions between these communications in the Ethernet (LAN) based protection network. A research platform conveniently allows us to implement several protection schemes with IEC 61850 enabled devices. Hence that, our work shall study the device behavior under normal traffic and perturbation, i.e. under heavy network traffic. The transfer time of the protection messages, i.e. GOOSE messages, requires low latency and low probability of loss in the

transmission and distribution substations. In addition, the standards imply specific constraints including low probability of unwanted commands such as spurious trip signals that could interrupt the supply of electrical power to designed feeders.

In modern substation communications, testing of IEDs needs careful considerations of the Ethernet LAN and the exchange of protection messages based on this LAN. In this context, the network traffic such as station-level file transfer, configuration commands and process-level/bay-level interactions would shape different traffic loads. Certain percentage of this traffic is periodic and depends on the substation events. Therefore, we aim also to analyze this traffic by adopting several scenarios imitating the real substation communication where GOOSE and SV messages exist. Moreover, to go a step forward, we inject background traffic with incremental percentage to observe the protection functions from one side and to evaluate the interaction among the network traffic from the other side. Within these scenarios, we shall measure the processing, transfer and transmission times according to the IEC 61850 framework. These experimental scenarios are used to identify:

a) Pre and post processing time (delay) at IEDs including processing time of logic solver and network stacking,
b) Transmission time between two IEDs (see Fig 3.4) that communicate using publisher/subscriber relationship and
c) Effects of periodic measurements stream, in context of IEC 61850-9-2 (SV), and other background traffic load.

To summarize, the platform performance must be evaluated according to the standard time requirements.

4.3.1. The Industrial Substation

To augment safety and dependability inside the industrial substation (under study), three protection schemes were implemented specifically a) Interlocking, b) Reverse Blocking and c) Inter-Trip. The substation has a main 50MVA transformer that convert 220 KV incoming electricity to 66 KV to supply several downstream loads at the industrial plant (Fig.4.2). A transformer (differential) IED protects the transformer bay. This IED incorporates multifunctional capabilities including: the measurement functions as depicted by the red arrow in the figure, differential protection relay, i.e. ANSI function 87 (see appendix B), in other words PDIF as per IEC 61850 LN naming convention, instantaneous and time delayed (inverse) overcurrent protection relays, i.e. ANSI 50/51, over temperature protection and inrush detection functions.

The feeders (Bay-2 to Bay-8) are protected with the feeder (overcurrent protection) IEDs that has two main functions (ANSI 50 and 51). Furthermore, the transformer and feeders IEDs control the connected circuit breakers and disconnectors as shown in the fig. 4.2 with black arrows.

The following figure (Fig 4.2) shows four bays, i.e. transformer bay; Bay-1, feeders' bays; Bay-2 and Bay-8, installed to cover protection zones. Seven feeders adjacent to Bay-1 exist in this substation, but for the following experiments, three IEDs were installed and configured (Transformer, Feeder1 and Feeder2 IEDs). Emulated MUs send SV message frames representing traffic of the feeders' measurements stream.

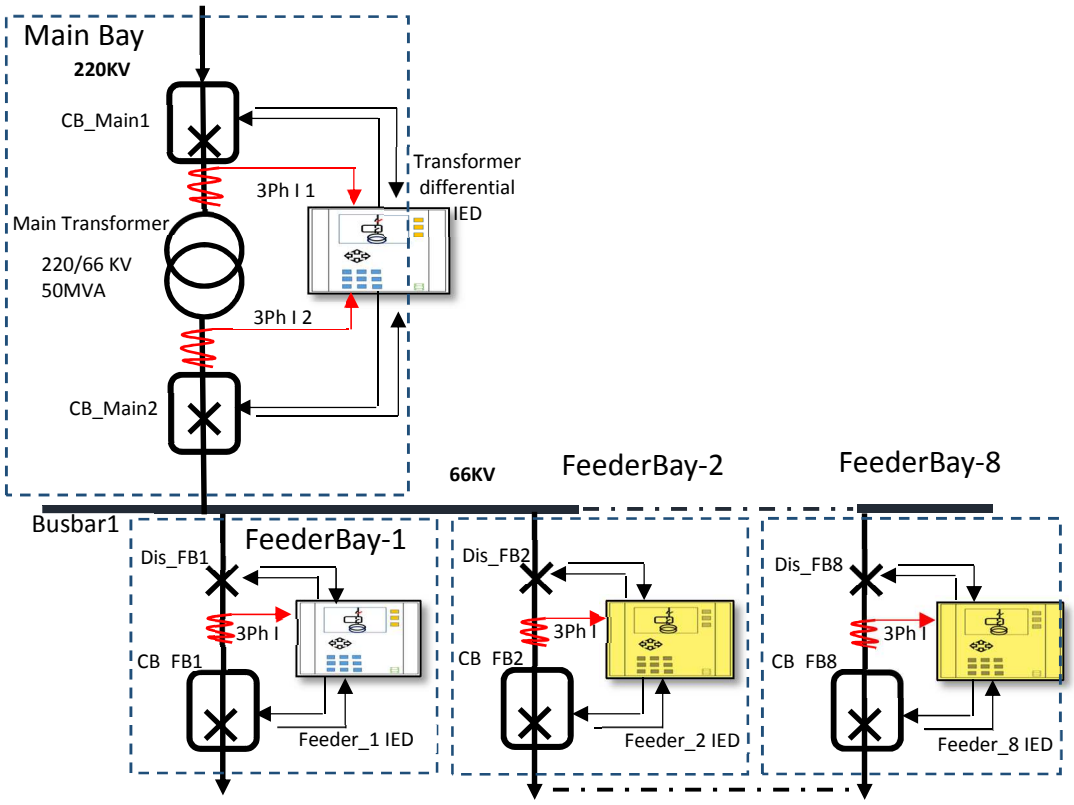


Figure 4.2: The industrial substation SLD: protective relays (IEDs) and switchyard equipment

The substation system encounters safety issues that involve some challenges that are explained in the following points:

i- Interlocking coordination is necessary when upgrades or maintenance take place. Regarding disconnectors at the feeders, i.e. Dis_1 in every feeder bay, interlocking should prohibit disconnectors of opening (interruption) of live circuits---due to technical constraints, circuit breakers can disconnect live circuits while disconnectors cannot interrupt high-voltage, because a disconnector lacks mechanism to suppress electric arcs. Thus disconnectors are used to be opened only in case of power has been interrupted by circuit breakers or other capable device [Megger, 2012]. In addition, disconnectors need maintenance every two years whereas circuit breakers need 15 years. Furthermore, similar issue will be faced, which is related to coordinating of automatic opening/closing of the switchyard equipment, or through an IED operation panel, i.e. HMI.

ii- The overcurrent protection function senses faults near the secondary side of the main transformer or downstream side causing protection function pickup, e.g. protection first stage, and resulting in a spurious trip that opens the second circuit breaker (CB2) leading to disruption of electricity supply to all downstream feeders. In this concern, speed and selectivity are needed to eliminate mis-coordination of protection operation between main transformer IED and feeders IEDs.

iii- At the downstream feeders, fail to clear a fault (trip) or circuit breaker failure (fail to trip) shall result in continuity of fault causing hazardous consequences including

harmful arc flash (see § 4.3.2) against the facility personnel and also causing equipment damage at the feeders (process-level) and the facility units, e.g. manufactory units. In this case inter-tripping shall be planed.

iv- Delayed overcurrent functions yield on slow clearance of faults (tripping) that results on long time of fault current, the consequence is high incident energy caused by arc-flash events.

4.3.2. The arc flash incident, at the process level (substation switchyard), is the main risk to be protected against

The industrial substation employs protective devices that function to de-energize the power system in the event of malfunction. The substation protection and control system operates to clear fault currents, mitigate resulted arc-flash, and blast hazards associated with fault currents, i.e. short-circuits and phase-to-phase faults. An arc-flash hazard is a dangerous condition associated with the possible release of energy caused by an electric arc [NFPA E70, 2015]. Thus, electric arc flash and shock can result in serious injury that require rapid fault clearance and isolation depending upon the fault clearance speed. This hazard threatens safety of personnel and causes equipment damage in indoor and outdoor substation systems including that one equipped with enclosed guarded installations. Therefore, the protection system shall guarantee short clearance time to avoid damage due to incident energy. The major risk here is a combination of the likelihood of occurrence and the severity of injury or damage to personnel health resulting from exposure to an arc-flash hazard [NFPA E70, 2015]. The protection schemes should be designed to compromise between equipment damage and availability of power service.

To increase service availability and to avoid equipment damage, an assessment is therefore required to identify the risk and to determine required protective measures. Selectivity and speed should be planned and implemented, e.g. blocking and intertripping. The economic consequences of the systems outage can be limited by shutting down only fault zones. The protection schemes should incorporate differential protection function and zone-selectivity interlocking (see § 4.3.1) to reduce arc-flash incident energy resulted from faults such as short-circuits or phase-to-phase fault currents [IEEE 1548-2002; NFPA E70, 2015].

The risk category is proportional to resulted incident energy from arc flash events (see table 4.1), which depends on the tripping time (Fig 4.3) of the protection device and related settings. The energy increases rapidly within sub-seconds, i.e. proportional to duration of arc flash incident and fault current [IEEE 1548-2002]. The choice of protection devices with fast tripping times reduces the incident energy and consequently the relevant costs of protection layers such as personnel protection equipment (PPE).

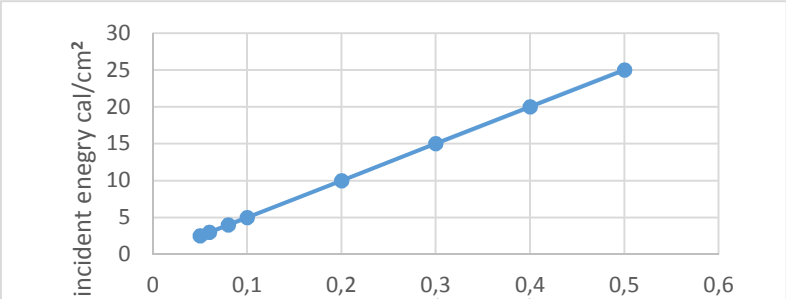


Figure 4.3: 30 kA fault current, tripping time vs arc-flash incident energy [Fuhr & Tran, 2015]

The risk of arc flash incidents is classified into five categories, starting with acceptable risk named category zero that has energy equals or less than 1.2 Cal/cm2 , whereas other categories that have an amount of arc-flash energy more than 1.2 Cal/cm2 leads to second degree burns and even worse consequences due to accompanied flash, blast and melted materials.

Table 4.1: Risk category according to arc flash incident energy [NFPA 70E, 2015]

Category	Incident energy E in (Cal/cm^2)
0	0 < E <=1.2
1	1.2 < E <=4
2	4 < E <=8
3	8 < E <=25
4	25 < E <=40
5	40<E<=100

4.3.3. The Protection Schemes

Fig 4.4 represents a subset of figure 4.2 in which fault currents, depicted at three positions, rise the previous mentioned safety issues (4.3.1 & 4.3.2). For instance, a three-phase short circuit at the feeder1 line may lead to fault currents (fault A). Feeder_1-IED will clear fault A by tripping the relevant circuit breaker (CB1 at feeder1), while both the transformer and the feeder_IEDs will sense fault B (fault at Busbar 1), e.g. same phase ground fault current, and little impedance exist between these two IEDs. The traditional overcurrent protection practice is to have main transformer IED delayed to afford feeder IED an opportunity to clear faults, though this method has its weakness as well considering faults B and C in the figure. The transformer_IED protection function becomes slower to clear faults since it is delayed in order to allow the feeder_IED to trip before. Normally delay of upstream IEDs is 200 ms referring to IEEE coordinating time delay recommendations [IEEE 242, 2001], faults will be cleared in around 300 ms including maximum estimated time of 83 ms for breaker opening. Therefore, delaying the secondary side overcurrent protection at the transformer_IED shall fulfill the required protection behavior against fault A and B by allowing feeder_IED to clear the faults. Nevertheless, this setting causes a delay around 300 ms, which is not suitable for fault C in the figure. Ground overcurrent faults will escalate into three phases resulting in more danger and allowing arcing to continue during this delay, causing high energy that exceeds 100 calories/cm^2 due to long period of arc-flash incident for 66kV (and above) enclosed

equipment with kA rated fault currents [Hill et al, 2014]. Otherwise, setting the Transformer_IED trip without intention delay limits the damage but the entire 66kV feeder will be tripped offline the consequence is loss of power supply to all feeders that may result in safety issue against the factory personnel. To overcome this issue a second stage instantaneous overcurrent protection is enabled at the Transformer_IED to trip immediately. Thus, faults at zone such as the fault at C location (or near, see Fig 4.4) shall be cleared by the second stage of the overcurrent protection function, i.e. ANSI/IEEE 50 Instantaneous overcurrent relay function. This practice allows minimum time clearance and lower energy of arc-flash incidents.

Our purpose is to implement GOOSE based protection schemes. These schemes shall be planned with the intention of solving the raised safety issues (as described in the previous paragraphs). Thus, three main protection schemes are designed namely reverse blocking, inter-tripping and interlocking. The inter-tripping scheme is closely related to the reverse blocking scheme. The following sections draw attention to these schemes with brief explanation of their roles.

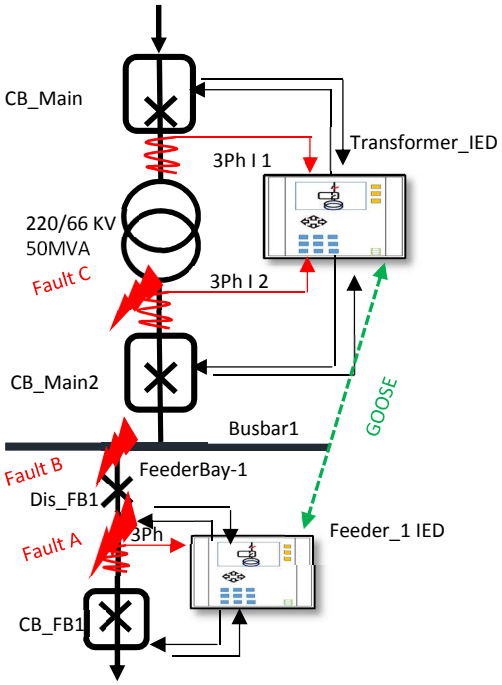


Figure 4.4: Two protective relays (IEDs) cooperate to achieve the protection scheme

4.3.3.1.The reverse blocking

This protection scheme is implemented at each feeder_IED with the purpose of sending block messages via GOOSE to the incomer zone (upstream Transformer_IED). This message blocks the overcurrent protection function of the Transformer_IED when faults exist between the CB2 at the Bay-1 and Dis_1 at the Bay-2, i.e. fault A and B (Busbar) at Fig 4.4. Further, the Feeder_1-IED senses the overcurrent fault and pickup besides publishing GOOSE messages carrying the overcurrent pickup status to block the Transformer_IED secondary side overcurrent function. The Transformer_IED subscribes

to this GOOSE, which blocks the overcurrent first stage, and waits for clearing the fault by the corresponding feeder_IED. For increasing the safety, a second stage overcurrent protection is configured. This protection function trips at very high overcurrent faults in order to clear faults in case that the feeder_IED does not trip or a breaker failure exists. The transformer_IED shall clear the fault by tripping the local CB2 in case that the fault lasts. Briefly, this scheme is used to clear faults selectively with fast speed and higher sensitivity to fault currents. IEDs at outgoing feeders (e.g. Feeder_1-IED) are responsible for blocking the incomer upstream IED (in this case Transformer_IED). A time delay therefore should be configured to allow outgoing feeders clear faults without shutting down all the substation services. In this approach, higher availability of power service will be achieved. Fig. 4.5 illustrates sequential steps to achieve this scheme.

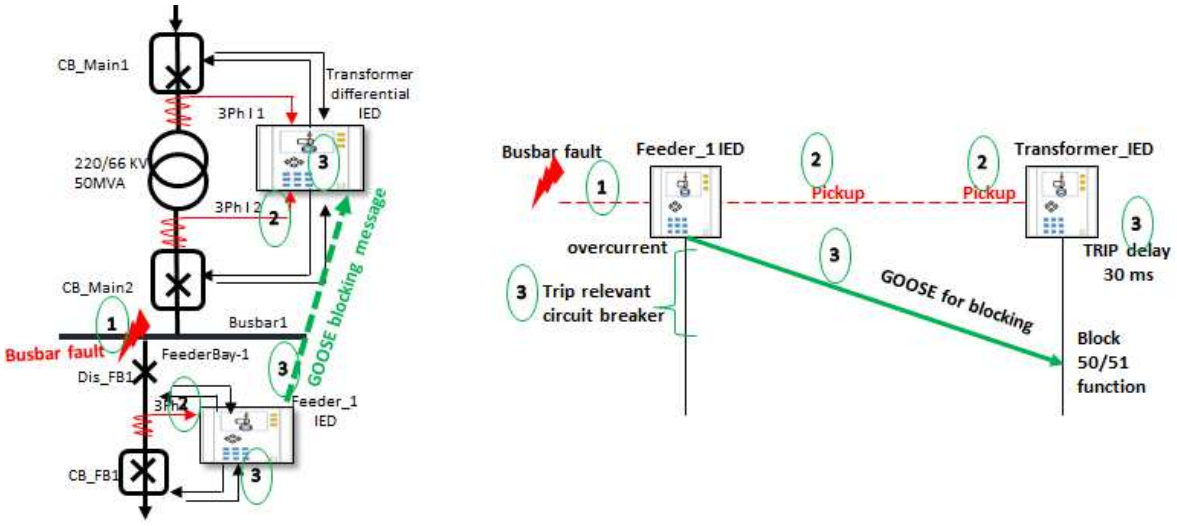


Figure 4.5: sequential diagram illustrates steps of reverse blocking scheme (Busbar failure clearing)

Fig. 4.5 shows three steps where fault current and fault sensing assumed to happen simultaneously, after that protection functions pickup, and finally Feeder_1-IED sends GOOSE messages that blocks the protection function for the secondary side of Transformer_IED. Obviously, Transformer_IED waits 30 ms, although second stage of the same protection function will operate (trip CB_Main2) if fault currents still exist to clear near faults. In addition, Feeder_1-IED is configured to send trip messages (intertripping) in case a breaker failure (CB_FB1) occurs.

4.3.3.2. The intertripping

The Feeder_1-IED shall clear local faults via tripping the local circuit breaker CB_FB1 and disconnecting the Dis_FB1. If the circuit breaker failure takes place or the fault cannot be cleared, Feeder_1-IED activates high-speed trip message (GOOSE inter-trip) to clear the circuit fault. Hence, Transformer_IED subscribes to this message and shall immediately clear this fault via tripping the local CB_Main2.

In the same manner, the Transformer_IED, after tripping the local corresponding circuit breaker, shall publish trip command to IEDs in other feeders in order to eliminate currents feedback. The other feeders' IEDs receive intertripping GOOSE messages and trip their

local circuit breakers as a reaction. Figure 4.6 depicts these steps as sequential actions where circuit breaker failure (RBRF) logical node is utilized as trigger for sending trip signal to near circuit breakers by IEDs in the related feeders.

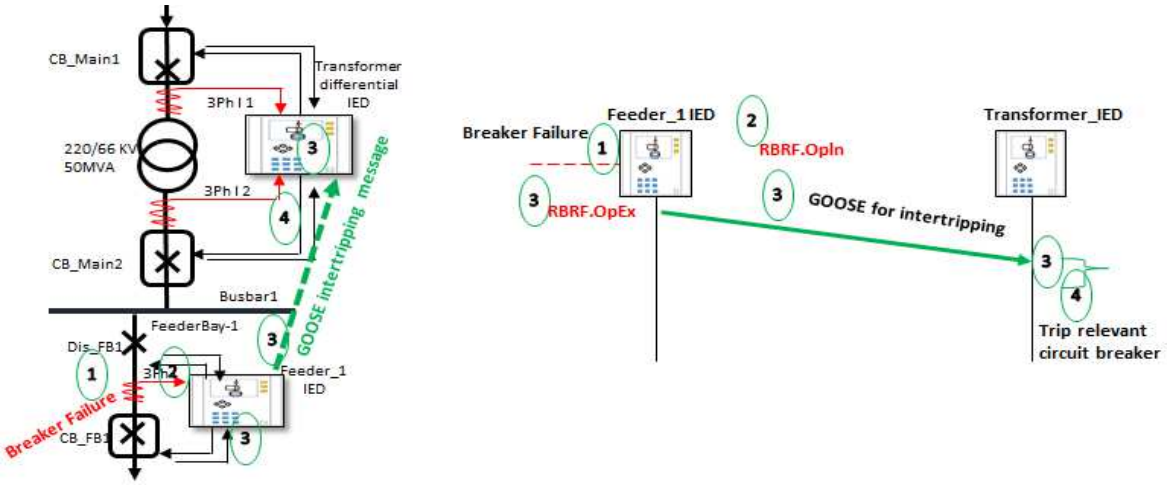


Figure 4.6: sequential diagram illustrates steps of intertripping scheme during breaker failure

4.3.3.3.The interlocking

The disconnectors (Dis_1) at the feeders' bays, e.g. feeder Bay-2, must not open/close while the electrical power flows (live circuit). In other words, circuit breakers can trip/close/reclose live circuits, i.e. designed to clear high voltage levels, in very short periods (between 20 and 83 ms) without damage for switchyard equipment. Thus, disconnectors must freely open/close when no live contacts exist. Therefore, IEDs should send status of connected switchyard. In the substation under study, Dis_1 can open/close freely when the second circuit breaker (CB2), at the Bay-1, is in open state or local circuit breaker at Bay-2 is opened. This protection scheme is identical for all feeders (every feeder bay from 2 to 8). GOOSE message is configured to deliver the status of CB2 at the Transformer_IED that publishes to all subscribed IEDs (each feeder_IED). Thus, the interlocking scheme allows only acceptable tripping and reclosing measures that fulfill these conditions. Figure 4.7 illustrates how IEDs exchange status (positions) of switchyard equipment (circuit breakers and disconnectors) in order to satisfy input of sequential logic processing at each IED.

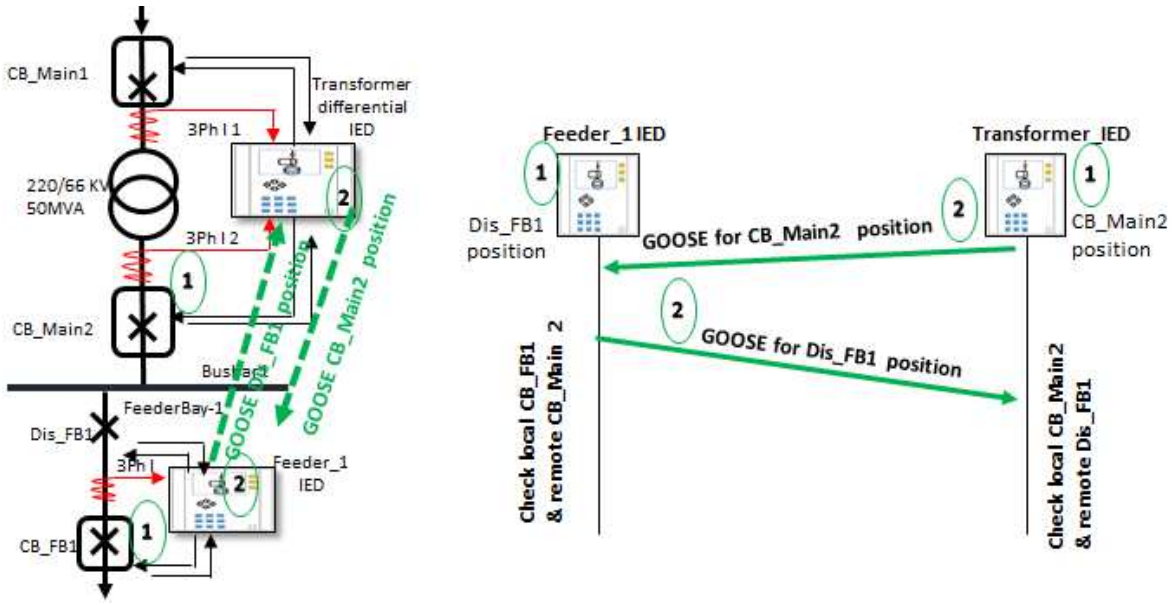


Figure 4.7: sequential diagram illustrates exchanging of switchyard data for interlocking coordination

4.3.4. Total clearance time within GOOSE based signaling

The total clearance time in case of teleprotection, i.e. existence of a communication channel, is the time for a protection relay to recognize a fault current until clearing the fault by the relevant circuit breaker associated with another relay; in the case under study intended protection relays are the transformer and the feeder IEDs. A fundamental diagram that shows a timing analysis of fault clearance is given in fig 4.8 according to IEC 60834-1 where teleprotection transmitter, telecommunication link and teleprotection receiver contribute to the transmission time of a GOOSE message.

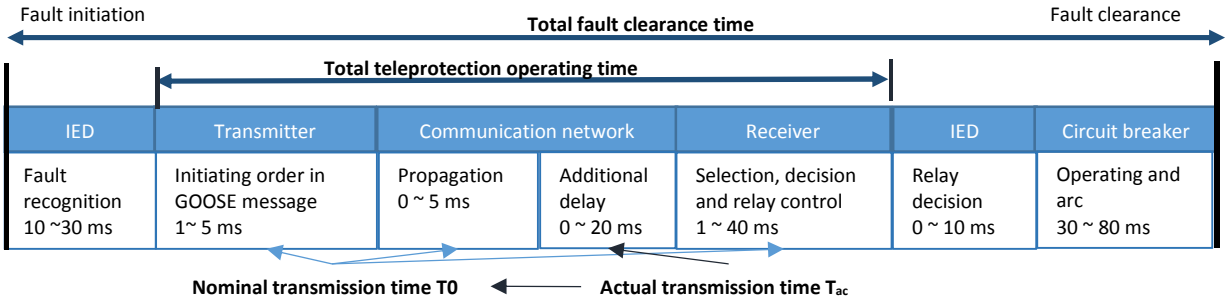


Figure 4.8: typical operating times of a protection system containing teleprotection [adopted from IEC 60834-1]

Fast clearance of switchyard faults requires real time response in substation automation applications. Protective relays collaborate in timely adjusted constraints to achieve the required protection and control functions. Total teleprotection time equals end-to-end delay between two IEDs where modern protective relays embed network interfaces within the IED module. The traffic load and network path are among factors that affect the transmission delay. The consequence of higher traffic load may cause delay and loss rate that affect straightly the transfer of GOOSE messages. Communication perturbations such as loss of GOOSE messages or inappropriate delay could cause long clearance period when power faults exist. The clearance

time depends directly on the IEDs processing time (pre and post), and the transmission time of the Ethernet network.

4.3.5. The coordination time interval

The standard IEEE 242-2001 mentions the minimum coordination time between protection relays, however it does not include the modern relays that are digital and microprocessor based devices, e.g. an IED is a digital relay. According to this standard, 200 ms (5 cycles for each) is the minimum coordination time between two digital static relays. During a configuration testing, the minimum coordination time is chosen to be 20 ms to test the interaction between two devices during the experimentation and to see the effect of signaling delay or loss.

The aims of coordination for the electrical system protection are [IEEE 242-2001]:

- To reduce the extent and duration of service outage for the duration of equipment failure, human error, or adverse natural hazard.
- To lessen damage to the system elements engaged in the failure.

4.3.6. Engineering the protection schemes

Engineering the protection schemes according to the IEC 61850 standard, needs full configuration of the connected IEDs. The configuration starts by adding and selecting the IED functionality such as: a) control logic device CTRL, b) disturbance recorder logical device DR, c) measurement logical device MEAS, and d) protection logical device PROT. Implementing the protection schemes requires integration of these functions among the IEDs. The fundamental part of the integration process depends on the events and status exchange through the GOOSE messages.

In our platform, we installed three IEDs namely Transformer_IED, Feeder1 and Feeder2 IEDs. For purposes of configuration testing, the current threshold is set to 500A and the trip delay to 20 milliseconds for the inverse delayed and instantaneous overcurrent protection functions (i.e. ANSI/IEEE 50/51 functions) at both IEDs (Feeder 1 and Feeder 2) and the instantaneous overcurrent protection at secondary side of the Transformer_IED.

Practically, different engineering software tools, such as ABB PCM 600® and Siemens scientific DIGSI 5®, are installed in the engineering workstation (Fig 4.11) to support the management of the installed IEDs. These tools manage the IEDs by means of client/server relationship, thus allowing setting network parameters, e.g. IP addresses and NTP setting. Furthermore, these tools are necessary for configuring the protection schemes (Fig 4.9 & 4.10), programming the logic and adjusting the protection and control functions.

Fig 4.9 shows the characteristics of this configuration for the Transformer_IED, the figure shows measurement points as 3 phase current (I 3ph) which is necessary for sensing the threshold overcurrent protection at relevant circuit breakers, i.e. circuit breaker 1 and 2 in the same figure.

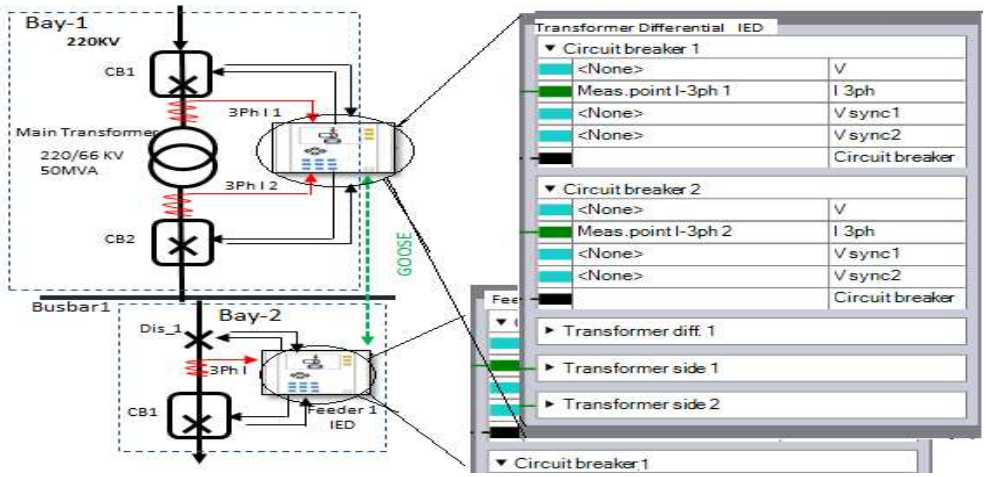


Figure 4.9: Configuring fundamental functionalities: at right side, green part represents current measurements, while black part represents circuit breaker positions

Additionally, fig 4.10 illustrates the protection function 50/51 characteristics (protection curves) for the Feeder_1-IED, which is configured with the same tools, that showing threshold parameters for the instantaneous (51 function) overcurrent is set to more than 500 A and a delayed trip time (20 ms) considering the coordination between IEDs.

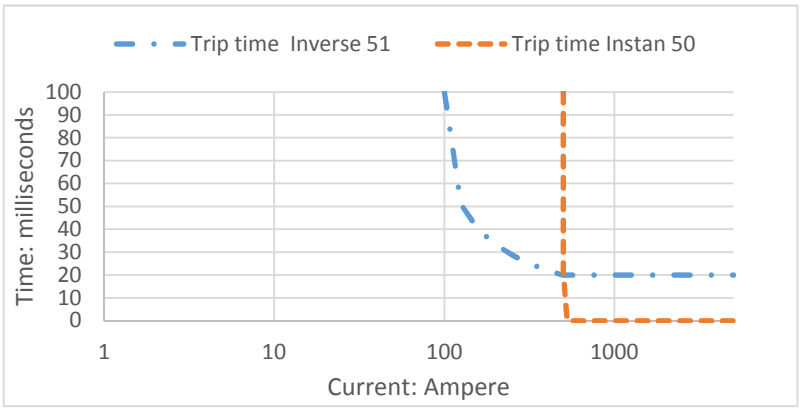


Figure 4.10: Inverse and instantaneous characteristics of the feeder_1-IED (50/51) overcurrent functions.

4.4. The Communications inside the experimental Substation

The protective relays (IEDs) communicate through a connected Ethernet switch (blue boxes in the middle of Fig 4.11). The network enables exchanging of GOOSE messages within 10/100 Mbps bandwidth limitations. The IEDs are equipped with three interfaces: one for management and configuration, the second and the third interfaces for protection and control purposes. The GOOSE messages therefore normally are sent in this setup through the second interface while the IEDs use the third interface for redundancy purpose.

The network architecture illustrates the synchronization of the devices' time through an NTP server, i.e. using an intranet access. Moreover, the industrial platform consists in more workstations and industrial devices in accordance with the real substations.

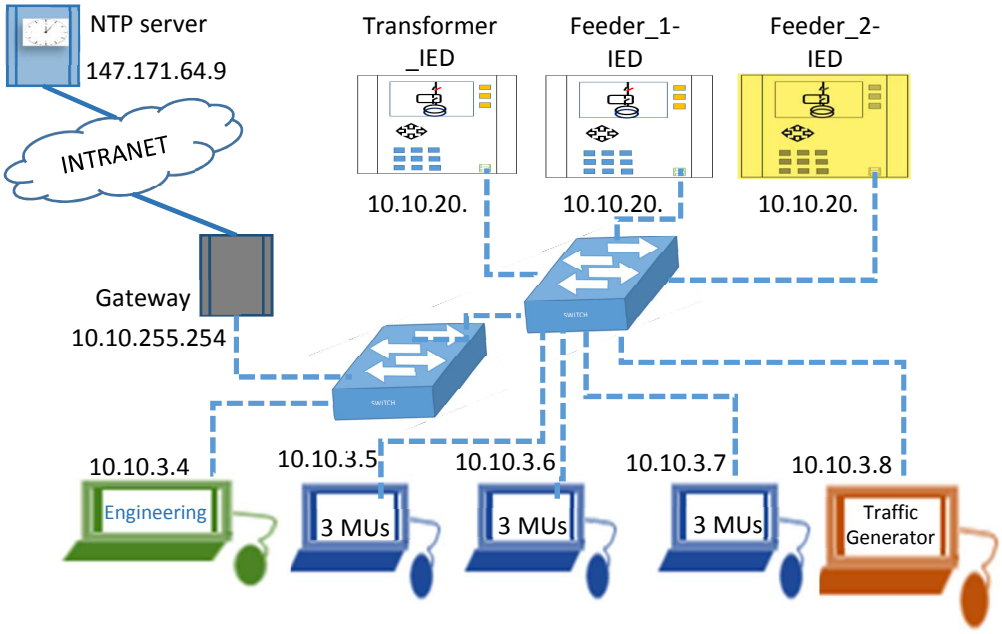


Figure 4.11: The network architecture shows the NTP server access and the switched Ethernet components

The management and the configuration of all IEDs are achieved remotely via the network management interfaces that are accessed via the engineering workstations. The architecture similarly contains four computers; three of them use virtual machines to emulate three MUs per PC (see later § 4.5.4), while the fourth generates background traffic. In this platform, implemented protection schemes incorporate three devices that publish functional GOOSE messages with a fixed frame size (table 4.2).

The main objective of this experimental study shall be testing the platform intensively with dynamic presence of both power transients and communication perturbations. Expected results will show various performances of the experimental platform which may have an impact on the specific aforementioned safety concerns as well as certain economic consequences when the system entering the operation service becomes unavailable, i.e. interruption of a delivered power from the substation platform.

Table 4.2 publishers (IEDs) and their GOOSE messaging frames attributes

Device name	**IED function**	**IP address**	**GOOSE APPID**	**Frame Size**
Transformer_IED	Transformer differential protection	10.10.20.5	1	1272 bits
Feeder_1-IED	Bay 1 overcurrent protection	10.10.20.6	2	1248 bits
			3	1288 bits
Feeder_2-IED	Bay 2 overcurrent protection	10.10.20.9	1	1269 bits

The following figure illustrates the communication of IEDs with Ethernet based GOOSE frames exchange. In the experimental platform, we implement these communications to achieve the time coordination between functions aiming to increase safety through speed and selectivity. The designated platform will contain three IEDs, 2 from the same supplier and the third from another supplier (IED with yellow color, fig 4.12).

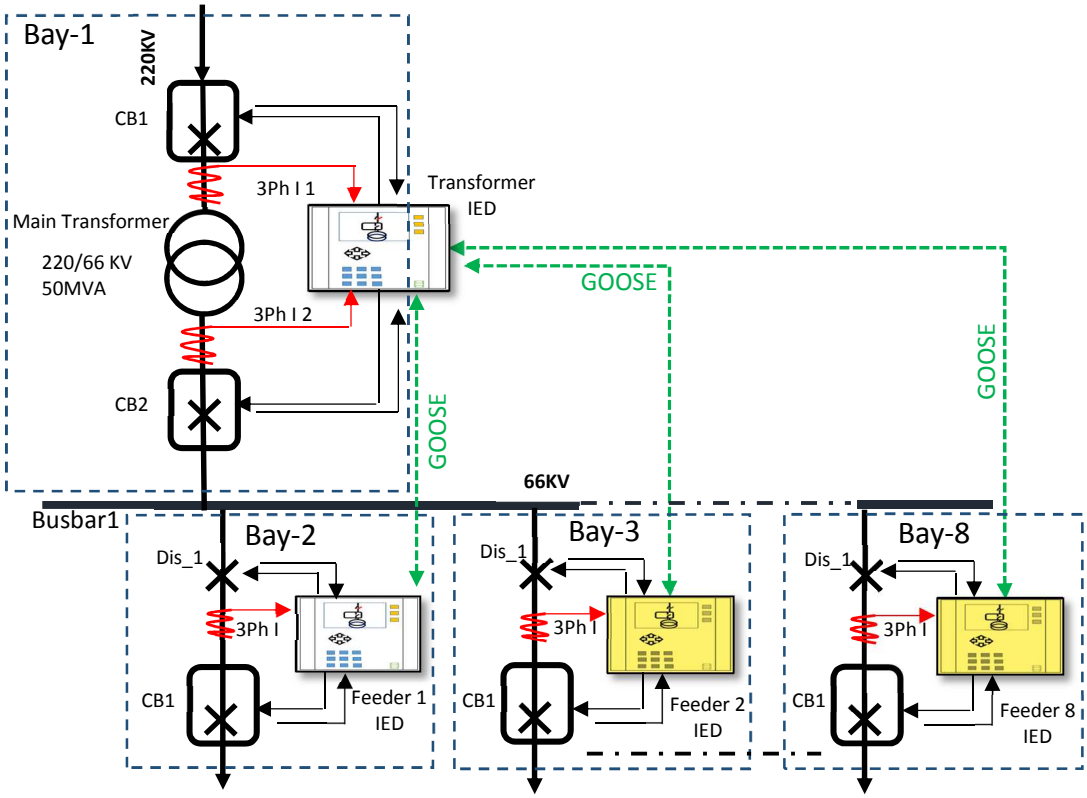


Figure 4.12: the substation under study Single line diagram with illustrations of protection communications

4.5. The Merits of the substation LAN

The previous sections clarified the Ethernet LAN concepts and helped to distinguish between the protection, control, measurement and the management LANs, beyond that the protection communications entail specific requirements such as low latency and higher availability of service. In this setup, I focus on the protection functions considering the effect of communication services on the substation functionalities. The speed of the data in the communication networks are limited by the network media such as fiber or cupper cables. Normally bits travel in the Ethernet media in two thirds of the light speed [Ruggedcom, 2008], i.e. twisted pair cables slow down the data bits because of the nature of media physics. Transfer delay is proportional to cable length (eq.4.1):

$$\delta_m = \frac{L}{\frac{2}{3}\times C} \qquad (4.1)$$

Where δ_m is the media latency, L is the cable length and C is the light speed (equals 3 x 10^8 m/s), e.g. in a 100 m cable δm equals 0.5 µs. This delay is negligible in short distances (i.e. our experiment conditions) comparing to other delay factors in the LAN communications. Technically, the transfer time of the data bits is not constant in the switched Ethernet due to the

non-deterministic nature of the switching process. In the following subsections, the reader shall realize nearly all sources of delay that may affect the transfer time of the GOOSE frames inside the substation LAN.

4.5.1. Pre and post processing

Preprocessing occur when IEDs prepare and publish GOOSE frame, while post processing such as decoding happened at the subscribers IEDs. Technically this time depends on the processing power (cycle) and the network interface stack at both publishers and subscribers. Many suppliers reveal that average processing time approximately equivalent to 0.5 ms and this time shall be within 1.4 ms limits [Meier et al, 2016]. Logically this time depends on the frame size and the processing logic, e.g. ABB states that an IED's processing capabilities can decode a GOOSE message in less than 1 ms [Starck & Kunsman, 2010].

4.5.2. Middle network boxes

Communication equipment in the modern Ethernet networks involves network devices that connect all communicated devices. That means all IEDs can communicate through these boxes such as Ethernet hubs and switches. The GOOSE protection messages transfer in the two-bottom layers of the ISO OSI standard model according to the IEC 61850. Ethernet switches are intelligent devices that forward messages to their destination by learning the MAC address from the Ethernet frame, while the hubs transmit all the messages causing high broadcast rate. The concept of shared Ethernet means that the hubs sense the carrier channel, to ensure it is not busy, and transmit the Ethernet frames. To solve frames conflict the hubs use the collision detection algorithm. While in the Ethernet switching, transmit and receive (full duplex) intend to function without collisions. The switch should keep a table of MAC addresses to speed up delivery of frames to their destinations. As described in (cf. § 3.3) switches store received frames in queue buffers and then forward them to their targets. The store and forward latency is proportional to frames size and rate. The transfer of frame in idle situation (no traffic) depends on the available Ethernet bandwidth, exactly on the throughput:

$$\delta_f = \frac{FS}{BR} \qquad (4.2)$$

Where δ_f is the frame transfer time (propagation delay), FS is the frame size, and BR is the bit rate. Theoretically, an Ethernet frame containing 1500 bytes (12000 bits) can transfer in 120 µs within 100 Mbps LAN configuration. However, Ethernet switches incorporate other latency artefacts.

4.5.2.1.The switching fabric latency

Switches are made of digital circuits (electronic integrated circuits) designed to accomplish the ingress to egress switching, e.g. input-output crossbar, and store and forward or cut-through algorithms. These circuits exhibit an operation latency termed the switching fabric delay (around 5 µs) [Ruggedcom, 2008]. During the experimental work, a Cisco 2960 switch with 48 fast Ethernet ports and 2 Gbps ports is used, which means a capacity of 13.6 Gbps

switching fabric. This switch has very short latency of switching fabric due to its switching crossbar capacity.

4.5.2.2.The queuing latency

Ethernet switches utilize memory as input buffers with the intention of lining up the ingress traffic, which has the same destination address, to avoid collisions of frames. If there is no priority policy and the buffer operates as first in first out (FIFO), the oldest frame will be forwarded firstly. When the input queue is overloaded a phenomenon of blocking, i.e. head-of-line blocking (HOL blocking), could cause higher latency and drop of frames. Thus, the blocking phenomenon causes a non-deterministic behavior of the switched Ethernet. To solve this problem use of output queues can overcome the frames dropping caused by HOL blocking but still the behavior of non-deterministic results in delay of frames delivery [Tanenbaum & Wetherall, 2011]. Buffered crossbar Ethernet switches decouple input from output buffers to handle variable length frames that enhance the queueing performance up to certain throughput level. The virtual output queues overcome the HOL blocking, nonetheless needs scheduled switch fabric to overpower the limited bandwidth of queue memory. The scheduling enables implementing of priority (class of service) to decrease delay and increases opportunity of frames delivery according to their importance (time-critical). The queuing latency in truthfulness manner depends on the buffering mechanism, i.e. buffer memory size and speed, and the percentage of the traffic load in the network. The modern switches employee advanced techniques to deal with the ingress-egress queuing delivery. These techniques allow coordinating the process of full-duplex switching. In an idle Ethernet network, we can neglect the queuing latency, but with a loaded network, the delivery time depends on the speed of queuing buffer and allocated memory. An Ethernet frame enters a queue line to take its sequence and waits until its delivery to a target egress port, e.g. assume that a 100 bytes Ethernet frame comes after 10 Ethernet frames with 100 bytes for each as average size, then this Ethernet frame will approximately wait a service time of delivering 1000 bytes. Further, the last bit of this frame leaves the egress port after time of delivering 1000 bytes and its 100 bytes in addition. For simplification, we assume that the queuing delay as Eq. 4.3:

$$\delta_Q = \delta_f + \frac{QL}{QR} \qquad (4.3)$$

Where δ_Q is the queuing latency, QL is the queue content (load) and QS is the queue service rate. If the queue already loaded with 1000 bytes and the internal queue (FIFO) service rate is 100 Mbps then a 100 bytes frame takes around 88 µs without considering the arrival time and the distribution of network load. Obviously, the queuing time is proportional to the traffic load percentage, and packets size. With higher frame rates the inter frame gap (IFG) must be considered in the calculation. The IFG size is 12 bytes that takes 0.96 µs to transfer in the 100-Mbps-LAN bandwidth.

4.5.3. The influence of GOOSE traffic

The GOOSE based protection and control utilizes the Ethernet LAN available capacity, i.e. throughput, to multicast (publish) high-speed GOOSE messages. The IEDs are responsible for publishing/subscribing mechanism. In this approach, the IEDs multicast the GOOSE messages without acknowledgment. The single technique to achieve reliability is the retransmission mechanism that shall guarantee delivering substation events. Accordingly, in this manner devices share the same network segment and exchange the substation events, e.g. switchgear status and protection events, via this mechanism assuming high probability of events delivery.

The retransmission rate depends on the event novelty, i.e. new events trigger spontaneous transmission of GOOSE message with minimum retransmission rate until gradually reaching the maximum time (heartbeat). After that, The IED regularly repeats the GOOSE message until occurring of new events or data changes. Notably GOOSE messages share same LAN segments and compete to reach the subscribers. IED suppliers are free to implement their GOOSE retransmission algorithm without any restriction considering the repetition mechanism [IEC 61850-8-1]. The standard sets specific data fields within the GOOSE message, such as the application identifier (APPID), status number (STNO) and the sequential number (SEQNO), that help the users distinguish between the repeated message frames. Ethernet switches multicast these GOOSE messages for all connected devices according to the multicast destination address.

IEDs publish high-speed GOOSE messages with predefined minimum (Min) and maximum (Max) time between events. The retransmission rate depends on these parameters. The time allowed to live (TATL) also characterizes the retransmission rate while the repetition can be distinguished with the same status no (SNO) accompanied by a counter, i.e. sequential number (SEQNO). Short time between retransmissions yields higher rates of GOOSE frames that increase the network load. The following equation demonstrates the repetition algorithm for specific supplier IEDs [Siemens AG, 2013]:

$$t_s = \begin{cases} 2^n \times t_{min}, & t_{min} < t_{max} \\ t_{max}, & t_{min} \geq t_{max} \end{cases} \qquad (4.4)$$

$$(n=0, 1, 2, 3....until\ t_{min} \geq t_{max})$$

Where t_s is the spontaneous time of GOOSE retransmission delay, t_{min} and t_{max} are the minimum and maximum repetition delay between GOOSE frames. Thus, a new substation event or data change triggers an IED logic, i.e. GOOSE Control Block (GOCB), to publish immediately a new GOOSE message with minimal retransmission (spontaneous) delay that keeps incrementing until reaching the maximum predefined retransmission interval (fig 4.13 in the following page).

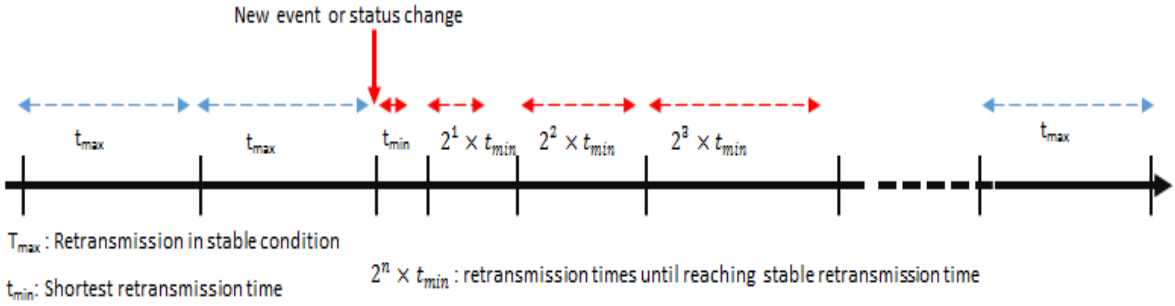


Figure 4.13: GOOSE retransmission mechanism showing minimum and maximum stable retransmission time

Within this approach, the generated GOOSE frames share a percentage of the substation (bay-level) network traffic. New events will introduce an amount of traffic containing Ethernet based GOOSE frames. This traffic utilizes the available shared Ethernet bandwidth. Assume that t_{min} and t_{max} have values of 5 ms and 1000 ms respectively, and the produced GOOSE frame has a size of 200 bytes, then 9 frames per second will be firstly generated (fig 4.14), i.e. creating 14.4 kbps (neglecting inter frame gap IFG), until reaching maximum transmission time as a result decreasing traffic to 1.6 Kbps (one frame/second).

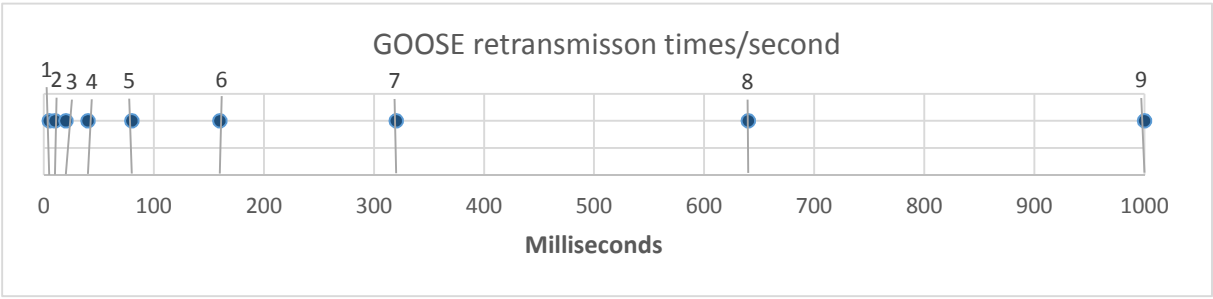


Figure 4.14: GOOSE retransmission mechanism according to Eq. 4.4 when tmin=5ms and tmax=1000ms.

4.5.4. The influence of SV traffic

Implementation of the IEC 61850 process-level technique involves use of SV publishing/subscribing mechanism. The merging unit multicasts synchronized high-speed SV data streams creating noticeable percentage of the SAS network load. One of the principle functions in the SAS is the measurement acquisitions; non-conventional instrumentation transformers (NCIT) exist in modern substation at process-level to empower the digital sampling of the voltage and current measurements. Furthermore, standalone merging units (SAMU) and integrated MU deliver these measurements according to standardized sampling rates [IEC 61850-9-2, 2003]. The protection systems compute metering quantities derived from measurements, i.e. active and reactive power [IEC 61869-9, 2016]. The merging units embed these measurements within the payload of Ethernet based sampled values (SV).

The UCA guideline [UCAIug 61850-9-2LE, 2004], known as the light edition, recommends two sampling profiles one for the protection functions while the other one for the measurements and metrics. These profiles are 80 and 256 samples per nominal cycle respectively. Accordingly, MU publishes 4000 samples/second within 50 Hz nominal frequency (in Europe) for the protection functions. Assuming that a SV frame has 115 bytes

then the produced traffic load from one MU will reach an average rate about 3.68 Mbps (Eq. 4.5). This assumption shows how one MU can consume around 3.7% of a 100 Mbps bandwidth in an Ethernet LAN.

$$L_{SV} = SR \times FS_{SV} \qquad (4.5)$$

Where LSV_{SV} is the SV load, SR is the sampling rate and FS_{SV} is the SV frame size, if the sampling profile is 80 samples per nominal cycle (50 Hz in Europe). Eq. 4.6 uses Eq. 4.5 to provide the total generated SV traffic. Publishing of SV frames by merging units will increase the generated data stream proportionally as per Fig 4.9 that demonstrates rates of SV streams according to number of merging units.

$$\sum_{i=1}^{n} L_{SV\_i} \qquad (4.6)$$

Where n denote the number of merging units sending SV message, and L_{SV_i} is the SV load of the ith MU.

4.6. Conclusion

In this chapter, an experimental testbed and platform is illustrated. This platform is a part of the GICS platform that is used to test and evaluate the process and bay levels communication interactions. The main aims are to determine the throughput profiles, network performance, quality of service, and their effect on the protection and control. Therefore, testing the real devices shall combine both implementing the protection schemes and setting the communication network.

The case study is an industrial substation with a single main transformer bay. The risk is evaluated preliminary in this chapter and proposed solutions are made to mitigate arc-flash hazard through coordinated time intervals. Some difficulties are encountered that are related to the complexity of IED configurations according to the standardized requirements such as achieving interoperability among different suppliers' devices and implementing the time coordination between devices while observing GOOSE data exchange. In fact every supplier implements IEC 61850 requirements according to their technical interpretation which enforce using their software tools to configure many parameters. The use of time synchronization needs repeatable calibration of synchronization enquiry periods. Additionally, configuring the Ethernet switches and related data needs technical efforts where the whole network traffic shall be observed through the switches.

Meanwhile, simulations will maintain the switchyard current, voltage measurements and binary input/output signals that represent power switchyard status and events as real production conditions. Mixing of simulation and real devices, for a certain level, will create a co-simulation environment. This environment helps to change in a flexible way specific parameters in order to test predefined scenarios. This approach may assess the stakeholders to perform functional and commissioning tests, and help them to achieve tasks of factory and site acceptance tests. These tests can be performed in laboratory setups within mentioned features to reduce time and efforts of development and design validation.

chapter 5 : The Experimental Scenarios: Measurements Setup, Observations and Results

5.1. Introduction

In this chapter, an illustrated experimental approach explains how to test Ethernet communication services for protection schemes and how to evaluate the performance and interactions of process/bay-levels functions. Aiming to provide flexibility for dynamic testing by means of hardware in the loop simulations, both the test set and the background traffic shaper afford repeatability of experimental conditions to check specific events. Alongside Ethernet enabled protection schemes, this approach facilitates the following steps:

a) Validating configuration setup prior to experimentations,
b) Evaluation of performance metrics during experimentations (explained in previous chapters) and
c) Verifying and validating coordination timing for distributed protection and control functions.

Therefore, mixing of simulation and real devices, for a certain level, will create a co-simulation environment. The experimental environment supports flexible changes for specific parameters in order to achieve and test designed scenarios. This approach assesses the utilities and designers to perform functional testing and commissioning tasks, and helps them to achieve tasks of factory and site acceptance tests (FAT and SAT).

This chapter details the dedicated experimental platform and explains in a detailed way the required settings and measurements setups in the introductory parts of section 5.2. Section 5.3 provides significant results of an experiment that is performed to compare hardwired signaling with GOOSE based data exchange. Emulation of SV streams and GOOSE as substation traffic loads are illustrated in section 5.4. An experimental work is used to determine the communication performance metrics during normal operation of the power system in section 5.5, whereas section 5.6 is used to achieve GOOSE reception acknowledgement in order to evaluate precisions of time synchronization service for substation events. Section 5.7 evaluates performance metrics during abnormal (transients) operation of the power system. The effects of traffic loads is mitigated through a proposed solution that uses quality of service policy and scheduling (section 5.8).

Section 5.9 discusses in overall manner the results obtained and the observation during the experimental work, while section 5.10 concludes this chapter.

5.2. An Experimental Framework

5.2.1. Preamble

The service level agreement for communication services in Ethernet based protection and control, e.g. GOOSE service, shall respect the requirements of the standards. For that, experimental tasks must follow a specific framework in order to measure performance metrics. Table 5.1 illustrates the designed experimental framework by presenting aims, methodology

and final objectives. The targeted dependability attributes (4th column in table 5.1) are correlated to requirements mentioned in the third chapter (see section 3.4). Chapter 6 will illustrate these attributes in line with well-established terminologies that are issued by the dependability community.

Table 5.1: The framework of the experimental scenarios

Measure	**How (method)**	**Why (aim)**	**Aimed dependability attribute**
Processing time	Round trip messages, timestamp in IED log files and hardwired I/O signal time	To estimate the processing time (response time including network stack) of an IED	Reliability
Delay	Difference between frames timestamp data at both (two IEDs) ends	To calculate the transfer time (delay) of GOOSE frames	Reliability and safety
Jitter	Variances of successive frames delay	To calculate SV jitter	Reliability
Loss rate	Number of published and received frames at both ends	To determine the percentage of missed commands	Reliability, availability and safety
Altering rate	Number of altered frames (payload content) and correct frames	To determine the percentage of unwanted commands	Reliability, safety and security
Time drift	Timestamp at IED log files and GOOSE events timestamp	To determine the accuracy of synchronization	Reliability

Table 5.1 is presented regarding relevant standardizations (for more details see sections 3.4 & 3.5). The presented measured metrics (performance indicators) shall satisfy the time and performance requirements, e.g. processing time, rates of frame loss and delay. Lost and delayed data frames influence missed commands probability, which have an effect on the service reliability. The unavailability of GOOSE communication service is interrelated to protection schemes unreliability. Considering the safety, degraded operation of protection schemes could cut down the protection and control function in case current faults exist. Altered frames however represent unwanted messages that reduce the security. In this chapter, the measurements shall be achieved in accordance with the objectives of this framework.

5.2.2. Experimental settings and configurations

The proposed protection schemes (see section 4.3) are prepared as prerequisite to evaluate the IEC 61850 GOOSE based protection functions in contrast to the hardwired I/O based protection. Hence, for justification that GOOSE is faster and a feasible technology, firstly a comparison between delay of hardwired I/O signaling and transfer delay of the Ethernet based signaling (GOOSE) is achieved. After that, real protection schemes and their related protection functions are configured to use GOOSE dataset parameters for exchanging the substation events. Therefore, different GOOSE application identifiers (APPID) shall be carefully configured. For that, the device under test publishes the GOOSE frames and the targeted subscriber (IED) receives these frames for further processing.

Predefined experiments (sections 5.3 and 5.4) are appointed in order to evaluate: a) the IED processing time, b) GOOSE transfer times, c) overall transmission delay in several traffic scenarios and d) related performance metrics, such as frame loss rate, etc. These metrics serve evaluating the dependability in several experimental scenarios performed later

in this chapter (see table 5.10). The effect of Ethernet network load on the protection and control functions shall be observed. Functional testing in traditional hardwired relays shall be accompanied by injection of noise signals to detect the probability of missed and unwanted commands (section 3.4.3 explains P_{mc} and P_{uc} according to IEC 60834-1). Although in the following experiments, the Ethernet based signaling (GOOSE) will encounter injection of background traffic, which is a suitable technique to observe the communication performance.

5.2.3. Validating the measurement Setup

Two computers are used to save all the captured traffic during the experimentation (fig 5.1), one computer (2NIC) with two identical network interfaces that have been synchronized to avoid drifts of timestamp data, while the second computer is a laptop used to capture the whole Ethernet traffic in the LAN of the experimental platform. The traffic load can be drawn from a mirrored port of the Ethernet switch, i.e. by configuring a switch port analyzer node (SPAN), which forwards all network frames to a configured analyzer (Fig 5.1) to measure the average traffic load.

Two passive network test access points (TAP) are installed to acquire the IEDs network traffic (see TAPs in Fig 5.1). The first TAP is at the publisher side (side a) while the second one is at the subscriber side (side b). In fact, the SPAN port is an active measurement port that incorporates some latency to copy and forward frames, while a TAP is a passive pass-through point.

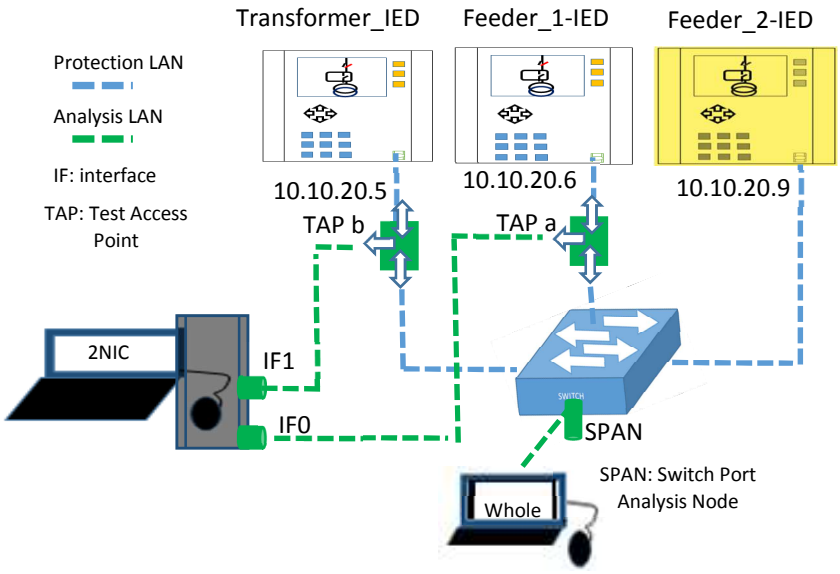


Figure 5.1: An experimental setup includes computer-based analyzers connected to TAPs and SPAN port

Transfer time (propagation time) of GOOSE messages can be calculated with this measurement setup through frames timestamp data. The same GOOSE frame (same APPID and SNO) appears in the whole traffic and in both interfaces of the 2NIC computer. Ordering the identical frames, captured at 2NIC, through the same sequential numbers

(SEQNO) facilitates extracting the timestamps to calculate the transfer time of the same GOOSE frame.

$$\delta_{GOOSE} = \tau_b - \tau_a \qquad (5.1)$$

Where δ_{GOOSE} represents the transfer time (propagation delay) of the GOOSE frame, τ_a and τ_b are timestamps at the publisher IED and the subscriber IED respectively. Eq. 5.2 calculates average transfer times for all captured frames between the publisher and the subscriber in different traffic scenarios.

$$AVG(\delta_{GOOSE\_n}) = \frac{1}{n}\sum_{i=1}^{n} \tau_{bi} - \tau_{ai} \qquad (5.2)$$

Where AVG is the average delay, n is the number of published frames and *i* is the ith frame. An algorithm uses Eq. 5.2 to compute the delay between the publisher and the subscriber for each scenario. This algorithm acquires timestamp data from GOOSE messages published by the device under test (DUT). Both interfaces (Fig 5.1) of the analyzer (2NIC) receive GOOSE frames, first and second interfaces (IF0 and IF1) capture publisher and subscriber IEDs traffic respectively. Hence, designated capture files should contain duplicated frames. Each capture and analysis session lasts 120 seconds according to predefined standardized scenarios (see section 3.5.2). Fig 5.2 shows a flowchart containing pseudocodes that explain algorithmic steps:

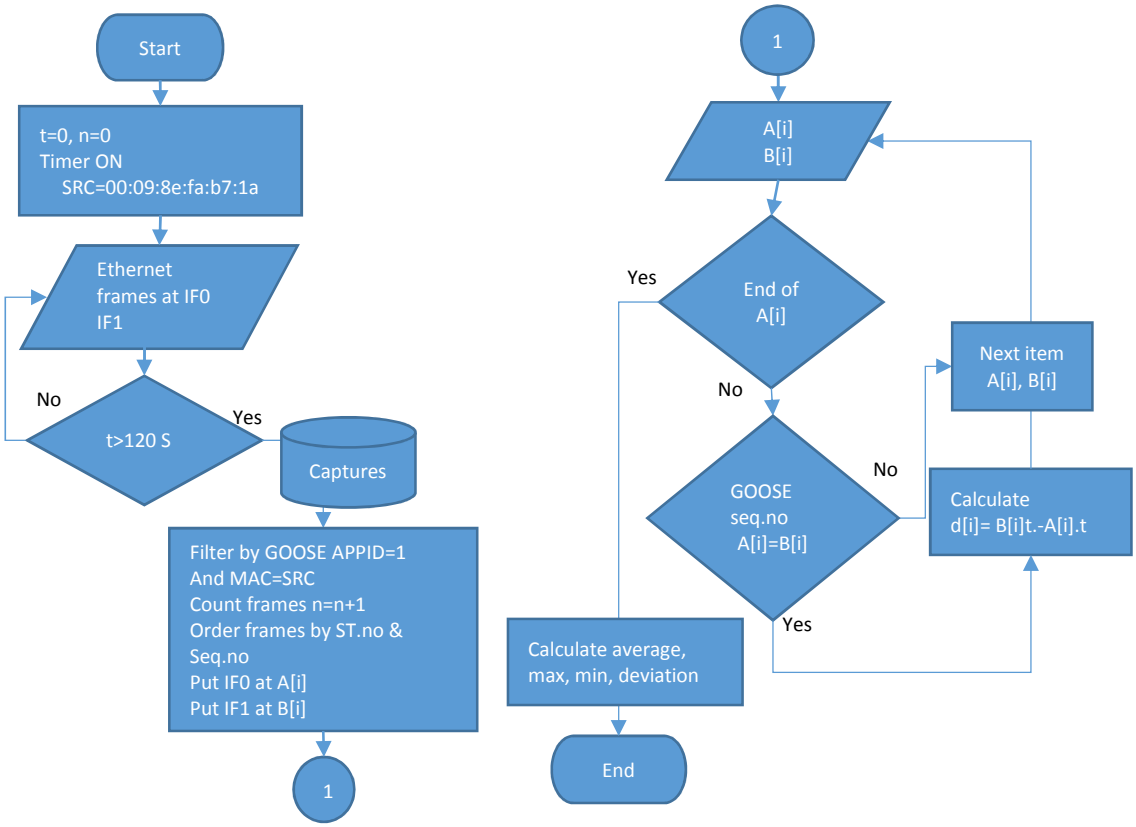


Figure 5.2: The flowchart contains pseudocode that explains the algorithm steps

5.2.4. Simulating switchyard status and process measurements

The process-level typically contains the physical power parameters and the switchyard equipment status, i.e. circuit breaker ready, open or closed. In this research steps, we used embedded cards (Input/output test-sets), which are developed in a cooperation between GIPSA-LAB and GICS team, to simulate the electrical power measurements, i.e. three phase and one neutral current signals (i_a, i_b, i_c, i_N), as well as circuit breakers and disconnectors status. The test-set (Fig 5.3a) permits adjusting parameters of secondary power signals, changing current measurements and switching of digital signals.

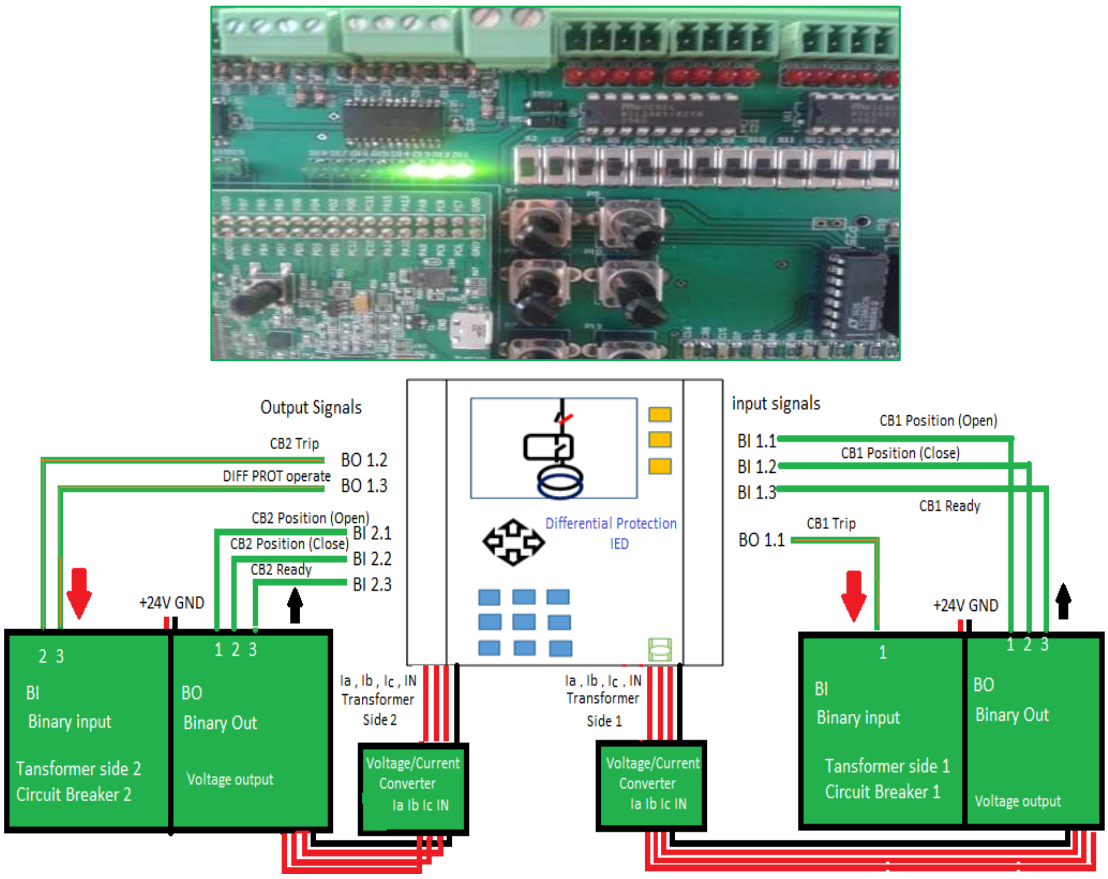


Figure 5.3: a) (top) the test set within the embedded card, STM32; top right digital output, top left digital input, and middle buttons to adjust three-phase current signals, i.e. frequency, voltage and current. b) Two test-set embedded cards simulate the switchyard I/O and the current measurements

The switching signals represent circuit breakers and disconnector during several experimental scenarios. This test-set embeds An STM32 (ST Microelectronics 32 bits) card based on the ARM® Cortex®-M processor. It offers very high performance, real-time capabilities, while maintaining flexible integration. A software tool was developed to control and interact with the card data to facilitate modifying the power current and digital I/O signals. These cards feed also a neutral phase to the corresponding IEDs. For instance, the transformer differential protection IED receives the simulated measurements, i.e. three phase and neutral current signals from two cards (Fig. 5.3a &b) representing both sides of the protected transformer.

For experimental testing, the test-set simulates the switchyard equipment status, e.g. the circuit breaker 1 and 2 (Fig 5.3b) status and positions (ready, open or closed). The IEDs

interact with the test-set card through analog and binary I/O. During experiments, adjusting these signals would be automatically (or manually) via the remote (networked) testing and simulation tool (communicated through UDP messages).

The remote manipulation of card signals enables conducting and repeating several experiments through a friendly graphical interface. In addition, script-programming enables customizing signal period and repetition profiles.

A voltage to current converter (Fig 5.3b) therefore changes the output voltage into three phase current signals. The three-phase current signals are voltage driven signals representing secondary values from 0A (Ampere) to 1A, i.e. ratio to primary value (0 A to 1000 A). In the other hand, the test-set card inputs and corresponding LEDs probe the IEDs output signals such as trip/close and protection function status.

5.3. Comparison between Ethernet and hardwired based signaling

This experiment is performed to justify feasibility of using Ethernet based signaling (exchange of data by means of communication network) in comparison to traditional hardwired input/output signaling where relay I/O connected to other relays via conventional cabling. The main comparison aspect is the relay response time where I/O and processing logic are observed to measure this time.

5.3.1. Measuring the response time of the hardwired I/O based signaling

An experimental setup is configured to measure the hardwired input/output response time for the device under test (DUT). This setup represents the traditional hardwired protection scheme. The hardwired input/output signals are tested within the transformer differential protection IED (Transformer_IED). The hardwired signaling time includes scanning the change of a connected input, processing of internal logical functions and issuing relay contact signaling (output).

An I/O test set card connects and controls both signals (see previous Fig 5.3). A logical sequential diagram of the IED under test is programmed to get digital input signal from the output of the test set and to connect this signal through a digital output to an input port of the test set. Digital gates formulate the logic of the continuous functional chart (CFC) inside the IED that employs different performance levels with customized priorities. The IED processing unit (microprocessor) executes CFC logic according to three levels that are normal trigger (low priority), interlocking (higher priority) and fast-trigger that has the highest priority. We changed the CFC priority to speed up the logic processing time. A digital oscilloscope is used to measure the response time, which traps the I/O signals and displays delta times (difference between pulses of two channels).

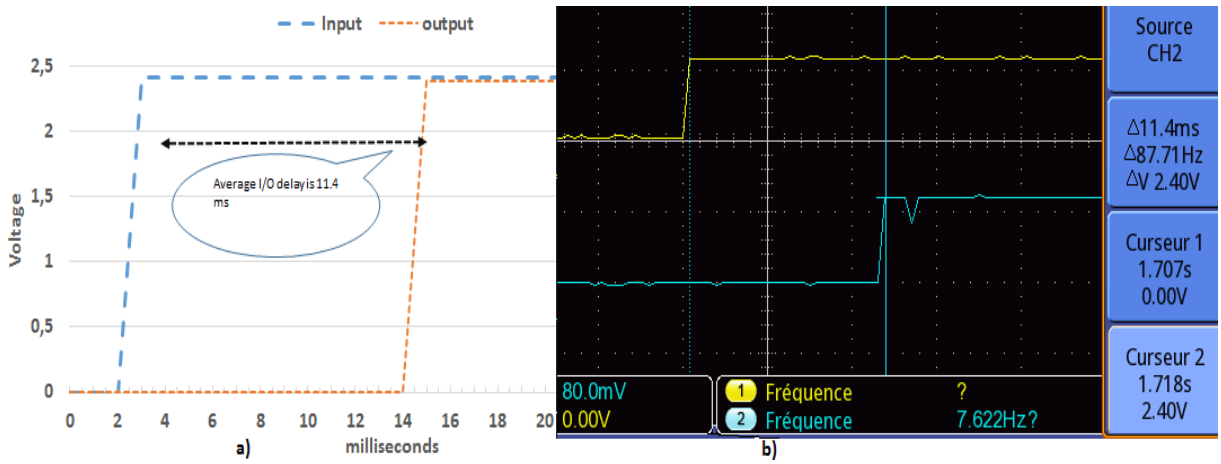


Figure 5.4: The Response time of the hardwired I/O a), Oscilloscope screenshot to measure I/O delay b)

The results obtained (Fig 5.4) indicate a delay between simulated fault current pulse-input (blue line) and the IED reaction relay-contact output (orange line). The oscilloscope is configured to save timing data during real-time trapping of these signals. These times are saved in text files during repeated experiments. Repeated measurements give an average value of 11.4 ms as an overall response time. This delay is higher than GOOSE based protection signaling (see 5.3.2) because of: a) scanning time of digital inputs, b) CFC logic processing time, and c) output contact time of the digital relay, which is a fast trip contact in this experiment setup. In addition, the hardwired input/output connections take large footprint compared to GOOSE enabled event signaling where only one network cable can carry several GOOSE messages (containing large number of I/O data) passing through an Ethernet LAN.

5.3.2. Measuring the response time of the Ethernet based signaling

We used the Internet Control Message protocol (ICMP) requests to get response from the IED under-test (DUT). A computer equipped with an analyzer tool captures the request and replay messages. The ICMP request/response timestamps and sequential numbers were compared with the analyzer-enabled timestamps. With this active technique, several size ping-pong messages help to determining the time of packets processing, i.e. encoding/decoding and transmit/receive (TX/RX) stacking, at the Transformer_IED. Different ICMP request payloads are used to get the round trip time (RTT), which is used to estimate the time of packet stacking and processing at the Transformer_IED.

The experiment setup contains direct connection to the targeted IED, i.e. without communication box in the middle. A computer uses high precision ping utility (hrPing version 5.00) that is configured to send ICMP messages with several payload size starting by 100 B (bytes), incrementing by 100 B, until reaching 1000 B. Each ICMP message stream (iteration) continues 100 times. In this setup, we assume that the IED response time, neglecting the wire transfer time, would be half of the round trip time, and we captured every ICMP request and response for comparison and detailed analysis. Hence that, the processing time includes further encapsulation and stacking of frames that provide approximate figure about the GOOSE based signaling (IED response time):

$$\delta_{proc} = \frac{RTT}{2} \qquad (5.3)$$

Where δ_{proc} is the processing delay including stacking time (IED response time) and RTT is the round trip time. Fig. 5.5 illustrates statistical representation for normal standard deviation of 1000 response times, 100 requests per 10 different payload sizes, for all ICMP request/response iterations. The blue, orange and gray colored bars show average, maximum and minimum response times respectively, whereas the black bar shows the standard deviation. Obviously average processing delay is less than 1.5 ms, although maximum processing delay is just below 4.5 ms with 900 bytes payload request.

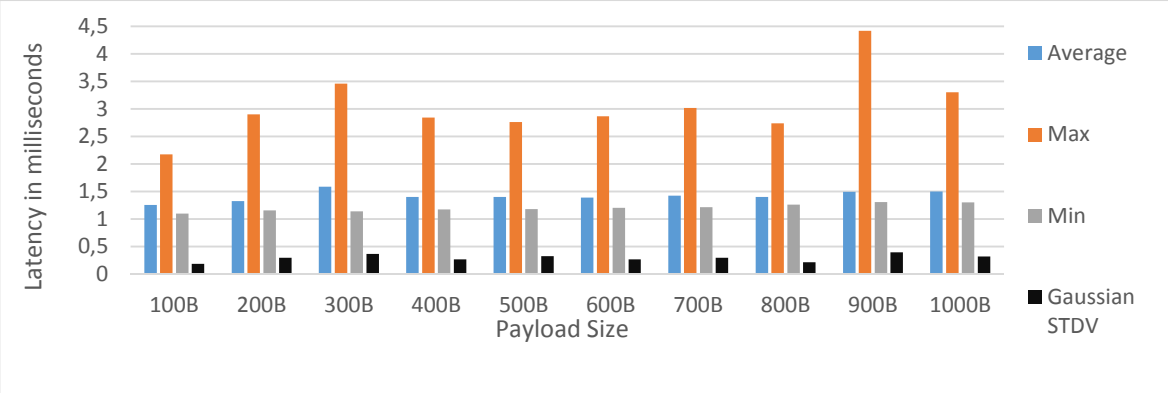


Figure 5.5: Statistical representation of the transformer IED response time with different payloads.

Clearly, the minimum response time is not less than 1.1 ms achieved by 100B payload. The IEC 61850 standard requirements limit the IED processing time to 40% of the required delay, which means 1.2 ms of 3 ms allocated for total transfer time. The measurement provide an average time more than this value. Table 5.2 shows detailed statistical figures about the response time considering several payload messages. ICMP request, with 900 bytes payload, reached a worst response time with a maximum delay just above 4.42 ms (table 5.2). The results shows a nonlinear relation between payload size and response where 300 bytes packets takes longer response time than 400 bytes packets.

Table 5.2 statistical data about the IED response time in milliseconds

Payload size (Bytes)	**Average**	**Max**	**Min**	**Standard deviation**
100	1,254	2,172	1,101	0,184
200	1,326	2,905	1,154	0,293
300	1,588	3,459	1,140	0,362
400	1,400	2,847	1,176	0,266
500	1,398	2,760	1,177	0,322
600	1,389	2,870	1,204	0,265
700	1,425	3,020	1,213	0,294
800	1,398	2,739	1,259	0,212
900	1,495	4,421	1,306	0,393
1000	1,499	3,302	1,299	0,318
Total data	**Average**	**Max**	**Min**	**Standard deviation**
	1,4	4,4	1,1	0,309

In the following figure, the distribution frequency of values representing the IED processing latency is shown in the following histogram (fig 5.6), which obviously provides frequent values of processing time.

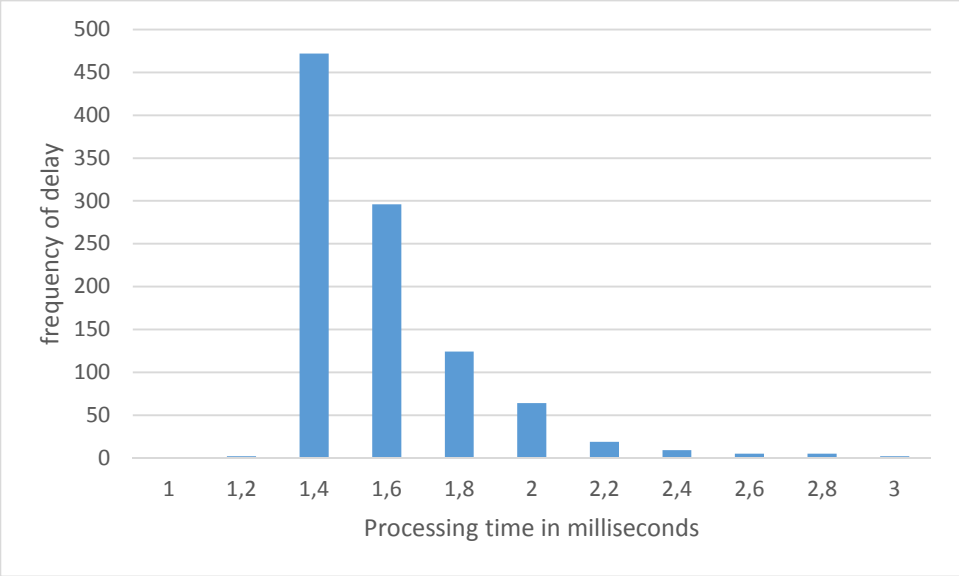


Figure 5.6: frequency of processing latency is illustrated by distribution histogram

Figure 5.7 shows all response time (one-way), ordered by payload size. The average response time is just above 1.4 ms regarding all payload requests. This value provides an estimation for the IED processing time considering GOOSE frames where the average size of GOOSE messages technically is about 300 bytes. Later the reader will observe that a generated GOOSE based protection and control messages are just above 200 bytes. In addition, the figure shows a maximum response time, about 4.4 ms, and increasing response behavior around ICMP requests within 600 bytes. In this experiment, the IED response for the requests is not constant which means that the processing time shall be around the average response time, but some values are above as clearly shown by the figure.

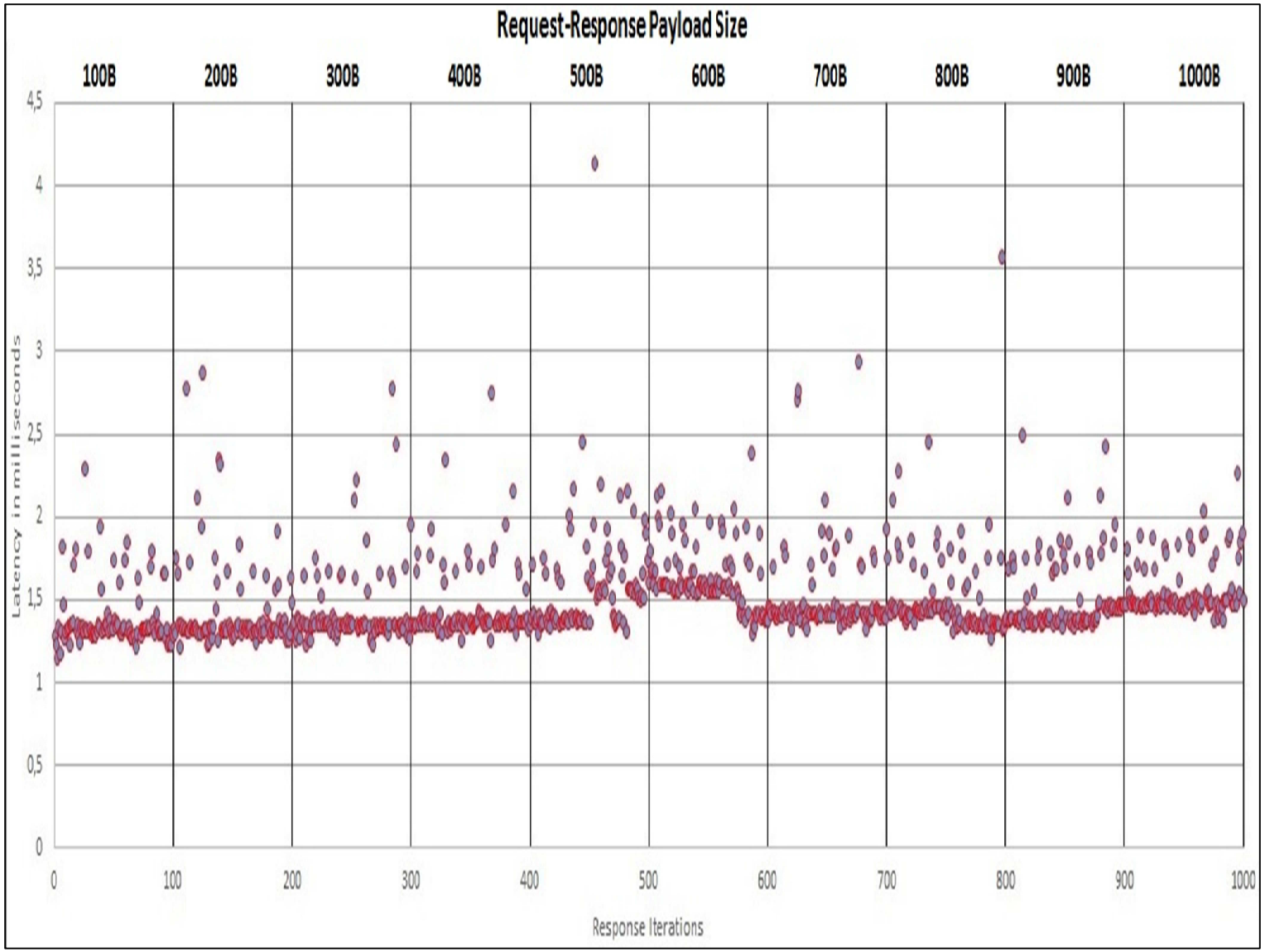


Figure 5.7: Different payload messages: the average response time around 1.42 ms

5.4. Emulation to generate SV streams and background traffic

The emulation in this context is the ability to use an application program to generate data frames according to specific standardized structures. In this section, GOOSE and SV data frames are generated with computers according to the standard and related guidelines [IEC 61850-8-1; IEC 61850-9-2LE]. The aim of this traffic is to simulate a real substation communication in a production environment where several network protocols and power communication protocols exist. Frame sizes are generated according to contemporary standardized recommendations dedicated for Ethernet activation testing [ITU-Y 1564, 2016].

5.4.1. Generating traffic of SV streams

At the beginning, an MU emulator is used to generate (publish) periodic sampled values frames according to the light edition guideline [IEC 61850-9-2LE, 2004] that recommends a sampling rate of 80 samples per nominal cycle for the protection profile. The Omicron SVScout® software tool (Fig 5.8) is used to validate SV data.

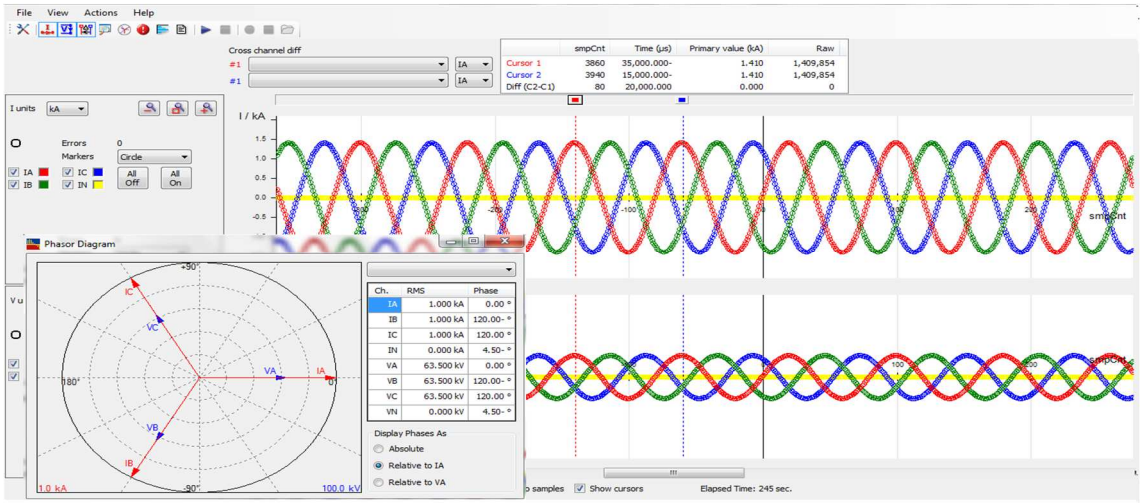


Figure 5.8: Verifying power data inside the generated sampled values

The tool subscribes to SV stream to monitor and display SV measurements (digital data), and used therefore to verify the SV streams delay and delay variation (jitter) metrics in a real-time with normal network traffic, then with additional small background traffic. The tool is used to verify three-phase (colored waveform in fig 5.8) current values (i.e. i_a, i_b and i_c currents) and phase degree (angle) between these phases (phasor diagram at bottom left of fig 5.8). After that, the emulators publish SV streams in order to observe the effects of generated traffic on the transfer of functional GOOSE messages, and to measure the SV messages qualities such as delay, jitter and loss rate. Three DELL® PCs, equipped with virtual machines software, are used consequently adding 2, 3, 6, 9 SV streams. Table 5.3 illustrates the SV publishing setup environment where three PCs generate three simultaneous streams of SV frames. The published SV streams shape a maximum traffic with 33.12 Mbps as an average load. These published SV streams should have attributes (data fields) as depicted by the header row of table 5.3 in which application identifier

(APPID) and sampled value identifier (SV ID) follow the standardized guideline IEC 61850-9-2LE.

Table 5.3: The attributes of emulated MU with the generated SV data

Size: 920 bits, frame rate: 4000 frames/second, APPID: 0x4000, sample counter: 0 to...3999 Destination MAC address: 01:0c:cd:04:00:00		
PC name	**IP address**	**SV ID**
GICS11	10.10.3.5	GICSMU0001
		GICSMU0002
		GICSMU0003
GICS12	10.10.3.6	GICSMU0004
		GICSMU0005
		GICSMU0006
GICS13	10.10.3.7	GICSMU0007
		GICSMU0008
		GICSMU0009

5.4.2. Shaping GOOSE messages as Background traffic

Ethernet frame generator, open source software (PacKETH 1.8.1), is used to shape a background traffic. This traffic is made of Ethernet based GOOSE messages with a fixed frame size equals 8000 bits. A changeable frame rate adds a certain percentage of traffic. To increase the generated traffic the time between frames (frame time) decreases. The generated traffic is validated by capturing the whole network load to know the augmented percentage (ramp) of GOOSE stream data. Table 5.4 shows the attributes of the generated background traffic. To insure consistency the GOOSE frame must include the mentioned attributes (fields of data) in the header of table 5.4 (see appendix A for more explanations).

Table 5.4: The attributes of the generated GOOSE frames data as background traffic load

Size: 8000 bits, APPID: 1, Time Allowed To Live: 3000, Test: false, Configuration Revision: 1, Needs Commissioning: false. Source MAC address: 00:09:8E:FA:B7:1D, Destination MAC address: 01:0C:CD:01:00:05				
Scenarios	**Additional %**	**Mbps**	**Frame rate Frames/second**	**Time between frames (µs)**
1	10%	10	1250	800
2	20%	20	2500	400
3	30%	30	3750	266,6
4	40%	40	5000	200
5	50%	50	6250	160
6	60%	60	7500	133,3
7	70%	70	8750	114,3
8	80%	80	10000	100

We used Eq. 5.4 and Eq. 5.5 to deduce the frequency (time between frames).

$$FR = \frac{BR_{target}}{FS} \qquad (5.4)$$

Where FR is the frame rate in bits/s, BR_{target} is the target bit rate per second (traffic load) and FS is the frame size (bits). The time between frames t_{frame} , is the reciprocal of the FR.

$$t_{frame} = \frac{1}{FR} \qquad (5.5)$$

Through employing several frame rates, i.e. time between frames (table 5.4), several scenarios augment network traffic rates until passing available Ethernet bandwidths, i.e. SV frames and background traffic (emulated GOOSE frames) exceeds the theoretical 100Mbps bandwidth. Table 5.5 and Fig. 5.8 compare between the calculated and the resulted observed Ethernet traffic load. The normal scenario (intrinsic) represents the functional GOOSE frames, i.e. generated by the substation IEDs, while three, six and nine merging units (3MU, 6MU and 9MU) represent the added sampled values, and the additional percentage of generated traffic to SV streams.

Table 5.5: The calculated vs the observed Ethernet traffic load

Scenarios	**Additional traffic type**	**Calculated traffic (average Mbps) considering a non-limited bandwidth (no saturation)**	**Observed traffic (average Mbps) considering the actual limited bandwidth**
Normal	(only GOOSE)	0,002	0,479
3MU	Adding Sampled Value	11,040	11,604
6MU	Adding Sampled Value	22,080	22,258
9MU	Adding Sampled Value	33,120	33,777
additional 10%	Adding GOOSE	43,120	43,805
additional 20%	Adding GOOSE	53,120	53,472
additional 30%	Adding GOOSE	63,120	63,497
additional 40%	Adding GOOSE	73,120	73,432
additional 50%	Adding GOOSE	83,120	82,621
additional 60%	Adding GOOSE	93,120	91,949
additional 70%	Adding GOOSE	103,120	93,576
additional 80%	Adding GOOSE	113,120	93,777

These scenarios of additional traffic represents 10, 20, 40, 60 and 80 Mbps of background (fake GOOSE frames) that are used to emulate the substation network traffic. This traffic may influence the protection and control functions as well as the IEDs behavior. In the other hand, Fig. 5.8 illustrates that the Ethernet switch, which has a maximum forwarding capacity of 6.8 Gbps and 32MB (256Mbits) shared buffer, starts dropping frames of the network traffic when the load passes just above 82% of the Ethernet bandwidth. Our objective in these circumstances is to observe the real GOOSE frames, i.e. functional messages, and their transfer time to find the effect of the SV traffic and the background imitated GOOSE messages on the delay of the functional GOOSE messages.

5.5. The observations

The duration of experiments scenarios lasts 120 seconds for each. Both analyzers capture the data frames (see section 5.1.3). For the first scenario, observations indicate that the observed traffic is bigger than the calculated load due to the existence of other real industrial protocols in the GICS platform. In the other hand, Fig. 5.9 illustrates that the Ethernet switch started dropping frames of the injected traffic when the average network load (observed) passes just above 80% of the Ethernet bandwidth.

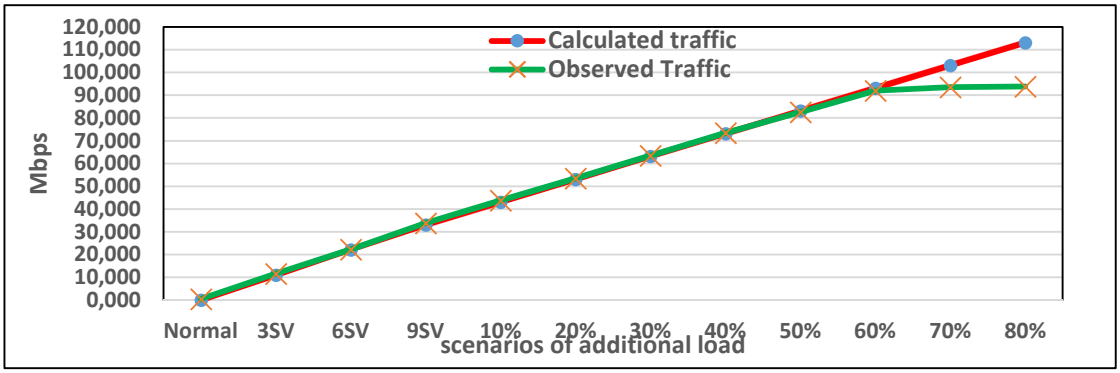


Figure 5.9: The calculated (with unlimited bandwidth) vs the observed (with the actual limited bandwidth) Ethernet traffic load

5.5.1. Published GOOSE frames

The Ethernet service is observed; GOOSE frames published by the Transformer_IED and their transfer time (Fig 5.10) to find the effect of the SV traffic and the background fake GOOSE messages on the delay of the functional messages. Results of all scenarios do not show any frame loss of functional GOOSE messages. Nevertheless, the observed maximum delay of the GOOSE propagation (transit) time increased when the average Ethernet network traffic passes just above 73% (73Mbps) with 3.3 milliseconds value.

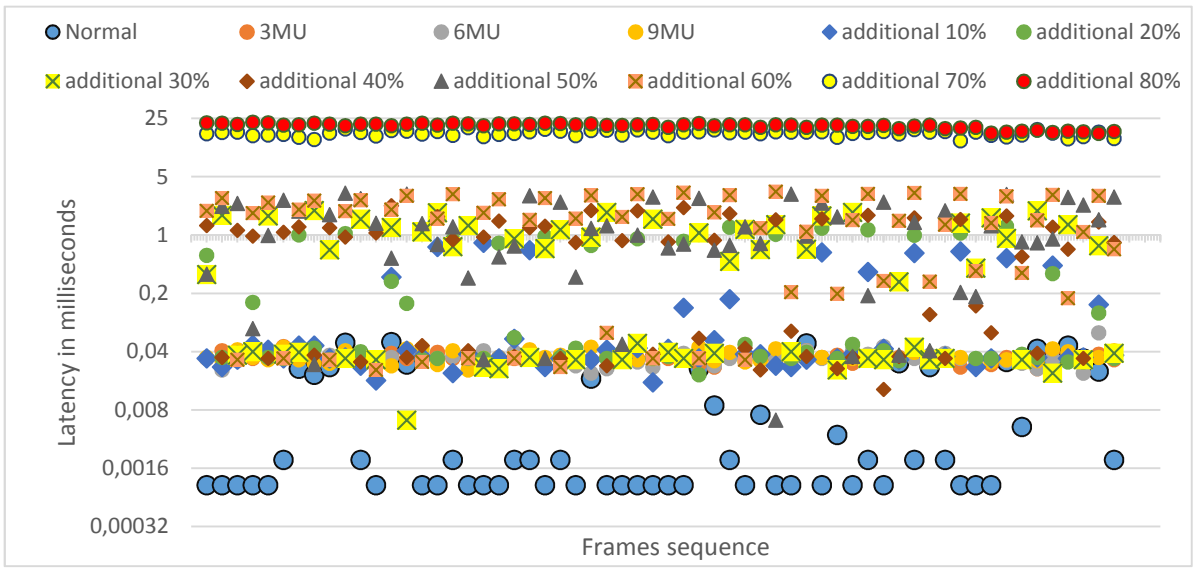


Figure 5.10: Delay of the GOOSE frames with various Ethernet load profiles

The delay dramatically reaches 20.4 milliseconds as average value within the observed 93 Mbps network load (Fig 5.10 and 5.11). Figure 5.10 illustrates GOOSE transfer (propagation t_b) times where 60 frames are transferred during 120 seconds per each traffic load. From the figure, it is clear that the GOOSE transfer delay passes 600 microseconds with 30% of additional load (just above 60 Mbps), which does not satisfy the standard requirements that insist on allocated 20% of 3 ms for total transfer (from an IED, t_a, to another IED, t_c) time. We can learn from the figure that traffic loads with more than 60 Mbps will cause higher GOOSE delays. This phenomenon provide us an obvious thought about the GOOSE propagation delay where a LAN network with a traffic load up to 40 Mbps (additional 10% to 9 MUs) can guarantee time requirements of P2/P3 performance classes (see table 3.2).

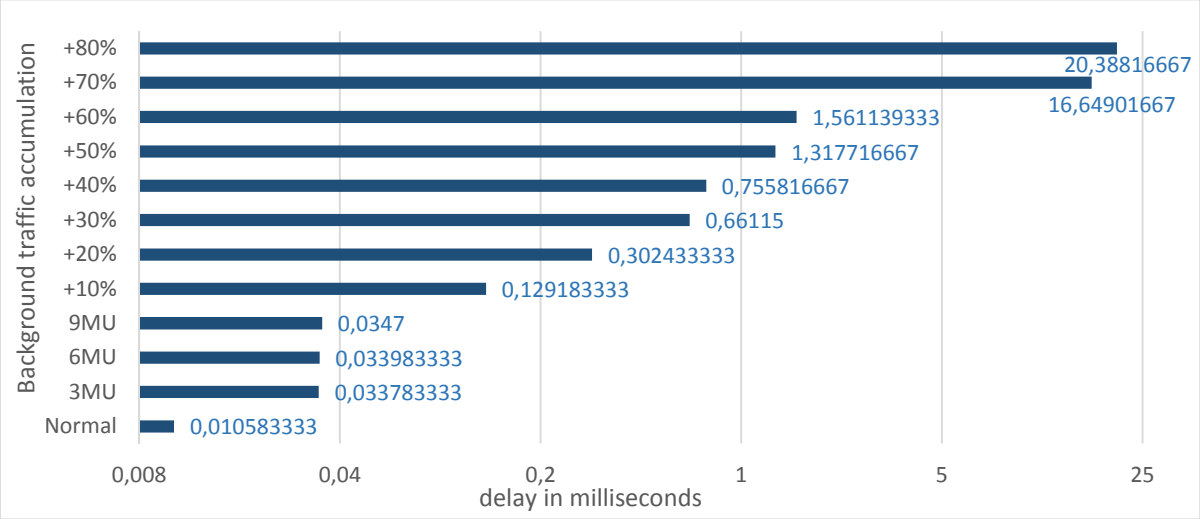


Figure 5.11: Background network traffic load vs. average delay of GOOSE propagation

The IEC 61850 time requirements are not satisfied within these circumstances (effects of background traffic), especially when propagation delay of GOOSE messages passes certain value of 3 ms assigned for transmission (in which 20% is allocated for GOOSE propagation) and even worse when it reaches more than 4 ms as depicted by the observed network load.

5.5.2. Streams of SV frames

A merging unit shall publish 4000/s SV frames within a profile of 80 samples per 50 Hz. These frames embed a sequential number (sample counter) field starts by zero and ends with 3999 that facilitates determining SV loss rate and inspecting of frames order at the receiver node (subscriber). In addition, calculating delay and delay variation (jitter) needs capturing data frames at both ends. We observed the SV frames, published by one merging unit (identifier GICSMU0001) during all scenarios, to determine the quality of service and performance indications that include throughput profiles, frame delay, frame loss ratio, out-of-order frames and frame delay variation (jitter). The average delay variation (jitter) for SV streams is obviously variable that does not conform to the IEC 61850-9-2 requirements, i.e. 9-2 light edition limits delay to 3 ms and jitter to no more than 200 µs.

Table 5.6: Ethernet performance metrics regarding SV published frames of a merging unit (GICSMU0001)

Traffic rate	Average delay (µs)	Maximum delay (µs)	Average Loss rate/s	Average non-ordered/s
33,777	0.718	39	No loss	-
43,805	0.970	69	No loss	-
53,472	1.231	173	No loss	-
63,497	1.790	130	No loss	-
73,432	1.438	41	No loss	-
82,621	2.188	87	5,00E-04	-
91,949	2.025	192	6,25E-03	-
93,576	168.0	1840	1,18E-01	472/4000
93,777	113.976	1630	3,05E-01	1220/4000

Table 5.6 depicts statistical information about the merging unit GICSMU0001 during nine traffic scenarios. These statistics provide indication about the SV service performance where average delays are varied due to background traffic loads. The Ethernet switch drops a significant amount of SV frames when traffic load reaches just above 80 Mbps. This loss rate is increased (from $5x10^{-4}$ up to more than $5x10^{-1}$) dramatically, which is not suitable for measurements where critical protection schemes shall use precise real-time power quantities, e.g. current value with accurate phase degree. The out-of-order arrival of SV frames is increased with higher traffic rates as depicted by the last two values where 472 and 1220 frames arrive lately due to overloaded switch buffer (queueing memory).

5.6. Methodology to acknowledge GOOSE reception

5.6.1. The method

Apparent flexibility of the GOOSE based protection schemes allows manipulating of functional messages communication in a real-time comportment. This real-time performance respects the standardized constraints when the communication environment enable delivering protection and control messages within very short latency. The only issue is that GOOSE communication depends on the retransmission mechanism to achieve reliability, i.e. attempts increase delivery of GOOSE messages, without any kind of acknowledgement means. Hence that, a method is proposed and experimentally tested to achieve acknowledgement (announce receiving of substation events) in a real-time manner. The concept suggested exchanging of GOOSE message to achieve status acknowledgment at the application level. In this approach, the application logic inside IEDs shall indicate the status of predefined protection functions or specific events at a bay-level. An algorithm is designed for acknowledgement where two IEDs namely Transformer_IED and Feeder_1-IED exchange acknowledgment messages. The idea is to announce the status of the protection functions and to indicate their status by mapping status to light emitting diode indicators (available for the user at the front panel of IEDs). Hence, the reverse blocking scheme (see chap 4 § 4.3.3.1) is chosen as an example of the protection functions interaction and coordination. Thus, the following sequential diagram illustrates steps (Fig 5.12) of implementation:

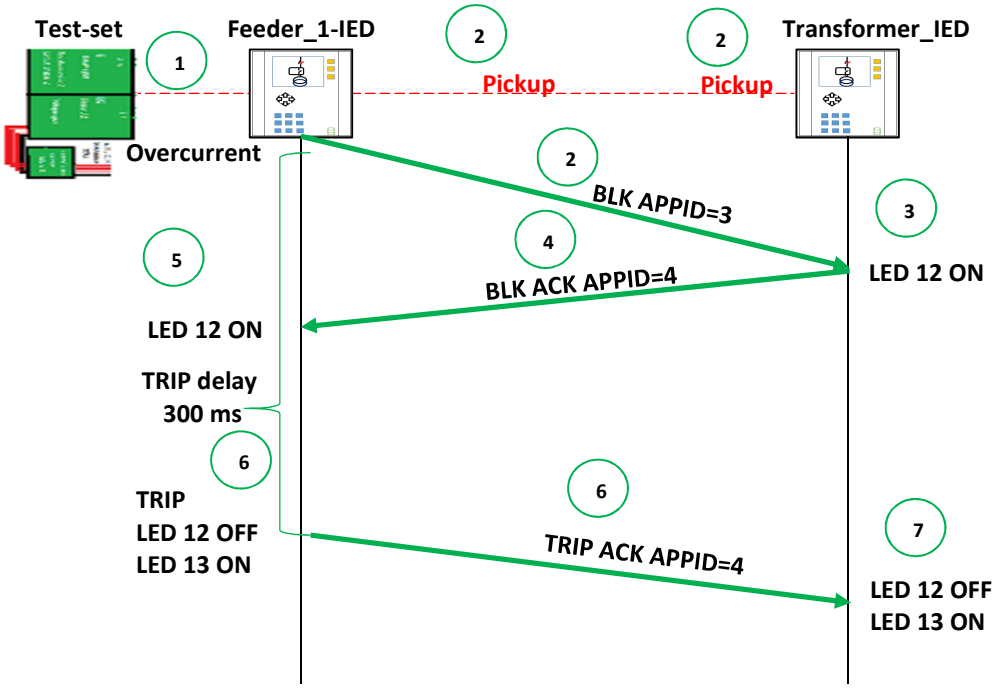


Figure 5.12: Sequence diagram of GOOSE messages reception acknowledgement

1) The test-set triggers an overcurrent signal (fault event), at the middle zone between the two bays, with a value passes the threshold of the overcurrent functions.
2) Transformer_IED and Feeder_1-IED sense a short circuit fault or higher currents (passing the predefined 500 A threshold) that pick up their overcurrent protection function (50/51). Feeder_1-IED publishes a GOOSE message (BLK) to block the Transformer_IED overcurrent function, exactly the secondary side overcurrent stage.
3) The Transformer_IED receives this GOOSE and according to that, the programmed logic blocks the first stage of the overcurrent protection function and activates an indicator on the front display panel, which is a Light Emitting Diode LED 12.
4) The Transformer_IED publishes the blocking state (BLK ACK) of its secondary side overcurrent function.
5) The Feeder_1-IED receives the BLK ACK from the Transformer_IED and activates LED 12 as an indicator.
6) After a predefined delay, i.e. in this setup and for testing purpose the trip delay is 300 milliseconds, the Feeder_1-IED trips (opens) the designed circuit breaker and publishes the trip event (TRIP ACK). Then activates LED 13 while deactivates LED 12.
7) The Transformer_IED receives the published GOOSE (TRIP ACK) and then deactivates LED 12 while activates LED 13.
8) During all GOOSE arrivals, a programmed logic keeps the events timestamp in log files at both IEDs. Log files are configured to retrieve events with precise synchronized time. These files are used to inspect the GOOSE data change during this experiment setup.

The three GOOSE messages contain application identifiers (APPID=3, APPID=4 and APPID=5). The first one for the Feeder_1-IED's overcurrent pickup that triggers block

message (BLK), while the second message for block acknowledgment message (BLK ACK) and the last one to indicate a trip operation (TRIP ACK). The abovementioned algorithm announces in real-time the protection and the control events with related acknowledgments. The above diagram illustrates messages sequence with associated delay between the Transformer_IED and the Feeder_1-IED. The test-set is programmed to trigger 12 times overcurrent events (over protection threshold). Several events were recorded in the IED log: a) pickup, b) block, c) block acknowledgement and c) trip acknowledgement.

5.6.2. Observations

The method achieved the designed goal where BLK and BLK ACK messages exchanged during observations. Table 5.7 illustrates the time between events where values represent seconds during 12 transients in this experiment (only second and millisecond parts of time). These values are derived from the IEDs log files. An operation delay between pickup and trip is set to 300 ms, although log records show varied time. The average trip delay is around 298 ms indicating that an amount of time possibly kept for relay contact (output time). The average end-to-end delay, between BLK initiated at the Feeder_1-IED and the BLK ACK as response from the Transformer_IED, is about 5.75 ms, which is enough for interval coordination between the IEDs functions in this setup. Table 5.7 shows the observed delays between BLK and BLK ACK from one side, and BLK and TRIP ACK from the other side. The delay, between blocking (BLK) messages sent by Feeder_1-IED and replied acknowledgement (BLK ACK) sent by Transformer_IED, is tabulated in this table with a maximum transfer time just above 6 ms that is enough for acknowledgment. In addition, the time between blocking (BLK) and tripping (TRIP ACK) is given that indicates delay with values near the expected 300 ms operation time.

Table 5.7: The period between the GOOSE messages including reception acknowledgement

Event no	BLK	BLK ACK	TRIP ACK	Delay between BLK & BLK ACK (milliseconds)	Delay between BLK & TRIP ACK (milliseconds)
1	145,277	145,283	145,574	6,094	297,808
2	158,302	158,308	158,598	5,909	296,416
3	173,317	173,323	173,613	5,700	295,605
4	237,372	237,377	237,669	5,770	297,682
5	249,367	249,373	249,672	6,248	305,150
6	285,397	285,403	285,697	5,729	299,593
7	10,585	10,591	10,885	5,592	299,569
8	27,602	27,607	27,902	5,257	299,901
9	60,630	60,636	60,927	5,405	296,387
10	75,636	75,641	75,931	5,809	295,261
11	96,662	96,668	96,960	5,795	297,291
12	110,678	110,683	110,974	5,714	296,087

GOOSE messages, as explained, deliver event changes in real-time. We observed the LED indicators during the experiment that showed fulfilled timely coordination between IEDs with perfect intervals. This method also enables verifying the accuracy of time synchronization at both devices. The operation delay (time to trip) depends on the IED clock, which drifts from the actual time when the IED clock is not precisely synchronized.

Remarkably, the NTP time precision is not reliable for interaction of bay/process level functions because we noticed timestamp drifts during the experimentation process. The reason is that the IED enquiries the NTP server according to the time setting, e.g. time request every one second. This inquiry does not compensate the network delay, which means that SNTP is not an appropriate method where protection and control functions require accurate time synchronization and compensation. Consequence of a time drift may cause an early or late tripping of the designed circuit breaker issued by the relay contact of the Feeder_1-IED protection function.

5.7. Dynamic testing of the protection schemes

Complexity of design and configuration open doors for human errors which in result require testing the protection schemes in dynamic conditions similar to that ones in real substations, although interaction between communication network, protection and control systems take place. Additionally, intensive dynamic testing is a vital measure to verify coordinated time interval (see section 4.3.5) among modern digital IEDs during variant network traffic loads and power transients. In this section, a practical method is developed that intends to test the dynamics of protection schemes considering the coordination time interval throughout numerous states of a loaded communication network. The aim is to reveal failure events and to observe the behavior of devices during power current transients in normal and abnormal states of communication networks.

5.7.1. The dynamic test setup

Two devices are observed during this setup, namely Transformer_IED and Feeder_1-IED. The chosen protection scheme therefore is the reverse blocking when Feeder_1-IED blocks the 50/51 overcurrent protection (see appendix B) function of Transformer_IED (in the main bay) as soon as short-circuit or overcurrent faults happen near their zone of protection. Both devices 50/51 protection function sense the fault, considering the fault B (Fig. 5.12), and pickup for preconfigured delay before tripping corresponding circuit breakers. Hence, during the delay period Feeder_1-IED should publish a blocking message that disables (blocks) the secondary side 50/51 function of Transformer_IED. The later IED subscribes to this blocking message, and receives the status of the Feeder_1-IED protection function. The received GOOSE shall block functions such as the Transformer_IED secondary side protection until clearance of faults. For acknowledgment, Transformer_IED is programmed to publish a GOOSE message (see section 5.8) to inform Feeder_1-IED about the blocking of its protection function (secondary side 50/51). In a normal situation, Feeder_1-IED clears the fault and publishes its status to Transformer_IED.

For safety enhancement if there is still an overcurrent fault near the secondary side of the main transformer the second stage 50/51 function of the Transformer_IED shall pickup and trip immediately. The coordinated time intervals between pickup and blocking from one side and blocking and tripping from the other side are critical for reliable operation of the protection scheme.

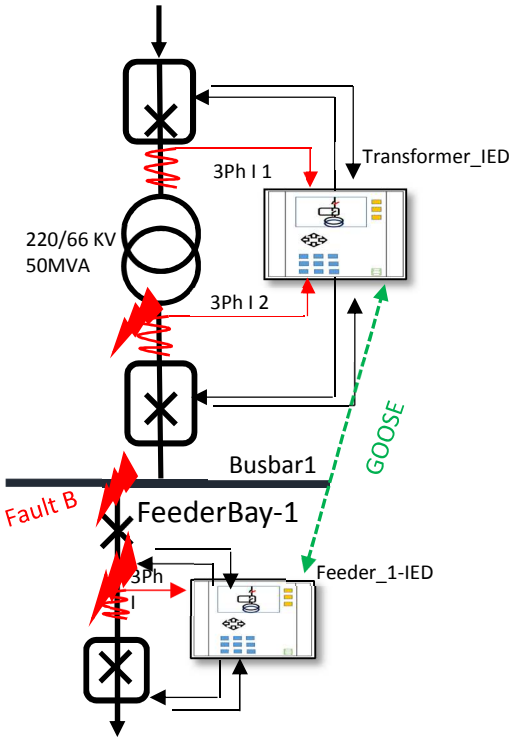


Figure 5.13: Overcurrent faults at Busbar 1, near protection zones of both IEDs

Figure 5.13 illustrates GOOSE message exchanges between both IEDs, where events and status exchange are necessary for time coordination. The IED in charge performs fault clearance (trip) in short time depending on time coordination of the protection scheme. The upstream IED should be blocked when faults out of its protection zone, such as Fault B, occur (fig 5.13). The transfer time of blocking message is vital for a perfect coordination between both IEDs. The trip time of Feeder_1-IED depends on the overcurrent fault magnitude (inversely proportional), where it trips very fast and immediately within higher overcurrent faults. For testing purpose, the overcurrent protection function delay (operate delay) of Transformer_IED is programmed to be 20 ms and the threshold is set to 300 A, while Feeder_1-IED is set to trip in 20 ms (operate delay) for a threshold less than 500 A and instantaneously for else.

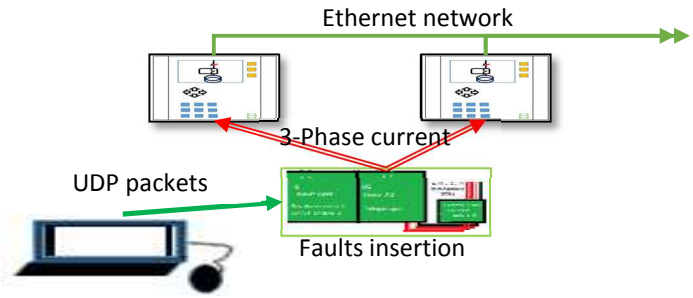


Figure 5.14: The test set: insertion of periodic faults through injection of current values

The network traffic scenarios are similar to those setups in the previous experiment (see section 5.4) but starting from scenario of nine merging units, then adding 10 Mbps background traffic respectively, until reaching an overloaded (over 100 Mbps) network scenario. Throughout these scenarios, the test set card is programmed to insert fault transients via analog current inputs, i.e. one phase and 3-phase faults current, of both devices (Fig 5.14) in a real-time. In this setup, both devices can be tested in a hardware-in-the-loop environment. The inserted overcurrent faults constantly repeated every 6 seconds, during running of 10 scenarios of network traffic where every scenario lasts 60 seconds, which means 100 times of transients are applied.

5.7.2. The observations and results

The whole network traffic and the two ends of IEDs GOOSE traffic were captured during the experiment scenarios. Ten variant traffic scenarios were observed during 600 seconds. In every scenario, 10 transient faults were injected resulting in overall 100 faults during this setup. These scenarios were repeated for 10 instants, i.e. every 60 seconds, to confirm that results obtained are consistent and conform to the standardized testing procedures.

Table 5.8: Time and quality metrics of GOOSE frames during dynamic testing

Scenarios	Observed traffic (average Mbps)	Average delay (ms)	Maximum delay (ms)	Minimum delay (ms)	Loss rate (%)
Normal	0.479	0.011	0.052	0.001	No loss
9MU	33.777	0.036	0.045	0.024	No loss
additional 10%	43.805	0.154	0.802	0.017	No loss
additional 20%	53.472	0.311	1.271	0.021	No loss
additional 30%	62.497	0.64	2.125	0.006	No loss
additional 40%	73.432	0.8	2.246	0.014	No loss
additional 50%	82.621	1.431	3.229	0.005	No loss
additional 60%	91.949	1.92	3.304	0.024	No loss
additional 70%	92.576	16.721	19.506	13.478	14%
additional 80%	93.777	20.549	22.542	16.489	20%

The delay of GOOSE-enabled blocking messages, i.e. messages with GOOSE identifier GOOSE ID=3, for the device under test (Feeder_1-IED) was determined by subtracting the timestamp of frames (at publisher and subscriber) that share same sequential and state numbers (see Eq. 5.1), where the number of lost frames identifies the loss rate. In addition, the traffic is inspected to verify GOOSE frames sequential order. Statistical results are tabulated in table 5.8, which shows that an average delay passes 600 microseconds (0.6 ms) when the observed network traffic reaches a value just above 60 Mbps. Maximum GOOSE transfer (propagation) delays represent worst-cases where values more than 0.6 ms do not satisfy the standardized requirements.

The dropped frames were identified by their sequential number in which we find that first frame (with seq.no=0) is dropped, during several traffic scenarios, and the result is that a second frame arrives after 22 ms due to queuing and switching latency in heavy traffic scenarios, i.e. just above 92% of theoretical throughput (bandwidth). Table 5.8 shows a remarkable loss rate in the last two rows, although no consecutive drop of frames is happen

which give an indication that probability of GOOSE delivery is higher but within long delays.

In other side, all network traffics between both devices are captured to determine predefined metrics about the network service of GOOSE based protection communications. These metrics comprise average delay, percentage of lost messages and amount of out-of-ordered message frames (table 5.8 and Fig 5.15). Figure 5.15 illustrates average delays of functional GOOSE messages during several traffic scenarios. First value of GOOSE delay shows 0.036 ms as an average delay where assumed nine merging units publish around 33.12 Mbps of SV measurements. Traffic is increased after that by 10%, in which GOOSE average delays pass a limit of 0.6 ms where the additional traffic reaches 30% (just above 62 Mbps). Cumulative traffic loads therefore affect propagation delays of GOOSE frames in these circumstances.

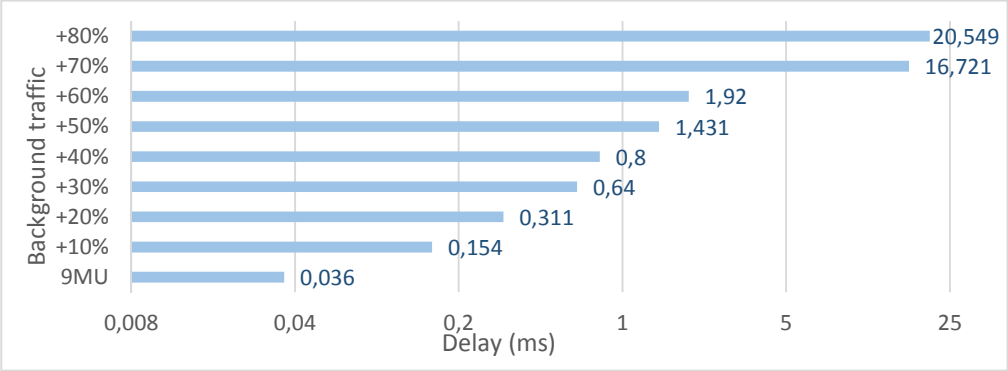


Figure 5.15: GOOSE messages average delay during dynamic testing

Figure 5.15 indicates results not so far from that explained by figure 5.10, but the reader should consider that frame rates is higher in this experiment due to intensive failure events that yield new GOOSE messages. In this manner, the behavior of the IED under test is normal, though during high traffic loads the Transformer_IED witnesses a failure. This failure holds the IED in fallback state. During this state, the observed GOOSE messages have bad quality, i.e. GOOSE quality field (GOOSE.q) is false.

5.7.3. Discussion of results

Comparing results obtained with the previous results (§ 5.5.1), we remarkably find that testing should incorporate injecting fault transients in order to reveal critical situations. Thus, behavior of protection schemes, for the duration of fault currents, changes due to high rate of GOOSE transmission. This dynamic behavior depends on both: magnitude and duration of fault currents and status of the communication network. These dynamics do not exist during normal operation of the protection schemes, and either when the Ethernet network is loaded, due to the limited repetition profile of the functional GOOSE messages. The delay and loss of GOOSE shall affect the time coordination of protection scheme and total clearance times.

SV frames that carry 3 phase measurement data were also observed during last scenarios. Arrival times of these frames encounter unstable delay causes varied frame arrivals (jitter). Furthermore, SV frames noticeably witness a significant loss rate as soon as observed average network traffic passes 92 Mbps. This loss rate varied from one merging unit to another.

Additionally, IEDs are programmed to save log files recording every fault event (sequential events record SER). These files accompanied by additional data that covers protection responses (functional behavior) at both IEDs. The collected facts from the log files include timestamped data that is used to observe timing behavior of the protection schemes. In the following subsections, the reader shall understand significant findings that are categorized into GOOSE quality effects on functions of protection and total clearance time.

5.7.3.1. Effects on the coordination of the protection schemes functions

In higher traffic insertions, GOOSE messages obviously struggle to reach its subscriber destination and encounter a long delay period. Even worse, when the Ethernet switch start drooping some GOOSE frames. Published GOOSE, by Feeder_1-IED, faces a delay that reaches longer periods than the setting (operate delay) of Transformer_IED, thus the later senses a fault current in the course of transient faults (fault B Fig 5.12), then pickups and starts delay before tripping. Transformer_IED will miss blocking GOOSE (Fig 5.16) during long waiting, to clear fault currents Transformer_IED initiates a spurious trip, i.e. safe failure status shall exist.

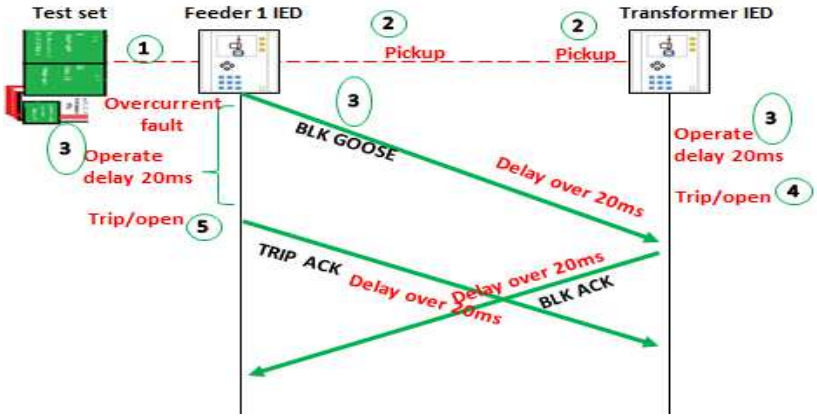


Figure 5.16: Miscoordination between protection functions due to GOOSE

Furthermore, delayed GOOSE messages shall block the 50/51 protection of Transformer_IED that resulting in delayed clearance of faults if the relevant circuit breaker recloses or encounters a failure. This situation is critical because that Transformer_IED turn into fallback state during the last two scenarios.

5.7.3.2. Effects on fault clearance time

Detailed time delay for ETE transmission is given by analyzing timing parameters. The timing diagram of initiating and publishing a GOOSE message over the Ethernet network is shown (Fig 5.17). The ETE delay (T_{ETE}) is identified as time from published IED sends a GOOSE until subscriber receives it. This delay incorporates three parts (see section 4.5) that are time delay at publisher IED, on the network, and at the subscriber IED. An assumption made that preprocessing time of an IED is equal to post processing time, which is identified by measuring an IED response time to ICMP requests (see section 5.3.2).

$$= T_{pre} + T_{net} + T_{post} \qquad (5.6)$$

This time is not fixed due to traffic load effect (variable delay) and message lost. The worst case when a transfer time (T_{net}) of a GOOSE message reaches just above 20 ms and an IED takes more than 4 ms to process this message. In result, an overall delay equals more than 24 ms, which is not suitable for time coordination where operation reaction of an upstream device is less than this time. The solution consists in either increasing operation delay of upstream devices, which is not an appropriate technique (considering arc flash), or decreasing message delays through guarantying performance via best service configuration and testing.

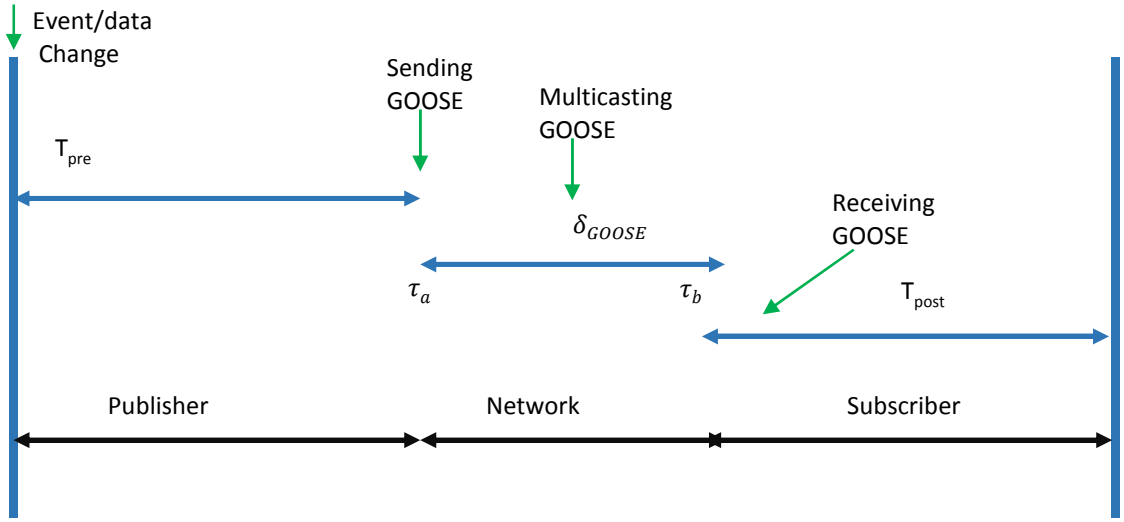


Figure 5.17: A timing analysis illustrating a delay of a GOOSE message from publisher to subscriber

5.8. Quality of service: priority to limit the GOOSE delay

5.8.1. Implementing the VLAN based priority

The IEEE 802.1.Q standard enables using tagged VLANs. This feature incorporates user (IED side) priorities as an embedded class of service field within the tagged frame. The managed Ethernet switches isolate tagged VLAN frames from other broadcast traffics (see section 3.3.2) according to their VLAN identifier (VLAN number and name). Switch ports based VLANs allow segregating the functional messages (IEDs GOOSE frames) from the other background traffic in the platform network. Using this mechanism, switches therefore guarantee better policing and scheduling of the protection and control related messages.

The IEDs are reprogrammed to enable tagged VLAN based priority in order to enhance the class of service for publishing/subscribing communication. The rewards shall be:

1. Isolating the functional GOOSE messages through VLAN ports.
2. Improving security by limiting GOOSE multicast to a dedicated VLAN.

3. Assigning priority levels to mission-critical GOOSE messages to boost and guarantee their delivery, and low priority (best effort) for non-tagged traffic.

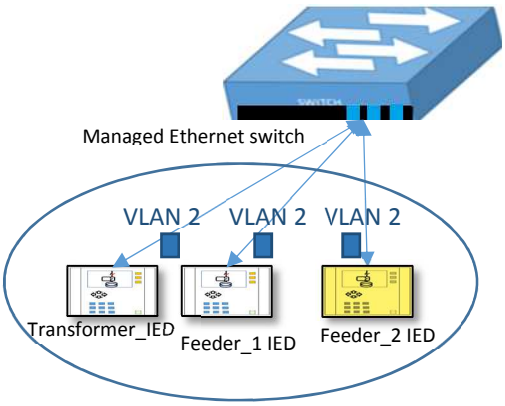


Figure 5.18: managed switch enables three IEDs communicating through VLAN 2

IEDs shall use the VLAN 2 as identifier and the value four as a priority class. In the other side, reconfiguration of switches is performed to create a protection VLAN network (protection_vlan) with a value 2 as the VLAN identifier. Three ports in this design allocated for the transformer, feeder 1 and feeder 2 (see figure 5.18). IEDs publish/subscribe to GOOSE messages only within this VLAN. Table 5.9 illustrates the GOOSE assigned priority in the Ethernet switch and devices where trip messages shall have higher priority (level 4) than other messages. Notice that switches have four priority classes while priority levels of Ethernet frames are eight (from 0 to 7). where best effort priority (0) and 3 are assigned (by default) to priority class 2 (Table 5.9).

Table 5.9: Assigned priority for messages frames

Device	**Message**	**priority**
Transformer_IED	switchgear status	3
Feeder_1-IED	Trip (open) blocking	4
Feeder_1-IED	switchgear status	3
Feeder_2 IED	Trip (open) blocking	4
Feeder_2 IED	switchgear status	3
Other devices	Other network traffic	Best effort

5.8.2. Observation of VLAN tagged GOOSE

In the platform network, traffic is observed to determine the efficiency of VLAN based priority. Noticeably, only VLAN tagged frames pass through the designated VLAN ports (see figure 5.16) or switching protocols such as the spanning tree protocol (STP), not alike previous scenarios when devices can receive all multicast traffics. A configured SPAN port allows trapping of these frames through non-stripping interfaces at the analyzer beside network TAPs that allow capturing VLAN circulated frames at both IEDs ends. The VLAN traffic almost has a fixed average load during all background traffic scenarios. Accordingly, the observed traffic load keeps an average utilization of 0.005 Mbps (of 100 Mbps allocated for each port). Each traffic scenario within this experiment lasts 60 seconds, and all scenarios prove no frame loss of the functional GOOSE messages. Additionally, the GOOSE transit (propagation) time keeps almost a fixed delay with a maximum value equals 40 microseconds, as depicted by Fig 5.19, which satisfies the performance requirement and respects the standards time constraints.

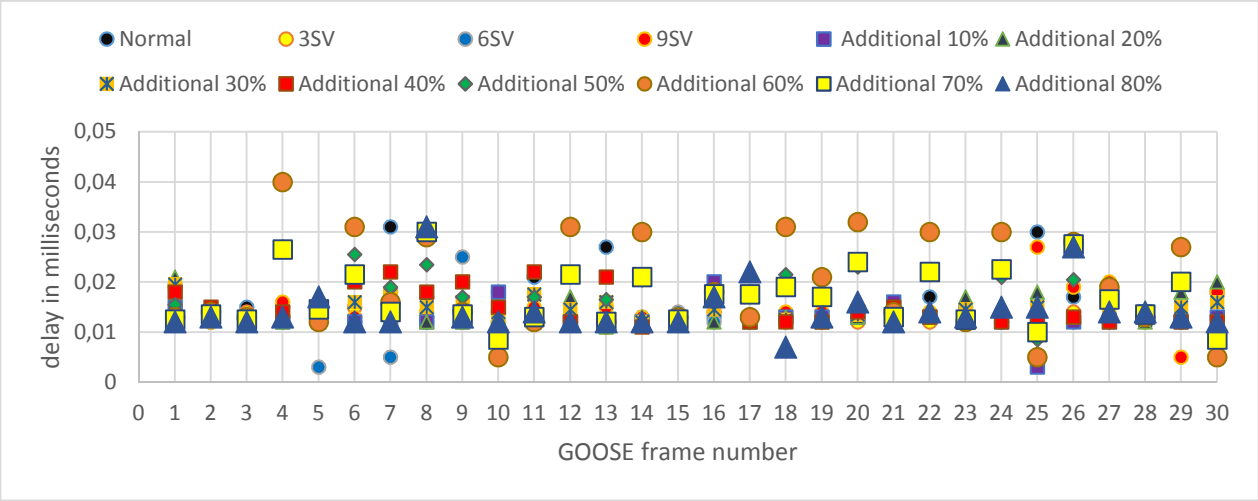


Figure 5.19: A suitable transfer time of GOOSE frames due to VLAN based priority scheduling

Figure 5.19 shows delays of captured GOOSE frames during several traffic scenario (illustrated above the figure). The Ethernet switch guarantees short transfer time of GOOSE frames that carry blocking messages via using high priority policy and isolating the traffic through VLAN encapsulation. The average delay of GOOSE messages in this setup is around 15 microseconds. Additionally the figure illustrates that the Ethernet switch can transfer GOOSE frames within short latency even during high traffic loads that saturate the network as depicted by adding 80 Mbps to nine streams of sampled value measurements. In other words, the switch give precedence to GOOSE messages according to their priority. The figure shows that maximum delay for a GOOSE message is below 32 microseconds for the maximum traffic scenario (around 93 Mbps throughput).

5.9. Overall discussion of results obtained

5.9.1. Timing analysis of the end-to-end delay

In this section, a timing analysis of GOOSE messages delay is given. The timing analysis illustrates initiating and publishing of the GOOSE message over the Ethernet network (Fig 5.17). An assumption made that preprocessing time (δ_{proc}) of an IED is equal to post processing time, which is assumed by measuring an average response time to internet control message protocol (ICMP) requests (see 4.5.3). This time depends on the IEDs hardware specification such as the memory size and the processing capability. A measurement setup already used to determine the network delay of GOOSE messages (δ_{GOOSE}), i.e. propagation and message transmission. Following equation (eq. 5.7) gives similar result as equation 5.6.

$$t_{ETE} = t_{sub} - t_{pub} \\ = (2 \times \delta_{proc}) + \delta_{GOOSE} \quad (5.7)$$

The worst-case end-to-end delay of a GOOSE frame reaches more than 22 milliseconds when the traffic load passes 80% of the LAN throughput. Table 5.10 shows probabilities of dependability and security according to IEC 60834-1 (detailed in chap 3 § 3.4.3). These performance metrics are determined, i.e. calculated from results obtained during the experiments, according to the standards requirements (see chap 3 § 3.4). In addition, the table shows worst-case end-to-end delay.

Table 5.10: Results obtained, platform experiments, for IED processing time and metrics of the GOOSE transmission

Measure	symbol	Without VLAN and priority	With VLAN and priority
Processing time	Average $\delta proc$	1.42 ms	1.42 ms
Delay	δ_{GOOSE}	Worst case 22 ms	Worst case 0.04ms
Loss rate	P_{mc}	Delayed frames About $1{,}11E^{-1}$	No loss or significant delay
Altering rate	P_{uc}	Not relevant	Not relevant
ETE delay (worst-case)	t_{ETE}	22.84 ms	2.88 ms

IEDs that publish GOOSE frames without VLAN based priority may cause inappropriate circumstances due to missing time coordination between the distributed functions in the protection scheme. The results obtained show the worst-case delay in this scenario that passes 22 milliseconds. This scenario causes missing blocking messages due to a large latency. Transformer_IED waits 20 ms (Fig 5.20) before issuing a trip assuming no blocking message (GOOSE) causing a power outage for the industrial facility. Figure 5.20 shows time delay between the two IEDs protection functions. This delay is used as time coordination between upstream (main transformer protection) and downstream (feeder protection) protection functions.

Even worse, a misconfigured switch shall cause delay or loss of sequences of GOOSE messages. The blocking scheme between the feeder_1_IED and the Transformer_IED in the

industrial substation is a safe measure. Tripping from the transformer IED will cause full power cut leading to cascade shutdown for the industrial facility. The delay would cause also degradation of other functions in the protection scheme such as the inter-tripping that needs special handling when coordinated tripping is important to avoid current feedback from the industrial facility. The delay of GOOSE could cause destructives consequences for interlocking if status of circuit breakers changed while not published in short time. In this scenario, the protection functions should coordinate within a reliable and available communication between the distributed functions and even the centralized control. Delayed blocking could cause in result a nuisance trip (power outage), but delayed interlocking leads to hazardous circumstance such as arc flash and melted materials (see section 4.3.2).

5.9.2. Consequence of network perturbations on protection schemes (bay-level)

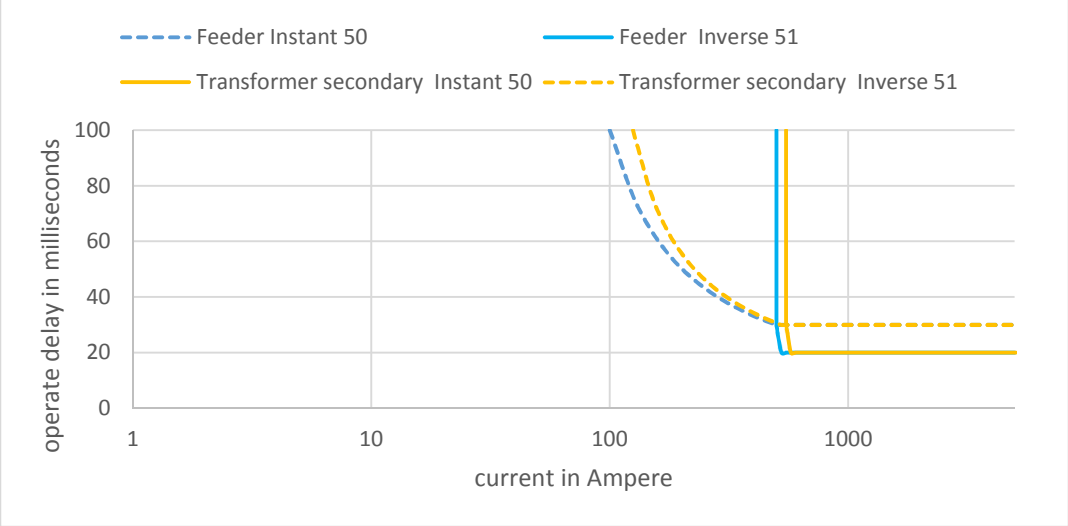


Figure 5.20: Short delay is mandatory for time coordination between protection functions

Higher traffic loads will influence transfer time of GOOSE messages yielding in inappropriate delays and loss of these messages. When faults exist in external zone, the protective IED near the fault pickups and block other IEDs. Missing or delayed blocking signal such as GOOSE message may lead to degraded operation of the protection and control, e.g. malfunction of reverse blocking scheme (safe failure) where possible consequence is a power outage. Even worse, critical schemes such as intertripping and interlocking do not operate efficiently when requested status change not delivered in a timely manner, i.e. , are sensitive to signaling delay and loss, as a result interlocking may not work properly (dangerous failure) due to missed status of switchyard equipment. This delay is not suitable for fast intertripping; resulting in long duration of arc flash incidents when faults need clearance in a real-time manner. The arc flash consequence, in high voltage substations, is a hazardous situation, especially in indoor substations, that causes an energy over 100 Calories/cm^2 , i.e. acceptable energy is less than or equal to 1.2 Cal/cm^2 with 100 ms or faster clearing time, for distance between about 90 and 122 cm [IEEE 1584, 2002].

5.9.3. Consequence of network perturbations on measurements (process-level)

As observed sample value streams face unstable delay that cause frame delay variation (jitter) that is not suitable for precise measurements. Obviously, higher traffic loads affect arrivals of SV streams that result in inaccurate measurements, and additionally related time synchronization frames shall face same issues. Moreover, the IEC 61850-9-2 standard insists on SV time synchronization with at least 4µs precision, which gives an acceptable phase error, i.e. phase error of 7.2 %, hence that implementation of process level technology obligates using reliable and accurate technique of time synchronization, which is important for precise phase measurements when a time drift results in phase errors. In these experiments varied jitter of SV frames does not satisfy the standard requirements.

5.9.4. The information rate and traffic profiles

Considering the standards requirements as service level agreement, i.e. delay and loss constraints, the traffic profiles are observed during all experiments. Then, the committed and excess information rates (see CIR and EIR in chap 3 § 3.5.2) are identified when the GOOSE message frames do not use any type of service quality such as policies of frames priority and VLAN tagging techniques. Fig 5.21 shows the maximum sustained information rate (CIR), which is 50 Mbps, for the Ethernet network to transfer GOOSE frames while meeting the 20% constraint, 0.6 ms of 3 ms transfer time, as performance level guaranteed in these tests. The Ethernet network can exceed the CIR, up to 60 Mbps, but some observations prove that the EIR might not guarantee the required performance level, i.e. transfer time of GOOSE less or equal to 0.6 ms as required by the standards (see chap 3 § 3.4.2). The figure also shows the red colored area where the performance level cannot be guaranteed. In experimental setup, VLAN based priority is used to overcome this issue, i.e. to overpass EIR traffic profile.

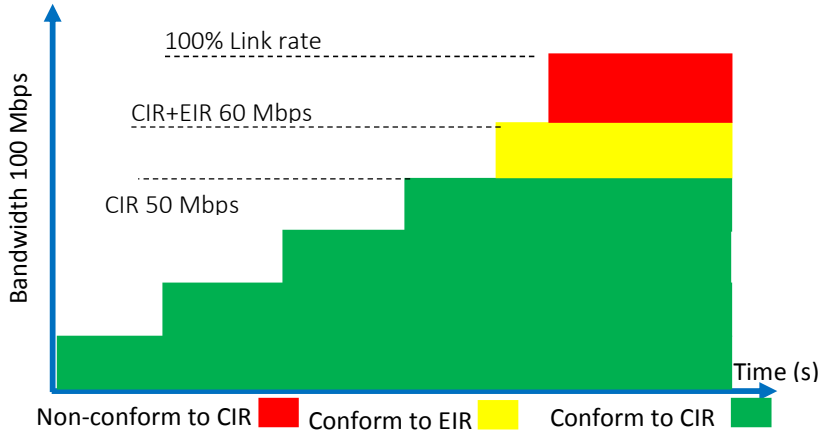


Figure 5.21: Traffic profiles and performance levels

5.10. Conclusion

In this chapter, experiments, with real protection IEDs and Ethernet network, are performed in order to test dynamically IEC 61850-based protection schemes. The experimental tests build a practical framework to evaluate performance of Ethernet enabled GOOSE communications. During these experiments, real functional GOOSE frames are observed. These frames are accompanied by traffic scenarios that include emulated SV streams and GOOSE (fake) as background traffic with several amount of loads. Furthermore, to determine their effects on the protection and control coordination, we find that high network traffic causes a long delay for protection and control messages (GOOSE) and loss of certain amount of these messages during dynamic transients of the power system. The delay and loss are observed, which support what expected during preparation of these experiments. Additionally the dynamic transients along the high rate of the network traffic influence the IED behavior, i.e. fallback is happened, that cause setting of bad quality for generated GOOSE datasets.

Numerous measurements are used to calculate predefined metrics mainly to inspect time critical requirements in order to determine:

a. Processing time of publishing and subscribing at IEDs including logic solver and communication stacking,
b. End-to-End transmission time between two IEDs in a publisher/subscriber pattern and,
c. Effects of SV stream, functional GOOSE and other background traffic within the context of IEC 61850.

Other metrics are calculated such as SV frame delay variation (jitter), probabilities of missed commands and unwanted commands. In addition, an empirical method for acknowledgment of event exchanges is proposed where events can be logged into sequential event records inside the devices. This method helped to check accuracy of time synchronization at the bay-level devices (IEDs) and to check sequential order of substation events.

To propose a solution for inappropriate GOOSE delays, essentially, a VLAN based priority is implemented that gives satisfied results to guarantee short transmission time of GOOSE frames through applying suitable class of priority. Alongside, the VLAN technique has advantages that include enhanced security by isolating functional GOOSE frames from other traffic and passing only tagged frames that belong to the same VLAN. Therefore, we recommend appropriate configuration and intensive testing of Ethernet technologies such as VLANs and priority class before putting a system in a production mode.

To sum up, these experimentations are useful techniques to evaluate performance of industrial substation automation systems and related platforms performance according to the standards requirements. In this approach, dynamic tests can be used to verify and validate conformance of devices and related communications to the standards requirements, specifically protection communications performance and related time requirements.

chapter 6 : The Dependability of the IEC 61850 Based Process/Bay Levels

6.1. Introduction

Designing of large and complex products and systems requires well-defined disciplines, i.e. selecting reliable components, building dependable architectures and satisfying customers' requirements. Dependability studies are vital for these phases. To answer whether dependability methodologies (with regard to dependability and functional safety) are well-suited/applicable to smart grids or not [CEN/CENELEC/ETSI, 2011], an illustrated case study is provided to evaluate protection functionalities in IEC 61850 based process/bay levels, where most of the modern protection schemes involve electrical, electronic and programmed functions. Considering the application of these functions, in this study, functional safety is addressed, besides; reliability and inherent availability are evaluated.

In this chapter, section 6.2 provides a historical overview with a chronological evolution of the term (dependability) and its related terms (taxonomy tree). Section 6.3 illustrates the main dependability attributes. The well-known reliability block diagram (RBD) technique is highlighted with a case study covering IEC 61850 based architectures in section 6.4. Functional safety concepts, related metrics and formulas are provided and implemented in section 6.5 with the same case study. Conformity of GOOSE service, and frames to safety communication requirements, is analyzed in section 6.6. Section 6.7 concludes this chapter.

6.2. Preliminaries for Dependability

Dependability studies play a vital role for improving dependability of systems or subsystems that operate for long periods or specific missions. The dependability is a wide multidiscipline term, so there are several definitions for it [Al-Kuwaiti, 2009]. Therefore, the well-established scientific community considers the dependability as an umbrella that incorporates many attributes. This section shall provide definitions and related terminology to help the reader understand the dependability and evolution of associated attributes. The dependability attributes, means and impairments are enlightened in order to clarify each part of them.

6.2.1. Dependability nomenclature

In academia, [Laprie, 1985] adapted firstly a definition from [Carter, 1982] in which the dependability was defined as "trustworthiness and continuity of the delivered service such that reliance can justifiably be placed on the service".

In practice, dependability is defined, i.e. the French terminology (sûreté de fonctionnement) as a science of failures [Dhaussy, 2002]. Measures are used to recognize and to reduce the number of failures exposed to the system user. In such sense, the dependability denotes the ability of a system to perform its desired function or tasks faultlessly in a certain environment on a planned period [Ahmed et al, 2017; Avizienis, 2004].

6.2.2. Evolution of dependability studies

In 50s, the reliability becomes an engineering exercise in The United States [Saleh & Marais, 2006] when electronics' industry necessitated a strict approach to evaluate the electronic components and so the systems made of the former [IRE, 1953]. Since 60s, the availability and the maintainability grow to become parts of the new trend to analyze the reliability of systems. The reliability engineering further extends its studies by covering related fields such as; maintainability and availability in the nuclear and the aeronautics domains where safety issues apparently evolved [McLinn, 2010].

In 1967, Avizienis found the basis for fault-tolerance techniques, as dependability means, by incorporating fault detection, diagnosis and recovery [Avizienis, 1967]. At the end of 70s and early 80s, major industrial players follow the new trend by taking into account the dependability techniques. In parallel, academia in late 80s identified impairments, means and attributes of the dependability [Laprie, 1992]. The leading standardization body, the IEC (International Electrotechnical Commission) defined and classified attributes of dependability as corresponding to delivered services or products. In 1990, an agreement, between TC56 members, i.e. technical committee 56 that was established in 1965 to address reliability standardization, was put on action to enlarge the scope of IEC TC56 to address generic dependability issues across all disciplines [Strandberg, 1990; Van Hardeveld & Kiang, 2012; Grover & Van Hardeveld, 2014].

6.2.3. The taxonomy tree of dependability: threats (impairments), means and attributes

Academia and standardization bodies associate the dependability to a set of attributes, which are evolving since its primary appearance as measures in a taxonomy tree drawn by Laprie in 1985. In this context, the dependability of a system is described as a set of properties or attributes (Fig 6.1) [Ahmed et al, 2017; Avizienis, 2004; Laprie, 1992].

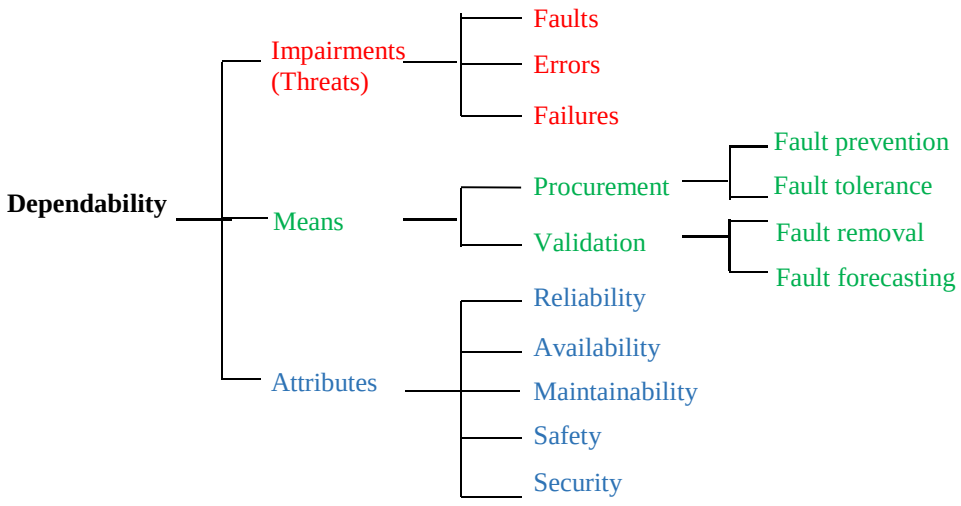


Figure 6.1: Dependability taxonomy tree adapted from [Al-Kuwaiti, 2009; Avizienis et al, 2004]

Van Hardeveld and Kiang state that dependability characteristics consist of availability, reliability, maintainability, and supportability that formerly referred to maintenance support [Van Hardeveld & Kiang, 2012]. Fig 6.2 illustrates the relation between main attributes of dependability emphasizing supportability association to maintenance and logistic support. The reader can distinguish the difference between the two figures where dependability attributes in the first figure include safety and security, while in the second figure supportability furtherly expanded to maintenance and logistics support

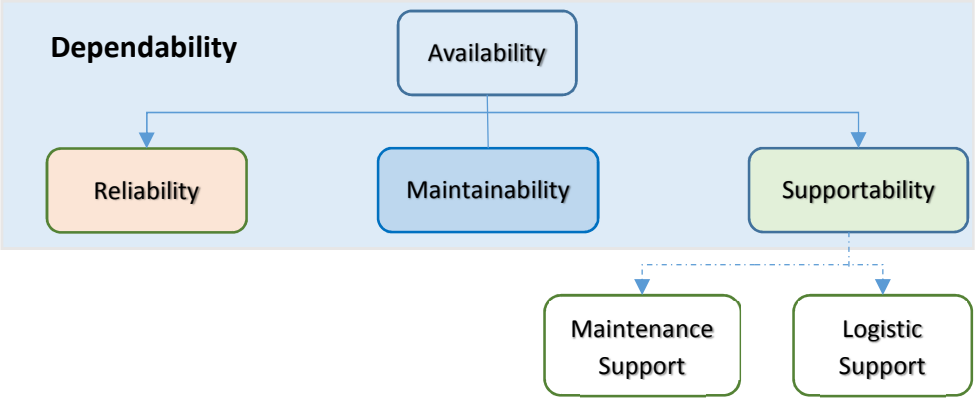


Figure 6.2: Dependability attributes in the context of a product life cycle [Grover & Van Hardeveld, 2014]

6.2.3.1. Qualitative vs. quantitative attributes

The attributes of the dependability such as reliability, availability and maintainability are quantifiable whilst some attributes are qualitative, e.g. safety and confidentiality [Al-Kuwaiti et al, 2009]. The quantifiable attributes can be used as variables to determine the quality of service of the communication network [Kyriakopoulos & Wilikens, 2000].

Considering the IEC 61850 based protection and control; a good example is a communication network that depends on the Ethernet physical and data link layers from one side and the IED network interface and application logic from another side. In this example, four quantifiable attributes do exist: availability of Ethernet LAN (average connectivity per time), integrity of Ethernet based GOOSE frames (percentage of correct frames over transmitted ones), utilization (amount of data transferred within GOOSE frames), and timelines (percentage of non-delayed GOOSE frames). Thus, the dependability of GOOSE based protection: availability, integrity, utilization and timelines can be mapped into the dependability attributes of the Ethernet LAN based protection and control.

6.2.3.2. Threats (impairments) against dependability

The impairments to dependability are undesired—but not in principle unexpected—circumstances resulting or causing from undependability, therefore when the delivered service no longer agrees with the specification then say a failure happened.

The dependability of services can be compromised by potential threats to their subsystems or components. In network-based services, two categories of threats happen: a) threats to the application and b) threats to the data communication service [Kyriakopoulos & Wilikens, 2000]. These threats termed impairments in general manner. An example, in the

context of the substation communications, is electromagnetic distortions that cause interference leading to transmission error rates that can lead to failure of the protection and control system. The failures can propagate, in this context, by causing partial or full interruption of other services such as the delivery of electric power.

6.2.3.3. Means for dependability

Dependable systems need systematic tools as methods and techniques (means) to: a) afford the ability to deliver a service on which reliance can be placed upon and b) reach a confidence on this ability [Laprie, 1992]. The dependability obligates many requirements, for instance, avoiding single point of failure, anticipating faults and reducing their effect to an acceptance level, and implementing fault-handling methods [Avizienis et al, 2001; Melhart & White 2000]. According to [Laprie, 1992], these means are classified into four categories (Fig 6.1):

i- Fault prevention: preventing fault occurrence,
ii- Fault tolerance: providing a service complying with specifications in spite of faults,
iii- Fault removal: reducing the presence (frequency and severity) of faults and
iv- Fault forecasting: estimating the present number, the future incidence, and the consequences of faults.

6.3. Underlining dependability attributes

In the following sections, detailed definitions intend to illustrate main attributes of dependability and to draw attention to their relationship. Some of these attributes shall be detailed such as reliability and availability, though other attributes are defined but considering them beyond of this research scope.

6.3.1. Reliability

The academia significantly contributes to forming the principle definitions where reliability is defined as the probability of a system or a subsystem component functioning correctly under certain conditions over a specified interval of time [Villemeur, 1992]. A precise definition is given as a conditional probability that the system will perform its intended function without failure at time interval [0 , t] provided it was fully operational at time t=0 [Pradhan, 1996].

Reliability is a part of the whole concept of dependability. Accordingly, reliability can be defined as the “ability to perform as required, without failure, for a given time interval under given conditions” [IEC 60050-191, 1990]. The prediction of a component reliability depends on its failure rate. During early life of the component, the failure rate is high, known as infant mortality period. After this period, the component enters a useful life period where failure occur at random times and due to chance. The failure rate becomes nearly constant during the useful life period when a component matures. This period ends when the component starts wearing-out. The failure rate increases dramatically during this time. A bathtub formed curve shall be viewed if the failure rate plotted against time. The exponential reliability function is a continuous density function with respect to time that is used to predict the component (or system) reliability considering constant failures during a useful life period [Chowdhury &

Koval, 2011]. If we calculate survived components of overall used components during a period, then we get the reliability of these components as number of survived components N_s divided by the original population N_o :

$$\mathrm{R(t)} = \frac{N_s}{N_o} \qquad (6.1)$$

Therefore, the original population can be calculated by summing survived with failed components N_f:

$$N_o = N_s + N_f \qquad (6.2)$$

The number of failures is varied and equals the failure rate times the number of components in the existing population, hence:

$$\frac{dN_f}{dt} = \lambda . N_f \qquad (6.3)$$

Then to find R(t) for components with constant failure rate, combining these equations according to [Chowdhury & Koval, 2011]:

$$\mathrm{R(t)} = \frac{N_s}{N_o} = 1 - \frac{N_f}{N_o}$$

$$\frac{dR(t)}{dt} = \frac{-1}{N_o}\frac{dN_f}{dt}$$

$$= -\lambda \frac{N_s}{N_o}$$

$$= -\lambda R(t)$$

$$\int \frac{1}{R} dR = -\int \lambda \, dt$$

$$\ln R(t) = -\lambda t$$

$$R(t) = e^{-\lambda t} \qquad (6.4)$$

One related metric for the reliability is the time to failure TTF that is an expected time until first failure of a non-repairable component. The reliability as a function is actually a failure density function, and the average time for the function is the average time for a failure to occur which is known as the mean time to failure MTTF. In this case, the MTTF is reciprocal of the failure rate, and can be obtained by integrating the reliability function over the entire period:

$$MTTF = \int_0^\infty R(t)dt \qquad (6.5)$$

During useful life, a component exhibits a constant failure rate. Thus exponential reliability function supports determining MTTF as following:

$$MTTF = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda} \qquad (6.6)$$

6.3.2. Availability

Another dependability attribute related closely to reliability is availability. To distinguish between them, availability refers to correct operation at a given time instance [Pradhan, 1996]. Availability is a measure that includes reliability and maintainability metrics, i.e. failure and repair rate, in order to identify operation (uptime) period and downtime.

In sight of dependability, quantifying alternation of failure and restoration permits evaluating dependability via its attributes: reliability and availability [Avizienis et al, 2004].

The most often applied and best-known availability measure is the inherent availability, A_{inh} defined as [Pukite & Pukite, 1998]:

$$A_{inh} = \frac{MTBF}{MTBF+MTTR} \qquad (6.7)$$

Where MTBF is mean time between failures that can be expressed as MTTF added to the mean time to repair MTTR. For a simple component, with constant failure rate, λ, and constant repair rate, μ, the equation 6.7 can be written [Pukite & Pukite, 1998]:

$$A_{inh} = \frac{\mu}{\lambda+\mu} \qquad (6.8)$$

Where μ, repair rate, is reciprocal of MTTR. In this context, availability at a given time means probability of not failed at time t, A(t) = P[not failed at time t].

6.3.3. Safety

Normally, when safety is mentioned risks are thought. Hazardous lead to risky situations when people or property face dangerous circumstances. Safety is the property that a system does not fail in a manner that causes catastrophic damage during a specified period of time [Nicol & Trivedi, 2004].

Safety S(t) of a system at time t is the probability that the system either performs its function correctly or discontinues its operation in a fail-safe manner in the interval [0, t], given that the system was operating correctly at time 0 [Dubrova, 2013].

Safety in practice is application-specific. In power substations, higher voltage levels are safety concern considering protection of workers and equipment. Furtherly, the protection and control shall guarantee safety of property by clearing faults and enabling fail-safe measures during hazardous situations, e.g. arc flash incidents. Safety is a measure of continuous safeness, or equivalently, of the time to catastrophic failure. Hence, safety related systems need availability of their means during demand.

For safety considerations, failures are partitioned into fail-safe and fail-unsafe ones [Dubrova, 2013]. For instance, a fail-safe failure considering main bus (without secondary backup) at power substation that experience a fault of a short-circuit causing overcurrent protection relay to tripping a corresponding circuit breaker, and as consequence resulting into power lines shutdown. Then, the power substation no longer supplying electrical power.

6.3.4. Maintainability

As stated by [IEC 60050-191, 1990] maintainability defined as “ability to be retained, or restored to a state to perform as required, under given conditions of use and maintenance”. Clearly, it is related to maintenance as this attribute depict the ability to be

maintainable. A high degree of maintainability means that repairs consume on average a short time and a little effort. This provides a probability that M(t) = P[repaired on [0,t]]. IEC TC56 and other stakeholders from industry and academia consider maintainability as an attribute for dependability.

6.3.5. Security

Security as an attribute is defined with respect to the prevention of unauthorized access and/or handling of information [Avizienis et al, 2004]. Security can compromise safety of substation systems, although it is not in the scope of this thesis. In terms of electrical power community and for historical reasons, security term is used to indicate safety. However, in this section, we refer to security as cyber security (electronic/digital).

Most threats to security and related issues are intentionally caused by malicious people trying to gain some benefits, get attention, or harm someone [Tanenbaum A. S., & Wetherall, 2011]. Security itself has three properties that help to define it as combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of the unauthorized withholding of information.

For detailed study, [Fries et al, 2010] reviewed the different aspects of security standardizations necessary to build and operate smart grid systems.

6.3.6. Reliability databases and sources of data

The sources of components' failures rate and failure events participate vitally in determining reliability of systems and products. These sources come into form of databases containing failure rates of components. The accountability must be sit on the end user to develop the overall failure rate for the application when precise knowledge about the system and its components is mandatory [Macdonald, 2003]. Some well-known sources of data are OREDA (offshore reliability data) data book and MIL-217F handbook. For the electrical data, the IEEE Gold Book presents failure rates of electrical distribution components. [Cadwallader & Eide, 2010] give a detailed and useful comparison among sources of failure data. [Rausand & Hoyland, 2004] classify hardware reliability databases into database of component failure events, database of accident and incident and database of component reliability.

6.4. The dependability of the IEC 61850

IEC 61850 part 3 section 4 insists on reliability as quality obligation. In this requirement, the standard concentrates on service of communication networks within substation automation systems. From another dimension, regarding the functional requirement of the standard, a backup protection function shall compensate a failed function; same manner a device shall replace other devices in case of failure.

The standard furtherly identifies the communication reliability inside substation levels as data exchange without failure, loss or intolerable delay of critical messages. Specifically, there shall be no single point of failure in substation networks, when failure occur outcomes may lead to damage of substation equipment. When there is no redundant switch (or redundant

path), an Ethernet switch is a single point of failure where all connected devices lose the connection. The loss of communication causes discrepancy of measurement delivery, which leads to missing of protection function. Severe circumstances shall happen when a control action is required in the event of communication loss and existence of critical faults. Therefore, the standard recommends a fail-safe design to avoid undesired control events [Altaher et al, 2016; Altaher et al, 2015; IEC 61850-3:2013].

In this section, computing of reliability and availability for IEC 61850 based process/bay architectures are performed to investigate their dependability. This study helps to understand the functional components and their role.

6.4.1. A case study: description of the process/bay level architecture

A transformer bay, in a distribution substation, is chosen as a case study to evaluate the dependability of an architecture incorporating IEC 61850 based bay components. The power transformer characterizes this distribution substation, i.e. converting 34.5 kV into 13.8 kV, that creates a transformer bay, accompanied by related power equipment, in a small distribution (D1-2) substation architecture [IEC 61850-1, 2010]. In this approach, process and bay levels interact cooperatively (integrated) to achieve the protection scheme. Primary and secondary equipment and devices are identified where primary equipment incorporates main process-level circuits that contain a bus bar, power lines, feeders and transformer, while secondary devices are bay-level auxiliary devices such as IEDs and Ethernet switches. The station-level is not in the scope of this study.

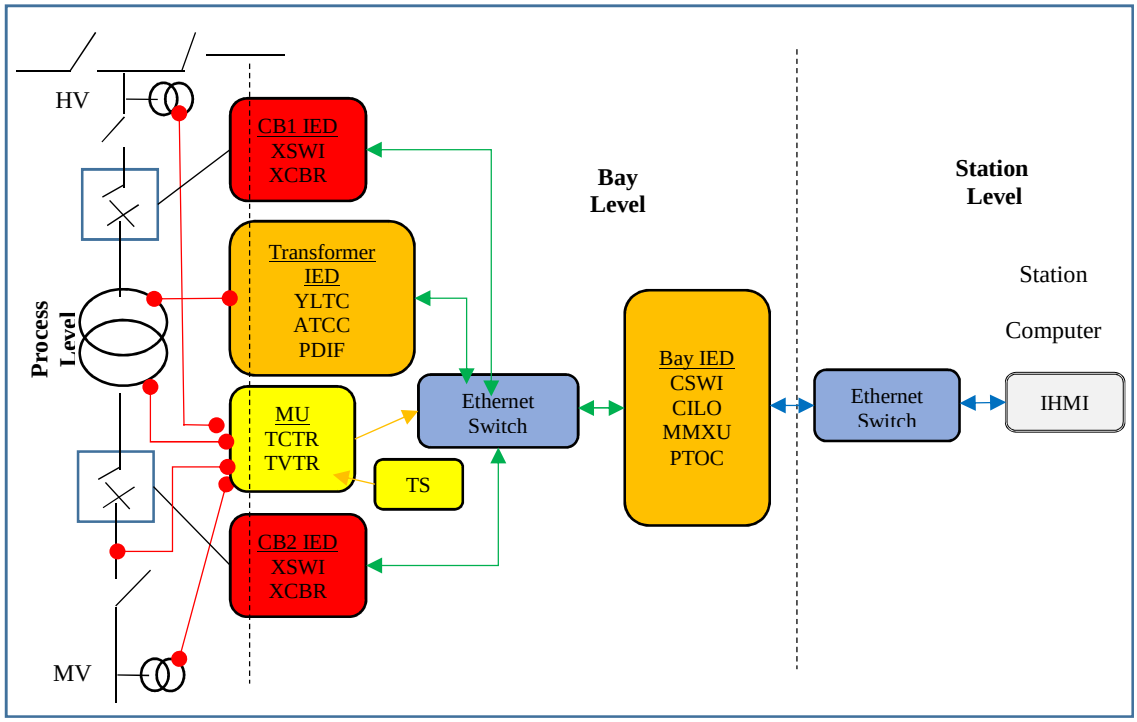


Figure 6.3 Substation communications among different levels, Logical Nodes within IEDs

(Fig. 6.3) presents a single line diagram denoting power switchyard and functional components of both process and bay levels. Electromechanical equipment such as two disconnectors and two CBs are shown, assuming they are commonly used in substation

architectures; however, they are not used in a detailed model. In the other hand, the shown components: bus bar, line, breakers and disconnectors are interconnected to construct the primary switchgear. To control these components, commands can be issued locally via an IED interface panel, or remotely via an Ethernet network. The bay-level would include protection and control IEDs that do handle protection and control functionalities of the process-level, and gather physical metrics and status information about the equipment. These protection and control IEDs are interconnected via a communication network (LAN) composed of Ethernet switches and connected cables (Fig. 6.3). Table 6.1 states the IEDs and related devices that coordinate to achieve the desired protection scheme. Table 6.2 details specific logical nodes (LNs) allocated to each IED, which commonly exist in such purposes.

Table 6.1: The transformer bay protection and control IEDs, and related devices

Device	Name	function
TS	Time synchronization source	To synchronize accurately an MU with a precise time.
MU	Merging unit	To acquire power measurements (analog 3 phase) and publish sampled values (digital) SV frames
ES	Ethernet switch	To connect networked devices in a tree topology
Bay IED	Bay relay (intelligent electronic device)	To coordinate protection and control functions such as interlocking, and to execute protection and control algorithms
Transformer IED	Transformer deferential relay (IED)	To protect both sides of a transformer and to get status data as well as to control online tap changer.
CB1 IED	Circuit breaker controller (IED)	To trip/close/reclose circuit breaker 1 (CB1) near primary side of transformer
CB2 IED	Circuit breaker controller (IED)	To trip/close/reclose circuit breaker 2 (CB2) near secondary side of transformer

Table 6.2: existing of logical nodes in the transformer bay IEDs

LN name	Function	Embedding Device
TCTR	Current transformer (secondary instrument)	MU
TVTR	Voltage transformer (secondary instrument)	
CSWI	Switch Controller	CB1 & CB2 IEDs
XCBR	Circuit Breaker Switch	
XSWI	Disconnector or Earth switch	Bay IED
CILO	Interlocking Controller	
PTOC	Overcurrent Protection	
MMXU	Metrics and measured	
YLTC	Transformer online tap changer	Transformer IED
ATCC	Automatic tap changer controller	
PDIF	Differential Protection	

6.4.2. The system block diagram

In this section, the success of SAS system functionalities is provided by means of required components (Fig 6.3). In order to quantify the reliability and the availability of this system, a reliability block diagram (RBD) is used to draw visually a functional architecture, made of components, and to represent the success path for the transformer bay (the system) indicating all relevant components. For dependability evaluation, the combinatory RBD model is used to illustrate the functional components, and to analyze different system architectures

such as parallel and series. A system works if there is a path of functioning components. The premise that for a service (or system) to be up (available) there must be at least one path across the diagram through components (or modules) that are all up. Thus, redundant modules are shown in parallel, while simplex modules are shown in series [Bauer, E., 2011]. The RBD model is an effective tool that provides flexibility to determine the reliability of a system. Employing this tool is a simple technique to deal with complexity of a system in order to investigate its reliability.

What important is to indicate that a failure of one device in a series structure shall cause a failure of this system. The source of power supply is excluded in this study due to assumption that similar systems benefit from identical power sources. We suppose that communication media (cable) is reliable, i.e. normal case for fiber optics based connections with long life expectations. Evaluation of dependability concerns; IEDs as hardware components, communication network as a component and proposed redundancy of critical components to avoid single point of failure. Functions of protection and control subsystems are allocated in series arrangements, while redundant components shall be represented by parallel arrangements.

The IEDs, merging unit and time source shall communicate through an Ethernet LAN. The main component of this LAN is the Ethernet switch that connects centrally all devices. Ethernet based GOOSE frames exchange protection and control data. In addition, a synchronized MU publishes process level measurements via stream of Ethernet based SV frames.

6.4.3. The reliability and the inherent availability of the system (under study)

Fig 6.4 illustrates an RBD model made of the protection and control components in the system (the transformer bay). In the system the components arranged into series, i.e. redundancy does not exist. Simplicity of the model makes the transformer bay main functions depend on each component, in other words the components must be functioning for the protection and control system to be available. Refereeing to Eq. 6.4, to calculate reliability of a system composed of series components then Eq. 6.9 is used:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = e^{-(\sum_{i=1}^{n} \lambda_i)t} \qquad (6.9)$$

In this equation, the system reliability $R_s(t)$ is calculated assuming independent failure of n individual components where λ_i, is the failure rate of the ith component. The overall failure rate of a system made of components (independent) arranged in a series structure is given by:

$$\lambda_s = \sum_{i=1}^{n} \lambda_i \qquad (6.10)$$

MTTF metrics are depicted in table 6.3, obtained from [Brand et al, 2003; Lindquist et al, 2008], are used as numerical values to calculate dependability attributes; reliability and availability of the transformer bay system shown in the RBD (Fig 6.4).

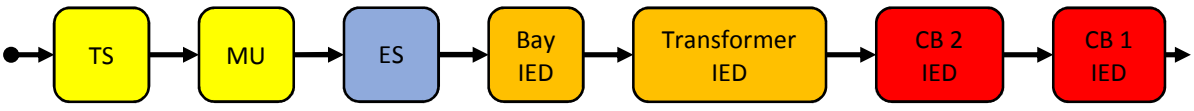


Figure 6.4: Illustrative reliability block diagram of protection and control components in the transformer bay

Table 6.3: MTTF and MTTR of the system components

Component	MTTF (Years)	MTTR (Hours)
Bay IED	150	8
Ethernet Switch	50	4
Merging Unit	150	8
CB IED	100	8
Transformer IED	150	8
Time source	150	4

The failure rate, can be determined according to Eq. 6.6 in order to calculate the system reliability, assuming that mission time t=1000 hours, using Eq. 6.10 and table 6.3 data. In addition assuming there are 8760 hours, i.e. 24 hours x 365 days, in one year to convert MTTF units into hours. The reliability of the basic bay system approximately equals 0.992418, which gives a reliability percentage of 99.242% where the mission time is 1000 hours.

Assuming that components are replaceable, and to calculate the system availability,A_s, MTTF values are used instead of MTBF (i.e. due to small MTTR periods). Eq. 6.11 is used to determine the inherent availability of the bay system by utilizing table 6.3 given values.

$$A_s = \prod_{i=1}^{n} A_{inh\_i} = \prod_{i=1}^{n} \left(\frac{MTBF_i}{MTBF_i + MTTR_i}\right) \qquad (6.11)$$

Where the inherent availability, A_{inh_i} of the ith component determined according to Eq. 6.7, and Eq. 6.11 determines the total system inherent availability. This basic architecture of the transformer bay gets a value of 0,999951, which provides an approximate availability percentage of 99.9951% that means a system downtime equals 25.75 minutes per year.

With the intention of enhancing the system both reliability and availability, the single point of failure from communication view is the Ethernet switch. Hence, a redundant switch is suggested to recover this issue. An active switch can recover the failed one in milliseconds order in this architecture, i.e. using rapid spanning tree protocol in simple topology (RSTP). Consequently, STP, RSTP are not reliable for real-time constraints, i.e. Networked Control Systems, thus adapted protocols are proposed such as dual path over multiple spanning trees [Kubler et al, 2012]. Recently, shortest switch over (recovery) times can be achieved with bump-less protocols such as parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR). These protocols are standardized by the IEC 62439-3 in 2016 to support high availability and short recovery in Ethernet based substation automation applications. The redundancy here is considered as redundant Ethernet switch, which is depicted in Fig. 6.5.

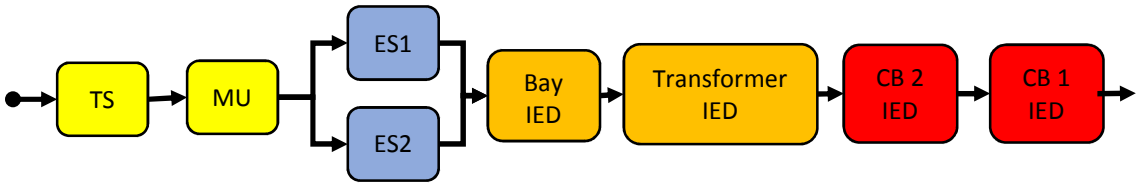


Figure 6.5: Reliability block diagram for the transformer bay system illustrating redundant Ethernet switch

To determine the reliability of parallel components (Ethernet switches), one shall compute the reliability of their structure according to Eq. 6.12 and 6.13 as following:

$$Q_i(t) = 1 - e^{-\lambda_i t} \qquad (6.12)$$

$$R_p(t) = 1 - \prod_{i=1}^{n} Q_i(t) \qquad (6.13)$$

Where the unreliability, $Q_i(t)$, is used to find the reliability of parallel structure. Hence, the reliability of redundant switches can be calculated using Eq. 6.13 and the reliability of this system therefore can be determined using a series structure afterward. The reliability of this system, with mission time t=1000 hours, gets a value of 0.994682, which gives a reliability percentage of 99.468%. To determine the inherent availability of parallel (redundant) components, Eq. 6.14 and 6.15 can be used.

$$U_{inh\_i} = 1 - A_{inh\_i} \quad (6.14)$$

$$A_{inh\_p} = 1 - \prod_{i=1}^{n} U_{inh\_i} \quad (6.15)$$

The inherent availability of the system then can be determined as a series structure. The system inherent availability is determined, equals 0.999960, which has an approximate availability percentage of 99.9960% that means a system downtime equals about 21 minutes per year.

Considering the interlock and inter-tripping schemes, if the functions inside the bay controller stop working then the system status shall become critical. To avoid this situation, i.e. single point of failure for both schemes, a backup IED shall compensate operation of the bay IED in case of failure. In result, the system guarantees high availability, within redundant Ethernet switch and active backup bay IED. Fig. 6.6 depicts redundancy for the Ethernet switch and the bay IED.

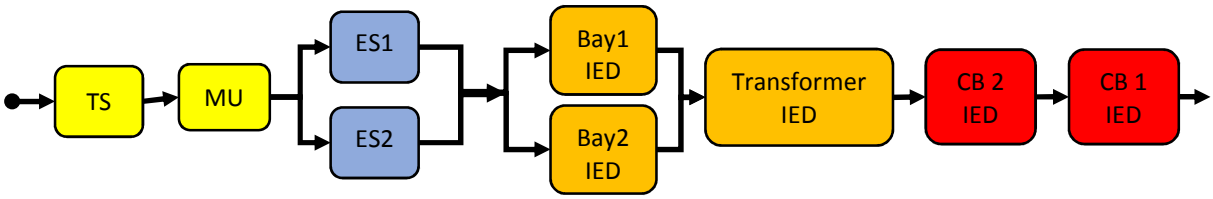


Figure 6.6: RBD diagram for the transformer bay system illustrating redundancy of Ethernet switch and Bay controller

With mission time t=1000 hours, the reliability of this system has a value of 0.995438, which gives a reliability percentage of 99.544%, and the inherent availability is 0.999966, with an approximate availability percentage of 99.9966% that means about 17.87 minutes downtime per year.

Table 6.4 shows a comparison between the three architectures in terms of percentages of reliability and inherent availability computed with at a given time (first year).

Table 6.4: the reliability and availability of the transformer bay architectures

Architecture	**Reliability%** (mission time t=1000 hours)	**Inherent Availability%**	**Yearly Downtime** (1 year=8760 hours)
Basic architecture	99.242	99.9951	25 mins & 45 secs
Redundant Ethernet	99.468	99.9960	21 mins
Redundant bay IED & Ethernet	99.544	99.9966	17 mins & 52 secs

Figure 6.7 shows results of reliability during a mission time, i.e. assuming the system in a useful life cycle.

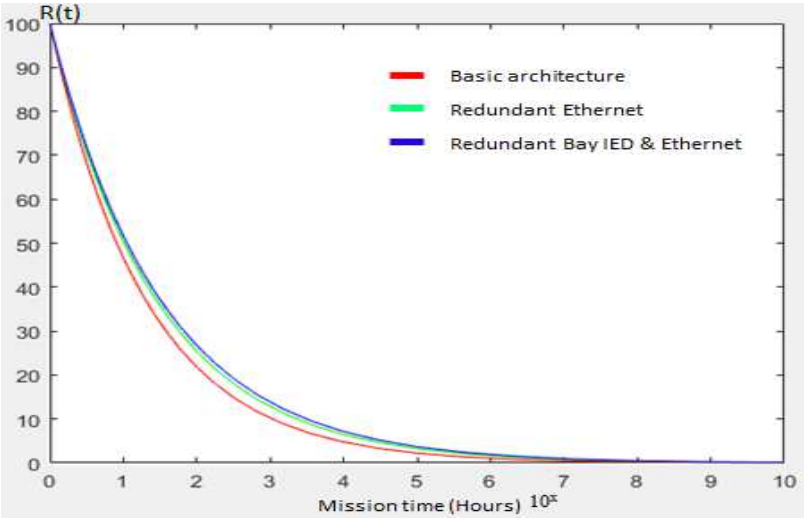


Figure 6.7: simulation of the reliability of the proposed three architectures

By simulating a mission time (fig 6.7) to compare the three architectures, results show that they almost have similar figures. First architecture (red colored curve in fig 6.7) has lowest reliability during the mission time between 10 to about 10^5, while the second (blue colored) and third (green colored) architectures are more reliable than the first, but they shall cost more than the basic architecture. In spite of that, the second and third architectures satisfy the requirement of the standard, i.e. communication requirements, considering that a redundant switch is allocated to avoid single point of failure. The designer should consider other factors such as the information rate and the network bandwidth (see chapter 5) where the protection and control messages compete to reach their destination within the target delay limit.

6.4.4. Discussions and outlooks

The dependability has several attributes, i.e. classified and grouped into taxonomy trees (Fig 6.1 & 6.2). These attributes are termed differently considering the electrical power nomenclatures, e.g. case of dependability and security. The North American Electric Reliability Corporation (NERC) whose mission is to ensure the reliability and security of the bulk power system in North America. In the outlooks of NERC standards, the reliability can be achieved via both dependability and security. In fact, at this point what are mentioned by dependability and security with NERC perspective, represents reliability and safety respectively within the community of dependability in academia. For example, in [Alstom, 2011] high security means that an inter-trip command does not spuriously pick up due to a noisy channel, and high dependability means a blocking or permissive command may easily pass through noise and still be received at the remote line end. In the same manner, dependability and security represent reliability and safety respectively within this context. Thus, in this thesis work, the international community is followed. The reader shall distinguish similarities and differences, e.g. using the term reliability instead of dependability to evaluate communication services in terms of messages delay or loss. Previous sections give a detailed view of the dependability and its attributes. Two of these attributes namely the reliability and the availability were explained through a case study of an IEC 61850 based process/bay level architecture where redundancy proposed to avoid single-point-of-failure.

Another view represents studying related terms are essential, particularly, the functional safety, which is not comparable to dependability. Hence, aiming to make an effort to answer whether dependability and functional safety methodologies are well-suited to Smart Grids or not, i.e. originally thought and questioned by the Smart Grid Joint Group belonging to the European Commission [CEN/CENELEC/ETSI, 2011]. Functional safety and related nomenclatures are clarified in the rest of this chapter.

6.5. The Functional Safety

This section introduces the concept of functional safety and defines the safety related systems. Additionally, related formulas to compute what known as safety integrity level and probability of failure of safety system are explained.

6.5.1. Definitions

IEC TC 65 in its standard IEC 61508 defines functional safety as a part of overall safety that depends on the correct functioning of the process or equipment in response to its inputs [IEC TC65, 2010]. [Von Krosigk, 2000] stated that "In order to achieve functional safety of a machine or plant the safety related protective or control system must function correctly and, when a failure occurs, must behave in a defined manner so that the plant or machine remains in a safe state or brought into a safe state".

Safety systems are designed to be activated upon hazardous process deviations (process demands) to protect people, environment and material assets [Rausand & Hoyland, 2004]. Protection layers are used to mitigate, reduce, separate and control the hazardous situation. The system, that safety function protects, is often referred as equipment under control (EUC).

6.5.2. Safety Instrumented System

[Macdonald, 2003] stated a definition, "*Safety instrumented systems are designed to respond to conditions of a plant that may be hazardous in themselves or if no action were taken could eventually give rise to a hazard. They must generate the correct outputs to prevent the hazard or mitigate the consequences"*, which is originally appeared in a report entitled "UK Health and Safety Executive: 'Out of Control'".

Moreover, Rausand and Hoyland added, "*A safety-instrumented system (SIS) is an independent protection layer that is installed to mitigate the risk associated with the operation of a specified hazardous system*" [Rausand & Hoyland, 2004]. Technically, these systems intend to reduce risks. In this manner other names exist such as trip and alarm system, safety interlock system, safety related system (SRS), etc. where SRS systems is a more general term for any system maintaining a safe state of any EUC [Macdonald, 2003].

6.5.3. Nature of safety related systems

Safety related systems (SRS) require a specific approach for evaluation, analysis and enhancement. These systems are intended to perform safety and safety related functions. From this standpoint, safety is a vital concept to protect people, property and environment.

Normally, a passive safety system is dormant until process situation demands intervention by protection means. This type of systems operates upon demands and called safety systems with low demand mode, while safety systems with high or continuous demands often are active [Rausand & Hoyland, 2004]. Low demand mode systems require periodic functional testing to reveal hidden faults to eliminate failing in passive state.

6.5.4. Highlighting safety in the context of substation automation

Protection functions in substations were found to be safety related with varying levels of risk [Purewal & Waldron, 2004]. These functions construct principal protection layer to prevent hazards. Among these hazards are short-circuits, arc flash and inter-phase short-circuits. A safety function (or protection function) in a substation generally incorporates instrumentations as sensors (e.g. CT/VT or NCIT), logic solvers as controllers (e.g. protective relays and IEDs) and final elements as actuators (e.g. circuit breakers).

Switchgear equipment faults could lead to critical failures such as failing to force sequential clearance of faults. In result, these events cause hazard consequences against substation technicians [Altaher et al, 2016; Gradwell, 2017]. In fact, power automation systems are safety related systems where the protection and control systems are continuously active systems. These systems and subsystems interact to mitigate and control faults in order to avoid (mainly) power system failures or outage, and to protect technicians, switchyard equipment and to lessen effects toward environment.

6.5.5. Risk Reduction and Safety Integrity

To reduce a risk one shall understand difference between hazard and risk. Hazard is defined as "an inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment" [Gruhn & Cheddie, 1998], although a risk is usually defined as the combination of the severity and probability of an event. In other words-- how often can it happen, and how bad is it when it does, thus risks can be evaluated qualitatively or quantitatively [Macdonald, 2003; Gruhn & Cheddie, 1998].

The concept of tolerable risk could mean frequent risks with low severity, but frequent risks are not acceptable when they cause degraded operation of a service considering its dependability. In other terms, acceptable risks are application or process dependent that cause no harm for people, property and environment. Then, tolerable risks can be considered as what are acceptable to society. Another term deals with remained risks is residual risk that remain after all protection layers, including SIS systems. Since that, risk reduction can be defined as reducing EUC risk to an acceptable level. Eq. 6.16 gives relation between unprotected and tolerable risks (risk reduction factor).

$$RRF = \frac{F_{np}}{F_t} \qquad (6.16)$$

Where RRF is risk reduction factor, F_{np} is unprotected risk frequency and F_t is tolerable risk frequency. In low demand mode, the metric average probability of failure per demand, (PFD_{AVG}) is used representing a reciprocal of RRF (Eq. 6.17). Another name for PFD_{AVG} is fractional dead time (FDT) that clearly means the fraction of time when a safety system is dead [Macdonald, 2003].

$$PFD_{AVG} = \frac{F_t}{F_{np}} = \frac{1}{RRF} \qquad (6.17)$$

With the same approach, Eq. 6.18 derives percentage of safety availability, from RRF, which is another metric for performance of a dedicated protection layer (SIS system).

$$SA\% = \frac{(RRF-1)\times 100}{RRF} \qquad (6.18)$$

Safety integrity level (SIL) is a measure of safety performance correlated to risk reduction. In the fourth part of IEC 61508 series; safety integrity is defined as "probability of a safety related system satisfactorily performing the required safety function under all stated conditions within a specified period of time" [IEC TC 65, 2010].

Safety practitioners adopt SIL measure to classify safety integrity. Table 6.5 depicts SIL levels, RRF and safety availability. Obviously, higher SIL level means more reliable (available) safety system. In result, calculating RRF or safety availability shall help to determine the required SIL level. Probability of failure per hour (PFH) signifies high demand mode, when a SIS system is demanded more than once per year, or operates continuously.

Table 6.5 safety integrity levels according to IEC 61508 standard

Safety Integrity Levels	**1**	**2**	**3**	**4**
Safety Availability	90%-99%	99%-99.9%	99.9%-99.99%	Non relevant
Risk Reduction Factor	10 to 100	100 to 1000	1000 to 10,000	10,000 to 100,000
Average Probability of Failure on Demand- PFD (Low rate demand)	$>=10^{-2}$ to 10^{-1}	$>=10^{-3}$ to 10^{-2}	$>=10^{-4}$ to 10^{-3}	$>=10^{-5}$ to 10^{-4}
Failure rate (λ) per hour – PFH (high rate or continuous demand)	$>=10^{-6}$ to 10^{-5}	$>=10^{-7}$ to 10^{-6}	$>=10^{-8}$ to 10^{-7}	$>=10^{-9}$ to 10^{-8}

6.5.6. Failure modes considering safety functions

Safety function operates when demand from EUC releases a threshold value or causing predefined situations. The function shall work as barrier against generated hazards. Mainly, intending to contain and to mitigate the risk. Accordingly, any function that specifically provides safety in any situation is a safety function [Macdonald, 2003].

Essentially, safety systems or its functional components shall suffer failure modes that can be classified into overt failures, i.e. revealed faults, and covert failures, i.e. dangerous failure until it is detected and rectified [Gruhn & Cheddie, 1998; Macdonald, 2003; Rausand & Hoyland, 2004].

Fig 6.8 illustrates main failure modes and their corresponding subcategories. Overt failures normally lead to a fail-safe response from a safety system often involving a plant trip [Macdonald, 2003]. An example of a safe failure is a power outage: imagine a substation that distributes power electricity through four feeders to an industrial facility. This substation distributes electricity via its switchyard system and its protection system is available to control faults. If the protection system suffers a failure that may laid to spurious trip (safe failure) then the result will be power outage (safe-failure). The consequence is that protection and power service are unavailable. Another failure is when the protection system does not respond to clear a short-circuit fault or experiences a hidden fault (dangerous failure), and then say protection system is unavailable.

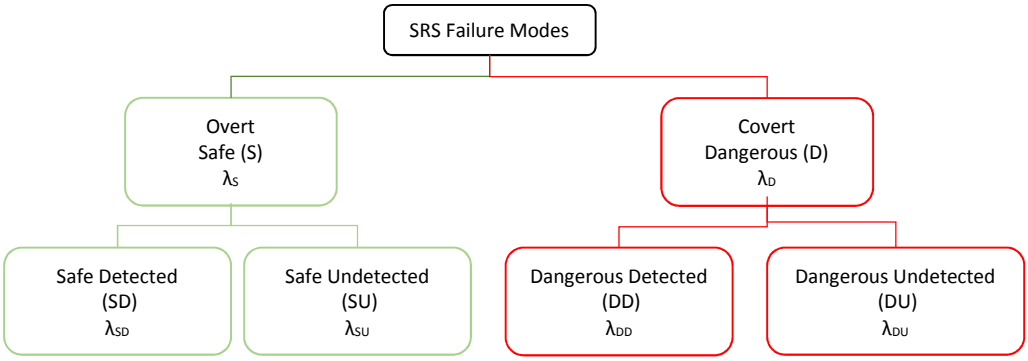


Figure 6.8 classification of SRS failure modes: λ represents failure rate

PFD_{AVG} calculation depends on the covert mode, e.g. frozen IED output, a safety system that does not fulfill its required safety-related functions upon demand when a dangerous failure occurs. In this situation, passive dormant safety system must undergo periodic testing and/or include automatic diagnostic feature.

For instance, a circuit breaker controller (IED) may either fail-to-close due to stuck-open relay contact or fail-to-open due to false-blocking (spurious block). In this situation, redundant or backup protection takes place to clear the fault. Safe failures result in shutdown or interruption of production that tend to be costly and stockholders therefore want to avoid them for economic reasons [Gruhn & Cheddie, 1998].

6.5.7. The role of manual proof-test and automatic diagnostics

Non-detected failures impair safety function goals and designers attempt to overcome these failures through detection techniques. Hence that, tests and self-diagnostics play an important role in revealing non-detected failures during normal operation. Detected dangerous failure is that one detected by automatic diagnostics, while undetected dangerous failure is revealed by manual tests [Gruhn & Cheddie, 1998].

Fast scanning automatic diagnostics can effectively detect the covert failures and put them into the overt failures [Macdonald, 2003]. Logic solvers (controllers) shall incorporate automatic diagnostics to reveal (automatically) hidden failures. This is the case when faults cause a protective relay (an IED) to trip in a SAS, and this relay could feature auto-diagnose to check its I/O (input/output) connections and logic. The fraction of failures that can be revealed by diagnostic self-testing is called diagnostic coverage [Rausand & Hoyland, 2004].

Manual proof-tests decrease the probability of failure per demand because of their role on discontinuing and revealing non-detected dangerous failures, which resulting in reducing (resetting) the failure rate [Macdonald, 2003]. In such systems that combine both the process and the protection, i.e. not separated safety system, automatic diagnostics, within high or continuous demand rate, are parts of the protection system. In this approach, demands on safety function themselves produce a testing procedure.

6.5.8. Metrics for high and continuous demand modes

If the safety function experiences more than one demand per year, or continuous demands, then it shall be treated as a high demand mode function. Handling safety integrity of this function shall take into account: the function structure, the probability of failure per hour and the automatic diagnostics.

The standard IEC 61508 sets SIL levels according to the probability of failure per hour (table 6.5) when the safety function operates on high/continuous mode of demand, and hence, dangerous detected (λ_{DD}) and undetected (λ_{DU}) failures shall be identified in this manner [IEC TC 65, 2010]. To identify these failures, one should quantify the diagnostic coverage of the automatic diagnostics when electronic, electrical, and electronic programmed systems are used, i.e. such as PLCs and IEDs. If the function is constructed as a simple architecture without redundancy then it forms one channel, while redundant architecture is grouped by parallel construction. The channel mean downtime , t_{CE}, therefore can be calculated according to Eq. 6.19:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \qquad (6.19)$$

Where T1 is the proof-test interval of the system, and λ_{DD}, and λ_{DU} can be determined according to Eq. 6.20 and 6.21 correspondingly:

$$\lambda_{DU} = \lambda_D \times (1 - DC) \qquad (6.20)$$

$$\lambda_{DD} = \lambda_D \times DC \qquad (6.21)$$

Where DC means the diagnostic coverage, i.e. automatic diagnostic given by vendor of components, to detect and reveal the dangerous failures. So in order to calculate probability of failure per hour (on continuous demand) PFH, the channel mean down time and the dangerous failures are used in Eq. 6.22:

$$PFH = 1 - e^{-\lambda_D t_{CE}} \qquad (6.22)$$

For redundant components, i.e. parallel structure, with MooN structures, designers shall consider common cause failures, represented by β factor in IEC 61508 [IEC TC 65, 2010]. For 1oo2 structure common cause (CCF) factor β and β_D, i.e. dangerous CCF, shall be used. Hence that, The group of channels, i.e. 1oo2, mean downtime (t_{GE}), therefore can be calculated according to Eq. 6.23:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \qquad (6.23)$$

With above equation, the PFH can be calculated according to the following equation:

$$PFH = 2 \times \left((1 - \beta_D) \times \lambda_{DD} + (1 - \beta) \times \lambda_{DU}\right)^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \times \left(\frac{T1}{2} + MTTR\right) \qquad (6.24)$$

6.5.9. The case study: SIL level of the IEC 61850 process/bay level architectures

The transformer bay (Fig 6.5) includes protection and control functions, i.e. safety related functions. This functions operate in a continuous mode and simultaneously protects the main transformer and controls (tripping/reclosing) circuit breakers and disconnectors.

Identifying the safety integrity level (see table 6.5) requires determining the probability of failures per hour PFH, i.e. continuous mode demand, and describing the safety functions.

It is assumed that statistically only every other failure is a potentially dangerous failure. This relation holds for electronic components when MTTR is significantly less than MTBF and ambient conditions must be met [Siemens, 2011]. For complex devices, such as electronic programmed devices such as IEDs, failure modes are assumed by dividing them into 50% safe and 50% dangerous, then to obtain safe and dangerous failures Eq. 6.25 is proposed:

$$\lambda_D = \lambda_S = \frac{1}{2} \times \lambda \qquad (6.25)$$

Eq. 6.26 determines the overall failure rate λ_P of two redundant identical components, i.e. with a constant failure rate, that approximately equals two thirds of the component failure rate:

$$\lambda_p = \frac{2\,\lambda_c}{3} \qquad (6.26)$$

Equations in section 6.5.8 are used to facilitate identifying probability of failure per hour PFH, alongside these assumptions: a) automatic diagnostic DC covers 90% of dangerous failures, b) proof-test interval T1 is one month, and c) common cause factor β=0.04, and dangerous CCF βD=0.02 for 1oo2 structure.

6.5.10. Results and Discussions

Table 6.6 tabulated the calculated PFH results. These architectures are suitable for safety integrity SIL1 level (see table 6.5), where PFH is in the range between 10^{-5} and 10^{-6}, in continuous demand mode. The first proposed system, basic architecture, has the highest probability of failure per hours among the three architectures. The redundancy improved the system availability where probability of failure per hour is decreased for the second and the third architecture.

Table 6.6: probability of failure per hour for the three architectures proposed for the protection function

Architecture	Probability of failure per hour PFH
Basic architecture	3.8E-06
Redundant Ethernet	2.7E-06
Redundant bay IED & Ethernet	2.3E-06

The failure rate of components affect significantly the dependability attributes of an IEC 61850 based protection and control functions where a substation automation system depends on coordination among these functions. The assessment of the abovementioned architectures includes a simple method to identify components depending on the required logical nodes, i.e. embedded logical nodes in a single IED.

Better performance of a safety function requires low probability of failure per hour (PFH), i.e. high availability of safety function when demands happen. In this way, reliability and availability of a safety function, i.e. protection function, straightforwardly depend on devices failure rate, failure mode and architecture. Hence, devices reliability is an important factor that contributes significantly to the overall function dependability.

Redundancy and suitable maintenance procedures shall optimize the system dependability by increasing the availability and maintainability attributes. Thus, reducing downtime increases availability, i.e. assuming constant failure rates, during long mission period of the system (or function).

One simple approach is to reduce the number of devices that coordinate to achieve a protection function (or scheme) in order to reduce the magnitude of the overall failure rate of this function. This can be reached through integrating many logical nodes into one device, e.g. integrating measurement with protection and control logical nodes; will reduce the number of required devices (IEDs). These IEDs communicate by means of GOOSE dataset to exchange status and substation events. The following section shall inspect the conformity of the GOOSE to the functional safety standardized requirements.

6.6. Analyzing conformity of GOOSE to functional safety requirements

The IEC 61850 motivates using Ethernet based messages to exchange critical information concerning events and status of substation components [IEC 61850-8-1, 2011]. These messages can carry several types of data, which provide flexibility for implementation of protection and control functionalities. These functionalities protect against hazards resulting from power system faults, e.g. short circuit currents, and instable functions that endanger safety of personnel and equipment considering exposure and inappropriate consequences.

The international functional safety standard IEC 61508 parts identify the safety requirements of safety functions and their associated components including the communication network. This section aims to analyze conformity of safety related communication services in modern substation automation systems to the safety integrity requirements. In particular, the conformity of IEC 61850 GOOSE to the functional safety requirements.

6.6.1. The functional safety requirements

The safety should work under regular conditions and must continue during faults presence, which entails designing products and systems to detect protection failure once faults or external impacts exist. Many standards employ safety in design approach that pave the way for the practice of the functional safety to become an independent discipline. This discipline incorporates risk requirements assessment, safety functions and architectures integrity, system operation, commissioning and maintenance of critical safety systems [Gradwell, 2017].

Many standards support these measures among them are: a) ANSI ISA 84.01 b) IEC 61508, c) IEC 61511 and d) IEC 62061. The standards cover certain introduced technologies namely safety instrumented and safety related systems for sectors such as electronic/electrical/programmable electronic, process industry and programmable electronic control. Designers of power system protection and control used similar concepts, e.g. integrity and automatic diagnostics. [Aeiker, 2014; Das, 2012; Gradwell, 2017] made several conclusions that, the functional safety practices can improve electrical safety design and control associated hazards.

6.6.2. The safety communication requirements

The section 7.4.11 of the second part of the standard IEC 61508-2 enforces additional requirements when data communication is used in the safety implementations. The requirements obligates that the safety of the safety function ought to be the identical, when realized with data communication such as fieldbus system. In addition, the standard refers to another standard the IEC 61784 that identifies additional failure modes of communication system and recommends measures to detect and mitigate errors. These failure modes can be raised within connected multiple bus nodes, reception of messages not for the node, co-existence of safety and standard communication, safety-related and non-safety related messages and sensitivity to electromagnetic compatible (EMC) interferences [Borcsok, & Schwarz, 2006]. In certain applications the transmission media, i.e. wired or wireless, such as optical fiber and twisted pair can withstand electromagnetic interference more than wireless radio signals. A list of known causes of transmission errors are given in table 6.7 [Borcsok, 2010; IEC 61784-3, 2010]:

Table 6.7: Data transmission failure modes according to IEC 61784-3, and their possible causes [Borcsok, 2010]

Causes of failures	Repetition	Loss	Insertion	Wrong sequence	Data falsification	Delay
Systematic error HW, SW	*	*	*	*	*	*
Uncalibrated instruments	*	*	*	*	*	*
Use of wrong HW	*	*	*	*	*	*
Crosstalk		*	*		*	
Electromagnetic fields		*			*	
Cable break		*			*	*
Cabling error		*	*		*	*
Wrong aerial arrangement		*			*	
Accidental error	*	*	*	*	*	*
Flash		*			*	*
Aging	*	*	*	*	*	*
Human error	*	*	*	*	*	*
Insertion		*		*	*	*
Overloaded network		*				*
Tapping	*	*	*	*	*	*

To mitigate the aforementioned causes of data errors in communication networks the standards obligates a sort of measures (table 6.8):

Table 6.8: mitigation measures against possible failure modes of the data communication

Failure modes	Description	Required measures
Data corruption	Data within message frame are corrupted due to bit errors	Data check such as Cyclic redundancy check CRC, duplication of message and echo feedback (acknowledgement)
Loss	Bridge devices drop message frames due to communication bit error rate and congestion state	Use of consecutive number, echo feedback. May use watchdog to verify consecutive number
Insertion	Unwanted messages that issued by intention or due to interference	Use of consecutive number, echo feedback and safe source addresses to identify any transmitter
Unwanted repetition	Bubbling from malfunction device or intentional retransmission through invader	Use of a time stamp and consecutive number
Wrong sequence	Congestion and priority mechanism may effect sequence delivery of message frames	Use of a time stamp and consecutive number
Unacceptable Delay	Due to Congestion, network alternative paths and traffic rate messages transfer with long time	Use of a time stamp and timeout. receiver shall check time window
Masquerade	Forged message frames that are not related to safety could cause inappropriate behavior from the receiver	Use of a specific source identifier and safe source addresses to identify the transmitter
Wrong addressing	Message frames could reach unwanted receiver due to wrong destination address	Use of source identifier and data check such as CRC

6.6.3. Analyzing the GOOSE Dataset

The substation events and equipment status are transmitted in a digital form through the Ethernet network. At bay levels protective IEDs embed and enclose GOOSE datasets into Ethernet frames. Within these messages, a status of protection function, e.g. pickup or operate, in one IED can be sent in this circumstance to block or unblock other protection function in another IED. Similarly, an event of circuit breaker failure shall enable tripping of remote circuit breaker attached to a relevant IED as backup fail-safe measure to continue normal operation or safely interrupt a power flow.

In a theoretical study, IEC 61850 communication services are analyzed to inspect parameters of GOOSE frames, the authors concluded that IEC 61850 implements a bunch of remedial measures to detect communication errors although the standard does not report what must be done when communication error is detected [Rocca et al, 2016].

Clearly, the safety functions in substations employ communication networks to deliver status and events for all involved parties according to the protection schemes design. GOOSE messages in this mechanism carry data of safety related function, which is vital for proper operation of the protection system. Table 6.9 inspect, experimentally, features of the GOOSE data that can be used to control and mitigate failure modes of data communications.

Table 6.9: GOOSE inherent measures against data communication errors

Ethernet based GOOSE		**Data corruption**	**Loss**	**Insertion**	**Unwanted repetition**	**Wrong sequence**	**Unacceptable Delay**	**Masquerade**	**Wrong addressing**
Ethernet overhead fields	CRC	*		*				*	*
	Ether type			*				*	
	Source address (MAC)			*				*	*
GOOSE control dataset	GOOSE ID			*				*	*
	APP ID			*				*	*
	Status number		*	*		*		*	
	Sequential number		*	*		*		*	
	Timestamp			*	*		*		
	Time allowed to live			*	*		*	*	
	Quality	*							

The only limitation of the GOOSE message service, in terms of safety communication requirements, is the absence of the acknowledgment technique. In the fifth chapter, a procedure to acknowledge GOOSE receiving is performed, but this measure is not standardized within the IEC 61850 framework. The reason for this is to avoid additional traffic of acknowledgement data. One strategy in this context is to test the GOOSE functionalities integrating the application level acknowledgement and stopping this measure after validation of the design. Researchers recommend certification of the IEC 61850 stack of communication services and related configuration software [Rocca et al, 2016].

6.7.Conclusion

In this chapter, a background about the dependability, its nomenclature and its evolution is given. The dependability taxonomy tree is drawn that include threats, attributes and means of the dependability. Additionally, the functional safety concept is illustrated. The safety functions inside substations are highlighted. Therefore, to answer whether techniques of dependability and functional safety are suitable for Smart Grids, the technique of reliability block diagram (RBD) is used to analysis and identify components of the protection and control functionalities. These functionalities are distributed between the proposed process/bay architectures according to the IEC 61850 based substation levels.

An illustrated case study is given to justify how system components (devices) contribute to an overall system dependability. Three architectures were evaluated to estimate the system reliability and inherent availability before and after adding redundant components. The results obtained showed that redundancy improved the reliability and availability merits, but minor differences are obtained comparing the three architectures in terms of the dependability.

Furtherly, the proposed architectures are evaluated according to the functional safety techniques, specifically the IEC 61508 standard. Results obtained showed that SIL level 1 is attained within a high demand mode computation formulas. The IEC 61850 GOOSE frames are evaluated considering conformity of embedded datasets to the functional safety requirements, i.e. safety communication constraints. Where inspection of the GOOSE data and the protocol mechanism showed limitations due to lack of acknowledgment mechanism.

The limitation of RBD technique, or similar technique such as failure tree analysis, that are only binary state, i.e. success or failure, of components and the systems can be represented and the state of network or GOOSE delay cannot be included in the analysis. Dynamic tests and performance evaluation can observe malfunctions or failures such as inappropriate GOOSE quality, delay or long time of IED processing. Thus, the need for diagnosis is important in this context to identify failure causes.

7. Integration of Diagnosis Aspects to Identify failures' causes of IEC 61850 based SAS

chapter 7 : Integration of Diagnosis Aspects to identify Failures' Causes of an IEC 61850 based SAS functionalities

7.1. Introduction

Classical reliability techniques use combinatorial logic or transition states with events representation. These approaches employ probabilistic methods to estimate the dependability of a system. In fact, these techniques are limited by binary (two) states, e.g. reliability block diagrams and fault tree analysis. These models should be mathematically sound and easy for understanding where decision makers possibly involved in several discussions to develop the system model. Recently, reliability studies evolved considering some uncertain (uncertainty) and randomly fluctuated events. Statistical models are exploited to represent such system events via random variables. Hence that, classical techniques are improved to do so. Within this improvement, the system modeling results in either conditional probability, i.e. system surviving during next year, or deduced numbers, i.e. MTTF or failure rate (Langseth & Portinale, 2007). All these requirements led to increase focus on flexible modeling frameworks. Since that, Bayesian networks (BN) based modeling is a tool that can be used flexibly to diagnose causes of faults and to flexibly estimate the system reliability.

This chapter briefly introduces the applications of Bayesian networks (BN) as diagnosis and prognosis tool where section 7.2 provides relevant studies. Section 7.3 provides bases for BN and section 7.4 syntheses a procedure to build a BN model. The steps of this procedure help to build a model for diagnosis purpose by introducing qualitative and quantitative parts of the required model. Section 7.5 is application oriented where a BN is built and its complexity is reduced by using a canonical model. Section 7.6 discusses results obtained by proposing diagnosis and prognosis scenarios. The validation techniques are proposed and explained in section 7.7. while section 7.8 concludes this chapter.

7.2. Applications of Bayesian Networks

(Weber et al, 2012) reviewed a large number of articles that showed incremental use of BN in dependability, risk analysis and maintenance. They noticed a growing interest focusing on BN modeling in reliability and risk analysis. Therefore, over the last two decades BN modeling approach witnessed increased trend in dependability studies. BN based modeling becomes a popular tool for modeling many kinds of statistical problems (Langseth & Portinale, 2007). (Barlow 1988; Almond, 1992) have been firstly performed BN modeling for reliability applications. All these applications involve top-down approach (prognosis), i.e. forward inference from cause to effect, where prior probabilities of root nodes, e.g. subsystem components states, are given to deduce the state of the final system variable, e.g. system availability or reliability. In reliability studies, BN models can handle multistate parameters, common environment conditions, uncertainty and coverage factors (Langseth & Portinale, 2007; Torres-Toledano & Succar, 1998). BNs can incorporate both qualitative and quantitative

measures such as human aspects that are often modeled via qualitative knowledge while technical aspects are often represented by quantitative measures and metrics such as components failure rates and mean repair time (Røed et al, 2009). In addition, modeling dynamics, i.e. temporal dimension, of systems is addressed by BNs. For instance, a sequence of continuous events, cause-effects evolution, operational effects and environmental influences can be represented through dynamic Bayesian networks DBN, for details about DBN algorithms a good reference is (Murphy, 2002). Langseth stated that BN modeling method is not the solution to all problems, but it seems to be very relevant in the context of complex systems (Langseth, 2008).

Another noticeable, application of Bayesian Networks, research works are the use of BN (inter) causal reasoning capabilities for diagnosis; where bottom-up (backward inference) approach is performed, i.e. diagnosis root causes via observing probability (evidence) of a system failure (effect) (Oniśko, 2003). With this approach, the diagnosis process aids to identify the root cause of a system failure given a set of system observations that may include test results, historical log data, error messages, sensor reading, monitoring data for subsystem operation, etc.

A study that investigated complex process to detect failures and to identify causes. This study classified causes according to both supervised and non-supervised diagnosis with BN model based multivariate card, which was implemented to diagnosis Tennessee Eastman process (Verron, 2007). This study later integrated the notion of distance rejection to detect and to diagnose faults, simultaneously (Verron et al, 2010). Additionally the work extended to use a data-driven method, i.e. system tests and measurements, which is then associated to another model-based method, i.e. the system analytical model. These two methods are first modeled under a Bayesian network (conditional Gaussian network), and then combined to evaluate the system state (Atoui et al, 2016).

7.3. Bayesian Networks Basics

A Bayesian network is a compact representation of a multivariate statistical distribution function (Pearl, 1988; Cowell et al, 1999, Jensen, 2001). The BN model encodes the probability density function governing a set of n random variables $\mathbf{X}=(X_1, X_2, \ldots, X_n)$ by identifying a set of conditional independence statements jointly with a set of conditional probability functions.

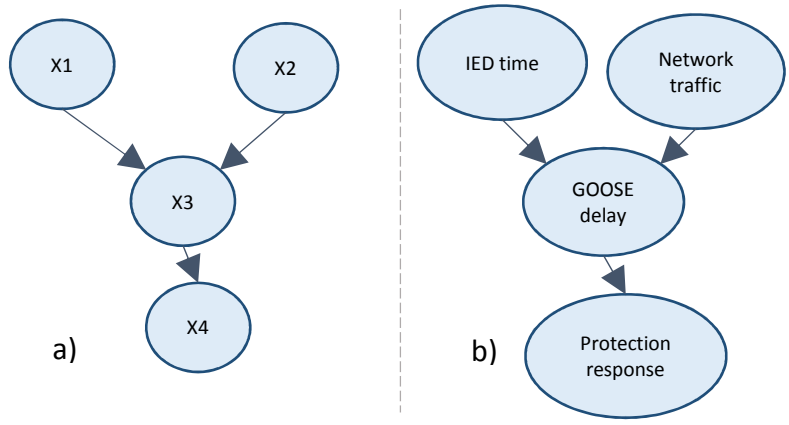


Figure 7.1: a) A graph as a qualitative part of a Bayesian network, b) An example related to our BN model

The BN model consists of a qualitative part, which is represented by a direct acyclic graph (DAG) where nodes reflect random variables and arcs represent relation (dependency) among these nodes, and a quantitative part that is represented by a set of conditional probability functions (CPF).

A given example in figure 7.1 shows a qualitative part of a modeled BN. The figure shows four nodes where nodes X_1 and X_2 represent parents of node X_3. Moreover, X_3 is a child of the former nodes, similarly, X_4 is a child of X_3 and clearly one can say that X_3 is a parent of X_4. For instance, the relation $Pa(X_3) =\{X_1,X_2\}$ represents that parents of X_3 are X_1 and X_2, while $Pa(X_4) =\{ X_3\}$ and descendants of $X_4=\emptyset$ and non-descendants of $X_4 = \{ X_1, X_2, X_3\}$. In this way, conditionally independence statements can be retrieved where we say that X_4 is conditionally independent of $\{ X_1, X_2\}$ given condition of $\{ X_3\}$, which written $X_4 \perp \{ X_1, X_2\} \mid X_3$. In the Fig 7.1b, the protection response depends on the GOOSE delay, which depends on both IED processing time and network traffic. The direct dependency in this example is depicted by direct arc from parent node to a child node. Conditional independency relationships are bases for inference (BN inference) where algorithms are invented to update probabilities through conditional probability functions (Pearl, 2014). The relation f(x|y) denotes conditional probability function of x given y. Considering random variable nodes x_i we get $\{f(x_i|Pa(xi)\}$ where i=1,2,…,n. then calculation of joint probability functions as:

$$f(x_1, \dots, x_n) = \prod_{i=1}^{n} f(x_i|Pa(x_i)) \qquad (7.1)$$

Root nodes (parentless) of BN shall have prior probabilities (a priori) while descendants normally have a conditional probability table (CPT) regarding their parent or parents. BN modelers shall identify each CPT via selecting parametric formula for each (xi|Pa(xi)) and determining values for all parameters given conditional probability functions as in table 7.1.

Table 7.1: A conditional probability table represents probability of X3 given states of X1 and X2

X_1	X_1		X_1'	
X_2	X_2	X_2'	X_2	X_2'
X_3	$X_3\mid X_1, X_2$	$X_3\mid X_1, X_2$'	$X_3\mid X_1$', X_2	$X_3\mid X_1$', X_2'

Where X_1' is complement of X_1 and so for other variables.

7.4. The Procedure of modeling by Bayesian Networks

Clearly, BN modeling procedure shall involve many interactions between the BN modeling expert and the domain experts where the later answers the BN expert's queries in such forming an expert knowledge to build the structure of the BN model. The domain expert can understand principles of the BN modeling through these interactions that result in elaboration and elicitation of conditional dependency (and independency) among model variables. In causal models, normally arcs represent direction from cause to effect where this causality relationship speeds up building BN

diagnosis based models. In this manner, the BN modeling has feasible advantages in which interactions between BN expert and domain experts become a feasible way for communication, e.g. implementation of causality and interpretation of objective probability such as events frequency. Constructing a model based on BN mostly entails three common tasks: a) identifying model variables and their states, b) draw a structure that links these variables according the domain application and c) providing probabilities to quantify the relation between the model variables.

7.4.1. The BN model building steps

According to (Torres-Toledo & Succar, 1998; Langseth & Portinale, 2007; Choi et al., 2011) building of BN shall incorporate predefined steps. This procedure involves interactions among domain experts, i.e. system relevant experts, and BN expert where they build a BN model through knowing the formal structure of the system. Additionally, other important sources of information for building the BN model are statistical data through experiences, evaluation tests and answers of domain experts to appropriate questions (expert knowledge) in order to build the target model (Choi et al., 2011). To synthetize these tasks into a procedure, the modeling activity are summarized into the following steps:

1- Step 0: identify the system boundaries that shall be incorporated into the BN model.
2- Step 1: determine the random variables that represent a range of continuous values or states of discrete variables. These variables become nodes into the Bayesian network model.
3- Step 2: build a graphical structure involving causal edges (of arcs) to connect variables in order to represent qualitative conditional dependency/ independency (lack of arcs). In this step BN expert interacts with domain experts to reveal relations in order to avoid inappropriate (void) edges.
4- Step 3: identify quantitative relationships among BN nodes (variables) by determining the conditional probability tables, to acquire all conditional probability functions within these tables, considering prior probabilities of root nodes.
5- Step 4: verification via sensitivity analysis as well as testing the model in order to refine and redefine either the parameters (variables) or the structure of the target BN model.

Additionally, data learning can be used to automatically build BN structure as well as learning the model parameters. In our work, we will use the developed reliability block diagram (see chap 6 § 6.6.4) as a basis for identifying the system's components and their functionalities (formal structure of the system). In addition to the system formal structure, a risk analysis tool that is the failure mode and effect analysis (FMEA) will be used to identify estimated failures of the protection schemes due to operation malfunctions or component faults and their effect on the system services. The BN model will exploit the data obtained during the experiments of dynamic tests and performance evaluation (see detailed information in chapter 4 and 5).

7.4.2. Risk analysis

Principle techniques of the risk analysis normally assist identifying occurrence frequency of the risks and related severity consequences due to their effects. Among these techniques are risk matrix (grid), hazard analysis, hazard and operability study HAZOP, layers of protection analysis LOPA, and failure modes and effect analysis FMEA that has extensions enabling determining criticality FMECA and diagnosis measures FMEDA (Carlson, 2014). Table 7.2 shows an example of FMEA analysis where failures and their effects can be easily distinguished.

Table 7.2: An example of failure mode and effect analysis (FMEA)

The system: protection and control system			Life-cycle: testing of the system design		Date: 13/12/2016 Time:16:00-18:00			
Equipment, component/ Function	Failure				criticality		RPN	Comments
	mode	causes	Local effect	Final effect	O	S		
Ethernet Network switch: Data forwarding	High delay	High network traffic	Delayed event messages	Long time clearance of Delayed power faults	3	8	24	Software updates, file transfer could cause higher traffic loads
	Data loss	High network traffic	Loss of event messages	Damage of equipment due to non-clearing of power faults	2	9	18	Software updates, file transfer could cause higher traffic loads, also switch errors (faults) would cause same failure.
Ethernet media: Ethernet frames transport	Data alteration	Noise, crosstalk	Modification of event messages	Malfunction of the protection and control	2	9	18	Wireless media is prone to electromagnetic radiation, also switch fault or cyber-attacks can cause so
Transformer protection IED: to protect the main transformer from overloads, power faults	No events data	Missing of suitable configuration	Non-clearance of power faults	Damage of equipment due to non-clearance of fault	1	9	9	Users omit configuration of an IED protection settings

The above table illustrates main parts of the FMEA analysis. This tool provides useful information about failures cause-effect relationship that would help to classify critical failures according to both occurrence and severity. The ranked priority number (RPN) column represents criticality, which is a multiplication of occurrence (O) and severity (S) values. These values range from 1 to 10, where severity rank 1 means non-noticeable effect while 10 means potentially safety-related effect on equipment or operators, similarly occurrence value (frequency) ranges from 1 to 10 where 1 means very low and 10 means very high (Carlson, 2014). Besides, FMEA helps to understand system functionalities, their requirements and performance constraints. Therefore, results of this analysis allow identifying important components and their critical relevance to the system operation.

FMEA aids to model causal relationships between cause and failure mode from one side, and failure and its effect from other side. This causality helps to build the Bayesian network structure.

7.4.3. Where do the numbers come from?

Building a model of Bayesian network involves qualitative and quantitative parts; the last part appears as a more daunting task because it requires obtaining objective probabilities (frequencies) and quantifying the relation between child nodes and their parents. The most common sources of probabilistic information are (statistical) data, literature about the domain and the knowledge of domain experts (Druzdzel & Van Deer Gaag, 2000). In this manner, building the BN model is a process that go over the systematic modeling steps (see section 7.4.1) until accomplishing the required accuracy. The quantitative values are important to identify prior probabilities for the random variables (BN nodes). Hence, these parameters are essential for determining (inferring) posterior probabilities over the condition probability distributions, i.e. conditional probability tables. Data collection should be achieved carefully because biases of data will lead to inaccurate performance of the BN model (Lucas et al, 2000). In dependability applications, most reliability databases include abundant probabilistic information (parameters) that help building BN models where components failure modes and rates reported. This information can be used for elicitation of prior probabilities. In other hand, modern innovative systems can be considered one-kind systems where past reliability data is not available; hence, uncertainty is obvious in this condition. Finally, knowledge and experiences of domain experts become the only source of probabilistic information. Elicitation of probabilistic data from experts shall help to tune parameters obtained along with verifying the conditional dependency (and independency) among these parameters.

I learnt, from dynamic tests and the performance evaluations (in previous experiments), the relation between system variables in the system platform and the test-bed experimental data that explains clearly the states and ranges of the collected data. Calibration of the probabilistic values in the BN model shall reduce imprecision of diagnosis. (Henrion et al, 1996) argues that diagnosis via using BN is insensitive to imprecision in probabilities. In addition, (Oniśko & Druzdzel, 2013) concluded that as long as they avoid zeroes among model parameters, diagnostic accuracy of Bayesian network models does not suffer from decreased precision of their parameters.

The BN model can be subject to sensitivity analysis through varying the model parameters to determine the accuracy of numbers in order to get satisfied results. Also varying simultaneously all probability distributions shall reveal the overall BN model reliability behavior and output, which is known as uncertainty analysis (Druzdzel & Van Der Gaag, 2000).

7.4.4. Reducing the complexity of the CPT and the structural relation

Possibly the BN model could contain tens to hundreds of random variables (nodes) that may entail up to thousands of probabilities, i.e. parameters of conditional probability tables. This parametrizing depends directly on the BN graphical structure where each node may enlarge exponentially the probability derivation (propagation), e.g. n states of parents produce 2^n states for their child node CPT. Additionally, Bayesian belief updating (inference) involves propagation of observed evidence, i.e. updating probabilities given observed variables. This process computationally is a complex

polynomial problem (Cooper, 1990), i.e. NP-hard problem, that require reducing the model complexity by specific techniques.

In order to reduce these probabilities (and relevant CPT), two techniques exist either reducing the graph structural relationship, or reducing the parameters of the probability distribution (CPT parameters). For instance, the first approach comprises either removing arcs between nodes where weak dependencies exist (Van Engelen, 1997), or divorcing parent nodes, i.e. adding intermediate nodes (Olesen et al., 1989). While reducing the parameters can be performed via using canonical models such as Noisy OR and/or Noisy MAX gates (Díez, 1993; Henrion, 1989; pearl, 1988). Using the canonical models assumes satisfaction of causal dependencies between child node and its parents' nodes. In this occasion, the complexity of parametrizing changes from exponential (2^n) to linear (n) relation between a child node and its parents (Oniśko & Druzdzel, 2013). This reduction of complexity will help to reduce the overwhelming effort to parametrize the BN model.

7.5. Building the Bayesian network model

To build the BN model, we start identifying the failures cause-effect through using a simple FMEA analysis. The system understudy is the substation automation system based on IEC 61850 communication services where both SV and GOOSE assumed as Ethernet based messages to deliver measurements from the process level to the protection and control functions at the bay level. This system has three protection schemes namely interlocking, blocking and intertripping (see chap 4 § 4.3.3) that use IEC 61850 GOOSE to coordinate functionalities between protective relays (IEDs).

7.5.1. Causal relationship

Failures can happen in communication networks according to some susceptible elements. For instance, in wireless networks transmission of data is more exposed to inference and electromagnetic radiation than wired media (cabling), while high traffic loads can affect both wired and wireless networks. Network perturbations indeed affect the quality of messages delivery service. Figure 7.2 shows an example that shall help to identify causal relationship, between failure and corresponding causes in communication networks. The figure illustrates commonly pragmatic failure modes in wired Ethernet networks. The figure links these failures to most known causes, e.g. the switch error refer to hardware, software and configuration errors where users may unintentionally make mistakes during setting of some parameters. Even though attackers intentionally jeopardize network systems to achieve specific goals.

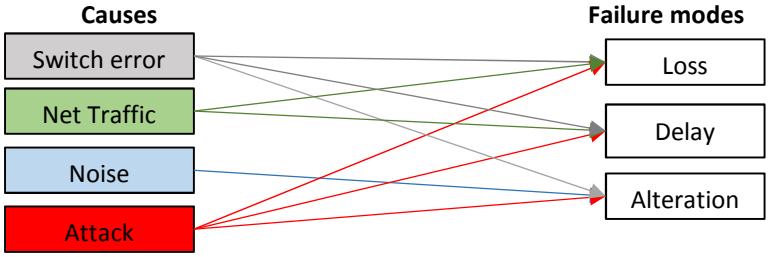


Figure 7.2: an example of communication network failures and their causes

Delay and loss may happen because of queuing and buffering mechanism at Ethernet switches, while out of order delivery occur due to service policing and scheduling such priority mechanism. In addition, within large and multi segment LANs frames can take alternative paths, especially with multicasting modes of transmission, e.g. publisher/subscriber pattern. The network traffic indeed is a main factor that shall affect networks quality of service, similarly noise such crosstalk can alter frames bits resulting in drops/ignoring of data frames according to frame check measures, e.g. cyclic redundancy check CRC.

7.5.2. Identifying (parametrizing) the BN model variables and building its structure

Models of Bayesian networks can represent causal relationships. A model that employs a BN helps to diagnose and understand the relation between cause of communication failures and their effect on protection schemes functionalities. Based on the system diagram (RBD, see chap 6 § 6.6.4) we start first drawing the BN structure as functional components and status of network due to some perturbation (causes) as risk factors. Then we link every cause to corresponding failure mode or many causes to many failures. Finally, the effect of failure is linked to the final consequence.

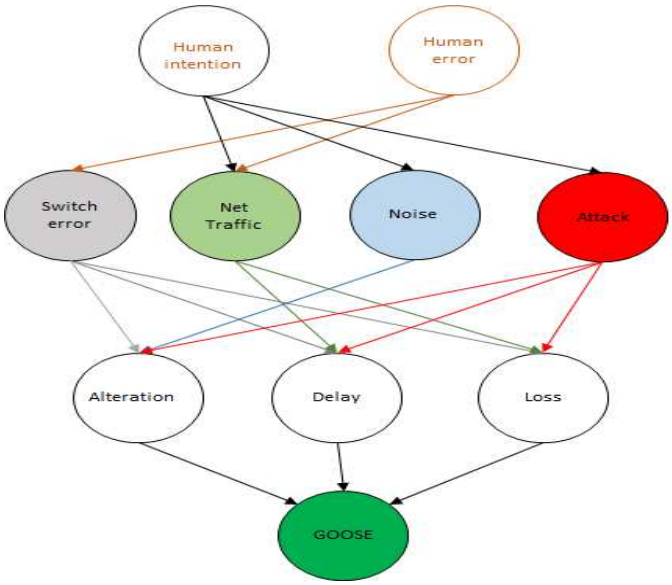


Figure 7.3: First iteration to build conceptual BN model: communication failure modes are divided into three nodes: alteration, delay and loss

Using brainstorming and knowledge from the platform experimental observation and collected data, the first model becomes sub-model of the developed BN model (Fig 7.3). In the first iteration of building the model, the lack of network service's quality is divided into three failure modes: frames loss, delay and alteration (fig 7.3) because they are independent states, i.e. existence of a failure does not prohibit other failure. To explain the variables of the BN model table 7.3 includes description of every variable in the first model.

Table 7.3: causes, failures and their effects (consequences)

Variable	Causal type	description	Example
Human intention	Root cause	Intention here is prior decision to cause harm for the network service	Injection, DOS, insertion and cable cut
Human error	Root cause	Without intention a person can make configuration or operation error such as misconfiguration of an Ethernet switch or huge file transfer	Configuration error Operation error
Attack	Cause	Related to human intention to spoil or make a damage	Cyber attack
Noise	Cause	Due to environment or activity that may produce electromagnetic or pulsed noise	Electromagnetic interference from electrical motors
Network traffic	Cause	Traffic load that may lead to long frames delay or loss	Large file transfer, device software update or upgrade
Switch error	Cause	Due to bad configuration	Bad VLAN configuration
Loss	Failure	Loss of GOOSE messages	Previous causes
Delay	Failure	Long transfer time	Previous causes
Alteration	Failure	Payload data modification	Previous causes
GOOSE	Effect (consequence)	Efficiency status of GOOSE Service.	Loss, delay or alteration

In addition, we identified the consequence of these failures on the GOOSE service, i.e. quality of GOOSE service due to Ethernet network status. In fact, we can classify the nodes into three categories a) observation nodes include causes that can be represented by risk factors, b) auxiliary nodes that could include symptoms, test results and failure modes and c) final consequence (effects) as target nodes (evidences). To estimate final effects of failures table 7.4 highlights some consequences on a protection scheme (reverse blocking).

Table 7.4: consequences of communication failure modes (quality of the GOOSE service) on protection scheme.

Failure	Event	Consequence
Delay	During power fault and due to delayed blocking message (reverse blocking) the result a false trip at upstream bay.	Economic due to loss of power supply (power outage)
Delay	False blocking after tripping	IED device fallback, i.e. which receives blocking, and loss of protection that may lead to safety hazard
Loss	During power fault and due to delayed blocking message the result is a false trip at upstream bay.	Economic due to loss of power supply (power outage)
Loss	Long clearance time for intertripping due to loss of GOOSE data	Safety hazard
Loss	Interlocking is not coordinated due to loss of switchyard status data, e.g. circuit breaker or disconnector position	Safety hazard
Alteration	Long clearance time – no trip	Safety hazard
Alteration	False trip	Economic due to power outage
Alteration	Interlocking is not coordinated due to false switchyard status data	Safety hazard

Table 7.4 focuses on and illustrates effects of network perturbations on the quality of GOOSE service. In fact, external faults can cause failures, e.g. faults of hardware or software components. In the second iteration, we rebuild the model due to our scope that we only focus on technical causes of failures due to lack of knowledge about the sociotechnical risk factors (human error and intention).

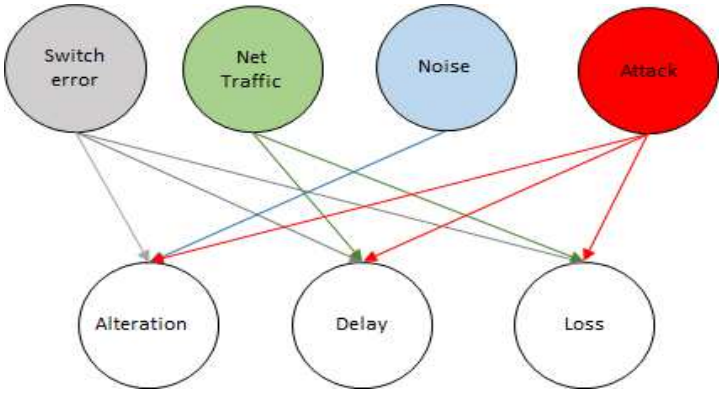


Figure 7.4: BN model shows direct link between causes and failure.

For simplicity, we assume both human error and human intention can contribute to failure causes. Then I neglect the sociotechnical layer (human contribution). These causes are not included in this study scope due to above mentioned reasons. What is important for diagnosis in this sub-model (communication case) it to classify direct and indirect causes of GOOSE frames loss, delay and alteration that affect the communication service and leads to inappropriate consequences. Figure 7.4 shows direct relation between cause and failure modes where several causes are distinguished by different colors.

Table 7.5: metrics used to identify failures during testing and performance evaluation

Metric	Value	Description
Loss rate	$<10^{-4}$	frames loss must be less than this value during perturbation such traffic loads or noisy interferences
Delay	<3ms	GOOSE transfer delay and IEDs processing must be less than this value
Alteration	$<10^{-4}$	Unwanted commands (altered GOOSE frames) must be less than this value

In our approach, we build the BN model (the structure) from the formal system structure (functional composition) as described early in this section. Other possible approaches are to build the model structure by means of: a) system data learning, i.e. automatically identify nodes and causal relationship, and b) combining both data learning and expert knowledge about the formal system structure.

Quantifying the parameters (BN nodes states and values) means determining the numbers. In this manner, frequencies of failure modes are derived from experimental results. Therefore, drifts from values of reference (see table 7.5), i.e. the protection and the control communication requirements, shall be considered as failures. Values of failure nodes (states) can be represented by prior probabilities driven from collected data. Finally, causes can be classified according to conditional probabilities tables (relation to failures). The computing of the posterior probabilities is backward inference

(diagnosis) to classify causes of the modeled failures (likelihood of causes). Large amount of data was collected. This data includes frequencies (statistical) data that are derived from several sources such as: a) IEDs operation and failure log files, b) ICMP request-response log file, c) captured data with a network analyzer (Wireshark) that comprise both GOOSE and SV quality metrics, e.g. delay and loss, and d) Overall data traffic captured with the SPAN port from the Ethernet switch. This data covers all experimental scenarios that consists of both non-VLAN and VLAN enabled priority data frames, i.e. GOOSE messages. The purpose here is to determine prior probabilities and to identify the relation between the traffic and the delay in a form of conditional probability table.

The BN model in this phase should be elaborated with pencil and paper via iterations, after that can be modeled through available software tools. There are many BN software packages for instance, SAMIAM, BNT Matlab toolbox, Microsoft BNTX, GeNIe and SMILE. In this research, I used the last two tools where SMILE stands for (Structural Modeling, Inference, and Learning Engine), which is a fully portable library based on C++ language classes and GeNIe is the graphical interface for decision-theoretic models. Both tools developed at The Decision Systems Laboratory at the University of Pittsburgh and become commercial products of BayesFusion, LLC.

Fig 7.5 illustrates a snapshot of the GeNIe graphical interface where a part of our model is shown. The graphical interface allows rapid and flexible modification of the BN structure.

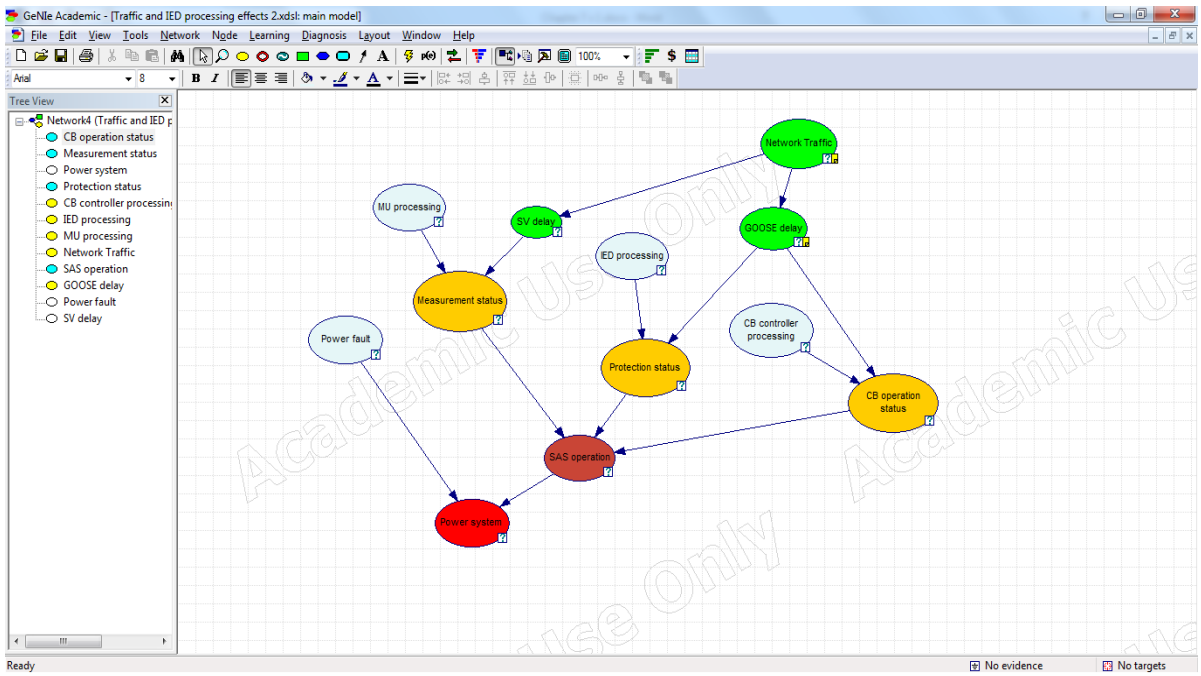


Figure 7.5: the GeNIe graphical interface: a part of our BN model is shown.

The figure shows Ethernet network related nodes in green color, protection and control components in light blue, status of substation automation functions in orange, status of the overall substation automation system in purple and the power system status in red. In this model, we made assumptions that circuit breaker equipment, network cables and electrical power supply are reliable due to their existence in most substations. Our objective here is to observe the future SAS functionalities and their dependency on

the IEC 61850 enabled services. These services comprise information exchanges, via an Ethernet network, between SAS components, such as:

a) Power quantities measurement shall be transferred from the MU at the process level to the bay level by means of sampled values, i.e. non-conventional instrumentation (NCIT) connected to Merging Units,
b) Protection and control functions, simultaneously achieved by multifunction IEDs, receive measurements by means of SV datasets and issue GOOSE events according to these measurements.
c) A circuit breaker controller, i.e. an IED embeds a network interface to exchange substation events, will receive implicit control commands via GOOSE datasets.

Finally, the power system status will be observed through modeling an electrical power fault, i.e. modeled by BN node, to represent presence or absence of short-circuit or power transients. In addition, target status of the power system will be derived from the power fault node and the SAS operation state (nodes at the bottom of the BN model).

To learn parameters data learning is done where sources of collected data (data files) are saved into files types include text and comma separated values (CSV). Figure 7.6 shows learning parameters process from a data file where mapping of the BN variables (nodes) and their states to columns and values of this file. The learning is performed with random variables initialization using EM Algorithm (Expectation Maximization Algorithm), which has roots back to works of (Dempster et al., 1977) and Lauritzen, 1995). In addition, the continuous variables such as traffic rate and GOOSE delay are discretized into specific states, e.g. traffic node states are low, medium and high.

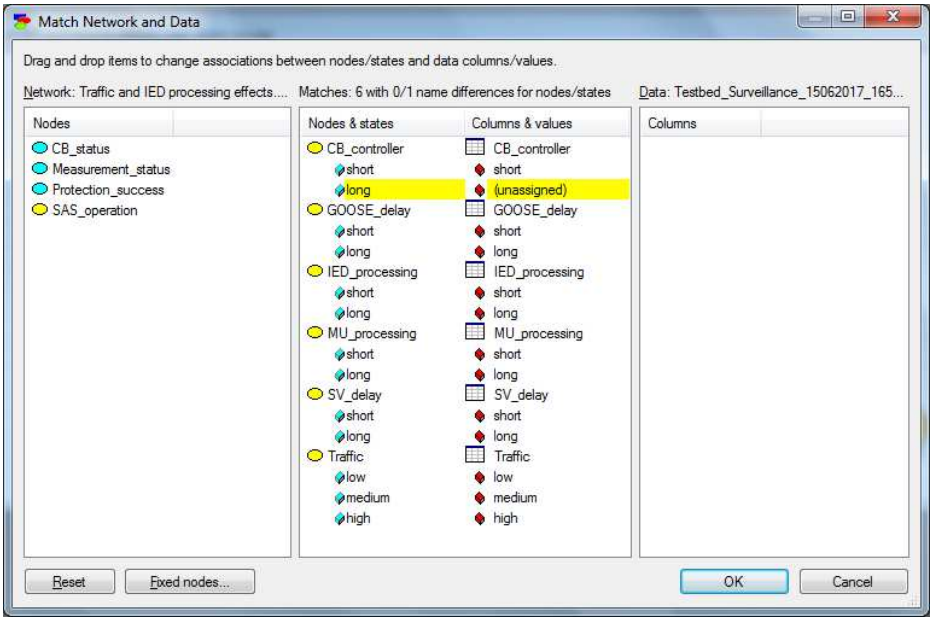


Figure 7.6: learning the BN model parameters from the experimental (monitoring)

7.5.3. Application of Noisy MAX gate

To reduce the conditional probabilities tables we used the canonical model Noisy-MAX (Noisy-OR). This gate approximates the CPT probability according to interested states of parents, which directly change the relation from exponential to linear according to states number. Judea Pearl explains that Noisy-OR gate is the simplest and most intuitive canonical model (Pearl, 1988). Some assumptions shall be satisfied to make this model applicable, in which causal relationship exists, where a) each $\boldsymbol{X_i}$ causes has a probability $\boldsymbol{P_i}$ and b) each cause is independent of the presence of the other causes. In other words, the causes of a failure $\boldsymbol{Y}$ are causally independent. These conditions help to reduce the CPT input to just $\boldsymbol{n}$ parameters from $\boldsymbol{P_1}$ to $\boldsymbol{P_n}$, where $\boldsymbol{P_i}$ provides that the failure will be true if any cause $\boldsymbol{X_i}$ exists and other causes are absent, i.e. $\boldsymbol{P_i} = Pr(\boldsymbol{Y}|\ \overline{\boldsymbol{x_1}}, \overline{\boldsymbol{x_2}}, .., \boldsymbol{x_i}, .. \overline{\boldsymbol{x_{n-1}}}, \overline{\boldsymbol{x_n}})$ where $i \neq j$ and all causes, except $\boldsymbol{X_i}$, are negated. This gate will derive the complete CPT of the failure $\boldsymbol{Y}$ given its parents (Oniśko, 2003). An extension to the Noisy-MAX model, to capture all modeled causes of the failure, supposes a leaky state where absence of all the failure's causes. The leaky probability $\boldsymbol{P_o}$ represents occurring of the failure spontaneously when all other causes are absent, i.e. combined effects of all unmodeled causes of the failure $\boldsymbol{Y}$ that is given by $\boldsymbol{P_o} = Pr(\boldsymbol{Y}|\ \overline{\boldsymbol{x_1}}, \overline{\boldsymbol{x_2}}, .., \overline{\boldsymbol{x_i}}, .. \overline{\boldsymbol{x_{n-1}}}, \overline{\boldsymbol{x_n}})$ (Díez & Druzdzel, 2006; Bolt & Van Der Gaag, 2010).

The use of leaky Noisy-Max is straightforward in our BN model. First we developed the CPTs for many variables (nodes) after that we improve the CPT through using the leaky Noisy-MAX gates. These CPTs have parameters obtained from the collected data and improved by our assessment via quantifying the relation between child nodes and their parents according to our experience on the testbed (see chapter 5). To insure consistency of states, i.e. leaky Noisy-MAX gate parameters, we verified the two conditions (see above-mentioned assumptions). For instance, to derive causal relation between the cause of GOOSE delay we should ask ourselves does this delay is the effect of long IED processing time or high traffic of the network. If the answer is, a) one of them at least can cause the delay (independency), b) they cause the delay (causality) then, and possibly other cause (not modeled) causes the delay, then the GOOSE delay node can be modeled by leaky Noise-MAX gate. Fig 7.7 illustrates a comparison between two CPTs for a same node (SAS operation), first with traditional node and secondly with leaky Noisy-MAX model (leaky Noisy-OR).

a)

Measurement status	Success				Fail			
Protection status	Success		Fail		Success		Fail	
CB operation status	Success	Fail	Success	Fail	Success	Fail	Success	Fail
Success	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Fail	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5

b)

Parent	Measurement status	Protection status	CB operation status	LEAK
State	Fail	Fail	Fail	
Fail	1	1	1	0.5
Success	0	0	0	0.5

Figure 7.7: A comparison between CPTs for a) traditional BN node and b) leaky Noisy-MAX

7.6. Results and discussions

Through setting evidences and providing observations, the elaborated model is exploited in both directions, backward reasoning (bottom-up) to classify causes of failures, i.e. diagnosis, by computing and classifying causes, and forward inference (top-down) to predict, i.e. prognosis, the reliability of the target nodes, e.g. SAS reliability that represents successful operation. Additionally, this model would be used to predict (prognosis) the power system states according to a given data about the SAS functionalities, Ethernet network status and assumed prior probability of power faults.

7.6.1. Diagnosis scenarios

The graphical tool of the BN inference engine allows setting nodes for ranked observations as causes and states of target nodes as failure states. The queries shall comprise testing the evidence given updating prior probabilities where some observations are provided such as:

a) What are the causes of SAS failure given the observations about Ethernet network state and evidence that the protection function is reliable?

a)

Ranked Targets (failures)	probability
Measurement status: Fail	0.030900
CB operation status: Fail	0.004990
Protection status: Fail	0

Ranked observations (causes)	Diagnostic value
MU processing	0.411464
CB Controller processing	0.099643
GOOSE delay	< 0.000001
SV delay	< 0.000001
IED processing	0

Other observations	Evidence	State
	Network Traffic	Low
	SAS operation	Fail

b)

Ranked Targets (failures)	probability
CB operation status: Fail	0.191288
Measurement status: Fail	0.186540
Protection status: Fail	0

Ranked observations (causes)	Diagnostic value
GOOSE delay	0.161321
SV delay	0.130344
MU processing	0.017065
CB Controller processing	0.003976
IED processing	0.000538

Other observations	Evidence	State
	Network Traffic	high
	SAS operation	Fail

c)

Ranked Targets (failures)	probability
CB operation status: Fail	0.084852
Measurement status: Fail	0.034791
Protection status: Fail	0

Ranked observations (causes)	Diagnostic value
GOOSE delay	0.295153
MU processing	0.139074
SV delay	0.017530
CB Controller processing	0.012419
IED processing	0.000894

Other observations	Evidence	State
	Network Traffic	medium
	SAS operation	Fail

Figure 7.8: a) Testing the diagnosis with observations. Ranked causes are classified in top right and given evidences are shown on bottom right, b) and c) Ranked causes are reclassified according to new evidences

By setting evidence that SAS operation is failed and varying the state of network traffic in this scenario case, a diagnosis obtained that main causes are classified according to the traffic state. For example when the traffic is low the first ranked cause is the MU processing, i.e. either takes long time or not operating reliably, second cause is the CB controller processing either due to delayed action or non-reliable operation (top right of Fig 7.8 a). Setting the traffic observation (new evidence) to a medium will invoke new probability propagation (inference) that ranked the observations (causes) according to the new state of the network traffic. In this situation, the first ranked cause is the GOOSE delay with higher likelihood, and second cause is the MU processing (Fig 7.8 b). Setting the traffic to a high state affects the classification of causes where GOOSE delay is classified as a first cause and the SV delay is the second (Fig 7.8 c).

b) What are the causes of power outage given that measurement and protection functions operate successfully, and the network traffic is low?
The evidence of low traffic enforces a belief that low delay, for both SV and GOOSE, transmission exists in this scenario case, then, the only possible cause is the presence of continuous power transients that are happened due to outages from the power source (fig 7.9).

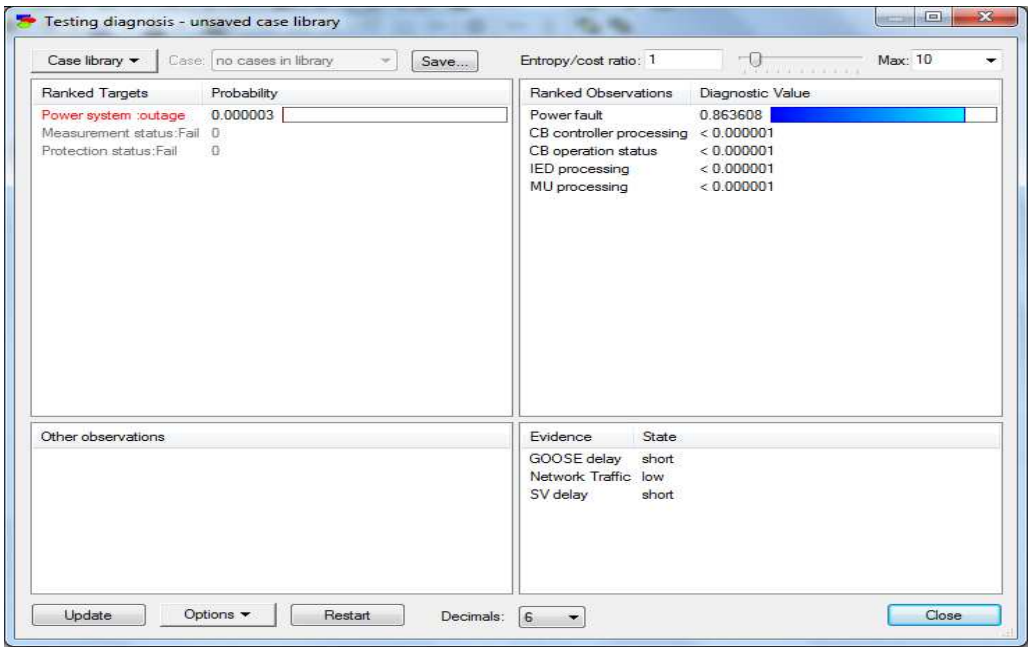


Figure 7.9: diagnosis causes of power outage when measurement and protection functions are reliable and network traffic is low

c) In order to diagnose and follow multi faults facing measurements, protection function, and CB operation, what are the causes of all SAS functionalities' (subsystems) failures? Pursuing multi-faults will provide most common causes in which the model diagnosis testing ranks the causes according to most likelihood as shown in (fig 7.10).

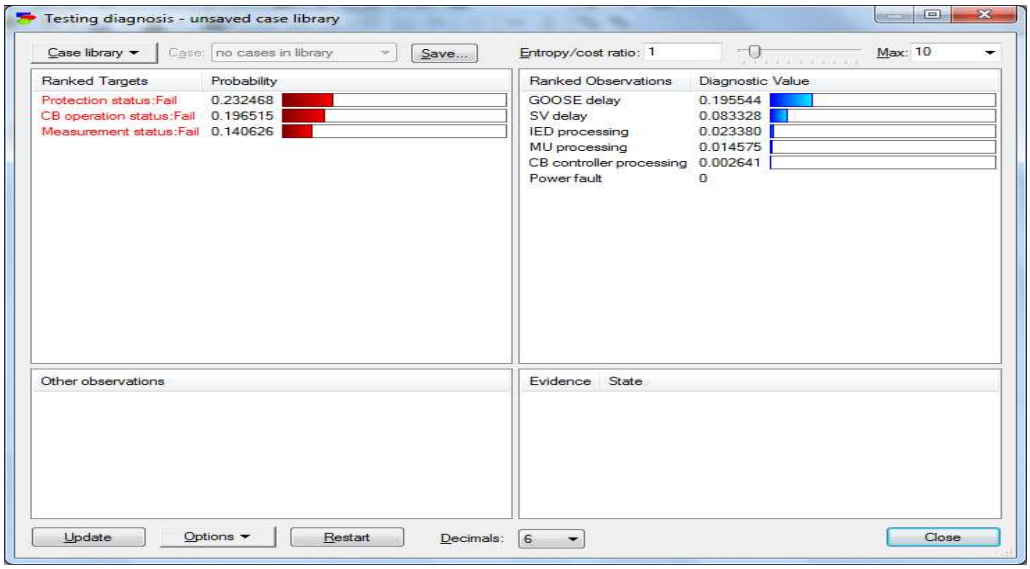


Figure 7.10: multi-fault scenario where many failures are followed to diagnose most causes

7.6.2. Prognosis scenarios

The prognosis in this model means estimating the state of final nodes that represent the reliability of relevant functions (success). Simulating predefined scenarios, i.e. providing prior probabilities for root nodes, will enable determining the final nodes states. This process probes the BN model via exploiting prior probabilities for particular conditions such as:

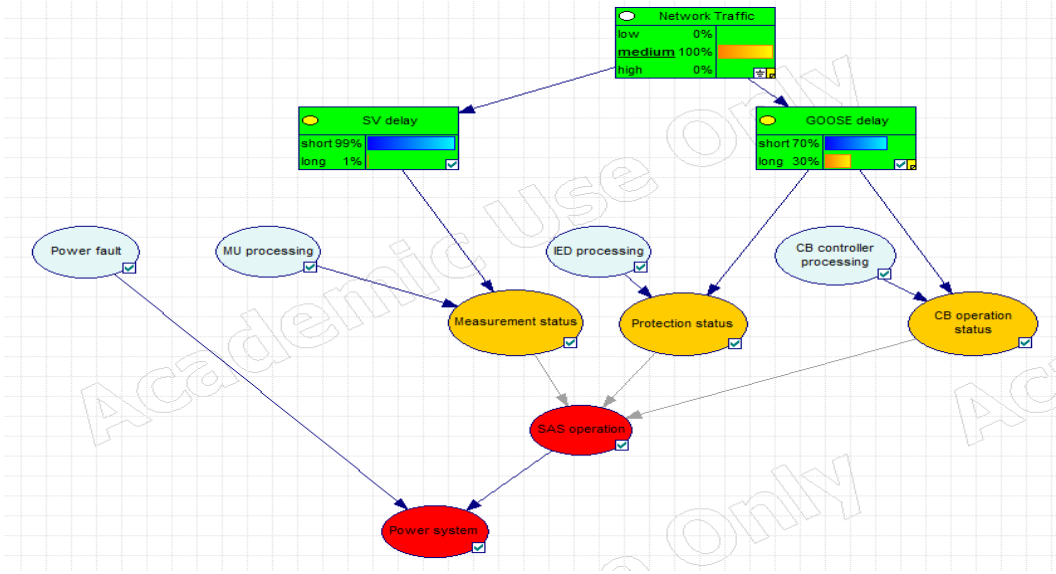


Figure 7.11: representation of posterior probabilities as bar charts for SV delay and GOOSE delay nodes

a) Given an evidence that the network traffic rate is medium (40Mbps < average network traffic < 80 Mbps) =100%, what are the states of the SV and GOOSE delay? This scenario gives posterior probabilities for both SV and GOOSE delay

when a traffic rate observation becomes evidence to compute posterior probabilities. Fig 7.11 shows a graphical representation of these probabilities.

b) What will be the effects of GOOSE and SV delay and loss scenarios on measurement, protection, control and circuit breaker operations. This scenario gives posterior probabilities for SAS functionalities (subsystem functions) when evidences such as long delays of both SV and GOOSE transmission and high loss of the later occur. Computed posterior probabilities is shown in Fig 7.12 as bar chart nodes. The figure shows setting evidence of 3 nodes, green with bar chart, SV delay node with 100% as long value, GOOSE delay with 100% as long value and GOOSE loss with 100% high value. The results are shown as posteriors for success and fail probabilities for measurement, protection and CB operation statuses (orange colored nodes). For instance, the measurement status node has probability of 58% for success and 42% for fail (Fig 7.12) and finally the influence on the SAS operation (red node with bar chart) is shown with probability of 90% for fail state.

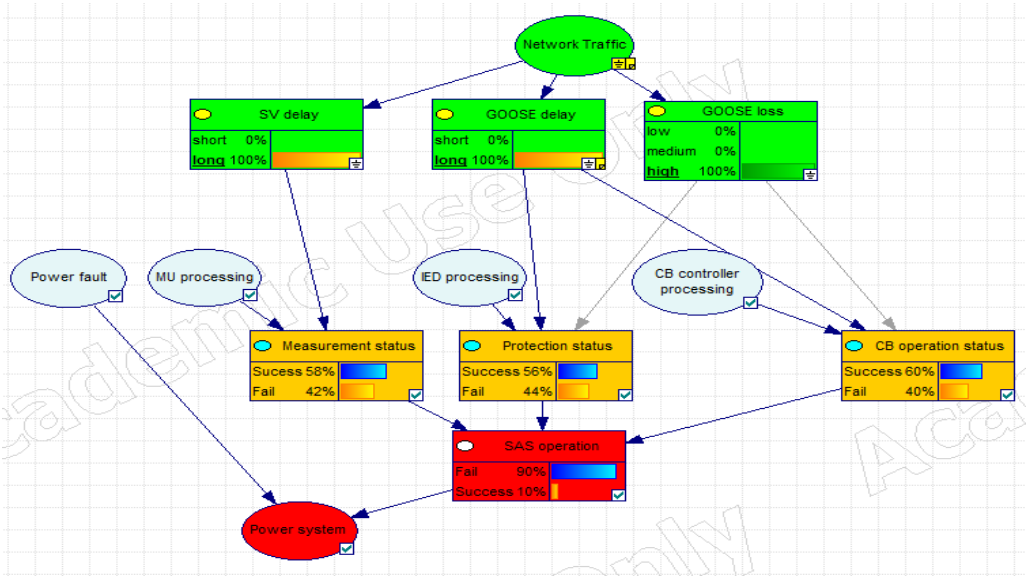


Figure 7.12: posterior probabilities for SAS functionalities: Measurement, protection and CB control

7.6.3. Discussions

The use of the developed BN model for diagnosis depends on the causal relationship between causes of failures and their effects. The model in this way has many layers namely the causes' layer, the failures layer and the effects layer. In this way, the structure should be appropriately designed especially when other context (auxiliary) nodes exist. These nodes represent relevant conditions such as SAS operation states, Power system states. When diagnostic scenario is performed the user should identify clearly the target nodes (failures) and the ranked observations (causes) and relevant evidences (given observed variables). This process depends on the user intuitive

thinking, therefore, lack of domain knowledge shall influence the diagnosis process. To overcome this limitation, we provide questions for elicitation of tests and evaluation results, as well as treatment and links to related documentation, e.g. IED device testing steps and related manual information.

Some inconsistent data made the data learning (parameters learning) process more daunting due to incompatible data types that require additional efforts to map data files contents to the BN model nodes and their states. This effort takes long time where assessment of child nodes CPT needs involvement of experts to tune the probabilities of these tables. To overcome the issue we used leaky Noisy-MAX model (gate) that also helps to reduce the complexity of CPT by only using interesting states of parents, e.g. fail state of parents to determine probability of child fail state.

For some prior probabilities, the values are assumed such as the probability of occurring of electrical power fault, while we omitted intentionally other nodes when we simulate prognosis of the power system service reliability, e.g. the sociotechnical aspects.

7.7. The validation process

In this section, we mean evaluation of the BN model where we check the model via testing real application data (the testbed-collected data). The idea is to learn the model parameters from the dataset (records) and leave one record for testing the diagnosis. Additionally, we generate synthetic data from the BN model to check its consistency and to test random cases comparing the results with our intuitive estimation of failure causes.

In addition, we used the available sensitivity analysis with the software tool by varying nodes probabilities and checking their influence on the posterior probabilities.

7.7.1. Evaluating the BN model for diagnosis cases

We test some failure cases in order to check the accuracy of estimated causes. This evaluation aids to evaluate the results by comparing them with the correct diagnosis explanations. Fig 7.13 illustrates testing by importing the protection failure case from a data file, in order to use the model to diagnose the causes. The figure shows a case of a protection failure where the target failure is the protection function and given observation are short GOOSE delay, low network traffic, short SV delay. The result of the diagnosis is consistent with our estimation as shown by fig 7.14

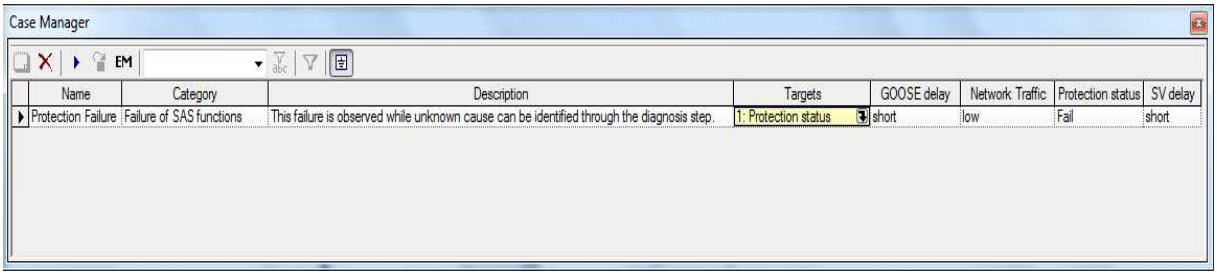


Figure 7.13: importing a protection failure case in order to diagnose its causes.

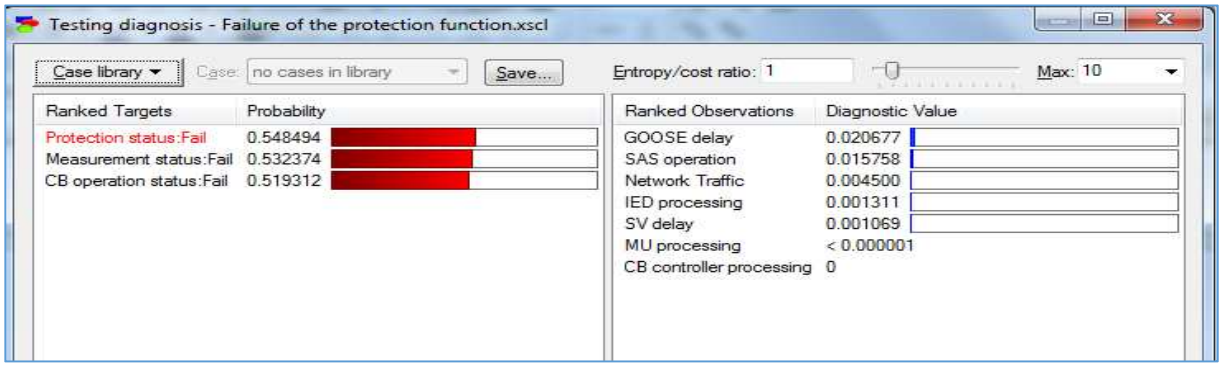
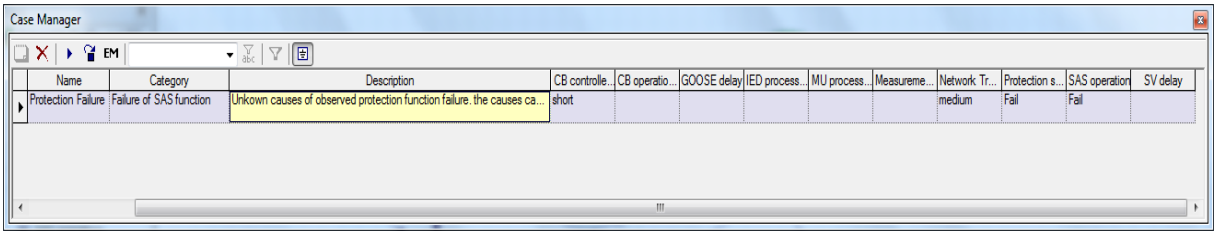


Figure 7.14: diagnostic results of the protection function failure given a case from a dataset record

Figure 7.14 shows the diagnosis' results of the case of protection function failure (Fig 7.13) where classified causes include GOOSE delay as first ranked cause with probability of 2%.

In addition, testing of another case that is more complicated than the above case. The protection function is assumed in a failure state. Observed evidences are updated to set an overall SAS system into failure state and the network traffic into a medium state. Fig 7.15 shows this scenario as a case record. The results are shown in fig 7.16, where no causes are given.



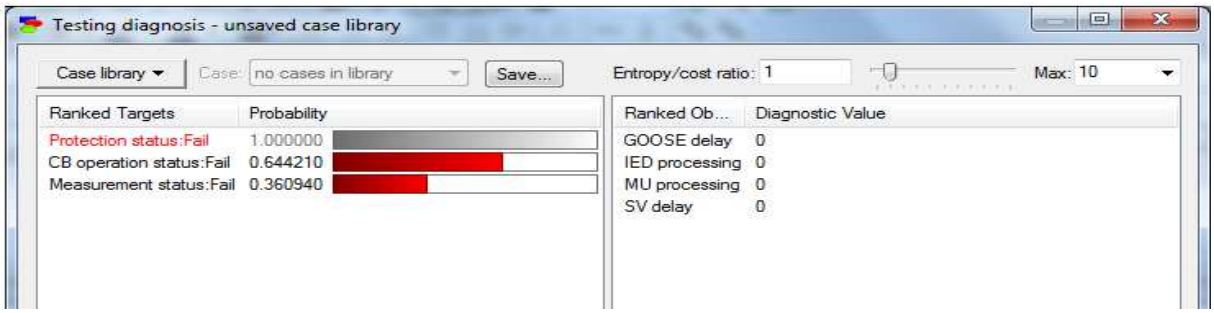


Figure 7.16: results of a modified case are logical due to insufficient evidences where only one observation is provided.

7.7.2. Generating synthetic data from the BN model

This step is used to generate a dataset with missed data (5% missed values), from the BN model, that shall be used for two purposes. The first purpose is to learn parameters from this dataset and the second purpose is to test randomly chosen records (random selection) in order to check the diagnosis performance. Fig 7.17 shows the setting of this task.

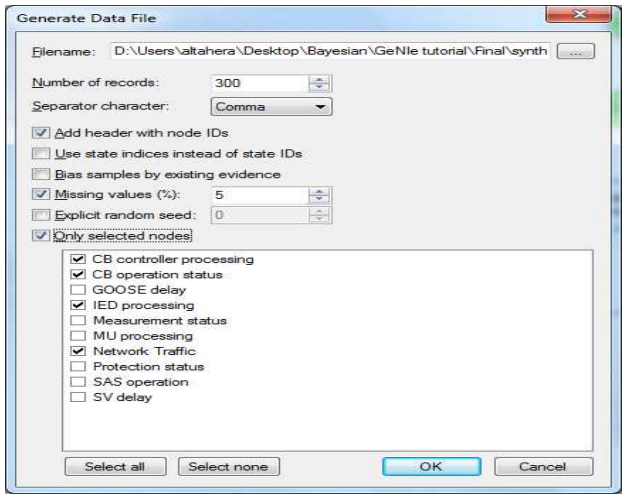


Figure 7.17: Generating a dataset with 5% missed values to evaluate the diagnosis performance of the BN model

This task is completed in about 20 ms, generating 300 records, which give an indicator about the feasibility of this step in order to evaluate the diagnosis performance. The generated dataset shall contain missed values distributed among the data fields (columns) as shown in the fig 7.18, where a 5% of the data is missed.

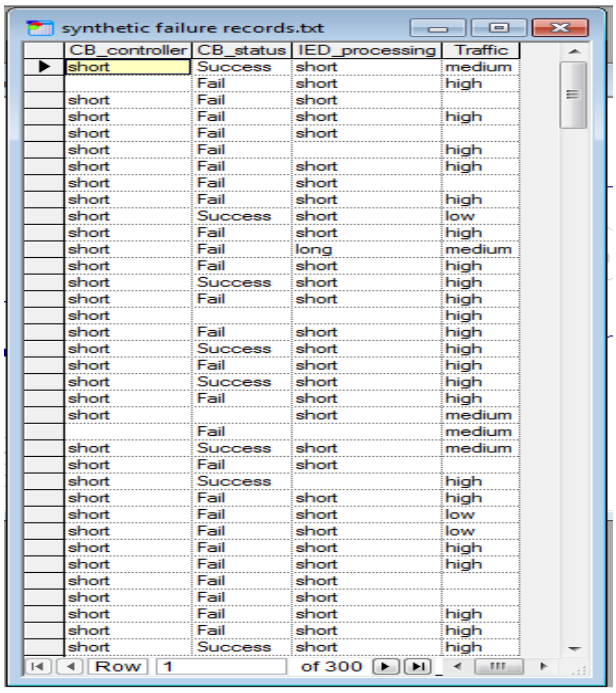


Figure 7.18: Generating a synthetic data with 5% missed data values: 300 records are created in about 20 ms

After generating the dataset, we use it to learn parameters (data learning) to update the model probabilities. Moreover, we select some records randomly to test the diagnosis performance from the same dataset. During these steps we leave this record out of the dataset, i.e. during learning step we remove the tested record. We inspected 10 cases in order to evaluate the diagnosis performance (Fig 7.18) and to check the consistency of data values. We noticed that the diagnosis can not identify the cause of CB (circuit breaker controlling function) operation failure in three cases among the 10 cases. Possibly, in this situation more data records about the circuit breaker operation and related information are required to improve the diagnosis accuracy.

7.7.3. Sensitivity analysis

To validate the model consistency, a sensitivity analysis step is vital to inspect causal relation among nodes and conditional dependency (and independency). This step means varying the nodes parameters (states values) and checking their influence on the other model contents. The technique of sensitivity analysis (Castillo et al., 1997; Kjærulff, Van Der Gaag, 2000) assists validating the probability parameters of the BN model through investigating the effect of small changes in numerical parameters, i.e. probabilities, on the output parameters, e.g. posterior probabilities). To analyze the sensitivity, a node (or several nodes) should be set as a target node, i.e. as in mathematical models where varying inputs to check effect on the model parameters. This step helps also to tune the model parameters when a BN expert can ignore (delete) some nodes due to their inconsistency and negligible influence on the model parameters. Fig 7.19 illustrates this task where red colored nodes represent most important parameters.

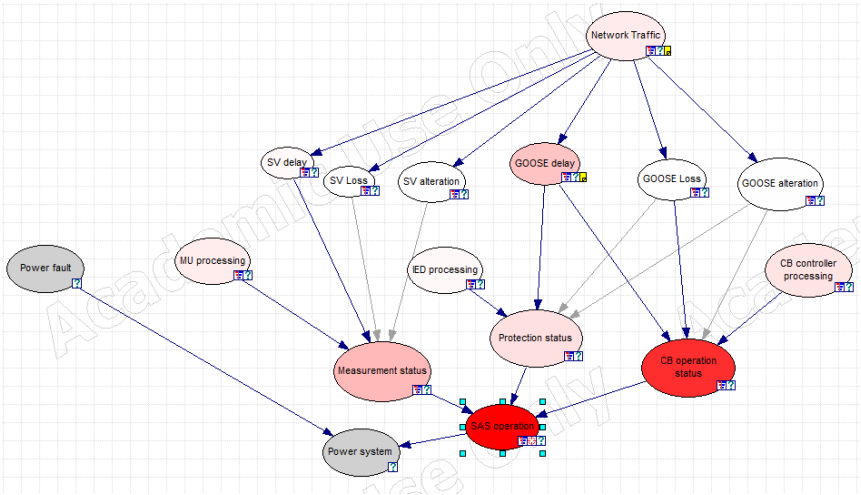


Figure 7.19: Sensitivity analysis step where SAS operation node is set as target node.

7.8. Conclusion

In this chapter, a modeling based on Bayesian networks (BN) is exploited mainly to perform diagnosis tasks, which also used flexibly to estimate the system state (reliability) according to given scenarios. This work enhances the system dependability by identifying faults and their causes. The user will understand the relation between the cause and the fault. This process will improve the user knowledge in which multidiscipline information can be learned.

The BN model is built upon collected data from experiments performed to test the IEC 61850 based protection schemes. Where the qualitative part (BN structure) is derived from the formal system architecture and related literature, and the quantitative part is identified by incorporating parameters from data obtained during the testing and performance evaluations (see chapter 5). In addition to tune up the model, validation and sensitivity analysis are performed to tune probabilities and CPT parameters.

The BN diagnosis model provides helpful reasoning that depends directly on the model structure (causal relationship) and the adjusted parameters (prior probabilities and CPT). Complexity of this model is the exponential relation between the child node and its parents' nodes. We used Noisy-MAX with leaky feature to overcome this issue. Furthermore, lack of knowledge about some causes such as sociotechnical auxiliary causes, because of uncertainties considering prior probabilities, leads to omitting this layer that needs more research efforts.

The BN modeling technique is a promising approach where its DBN (Dynamic BN) extension can provide means to model temporal evolutions such as network traffic dynamics, e.g. variation of average flow. Hence, dynamics of network quality metrics such as delay can be simulated in this practice.

Real-time diagnostics of failures can be improved through on-line collections of data, classifying causes according to causal relationships in which failure detection step can be included within facility of an embedded system. This system can be deployed within the future IEC 61850-based process level equipment, where SV measurement based on stand-alone Merging Units and embedded circuit breakers controllers, with network interfaces, provide enough amount of data that shall be used for advanced diagnostics.

chapter 8 : Conclusions and Perspectives

8.1. Conclusions

This thesis presents efforts that aim mainly to investigate dependability of Smart Grid technologies. In particular, an IEC 61850 based substation automation system has been investigated. These efforts proposed dynamic testing techniques for evaluating the performance of communication networks, protective relays (IEDs) and their interactions. These tests help to inspect conformity of devices to specific performance requirements that are adjusted by relevant standards.

This study has used Ethernet performance metrics and traffic profiles to build a strict framework. The experimental methods will aid designers, developers and integrators to inspect developed technologies within laboratory setups for research and industrial activities.

Dependability and functional safety techniques were employed for evaluating Smart Grid technologies. Suitability of these techniques are shown through a case study. The IEC 61850 communication protocol (GOOSE messaging service) is inspected to check their conformity to requirements of functional safety standards.

The data obtained during the experiments of dynamic testing and performance evaluation were used for learning parameters of a designed Bayesian Network (BN) model. This model was exploited for diagnosis purpose, and was adapted to present a prognosis application.

Main findings of this work:

Unit testing of protective relays provides indications about tripping, blocking and time coordination performance. These functions cannot be tested without functional interaction among the interconnected protective relays.

Interactions between substation devices, to achieve coordination tasks, depend on performance of the communication network and related services inside these devices. The Ethernet network provides flexibility, but it requires effort to reach well design and configuration. Ethernet network perturbations regarding high traffic loads and poor quality of service could cause degraded performance of protective relays (IED devices). The degraded performance beside power system transients could initiate overloaded functionalities that lead to a fallback state.

Dependability and functional safety techniques can be applied to the Smart Grid technologies. The digital substation automation system exploits a large amount of data. This data can be used for diagnosis and prognosis to enhance the system dependability. These tasks can help many stakeholders such as designers, integrators, testers, and maintenance staff during several phases of a substation life cycle.

Contributions of this research and its importance:

Providing invaluable information for understating the IEC 61850 standard, its technical parts and related services such as communication technologies (SV, GOOSE and time synchronization) throughout implementing empirical testing methods.

Testing methods were developed in this thesis to observe dynamics of protection schemes and behavior of Ethernet networks. These methods aid in evaluating the performance of designed and developed technologies of substation automation systems. Another promising application of these techniques is to validate designs through implementing experimental platforms within academia and industry. Quantifying the performance metrics were performed according to requirements of information technology such as Ethernet communications, and operation technology as power protection schemes. Quality of service features within Ethernet technologies were investigated. VLAN based priorities were implemented to enable prioritizing GOOSE messages and to guarantee their delivery during high traffic profiles. VLAN is observed in which associated tangible benefits are security and reliability enhancement due to the passing of protection messages via dedicated VLAN ports.

Dependability and functional safety techniques have been implemented in a design case study where proposed process and bay level functionalities were investigated by using component based reliability. Reliability block diagrams were used and reliability, inherent availability and safety integrity levels were calculated. Furthermore, GOOSE messages were inspected according to requirements of safety communications.

Data obtained from the experimental platform was exploited. These data helped to learn parameters within a Bayesian Network model, and to classify causes of observed failures. The complexity of this model is reduced by using a canonical model (Noisy Max gate).

Moreover, practical recommendations were raised during the experimental works. Future digital substations will incorporate information and communication

technologies inside all their levels. Thus, substation engineers, technicians and operators should acquire essential knowledge that helps to better design, test, operate and maintain reliable substations. For example, VLAN and redundancy shape important requirements of information and operation technologies. The performance evaluation approach is recommended, in this context, to achieve designed objectives of an overall system test (factory or site acceptance testing). Therefore, the test should begin by IED devices as unit testing, and then emphasize functional testing of the devices (e.g. time synchronization and coordination) that needs setting of real protection schemes.

The current study experiences some limitations due to a limited availability of some advanced features of substation automation systems. The experimental work covers only a single transformer bay and a single feeder bay. These bays do not support direct acquisition and manipulation of IEC 61850-9-2 process bus (Sampled Value) measurements.

Synchronization of devices' time was performed through available software based services such SNTP/NTP protocols, which limits the precision of devices' time-synchronization and accuracy of substations timing data.

We should mention that the experimental study does not inspect network redundancy tools and techniques that aid to enhance service availability of Ethernet networks.

Furthermore, in this work, the BN based modeling is limited to offline diagnostics, however, sociotechnical factors are not covered in this work. These factors act as vital roles in the dependability of the system where human errors contribute to reliability of substations design, configuration and operation. Human error in the context of the IEC 61850-based substations dependability is still potential for further research activities.

8.2. Perspectives and Further research suggestions

Potential research ideas are raised during the thesis work. Firstly by considering the communication network where the local Ethernet networks exist inside the substations. Substation devices shape an essential part of the Smart Grid cybersecurity, for instance, ICMP responses from IED devices to Ping requests are actively observed working which create vulnerable points, e.g. ARP attacks. Another point is VLAN security when port based configuration can be a potential vulnerability for similar kinds of attacks. Some studies propose routing GOOSE messages between remote substations. Protection schemes such as distance protection will be an experimental issue that requires further investigation to cover time performance and cybersecurity related issues.

The experimental platform in this work can be furtherly expanded to support full process bus features such as Merging Units as publishers and IED devices as subscribers. This mechanism will support acquisition of Sampled Value (SV) messages. Then, development of modules or devices for process bus can be inspected with these features, which in result open potentials for research topics such as testing of developed devices. The testing technique in this context will require software based capabilities that depend on Substation Configuration Language (SCL) based test-set, i.e. to generate required signaling. Publishing of or subscribing to SV, GOOSE and related data can be performed through this test-set. This technique allows testing devices and equipment in laboratory settings, which possibly increases flexibility and reduces time, efforts and costs by utilizing software based modules.

Second further research considers the real-time diagnosis of the designed system where IED devices and other equipment such as MUs can provide a large amount of high quality data. This data will be increased inside modern as well as future digital substations. The increased amount of data shall help the investigation of malfunctions and failures, and diagnosis of their causes. Improving the BN based diagnosis with expert knowledge, and use of online-embedded systems can exploit available data from the Ethernet network (SV and GOOSE), IED devices (fault recorders, log files etc.) and experimental test-beds.

Appendix A

A.1. International Standard Organization/ Open Systems Interconnection (ISO OSI) model

Seven layers shape the international standard model (ISO OSI) that allows open intercommunication to connect devices from different vendors (hardware and software providers). Ethernet switches use the lower layers where the physical layer transfers bits into form of electromagnetic, electrical or optical signals. The datalink contains two sublayers Media Access Control (MAC) and Logic Link Control (LLC).

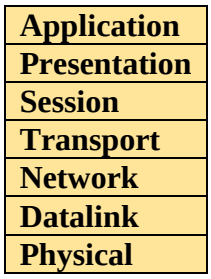


Figure A.1: ISO-OSI seven layers model, Ethernet switches use two lower layers.

A.2. Contents of an Ethernet frame (with IEEE 802.1p/q)

At the second layer, Ethernet frames contain control data and quality of service fields. Fig A.2 shows an IEEE 802.1p/q enabled structure of Ethernet frames.

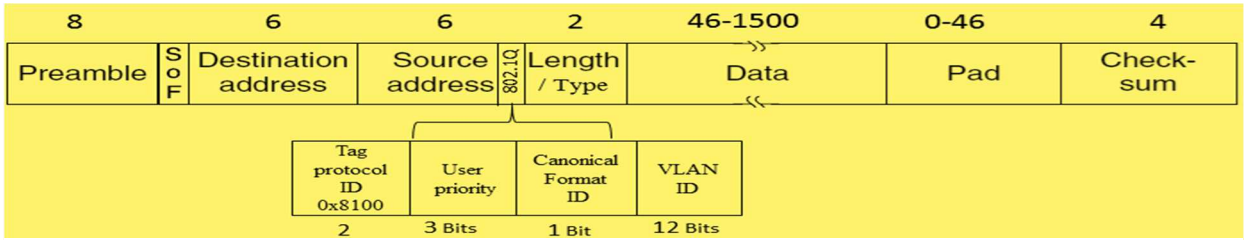
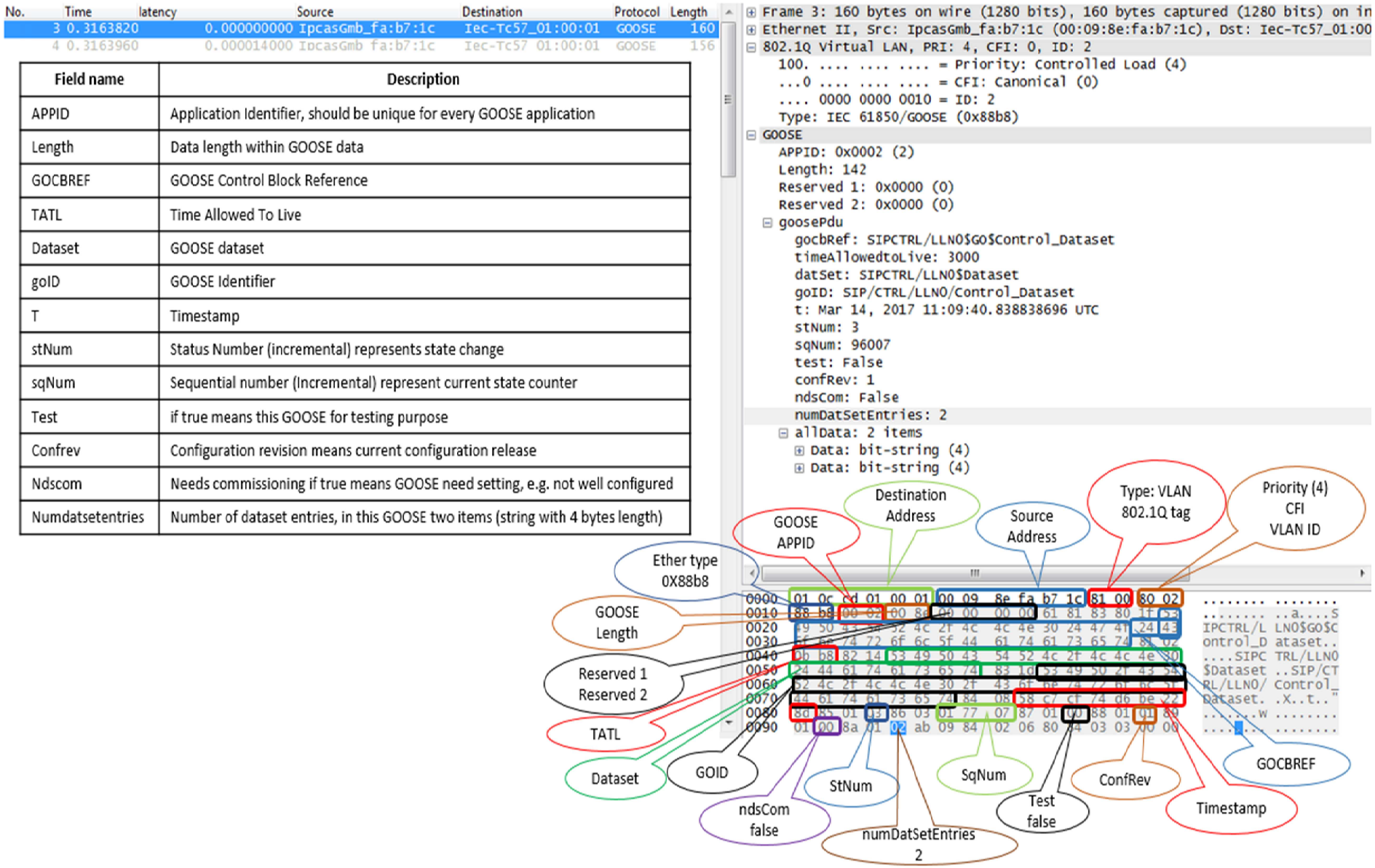


Figure A.2: Ethernet based frame with VLAN tagging and priority (IEEE 802.1p/q)

A.3. Frame structure of GOOSE (Generic Object Oriented Substation Event) messages

According to the standards [IEC 61850-8-1 and UCA 2.0], GOOSE is built upon Abstract Syntax Notation/Basic Encoding Rules (ASN.1/ BER) that use tag/length, i.e. TLV (type/length/value), for every field of data. Fig A.3 shows a GOOSE message with detailed fields. This message is embedded into an Ethernet frame with VLAN and priority tagging. The Wireshark analyzer is used to analyze contents of this frame. Fields of data are described according to their rules.

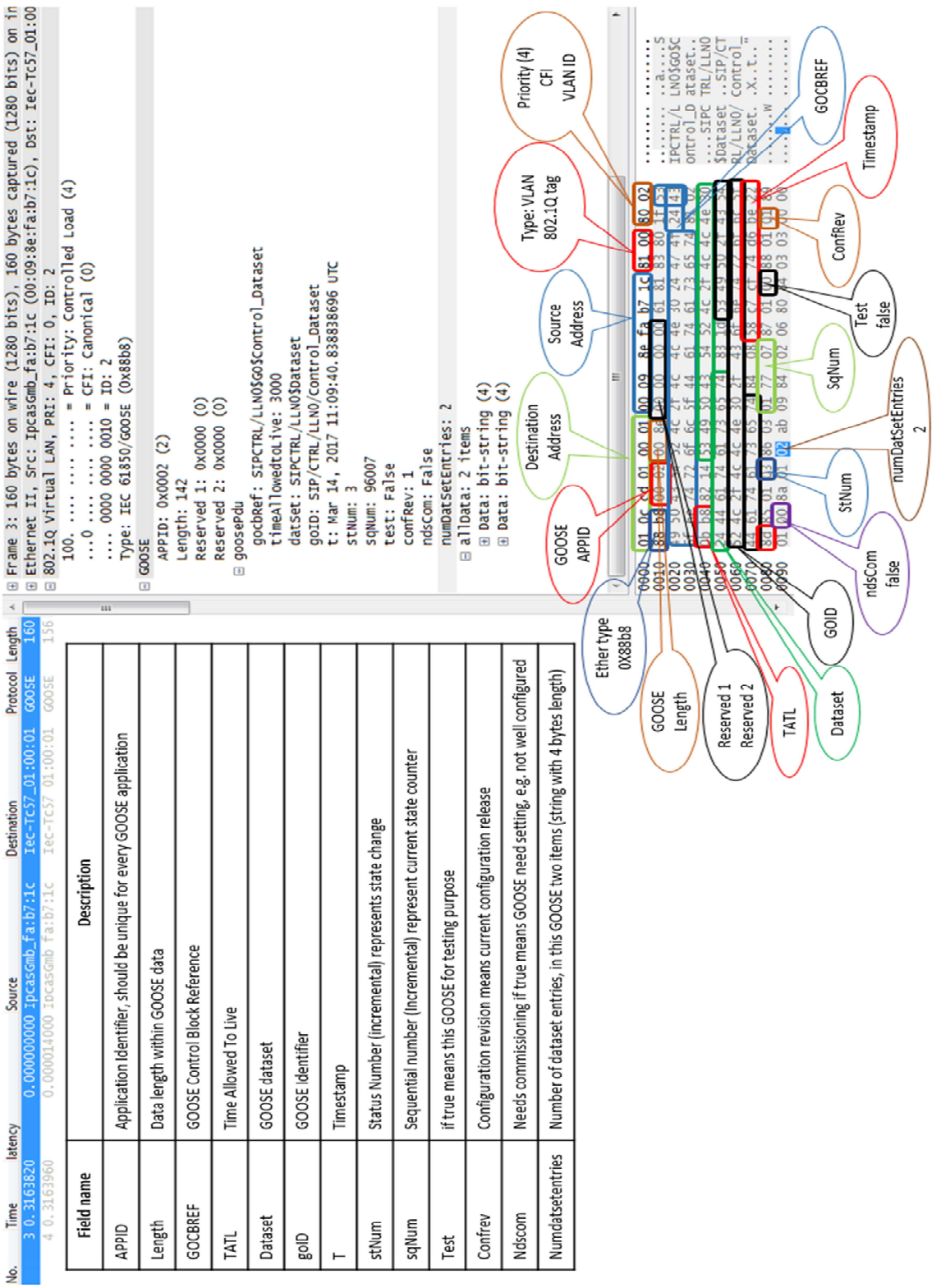


Field name	Description
APPID	Application Identifier, should be unique for every GOOSE application
Length	Data length within GOOSE data
GOCBREF	GOOSE Control Block Reference
TATL	Time Allowed To Live
Dataset	GOOSE dataset
goID	GOOSE Identifier
T	Timestamp
stNum	Status Number (incremental) represents state change
sqNum	Sequential number (Incremental) represent current state counter
Test	if true means this GOOSE for testing purpose
Confrev	Configuration revision means current configuration release
Ndscom	Needs commissioning if true means GOOSE need setting, e.g. not well configured
Numdatsetentries	Number of dataset entries, in this GOOSE two items (string with 4 bytes length)

Figure A.3: GOOSE message embedded into an Ethernet frame with VLAN and priority

A.4. Frame structure of SV (Sampled Value) messages

According to the standards [IEC 61850-9-1/2 and UCA IEC 61850-9-2 lite edition guide], SV is built upon Abstract Syntax Notation/Basic Encoding Rules (ASN.1/ BER) that use tag/length, i.e. TLV (type/length/value), for every field of data. Fig A.4 shows a SV message with detailed fields.



Field name	Description
APPID	Application Identifier, should be unique for every GOOSE application
Length	Data length within GOOSE data
GOCBREF	GOOSE Control Block Reference
TATL	Time Allowed To Live
Dataset	GOOSE dataset
goID	GOOSE identifier
T	Timestamp
stNum	Status Number (incremental) represents state change
sqNum	Sequential number (incremental) represent current state counter
Test	if true means this GOOSE for testing purpose
Confrev	Configuration revision means current configuration release
Ndscom	Needs commissioning if true means GOOSE need setting, e.g. not well configured
Numdatsetentries	Number of dataset entries, in this GOOSE two items (string with 4 bytes length)

Figure A4. Sampled Value measurment embeded into Ethernet Frame

Appendix B

B.1. Fundamental functions of power protection and control

ANSI/IEEE protective relay functions from [IEEE C37.2-2008 - IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations] and corresponding IEC 61850 logical nodes names.

Table B.1: protective relay functions according to ANSI/IEEE, and corresponding IEC 61850 Logical Nodes

IEEE C37.2-2008 Device number	IEC 61850 Logical node	Function
50	PIOC	Instantaneous overcurrent protection
51	PTOC	Time delayed overcurrent protection
87	PDIF	Differential protection
21	PDIS	Distance protection
67	PDIR	Directional overcurrent protection
59	PTOV	Time delay overvoltage protection
81	PFRQ	frequency protection
79	RREC	Automatic reclosing
50BF	RBRF	Breaker failure
27	PTUV	Under voltage protection
49	PTTR	Thermal overload protection
85	RCPW	Carrier or pilot wire receiver
25	RSYN	Synchronism check
68	RPSB	Power swing blocking
52	XCBR	AC Circuit breaker switching
89	XSWI	Line switch (Disconnector) switching

B.2. Definition of 50/51 overcurrent protection functions

An overcurrent function is a type of protective relay function, which operates when the load current exceeds a pickup value. The ANSI device number is 50 for an instantaneous over current (IOC) or a Definite Time Overcurrent (DTOC). Typically the over current relay is connected to a current transformer. When the relay operates, one or more contacts will operate and energize to trip (open) a circuit breaker. The Inverse Definite Minimum Time (IDMT) protective relays were developed to overcome the shortcomings of the Definite Time Overcurrent Relays.

B.3. Definition of IDMT curve (IEC 60255: Trip Curve Equation)

For protection coordination, the 51-protection function has the following curve formula [IEC 60255-trip curves equation] that is called 51 (IDMT) function:

$$td(I) = \frac{k}{\left(\frac{I}{Is}\right)^{\alpha} - 1} \times \frac{T}{\beta}$$

Where td is the delay, *k, α,* and *β* are constants (with standard inverse k=0.14, α=0.02 and β=2.97). *T* is the coordination time (time multiplier setting), *I* is measured current (actual secondary current) and *Is* represents pickup current (relay operation current setting) value.

Appendix C

C.1. Bayesian Network (BN) model for prognosis:

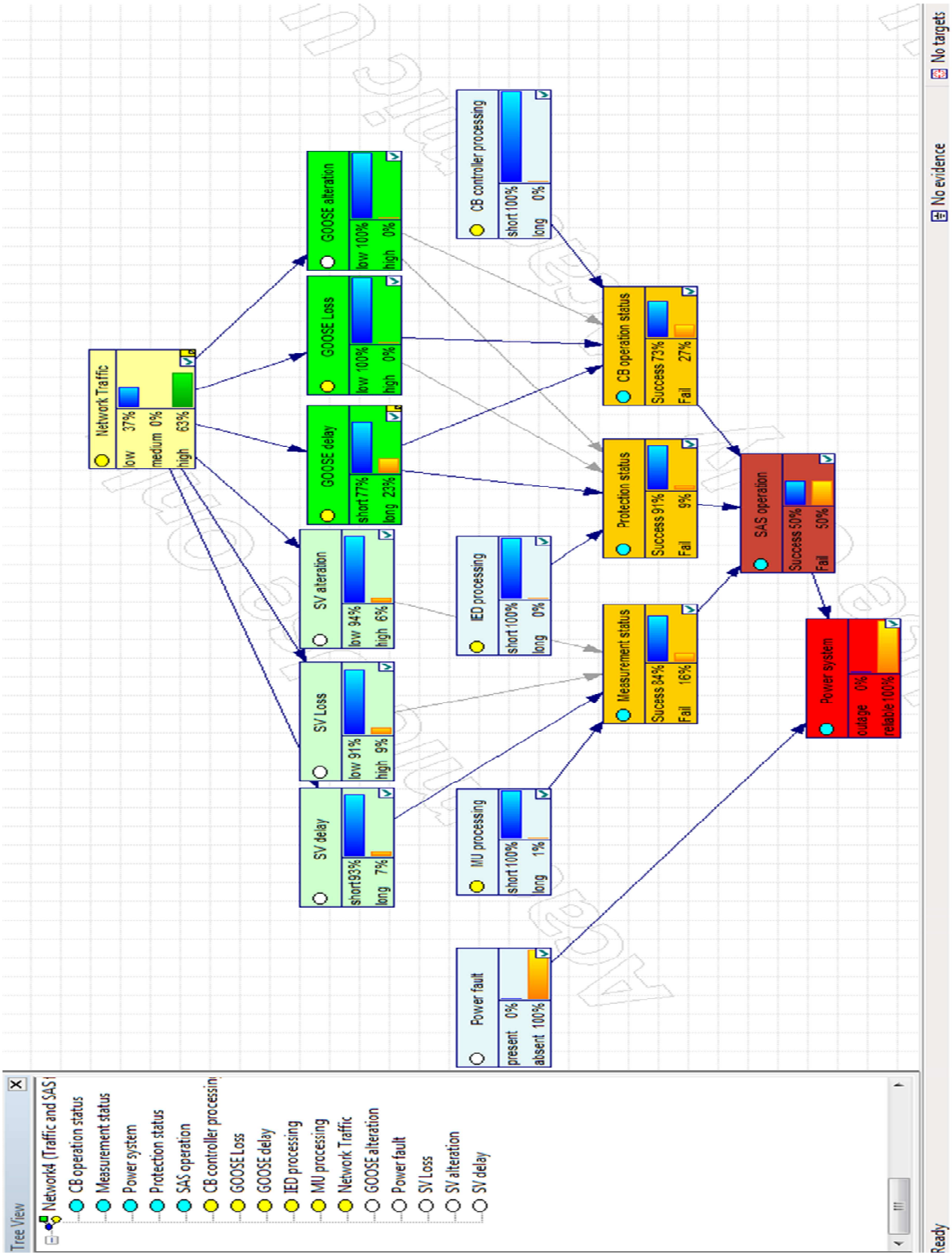


Figure C.1: BN model with nodes in bar chart view showing states value for every node

C.2. prognosis scenarios using a modified BN model:

a) What will be the effect of medium network traffic rate and long IED processing time on the SAS functionalities?

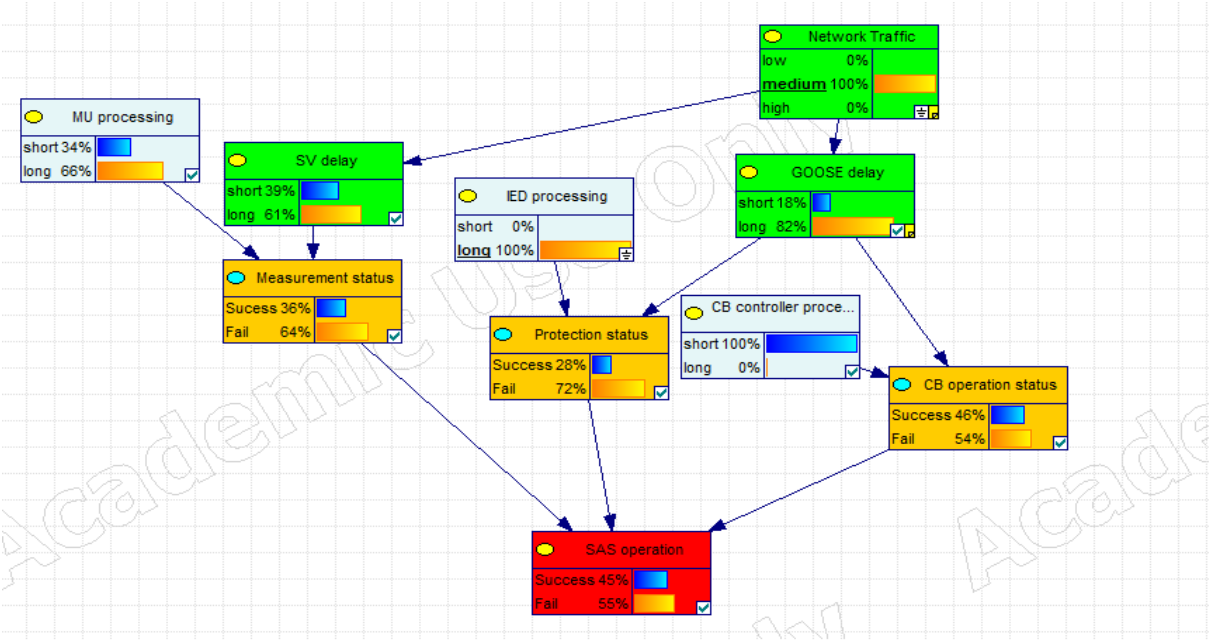


Figure C.2: BN model shows state of SAS operation, given state of medium network traffic and long IED processing time

b) With same previous conditions, what will be the effect of long CB controller processing state on the SAS operation state during a power fault?

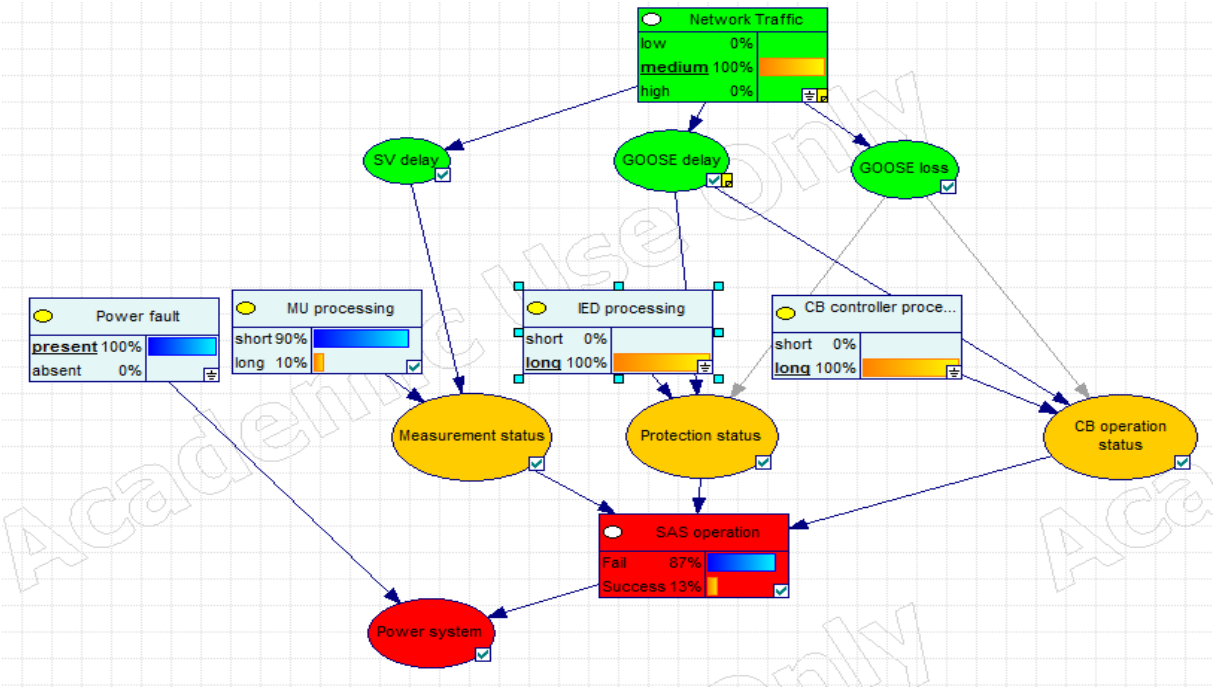


Figure C.3: same previous condition, but providing fault state of the power system (see left node entitled power fault)

c) What will be the effect of protection operation failure on the SAS and overall power system?

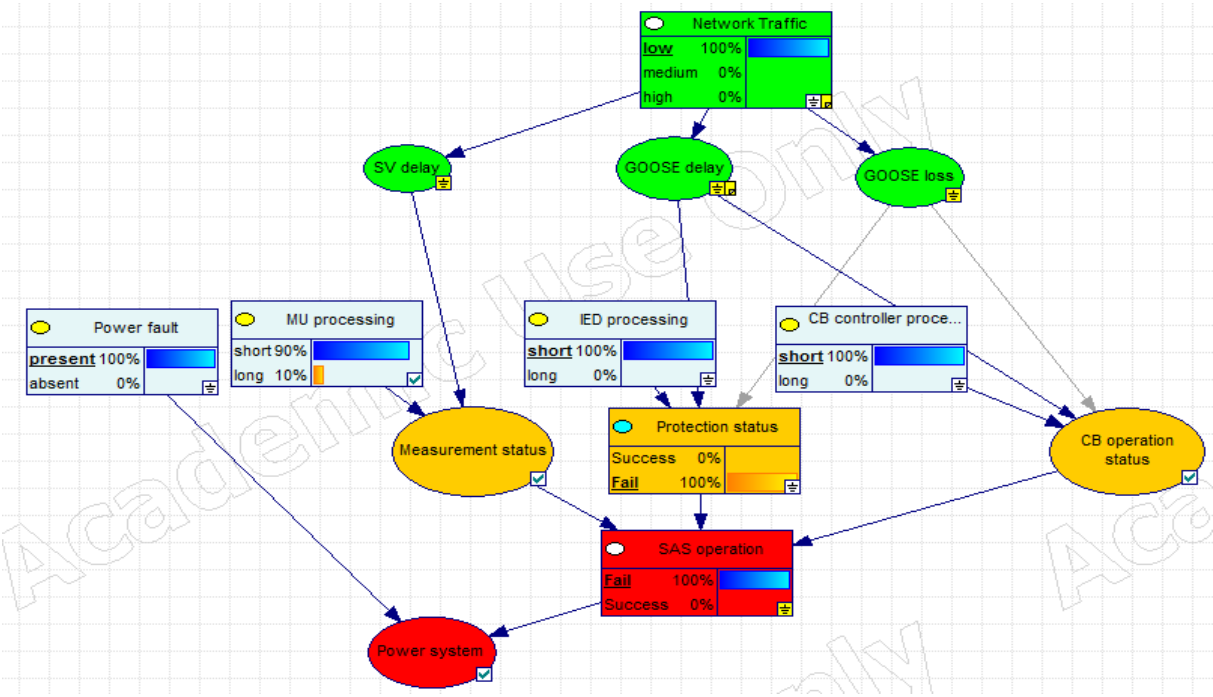


Figure C.4: protection failure during power fault leads to failure of SAS operation

d) What will be the effect of (GOOSE loss rates $>10^{-4}$=100%) on the SAS failure (reliability of the system)?

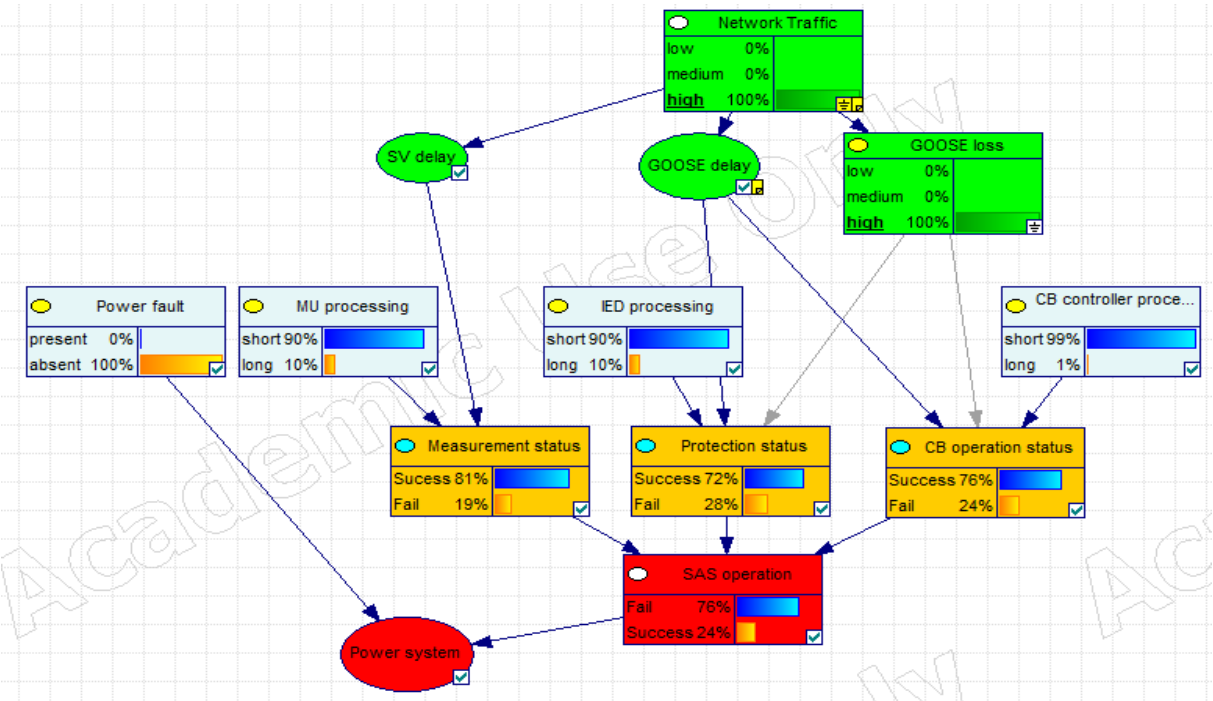


Figure C.5: high loss rate of GOOSE messages (normally due to high traffic) causes high probability of SAS failure (76%)

Publications

- Ahmed Altaher & Hasan Madi. Investigating Conformance of Modern Communication Networks inside Modern Digital Substations. Accepted paper, Libyan International Conference on Electrical Engineering and Technologies (LICEET2018). Tripoli, Libya, March 2018.

- Ahmed Altaher, Stéphane Mocanu, Jean-Marc Thiriet. Dependability Optimization of Process-level Protection in an IEC-61850-Based Substation. Walls, Revie & Bedford. 26th European Safety and Reliability Conference (ESREL 2016), Sep 2016, Glasgow, United Kingdom. Taylor & Francis Group, Risk, Reliability and Safety: Innovation Theory and Practices - pp.284, 2016.

- Ahmed Altaher, Stéphane Mocanu, Jean-Marc Thiriet. Evaluation of Time-Critical Communications for IEC 61850-Substation Network Architecture. In proceedings, Surveillance 8 International Conference, Oct 2015, Roanne, France.

- Ahmed Altaher, Stéphane Mocanu, Jean-Marc Thiriet. Experimental Evaluation of an IEC 61850-Station Bus Communication Reliability. Journées Nationales des Communications Terrestres (JNCT 2015), Jun 2015, Valence, France. 2015.

- Ahmed Altaher, Jean-Marc Thiriet, Stéphane Mocanu. Performance Evaluation of IEC 61850 safety-related communication architecture. International Summer School on Cyber-Physical Systems - 2014 Edition, Jul 2014, Grenoble, France.

Bibliography

1. Aeiker, J. D., & Liggett, D. P. (2014). Electrical hazard analysis from a PSM perspective. In Electrical Safety Workshop (ESW), 2014 IEEE IAS (pp. 1-5). IEEE.
2. Ahmed, W., Hasan, O., Pervez, U., & Qadir, J. (2017). Reliability modeling and analysis of communication networks. Journal of Network and Computer Applications, Vol (78), pp. 191-215.
3. Ali I., & Thomas M., (2008) Substation Communication Networks Architecture, in joint international conference on power system technology and IEEE power India conference, POWERCON, pp. 1-8.
4. Ali I., (2012), High-speed Peer-to-Peer Communication based Protection Scheme Implementation and Testing in Laboratory, in International Journal of Computer Applications, vol. 38, No. 4, pp. 16-24.
5. Ali N., Ali B., Abdala M., Othman M., & Hashim F., (2014), Comparisons process-to-bay level peer-to-peer network delay in IEC61850 substation communication systems, in Journal of Electrical Systems and Information Technology, Vol. 1, No. 3, pp. 266-275.
6. Al-Kuwaiti, M., Kyriakopoulos, N., & Hussein, S. (2009). A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, pp. 106-124.
7. Almond, R. G. (1992). An extended example for testing Graphical Belief. Statistical Science Research Report, 6, 1-18.
8. Alstom Grid., (2011), Network Protection and Automation Guide NPAG.
9. Altaher, A., Mocanu, S., & Thiriet, J. M. (2015). Evaluation of Time-Critical Communications for IEC 61850-Substation Network Architecture. In Proc. Surveillance 8 2015, Surveillance 8 International Conference, Roanne, France.
10. Altaher, A., Mocanu, S., & Thiriet, J. M. (2016). Dependability Optimization of Process-level Protection in an IEC-61850-Based Substation. In proc. 26th European Safety and Reliability, Conference (p. 284). Taylor & Francis Group.
11. Amin M. (2011) Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control, in European Journal of Control, (2011)5-6: pp. 547–567
12. Apostolov, A., Brunner, C., & Clinard, K., (2003), Use of IEC 61850 object models for power system quality/security data exchange. In Quality and Security of Electric Power Delivery Systems, 2003, CIGRE/PES., CIGRE/IEEE PES international symposium (pp. 155-164). IEEE.
13. Atoui, M. A., Verron, S., & Kobi, A. (2016). A Bayesian network dealing with measurements and residuals for system monitoring. Transactions of the Institute of Measurement and Control, 38(4), 373-384.
14. Avizienis, A. (1967), Design of fault-tolerant computers, In Proc. conference on the fall joint computer, November 14-16, 1967, pp. 733-743, ACM.
15. Avizienis, A., Laprie, J. C., & Randell, B. (2001). Fundamental concepts of dependability. University of Newcastle upon Tyne, Computing Science.

16. Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, Vol 1, No. 1, pp. 11-33.
17. Baranov P., Muravyov S., Sulaymanov A., & Khudonogova L., (2013), Software for Emulating the Sampled Values Transmission in Accordance with IEC 61850 Standard, in 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013), Atlantis Press, pp. 478-481.
18. Barlow, R. E. (1988). Using influence diagrams. In C. A. Clarotti & D. V. Lindley (Eds.), Accelerated life testing and experts' opinions in reliability (p. 145-157).
19. Bauer, E. (2011). Analyzing and Modeling Reliability and Robustness, Design for Reliability: Information and Computer-Based Systems, pp. 145-168, John Wiley & Sons.
20. Bindra S. & Salih N., (2014), UNCSD Rio +20 Libya National Report Future We Want Focal Point on Renewable in Libya 2014, 2014 1st International Congress on Environmental, Biotechnology, and Chemistry Engineering, IPCBEE vol.64, IACSIT Press, Singapore.
21. Bio M. J. (2001), Air Insulated Substations — Bus/Switching Configurations, in Grigsby, L. L. (Ed.), The Electric Power Engineering Handbook. Boca Raton: CRC Press LLC.
22. Blair S., Coffele F., Booth C., & Burt G., (2013) An Open Platform for Rapid-Prototyping Protection and Control Schemes with IEC 61850, in IEEE TRANSACTIONS ON POWER DELIVERY, Vol. 28, No. 2, pp. 1103-1110.
23. Blair S., Coffele F., Booth C., De Valck B., & Verhulst D, (2014), Demonstration and analysis of IP/MPLS communications for delivering power system protection solutions using IEEE C37.94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols, in CIGRE 2014.
24. Bolin P. (2001), Gas Insulated Substations, in Grigsby, L. L. (Ed.), The Electric Power Engineering Handbook. Boca Raton: CRC Press LLC.
25. Bolt, J. H., & Van Der Gaag, L. C. (2010). An empirical study of the use of the noisy-OR model in a real-life Bayesian network. In International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems (pp. 11-20). Springer, Berlin, Heidelberg.
26. Bombardier, V., Georges, J. P., Rondeau, E., & Diouri, I. (2018). Using fuzzy rules for network behaviour identification: application for differentiated services in an Ethernet network. *International Journal of Computational Intelligence Systems*, *11*(1), 316-329.
27. Bonica R., Bryant S. (2012), RFC 2544 Testing in Production Networks, IETF NWG
28. Borcsok, J. (2010). Safety sensor bus system. Mechatronic Systems, vol. (1).
29. Borcsok, J., & Schwarz, M. H. (2006). Principles of safety bus system. In Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on (pp. 188-188). IEEE.
30. Botza Y., Shaw M., Allen P., Staunton M., and Cox R., Boughman M., Roberts C., & Rominger W., (2008), Configuration and Performance of IEC 61850 for First-Time Users – UNC Charlotte Senior Design Project, in Schweitzer Engineering Laboratories (SEL) journal: USA, pp. 1-11.
31. Brand, K. P., Lohmann, V., & Wimmer, W. (2003). Substation automation handbook. Bremgarten: Utility Automation Consulting Lohmann.

32. Cadwallader, L. C., & Eide, S. A. (2010). Component failure rate data sources for probabilistic safety and reliability. Process Safety Progress, 29(3), 236-241.
33. Carlson, C. S. (2014). Understanding and applying the fundamentals of FMEAs. In Annual Reliability and Maintainability Symposium (RAMS 2014). Colorado Springs, CO, USA.
34. Carter, W. C. (1982), A time for reflection, in the proceeding of 12th Int. Symposium On Fault-Tolerant Computing, pp. 41, Los Angles, The United States.
35. Carvalheira, E., & Coronel, J. (2014, October). Testing the protection system in IEC 61850 communication based substations. In ANDESCON, 2014 IEEE, Bolivia.
36. Castillo, E., Gutiérrez, J. M., & Hadi, A. S. (1997). Sensitivity analysis in discrete Bayesian networks. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 27(4), 412-423.
37. Čelebić V., Kabović A., Kabović M., Gajica J., & Salom I., (2016), Solutions for the Alternative Route of the Teleprotection Communication Channel , First South East European Regional CIGRÉ Conference, Portoroz 2016.
38. CEN/CENELEC/ETSI, (2011), Standards for Smart Grids, Final report of the CEN/CENELEC/ETSI Joint Working Group on 4 may 2011.
39. Chen L., Zhan K., Xia Y., & Hu G., (2013), Structure Design and Performance Analysis of Substation Area Backup Protection Communication Network in Smart Substation, in PRZEGLĄD ELEKTROTECHNICZNY "Journal of Electric Engineering", Vol. 89, No. 5, pp. 182-186.
40. Choi S., Kim C., Choi S., Kim I., & Jeong T., (2012), Communication Interconnection Network Architecture and Logical Devices Application, in International Journal of Software Engineering and Its Applications, Vol. 6, No. 3, pp. 75-80.
41. Chowdhury, A., & Koval, D. (2011). Power distribution system reliability: practical methods and applications (Vol. 48). John Wiley & Sons.
42. CIGRE, (2001), Technical Report, Ref.No.180 – Communication requirements in terms of data flow within substations. CE/SC 34 03, 2001, 112 pp. Ref. No. 180
43. Cooper, G. F. (1990). The computational complexity of probabilistic inference using Bayesian belief networks. Artificial intelligence, 42(2-3), 393-405.
44. Cowell, R. G., Dawid, A. P., Lauritzen, S. L., & Spiegelhalter, D. J. (1999). Probabilistic networks and expert systems. New York, NY: Springer-Verlag.
45. Cruz, R. L. (1991a). A calculus for network delay. I. Network elements in isolation. IEEE Transactions on information theory, 37(1), 114-131.
46. Cruz, R. L. (1991b). A calculus for network delay, part ii: Network analysis. IEEE Transactions on Information Theory, 37(1), 132-141.
47. Das, J. C. (2012) Safety and Prevention through Design: A New Frontier. Arc Flash Hazard Analysis and Mitigation, in Arc Flash Hazard Analysis and Mitigation, Piscataway, NJ, USA, IEEE Press, John Wiley & Sons, 2012, pp. 40-59.
48. Dempster, A, N. Laird & D. Rubin (1977). Maximum likelihood from incomplete data via the EM algorithm. Journal of the Royal Statistical Society, Series B 39, 1-38.
49. Dhaussy, M. (2002). Les méthodes de la sûreté de fonctionnement et leur utilisation : Fiabilité, disponibilité, maintenabilité, sécurité des systèmes électriques. REE. Revue de l'électricité et de l'électronique, (1), pp. 24-29.
50. Díez, F. J. (1993). Parameter adjustment in Bayes networks. The generalized noisy OR-gate. In Proceedings of the Ninth international conference on Uncertainty in artificial intelligence (pp. 99-105). Morgan Kaufmann Publishers Inc. CA: USA.

51. Díez, F. J., & Druzdzel, M. J. (2006). Canonical probabilistic models for knowledge engineering. Technical Report CISIAD-06-01, UNED, Madrid, Spain.
52. Dolezilek D., (2006). IEC 61850: What you need to know about functionality and practical implementation, in Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources (vol. 6, pp. 1-17).
53. Druzdzel, M. J., & Van Der Gaag, L. C. (2000). Building probabilistic networks: Where do the numbers come from. IEEE Transactions on knowledge and data engineering, 12(4), 481-486.
54. Dubrova, E. (2013). Fault-tolerant design (pp. 55-65). Berlin : Springer.
55. Ekhlat, M, M Salah Ibrahim and N. M. Kreama. (2007), Mediterranean and National Strategies for Sustainable Development: Energy Efficiency and Renewable Energy Libya - National study, Sophia Antipolis: UNDP
56. Enslin J., Ramakumar R., Mancini T., Messenger R., Ventre J., Hoogers G. (2006), Alternative Power Systems and Devices, in Dorf R. C., Electronics, power electronics, optoelectronics, microwaves, electromagnetics, and radar. CRC press.
57. European Commission, (2006), European Technology Platform – Smart Grids Vision and Strategy for Europe's Electricity Networks of the Future", retrieved 21/07/2016 http://www.ec.europa.eu/.
58. Farhangi, H. (2010). The path of the smart grid. IEEE power and energy magazine, 8(1).
59. Fernandes F, Borkar S., & Gohil J., (2014), Testing of Goose Protocol of IEC61850 Standard in Protection IED, in International Journal of Computer Applications, vol. 93, No. 16, PP. 30-35.
60. Fries, S., Hof, H. J., Dufaure, T., & Seewald, M. G. (2010). Security for the smart grid-enhancing IEC 62351 to improve security in energy automation control. Int'l. J. Advances in Security, vol. 3 No. 3-4, pp.169-183.
61. Fuhr R. & Tran V. (2015), Arc Flash Hazard -The Basics, www.powerstudies.com
62. George H., Dorsch N., Putzke M., & Wietfeld C., (2013), Performance Evaluation of Time-critical Communication Networks for Smart Grids based on IEC 61850, in 2013 IEEE INFOCOM Workshop on Communications and Control for Smart Energy Systems, pp. 43-48.
63. Georges, J. P., Rondeau, E., & Divoux, T. (2002). How to be sure that switched Ethernet networks satisfy the real-time requirements of an industrial application. In IEEE international symposium on industrial electronics, ISIE 2002 (Vol. 1, pp. 158-163).
64. Gradwell, B. (2017). Arc Flash\Blast, Safe by Design a Safety Integrity Level approach (SIL). In Electrical Safety Workshop (ESW), 2017 IEEE IAS (pp. 1-10). IEEE.
65. GridWise Architecture Council, (2005). "Interoperability Constitution Whitepaper, v1.1," December 2005.
66. Grover, M. S., & Van Hardeveld, T., (2014) International Standards on Maintainability and Supportability and Their Application to the Nuclear Industry, In Proc., 10th international conference on CANDU Maintenance, 25-27 May 2014, Toronto, Canada.
67. Gruhn, P., & Cheddie, H. (1998). Safety Shutdown Systems: Design, Analysis, and Justification. ISA.
68. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: communication technologies and standards. IEEE transactions on Industrial informatics, 7(4), 529-539.

69. Haffar M., Thiriet J. M., & Nachar M., (2010), A Hardware in the Loop module in an IEC61850 Co-Simulation platform for advanced substation automation system tests, in 2010 IEEE International Energy Conference and Exhibition (EnergyCon), pp. 859-864.
70. Henrion, M. (1989). Some practical issues in constructing belief networks Uncertainty in artificial intelligence 3. pp. 161-173 Elsevier, Amsterdam : North-Holland.
71. Henrion, M., Pradhan, M., Del Favero, B., Provan, G., & O'Rorke, P. (1996). Why is diagnosis using belief networks insensitive to imprecision in probabilities?. In Proceedings of the Twelfth international conference on Uncertainty in artificial intelligence (pp. 307-314). Morgan Kaufmann Publishers Inc.
72. Hill, D. J., Brannon, D. D., Ruhland, P. R., & Werner, J. M. (2014). Improving safety with IEC 61850 over long distance. In Electrical Safety Workshop (ESW), 2014 IEEE IAS (pp. 1-9). IEEE.
73. IEA (2009), World Energy Outlook 2009: Executive Summary, Paris: International Energy Agency.
74. IEA, (2011), International Energy Agency (IEA). Heat and Electricity in Libya 2011, Paris: IEA.
75. IEC 60050-191, (1990), International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service, Geneva, Switzerland.
76. IEC 60834-1 (1999). Teleprotection equipment of power systems - Performance and testing - Part 1: Command systems.
77. IEC 61784-3. (2010), "Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions".
78. IEC 61869-9, (2016), Instrument transformers - Part 9: Digital interface for instrument transformers, international std., International Electrotechnical Commission (ed1.0), Geneva, Switzerland.
79. IEC TC 57 (2003), International Standard IEC 61850-7-1: Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models, first edition: Geneva.
80. IEC TC 57 (2003), International Standard IEC 61850-7-4: Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes, first edition: Geneva.
81. IEC TC 57 (2003), International Standard IEC 61850-8-1: Communication networks and systems in substations – Part 8-1
82. IEC TC 57 (2003), International Standard IEC 61850-9-1: Communication networks and systems in substations – Part 9-1
83. IEC TC 57 (2003), International Standard IEC 61850-9-2: Communication networks and systems in substations – Part 9-2
84. IEC TC 57 (2003), Technical Report IEC/TR 61850-1: Communication networks and systems in substations – Part 1: Introduction and overview, first edition: Geneva.
85. IEC TC 57 (2005), International Standard IEC 61850-10: Communication networks and systems in substations – Part 10: Conformance testing, first edition: Geneva.
86. IEC TC 65 (2010). IEC 61508: Functional safety of E/E/PE: electrical, electronic, and programmable electronic safety related systems, International Electro technical Commission Std. Geneva: IEC, 2010.
87. IEC/IEEE 61850-9-3, (2016), Communication networks and systems for power utility automation –Part 9-3: Precision time protocol profile for power utility automation

88. IEC/TR 61850-90-4, (2013), Communication networks and systems for power utility automation-Part 90-4: Network engineering guidelines, IEC: Geneva.
89. IEEE 1584-2002, (2002), IEEE Guide for Performing Arc-Flash Hazard Calculations, Part 5.4, New York, NY: IEEE.
90. IEEE 242-2001, (2001), IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems (IEEE Buff Book), New York: IEEE.
91. IEEE 802.1Q, (2003) Edition - IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
92. IEEE PSRC, (2005). Protection Systems Relay Committee H6 SPECIAL REPORT Application Considerations of IEC 61850.
93. IEEE std. C37.2 (2008). Electrical Power System Device Function Numbers and Contact Designation, International Standard, New York: IEEE.
94. Ingram, D. M., Campbell, D. A., Schaub, P., & Ledwich, G. (2011, June). Test and evaluation system for multi-protocol sampled value protection schemes. In Proceedings of IEEE PES Trondheim PowerTech, 2011 IEEE Trondheim (pp. 1-7). IEEE.
95. IRE (Institute of Radio Engineers with Institute of Electrical and Electronics Engineers) National Convention (1953), Diagnostic programs and marginal checking for large-scale digital computers, In symposium, session 14: Convention Record of the Symposium, March 1953.
96. ITU-T G.8011/Y.1307, (2004). Ethernet service characteristics.
97. ITU-Y 1564, (2016), Ethernet service activation test methodology.
98. Jamborsalamati P., Sadu A., Ponci F., & Monti A. (2016), A Flexible HiL Testing Platform for Performance Evaluation of IEC 61850-based Protection Schemes, in Power and Energy Society General Meeting (PESGM), IEEE, pp. 1-5.
99. Jensen, F. V. (2001). Bayesian networks and decision graphs. New York, NY: Springer-Verlag.
100. Josephson M. (1959), Edison: a biography, New York: McGraw-Hill.
101. Juárez J., Rodríguez-Morcillo C., & Rodríguez-Morcillo J., (2012), Simulation of IEC 61850-based substations under OMNeT++, in 5th International ICST Conference on Simulation Tools and Techniques, pp. 319-326.
102. Kanabar M., & Sidhu T., (2011), Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying", in IEEE Transactions on Power Delivery, Vol. 26, No. 2, pp. 725-735.
103. Karady G.G. & Short T. (2006), Energy Distribution, in Dorf R. C., The Electrical Engineering Handbook, Systems, Controls, Embedded Systems, Energy, and Machines. CRC press.
104. Karady G.G. (2006), Conventional Power Generation, in Dorf R. C., Electronics, power electronics, optoelectronics, microwaves, electromagnetics, and radar. CRC press.
105. Khavnekar A., Wagh S., & More A., (2015), Comparative Analysis of IEC 61850 edition I and II standards for substation automation. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). pp. 1-6.
106. Kjærulff, U., & van der Gaag, L. C. (2000). Making sensitivity analysis computationally efficient. In Proceedings of the Sixteenth conference on Uncertainty in artificial intelligence (pp. 317-325). Morgan Kaufmann Publishers Inc.
107. Kubler, S., Robert, J., Georges, J. P., & Rondeau, É. (2012). Dual path communications over multiple spanning trees for networked control systems. Engineering Applications of Artificial Intelligence, 25(7), 1460-1470.

108. Kyriakopoulos, N., & Wilikens, M. (2000). Dependability of complex open systems: a unifying concept for understanding internet-related issues. In Proc. 3rd Information Survivability Workshop (ISW2000), pp. 24-26.
109. Langseth, H. (2008). Bayesian networks in reliability: The good, the bad, and the ugly. Advances in Mathematical Modeling for Reliability, Vol. 1.
110. Langseth, H., & Portinale, L. (2007). Bayesian networks in reliability. Reliability Engineering & System Safety, 92(1), 92-108.
111. Laprie, J. C. (1985). Dependable computing and fault-tolerance. Digest of Papers FTCS-15, pp. 2-11.
112. Laprie, J. C. (1992). Dependability: basic concepts and terminology in English, French, German, Italian and Japanese, in A. Avizienis, H. Kopetz, J.C Laprie (eds.), Dependable computing and fault tolerance systems (5), pp. 3-44, Vienna: Springer.
113. Lauritzen, S.L. (1995). The EM algorithm for graphical association models with missing data. Computational Statistics and Data Analysis 19. 191-201.
114. Lee, K. C., & Lee, S. (2002). Performance evaluation of switched Ethernet for networked control systems. In IECON 02 [Industrial Electronics Society, IEEE 2002 28th Annual Conference of the] (Vol. 4, pp. 3170-3175). IEEE.
115. Li F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y. & Zhang, P., (2010). Smart transmission grid: Vision and framework. IEEE transactions on Smart Grid, 1(2), 168-177.
116. Liang Y., & Campbell R., (2008), Understanding and Simulating the IEC 61850 Standard, in research report, Dept. of Computer Science, University of Illinois at Urbana-Champaign, USA, 12 pages.
117. Lindquist, T. M., Bertling, L., & Eriksson, R. (2008). Circuit breaker failure data and reliability modelling. IET generation, transmission & distribution, Vol. 2, No. 6, pp. 813-820.
118. Lopes Y., Muchaluat-Saade D., Fernandes N., & Fortes M., (2015), Geese: A Traffic Generator for Performance and Security Evaluation of IEC 61850 Networks, in IEEE 24th International Symposium on Industrial Electronics (ISIE), pp. 687-692.
119. Macdonald, D. (2003). Practical industrial safety, risk assessment and shutdown systems. Newnes.
120. Mackiewicz R., (2006), Overview of IEC 61850 and Benefits, in IEEE Power engineering society general meeting, IEEE: USA.
121. Mahlia, T. M. I., Saktisahdan, T. J., Jannifar, A., Hasan, M. H., & Matseelar, H. S. C. (2014). A review of available methods and development on energy storage; technology update. Renewable and Sustainable Energy Reviews, 33, 532-545.
122. McDonald J., (2001), Substation Automation, in Grigsby, L. L. (Ed.). The Electric Power Engineering Handbook. Boca Raton: CRC Press LLC.
123. McDonald J., (2007), Substation Automation Basics –The Next Generation, in Electric Energy Transmission and Distribution Magazine, May-June 2007 Issue.
124. McLinn, J. (2010). A short history of reliability, Reliability Review: The R&M Eng. J. March.
125. Megger, (2012) Circuit Breaker testing guide, Dover, UK.
126. Meier, S., Werner, T., & Popescu-Cirstucescu, C. (2016). Performance considerations in digital substations. In Development in Power System Protection 2016 (DPSP), 13th International Conference on (pp. 1-9). IET.

127. Melhart, B., & White, S. (2000). Issues in defining, analyzing, refining, and specifying system dependability requirements, In Proc. Engineering of Computer Based Systems 2000, (ECBS 2000), Seventh IEEE International Conference and Workshop on the (pp. 334-340). IEEE.
128. Merrill H. M., (2001) Power System Planning, in Grigsby, L. L. (Ed.). The Electric Power Engineering Handbook. Boca Raton: CRC Press LLC.
129. Mohagheghi S., Stoupis J., & Wang Z., (2009), Communication Protocols and Networks for Power Systems - Current Status and Future Trends, In Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES, pp. 1-9.
130. Morton, A., Dubray, K., McQuaid, J., & Bradner, S. (2012). Applicability Statement for RFC 2544: Use on Production Networks Considered Harmful.
131. Murphy K. (2002). Dynamic Bayesian Networks: Representation, Inference and Learning. PhD. University of California.
132. NFPA 70E, (2015). Standard for Electrical Safety in the Workplace, National Fire Protection Association, Quincy, Massachusetts, USA.
133. Nicol, D. M., Sanders, W. H., & Trivedi, K. S. (2004). Model-based evaluation: from dependability to security. IEEE Transactions on dependable and secure computing, 1(1), 48-65.
134. Olesen, K.G., Kjñrulff, U., Jensen, F., Jensen, F.V., Falck, B., Andreassen, S. & Andersen, S.K. (1989) A MUNIN Network for the Median NerveDA Case Study on Loops, in Applied Artificial Intelligence, vol. 3, pp. 385-404.
135. Oniśko, A. (2003). Probabilistic causal models in medicine: Application to diagnosis of liver disorders. In Ph. D. dissertation, Inst. Biocybern. Biomed. Eng., Polish Academy Sci., Warsaw, Poland.
136. Oniśko, A., & Druzdzel, M. J. (2013). Impact of precision of Bayesian network parameters on accuracy of medical diagnostic systems. Artificial intelligence in medicine, 57(3), 197-206.
137. Pearl, J. (1988). Probabilistic reasoning in intelligent systems: Networks of plausible inference. San Mateo, CA. Morgan Kaufmann Publishers.
138. Pearl, J. (2014). Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann.
139. Peirelinck T., Bratcu A., & Besanger Y., (2016), Impact of IEC 61850 GOOSE Communication Quality on Decentralized Reactive Power Control in Smart Distribution Grids– a Co-simulation Study, in 2016 IEEE Electrical Power and Energy Conference (EPEC), pp 1-6.
140. Pradhan, D. K. (1996). Fault-tolerant computer system design. Prentice-Hall, Upper Saddle River, NJ, USA.
141. PSERC, (2010), The 21st Century Substation Design, Publication 10-15, Final Project Report, Power Systems Engineering Research Center, Arizona State University
142. Pujolle, G., (2008). Cours Réseaux et télécoms [Network and Telecom Courses], (3em éd) in French, Edition Eyrolles, Paris.
143. Pukite, P., & Pukite, J. (1998). Modeling for reliability analysis: Markov modeling for reliability, maintainability, safety, and supportability, Wiley-IEEE Press.
144. Purewal S. & Waldron M.A. (2004). Functional safety in application of programmable devices in power system protection and automation. Eighth IEE International Conference on Developments in Power System Protection; Proc. Intern. Conf. Amsterdam 5-8 April 2004, pp. 295-298.

145. Rausand, M., & Hoyland, A., (2004). System reliability theory: models, statistical methods, and applications (2nd edition). John Wiley & Sons: The United States.
146. Rocca, L., Pinceti, P., & Magro, M. C. (2016). Can we use IEC 61850 for safety related functions? Transactions on environment and electrical engineering, 1(3), 35-40.
147. Røed, W., Mosleh, A., Vinnem, J. E., & Aven, T. (2009). On the use of the hybrid causal logic method in offshore risk analysis. Reliability engineering & System safety, 94(2), 445-455.
148. Ruggedcom Inc. (2008), Latency on a Switched Ethernet Network, Application Note 8, pp. 1-8.
149. Saleh, J. H., & Marais, K. (2006). Highlights from the early (and pre-) history of reliability engineering. Reliability Engineering & System Safety, Vol. 91, No. 2, pp. 249-256.
150. Sauter T. & Lobashov M. (2011). End-to-end communication architecture for smart grids. IEEE Transactions on Industrial Electronics, 58(4), 1218-1228.
151. Scheer, G. W., & Woodward, D. (2001). Speed and Reliability of Ethernet Networks for Teleprotection and Control. Schweitzer Engineering Laboratories, Inc., Vol 2. Pp 1-13.
152. Schossig, T., (2014), Functional testing of substations according to IEC 61850- A new approach. In 12th IET international conference on developments in power system protection (DPSP 2014), pp. 1-4.
153. Schwarz K., (2004), IEC 61850 and UCA™ 2.0: A Discussion of the History of Origins, retrieved online from www.nettedautomation.com on 22/05/2014.
154. Sichwart N., Eltom A., & Kobet G., (2013), Transformer Load Tap Changer Control Using IEC 61850 GOOSE Messaging, in Power and Energy Society General Meeting (PES), IEEE, pp. 1-5
155. Sidhu T. & Yin Y., (2007) Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems, IEEE Transactions on Power Delivery, VOL. 22, NO. 3, JULY 2007, pp. 1482-1489.
156. Siemens AG. (2013), SIPROTEC 5 Application, NoteSIP5-APN-009: Communication Architecture under Cyber Security Aspects, Nuremberg, Germany.
157. Siemens, (2011), Meantime Between Failures (MTBF): background information in MTBF V1.1 03.01.2011
158. Skeie T., Johannessen S., & Holmeide O., (2006), Timeliness of real-time IP communication in switched industrial Ethernet networks, IEEE Transactions on Industrial Informatics, vol. 2, no. 1, pp. 25 – 39.
159. Skendzic V. & Guzma A., (2006). Enhancing Power System Automation through the use of Real-Time Ethernet, in Power Systems Conference: Advanced Metering, Protection, Control, Communication and Distributed Resources, pp. 480-495.
160. Stanton K. N., Giri J. C., & Bose A., (2001), Energy Management, in Grigsby, L. L. (Ed.). The Electric Power Engineering Handbook. Boca Raton: CRC Press LLC.
161. Starck, J., & Kunsman, S. A., (2010). Pushing the limits, in Terwiesch, P. et al, (eds.) ABB Review Special Report IEC 61850, August 2010, ABB Group R&D and Technology, Zurich, Switzerland.
162. Strandberg, K. (1990). IEC/TC56–25 years of International Cooperation. R&M ISRM 90, Tokyo, Japan.
163. Tanenbaum A. S., & Wetherall D. J., (2011), Computer Networks, 5th edition, Pearson, Prentice Hall, The United States.

164. Thomas M., & Ali I., (2010), Reliable, Fast, and Deterministic Substation Communication Network Architecture and its Performance Simulation, in IEEE Transactions on Power Delivery, Vol. 25, No. 4, pp. 2364–2370.
165. Torres-Toledano, J., & Succar, L. (1998). Bayesian networks for reliability analysis of complex systems. Progress in Artificial Intelligence—IBERAMIA 98, 465-465.
166. UCAIug, (2004) IEC 61850-9-2LE (Light edition): Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2, Utility Communication Architecture International Users Group, Raleigh, The United States.
167. Van Engelen, R. A. (1997). Approximating Bayesian belief networks by arc removal. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(8), 916-920.
168. Van Hardeveld, T., & Kiang, D. (2012). Achieving Dependability Value for Pipelines and Facilities. In proc. 9th International Pipeline Conference 2012, pp. 531-540, American Society of Mechanical Engineers.
169. Veleba J., Buhawa Z., (2011), Perspectives of Large Wind Power Plant Installations to the National Transmission Power System of Libya, in Intensive Program "Renewable Energy Sources", University of West Bohemia, Czech Republic,
170. Verron, S. (2007) Diagnostic et surveillance des processus complexes par réseaux bayésiens. Sciences de l'ingénieur [physiques]. Université d'Angers, Français.
171. Verron, S., Tiplica, T., & Kobi, A. (2010). Fault diagnosis of industrial systems by conditional Gaussian network including a distance rejection criterion. Engineering applications of artificial intelligence, Elsevier, 23(7), 1229-1235.
172. Villemeur, A. (1992). Reliability, Availability, Maintainability and Safety Assessment, Assessment, Hardware, Software and Human Factors (Vol. 2). Wiley.
173. Von Krosigk, H. (2000). Functional safety in the field of industrial automation. The influence of IEC 61508 on the improvement of safety-related control systems. Computing & Control Engineering Journal, Vol. 11, No. 1, pp. 13-18.
174. Wadi M., Bara M., Carlson O., Elarroudi K., (2009), Voltage Stability Analysis for the South-West Libyan Electrical Power System: Problem Simulation and Analysis, in Proceedings of the 44th International Universities Power Engineering Conference (UPEC), Glasgow, UK, pp. 1-5.
175. Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence, 25(4), 671-682.
176. Xin J., & Duan X., (2005), A Priority-Based Transfer Scheme Based On Information Models In Switched Ethernet For Substation Process-Level, in journal of electrical and electronic engineering, 2005, Vol. 5, No. 2, pp. 1403-1409.
177. Zhang Y., Cai Z., Li X., & He R., (2015), Analytical Modeling of Traffic Flow in the Substation Communication Network. IEEE Transactions on Power Delivery, Vol. 30 No. 5, pp. 2119-2127.