Cape Peninsula
University of Technology

ALGORITHMS FOR COMMUNICATION CONTROL AND AUTOMATION IN A POWER SYSTEM NETWORK USING IEC 61850 STANDARD

by

Abdalla Yahia Daffalla Adam

Dissertation submitted in partial fulfilment of the requirements for the degree

Master of Engineering: Electrical Engineering (Smart Grid)

in the Faculty of Engineering and the Built Environment

at the Cape Peninsula University of Technology

Supervisor: Dr. M.E.S Mnguni
Co-supervisor: Mr. M Ratshitanga

Bellville
November 2022

DECLARATION

I, Abdalla Yahia Daffalla Adam, declare that the contents of this dissertation represent my own unaided work, and that the dissertation has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed **Date** 30/11/2022

ABSTRACT

Distributed energy resources are important components of the smart grid architecture. They play a key role in utilizing renewable energy sources and realizing the benefits of decentralized energy production. However, the distribution over geographically wide areas and the dynamic structures associated with distributed energy resources have imposed several challenges on utility systems. The IEC 61850 standard has established comprehensive information models and communication services that have achieved a great deal in solving interoperability issues between substations and distributed energy resources systems. Moreover, the IEC 61850 standard has simplified the design and engineering process when integrating new equipment by standardizing the information model for most distributed energy resources' devices. The standard has recommended the extensible messaging and presence protocol for communication over wide area networks due to its scalability and cybersecurity capabilities. Nevertheless, more challenges are associated with communications over wide area networks such as the increased cost of network bandwidth required for handling large volumes of data generated from distributed energy resources' sites and extended latency times. The research project addresses these challenges by building over mentioned standards and implementing the edge computing concept to communication systems of distributed energy resources. Edge computing refers to a concept where data analysis and decision-making capacity are shared amongst the network's endpoints "edge". It is a concept that is driving the Internet of things initiative which enables bringing central intelligence closer to data sources to reduce decision latency and response times. Hence, the proposed solution involves designing a model of an intelligent gateway that performs initial analytics on distributed energy resources sites' data. The gateway model is based-on IEC 61850 standard and utilizes the specified communication protocols which are the generic object-oriented substation event and the manufacturing messaging specifications for local area networks. Furthermore, the gateway model integrates the local area connection into a wide area network utilizing IEC 61850-8-2 XMPP standard. The primary aim of the research study focuses on investigating the impact of implementing an edge computing algorithm on the communication quality of service considering latency and bandwidth usage as performance indicators. The algorithm is designed to perform data fusion to reduce traffic on the communication network. Additionally, the research study takes a closer look at IEC 61850-8-2 XMPP-based communications to review the data exchange and cybersecurity mechanisms. The experimentation results have shown a significant enhancement of communication performance through the reduction of bandwidth and latency which was evaluated using the Wireshark packet-capturing software.

Keywords: Communication system, IEC 61850, Internet of Things, XMPP, smart grid, distributed energy resources, edge computing, RTDS.

ACKNOWLEDGEMENTS

I wish to thank:

- My mother and my family for their continued motivation, and support.
- My supervisor Dr M.E.S Mnguni for all the support and guidance. My gratitude is extended to my co-supervisor Mr M Ratshitanga, and the entire Centre for Substation Automation and Energy Management Systems (CSAEMS) led by Dr Carl Kriger for the motivation and support.
- Mr Eric Liu from Elipse software™ for all the technical support provided.
- Remarkably my dearest friends Mr Mohammed Hassan and Ms Mischka Lewis for their unlimited support from the start and throughout this journey.

The financial assistance of CPUT Postgraduate Bursary towards this research is acknowledged. Opinions expressed in this dissertation and the conclusions arrived at, are those of the author, and are not necessarily to be attributed to the CPUT Postgraduate Bursary.

DEDICATION

To My Mother
Artist: Amna Osman

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

Abbreviation/Acronym	
µs	Microsecond
µF	Microfarad
3PC	Triple Processor Cards
4G-LTE	Fourth Generation Long-Term Evolution
AC	Alternating Current
ACSI	Abstract Communication Services Interface
ADN	Active Distribution Network
ADSL	Asymmetric Digital Subscriber Line
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
API	Application Program Interface
ASN.1	Abstract Syntax Notation One
BER	Binary Encoding Rules
bits/s	bits per second
CC	Cloud Computing
CDC	Common Data Class
CFC	Continuous Functional Chart
CHP	Combined Heat and Power
CID	Configured IED Description
Cp	Coefficient of Power
CSV	Comma Separated Values
DA	Data Attribute
DC	Direct Current
DER	Distributed Energy Resource
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Space
DO	Data Object
DLL	Dynamic Linked Library
DSM	Demand Side Management
DSO	Distribution System Operator
DSP	Digital Signal Processor
DSTATCOM	Distribution Static Compensators
E2E	End-to-End
E2E SecProtocol	E2E Security Protocol
E2M	End-to-Middle
EC	Edge Computing
EMS	Energy Management System
EV	Electric Vehicle
FC	Functional Constraints
GBH	Global Bus Hub
GOOSE	Generic Object Orientated Substation Event
GoCB	GOOSE Control Block
GFA	Grid Friendly Appliances
GPC	Giga Processor Cards
GSSE	Generic Substation Status Event
GTFPI	Gigabit Transceiver Front Panel Interface

GTNET	Gigabit Transceiver Network interface
GTSYNC	Gigabit Transceiver Synchronization
GTWIF	Gigabit Transceiver Workstation Interface
GUI	Graphical User Interface
HAN	Home Area Network
HMI	Human Machine Interface
HTTP	Hyper Text Transfer Protocol
I/O	Input/Output
ICD	IED Capability Description
ICT	Information and Communication Technologies
IEC	International Electrotechnical Committee
IED	Intelligent Electronic Device
INS	Setpoint Information
IoT	Internet of Things
IP	Internet Protocol
IPsec	IP Security
ITU	International Telecommunication Union
JID	Jabber Identifier
kV	Kilo Volts
LAN	Local Area Network
LD	Logical Device
LN	Logical Node
ML	Machine Learning
MMS	Manufacturing Messages Specifications
ms	milliseconds
MX	‘Measurement’ functional constrain in IEC 61850 standard
NAN	Neighbourhood Area Network
NAT	Network Address Translation
OLE	Object Linking & Embedding
OPC-UA	OLE for Process Control - Unified Architecture
OpenADR	Open Automatic Demand Response
OSI	Open Systems Interconnection
PaaS	Platform as a Service
PDU	Protocol Data Unit
PMU	Phasor Measurement Unit
pu	per unit
PC	desktop workstation
PV	Photovoltaic
QoS	Quality of Service
R-GOOSE	Routable GOOSE
rad/s	Radiance per Second
RES	Renewable Energy Sources
RESTful	Representational State Transfer
RFID	Radio Frequency Identification
RISC	Reduced Instruction Set Computer
rms	Root Mean Square
rpm	revolution per minute
RSCAD	Real-time Simulation Computer-Aided Design
RTAC	Real-Time Automation Controller
RTC	Real-Time Collaboration

RTDS	Real-Time Digital Simulator
RTT	Round-Trip Time
RTU	Remote Terminal Unit
SaaS	Software as a Service
SASL	Simple Authentication and Security Layer
SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description
SCL	Substation Configuration description Language
SCSM	Specific Communication Service Mapping
SEL	Schweitzer Engineering Laboratories
SMV	Sampled Measured Values
SPS	Single Point Status
ST	Structured Text
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAV	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
VPN	Virtual Private Network
VPP	Virtual Power Plant
WAN	Wide Area Network
WS	Web Services
WSN	Wireless Sensor Network
XER	XML Encoding Rules
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

GLOSSARY

Term	
Abstract Communication Services Interface	a network independent interface that describes the semantics of communication services, data models, their attributes and defines their purposes.
Communication Quality of Service	a set of parameters that measure and quantify the performance of communication networks
Bandwidth	is the measure of the transfer rate capacity of a communication network defined as bits/seconds.
Latency	the time delay of communications between the sender and receiver.
Cloud computing	a concept in which the computing and storage resources are provided through clustered data centres that can be accessed and configured via Internet networks.
Distributed Energy Resources	relatively small-scale power generating plants that are connected to the grid mostly at distribution-level voltages. The energy sources can be renewable energy sources or fossil fuel.
Edge Computing	a concept in which data analysis and decision-making capacity are shared amongst the network's endpoints.
IEC 61850 standard	an object-oriented standard developed by the International Electrotechnical Committee (IEC) for communications of substation automation systems.
Internet of Things	an abstract concept of linking devices via Internet networks to exchange information and interact without human intervention.
Interoperability	is the ability of IEDs from different vendors to seamlessly exchange information and interoperate without the need for proxies and protocol gateways.
Specific Communication Services Mapping	is a part of the IEC 61850 standard that defines mappings to the Open System Interconnect (OSI) model layers, the syntax and encoding of the messages.

CHAPTER ONE
INTRODUCTION

1.1 Background

In recent times, there has been a growing paradigm shift toward renewable energy to replace traditional fossils energy. This global orientation has been largely propelled by the negative environmental impacts of fossils energy on the ecosystem. Moreover, the finite nature of fossils energy, presents a strategic threat to the future of energy supply. The smart grid initiative is the main driving framework of this orientation as it incorporates renewable energy utilization by dynamic structures such as Distributed Energy Resources (DERs), microgrids, and Virtual Power Plants (VPPs).

The smart grid can be described as an intelligent structure that manages the electrical power network. A smart grid incorporates decentralized Information and Communication Technologies (ICT), distributed management of electrical energy through renewables, storage systems, and automation systems. Furthermore, it comprises advanced features, such as demand response, microgrids, bi-directional communications, and other innovative solutions to enhance the infrastructure of energy delivery. As seen in figure 1.1 below, a conceptual diagram of the smart grid shows the integration of Renewable Energy Sources (RESs), and demand side being heavily involved in the smart grid communication platform (Sayed & Gabbar, 2017).

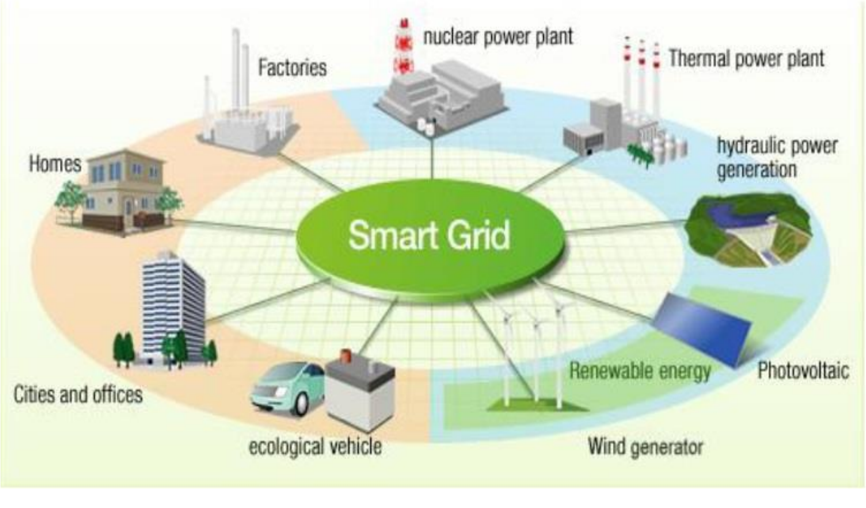


Figure 1.1: **An illustration of a smart grid architecture (Sayed & Gabbar, 2017).**

In a microgrid, DERs are controlled in coordination to enhance the productivity of power generation, minimize losses, ensure efficiency and security of power distribution (Mao et al., 2014). However, the geographically dispersed nature of DERs and their irregular generation of power, cause substantial technical challenges for utilities to efficiently manage and control DERs, and to ensure the stability and reliability of power supply.

Achieving interoperability is another challenge given the proprietary communication protocols and multi-vendor devices used in today's DERs systems. As well, most of these protocols are not equipped for cybersecurity over Wide Area Networks (WANs), which makes the utilities' communications systems vulnerable to cyberattacks and downtimes. In view of the abovementioned challenges, a need arise for standardization of communication architectures and data models for DERs, taking into consideration cybersecurity of data transfer over WANs (Liu & Gu, 2019).

The development of the IEC 61850 standard was a breakthrough in the communications systems of power grids. It provided solutions for the interoperability issues by adopting object-oriented modelling of information. The standard has enabled communications over advanced Ethernet technology. The initial scope of the standard was limited to Intelligent Electronic Devices (IEDs) inside Local Area Networks (LANs) of substations. Afterward, it was extended to provide information models for DERs defined in part IEC 61850-7-420. A more recent extension was published to enable communication over WANs by defining the specifications for mapping communication services to the eXtensible Messaging and Presence Protocol (XMPP) in part IEC 61850-8-2 (Liu & Gu, 2019). Yet, the growing penetration of DERs has significantly increased the amount of data exchanged across utilities' networks leading to various new challenges.

The substantial increase in communication latency is the most critical issue, in addition to the costs of bandwidth usage, cybersecurity threats and reliability. Such situation called for the prospect of adopting relatively new concepts from the Internet of Things (IoT) initiative for power systems communications. Specifically, the concepts of Edge Computing (EC) and data analytics are being extensively implemented within the industrial sector enterprises to address the concerns of high data traffic within their networks (Aslett, 2019). Tseng et al., 2018 have defined the EC as distribution of data processing capabilities in a manner that spreads throughout the communication routes from data sources to the cloud. The EC and data analytics have been increasingly adopted by utilities and the energy sector at large. Several factors are driving the growing acceptance of EC including its massive potential to enhance the communication performance, consequently, improving the overall efficiency and reliability of applications.

This thesis presents an implementation of an EC gateway model that monitors a remote DER integrated to a modern power network. The gateway model is based-on the IEC 61850 standard whereby it utilizes the communication protocols "Generic Object

Orientated Substation Event (GOOSE) and Manufacturing Messages Specifications (MMS)" which were specified by the standard for communications over a LAN. The gateway model integrates the LAN connection to a WAN utilizing IEC 61850-8-2 XMPP standard. The primary aim of the research study is, to investigate the impact of implementing an EC algorithm on the communication Quality of Service (QoS), focusing on latency and bandwidth usage as performance indicators. Additionally, the research study takes a closer look at the IEC 61850-8-2 XMPP standard to examine its data exchange and cybersecurity mechanisms.

In this introductory chapter, awareness of the problem, problem statement, research aim and objectives, motivation for the research project, hypothesis, delimitation of research, assumptions, the research methodology, and the documentation method are presented.

1.2 Awareness of the problem

The IEC 61850 standard information models and communication services have simplified the design and engineering work, which is required for the integration of devices and IEDs in the electrical grid. The standard is a key enabler of interoperability amongst multi-vendor devices and protocols. The need for communications over WANs has led to developments in the IEC 61850 standard to incorporate XMPP as a preference for communication over WANs. The XMPP standard is based-on the eXtensible Markup Language (XML) that provides flexibility and ease of use, it enhances the scalability of XMPP to suit applications of many sizes and several clients (Kuntschke et al., 2017; Saraiva et al., 2019).

The wide adoption and deployment of XMPP on the IoT architectures indicate the high scalability of XMPP because IoT applications require the downsizing of XMPP to suit edge devices with limited hardware and processing capacities. Furthermore, the XMPP standard provides strong cybersecurity schemes by integrating Transport Layer Security (TLS) protocol, peer authentication, and encryption of the data. Hence, applying and analysing XMPP and its implementation with IEC 61850, is crucial to driving more deployments of the IEC 61850-8-2 XMPP for communications over WANs in smart grids (Hussain et al., 2018; Nadeem et al., 2019; Wang et al., 2017).

Implementing the EC concept has found large acceptance from numerous industries and infrastructure sectors especially for monitoring applications. An essential driver to implement the EC scheme is to reduce network traffic by distributing data processing capacity throughout the network's edge devices. This advantage allows for reducing bandwidth usage and minimizing communication and decision-making latencies. The DERs sites present a viable use case for EC due to the large volumes of data generated in a single site. Therefore, implementing the EC concept and evaluating its impact on communication performance is critical for further deployments of the technology for DERs systems (Samie et al., 2019; Ullah et al., 2021; Chen et al., 2019).

1.3 Problem statement

The QoS of communication networks drastically impacts the operations of smart grids. Specifically, the integration of DERs and their management systems which are required to be efficient and reliable to ensure optimal performance. Challenges such as interoperability and high data traffic in smart grid networks, negatively impacts the communication QoS which is quantified via performance indicators such as bandwidth usage and latency.

The IEC 61850-8-2 XMPP standard was published to extend IEC 61850 to operate on WANs. However, there were few attempts in the reviewed literature to practically examine the IEC 61850-8-2 XMPP data exchange and cybersecurity mechanisms.

1.4 Research aims and objectives

1.4.1 Aims

The research aims to study the IEC 61850-8-2 XMPP standard for communications over WANs. Furthermore, the research aims to investigate the impact of the EC concept, from the IoT paradigm, on communication performance over WANs for DERs systems. The commenced research study includes designing and testing an intelligent gateway that perform initial data analytics and applies IEC 61850 and XMPP standards.

1.4.2 Objectives

The research study aims stated above, are achieved through the following objectives:

- To review and analyse the existing literature on the communication systems performance and their impact on power systems and smart grid operations.
- To review and analyse the literature on IEC 61850 and XMPP standards, and their applications in DERs communication systems.
- To develop a theoretical study on IoT and the concept of EC, and their existing applications in smart grids.
- To develop a simulation model based-on IEC 61850 standard of a power network integrated with a wind energy DER.

- To implement an intelligent EC gateway model, using a Real-Time Automation Controller (RTAC) SEL-3555” and IEC 61850 communication drivers from Elipse software™.
- To design a data fusion algorithm within the gateway model.
- To investigate the performance of the proposed scheme considering bandwidth usage and latency parameters by utilizing Wireshark software to capture the network traffic.

1.5 Hypothesis

Enhancement of the communication QoS is possible for DERs in remote sites, via the implementation of an EC gateway model that is equipped with an embedded algorithm for initial analysis of data before transmission over a network. The rationale of the research study is to develop a lab-scale testbed of a monitoring scheme and to examine the impact of EC on the communication performance and the results will be scalable to real-life applications.

1.6 Delimitations of research

The research project primarily focuses on the application of IEC 61850 and XMPP standards in communication systems of DERs and incorporates an EC algorithm to decrease data traffic in the network. Components of the proposed scheme will be implemented using the following software/hardware:

- The DER model will be simulated using a Real-Time Digital Simulator (RTDS)™ platform.
- The EC gateway model with the embedded algorithm will be implemented using RTAC SEL-3555 and IEC 61850 communication drivers from Elipse software™.
- The control centre or the cloud will be implemented using an IEC 61850 communication driver on Elipse Power application.
- The XMPP server will be implemented using Openfire from Ignite Realtime™ open-source community (Ignite Realtime, 2022).

The criteria for evaluation of the communication system performance will be based-on comparing bandwidth usage and latency in two test cases; with and without executing the data fusion algorithm, to determine its impact on the communication performance. The research’s limitations are described as follows:

- The implemented EC gateway model comprises an RTAC SEL-3555 unit and an Elipse Power application which is hosted on a desktop workstation (PC) machine. This setup significantly affects the communication performance due to the existence of multiple processing points on the communication route.

- The wind energy model which is simulated on RTDS transmits a limited number of data tags via IEC 61850-8-1 GOOSE protocol to the gateway model.
- An Internet-based WAN is utilized, yet all components of the testbed are located in the same room which would not provide a measure for communications over long distances.
- Evaluation of the communication performance is conducted using Wireshark software which captures network traffic for a specified period. Thereafter, the captured traffic would be analysed to determine bandwidth usage and latency.
- The evaluation of latency is based-on the Round-Trip Time (RTT) of data packets between each XMPP client and the XMPP server.

1.7 Motivations for the research project

The DER management systems allow the decentralization of electric power generation which addresses the increased demand for effective, reliable, and affordable electricity supply. The use of standards “IEC 61850 and XMPP” to manage DERs, results in simplified design procedures, reduced maintenance costs, and improved overall performance (Liu & Gu, 2019). The application of IEC 61850-8-2 XMPP standard is very promising due to the vast potential of XMPP in terms of cybersecurity mechanisms, which are critical in Internet Protocols (IP)-based public networks that are usually used by utilities to deploy their communication systems.

Embedding intelligence in devices at an edge of a network, is essential to address challenges of increased latency in response time created by large volumes of data that are transferred across networks (Tseng et al., 2018). Thus, enabling the capability of data analytics in DERs remote sites is viable due to the reduction of decision latency, improvement of data privacy and cybersecurity (Liu & Gu, 2019). Furthermore, edge data analytics can substantially reduce costs of communication bandwidth and facilitate optimization of components’ performance (Tseng et al., 2018).

The conducted data mining, revealed that considerable research has been carried-out to implement the EC within the smart grid architecture in various applications (Liao & He, 2020; Yang et al., 2019; Chen et al., 2019; Prajeesha & Anuradha, 2021; Tito et al., 2021; Li et al., 2021; Samie et al., 2019; Sirojan et al., 2019). Yet, a few attempts were carried-out to integrate the EC in DERs’ communication systems. The substantial added value that can be obtained through the EC, motivated the decision to investigate the application of this concept with IEC 61850 and XMPP standards to DERs systems.

1.8 Assumptions

An EC gateway device should be able to perform multiple functions including protocol mapping, data processing, and networks integration. The following assumptions are made for the purposes of this research study:

- The EC gateway model consists of two components which are RTAC SEL-3555 and ‘PC-1’ that hosts Elipse Power drivers. In the research project, they are assumed to be one entity for the evaluation of EC impact on communication QoS. Meaning that, the communication performance evaluation does not include the local area connection between the two components of the gateway model.
- The number of data tags from the power network model on RTDS, is assumed to be sufficient to provide solid and clear evaluation of communication performance.

1.9 Research design and methodology

The research aims to study and investigate the communications performance in smart grids systems by implementing an EC gateway model that is based-on IEC 61850 and XMPP standards for communications over WANs. The applied algorithm is designed to reduce the data volume to be transmitted over a network to minimize bandwidth usage and communication latency. The research methodology which is used to accomplish the research aims and objectives, consists of the following:

1.9.1 Literature review

A detailed review of the literature is carried-out focusing on the core components and topics of the research study which are:

- The impact of communication systems performance on smart grid applications.
- The IEC 61850-8-2 XMPP standard applications in DERs systems.
- The EC and data analytics applications in the smart grid structure.

Many resources are explored including but not limited to published articles, related textbooks, and google scholar.

1.9.2 Simulation

As noticed in figure 1.2 below, the illustration shows the system architecture for the proposed EC-based monitoring scheme. A model of a power network integrated with a DER, is simulated using the RTDS platform and transmits data using IEC 61850-8-1 GOOSE protocol over a LAN. The gateway model consists of RTAC SEL-3555 unit that forwards data to an Elipse Power IEC 61850-8-1 MMS client ‘Driver 1’. The Elipse

Power ‘Driver 2’ integrates the LAN connection to an Internet-based WAN and communicate to the control centre ’PC-3’ using IEC 61850-8-2 XMPP standard.

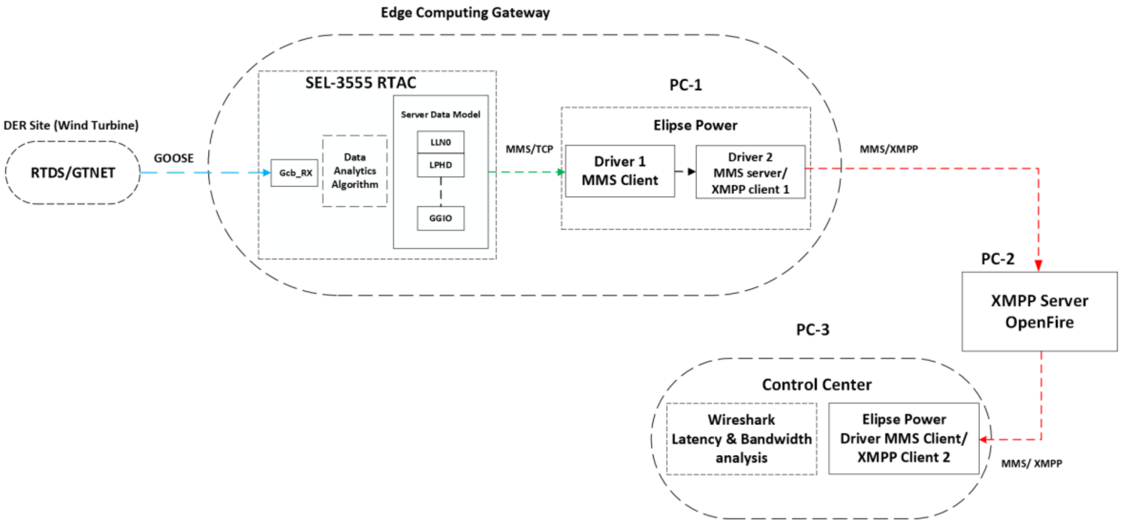


Figure 1.2: **A block diagram of the EC gateway lab-scale testbed.**

The communication performance is evaluated by capturing and analysing the network traffic using Wireshark packet-capturing software. The evaluation process will be based-on comparing the bandwidth usage and latency, in two cases, with and without executing the data fusion algorithm on the gateway model.

1.9.3 Documentation method

A thesis is written to document the theoretical studies and to describe the conducted simulations on the developed testbed. Moreover, discussions and analysis of the simulation results are documented as well. The thesis consists of six chapters described as follows:

- **Chapter One: Introduction**

  In this introductory chapter, awareness of the problem, problem statement, research aim, and objectives, motivation for the research project, hypothesis, delimitation of research, assumptions, the research methodology, and the documentation method are presented.

- **Chapter Two: Literature review**

  The chapter outlines a review of the existing literature on the research problem which is the impact of communication performance on smart grids operations. The review introduces the QoS indicators and their use in measuring the performance of communication networks. The review focuses on identifying the requirements for optimum performance and state-of-the-art technologies that are utilized in communication systems of power grids. Moreover, the review highlights the impact of the communication performance on operations in smart grids. Thereafter, the chapter reviews the literature on the research components including IEC 61850 and XMPP standards, and their existing implementations in communication systems of DERs within smart grids.

- **Chapter Three: Internet of Things applications in the smart grid**
  The chapter delivers an introduction to the IoT which is covering the common architectures of IoT networks. The chapter zooms into the features and structure of EC, and illustrates many benefits in terms of reducing computation and communication load in IoT networks. Furthermore, the chapter discusses the application of IoT and EC in smart grids and underlines massive opportunities for improving the performance in various domains of a smart grid including generation, transmission, and distribution.

- **Chapter Four: Implementation of the monitoring scheme testbed**
  The chapter describes the research testbed and configurations of each component to achieve the testbed objectives. Firstly, all the components are introduced including RTDS, RTAC SEL-3555 and Elipse Power software. The configuration of each component is described in details. Starting with the power network model on RTDS, and the configuration of IEC 61850-8-1 GOOSE communications. After that, the gateway model which consists of the RTAC SEL-3555 unit along with the Elipse Power communication drivers are described. The chapter outlines the configuration of the Openfire XMPP server application which is used in the testbed to enable IEC 61850-8-2 XMPP communications.

- **Chapter Five: The Edge Computing algorithm and network performance analysis**
  The chapter presents the analysis of communications in the developed testbed using Wireshark packet-capturing software. Firstly, the data exchange and cybersecurity mechanisms of the XMPP standard are examined by analyzing captured traffic. Secondly, the chapter describes the design of a data fusion algorithm which reduces traffic in a network. Thirdly, the chapter outlines an evaluation of the EC algorithm’s impact on the communication QoS, based-on Wireshark. The methodology of evaluation consists of, capturing the network traffic for an equal period of time, for two test cases; with and without execution of the EC algorithm. Wireshark Input/Output (I/O) Graphs tool and Microsoft Excel are utilized to analyze bandwidth usage and latency for both cases.

- **Chapter Six: Conclusions and recommendations**

  The chapter summarizes the work performed to achieve the aims and objectives of the research work. The chapter outlines the thesis deliverables which includes the research findings, recommendations for future work, publications from the thesis, academic, and industrial applications of the research study.

1.10 Conclusion

The chapter has provided an introduction for the research project by outlining the awareness of the research problem, the problem statement, and the research aims and objectives. The chapter has highlighted the motivations to answering the research problem. Furthermore, the hypothesis, assumptions and delimitations of the research were presented. Lastly, the research methodology described as it consists of the literature review, simulations, and documentations methods.

The following chapter presents the literature review which is conducted on the research problems, questions, and all components of the study. Many sources were reviewed and consulted including but not limited to journal papers, conference proceedings, and books.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

The concept of smart grids is realized through transformation of traditional power grids by incorporating advanced ICT in the grid structure. The advanced ICT infrastructure facilitates the deployment of emerging smart grids entities and applications, such as automated control, Advanced Metering Infrastructure (AMI), and integration of RESs. Furthermore, the smart grid achieves numerous objectives regarding grid performance such as enhancing reliability and quality of power delivery, minimization of costs, and reducing the environmental damage. Various applications and domains within smart grids have diverse communication requirements. Communication systems must satisfy these requirements to enable reliable operation of smart grid applications (Ghanem et al., 2020; Bhattarai et al., 2020; Kolenc et al., 2016).

Generally, the smart grid comprises interconnection of an extremely large number of devices from distinct vendors. Hence, interoperability is recognized as a critical requirement for the realization of smart grid objectives. Interoperability can be defined as the ability of devices from diverse vendors to interoperate and exchange information seamlessly without the need for proxies and gateways. Interoperability can only be achieved through standardization of information and communication systems. Therefore, many international bodies and research efforts have focused on developing and implementing different standards for communication systems in a smart grid (Worighi et al., 2019; Panda & Das, 2021; Ancillotti et al., 2013).

The IEC 61850 is one of the most prominent standards for communication systems in smart grids. The IEC 61850 standard defines object-oriented information models of power system functions, in addition to defining a variety of communication services for information exchange. The standard was primarily designed for substation automation, operating on LANs inside substations. As a result of the proven success of the standard's information models in achieving interoperability, it has been extended to provide DERs systems modelling. Consequently, the IEC 61850 standard was extended to operate on WANs to accommodate DER systems due to their usual deployment in large-scale geographical areas (Honeth et al., 2011; Sanchez et al., 2018; Huang et al., 2016).

Several previous studies in the reviewed literature have proposed multiple protocols and standards as middleware for IEC 61850 such as Object Linking & Embedding (OLE) for Process Control - Unified Architecture (OPC-UA) and Web Services (WS).

However, the XMPP standard has been chosen by the International Electrotechnical Committee (IEC) for communications over WANs. The XMPP is an open-source communication standard that is based-on XML, and it is widely utilized on the Internet for instant messaging and other applications. The XMPP has many advantages in terms of scalability, cybersecurity, and other features that were recognized by the IEC. Hence, it was specified as the middleware solution for IEC 61850, and the extension ‘IEC 61850-8-2’ was published to define specifications for mapping to XMPP. In the reviewed literature, the XMPP standard was explored with regards to its applications as a middleware for IEC 61850 in DERs communication systems, showing a number of benefits in terms of communication system enhancement (Shin et al., 2016; Nadeem et al., 2019; Aftab et al., 2018).

The smart grid involves integration of multiple sensors and intelligent devices for control and monitoring of operations. These devices exchange massive amounts of data across communication networks in smart grids. The high increase in data traffic negatively impacts the performance of communication networks in terms of the QoS. Monitoring QoS metrics such as latency, bandwidth, and packet loss ratio provide quantifiable indicators of the level of communication performance. The successful operation of a smart grid highly depends on the performance of the communication systems. Numerous research efforts in the reviewed literature have focused on the impact of communication QoS on the performance of several smart grid applications. Various factors affecting QoS were identified, in addition to proposing and developing different methodologies and techniques to enhance communication QoS (Vallejo et al., 2012; Kolenc et al., 2016; Ghanem et al., 2020).

Handling vast amounts of data generated by smart grid devices and enhancement of communication QoS were the main motivations for researchers to explore the potential of incorporating technologies from the IoT paradigm in smart grids. The EC is a key concept that has been investigated in the reviewed literature for application within the smart grid. It is a concept of embedding intelligence, data processing, and decision-making capacities in the network edge devices such as gateways. Thus, the EC eliminates the need to transmit all generated data to a central processing facility over a network. Instead, processing of data takes place at the edge near the devices “data sources”. This results in reducing data traffic in communication networks, which will lead to significant improvements of communication QoS (Samie et al., 2019; Prajeesha & Anuradha, 2021).

The research study attempts to develop a solution to enhance the communication QoS for monitoring DER systems in remote locations. The proposed solution is an EC gateway model based-on IEC 61850 and XMPP standards. The gateway model utilizes GOOSE and MMS protocols specified in IEC 61850-8-1 for local area communications with a model of a power network integrated with a DER. It applies IEC 61850-8-2 XMPP standard for communications over a WAN to a control centre model. Moreover, the gateway model executes an algorithm for data fusion before transmission of data over the network to enhance communication QoS in terms of bandwidth and latency.

The chapter provides a theoretical background from the reviewed literature on the QoS requirements of communication systems in smart grids. Firstly, to identify common communication requirements in smart grids, and secondly, to provide insights on the impact of communication QoS on various applications in smart grids. Thirdly, a review is conducted on IEC 61850 standard to identify its structures, features, and implementations in WANs. Thereafter, the review zooms into IEC 61850-8-2 mapping to XMPP, initially, describing the XMPP standard, then, examining the exchange and cybersecurity mechanisms of IEC 61850-8-2 XMPP. Finally, a literature review is conducted on applications of the IEC 61850-8-2 XMPP standard in DER systems.

The chapter is constructed as follows, section 2.2 introduces the communication requirements and QoS parameters for smart grid applications. The section highlights the communication technologies and the impact of communication performance on smart grid operations. Thereafter, section 2.3 presents description of DERs from the reviewed literature. Furthermore, the section underlines the communication requirements for DER communication systems. Section 2.4 provides a literature review on the IEC 61850 standard features, and performance over WANs. In section 2.5, the XMPP standard is introduced, and the IEC 61850-8-2 mapping to XMPP is described. The section delivers a literature review on IEC 61850-8-2 XMPP applications in DER communication systems. Section 2.6 provides the discussion and analysis of the literature review, and finally, conclusions are provided in section 2.7.

2.2 Communication systems in smart grid

A smart grid can be characterized as a highly advanced electricity grid that interconnects power supply and demand entities utilizing intelligent ICT infrastructure that allows for massive enhancements in power delivery in terms of reliability, safety, efficiency, long-term sustainability, cost reduction, and many other aspects (Saleh et al., 2019; Bouhafs & Merabti, 2011; Vallejo et al., 2012; Pourmirza et al., 2021).

In general, a core capability of smart grids is the automation of grid operations such as control, monitoring, protection, and service restoration or self-healing (Vallejo et al., 2012). The introduction of technologies such as advanced metering in smart grids enables demand response capabilities through extensive bi-directional interaction with consumers. A robust, secure, and pervasive communication infrastructure is crucial for achieving numerous smart grid capabilities especially DERs management and control (Saleh et al., 2019). Furthermore, a feature of smart grids is the increasing integration of distributed power generation as complementary to traditional centralized generation plants. The development of distributed generation schemes is mainly driven by the need to integrate RES such as Photovoltaic (PV), wind turbines, and fuel cells along with energy storage systems to support their operations. To facilitate optimal operation and control of DERs, they are clustered in many architectures such as microgrids.

The high reliance on communication systems for the success of smart grid operations makes it imperative to analyse the communication requirements in smart grids such as interoperability, QoS, and cybersecurity (Gonzalez-Redondo et al., 2016). A proper analysis of the abovementioned requirements would facilitate the design process and selection of the best technologies, standards, protocols, and topologies to achieve optimal performance. Therefore, it is of a high importance to analyse the impact of communication performance on smart grid operations (Saleh et al., 2019).

The communication performance is primarily measured through QoS metrics such as latency, bandwidth, and packet loss ratio. The following section presents a literature review on identifying the requirements of communication systems for multiple smart grid applications, describing communication QoS metrics and common technologies utilized in smart grid communication systems.

2.2.1 Communication requirements, technologies, and Quality of Service in smart grids

According to Ancillotti et al., 2013, the communication requirements for smart grids can be classified as qualitative and quantitative. The qualitative requirements describe the features that must be available in communication systems, while the quantitative requirements determine quantifiable performance metrics that must be maintained by the communication system. Typically, the qualitative are general requirements that are common to the whole communication system in a smart grid irrespective of the application. They include scalability, interoperability, flexibility, resiliency, feasibility, cost-effectiveness, and cybersecurity (Ancillotti et al., 2013, Bouhafs & Merabti, 2011; Ghanem et al., 2020).

There are numerous applications within the smart grid, such as demand response, DERs management architectures “microgrids and VPPs”, substation automation, wide area monitoring, protection, and control. Each application has specific communication requirements in terms of the expected traffic volume, the required coverage area, and strength (Ghanem et al., 2020). Furthermore, according to Bhattarai et al., 2020, the core communication requirements for any smart grid application include the response time and QoS that fall in the quantitative requirements category. QoS metrics include reliability, latency, packet delivery ratio, and bandwidth (Ancillotti et al., 2013; Bhattarai et al., 2020).

In alignment with the objectives of the research study, an emphasis is made on latency and bandwidth as performance metrics. Hence, in the following section, an analysis is conducted on these two parameters from the reviewed literature.

2.2.1.1 Quality of Service metrics “bandwidth and latency”

Monitoring networks’ QoS has been well established and utilized in communication systems to guarantee an adequate performance level of the system components to the user’s satisfaction (Kolenc et al., 2016). Previous research studies have considered analysing QoS requirements for communication networks in multiple smart grid applications. Bandwidth was the focus of Bouhafs & Merabti, 2011 as they have highlighted the need to consider optimal bandwidth in network design for handling large amounts of data from smart grid devices such as smart meters and wireless sensors.

Ghanem et al., 2020 have emphasised that, a network bandwidth should be sufficient to accommodate for the implementation of IP stacks and cybersecurity protocols. The authors have conducted a study on IP-based networks to measure the impact of the overhead of two cybersecurity protocols, namely IP Security (IPsec) and TLS, on the network bandwidth. Results from the experimental testbed have revealed that implementing IPsec adds an overhead of 25% of the bandwidth depending on the network configuration. Combining both protocols “IPsec and TLS” adds a significant overhead estimated to be two to three times the bandwidth usage without applying the protocols. Moreover, Ancillotti et al., 2013 have noted the impact of network bandwidth on other QoS parameters. They have reported that, many research studies have recommended considering implementing communication systems with excess bandwidth to improve latency and packet delivery ratio.

Communication latency or delay time was defined by Bhattarai et al., 2020 as the time it takes to successfully transfer a packet of data over a network channel. According to the authors, latency depends on several factors including network topology, available bandwidth, and the efficiency of utilized technologies and protocols. Vallejo et al., 2012 have studied the information delivery times or latency specifications of communication in substations for protection, recovery upon failure, monitoring, and control according to the requirements defined in the IEC 61850-5 standard. The authors have noted that, these requirements would apply to electrical distribution networks, as the whole grid operates on one cycle “16.6 – 20 milliseconds (ms)”.

The QoS of any communication network mainly depends on the topology and technologies used to build that network. Therefore, in the following section, a review of the common technologies for WANs is outlined.

2.2.1.2 Wide area communication technologies

In general, communication requirements vary across the hierarchical architectures of smart grid systems from field level to control centres and data management level. That was reported by Saleh et al., 2019 where the authors have presented a multi-layer communication system architecture for a cluster of microgrids as shown in figure 2.1 below. The architecture consists of lower-layer Home Area Networks (HANs), connected by middle-layer Neighbourhood Area Networks (NANs), and a WAN on the top layer. Each layer has specific communication requirements considering speed, coverage range, and QoS. Typically, WANs and NANs should have much wider coverage ranges and higher bandwidth than HANs.

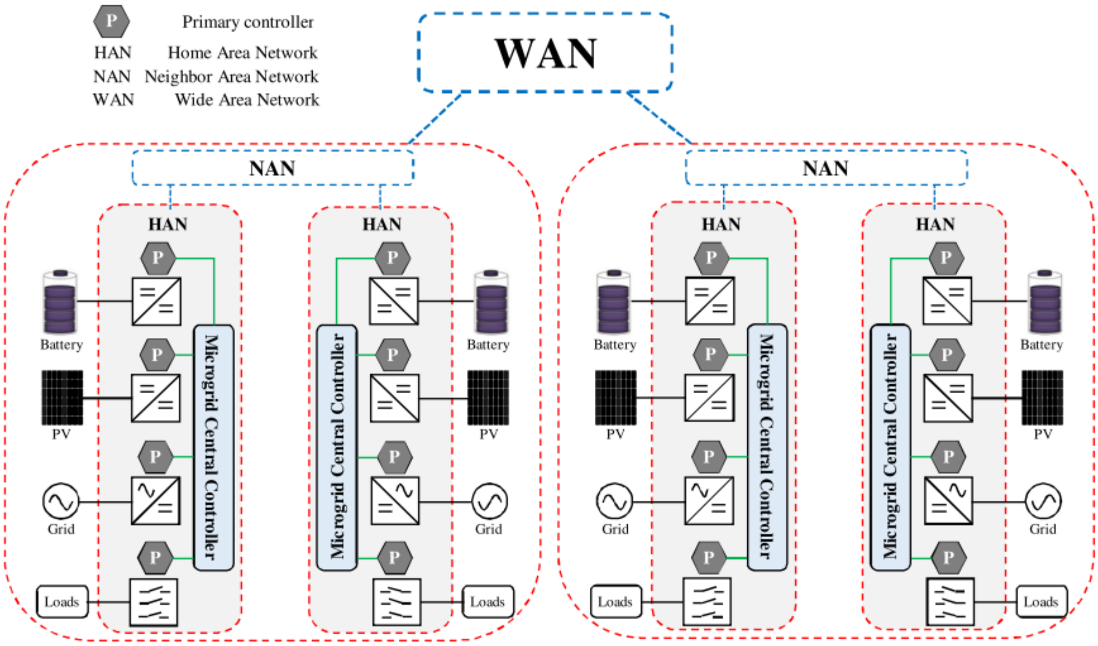


Figure 2.1: A hierarchical communication architecture in a smart grid (Saleh et al., 2019).

The communication requirements must be thoroughly defined for any smart grid application to determine the most suitable communication technologies (Bhattarai et al., 2020; Ancillotti et al., 2013). The requirements and suitable technologies for multiple communication network types are listed in table 2.1 below, which provides standard values for the bandwidth, coverage area, and latency requirements. The bandwidth is the transfer rate of data and is measured in bits per second (bits/s). It is noted that, a strict latency requirement "less than ten ms" is specified for the NANs, therefore, the technology must be suitable for such application.

Table 2.1: Requirements and suitable technologies for communication networks (partial) (Bhattarai et al., 2020).

Type	Coverage	Bandwidth	Latency	Technologies
LAN	1000 ft^2	1-10 Kb/s	< 2 s	WiFi, Zigbee
NAN	1-10 mi^2	10-100 Kb/s	< 10 ms	WiMAX, LTE
WAN	1000 mi^2	500 Kb/s – 10 Mb/s	< 50 ms	Ethernet, fibre optics

In the research project, the focus is on WAN communications, which can be deployed using wired or wireless mediums. Wired mediums such as fibre, Ethernet cables, and power lines are well established and widely utilized due to their superior performance compared to wireless links. This was reported by Kolenc et al., 2016, where the authors have conducted an experimental study that compared the communication performance of a wired link and a cellular one. The results have shown the superior performance of wired links. However, wireless technologies are gaining momentum in deployment due to numerous advantages which were reported in the reviewed literature.

Ghanem et al., 2020 have discussed the advantages of utilizing wireless technologies for secondary substations automation, as they are cost-effective and easy to deploy. Saleh et al., 2019 have suggested that, wireless mediums could be used as backup for wired mediums to increase reliability and to prevent network congestion. The authors have presented features and average latencies of the most common wireless technologies, in table 2.2 below.

Table 2.2: Comparison of some wireless communication technologies (Saleh et al., 2019).

Technology	Zigbee	LTE M2M	HSPA M2M	WiFi
Average delay (ms)	50 - 140	30 – 40	10 - 26	Up to 300
Coverage range	Short	Wide	Wide	Short
Main features	Low cost, power & scalable	Reliable	Low latency	Ease of use

The IP-based networks are considered to be the optimal solution for communication over WANs in smart grids. The advantages of using IP-based networks were discussed in numerous studies in the reviewed literature. For example, Zeinali & Thompson, 2021 have argued that IP-based networks would satisfy many communications requirements in smart grids including high speed, reliability, and sufficient bandwidth for large data volumes. The authors have presented a broad evaluation of public IP-based networks in the United Kingdom, to provide a guideline for deployment of smart grid applications. The evaluation metrics included statistical latency and reliability of data which were recorded over six weeks' period. Extensive tests were conducted on a client/server testbed using five different wired and wireless technologies with various combinations and configurations using transport layer protocols, which are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The evaluation results have verified the superiority of TCP in reliability and latency (Zeinali & Thompson, 2021).

Vallejo et al., 2012 have considered pervasiveness, low cost of deployment, and interoperability as key advantages of IP-based networks to support their suitability as a solution for smart grids. Nonetheless, the authors have highlighted the fact that, the distributed nature of a smart grid architecture dictates the use of multiple communication technologies to build the optimum communication system. Finally, the communication requirements highly influence the decision of whether to employ dedicated Virtual Private Networks (VPNs), public IP-based networks, or a hybrid model of both (Ancillotti et al., 2013). However, Zeinali & Thompson, 2021 have emphasised that, the cost of deployment is a decisive factor in preference of using public IP-based networks instead of VPNs.

The section showed the significance of defining communication system requirements including QoS requirements of smart grid applications. The selection of suitable communication technologies that will result in optimal performance is essential. The importance of communication systems has played a critical role in motivating plenty of research to study the impacts of communication performance on operations of smart grids. The following section presents a review of the literature on evaluating the communication performance impact on applications of smart grids with a major emphasis on DERs systems.

2.2.2 Impact of communication performance on smart grid operations

It is evident from the reviewed literature that, the communication system represents the backbone of modern smart grids. The successful operation of smart grid functions critically depends on the performance of communication systems. Consequently, any failures in the communications system could prove catastrophic, especially for key applications such as monitoring, protection, and control. Such effects were reported by Wang et al., 2016, they have highlighted the consequences of communication system failures such as high latencies, data loss, and interruption of service in the power system operation. Such failures can cause consecutive faults in the power system resulting in total blackouts in severe cases. The authors have provided a number of examples, such as cascading failures of transmission system protection in south China which occurred due to high latency and data errors. Similarly, blackouts in south London, United States of America, and Canada in the year 2003, were caused by either receiving faulty data or communication interruptions.

The successful integration and management of DERs systems, depends heavily on the communication system. Thus, the focus of numerous research efforts to evaluate the impact of communication performance on DERs operations. Saleh et al., 2019 have simulated a centrally controlled microgrid which comprises of multiple DERs, by using mathematical models to examine the impact of communication latency on the operation. According to the results, the impact of latency varies with two parameters, the mismatch current and the capacitance ratio of the power electronics converters.

The authors have argued that, since the mismatch current is an unpredictable factor, hence, manipulating the capacitance ratio of converters represents a physical solution to minimize the impact of communication latency. The study outcomes have recommended that, the design process of microgrids should consider several factors to achieve optimal performance. The factors include expected communication system’s latency, protection settings, capacitance ratio of converters, simulation, and testing before deployment.

Besides numerical and mathematical methods, cyber-physical simulations using many software were adopted in a number of research studies. Bhattarai et al., 2020 have conducted a cyber-physical co-simulation of a microgrid control/power system to examine the impact of latency on stability of power system operations. Three scenarios of communication network’s status were simulated which are ideal, congested, and congested with integration of Grid Friendly Appliances (GFA). The simulation results have showed that, the congested network scenario yielded a significant communication latency which drove the power system to an unstable state. This effect was mitigated by applying the GFA devices which apply an under-frequency load shedding scheme that helped to maintain the balance.

A study conducted by Wang et al., 2021 has applied a cyber-physical simulation approach, and has aimed to evaluate the communication performance impact on frequency control services provided by DERs in a power grid. In the simulation model, a frequency control signal is sent from the control centre to DERs every four seconds. The open-source Python library "ANDES" was utilized to record the dynamic responses of DERs and the system frequency (ANDES, 2022). The simulation results have demonstrated that, increased communication latency raises the risk of system instability. Zwartscholten et al., 2020 have employed MATLAB Simulink™ to evaluate the impact of communication latency on stability of the control system of Active Distribution Networks (ADNs) comprising integrated DERs. The parameters of interest of the control system were the settling time, overshooting, and stability. From the simulation results, it was observed that, there is a strong correlation between latency and all three parameters. In particular, the correlation between latency and settling time follows an exponential form that indicates the existence of a threshold latency range beyond which the system becomes unstable.

The previewed studies have revealed the large impact of communication system performance on operations of smart grid applications, focusing on DERs systems. Hence, there's a high motivation to study and improve the performance of communication systems to ensure optimal operations of smart grids. Therefore, in the research project, a solution of an intelligent gateway was proposed to enhance communication performance over WANs for DERs in remote sites. Bandwidth usage and latency are selected as QoS metrics for performance evaluation.

The section provided insights on the impacts of communication system performance on smart grid operations. Particularly on DERs management systems, which are the focus in the research project. Consequently, the following section provides a review of DERs, their definitions, functions, and types of information exchange in their management systems. As well, their most common communication requirements are identified from the reviewed literature.

2.3 Distributed energy resources

In recent years, the global warming phenomenon has intensified recording significant surges in temperatures across the globe. The greenhouse effects of Carbon Dioxide gas from fossils energy are the major drivers of global warming. Bearing in mind, the electrical power sector is leading in fossils energy consumption. As a result, the RESs must be used intensively to provide clean and safe electricity supply, and to achieve long-term sustainability. In addition to addressing global warming and other environmental motives, utilizing renewable energy extends access to electrical power and enhances energy security (Chang et al., 2022).

The reliable and sustainable utilization of renewable energy and the increasing orientation towards energy sector deregulation are key factors encouraging the shift from centralized to distributed generation. These factors have motivated the advancements in distributed generation technologies to increase efficiency and reduce costs of power generation. The DERs can be defined as small-scale generation units integrated on either transmission, distribution, or demand side in power grids. The integration of DERs in power grids can serve numerous purposes such as peak load services, or they can directly supply specific loads and areas in the isolated mode (Adefarati & Bansal, 2016).

The DERs can utilize either non-renewables or RESs, and a single DER can provide energy production, storage, or a combination of both services. A number of factors dictate the selection of a geographical location of a DER, including the atmospheric conditions “for renewable energy”, power demand, and land logistics (Honeth et al., 2011). Adefarati & Bansal, 2016 and Choobkar & Rahmani, 2019 have identified multiple benefits for integrating DERs in distribution networks in terms of reliability, minimizing power losses, and enhancing the voltage profile. Consequently, improving the grid resiliency, efficiency of power delivery, and reducing service interruption. Hence, substantial economic gains can be obtained from reducing power losses and minimizing investments in distribution and transmission systems.

Choobkar & Rahmani, 2019 have discussed options for interfacing DERs in power grids. A single DER can be coupled directly to the distribution or transmission systems, or it can be integrated within autonomous structures like microgrids or VPPs. Regardless, the exchange of information and control signals via a communication network are the keystone for the successful operation of DERs. Additionally, the authors have highlighted several factors to be considered when designing the interface of DERs including the following:

- DER size.
- Current output type “Direct or Alternating Current (DC/AC)”.
- The geographical location which determines the coupling point to the grid.
- The applied communication technologies.

The required data exchange type for the specified DER can be internal “between the DER controller and sensors”, or external “between the DER controller and grid management systems". Based-on these types of data exchange, the authors have identified multiple communication traffic profiles that can be used in DER systems, which include time critical "fast", periodic, event-driven, multicast, or broadcast messages. Thus, the communication infrastructure should be reliable enough to handle this variety of data exchange profiles, to carry-out energy management, monitoring, and control.

According to Ustun et al., 2011, typical functions of DER controllers include on/off switch control, which is the most basic function. Other functions are summarized as follows:

- Control of the interconnection to power systems components such as protection devices "switches and circuit breakers".
- Overall monitoring and control of numerous systems of DERs units, which include excitation systems, energy conversion, and auxiliary systems.
- Monitoring of the physical attributes of DERs devices such as heat, pressure, vibration, and atmospheric conditions.

The section presented a brief introduction to DERs and benefits of their integration in power grids. Additionally, the section underlined a variety of functions in DERs systems, and the data exchange profiles required for a successful operation of DERs. Hence, it is essential to identify the requirements of communication systems to optimally operate DERs. The following section provides a review of the literature on communication requirements for DERs systems.

2.3.1 Communication requirements for distributed energy resources systems

A core feature in smart grids is the massive incorporation of DERs, organized in the form of energy societies, microgrids, VPPs, or other aggregator entities. The trend has led to developing the concept of a prosumer-based energy system since consumers can produce power simultaneously. The concept has transformed all aspects of communication and data exchange, along with the operational and planning concepts of the traditional single-directional power system (Keserica et al., 2019). The bi-directional exchange of power and information in a smart grid creates a delivery network that is efficient and widely spread (Yan et al., 2013).

Previous research studies have highlighted major requirements for DERs communications systems. Gonzalez-Redondo et al., 2016 have discussed DERs management applications, they emphasized on the indispensable need for flexibility of the deployed communication system to accommodate the dynamic nature of DERs control architectures. As well, the authors have identified reliability, cybersecurity, and scalability to be essential requirements for these important smart grid structures. Whereas, Kolenc et al., 2016 have focused on VPPs, which are clusters of DERs coordinated to operate as a traditional power plant to provide ancillary services to the power grid. Both studies have agreed on, the imperative dependence of optimal operation of DERs control architectures on the communication system QoS level. Failure and poor communication performance can cause severe effects on the stability of the DERs systems operation leading to further power system instability and economic losses. Marzal et al., 2018 have underlined QoS requirements to accommodate the increased volume of data traffic in microgrids networks. They have summarized a range of latency and bandwidth requirements for a few microgrid applications as shown in table 2.3 below.

Table 2.3: QoS requirements for a few applications in microgrids (Marzal et al., 2018).

Microgrid Applications	Bandwidth	Latency
Demand Response	10-100 Kb/s	500 ms – few minutes
DERs & Storage systems	9.6-56 Kb/s	20 ms – 15 s
Distributed Management	9.6-100 Kb/s	100 ms – 2 s

The authors have emphasized that, the impact of insufficient communication bandwidth can cause bottlenecks, packet loss, and corruption. While, increased latency can cause severe electrical damages in the worst-case-scenarios. Furthermore, the authors have identified scalability and flexibility as key requirements for communication systems in microgrids. This is to accommodate the dynamic integration and removal of DERs in microgrids. Finally, the authors have underlined the need for redundancy and backup to avoid frequent failures. Additionally, Yan et al., 2013 have identified interoperability as a core requirement in DERs communication systems that must be addressed by standardization of the information models for all interconnected devices.

In conclusion, the prime communication systems requirements for DERs systems can be summarized as follows:

- Interoperability: to accommodate existing DERs devices from different vendors.
- Flexibility and Scalability: to address the dynamic nature of DERs with frequent installation and removal.
- Cybersecurity: due to the typical deployment of DER communication systems over public IP-based networks.
- QoS metrics including reliability, bandwidth, and latency.

Compelled by the abovementioned and other requirements of DER communication systems, standardization of communication systems has been considered as a key solution for the successful integration and operation of DER systems. The following section provides an introduction to the concept of standardization and its importance in smart grids and DER systems.

2.3.2 Standardization of distributed energy resources systems

Effective and seamless integration of DERs in power grids has been a paramount concern of many research efforts in the field around the globe. Zanabria et al., 2015 have noted that, the advanced ICT infrastructure in smart grids plays a key role to accommodate high penetration of DERs. Interoperability across all ICT architectures is identified as a critical requirement, it enables seamless integration of DER devices from diverse vendors (Ali et al., 2014).

Besides providing interoperability, another motivation for standardization is that, the developed standards should improve communication performance and accommodate any future developments (Timbus et al., 2008). Huang et al., 2016 have noted that, standardization would facilitate real-time monitoring which requires accurate data, an effective, reliable, and secure communication system. Therefore, standardization has been a great concern for various international organizations and entities. The IEC is a leading organization in the efforts of publishing standards for smart grids (Zanabria et al., 2015).

Timbus et al., 2008 have identified a set of attributes that must exist in communication standards for power systems, including openness, extensibility, and support for the device's self-description. One of the most prominent standards for smart grids is the IEC 61850 standard, which was mainly published for substation automation systems. Due to the massive success of the standard, it was later extended to include the modelling of DERs and wind turbine systems by publishing the parts IEC 61850-7-420 and IEC 61400-25 respectively (Yan et al., 2013; Ali et al., 2014; Zanabria et al., 2015). The section introduced the standardization of communication systems in smart grids. The following section presents a review of the IEC 61850 applications in DER systems.

2.4 IEC 61850 standard

The IEC 61850 refers to a series of standards that were issued by the IEC to provide a unified framework for the communication architecture of power systems (Huang et al., 2016). The IEC 61850 standard defines generic information models of power systems functions by using Data Objects (DOs) that can be organized in specific structures to perform the required task (Hänsch et al., 2018). Ali & Suhail Hussain, 2018 have defined information modelling as the process of producing unified syntax, semantics, and structures of data, to simplify information exchange across devices and systems. Thus, the result of the object-oriented modelling is a hierarchical data model, organizing DOs and Data Attributes (DAs), in Logical Nodes (LNs), and Logical Devices (LDs) as depicted in figure 2.2 below (Hänsch et al., 2018).

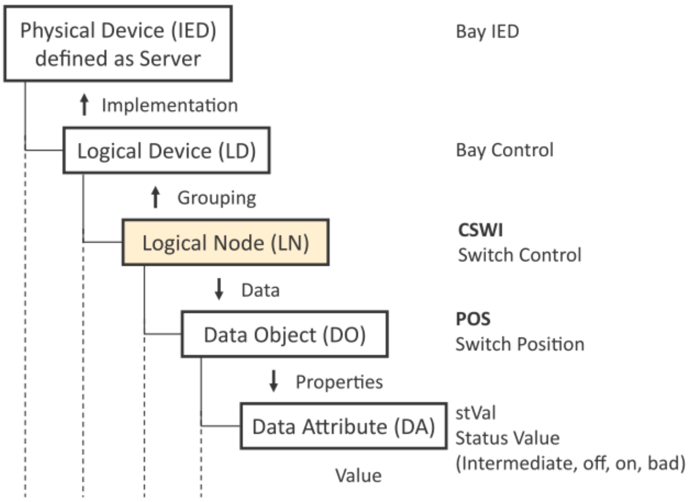


Figure 2.2: The IEC 61850 hierarchical data model (Hänsch et al., 2018).

Several LDs can exist in a physical device, and each LD consists of multiple LNs. Each LN represents a specific function, and comprises DOs, which consist of DAs, that contain the data values (Hänsch et al., 2018). The structure of a control switch LN ‘CSWI1’ is displayed in figure 2.3 below.

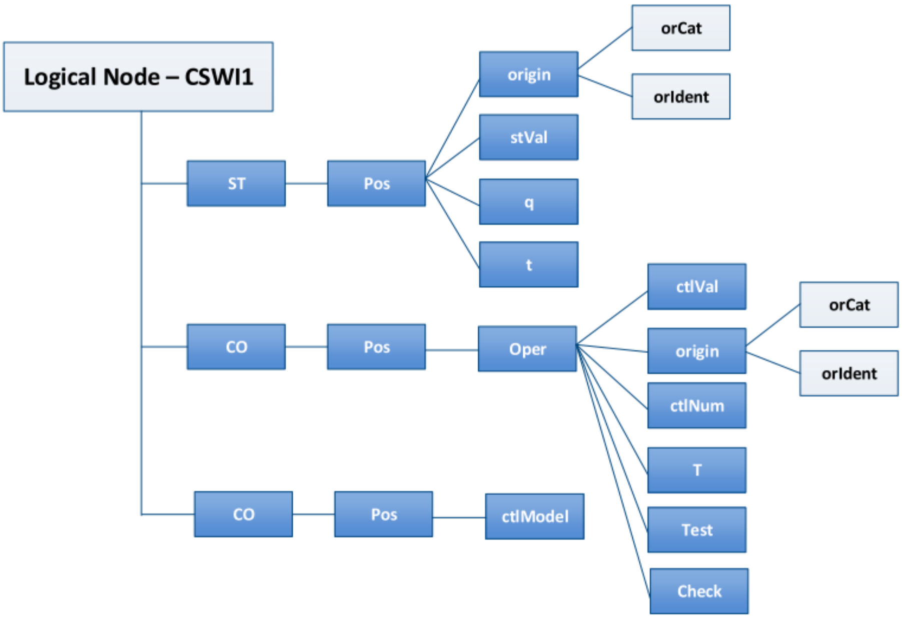


Figure 2.3: A structure of a LN instance (Keserica et al., 2019).

As noted from figure 2.3 above, the DAs are categorized according to Functional Constraints (FCs), such as ‘ST’ for status and ‘CO’ for control. The DOs are grouped according to their data types, into Common Data Classes (CDCs) such as Single Point Status (SPS) and Setpoint Information (INS) (Adamiak et al., 2009). The object-oriented approach for data modelling, provides the flexibility of design for developers and engineers, and simplifies the operation of power systems (Ustun et al., 2011).

The core of the IEC 61850 standard consists of ten parts, before extensions were later published. Parts “3, 4, and 5” define operational and communication requirements in substations. Parts “7-2” and “7-4” specify the abstract services and data models, while part “7-3” outlines CDCs which group DOs. Moreover, part “8-1” specifies the mappings of communication services and DOs to the MMS protocol. Part “10” specifies the conformance tests for equipment (Ali et al., 2014). Part “6” defines the System Configuration description Language (SCL), which is an XML-based language utilized to describe the data models and configurations of devices. The SCL files can easily be exchanged between devices and engineering software (Zanabria et al., 2015).

The IEC 61850 standard has achieved huge success and received wide acceptance in the power systems industry due to multiple benefits in terms of achieving simplicity of design and interoperability. According to Etherden et al., 2016, around ninety manufacturers around the world had produced IEC 61850 compliant devices by the end of the year 2013. The motivations by the smart grid initiatives, has led to numerous extensions for the standard to be published in order to cover many domains and applications within smart grid architectures. Extensions were published for the modelling of wind turbines “IEC 61400-25”, various DERs “IEC 61850-7-420”, and hydro power plants “IEC 61850-410” (Hänsch et al., 2018).

The IEC 61850-7-420 defines information models and services for DER devices such as PV, diesel generator, Combined Heat and Power (CHP), and fuel cells. The standard has specified LNs for various functions for the control and operation of DERs systems The LNs specified by IEC 61850-7-420, are illustrated in figure 2.4 below (Ustun et al., 2011). The information model standardizes internal and external communications of the DER controller such as interacting with a sensor, and with a microgrid management system, respectively (Choobkar & Rahmani, 2019). The information models of wind turbines are provided by the IEC 61400-25 standard extension, numerous LNs were specified to model the function of each part of a wind turbine.

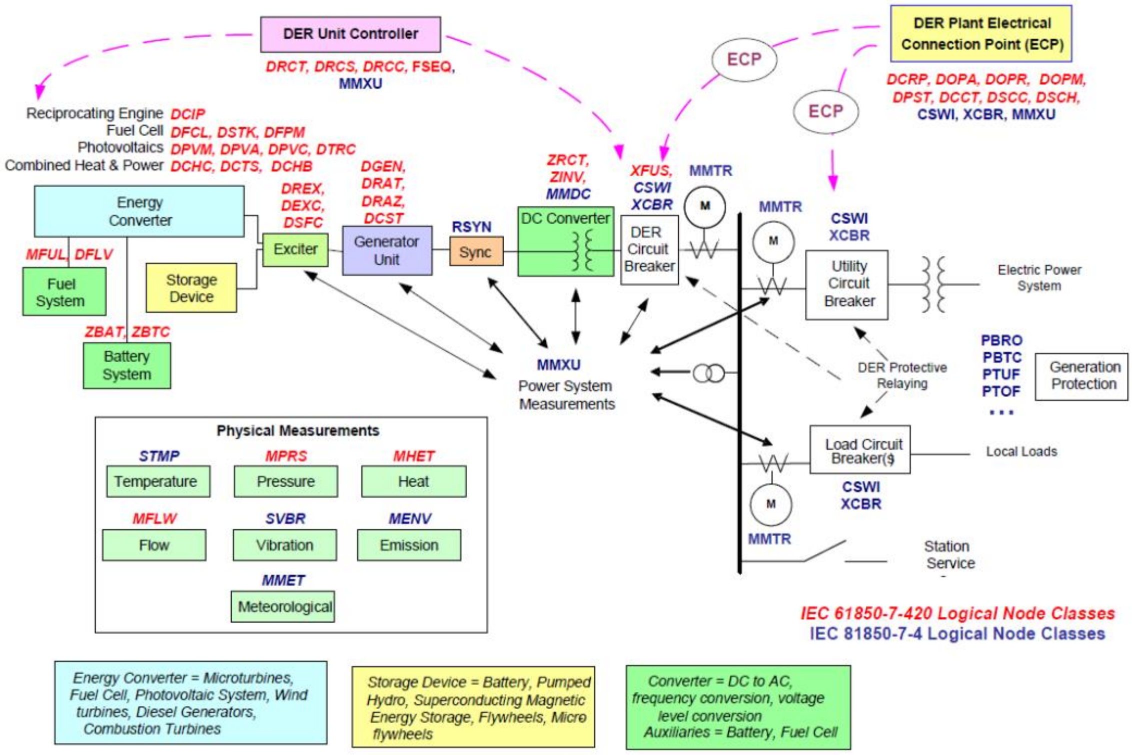


Figure 2.4: The IEC 61850-7-420 LNs (Ustun et al., 2011).

Turbine parts such as the rotor, generator, and yaw are mapped to their respective LNs ‘WROT’, ‘WGEN’, and ‘WYAW’. However, as shown in figure 2.5 below, the turbine coupling points to the grid are modelled by LNs from other parts of the IEC 61850 standard depending on the power system configuration.

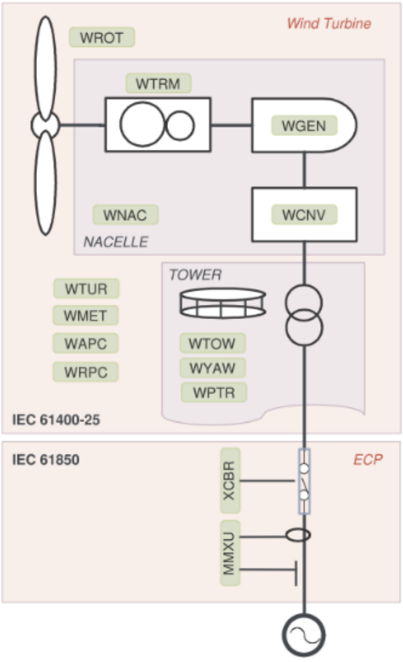


Figure 2.5: Modelling of wind turbine systems using IEC 61400-25 & IEC 61850 standards (Timbus et al., 2008).

In the research project, a DER model is developed, consisting of a wind turbine with an induction machine generator, integrated to a power network. The task performed on the model is monitoring of numerous mechanical and electrical parameters of the DER model via a communication gateway. The power network model is simulated in RTDS, whereby communication is handled by a virtual generic IED model that uses a GGIO LN to model the turbine and generator data. This virtual IED contains a GOOSE control block (GoCB) and transmits analog data to the gateway utilizing the GOOSE communication profile.

The following section provides a review of IEC 61850 standard communication services, their definition, and used protocols.

2.4.1 IEC 61850 communication services

The communication structure of the IEC 61850 standard involves several factors namely modelling of communication services, mapping to communication protocols, and the communications channel media (Ali & Suhail Hussain, 2018). Generic or abstract communication services are specified by the standard to execute various actions on information models of devices including Get/Set data values, control commands, file transfer, reporting, and logging. These services collectively formulate the Abstract Communication Service Interface (ACSI) which defines the information exchange for client/server interactions (Aftab et al., 2018; Hänsch et al., 2018).

The ACSI services specify standardized data exchange profiles for devices implemented as IEC 61850 servers. As a result, any IEC 61850-compliant client application can initiate and control an autonomous IEC 61850 subsystem. The following ACSI services are necessary for constructing smart grid management applications:

- Association ACSI: allows for bi-directional data transmission between client/server.
- Data model ACSI: allows for data model browsing and management.
- Settings group ACSI: allows for assigning a predetermined set of values for a set of DOs.
- Control ACSI: allows for relaying control instructions
- Reporting ACSI: allows for exchanging event-based data using a publish/subscribe mechanism.
- Logging ACSI: allows for logging and archiving the sequence of events (Keserica et al., 2019).

Besides ACSI, the standard specifies other communication profiles including Generic Substation Status Event (GSSE), GOOSE, and Sampled Measured Values (SMV). These profiles are designed for high-speed publish/subscribe interactions over a network. Additionally, time synchronization service messages are specified by the standard (Liang & Campbell, 2008). Each profile is mapped to a certain layer protocol of the Open System Interconnection (OSI) communication stack, depending on the profile characteristics and requirements (Adamiak et al., 2009).

As noticed in figure 2.6 below that, the GOOSE protocol is directly mapped to the Ethernet frame because it transferes high-speed “Type-1 and 1A” fast messages, according to the transfer time requirements as specified in IEC 61850-5 (IEC, 2004). Hence, the direct mapping removes the overhead of processing middle layers protocols (Adamiak et al., 2009).

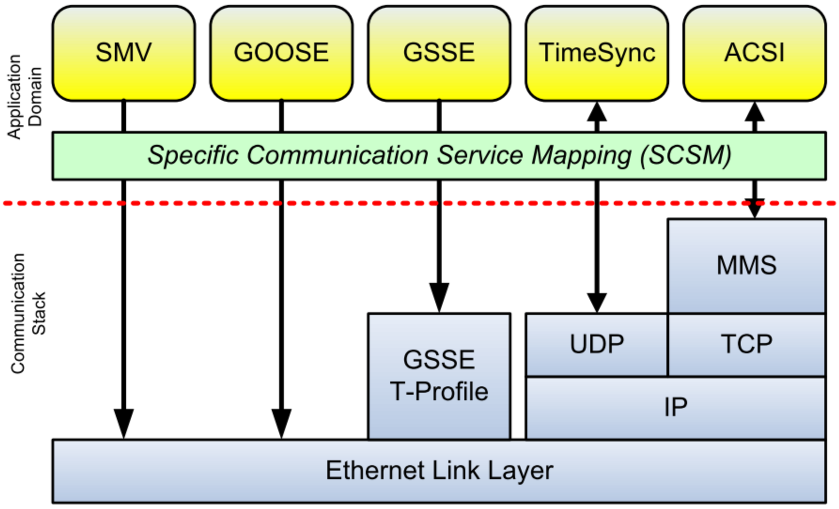


Figure 2.6: **IEC 61850 communication profiles (Liang & Campbell, 2008).**

The GOOSE messages are exchanged via a publish/subscribe mechanism controlled by an object model which is the GoCB. The publisher broadcasts GOOSE messages on the network and subscribers identify which messages to receive and process. The GoCB has a set of parameters to specify message identifiers, messaging frequency, and network specifications (Huang, 2018). The following section introduces mapping of ACSI services to MMS protocol as defined in part IEC 61850-8-1.

2.4.2 IEC 61850-8-1 mapping to manufacturing messaging specification standard

Specific Communication Service Mapping (SCSM) is the process of mapping ACSI services to application layer protocols (Aftab et al., 2018). Part IEC 61850-8-1 specifies the mapping of ACSI services and DOs to MMS standard which is selected due to its openness and high capacity of objects names and services, that perfectly suit the IEC

61850 standard structure. A part of ACSI services mappings to specific MMS services, and IEC 61850 objects mappings to MMS objects are demonstrated in table 2.4 below (Adamiak et al., 2009).

Table 2.4: **IEC 61850-8-1 objects and services mapping to MMS (partial) (Adamiak et al., 2009).**

IEC 61850 Objects	MMS Objects	IEC61850 Services	MMS Services
Logical Device	Domain	LogicalDeviceDirectory	GetNameList
Logical Node	Named Variable	GetDataValues	Read
Data	Named Variable	SetDataValues	Write
Data Set	Named Variable List	CreateDataSet	CreateNamedVariableList
Log	Journal	QueryLogByTime	ReadJournal
Log Control Block	Named Variable	Report (Buffered/Unbuffered)	InformationReport

The messages in MMS are described using the Abstract Syntax Notation One (ASN.1) standard, which specifies guidelines for encoding and decoding of protocol syntax to be transmitted over a network. In addition, it defines the sequence in which bits can be transferred over communication media using the Binary Encoding Rules (BER). The ASN.1 standard specifies relevant keywords for use by MMS and other protocols to facilitate the development of semantics and encodings (Falk & Burns, 1997).

Each element in the IEC 61850 data model is represented by a unique MMS Named Variable (NV). Each NV of a specific object consists of joining names of the hierarchy path of the object, separated using the letter “$” (Keserica et al., 2019). The MMS NV for the status value ‘stVal’ of a circuit breaker mode of operation ‘Loc’ is shown in figure 2.7 below, the NV shows the hierarchy path for the specified data value. Furthermore, the NVs for elements of the ‘CSWI1’ LN mentioned previously in section 2.3.2 are displayed in figure 2.8 below. The MMS standard is highly reliable and effective for communication over LANs in substations. The performance of MMS satisfies the time requirements specified in IEC 61850-5 for protection, monitoring, and control applications (Ali et al., 2014).

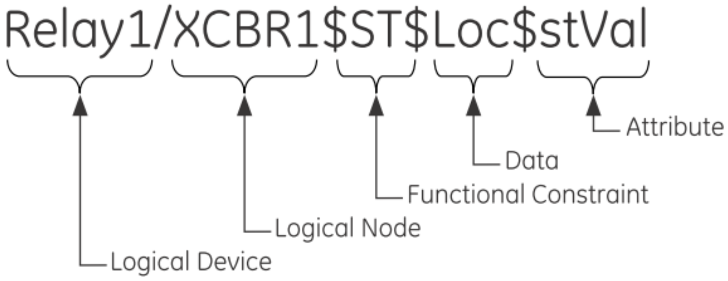


Figure 2.7: **An MMS NV structure (Adamiak et al., 2009).**

CSWI1

CSWI1$ST
CSWI1STPos
CSWI1STPos$origin$orCat
CSWI1STPos$origin$orIdent
CSWI1STPos$q
CSWI1STPos$t
CSWI1$CO
CSWI1COPos
CSWI1COPos$Oper
CSWI1COPos$Oper$ctlVal
CSWI1COPos$Oper$origin$orCat
CSWI1COPos$Oper$origin$orIdent
CSWI1COPos$Oper$ctlNum
CSWI1COPos$Oper$T
CSWI1COPos$Oper$Test
CSWI1COPos$Oper$Check
CSWI1COPos$origin$orCat
CSWI1COPos$orgi
CSWI1$CF
CSWI1CFPos
CSWI1CFPos$ctlModel

Figure 2.8: The MMS NVs for CSWI LN (Keserica et al., 2019).

Nevertheless, the MMS is unsatisfactory to solve the problems and challenges associated with communications over WANs in smart grids. Fundamental challenges such as cybersecurity and privacy have resulted from the fact that, public IP-based networks are used frequently to deploy smart grid communications on WANs (Hussain et al., 2018). Furthermore, a smart grid network architecture is subjected to continuous changes and expansion due to reasons such as the increasing dissemination of DERs.

These challenges necessitate a scalable network, that provides reliable and secure data exchange to ensure the stability of power systems (Liu & Gu, 2019). Extending IEC 61850 standard to operate on WANs has been a major concern in the reviewed literature. Consequently, several research studies have focused on evaluating IEC 61850-based communications in WANs and analysing the factors that impact the communication performance. In alignment with the objectives of the research study, the literature search is narrowed to the analysis of communication performance from QoS aspects specifically latency and bandwidth.

The search for a suitable middleware protocol to extend IEC 61850 for communications over WANs has received significant attention in the reviewed literature. A number of middleware protocols and standards were proposed, and their mappings to the IEC 61850 standard were provided. In addition to presenting discussions on the suitability of their applications within smart grid networks. In the following section, a review of the literature on the abovementioned points is provided.

2.4.3 IEC 61850-based communication over wide area networks

The performance of IEC 61850-based communications over WANs has been investigated by numerous research studies in the reviewed literature. Many simulation and implementation techniques were presented to provide insights on adapting the standard to wide area applications. In this section, the focus is on analysing the performance from aspects of QoS metrics, in particular latency and bandwidth usage. Transfer time or latency typically consists of two components which are time of transmitting data on a network, and the time to process data at both ends of the exchange “sender/receiver”. Therefore, the size and type of exchanged data determine the processing time on each side which directly affects the transfer time of messages.

Gonzalez-Redondo et al., 2016 have analysed the impact of IEC 61850 DOs and types on the transfer time of messages. They have developed a small-scale testbed for client/server communication to minimize the impacts of network conditions on transfer time to focus on data related influence. The test results has shown that, the total transfer time is directly impacted by the structure of data sets and LNs. They have noted that, this direct dependence must be considered when designing LNs and other IEC 61850 data models for diverse applications with different time requirements. However, the impact of network conditions in terms of deployed topologies and technologies, is essential to ensure the successful operation of any application.

Saraiva et al., 2019 have investigated the performance of IEC 61850 communication services over numerous topologies and technologies of WANs. The authors have implemented a testbed for IEC 61850 MMS client/server, GOOSE, and Routable GOOSE (R-GOOSE) communications. The IP and VPN topologies were used for the tests utilizing various commercial technologies including Fourth Generation Long-Term Evolution (4G-LTE), fibre optics, and Asymmetric Digital Subscriber Line (ADSL). The test results were positive in terms of satisfying transfer time requirements specified in the IEC 61850-90-12 guidelines for WAN communications.

The other QoS parameter under consideration in the research project is bandwidth usage. It is a critical parameter as insufficient bandwidth creates more latency and data losses which will lead to further negative impacts. Hence, IEC 61850-based communications were analysed in terms of bandwidth usage by several works in the reviewed literature. For example, Etherden et al., 2016 have implemented an IEC 61850-based communication architecture for VPPs over a WAN. They have investigated bandwidth usage of multiple IEC 61850 communication profiles including reporting, data polling “request/response”, and GOOSE services. The test results have shown that, high network bandwidth is required for IEC 61850-based communications. The authors have justified the outcome by the large volume of IEC 61850 DOs exchanged on the network such as object names, types, quality indicators, and timestamps. The authors have estimated that, IEC 61850 application layer protocol “MMS” consumes around three to ten times the bandwidth required for other protocols.

The high bandwidth usage by the IEC 61850 standard can be an unavoidable feature but it can be minimized using techniques such as converting from R-GOOSE to MMS as was reported by Wong et al., 2022. The authors have proposed a gateway model based-on the proxy gateway architecture for inter-substation communications over WANs which were specified in the IEC 61850-90-12 guidelines. The gateway maps IEC 61850 “Type-1, 1A” fast messages to TCP-based MMS protocol instead of UDP-based R-GOOSE for transmission over a WAN. The main objective is to eradicate the negative impact of R-GOOSE cyclic transmission which overloads network traffic. The gateway model was simulated to examine the communication latency and bandwidth over different communication link speeds. Results from the simulation has proven the feasibility of the gateway to save significant network bandwidth while maintaining latency within IEC 61850 standard transfer time requirements for fast messages.

According to the previewed research studies, it can be noticed that, the performance of IEC 61850-based communications, is more dependent on the size of data transmitted on a network compared to the network conditions. This is because in many cases there’s a limited ability to control network-related aspects in terms of technologies and hardware due to financial costs. Consequently, there is only a space for optimizing and reducing the data traffic to enhance communication performance. In the research project, the approach from Wong et al., 2022 was adopted in the developed testbed whereby values from the power network model are transmitted via GOOSE, then mapped to MMS by the gateway model. However, in the testbed of the research study, the MMS standard is not used for WAN due to the limitations which were mentioned in section 2.4.2 regarding scalability and cybersecurity.

Meanwhile, numerous research efforts have sought to extend the IEC 61850 standard for WAN communications by mapping to diverse protocols. For example, the OPC-UA standard “IEC 62541” was proposed by Lehnhoff et al., 2011 and Shin et al., 2016. The standard is highly efficient and powerful, nevertheless, its commercial aspects are considered a major flaw limiting deployments within smart grids. Similarly, the WS were suggested as middleware for IEC 61850, and mappings were described by Schmutzler et al., 2011 and Mercurio et al., 2009. However, amongst various middleware standards and protocols, the IEC 61850-8-3 technical report has recommended the XMPP as the solution for WAN communications in smart grids. This was due to multiple advantages of XMPP including its openness, decentralized architecture, high network extensibility, and strong cybersecurity measures (Hussain et al., 2018).

The following section presents an introduction to XMPP and the IEC 61850-8-2 specifications of mapping to the XMPP from the reviewed literature, highlighting the data exchange and cybersecurity mechanisms. In addition, the section reviews the literature on applications of IEC 61850-8-2 XMPP in smart grid applications specifically DER systems.

2.5 The extensible messaging and presence protocol

The XMPP is a message-oriented application layer protocol typically implemented over TCP network layer. It involves TLS End-to-End (E2E) encryption for securing communications over a network (Veichtlbauer et al., 2016). The XMPP is built using XML, which is a text-based markup language that describes data structures independent of the language and platform. The XML is extensible which means that, it enables different users to define their own data structures considering their requirements (Wang et al., 2017). The XMPP comprises two fundamental entities:

- **XML Stream**: it represents the vessel that encapsulates all XML elements to be exchanged between entities over a network. It is represented as a tag that describes the contents of the stream.
- **XML Stanza**: it represents the building block of an XML stream, contained in the stream tag (Kampars et al., 2021).

The XMPP forms a connection path through the stream and conveys the stanzas. There are three types of stanzas:

- **<iq>..</iq> info query stanza**: contains the requests Get/Set, and the responses Result/Error of exchanging information between entities.
- **<message>..</message> message stanza**: contains asynchronous information that is routed between two entities. The server is responsible for routing and delivering messages to recipients in real-time. The server supports storage and delayed delivery of messages depending on the network availability of recipients.
- **<presence>..</presence> presence stanza**: contains status information of an entity, mainly the entity’s availability on the network “online, available, and busy”. The stanza is published by clients to the server, and the server broadcasts it to clients associated with that client of origin (Hornsby et al., 2009; Kuntschke et al., 2017).

A stanza is the minimum amount of XML data that can be transferred between a client and a server in one package (Liu & Gu, 2019). It comprises identification of entities exchanging XMPP messages including address, type, and network status. A representation of an XML stream and stanzas is shown in figure 2.9 below (Kampars et al., 2021). A stanza is similar to a mail message, whereby the addresses of the message source and destination are specified with ‘from’ and ‘to’ attributes contained in the stanza (Liu & Gu, 2019).

```
<stream>
    <presence>
        <show/>
    </presence>
    <message to ='foo'>
        <body/>
    </message>
    <iq to ='bar'>
        <query/>
    </iq>
</stream>
```

Figure 2.9: The presence, message, and IQ stanzas in an XML stream (Kampars et al., 2021).

The XMPP standard specifies request/response “bidirectional” and publish/subscribe “multi-directional” communication modes. However, subscription is modular, meaning that entities can subscribe to specific XML stanza values of other entities such as a presence tag (Kampars et al., 2021). Furthermore, the XMPP adopts a client/server architecture (Nadeem et al., 2019). Similar to the email service architecture, clients register and connect to servers within their domain over a WAN to exchange XML stanzas (Veichtlbauer et al., 2016; Aftab et al., 2018).

The responsibilities of a server include saving messages of clients, managing connections between entities, and routing messages between clients. The XMPP standard uses a unique address called Jabber IDentifiers (JID) (Jun & Yang, 2021). A valid JID comprises numerous elements, including local parts, domain parts, and resource parts in a format “localpart@domainpart/resourcepart”. The architecture of an XMPP-based communication system is exhibited in figure 2.10 below, which shows client/server and server/server XMPP interactions, and communications with non-XMPP servers via ‘Protocol Gateways’ (Wang et al., 2017).

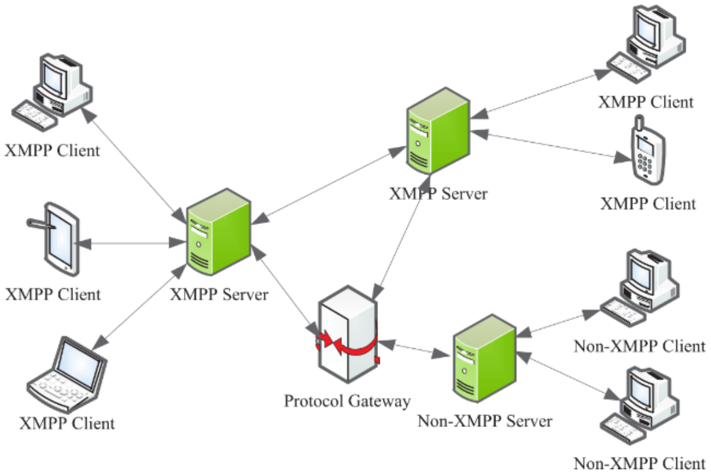


Figure 2.10: An XMPP communication architecture (Wang et al., 2017).

The JID for XMPP servers is expressed as “domain.org”, and for clients, the JID format is “client_name@domain.org”. The XMPP connections apply TLS which provides communication privacy and data integrity (Aftab et al., 2018).

The section introduced the basic concepts and structures of XMPP. It highlighted the scalable and extensible structure of XMPP due to the simplicity of adding client nodes to the network in addition to the TLS cybersecurity protocol specified by the XMPP. The following section introduces the mapping of IEC 61850 communication services to XMPP which was specified and published in part IEC 61850-8-2.

2.5.1 IEC 61850-8-2 mapping to the extensible messaging and presence protocol

The IEC 61850-8-2 standard specifies an SCSM for mapping IEC 61850 ACSI services to the XMPP. The standard adopted a serialization of MMS mapping, based-on ASN.1 XML Encoding Rules (XER) (ITU-T, 2001). Using this approach, the MMS request/response messages and reporting services, are mapped to the “iq and message” XMPP messages respectively (Hussain et al., 2018). The serialization of three types of ACSI services to MMS messages to XMPP stanzas are listed in table 2.5 below. The approach serves to simplify the adoption of XMPP for smart grid communications. It utilizes the power of XML to easily represent data from any namespace (Aftab et al., 2018).

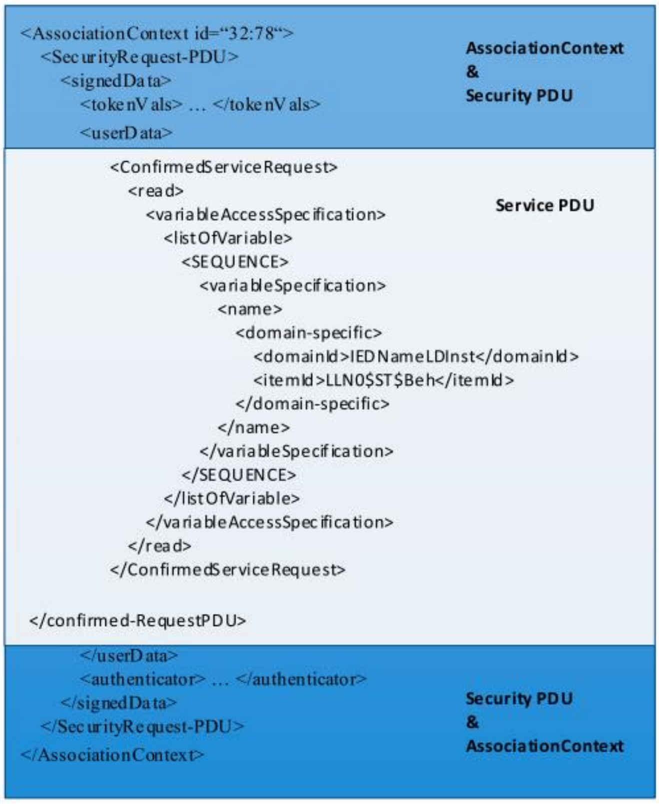
The XMPP architecture allows XML data to be streamed via an XMPP server. The IEC 61850 ACSI services are wrapped in XML stanzas which are then transmitted in a data stream from an XMPP client to the server, where it will be routed to a new XMPP client.

Table 2.5: **IEC 61850-8-2 SCSM ACSI services MMS serialization to XMPP (Aftab et al., 2018).**

ACSI Service	MMS-based SCSM	SCSM-2 (Serialized XMPP Stanzas)
SetGoCB Values	Write-MMS Request Write-MMS Response	IQ Type-Set IQ Type-Result
SendGOOSEMessage	GoosePDU	Message
GetDataValues	Read-MMS Request Read-MMS Response	IQ Type-Get IQ Type-Result

As seen in figure 2.11 below, a single XML message is made up of three distinct and layered parts which are described as follows (Keserica et al., 2019):

- **Service Protocol Data Unit (PDU)**: sits in the deepest layer of the stanza and implements the ACSI service. For each request/response message, it is stated as '<confirmed-RequestPDU> <confirmed-ResponsePDU>, or <unconfirmed-PDU>' for unsolicited messages.
- **Secure PDU**: wraps the service PDU and contains security information such as certificates and session keys. It is responsible for providing a secure E2E communication connection.
- **Association Context**: sends the attribute ID to establish and maintain the application association. It wraps both service PDU and secure PDU.



```
<AssociationContext id="32:78">
  <SecurityRequest-PDU>
    <signedData>
      <tokenVals> … </tokenVals>
      <userData>
          <ConfirmedServiceRequest>
            <read>
              <variableAccessSpecification>
                <listOfVariable>
                  <SEQUENCE>
                    <variableSpecification>
                      <name>
                        <domain-specific>
                          <domainId>IEDNameLDInst</domainId>
                          <itemId>LLN0$ST$Beh</itemId>
                        </domain-specific>
                      </name>
                    </variableSpecification>
                  </SEQUENCE>
                </listOfVariable>
              </variableAccessSpecification>
            </read>
          </ConfirmedServiceRequest>

   </confirmed-RequestPDU>
      </userData>
      <authenticator> … </authenticator>
    </signedData>
  </SecurityRequest-PDU>
</AssociationContext>
```

Figure 2.11: **An example of XML message contents (Keserica et al., 2019).**

The IEC 61850-8-2 XMPP standard specifies that, IEC 61850 devices are to be hosted by XMPP clients as depicted in figure 2.12 below (Liu & Gu, 2019). All XMPP clients are linked across a WAN to an XMPP server and given unique JID addresses (Nadeem et al., 2019). Client/server architecture is used in XMPP communication, whereby TCP/IP connections to an XMPP server are established by XMPP clients, and a TLS connection is negotiated. When the ‘IEC 61850 Client’ sends a request, its hosting ‘XMPP Client-1’ encodes and wraps the request in XER message format. The message is typically composed of security components that are wrapped around the encoded service PDU of the MMS message (Nadeem et al., 2019). Then, the XER request is forwarded to the ’XMPP Client-2’ through the XMPP server.

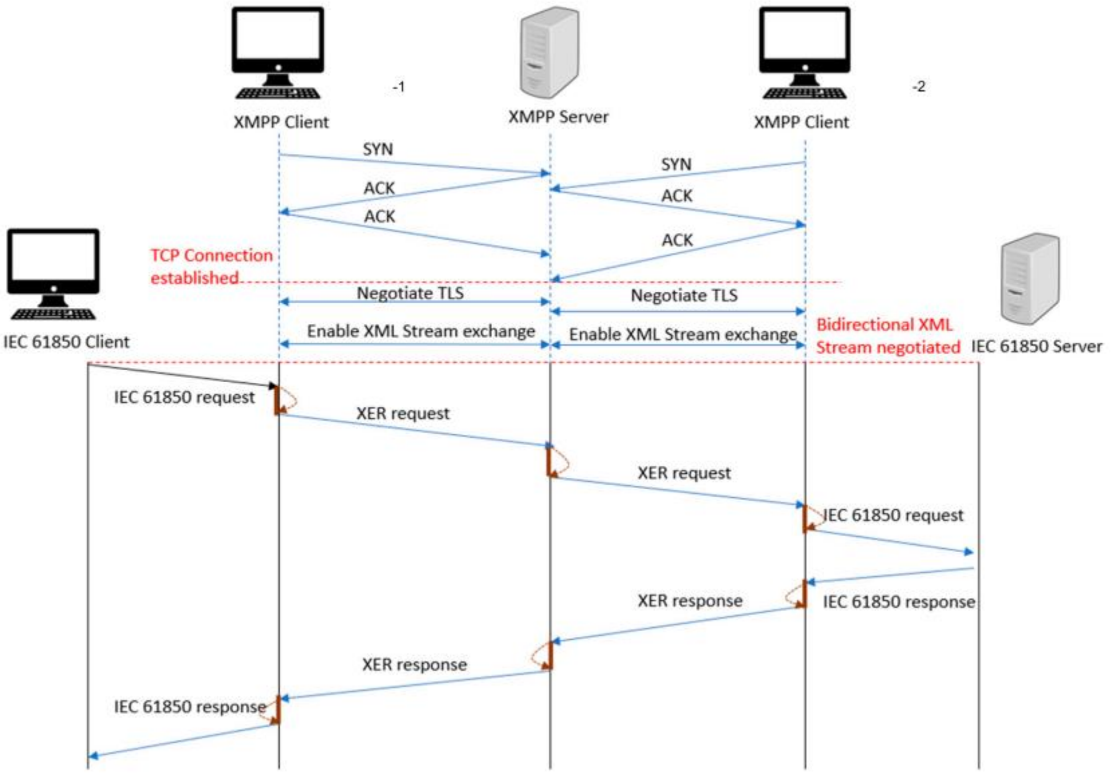


Figure 2.12: Communication flow according to IEC61850-8-2 XMPP (Liu & Gu, 2019).

The ‘XMPP Client-2’, which hosts the ‘IEC 61850 Server’, unwraps the XER message and reroutes the MMS request to the ‘IEC 61850 Server’ which responds to the MMS request. Thereafter, the ‘XMPP Client-2’ wraps the response message in XER message format and sends it back to the XMPP server which deliveres the response to ‘XMPP Client-1’. Finally, the ‘XMPP Client-1’ unwraps it to get the MMS response and delivers it to the ‘IEC 61850 Client’ (Liu & Gu, 2019). Considering the high importance of cybersecurity in WAN communications, the following section provides a detailed description of the cybersecurity measures as specified in the IEC 61850-8-2 XMPP standard.

2.5.2 IEC 61850-8-2 XMPP cybersecurity mechanisms

The communication networks and systems security standard “IEC 62351-1” stipulates several requirements for the security of smart grid communications including accessibility, integrity, authentication, and privacy (IEC TC57, 2007). The IEC 61850-8-2 XMPP communication interfaces are generally categorized as End-to-Middle (E2M) transport layer interfaces between the XMPP client/server or server/server, and E2E application layer interfaces between IEC 61850 client/server (Aftab et al., 2018). The Simple Authentication and Security Layer (SASL) and TLS protocols are implemented at the transport layer in E2M XMPP communications. The TLS protocol provides a channel encryption mechanism to secure it from tampering and eavesdropping (Saint-Andre, 2011). It implements an encryption cipher suite that is specified by the IEC 62351-4:2018 standard (Ustun & Hussain, 2020).

Once a TCP connection is created between XMPP client/server, a TLS connection is authenticated by exchanging initiation commands “STARTTLS” and any external certificates. Thereafter, a secure and encrypted transport layer channel will be established resulting in realizing integrity and confidentiality for E2M communications. Consequently, upon completion of a successful TLS negotiation, the SASL authentication messages are interchanged to verify end peers as authenticated users for the XMPP client/server channel (Saint-Andre, 2011; A. Melnikov, 2006).

The IEC 62351-4:2018 security standard defines an E2E Security Protocol (E2E SecProtocol) to secure MMS communication sessions. The protocol was adopted in IEC 61850-8-2 SCSM to achieve application layer E2E security (Ustun & Hussain, 2020). Upon establishing an association between IEC 61850 client/server, they exchange the E2E SecProtocol messages “Handshake_request and Handshake_accept” to authenticate each other as end points (Hussain et al., 2018). The cybersecurity measures in XMPP are illustrated in figure 2.13 below, which shows the integration of the TLS protocol with peer authentication (Liu & Gu, 2019).

In addition to all cybersecurity mechanisms provided by XMPP, there is one feature that stems from the client/server architecture of XMPP. All information exchanges are handled by an XMPP server that provides authentication and authorization services for all connected clients. Therefore, clients only need to use outbound communication services “e.g., outgoing messages” to connect to the server. Thus, eliminating the need for open communication ports “listening for connections” on the clients’ side which allows clients to communicate through Network Address Translation (NAT) gateways or firewalls and restricts cyber-threats (Kuntschke et al., 2017).

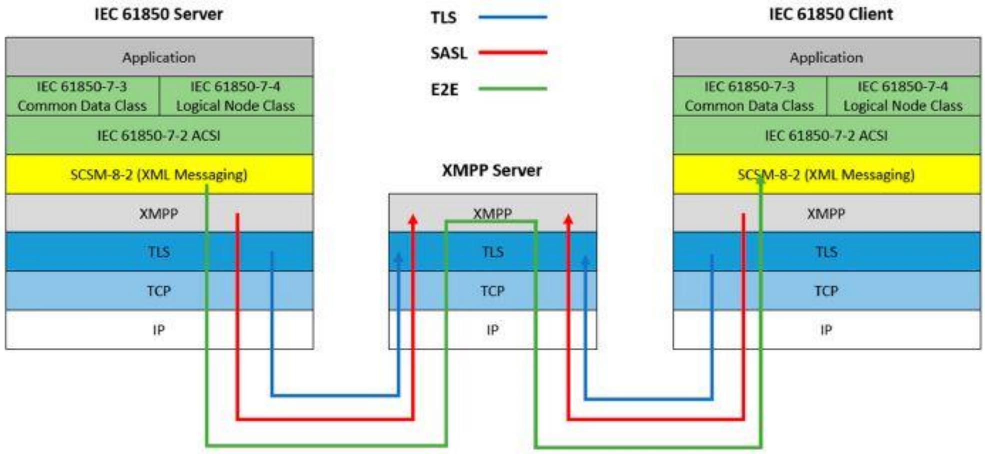


Figure 2.13: Cybersecurity mechanisms of XMPP (Liu & Gu, 2019).

In the section, the data exchange and cybersecurity mechanisms IEC 61850-8-2 XMPP standard has been described. In the following section, a review of the literature on applications of the standard within smart grids is presented. The review focuses on DER systems in alignment with the research objectives.

2.5.3 Literature review on applications of IEC 61850-8-2 XMPP standard

The IEC 61850-8-2 XMPP standard has been implemented in the reviewed literature for many applications. However, in alignment with the objectives of the research study, the literature review focuses on applications in DER systems. An argument can be made that, the main motivation to implement XMPP is to accommodate for the dynamic nature of DER networks, manifesting in the high frequency of DERs integration and dismantling. Furthermore, DER communication systems are typically deployed over public IP-based networks which require strong cybersecurity measures. Hence, the XMPP standard represents the optimal solution for DER communication systems due to its flexibility, scalability, and comprehensive cybersecurity suits.

Utilizing XMPP was suggested by Okuno et al., 2016 to enable interoperability for communications amongst application programs in smart grids such as demand response aggregators, Distribution System Operators (DSOs), and Energy Management Systems (EMS). Interactions between these entities might involve numerous standards including Open Automatic Demand Response (OpenADR 2.0b) and IEC 61850 standards as displayed in figure 2.14 below. The authors have proposed and implemented a common communication platform for EMS that utilizes XMPP to achieve interoperability and ease of integration. The platform comprises communication libraries for both standards that interact with an XMPP communication library. Additionally, the platform comprises common databases of information models and client/server services for each standard. The authors have stated that, the common platform approach is promising in terms of achieving interoperability and minimizing development time for EMS applications with multiple standards. Nonetheless, the authors have not provided an evaluation to support their claim and demonstrate evidence for feasibility of the approach for large-scale deployments.

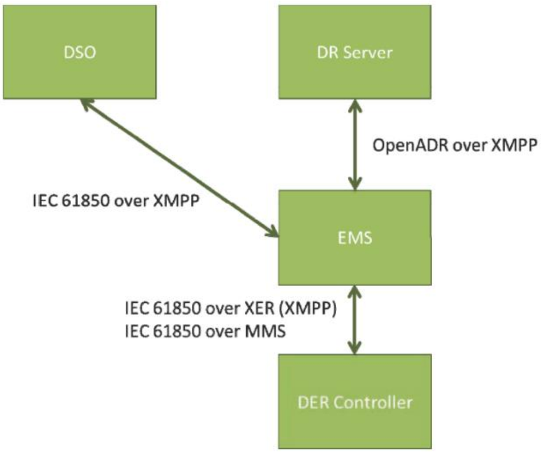


Figure 2.14: The EMS scheme with multi-protocol communications (Okuno et al., 2016).

Aftab et al., 2018 have addressed the problem of Electric Vehicle (EVs) scheduling in microgrids EMS. They have presented an IEC 61850-based description of a microgrid's EMS scheme that includes the management and scheduling of EVs. Additionally, the authors have proposed, extending the part IEC 61850-90-8 which defines the data model of EVs. However, it covers only the charging mode “grid to vehicle”, hence, the authors have extended the LNs to accommodate the discharging process whereby EVs supply power to the grid “vehicle to grid”. Furthermore, the authors have described a communication profile for the microgrid's EMS based-on the IEC 61850-8-2 XMPP standard whereby mapping of all communication services of the EMS to XMPP is demonstrated.

Hussain et al., 2018 have provided a solution for a harmonized control of DERs and Distribution STATic COMpensators (DSTATCOM) devices for optimal management of reactive power in microgrids. They have proposed a modelling of DSTATCOM according to the IEC 61850 information model by defining new LNs to model the functions of DSTATCOMs. Thereafter, they have demonstrated the communication flow for several scenarios of DSTATCOM operation in a microgrid applying the IEC 61850-8-2 XMPP standard. They have concluded that, the proposed communication system can enable plug-and-play capabilities for DSTATCOM and DERs in the microgrid utilizing interoperability, scalability, and cybersecurity benefits provided by IEC 61850 and XMPP standards.

Nadeem et al., 2019 have described IEC 61850-8-2 XMPP as a communication solution for the energy management of VPPs. IEC 61850-based energy management messages for a VPP and mappings to XMPP were showcased in the study. Additionally, the authors have presented a multi-domain configuration of XMPP as a solution to interconnect DERs from different domains in VPPs. The XMPP defines a federation link that enables the communication between servers of distinct XMPP domains. As seen in figure 2.15 below, a federation link is created between XMPP servers ‘VPP.net’, ‘DSO.com’, and ‘VPP.org’ to enable inter-domain communications.

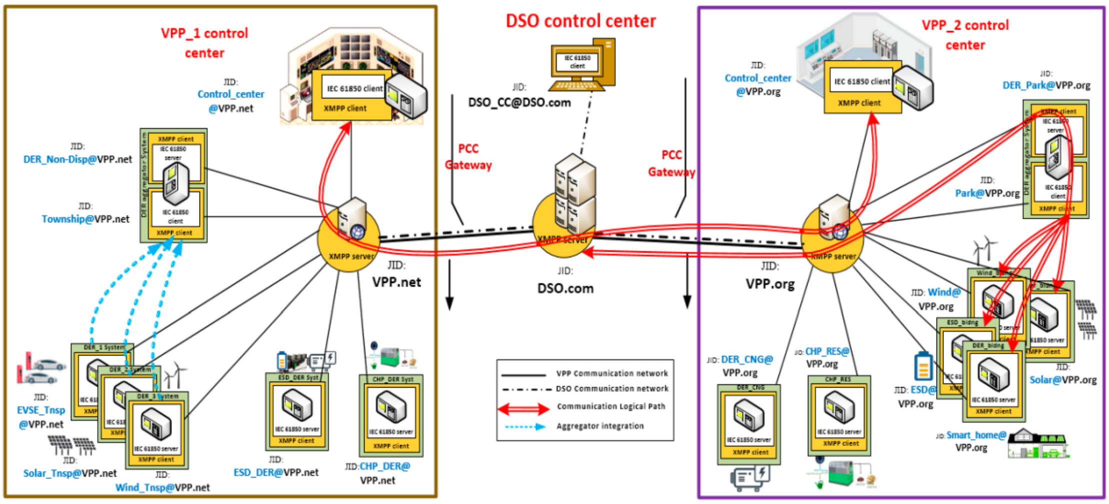


Figure 2.15: The federation link between multiple domain XMPP servers (Nadeem et al., 2019).

All the previewed works have focused on demonstrating the IEC 61850-8-2 XMPP standard as a solution for DER systems. They have showcased the development of IEC 61850-based information models and mappings to XMPP. However, they have not provided a performance evaluation of IEC 61850-8-2 XMPP using implementations and simulations to verify the feasibility of the standard in real-time applications.

This gap was addressed by Keserica et al., 2019 who have aimed to demonstrate feasibility of the IEC 61850-8-2 XMPP as a solution for DER systems applications such as VPPs and microgrids. Hence, they have developed a prototype implementation of an IEC 61850-8-2 XMPP client/server communication stack, which deployed on personal computers for the client, server, and the XMPP server. To evaluate the communication performance, tests were conducted on a LAN over Ethernet, and on a WAN connection via a public IP-based network. A number of IEC 61850 data exchange profiles were tested including unsolicited messages “reports”, request/response messages, and the impact of IEC 61850 cybersecurity measures whereby encryption of messages was applied.

All tests were performed on the request/response mechanism between client/server. When testing for the unsolicited messages, larger data sets were sent as reports, while in testing for request/response a write service “Set” of small data sizes was implemented. The total time of response was adopted as the metric for evaluation of communication performance. For both reporting and request/response messages, the response time was less than one second in both LAN and WAN. The difference in response time for message encryption was around twenty ms for reports and less than one ms for request/response messages. The results have indicated that, encryption of IEC 61850 messages does not have a significant impact on XMPP-based communications. The results are promising in terms of feasibility of the proposed stack for real-time applications with relatively slow time requirements such as measurements data acquisition and Human Machine Interface (HMI) control in DER management systems “VPPs”.

According to the authors, the solution can ultimately enhance the integration process for DERs in smart grids. However, the implementation has omitted a vital factor which is, most existing DER devices use proprietary protocols. Thus, consideration must be made for conversion from various protocols to IEC 61850 information model before mapping to XMPP for communication over WANs. This condition was addressed by Liu & Gu, 2019 and Cho et al., 2019. Both studies have introduced concepts from the IoT paradigm to monitor DER systems using the IEC 61850-8-2 XMPP standard. Liu & Gu, 2019 have proposed a gateway model for DER sites for communications with the cloud or control centres. The gateway model is implemented with a concept of EC whereby it can perform numerous functions on the data before transmission over a network. The proposed gateway performs conversion and information mapping from many proprietary protocols “Modbus and DNP3” to IEC 61850 information models of DERs and maps IEC 61850 communication services to XMPP according to IEC 61850-8-2.

A Supervisory Control And Data Acquisition (SCADA) environment from Elipse software™ was utilized for simulating the PV site data and implementing the IEC 61850-8-2 gateway model. The performance evaluation was based-on calculating communication latency and the tests were conducted on a scenario of data generated from the PV site relayed over Modbus TCP to the gateway model and then forwarded over IEC 61850-8-2 via the XMPP server to the control centre. A simple diagram illustrating the architecture of the testbed is shown in figure 2.16 below. The tests methodolgy included applying the XMPP server in five distinct locations in Taiwan and Thailand, and using several wired and wireless WAN technologies to obtain inclusive results. The test results have proven good communication performance of the gateway model in terms of observed latency. The results have satisfied the performance specifications for WAN communications defined in IEC 61850-90-12 guidelines.

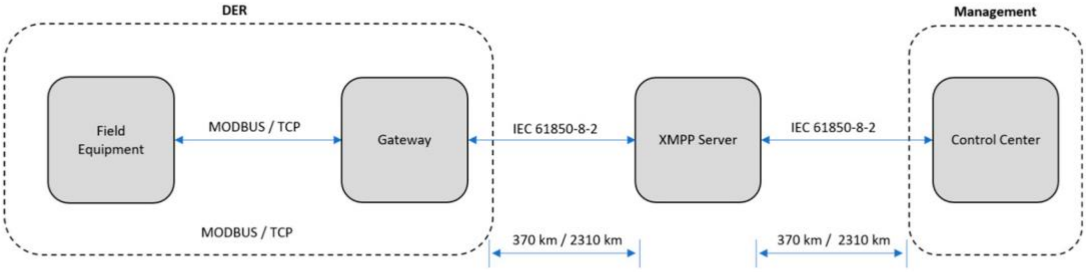


Figure 2.16: **Architecture of the test environment (Liu & Gu, 2019)**.

The authors have argued that, the proposed gateway model can considerably improve communication performance in terms of enhancing data privacy and cybersecurity, reducing latency, and optimizing bandwidth usage which significantly minimizes operational costs for communications. Nevertheless, the authors have noted that, XMPP communication architecture is applied as a central server to manage the traffic between clients, which adds more processing time and delay to the communication path. This feature limits the usage of XMPP for time sensitive applications such as protection. Therefore, the authors have recommended utilizing R-GOOSE with XMPP for future research to achieve stringent time requirements. However, the implementation of the EC gateway have not include deploying a data analytics algorithm to further enhance communication performance.

Cho et al., 2019 have presented a description of the actual site construction of an IoT architecture for monitoring DER sites. The architecture is based-on the IEC 61850-7-420 standard data model of DERs and the IEC 61850-8-2 XMPP standard for transmitting data to the cloud. The IoT-based cloud platform is illustrated in figure 2.17 below, it consists of three layers each with a different function and a structure. The lower layer is where various communication protocols of DER devices “Modbus and DNP3” are converted to the IEC 61850-8-2 XMPP standard to enable interoperability and plug-and-play capability for DERs.

The cloud platform layer provides Platform as a Service (PaaS) which is a cloud environment that allows the development and deployment of applications such as the XMPP server and device management applications. In addition, there is an information management layer, which provides Software as a Service (SaaS) services whereby interface and access of applications are enabled for multiple end-users using WS such as Hyper Text Transfer Protocol (HTTP), REpresentational State Transfer (RESTful), and Application Program Interfaces (APIs).

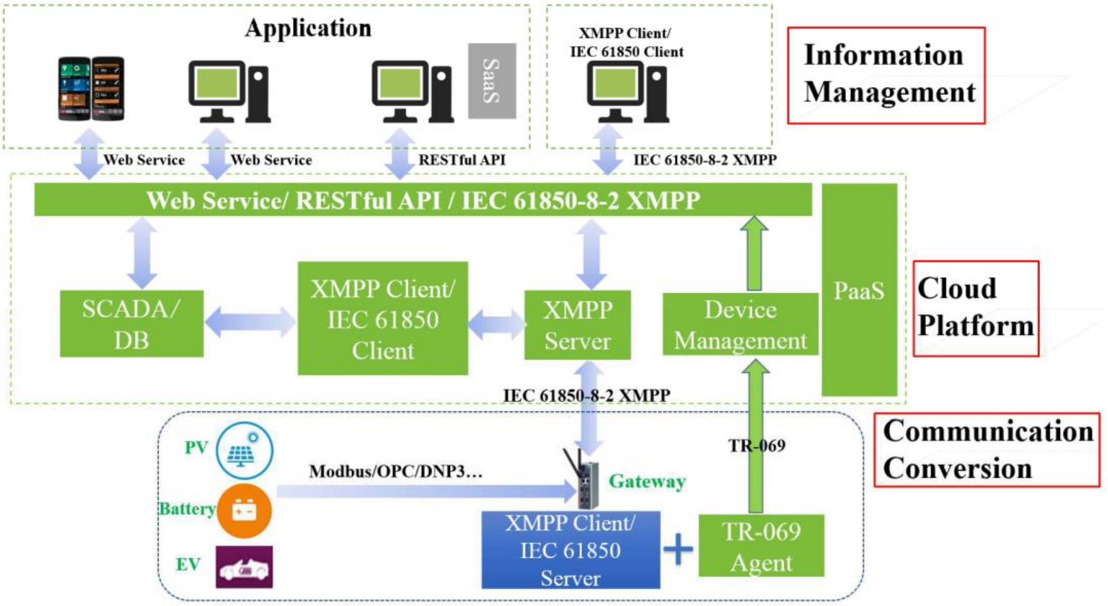


Figure 2.17: Architecture of IoT-based IEC61850 XMPP cloud platform (Cho et al., 2019).

The platform architecture was constructed at a PV site owned by Taiwan Power Company (TPC). Conversion from Modbus to IEC 61850 took place through gateways. Moreover, a publish/subscribe communication was established between two XMPP clients “IEC 61850 client/server” geographically distant from the XMPP server, and latency was observed as a metric of performance evaluation. The test results have shown latency values that fell within the class TL1000 for WAN communications according to IEC 61850-90-12 guidelines, which is adequate for monitoring and data acquisition applications.

The authors have highlighted that, a major obstacle in the implementation, was the conversion from proprietary protocols to the IEC 61850 standard, due to the extreme diversity of address mapping rules and information models between protocols. Hence, the authors have recommended using IEC 61850-based equipment for DER sites as much as possible to eliminate the need for protocol conversion. Another recommendation is that, XMPP can be combined with R-GOOSE to achieve time requirements for control and protection applications in DER systems.

The section provided a review of previous research studies on applications of the IEC 61850-8-2 XMPP standard in DER systems. In the following section, a discussion on the reviewed literature in the chapter is carried-out and presented.

2.6 Discussion

From the literature review, it is clear that, the performance of communication systems is a critical aspect in ensuring the stability and success of smart grid operations. Typically, communication performance is quantified and measured by the concept of QoS which consist of multiple performance indicators including latency, bandwidth, and packet delivery. Different applications within the smart grid have distinct communication requirements, nonetheless, in the research project, the focus is on DER systems due to their massive potential to enhance smart grid performance and increase the utilization of renewable energy resources.

Standardization was identified as an important solution to satisfy communication requirements in DER systems. It is the direct solution to interoperability issues when integrating devices from diverse vendors. The IEC 61850 standard is prominent amongst the standards which are specified for smart grids. It provides object-oriented modelling of functions in power systems and specifies a set of services to exchange information between devices. IEC 61850 standard was primarily designed for LANs, and it has specified mapping to MMS as an application layer protocol for client/server communications. However, utilizing the standard in DER communication systems was one of the motivations to extend the standard to operate on WANs.

The XMPP was identified by the IEC 61850-8-3 technical report as the best option for IEC 61850-based communications over WANs. Numerous advantages of XMPP have encouraged its selection, which include high scalability, availability of many open-source implementations, and the extensive use in the Internet paradigm. In addition to the strong cybersecurity measures which make the XMPP a perfect solution for deployment over public IP-based networks.

Mapping of IEC 61850-8-1 MMS services to XMPP was specified in part IEC 61850-8-2. The literature review has covered several studies that implemented the IEC 61850-8-2 XMPP standard in DER systems (Aftab et al., 2018; Hussain et al., 2018; Nadeem et al., 2019). These studies have described information models of various DERs utlizing the IEC 61850 standard and the communication in their management systems are based-on IEC 61850-8-2 XMPP. Conversely, the studies have not provided evaluations for the communication performance of the standard. It was attempted by Keserica et al., 2019, where the performance results have verified the validity of IEC 61850 for monitoring and data acquisition applications. Nevertheless, the authors have not considered the fact that, integration of existing DER devices would include conversion from proprietary protocols to IEC 61850 to be able to implement IEC 61850-8-2 XMPP.

In the context of enhancing communication performance in smart grids, there have been continuous efforts to introduce advanced technologies and concepts such as the IoT. The XMPP has already been implemented extensively in the IoT paradigm due to its decentralized architecture, cybersecurity measures, and high scalability. Cho et al., 2019 and Liu & Gu, 2019 have introduced concepts such as cloud and EC from the IoT paradigm. The authors Cho et al., 2019 have provided a description of the actual site construction process of an IoT cloud platform for monitoring a PV site, while Liu & Gu, 2019 have introduced the concept of EC, whereby intelligence is added to network edge devices, in this case, the site communication gateway.

Both studies have took into consideration conversion from proprietary protocols to the IEC 61850 standard and then mapping to the IEC 61850-8-2 XMPP standard. However, Cho et al., 2019 have highlighted the fact that, in actual real world implementations, protocol conversion is a challenging process that consumes a lot of work and effort. Hence, they recommended replacing proprietary with IEC 61850-compliant devices in DER sites. Both studies have confirmed the results from Keserica et al., 2019 which have indicated the suitability of IEC 61850-8-2 XMPP standard for applications with relatively slow time requirements such as monitoring and data acquisition. Both authors have recommended using a combination of R-GOOSE with XMPP to achieve time requirements that can accommodate wide area protection functions. The intelligence in the EC gateway model presented by Liu & Gu, 2019 have consisted of protocol conversion only, as they have not implemented a data analytics algorithm to further enhance the communication performance.

From the literature review, it can be argued that, communication performance is dependent on the amount and size of data transmitted on the network, compared to the network conditions. This is because in many cases there’s a limited ability to control network related aspects in terms of technologies and hardware due to financial cost factors. Consequently, there is only a space for optimizing and reducing the data traffic to enhance communication performance. Additionally, it was noted that adopting IoT concepts such as EC in DER systems can have a considerable impact to enhance communication performance. Nonetheless, there was no attempt in the reviewed literature to implement algorithms for data fusion in an EC gateway that is based-on the IEC 61850-8-2 XMPP standard, to improve communication performances for DER remote sites.

The research study attempts to showcase the concept of an EC gateway model that utilizes the IEC 61850 and XMPP standards, which has been mainly motivated by these findings from the reviewed literature. The research aims to study the impact of implementing an algorithm for data fusion on communication performance. Based-on the recommendation from Cho et al., 2019 to eliminate the need for protocol conversion, a wind turbine model is simulated in RTDS and measured values are extracted using IEC 61850-8-1 GOOSE protocol. The intelligent gateway model is implemented using RTAC from Schweitzer Engineering Laboratories (SEL)™ and adopts a concept from Wong et al., 2022 who implemented a mapping of R-GOOSE to MMS for wide area communication. However, in the research project, the GOOSE is mapped to MMS on a local area connection. Mapping to the IEC 61850-8-2 XMPP standard is accomplished using an Elipse Power application and the performance evaluation is based-on measuring bandwidth usage and communication latency.

In the research study, an emphasis is made on the IoT concept and its introduction in the smart grid paradigm. Hence, the following chapter will provide a brief theoretical background on the IoT major concepts including the cloud computing (CC), the EC, and their applications in smart grids.

2.7 Conclusion

In this chapter, the literature was reviewed on communication systems in smart grids focusing on DERs. Firstly, the communication system requirements and commonly used technologies in smart grids were identified from the reviewed literature from a perspective of communication’s QoS requirements. Thereafter, the chapter studied DER systems, identifying their communication requirements and the impact of communication performance on their systems. Standardization was highlighted as a major communication requirement in DER systems. Furthermore, the review focused on the IEC 61850 standard and the factors that affect its communication performance in WANs. Thereafter, the XMPP standard was analysed as it is the standardized middleware to enable IEC 61850 communications over WANs. Finally, the applications of IEC 61850-8-2 XMPP in DER systems were evaluated and discussed.

CHAPTER THREE

INTERNET OF THINGS APPLICATIONS IN THE SMART GRID

3.1 Introduction

The IoT is an abstract concept of linking several devices to exchange information and interact without human intervention. The concept has firstly exhibited in the Radio Frequency Identification (RFID) technology, which is widely adopted within the retail and transportation industries. The conversation about the IoT was initiated by the RFID developer community back in the year 1999. Thereafter, the exponential advancement in ICT around the world played a key role in driving the IoT concept toward large-scale implementations in various fields of life.

A common shared vision for the IoT is described by interconnection of physical devices such as sensors, actuators, and other objects through IP networks. This enables bi-directional communication between these devices whether with or without human involvement. The bi-directional interconnection results in very large amounts of data exchanged between devices. The data is acquired and analysed to be used for planning, management, and decision-making (Pramudhita et al., 2018; Kirsche & Klauck, 2012; Saleem et al., 2022).

The IoT has a massive potential to improve quality of living, whereby it can be adapted and utilized to enhance many domains and sectors such as healthcare, industrial automation, energy, and transportation. As seen in figure 3.1 below, the concept of IoT incorporates interaction of smart devices and their applications within numerous domains referred to as ‘vertical markets’ with central analytical and computing services referred to as ‘horizontal markets’. Currently, billions of objects are continuously being added to IoT architectures at an extraordinary rate. Embedded intelligence is increasingly being implemented in objects to be able to share and analyse information, and perform tasks in an intelligent and coordinated manner. The IoT employs technologies such as embedded and centralized computing, Wireless Sensor Networks (WSNs), Internet services and applications, to achieve different functions ranging from real-time online monitoring to direct control (Al-Fuqaha et al., 2015; Pramudhita et al., 2018).

This chapter provides a theoretical background on the IoT concept including the architecture, advantages, and applications. The chapter is structured in the following manner, section 3.2 introduces a common layered architecture of IoT networks and devices, introducing the CC.

Figure 3.1: A conceptual view of IoT showing horizontal integration of multiple domains (Al-Fuqaha et al., 2015).

The section elaborates on the EC architecture, data processing techniques, benefits, and applications. Section 3.3 introduces IoT applications in the smart grid. Section 3.4 further explores EC applications within smart grid's various domains including generation, transmission, and distribution. Section 3.5 provides a brief introduction of the EC gateway implementation in the research project. Section 3.6 presents points of discussion and finally, conclusions are delivered in section 3.7.

3.2 Internet of Things architecture

The IoT architecture comprises three types of components which are described as follows:

- **Terminal devices**: installed across a network in a specific domain in an IoT architecture. They can either be sensing devices that provide data and measurements about a process, or final elements executing the control commands such as actuators.
- **Gateways**: the main function of gateways is to interconnect communication networks. They are often utilized to perform pre-processing of data before transmission to the cloud servers.
- **Cloud**: consists of servers and facilities that have high processing capacities to perform a variety of processes on large amounts of data in IoT applications (Yu et al., 2017).

An illustration of an IoT architecture is noted in figure 3.2 below. The sensors or devices collect measurements data and transmit these data over a network through gateways to the cloud. Data storage, processing, and decision-making take place in the cloud, and the responses are forwarded back across the network to interested devices to execute the required function or task.

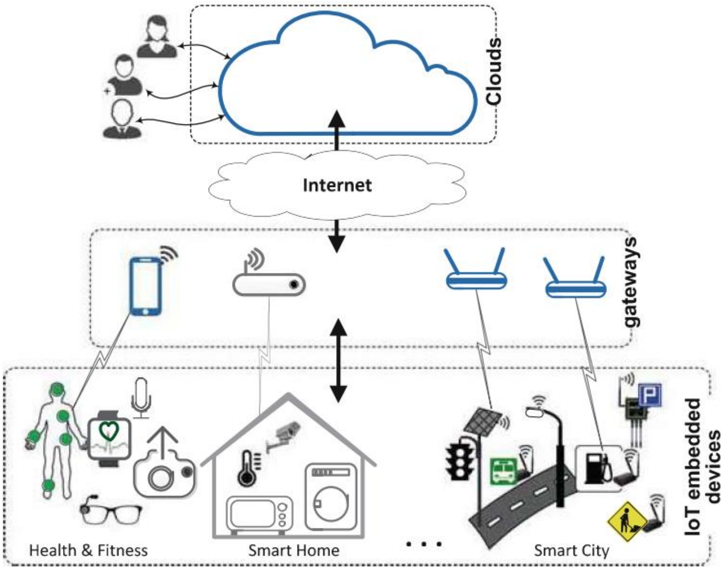


Figure 3.2: **An illustration of the IoT architecture (Samie et al., 2019).**

The architecture is cloud-centric whereby all data processing is carried-out in the cloud. The role of gateways is to integrate local networks of devices in wide area Internet-based networks (Samie et al., 2019). The following section provides further details on the CC concept.

3.2.1 Cloud computing

The CC emerged with recent advancements in data processing and networking technologies. The computing and storage resources are provided through clustered data centres that can be accessed and configured via IP-based networks. These data centres consist of powerful servers and hardware that offer rich resources in terms of storage and processing capacities. The CC offers the necessary processing power to handle large amounts of data generated by IoT devices.

The CC has been increasingly utilized by industries for their operations due to advantages such as computing flexibility. However, depending on the CC means that, large volumes of data generated in IoT environments must be transferred to the cloud for processing which creates numerous challenges including the following:

- High data traffic that can create bottlenecks and cause communication service interruption.

- Increased costs of bandwidth required to handle the high data traffic.
- Increased communication latency which makes it difficult to implement real-time critical operations that require low latency.
- Cybersecurity concerns that arise from exposing large amounts of data on public IP-based networks which increases the probability of cyber assaults and eavesdropping (Ullah et al., 2021; Sharma & Wang, 2017; Chen et al., 2019; Samie et al., 2019).

To provide a solution for these problems and enhance efficiency of IoT systems, the EC was introduced as a complementary to the CC. The following section introduces the EC concept.

3.2.2 Edge computing

The EC can be defined as enabling data processing capabilities at the network edge near data sources. In other words, an EC refers to any computing or networking unit between the cloud and data sources (Ullah et al., 2021). Typically, edge nodes have less computation resources than cloud servers. Edge nodes can be assigned with pre-processing of data before forwarding the data to cloud servers, for example, data aggregation and classification. Therefore, the EC enhances the performance in IoT communication systems in terms of minimizing costs, latencies, and energy consumption (Huang et al., 2018). To further comprehend “the end” concept in networks, a conceptualized architecture of IoT is described in figure 3.3 below. The figure shows ‘front-end’, ‘near-end’, and ‘far-end’ areas in IoT networks.

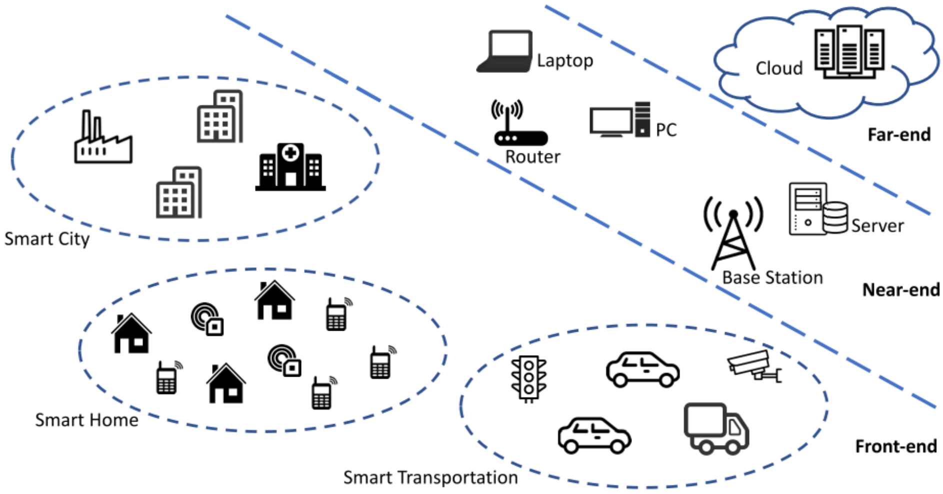


Figure 3.3: **Areas in the IoT architecture (Yu et al., 2017).**

Each area has specific features that can be summarized as follows:

- **Front-end**: consists of end devices that directly interact with users and applications in the physical world. These devices have extremely limited computation resources and perform basic functions such as gathering data “sensors” or executing actions “actuators”.

- **Near-end**: comprises of entities that mainly manage communication network integration and data flow. This area is where the EC concept is applied by deploying servers and gateways equipped with adequate computation resources to perform more tasks. They can process data from far-end devices and provide real-time responses. Additionally, they can provide a reasonable data storage capacity.
- **Far-end**: involves the cloud servers that typically have unlimited computation and storage resources and perform complex data processing and analysis such as Machine Learning (ML) algorithms and big data management.

Typically, the EC nodes are geographically located close to end devices and users. Despite having limited computation capacity, they can massively enhance communication QoS for end users (Yu et al., 2017). An EC as a concept means that data processing tasks are distributed across all layers in the IoT structure. This means that, the processing tasks are only forwarded to upper layers if they are not possible or inefficient to perform them at a lower layer, starting from front-end devices which can perform simple tasks such as aggregation and noise filtering. An IoT architecture is illustrated in figure 3.4 below, which shows the edge, fog, and cloud layers.

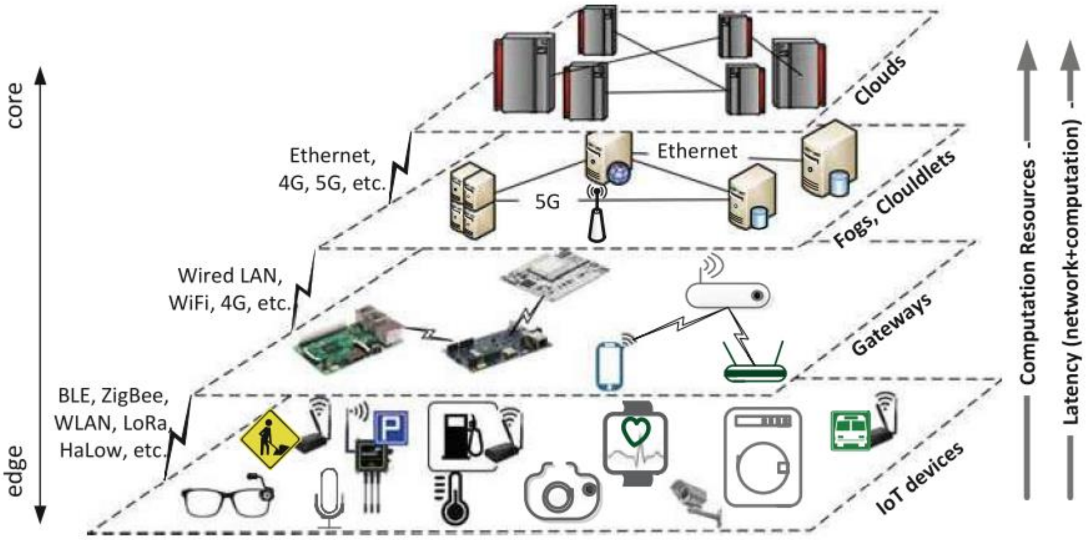


Figure 3.4: **Computation layers in the IoT architecture (Samie et al., 2019).**

The edge gateways perform computing and storing tasks on top of their basic function which is networks integration. Fog is an extra layer that usually has more computation and storage resources than the edge layer. Fog computing is typically implemented to provide computing support for edge devices in a shorter range than distant cloud servers. Hence, it further boosts the distributed computing architecture in IoT systems by reducing the load on communication networks and cloud servers. The cloud layer is essential for providing unlimited storage and handling complex computation tasks such as analysis of long-term data and execution of ML and prediction models (Li et al., 2021; Samie et al., 2019).

The EC concept of processing data near the source, provides numerous benefits for the performance of IoT systems, which can be summarized in the following points:

- Reducing computation latency for real-time applications that require quick data analysis and decision-making (Ullah et al., 2021).
- Significant reduction of the operating costs in terms of communication bandwidth and costs of cloud servers (Skirelis & Navakauskas, 2018).
- Minimizing the data transmitted over networks improves cybersecurity and enhances communication QoS in terms of reliability, bandwidth usage, packet loss, transmission delay (Yu et al., 2017; Prajeesha & Anuradha, 2021).
- Providing location related information such as status information of events, end-user, and local network status will result in improved performance of location related applications (Sharma & Wang, 2017).

The following sections present a description of EC devices to study and understand how they interact within the IoT architecture.

3.2.2.1 Structure of edge computing devices

Typically, the structure of EC devices consist of three layers namely network, data, and application layers. As displayed in figure 3.5 below, the structure comprises management modules for networking, computing, and memory. Each layer consists of several functions and coordinates with the management modules to handle the specific requirements of that layer. The network layer handles interaction with IoT devices via wired or wireless networks. Interaction with the cloud is managed by the application layer via APIs. While the data layer performs required data processing tasks which enables local computing tasks such as real-time responses, data optimization, and aggregation (Chen et al., 2019).

The EC can enable the implementation of many IoT applications with requirements that cannot be accommodated by the CC alone such as the following:

- Extremely low latency: required in applications such as video streaming and E-Healthcare.
- Mobility support: for example, smart transportation applications.
- Geographical dispersion: for instance, WSNs.
- Distributed control systems: a major example is the smart grid (Sharma & Wang, 2017).

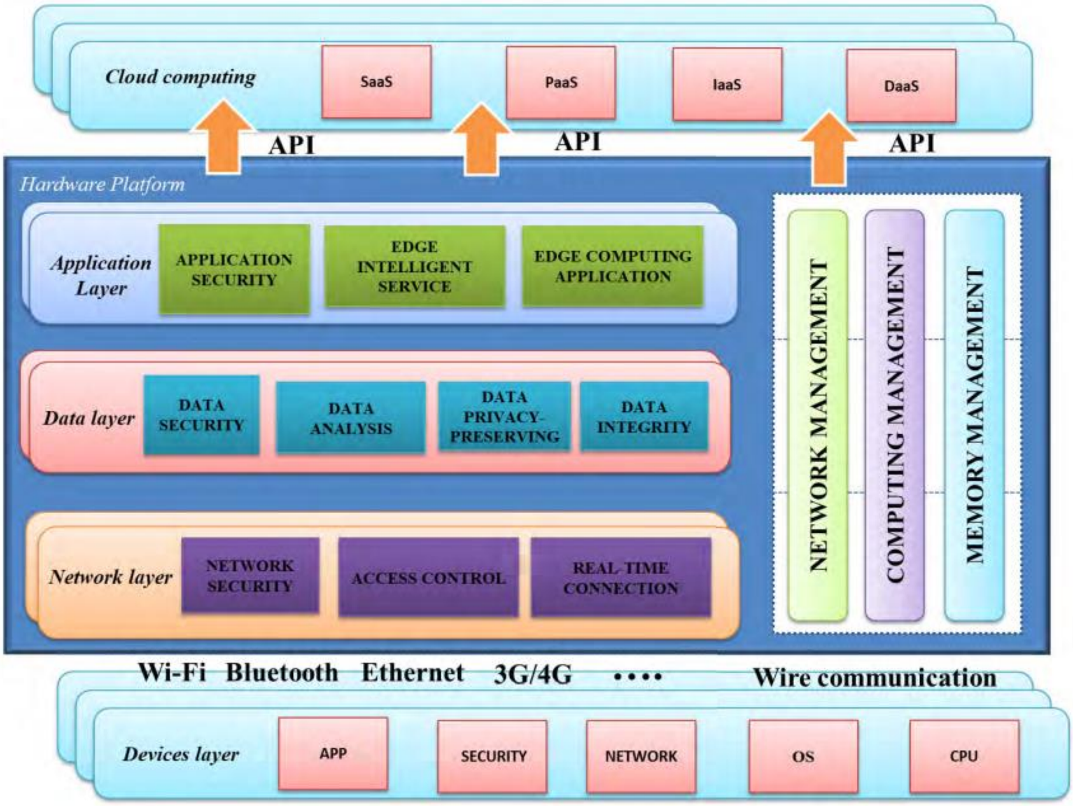


Figure 3.5: An architecture of EC (Chen et al., 2019).

The following section introduces the most common processing techniques implemented in edge devices.

3.2.2.2 Major data processing techniques at the edge

Depending on the available computation and storage resources, the EC nodes can perform different processing techniques on raw data received from terminal devices. The principal techniques performed are briefly described below:

- **Data Fusion**: EC nodes can perform a harmonized fusion of heterogeneous data to deliver a proper understanding of a specific process. For example, heterogeneous voltage and current data of battery cells can be combined to minimize measurement error percentage and can provide an indication of the battery's performance and age. Data fusion is vital in minimizing the volume of data transmitted to the cloud.
- **Data Analysis**: refers to analysing historical data records to achieve desired results. ML algorithms are widely utilized for this technique.
- **Data Storage**: edge devices are typically equipped with sufficient storage capacities to enable the processing and analysis of data.
- **Data Security**: EC nodes can perform encryption and integrity evaluation techniques on data to enhance cybersecurity and data privacy. Furthermore, critical data can be prioritized for processing at the edge to prevent exposure over communication networks (Li et al., 2021).

In the research project, the data fusion technique was used to develop the EC algorithm. The applications of IoT and EC in smart grids are the focus of this research study. Therefore, the following section briefly explores IoT applications in smart grids, and highlights the impact of the EC on various domains of a smart grid including generation, transmission, and distribution.

3.3 Internet of Things in smart grids

The main task of a power grid is to provide reliable and efficient delivery of electrical power from generation to consumption. However, there are several challenges encountered by traditional power grids such as unpredictable power outages, consumer fraud, and fixed pricing. These challenges along with others cause significant increases in the cost of power delivery due to high power losses and economic losses resulting from frequent service interruption (Samie et al., 2019; Huang et al., 2018).

The concept of a smart grid emerged as an upgrade of traditional power grids by integrating ICT to improve power delivery in terms of efficiency, reliability, and cost-effectiveness. Integrated advanced ICT infrastructure enables a bi-directional information and power flow across the smart grid. This leads to realization of automated intelligent EMSs that deliver power in a reliable, secure, and cost-effective manner. The smart grid incorporates advanced sensing technologies to enable real-time monitoring of all aspects of power generation, transmission, and distribution. For instance, intelligent sensors for humidity, temperature, and vibration in addition to video cameras are all integrated to form rigorous and effective monitoring systems. The smart grid uses the monitored data to enable automated and intelligent response functions such as threat detection and self-healing (Prajeesha & Anuradha, 2021; Yang et al., 2019).

Smart grids accommodate the growing integration of renewable energy resources. It involves smart Demand Side Management (DSM) through the introduction of smart metering and AMI that enables a bi-directional interaction between consumers and the grid operators. The core entities in a smart grid are seen in figure 3.6 below. Management systems handle monitoring and executing smart grid applications including demand response management, supply and demand prediction, and dynamic pricing. Furthermore, the figure shows the integration of RESs in the generation domain in a form of large plants. RESs are utilized in the distribution domain in the form of DERs which are managed by microgrids management systems.

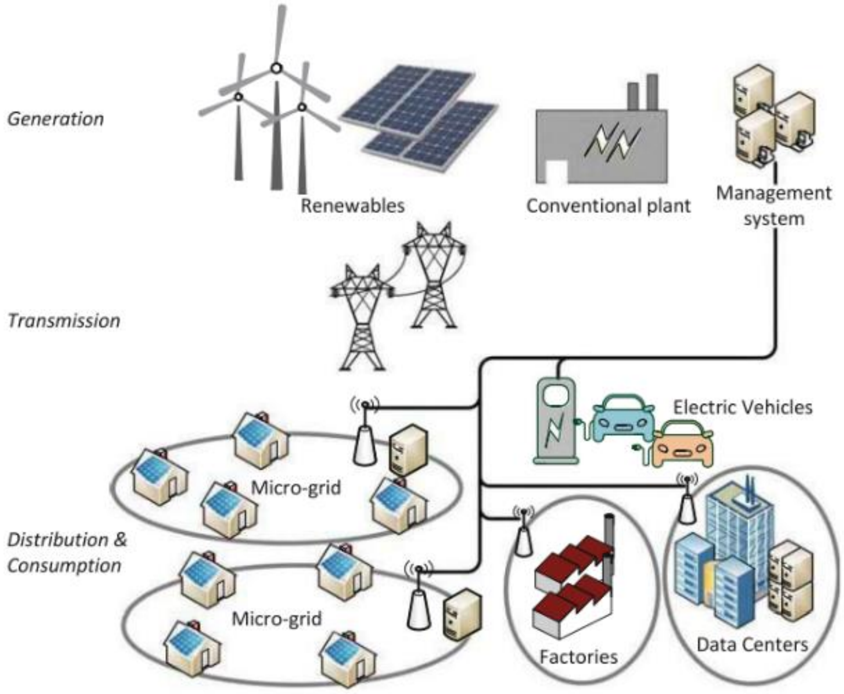


Figure 3.6: **Major components of a smart grid (Samie et al., 2019).**

Consumers including smart buildings, EVs, and other entities are all integrated in the grid management systems via an ICT infrastructure (Samie et al., 2019). Recently, there has been a growing trend toward introducing advanced technologies such as IoT and Artificial Intelligence (AI) in smart grids as the next step to realizing intelligent and reliable power delivery systems (Huang et al., 2018).

Introducing IoT technologies in smart grids offers numerous advantages and features that can be enabled such as plug-and-play capabilities for terminal devices, rigorous monitoring of grid status via advanced sensing technologies, and significant efficiency enhancement of distributed power systems. Several technologies are required to build IoT-based smart grids, including:

- Standardized communication protocols.
- Cost-effective communication networks equipped with advanced cybersecurity technologies.
- Advanced sensors technologies.
- An EC-based architecture.

The significance of EC in smart grids is centred around the distributed nature and low latency requirements in most applications. Furthermore, the large volume and heterogeneity of generated data from different devices make the adoption of EC a vital solution for IoT-based smart grids (Li et al., 2021; Chen et al., 2019). Similar to the general EC architecture presented in section 3.4, a reference architecture for the EC in smart grids is depicted in figure 3.7 below. The architecture consists of four layers which are, perceptual, network, EC, and application “cloud”. The perceptual layer consists of terminal devices that acquire real-time data from various applications. Thereafter, the data will be forwarded via the first network layer to EC nodes which will perform preliminary data processing such as encryption and aggregation.

Decisions can be taken by edge nodes and sent directly to devices or controllers in the perceptual layer. Lastly, pre-processed data along with records of all actions taken will be forwarded via the second network layer to the cloud for archiving, advanced analysis, and to be used for coordination of operations in smart grids. The network layers employ a variety of technologies according to the data transfer requirements. Wireless technologies are mostly deployed for ‘network layer 1’ because it transfers raw data from devices to EC nodes which are mostly in the same vicinity. While ‘network layer 2’ covers a much wider range and must have larger bandwidth. Hence, wide area communication technologies are preferred such as fibre optics and VPNs. However, for EC nodes in remote areas with minimum security requirements, public IP-based networks can be utilized to minimize the costs (Li et al., 2021).

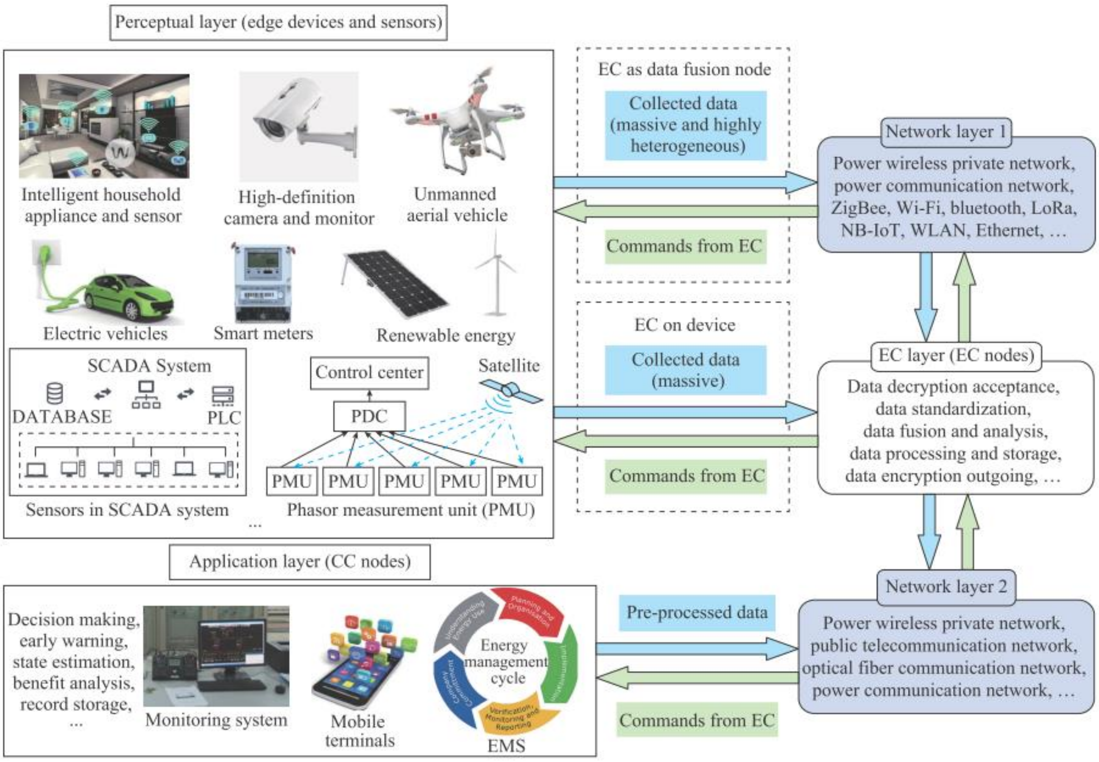


Figure 3.7: Architecture for EC in smart grid (Li et al., 2021).

The section presented architectures and applications of IoT in smart grids. The following section outlines some EC applications in different domains in a smart grid.

3.4 Edge computing applications in smart grids

The EC plays a crucial role in improving the overall performance in many domains of smart grids including generation, transmission, and distribution as discussed in sections “3.4.1, 3.4.2, 3.4.3” respectively.

3.4.1 Generation

The EC represents an effective solution for monitoring power generation plants in general and specifically RESs such as wind turbines and PV plants. The EC devices analyse the real-time data generated from sensors installed across the units with very low latency in analysis and protection decisions. In synchronisation with the cloud, control and coordination strategies can be implemented such as maintenance scheduling and lifecycle management to achieve a seamless operation. Various benefits can be achieved from monitoring electrical and mechanical health of generators using the EC such as the prediction of faults and power output. Thus, it will minimize downtime and operation costs (Liao & He, 2020; Li et al., 2021).

3.4.2 Transmission

The EC can significantly enhance the safety and reliability of transmission networks by enabling smart, automated, and efficient monitoring systems. Transmission lines can be monitored by video surveillance using drones or Unmanned Aerial Vehicles (UAV). The EC monitoring schemes involve other major equipment in transmission systems such as transformers and circuit breakers. For transformers, monitoring is conducted for grounding currents, fire hazards, humidity, and oil temperature. As for circuit breakers, parameters such as gas pressure and partial discharge are considered essential, thus, they are subjected to systemic monitoring via the EC.

The EC devices can utilize AI and ML algorithms for processing images and real-time data to identify faults and critical situations, which will enable fault prediction and result in very fast responses to emergencies. Thereafter, only the records of taken actions and detected faults can be uploaded to the cloud for further analysis. This will considerably reduce the computation load on cloud servers, minimization of the decision latency for emergencies, and saves large communication bandwidth which prevents network bottlenecks (Li et al., 2021; Prajeesha & Anuradha, 2021).

3.4.3 Distribution

Applications of EC in distribution systems include faults and overload detection and taking corrective actions at extremely low latency which effectively enables self-healing capabilities in the system. This will significantly enhance the safety and reliability of distribution systems. Furthermore, the EC enhances interactivity between consumers and the distribution system by improving the communication system performance. The EC can be used to implement automated and intelligent monitoring systems for numerous entities within distribution networks such as microgrids. In addtion, the EC plays a major role in enabling demand response applications in smart homes, which contribute to the optimization of electricity consumption and enhance power system stability (Li et al., 2021).

Smart meters are considered to be the most suitable terminal devices to implement the EC concept. The main function of the smart meter is to read and calculate power consumption, it can be applied to receive power demand information from utility operators via the network. Thereafter, using embedded intelligence, the smart meter can process the data, perform demand response actions, and send only the results to utility operators instead of raw data. This approach notably reduces bandwidth usage, response latency, and minimizes cybersecurity risks on users' consumption information (Sirojan et al., 2019).

The following section reviews the implementation of an EC gateway model in the research study, explaining the features of the developed simulation model.

3.5 The lab-scale implementation of an edge computing gateway

In the research work, a lab-scale testbed was developed to implement an EC gateway model for monitoring a power network integrated with a DER model utilizing IEC 61850 and XMPP standards. A wind turbine model is operated in the lab-scale testbed to evaluate the impact of the EC on communication system performance. The choice of wind energy was mostly motivated by its massive contribution being the most utilized RES to produce clean energy. This fact, is primarily driven by the low cost of energy produced from wind (Chang et al., 2022). Additionally, wind power generation has many other advantages including the long life span of system parts, reactive power injection, minimized costs of installation, operation, and maintenance (Adefarati & Bansal, 2016).

Integration of such high penetration of wind power generation necessitates stability of power systems and proper coordination of their operation and protection schemes. Communication systems performance is a critical factor in achieving seamless integration of wind generation systems in smart grids (Timbus et al., 2008). Wind turbines are built on land or offshore, usually at very distant locations from control centers (Chang et al., 2022). Hence, an EC gateway can be employed to reduce data transmitted from wind turbines' sites to enhance the performance of communication networks. A DER model consisting of a wind turbine coupled with an electrical generator, is simulated on RTDS representing a remote generation site. Several mechanical and electrical data values are generated from the simulation model and forwarded to the gateway model over a LAN. The architecture of the testbed is illustrated in figure 3.8 below. It shows the gateway model which consists of an RTAC SEL-3555 from SEL™ and Elipse Power which is an advanced SCADA application from Elipse software™.

The EC concept is implemented on the gateway model whereby an algorithm for data fusion is implemented on the RTAC SEL-3555. While the LAN integration to a WAN is carried-out using Elipse Power which is implemented on 'PC-1'. Thereafter, the data is forwarded over an Internet-based WAN to the cloud which is implemented on 'PC-2' using Elipse Power.

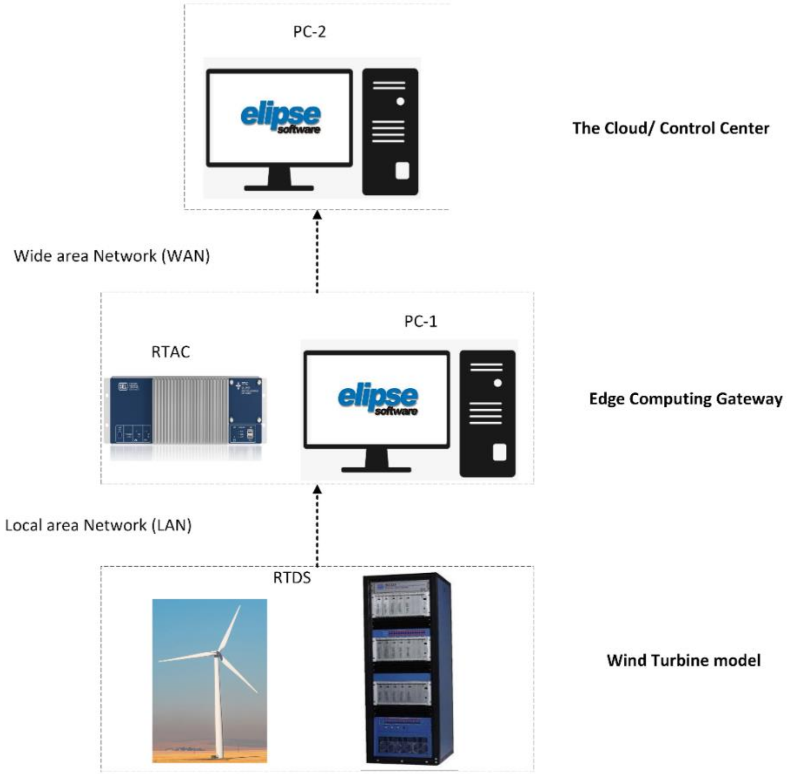


Figure 3.8: **The EC-based architecture of the lab-scale implementation.**

The implementation aims to measure the impact of executing a data fusion algorithm on communication performance in terms of bandwidth usage and latency. The next chapter presents a detailed description of the lab-scale implementation including a description of all incorporated components and their configurations. The chapter covers the LAN and WAN communication domains for the monitoring scheme including the wind turbine model on RTDS and the gateway model implementation using RTAC SEL-3555 and Elipse Power. The WAN domain applies IEC 61850-8-2 XMPP-based communications that is run via an XMPP server application which is Openfire from Ignite Realtime™.

3.6 Discussion

The integration of RESs remains a key challenge that is facing the future of smart grids. The aim is to achieve a seamless integration resulting in reliable, cost effective, and secure energy delivery systems. This can be accomplished via a standardized and flexible communication system that includes advanced technologies such as the IoT.

The prospect of implementing the IoT in smart grids is promising in terms of enhancing several aspects of energy generation and delivery systems. The implementation of an IoT architecture necessitates the existence of advanced infrastructure of networking and data processing capacities to achieve its objectives. These technologies have been increasingly utilized in various fields and sectors, including the industrial sector which has been a large contributor in implementing the IoT concept to imporove their systems. Within the IoT paradigm, the EC stands out as a concept that targets improvement of decision-making and response times. Simultaneously, the EC reduces data traffic in communication networks which will cut operational costs, enhance reliability, minimizes downtimes, and risk of failure. The EC plays a signifcant role in enhancing communication performance for all domains of power grids and energy delivery systems including genration, transmission, and distibution.

From the reviewed literature, the EC has been mainly employed for monitoring applications within smart grids. Monitoring applications have less strict requirements compared to the protection and control applications, which motivated the decision to implement a monitoring application in this research project. Unlike protection or control applications, the eased time requirments of monitoring applications is suitable for the available lab-scale testbed. It allows for evaluating the impact of EC on communication performance without the concern of strict time requirements that would affect the research scope.

The implementation of the EC concept is extremely flexible and scalable to the highest degree. The concept can be applied on a wide range of hardware and networking capacities. The research study presents an application of the EC concept in conjunction with prominent communication standards namely, IEC 61850 and XMPP standards. As noted from the literature review, the XMPP provides a suitable solution to run the EC and IoT applications due to its high scalability and strong cybersecurity mechanisms.

3.7 Conclusion

The chapter offered a brief introduction to the IoT concept, it covered the common architecture of IoT networks. The chapter zoomed into the features and structure of the EC. The chapter highlighted multiple benefits of the EC in terms of reducing computation and communication load in IoT networks. Furthermore, the concept of processing data at a network’s edge, opens doors for enabling many applications with numerous requirements including extremely low latency and location context. Thereafter, the chapter discussed the application of IoT and EC in smart grids and emphasised on the massive opportunities for improving the performance in various domains including generation, transmission, and distribution. Finally, a brief introduction to the lab-scale implementation of the research study was provided.

CHAPTER FOUR
IMPLEMENTATION OF THE MONITORING SCHEME TESTBED

4.1 Introduction

The IoT architecture has been introduced and implemented in smart grids especially for monitoring applications. In the research study, the EC is implemented whereby data processing at the edge of a network "gateway" was enabled before transmiting data to a control centre or the cloud. The research aims to showcase and analyse an implementation of IEC 61850 standard communication protocols including GOOSE and MMS which are defined in part IEC 61850-8-1. As well, to study the implementation of IEC 61850 for communications over WANs by mapping to XMPP which was defined in part IEC 61850-8-2. The implementation has a huge potential to confront interoperability challenges in future smart grids by adopting IEC 61850 information models. Furthermore, cybersecurity is one of the main benefits that can be realized from implementing XMPP for wide area communications. In addition, to evaluate impact of the EC on communication QoS in terms of bandwidth usage and latency.

The chapter presents a lab-scale implementation of an EC gateway model that is based-on IEC 61850 and XMPP standards. A monitoring scheme is implemented whereby the gateway model acquires measurement data from a power network model simulated in RTDS utilizing IEC 61850-8-1 GOOSE standard over a LAN connection. Thereafter, the gateway model performs integration of LAN to an Internet-based WAN utilizing XMPP as a middleware protocol. An SCADA client application that is implemented to simulate a control centre or the cloud, receives the transmitted data from the gateway model.

The chapter is structured as follows, section 4.2 provides brief introduction of the testbed components namely RTDS, RTAC SEL-3555, and Elipse Power, describing their features, functions, and structures. Section 4.3 delivers a detailed description of performed configurations of each component to achieve a successful monitoring scheme. Section 4.3.1 describes the power network model that is integrated to a wind energy model simulated in RTDS and the configuration of IEC 61850-8-1 GOOSE standard which is utilized to publish the data tags intended for monitoring. Section 4.3.2 explains the gateway model which consists of an RTAC SEL-3555 and Elipse Power, it describes the configuration of RTAC SEL-3555's subscription to GOOSE from RTDS and highlights configuration of RTAC SEL-3555's MMS server model.

The section describes Elipse Power IEC 61850 communication drivers and their configuration as IEC 61850-8-1 MMS client and IEC 61850-8-2 XMPP server. The

MMS client driver is configured to poll data from RTAC SEL-3555, and the XMPP server driver is set to enable XMPP communication with a remote IEC 61850-8-2 XMPP client driver. All IEC 61850-8-2 XMPP-based communications configurations are described in section 4.3.3, including the Openfire XMPP server application which manages XMPP communications over an Internet-based WAN. Section 4.4 provides points of discussion and the chapter is concluded in section 4.5.

4.2 Testbed components

The primary components used to develop the lab-scale implementation of a monitoring scheme based-on an EC gateway model, are listed as follows:

- RTDS.
- RTAC SEL-3555.
- Elipse Power from Elipse software™.

A brief introduction on each component are presented in the following sections.

4.2.1 Real-time digital simulator

The RTDS is a digital computing machine designed to run real-time simulations of power systems to study electromagnetic transients. Real-time simulations require extremely fast computing which is achieved via parallel computing technologies implemented in RTDS hardware. Being a digital simulator, RTDS calculates state of power system models at discrete time instants with a time-step of 50 microsrconds (µs) to satisfy requirements of real-time operations. The primary hardware comprises of Digital Signal Processors (DSP) and a Reduced Instruction Set Computer (RISC) (RTDS, 2012).

The processors are built in cards which are interconnected using backplane racks contained in cubicles as noticed in figure 4.1 below. The first generation of processor cards was Triple Processor Card (3PC), followed by Giga Processor Cards (GPC) and PB5 processor cards. The latest version and the most advanced release are the Nova Core processor cards. Design of RTDS is modular, whereby each rack in RTDS may consist of any combination of PB5 and GPC processor cards. In addition, several types of cards, each with a specific function are included in RTDS racks including:

- Giga Transceiver Workstation InterFace card (GTWIF): responsible for communication and data transfer between a rack and the workstation hosting the Real-time Simulation Computer-Aided Design (RSCAD) software over Ethernet. It is responsible for coordinating inter-rack processing tasks.
- Gigabit Transceiver Front Panel Interface card (GTFPI): serves as interface between the front digital panel and processor cards.

- Gigabit Transceiver NETwork interface card (GTNET): enables real-time communications with external devices using a variety of protocols including the IEC 61850 standards “GSSE, GOOSE, SMV”, DNP3, and IEEE C37.118 for Phasor Measurement Unit (PMU).
- Gigabit Transceiver SYNChronization card (GTSYNC): enables synchronization of simulations to external time references.

In addition, RTDS involves other hardware components such as the Global Bus Hub (GBH) which is required to coordinate operations in simulators comprising of at least three racks (RTDS, 2022).

Figure 4.1: **Different sizes RTDS cubicles (RTDS, 2012).**

The RSCAD is a software package that provides a Graphical User Interface (GUI) to RTDS. The RSCAD consists of several modules and tools, the three major modules are described as follows:

- File Manager: handles organization of projects and simulation cases, it enables data sharing between RTDS users.
- Draft: provides a graphical interface to build simulation cases and configure parameters of different components. It contains numerous graphical libraries for components of power systems, controls, and communications.
- Runtime: enables an interface to run and control simulation cases which are executed on RTDS. Various controls are enabled including start/stop the case, applying faults, and set point control (RTDS, 2012).

In the research project, the lab-scale testbed involves utilization of IEC 61850-8-1 GOOSE to publish values from the power network model in RTDS to an external gateway. Therefore, the following section presents more details on the GTNET card and implementation of GOOSE.

4.2.1.1 Generic object orientated substation event communications using the gigabit transceiver network interface card

The GTNET card is designed to enable the RTDS simulator to interface with external devices using a variety of communication protocols including IEC 61850-8-1 GOOSE. The GTNET communicates with external devices over Ethernet in a LAN. The connection diagram of GTNET to external devices is provided in figure 4.2 below. The GTNET card acts as a protocol converter between external devices and RTDS processor cards “GPC/PB5” which are connected to GTNET via fibre cables.

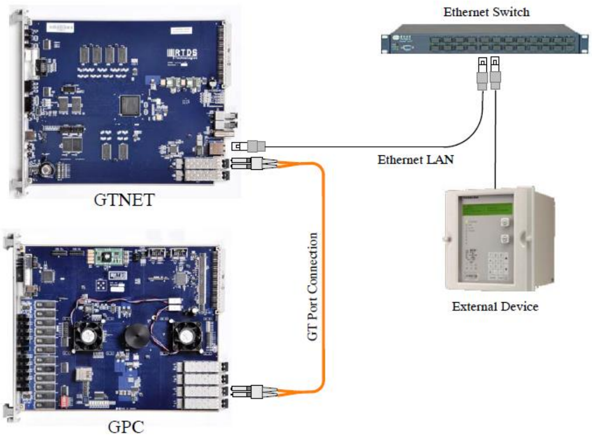
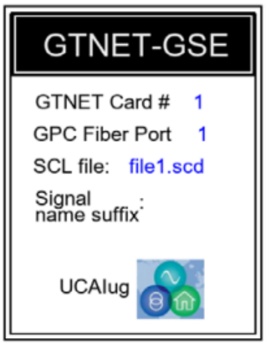


Figure 4.2: **GTNET card connection to external devices (RTDS, 2012).**

The IEC 61850-8-1 GOOSE can be enabled in RSCAD Draft module using GTNET-GSE v5 component from the automation and potection tab in the master library. The GTNET-GSE v5 component which is seen in figure 4.3 below, provides four receiving and transmitting modules “Rx/Tx” which can be organized to simulate up to four soft IEDs. A template Substation Configuration Description (SCD) file embedded in the GTNET-GSE component, describes the GTNET soft IED. The SCD editor is a tool embedded in the RSCAD Draft module which is used to edit the template SCD file and configure GOOSE. In the case of subscribing to GOOSE from external devices, the SCD editor allows for importing SCD files of these devices to map incoming GOOSE to GTNET-GSE inputs.


GTNET-GSE

GTNET Card # 1
GPC Fiber Port 1
SCL file: file1.scd
Signal name suffix:

Figure 4.3: **GTNET-GSE v5 (RTDS, 2019).**

Whereas, in the case of transmitting GOOSE, the SCD editor enables exporting an IED Capability Description (ICD) file of GTNET-GSE which can be loaded in other configuration tools to map GOOSE messages to receiving devices. An output dataset for GOOSE transmission from GTNET may contain up to sixty four data tags that may be configured to any data type including boolean, 32-bit floating point, 32-bit integer or 13-bit quality bitmaps (RTDS, 2019).

4.2.2 Real-time automation controller

The RTAC SEL-3555 is a powerful microcomputer equipped with a real-time operating system. It is a resourceful data concentrator that can gather data from IEDs and forward it to upper layers of SCADA systems. The RTAC SEL-3555 supports protocol conversion between various communication protocols. Additionally, it provides a platform for developing and executing programmable logic automation tasks that is developed using IEC 61131-3 standard language. The front view of an RTAC SEL-3555 unit is shown in figure 4.4 below. The RTAC SEL-3555 is configured using AcSELerator RTAC SEL-5033 software, which is employed to create projects, define source devices with their communication protocols, map data tags from source to destination, and to construct IEC 61131-3 custom logic programs (Schweitzer Engineering Laboratories Inc., 2018)..

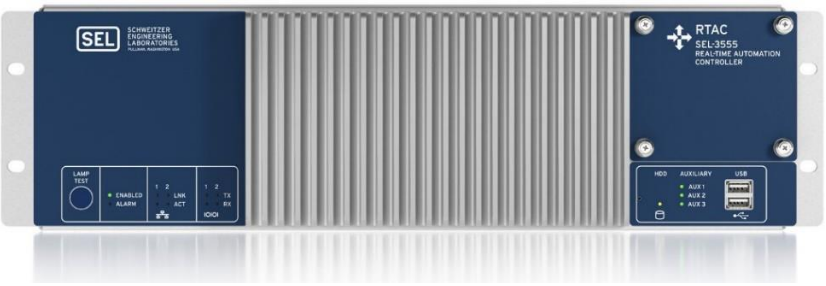


Figure 4.4: **RTAC SEL-3555 unit (Schweitzer Engineering Laboratories Inc., 2018).**

Tags are points in the database that are used to store numerous types of data in RTAC SEL-3555 including imported data, system values, and user-defined variables. A variable is a data tag identified by a name and data type within RTAC SEL-3555 logic, and can be declared and utilized by programs, functions, or function blocks. Tags or variables that can be accessed by all processes in RTAC SEL-3555, are called global tags such as system values, devices tags, virtual tags, and global tags defined in Global Variables Lists (GVLs). Or they can only be accessed by a specific function or program in which they were defined, these are called local variables (Schweitzer Engineering Laboratories Inc., 2018).

The RTAC SEL-3555 fully supports the IEC 61850 information model and communication services including MMS and GOOSE. The data tags are structured using the hierarchical model of the IEC 61850 standard in which each DO has multiple attributes including instantaneous value, time stamp, and quality attributes. The IEC 61850 information model and communication services are defined in the SCD file which includes definition of the server model, LNs, datasets, reports, and GOOSE services(Schweitzer Engineering Laboratories Inc., 2011).

The SCD file is configured using SEL-5032 AcSELerator Architect software, then it can be imported in AcSELerator RTAC SEL-5033 to complete the overall configuration before compiling and sending the file to RTAC SEL-3555. The AcSELerator Architect SEL-5032 software is employed to configure the IEC 61850-based information models Configured IED Description (CID), and ICD files of SEL and non-SEL IEDs. Designers use the software GUI to edit SCL files and configure datasets, GOOSE, reports, and MMS client/server settings and produce SCD configuration files (Schweitzer Engineering Laboratories Inc., 2011).

4.2.3 Elipse Power

Elipse Power is a software tool developed and promoted by Elipse software™, which is used to build SCADA applications for power systems. It runs on various versions of Windows operating systems and can be run on an Internet browser. Elipse Power has a modular structure whereby the functions are distributed across several modules. A Kernel program manages and coordinates the modules to ensure execution of required tasks. This modular structure allows independent modules and components to run on different machines simultaneously. There are four major modules in Elipse Power:

- **E3 Server:** the main application that is responsible for executing core tasks such as real-time communications with field devices and to run multiple projects simultaneously. The server is responsible for communicating with client applications to update data values or with other E3 servers to share the processing load and achieve redundancy.
- **Elipse Power Studio**: a platform consisting of graphical and script editors and libraries employed for configuring domains and projects.
- **Elipse Power Viewer:** a client application for visualizing and operating projects, and applications executed in the E3 server. It can be run on a browser connected to the server via the Internet.
- **E3 Admin:** an application that provides user interface to the E3 server and other Elipse Power applications. Users can utilize it to send control commands to the server.

The modular architecture of Elipse Power is exhibited in figure 4.5 below, which illustrates the basic components. Elipse Power applies a domain concept whereby the E3 server executes an E3 Runtime process “Domain” which is responsible for executing and managing independent servers and databases. Projects share resources “servers/databases” depending on their configuration, meaning that numerous projects can be executed concurrently within a single domain. Links can be established amongst multiple objects shared by various projects within the same domain as any value change of an object is instantly distributed to all linked objects.

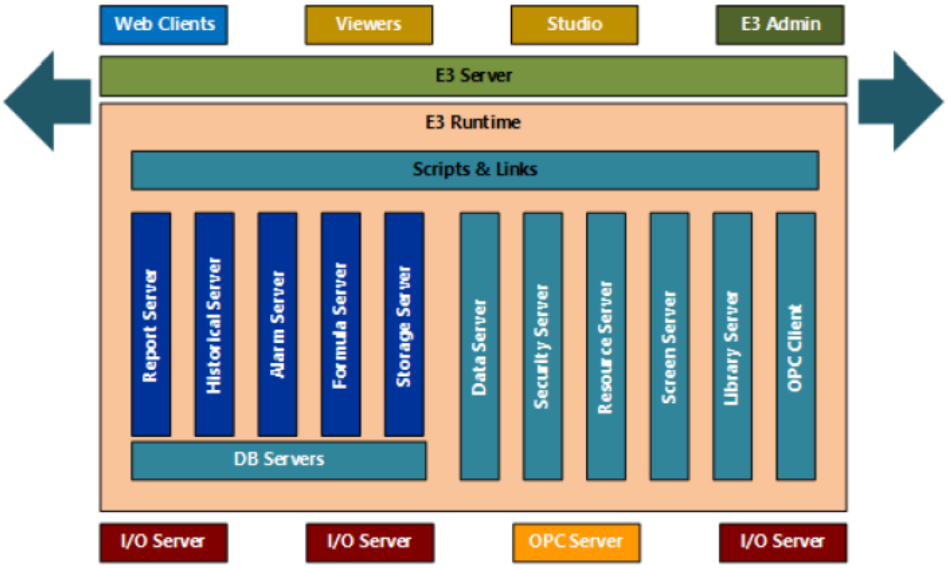


Figure 4.5: Elipse Power software architecture (Elipse Software Ltda, 2021).

Elipse Power utilizes I/O drivers to communicate with many types of controllers, data concentrators, and Remote Terminal Units (RTUs). Each driver hosts an I/O server process that executes a Dynamic Linked Library (DLL) file which defines communications via a specific protocol. I/O tags are assigned to each driver object to enable interaction from external devices. Each tag has a specific defined scan time which is used as an update interval for these tag values (Elipse Software Ltda, 2021).

4.2.3.1 IEC 61850 standard drivers

Elipse software™ have developed drivers for IEC 61850-based communications using MMS protocol over the Ethernet protocols suite “TCP/IP”. There are IEC 61850 client/server drivers implemented as DLL files that can be loaded into an I/O driver object in Elipse Power. Both drivers support importing SCL configuration files of devices and extracting the information model containing datasets and DOs. Additionally, both drivers support IEC 61850 features including reporting, single data polling, quality, and timestamps. The client driver can communicate with multiple devices simultaneously.

While, the server driver can only communicate with one client at a time. The latest version of IEC 61850 drivers in Elipse Power support IEC 61850-8-2 XMPP-based communications over WANs (Elipse Software Ltda, 2022; Elipse Software Ltda, 2019).

The following section presents a detailed description of the lab-scale implementation describing the configuration of the implemented models.

4.3 The lab-scale testbed configurations

In the research project, a lab-scale testbed was developed to implement the concept of an EC gateway for monitoring a modern power network integrated with a DER. A block diagram is noticed in figure 4.6 below, that illustrates the major components of the testbed. The model of the power network integrated to a DER, is implemented in RTDS and simulates a wind energy power generation unit. Data from the DER model is transmitted using IEC 61850-8-1 GOOSE protocol to the EC gateway model which is implemented using the RTAC SEL-3555 unit combined with Elipse Power. The RTAC SEL-3555 unit receives GOOSE messages and maps them to its server model. Additionally, a data fusion algorithm that reduces the data volume is implemented in RTAC SEL-3555 to apply the concept of EC. Thereafter, the data is forwarded to Elipse Power running on 'PC-1'.

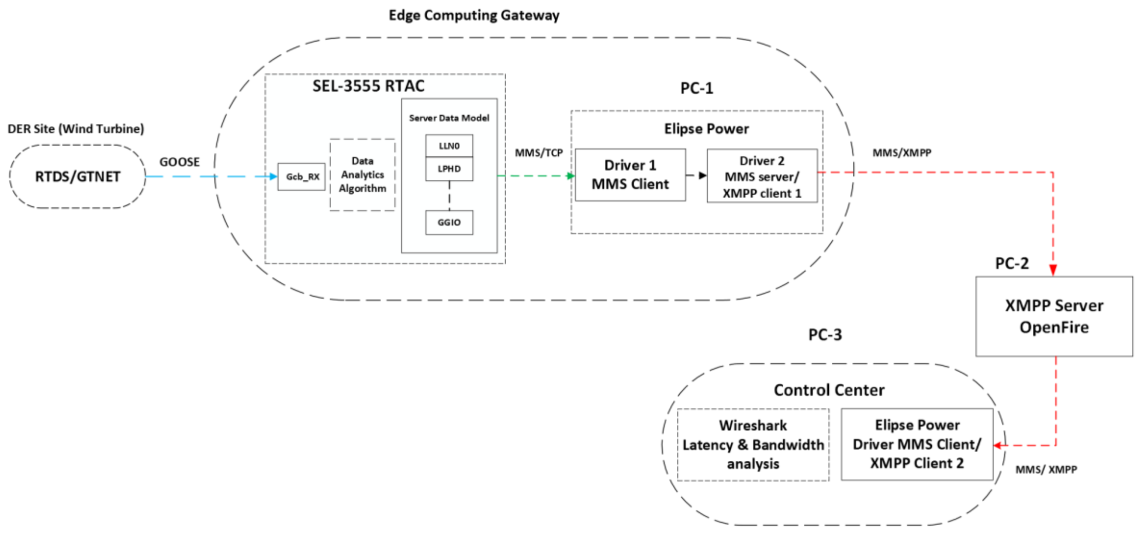


Figure 4.6: **A block diagram of the lab-scale testbed of a monitoring scheme.**

An IEC 61850-8-1 MMS client communication driver in Elipse Power is employed to poll data from RTAC SEL-3555 via MMS protocol over a LAN connection. Thereafter, the data is mapped to an IEC 61850-8-2 XMPP server driver that enables XMPP as a transport layer protocol according to the IEC 61850-8-2 XMPP standard. The XMPP-based communications take place over an Internet-based WAN through an Openfire XMPP server application installed on 'PC-2'. Finally, an IEC 61850-8-2 XMPP client driver within an Elipse Power application installed on ‘PC-3’ which is utilized to establish communications with the server driver in ‘PC-1’ and exchange data over an XMPP-based WAN communication. In the following sections, each component of the testbed is described in details, showing configurations of these components, and demonstrating the operation flow of the models and communications.

4.3.1 Wind energy power network model

A model was developed by RTDS Inc.™ to simulate the wind generation system at St. Leon windfarm which is integrated with the Manitoba Hydro power system in Manitoba, Canada (RTDS, 2008). The model simulates a wind turbine coupled with an induction generator and connected to the power grid through transformers. The RSCAD Draft model consists of a hierarchy box with a picture of wind turbines connected to a voltage source as displayed in figure 4.7 below. The voltage source is configured as voltage behind impedance to simulate a simple load (RTDS, 2008).

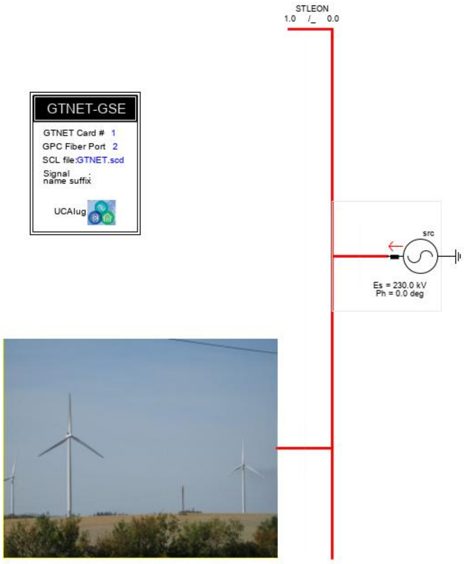


Figure 4.7: **RSCAD Draft model of a power network integrated with a wind energy DER.**

The GTNET-GSE v5 component is added to the model and configured to publish various values via GOOSE to an external gateway device. The RSCAD Draft model of the wind generation system inside the hierarchy box is illustrated in figure 4.8 below. The model consists of several components which are:

- A wind turbine.
- An induction machine generator.
- Grid coupling components “transformers and a circuit breaker”.

The following sections present descriptions of each component and an overview for operation flow of the model.

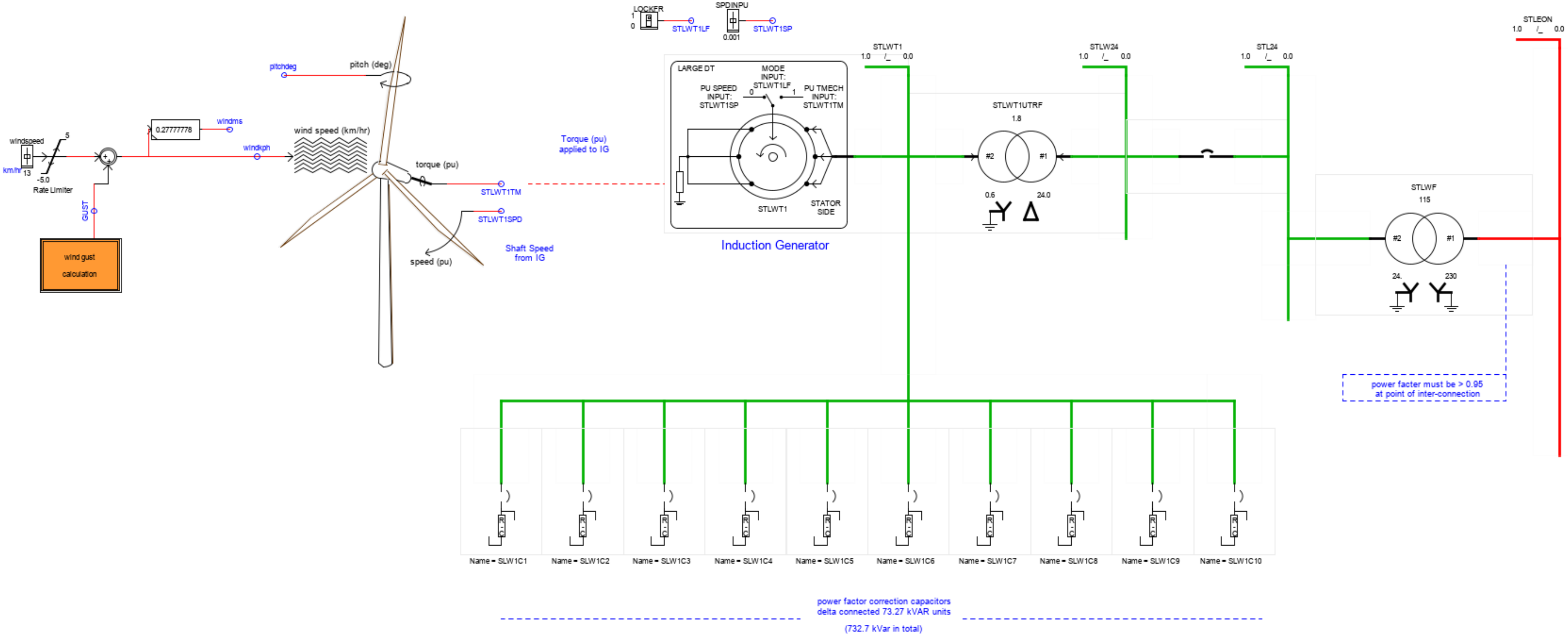


Figure 4.8: The RSCAD Draft model of the wind power generation system (RTDS, 2008).

4.3.1.1 Wind turbine model

The turbine model in RTDS takes atmospheric parameters as inputs to calculate the air density, the available wind energy, and the turbine's conversion efficiency. The atmospheric parameters are wind speed, air temperature, barometric pressure, and relative humidity. They are configured to be manually controlled in RSCAD Runtime module. Additionally, the model includes a simulation of wind gusts which are sudden wind blows. The simulator allows one to manually set the gust duration and speed. Efficiency of the wind turbine which is reffered to as the coefficient of power (Cp), is an extremely non-linear function of the wind speed as depicted in the plot diagram in figure 4.9 below. A set of Cp versus wind speed curves is often determined by measurements and used to calculate the amount of power produced by the turbine at a specific wind speed (RTDS, 2008).

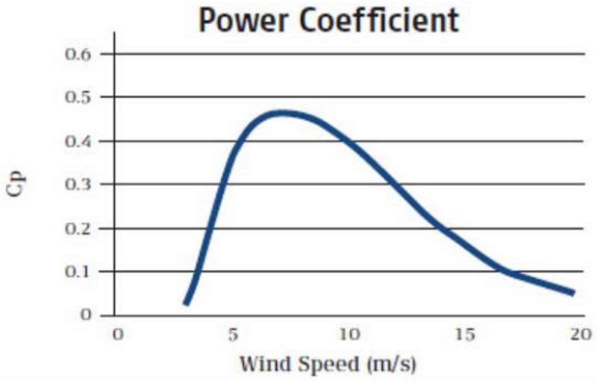


Figure 4.9: **A diagram for power coefficient Vs wind speed (RTDS, 2008).**

The Cp curve is required to enable the blades' pitch angle control to maintain a rated power output at different wind speeds. Controlling the blades' pitch angle is done by active stall of the turbine if the wind speed exceeds the one that produces rated power. The Cp curve which is noted in figure 4.9 above, is for a Vestas V82 turbine which is operated at the St. Leon windfarm and simulated in the RTDS model. Table A.1 in the appendix presents the specifications of Vestas V82 turbines (RTDS, 2008).

The turbine model drives an induction machine generator; thus, it computes turbine torque in per unit (pu) which is fed to the generator. The model receives the generator's rotor speed as the input to maintain synchronization. The specifications of the induction generator model are provided in table A.2 in the appendix. The generator model in RTDS uses a self-excitation technique whereby specific capacitance is connected at the generator terminals to stabilize the voltage output. Two step-up transformers are utilized to adapt the generator's voltage output for grid integration over two stages (RTDS, 2008).

In the first stage, a “0.6:24” kilo Volts (kV) transformer is used and connected to a circuit breaker which controls coupling of the generator to the grid. Thereafter, a “24:115” kV transformer is placed at the final stage before connection to the grid (RTDS, 2008).

4.3.1.2 Pitch angle controller

The model uses a feedback control system for turbine blades’ pitch angle control as seen in figure A.2 in the appendix. The controller consists of two control loops and only one loop can be active at a time. The inactive loop tracks the pitch degree from the active one so that it will initialize from the current value. One loop controls blades’ pitch angle according to the turbine speed during start-up when the grid coupling breaker is open. Once the turbine is synchronized and coupled to the grid, the other loop controls blades’ pitch angle according to the setpoint of output power order (RTDS, 2008).

4.3.1.3 Power factor controller

Ten capacitors, each with “800” micro Farad (μF) capacitance, are connected in parallel at the generator’s terminals. They are utilized for self-excitation of the generator when it is not coupled to the grid. The RSCAD Draft model of the controller is shown in figure A.3 in the appendix. When the generator is coupled to the grid, the capacitors are controlled to maintain the power factor at unity for the rated power output (RTDS, 2008).

4.3.1.4 Simulation and operation

Following the methodology of RSCAD, firstly, a circuit diagram for the modelling case is built on the Draft module. Secondly, the case is compiled and downloaded to RTDS processors, and the simulation is run on RSCAD Runtime module where inputs are controlled by the user and measurements are displayed. The Runtime module for the wind generation system is displayed in figure 4.10 below. The user has control of the atmospheric input variables including air temperature, pressure, and humidity. Additionally, the model allows for simulating wind gusts by setting the gust duration, wind speed, and a pushbutton to activate the gust condition (RTDS, 2008).

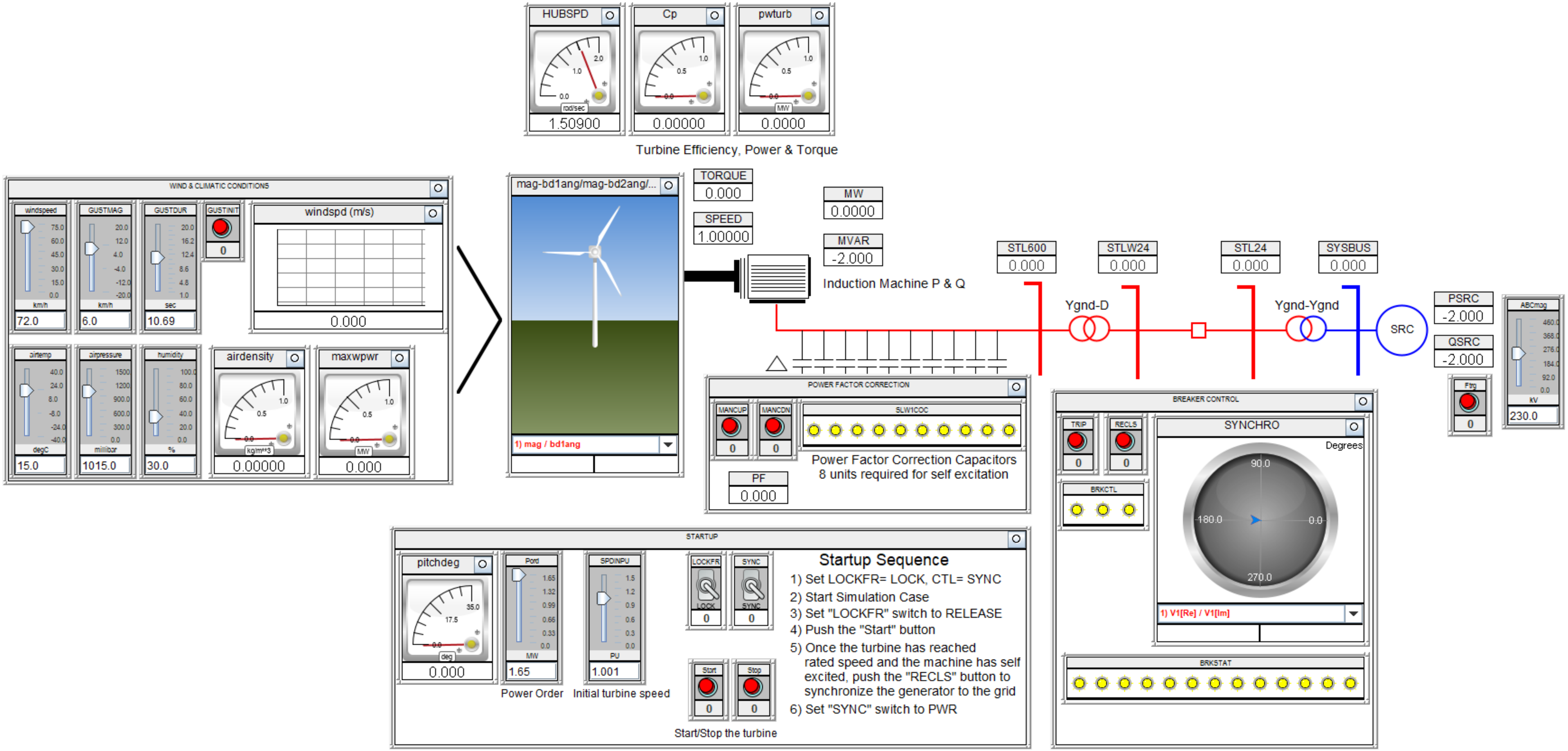
Moreover, the model allows the user to start/stop the wind turbine. The user can control grid coupling circuit breaker with two pushbuttons ‘TRIP’ and ‘RECLS’. the model includes control of coupling the induction generator to the wind turbine via a mode selector ‘LOCKFR’ that switches between ‘LOCK’ and ‘RELEASE’ modes. Furthermore, The model allows for setting setpoints and controlling the mode for pitch angle control between power order and turbine speed (RTDS, 2008).

The simulation can be started with the wind turbine at a standstill, in this case, it takes the turbine model few minutes to reach rated speed. It is possible to start the simulation with turbine at rated speed. Considering turbine speed is started from a standstill state, the standard start-up process of the turbine model consists of the following steps:

- Induction machine mode is set to ‘RELEASE’ and pitch angle control is set to speed control by setting the ‘SYNC’ switch to ‘SYNC’ mode.
- The turbine is started by pressing the ‘START’ pushbutton which activates the speed control loop of the pitch angle controller with speed set to ‘1.001’ pu. The pitch angle will be set to zero initially to extract maximum torque from the wind.
- When reaching the set-point speed, the induction machine should be self-excited utilizing the connected capacitors.
- The generator is coupled to the grid by closing a circuit breaker.
- The pitch angle control mode is changed to power order by setting the ‘SYNC’ switch to ‘PWR’. It enables control of power output using pitch angle control (RTDS, 2008).

4.3.1.5 Measured values

Several values are extracted from the model and transmitted to the gateway via GOOSE. Monitoring of data in RSCAD takes place using signal names that are similar to register addresses. Each name refers to a specific parameter or data tag and stores the data value to be utilized in any configuration in the Draft module or for monitoring in the Runtime module using meters and graphs. The signal names considered for the monitoring scheme in the implementation are listed in table A.3 in the appendix. Data tags taken from the wind turbine and the induction generator models are included, in addition to two atmospheric parameters “wind speed and air density” which are computed by the wind turbine model.



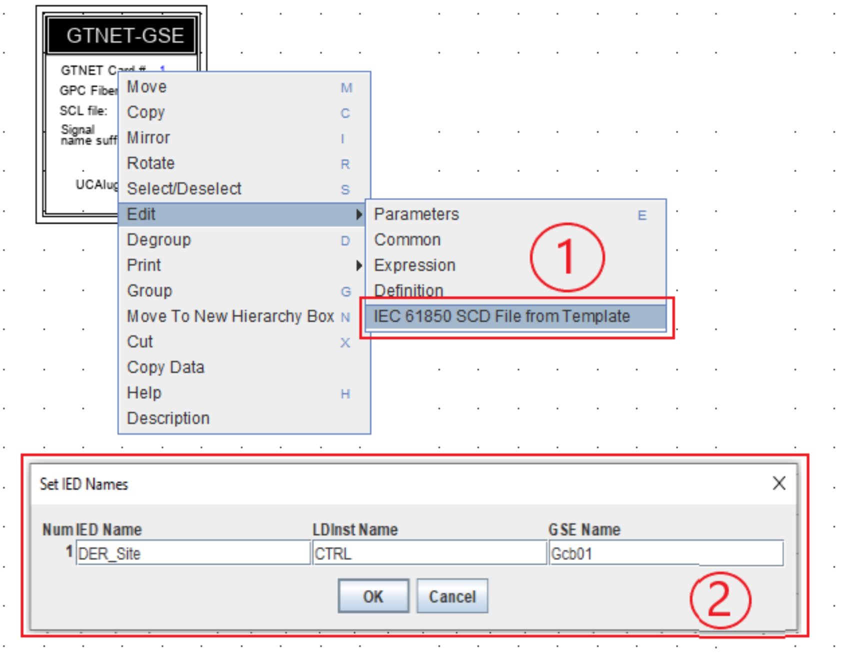
Startup Sequence

1) Set LOCKFR= LOCK, CTL= SYNC
2) Start Simulation Case
3) Set "LOCKFR" switch to RELEASE
4) Push the "Start" button
5) Once the turbine has reached rated speed and the machine has self excited, push the "RECLS" button to synchronize the generator to the grid
6) Set "SYNC" switch to PWR

Figure 4.10: RSCAD Runtime model of the wind power generation system.

4.3.1.6 IEC 61850-8-1 GOOSE configurations

As mentioned in section 4.2.1.1 above, IEC 61850-8-1 GOOSE messages can be published from RTDS/RSCAD via the GTNET card. The following steps demonstrate configuration of the GTNET-GSE v5 component to achieve the publishing of GOOSE messages. Firstly, a GTNET-GSE v5 component must be imported from the master library in RSCAD Draft module. Right click on it and navigate to edit the template SCD file. The SCD editor tool will be launched by prompting a window to define names for the soft IED, the LD, and the GoCB as demonstrated in figure 4.11 below.

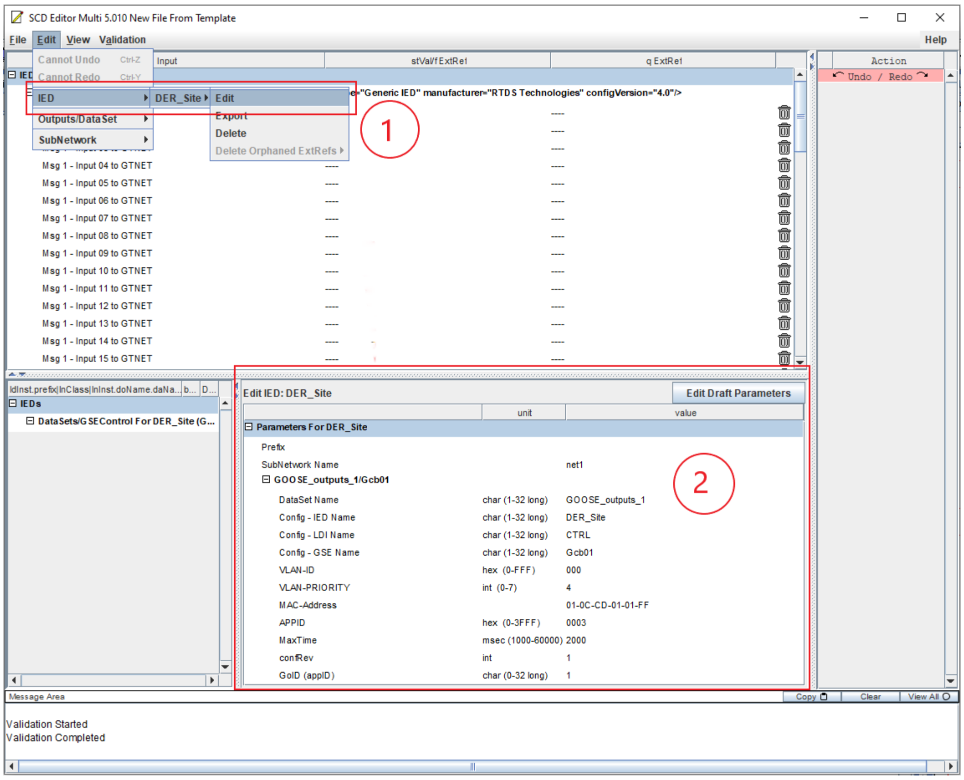


Set IED Names

Num	IED Name	LDInst Name	GSE Name
1	DER_Site	CTRL	Gcb01

Figure 4.11: Launching SCD editor tool of GTNET-GSE component.

Once all required names are entered and confirmed, the SCD editor window opens. It allows for editing the GTNET's soft IED parameters, including names and communication parameters. To do this, navigate to 'Edit' tab, select the created IED 'DER_Site', and click on edit as noticed in figure 4.12 below.



e="Generic IED" manufacturer="RTDS Technologies" configVersion="4.0"/>

Msg 1 - Input 04 to GTNET
Msg 1 - Input 05 to GTNET
Msg 1 - Input 06 to GTNET
Msg 1 - Input 07 to GTNET
Msg 1 - Input 08 to GTNET
Msg 1 - Input 09 to GTNET
Msg 1 - Input 10 to GTNET
Msg 1 - Input 11 to GTNET
Msg 1 - Input 12 to GTNET
Msg 1 - Input 13 to GTNET
Msg 1 - Input 14 to GTNET
Msg 1 - Input 15 to GTNET

ldInst.prefix|lnClass|lnInst.doName.daNa... b... D...
IEDs
DataSets/GSEControl For DER_Site (G...

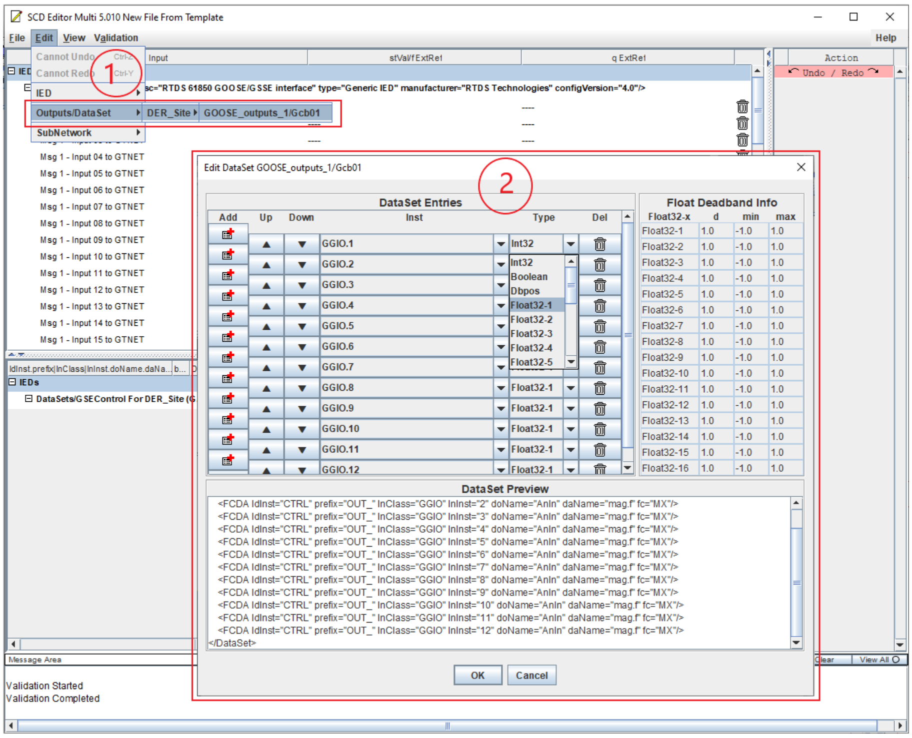
Edit IED: DER_Site

Parameters For DER_Site	unit	value
Prefix		
SubNetwork Name		net1
GOOSE_outputs_1/Gcb01		
DataSet Name	char (1-32 long)	GOOSE_outputs_1
Config - IED Name	char (1-32 long)	DER_Site
Config - LDI Name	char (1-32 long)	CTRL
Config - GSE Name	char (1-32 long)	Gcb01
VLAN-ID	hex (0-FFF)	000
VLAN-PRIORITY	int (0-7)	4
MAC-Address		01-0C-CD-01-01-FF
APPID	hex (0-3FFF)	0003
MaxTime	msec (1000-60000)	2000
confRev	int	1
GoID (appID)	char (0-32 long)	1

```
Validation Started
Validation Completed
```

Figure 4.12: GTNET soft IED parameters.

The dataset that will be published via GOOSE can be created and configured from the SCD editor. Navigate to 'Edit' tab, select 'Outputs/Dataset', highlight the IED "DER_Site", then click on 'GOOSE_outputs_1/Gcb01'. A window will be prompted for adding DOs to the output dataset and configuring their data type to 'Float32', which is suitable for the analog values that are to be published from RTDS as depicted in figure 4.13 below.



sc="RTDS 61850 GOOSE/GSSE interface" type="Generic IED" manufacturer="RTDS Technologies" configVersion="4.0"/>

Msg 1 - Input 04 to GTNET
Msg 1 - Input 05 to GTNET
Msg 1 - Input 06 to GTNET
Msg 1 - Input 07 to GTNET
Msg 1 - Input 08 to GTNET
Msg 1 - Input 09 to GTNET
Msg 1 - Input 10 to GTNET
Msg 1 - Input 11 to GTNET
Msg 1 - Input 12 to GTNET
Msg 1 - Input 13 to GTNET
Msg 1 - Input 14 to GTNET
Msg 1 - Input 15 to GTNET

ldInst.prefix|lnClass|lnInst.doName.daNa... b...
IEDs
DataSets/GSEControl For DER_Site (G

Edit DataSet GOOSE_outputs_1/Gcb01

DataSet Entries

Inst	Type
GGIO.1	Int32
GGIO.2	
GGIO.3	
GGIO.4	
GGIO.5	
GGIO.6	
GGIO.7	
GGIO.8	Float32-1
GGIO.9	Float32-1
GGIO.10	Float32-1
GGIO.11	Float32-1
GGIO.12	Float32-1

Float Deadband Info

Float32-x	d	min	max
Float32-1	1.0	-1.0	1.0
Float32-2	1.0	-1.0	1.0
Float32-3	1.0	-1.0	1.0
Float32-4	1.0	-1.0	1.0
Float32-5	1.0	-1.0	1.0
Float32-6	1.0	-1.0	1.0
Float32-7	1.0	-1.0	1.0
Float32-8	1.0	-1.0	1.0
Float32-9	1.0	-1.0	1.0
Float32-10	1.0	-1.0	1.0
Float32-11	1.0	-1.0	1.0
Float32-12	1.0	-1.0	1.0
Float32-13	1.0	-1.0	1.0
Float32-14	1.0	-1.0	1.0
Float32-15	1.0	-1.0	1.0
Float32-16	1.0	-1.0	1.0

DataSet Preview

```
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="2" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="3" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="4" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="5" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="6" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="7" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="8" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="9" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="10" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="11" doName="AnIn" daName="mag.f" fc="MX"/>
<FCDA ldInst="CTRL" prefix="OUT_" lnClass="GGIO" lnInst="12" doName="AnIn" daName="mag.f" fc="MX"/>
</DataSet>
```

```
Validation Started
Validation Completed
```

Figure 4.13: Editing output Datasets.

Now, the SCD file is ready to be saved by navigating to ‘File’ tab and clicking on ‘Save’. A window will prompt to enter a name for the SCD file which will be saved in RSCAD Draft directory. The next step is to configure RTAC SEL-3555 to subscribe to GOOSE from RTDS. The RTAC SEL-3555 is the first component of the EC gateway model. The steps to configure the components of the EC gateway model are described in the following section.

4.3.2 Edge computing gateway model

The EC gateway model consists of two components, namely an RTAC SEL-3555, and ‘PC-1’ that hosts an Elipse Power application as described in figure 4.14 below.

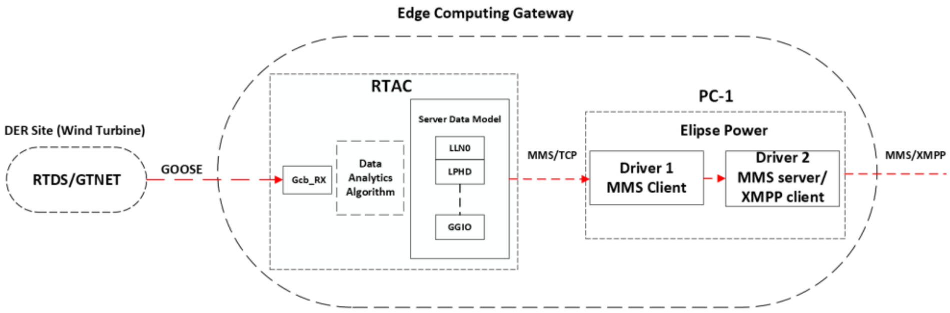
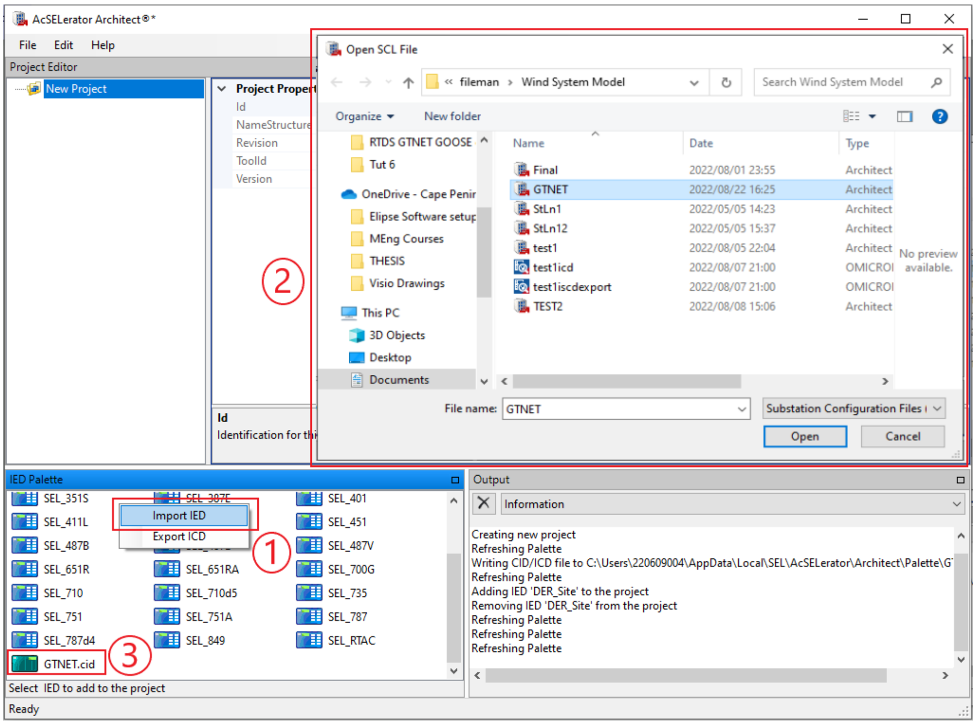


Figure 4.14: **A diagram of the EC gateway model.**

The following sections present configuration steps for each component of the EC gateway model.

4.3.2.1 Configuration of RTAC SEL-3555

The first step is to configure the IEC 61850 SCD file of RTAC SEL-3555 to subscribe to GOOSE messages from RTDS. This is accomplished by using AcSELerator Architect SEL-5032 software that produces the configured SCD file. Thereafter, the SCD file is uploaded to AcSELerator RTAC SEL-5033 software to complete the configuration of RTAC SEL-3555. The first step after opening AcSELerator Architect SEL-5032 is to import the CID file of the GTNET. To achieve this, right-click anywhere in the IED palette and click on import IED, then browse to select the previously saved GTNET SCD file as seen in figure 4.15 below.



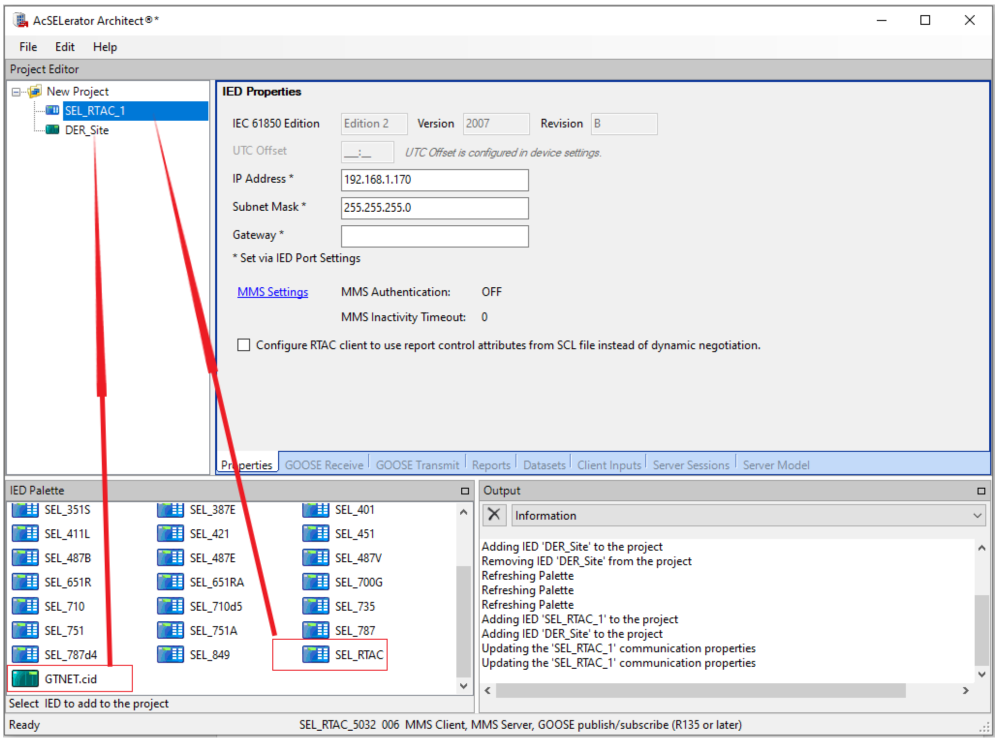
Name	Date	Type
Final	2022/08/01 23:55	Architect
GTNET	2022/08/22 16:25	Architect
StLn1	2022/05/05 14:23	Architect
StLn12	2022/05/05 15:37	Architect
test1	2022/08/05 22:04	Architect
test1icd	2022/08/07 21:00	OMICROI
test1iscdexport	2022/08/07 21:00	OMICROI
TEST2	2022/08/08 15:06	Architect

File name: GTNET

```
Creating new project
Refreshing Palette
Writing CID/ICD file to C:\Users\220609004\AppData\Local\SEL\AcSELerator\Architect\Palette\G
Refreshing Palette
Adding IED 'DER_Site' to the project
Removing IED 'DER_Site' from the project
Refreshing Palette
Refreshing Palette
Refreshing Palette
```

Figure 4.15: Importing GTNET CID file to AcSELerator Architect SEL-5032.

The next step is to import the GTNET and RTAC SEL-3555 SCD files into the project editor pane using drag and drop as shown in figure 4.16 below. It is noted that, when dragging the GTNET file, the IED appears with the name “DER_Site” which is the original configured name for the GTNET soft IED in the RSCAD SCD editor. While ‘GTNET’ is the name that was used when saving the SCD file after the configuration was accomplished.



IEC 61850 Edition: Edition 2 Version: 2007 Revision: B

UTC Offset: __:__ *UTC Offset is configured in device settings.*

IP Address *: 192.168.1.170

Subnet Mask *: 255.255.255.0

Gateway *:

* Set via IED Port Settings

MMS Authentication: OFF

MMS Inactivity Timeout: 0

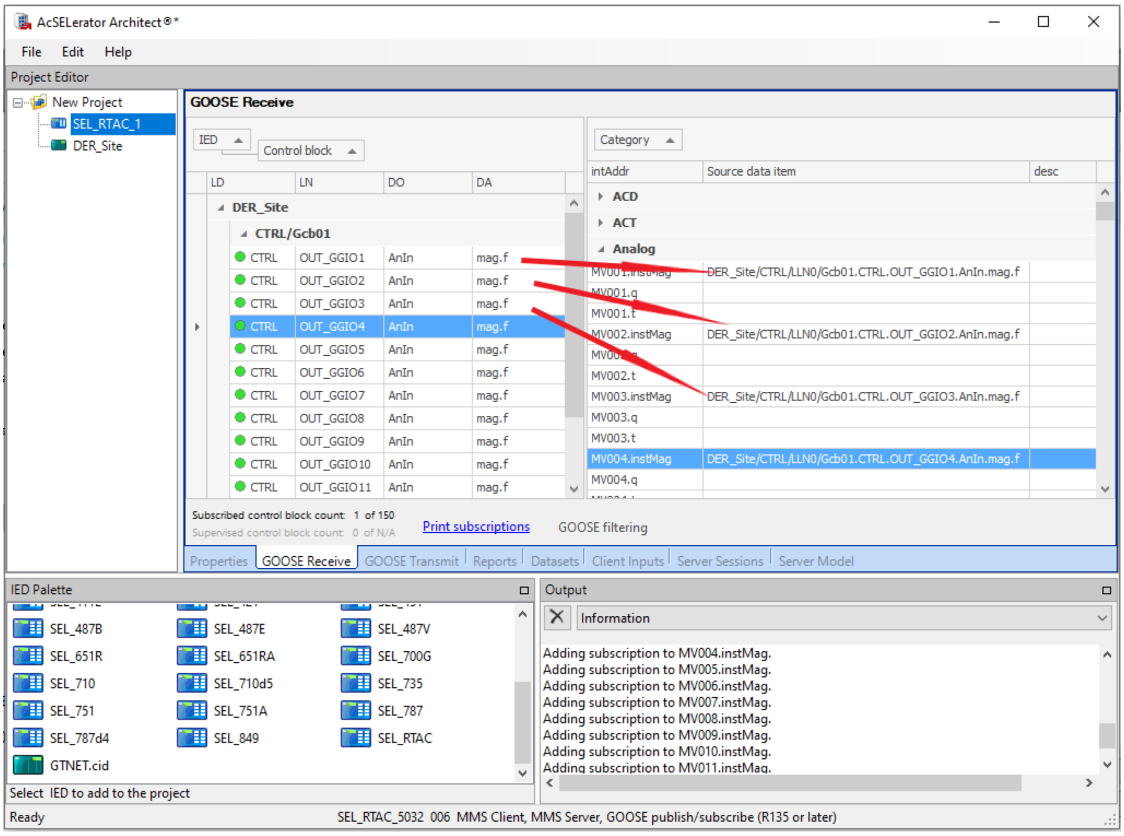
☐ Configure RTAC client to use report control attributes from SCL file instead of dynamic negotiation.

```
Adding IED 'DER_Site' to the project
Removing IED 'DER_Site' from the project
Refreshing Palette
Refreshing Palette
Refreshing Palette
Adding IED 'SEL_RTAC_1' to the project
Adding IED 'DER_Site' to the project
Updating the 'SEL_RTAC_1' communication properties
Updating the 'SEL_RTAC_1' communication properties
```

SEL_RTAC_5032_006 MMS Client, MMS Server, GOOSE publish/subscribe (R135 or later)

Figure 4.16: Importing IEC 61850 CID files of RTAC SEL-3555 and GTNET.

When RTAC SEL-3555 object is highlighted in the project editor, multiple configuration tabs appears on the right side of the window. The first tab 'Properties' contains communication parameters of RTAC SEL-3555, including IP, subnet mask, and gateway addresses as displayed in figure 4.16 above. The tab 'GOOSE Receive' enables configuring subscription to GOOSE messages published by the GTNET soft IED "DER_Site". Each DO from the IED "DER_Site" is mapped to an analog object in the RTAC SEL-3555's GoCB as noticed in figure 4.17 below.



DER_Site
CTRL/Gcb01

LD	LN	DO	DA
CTRL	OUT_GGIO1	AnIn	mag.f
CTRL	OUT_GGIO2	AnIn	mag.f
CTRL	OUT_GGIO3	AnIn	mag.f
CTRL	OUT_GGIO4	AnIn	mag.f
CTRL	OUT_GGIO5	AnIn	mag.f
CTRL	OUT_GGIO6	AnIn	mag.f
CTRL	OUT_GGIO7	AnIn	mag.f
CTRL	OUT_GGIO8	AnIn	mag.f
CTRL	OUT_GGIO9	AnIn	mag.f
CTRL	OUT_GGIO10	AnIn	mag.f
CTRL	OUT_GGIO11	AnIn	mag.f

Subscribed control block count: 1 of 150
Supervised control block count: 0 of N/A

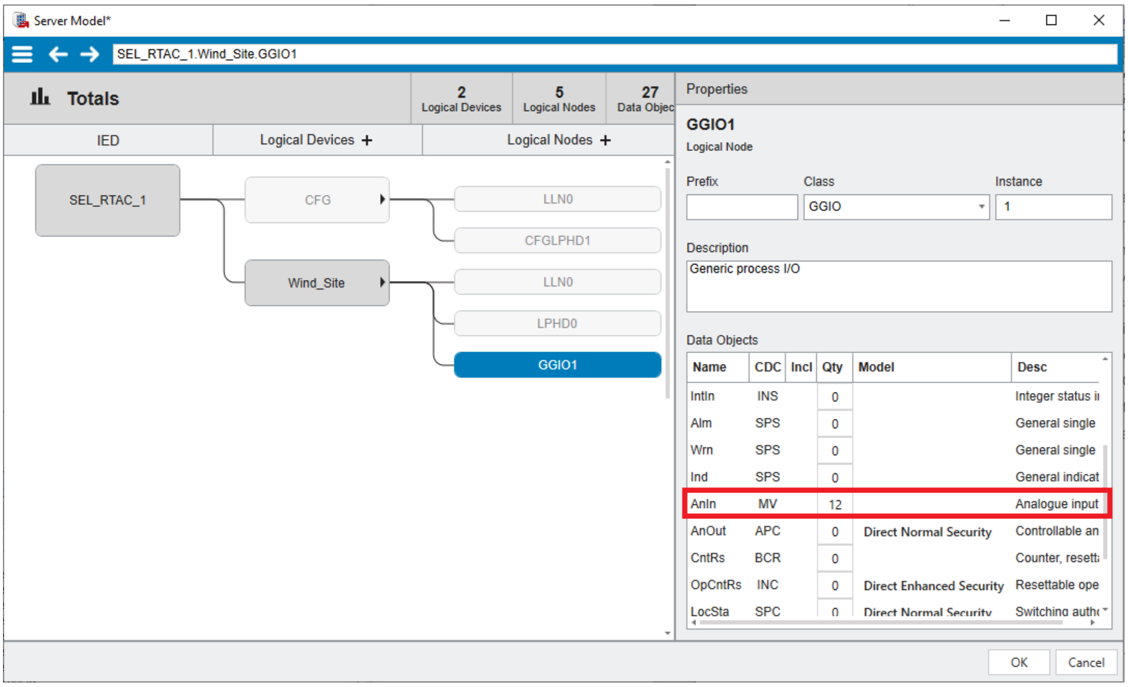
intAddr	Source data item	desc
ACD		
ACT		
Analog		
MV001.instMag	DER_Site/CTRL/LLN0/Gcb01.CTRL.OUT_GGIO1.AnIn.mag.f	
MV001.q		
MV001.t		
MV002.instMag	DER_Site/CTRL/LLN0/Gcb01.CTRL.OUT_GGIO2.AnIn.mag.f	
MV002.q		
MV002.t		
MV003.instMag	DER_Site/CTRL/LLN0/Gcb01.CTRL.OUT_GGIO3.AnIn.mag.f	
MV003.q		
MV003.t		
MV004.instMag	DER_Site/CTRL/LLN0/Gcb01.CTRL.OUT_GGIO4.AnIn.mag.f	
MV004.q		

```
Adding subscription to MV004.instMag.
Adding subscription to MV005.instMag.
Adding subscription to MV006.instMag.
Adding subscription to MV007.instMag.
Adding subscription to MV008.instMag.
Adding subscription to MV009.instMag.
Adding subscription to MV010.instMag.
Adding subscription to MV011.instMag.
```

Ready SEL_RTAC_5032 006 MMS Client, MMS Server, GOOSE publish/subscribe (R135 or later)

Figure 4.17: **IEC 61850 GOOSE subscription configuration.**

The RTAC SEL-3555 acts as an MMS server that forwards the received data to the next component in the gateway model which is an IEC 61850-8-1 MMS client driver in the Elipse Power application. Hence, the received GOOSE messages must be mapped from the GoCB in RTAC SEL-3555 to the server model. First, the server model of RTAC SEL-3555 must be configured by defining a new LD and a generic LN with multiple analog inputs. This is done by navigating to the 'Server Model' tab and then clicking on 'edit' to open the server model configuration window as illustrated in figure 4.18 below. The figure shows the created LD "Wind_Site" and the LN of type "GGIO" with twelve analog inputs to match the number of received GOOSE messages.



SEL_RTAC_1.Wind_Site.GGIO1

GGIO1
Logical Node

Prefix:
Class: GGIO
Instance: 1

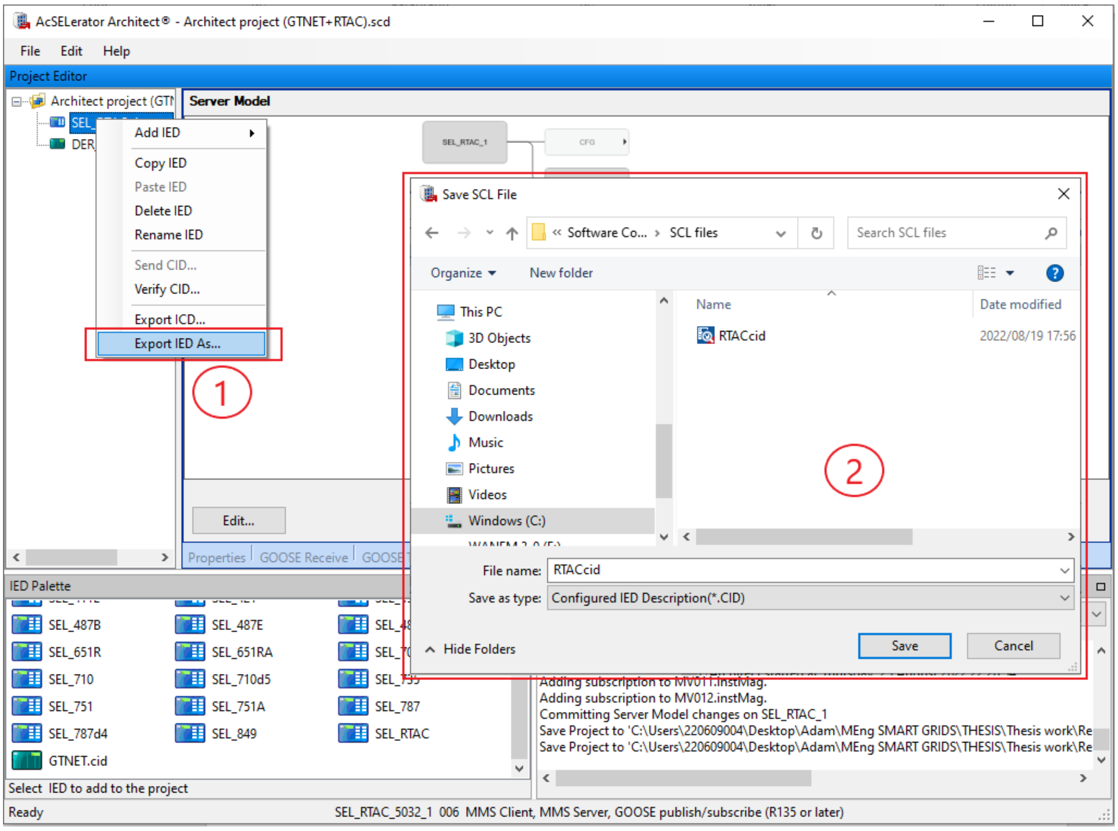
Description: Generic process I/O

Data Objects

Name	CDC	Incl	Qty	Model	Desc
IntIn	INS		0		Integer status i
Alm	SPS		0		General single
Wrn	SPS		0		General single
Ind	SPS		0		General indicat
AnIn	MV		12		Analogue input
AnOut	APC		0	Direct Normal Security	Controllable an
CntRs	BCR		0		Counter, resett
OpCntRs	INC		0	Direct Enhanced Security	Resettable ope
LocSta	SPC		0	Direct Normal Security	Switching auth

Figure 4.18: RTAC SEL-3555 server model.

The SCD file must be saved under a custom name and finally, a CID file of RTAC SEL-3555 must be individually exported as depicted in figure 4.19 below. The CID file will be used later for configuring the MMS client driver in Elipse Power.



RTACcid 2022/08/19 17:56

File name: RTACcid

Save as type: Configured IED Description(*.CID)

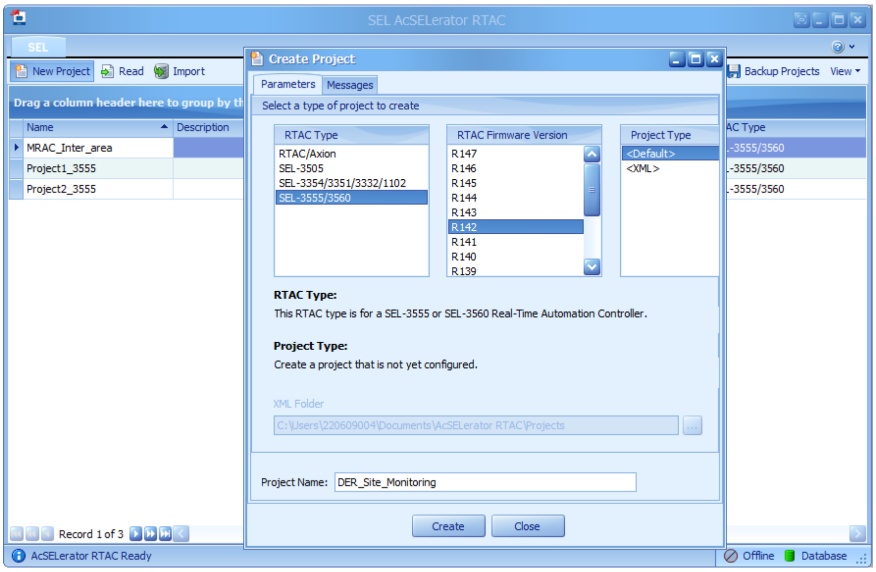
```
Adding subscription to MV011.instMag.
Adding subscription to MV012.instMag.
Committing Server Model changes on SEL_RTAC_1
Save Project to 'C:\Users\220609004\Desktop\Adam\MEng SMART GRIDS\THESIS\Thesis work\Re
Save Project to 'C:\Users\220609004\Desktop\Adam\MEng SMART GRIDS\THESIS\Thesis work\Re
```

Select IED to add to the project

Ready   SEL_RTAC_5032_1 006 MMS Client, MMS Server, GOOSE publish/subscribe (R135 or later)

Figure 4.19: Exporting the CID file of RTAC SEL-3555.

The remainder of RTAC SEL-3555 configuration is performed in AcSELerator RTAC SEL-5033 software. The first step is to create a new project by clicking on 'New Project' button on the top left of the window. This will prompt a window to enter a project name and to determine type and firmware version of RTAC as shown in figure 4.20 below. 'DER_Site_Monitoring' was entered as the project name, RTAC type 'SEL-3555' and firmware version 'R142' were selected as per the used unit specifications.



Select a type of project to create

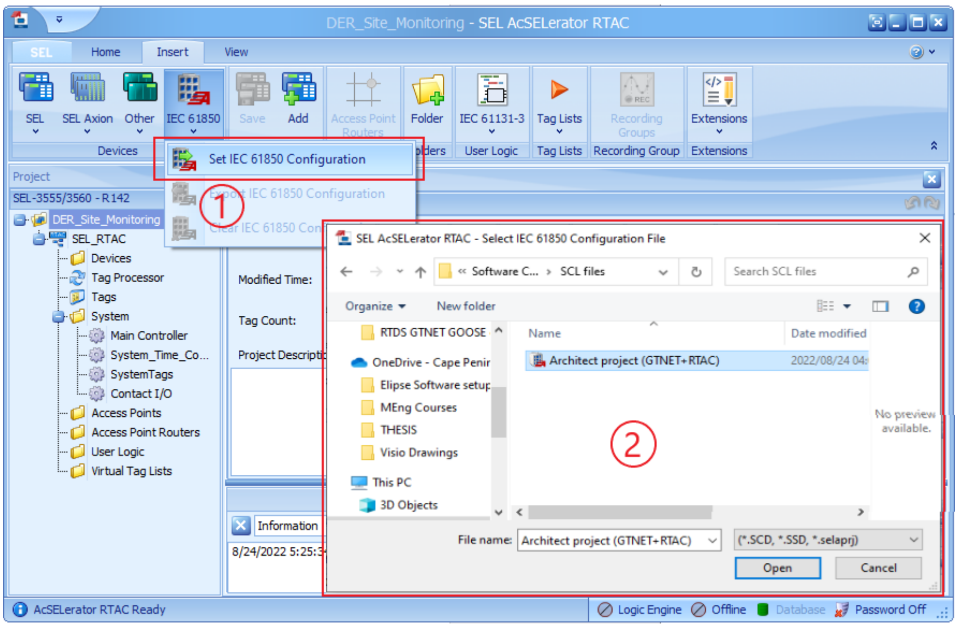
RTAC Type:
This RTAC type is for a SEL-3555 or SEL-3560 Real-Time Automation Controller.

Project Type:
Create a project that is not yet configured.

Project Name: DER_Site_Monitoring

Figure 4.20: Creating a new project in AcSELerator RTAC SEL-5033.

The IEC 61850 SCD file which was previously configured via AcSELerator Architect SEL-5032 software must be imported. This is done by navigating to 'Insert' tab, clicking on 'IEC 61850' drop-down menu, and clicking 'Set IEC 61850 Configuration'. Then, a window is prompted to browse and select the specified SCD file as seen in figure 4.21 below.

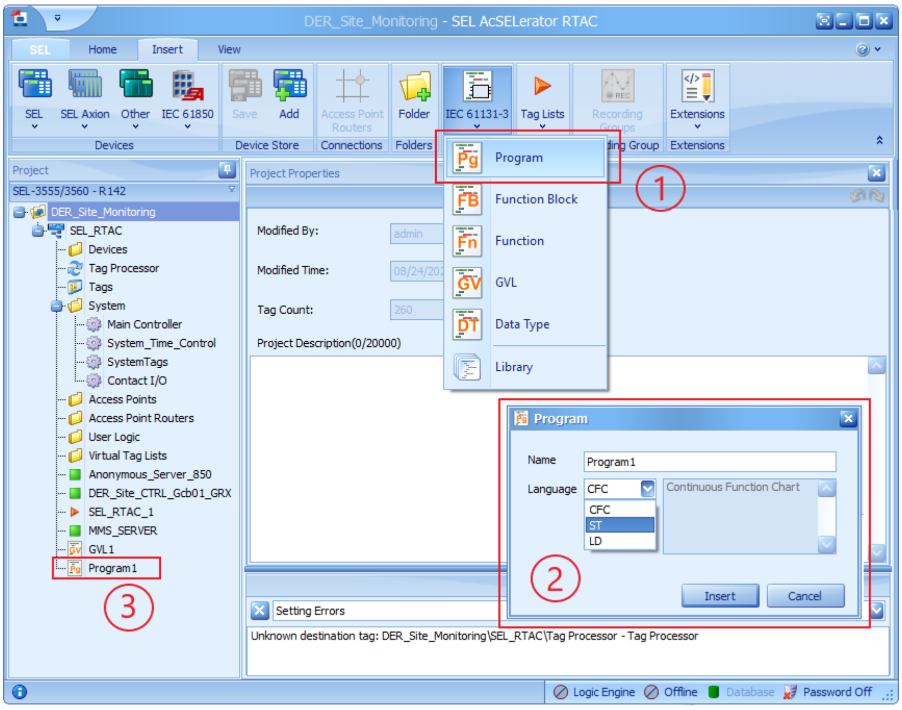


File name: Architect project (GTNET+RTAC)
(*.SCD, *.SSD, *.selaprj)

Figure 4.21: Importing IEC 61850 SCD file.

Upon importing the IEC 61850 configuration file, multiple entities appear in the project windowpane. They include the GoCB of the GTNET IED “DER_Site”, RTAC SEL-3555’s anonymous MMS server, and an IEC 61850 shared map of the server model tags. The MMS server model of RTAC SEL-3555 can be configured in order to allow connection to anonymous clients, or to respond to ten identified clients. The default setting is to allow anonymous clients which was maintained in the configuration.

Mapping GOOSE messages to the RTAC SEL-3555’s server model is accomplished via IEC 61131-3 custom logic. The logic is developed in a ‘Program’ instant that is added to the project from IEC 61131-3 drop-down menu. Click on ‘Program’ and a window will be prompted that enables entering a name and selecting the language type as noted in figure 4.22 below. Three options are available for IEC 61131-3 language; Continuous Functional Chart (CFC), Ladder Diagram, and Structured Text (ST). The ST language was chosen for the implementation. From the same menu, a GVL instant ‘GVL1’ is added to the project. Global variables will be used in building the EC algortihm which will be demonstrated in details in the next chapter.



Modified By: admin

Modified Time: 08/24/20

Tag Count: 260

Project Description(0/20000)

Name: Program1

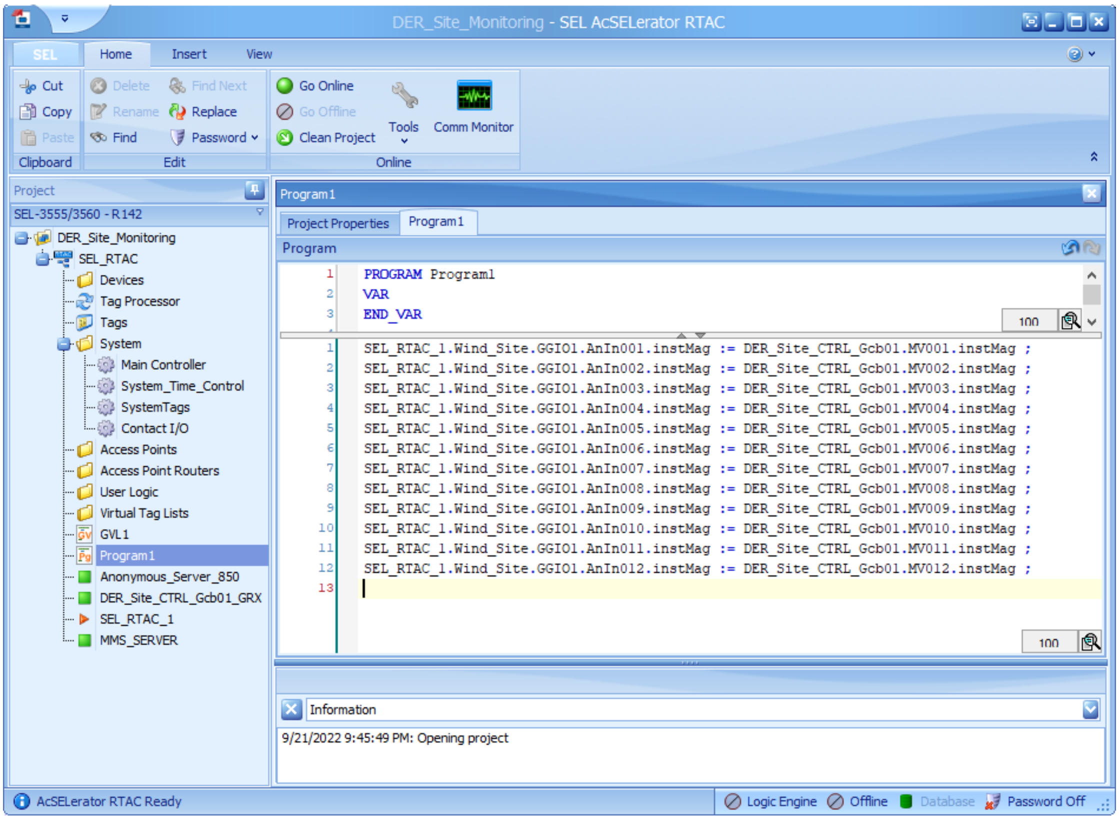
Language: CFC — Continuous Function Chart

Setting Errors

Unknown destination tag: DER_Site_Monitoring\SEL_RTAC\Tag Processor - Tag Processor

Figure 4.22: **Inserting a program for custom logic development.**

The next step is to write the algorithm that maps incoming GOOSE tags to the analog inputs’ objects of the GGIO LN of the LD “Wind_Site” of the RTAC SEL-3555 server model. The algorithm simply assigns GOOSE tags to analog inputs’ objects of the server model as described in figure 4.23 below.



```
PROGRAM Program1
VAR
END_VAR
```

```
SEL_RTAC_1.Wind_Site.GGIO1.AnIn001.instMag := DER_Site_CTRL_Gcb01.MV001.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn002.instMag := DER_Site_CTRL_Gcb01.MV002.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn003.instMag := DER_Site_CTRL_Gcb01.MV003.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn004.instMag := DER_Site_CTRL_Gcb01.MV004.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn005.instMag := DER_Site_CTRL_Gcb01.MV005.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn006.instMag := DER_Site_CTRL_Gcb01.MV006.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn007.instMag := DER_Site_CTRL_Gcb01.MV007.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn008.instMag := DER_Site_CTRL_Gcb01.MV008.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn009.instMag := DER_Site_CTRL_Gcb01.MV009.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn010.instMag := DER_Site_CTRL_Gcb01.MV010.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn011.instMag := DER_Site_CTRL_Gcb01.MV011.instMag ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn012.instMag := DER_Site_CTRL_Gcb01.MV012.instMag ;
```

```
9/21/2022 9:45:49 PM: Opening project
```

Figure 4.23: An algorithm to map GOOSE tags to RTAC SEL-3555's server model tags.

Finally, the project is saved from the 'SEL' tab in the top left corner of the window or simply use the shortcut "Ctrl+S". Instantly, it will compile the project, however, if there are no errors, then the project is ready to be sent to RTAC SEL-3555 for implementation.

The data fusion algorithm will be developed within the same IEC 61131-3 logic instant 'Program1' to achieve the purpose of data reduction before forwarding data to an MMS client. The algorithm will be described in details in the next chapter. The next section presents configurations of the second component of the EC gateway model, which is the Elipse Power communication drivers implemented on 'PC-1'.

4.3.2.2 Elipse Power communication drivers

As previously introduced in section 4.2.3, Elipse Power is an advanced SCADA application developed by Elipse Software™. The software provides implementations of IEC 61850-based communication drivers that enable MMS and XMPP communications over TCP/IP Ethernet connections. These drivers are utilized to implement the testbed of an EC gateway model. Elipse Power Studio is the application that is used to create projects and configure communications. Upon launching Elipse Power application, a window prompts with three options as displayed in figure 4.24 below.

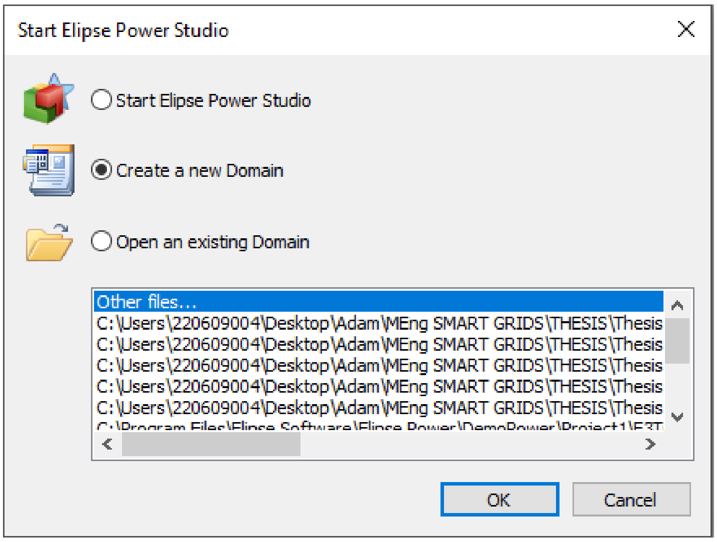
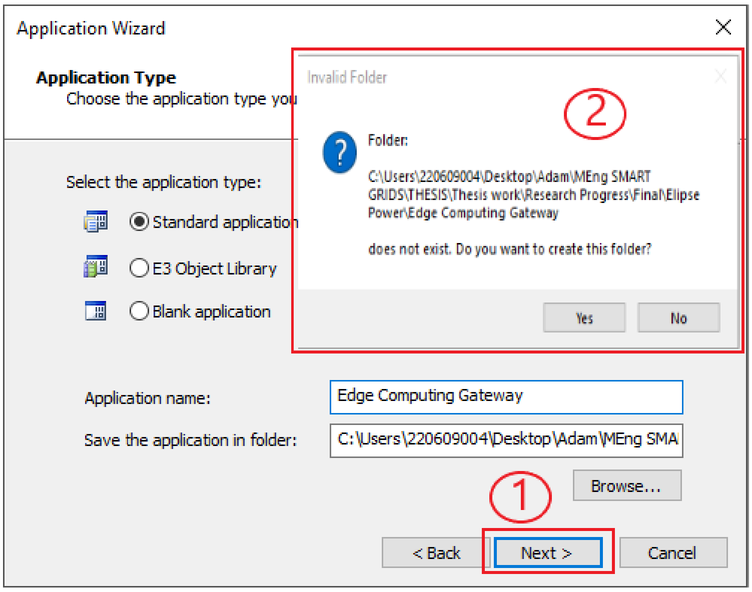


Figure 4.24: Starting Elipse Power Studio.

Selecting 'Create a new Domain' will prompt a wizard to create an Elipse Power SCADA application with all components including a database and an I/O driver. Firstly, the wizard starts with a window to configure the application's name, type, and directory folder. Then, click next and an error window will be prompted to create the directory folder as noticed in figure 4.25 below.


Invalid Folder

Folder:
C:\Users\220609004\Desktop\Adam\MEng SMART GRIDS\THESIS\Thesis work\Research Progress\Final\Elipse Power\Edge Computing Gateway

does not exist. Do you want to create this folder?

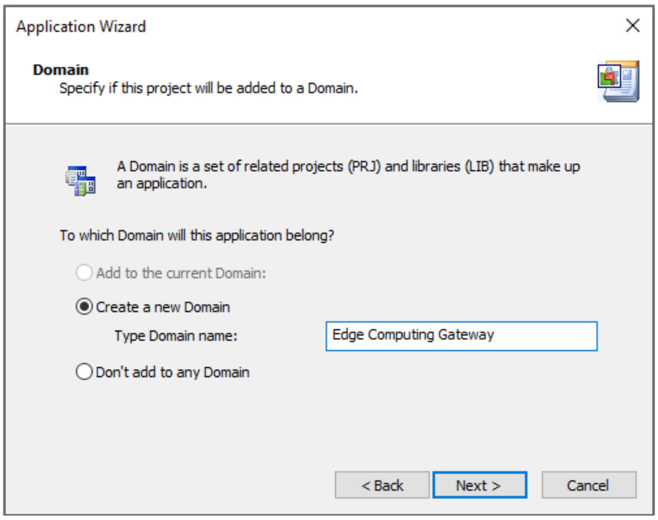
Select the application type: ● Standard application

Application name: Edge Computing Gateway

Save the application in folder: C:\Users\220609004\Desktop\Adam\MEng SMA

Figure 4.25: Configuration of the Elipse Power application.

The next step is to create a domain that would host the application. As previously introduced in section 4.2.3 above, a domain is an E3 Runtime process that executes and manages independent E3 servers and databases, which can be shared by multiple projects running within a domain. The prompted window to create the domain is depicted in figure 4.26 below.


Application Wizard

Domain
Specify if this project will be added to a Domain.

A Domain is a set of related projects (PRJ) and libraries (LIB) that make up an application.

To which Domain will this application belong?

○ Add to the current Domain:

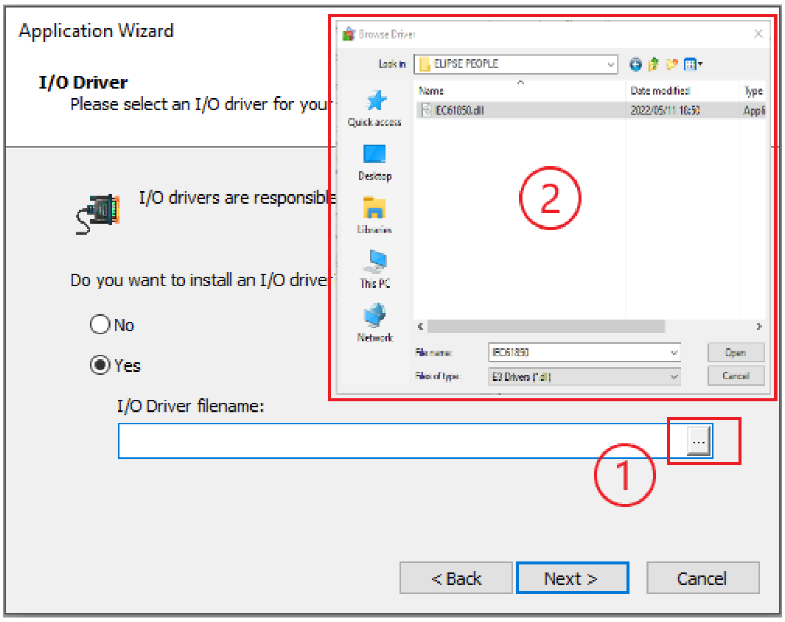
● Create a new Domain

Type Domain name: Edge Computing Gateway

○ Don't add to any Domain

Figure 4.26: Creating a domain.

Next, the wizard enables configuring an I/O driver for the application. An IEC 61850-8-1 MMS client driver is configured in this step. As previously introduced in section 4.2.3.1, the I/O drivers are implemented as DLL files that must be imported into the drivers' objects. Hence, the configuration window allows the user to browse the specified DLL file as illustrated in figure 4.27 below. Alternatively, an I/O driver can be added from the 'Organizer' windowpane on the left side of the application window after it launches as will be the case for the second IEC 61850-8-2 server driver.


Application Wizard

I/O Driver
Please select an I/O driver for you

I/O drivers are responsible

Do you want to install an I/O drive

○ No

● Yes

I/O Driver filename:

Browse Driver

Look in: ELIPSE PEOPLE

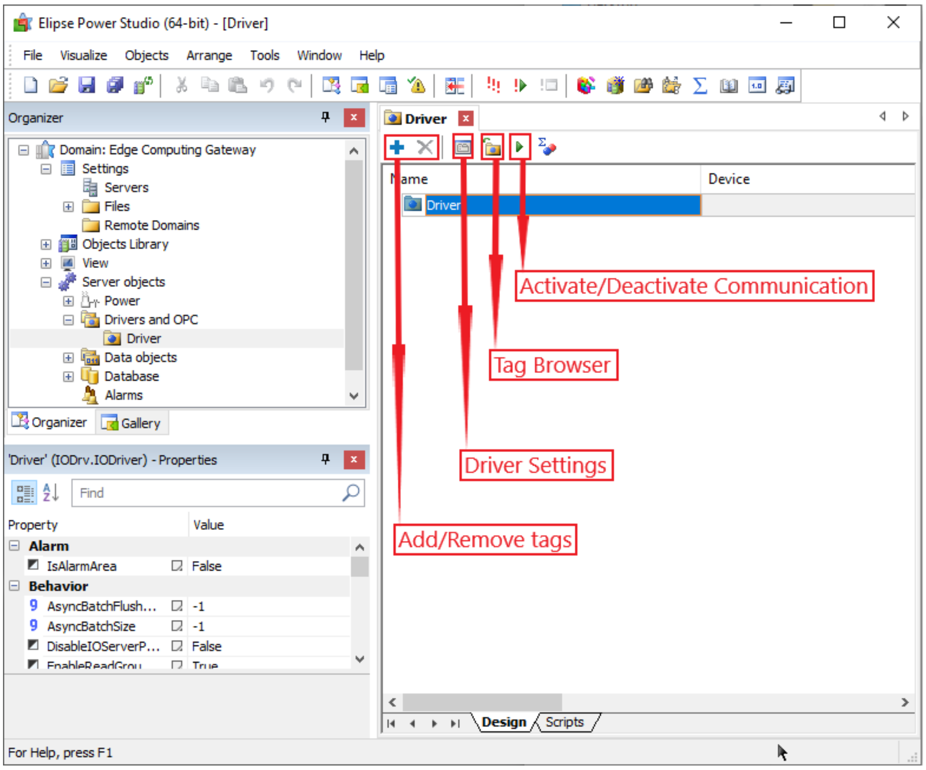
Name	Date modified	Type
IEC61850.dll	2022/05/11 16:50	Appli

File name: IEC61850

Files of type: E3 Drivers (*.dll)

Figure 4.27: Adding an IEC 61850-8-1 MMS client driver.

The final step is to create a local database for the application which will be used to store all the data and objects. Afterward, the wizard finishes, and the application gets created and launched. The next step is to configure an IEC 61850-8-1 MMS client driver to poll data from RTAC SEL-3555. To do this, firstly, double-click on the driver object under 'Drivers and OPC' in 'Organizer'. The driver opens as shown in figure 4.28 below.

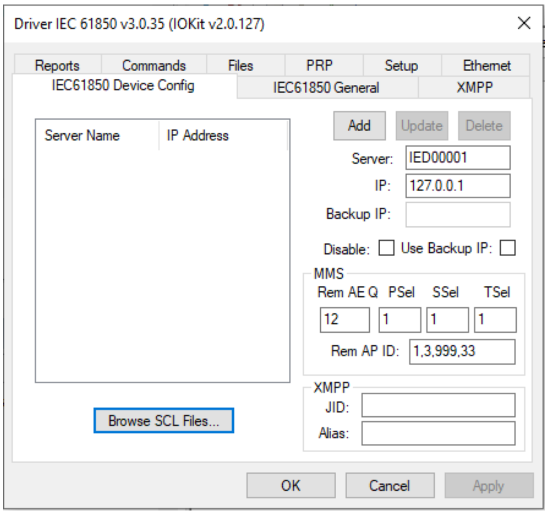


'Driver' (IODrv.IODriver) - Properties

Property	Value
Alarm	
IsAlarmArea	False
Behavior	
AsyncBatchFlush…	-1
AsyncBatchSize	-1
DisableIOServerP…	False
EnableReadGrou…	True

Figure 4.28: IEC 61850-8-1 MMS client driver window.

There are various buttons including 'Driver Settings', 'Tag Browser', 'Activate/Deactivate Communication', and two buttons for adding or removing of I/O tags, to manage and configure the driver. Clicking on 'Driver Settings' button prompts a settings window which consists of several tabs. The tab 'IEC 61850 Device Config' allows a user to configure the MMS server device by importing its SCD file using the button 'Browse SCL files', as seen in figure 4.29 below.



Server: IED00001

IP: 127.0.0.1

Backup IP:

Disable: ☐ Use Backup IP: ☐

MMS

Rem AE Q	PSel	SSel	TSel
12	1	1	1

Rem AP ID: 1,3,999,33

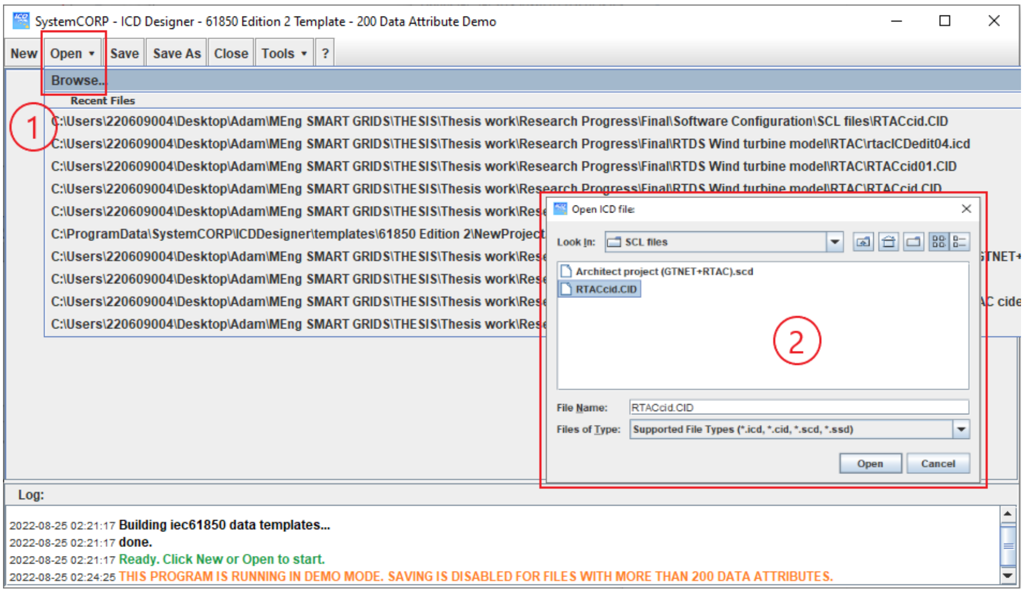
XMPP

JID:

Alias:

Figure 4.29: IEC 61850-8-1 MMS client driver settings.

After many unsuccessful attempts to establish communication, the CID file of RTAC SEL-3555 was examined as part of the troubleshooting procedures. This was done using a software known as 'ICD Designer' from SystemCORP™ which is a software that enables browsing and editing of IEC 61850 SCL files. After careful examination of the RTAC SEL-3555's CID file, several parameters were required to be modified which are described as follows. Firstly, the RTAC SEL-3555's CID file must be imported in the software, to accomplish this, click on 'Open' drop-down menu, then click on 'Browse' to select the CID file as noted in figure 4.30 below.



Look In: SCL files

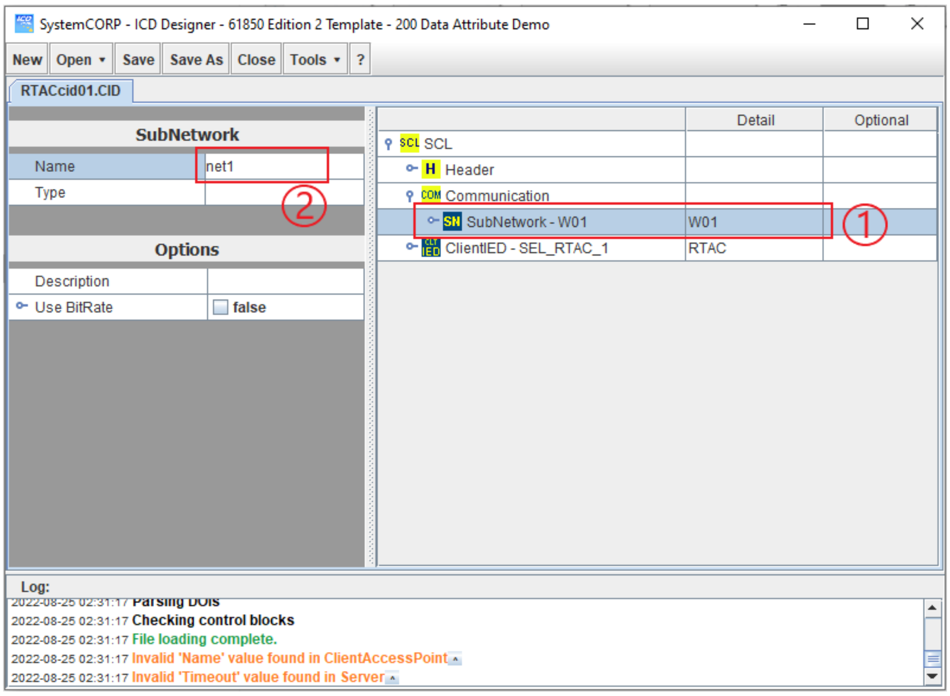
File Name: RTACcid.CID

Files of Type: Supported File Types (*.icd, *.cid, *.scd, *.ssd)

```
2022-08-25 02:21:17 Building iec61850 data templates...
2022-08-25 02:21:17 done.
2022-08-25 02:21:17 Ready. Click New or Open to start.
2022-08-25 02:24:25 THIS PROGRAM IS RUNNING IN DEMO MODE. SAVING IS DISABLED FOR FILES WITH MORE THAN 200 DATA ATTRIBUTES.
```

Figure 4.30: Importing RTAC SEL-3555's CID file into ICD Designer.

The first parameter to be modified is the subnetwork name, and it was changed from 'W01' to 'net1' as displayed in figure 4.31 below. The 'net1' is the subnetwork name which was defined for GTNET soft IED, thus, the RTAC SEL-3555 must be assigned to the same subnetwork.



SubNetwork	
Name	net1
Type	

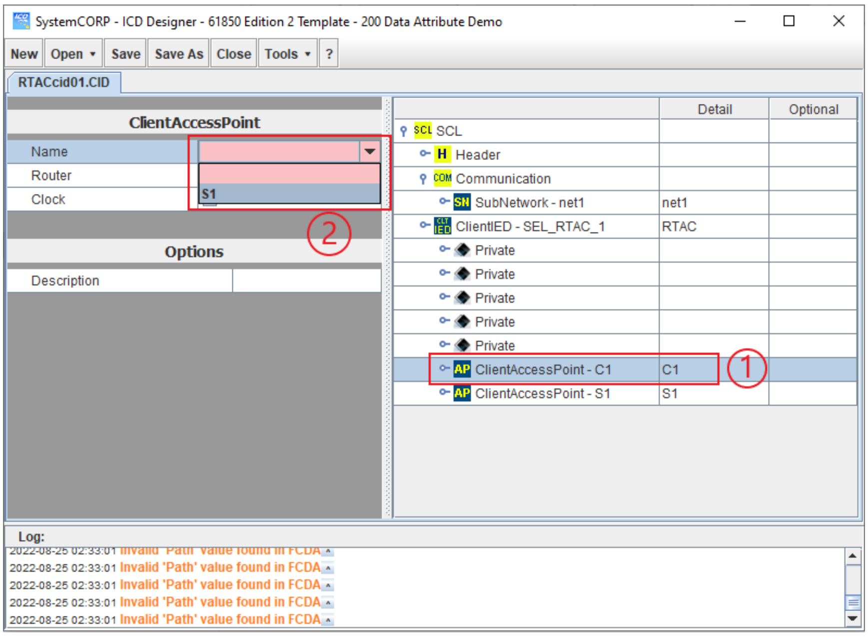
Options	
Description	
Use BitRate	☐ false

	Detail	Optional
SCL SCL		
H Header		
COM Communication		
SN SubNetwork - W01	W01	
ClientIED - SEL_RTAC_1	RTAC	

```
2022-08-25 02:31:17 Parsing DOIs
2022-08-25 02:31:17 Checking control blocks
2022-08-25 02:31:17 File loading complete.
2022-08-25 02:31:17 Invalid 'Name' value found in ClientAccessPoint
2022-08-25 02:31:17 Invalid 'Timeout' value found in Server
```

Figure 4.31: Modifying the subnetwork name.

Next parameter is ‘ClientAccessPoint’, it was found to indicate ‘C1’ in the parameter’s windowpane on the right, but in ‘ClientAccessPoint’ windowpane to the left it was empty and highlighted in red color which indicated an error. Hence, it was set to ‘S1’ as it is the defined access point in the drop-down menu as described in figure 4.32 below.



Name:

Router:

Clock:

S1

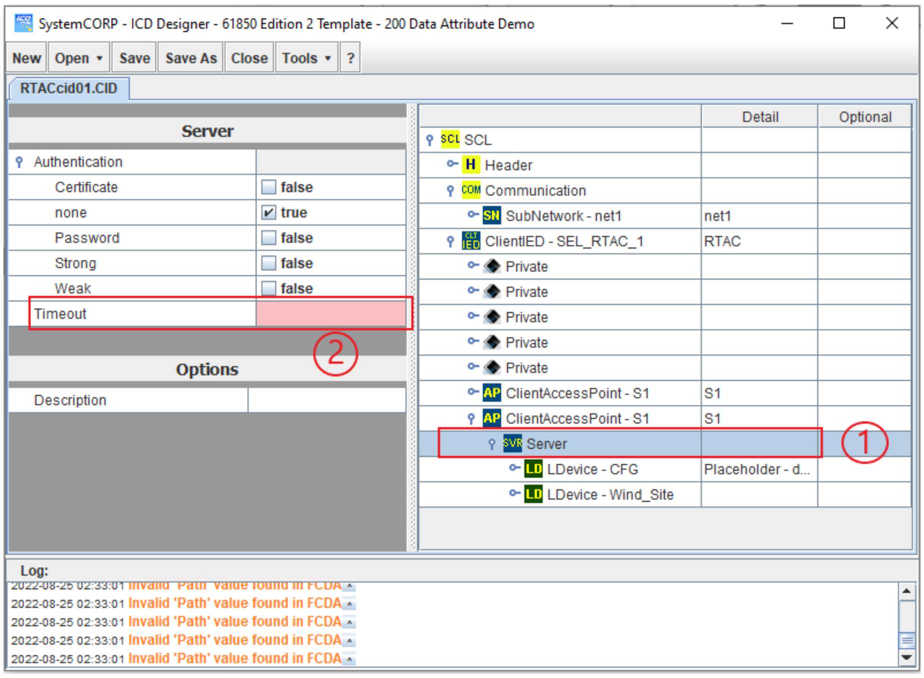
Description:

	Detail	Optional
SCL SCL		
H Header		
COM Communication		
SN SubNetwork - net1	net1	
IED ClientIED - SEL_RTAC_1	RTAC	
Private		
Private		
Private		
Private		
Private		
AP ClientAccessPoint - C1	C1	
AP ClientAccessPoint - S1	S1	

```
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
```

Figure 4.32: Assigning client access point ‘S1’.

The next parameter is the ‘Timeout’ interval of the server model, it was found to be empty with a red colour indication as noticed in figure 4.33 below. It was set to 5 seconds, and the same value was configured in the IEC 61850-8-1 MMS client driver in Elipse Power as will be shown later in the driver configuration.



Authentication

Certificate: ☐ false

none: ☑ true

Password: ☐ false

Strong: ☐ false

Weak: ☐ false

Timeout:

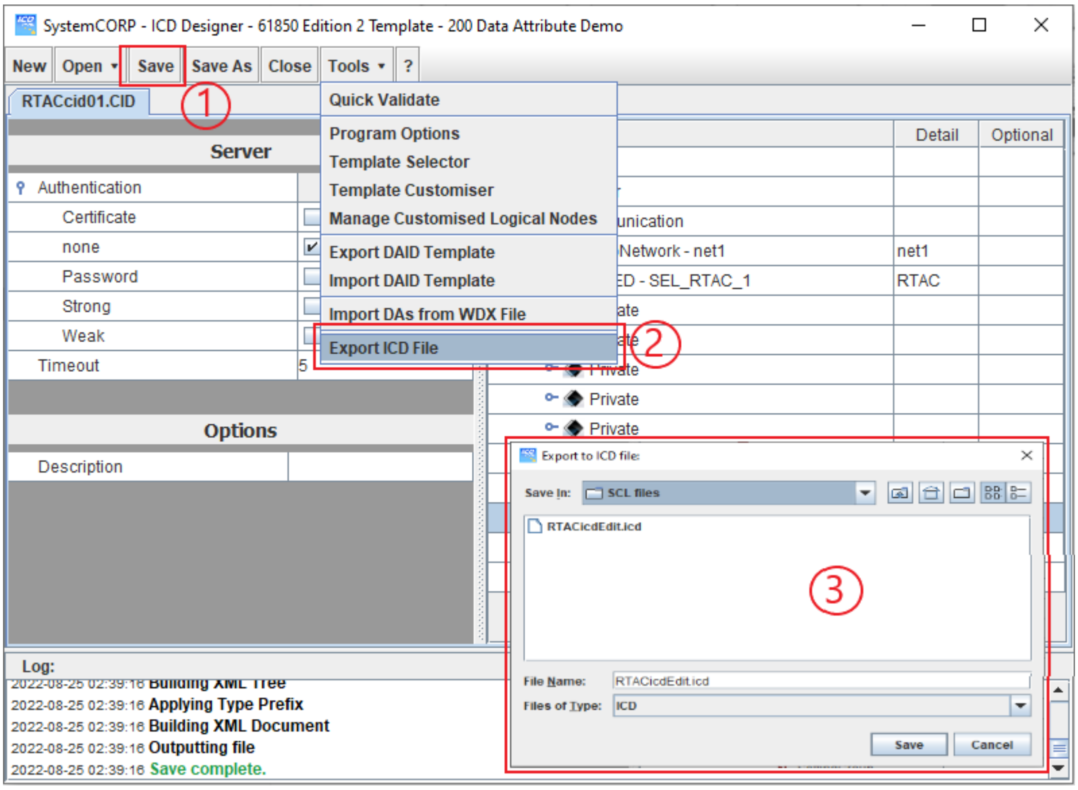
Description:

	Detail	Optional
SCL SCL		
H Header		
COM Communication		
SN SubNetwork - net1	net1	
IED ClientIED - SEL_RTAC_1	RTAC	
Private		
Private		
Private		
Private		
Private		
AP ClientAccessPoint - S1	S1	
AP ClientAccessPoint - S1	S1	
SVR Server		
LD LDevice - CFG	Placeholder - d...	
LD LDevice - Wind_Site		

```
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
2022-08-25 02:33:01 Invalid 'Path' value found in FCDA
```

Figure 4.33: Server model ‘Timeout’ value.

Finally, the configuration was saved and exported as an ICD file as depicted in figure 4.34 below.



Timeout: 5

Network - net1: net1

ED - SEL_RTAC_1: RTAC

Save In: SCL files

RTACicdEdit.icd

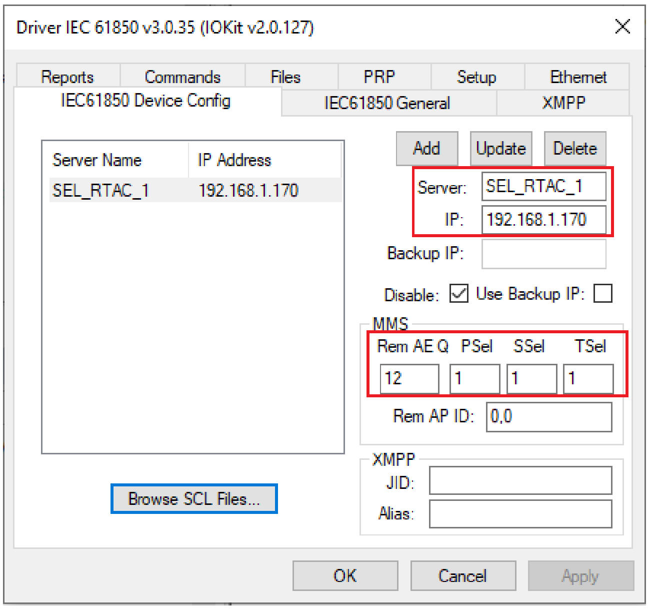
File Name: RTACicdEdit.icd

Files of Type: ICD

```
2022-08-25 02:39:16 Building XML Tree
2022-08-25 02:39:16 Applying Type Prefix
2022-08-25 02:39:16 Building XML Document
2022-08-25 02:39:16 Outputting file
2022-08-25 02:39:16 Save complete.
```

Figure 4.34: Exporting RTAC SEL-3555's ICD file.

Now, the ICD file can be imported in the driver, whereby the IED name, IP address, and MMS communication parameters will be automatically extracted from the ICD file in the designated fields as illustrated in figure 4.35 below.



Server Name	IP Address
SEL_RTAC_1	192.168.1.170

Server: SEL_RTAC_1

IP: 192.168.1.170

Backup IP:

Disable: ☑ Use Backup IP: ☐

MMS

Rem AE Q	PSel	SSel	TSel
12	1	1	1

Rem AP ID: 0,0

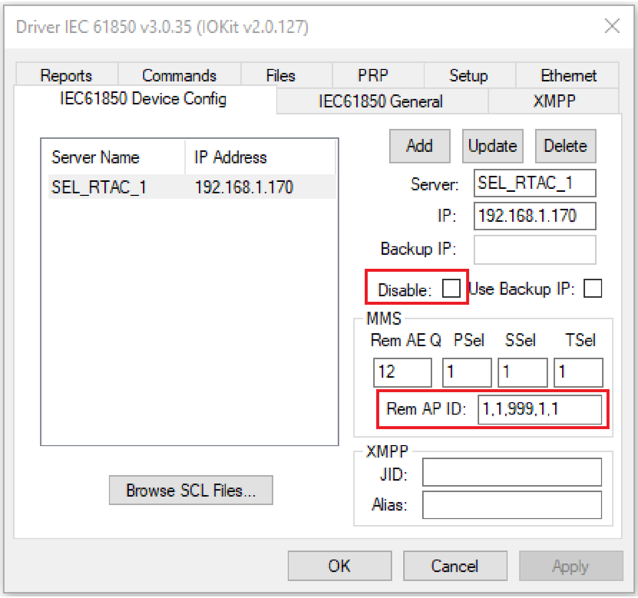
XMPP

JID:

Alias:

Figure 4.35: IEC 61850-8-1 MMS client driver after importing RTAC SEL-3555's ICD file.

The next step is to enable the server device by unticking ‘Disable’ checkbox and adding an ‘Rem AP ID’ which should be the same as the ‘Local App ID’ which is ”.1.999.1.1” as shown in figure 4.36 below.



Server Name	IP Address
SEL_RTAC_1	192.168.1.170

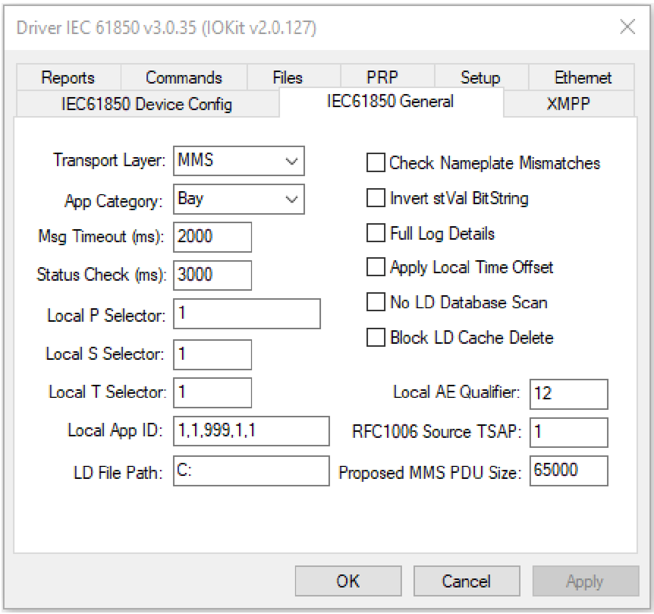
Server: SEL_RTAC_1
IP: 192.168.1.170
Backup IP:
Disable: ☐ Use Backup IP: ☐

Rem AE Q	PSel	SSel	TSel
12	1	1	1

Rem AP ID: 1,1,999,1,1
JID:
Alias:

Figure 4.36: Configuration of the server device parameters.

The tab ‘IEC 61850 General’ contains the settings for the transport layer, it was configured as seen in figure 4.37 below. Only the message timeout ‘Msg Timeout’ and ‘Status Check’ parameters were modified with two and three seconds respectively. Note that, the transport layer protocol is set to MMS and the ‘Local App ID’ value is the same that was used for the ‘Rem AP ID’ for the MMS server in the abovementioned tab which is noted in figure 4.36.



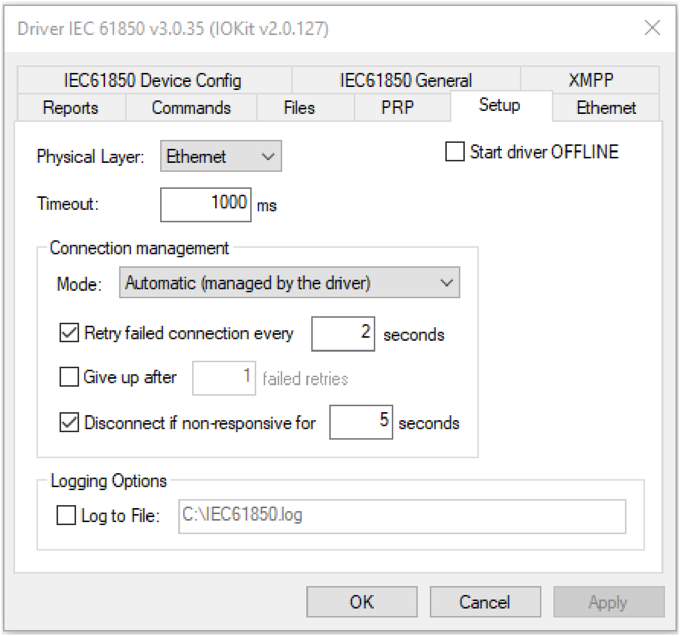
Transport Layer: MMS
App Category: Bay
Msg Timeout (ms): 2000
Status Check (ms): 3000
Local P Selector: 1
Local S Selector: 1
Local T Selector: 1
Local App ID: 1,1,999,1,1
LD File Path: C:

☐ Check Nameplate Mismatches
☐ Invert stVal BitString
☐ Full Log Details
☐ Apply Local Time Offset
☐ No LD Database Scan
☐ Block LD Cache Delete

Local AE Qualifier: 12
RFC1006 Source TSAP: 1
Proposed MMS PDU Size: 65000

Figure 4.37: IEC 61850-8-1 MMS client driver transport layer configuration.

The next tab to modify is the ‘Setup’ tab which contains the physical layer settings, it was designed as displayed in figure 4.38 below. The physical layer protocal is set to ‘Ethernet’ and the time parameters are set as described in the figure below. Note that, the ‘Disconnect if not responsive’ parameter is configured to five seconds matching the timeout interval which was preset in RTAC SEL-3555’s server model.



Driver IEC 61850 v3.0.35 (IOKit v2.0.127)

Physical Layer: Ethernet

☐ Start driver OFFLINE

Timeout: 1000 ms

Connection management

Mode: Automatic (managed by the driver)

☑ Retry failed connection every 2 seconds

☐ Give up after 1 failed retries

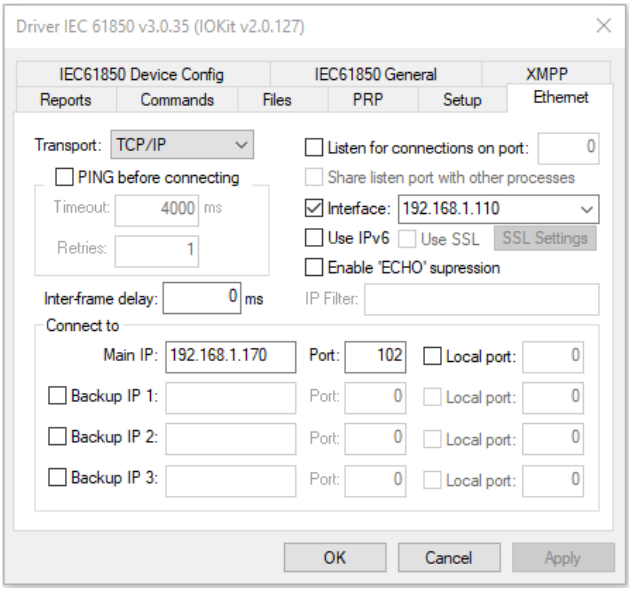
☑ Disconnect if non-responsive for 5 seconds

Logging Options

☐ Log to File: C:\IEC61850.log

Figure 4.38: **IEC 61850-8-1 MMS client driver physical layer configuration.**

Next is ‘Ethernet’ tab which contains the link layer settings, it was desinged as noticed in figure 4.39 below. The TCP is set as ‘Transport’ layer protocol and the driver is configured to connect to RTAC SEL-3555 unit with the IP address ‘192.168.1.170’ and connection port set to ‘102’.



Driver IEC 61850 v3.0.35 (IOKit v2.0.127)

Transport: TCP/IP

☐ PING before connecting

Timeout: 4000 ms

Retries: 1

Inter-frame delay: 0 ms

☐ Listen for connections on port: 0

☐ Share listen port with other processes

☑ Interface: 192.168.1.110

☐ Use IPv6 ☐ Use SSL

☐ Enable 'ECHO' supression

IP Filter:

Connect to

Main IP: 192.168.1.170 Port: 102 ☐ Local port: 0

☐ Backup IP 1: Port: 0 ☐ Local port: 0

☐ Backup IP 2: Port: 0 ☐ Local port: 0

☐ Backup IP 3: Port: 0 ☐ Local port: 0

Figure 4.39: **IEC 61850-8-1 MMS client driver link layer configuration.**

All the other tabs are left unchanged, once the configuration is complete, the ‘Tag Browser’ window is prompted as depicted in figure 4.40 below. It enables browsing the RTAC SEL-3555’s server model which is imported in ICD file, in an ‘Offline’ mode before any connection is established. The DOs belonging to the ‘GGIO’ LN under the FC “Measurement” (MX), are imported to the driver application by drag and drop to the windowpane on the left. These are DOs of RTAC SEL-3555 server model which hold GTNET‘s GOOSE values.

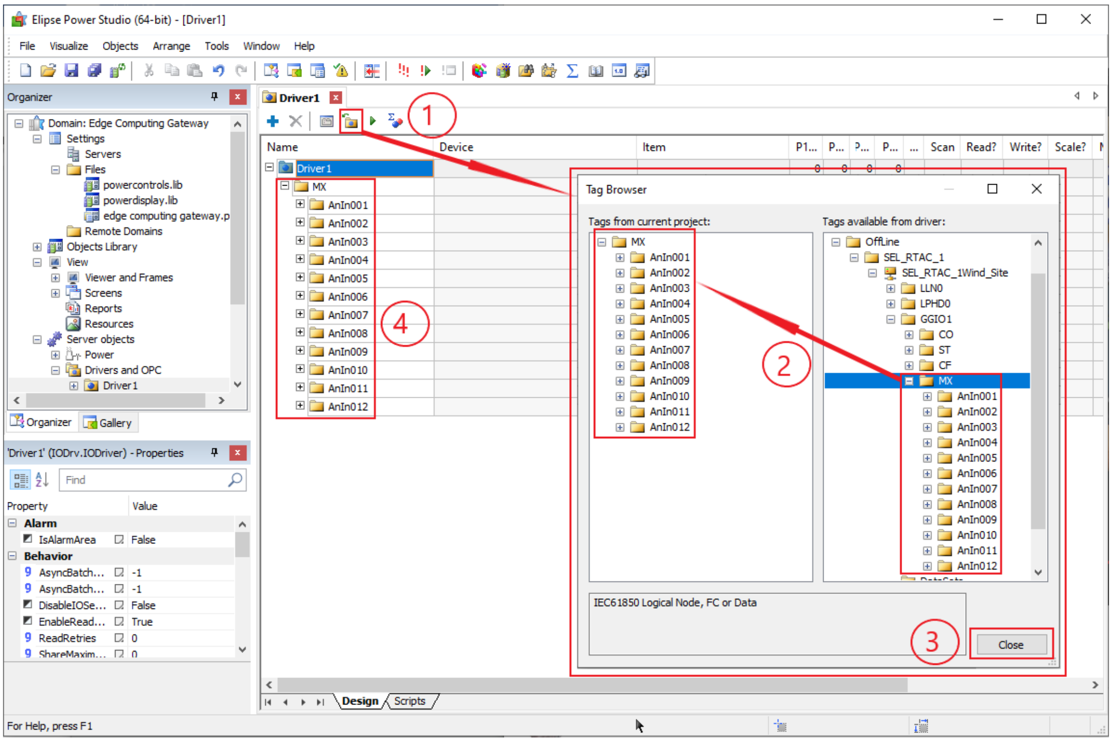
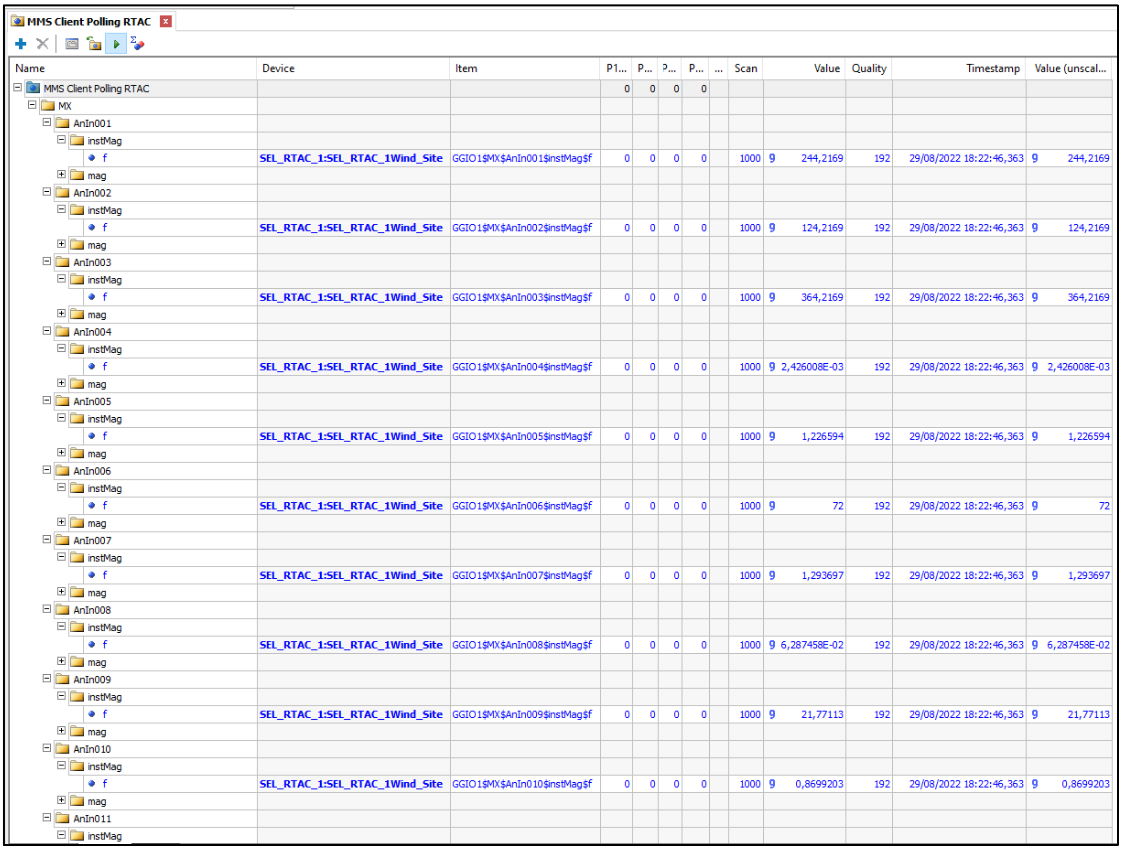


Figure 4.40: **The tag browser tool of the IEC 61850-8-1 MMS client driver.**

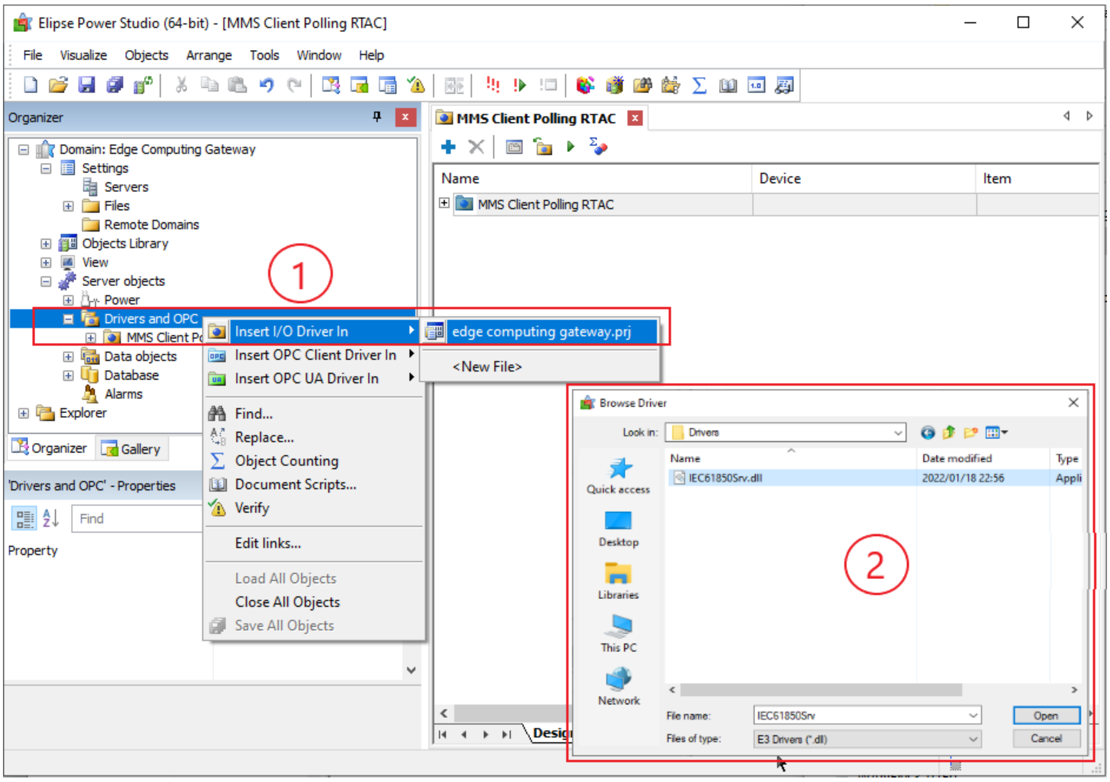
After closing ‘Tag Browser’, the imported tags appear on the application window of the driver. Now, the driver can be activated to establish MMS client/server communication with RTAC SEL-3555, polling the twelve data tags and assigning a timestamp to each point as illustrated in figure 4.41 below. Optionally, the driver object can be renamed with a unique name to distinguish it from other drivers if necessary.



Name	Device	Item	P1...	P...	P...	P...	...	Scan	Value	Quality	Timestamp	Value (unscal...
MMS Client Polling RTAC			0	0	0	0						
MX												
AnIn001												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn001$instMag$f	0	0	0	0		1000	9 244,2169	192	29/08/2022 18:22:46,363	9 244,2169
mag												
AnIn002												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn002$instMag$f	0	0	0	0		1000	9 124,2169	192	29/08/2022 18:22:46,363	9 124,2169
mag												
AnIn003												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn003$instMag$f	0	0	0	0		1000	9 364,2169	192	29/08/2022 18:22:46,363	9 364,2169
mag												
AnIn004												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn004$instMag$f	0	0	0	0		1000	9 2,426008E-03	192	29/08/2022 18:22:46,363	9 2,426008E-03
mag												
AnIn005												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn005$instMag$f	0	0	0	0		1000	9 1,226594	192	29/08/2022 18:22:46,363	9 1,226594
mag												
AnIn006												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn006$instMag$f	0	0	0	0		1000	9 72	192	29/08/2022 18:22:46,363	9 72
mag												
AnIn007												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn007$instMag$f	0	0	0	0		1000	9 1,293697	192	29/08/2022 18:22:46,363	9 1,293697
mag												
AnIn008												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn008$instMag$f	0	0	0	0		1000	9 6,287458E-02	192	29/08/2022 18:22:46,363	9 6,287458E-02
mag												
AnIn009												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn009$instMag$f	0	0	0	0		1000	9 21,77113	192	29/08/2022 18:22:46,363	9 21,77113
mag												
AnIn010												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn010$instMag$f	0	0	0	0		1000	9 0,8699203	192	29/08/2022 18:22:46,363	9 0,8699203
mag												
AnIn011												
instMag												

Figure 4.41: IEC 61850-8-1 MMS client driver activated.

The next step is to achieve the local area to WANs integration, which is a basic function of the communication gateway. To do this, an IEC 61850-8-2 server driver ‘Driver 2’ in the gateway model as shown in figure 4.14 above, is configured to enable communications with an IEC 61850-8-2 client driver on the remote machine ‘PC-3’ over a WAN utilizing XMPP as the transport layer protocol. The first step is to add the server driver to Elipse Power by importing the DLL file named ‘IEC61850Srv’ as seen in figure 4.42 below.



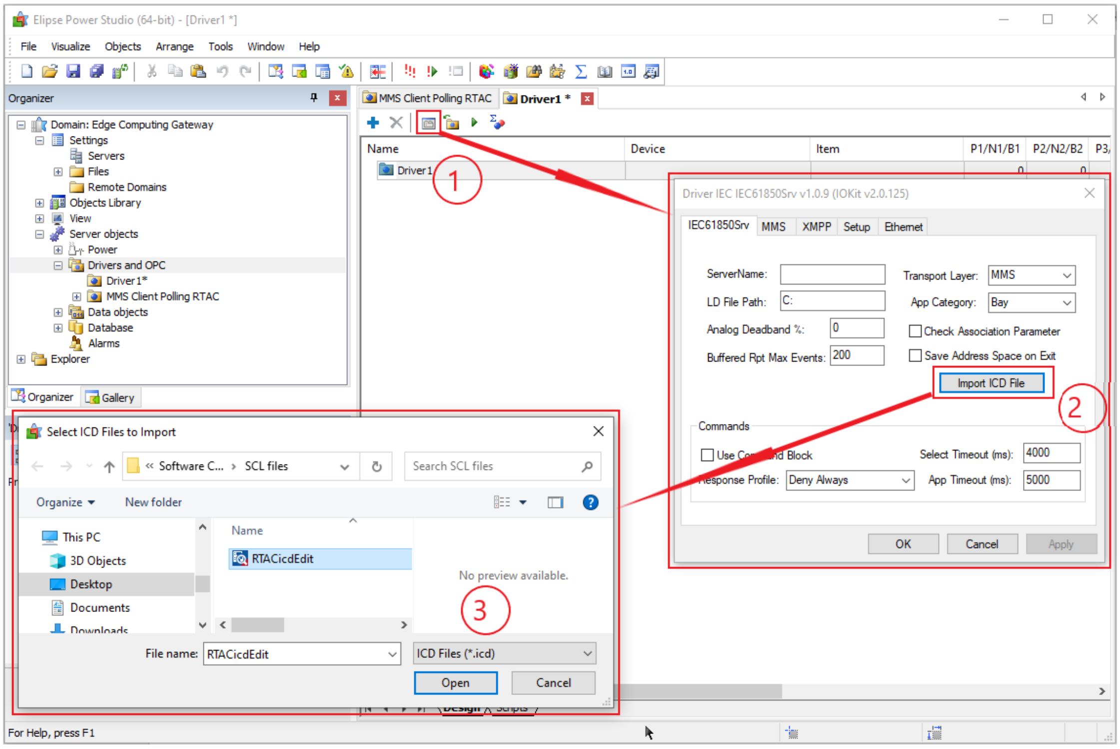
Look in: Drivers

File name: IEC61850Srv

Files of type: E3 Drivers (*.dll)

Figure 4.42: Adding the IEC 61850-8-2 server driver.

Similar to the client driver configuration, the RTAC SEL-3555's ICD file is imported into the server driver object as noted in figure 4.43 below. This will enable the driver application to browse the RTAC SEL-3555 information model.



Transport Layer: MMS

LD File Path: C:

App Category: Bay

Analog Deadband %: 0

☐ Check Association Parameter

Buffered Rpt Max Events: 200

☐ Save Address Space on Exit

☐ Use Command Block

Select Timeout (ms): 4000

Response Profile: Deny Always

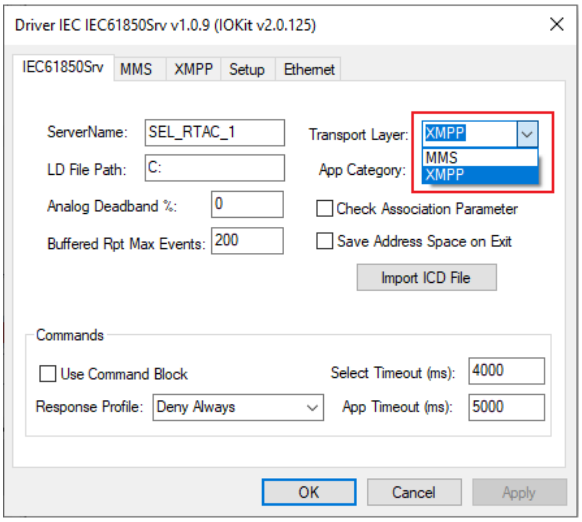
App Timeout (ms): 5000

File name: RTACicdEdit

ICD Files (*.icd)

Figure 4.43: Importing RTAC SEL-3555's ICD file into IEC 61850-8-2 server driver.

The next step is to set the transport layer protocol to XMPP as displayed in figure 4.44 below, to enable the driver to communicate via XMPP according to the IEC 61850-8-2 standard.



Driver IEC IEC61850Srv v1.0.9 (IOKit v2.0.125)

ServerName: SEL_RTAC_1

LD File Path: C:

Analog Deadband %: 0

Buffered Rpt Max Events: 200

Transport Layer: XMPP

App Category:

☐ Check Association Parameter

☐ Save Address Space on Exit

Commands

☐ Use Command Block

Response Profile: Deny Always

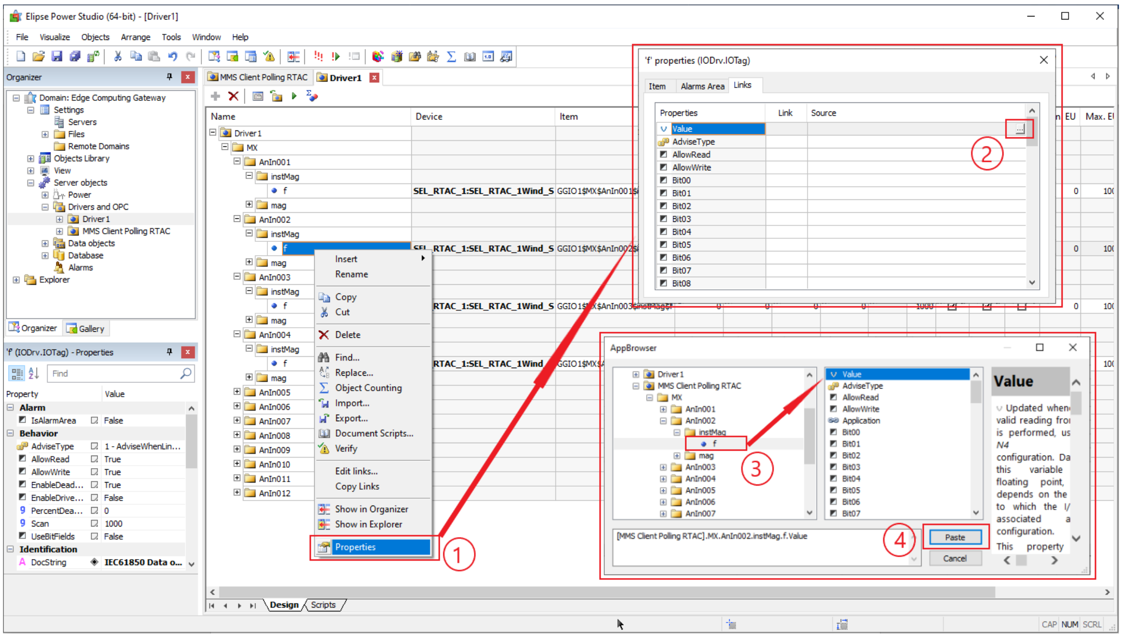
Select Timeout (ms): 4000

App Timeout (ms): 5000

Figure 4.44: **Setting XMPP as the transport layer protocol.**

Now, the RTAC SEL-3555 information model can be browsed to import data tags into the driver using the ‘Tag Browser’ tool as previously demonstrated in figure 4.40 above for the MMS client driver.

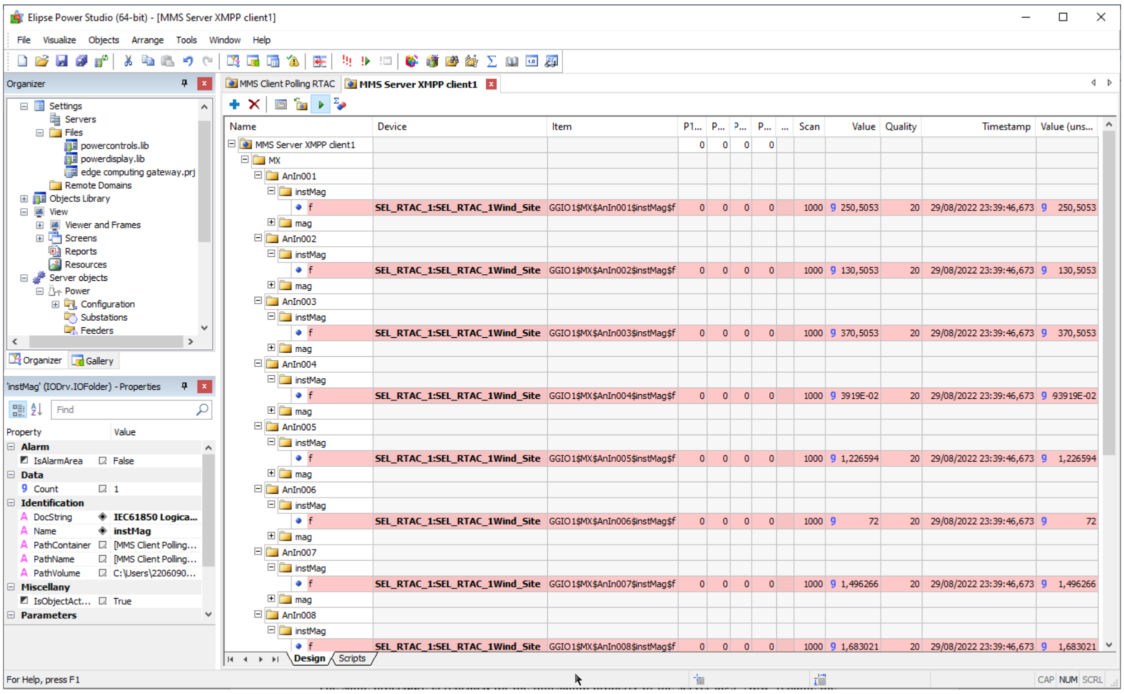
The next step is to link IEC 61850-8-2 XMPP server driver ’Driver1’ tags to the IEC 61850-8-1 MMS client driver tags, consequently, values and timestamps of ’Driver1’ tags would be updated in synchronization with the IEC 61850-8-1 MMS client tags. Elipse Power enables linking data tags within a single or between different projects within the same domain. To achieve this, right-click on the data tag of ’Driver1’ and navigate to ‘Properties’. Go to tab ‘Links’, highlight the first property ‘Value’ and click the button under ‘Source’ column to browse for ‘Value’ of the source tag which belongs to the MMS client driver tag as described in figure 4.45 below.



[MMS Client Polling RTAC].MX.AnIn002.instMag.f.Value

Figure 4.45: Linking values of the IEC 61850-8-2 XMPP server driver objects to the IEC 61850-8-1 MMS client driver objects.

The same procedure is repeated to link the 'Timestamp' property of 'Driver1' tags to those of the MMS client tags, as noticed in figure A.1 in the appendix. Now, rename the driver and activate it to verify that, the linking configuration is successfully working as shown in figure 4.46 below. Note that, both drivers 'MMS Client Polling RTAC' and 'MMS Server XMPP client1' must be running simultaneously for the link to work.



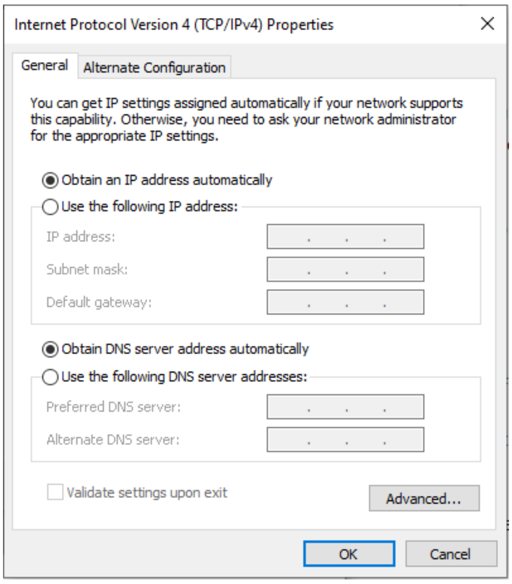
Name	Device	Item	P1...	P...	P...	P...	...	Scan	Value	Quality	Timestamp	Value (uns...
MMS Server XMPP client1			0	0	0	0						
MX												
AnIn001												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn001$instMag$f	0	0	0	0		1000	250,5053	20	29/08/2022 23:39:46,673	250,5053
mag												
AnIn002												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn002$instMag$f	0	0	0	0		1000	130,5053	20	29/08/2022 23:39:46,673	130,5053
mag												
AnIn003												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn003$instMag$f	0	0	0	0		1000	370,5053	20	29/08/2022 23:39:46,673	370,5053
mag												
AnIn004												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn004$instMag$f	0	0	0	0		1000	3919E-02	20	29/08/2022 23:39:46,673	93919E-02
mag												
AnIn005												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn005$instMag$f	0	0	0	0		1000	1,226594	20	29/08/2022 23:39:46,673	1,226594
mag												
AnIn006												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn006$instMag$f	0	0	0	0		1000	72	20	29/08/2022 23:39:46,673	72
mag												
AnIn007												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn007$instMag$f	0	0	0	0		1000	1,496266	20	29/08/2022 23:39:46,673	1,496266
mag												
AnIn008												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn008$instMag$f	0	0	0	0		1000	1,683021	20	29/08/2022 23:39:46,673	1,683021

Figure 4.46: IEC 61850-8-2 Server driver renamed and activated.

The following section describes the configuration of XMPP communications over a public IP-based WAN.

4.3.3 XMPP communications over wide area network

The CPUT Internet-based WAN was utilized for the testbed and all three PC machines were connected to it via an Ethernet switch. The Ethernet adapters of all three PCs are set to automatically obtain IP and Domain Name Space (DNS) server addresses as depicted in figure 4.47 below.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

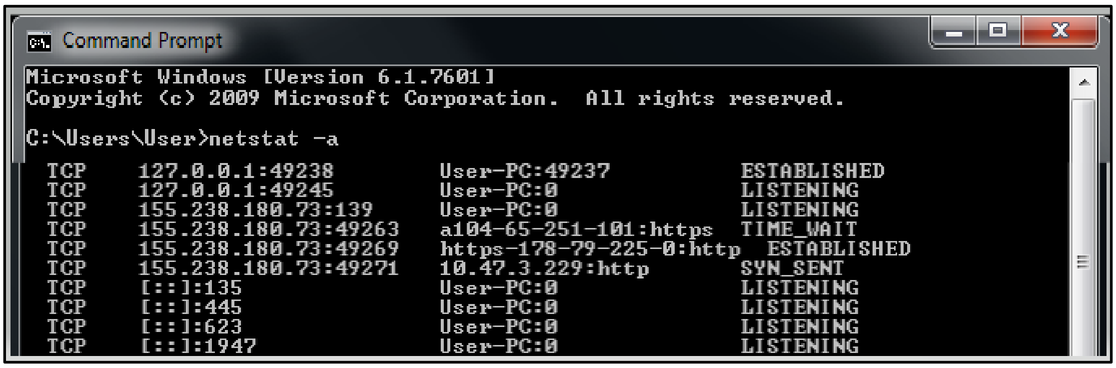
● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

Figure 4.47: **Network adapter settings of PCs for Internet service access.**

The network server uses Dynamic Host Configuration Protocol (DHCP) to automatically assign IP addresses to connected devices. The DHCP server assigns other network configurations to connected devices including the DNS server address to enable these devices to access the Internet. The DNS is an Internet service that converts domain names to IP addresses. This is the case for all three machines, whereby they are dynamically assigned different IP addresses. Using the network status command ’netstat –a’ on the ‘Command Prompt’ terminal, all network configurations of a device can be displayed including active IP addresses and local ports. The terminal of ‘PC-2' which host the XMPP server application is illustrated in figure 4.48 below.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>netstat -a

  TCP    127.0.0.1:49238        User-PC:49237          ESTABLISHED
  TCP    127.0.0.1:49245        User-PC:0              LISTENING
  TCP    155.238.180.73:139     User-PC:0              LISTENING
  TCP    155.238.180.73:49263   a104-65-251-101:https  TIME_WAIT
  TCP    155.238.180.73:49269   https-178-79-225-0:http  ESTABLISHED
  TCP    155.238.180.73:49271   10.47.3.229:http       SYN_SENT
  TCP    [::]:135               User-PC:0              LISTENING
  TCP    [::]:445               User-PC:0              LISTENING
  TCP    [::]:623               User-PC:0              LISTENING
  TCP    [::]:1947              User-PC:0              LISTENING
```

Figure 4.48: **Active network status on ‘PC-2’.**

The XMPP communication architecture is similar to the email service architecture, whereby clients register and connect to a server within their domain to exchange XML stanzas over a WAN (Veichtlbauer et al., 2016; Aftab et al., 2018). The responsibilities of an XMPP server include managing connections, saving, and routing messages between clients. The XMPP clients/servers are identified using a unique address named the JID. In the testbed, an Openfire XMPP server application is utilized which is a Real-Time Collaboration (RTC) server developed by Ignite Realtime™ (Ignite Realtime, 2022). The XMPP clients are Elipse Power IEC 61850-8-2 client/server drivers exchanging information according to IEC 61850-8-2 XMPP. In figure 4.49 below, it shows the clients and an Openfire XMPP server application in the testbed.

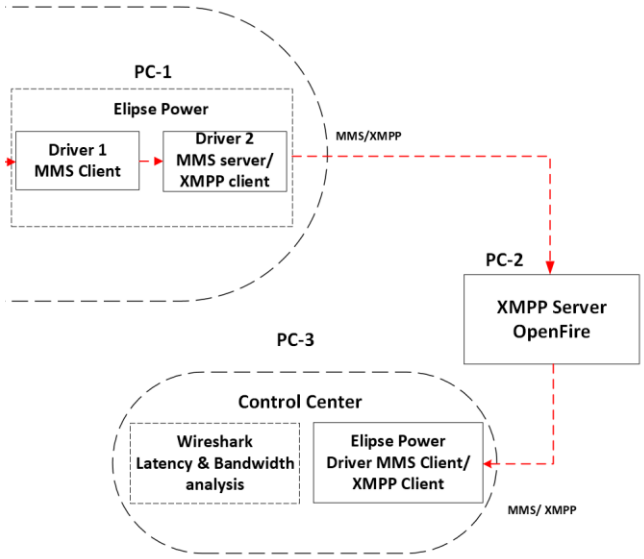
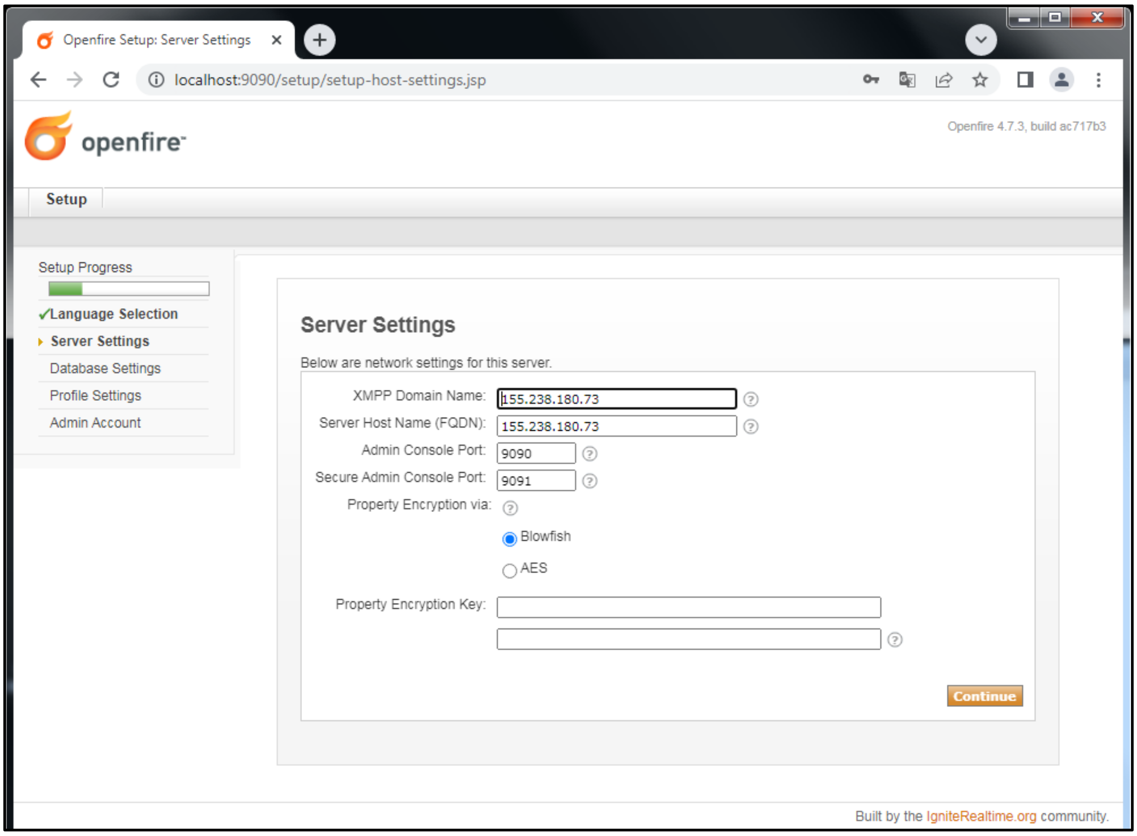


Figure 4.49: **IEC 61850-8-2 XMPP WAN communications components.**

The Openfire server software package is installed on ‘PC-2’ and executed on the local server of the machine “localhost”. Openfire can be accessed via an Internet browser on local ports ‘9090’ or ‘9091’ which are designated for an administrative consol. The server setup and registration of clients ‘Users’ are completed as described in the following steps. After selecting the language, the server settings window is prompted where the XMPP domain and the server host names are set to the IP address of the host PC. Additionally, the encryption technique, and the ‘Administrator Console’ ports can be modified as seen in figure 4.50 below.



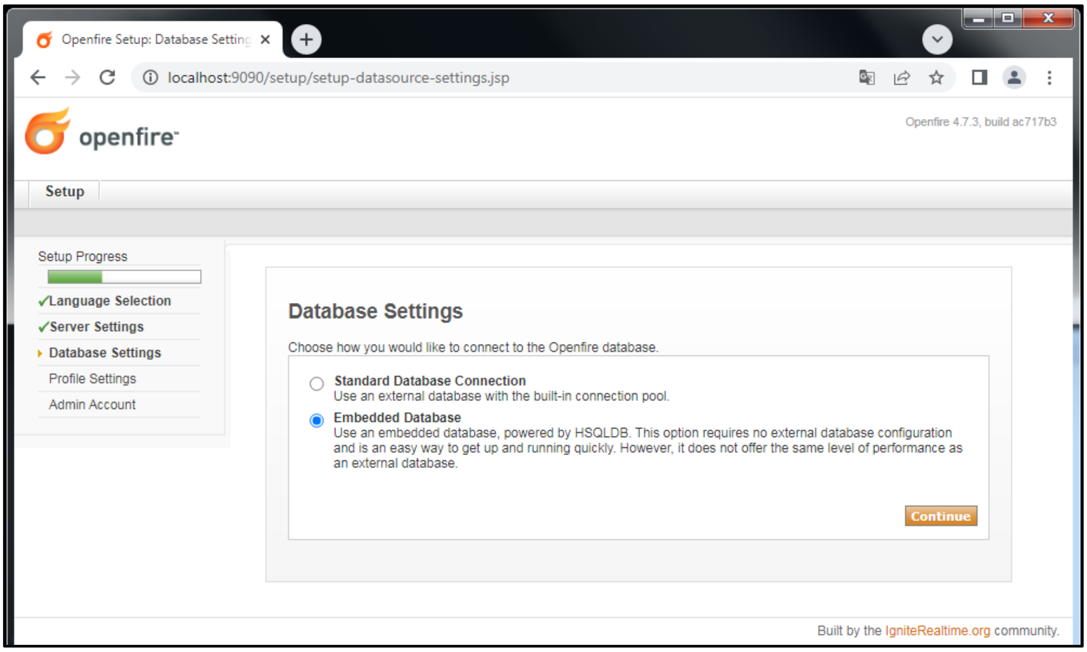
Server Settings

Below are network settings for this server.

XMPP Domain Name: 155.238.180.73
Server Host Name (FQDN): 155.238.180.73
Admin Console Port: 9090
Secure Admin Console Port: 9091
Property Encryption via:
● Blowfish
○ AES
Property Encryption Key:

Figure 4.50: The Openfire XMPP server setup.

The next step is to configure the database settings whereby an embedded database is selected as displayed in figure 4.51 below. This setting is suitable for simple applications whereby a small size embedded database is sufficient to handle the application.



Database Settings

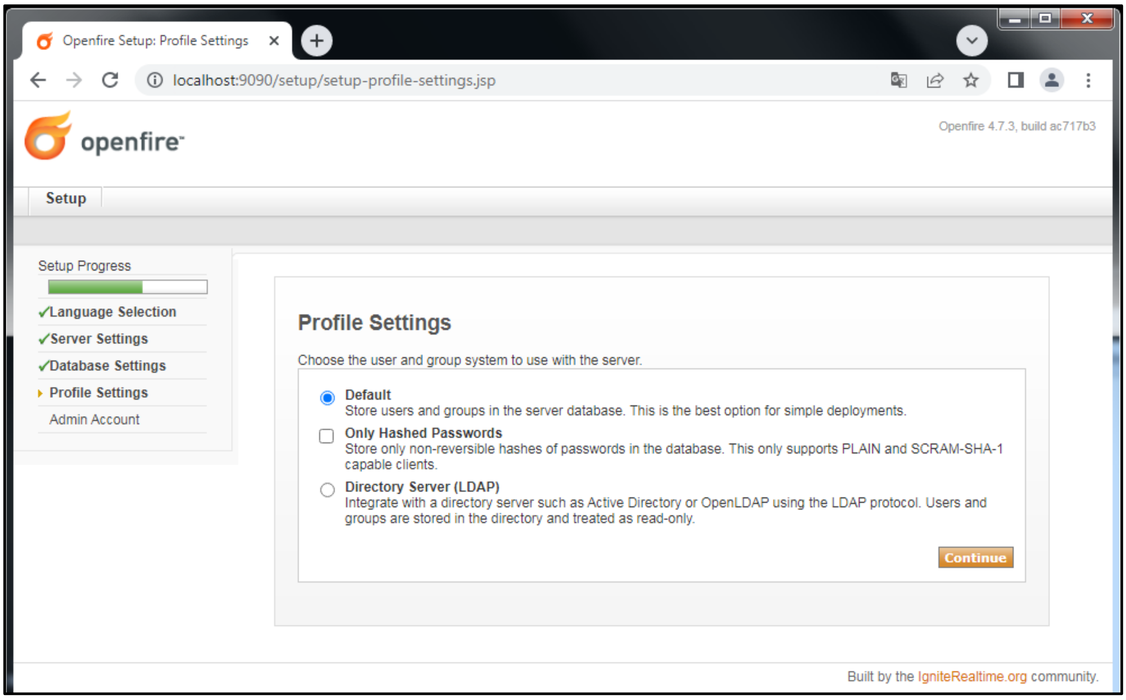
Choose how you would like to connect to the Openfire database.

○ **Standard Database Connection**
Use an external database with the built-in connection pool.

● **Embedded Database**
Use an embedded database, powered by HSQLDB. This option requires no external database configuration and is an easy way to get up and running quickly. However, it does not offer the same level of performance as an external database.

Figure 4.51: Openfire database settings.

The ‘Profile Settings’ which set the mode for data storage, was maintained to ‘Default’ mode which enables storage of data in the embedded database as described in figure 4.52 below.



Profile Settings

Choose the user and group system to use with the server.

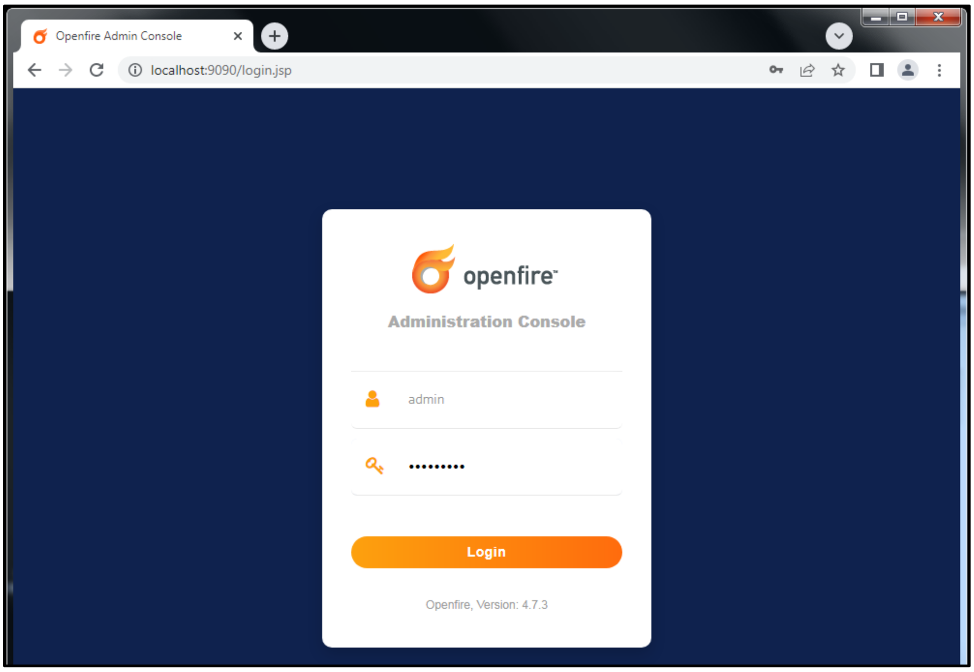
● **Default**
Store users and groups in the server database. This is the best option for simple deployments.

☐ **Only Hashed Passwords**
Store only non-reversible hashes of passwords in the database. This only supports PLAIN and SCRAM-SHA-1 capable clients.

○ **Directory Server (LDAP)**
Integrate with a directory server such as Active Directory or OpenLDAP using the LDAP protocol. Users and groups are stored in the directory and treated as read-only.

Figure 4.52: Openfire profile settings.

The last step is to create an administrator account for the server and use it to login into the server ‘Administration Console’ as noticed in figure 4.53 below.

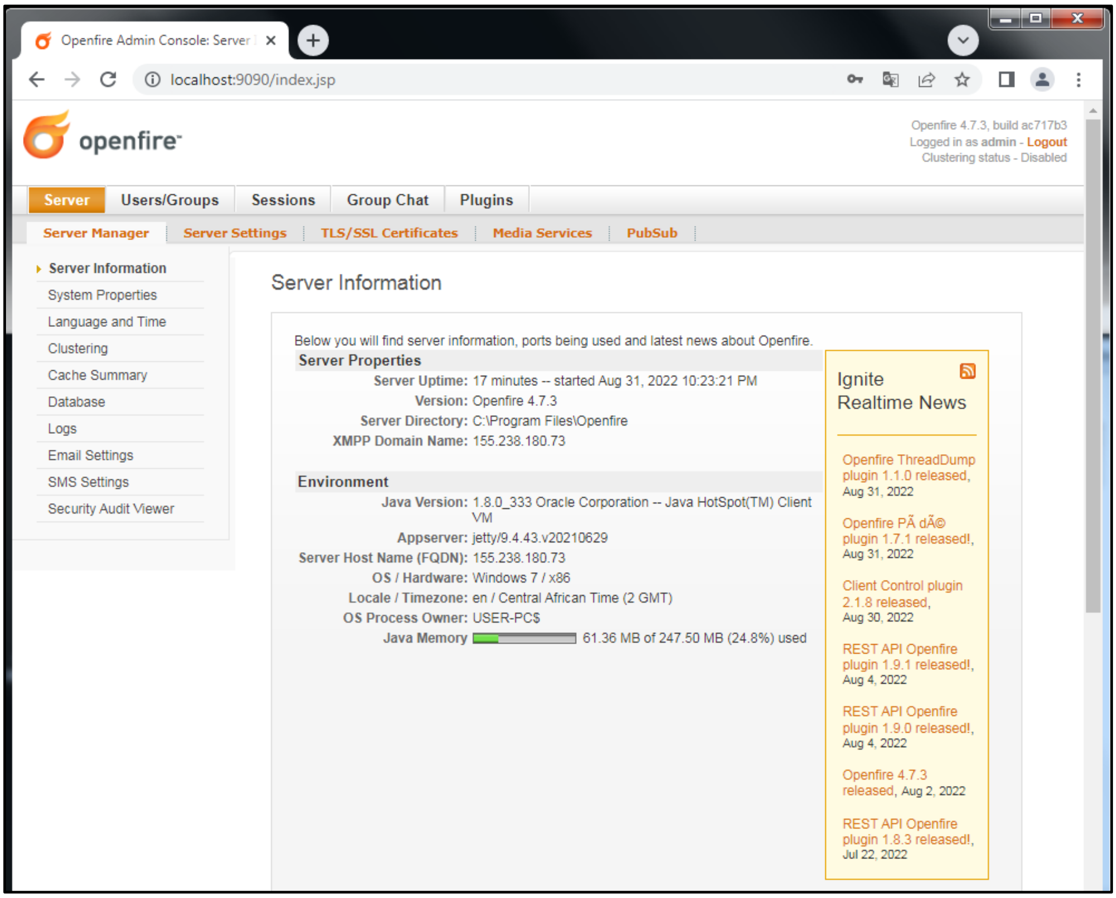


admin

•••••••••

Figure 4.53: Openfire server administration console login screen.

The ‘Administration Console’ of the server consists of several tabs containing various settings and configurations, which demonstrate the flexibility and variety of options provided by the Openfire application. The server information are depicted in figure 4.54 below, which provide detailed information about the server including uptime, version, and environment details.



Server Information

Below you will find server information, ports being used and latest news about Openfire.

Server Properties

Server Uptime: 17 minutes -- started Aug 31, 2022 10:23:21 PM
Version: Openfire 4.7.3
Server Directory: C:\Program Files\Openfire
XMPP Domain Name: 155.238.180.73

Environment

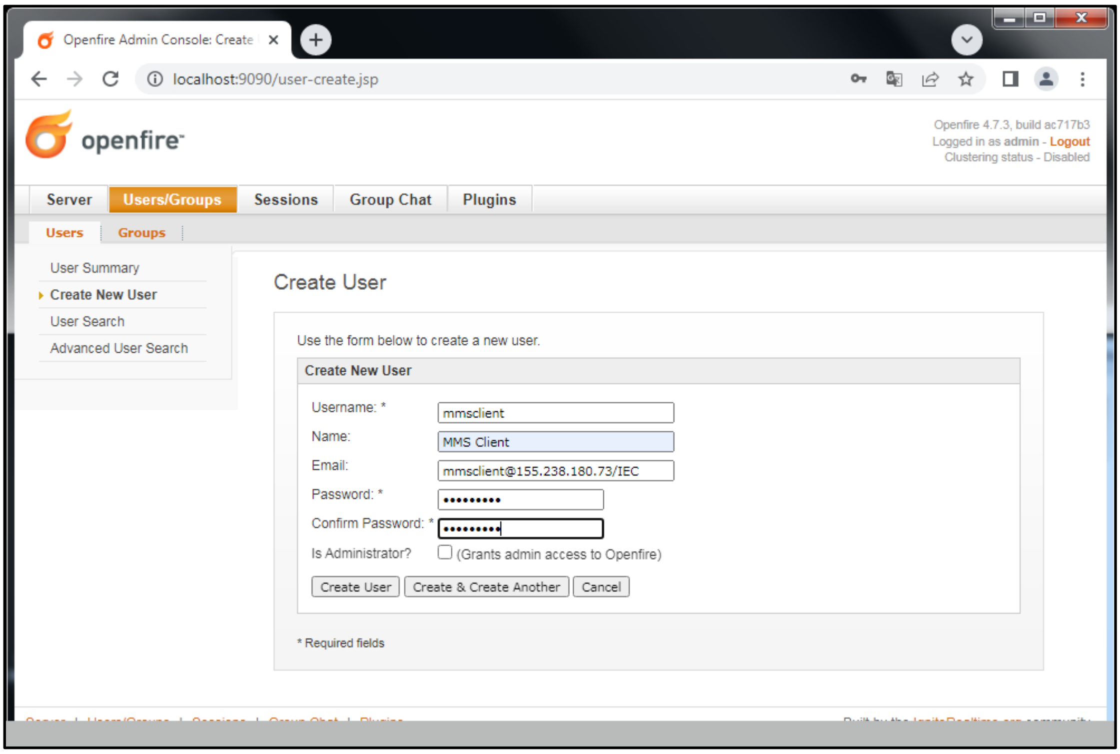
Java Version: 1.8.0_333 Oracle Corporation -- Java HotSpot(TM) Client VM
Appserver: jetty/9.4.43.v20210629
Server Host Name (FQDN): 155.238.180.73
OS / Hardware: Windows 7 / x86
Locale / Timezone: en / Central African Time (2 GMT)
OS Process Owner: USER-PC$
Java Memory 61.36 MB of 247.50 MB (24.8%) used

Ignite Realtime News

Openfire ThreadDump plugin 1.1.0 released, Aug 31, 2022
Openfire PÃ dÃ© plugin 1.7.1 released!, Aug 31, 2022
Client Control plugin 2.1.8 released, Aug 30, 2022
REST API Openfire plugin 1.9.1 released!, Aug 4, 2022
REST API Openfire plugin 1.9.0 released!, Aug 4, 2022
Openfire 4.7.3 released, Aug 2, 2022
REST API Openfire plugin 1.8.3 released!, Jul 22, 2022

Figure 4.54: The Openfire XMPP server information.

The next step is to create two user accounts for the Elipse Power IEC 61850-8-2 XMPP drivers. To do this, navigate to the ‘Users/Groups’ tab, then on ‘Users’ tab click on ‘Create New User’. The first account is created for the IEC 61850-8-2 XMPP client driver as illustrated in figure 4.55 below, with a JID ‘mmsclient@155.238.180.73/IEC’ and a password, then to click on ‘Create User’.



Create User

Use the form below to create a new user.

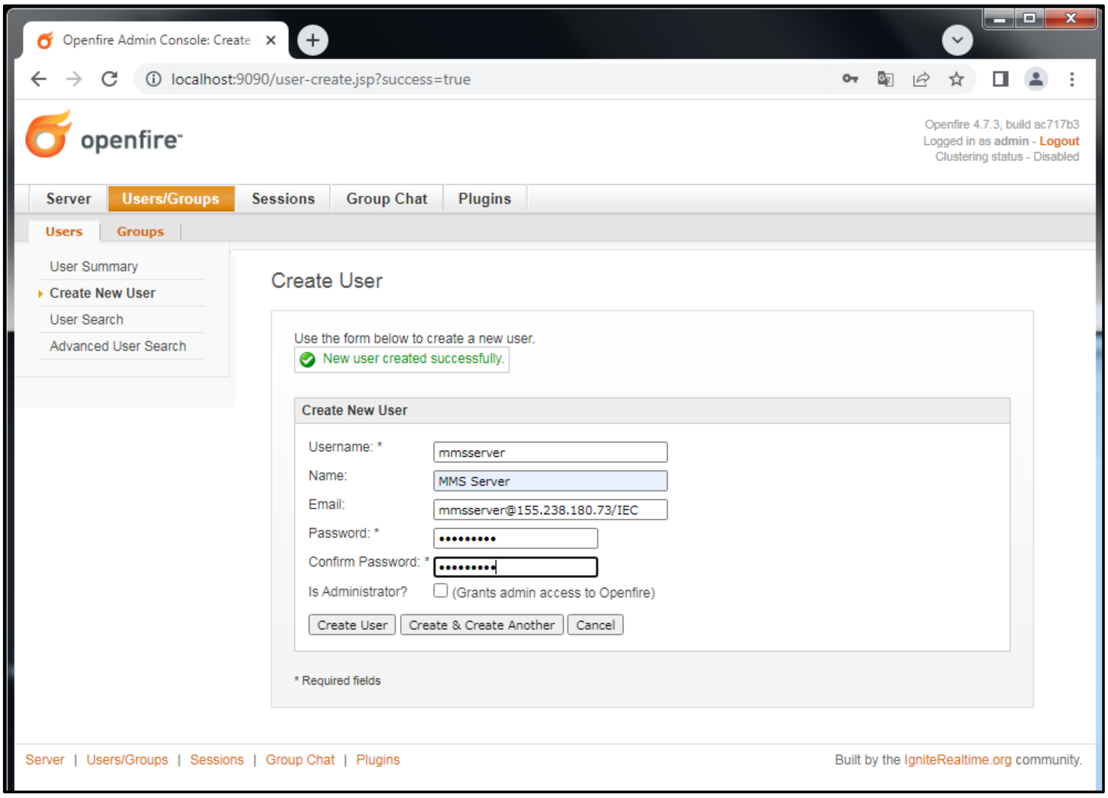
Create New User

Username: * mmsclient
Name: MMS Client
Email: mmsclient@155.238.180.73/IEC
Password: * •••••••••
Confirm Password: * •••••••••
Is Administrator? ☐ (Grants admin access to Openfire)

* Required fields

Figure 4.55: An IEC 61850-8-2 XMPP client user account.

Another account for the IEC 61850-8-2 XMPP server driver was created as shown in figure 4.56 below, with a JID 'mmsserver@155.238.180.73/IEC' and a password then to click on 'Create User'.



Create User

Use the form below to create a new user.

✓ New user created successfully.

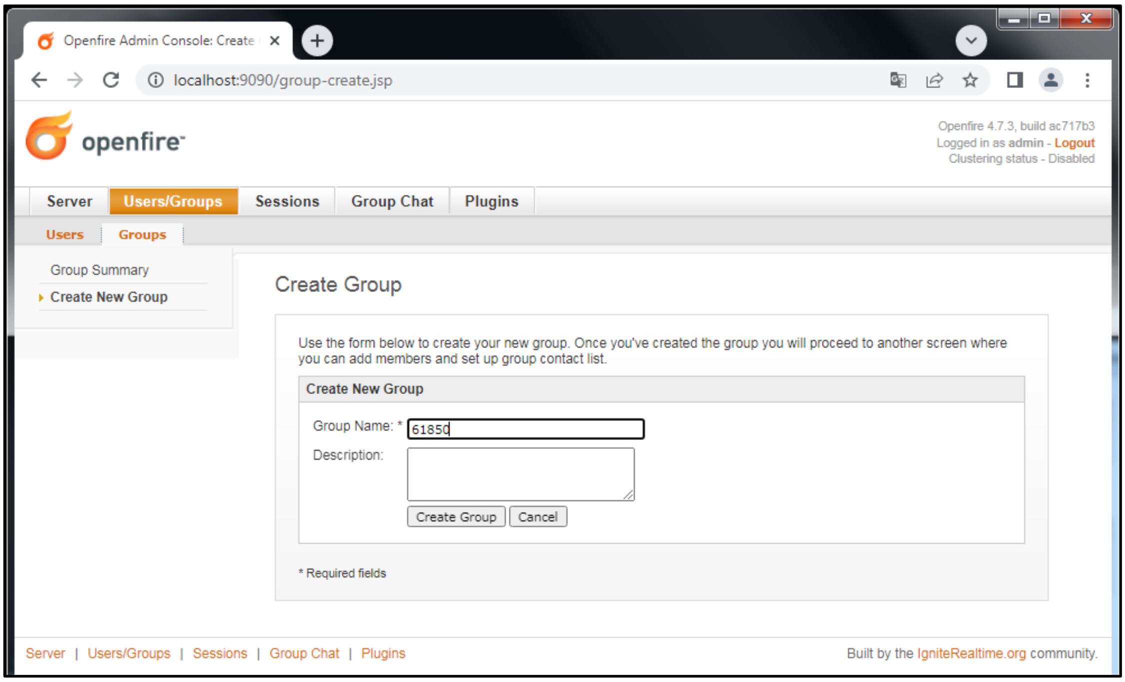
Create New User

Username: * mmsserver
Name: MMS Server
Email: mmsserver@155.238.180.73/IEC
Password: * •••••••••
Confirm Password: * •••••••••
Is Administrator? ☐ (Grants admin access to Openfire)

* Required fields

Figure 4.56: The IEC 61850-8-2 XMPP server user account.

The next step is to create ‘Group’ that the XMPP server uses to manage the XMPP clients ‘Users’. To do this, navigate to ‘Groups’ tab and click on ‘Create New Group’ then a name must be entered and optionally a description can be added as seen in figure 4.57 below.



Create Group

Use the form below to create your new group. Once you've created the group you will proceed to another screen where you can add members and set up group contact list.

Create New Group

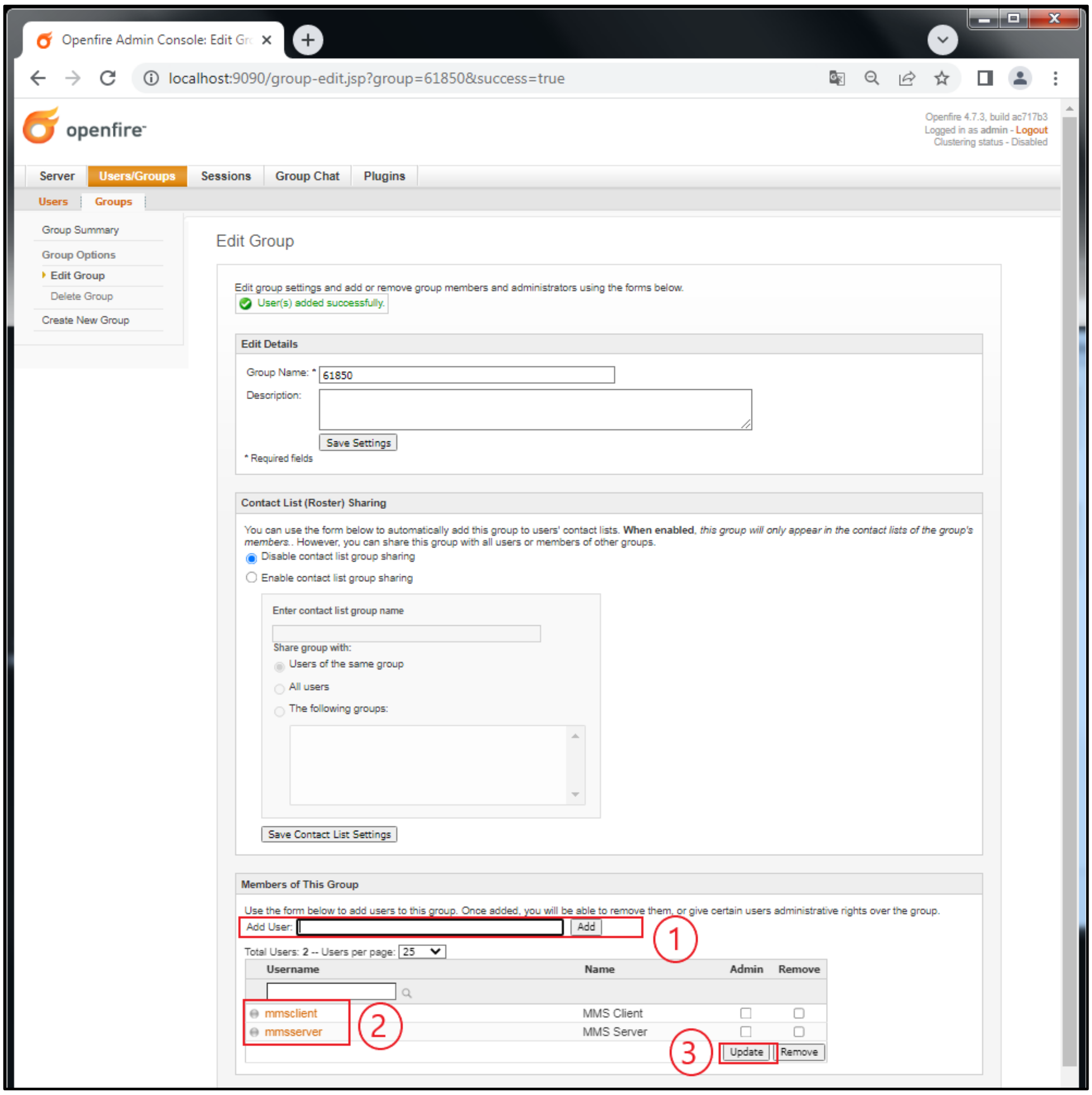
Group Name: * 61850

Description:

* Required fields

Figure 4.57: **Create a new group in Openfire server.**

Now the users can be added to the group ‘61850’ by typing in the username and clicking ‘Add’. When all users are added click on ‘Update’ to save the settings as displayed in figure 4.58 below.



Edit Group

Edit group settings and add or remove group members and administrators using the forms below.

User(s) added successfully.

Edit Details

Group Name: * 61850

Description:

* Required fields

Contact List (Roster) Sharing

You can use the form below to automatically add this group to users' contact lists. **When enabled**, *this group will only appear in the contact lists of the group's members.*. However, you can share this group with all users or members of other groups.

● Disable contact list group sharing

○ Enable contact list group sharing

Members of This Group

Use the form below to add users to this group. Once added, you will be able to remove them, or give certain users administrative rights over the group.

Add User:

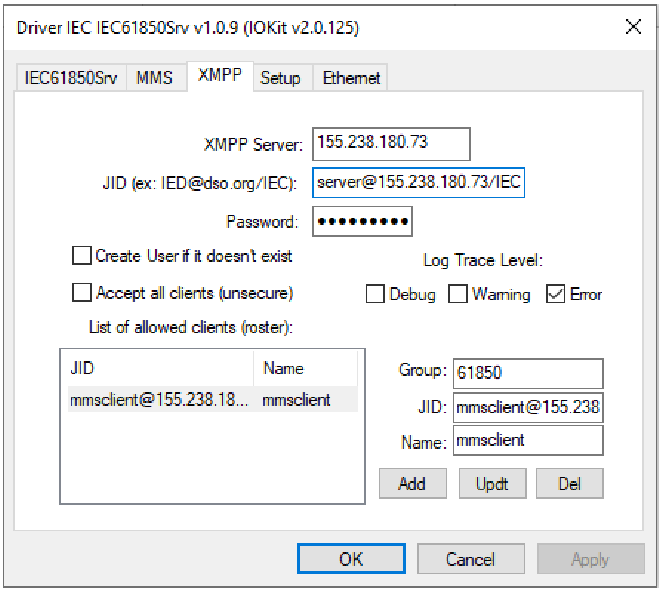
Total Users: 2 -- Users per page: 25

Username	Name	Admin	Remove
mmsclient	MMS Client	☐	☐
mmsserver	MMS Server	☐	☐

Figure 4.58: Adding users to the group.

The users' group configuration is a feature in the architecture of XMPP which is used by the XMPP server to manage communications between users in a group. This feature is implemented in WhatsApp where a user can broadcast messages to all other users in the group and subscribe to the presence feature which allows to know when other users are online. Now, the Openfire XMPP server setup and configuration are finished.

The XMPP communication parameters in Elipse Power IEC 61850-8-2 XMPP server driver are set by entering addresses of the Openfire XMPP server domain, a JID, and password of the 'mmsserver' user account. The 'mmsclient' user account information along with the group ID must be entered in the 'List of allowed clients' as described in figure 4.59 below.



XMPP Server: 155.238.180.73

JID (ex: IED@dso.org/IEC): server@155.238.180.73/IEC

Password: ●●●●●●●●●

☐ Create User if it doesn't exist

☐ Accept all clients (unsecure)

Log Trace Level: ☐ Debug ☐ Warning ☑ Error

List of allowed clients (roster):

JID	Name
mmsclient@155.238.18...	mmsclient

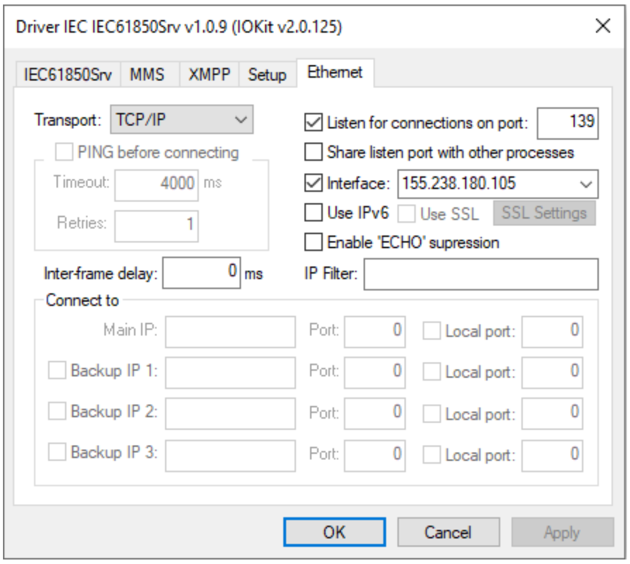
Group: 61850

JID: mmsclient@155.238

Name: mmsclient

Figure 4.59: **XMPP parameters in Elipse Power IEC 61850-8-2 server driver.**

The configuration of 'Setup' tab which contains physical layer settings, is identical to the IEC 61850-8-1 MMS client driver as noticed in figure 4.38 above. The final step is to configure 'Ethernet' tab which contains network layer settings. The driver was preset to listen for connections on local port '139' via the interface '155.238.180.105' which is the IP address of 'PC-1' as depicted in figure 4.60 below.



Transport: TCP/IP

☐ PING before connecting

Timeout: 4000 ms

Retries: 1

Inter-frame delay: 0 ms

Connect to

Main IP: Port: 0 ☐ Local port: 0

☐ Backup IP 1: Port: 0 ☐ Local port: 0

☐ Backup IP 2: Port: 0 ☐ Local port: 0

☐ Backup IP 3: Port: 0 ☐ Local port: 0

☑ Listen for connections on port: 139

☐ Share listen port with other processes

☑ Interface: 155.238.180.105

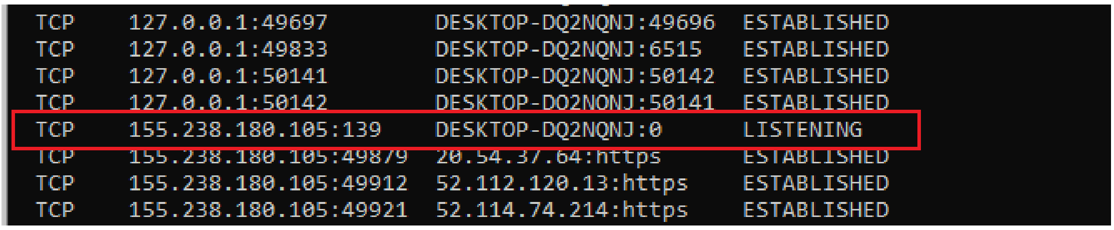
☐ Use IPv6 ☐ Use SSL

☐ Enable 'ECHO' supression

IP Filter:

Figure 4.60: **IEC 61850-8-2 server driver network layer settings.**

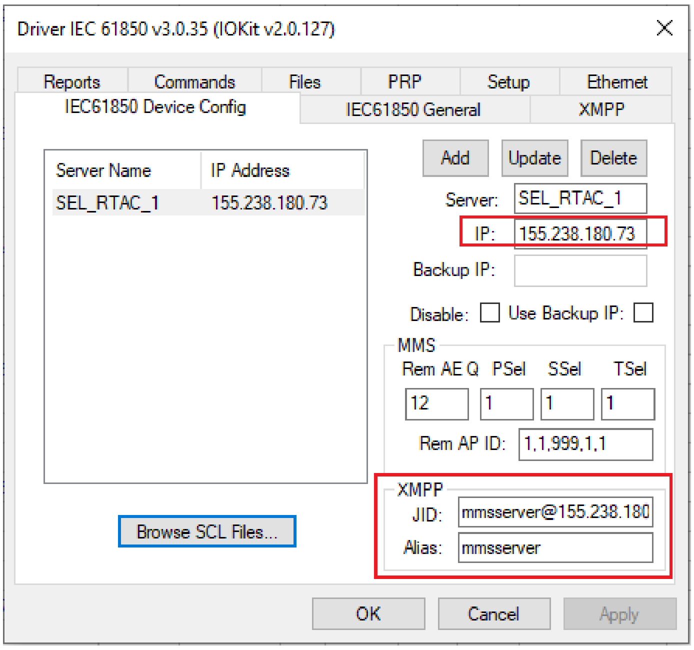
The local port '139' was identified from the network activities on 'PC-1' which host Elipse Power application using the command 'netstat –a' on the 'Command Prompt' terminal as noticed in figure 4.61 below. It shows that, the TCP interface '155.238.180.105' is listening for connections on port '139'.



```
TCP    127.0.0.1:49697        DESKTOP-DQ2NQNJ:49696  ESTABLISHED
TCP    127.0.0.1:49833        DESKTOP-DQ2NQNJ:6515   ESTABLISHED
TCP    127.0.0.1:50141        DESKTOP-DQ2NQNJ:50142  ESTABLISHED
TCP    127.0.0.1:50142        DESKTOP-DQ2NQNJ:50141  ESTABLISHED
TCP    155.238.180.105:139    DESKTOP-DQ2NQNJ:0      LISTENING
TCP    155.238.180.105:49879  20.54.37.64:https      ESTABLISHED
TCP    155.238.180.105:49912  52.112.120.13:https    ESTABLISHED
TCP    155.238.180.105:49921  52.114.74.214:https    ESTABLISHED
```

Figure 4.61: The ‘PC-1’ network activities status.

The final component in the testbed is a remote IEC 61850-8-2 XMPP client driver that polls data using XMPP as transport layer protocol. It is hosted on ‘PC-3’ which represents a control centre or a data server “cloud”, that are typically located in distant locations. The XMPP configurations of the driver start with ‘IEC 61850 Device Config’ tab, which contains settings of the server device as illustrated in figure 4.62 below. The IP address of the IEC 61850-8-2 XMPP server is set to the IP address of the Openfire XMPP server domain ‘155.238.180.73’, and the JID address and name of IEC 61850-8-2 XMPP server user ‘mmsserver’ are entered in the highlighted ‘XMPP’ segment.



Server Name	IP Address
SEL_RTAC_1	155.238.180.73

Server: SEL_RTAC_1
IP: 155.238.180.73
Backup IP:
Disable: ☐ Use Backup IP: ☐

MMS

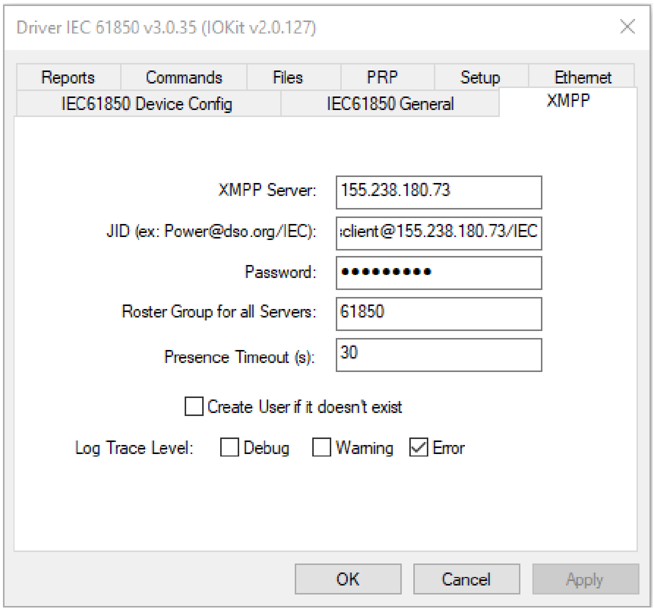
Rem AE Q	PSel	SSel	TSel
12	1	1	1

Rem AP ID: 1,1,999,1,1

XMPP
JID: mmsserver@155.238.180
Alias: mmsserver

Figure 4.62: Configuration of the IEC 61850-8-2 XMPP client driver.

In the next tab ‘IEC61850 General’, only the transport layer protocol setting is changed to XMPP instead of MMS. Thereafter, the ‘XMPP’ tab is configured by entering addresses of the XMPP server domain, the IEC 61850-8-2 XMPP client user JID, and the group name ‘61850’ as shown in figure 4.63 below.



XMPP Server: 155.238.180.73

JID (ex: Power@dso.org/IEC): :client@155.238.180.73/IEC

Password: ●●●●●●●●●

Roster Group for all Servers: 61850

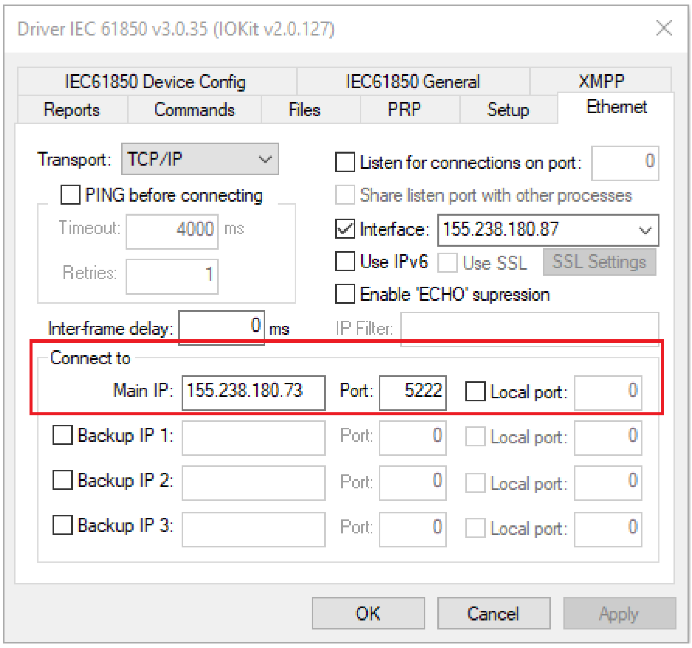
Presence Timeout (s): 30

☐ Create User if it doesn't exist

Log Trace Level: ☐ Debug ☐ Warning ☑ Error

Figure 4.63: The ‘XMPP’ tab in IEC 61850-8-2 XMPP client driver settings.

The physical layer settings are identical to previous drivers, however, the network layer is configured as seen in figure 4.64 below. The driver connects to the Openfire XMPP server in ‘PC-2’ via a local port ‘5222’ which is designated for XMPP communications.



Transport: TCP/IP

☐ PING before connecting

Timeout: 4000 ms

Retries: 1

Inter-frame delay: 0 ms

☐ Listen for connections on port: 0

☐ Share listen port with other processes

☑ Interface: 155.238.180.87

☐ Use IPv6 ☐ Use SSL

☐ Enable 'ECHO' supression

IP Filter:

Connect to

Main IP: 155.238.180.73 Port: 5222 ☐ Local port: 0

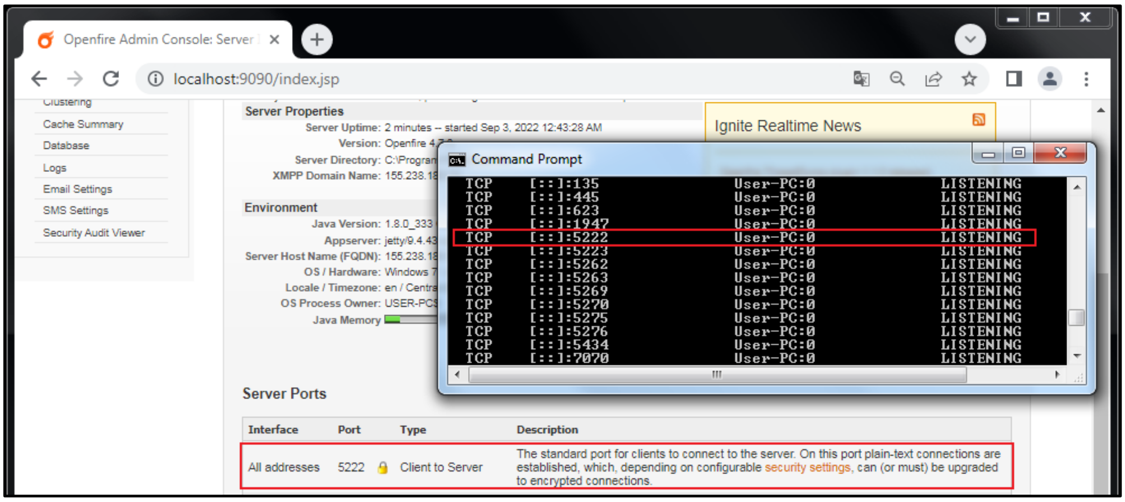
☐ Backup IP 1: Port: 0 ☐ Local port: 0

☐ Backup IP 2: Port: 0 ☐ Local port: 0

☐ Backup IP 3: Port: 0 ☐ Local port: 0

Figure 4.64: Network layer configuration of IEC 61850-8-2 XMPP client driver.

The designated ports for XMPP communications are listed in the ‘Adminstration Console’ of Openfire in tab ‘Server Ports’, in the server information tab as noted in figure 4.65 below.



Server Properties

Server Uptime: 2 minutes -- started Sep 3, 2022 12:43:28 AM
Version: Openfire 4.
Server Directory: C:\Progran
XMPP Domain Name: 155.238.18

Environment

Java Version: 1.8.0_333
Appserver: jetty/9.4.43
Server Host Name (FQDN): 155.238.18
OS / Hardware: Windows 7
Locale / Timezone: en / Centra
OS Process Owner: USER-PC$
Java Memory

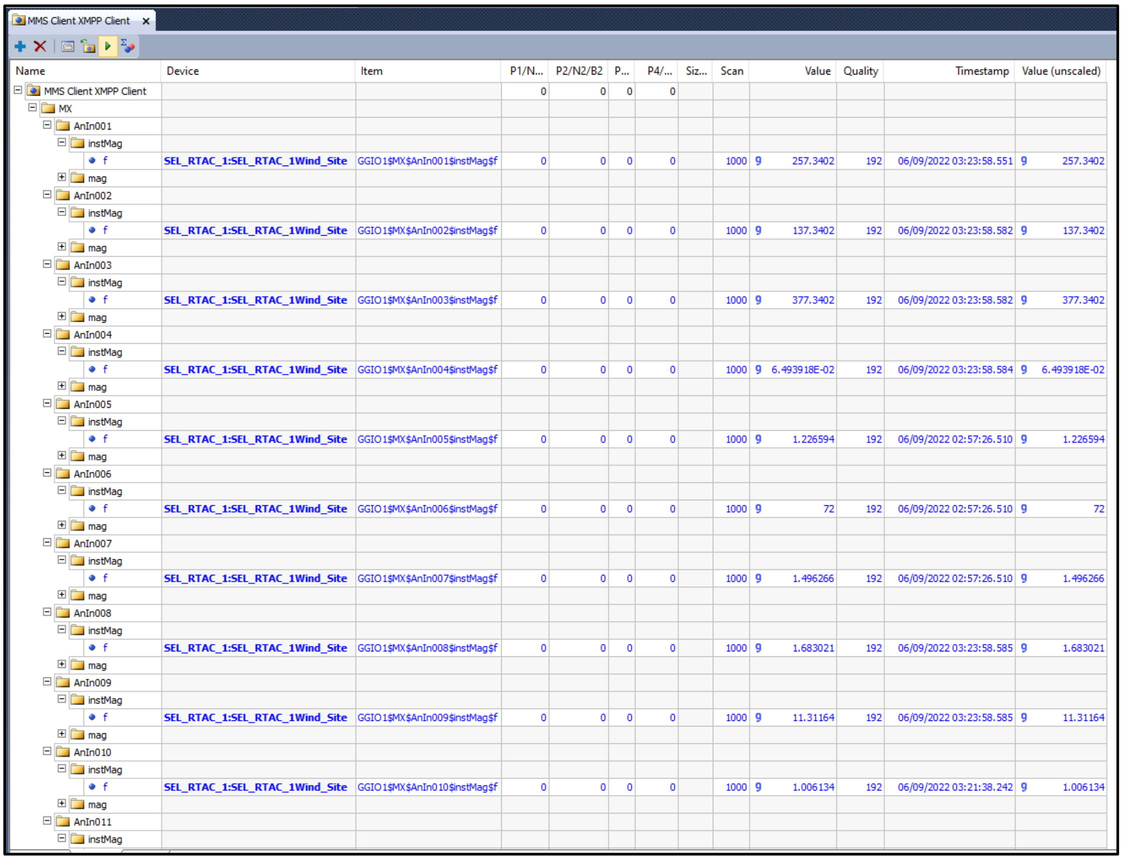
```
  TCP    [::]:135               User-PC:0              LISTENING
  TCP    [::]:445               User-PC:0              LISTENING
  TCP    [::]:623               User-PC:0              LISTENING
  TCP    [::]:1947              User-PC:0              LISTENING
  TCP    [::]:5222              User-PC:0              LISTENING
  TCP    [::]:5223              User-PC:0              LISTENING
  TCP    [::]:5262              User-PC:0              LISTENING
  TCP    [::]:5263              User-PC:0              LISTENING
  TCP    [::]:5269              User-PC:0              LISTENING
  TCP    [::]:5270              User-PC:0              LISTENING
  TCP    [::]:5275              User-PC:0              LISTENING
  TCP    [::]:5276              User-PC:0              LISTENING
  TCP    [::]:5434              User-PC:0              LISTENING
  TCP    [::]:7070              User-PC:0              LISTENING
```

Server Ports

Interface	Port	Type	Description
All addresses	5222 🔒	Client to Server	The standard port for clients to connect to the server. On this port plain-text connections are established, which, depending on configurable security settings, can (or must) be upgraded to encrypted connections.

Figure 4.65: XMPP server designated local ports.

The setup is complete for XMPP communications, and the data is being received upon driver activation, as displayed in figure 4.66 below.



Name	Device	Item	P1/N...	P2/N2/B2	P...	P4/...	Siz...	Scan	Value	Quality	Timestamp	Value (unscaled)
MMS Client XMPP Client			0	0	0	0						
MX												
AnIn001												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn001$instMag$f	0	0	0	0		1000	257.3402	192	06/09/2022 03:23:58.551	257.3402
mag												
AnIn002												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn002$instMag$f	0	0	0	0		1000	137.3402	192	06/09/2022 03:23:58.582	137.3402
mag												
AnIn003												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn003$instMag$f	0	0	0	0		1000	377.3402	192	06/09/2022 03:23:58.582	377.3402
mag												
AnIn004												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn004$instMag$f	0	0	0	0		1000	6.493918E-02	192	06/09/2022 03:23:58.584	6.493918E-02
mag												
AnIn005												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn005$instMag$f	0	0	0	0		1000	1.226594	192	06/09/2022 02:57:26.510	1.226594
mag												
AnIn006												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn006$instMag$f	0	0	0	0		1000	72	192	06/09/2022 02:57:26.510	72
mag												
AnIn007												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn007$instMag$f	0	0	0	0		1000	1.496266	192	06/09/2022 02:57:26.510	1.496266
mag												
AnIn008												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn008$instMag$f	0	0	0	0		1000	1.683021	192	06/09/2022 03:23:58.585	1.683021
mag												
AnIn009												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn009$instMag$f	0	0	0	0		1000	11.31164	192	06/09/2022 03:23:58.585	11.31164
mag												
AnIn010												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn010$instMag$f	0	0	0	0		1000	1.006134	192	06/09/2022 03:21:38.242	1.006134
mag												
AnIn011												
instMag												

Figure 4.66: IEC 61850-8-2 XMPP client driver activated.

The following section underlines points of discussion and encountered challenges throughout the implementation of the testbed.

4.4 Discussion

The chapter presented an implementation of a lab-scale testbed of a monitoring scheme that is based-on an EC gateway model. A model of a power network integrated with a wind enregy power generation was developed and simulated on RTDS. The model was set to communicate to an EC gateway utilizing IEC 61850-8-1 GOOSE via an RTDS GTNET card. The gateway performs mapping GOOSE to MMS before forwarding data to Elipse Power. Conversely, using GOOSE is one of the limitations in the research testbed due to the used GTNET hardware. The latest version “GTNETx2” enables IEC 61850-8-1 MMS standard, which could save significant processing time in the gateway model, that is based-on IEC 61850-8-1 MMS. Hence, it will be possible to establish a direct client/server connection between the GTNETx2’s MMS server and the gateway model rather than using GOOSE. Another limitation which is caused by GTNET hardware, is the number of data tags in the monitoring scheme. It is possible to transmit more than twelve data tags when using the latest hardware “GTNETx2”.

Elipse Power IEC 61850 comnmunication drivers are leading implementations of IEC 61850-8-2 XMPP standard in the market of SCADA software. The product is promising in terms of enabling applications of the standard for WANs. However, the implementation is relatively new with no available documentation or guidelines which made it a challenging task to fathom the configuration parameters for the drivers. The techincal support, guidance, and contribution received from Elipse Software™ Taiwan, by Mr Eric Liu in the course of troubleshooting and configuration procedures are well acknoweldged and appreciated.

It is noteworthy that, the Elipse Power application was used under a limited license for research purposes provided kindly by Elipse Software™ Taiwan. As part of the troubleshooting it is worth mentioning that, the SCL browsing software ‘ICD Designer’ from SystemCORP™ is a demo version that has a limitation of processing SCL files with less than two hundered DAs. Nonetheless, it was sufficient to perform the task in hand. The choice of using ‘Openfire’ from Ignite Realtime™ to implement the XMPP server in the research testbed, was motivated by its simplicity, effeciency, and wide acceptance within the XMPP developers’ community. The following section concludes the chapter.

4.5 Conclusion

In the chapter, the research testbed was described and configurations of each component to achieve the testbed successfully were presented. Firstly, all the components were introduced including RTDS, RTAC SEL-3555, and Elipse Power software. Thereafter, the configuration of each component was explained in details. Starting by exploring the power network model on RTDS and configuration of IEC 61850 GOOSE communications. Thereafter, the gateway model was described which consists of RTAC SEL-3555 along with Elipse Power communication drivers. An RTAC SEL-3555 was configured to subscribe to GOOSE messages from RTDS, and the RTAC SEL-3555's IEC 61850 information model was designed to enable MMS communications with Elipse Power communication drivers in the EC gateway model.

An algorithm was developed using AcSELerator RTAC SEL-5033 software to map the received GOOSE messages from the GoCB to the RTAC SEL-3555's server model. Two IEC 61850 communication drivers on Elipse Power were configured to achieve the integration of the local area to wide area communications. One is an MMS client driver which communicates to RTAC SEL-3555 according to IEC 61850-8-1 MMS standard and polls the data over a LAN. The second driver was configured as an MMS server and set to communicate over XMPP according to IEC 61850-8-2 standard over a WAN. The Openfire XMPP server application was utilized in the testbed to enable IEC 61850-8-2 XMPP communications.

The Openfire server application setup and creation of users for the client/server drivers were described. Finally, an Elipse Power IEC 61850-8-2 client driver was configured on 'PC-3' to communicate to the IEC 61850-8-2 server driver on 'PC-1' over an Internet-based WAN utilizing XMPP as middleware. The testbed configurations were completed and data was received in 'PC-3', successfully.

The following chapter describes the development of the data fusion algorithm on RTAC SEL-3555. Furthermore, the chapter presents communications analysis using Wireshark software tool to study XMPP communications and the impact of EC on the communication QoS.

CHAPTER FIVE

THE EDGE COMPUTING ALGORITHM AND NETWORK PERFORMANCE ANALYSIS

5.1 Introduction

As described previously in chapter four, a monitoring scheme testbed is developed to monitor a model of a power network integrated with a wind enregy DER simulated on the RTDS. Data from the model is acquired by an EC gateway model over a LAN connection. The gateway model consists of RTAC SEL-3555 and two IEC 61850 communication drivers in Elipse Power application. The RTAC SEL-3555 forwards data over a local area connection to the first driver in Elipse Power which is an IEC 61850-8-1 MMS client. Thereafter, data is forwarded to the second driver which is an IEC 61850-8-2 XMPP server that enables XMPP-based communication over WANs.

The workstation 'PC-3' which represents a control center in a distant location, hosts a remote IEC 61850-8-2 XMPP client driver that polls data from the IEC 61850-8-2 XMPP server driver on 'PC-1'. The XMPP-based communications are managed by the Openfire XMPP server application implemented on 'PC-2'. The chapter presents an evaluation of the EC impact on communications QoS for monitoring remote DER sites in a smart grid. An algorithm for data fusion is implemented in RTAC SEL-3555 to reduce data volume before transmission over an Internet-based WAN. Wireshark software is used to capture and analyze the network traffic to measure the QoS metrics of interest, which are latency and bandwidth usage. Additionally, data packets in the network traffic are analyzed to examine IEC 61850-8-2 XMPP standard data exchange and cybersecurity mechanisms.

The chapter is organised as follows, section 5.2 describes the setup for testing the communication network using Wireshark software. Section 5.3 provides analysis of IEC 61850-8-2 XMPP data exchange and cybersecurity features. Furthermore, section 5.4 outlines a description of the developed data fusion algorithm. Section 5.5 provides an evaluation of the data fusion algorithm's impact on the communication QoS parameters bandwidth usage and latency. Section 5.6 highlights points of discussion and the chapter is concluded in section 5.7.

5.2 Setting up Wireshark

Wireshark is a prominent open-source software for capturing and analysing data traffic in communication networks. The host machine of Wireshark was plugged into the main switch of the lab-scale monitoring testbed as described in figure 5.1 below. It was operated to capture IEC 61850-8-2 XMPP communications traffic over an Internet-based WAN.

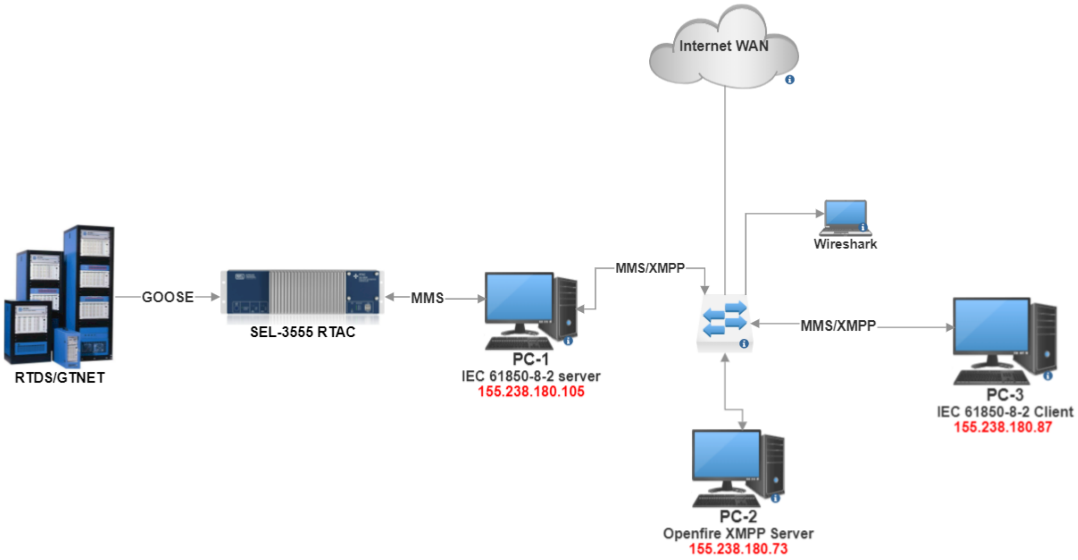


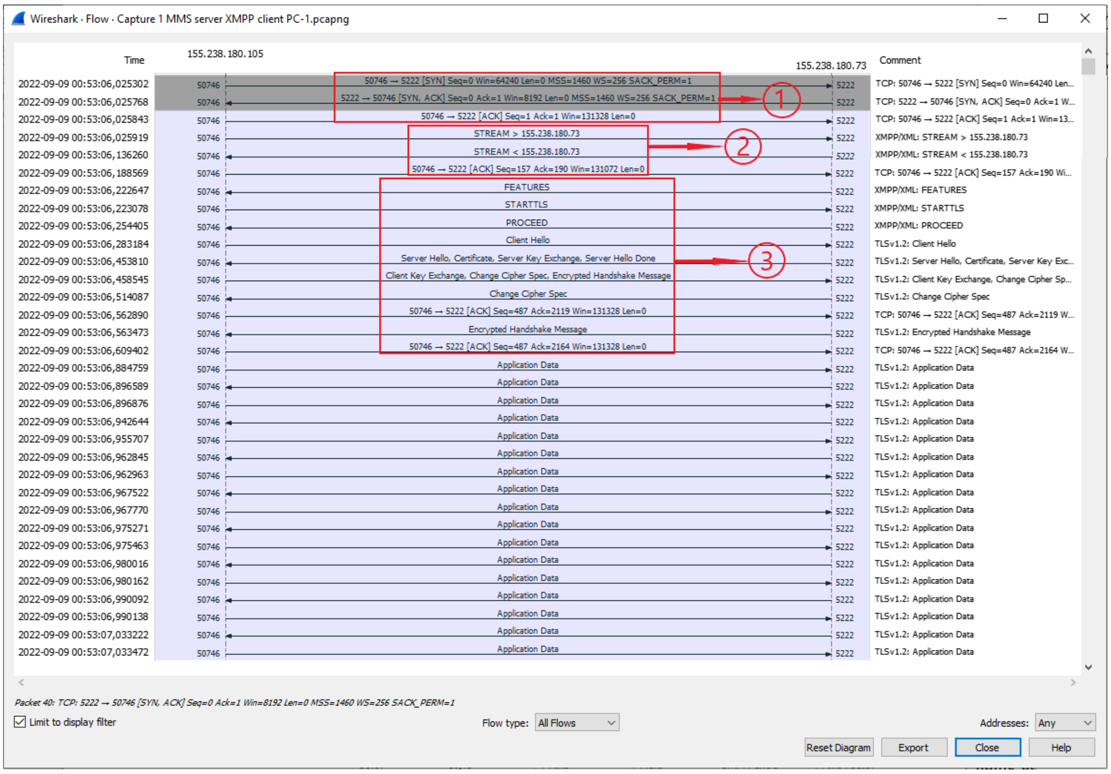
Figure 5.1: **Wireshark capturing point in the lab-scale testbed.**

The utilized network switch is configured to reroute traffic from all ports to a monitoring port, where Wireshark machine is plugged. This was achieved by activating the 'Mirror' port feature as noticed in figure A.4 in the appendix. The 'Mirror' port allows Wireshark to monitor all network traffic between XMPP clients and Openfire server. This point is the best option to get an accurate and synchronized capture of network traffic.

The following section presents a visual break down of the XMPP data exchange and cybersecurity aspects using the captured packets.

5.3 Analysis of IEC 61850-8-2 XMPP standard data exchange and cybersecurity mechanisms

The section describes a visual analysis of the data exchange and cybersecurity mechanisms of IEC 61850-8-2 XMPP standard. The data exchange profile specifies that IEC 61850 devices are to be hosted by XMPP clients. This is implemented in Elipse Power IEC 61850 drivers as they host the IEC 61850-8-1 MMS client/server entities, and uses XMPP as the transport layer protocol. All XMPP clients are linked across a WAN to an XMPP server and are given unique JID addresses (Nadeem et al., 2019). The Client/server architecture is used in XMPP communications whereby TCP/IP connections to the XMPP server are established by XMPP clients. The data exchange stream captured by Wireshark, between IEC 61850-8-2 XMPP client in 'PC-1' with IP address "155.238.180.105" and Openfire XMPP server hosted in 'PC-2' with IP address "155.238.180.73", are illustrated in figure 5.2 below.



Time	155.238.180.105		155.238.180.73	Comment
2022-09-09 00:53:06,025302	50746	50746 → 5222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	5222	TCP: 50746 → 5222 [SYN] Seq=0 Win=64240 Len...
2022-09-09 00:53:06,025768	50746	5222 → 50746 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	5222	TCP: 5222 → 50746 [SYN, ACK] Seq=0 Ack=1 W...
2022-09-09 00:53:06,025843	50746	50746 → 5222 [ACK] Seq=1 Ack=1 Win=131328 Len=0	5222	TCP: 50746 → 5222 [ACK] Seq=1 Ack=1 Win=13...
2022-09-09 00:53:06,025919	50746	STREAM > 155.238.180.73	5222	XMPP/XML: STREAM > 155.238.180.73
2022-09-09 00:53:06,136260	50746	STREAM < 155.238.180.73	5222	XMPP/XML: STREAM < 155.238.180.73
2022-09-09 00:53:06,188569	50746	50746 → 5222 [ACK] Seq=157 Ack=190 Win=131072 Len=0	5222	TCP: 50746 → 5222 [ACK] Seq=157 Ack=190 Wi...
2022-09-09 00:53:06,222647	50746	FEATURES	5222	XMPP/XML: FEATURES
2022-09-09 00:53:06,223078	50746	STARTTLS	5222	XMPP/XML: STARTTLS
2022-09-09 00:53:06,254405	50746	PROCEED	5222	XMPP/XML: PROCEED
2022-09-09 00:53:06,283184	50746	Client Hello	5222	TLSv1.2: Client Hello
2022-09-09 00:53:06,453810	50746	Server Hello, Certificate, Server Key Exchange, Server Hello Done	5222	TLSv1.2: Server Hello, Certificate, Server Key Exc...
2022-09-09 00:53:06,458545	50746	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	5222	TLSv1.2: Client Key Exchange, Change Cipher Sp...
2022-09-09 00:53:06,514087	50746	Change Cipher Spec	5222	TLSv1.2: Change Cipher Spec
2022-09-09 00:53:06,562890	50746	50746 → 5222 [ACK] Seq=487 Ack=2119 Win=131328 Len=0	5222	TCP: 50746 → 5222 [ACK] Seq=487 Ack=2119 W...
2022-09-09 00:53:06,563473	50746	Encrypted Handshake Message	5222	TLSv1.2: Encrypted Handshake Message
2022-09-09 00:53:06,609402	50746	50746 → 5222 [ACK] Seq=487 Ack=2164 Win=131328 Len=0	5222	TCP: 50746 → 5222 [ACK] Seq=487 Ack=2164 W...
2022-09-09 00:53:06,884759	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,896589	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,896876	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,942644	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,955707	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,962845	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,962963	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,967522	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,967770	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,975271	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,975463	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,980016	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,980162	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,990092	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:06,990138	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:07,033222	50746	Application Data	5222	TLSv1.2: Application Data
2022-09-09 00:53:07,033472	50746	Application Data	5222	TLSv1.2: Application Data

Packet 40: TCP: 5222 → 50746 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

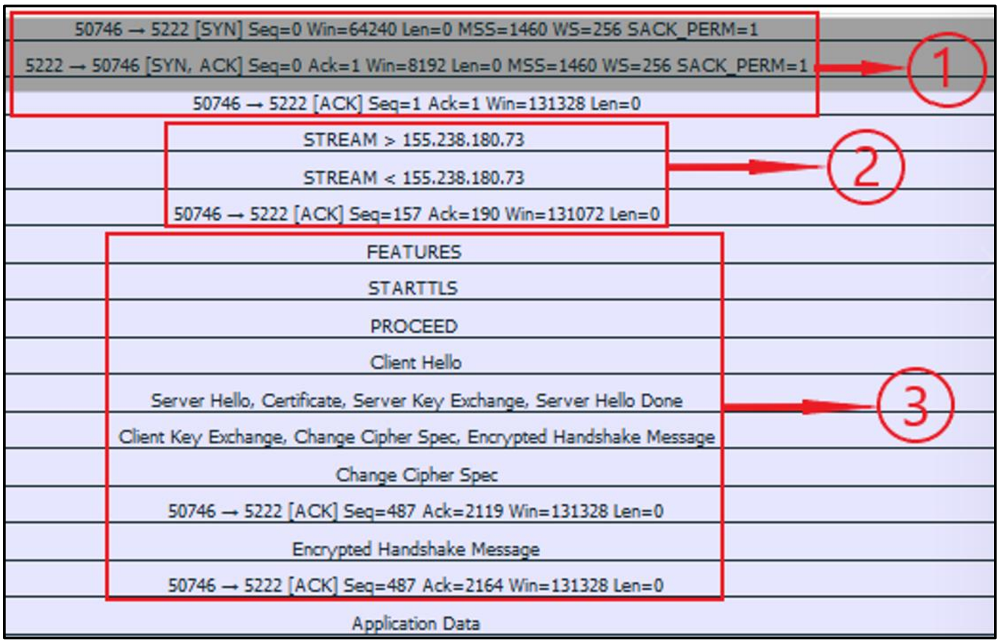
☑ Limit to display filter

Flow type: All Flows

Addresses: Any

Figure 5.2: XMPP exchanged packets between client/server.

The XMPP client initiates communications by sending a connection request, and the server responds to establish a TCP/IP connection as seen in the first three packets highlighted with number one. A magnified view of the exchanged data packets, is provided in figure 5.3 below. Once a TCP/IP link is established, an XML stream is enabled between client/server as indicated in the second packet group. Thereafter, a TLS connection is negotiated between client/server as highlighted in the third packet group.



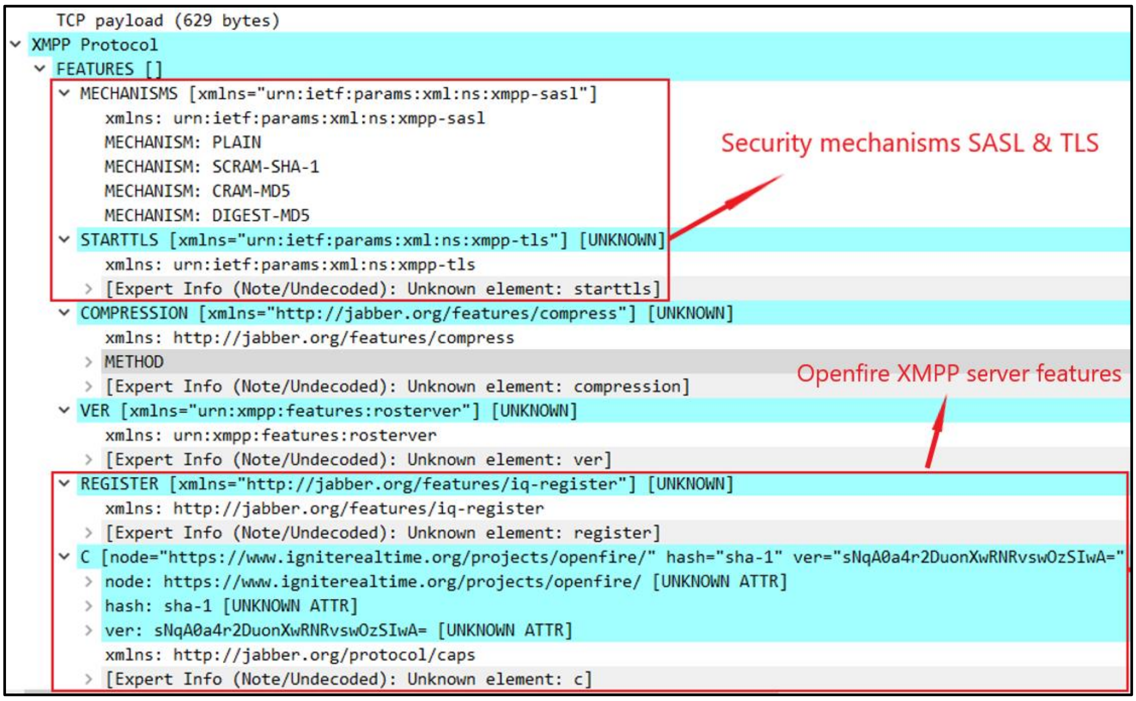
50746 → 5222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5222 → 50746 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
50746 → 5222 [ACK] Seq=1 Ack=1 Win=131328 Len=0
STREAM > 155.238.180.73
STREAM < 155.238.180.73
50746 → 5222 [ACK] Seq=157 Ack=190 Win=131072 Len=0
FEATURES
STARTTLS
PROCEED
Client Hello
Server Hello, Certificate, Server Key Exchange, Server Hello Done
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Change Cipher Spec
50746 → 5222 [ACK] Seq=487 Ack=2119 Win=131328 Len=0
Encrypted Handshake Message
50746 → 5222 [ACK] Seq=487 Ack=2164 Win=131328 Len=0
Application Data

Figure 5.3: A magnified view of the XMPP exchanged packets.

The XMPP-based communications take place in secured and an encrypted fashion. The TLS and SASL security protocols are implemented at the transport layer in E2M XMPP communication. The TLS protocol provides channel encryption to secure data from tampering and eavesdropping (Saint-Andre, 2011). As noted in TLS negotiation packets in figure 5.3 above, the client receives the ‘Features’ packet from the server and then initiates a ‘STARTTLS’ command.

A handshake is intitatied by the client ‘Client Hello’ and the server responds by sending a security certificate and a server key “authentication identity”. The client negotiates by requesting a ‘Change Cipher Spec’ to the server which is a request to change the encryption cipher specifications to be applied. The server acknowledges this request of change, and a secured and encrypted transport channel will be established, which will lead to realizing integrity and confidentiality for E2M XMPP communications. Consequently, upon completion of a successful TLS negotiation, the E2E SecProtocol authentication messages are interchanged in the form of encrypted handshakes to verify the IEC 61850 MMS client/server end peers as authenticated users.

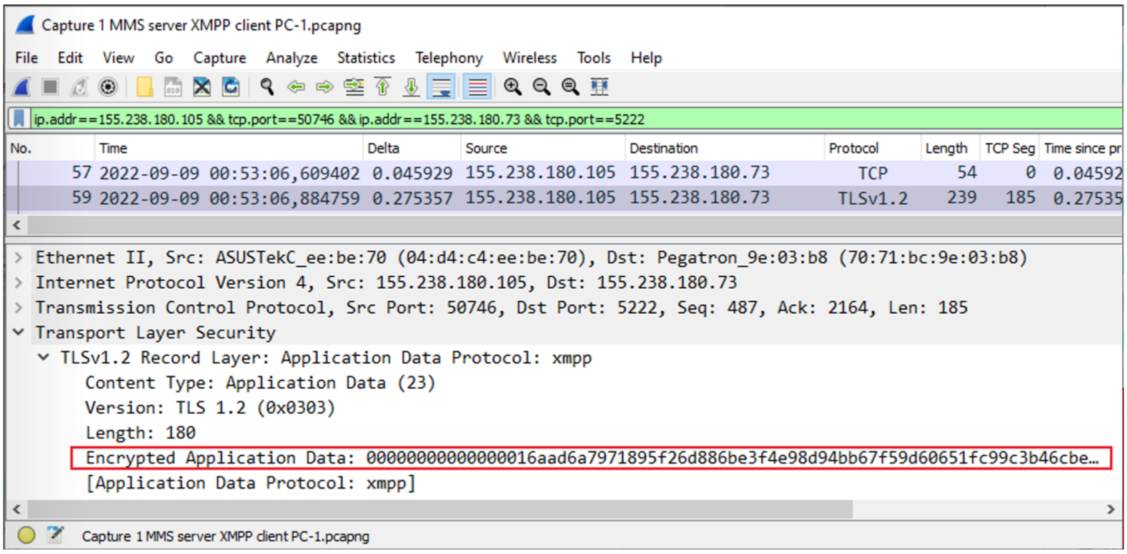
The ‘Features’ packet is the first to be sent by an XMPP server to any XMPP client after establishing the XML stream. It carries all the server’s information in the XMPP payload. As depicted in figure 5.4 below, the XMPP server declares all its features to the client including server information, cybersecurity mechanisms, encryption cipher, and compression method. After receiving this packet, the client requests to start TLS negotiations.



```
    TCP payload (629 bytes)
v XMPP Protocol
  v FEATURES []
    v MECHANISMS [xmlns="urn:ietf:params:xml:ns:xmpp-sasl"]
        xmlns: urn:ietf:params:xml:ns:xmpp-sasl
        MECHANISM: PLAIN
        MECHANISM: SCRAM-SHA-1
        MECHANISM: CRAM-MD5
        MECHANISM: DIGEST-MD5
    v STARTTLS [xmlns="urn:ietf:params:xml:ns:xmpp-tls"] [UNKNOWN]
        xmlns: urn:ietf:params:xml:ns:xmpp-tls
      > [Expert Info (Note/Undecoded): Unknown element: starttls]
    v COMPRESSION [xmlns="http://jabber.org/features/compress"] [UNKNOWN]
        xmlns: http://jabber.org/features/compress
      > METHOD
      > [Expert Info (Note/Undecoded): Unknown element: compression]
    v VER [xmlns="urn:xmpp:features:rosterver"] [UNKNOWN]
        xmlns: urn:xmpp:features:rosterver
      > [Expert Info (Note/Undecoded): Unknown element: ver]
    v REGISTER [xmlns="http://jabber.org/features/iq-register"] [UNKNOWN]
        xmlns: http://jabber.org/features/iq-register
      > [Expert Info (Note/Undecoded): Unknown element: register]
    v C [node="https://www.igniterealtime.org/projects/openfire/" hash="sha-1" ver="sNqA0a4r2DuonXwRNRvswOzSIwA="
      > node: https://www.igniterealtime.org/projects/openfire/ [UNKNOWN ATTR]
      > hash: sha-1 [UNKNOWN ATTR]
      > ver: sNqA0a4r2DuonXwRNRvswOzSIwA= [UNKNOWN ATTR]
        xmlns: http://jabber.org/protocol/caps
      > [Expert Info (Note/Undecoded): Unknown element: c]
```

Figure 5.4: XMPP server ‘Features’ packet contents.

As seen in figure 5.5 below, the contents of an ‘Application Data’ packet are encrypted and any attempt from possible attackers to eavesdrop on XMPP communications using packet-capturing tools such as Wireshark, would be useless to get any information.



```
ip.addr==155.238.180.105 && tcp.port==50746 && ip.addr==155.238.180.73 && tcp.port==5222
```

```
No.  Time                        Delta     Source           Destination     Protocol  Length  TCP Seg  Time since pr
  57 2022-09-09 00:53:06,609402 0.045929  155.238.180.105  155.238.180.73  TCP           54        0  0.04592
  59 2022-09-09 00:53:06,884759 0.275357  155.238.180.105  155.238.180.73  TLSv1.2      239      185  0.27535
```

```
> Ethernet II, Src: ASUSTekC_ee:be:70 (04:d4:c4:ee:be:70), Dst: Pegatron_9e:03:b8 (70:71:bc:9e:03:b8)
> Internet Protocol Version 4, Src: 155.238.180.105, Dst: 155.238.180.73
> Transmission Control Protocol, Src Port: 50746, Dst Port: 5222, Seq: 487, Ack: 2164, Len: 185
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: xmpp
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 180
      Encrypted Application Data: 0000000000000016aad6a7971895f26d886be3f4e98d94bb67f59d60651fc99c3b46cbe…
      [Application Data Protocol: xmpp]
```

Figure 5.5: The ‘Application Data’ packet encrypted content.

The following section presents the developed algorithm to reduce the data volume transmitted on a network.

5.4 Edge computing algorithm for data reduction

A data fusion algorithm is implemented in RTAC SEL-3555 using IEC 61131-3 ST language. The main purpose of the algorithm is to reduce the number of transmitted data tags over a network. In the research testbed, a total of twelve data tags are used for monitoring the power network model in RTDS, which are listed in table A.2 in the appendix. The first three points are root mean square (rms) values of single-phase voltages of the generator busbar ‘STWLT1a, STWLT1b, STWLT1c’. The equivalent three-phase value can be transmitted instead of three individual values, it is calculated by using equation 5.1 below, where V_A represents the single-phase voltage.

$$V_{3ph} = \sqrt{3} * V_A \tag{5.1}$$

The three tags, wind gust ‘GUST’, wind speed ‘windkph’, and pitch degree ‘pitchdeg’, are reduced to a single point by using the gust value as an alarm for wind overspeed which can damage the turbine. In the occurrence of wind gust, the gateway must transmit the pitch degree value to inform the control centre that, the pitch angle control is operative. In the event that, pitch angle control is not operative, a manual intervention would be needed to prevent turbine damage during high wind speeds. However, the gateway keeps monitoring the wind speed during normal and low wind speeds. This logic can be expressed in the following steps:

- If ‘GUST’ > 1
- Transmit pitch degree ‘pitchdeg’
- Else
- Transmit wind speed ‘windkph’

A similar concept is applied to combine the power output of the induction machine ‘STLWT1P’ and the power output of the wind turbine ‘pwturb’. For the duration of the wind turbine startup and before reaching rated speed and coupling to the grid, the gateway must transmit the power output of the turbine. During this period, the power output of the generator would be very small or even a negative value. Thereafter, when rated speed is achieved and the generator is coupled to the grid, priority shifts to the generator power output to be monitored. This logic can be articulated in the following steps:

- If generator output power ‘STLWT1P’ < 0
- Transmit turbine output power ‘pwturb’
- Else
- Transmit generator’s output power ‘STLWT1P’

The final part of the algorithm combines generator rotor speed ‘STLWT1SPD’ and turbine hub speed ‘HUBSPD’, which are interrelated via the gear ratio. Both values are calculated by the turbine model in RTDS, using different units. The rotor speed is provided in pu and the hub speed in radiance per second (rad/s). The rotor speed can be converted to turbine hub speed using the gear ratio value. Henceforth, the EC gateway can transmit only the difference between the converted and the monitored hub speed ‘HUBSPD’ instead of transmitting two data tags. The difference should be very small “optimally zero” and any significant change in the value would indicate existence of mechanical faults in the coupling parts between turbine and generator.

According to the technical specifications of the turbine model “Vestas V82” listed in table A.1 in the appendix, the gear ratio is “84.5”, and the rated speed of the generator machine is “1200” revolution per minute (rpm) which is the base value for the rotor speed in pu. In order to convert the rotor speed to hub speed, the following steps are performed using equations 5.2 up to 5.5:

- Convert pu to rpm

$$1\,pu = 1200\,rpm \tag{5.2}$$

$$STLWT1SPD * 1200 = rotor\ speed\ in\ rpm \tag{5.3}$$

- Apply the gear ratio to convert to the hub speed

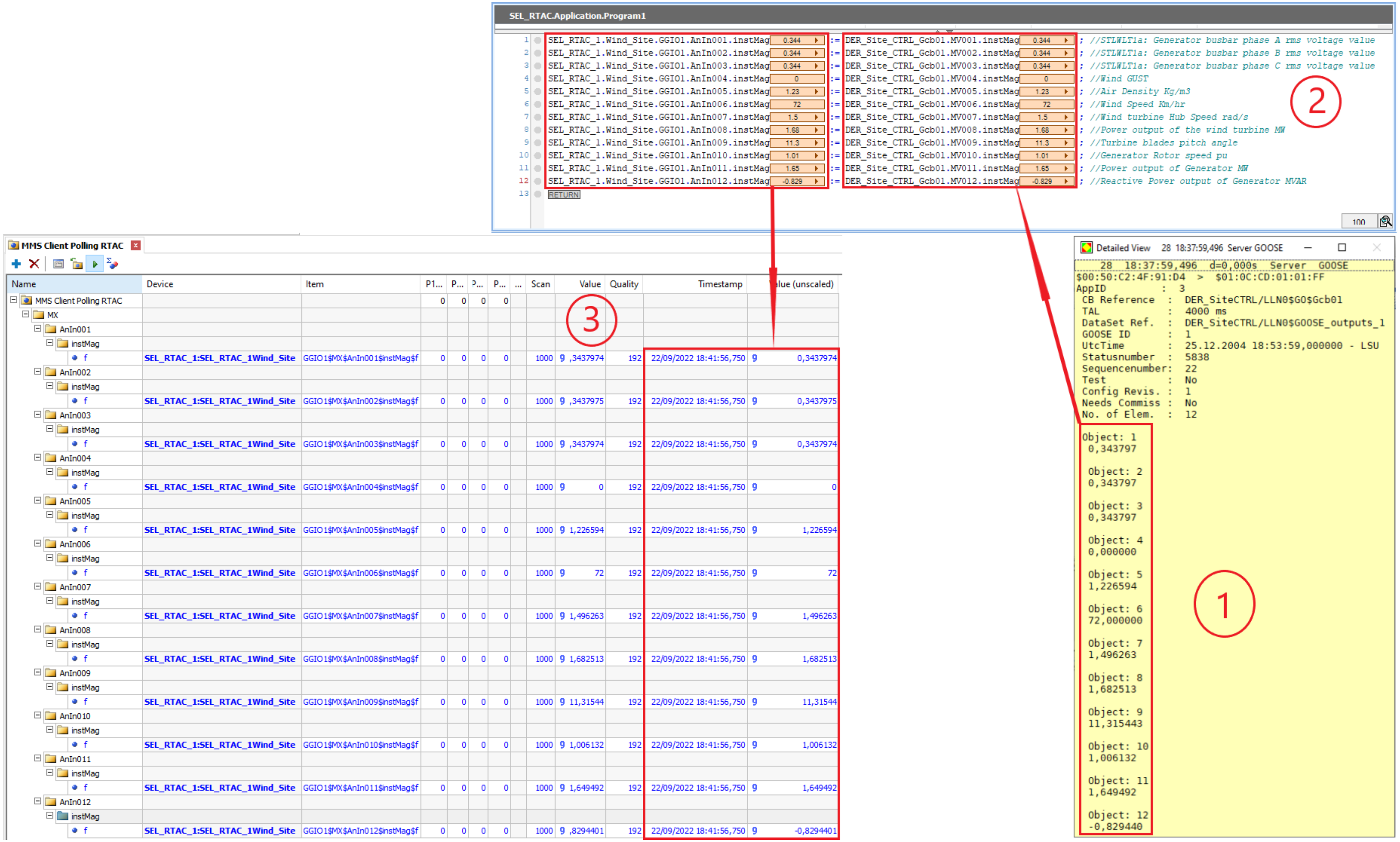
$$rotor\ speed\ in\ rpm * 1/84.5 = hub\ speed\ in\ rpm \tag{5.4}$$

- Convert hub speed to rad/sec

$$hub\ speed\ in\ rad/s = hub\ speed\ in\ rpm * (2\pi/60) \tag{5.5}$$

The converted value of the hub speed in equation 5.5 above, is subtracted from the monitored hub speed value which is provided via GOOSE from the turbine model in RTDS, and the difference is transmitted by the gateway. The algorithm is developed using IEC 61131-3 ST language in RTAC SEL-3555 as shown in figure A.5 in the appendix.

Simulations were run for the two test cases, with and without executing the data fusion algorithm. When the algorithm is not executed, all twelve data tags are transmitted without any reduction as displayed in figure 5.6 below. Data was tracked across the testbed in order to verify the algorithm effect. GOOSE messages which are published by the DER model on RTDS, were monitored using GOOSE Inspector software indicated by number one in the figure. Then, the GOOSE is mapped to the server model of RTAC SEL-3555, and the online monitoring mode in RTAC SEL-3555 was used to observe data values in real-time, as highlighted by number two in the figure. Finally, the online view of the IEC 61850-8-1 MMS client driver in Elipse Power was captured as indicated by number three in the figure.



SEL_RTAC.Application.Program1

```
SEL_RTAC_1.Wind_Site.GGIO1.AnIn001.instMag 0.344 := DER_Site_CTRL_Gcb01.MV001.instMag 0.344 ; //STLWLT1a: Generator busbar phase A rms voltage value
SEL_RTAC_1.Wind_Site.GGIO1.AnIn002.instMag 0.344 := DER_Site_CTRL_Gcb01.MV002.instMag 0.344 ; //STLWLT1a: Generator busbar phase B rms voltage value
SEL_RTAC_1.Wind_Site.GGIO1.AnIn003.instMag 0.344 := DER_Site_CTRL_Gcb01.MV003.instMag 0.344 ; //STLWLT1a: Generator busbar phase C rms voltage value
SEL_RTAC_1.Wind_Site.GGIO1.AnIn004.instMag 0     := DER_Site_CTRL_Gcb01.MV004.instMag 0     ; //Wind GUST
SEL_RTAC_1.Wind_Site.GGIO1.AnIn005.instMag 1.23  := DER_Site_CTRL_Gcb01.MV005.instMag 1.23  ; //Air Density Kg/m3
SEL_RTAC_1.Wind_Site.GGIO1.AnIn006.instMag 72    := DER_Site_CTRL_Gcb01.MV006.instMag 72    ; //Wind Speed Km/hr
SEL_RTAC_1.Wind_Site.GGIO1.AnIn007.instMag 1.5   := DER_Site_CTRL_Gcb01.MV007.instMag 1.5   ; //Wind turbine Hub Speed rad/s
SEL_RTAC_1.Wind_Site.GGIO1.AnIn008.instMag 1.68  := DER_Site_CTRL_Gcb01.MV008.instMag 1.68  ; //Power output of the wind turbine MW
SEL_RTAC_1.Wind_Site.GGIO1.AnIn009.instMag 11.3  := DER_Site_CTRL_Gcb01.MV009.instMag 11.3  ; //Turbine blades pitch angle
SEL_RTAC_1.Wind_Site.GGIO1.AnIn010.instMag 1.01  := DER_Site_CTRL_Gcb01.MV010.instMag 1.01  ; //Generator Rotor speed pu
SEL_RTAC_1.Wind_Site.GGIO1.AnIn011.instMag 1.65  := DER_Site_CTRL_Gcb01.MV011.instMag 1.65  ; //Power output of Generator MW
SEL_RTAC_1.Wind_Site.GGIO1.AnIn012.instMag -0.829 := DER_Site_CTRL_Gcb01.MV012.instMag -0.829 ; //Reactive Power output of Generator MVAR
RETURN
```

MMS Client Polling RTAC

Name	Device	Item	P1...	P...	P...	P...	...	Scan	Value	Quality	Timestamp	Value (unscaled)
MMS Client Polling RTAC			0	0	0	0						
MX												
AnIn001												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn001$instMag$f	0	0	0	0		1000	,3437974	192	22/09/2022 18:41:56,750	0,3437974
AnIn002												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn002$instMag$f	0	0	0	0		1000	,3437975	192	22/09/2022 18:41:56,750	0,3437975
AnIn003												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn003$instMag$f	0	0	0	0		1000	,3437974	192	22/09/2022 18:41:56,750	0,3437974
AnIn004												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn004$instMag$f	0	0	0	0		1000	0	192	22/09/2022 18:41:56,750	0
AnIn005												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn005$instMag$f	0	0	0	0		1000	1,226594	192	22/09/2022 18:41:56,750	1,226594
AnIn006												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn006$instMag$f	0	0	0	0		1000	72	192	22/09/2022 18:41:56,750	72
AnIn007												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn007$instMag$f	0	0	0	0		1000	1,496263	192	22/09/2022 18:41:56,750	1,496263
AnIn008												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn008$instMag$f	0	0	0	0		1000	1,682513	192	22/09/2022 18:41:56,750	1,682513
AnIn009												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn009$instMag$f	0	0	0	0		1000	11,31544	192	22/09/2022 18:41:56,750	11,31544
AnIn010												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn010$instMag$f	0	0	0	0		1000	1,006132	192	22/09/2022 18:41:56,750	1,006132
AnIn011												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn011$instMag$f	0	0	0	0		1000	1,649492	192	22/09/2022 18:41:56,750	1,649492
AnIn012												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn012$instMag$f	0	0	0	0		1000	,8294401	192	22/09/2022 18:41:56,750	-0,8294401

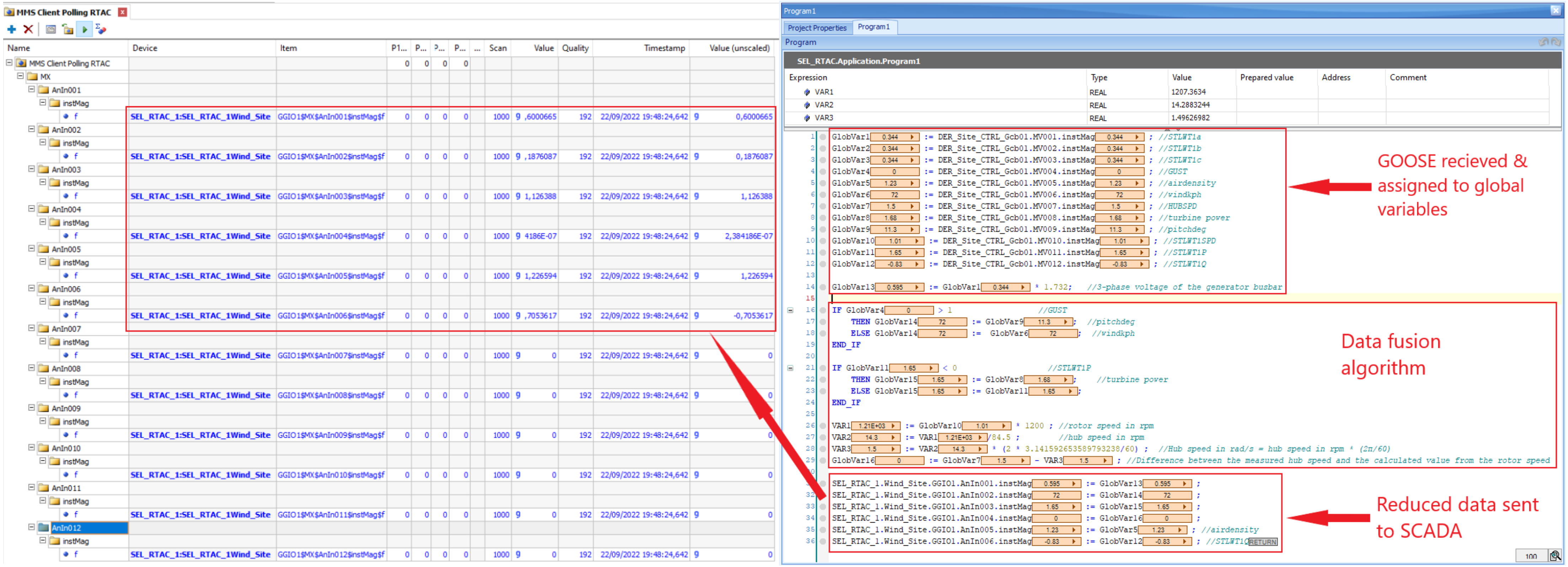
Detailed View 28 18:37:59,496 Server GOOSE

```
   28  18:37:59,496  d=0,000s  Server  GOOSE
$00:50:C2:4F:91:D4  >  $01:0C:CD:01:01:FF
AppID          :  3
 CB Reference   :  DER_SiteCTRL/LLN0$GO$Gcb01
 TAL            :  4000 ms
 DataSet Ref.   :  DER_SiteCTRL/LLN0$GOOSE_outputs_1
 GOOSE ID       :  1
 UtcTime        :  25.12.2004 18:53:59,000000 - LSU
 Statusnumber   :  5838
 Sequencenumber:  22
 Test           :  No
 Config Revis.  :  1
 Needs Commiss  :  No
 No. of Elem.   :  12

 Object: 1
  0,343797

  Object: 2
  0,343797

  Object: 3
  0,343797

  Object: 4
  0,000000

  Object: 5
  1,226594

  Object: 6
  72,000000

  Object: 7
  1,496263

  Object: 8
  1,682513

  Object: 9
  11,315443

  Object: 10
  1,006132

  Object: 11
  1,649492

  Object: 12
  -0,829440
```

Figure 5.6: Data across the gateway model without execution of the EC algorithm.

After the data fusion algorithm was executed, the data tags were effectively reduced from twelve to six tags. As illustrated in figure 5.7 below, twelve data tags are received via GOOSE, assigned to global variables, then the algorithm operates on these variables. Thereafter, the resulting data tags are assigned to DOs of the RTAC SEL-3555’s server model. Six tags are forwarded to the IEC 61850-8-1 MMS client driver in Elipse Power.

The following section presents an analysis of the communication performance using Wireshark packet-capturing software.



Name	Device	Item	P1...	P...	P...	P...	...	Scan	Value	Quality	Timestamp	Value (unscaled)
MMS Client Polling RTAC			0	0	0	0						
MX												
AnIn001												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn001$instMag$f	0	0	0	0		1000	9 ,6000665	192	22/09/2022 19:48:24,642	9 0,6000665
AnIn002												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn002$instMag$f	0	0	0	0		1000	9 ,1876087	192	22/09/2022 19:48:24,642	9 0,1876087
AnIn003												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn003$instMag$f	0	0	0	0		1000	9 1,126388	192	22/09/2022 19:48:24,642	9 1,126388
AnIn004												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn004$instMag$f	0	0	0	0		1000	9 4186E-07	192	22/09/2022 19:48:24,642	9 2,384186E-07
AnIn005												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn005$instMag$f	0	0	0	0		1000	9 1,226594	192	22/09/2022 19:48:24,642	9 1,226594
AnIn006												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn006$instMag$f	0	0	0	0		1000	9 ,7053617	192	22/09/2022 19:48:24,642	9 -0,7053617
AnIn007												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn007$instMag$f	0	0	0	0		1000	9 0	192	22/09/2022 19:48:24,642	9 0
AnIn008												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn008$instMag$f	0	0	0	0		1000	9 0	192	22/09/2022 19:48:24,642	9 0
AnIn009												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn009$instMag$f	0	0	0	0		1000	9 0	192	22/09/2022 19:48:24,642	9 0
AnIn010												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn010$instMag$f	0	0	0	0		1000	9 0	192	22/09/2022 19:48:24,642	9 0
AnIn011												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn011$instMag$f	0	0	0	0		1000	9 0	192	22/09/2022 19:48:24,642	9 0
AnIn012												
instMag												
f	SEL_RTAC_1:SEL_RTAC_1Wind_Site	GGIO1MXAnIn012$instMag$f	0	0	0	0		1000	9 0	192	22/09/2022 19:48:24,642	9 0

Expression	Type	Value	Prepared value	Address	Comment
VAR1	REAL	1207.3634			
VAR2	REAL	14.2883244			
VAR3	REAL	1.49626982			

```
GlobVar1 0.344 := DER_Site_CTRL_Gcb01.MV001.instMag 0.344 ; //STLWT1a
GlobVar2 0.344 := DER_Site_CTRL_Gcb01.MV002.instMag 0.344 ; //STLWT1b
GlobVar3 0.344 := DER_Site_CTRL_Gcb01.MV003.instMag 0.344 ; //STLWT1c
GlobVar4 0 := DER_Site_CTRL_Gcb01.MV004.instMag 0 ; //GUST
GlobVar5 1.23 := DER_Site_CTRL_Gcb01.MV005.instMag 1.23 ; //airdensity
GlobVar6 72 := DER_Site_CTRL_Gcb01.MV006.instMag 72 ; //windkph
GlobVar7 1.5 := DER_Site_CTRL_Gcb01.MV007.instMag 1.5 ; //HUBSPD
GlobVar8 1.68 := DER_Site_CTRL_Gcb01.MV008.instMag 1.68 ; //turbine power
GlobVar9 11.3 := DER_Site_CTRL_Gcb01.MV009.instMag 11.3 ; //pitchdeg
GlobVar10 1.01 := DER_Site_CTRL_Gcb01.MV010.instMag 1.01 ; //STLWT1SPD
GlobVar11 1.65 := DER_Site_CTRL_Gcb01.MV011.instMag 1.65 ; //STLWT1P
GlobVar12 -0.83 := DER_Site_CTRL_Gcb01.MV012.instMag -0.83 ; //STLWT1Q

GlobVar13 0.595 := GlobVar1 0.344 * 1.732;   //3-phase voltage of the generator busbar

IF GlobVar4 0 > 1                       //GUST
    THEN GlobVar14 72 := GlobVar9 11.3 ;  //pitchdeg
    ELSE GlobVar14 72 :=  GlobVar6 72 ;  //windkph
END_IF

IF GlobVar11 1.65 < 0                    //STLWT1P
    THEN GlobVar15 1.65 := GlobVar8 1.68 ;    //turbine power
    ELSE GlobVar15 1.65 := GlobVar11 1.65 ;
END_IF

VAR1 1.21E+03 := GlobVar10 1.01 * 1200 ; //rotor speed in rpm
VAR2 14.3 := VAR1 1.21E+03 /84.5 ;        //hub speed in rpm
VAR3 1.5 := VAR2 14.3 * (2 * 3.1415926535897932 38/60) ;  //Hub speed in rad/s = hub speed in rpm * (2π/60)
GlobVar16 0 := GlobVar7 1.5 - VAR3 1.5 ; //Difference between the measured hub speed and the calculated value from the rotor speed

SEL_RTAC_1.Wind_Site.GGIO1.AnIn001.instMag 0.595 := GlobVar13 0.595 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn002.instMag 72 := GlobVar14 72 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn003.instMag 1.65 := GlobVar15 1.65 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn004.instMag 0 := GlobVar16 0 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn005.instMag 1.23 := GlobVar5 1.23 ; //airdensity
SEL_RTAC_1.Wind_Site.GGIO1.AnIn006.instMag -0.83 := GlobVar12 -0.83 ; //STLWT1Q
```

Figure 5.7: Data across the gateway model with the execution of the EC algorithm.

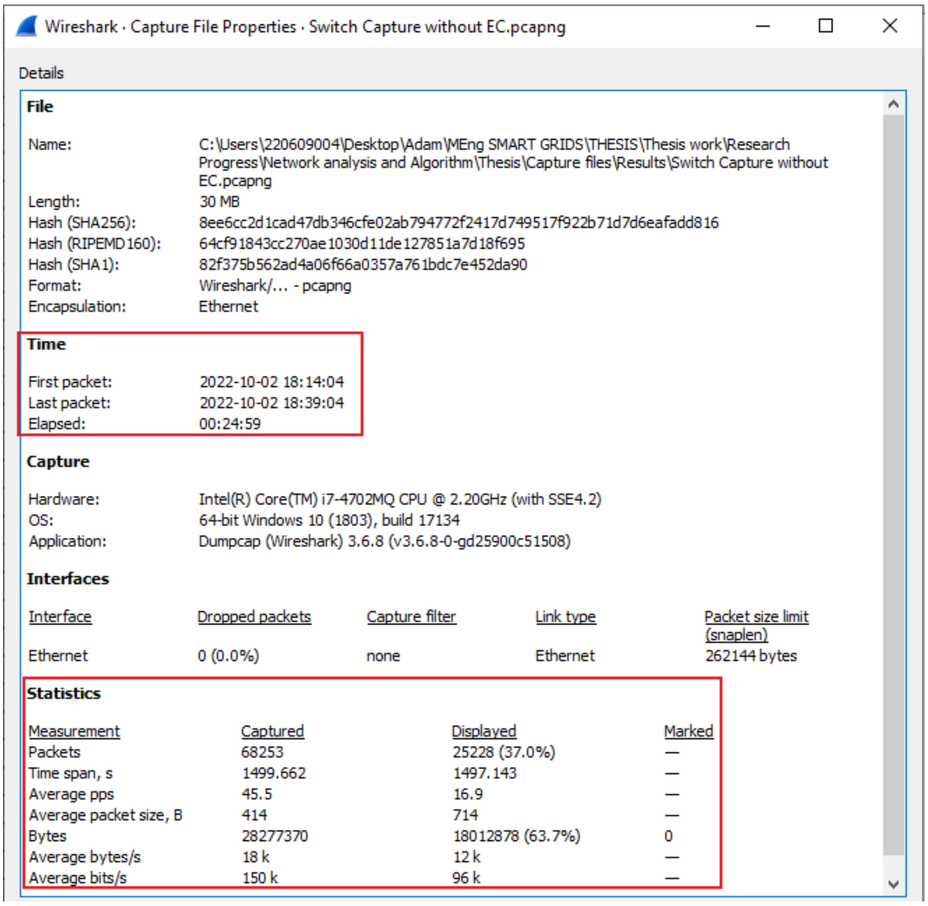
5.5 Analysis of the communication Quality of Service using Wireshark

The QoS metrics such as bandwidth and latency are performance indicators of communication networks. Bandwidth is the transmission capacity of a network that determines the data volume which can be transferred across a network in a specific period of time. Bandwidth is measured in bits/s, and is the main characteristic that decides the quality of a communication network. Insufficient bandwidth affects the overall network performance and causes congestions that result in excessive latencies, packet losses, and poor connectivity. Therefore, minimizing the bandwidth usage in a network is critical to ensure the best possible performance.

A major purpose of implementing the EC concept, is to reduce data traffic in a network by processing data near the source before transmission, consecuently, reducing the bandwidth usage will improve the overall network performance. In the testbed, Wireshark was employed to capture data traffic in the network and to provide measurements for communications QoS metrics “bandwidth usage and latency”. These measurements are used to evaluate the impact of implementing the EC algorithm on the performance of a communication network. The methodology of evaluation is established on comparing QoS measurements in two test cases, with and without executing the EC algorithm. The following sections present methodologies and results of Wireshark analysis tools.

5.5.1 Description of Wireshark ‘Capture Files’

The traffic captures for both test cases were taken for equal period of time twenty five minutes, to provide an accurate comparison of the network performance. A display filter was applied to extract the traffic of interest between the Openfire XMPP server and Elipse Power drivers “XMPP clients” in the testbed. The applied filter is written in the format “ip.addr == 155.238.180.73 && ip.addr == 155.238.180.105 or ip.addr == 155.238.180.73 && ip.addr == 155.238.180.87”. As a result, the displayed packets are only the conversations between the Openfire XMPP server hosted on ‘PC-2’ with IP address “155.238.180.73”, and the IEC 61850-8-2 XMPP clients hosted on ‘PC-1’ and ‘PC-3’ with IP addresses “155.238.180.105” and “155.238.180.87” respectively. Wireshark produces statistics for both captured and filtered data. The properties of the ‘Capture Files’ for the test cases are displayed in figures 5.8 and 5.9 below.



Wireshark · Capture File Properties · Switch Capture without EC.pcapng

Details

File

Name: C:\Users\220609004\Desktop\Adam\MEng SMART GRIDS\THESIS\Thesis work\Research Progress\Network analysis and Algorithm\Thesis\Capture files\Results\Switch Capture without EC.pcapng
Length: 30 MB
Hash (SHA256): 8ee6cc2d1cad47db346cfe02ab794772f2417d749517f922b71d7d6eafadd816
Hash (RIPEMD160): 64cf91843cc270ae1030d11de127851a7d18f695
Hash (SHA1): 82f375b562ad4a06f66a0357a761bdc7e452da90
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2022-10-02 18:14:04
Last packet: 2022-10-02 18:39:04
Elapsed: 00:24:59

Capture

Hardware: Intel(R) Core(TM) i7-4702MQ CPU @ 2.20GHz (with SSE4.2)
OS: 64-bit Windows 10 (1803), build 17134
Application: Dumpcap (Wireshark) 3.6.8 (v3.6.8-0-gd25900c51508)

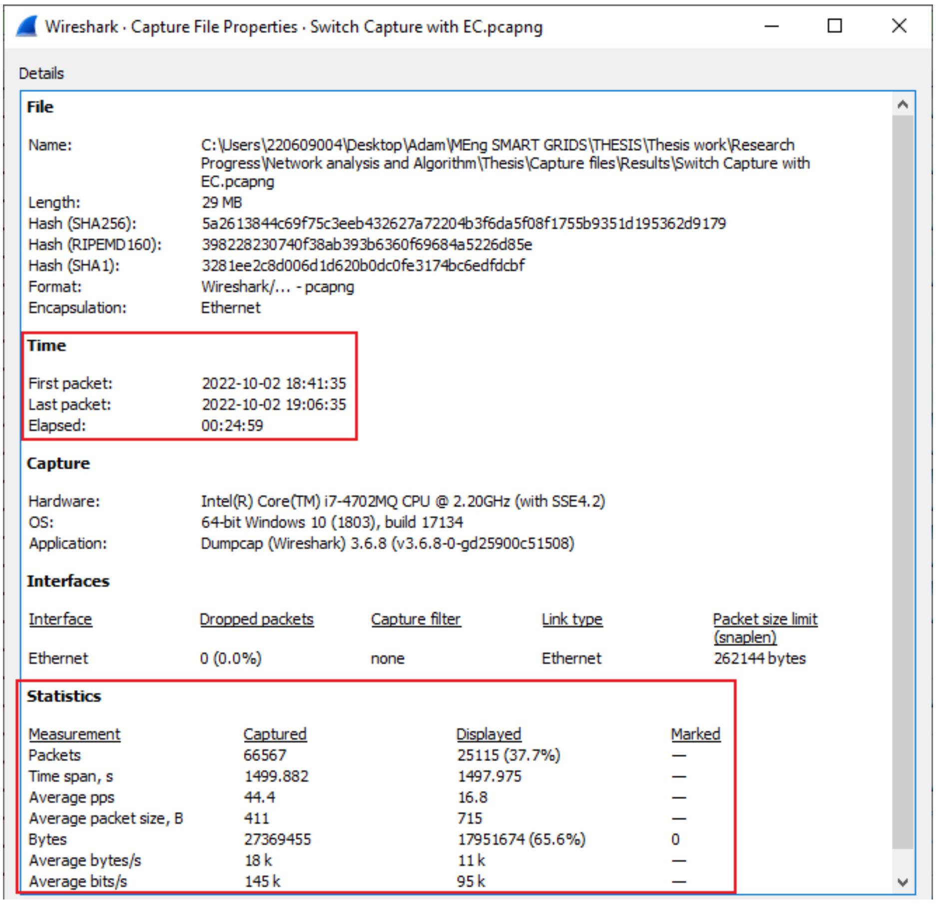
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	68253	25228 (37.0%)	—
Time span, s	1499.662	1497.143	—
Average pps	45.5	16.9	—
Average packet size, B	414	714	—
Bytes	28277370	18012878 (63.7%)	0
Average bytes/s	18 k	12 k	—
Average bits/s	150 k	96 k	—

Figure 5.8: The capture file properties without execution of the EC algorithm.



Wireshark · Capture File Properties · Switch Capture with EC.pcapng

Details

File

Name: C:\Users\220609004\Desktop\Adam\MEng SMART GRIDS\THESIS\Thesis work\Research Progress\Network analysis and Algorithm\Thesis\Capture files\Results\Switch Capture with EC.pcapng
Length: 29 MB
Hash (SHA256): 5a2613844c69f75c3eeb432627a72204b3f6da5f08f1755b9351d195362d9179
Hash (RIPEMD160): 398228230740f38ab393b6360f69684a5226d85e
Hash (SHA1): 3281ee2c8d006d1d620b0dc0fe3174bc6edfdcbf
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2022-10-02 18:41:35
Last packet: 2022-10-02 19:06:35
Elapsed: 00:24:59

Capture

Hardware: Intel(R) Core(TM) i7-4702MQ CPU @ 2.20GHz (with SSE4.2)
OS: 64-bit Windows 10 (1803), build 17134
Application: Dumpcap (Wireshark) 3.6.8 (v3.6.8-0-gd25900c51508)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	66567	25115 (37.7%)	—
Time span, s	1499.882	1497.975	—
Average pps	44.4	16.8	—
Average packet size, B	411	715	—
Bytes	27369455	17951674 (65.6%)	0
Average bytes/s	18 k	11 k	—
Average bits/s	145 k	95 k	—

Figure 5.9: The capture file properties with the execution of the EC algorithm.

The displayed properties include the capture file name, length, date and time of the capture, and statistics of captured and displayed traffic “filtered XMPP data traffic”. As noticed from the ‘Statistics’ part in the figures above, the average bandwidth usage reflects the impact of the EC algorithm. In the capture file ‘Switch Capture without EC’ in figure 5.8 above, the bandwidth usage is ‘96 Kbits/s’ for the filtered XMPP traffic. While in the capture file ‘Switch Capture with EC’ in figure 5.9 above, the bandwidth usage reads ‘95 Kbits/s’. This indicates a bandwidth usage reduction by one Kbits/s.

Wireshark provides comprehensive tools to evaluate the bandwidth usage and latency from the captured traffic. The I/O Graphs tool gives accurate measurments of QoS metrics. The following section provides an analysis of communication QoS for both test cases in the testbed using Wireshark I/O Graphs.

5.5.2 Communication Quality of Service analysis using Wireshark I/O Graphs

The bandwidth usage in each test case of the implementation, are provided in figures 5.10 and 5.11 below.

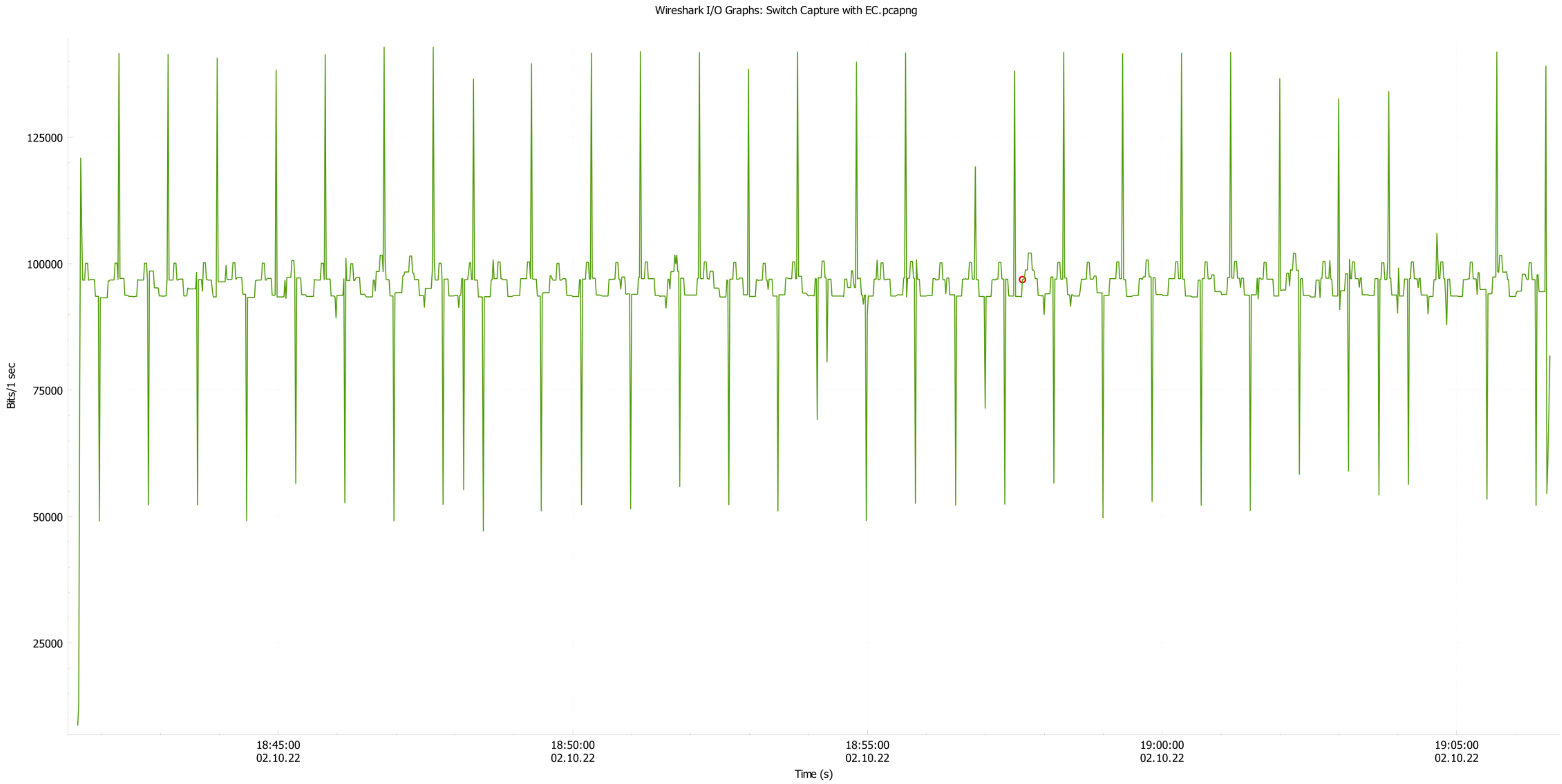


Figure 5.10: Bandwidth usage of XMPP communications with execution of the EC algorithm.

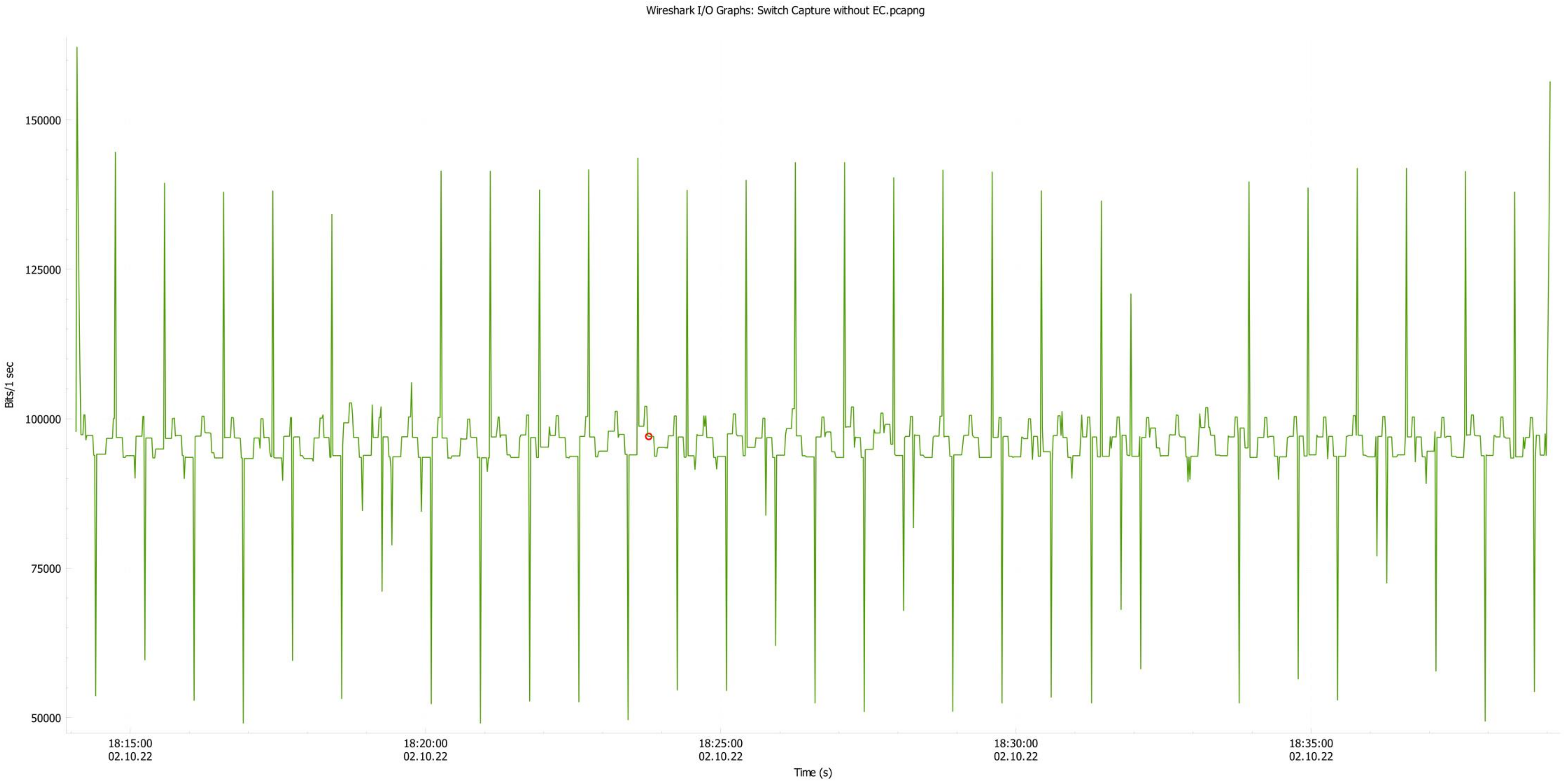


Figure 5.11: Bandwidth usage of XMPP communications without execution of the EC algorithm.

The latency is calculated from the time delay between consecutive packets in a TCP stream, which can be displayed using the filter expression “tcp.time-delta”. The I/O Graphs tool computes and plots the average latency values for each case as shown in figures 5.12 and 5.13 below.

A key feature of I/O Graphs is that, it allows for exporting the plots to a Comma Separated Values (CSV) format which can be further analysed using Microsoft Excel. Consequently, Microsoft Excel was used to calculate the average “arithmetic mean” of data values for bandwidth usage, and to determine the maximum latency recorded in each case. The bandwidth and latency results for each case are listed in table 5.1 below.

Table 5.1: **The QoS results for the two test cases.**

QoS parameter	With EC algorithm	Without EC algorithm	Impact
Average Bandwidth (bits/s)	95742.26	96132.77	390.51
Maximum Delay (s)	8.09644	8.53397	0.43753

From the results in table 5.1 above, the impact of the EC algorithm on the communication QoS is detected. The following section presents points of discussion on the testbed simulations, the recorded results, and the impact of EC on communication QoS.

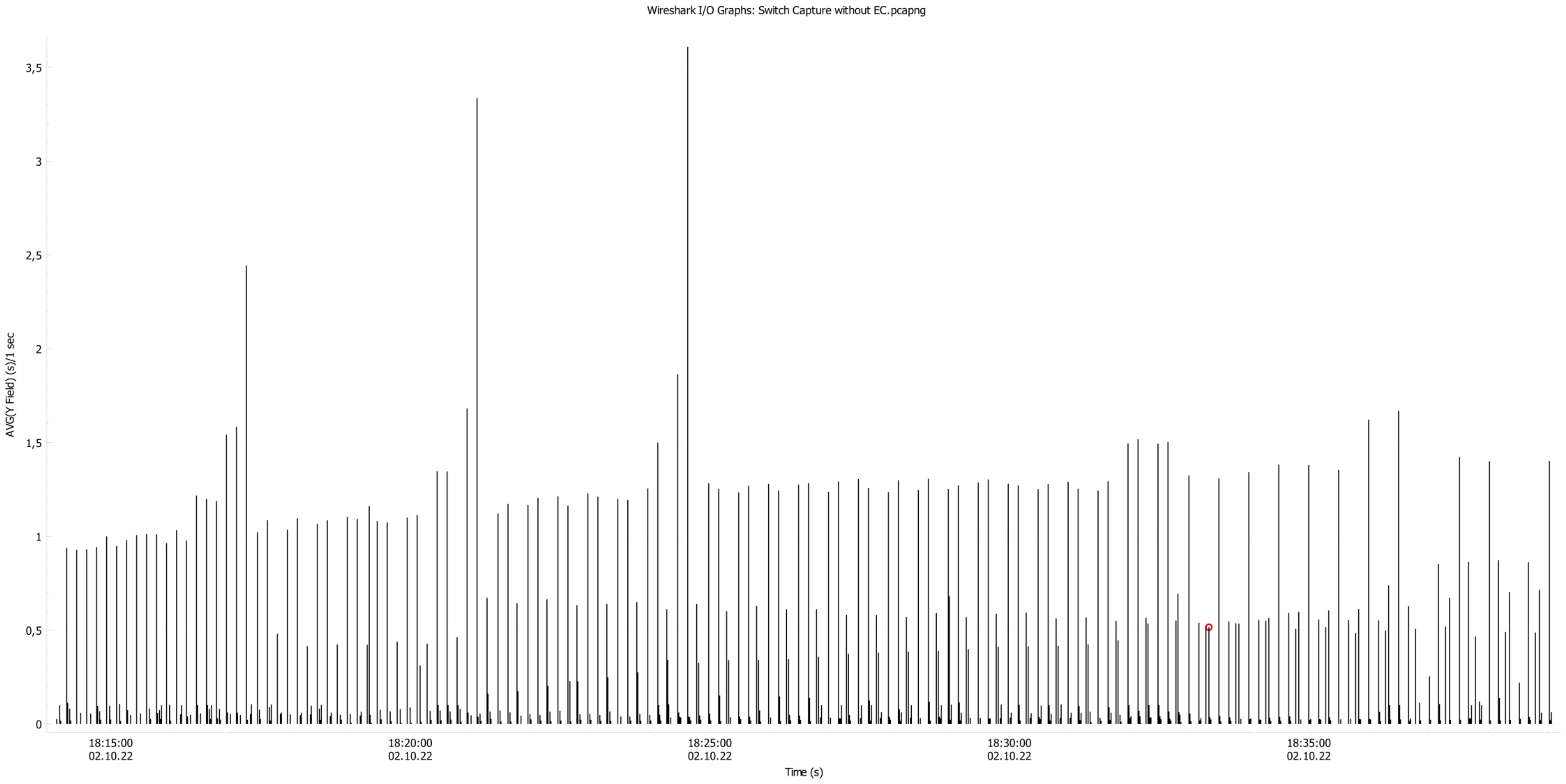


Figure 5.12: Average latencies in the TCP stream of the network traffic without the EC algorithm.

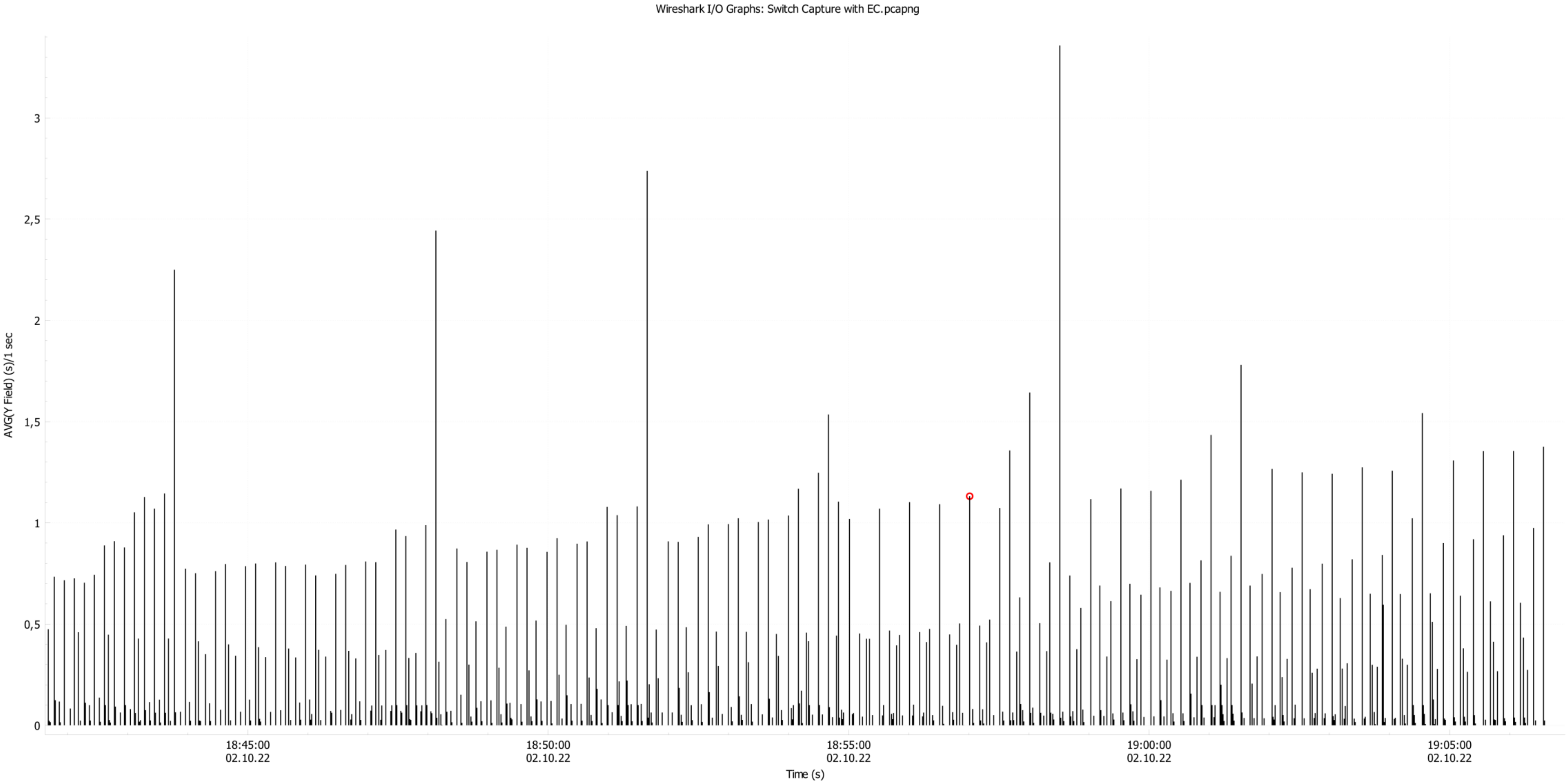


Figure 5.13: Average latencies in the TCP stream of the network traffic with the EC algorithm.

5.6 Discussion

Substantiated by the results of QoS metrics from Wireshark, the impact of EC was observed to be a reduction of ‘340.9 bits/s’ for bandwidth usage and ‘0.437 seconds’ for latency. It is noted that, the impact is a reasonably small amount which is due to several factors. The exchanged data in the testbed is objectively a minor amount compared to real-life applications, because it consists of only twelve data tags transmitted via GOOSE and enveloped in IEC 61850 MMS and XMPP headers according to IEC 61850-8-2. This can be recognized from the bandwidth usage without execution of the EC algorithm which is slightly over ‘96’ Kbits/s.

As previously explained in section 5.5.2, the latency is calculated based-on the time delay between consecutive packets in a single TCP stream, between each client and the XMPP server. Wireshark provides this important measurement because it represents the RTT for a data packet in a TCP conversation between client/server. This value is not an E2E latency “between PC-1 and PC-3”, it is rather an E2M latency between ‘PC-2’ and either ‘PC-1’ or ‘PC-3’. However, it provides a measure for the latency in the network.

5.7 Conclusions

The chapter presented an analysis of IEC 61850-8-2 XMPP communications in the developed testbed using Wireshark packet-capturing software. Initially, the data exchange and cybersecurity mechanisms of the XMPP standard were examined. Thereafter, a description was provided for the data fusion algorithm, which was developed to reduce the amount of transmitted data over the network. The simulation captions of the EC gateway model were illustrated to verify the impact of the algorithm to reduce the transmitted data tags from twelve to six. Furthermore, a Wireshark-based evaluation of the EC algorithm’s impact on the communication QoS was outlined. The methodology of the evaluation consisted of capturing data traffic for an equal period of time with and without execution of the EC algorithm.

Wireshark I/O Graphs and Microsoft Excel were applied to analyze bandwidth usage and latency for both test cases and the results were provided. The impact of executing the EC algorithm was observed. From the analysis, it was noticed that, the impact was comparatively small due to the limited capacity of the lab-scale testbed. However, the EC impact can be scaled to real-life applications where large data are being exchanged and transmitted over the network.

CHAPTER SIX
CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

The RESs are operated in many forms and structures within smart grids such as DERs, microgrids, and VPPs. The management and coordination of DERs' operations pose various significant challenges including interoperability between multi-vendor equipment, complex integration process, and large data that need to be exchanged over communication networks. Furthermore, cybersecurity challenges arise from deployment of DERs communication systems over public IP-based WANs. Hence, the effective and reliable management of DERs systems relies heavily on communication system performance.

The research project investigated solutions for the abovementioned challenges by studying and implementing IEC 61850 standards in a DER communication system. The IEC 61850 standards have achieved massive success in solving interoperability concerns due to the object-oriented modelling of power systems and DERs functions. The cybersecurity vulnerabilities over WANs are addressed by specifying the open-source messaging protocol "XMPP" as the middleware for WANs communication. The XMPP standard was chosen by the IEC due to its high scalability and strong cybersecurity mechanisms. The big data which are transmitted from DER sites cause overusage of the network bandwidth, which negatively impacts communication performance.

The research project explored the implementation of the EC concept from the IoT paradigm to minimize data traffic over networks. The research study involved a lab-scale testbed implementation of a monitoring scheme for a power network integrated to a DER utilizing an EC gateway model that reduces the amount of data transmitted over communication networks. Moreover, the gateway model performs integration of a LAN to a WAN by utilizing IEC 61850-8-1 GOOSE, MMS, and IEC 61850-8-2 XMPP standards. A model of a power network integrated with a wind energy DER, was developed, modified, and implemented on RTDS. The EC gateway model consists of RTAC SEL-3555 and IEC 61850 communication drivers from Elipse software™. Analysis and evaluation of the communication performance was done using Wireshark software that captured the data traffic in the network.

The chapter summarizes the conducted research study which has successfully achieved the outlined aims and objectives. Section 6.2 reports the thesis deliverables and section 6.3 highlights the recommendations for future work.

6.2 Thesis deliverables

The section outlines the outcomes of the research study, listing publications from the thesis outcomes, and describing academic and industrial uses of the research componenets and outcomes. In addition, the section describes the reseach works that were performed to achieve the research aims and objectives.

6.2.1 Publication

A paper titled “An IEC 61850 standard-based EC algorithm to enhance communications in modern power systems” by authors, A. Adam, M. Mnguni, and M. Ratshitanga has been submitted and accepted to the 31st annual IEEE SAUPEC conference, and it will be published after the conference proceedings in January 2023.

6.2.2 Academic and industrial applications

In the thesis, a testbed for a monitoring scheme was developed. The wind energy DER model simulated on RTDS forms a solid basis for further research on wind turbines power generation. The IEC 61850-8-1 MMS and IEC 61850-8-2 XMPP communication drivers from Elipse software™ are one of the first implementations of the IEC 61850 standard in the market of SCADA software. The product has massive potential for building IEC 61850-compliant SCADA monitoring and control applications especially for modern power system networks with integrated DERs.

The RTAC SEL-3555 unit is an extremely powerful micro-computer utilized in the industry to implement complex control algorithms on top of its capabilities as a protocol gateway. The developed algorithm on RTAC SEL-3555 forms a basis for understanding the concept of EC from the perspective of reducing data volumes. Hence, this work represents a foundation for more research and development of EC schemes for smart grid applications.

6.2.3 Literature review

The literature review in the research study covered numerous sources such as journal papers, conference proceedings, and books. The review was conducted on communication systems in smart grids with a focus on DERs. The review has identified the critical QoS requirements for communication systems in smart grids and the latest trends in the used technologies to build these systems. Furthermore, the review provided theoretical information on DER systems, and a background on the main research problem was outlined, which is the impacts of communication systems performance on the operations of smart grids and DER systems. In addition, standardization was identified as a key requirement in DER systems. The review focused on IEC 61850 and the factors that impact its communication performance in WANs. Thereafter, the XMPP standard was reviewed as the standardized middleware “IEC 61850-8-2” to enable communications over WANs. Finally, the applications of IEC 61850-8-2 XMPP in DER systems were reviewed.

6.2.4 Theoretical background on Internet of Things

A brief introduction of the IoT concept was provided in the research study, it covered common architectures of IoT networks that comprises multiple computation layers including cloud, fog, and edge. An emphasis was made on the EC features, structure and numerous benefits in terms of reducing the computation and communication loads in IoT networks. Thereafter, applications of IoT and EC in smart grids were discussed and highlighting the massive potential of these technologies to improve the performance of smart grids in their various domains including generation, transmission, and distribution.

6.2.5 Implementation of a lab-scale testbed

The thesis presented an implementation of a monitoring scheme of a DER model. The scheme composes of an EC gateway, IEC 61850, and XMPP standards. Different hardware and software components were utilized including RTDS, RTAC SEL-3555, and Elipse Power software. The configuration of each component was described in details. Starting with the wind energy model on RTDS, and the configuration of IEC 61850 GOOSE communications. Thereafter, the gateway model was described which consists of the RTAC SEL-3555 unit along with the Elipse Power communication drivers.

The RTAC SEL-3555 unit was configured to subscribe to GOOSE messages from RTDS, and the RTAC SEL-3555’s IEC 61850 information model was designed to enable MMS communications with the other component in the EC gateway model. Two IEC 61850 communication drivers on Elipse Power were configured to achieve the integration of the LAN to a WAN. An MMS client driver was configured to communicate to RTAC SEL-3555 according to IEC 61850-8-1 MMS standard and polls data over a LAN connection. The second driver was configured as an IEC 61850-8-2 XMPP server and set to communicate to an IEC 61850-8-2 XMPP client driver over an IP-based WAN. The Openfire XMPP server application on ‘PC-2’ was described including the configuration and creation of users for the client/server drivers.Finally, an Elipse Power IEC 61850-8-2 client driver was configured on ‘PC-3’ to communicate . The testbed configurations were completed successfully, and the data was received in ‘PC-3’.

6.2.6 Analysis of IEC 61850-8-2 XMPP

Wireshark was utilized to capture the network traffic that was analyzed to examine the data exchange and cybersecurity mechanisms of the IEC 61850-8-2 XMPP standard. This visual analysis was in conjunction with the theoretical description of the standard. It serves to consolidate the theoretical study and strengthen the understanding of the important XMPP standard.

6.2.7 Evaluation of edge computing impact on communication Quality of Service

The research study presented an evaluation of the EC impact on communication QoS in terms of bandwidth usage and latency. The evaluation was based-on comparing these parameters in two test cases, with and without the execution of the data fusion algorithm. The algorithm was developed on RTAC SEL-3555 which is the intelligent component of the EC gateway model. The algorithm effectively reduces data volume that is transmitted over the network. The impact of the algorithm was observed from the test results and indicated a minor improvement due to the volume of the exchanged data in the testbed. Conversely, if scaled to larger data volumes, the impact can be rather significant.

6.3 Recommendations and future work

The research study forms a solid basis for more future work. The following points describe suggestions for future research and modifications which can be applied:

- RTDS enables the use of IEC 61850-8-1 MMS for communications via the latest version of the GTNET card “GTNETx2”. This will eliminate the need for using GOOSE to transfer analog values from the DER model, which will save processing time of GOOSE and mapping to MMS performed by RTAC SEL-3555.
- The application of IEC 61850-8-2 can be further extended to include control schemes that involve sending control commands over a WAN and investigating the effects of communication QoS on the scheme.
- E2E latency can be obtained utilizing the Elipse Power SCADA application. In addition, HMI screens can be developed using the software to visualize the monitoring scheme. Furthermore, the testbed can be examined using various WAN technologies to obtain more clarity on impacts of EC on communications QoS.
- Future research works involve applying the scalability of XMPP by implementing more than one IEC 61850-8-2 XMPP server which will forward data to a single IEC 61850-8-2 XMPP client in a distant control centre.

REFERENCES

A. Melnikov. 2006. RFC 4422 - Simple Authentication and Security Layer (SASL). https://datatracker.ietf.org/doc/html/rfc4422 22 April 2022.

Adamiak, M., Baigent, D. & Mackiewicz, R. 2009. IEC 61850 Communication Networks and Systems In Substations: An Overview for Users IEC 61850 Communication Networks and Systems In Substations: An Overview for Users.

Adefarati, T. & Bansal, R.C. 2016. Integration of renewable distributed generators into the distribution system: A review. IET Renewable Power Generation, 10(7): 873–884.

Aftab, M.A., Hussain, S.M.S., Ali, I. & Ustun, T.S. 2018. IEC 61850 and XMPP communication based energy management in microgrids considering electric vehicles. IEEE Access, 6: 35657–35668.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials, 17(4): 2347–2376.

Ali, I., Member, Senior, Suhail Hussain, S.M. & Member, Student. 2014. IEC 61850-7-420 based Communication Configuration to Integrate DER to Distribution System.

Ali, I. & Suhail Hussain, S.M. 2018. Communication Design for Energy Management Automation in Microgrid. IEEE Transactions on Smart Grid, 9(3): 2055–2064.

Ancillotti, E., Bruno, R. & Conti, M. 2013. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. Computer Communications, 36(17–18): 1665–1697.

ANDES. 2022. ANDES documentation — ANDES 1.8.3.post9+g21d7bbf7 documentation. ANDES documentation. https://docs.andes.app/en/latest/ 29 November 2022.

Aslett, M. 2019. Data Analytics at the Edge.

Bhattarai, B., Marinovici, L., Touhiduzzaman, M., Tuffner, F.K., Schneider, K.P., Xie, J., Mana, P.T., Du, W. & Fisher, A. 2020. Studying impacts of communication system performance on dynamic stability of networked microgrid. IET Smart Grid, 3(5): 667–676.

Bouhafs, F. & Merabti, M. 2011. Managing communications complexity in the smart grid using data aggregation. In Dummy Source Innodata. Institute of Electrical and Electronics Engineers Inc.: 1315–1320.

Chang, L., Saydaliev, H.B., Meo, M.S. & Mohsin, M. 2022. How renewable energy matter for environmental sustainability: Evidence from top-10 wind energy consumer countries of European Union. Sustainable Energy, Grids and Networks, 31.

Chen, S., Wen, H., Wu, J., Lei, W., Hou, W., Liu, W., Xu, A. & Jiang, Y. 2019. Internet of Things Based Smart Grids Supported by Intelligent Edge Computing. IEEE Access, 7: 74089–74102.

Cho, C.S., Chen, W.G., Liao, C.K.C., Liao, J.L., Chen, F.F. & Shen, T.C. 2019. Building on the distributed energy resources IoT based IEC 61850 XMPP for TPC. Proceedings - 2019 IEEE International Conference on Industrial Cyber Physical Systems, ICPS 2019: 61–66.

Choobkar, S. & Rahmani, M. 2019. Communication Routes for DER Interconnection with Power Grid. In 34th International Power System Conference, PSC 2019. Institute of Electrical and Electronics Engineers Inc.: 696–701.

Elipse Software Ltda. 2021. Elipse Power User’s Guide.

Elipse Software Ltda. 2022. IEC 61850 Driver v3.0.31.

Elipse Software Ltda. 2019. IEC61850 Server Driver v1.0.4.

Etherden, N., Vyatkin, V. & Bollen, M.H.J. 2016. Virtual Power Plant for Grid Services Using IEC 61850. IEEE Transactions on Industrial Informatics, 12(1): 437–447.

Falk, H. & Burns, M. 1997. MMS and ASN.1 Encodings Simple Examples and Explanations on How to Crack an MMS PDU MMS and ASN.1.

Ghanem, K., Asif, R., Ugwuanyi, S. & Irvine, J. 2020. Bandwidth and security requirements for smart grid. In IEEE PES Innovative Smart Grid Technologies Conference Europe. IEEE Computer Society: 36–40.

Gonzalez-Redondo, M.J., Moreno-Munoz, A., Pallares-Lopez, V. & Real-Calvo, R.J. 2016. Influence of data-related factors on the use of IEC 61850 for power utility automation. Electric Power Systems Research, 133: 269–280.

Hänsch, K., Naumann, A., Wenge, C. & Wolf, M. 2018. Communication for battery energy storage systems compliant with IEC 61850. International Journal of Electrical Power and Energy Systems, 103: 577–586.

Honeth, N., Yiming, W., Etherden, N. & Nordström, L. 2011. Application of the IEC 61850-7-420 data model on a hybrid renewable energy system. In 2011 IEEE PES Trondheim PowerTech: The Power of Technology for a Sustainable Society, POWERTECH 2011.

Hornsby, A., Belimpasakis, P. & Defee, I. 2009. XMPP-based wireless sensor network and its integration into the extended home environment. Digest of Technical Papers - IEEE International Conference on Consumer Electronics: 794–797.

Huang, R., Shi, W., Yao, D., Chu, C.C., Gadh, R., Song, Y. jin & Sung, Y. dong. 2016. Design and implementation of communication architecture in a distributed energy resource system using IEC 61850 standard. International Journal of Energy Research, 40(5): 692–701.

Huang, W. 2018. A Practical Guide of Troubleshooting IEC 61850 GOOSE Communication. In Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference. Institute of Electrical and Electronics Engineers Inc.

Huang, Y., Lu, Y., Wang, F., Fan, X., Liu, J. & Leung, V.C.M. 2018. An Edge Computing Framework for Real-Time Monitoring in Smart Grid. In Proceedings - 2018 IEEE International Conference on Industrial Internet, ICII 2018. Institute of Electrical and Electronics Engineers Inc.: 99–108.

Hussain, S.M.S., Aftab, M.A. & Ali, I. 2018. IEC 61850 Modeling of DSTATCOM and XMPP Communication for Reactive Power Management in Microgrids. IEEE Systems Journal, 12(4): 3215–3225.

IEC. 2004. Communication networks and systems in substations-Part 8-1: Specific Communication Service Mapping (SCSM)-Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. www.iec.ch/searchpub.

IEC TC57. 2007. Power systems management and associated information exchange-Data and communications security Part 1: Communication network and system security-Introduction to security issues. www.iec.ch.

Ignite Realtime. 2022. Ignite Realtime: Openfire Server. Openfire Server. https://www.igniterealtime.org/projects/openfire/ 29 August 2022.

ITU-T. 2001. ITU-T Information technology-ASN.1 encoding rules: XML Encoding Rules (XER). TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU .

Jun, H.J. & Yang, H.S. 2021. Performance of the xmpp and the mqtt protocols on iec 61850-based micro grid communication architecture. Energies, 14(16): 1–13.

Kampars, J., Tropins, D. & Matisons, R. 2021. A Review of Application Layer Communication Protocols for the IoT Edge Cloud Continuum. ITMS 2021 - 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University, Proceedings, (1): 1–6.

Keserica, H., Sučić, S. & Capuder, T. 2019. Standards-compliant chat-based middleware platform for smart grid management. Energies, 12(4).

Kirsche, M. & Klauck, R. 2012. Unify to bridge gaps: Bringing XMPP into the Internet of Things. 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2012, (March): 455–458.

Kolenc, M., Suljanovic, N., Nemcek, P. & Zajc, M. 2016. Monitoring communication QoS parameters of distributed energy resources. In 2016 IEEE International Energy Conference, ENERGYCON 2016. Institute of Electrical and Electronics Engineers Inc.

Kuntschke, R., Winter, M., Glomb, C. & Specht, M. 2017. Message-oriented machine-to-machine communication in smart grids: An Approach for and Experiences from Mapping IEC 61850 and CIM to XMPP. Computer Science - Research and Development, 32(1–2): 131–145.

Lehnhoff, S., Rohjans, S., Mahnke, W. & Uslar, M. 2011. IEC 61850 based OPC UA communication-The future of smart grid automation Technische und ökonomische Machbarkeit Energetischer Nachbarschaften View project Monitoring and Management System for Smart Distribution Networks View project IEC 61850 based OPC UA Communication-The Future of Smart Grid Automation. In 17th Power Systems Computation Conference - Stockholm Sweden. https://www.researchgate.net/publication/267561083.

Li, J., Gu, C., Xiang, Y. & Li, F. 2021. Edge-Cloud Computing Systems for Smart Grid: State-of-the-Art, Architecture and Applications. JOURNAL OF MODERN POWER SYSTEMS AND CLEAN ENERGY.

Liang, Y. & Campbell, R.H. 2008. Understanding and Simulating the IEC 61850 Standard Understanding and Simulating the IEC 61850 Standard. https://www.researchgate.net/publication/32964907.

Liao, Y. & He, J. 2020. Optimal smart grid operation and control enhancement by edge computing. In 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2020. Institute of Electrical and Electronics Engineers Inc.

Liu, C.H. & Gu, J.C. 2019. Modeling and integrating pv stations into IEC 61850 XMPP intelligent edge computing gateway. Energies, 12(8).

Mao, M., Mei, F., Jin, P. & Chang, L. 2014. Application of IEC61850 in energy management system for microgrids. In 2014 IEEE 5th International Symposium on Power Electronics for Distributed Generation Systems, PEDG 2014. IEEE Computer Society.

Marzal, S., Salas, R., González-Medina, R., Garcerá, G. & Figueres, E. 2018. Current challenges and future trends in the field of communication architectures for microgrids. Renewable and Sustainable Energy Reviews, 82: 3610–3622.

Mercurio, A., Di Giorgio, A. & Cioci, P. 2009. Open-source implementation of monitoring and controlling services for EMS/SCADA systems by means of web services-IEC 61850 and IEC 61970 standards. IEEE Transactions on Power Delivery, 24(3): 1148–1153.

Nadeem, F., Aftab, M.A., Suhail Hussain, S.M., Ali, I., Tiwari, P.K., Goswami, A.K. & Ustun, T.S. 2019. Virtual power plant management in smart grids with XMPP based IEC 61850 communication. Energies, 12(12).

Okuno, Y., Arai, Y., Hoshi, Y., Henmi, H., Otani, T. & Ohba, E. 2016. XMPP-based energy management system architecture for communications systems. INTELEC, International Telecommunications Energy Conference (Proceedings), 2016-Septe: 1–6.

Panda, D.K. & Das, S. 2021. Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. Journal of Cleaner Production, 301.

Pourmirza, Z., Walker, S. & Brooke, J. 2021. Data reduction algorithm for correlated data in the smart grid. IET Smart Grid, 4(5): 474–488.

Prajeesha & Anuradha, M. 2021. EDGE Computing Application in SMART GRID-A Review. In Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESC 2021. Institute of Electrical and Electronics Engineers Inc.: 397–402.

Pramudhita, A.N., Asmara, R.A., Siradjuddin, I. & Rohadi, E. 2018. Internet of Things Integration in Smart Grid. In Proceedings - 2018 International Conference on Applied Science and Technology, iCAST 2018. Institute of Electrical and Electronics Engineers Inc.: 718–722.

RTDS. 2022. Hardware – RTDS Technologies. https://knowledge.rtds.com/hc/en-us/categories/360002176414-Hardware 20 July 2022.

RTDS. 2012. Real Time Digital Simulator (RTDS) Power System User’s Manual.

RTDS. 2019. RSCAD Controls Library Manual.

RTDS. 2008. Simulating the Manitoba Hydro power system using RTDS, Modelling St. Leon Wind Farm.

Saint-Andre, P. 2011. Extensible Messaging and Presence Protocol (XMPP): Core. https://datatracker.ietf.org/doc/html/rfc6120 5 April 2022.

Saleem, M.U., Usman, M.R., Usman, M.A. & Politis, C. 2022. Design, Deployment and Performance Evaluation of an IoT Based Smart Energy Management System for Demand Side Management in Smart Grid. IEEE Access, 10: 15261–15278.

Saleh, M., Esa, Y. & Mohamed, A. 2019. Impact of Communication Latency on the Bus Voltage of Centrally Controlled DC Microgrids during Islanding. IEEE Transactions on Sustainable Energy, 10(4): 1844–1856.

Samie, F., Bauer, L. & Henkel, J. 2019. Edge computing for smart grid: An overview on architectures and solutions. In Power Systems. Springer Verlag: 21–42.

Sanchez, O.F.A., Reina, G. & Mauledoux, M. 2018. Modeling a microgrid that integrates renewable energies in IEC 61850-7-420 and IEC 61400-25-3. Journal of Engineering Science and Technology Review, 11(4): 174–179.

Saraiva, D.M., Corujo, D. & Aguiar, R.L. 2019. IEC 61850 Data Transfer Evaluation over Public Networks. In International Symposium on Wireless Personal Multimedia Communications, WPMC. IEEE Computer Society.

Sayed, K. & Gabbar, H.A. 2017. Scada and smart energy grid control automation.

Schmutzler, J., Gröning, S. & Wietfeld, C. 2011. Management of distributed energy resources in IEC 61850 using web services on devices. In 2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011. 315–320.

Schweitzer Engineering Laboratories Inc. 2011. ACSELERATOR RTAC ® SEL-5033 Software Instruction Manual 20210713 *PM5033-01-NB*.

Schweitzer Engineering Laboratories Inc. 2018. Instruction Manual SEL-3555-2 Instruction Manual 20210720 Real-Time Automation Controller (RTAC).

Sharma, S.K. & Wang, X. 2017. Live Data Analytics with Collaborative Edge and Cloud Processing in Wireless IoT Networks. IEEE Access, 5: 4621–4635.

Shin, I.J., Song, B.K. & Eom, D.S. 2016. Auto-mapping and configuration method of IEC 61850 information model based on OPC UA. Energies, 9(11).

Sirojan, T., Lu, S., Phung, B.. & Ambikairajah, E. 2019. Embedded Edge Computing for Real-time Smart Meter Data Analytics. In 2019 International Conference on Smart Energy Systems and Technologies (SEST).

Skirelis, J. & Navakauskas, D. 2018. Classifier based Gateway for Edge Computing. In 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE) : proceedings of the 6th IEEE workshop : November 8-10, 2016, Vilnius, Lithuania.

Timbus, A., Larsson, M. & Yuen, C. 2008. Integration of Wind Energy Resources in the UtilityControl and Information Technology Infrastructures. In IEEE International Symposium on Industrial Electronics, 2008. ISIE 2008. . I E E E.

Tito, S.R., Soltic, S., Parkash, B., Rehman, A.U., Nieuwoudt, P., Aslam, S., Lie, T.T., Pandey, N. & Ahmed, M.D. 2021. Is Edge Computing the Answer for Smart Building Energy

Management System? In ICT-PEP 2021 - International Conference on Technology and Policy in Energy and Electric Power: Emerging Energy Sustainability, Smart Grid, and Microgrid Technologies for Future Power System, Proceedings. Institute of Electrical and Electronics Engineers Inc.: 378–383.

Tseng, M., Edmunds, T. & Canaran, L. 2018. Introduction to Edge Computing in IIoT. www.iiconsortium.org/IISF.

Ullah, M., Narayanan, A., Wolff, A. & Nardelli, P. 2021. Smart Grid Information Processes Using IoT and Big Data with Cloud and Edge Computing.

Ustun, T.S. & Hussain, S.M.S. 2020. IEC 62351-4 Security Implementations for IEC 61850 MMS Messages. IEEE Access, 8: 123979–123985.

Ustun, T.S., Ozansoy, C. & Zayegh, A. 2011. Extending IEC 61850-7-420 for distributed generators with fault current limiters. In 2011 IEEE PES Innovative Smart Grid Technologies, ISGT Asia 2011 Conference: Smarter Grid for Sustainable and Affordable Energy Future.

Vallejo, A., Zaballos, A., Selga, J.M. & Dalmau, J. 2012. QOS CONTROL NEEDS IN THE SMART GRIDS. IEEE Communications Magazine (Volume: 50, Issue: 5, May 2012): 128–134.

Veichtlbauer, A., Parfant, M., Langthaler, O., Andren, F.P. & Strasser, T. 2016. Evaluating XMPP communication in IEC 61499-based distributed energy applications. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, 2016-Novem.

Wang, H., Xiong, D., Wang, P. & Liu, Y. 2017. A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices. IEEE Access, 5: 16393–16405.

Wang, Q., Pipattanasomporn, M., Kuzlu, M., Tang, Y., Li, Y. & Rahman, S. 2016. Framework for vulnerability assessment of communication systems for electric power grids. IET Generation, Transmission and Distribution, 10(2): 477–486.

Wang, W., Fang, X. & Florita, A. 2021. Impact of der Communication Delay in AGC: Cyber-Physical Dynamic Co-simulation. In Conference Record of the IEEE Photovoltaic Specialists Conference. Institute of Electrical and Electronics Engineers Inc.: 2616–2620.

Wong, T.Y., Lau, W.H., Chung, H.S.H. & Shum, C. 2022. A feasibility study of using Manufacturing Message Specification report gateway model for IEC61850 inter-substation type-1 messaging over Wide Area Network. Sustainable Energy, Grids and Networks, 30.

Worighi, I., Maach, A., Hafid, A., Hegazy, O. & Van Mierlo, J. 2019. Integrating renewable energy in smart grid system: Architecture, virtualization and analysis. Sustainable Energy, Grids and Networks, 18.

Yan, Y., Qian, Y., Sharif, H. & Tipper, D. 2013. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE Communications Surveys and Tutorials, 15(1): 5–20.

Yang, C., Chen, X., Liu, Y., Zhong, W. & Xie, S. 2019. Efficient Task Offloading and Resource Allocationfor Edge Computing-based Smart Grid Network. In ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE.

Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J. & Yang, X. 2017. A Survey on the Edge Computing for the Internet of Things. IEEE Access, 6: 6900–6919.

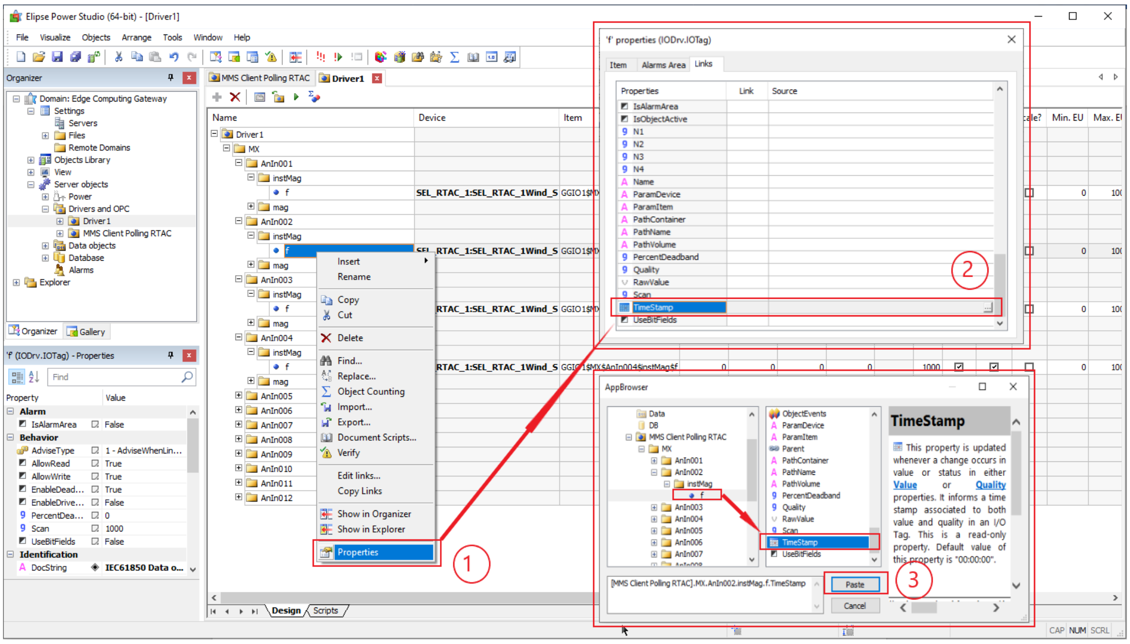
Zanabria, C., Andren, F., Leimgruber, F., Brundlinger, R. & Strasser, T. 2015. A low cost open source-based IEC 61850/61499 automation platform for distributed energy resources. In 2015 IEEE Eindhoven PowerTech, PowerTech 2015. Institute of Electrical and Electronics Engineers Inc.

Zeinali, M. & Thompson, J. 2021. Comprehensive practical evaluation of wired and wireless internet base smart grid communication. IET Smart Grid, 4(5): 522–535.

Zwartscholten, J., Klaes, M., Gonzalez, D.M., Subhan, F., Narayan, A. & Rehtanz, C. 2020. Impact of increased ICT latency on active distribution network control. In 6th IEEE International Energy Conference, ENERGYCon 2020. Institute of Electrical and Electronics Engineers Inc.: 864–869.

APPENDIX

Testbed Information



[MMS Client Polling RTAC].MX.AnIn002.instMag.f.TimeStamp

TimeStamp

This property is updated whenever a change occurs in value or status in either Value or Quality properties. It informs a time stamp associated to both value and quality in an I/O Tag. This is a read-only property. Default value of this property is "00:00:00".

Figure A.1: Linking timestamps of the IEC 61850-8-2 XMPP server driver objects to the IEC 61850-8-1 MMS client driver objects.

Table A.1: Technical Specifications of Vestas V82 wind turbines (RTDS, 2008).

Parameter	Value
Rotor Blade Radius	41 m
Hub height above ground	80 m
Wind Speed (cut−in/nominal/cut−out)	3.5 / 13 / 20 m/s 12.6 / 46.8 / 72 km/hr
Nominal turbine speed	14.4 rpm
Rated Power	1.65 MW
Rated MVA	1.808 MVA
Induction machine	6 pole, 1200 rpm
Induction machine speed at rated power	1214 rpm
Rated slip	0.01167
Gear box ratio	84.5

Table A.2: **Technical specifications of the induction generator model (RTDS, 2008).**

Parameter	Value
3 phase MVA rating	1.808
Terminal voltage	0.6 kV rms
1 per unit impedance	0.1991 ohms
Stator Leakage reactance	0.0697 pu
Stator resistance	0.0077 pu
Rotor leakage reactance	0.0834 pu
Rotor resistance	0.0062 pu

Table A.3: **Signal names of the data tags under the monitoring scheme**

Parameter	Value
Generator’s busbar phase A voltage	STLWT1a
Generator’s busbar phase B voltage	STLWT1b
Generator’s busbar phase C voltage	STLWT1c
Wind Gusts value	GUST
Computed Air Density	airdensity
Wind speed in Km/hr	windkph
Hub Speed in rad/sec	HUBSPD
Turbine Power in Mega Watts	pwrturb
Blades Pitch degree	pitchdeg
Rotor Speed in pu	STLWT1SPD
Stator active power (P) in Mega Watts	STLWT1P
Stator reactive power (Q) in Mega VAR	STLWT1Q

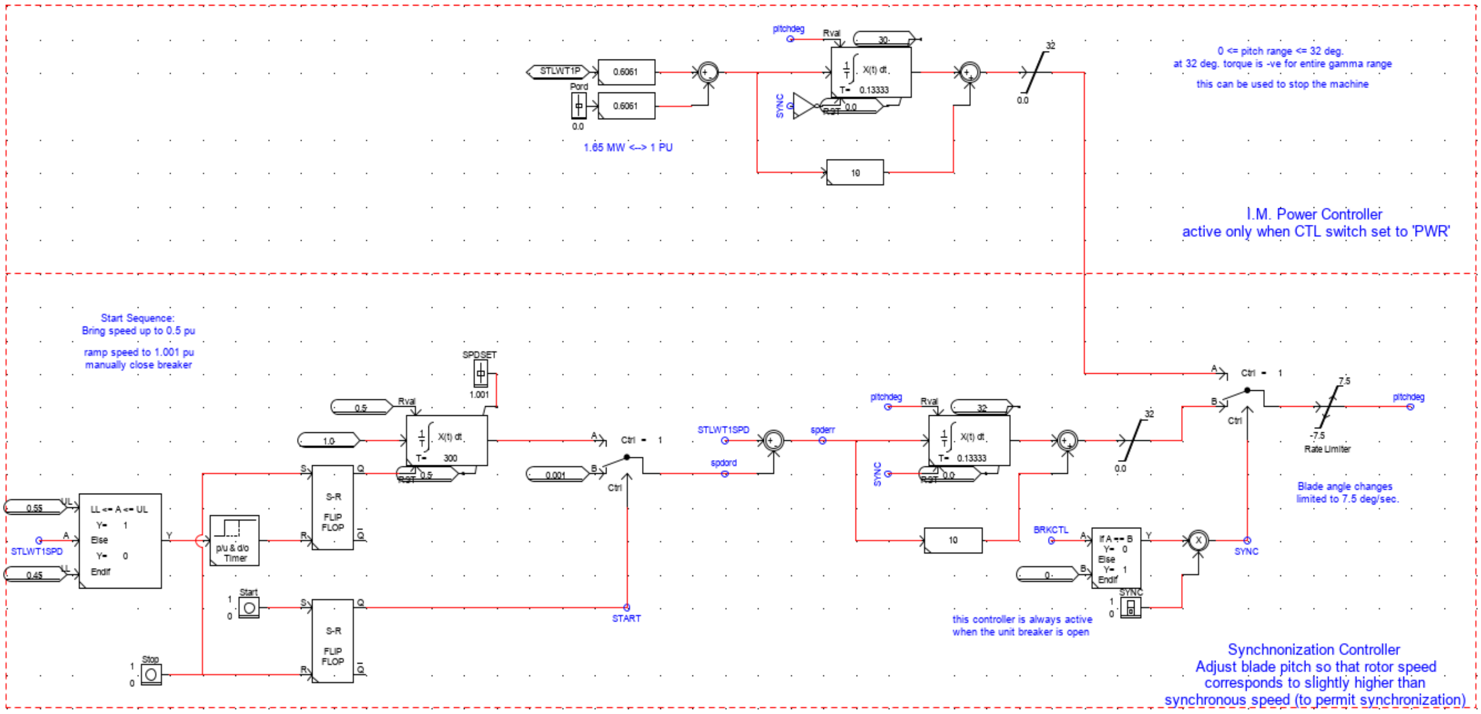


Figure A.2: Turbine pitch angle control loops.

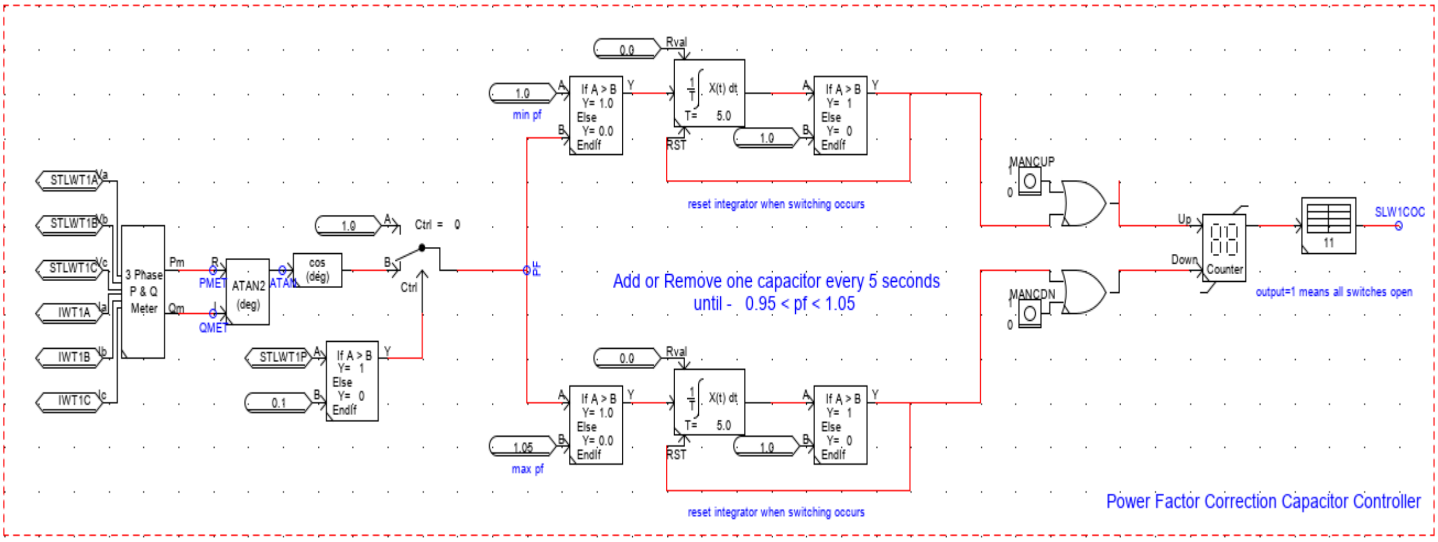
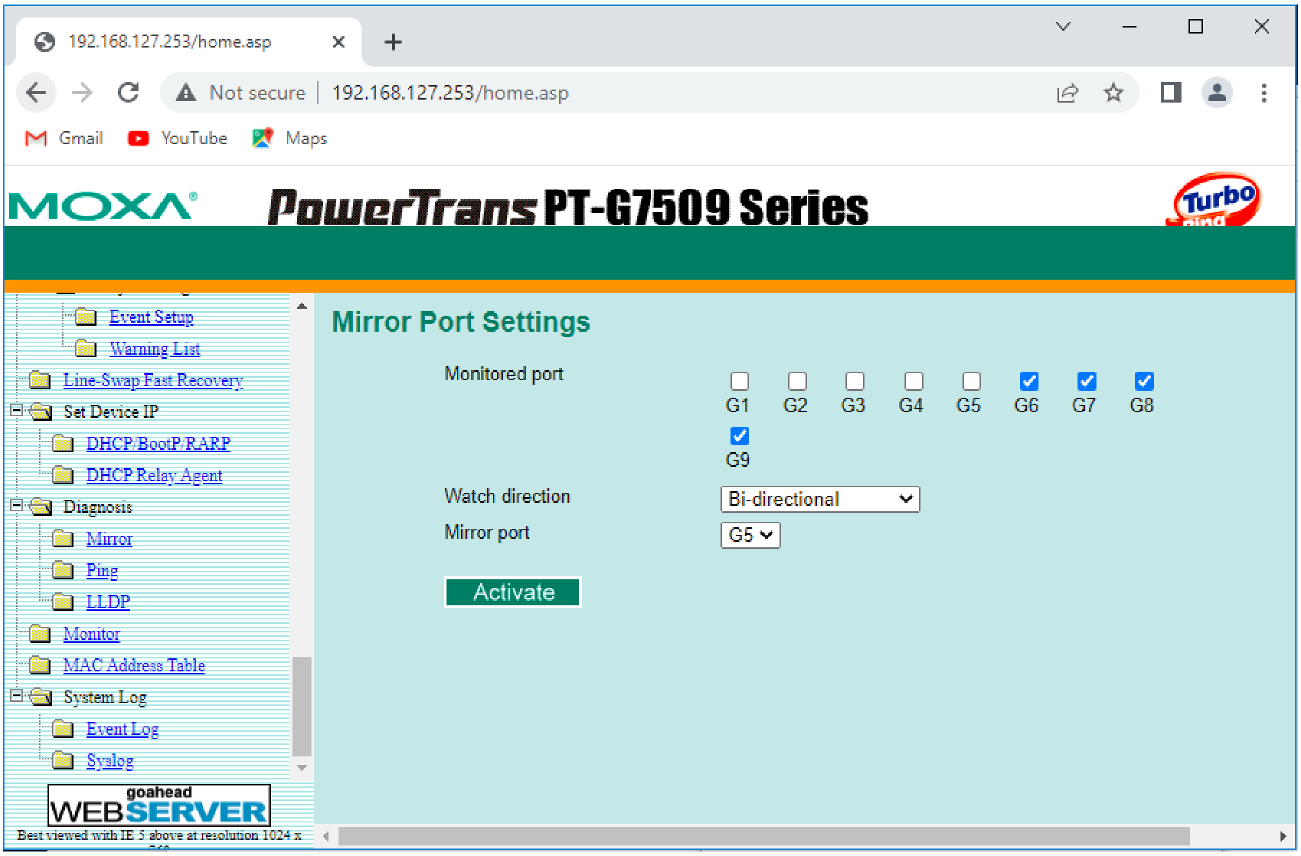


Figure A.3: Power factor control loop.



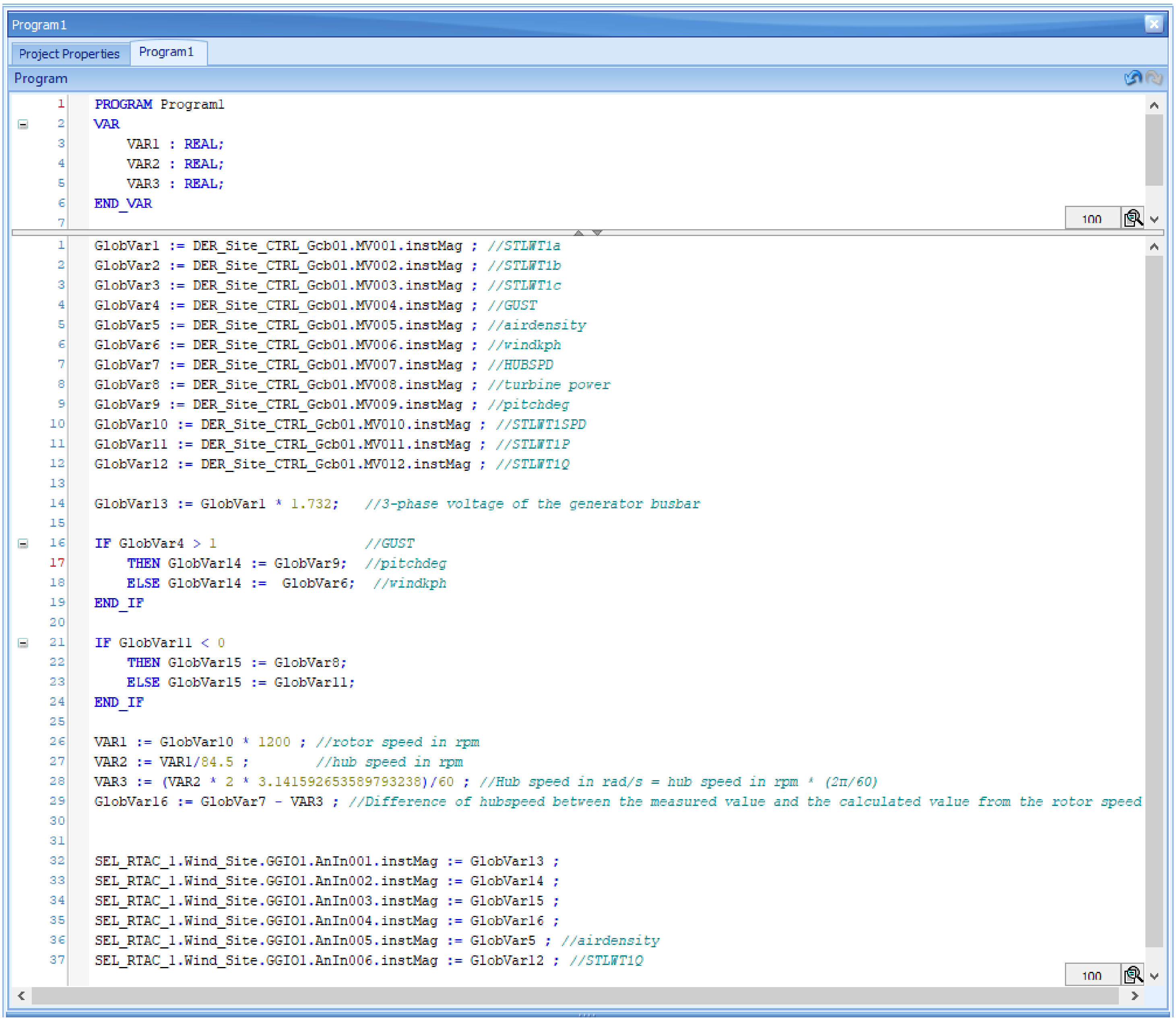
Mirror Port Settings

Monitored port: ☐ G1 ☐ G2 ☐ G3 ☐ G4 ☐ G5 ☑ G6 ☑ G7 ☑ G8 ☑ G9

Watch direction: Bi-directional

Mirror port: G5

Figure A.4: Mirror port activation in the network switch.



```
PROGRAM Program1
VAR
    VAR1 : REAL;
    VAR2 : REAL;
    VAR3 : REAL;
END_VAR

GlobVar1 := DER_Site_CTRL_Gcb01.MV001.instMag ; //STLWT1a
GlobVar2 := DER_Site_CTRL_Gcb01.MV002.instMag ; //STLWT1b
GlobVar3 := DER_Site_CTRL_Gcb01.MV003.instMag ; //STLWT1c
GlobVar4 := DER_Site_CTRL_Gcb01.MV004.instMag ; //GUST
GlobVar5 := DER_Site_CTRL_Gcb01.MV005.instMag ; //airdensity
GlobVar6 := DER_Site_CTRL_Gcb01.MV006.instMag ; //windkph
GlobVar7 := DER_Site_CTRL_Gcb01.MV007.instMag ; //HUBSPD
GlobVar8 := DER_Site_CTRL_Gcb01.MV008.instMag ; //turbine power
GlobVar9 := DER_Site_CTRL_Gcb01.MV009.instMag ; //pitchdeg
GlobVar10 := DER_Site_CTRL_Gcb01.MV010.instMag ; //STLWT1SPD
GlobVar11 := DER_Site_CTRL_Gcb01.MV011.instMag ; //STLWT1P
GlobVar12 := DER_Site_CTRL_Gcb01.MV012.instMag ; //STLWT1Q

GlobVar13 := GlobVar1 * 1.732;   //3-phase voltage of the generator busbar

IF GlobVar4 > 1                  //GUST
    THEN GlobVar14 := GlobVar9;  //pitchdeg
    ELSE GlobVar14 :=  GlobVar6;  //windkph
END_IF

IF GlobVar11 < 0
    THEN GlobVar15 := GlobVar8;
    ELSE GlobVar15 := GlobVar11;
END_IF

VAR1 := GlobVar10 * 1200 ; //rotor speed in rpm
VAR2 := VAR1/84.5 ;        //hub speed in rpm
VAR3 := (VAR2 * 2 * 3.1415926535897932 38)/60 ; //Hub speed in rad/s = hub speed in rpm * (2π/60)
GlobVar16 := GlobVar7 - VAR3 ; //Difference of hubspeed between the measured value and the calculated value from the rotor speed


SEL_RTAC_1.Wind_Site.GGIO1.AnIn001.instMag := GlobVar13 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn002.instMag := GlobVar14 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn003.instMag := GlobVar15 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn004.instMag := GlobVar16 ;
SEL_RTAC_1.Wind_Site.GGIO1.AnIn005.instMag := GlobVar5 ; //airdensity
SEL_RTAC_1.Wind_Site.GGIO1.AnIn006.instMag := GlobVar12 ; //STLWT1Q
```

Figure A.5: Data fusion algorithm in RTAC SEL-3555.