

BRNO UNIVERSITY OF TECHNOLOGY
Faculty of Electrical Engineering
and Communication

MASTER'S THESIS

Brno, 2025

Bc. Bogdan Adrian Stoican



BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF ELECTRICAL POWER ENGINEERING

ÚSTAV ELEKTROENERGETIKY

CONFIGURATION OF SCADA SYSTEM AND IEC 61850 COMMUNICATION ANALYSIS ON A LABORATORY MODEL OF THE SUBSTATION

KONFIGURACE SYSTÉMU SCADA A ANALÝZA KOMUNIKACE IEC 61850 NA LABORATORNÍM MODELU
ROZVODNY

MASTER'S THESIS

DIPLOMOVÁ PRÁCE

AUTHOR

AUTOR PRÁCE

Bc. Bogdan Adrian Stoican

SUPERVISOR

VEDOUCÍ PRÁCE

Ing. Viktor Jurák

BRNO 2025

Master's Thesis

Master's study program Electrical Power Engineering

Department of Electrical Power Engineering

Student: Bc. Bogdan Adrian Stoican

ID: 187792

**Year of
study:** 2

Academic year: 2024/25

TITLE OF THESIS:

**Configuration of SCADA system and IEC 61850 communication analysis on
a laboratory model of the substation**

INSTRUCTION:

1. Description of the IEC 61850 communication protocol and its application in the energy sector
2. Analysis of available SCADA system solutions and selection of a suitable solution
3. Implementation of a SCADA system on a laboratory substation model
4. Analysis of IEC 61850 communication in the laboratory substation model (MMS and GOOSE)

RECOMMENDED LITERATURE:

doporučená literatura podle pokynů vedoucího závěrečné práce

**Date of project
specification:** 10.2.2025

**Deadline for
submission:** 26.5.2025

Supervisor: Ing. Viktor Jurák

prof. Ing. Petr Toman, Ph.D.
Chair of study program board

WARNING:

The author of the Master's Thesis claims that by creating this thesis he/she did not infringe the rights of third persons and the personal and/or property rights of third persons were not subjected to derogatory treatment. The author is fully aware of the legal consequences of an infringement of provisions as per Section 11 and following of Act No 121/2000 Coll. on copyright and rights related to copyright and on amendments to some other laws (the Copyright Act) in the wording of subsequent directives including the possible criminal consequences as resulting from provisions of Part 2, Chapter VI, Article 4 of Criminal Code 40/2009 Coll.

Abstract

This thesis deals with the analysis of the IEC 61850 standard and its applications for the energy domain. It contains a summary description of the functional and data models of the standard and of the defined configuration language and communication network protocols. It includes research on the options available for implementing substation SCADA systems based on support IEC 61850. Based on the ABB COM600 management unit platform, a SCADA system is deployed and integrated with a substation laboratory model. In addition to IEC61850 network integration, the COM600 network protocol gateway function is implemented for emulating data communication with a remote enterprise system. In the last part of the thesis, a traffic network analysis of the laboratory model communication is performed. This analysis includes the MMS, GOOSE and IEC 60870-5-104, which are deployed as part of the implemented SCADA system.

Keywords

IEC 61850, IED, GOOSE, MMS, IEC104, ABB COM600, OpenMUC, substation automation system, abstract data models for communication, network traffic analysis.

Abstrakt

Tato práce se zabývá analýzou normy IEC 61850 a jejími aplikacemi v energetice. Obsahuje souhrnný popis funkčního a datového modelu normy, definovaného konfiguračního jazyka a komunikačních síťových protokolů. Součástí práce je výzkum dostupných možností implementace SCADA systémů v rozvodnách založených na podpoře IEC 61850. Na platformě ABB COM600 je konfigurován SCADA systém pro laboratorní model rozvodny. Kromě síťové integrace IEC 61850 je implementována funkce COM600 síťové protokolové brány pro emulaci datové komunikace se vzdáleným podnikovým systémem. V poslední části práce je provedena analýza síťového provozu komunikace laboratorního modelu. Tato analýza zahrnuje protokoly MMS, GOOSE a IEC 60870-5-104, které jsou konfigurovány jako součást implementovaného SCADA systému.

Klíčová slova

IEC 61850, IED, GOOSE, MMS, IEC104, ABB COM600, OpenMUC, automatizovaný systém rozvodny, abstraktní datové modely pro komunikaci, analýza síťového provozu.

Rozšířený abstrakt

Tato práce se zabývá studiem normy IEC 61850 a její použitelností v oblastech energetického sektoru. Z teoretického hlediska představuje souhrnný pohled na vznik normy, zdůrazňuje význam objektově orientovaného modelování jako metody popisu funkcí IED a souvisejících dat, použití IEC 61970 Common Information Model (CIM) jako metody popisu komunikačního modelu a jazyka ANSI XML pro definici konfiguračního jazyka IEC 61850. Tyto prvky jsou základem pro definici normy. Na jejich základě jsou ustaveny datový model a jeho související sémantika, síťové protokoly a konfigurační jazyk rozvodny.

Ve druhé kapitole práce je proveden výzkum komerčně dostupných SCADA řešení a jejich použitelnosti pro domény energetického sektoru. Zaměřuje se na identifikaci podporovaných funkcí SCADA, implementovaných vlastností a podporu průmyslových síťových protokolů. Na základě veřejně dostupných informací jsou získány poznatky o odolnosti a bezpečných návrhových vzorech, které analyzovaný produkt podporuje.

Pro implementaci a testování SCADA řešení pro laboratorní model rozvodny byla použita řídicí jednotka ABB COM600. Pro konfiguraci COM600 je vyžadován nástroj ABB Substation Automation Builder (SAB600).

Ve třetí kapitole jsou popsány konfigurační kroky potřebné pro nastavení SCADA funkcí. To zahrnuje konfiguraci OPC serverů COM600 nasazených v konfiguraci pro vertikální komunikaci IEC 61850, GOOSE intrusion, Simple Network Time Services (SNTP) a OPC Slave server pro komunikaci vzdáleného pracoviště s externím SCADA systémem. Externí SCADA systém byl nastaven na základě frameworku OpenMUC. Pro emulaci realistického případu síťové komunikace vyšší úrovně podnikového systému byla komunikace brány COM600 s vzdáleným systémem OpenMUC založena na protokolu IEC 60870-5-104.

V poslední části této práce jsou analyzovány síťové protokoly nasazené v konfiguraci SCADA systému. Pro protokol MMS je podrobně popsán proces přidružení klientského serveru. Odstraňování problémů GOOSE je provedeno na základě COM600 GOOSE Analyzer a demonstruje použití funkce analyzátoru pro odstraňování problémů s chybnou konfigurací aplikace. Analýza komunikace protokolu IEC104 je provedena pro emulované serverové prostředí založené na knihovně MZ-Automation GmbH Source Code Library IEC 60870-5 komunikující s frameworkem OpenMUC.

Bibliographic citation

STOICAN, Bogdan Adrian. Configuration of SCADA system and IEC 61850 communication analysis on a laboratory model of the substation. Online, master's Thesis. Viktor JURÁK (supervisor). Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, 2025. Available at: <https://www.vut.cz/en/students/final-thesis/detail/165910>. [accessed 2025-05-23].

Author's Declaration

Author:	Bogdan Adrian Stoican
Author's ID:	187792
Paper type:	Master's Thesis
Academic year:	2024/25
Topic:	Configuration of SCADA system and IEC 61850 communication analysis on a laboratory model of the substation

I declare that I have written this paper independently, under the guidance of the advisor and using exclusively the technical references and other sources of information cited in the project and listed in the comprehensive bibliography at the end of the project.

As the author, I furthermore declare that, with respect to the creation of this paper, I have not infringed any copyright or violated anyone's personal and/or ownership rights. In this context, I am fully aware of the consequences of breaking Regulation S 11 of the Copyright Act No. 121/2000 Coll. of the Czech Republic, as amended, and of any breach of rights related to intellectual property or introduced within amendments to relevant Acts such as the Intellectual Property Act or the Criminal Code, Act No. 40/2009 Coll., Section 2, Head VI, Part 4.

Brno, May 22, 2025

author's signature

Poděkování

Rád bych zde poděkoval Ing. Viktoru Jurákovi za cenné rady, věcné připomínky, vstřícnost při konzultacích, trpělivost, podporu a porozumění při zdolávání úrovně mé češtiny při zpracovávání mé diplomové práce.

Brno, May 22, 2025

Author's signature

Contents

1. OBJECTIVES	13
2. DESCRIPTION OF THE STANDARD AND ITS APPLICATION IN THE ENERGY SECTOR.....	14
2.1 “THREE PILLARS OF INTEROPERABILITY AND CONFORMANCE TESTING”	15
2.2 OVERVIEW OF THE IEC61850 STANDARD.....	15
2.2.1 IEC 61850 Data Model	16
2.2.2 IEC 61850 Communication Protocols	17
2.2.3 IEC 61850 Substation Configuration Language	19
2.3 SUMMARY	21
3. SCADA SYSTEMS RESEARCH	22
3.1 OVERVIEW.....	22
3.2 COPA-DATA ZENON ENERGY EDITION	23
3.3 AVEVA PLANT SCADA	24
3.4 SCHNEIDER ELECTRIC EcoSTRUCTURE™ GEO SCADA EXPERT	26
3.5 GENERAL ELECTRIC DIGITAL CIMPLICITY HMI/SCADA	28
3.6 SIEMENS SPECTRUM POWER™- SICAM 8 AUTOMATION PLATFORM AND SICAM S8000.....	30
3.7 ABB COM600 GATEWAY	31
3.8 OPENMUC FRAMEWORK.....	33
3.9 SUMMARY	35
4. SCADA SYSTEM IMPLEMENTATION.....	36
4.1 OVERVIEW.....	36
4.2 SUBSTATION BAYS IED CONFIGURATION – PCM600 UPDATES	38
4.2.1 Substation Client-Server (vertical) communication setup.....	39
4.2.2 Substation GOOSE (horizontal) communication setup.....	40
4.2.3 Substation SNTP configuration	41
4.2.4 PCM600 substation model SCL configuration export	42
4.3 SAB600 CONFIGURATION WIZARD	42
4.4 SAB600 SCADA SERVICES CONFIGURATION	44
4.5 SAB600 SUBSTATION CONFIGURATION	45
4.6 COM600 COMMUNICATION GATEWAY CONFIGURATION.....	49
4.6.1 OPC Client for IEC 60870-5-104 Slave configuration	50
4.6.2 Remote SCADA configuration - IEC 60870-5-104 protocol.....	53
4.7 SUMMARY	56
5. ANALYSIS OF THE LABORATORY MODEL COMMUNICATION.....	57
5.1 MMS COMMUNICATION ANALYSIS.....	57
5.1.1 MMS communication session setup.....	59
5.1.2 Confirmed MMS services communication	63
5.1.3 Unconfirmed MMS services communication	64
5.2 GOOSE COMMUNICATION ANALYSIS.....	66
5.3 IEC104 TESTING.....	75
5.4 SUMMARY	78

6. CONCLUSION.....	80
LITERATURE	82
SYMBOLS AND ABBREVIATIONS.....	85
LIST OF APPENDICES	87

FIGURES

2.1	IEC/TR 62357-1 architecture framework [2]	14
2.2	IEC61850 main standard parts relationship.....	16
2.3	IEC61850 hierarchical data model –ABB SAB600 view.....	17
2.4	IEC61850 communication protocols [5]	18
2.5	SCL configuration information flows	20
3.1	zenon energy edition architecture [10].....	23
3.2	AVEVA Plant SCADA architecture [11].....	25
3.3	EcoStruxure™ Geo SCADA security architecture [12].....	27
3.4	GE iPower IEDs control and alarm management [14].....	29
3.5	OpenMUC framework architecture [18]	33
4.1	Substation SCADA communication model [17][18].....	36
4.2	COM600 OPC Server-Client communication model [17]	38
4.3	PCM600 Client-Server Report Controls configuration	39
4.4	PCM600 GOOSE configuration.....	41
4.5	PCM600 SNTP configuration	41
4.6	COM600 Gateway communication setup	42
4.7	COM600 substation SCD configuration import.....	43
4.8	COM600 SNTP OPC server setup	43
4.9	COM600 SCADA server properties.....	44
4.10	SAB600 SNTP configuration.....	45
4.11	SAB600 single line diagram update	46
4.12	SAB600 SLD Logical Nodes association.....	46
4.13	SAB600 laboratory substation SLD	47
4.14	COM600 gateway configuration update	47
4.15	COM600 WebHMI console SLD.....	48
4.16	COM600 WebHMI console SLD.....	48
4.17	COM600 control issue for IED00000004	49
4.18	SAB600 IEC104 Slave OPC client service addition	50
4.19	SAB600 IEC104 Slave OPC client	50
4.20	SAB600 IEC104 Slave OPC client details	51
4.21	SAB600 IEC104 channel (subnet) configuration.....	51
4.22	SAB600 IEC104 IED properties	52
4.23	SB600 IEC104 IED Cross-References menu	52
4.24	SAB600 IEC104 Cross-References set up	53
4.25	OpenMUC framework rebuild	54
4.26	OpenMUC framework start.....	54
4.27	OpenMUC IEC60870 communication configuration.....	55
4.28	IEC61850 to IEC60870 communication data flow	56
5.1	COM600 OPCS1 IED server-client communication (SCL).....	58
5.2	PCM600 REF615 IEDs client-server communication configuration	58
5.3	MMS Communication session initiation (Wireshark).....	59
5.4	TPKT/COTP Transport layer connection setup (Wireshark decoding).....	60
5.5	MMS Session layer connection setup.....	60
5.6	MMS Presentation layer connection setup	61
5.7	MMS Application layer connection acceptance.....	62
5.8	MMS “initiate-RequestPDU” and “initiate-ResponsePDU”	62

5.9	MMS confirmed PDU example.....	63
5.10	MMS SBO control model operation example	64
5.11	MMS SBO control model operation example	65
5.12	SAB600 GOOSE Analyzer configuration wizard	66
5.13	SAB600 GOOSE Analyzer configuration wizard	67
5.14	SAB600 GOOSE Analyzer OPC server	68
5.15	GOOSE Analyzer OPC server communication structure	68
5.16	COM600 WebUI GOOSE Analyzer IED view	69
5.17	IED00000004 GOOSE communication errors	70
5.18	IED00000004 incoming/outgoing GOOSE control block signals.....	70
5.19	COM600 Historical Events Dashboard for IED00000004	71
5.20	COM600 Network Statistics Dashboard for IED00000004	71
5.21	COM600 GOOSE Test Manager.....	72
5.22	COM600 GOOSE Test Manager – manual mode	72
5.23	COM600 GOOSE Packet analysis insights.....	73
5.24	GOOSE configuration revision analysis (Wireshark)	73
5.25	COM600 GOOSE communication status after IEC00000003 corrective configuration update	74
5.26	lib60870.NET test environment	76
5.27	cs104-server.exe server execution.....	76
5.28	cs104-server IOA data objects definition example.....	77
5.29	IEC104 Test – Wireshark network traffic analysis	78

.

TABLES

3.1	zenon SCADA functions, features and standards [10]	24
3.2	AVEVA Plant SCADA functions, features and standards [11].....	26
3.3	EcoStruxure™ Geo SCADA Expert functions, features and standards [12].....	28
3.4	General Electric CIMPLICITY HMI/SCADA Expert functions, features and standards [13].....	29
3.5	Siemens SICAM S8000 functions, features and standards [16].....	31
3.6	ABB COM600 functions, features and standards [17].....	32
3.7	OpenMUC framework functions, features and standards [18]	34
4.1	Substation IEDs IEC 61850/MMS network configuration.....	39
4.2	Substation IEDs GOOSE communication configuration	40
5.1	IED00000004 – analyzed configuration errors	74
5.2	MZ-Automation IEC104 source library features and standards [24]	75

INTRODUCTION

The development of the IEC 61850 standard started in late 1990 having as goal the establishment of a framework for enabling vendor inter-operability inside the substation automation system (SAS) and, together with this, the definition of new (modern) network communication protocols that would be specialized for enabling the data communication required by the new standard models and functions.

The foundation for the inception of a modern SAS communication standard was the advance in microprocessor development. This allowed substation relays, disconnect switches, current and voltage meter sensors, merging units, and bay terminals to be developed based on microcontrollers' electronics, becoming digitally operated devices that have been generically named Intelligent Electronic Devices (IEDs).

IEC 61850 decomposes the substation functional model and maps this to a virtual logical representation that is defined based on Object Oriented data modeling. IEC 61850 focuses on vendor interoperability and enables flexibility and optimization for the substation engineering and management processes in all phases of the life-cycle of SAS solutions.

IEC 61850 defines compatible devices configuration a dedicated Substation Configuration Language (SCL). The syntax in SCL is based on Extensible Markup Language (XML) which enables the use of natural language for the configuration definition. This is complemented by the semantics of the IEC 61850 data model, which further simplifies data model learning, and utilization of the data model.

In 2003, the International Electrotechnical Commission (IEC) published the first Technical Report “IEC TR 61850-1 Communication networks and systems” making this the foundation document of the IEC standard for “communication networks and systems for power utility automation” [1].

IEC 61850 is a comprehensive standard. It is layered and modular, and its architecture is characterized through multiple views, enabling the decomposition and characterization of the SAS functional requirements to enable a modern design and efficient data communication. The architecture of the standard enables its expansion for use beyond the boundaries of the substation automation systems.

Together with the technological capabilities advance, the introduction and use of the IEC 61850 standard creates also additional complexity and challenges.

Overall, the benefits of deploying IEC 61850 SAS systems largely exceed the downsides and the associated risks. IEC 61850 offers increased integration, visibility, and control, some of these characteristics being analyzed in this thesis.

The standard enables resilient and secure operations and enables efficient design, deployment, commissioning, and testing of IEC 61850 substations or any other IEC 61850 electrical energy production, management, and transport systems.

1. OBJECTIVES

The first objective of this thesis is to analyze the IEC 61850 communication protocol, and its application use cases inside the energy sector domain. This analysis is detailed in Chapter 2, which includes a description of the architectural framework of the standard. The chapter discusses the role and relevance of the main parts of the standard, with focus on the IEC 61850 data model, the configuration language, and mapping to network communication protocols.

The second objective is addressed in Chapter 3, containing research on the available IEC 61850 based SCADA systems. The analysis includes an overview of the deployment architecture and the main components of the SCADA system, information on the functions implemented, and the supported technical features. An extract of the supported industrial standards and communication protocols is included. Network design and cybersecurity related aspects are presented in the analysis for products for which the vendor provides online documentation for these topics. The chapter also presents the applicability of the selected SCADA systems for applications in the electrical energy domain.

The third objective of this thesis focuses on the implementation of a SCADA system to supervise and control a substation laboratory model. This objective is to configure the SCADA system based on the functions provided by the ABB COM600 gateway appliance and to integrate the SCADA with the IEC 61850 substation communication parameters. The implementation aims to replicate a real-world substation environment that implements horizontal and vertical communication, and, also, deploys communication to a higher-level SCADA, emulating an enterprise system outside the substation. The deployment of SCADA in the outstation was based on the OpenMUC framework produced by the Fraunhofer Institute for Solar Energy Systems in Freiburg, Germany. The OpenMUC framework was selected because, among other protocols, it implements both the IEC61850 and the IEC 60870 communication standards.

The last objective of this thesis is to perform an analysis of the IEC 61850 MMS (Manufacturing Message Specification) and GOOSE (Generic Object Oriented Substation Event) network protocols inside the substation laboratory model. The analysis is performed following several objectives: for MMS to use map theoretical knowledge to the network communication flows inside the substation network, for GOOSE to give a practical example of using COM600 analysis tools for GOOSE communication errors analysis and removal. A third test involving communication based on the IEC 60870-5-104 protocol is performed to demonstrate the use of various tools, as part of the regular life cycle of an electrical substation SAS system.

2. DESCRIPTION OF THE STANDARD AND ITS APPLICATION IN THE ENERGY SECTOR

The IEC 61850 standard is designed to provide a comprehensive framework for vendor-interoperable communication networks and subsystems within the automation, monitoring, control, and protection systems of electrical power substations. It is developed by the IEC Technical Committee (TC) 57 - Power Systems Management and Associated Information Exchange, in collaboration with other technical committees of the IEC responsible for creating standards related to connected technologies and functions. IEC 61850 is part of a larger scope of work of the TC75 “to provide interoperability standards for the information exchange within and to power systems” [2], IEC 61850 components being integrated to IEC/TR 62357-1 architecture framework for smart grid standardization.

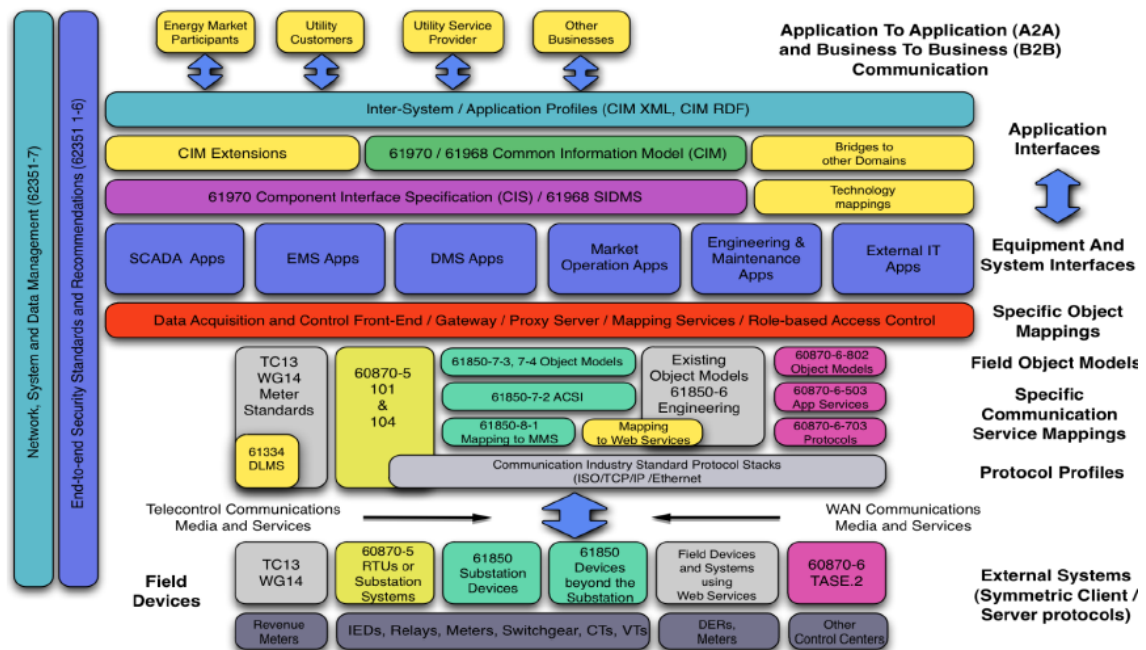


Fig. 2.1 IEC/TR 62357-1 architecture framework [2]

Initially, the standard's scope was confined to the boundaries of substation automation systems (SAS). As the electric power industry and technologies evolved over the years, the standard footprint has been increased to incorporate additional capabilities. Besides IEC 61850 published standard parts, documentation of the standard contains Technical Reports (TRs) that define aspects related to individual domains and subjects using or in communication with IEC 61850 enabled domains, such as substations, distributed energy resources or distribution automation systems.

While not all the planned standard parts have been released, IEC TC57 has updated the standard to incorporate new technological developments and requirements, thereby expanding the capabilities and scope of the standard.

2.1 “Three pillars of interoperability and conformance testing”

In IEC 61850 Object Oriented Modeling, based on Universal Modeling Framework (UMF) is used for decomposing and characterizing the IED’s components, functions, behaviors and data characteristics. This is the first foundational pillar selected by standard developers to enable the modeling of IED functions and properties based on a unified language developed and applied for the development of software IT applications.

Retrospectively, the use of UMF and OOM can be seen as a natural choice: IEDs are processor-based computer systems, so choosing UMF at the inception of the IEC 61850 work (year 1995) could be seen as a strategic choice. Object Management Group (OMG) released the Unified Modeling Language (UML) in 1997 [3]. It is interesting to note that the use of UMF in TC57 work preceded, or at least came along at the same time, with the establishment of UMF as a proven IT architecture modeling framework.

The second foundational pillar of the standard is the use of IEC 61970 Common Information Model (CIM). Through this, IEC 61850 adopted a standardized information communication model that allowed expansion of the interoperability of IED and SAS systems to the broader power utility/grid control ecosystem, covering all domains of electricity generation, transmission, and distribution.

The third foundational pillar is the use of ANSI’s XML language for definition of the IEC 61850 configuration language. This enabled the adoption and usability of the configuration language used within the standard and enabled the portability of the IED configuration. Portability is used inside a project, between different engineering and configuration tools, and between different projects or vendors.

Lastly, the standard provides methods to be implemented for compatible IEDs and compatible systems development. Having as goal achieving compatibility and interoperability, it also provides a conformance testing framework to be applied for validating the adherence to standard's requirements. Testing as a capability and activity is pervasive in the standard. The implemented data model includes dedicated test data objects that enable efficient testing in all phases of design, deployment, commissioning, and operations of an IEC 61850 based substation.

2.2 Overview of the IEC61850 standard

The individual parts of the standard (including associated technical reports) have the role of either providing a high-level overview of the decisions, methods, objects and assets defined by the standard, or providing an in-depth, exhaustive, low-level definition

of the standard's content (data model, configuration language, communication protocols and their mapping to the information model). Fig. 2.2 provides an overview of the main standard parts and their interactions.

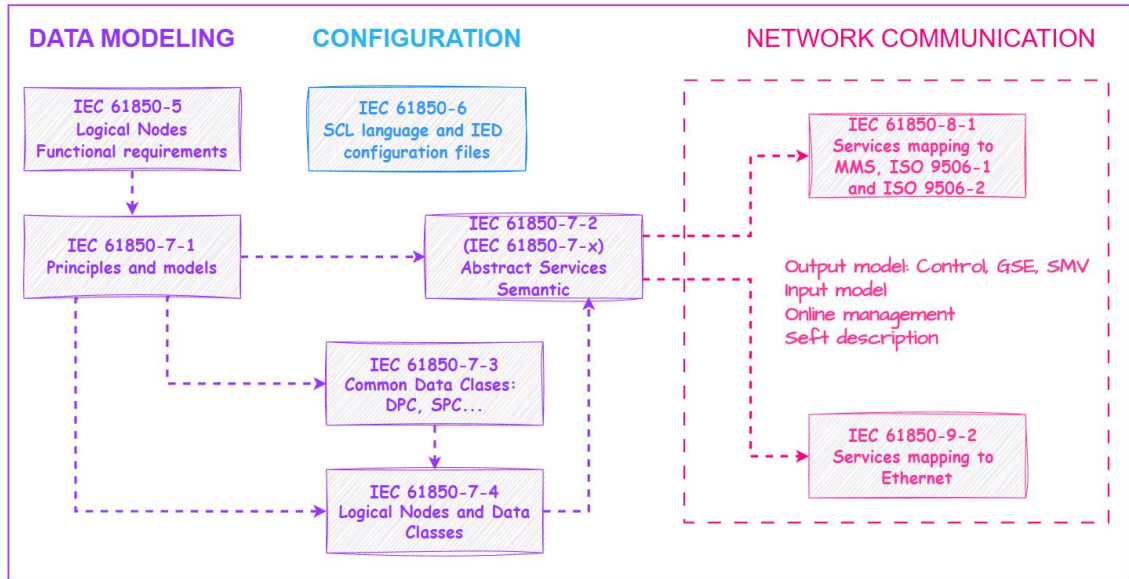


Fig. 2.2 IEC61850 main standard parts relationship

2.2.1 IEC 61850 Data Model

As introduced in the previous section, based on OOM the standard provides functional and data modeling for compatible IEDs. OOM based data modeling enabled the description of the substation components based on their intrinsic functions. A full logical decomposition is done for the representation of IED functions properties and behaviors to their most detailed useful characteristics. For this, the physical devices (IEDs) are decomposed into Logical Device classes, each class presenting a standardized substation role. Individual functions associated with a specific Logical Device are further deconstructed and modeled through the Logical Node classes.

Logical nodes are grouped in the standard based on their purpose. The grouping denotes the fact that the IEC 61850 standard was designed for uses also outside the classical substation. Example of such applications are the following groups: Distributed Energy Resources - group indicator D, Hydro power - group indicator H, Wind - group indicator W. Future (power system) equipment - group indicator Z, enables further expansion of LN domain [4]. Additionally, the standard enables vendors provisioning proprietary/non-standardized logical nodes.

The data content of the Logical Node class is characterized through the Data class model. In the substation data model hierarchy, Data Object's role is to uniquely identify the location of the Data Attribute class.

Data Object class is further standardized through two properties:

- Common Data Classes (CDC) model - standardizing the data content of the Data Object.
- Functional Constraint (FC) model – standardizing the behavior or the use the Data Object.

The Data Attribute class models the data content that properties defining the Logical Nodes Data Objects can hold. This is the lowest function decomposition object property in the IEC61850 data model.

Fig. 2.3 presents the IEC 61850 Data Model as displayed in ABB Substation Automation Builder (SAB) 600 application. The data model objects have been annotated. Data Attributes objects are not displayed, but their content can be associated with the assigned Common Data Class type.

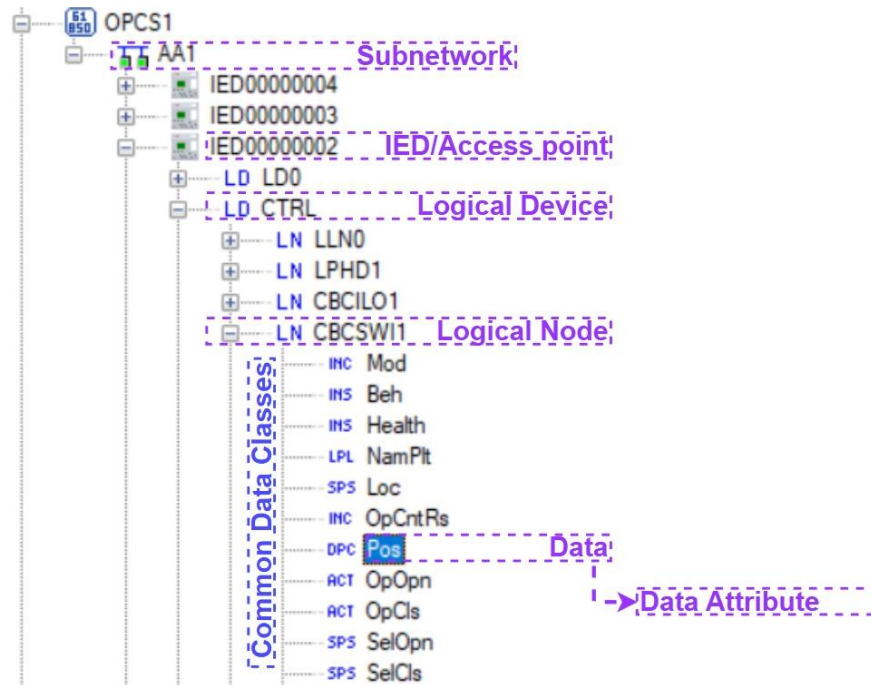


Fig. 2.3 IEC61850 hierarchical data model –ABB SAB600 view

2.2.2 IEC 61850 Communication Protocols

For data network communication, the IEC 61850 defines and maps its data exchange model to (specialized) network communication protocols. This is based on the use of the Application Communication Service Interface (ACSI) which maps IEC 61850 data model to the data exchange model enabled by the deployed network protocols.

IEC 61850 organizes the SAS network architecture based on a three-layer model:

- Level 0 – process level – process bus communication uses SMV protocol.
- Level 1 – bay level – GOOSE protocol communication.
- Level 2 – station level – client-server MMS protocol communication.

Process and bay level communications are characterized, traditionally, by the property that the time -sensitive communication flows generated at these layers are not forwarded to a different layer. The communication is called generic „horizontal“.

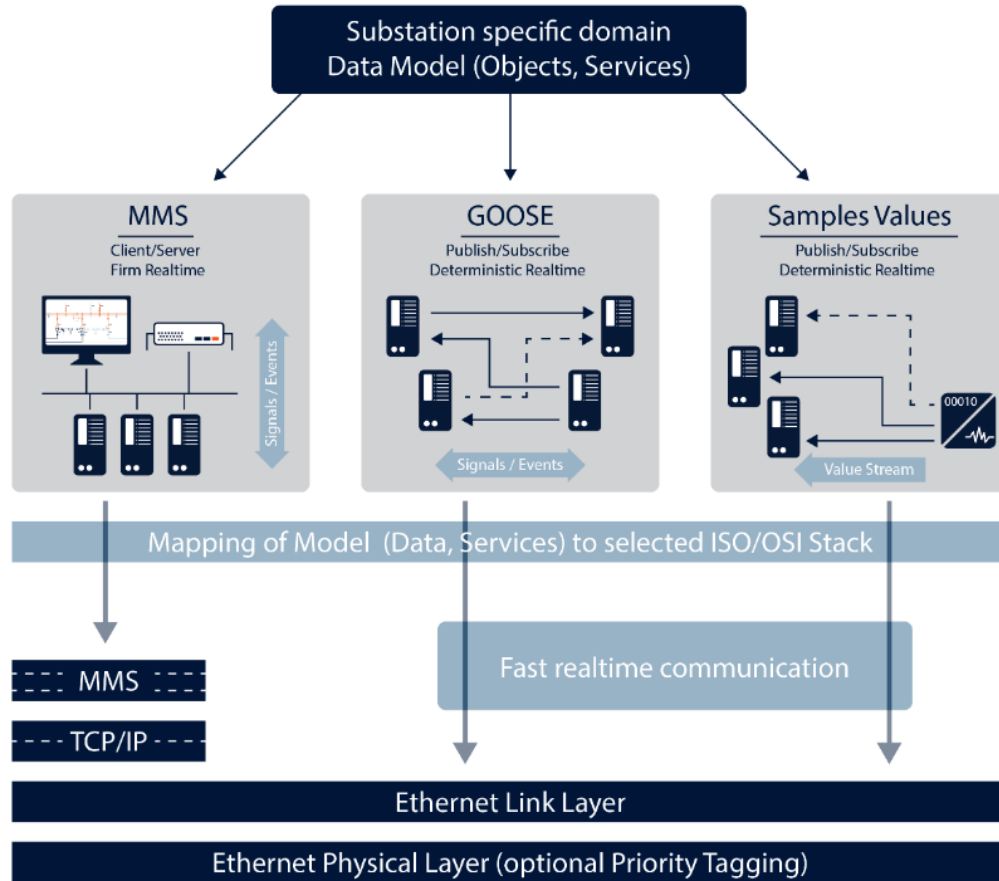


Fig. 2.4 IEC61850 communication protocols [5]

Both GOOSE and SMV are connection-less, non-reliable communication protocols specialized for fast data transmission. They are based on multicast frames transported over OSI Layer 2 Ethernet and using a publisher-subscriber communication registration mechanism.

SMV performs the transfer of time-synchronized, high volume measurement data (e.g., current and voltage data) in digital substations. GOOSE enables high-speed, event-driven communication for time-critical operations (e.g., tripping commands, interlocking) realizing real-time protection and control coordination.

MMS is a client-server connection oriented, reliable transport communication protocol enabling control, monitoring, configuration communication between SAS devices and systems. MMS performs vertical integration of data flows between bay-level IEDs and substation-level systems to enable centralized control and supervision. Being a COTP based Layer 3 network protocol, MMS can be used for communication between hosts that

are part of different network subnets, which makes MMS suited for remote station data communication.

Expansion of the use of IEC 61850 to domains outside substation perimeter, raises new requirements for forwarding the process and bay level generated data to remote networks. This is possible using communication gateways which UDP encapsulate L2-GOOSE frames and forward them to the remote receiver based on UDP routed protocol (R-GOOSE routed frame). Additional time delay introduced by encapsulation, routing (forward delay) and encryption/decryption processes should be considered, as the strict GOOSE maximum 4ms standard forward delay GOOSE requirements will not be met in network communication to a remote network [6].

Real-time critical events (GOOSE communication) necessitate stringent time synchronization requirements for IEDs, demanding accuracy at the microsecond level. To ensure precise and reliable operation within the substation environment, IEDs must achieve the highest possible synchronization accuracy. Real-time non-critical events, as the SMV process level sourced data, streams require, as well, accurate time synchronization for correct processing of the data stream information.

The Precision Time Protocol (PTP), as defined by the IEEE 1588-2008 standard, is widely adopted as synchronization protocol that enables microsecond-level clock accuracy in digital substations. PTP (as an alternative the Simple Network Time Protocol can be used) facilitates the precise alignment of device clocks within an Ethernet network, ensuring that all synchronized devices automatically adjust to the most accurate clock available. The protocol supports sub-microsecond synchronization accuracy while requiring minimal computational and network resources, making it a highly efficient solution for time-sensitive substation automation applications.

Additional network protocols standards are incorporated into substation communication systems for enabling redundancy and resilience for network communication. In the communication profiles associated with the protocols the use of these protocols is optional. Examples of such a protocol are the High Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP1), both part of IEC 62439-3, and Rapid Spanning Tree Protocol, defined by IEEE 802.1D.

2.2.3 IEC 61850 Substation Configuration Language

System Configuration Language (SCL) is the standardized description language used for engineering definition and configuration of the IEC61850 compliant systems. SCL is based on eXtensible Markup Language (XML). The standard defines the XML Schema Definition (XSD) to be implemented as a self-describing method for managing online and offline substation components and network communication configuration. This is done by implementing the configuration language for substation functions and IED in accordance with IEC61850 data modeling, the communication services requirements and the communication services mappings [7].

- IED Capability Description (ICD) describes the capabilities of individual IEDs. Vendors are required by the standard to provide ICDs for IEC 61850 compatible IEDs.
- Instantiated IED Description (IID) contains data of a specific IED and realizing transfer of IED configuration information in between an ICD Configuration Tool and a System Configuration Tool.

SCL permits manufacturers to extend the SCL configuration scheme, through addition of private type LNs (done in accordance with IEC 61850-6 rules). Together with the support of the standard for the addition of new data attributes (i.e.: non-substation and non-electrical data attributes), this enables the expansion and use of the standard for IED's functions that, otherwise, are not part of the scope of the formal standard.

2.3 Summary

Benefits of implementing IEC 61850 standard for substation automation include enhanced system interoperability, improved operational efficiency, scalability and flexibility, including the native compatibility with distributed automation smart grid architecture and distributed energy resources systems. The standard also provides a foundation for enabling an efficient substation engineering process within SAS development, based on compatible configuration data flows.

A key feature of the standard is that it is designed to allow its expansion into new domains. This is enabled by the high level of abstraction used to characterize the modeled functions, which allows the creation and use of new objects inside the standard. Dedicated standard parts provide communication mapping for hydroelectric power plants (IEC 61850-7-410), distributed energy resources and distribution automation logical nodes (IEC 61850-7-410). Published IEC 61850 technical reports provide modeling and communication guidance on the use of the standard for hydroelectric power plants, steam and gas turbines, communication between substations and communication between substations and control centers, transmission of Synchrophasor information, use for Distribution Automation Systems and Distributed Energy Resources, E-mobility, Electrical Energy Storage, Smart Energy Automation, FACTS and HVDC transmission systems [9].

3. SCADA SYSTEMS RESEARCH

Supervisory Control and Data Acquisition defines the IT architecture solution which enables industrial processes control and management. SCADA systems are focused on enabling companies to reach their operational goals and have been present in the energy production and distribution domain since the beginning of this industry. Today, SCADA systems, as integral components of the enterprise IT architecture, represent indispensable solutions to ensure efficient and reliable control of the supervised electrical energy production, storage, transformation and distribution infrastructure.

3.1 Overview

All SCADA systems have in common capabilities associated with performing real-time operational status monitoring and control of the supervised processes. They enable logging of data generated by the involved systems and provide HMIs consoles through which operators can visualize and operate the managed processes. Through the data historian function, SCADA enables recorded data analysis.

SCADA systems integrate with other external systems, including other SCADAs. To enable communication with other systems, gateway and protocol translation capabilities are required. These are deployed as internal SCADA capabilities or using external gateway components and functions.

Based on geographical distribution of the supervised processes, SCADA systems can be centralized or distributed. Depending on the complexity of the processes, the deployments can be based on hierarchical architecture, in which lower-level SCADA systems are aggregated to higher-level ones.

As managed processes in energy domain are critical, SCADA systems require robust designs that include high availability, resiliency and redundancy. These objectives require the deployment of SCADA workloads based on configurations that include redundant nodes for critical components. IT solutions virtualization is used to enable efficient and flexible use of the deployed resources, virtualization being a technological vector that already crosses all functional layers of the substation automation solution.

In the substation automation systems architectures, the SCADA systems can contain or can seamlessly integrate with engineering, commissioning and testing tools, which enables optimization of the engineering and management processes inside the digital substations.

3.2 COPA-DATA zenon energy edition

COPA-DATA's zenon Software Platform is a complete solution for enabling full monitoring and control of the management processes and includes capabilities of automation and analysis of SCADA collected data. The provided HMI delivers real-time data access and visualization capabilities. The platform allows safe data storage capabilities for the collected information.

Flexible operations with zenon SCADA provide consistent alarming capabilities over multiple users and geographically distributed energy infrastructure. Visualization and programming capabilities are enabled by predefined templates that are defined by COPA-DATA for ready 'out-of-the-box' use. The demo version provided, includes instances of the main functions and applications supported by the platform. The deployment architecture enables nodes workload distribution and redundancy with individual functions hosted on defined servers, as detailed in Fig. 3.1.

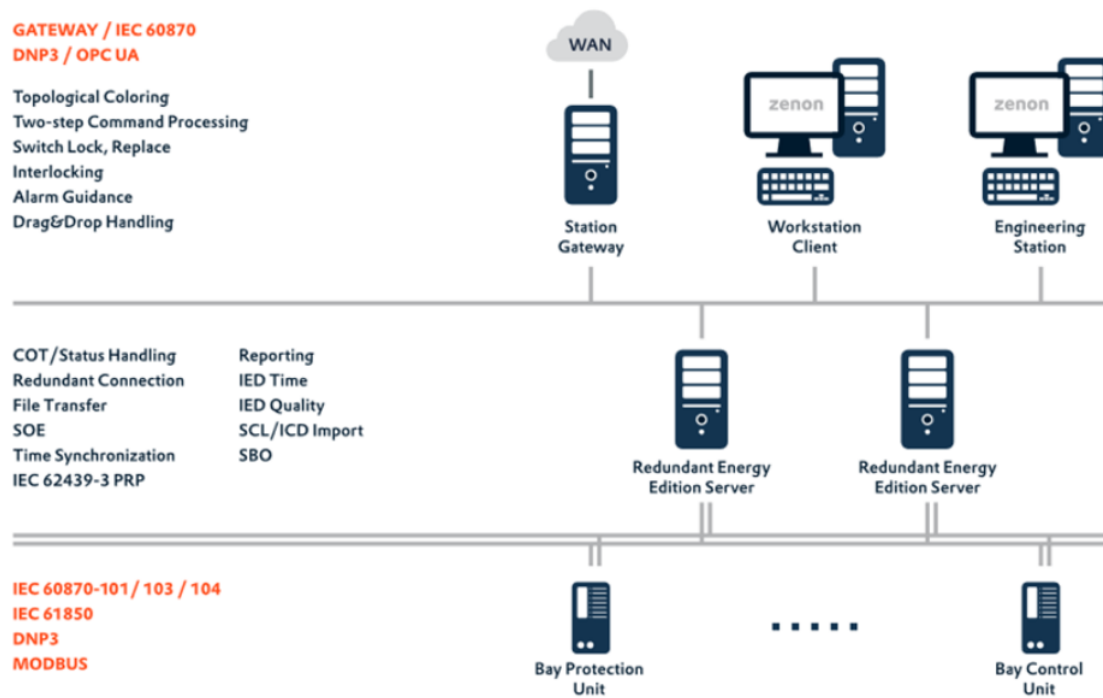


Fig. 3.1 zenon energy edition architecture [10]

An energy domain-dedicated version is provided that includes capabilities for supervision and control of substation or energy production and energy management systems. Applications include substation automation, renewable energy management platforms for distributed energy generation, hydropower plant management, distribution management systems, energy storage and public transport. zenon Software Platform documentation lists more than 300 standard and independent native drivers and communication protocols that include the main energy domain communication protocols.

Table 3.1 zenon SCADA functions, features and standards [10]

SCADA functions	Technical features	Energy communication standards
• Data Acquisition • Data Management • Visualization and Control • Analytics and Reporting • Historian • Application Engineering and Maintenance • Integrating IT and OT	• Command processing • Topology check • Command sequencer • Simulation • Alarm management • Status flags • High availability (active-active/active-standby) • Slave/Server Side with the zenon Process Gateway • IEC 62443-4-1 compliant	• IEC 61850 • IEC 60870-5-101/103/104 • DNP3 • IEC 62056-21 • IEC 61400-25 • OPC UA • MODBUS • IEEE C37.118 SYNCHROPHASOR • IEC 60870-6 • PARALLEL REDUNDANCY PROTOCOL SUPPORT (PRP)

zenon SCADA is an enterprise grade, mature solution with an extensive base of active installations over multiple countries (100+). The integration of IED management is supported by a large base of native drivers. As per the consulted documentation, the solution has strong capabilities for application engineering and maintenance, enabling a complete SCADA software platform for automated operations of substation equipment, with applicability in all electrical energy domains.

3.3 AVEVA Plant SCADA

Part of AVEVA monitoring and control industrial suite (AVEVA Industrial Software portfolio), AVEVA Plant SCADA (former Citec SCADA) is a supervisory control and data acquisition software platform designed for industrial automation and process control applications. The system includes versatile features that enable real-time monitoring, control, and data visualization for a wide range of industries, including manufacturing, utilities, energy, oil and gas, and others. For the energy domain applications substation automation, energy production, energy storage and energy distribution management systems, including renewable and electric vehicle (EV) connected mobility, are supported.

AVEVA documentation lists functions for notification and support of the decision process through context aware supervisory applications. Contextual navigation and hierarchical navigation is aligned with process flows for support of improved operations reaction times. Advanced alarm management ensures critical events are being handled, visualization options supporting visibility of status and alarm notification [11].

AVEVA energy industry domain applications and features include visualization, alarms, trends, context-aware visualization for interlocks and control, secure remote access through Plant SCADA Access Anywhere extension, object-based overlay on a tag-based database, graphics library, alarm management and real-time reporting. The process analyst function enables operators to monitor the trends of events and alarm data trends.

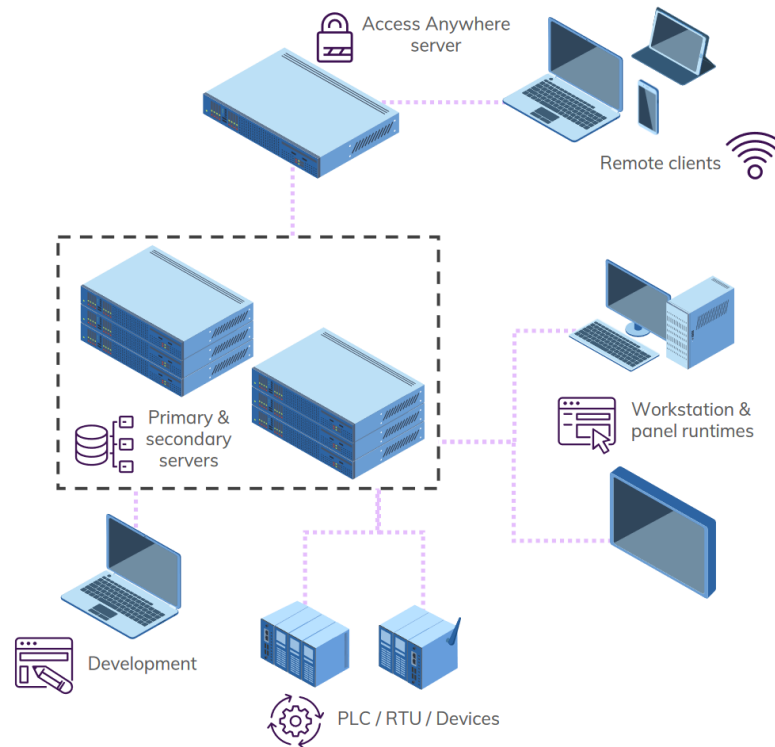


Fig. 3.2 AVEVA Plant SCADA architecture [11]

The solution is based on a centralized client-server architecture including client and server redundancy through clustering. Distributed deployment design options enable high control performance and data operational data integrity. Connectivity library includes more than 150 communication drivers, including native integration with Schneider Electric devices. Table 3.1 details an extract of the functions, features and the energy communication standards and protocols supported.

AVEVA Plant Scada functions are completed by deployment of AVEVA Historian for capture and store of process and event data, AVEVA Insight for AI-infused analytics and AVEVA Teamwork for documentation procedure store and best practices collaboration. SCADA solution can be deployed based on a secure design that takes advantage of defense in depth characteristics. In this design, secure interfaces enable data exchange with external enterprise systems based on the enterprise established security design practices.

Table 3.2 AVEVA Plant SCADA functions, features and standards [11]

SCADA functions	Technical features	Energy communication standards
• Handle communication with I/O devices • Monitor Alarm Conditions • Report Data Output • Display trending and visuals • Cybersecurity	• Equipment-based tag referencing • Broad graphics library • Alarm management • Scheduler tool • Centralized client-server architecture • Cicode programing language • Role-based user security permissions and multi-language support • Operational insights: Process analyst and trends • Integration with Schneider Electric • High availability and resilience	• OPC UA • BACNET • IEC61850 • MODBUS • DNP3 • IEC60870 • Connectivity library (150 native protocol drivers)

Not limited to the energy industry, the supported features and the integration capabilities enable AVEVA Plant SCADA to be deployed for operations streamlining for a wide range of industries. As an enterprise-grade solution, AVEVA Plant SCADA is a comprehensive and versatile SCADA software solution designed to optimize industrial processes, improve efficiency, and enhance decision-making through real-time monitoring and control.

3.4 Schneider Electric EcoStructure™ Geo SCADA Expert

EcoStruxure™ Geo SCADA Expert is an advanced open architecture industrial automation and control solution provided by Schneider Electric. Enables real-time management of geographically dispersed infrastructure based on high performance graphics, geographical displays, intelligent alarming, and historian analytics. For large environments the hierarchical deployment architecture is based on local gateways systems that provide connectivity to local IEDs, local HMI and data gateway function for information transfer to higher level SCADA systems. The deployment architecture includes a dedicated client application.

The deployment architecture is enabled by a multilayer server deployment pattern based on three distinct layers: “Collection & Control”, “Data Aggregation” and “Business” layers servers. This enhances the security and resilience of the overall

SCADA solution by localizing functions performed by servers and data based on the operational domain configuration related to the controlled field devices and the business needs of the categories of users accessing the individual SCADA servers. Two- and three-way redundant design patterns enable nonstop operations during SCADA system component maintenance and upgrades.

For a secure plant architecture Schneider Electric is integrating the deployment of EcoStruxure™ Geo SCADA Expert based (and the related ecosystem components) based on IEC 62443 core cybersecurity recommended practices.

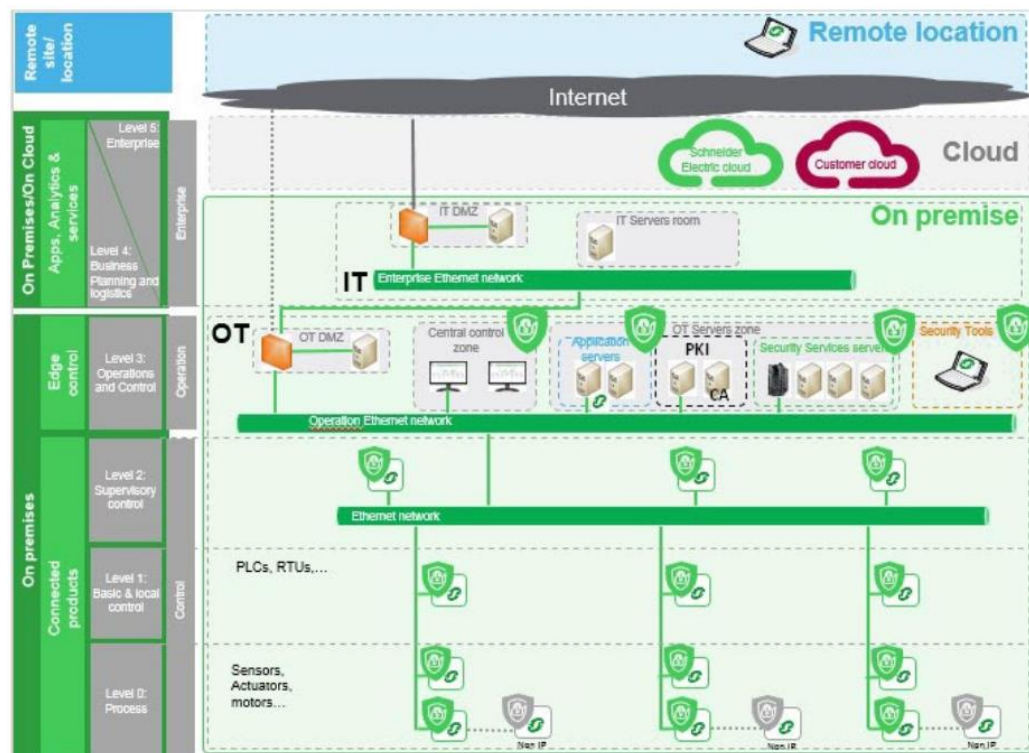


Fig. 3.3 EcoStruxure™ Geo SCADA security architecture [12]

The solution architecture establishes an “defense in depth” protection strategy. This is enabled through integration into the enterprise solution of dedicated cybersecurity components and functions such as Enigmedia and Schneider Electric Harmony Edge Box with Mercury Cipher. The security framework includes network separation of control systems to other enterprise systems through physical separation and implementation of network DMZs, use of firewalls, VPN connectivity for remote access, and enforcement of perimeter authentication. Further network segmentation into network zones permits communication monitor and firewall protection of individual network zones, to contain a successful harmful connection only to one affected zone and to prevent spillage of the connection to the entire site network. In addition, the end-to-end security of the enterprise solution is enabled through advanced encryption and authentication based on external devices that protect transparently the process devices. [12]

Table 3.3 EcoStruxure™ Geo SCADA Expert functions, features and standards [12]

SCADA functions	Technical features	Energy communication standards
• Real time plant visualization • Customization of alarm rules (persistence and suppression) • Notifications automation • Control and management of IEDs/RTUs – “Digital Twin” • Monitor and telemetry data acquisition • Data feeds to other enterprise systems • Cybersecurity	• Redundant architecture (3 redundant with 3 load load-sharing application servers) • ViewX client/multi-platform web clients • Redundant communication (Dual LAN/WAN) • Configuration templates • Multi-level security and two-factor user login • Historian and analytics data feed to AVEVA PI and AVEVA Data Hub • Deep integration with Schneider Electric products	• IEC61850 • MODBUS • DNP3 • IEC60870 • SQL INTERFACE (ODBC, OLE-DB) • WEB SERVICES - SOAP/XML • NET PROGRAMMING • OPC DA

EcoStruxure™ Geo SCADA Expert is an enterprise grade SCADA solution that integrates with a larger Schneider Electric products ecosystem with the goal of establishing a resilient and secure architecture, with wide applicability in all energy industry domains. The solution framework includes adoption of IT security architecture, functions and practices compliant with the IEC 62443 standard to enable deep defense and end-to-end security of the enterprise systems.

3.5 General Electric Digital CIMPLICITY HMI/SCADA

CIMPLICITY HMI/SCADA from GE Vernova is a highly scalable enterprise solution for industrial domains. It enables process visualization analysis and control of managed industrial processes. Operations efficiency is enhanced through leveraging alarm pattern recognition based on AI/ML templates and control loops for health monitoring.

HMI is based on HTML5 for a “single-client” experience that enables minimizing operator training requirements and enhances action and decision-making efficiency. The HMI features a graphical incident playback for remote analysis of the events and integrates operations management assets such as action calendars, change approvals, and KPI reporting and dashboards. The SCADA system data model leverages OPC UA and delivers an MQTT5 to OPC UA translator for IoT sensors and devices data communication. Besides OPC and MQTT CIMPLICITY supports IEC and ISA open standards [13].

Table 3.4 General Electric CIMPLICITY HMI/SCADA Expert functions, features and standards [13]

SCADA functions	Technical features	Energy communication standards
- Real-time data acquisition and enhanced visualization - Supervisory control - Alarm management and event logging - Historical data archiving and reporting - Consolidation and integration with other systems - Process control and optimization - Cybersecurity	- HTML5 HMI - AI and ML for analytics - Server clustering and cloud based hosting - LAN/WAN and VPN - Configuration templates - Open standards (ISA, IEC, OPC, MQTT) - Historian and analytics - Secure design support for enterprise servers' deployment and network communication.	- IEC, ISA protocols - OPC UA - SQL - MQTT5 - ISO 27001 and IEC 62443

In the electrical utilities' context, General Electric is providing the GE Vernova iPower application which is an additional software solution which enhances CIMPLICITY SCADA for electricity control room operations. iPower provides HMI, process visualization, supervisory control and real-time data collection, online screens and centralized IED and alarms management. iPower includes control and authorization features, threshold updates, operator notes and enhanced reporting for contributing to safe operations and decision making contributing to enhanced productivity and minimizing costs [14].



Fig. 3.4 GE iPower IEDs control and alarm management [14]

For substation automation, General Electric product range includes hardware appliances (bay controllers/remote terminal units) for managing the substation automation use cases as: substation automation processor, sequence of events processor, automatic voltage regulator or load shedding controller.

GE advanced gateway platforms such as Multilin G100 (Multilin G100 : GE Grid Solutions) and G500 (G500 Multi-function Controller Platform : GE Grid Solutions) are providing SCADA concentrator functions, HMI, RTU, advanced cyber security features. GE OMNI MU360 process interface unit (OMNI MU360) is another example of an IEC 61850-based digital substation appliance automation and control solution.

GE Vernova Grid Solutions based on dedicated hardware process interface units, remote terminal units and SCADA concentrator gateways integrate with higher level SCADAs (CIMPLICITY HMI/SCADA) for centralized management. CIMPLICITY HMI/SCADA is not deployed and communicating directly with substation process devices, but acts as a centralized SCADA system, enabling aggregated processes management. As enterprise grade solution CIMPLICITY HMI/SCADA deployment is enabled by a resilient, secure architecture.

In conclusion, as an enterprise-grade solution, CIMPLICITY HMI/SCADA deployment is enabled by a resilient, secure architecture. GE Vernova iFix platform enhances the supervisory, control and automation capabilities at the substation and network operation center level. GE Vernova Grid Solutions based on dedicated hardware PIUs, RTUs and SCADA concentrator gateways integrate with higher-level SCADAs (CIMPLICITY HMI/SCADA) for centralized management. GE VERNOVA offers solutions for all electrical energy domains.

3.6 Siemens Spectrum Power™- SICAM 8 Automation Platform and SICAM S8000

Siemens Spectrum Power™ is a suite of application developed for power grid management. The solution portfolio includes power production and trading, transmission management, including advanced distribution management, railway electrification, and industry and infrastructure energy management. For the substation automation domain, Siemens SICAM 8 – Power Automation Platform provides an all-in-one secure and scalable SCADA solution. Providing flexibility of choice and including uniformity for supported cases based on identical software, the solution can be deployed based on software- or hardware-based platforms.

As a tailor-made solution, the applicability of SICAM 8 includes power transmission and distribution, hydro plant, solar, wind, railway and industry. The goal is the enablement of a modular but consistent platform that is adaptable and scalable, for enabling cost savings, employs reduction of components, and includes state of the art cybersecurity. SICAM 8 use cases include communication gateway function for enabling communication to enterprise systems implementing different communication protocols. Solutions will be expanded to include microgrid, photovoltaic power plant, load shedding and self-optimizing grid. Similarly, in the future enhanced grid sensor capabilities will be added to the SICAM 8 products family [15].

For energy automation, Siemens S8000 is software-based solution that is part of SICAM 8 family. To respond to individual plants requirements, it can be deployed on industrial PC based platforms or as a fully virtualized component. This adds versatility for possible design options, enabling cost efficiency through the deployment of fit-for-purpose solutions. Multiple hypervisors and multiple operating systems are supported. Engineering software for S8000 is based on SICAM 8 manager. Communication integrity and confidentiality are provided through IPsec and advanced security functions. The platform supports CIS Benchmark Level 2 deployments. The solution enables SCADA for power automation and control, in combination with other SICAM 8 family products [16].

Table 3.5 Siemens SICAM S8000 functions, features and standards [16]

SCADA functions	Technical features	Energy communication standards
- Substation automation and control - Control and monitor HMI - Data logging and alarm management - Diagnostics and simulation - Custom applications support (SIAPPs)	- Virtualization - Linux industrial PCs - Hypervisors: VMware and Hyper-V - Up to 1200 IED integration - Digital Twin - Communication gateway - TLS and IPSEC encryption - HTTPS - NTP Client & Server - VLAN	- IEC 61850 - IEC 60870-5-104 - DNP 3.0i - Modbus - OPC UA Server - OCPP Client - IEC 62443 - IEC 62351

Similarly to the previously analyzed solution, Siemens SICAM 8 SCADA is a mature and robust business solution that can be used for managing all electrical energy production, distribution and storage use cases. Siemens' point of view for this product family is a holistic solution that combines hardware and software components that can be flexibly implemented for the setup of an optimized, fit for purpose management, control and automation solution. For the core components the flexibility is further expanded by the possibility of deployments based on a dedicated hardware platform, industrial PC hosting compute or as a fully virtualized hypervisor-based hosting solution.

3.7 ABB COM600 gateway

ABB COM600 Substation Automation Unit platform is a hardware-based appliance that allows the implementation of SCADA solutions for substations and smart grids. The features of the platform address the ANSI and IEC markets and is focused on Relion® 615 and 620 series relays. For substation SCADA solutions implementation, the COM600 platform provides WebHMI, control, visualization, monitoring, data logging, automation.

As communication gateway function, COM600 provides mapping and translation for IEC 61850 and LAN or serial-based communication for DNP3, Modbus, and IEC60870-5 protocols.

For substation visualization and control, COM600 provides single-line diagram functionality. The substation device configuration can be imported into the COM600 configuration using SCL files. Direct visualization and control of substation IEDs is enabled from the COM600 WebHMI console.

For direct remote communication and control, the IEC 61850 proxy function is supported. The communication protocol gateway function is enabled for OPC servers' model and for cross-referencing of IEC 61850 logical nodes data objects to DNP3, Modbus, or IEC60870-5 data models.

The COM600 automation event automation controller includes a programmable logic processor based on the EC 61131-3 standard. Data sources for the logic processor can be based on any of the communication protocols supported by the gateway appliance.

The event logging, alarm lists, and historian function support operator access and use of the substation generated and recorded data. The COM600 gateway includes functions for downloading and visualizing disturbance records based on the COMTRADE format.

For substation configuration testing, audit, and analysis, COM600 provides an Analyzer function that includes GOOSE application visualization and real-time diagnostics, which includes GOOSE traffic plotting and captured data recording and export [17].

Table 3.6 ABB COM600 functions, features and standards [17]

SCADA functions	Technical features	Energy communication standards
- Control and monitor WebHMI - Real time visualization - Data and event logging - Historian - Communication gateway - Analyzer	- Data object mapping and protocol translation - OPC Server/Slave - IEC 61850 proxy - SCL import/export - GOOSE intrusion and capture - Logic processor - Sequence control - Event printer - Diagnostics - Security settings - Network fault tolerance	- IEC 61850 - IEC 60870-5-101/103/104 - DNP 3.0 - Modbus - IEC 62439 - PRP

In general, the COM600 gateway offers a versatile product for implementing substation-based SCADA systems that can be integrated with external enterprise systems. The proxy and gateway function allow integration and creation of higher complexity

smart-grid systems, but as the main role the COM600 gateway is dedicated to substation automation, management, and monitoring. Except for intrinsic capabilities of IEC61850, the functions provided do not offer dedicated applicability to wind, hydro, distributed energy resources, or other applications outside the substation perimeter.

In the practical part of this thesis, COM600 gateway has been selected as the platform to enable the substation laboratory model SCADA system. The configuration and testing of the network configuration and integration, control, analysis, and protocol gateway are detailed in Chapter 5.

3.8 OpenMUC framework

The last platform included in the research performed is the OpenMUC - "Open Monitoring and Control" solution. The solution is developed by the Smart Grid Communication department at the Fraunhofer Institute for Solar Energy Systems in Freiburg, Germany.

OpenMUC is an OSGi (Open Services Gateway initiative) GPLv3 licensed open-source framework that can be used for development of SCADA systems. It implements functions that can be used for industrial control, automation, monitoring and data logging and it provides support for industrial network communication. The solution includes support message queue technologies to publish recorded data to remote brokers.

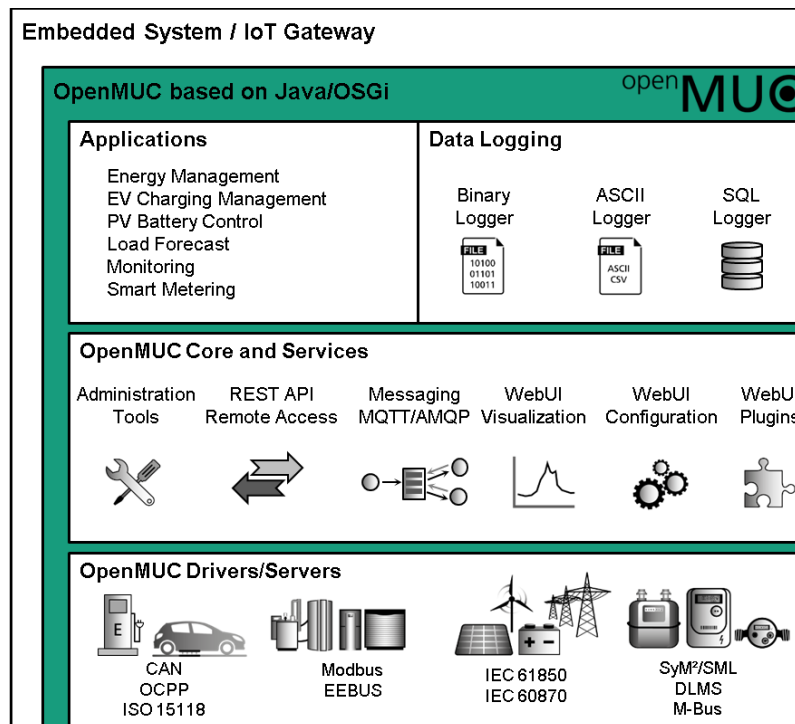


Fig. 3.5 OpenMUC framework architecture [18]

As functions, OpenMUC permits implementation of development of multiple applications which are enabled to communicate using multiple communication drivers. The communication structure is based on the driver/device/data channel hierarchy. Data sampling, listening, and logging settings can be enabled at individual channel level. For conditions requiring data normalization, data offset, and data multiplication functions are supported. A dedicated 'Math' driver allows mathematical operations on received channel data.

The platform is suited for custom made SCADA applications in environments in which Java programming skills are available for programming code creation and maintenance. OpenMUC package includes predefined applications that can be used for IED communication with minimal update or customization required. For customized applications in which visualization and control functions are required, custom code development is required.

OpenMUC IEC 61850 MMS protocol driver supports logical nodes and data object discovery. As the software package contains, out of the box, many industrial communication drivers, besides SCADA functions, OpenMUC can be used with minimal set up resources as a communication testing and communication gateway solution.

During the realization of the practical part of this thesis, the framework was deployed as a testing tool to validate the ABB COM600 communication gateway function for IEC 61850 substation data communication with an IEC 60780-5-104 remote gateway (based on the OpenMUC framework).

Table 3.7 OpenMUC framework functions, features and standards [18]

SCADA functions	Technical features	Energy communication standards
- Control and monitor HMI - Data and event logging - Messaging	- Individual driver/channel configuration - Math driver - Data plotter and visualization - Media viewer - Rest API Remote Access - OSGi/Java framework for Custom applications - Custom WebUI development	- Modbus - IEC 61850 - IEC 60870-5-104 - IEC 62056-21 - KNX - M-Bus (wired) - wireless M-Bus - eHz meters/SML - REST/JSON - SNMP - CSV - MQTT/AMQP

In summary, OpenMUC is an open-source framework that can be deployed based on small footprint resources and provides control, visualization, data logging and data gateway functions in non-commercial applications. Commercial use is possible based on licensed versions. It is design to be used for electrical power monitor and logging systems

and has data visualization capabilities. It can be used as a development and testing platform, being easy to deploy and configure. It fits well the deployment cases for monitoring and controlling small power production applications (ex: photovoltaic plants), especially as a primary data store and as a gateway for data transitions to a higher-level SCADA system.

3.9 Summary

This chapter of the thesis included research on the available SCADA solutions. Although the search was not exhaustive, the options selected have been analyzed and details presented in regards with supported SCADA functions, technical features included in the products and the supported energy domain network communication protocols and other associated standards, network redundancy and resiliency, cybersecurity or supported data models standards.

The solutions analyzed show that coverage for all energy domains is provided. This is performed either through the product's internal functions that address individual domain-specific use cases (i.e.: direct setup for hydro, wind, or DER) or through composability of the solution to add the required capabilities. Based on multiple hardware and software products (including virtualization) the aggregated solution addresses domain-specific applications.

Requirements related to resilience and high availability are addressed by all modern solutions. The certification of the cybersecurity deployment model, the integrity and the confidentiality of the data are requirements that are supported by certifications and the direct use of security standards. Physical and logical deployment models and the design of required application communication flows are also subject to being integrated into the cybersecurity design of modern SCADA solutions. These design considerations include the integration of SCADA systems with wider enterprise systems.

The ABB COM600 gateway was selected for the SCADA system implementation performed in the practical work of this thesis. Main reasons for this choice were availability as solution ready to be deployed, the small footprint required and the built-in support of the SCADA control, visualization, gateway, and analysis functions that have been selected for the implementation and testing.

Together with the ABB COM600 based SCADA deployment, two other virtualized systems have been included in the practical work: MZ-Automation GmbH C#.Net Source Code Library IEC 60870-5 and the OpenMUC framework. Both solutions have been deployed with the scope of performing the integration and testing communication based on the COM600 protocol gateway function with a remote command center solution (remote/higher-level SCADA).

4. SCADA SYSTEM IMPLEMENTATION

As mentioned above, for the implementation of the practical part of this thesis, the ABB COM600 Series 5.1 Substation Management Unit was used and configured for the implementation of the SCADA system for the laboratory substation model. ABB COM600 is a versatile product that can be used for substation and smart grid control and automation. The substation laboratory model used emulates a double bus-bar configuration with three line bays and one bus coupler bay. The substation model and its initial IEC 61850 configuration were based on the substation model defined in the thesis [19].

4.1 Overview

For the substation laboratory model, the COM600 Substation Management Unit was set up to provide IED's real-time monitoring and control, WebHMI and visualization, alarm/event logging, event reporting and historical data recording based on IEC 61850-8-1 protocols. In addition, communication gateway functions and SNTP and GOOSE intrusion servers have been implemented.

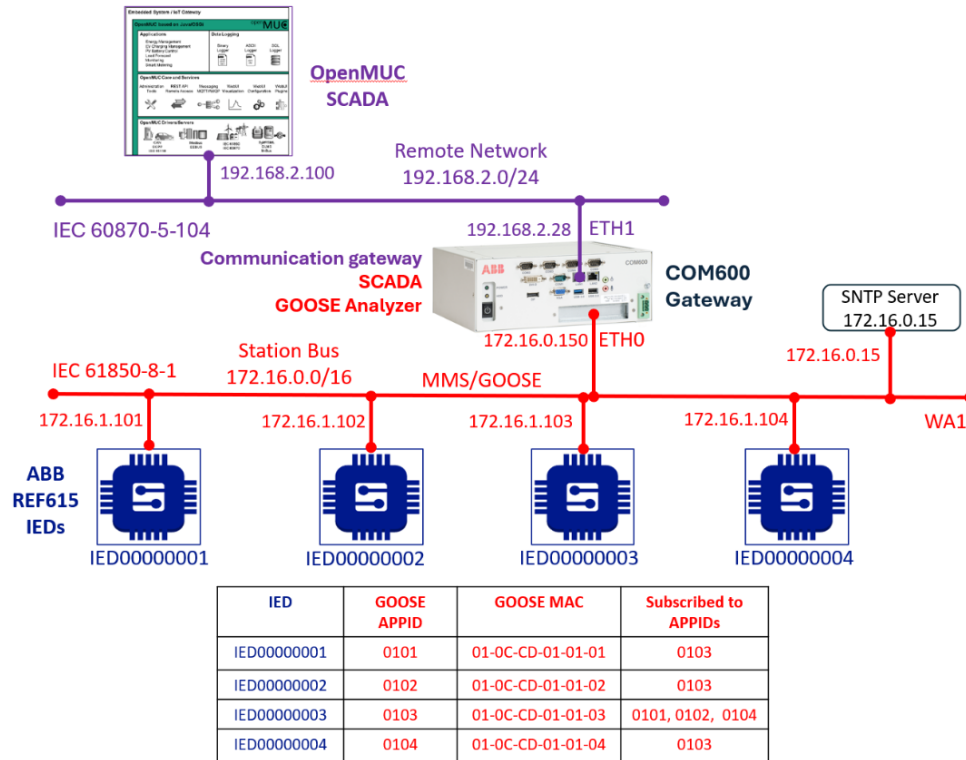


Fig. 4.1 Substation SCADA communication model [17][18]

Once the basic SCADA functions were configured, the multiprotocol communication gateway function was configured and tested. The goal was to enable vertical communication integration between the SCADA substation and a remote SCADA

network command center. The remote SCADA was deployed based on the OpenMUC platform and configured to receive operational events and status information generated at the process level of the substation model based on the communication of the IEC 60870-5-104 protocol.

For accurate time synchronization at substation level, the COM600 appliance implements a Simple Network Time Protocol server. A second server, provided by the network switch used for providing connectivity, was enabled.

For substation horizontal communication analysis, troubleshooting and logging, COM600 was configured to provide also a GOOSE intrusion server.

No network firewall or network router was deployed inside the test configuration, but for emulation of a realistic substation configuration pattern, the communication inside the laboratory model implemented two network layers that were based on distinct network subnet and IP addressing and that used, at COM600 level, distinct physical network interfaces. The network design deployed is shown in Fig 4.1.

The local station bus subnet deployed horizontal and vertical communication based on the following protocols:

- MMS for REF615 to COM600 vertical communication and for PCM600 IEDs management (tcp-102).
- GOOSE for REF600 horizontal communication and COM600 GOOSE intrusion for troubleshooting and GOOSE data collection (I2-multicast).
- SNTP for accurate time configuration (tcp-123).
- FTP for REF615 disturbance data transfer to COM600 (tcp-20, tcp-21).
- HTTP/S for COM600 WebUI functions (tcp-80, tcp-443).
- HTTP/S for SAB600 configuration/management data forward to COM600 (tcp-8080).
- IEC104 for communication to the remote OpenMUC SCADA (tcp-2404) [20].

The remote IEC104 communication to OpenMUC SCADA, was enabled from a subnet which was separated from the substation process bus. From a logical designation perspective this can be seen as a DMZ subnet which, physically and logically, separates the internal station bus network (used for substation horizontal and vertical communication), to the external networks (in the case of the laboratory configuration, from the network hosting the external SCADA system).

Substation IEC 61850 engineering and configuration applications used were ABB PCM600 for REF615 configuration and ABB SAB600 for COM600 system configuration. For the laboratory model, both tools were hosted inside the station bus network. Both PCM600 and SAB600 management tools are IEC 61850 compatible. Configuration import, export, and backup performed using these tools, being enabled based on this SCL configuration model.

COM600 implements IEC 61850 Common Data Model and Open Platform Communication Unified Architecture (IEC 62541) for enabling multiprotocol gateway

functions. Different OPC DA server and/or client processes configured and run independently for all configured communication protocol. The OPC DA communication model is detailed in Fig. 4.2.

As only IEC61850 provides semantics for its data model, OPC interfaces are translating non-IEC 61850 data models to IEC61850 model. This mapping is fundamental to enable the COM600 gateway functions.

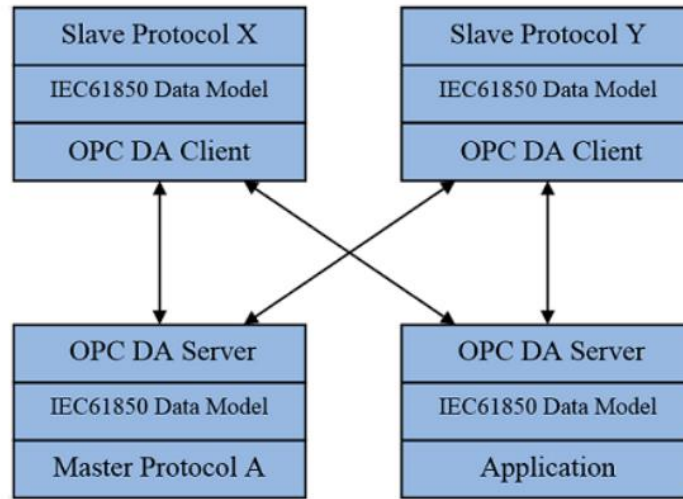


Fig. 4.2 COM600 OPC Server-Client communication model [17]

In the substation laboratory model an IEC 61850 OPC server was configured and deployed for providing communication and control of the substation REF615 terminal units (MMS based communication). An IEC 60878-5-104 protocol, slave process server was deployed to enable remote communication to the remote network command center emulated by the OpenMUC framework deployment. Additionally, SNTP, GOOSE intrusion, and Syslog OPC servers were deployed in the COM600 configuration.

Because no dedicated time source server was present in the substation lab environment, the COM600 appliance SNTP OPC server was enabled to provide REF615 IED time synchronization. Later, a secondary time server was added to the configuration for providing redundancy of the time synchronization function.

Besides IEC 61850 and IEC 60878-5-104, for Ethernet communication the COM600 gateway implements also DNP3.0-LAN, MODBUS-TCP protocols for substation automation and smart-grid communication and SNMP for network events monitor and alerting. These protocols have not been enabled and tested in the deployed configuration.

4.2 Substation bays IED configuration – PCM600 updates

For the integration with the COM600 SCADA system, the laboratory model IEDs configuration sourced from [19] was imported and updated. These updates included the IEDs IP address configuration, the NTP client configuration, the GOOSE App ID and

assigned multicast MAC addresses configuration. The IED IP addresses, which are part of the substation's Client-Server subnet configuration, have been updated as per Table 4.1.

Table 4.1 Substation IEDs IEC 61850/MMS network configuration

Access point	Subnetwork	IP	IP-Subnet	Gateway
IED00000001.LD0	WA1	172.16.1.101	255.255.0.0	192.168.2.1
IED00000002.LD0	WA1	172.16.1.102	255.255.0.0	192.168.2.1
IED00000003.LD0	WA1	172.16.1.103	255.255.0.0	192.168.2.1
IED00000004.LD0	WA1	172.16.1.104	255.255.0.0	192.168.2.1

To avoid incompatibility of the configuration with configuration models implemented by other laboratory deployments, the network subnet mask already defined for the model was not updated. Network communication with the IEDs implemented in the substation was allowed only from the local subnet. As the IEDs default gateway is configured based on an IP address external to the IP subnet to which the IED IP addresses are assigned, the implemented configuration can be seen as a simple network protection mechanism for preventing remote access to the IED network interfaces from a remote location.

4.2.1 Substation Client-Server (vertical) communication setup

The IEDs Client-Server datasets are based on default REF615 configuration. MMS data sets names or Report Controls configuration have not been updated. Fig.4.3 details the Client-Server configuration for IED00000003.

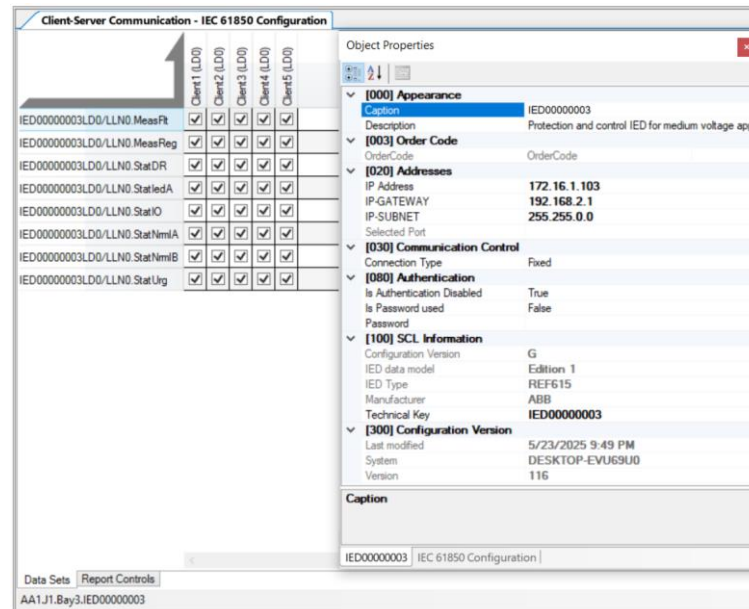


Fig. 4.3 PCM600 Client-Server Report Controls configuration

Client-Server communication based on the MMS protocol, uses Report Control blocks for sending information on data object data updates. Full communication of Report Control blocks data content, it is performed at first time a client establishes its association

with a server. Unsolicited updates are sent spontaneously, in case of an update that changes the content of the data objects data part of a specific Report Control Block. The Report Control Block Data Sets were reused and updated only for two IEDs, as detailed later in this chapter.

4.2.2 Substation GOOSE (horizontal) communication setup

GOOSE services settings have been updated for all substation IEDs. GOOSE App IDs and destination MAC addresses were reassigned. The update was cosmetic and performed for a closer logical relationship between the IED name, the IP address (last octet) assignment and GOOSE configuration parameters.

The updates performed are part of the IEC 61850 engineering process. As defined by IEC 61850-8-1 App ID (APPID - Application Identification) must be unique for the entire substation system. In the case of the substation laboratory model, REF615 IEDs have no Sampled Values blocks available, but, from a substation automation system design perspective, the App ID uniqueness requirement should be understood as including the definitions of GSE and SMV control blocks definitions [21].

IEC 61850-8-1 Annex B recommends for GOOSE multicast address selection use of the range 01-0C-CD-01-00-00 to 01-0C-CD-01-01-FF. The multicast addresses configured for the substation model were set up according to this recommendation.

Table 4.2 Substation IEDs GOOSE communication configuration

Application	Dataset	Access point	GOOSE APP ID	GOOSE MAC Address	Sub network	VLAN ID	VLAN Priority
IED00000001LD0/LN0.gcbFEEDER	FEEDER	LD0	0x0101	01-0C-CD-01-01-01	WA1	000	4
IED00000002LD0/LN0.gcbFEEDER	FEEDER	LD0	0x0101	01-0C-CD-01-01-02	WA1	000	4
IED00000003LD0/LN0.gcbBUS_COUPLER	BUS_CUPPLER	LD0	0x0101	01-0C-CD-01-01-03	WA1	000	4
IED00000004LD0/LN0.gcbFEEDER	FEEDER	LD0	0x0101	01-0C-CD-01-01-04	WA1	000	4

Similarly, the GOOSE App IDs were updated and defined in accordance to IEC 61850-8-1 Annex C.2 which recommends for GOOSE Type 1 - Ethertype value 88-B8 (hexadecimal) use for App ID definition the range 0x0000 to 0x3FFF.

Fig. 4.4 details the IEC 61850 GOOSE configuration, with communication settings details for IED00000001.

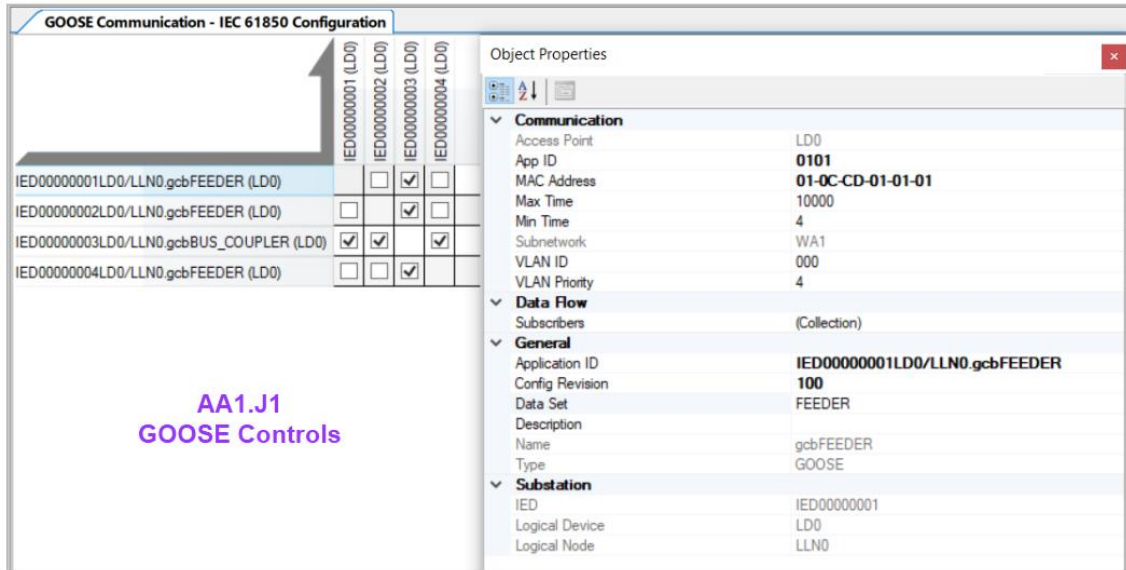


Fig. 4.4 PCM600 GOOSE configuration

As the original PCM600 substation configuration model sourced from [19] included a partial interlocking and control configuration, the configuration was updated so that the substation bay operations correspond to the logic required for implementing correct interlocking and control blocking operations.

4.2.3 Substation SNTP configuration

As part of the substation infrastructure configuration, the network switch hosting the substation automation system Ethernet connections and the COM600 server have been configured as SNTP servers and provide time synchronization information to REF615 IEDs, for which the Time configuration has been updated to include as time sources 172.16.0.15 (network switch SNTP server) and 172.16.0.150 (COM600 SNTP server).

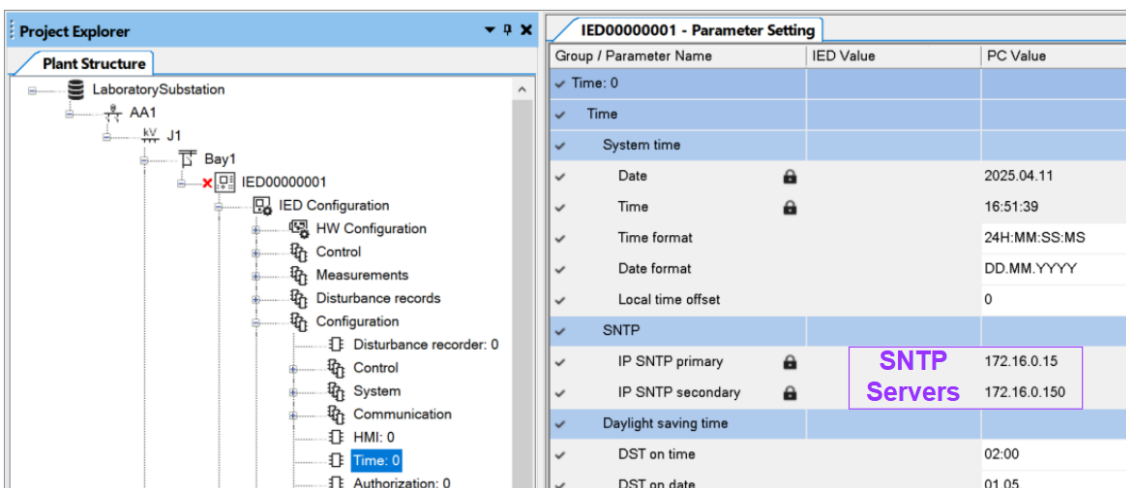


Fig. 4.5 PCM600 SNTP configuration

COM600 SCADA appliance can be configured as SNTP client and SNTP server. For testing both use cases, COM600 was configured to act as an SNTP client and receive time information from the network switch, and as detailed before, act as an SNTP server and provide time information to REF615 IEDs (secondary source).

4.2.4 PCM600 substation model SCL configuration export

Once PCM600 substation configuration was completed an SCD export of the entire IEC 61850 laboratory model settings was performed. The substation model is based on IEC61850 Edition 1, the SCD export was done based on this version. The *PCM600_LaboratorySubstation.scd* file is attached as an Appendix A of this document.

For the instantiation of COM600 configuration the *SubstationLab.scd* SCD file was imported for integrating the substation IEC 61850 configuration to the COM600 SCADA services configuration. For COM600 configuration the SAB600 engineering application was used, as per the details included in the next section.

4.3 SAB600 configuration wizard

ABB Substation Automation Builder - SAB600 is a dedicated engineering tool required for configuring COM600 appliances. Similarly to the configuration model implemented by ABB in the PCM600 tool used for configuration management of REF615 terminals, SAB600 is used to instantiate and update the COM600 configuration.

During the initial configuration instantiation process, network connectivity to COM600 is required to enable the online discovery of the substation management unit capabilities and for the discovery of licenses (Read License).

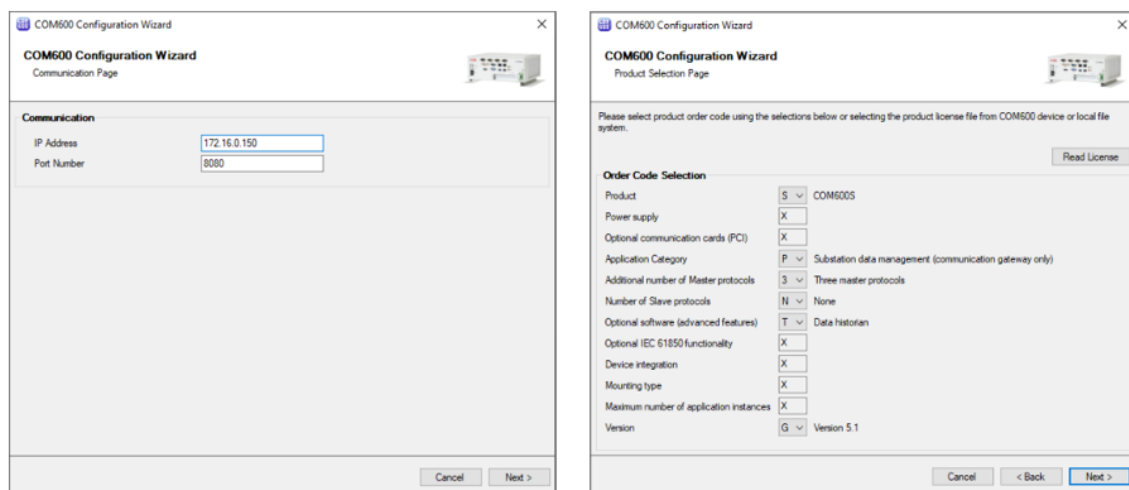


Fig. 4.6 COM600 Gateway communication setup

The configuration continued with the definition of the first OPC server, through the import of the substation SCD file (generated through the PCM600 substation configuration export). A single IEC 61850 OPC server was activated as part of the SCADA system configuration.

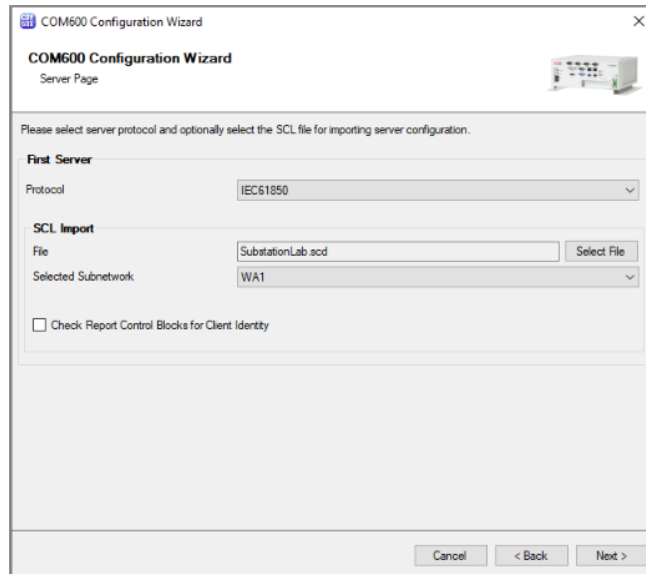


Fig. 4.7 COM600 substation SCD configuration import

In the next steps of the configuration wizard, two additional OPC servers were defined. The configuration of the COM600 OPC server can also be performed after the initial gateway configuration instantiation. For the laboratory model setup, the entire substation IEC 61850 configuration was imported. Creation of all required OPC servers is not required during the initial configuration wizard. All settings can be applied separately after the wizard is complete. The last step of the initial configuration wizard process is the selection of additional servers to be created during the wizard. In the laboratory model configuration instantiation process the SNTP server has been selected to be created and configured, followed by the display of the summary of the configuration defined during the wizard process, as detailed in Fig 4.8.

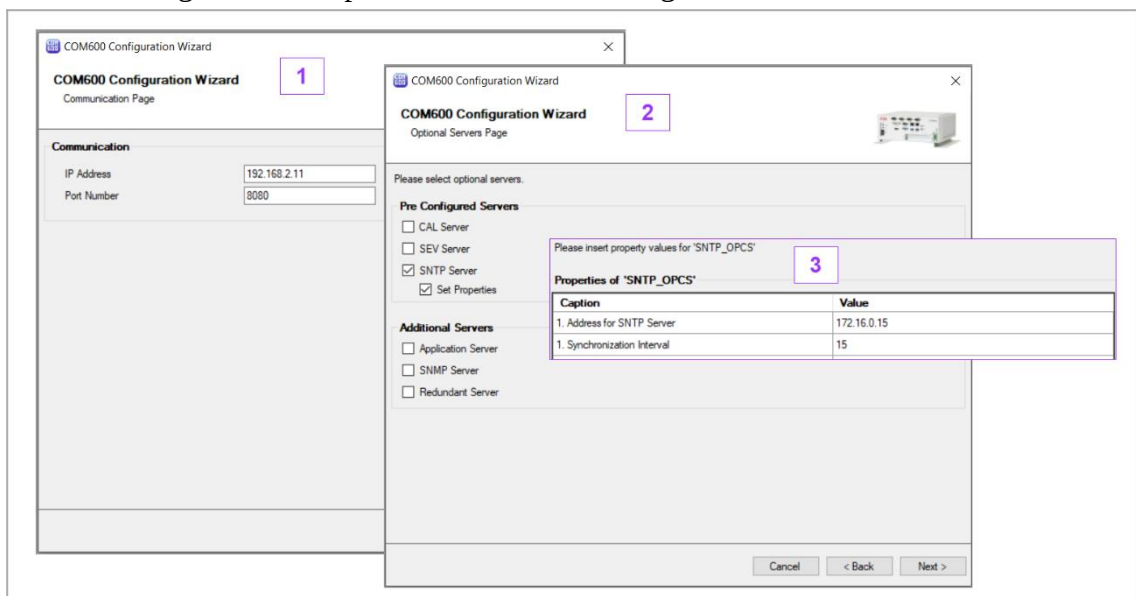


Fig. 4.8 COM600 SNTP OPC server setup

This completes the initial configuration wizard process, the laboratory substation SCADA services setup continued in the main SAB600 application console for the definition of additional service properties that were not included in the wizard process.

4.4 SAB600 SCADA services configuration

COM600 configuration is based on the two main SAB600 application interface tabs: Communication, defining communication properties of configured OPC servers, and the Substation Structure tab.

This Substation Structure tab enables configuration of the single line diagrams that will be available in WebHMI, the GOOSE analyzer intrusion properties or IEC 61850 logical nodes and data objects properties that are part of the IED control settings or of the substation data collection and logging.

Using Object Properties menu the COM600 gateway caption was updated from “Gateway 5.1.x” to “COM600 SCADA”. Management configuration control options are available only when SAB600 has online network connectivity to the COM600 gateway.

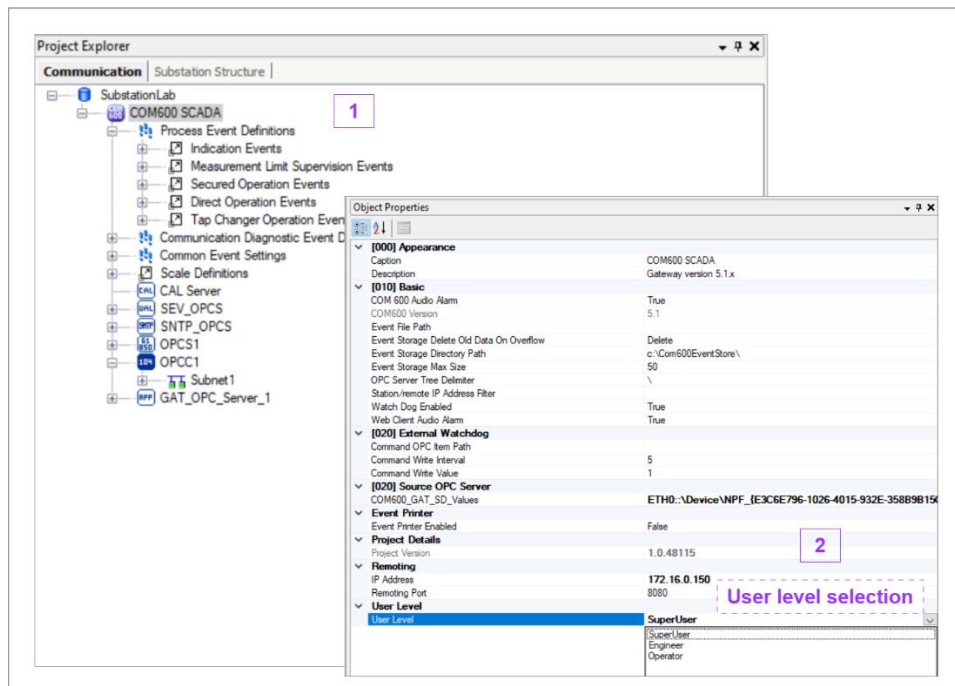


Fig. 4.9 COM600 SCADA server properties

SAB600 configuration is based on three access levels that enable application users for managing the COM600 gateway configuration: “Operator”, “Engineer”, and “SuperUser”. Fig.4.9 details the selection of the user privileges level as part of gateway server configurable properties.

For the COM600 SCADA services set up, the default Engineer level was used. This user level is sufficient for performing all the configuration tasks required for the substation laboratory model. The availability of the three profiles provides flexibility for

the integration of SAB600 configuration tool in the substation engineering process and enables that, during regular operations, inadvertent configuration changes are prevented if the operator role is used for operations in the SAB600 application.

During the initial SAB600 configuration wizard the OPC SNTP server service was set up. This enabled the COM600 gateway to act as an STNP client. For the laboratory model SCADA, the SNTP server was enabled. This is done by updating the SNTP_OPCODES Server parameter '*Enable Time Synchronization Server = True*', available in the server's object properties, as shown in Fig.4.10. With these settings, STNP clients present on the laboratory substation network will synchronize time information also with the SCADA server.

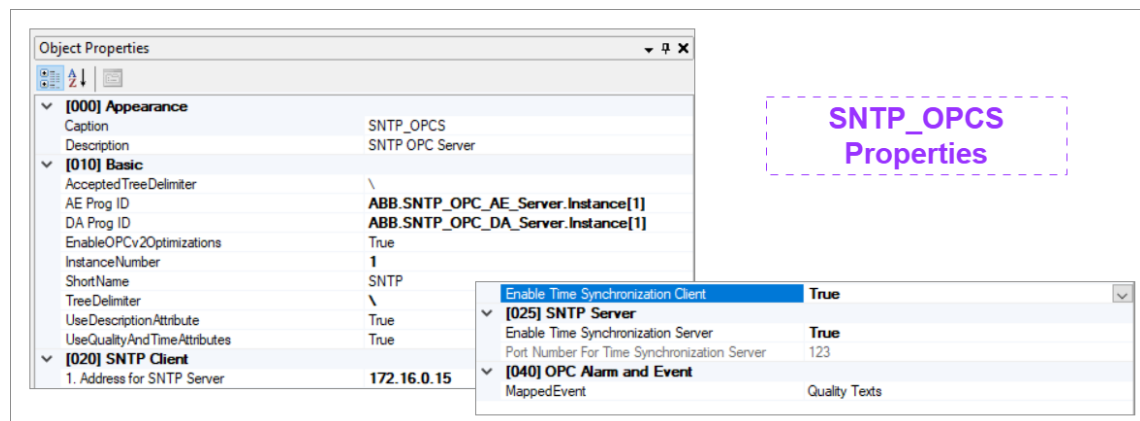


Fig. 4.10 SAB600 SNTP configuration

Besides protocol or process-based requirements, accurate time synchronization is important for correct time correlation of the SCADA generated and recorded events. This is important, especially for cases where logging functions are distributed among several systems.

4.5 SAB600 substation configuration

The next step of the SCADA system configuration process was the update of the substation structure. This is a two-step process, in which, first, the Single Line Diagram (SLD) of the substation was defined, followed, secondly by the setup of IEC 61850 data connection configuration for the objects defined in the SLD.

The SCL file used for the import of the IEC61850 configuration of the substation contains the SLD definitions for the bays/IEDs. As a result of the import, the initial COM600 SLD contained the imported objects but had a wrong representation of these objects in the SLD. Corrections were required for objects overlaps and for incorrect or incomplete definition in the SLD.

If SLD objects of the different IEDs have the same location in the COM600 SLD they will overlap in the overall substation level view. To correct this, the SLD diagram of each bay was updated, and the SLD objects moved in the diagram canvas to their proper

diagram location. In this process, the additional conducting equipment such as bus bars and connectors or missing switch gear objects such as circuit breakers, disconnect switches or earthing switches were added to individual bays configuration, as necessary.

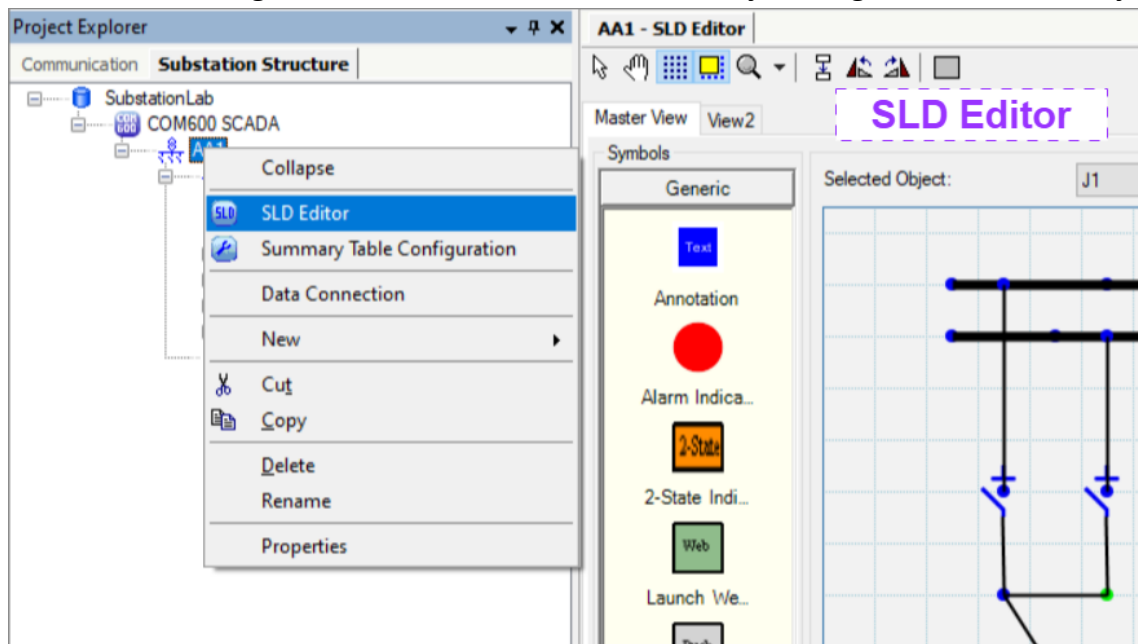


Fig. 4.11 SAB600 single line diagram update

After all the SLD objects were defined and placed in the diagram, the substation structure configuration continues with Data Connection definition for Logical Node associations with required SLD objects. Fig. 4.12 details LN associations for the Bay2 IED.

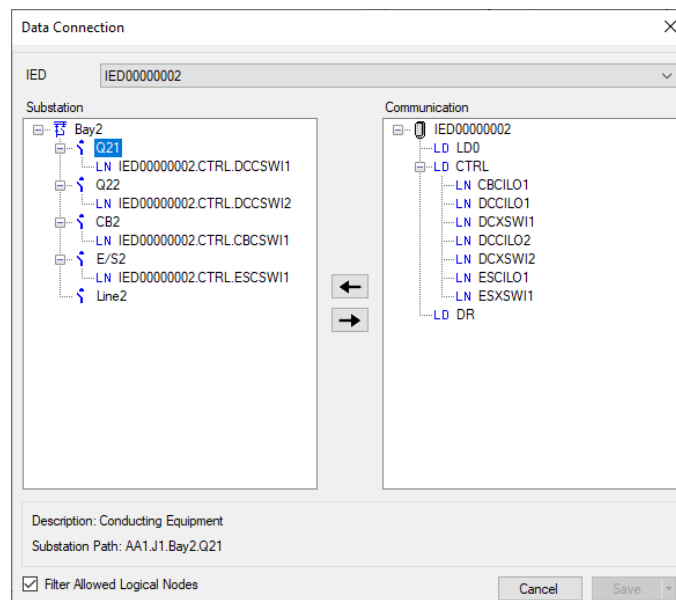


Fig. 4.12 SAB600 SLD Logical Nodes association

The result of the substation structure update steps is a valid substation visualization and correct IEC 61850 control configuration which can be uploaded to the COM600 unit. As shown in Fig. 4.13, the updated substation SLD included all bays present in the laboratory substation model. The logical nodes data objects associations to switch gear SLD objects enabled the visualization of their functional state and their control from COM600 SCADA WebHMI.

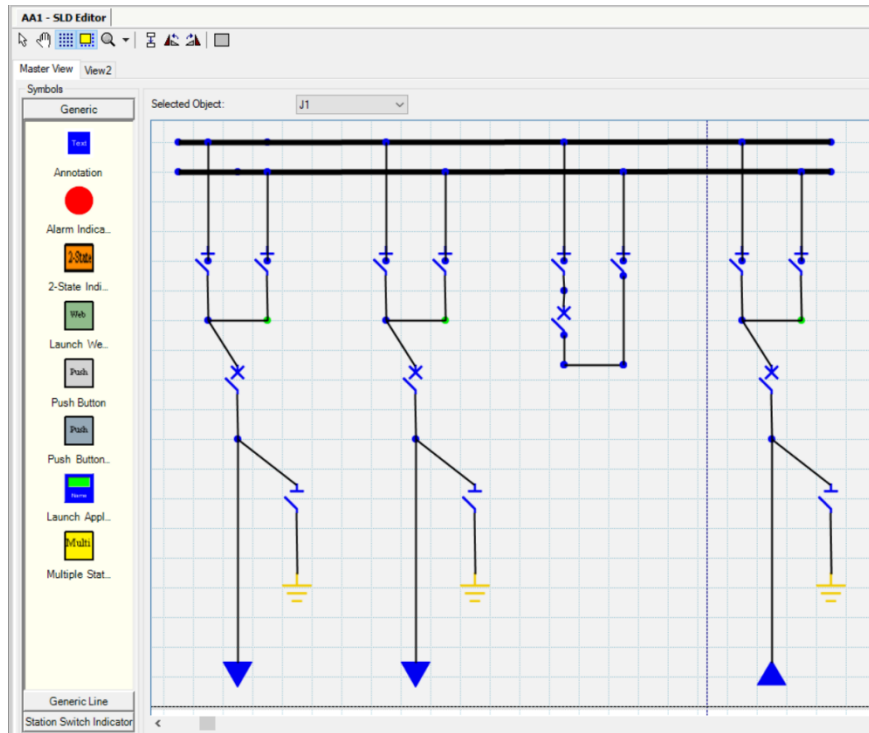


Fig. 4.13 SAB600 laboratory substation SLD

The update of the running configuration of the COM600 gateway was performed in Project Explorer by selecting gateway Management option and by deploying the configuration using Configuration control options menu. The successful deployment of the configuration on the COM600 unit is confirmed at the end of the update process.

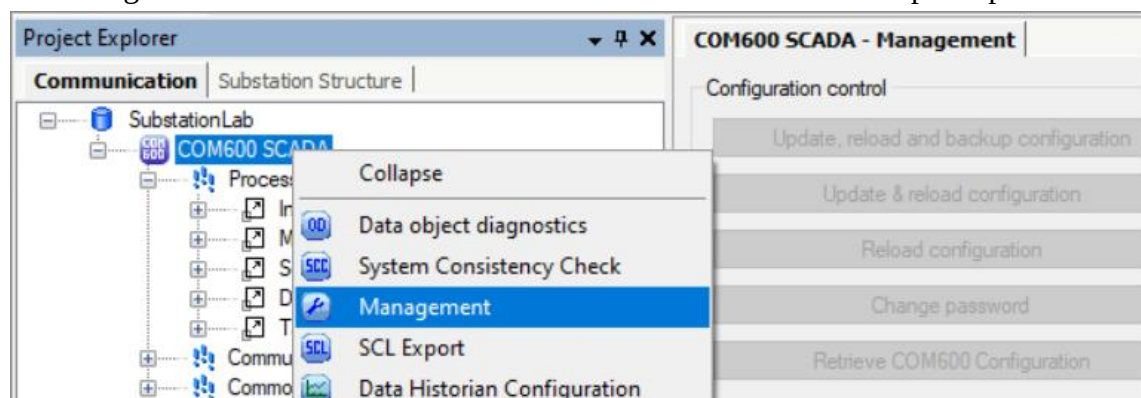


Fig. 4.14 COM600 gateway configuration update

Once services are reloaded, the COM600 WebHMI client interface was used for performing supervisory and control operations on the laboratory substation IEDs, as shown in Fig. 4.14. The single line diagram provides visualization of the status and allows control of the IEDs functions in the substation.

Multiple SLD views can be defined based on SAB600 SLD configuration. SLD view in COM600 WebHMI can be substation-wide or focused on individual substation bays. The single line diagram allows visualization of the status and allows control of the IEDs. As displayed in Fig. 4.15 the „select before operate” (SBO) control model was implemented for the Bay2 disconnector switch Q21.

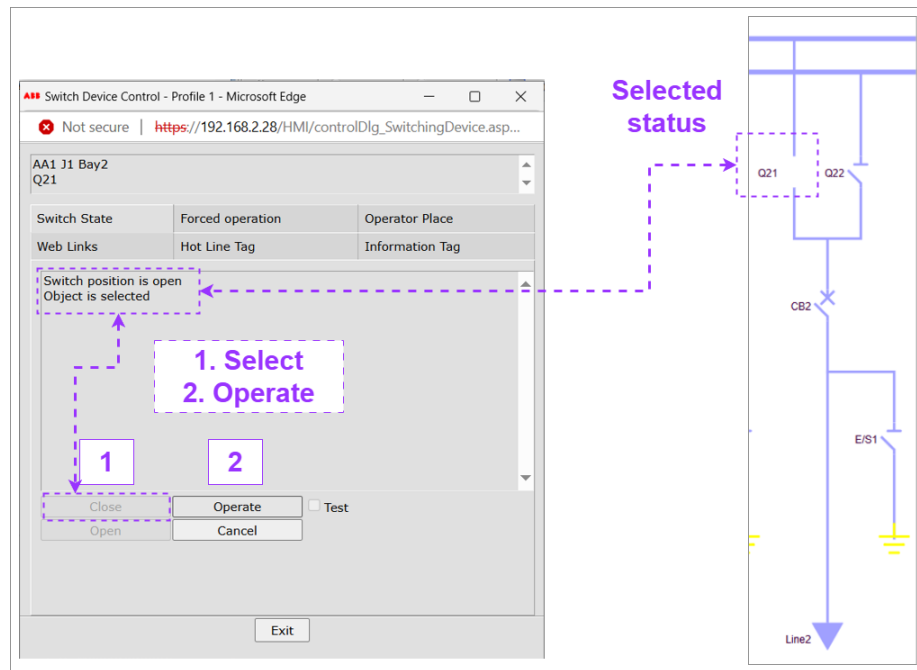


Fig. 4.15 COM600 WebHMI console SLD

As shown in Fig. 4.16. the 'Substation' menu provides access to Alarms and Events recorded for the substation bays.

Date	Time	Bay	Device	Object Text	Event
11. 3. 2025	18:28:23.089	Bay3	IED00000003		acknowledged
11. 3. 2025	18:28:23.089	Bay4	IED00000004		acknowledged
11. 3. 2025	18:28:23.088	Bay2	IED00000002		acknowledged
11. 3. 2025	18:28:23.088	Bay1	IED00000001		acknowledged
11. 3. 2025	18:18:21.913	Bay3	Q32	I<->O DCC(2) switch position	Open
11. 3. 2025	18:18:18.636	Bay3	Q31	I<->O DCC(1) switch position	Open
11. 3. 2025	18:18:16.267	Bay3	CB3	I<->O CB(1) switch position	Open
11. 3. 2025	18:18:04.897	Bay3	CB3	I<->O CB(1) switch position	Closed

Fig. 4.16 COM600 WebHMI console SLD

Fig. 4.17 shows a problem discovered during the testing of the IEDs control operations. An issue affected the control state of the IED00000001 and IED00000004.

These IEDs were not controllable with a „quality bad“ status being reported for all logical nodes that are part of the IED's CRTL logical device.

No indication of network communication quality was found and accurate time synchronization of the IEDs with the SCADA server has not eliminated the issue.

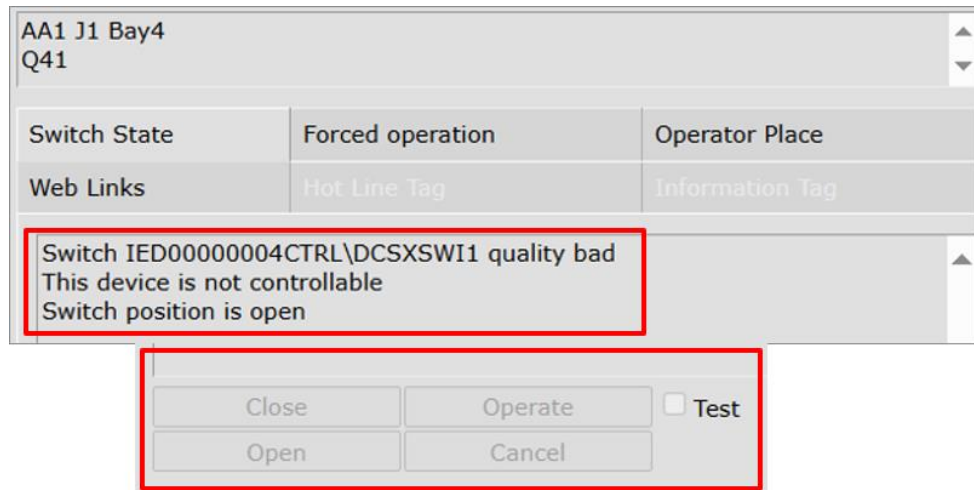


Fig. 4.17 COM600 control issue for IED00000004

The issue was identified as being caused by two sources that impacted the control status of the IED. The first issue was related to the fact that the data object CTRL/LLN0.LocRem (ST) and CTRL/LLN0.LocSta (ST) was missing from the IED's LD0/LLN0.StatUrg data set.

The addition corrected the issue for WebHMI control status "Remote", control operations being possible on both IED00000001 and IED00000004.

The second issue was related to the fact that the affected IEDs do not support multilevel control operations. Control of these IEDs from the COM600 WebHMI console under control status 'Station' was not possible. An indication that this was a software issue is the fact that both IEDs had no status functional constraint associated with the LLN0.StaAuth data object. This issue for „Station“ level control was not fixed, as a software update of the IEDs was not possible.

The "Remote" control status of these devices was used for the implementation of the substation testing.

SAB600 configuration „SAB600_Exported_Project_SubstationLab.pcmp“ file was attached to the Appendix A of this thesis.

4.6 COM600 communication gateway configuration

Electrical substations SCADA systems are deployed and integrated into larger enterprise systems which are enabled to receive substation status, monitor and alarm information and to execute remote control operations. The data communication between such remote systems is enabled through standard protocols, the most common ones being

DNP3 or IEC 60870-5-104 protocols using Ethernet based high bandwidth communication.

As these protocols employ different data representation, data object mapping to the IEC 61850 data model content is required. IEC 61850 MMS protocol can communicate over routed networks with remote systems, but it is not used for this purpose. IEC 61850 was designed as a substation level protocol. It has advantages over legacy protocols, but adoption to use beyond the substation was hindered by its additional complexity. As a communication protocol with remote command centers its use would require implementation of additional logical nodes modeled based on IEC61850 [22].

In the substation laboratory model, IEC 60870-5-104 protocol was used for testing the COM600 communication gateway function for communication with an external SCADA system.

4.6.1 OPC Client for IEC 60870-5-104 Slave configuration

For enabling COM600 SCADA communication to the remote OpenMUC SCADA, an IEC104 Slave OPC Client was configured. This was done by adding the new IEC104 Slave object to the COM600 SCADA gateway configuration.

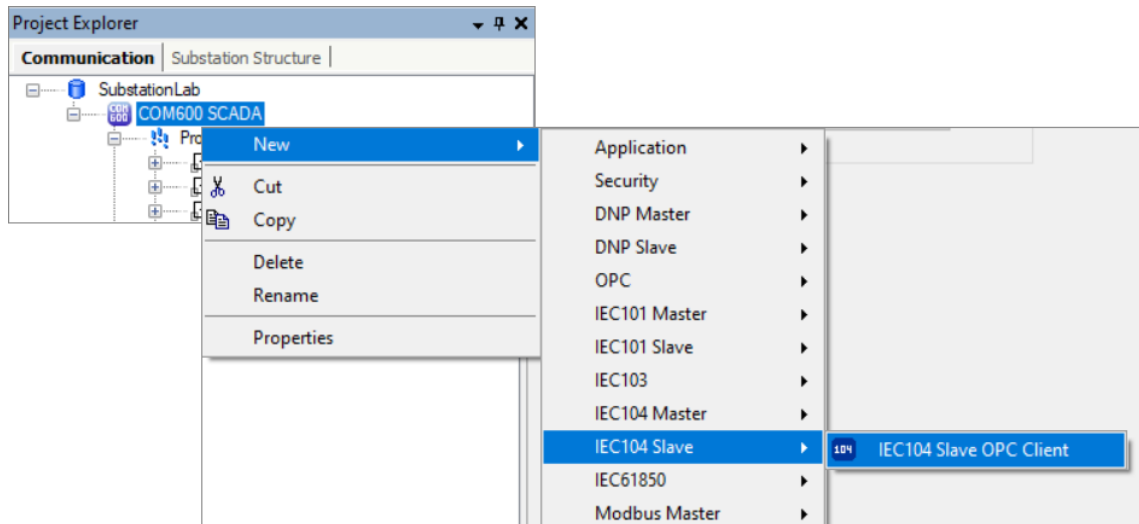


Fig. 4.18 SAB600 IEC104 Slave OPC client service addition

This was followed by the addition of a new IEC104 subnet (channel) and a new IEC104 IED that represent in the data communication design the remote IEC104 enabled SCADA system. The resulting substation structure is shown in Fig. 4.19.

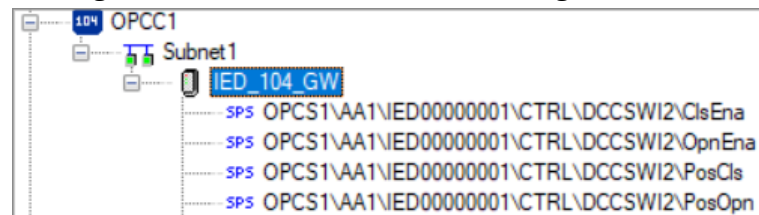


Fig. 4.19 SAB600 IEC104 Slave OPC client

For a functional configuration, the IEC104 Slave OPC Client object contains a subnet and an IEC104 IED. The OPC client properties contain the Basic configuration properties for the OPC server. The “SuperUser” profile is required to update these properties in the COM600 gateway configuration. The parameters of the station/remote switch profile can be updated based on the Engineer profile, active in the configuration demonstrated in Fig. 4.20. To enable secure operations of the substation bays, the Station/Remote Switch Error setting was set to “*Reject commands if position bad or unknown*”.

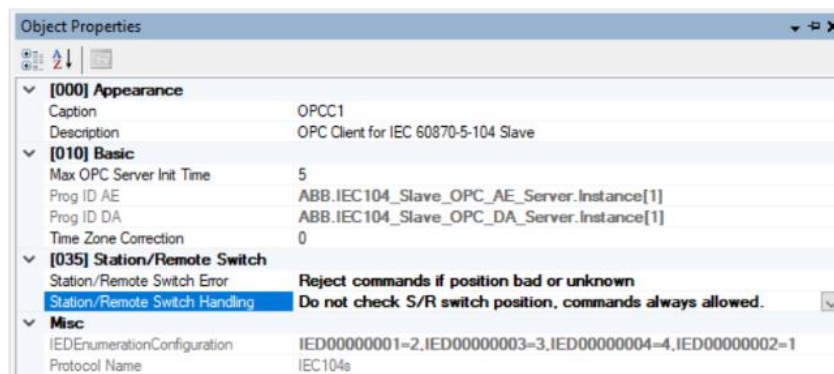


Fig. 4.20 SAB600 IEC104 Slave OPC client details

The subnet *Subnet1* object defines the network configuration for IEC104 profile at the COM600 gateway level. The IEC104 communication is enabled based on the DMZ IP address of the COM600 gateway 192.168.2.28 and, as a communication authorization mechanism, the network connections can be filtered to enable connectivity only for defined remote IP addresses.

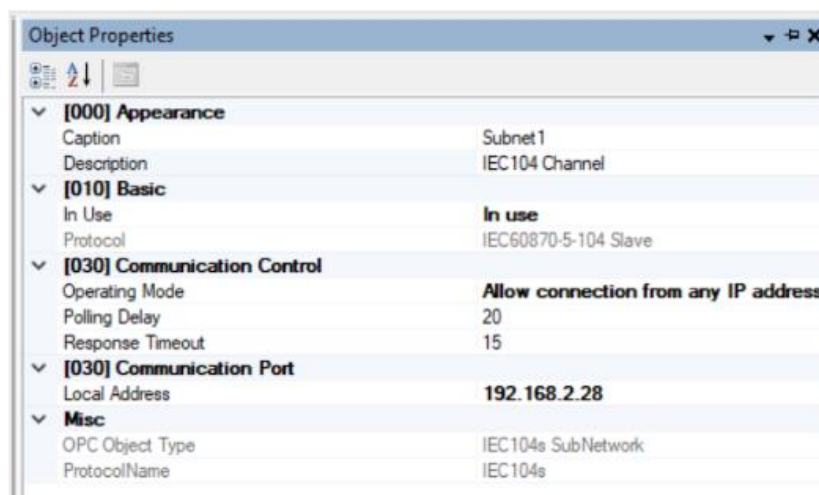


Fig. 4.21 SAB600 IEC104 channel (subnet) configuration

The virtual IED IED_104_GW enables the substation communication structure for the remote OpenMUC SCADA system and defines the general IEC104 communication parameters. As displayed on Fig. 4.22 four remote IEC104 clients can be associated with this object. The OpenMUC client IP address defined was 192.168.2.100. The IEC105

communication with the remote station can be disabled or updated to include a configuration for link redundancy.

The configuration options available include the definitions of IEC104 communication parameters such as the Station Address (SA), the Information (Object) Address Length, the Length of Cause of Transmission, the Maximum Message Length, and Station Address Length.

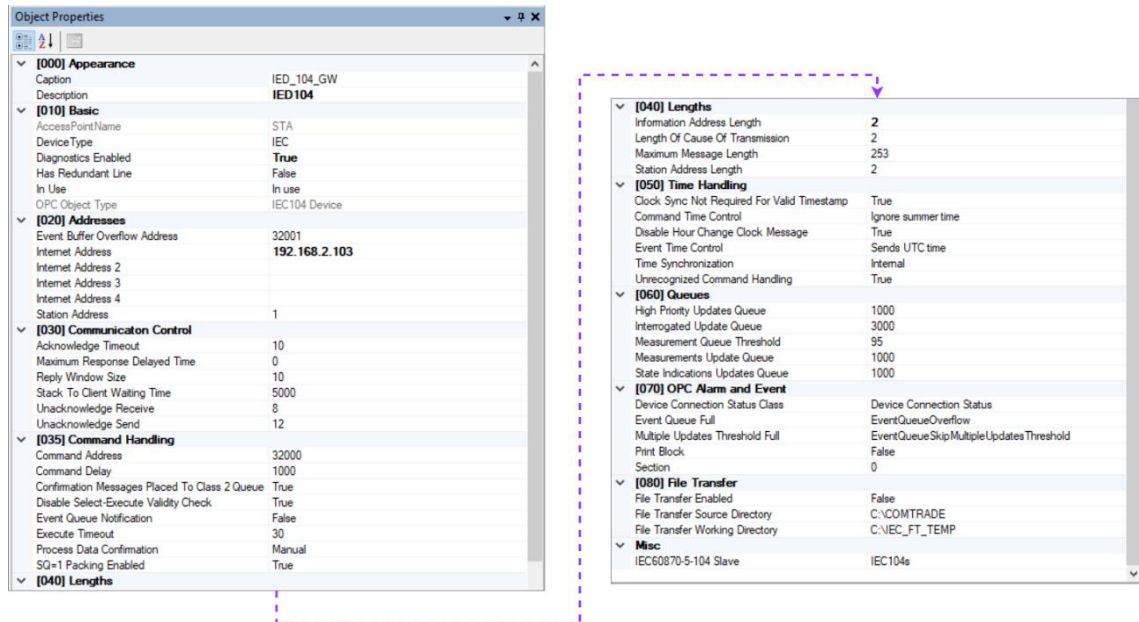


Fig. 4.22 SAB600 IEC104 IED properties

The Communication Control settings permit TCP communication profile tuning based on the network round-trip time and available network bandwidth for the communication with the remote host. Higher round-trip time requires higher time-out values, higher network bandwidth available permits a larger acknowledgment window size, enabling less communication overhead and, in a more efficient data transfer. For the laboratory substation model, no update of the communication profile was required.

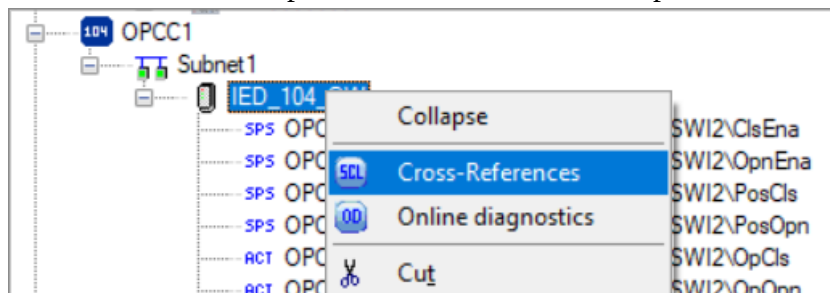


Fig. 4.23 SB600 IEC104 IED Cross-References menu

The IEC104 Slave OPC Client, the IEC104 subnet and the IEC104 IED contain the basic IEC104 network protocol configuration settings for enabling the communication to the remote OpenMUC SCADA system. As IEC104 is based on a different data model, for enabling application communication IEC104 IOAs mapping to the substation IEDs

logical node data objects is required. This operation was performed using the IED_104_GW Cross-References function, as shown in Fig. 4.23.

The cross-reference's setup is a two-step process. First, the required data object was selected from the IEC 61860 OCP server - IEC subnet – Bay IED - Logical node structure and dragged and dropped in the IED_104_GW Cross-References table. In the second step, the IOA addresses assignment are set for the IEC104 mapped data object.

iedName	IdInst	InClass	doName	Object Nam	Description	61850-Type	SubType	Indication Address
OPCS1AA1IED000000001	CTRL	ESCSwI1	Pos	OPCS1AA	Controllabe	DPC	BASIC	141
OPCS1AA1IED000000001	CTRL	ESCSwI1	OpOpn	OPCS1AA	Protection A	ACT		
OPCS1AA1IED000000001	CTRL	ESCSwI1	OpCls	OPCS1AA	Protection A	ACT		
OPCS1AA1IED000000001	CTRL	ESCSwI1	PosOpn	OPCS1AA	Single Point	SPS		144
OPCS1AA1IED000000001	CTRL	ESCSwI1	PosCls	OPCS1AA	Single Point	SPS		145
OPCS1AA1IED000000001	CTRL	ESCSwI1	OpnEns	OPCS1AA	Single Point	SPS		146

Fig. 4.24 SAB600 IEC104 Cross-References set up

Data attributes contained in a logical node data object will require assignments of individual IOAs IDs. The General table view contains all cross-referencing parameters. The data objects can be reviewed and updated using the common data class tab groups of the cross-references table.

The assigned IOAs values should be part of the address range of values enabled by the Information Address Length configuration. The range can contain values starting from 1 up to $8^n - 1$, where n is the number of bytes defining the Information Address Range parameter of the IEC104 IED object. The contextual help available in the cross-reference table displays the range of IOA values as 0 to 16777215, irrespective of the configured IED Information Address Length parameter. Given the implemented configuration, attention should be paid to respecting the maximum value allowed for the IOA length.

For the laboratory substation model, a two-byte Information Address Length was set up. The available range for IOA addresses assignments being 1 to 65535. The two-byte configuration was chosen for compatibility with the OpenMUC framework configuration. The file “*IED_104_GW_23_5_2025_12_24_14.xls*” containing the complete IOA mapping of the laboratory substation model IEDs logical nodes data objects was enclosed to Appendix A of this thesis.

Next the IEC104 configuration of the remote SCADA system was performed, as per the details in the next section.

4.6.2 Remote SCADA configuration - IEC 60870-5-104 protocol

The remote IEC104 SCADA function was implemented based on the OpenMUC software framework installed on the Raspberry PI 4 integrated computer (PI OS 64-bit operating system). The Java framework was installed as a prerequisite for OpenMUC deployment. The installation instructions available at: <https://www.openmuc.org/openmuc/user-guide/>.

As shown in Fig 4.27 the OpenMUC driver configuration requires insertion of the driver ID “*iec60870*” (the default connect retry interval is 60 seconds). The OpenMUC configuration is similar for IEC 61850 driver (“*iec61850*”).

Driver configurations:

Driver ID * iec60870 N.A. **	Channel Address ca=1; t=3; ioa=311 Synopsis: ca= <common_address>; t= <type_id>; ioa= <ioa> [dt= <data_type>] [i= <index>] [m= <multiple>] [s= <select>]
Sampling Time 0 0 (unlimited) **	ID * COM600_SlaveStation N.A. **
Connect Retry 60000 60000 (60s) **	Channel Type BYTE_ARRAY DOUBLE **
Description N.A. **	Value Length 2 N.A. **
Disabled ☐ False **	Device Address ca=1 ;p= 2404; h= 192.168.2.28 Synopsis: [ca= <common_address>] [p= <port>] [h= <host_address>]

Fig. 4.27 OpenMUC IEC60870 communication configuration

For the remote device configuration (COM600 station), the IEC 60870 Device Address configuration was set up: “*ca=1 ;p= 2404 ;h= 192.168.2.28*”.

The last step is the configuration of the data channels. This is used for interrogation of the remote COM600 SCADA IEC104 OPC server. The mapping required corresponds to the COM600 internal substation cross-reference IEC104 IED mapping as shown in Fig. 4.24.

For the channel “*OPCS1_AA1_IED00000003_CTRL_CBCSWI1_Pos*” (IOA 311), the Channel Address configuration required was: “*ca=1; t=1; ioa=131*”, channel type “*Byte_Array*”, value length “2” (bytes).

The ASDU type number (CDC DPC type “3” in this example) should match the remote IOA ASDU type. The OpenMUC channel data type needs to match the CDC of the remote logical node data attribute and the corresponding cross-referenced IOA.

Fig. 4.28 displays the one data attribute data set (PCM600 and IED), the cross-referenced IEC104 mapping at level of COM600 gateway, and the channel data, as received by the OpenMUC channel.

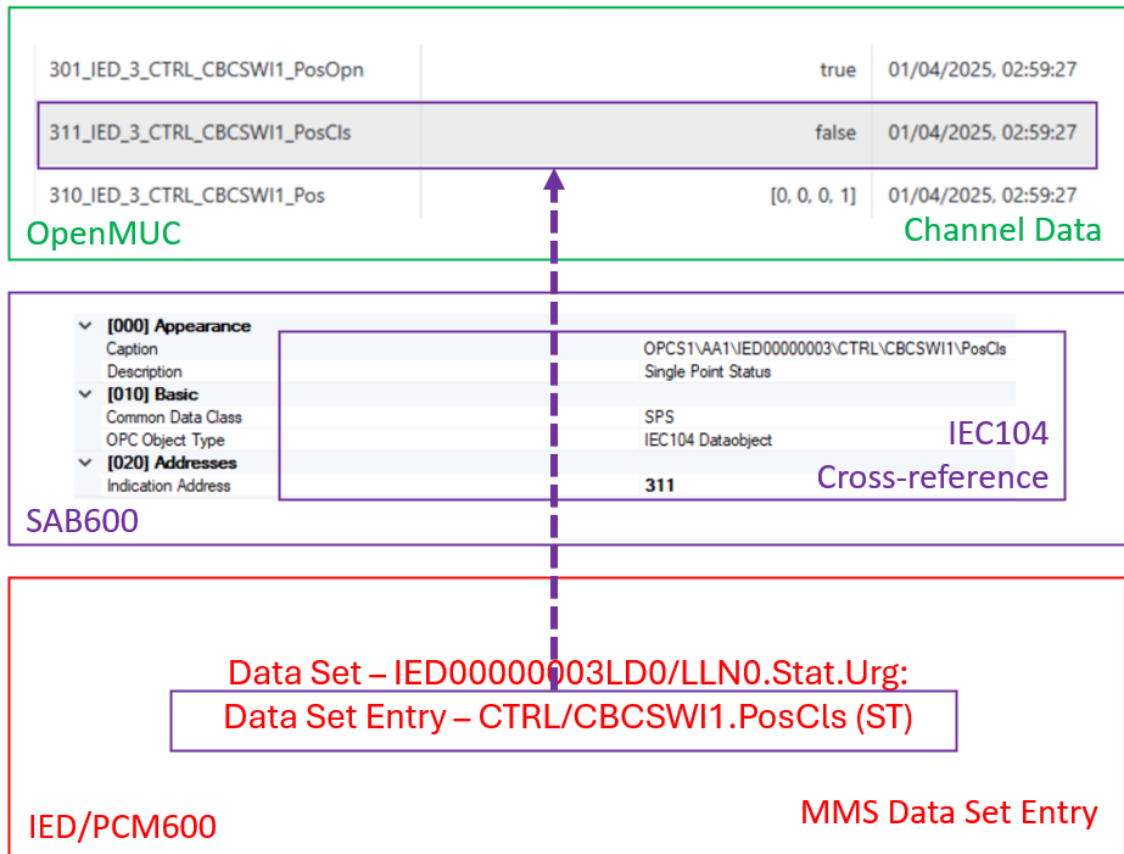


Fig. 4.28 IEC61850 to IEC60870 communication data flow

The view is an example to detail the inherent loss of object contextual information when translating from IEC 61850 semantics to pointer-based data model used by the legacy communication protocols, like IEC104.

4.7 Summary

This chapter details the configuration of the selected SCADA solution for the laboratory substation model. The configuration started with the implementation of the substation IEDs configuration. The initial SCL configuration of the substation was sourced from a previous master thesis. This was updated to fit the SCADA system deployment requirements.

The SCADA system configuration continued with the import of the SCL substation and the configuration of the ABB COM600 Substation Management Unit services. COM600 SCADA services have been configured and enabled to implement the SLD substation, IED control configuration, time synchronization services, and communication gateway function.

The test discovered control issues affecting two of the IEDs. A hypothesis of the cause of the 'Station' control issue (not resolved) was presented. A solution was found in the IED configuration to resolve the 'Remote' control model issue.

5. ANALYSIS OF THE LABORATORY MODEL COMMUNICATION

The network protocols communication troubleshooting is an integral part of the IEC 61850 substation. Dedicated tools are available for being used in all stages of design, implementation, commissioning, and operations. In the initial phases of design and engineering, the emphasis is placed on validation of the logical configuration. In the later stages of substation deployment, commissioning, and operations, functional and communication testing is required. This includes analysis of network protocols communication.

The goal is to analyze and confirm the correct substation control, protection, and communication functions. Dedicated network analysis functions and tools for performing the monitor or troubleshooting of the substation network communication are used.

This chapter focuses on an analysis of the IEC 61850-8-1 MMS and GOOSE and IEC-60870-5-104 network protocols.

The theoretical information used in this chapter for the analysis of the IEC 61850 protocols communication were sourced from [23]. The Wireshark application version 4.4.6 (v4.4.6-0-gaebb20483889) was used for network communication capture and packets inspection and analysis. Protocol inspection and decoding figures displayed in this chapter use outputs from the Wireshark console.

5.1 MMS communication analysis

The goal of the analysis is the confirmation of the MMS session establishment parameters by comparing the SCL settings of the COM600 SCADA and the substation model bays REF615 IEDs.

For analyzing the MMS communication, a traffic capture was set up inside substation network. A network monitor function was implemented at the substation network switch level, and traffic for the monitored host was redirected to a network port attached to a computer running the Wireshark application.

All network communication that takes place between COM600 SCADA (IP address 172.16.0.150) and IED00000003 (172.16.1.103) was redirected and captured for analysis.

The client-server communication configuration of COM600 SCADA OCPS1 server IED is shown on Fig. 5.1.

```

<ConnectedAP iedName="OPCS1" apName="OPCS1:ETH0">
  <Address>
    <P type="IP" xsi:type="tP_IP">127.0.0.1</P>
    <P type="OSI-TSEL" xsi:type="tP_OSI-TSEL">00000001</P>
    <P type="OSI-SSEL" xsi:type="tP_OSI-SSEL">0001</P>
    <P type="OSI-PSEL" xsi:type="tP_OSI-PSEL">0001</P>
    <P type="OSI-AP-Title" xsi:type="tP_OSI-AP-Title">1,3,9999,23</P>
    <P type="OSI-AE-Qualifier" xsi:type="tP_OSI-AE-Qualifier">23</P>
  </Address>
</ConnectedAP>

```

Fig. 5.1 COM600 OPCS1 IED server-client communication (SCL)

The laboratory model substation MMS protocol configuration is composed of the IEC 61850 subnetwork object and the individual IEDs access point and MMS connectivity profile configuration. As IED's IP addresses are unique, the MMS parameters are the same for all IEDs.

Subnetwork Configuration - IEC 61850 Configuration

Access Point	Subnetwork	IP	IP-SUBNET	IP-GATEWAY
IED00000003.LD0	WA1	172.16.1.103	255.255.0.0	192.168.2.1

Project Explorer

Plant Structure

- LaboratorySubstation
 - AA1
 - J1
 - Bay1
 - IED000000001
 - Bay2
 - IED000000002
 - Bay3
 - IED000000003
 - Bay4
 - IED000000004

IED00000003 MMS Server configuration

IP	172.16.1.103
IP-GATEWAY	192.168.2.1
IP-SUBNET	255.255.0.0
IP-TCP-PORT	
IP-UDP-PORT	
OSI-AE-Invoke	
OSI-AE-Qualifier	23
OSI-AP-Invoke	
OSI-AP-Title	1,3,9999,23
OSI-NSAP	
OSI-PSEL	00000001
OSI-SSEL	0001
OSI-TSEL	0001
Communication	
Subnetwork	WA1
General	
Description	
Name	LD0
Substation	
Name	

IED00000003 IEC 61850 Configuration

Fig. 5.2 PCM600 REF615 IEDs client-server communication configuration

OSI transport selector (OSI-TSEL), the OSI session selector (OSI-SSEL), and the OSI presentation selector (OSI-PSEL) are mandatory elements for the client-server configuration. Either the IP address or the OSI-NSAP elements should be configured for remote addressing (both elements can be configured for local addressing) [8]. By analyzing the configuration of the REF615 IEDs, the conclusion is that the T-Type profile was implemented.

5.1.1 MMS communication session setup

As detailed in the Fig 5.3., the MMS application communication setup is performed in three several sequential steps that are setting up the communication sessions at OSI Transport (L4) in steps „1“ and „2“ and Session (L5), Presentation (L6) and Application (L7) layers in step „3“.

The first step in the initiation of communication is the establishment of the connection through the 3-Way Handshake. In this process (marked with „1“ in Fig. 5.3) the two communicating hosts perform the basic 3-way handshake for connection synchronization (SYN, SYN-ACK, ACK), as described by RFC793. This establishes the communication session on the OSI Network Layer (L3).

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	172.16.0.150	172.16.1.103	TCP	66 53869 → 102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000288	172.16.1.103	172.16.0.150	TCP	62 102 → 53869 [SYN, ACK] Seq=0 Ack=1 Win=5816 Len=0 MSS=1454 WS=1
3	0.001404	172.16.0.150	172.16.1.103	TCP	60 53869 → 102 [ACK] Seq=1 Ack=1 Win=66816 Len=0
4	0.001689	172.16.0.150	172.16.1.103	COTP	78 CR TPDU src-ref: 0x0204 dst-ref: 0x0000
5	0.002271	172.16.1.103	172.16.0.150	COTP	78 CC TPDU src-ref: 0x1000 dst-ref: 0x0204
6	0.002603	172.16.0.150	172.16.1.103	MMS/IEC61850	246 Associate Request
7	0.004555	172.16.1.103	172.16.0.150	MMS/IEC61850	214 Associate Response
8	0.050697	172.16.0.150	172.16.1.103	TCP	60 53869 → 102 [ACK] Seq=217 Ack=185 Win=66560 Len=0
9	0.099752	172.16.0.150	172.16.1.103	MMS/IEC61850	90 GetServerDirectoryRequest
10	0.100286	172.16.1.103	172.16.0.150	MMS/IEC61850	134 GetServerDirectoryResponse IED00000003LD0
11	0.167683	172.16.0.150	172.16.1.103	TCP	60 53869 → 102 [ACK] Seq=253 Ack=265 Win=66560 Len=0
12	0.500061	172.16.0.150	172.16.1.103	MMS/IEC61850	123 GetDataDirectoryRequest IED00000003LD0 LLN0\$BR\$rcbMeasFlt01
13	0.500866	172.16.1.103	172.16.0.150	MMS/IEC61850	293 GetDataDirectoryResponse
14	0.550972	172.16.0.150	172.16.1.103	TCP	60 53869 → 102 [ACK] Seq=322 Ack=504 Win=66304 Len=0

Fig. 5.3 MMS Communication session initiation (Wireshark)

The connection established by the COM600 client to the IED00000003 server is based destination port 102, the TPKP protocol port (source port 53969 is randomly chosen when connection is initiated and assigned to client).

MMS is implementing at OSI Transport Layer the ISO Transport Service on top of the TCP (RFC1006), which is the RFC defining TPKT protocol. COTP protocol (ISO 8073/X.224) is used for reliable data transport inside the OSI Transport Layer.

The second step of the MMS communication connection setup is the COTP “*Connection Request (CR)*”/”*Connection Confirm(CC)*” TPDU handshake. This establishes the communication session on the OSI transport layer. The COTP communication is marked with „2“ in Fig. 5.3 and the details of the COTP CR/CC TPDUs data contents are detailed in Fig. 5.4.

From a communication analysis perspective, it is important to note that TSAP parameters display match the substation server-client configuration. The COTP destination TSAP field value “0001”, is matching the OSI-TSEL parameter value configured for IED00000003 client-server communication (Fig. 5.2). Similarly, the Source TSAP field value “00000001” is matching the COM600 SCADA OPC Server OPCS1 OSI-TSEL transport selector value (Fig. 5.1).

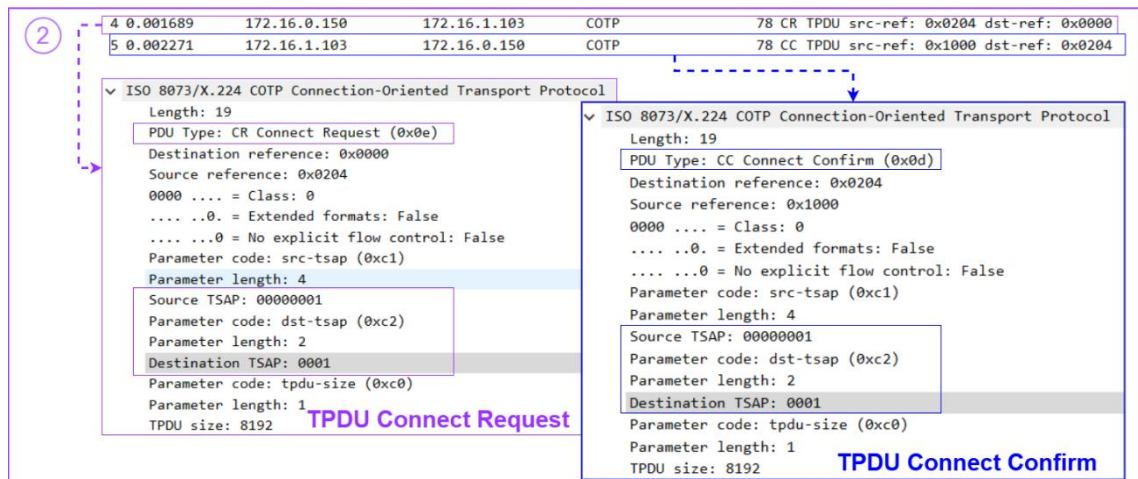


Fig. 5.4 TPKT/COTP Transport layer connection setup (Wireshark decoding)

In the third step of the MMS Associate Request/Associate Response is performing the communication association for all three layers: Session, Presentation, and Application. The packet exchange is marked with „3: in in Fig. 5.3. The MMS Associate Request/Associate Response encapsulate PDUs for all Transport, Session, and Presentation layer.

MMS is using ISO 8327-1 OSI Session Protocol, the session connection initiation is performed based on a “*Connect (CN) SPDU (type 13)*” that is confirmed by an “*Accept (AC) SPDU (type 14)*”. As shown in Fig. 5.5 (left), the “*Calling Session Selector*” field value “0001” is equal to the value of OSI-SSEL Session Selection parameter in OPCS1 configuration (Fig. 5.1).

The value of the “*Session Selector*” field value “0001” is equal to the value of the OSI-SSEL “*Session Selection*” parameter in the IED00000003 configuration (Fig.5.2).

The acceptance of the session-oriented connection is confirmed by the “*Connect Accept parameter (type 5)*”, contained in the Accept SPDU.

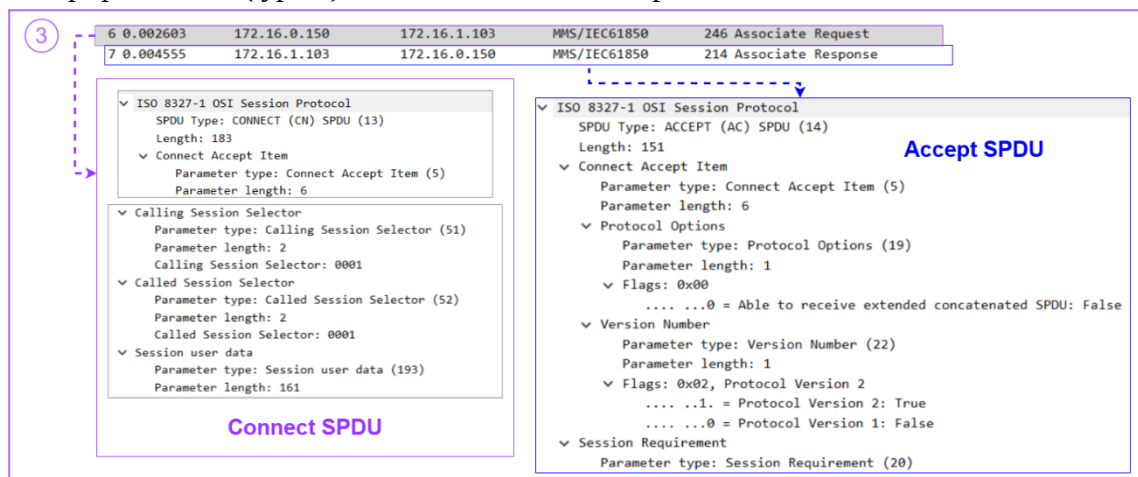


Fig. 5.5 MMS Session layer connection setup

As shown in Fig. 5.6, ISO 8223 OSI Presentation Protocol is providing for the MMS protocol the PPDU encapsulation protocol. The value of the Connect Presentation (CP) PPDU “*calling-presentation-selector*” parameter “0001” matches the OCPS1 OSI-PSEL value.

Similarly, the Connect Presentation Accept (CPA) PPDU “*called-presentation-selector*” parameter value “00000001” is matching the value of IED00000003 OSI-PSEL Presentation Selector parameter. CPA-PDU result: acceptance (0) field, which is part of “*presentation-context-definition-result-list*”, confirms the presentation-oriented session was setup.

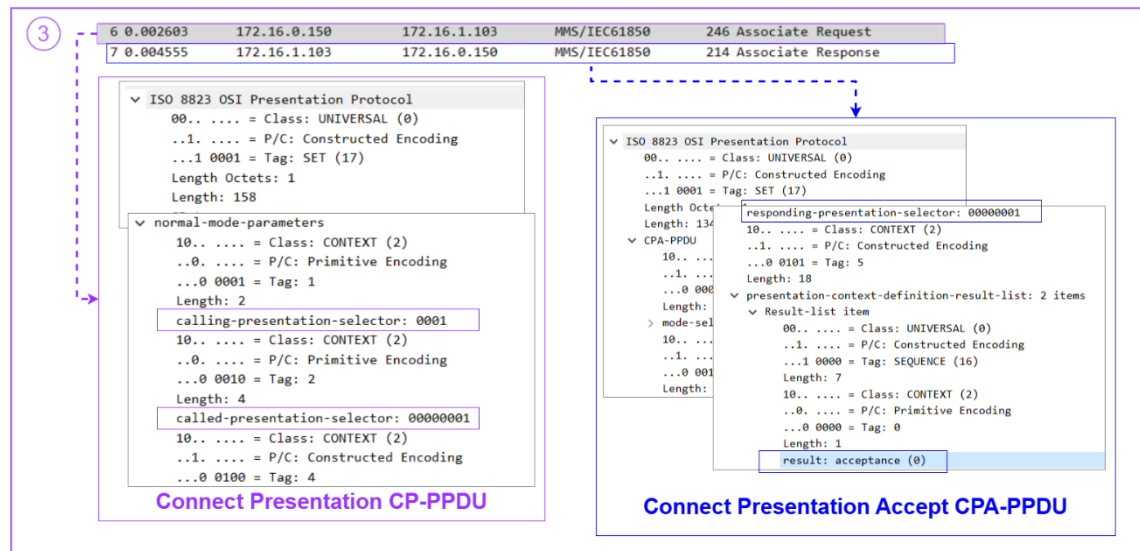


Fig. 5.6 MMS Presentation layer connection setup

ISO 8650-1 OSI Application Control Service protocol is providing the APDUs that are used for the setup of MMS Application Layer connection initialization. The aarp APDU form “*called-AP-title-form2*” contains the object “*ap-title-form2*” with field value “1.3.9999.23”. The value corresponds to the OSI-AP-Title value assigned to IED00000003. Similarly. The aarp APDU communicates in the list “*calling-AP-title-form2*” the object “*ap-title-form2*” with field value “1.3.9999.23”, corresponding to the COM600 OPCS1 IED OSI-AP-Title value.

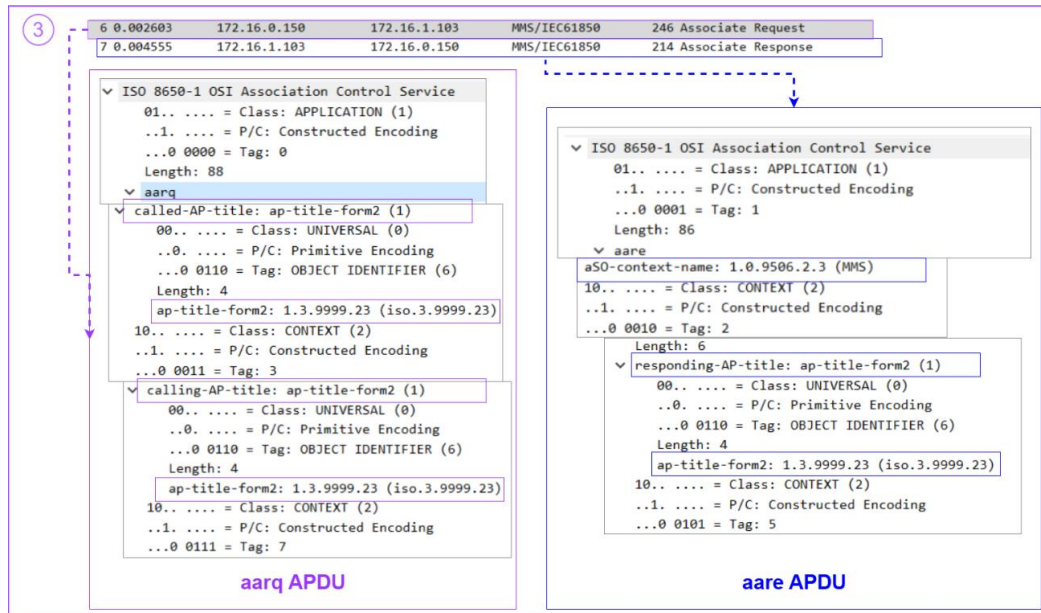


Fig. 5.7 MMS Application layer connection acceptance

The aare APDU confirms the ap-title-form2 with field value “1.3.9999.23” contained in the “responding-AP-title-form2” form. aarq and aare APDUs encapsulate MMS PDUs. These PDUs perform the MMS communication initialization parameters through the MMS initiate-Request-PDU (contained in aarq APDU) and “initiate-Response-PDU” (contained in aare APDU).

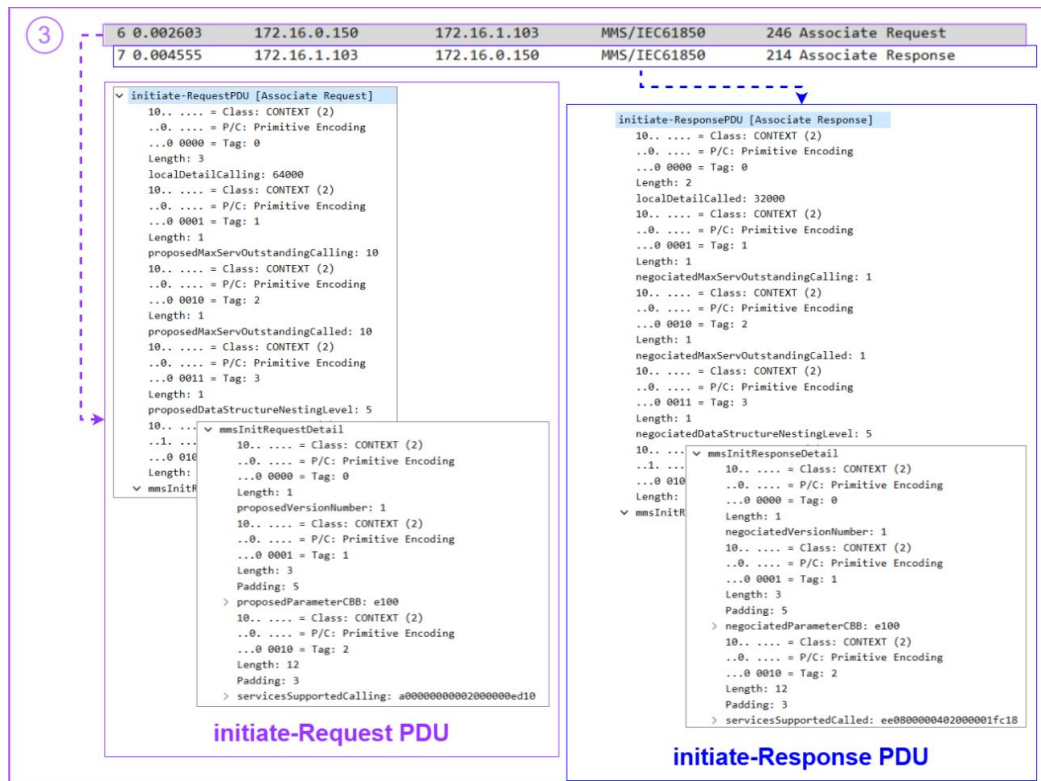


Fig. 5.8 MMS “initiate-RequestPDU” and “initiate-ResponsePDU”

As the name suggests, “*servicesSupportedCalling*” (12 bytes length) details all the MMS services supported by the IED. The IED00000003 “*servicesSupportedCalled*” field that was decoded using Wireshark is enclosed in Appendix C.

As the two-way session establishment was completed successfully at all 4 OSI layers (Transport, Session, Presentation and Applications), the MMS client-server communication services are established.

5.1.2 Confirmed MMS services communication

In this section the MMS protocol analysis continues with the demonstration of confirmed MMS services communication. For this purpose, the communication session analyzed in Section 5.1.1 is used. After the establishment of the two-way session, the MMS application communication session continues, as shown in Fig. 5.3, Step „4“, with a confirmed MMS Services request.

If successful, this is a request-response transaction. An MMS “*confirmed-RequestPDU*” is sent by the COM600 OPCS1 IED. At the MMS application layer, this is answered by IED00000003 with a “*confirmed-ResponsePDU*”.

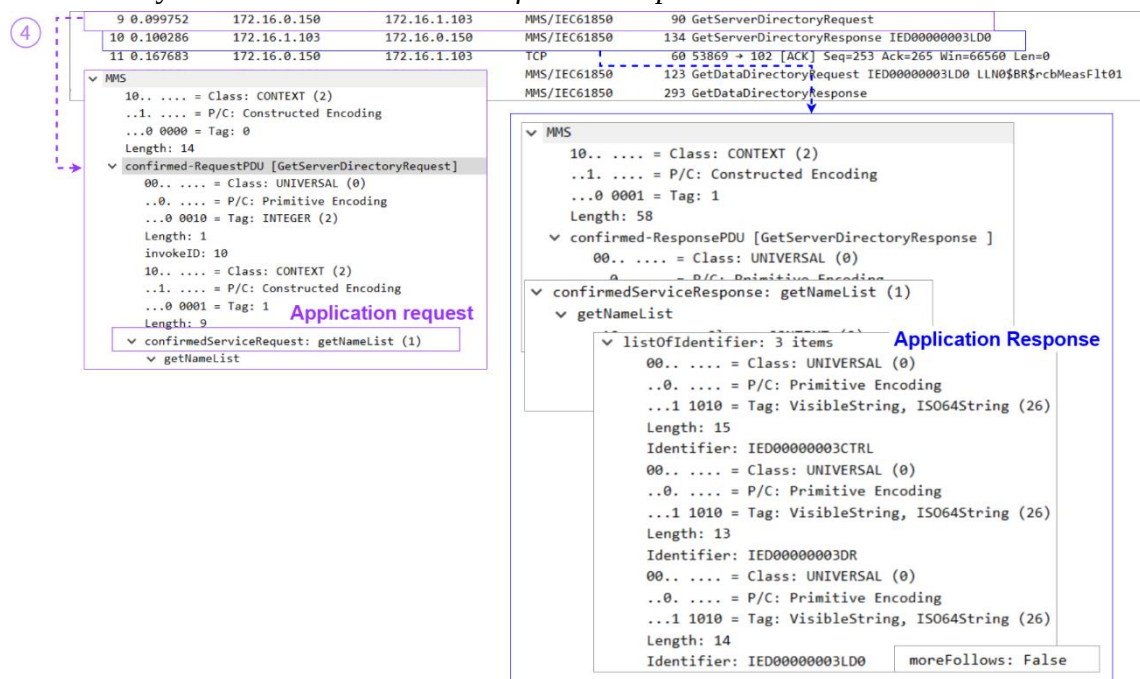


Fig. 5.9 MMS confirmed PDU example

The IEC 61860 object-oriented model characteristic is visible in the confirmed MMS services communication. The request “*getNameList (objectClass domain)*” is answered with a list of identifiers containing the logical nodes objects IED00000003CTRL, IED00000003DR and IED00000003LD0. The MMS services application response contains also the information that the response is complete: “*moreFollows*” flag indication is “*False*”. Transaction was completed.

As detailed in [23] an MMS “*confirmed-RequestPDU*” can be followed on client side (requester) by a “*Cancel-RequestPDU*”. The possible MMS server answers are “*confirmed-ResponsePDU*” (as demonstrated in this section) or “*confirmed-ErrorPDU*” (not present in analyzed communication). A client sent “*Cancel-RequestPDU*” the possible server answers are “*Cancel-ReponsePDU*” or “*Cancel-ErrorPDU*”.

5.1.3 Unconfirmed MMS services communication

For realizing timely, unsolicited, communication of monitored data updates, MMS communication services deploy unconfirmed services. These services are performed through the “*unconfirmed-PDU*” APDU type.

The MMS servers monitor their defined report control blocks data objects, and, once an update is detected, a report will be forwarded using the “*unconfirmed-PDU*” type. As the MMS communication is connection oriented, the reports are forwarded only to the associated clients that are defined as recipients of the report. A report is sent by the server IED after an update was detected. The unconfirmed APDUs are not followed by replies from the clients. Fig. 5.10 details SBO control operation on IED00000003 disconnector switch 1 (logical node DCCSW1).

Time	Source	Destination	Protocol	Length	Info	
779 28.700025	172.16.1.103	172.16.0.150	MMS/IEC61850	734	Unconfirmed <RPT>	
780 28.749098	172.16.0.150	172.16.1.103	TCP	60	53869 → 102 [ACK] Seq=18275 Ack=44685 Win=66816 Len=0	
781 34.320031	172.16.0.150	172.16.1.103	MMS/IEC61850	165	SetDataValueRequest IED00000003CTRL DCCSW1\$C05Pos\$SBOw	1. SBO (request-response)
782 34.323296	172.16.1.103	172.16.0.150	MMS/IEC61850	84	SetDataValueResponse	
783 34.374063	172.16.0.150	172.16.1.103	TCP	60	53869 → 102 [ACK] Seq=18386 Ack=44715 Win=66816 Len=0	
784 34.620147	172.16.1.103	172.16.0.150	MMS/IEC61850	186	Unconfirmed <RPT>	Unconfirmed-PDU
785 34.680085	172.16.0.150	172.16.1.103	TCP	60	53869 → 102 [ACK] Seq=18386 Ack=44847 Win=66560 Len=0	
786 37.088946	172.16.0.150	172.16.1.103	MMS/IEC61850	165	SetDataValueRequest IED00000003CTRL DCCSW1\$C05Pos\$Oper	2. Switch Position Operation (request-reponse)
787 37.099958	172.16.1.103	172.16.0.150	MMS/IEC61850	84	SetDataValueResponse	
788 37.151041	172.16.0.150	172.16.1.103	TCP	60	53869 → 102 [ACK] Seq=18497 Ack=44877 Win=66560 Len=0	
789 37.290361	172.16.1.103	172.16.0.150	MMS/IEC61850	209	Unconfirmed <RPT>	Unconfirmed-PDU (detailed)
790 37.340161	172.16.0.150	172.16.1.103	TCP	60	53869 → 102 [ACK] Seq=18497 Ack=45032 Win=66384 Len=0	

Fig. 5.10 MMS SBO control model operation example

Fig 5.10 details the unconfirmed-PDUs forwarded once disconnector switch control operations were performed. The SBO control operation is performed in two steps.

The First step is the select with value operation for the disconnector switch DCCSW1.Pos.SBOw data attribute (marked with 1, above). This is performed through the exchange of a “*Confirmed-RequestPDU/SetDataValueRequest*” (write), followed by a “*confirmed-ResponsePDU/SetDataValueResponse*” (write success) that confirms the success of the write operations.

As the operation triggered an update of the report control block data entries that are defined for DCCSW1 logical node, the server issues an “*unconfirmed-PDU*” to inform immediately the associated clients of the data attributes values change. The PDU is indicated as the “*Unconfirmed-PDU*” (packet 784) in Fig. 5.10.

The second step of the disconnector switch control operation (indicated with 2. in the figure) is the write operation performed on DCCSW1.Pos.Oper data attribute. Similarly to the SBO control operation, the switch position control operation communication is performed based on an exchange of a “*Confirmed-RequestPDU/SetDataValueRequest*” write request, followed by a write success response based on a “*confirmed-ResponsePDU/SetDataValueResponse*” PDU.

This control operation triggers a new “*unconfirmed-PDU*” informing the connected client of the data updates triggered by the control operation (packet 789).

The PDU data content shows that the “*unconfirmedService*” type is “*informationReport(0)*” and that the report is implemented for the report control block “*rcbStatIO01*” (object ID “*IED00000003/LD0/LLN0\$rcbStatIO01*”) part of the data set IED00000003LD0/LLNStatIO. The SeqNum sequence number field SeqNum details the position of the data set entry in the data set (position number 26 in the list). The data set entry position ID can also be evaluated in the IED CID file.

The figure consists of two screenshots from a network analysis tool. The top screenshot shows a window titled "Data Set - IED00000003LD0/LLN0.StatIO". It displays a list of data set entries. The entry "LD0/XGGIO110.SPCS02 (ST)" is highlighted in blue. A purple dashed line points to this entry with the label "RCB Dataset entry sequence number 26". The bottom screenshot shows a packet capture window for packet 789, which is an "unconfirmed-PDU [RPT]". The packet structure is expanded to show the "unconfirmedService: informationReport (0)" and "informationReport" fields. The "SeqNum" field is highlighted in blue and labeled "Data object SeqNum". The "Report Control Block" field is also highlighted and labeled "Report Control Block".

Fig. 5.11 MMS SBO control model operation example

The data set entry corresponds to the binary output logical node data object LD0/XGGIO110.SPCSO2 (single point control binary output 2). In the IED's functional application model, this signal corresponds to the DCXSWI1 execute close disconnector control output.

Additional report information (i.e. the time of event of event entry) can be further analyzed based on the “*unconfirmed-PDU*” data content. This example demonstrates the initiation of transmission of the unconfirmed-PDUs. From the data analyzed, the conclusion was that a close operation of the disconnector switch DCXSWI1 was performed. Data set entry “LD0/XGGIO110.SPCSO2” monitors the status of Close Execute binary signal input.

5.2 GOOSE communication analysis

GOOSE communication analysis and troubleshooting is required as part of commissioning and regular operations processes that are part of the digital substation life-cycle. For this, software and hardware-based tools and products are used. Examples of software tools and products are Omicron IEDScout, Siconet GOOSE Monitor, Triangle Microworks GOOSE Testing. SMC GOOSEMetter-One is an example of hardware based GOOSE network traffic intrusion tester.

The COM600 gateway includes a GOOSE analyzer function that can be used for live troubleshooting and monitoring of substation GOOSE communication. This requires that the GOOSE intrusion is active substation IEC 61850 OPC server level.

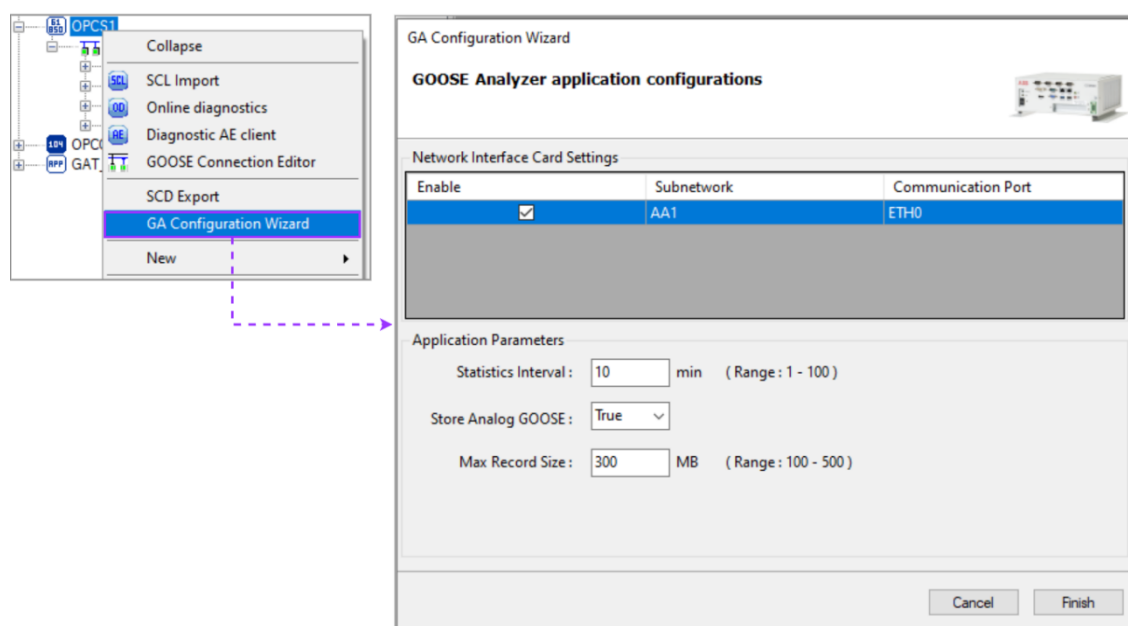


Fig. 5.12 SAB600 GOOSE Analyzer configuration wizard

As shown in Fig. 5.12 the parameters configurable for GOOSE intrusion are the function state (Enable/Disable), the substation objects for which the GOOSE intrusion is performed and the statistics collection parameters. For the substation model testing, the default parameters were implemented.

As a troubleshooting tool, the GOOSE intrusion might not be permanently required. The substation wizard can be utilized for activation and deactivation of the GOOSE analyzer functions. The GOOSE monitor analysis configuration can be customized using the SAB600 GOOSE Connection Editor. The default configuration created by the wizard process was sufficient for performing the analysis and troubleshooting.

The monitor configuration does not offer an option for the data display of unknown IEDs GOOSE data, but as demonstrated in this chapter, this type of issue can be assessed with the available COM600 GOOSE Analysis tools.

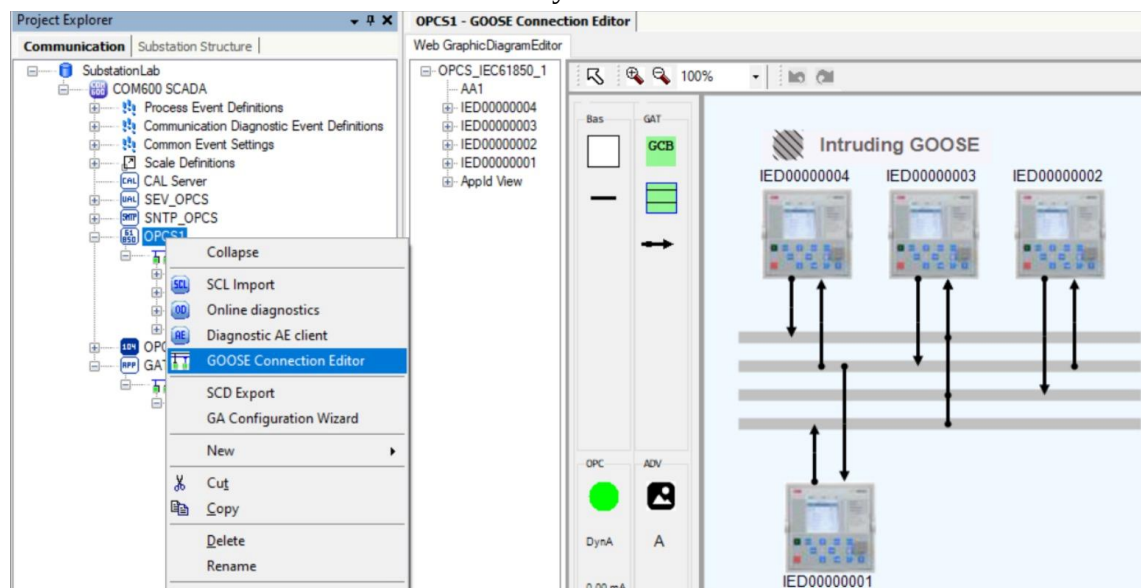


Fig. 5.13 SAB600 GOOSE Analyzer configuration wizard

The wizard adds to the substation communication structure a new Application OPC Server (“*GAT_OPC_Server_1*”) and maps to its communication structure the GOOSE intrusion configuration: the virtual subnet “*GAT_AA1*” and the virtual “*IED GATIED_1*”. The role of a virtual IED is to map to its data model the properties of the GOOSE intrusion service. As configured, the “*IED GATIED_1*” data objects were used by the intrusion process for all substation IEDs part of the “*AA1*” subnet. The logical nodes that are components of the GOOSE virtual IED are mapped to IEDs GOOSE data.

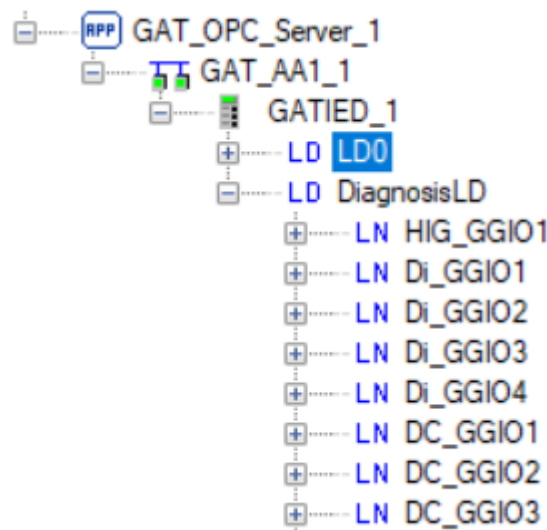


Fig. 5.14 SAB600 GOOSE Analyzer OPC server

The virtual IED GATIED_1 Logical Node “Di_GGIO1” is mapped to SPS Status Data Attribute GOOSE Disorder Event Indication for the substation IED00000004 GOOSE Control Block “*IED00000004LD0/LLN0.gcbFEEDER*”. The Data Attribute object is mapped to the internal analyzer event “*GATBinaryDiagnosisEvent*” that is triggered if a disorder event is detected.

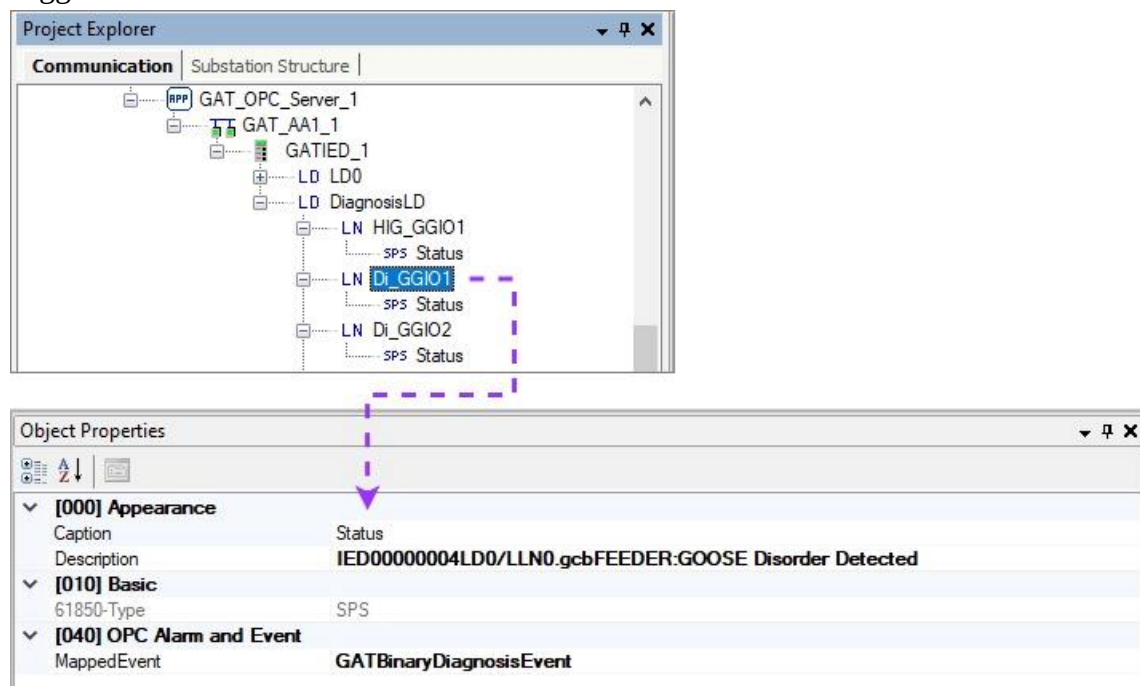


Fig. 5.15 GOOSE Analyzer OPC server communication structure

GOOSE communication analysis was performed using the COM600 Station WebHMI. The data reported in the GOOSE Analyzer WebHMI console is sourced by the GOOSE Virtual IED “GATIED_1” Logical Nodes Data Attributes and displayed by the SAB600 GOOSE Connection Editor.

Fig. 5.16 shows an aggregated view of IED00000003 subscribed and published Control Blocks. The GOOSE table level view contains the GOOSE Control Block online status information for the selected IED/published GOOSE Control Block.

Options for monitor function are also the Subnet view and the GOOSE App_Id view, which is a subset of the subnet view and presents information for the selected App ID.

Status information for IED00000003 lists VLAN configuration issues. This is because the lab (IEE802.3) Ethernet network infrastructure does not implement IEEE 802.1Q VLAN encapsulation. For GOOSE troubleshooting of the laboratory substation network, these items do not represent issues. No other issues were reported for IED00000003.

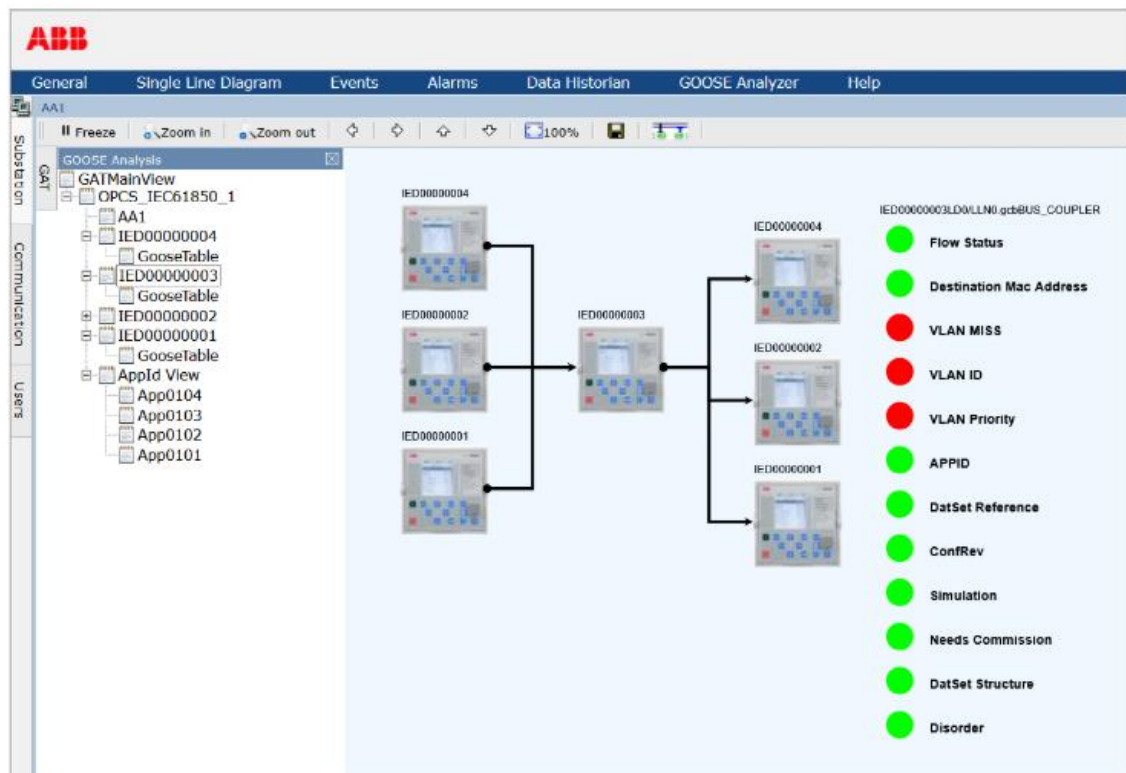


Fig. 5.16 COM600 WebUI GOOSE Analyzer IED view

IED00000004 presented errors that were issues and required investigation. These issues are displayed in the status information as per the IED and GOOSE Table views presented in Fig. 5.17:

- incorrect GOOSE destination MAC address.
- incorrect IED GOOSE application identifier (AppID).
- incorrect configuration version.
- incorrect GOOSE control block dataset structure.

The displayed issues should be understood as triggered by the difference in between IED GOOSE configuration imported to the COM600 substation OPC configuration that was set up the initial phase of the IEC61850 COM600 management unit configuration

(based on the substation SCL configuration import). Errors were identified as GOOSE frames received by COM600 intrusion process have a different data content.

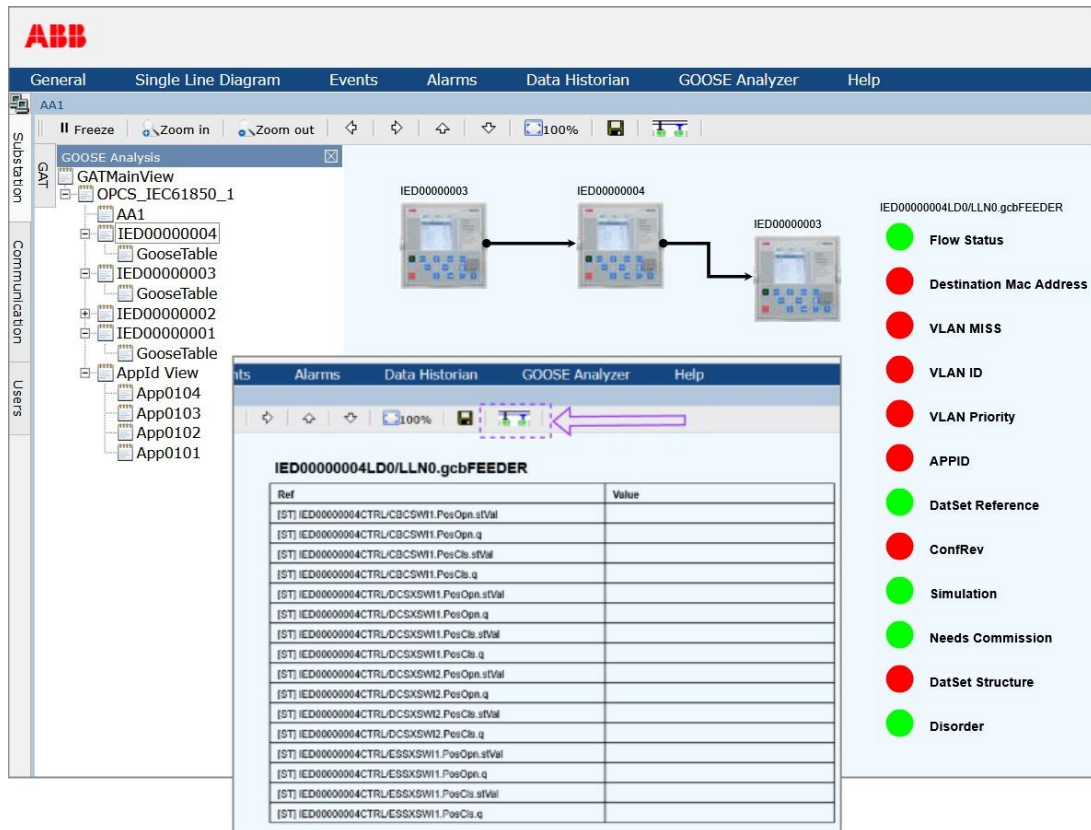


Fig. 5.17 IED00000004 GOOSE communication errors

IED00000004 GOOSE Table view for gcbFEEDER control block displays no data values for the data attributes configured. This gives a first indication of the incorrect configuration of the IED GOOSE communication. For continuing the investigation, the GOOSE Analyzer tool will be started, as indicated by the arrow inside Fig. 5.18.

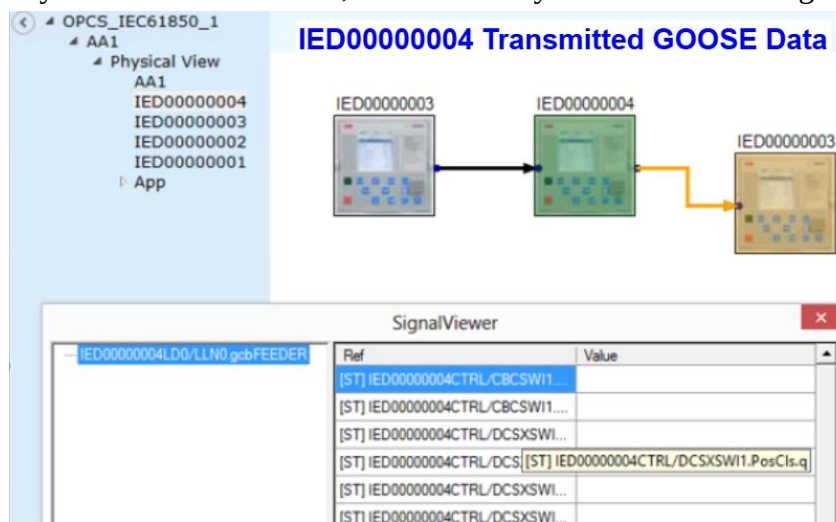


Fig. 5.18 IED00000004 incoming/outgoing GOOSE control block signals

The IEC00000004 outgoing GOOSE flows to IEC00000003 contained no data attributes content. Same information was visible in the GOOSE monitor, however, the GOOSE analyzer view gave flexibility for a quick investigation of the outgoing IED flows, as presented above.

The troubleshooting continued with the exploring the Events dashboard. Filtering data for a specific OPC Server, Subnet, IED or GOOSE control block was possible. The data entries displayed were not relevant for the investigation of the communication issue. GOOSE disorder events detected (Fig. 5.19) were caused by transitory network events caused by reconnection of the network cabling in the laboratory network.

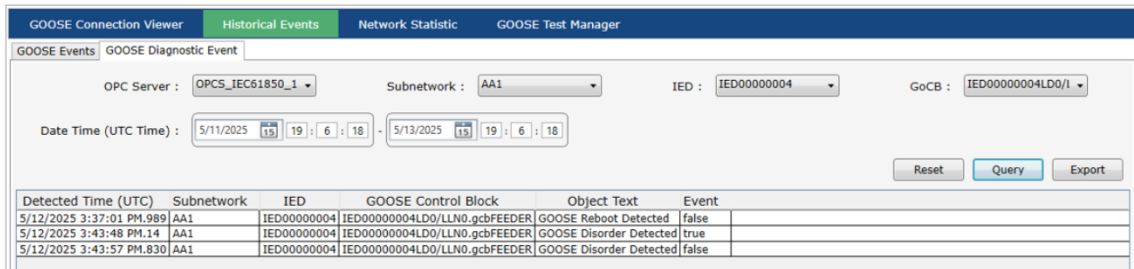


Fig. 5.19 COM600 Historical Events Dashboard for IED00000004

The Network Statistics dashboard presents GOOSE control block communication sourced by IED00000004. The communication intervals correspond to the periodic retransmission of the GOOSE data.

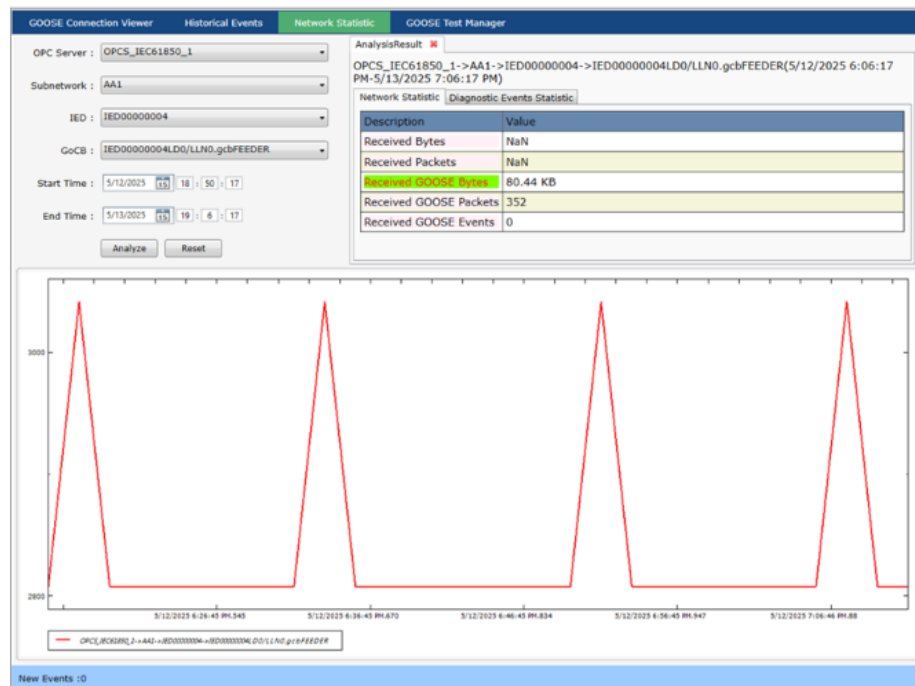


Fig. 5.20 COM600 Network Statistics Dashboard for IED00000004

For further analyzing the IED00000004 communication data, the GOOSE Test Manager function was used. Testing can be set up based on an auto-trigger configuration. Objects and events can be selected to be in the trigger analysis, as visible in Fig. 5.21.

The test running information displayed the status of new events being collected (12 events collected).

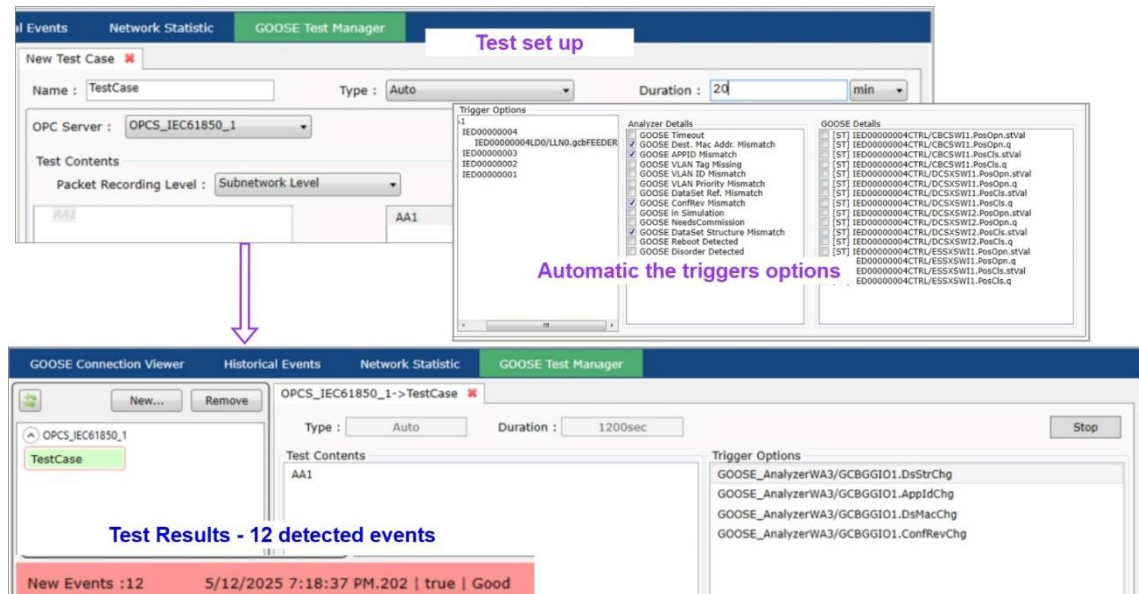


Fig. 5.21 COM600 GOOSE Test Manager

For an analysis of the entire substation communication a manual test was deployed (no filter applied). This test recorded all GOOSE events present in the network at AA1 subnet level.

One new issue was identified in the test output information window: an unknown IED was present in the substation network. As indicated by the red arrows in Fig 5.22, this IED published the GOOSE control block name “P5U20VPv2Relay/LLN0.gcb1”.

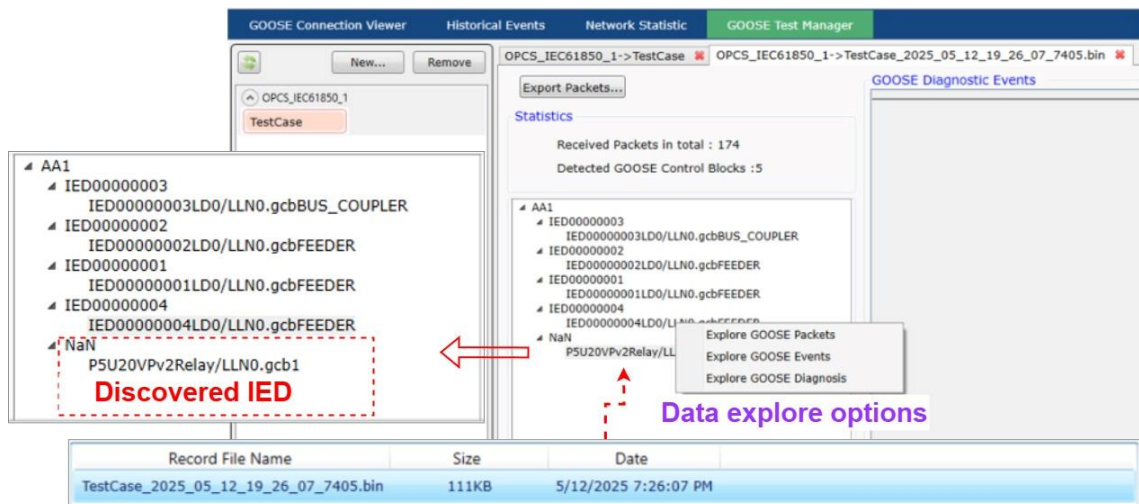


Fig. 5.22 COM600 GOOSE Test Manager – manual mode

The recorded events were further analyzed by using the GOOSE Diagnosis options available as shown in Fig. 5.22. GOOSE packets, events or diagnosis outputs can be analyzed.

The packet analysis tool gave a full indication of the IED00000004 GOOSE configuration issues. The IED configuration was updated by different work in the laboratory and was no longer conforming with the COM600 SCADA setup of the laboratory substation.

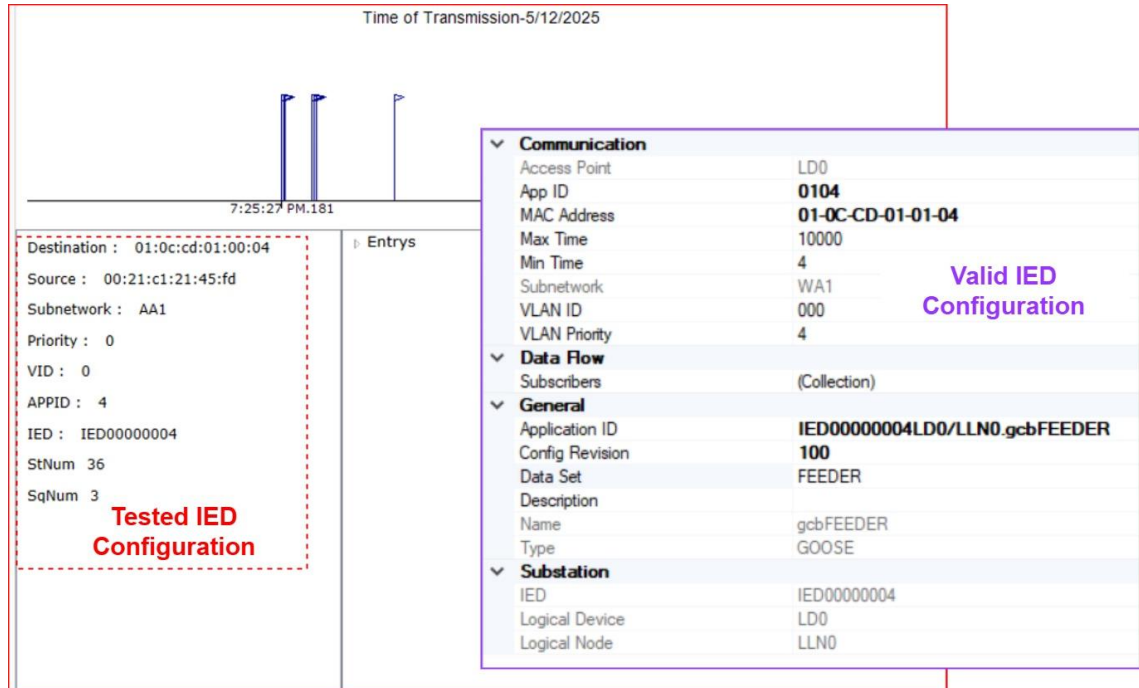


Fig. 5.23 COM600 GOOSE Packet analysis insights

At this stage, out of four issues identified by the GOOSE monitor dashboard, the cause for three issues was identified. The remaining one is the ConfRev configuration revision parameter, which was the analysis based on the packet capture export function provided by the COM600 GOOSE Analyzer. Wireshark output displayed in Fig. 5.24.

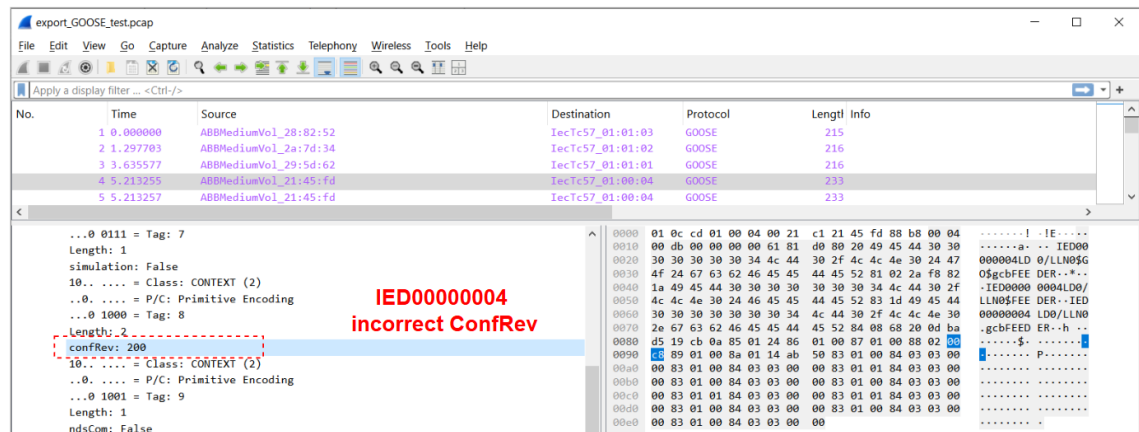


Fig. 5.24 GOOSE configuration revision analysis (Wireshark)

Table 5.1 contains a summary of GOOSE communication issues identified in the IED00000004 configuration.

Table 5.1 IED00000004 – analyzed configuration errors

GOOSE Analysis Monitor Error Type	Correct COM600/ IED00000004 GOOSE configuration	Detected (faulty) configuration
Destination MAC Address	01-0C-CD-01-01-04	01-0C-CD-01-00-04
Subnetwork	WA1	AA1
APPID	0104	4
ConfRev	100	200

For removing the identified issues, IED00000004 configuration was updated using PCM600 for restoring its correct configuration. The new IED discovered by the test was removed from the substation network.

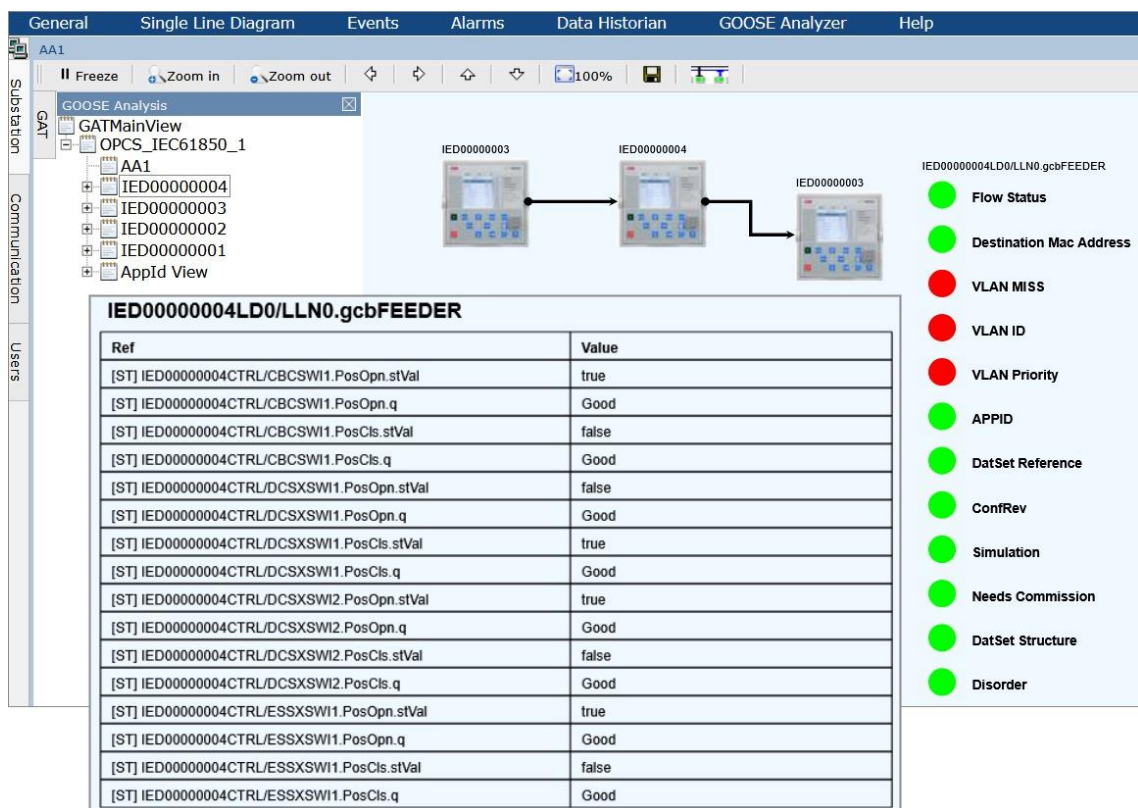


Fig. 5.25 COM600 GOOSE communication status after IEC00000003 corrective configuration update

In summary, the troubleshooting performed with the help of the COM600 GOOSE Analyzer capabilities enabled the identification of causes for all four issues present in the IED00000004 GOOSE communication. For the correction of the issue, the IED00000004 configuration was updated to the correct one using PCM600. After the configuration is updated, the GOOSE status nominal and Control Blocks reporting is correct (Fig. 5.25).

Besides the GOOSE communication issues causes for IED00000004, based on COM600 GOOSE Analyzer, an additional issue related with presence in the substation

network of a new IED was identified. The ability to monitor and detect problems and events in substation communication protocols issues and events is important for ensuring the security and operational integrity of substation networks and operations. The tests performed demonstrated the GOOSE protocol network analysis and troubleshooting capabilities based on the COM600 gateway functions.

5.3 IEC104 testing

For validating OpenMUC framework IEC104 communication configuration a test environment was deployed outside the laboratory model. As test platform, the C#.Net Source Code Library IEC 60870-5 (IEC 104 and 101) made available by MZ-Automation GmbH.

The MZ-Automation IEC104 source library is designed to be used for implementing communication systems between local and central stations.

Table 5.2 MZ-Automation IEC104 source library features and standards [24]

Technical features	Standards
• Master/Slave (CS 101) and Client/Server (CS 104) implementation • Implements all command, monitoring, parameter, file message types • Available as nuget package and C# source code • Compatible with .NET Framework 4, .NET 5, .NET standard 2.0, and Mono • Comes with a lot of examples to simplify learning • Field proven • Easy to use API • Compatible with the latest version of IEC 60870-5-101 and IEC 60870-5-104	• CS 101 master/slave (RS 232/485 serial communication) • CS 101 balanced and unbalanced mode • CS 104 client/server (TCP/IP) • CS 104 redundancy group supported • Support for all standard message types (M_XX, C_XX, P_XX, F_XX) for messages in monitoring direction, commands, parameter loading, file transmission. • Send and receive messages in standard and reverse direction • spontaneous transmission of events • periodic transmission of measurements • command and set point transmission (direct and select/execute)

Besides IEC104, MZ-Automation portfolio includes source code libraries for IEC 61850 (Editions 1, 2 and 2.1, with support for MMS, GOOSE and SMV) and for IEC60870-6 Inter-Control Center Communications Protocol (ICCP) Protocol (referred also as TASE.2). ICCP protocol is used for the exchange of monitor, time-critical control and data transfer in between different control center SCADA systems over local area and wide-area networks [25].

The test performed was based on Client/Server (CS 104) case, the source library was downloaded from [mz-automation/lib60870.NET](https://github.com/mz-automation/lib60870.NET) GIT-HUB repository source [24] and opened in Visual Studio Code (Windows 10 workstation).

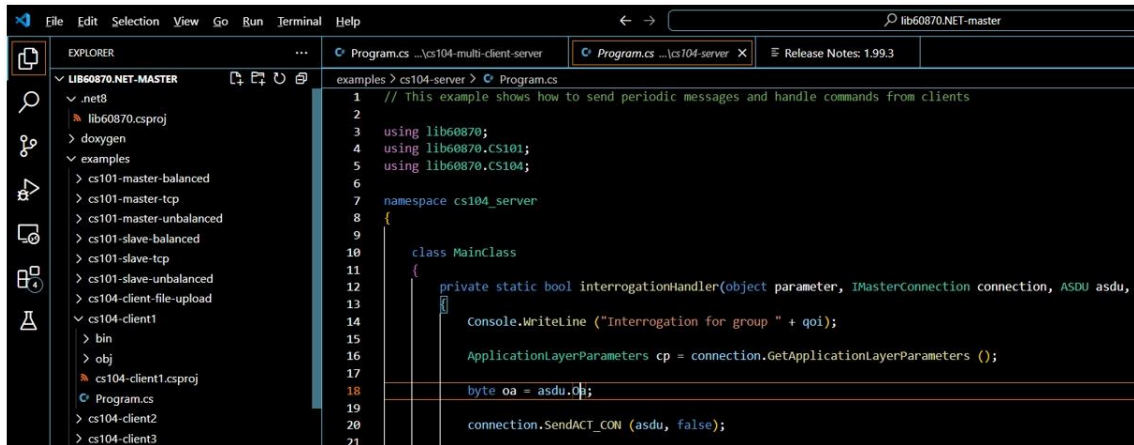


Fig. 5.26 lib60870.NET test environment

For starting the communication test, the cs-104-server\Program.cs program was compiled and run. The successful compilation and execution of the program was displayed in the terminal output window. As per Fig. 5.27 the program is queuing and listens for client connections.

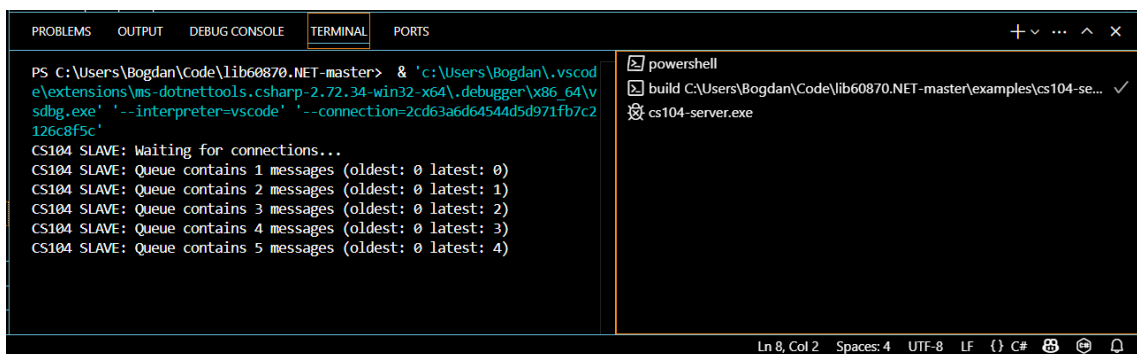


Fig. 5.27 cs104-server.exe server execution

In IEC104, the combination of Common Address of the ASDU (CAA) and Identification Object Address (IOA) identifies uniquely the data objects of an RTU. IEC104 requires that each substation RTU will be assigned a unique Common Address of the ASDU but doesn't formalize IOA address allocation inside the data objects domain of each RTU [26].

The cs-104-server program publishes data object IOAs of several data types: 32 bit integral, CP56Time2a, Boolean and float. The data object values in the "cs-104-server" program can be observed directly in the programming code, as per Fig. 5.28.

```

connection.SendASDU (newAsdu);

newAsdu = new ASDU (cp, CauseOfTransmission.INTERROGATED_BY_STATION, false, false, oa, 1, true);

newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (300, -1.0f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (301, -0.5f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (302, -0.1f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (303, .0f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (304, 0.1f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (305, 0.2f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (306, 0.5f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (307, 0.7f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (308, 0.99f));
newAsdu.AddInformationObject (new MeasuredValueNormalizedWithoutQuality (309, 1f));

```

Fig. 5.28 cs104-server IOA data objects definition example

From a communication test perspective, the objective was to enable OpenMUC client to access the published IOA data. This required the identification and correct configuration of the OpenMUC channels associated with each published IOA.

The mandatory items required for the channel configuration are the Common Address (CA) parameter (unique for all IOAs belonging to same RTU), the ASDU type (standardized for individual data types, commands or data operations) and the IOA value mapped to the respective channel. For an IOA object publishing a Sequence Information Element, an index parameter will define the location of single data values accessed by the channel [24]. An incorrect set up of the ASDU type will cause an OpenMUC driver error or an incorrect read of the data channel.

It is assumed that correct identification of data object types is defined prior to remote systems communication integration; however, in case of an error or lack of documentation the Wireshark network traffic capture application can be used for the identification of the ASDU type associated with a specific IOA.

Fig. 5.29 demonstrates visibility of the ASDU type 1 (M_SP_NA_1) - Single-point information without time tag. In the analyzed network packet, the Sequence Information Element structure is also visible, IOA 200 being present at index 0, followed by the remaining IOA's up to index 8, containing IOA 207 data. An accurate OpenMUC channel index configuration is required to receive the correct content of the IOA data object.

Single point information with quality descriptor (SIQ) byte details that SPI data is Boolean "True" and data quality descriptors present are: "Valid", "Topical", "Non-Substituted", "Non-Blocked data" [24].

OpenMUC channels configuration file included in Appendix A contains all the source IOA data objects configuration and the associated OpenMUC channel configuration, channel data type and the resulting data representation.

The test result confirmed that OpenMUC framework configuration could properly access data objects published by the cs-104-server test program based on IEC104 communication protocol. OpenMUC "channels.xml" configuration used for implementing this test was attached to the Appendix A of this document.

```

> Frame 166: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{27198710
> Ethernet II, Src: Intel_47:59:eb (48:89:e7:47:59:eb), Dst: RaspberryPi_16:04:31 (2c:cf:67:16:04:31)
> Internet Protocol Version 4, Src: 192.168.2.110, Dst: 192.168.2.111
> Transmission Control Protocol, Src Port: 2404, Dst Port: 53160, Seq: 431, Ack: 49, Len: 23
> IEC 60870-5-104: -> I (560,80)
▼ IEC 60870-5-101/104 ASDU: ASDU=1 M_SP_NA_1 Inrogen IOA[8]=200-207 'single-point information'
  TypeId: M_SP_NA_1 (1)
  1... .... = SQ: True
  .000 1000 = NumIx: 8
  ..01 0100 = CauseTx: Inrogen (20)
  .0.. .... = Negative: False
  0... .... = Test: False
  OA: 0
  Addr: 1
  ▼ IOA: 200
    IOA: 200
    ▼ SIQ: 0x01
      .... ...1 = SPI: On
      ...0 .... = BL: Not blocked
      ..0. .... = SB: Not Substituted
      .0.. .... = NT: Topical
      0... .... = IV: Valid
  > IOA: 201
  > IOA: 202
  > IOA: 203
  > IOA: 204
  > IOA: 205
  > IOA: 206
  > IOA: 207

  TypeId: M_SP_NA_1 (1)
  1... .... = SQ: True
  .000 1000 = NumIx: 8
  ..01 0100 = CauseTx: Inrogen (20)
  .0.. .... = Negative: False
  0... .... = Test: False
  OA: 0
  Addr: 1
  ▼ IOA: 200
    IOA: 200
    ▼ SIQ: 0x01
      .... ...1 = SPI: On
      ...0 .... = BL: Not blocked
      ..0. .... = SB: Not Substituted
      .0.. .... = NT: Topical
      0... .... = IV: Valid

```

Fig. 5.29 IEC104 Test – Wireshark network traffic analysis

The result was significant for the practical work done in this thesis because it demonstrates the use of testing and commissioning tools as part of the substation SCADA system engineering process. The testing was performed outside the laboratory containing the COM600 management unit and it confirmed that the IEC104 OpenMUC configuration implemented was functional. Next, the IEC104 communication integration in between COM600 and OpenMUC was up, accordingly to the details presented in Chapter 4.6.

5.4 Summary

In this chapter the network communication protocols deployed in the laboratory substation SCADA system was performed. The MMS analysis focused on the study of the connection-oriented nature of the protocol. The analysis performed had as scope the identification of the IED client-server connection configuration parameters in the captured data flow. The Wireshark application was used as a network traffic inspection and analyzer tool. In the case of the laboratory substation model, no issue affected the setup of the MMS client-server application connectivity. The PDU analysis done mapped the theoretical basis used for this analysis with the information that was extracted and analyzed from the captured network communication flows.

Together with the application session establishment, the analysis included the inspection of confirmed and unconfirmed MMS services PDUs, which are the core of IEC 61850 MMS protocol communication. Not all PDU types have been analyzed, but

the details presented in the analysis can be useful for troubleshooting real MMS communication issues.

The second part of this chapter focused on GOOSE protocol analysis and offered a practical example of using COM600 WebHMI GOOSE Analyzer application as an effective tool for the substation horizontal communication issues discovery and troubleshooting.

During the implementation of the GOOSE analysis, a “foreign” IED was discovered attached to the substation network. This IED was also part of a different labor work and was turned on unintentionally during the test preparation. The event proved useful to demonstrate the GOOSE analyzer capability to inspect and monitor the substation traffic not only as a tool used for troubleshooting issues, but also as an effective option for detection and alarming on new or foreign (maybe also potentially harmful) GOOSE based hosts attached to the substation network.

The last part of this chapter detailed the use of a virtual application environment to study the IEC 60870-5-104 communication. The testing work done was intended to demonstrate the importance of using different tools as part of the engineering process required for the design and commissioning of a substation network communication environment.

6. CONCLUSION

This thesis deals with the subject of the IEC 61850 standard, which enables digital substations with substantial benefits for interoperability, scalability, and flexibility. The standard streamlines the substation engineering process at all stages of the solution development and deployment and offers a platform that enables efficient, reliable, and secure substation operations.

Even if it is simple at the core, the IEC 61850 is a complex standard. The first part of the thesis focuses on presenting the main characteristics of the standard and their importance. The implementation and use of the standard requires a good understanding of its data, communication and configuration models, and relationships and interactions with the engineering tools, the physical IEDs, and other substation systems.

A key feature of the standard is its expandability to new domains. This is founded on the capability of the standard to permit the modeling on new logical and allow expanding the applicability of the IEC 61850 standard. This enables the use of the IEC61850 standard beyond the boundaries of substation automation systems and its use for protection and control in hydroelectric power plants, distributed energy resources and distribution automation systems, energy storage systems, FACTS, and HVDC transmission systems.

This thesis also investigated available SCADA solutions, analyzing their supported functions, technical features, communication protocols, network redundancy, cybersecurity measures, and data model standards. The analysis revealed that modern SCADA solutions provide comprehensive coverage for all energy domains, either through internal domain-specific functions or through the composability of multiple hardware and software products. Resilience and high availability are inherent features of these solutions. Cybersecurity is a key concern, addressed through certifications, data integrity, and confidentiality, with SCADA systems designed to integrate securely with broader enterprise systems.

In the practical part of this thesis the implementation of a SCADA system was performed. This allowed the application of theoretical knowledge to the actual configuration tasks required by the deployment of the SCADA system functions and the integration of these functions with the substation laboratory model used for this deployment. As enabled by the IEC 61850 standard engineering design process, the configuration tasks required the use of multiple tools and the migration of SCL configuration data in between these tools. For the implementation of the protocol gateway function, mapping of the IEC 61850 data objects to the IEC 60870-5-104 protocol was required. This allowed understanding the advantages of the IEC 61850 data model semantics over the legacy protocols data models. At the same time, offered insight on the fact that the additional data model complexity of the IEC 61850 standard hinders its

application for communication to remote command center or higher hierarchy enterprise SCADA systems.

The network protocols testing, performed as part of the practical part of this thesis, allowed further application of the theoretical knowledge gained. In the IEC 61850 technical environment, this is enabled by dedicated monitoring, testing, and analysis tools that further enhance the productivity of the analysis and troubleshooting tasks. The tests performed in this thesis highlighted the fact that, even if complex by nature, network layer communication is a transparent medium that enables the monitoring and troubleshooting tasks required for the successful implementation of an IEC 61850 substation supervisory and control environment.

LITERATURE

- [1] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850, Communication networks and systems for power utility automation - Part 1: Introduction and overview. IEC TR 61850-1:2013.
- [2] INTERNATIONAL ELECTROTECHNICAL COMMISSION - POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE, 2025. *IEC TC57 "Power system management and associated information exchange" Current and future smart grid standardization activities*. Online. IEC - TC57 Web Site. Available at: https://www.iec.ch/resources/tcdash/Poster_IEC_TC57.pdf. [accessed 2025-03-11].
- [3] An introduction to the Unified Modeling Language, 2023. Online. *IBM Developer webpage*. Č. 25 June 2023, p. 1. Available at: <https://developer.ibm.com/articles/an-introduction-to-uml/>. [accessed 2025-02-11].
- [4] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850-7-1, Communication networks and systems for power utility automation - Part 7-1: Basic communication structure - Principles and models. IEC 61850-7-1:2011+AMD1:2020 CSV.
- [5] Successful digitalization in energy projects with IEC 61850: An executive overview. Online. *Successful digitalization in energy projects with IEC 61850 - An executive overview: An executive overview*. P. 22. Available at: https://f.hubspotusercontent30.net/hubfs/5842238/Campaigns/2021/White%20Paper/WhitePaper%20IEC61850_EN.pdf. [accessed 2025-05-11].
- [6] MAZAN, Jan, 2022. IEC 61850 GOOSE Gateway. Online. *PACWORD Magazine*. Č. 05, p. 1. Available at: <https://www.pacw.org/iec-61850-goose-gateway>. [accessed 2025-05-11].
- [7] BRAND, Klaus-Peter and WIMMER, Wolfgang, 2010. The concept of IEC 61850. Online. *ABB Review Special Report*. P. 64. Available at: <https://search.abb.com/library/Download.aspx?DocumentID=3BSE063756&LanguageCode=en&DocumentPartId=&Action=Launch>. [accessed 2025-02-18].
- [8] IEC. IEC 61850, Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs. IEC 61850-6:2009.
- [9] *IEC 61850 Series*. Online. Available at: <https://webstore.iec.ch/en/publication/6028>. [accessed 2025-05-15].
INDUSTRY SOLUTIONS zenon Energy Edition, 2019. Online. P. 9. Available at: https://www.copadata.com/hubfs/Downloads/Brochures/Energy_zenon_BR_EN.pdf. [accessed 2025-05-14]

- [10] Technical solution overview, 2021. Online. Cybersecure Brownfield Plant Automation Architecture Solution. P. 40. Available at: https://d2uars7xkdmztq.cloudfront.net/app_resources/44917/documentation/286603_en-US.pdf. [accessed 2025-05-16].
- [11] Datasheet AVEVA™ Plant SCADA formerly Citect SCADA, 2024. Online. P. 7. Available at: https://www.aveva.com/content/dam/aveva/documents/datasheets/Datasheet_AVEVA_PlantSCADA_24-01.pdf?_gl=1*17h8qav*_up*MQ.*_gs*MQ..&gclid=EAIaIQobChMI3fnm17rLjAMVxJ2DBx0vvS7-EAAYASAAEgJbxvD_BwE. [accessed 2025-03-14].
- [12] Cybersecure Brownfield Plant Automation Architecture Solution Technical Solution Overview, 2021. Online. Č. Version 1.0, p. 40. Available at: https://d2uars7xkdmztq.cloudfront.net/app_resources/44917/documentation/286603_en-US.pdf. [accessed 2025-03-21].
- [13] CIMPLICITY® 2024 – PROFICY® HMI/SCADA SOFTWARE. Online. P. 2. Available at: <https://www.gevernova.com/software/resources/datasheet/enhance-operations-cimplicity-hmiscada>. [accessed 2025-03-21].
- [14] GE VERNOVA. HMI/SCADA WITH iPOWER. Online. Available at: <https://www.gevernova.com/software/resources/datasheet/optimize-utility-operations-ipower>. [accessed 2025-03-21].
- [15] SICAM 8 – Automation Platform for versatile application, 2023. Online. P. 2. Available at: <https://assets.new.siemens.com/siemens/assets/api/uuid:736a74c1-2407-4a0e-9776-82aaaa345621/SICAM-8-Profile.pdf>. [accessed 2025-03-10].
- [16] ENERGY AUTOMATION PRODUCTS SICAM S8000, 2025. Online. P. 2. Available at: <https://assets.new.siemens.com/siemens/assets/api/uuid:6a70847e-d326-4229-a53e-359ad220fb36/SICAM-S8000-Profile.pdf>. [accessed 2025-05-03]
- [17] COM600 series 5.1 User's Manual, 2018. Online. P. 136. Available at: https://library.e.abb.com/public/5189585834da437fbbc318ae964d7f3a/COM600_series_5.1_usm_756125_ENm.pdf. [accessed 2024-10-22].
- [18] FRAUNHOFER INSTITUTE FOR SOLAR ENERGY SYSTEMS ISE, 2024. *OpenMUC User Guide*. Online. 2024-11-11. Available at: <https://www.openmuc.org/openmuc/user-guide/>. [accessed 2025-02-18].
- [19] RYŠAVÝ, Tomáš. Design of a laboratory model of a substation with communication according IEC61850. Online, master's Thesis. Viktor JURÁK (Supervisor). Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, 2023. Available at: <https://www.vut.cz/studenti/zav-prace/detail/151320>. [accessed 2025-01-10].
- [20] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850-8-2, Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP). IEC 61850-8-2:2018

- [21] COM600 series 5.1 Cyber Security Deployment Guideline, 2018. Online. P. 50. Available at: https://library.e.abb.com/public/5189585834da437fbbc318ae964d7f3a/COM600_series_5.1_usm_756125_ENm.pdf. [accessed 2025-02-22].
- [22] MOHAGHEGHI, S.; STOUPIIS, J. and WANG, J., 2009. Communication protocols and networks for power systems-current status and future trends. Online. *2009 IEEE/PES Power Systems Conference and Exposition*. Pp. 2025-03-28. Available at: <https://doi.org/10.1109/PSCE.2009.4840174>. [accessed 2025-05-22].
- [23] MATOUŠEK, Petr. *Description of IEC 61850 Communication*. Online. FIT-TR-2018-01, Brno: Faculty of Information Technology BUT, p. 88. Available at: <https://www.fit.vut.cz/research/publication-file/c168181/279779/TR-61850.pdf>. [accessed 2025-05-10].
- [24] MZ AUTOMATION GMBH, 2025. *Lib60870.NET 2.3.0 User Guide*. Online. 2025. Available at: https://github.com/mz-automation/lib60870.NET/blob/master/user_guide_dotnet.adoc. [accessed 2025-05-10].
- [25] INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016. IEC 60870-5-104, Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles. 2.1. IEC.
- [26] Protocol Implementation Document IEC 60870-5-104 Ed.2, 2022. Online. *TR02-04-04E*. Article TR02-04-04E rev 2, p. 36. Available at: <https://www.svk.se/siteassets/aktorsportalen/entreprenorer-i-elnetet/tekniska-riktlinjer/tr02/tr02-04-04e-2-2022-10-25.pdf>. [accessed 2025-05-22].

SYMBOLS AND ABBREVIATIONS

Abbreviations:

FEEC	Faculty of Electrical Engineering and Communications
BUT	Brno University of Technology
IEC	International Electrotechnical Commission
SAS	Substation Automation System
IED	Intelligent Electronic Devices
SCL	Substation Configuration Language
XML	Extensible Markup Language
TR	Technical Report
SCADA	Supervisory Control and Data Acquisition
DER	Distributed Energy Resources
MMS	Manufacturing Message Specification
GOOSE	Generic Object Oriented Substation Event
SMV	Sampled Measured Values
GSE	Generic Substation Events
ABB	Asea Brown Boveri
OOM	Object Oriented Modeling
UMF	Universal Modeling Framework
CIM	Common Information Model
ANSI	American National Standards Institute
LD	Logical Device
LN	Logical Node
DO	Data Object
DA	Data Attribute
CDC	Common Data Classes
FC	Functional Constraint
SAB	Substation Automation Builder
DTF	Discrete Fourier Transform
PTP	Precision Time Protocol
IEEE	Institute of Electrical and Electronics Engineers
SNTP	Simple Network Time Protocol
HSR	High Availability Seamless Redundancy
PRP1	Parallel Redundancy Protocol version 1
XSD	XML Schema Definition
SSD	System Specification Description
SCD	System Configuration Description
SED	System Exchange Description

CID	Configured IED Description
ICD	IED Capability Description
IID	Instantiated IED Description
SCT	System Configuration Tool
SST	System Specification Tool
FACTS	Flexible Alternating Current Transport Systems
HVDC	High-Voltage Direct Current
IT	Information Technology
HMI	Human Management Interface
OPC	Open Platform Communications
UA	Unified Architecture
EV	Electric Vehicle
DMZ	Demilitarized Zone
VPN	Virtual Private Network
RTU	Remote Terminal Unit
AI	Artificial Intelligence
ML	Machine Learning
HTML	Hypertext Markup Language
MQTT	Message Queuing Telemetry Transport
PIU	Process Interface Unit
OSGi	Open Service Gateway Initiative
FTP	File Transfer Protocol
HTTP/S	HyperText Transfer Protocol/Secure
SLD	Single Line Diagram
SBO	Select Before Operate
SA	Station Address
IOA	Information Object Address
TCP	Transmission Control Protocol
COTP	Connection Oriented Transport Protocol
OS	Operating System
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
CAA	Common Address of ASDU
ASDU	Application Service Data Unit
SIQ	Single Point information with Quality

LIST OF APPENDICES

APPENDIX A – ATTACHMENT FILES	88
APPENDIX B – OPENMUC FRAMEWORK	89
APPENDIX C – WIRESHARK DECODING	90

Appendix A - Attachment files

Archive file DP_Attachments.zip contains the following attachments:

1. SAB600_Exported_Project_SubstationLab.pcmp – SAB600 project export file;
2. PCM600_Laboratory_Substation.scd – PCM600 project export file;
3. OpenMUC__channels.xml – export of OpenMUC framework channels configuration;
4. IED_104_GW_23_5_2025_12_24_14.xls – export of SAB600 IED_104_GW IOA cross-references configuration.

Appendix B - OpenMUC framework

MicroSD card containing Raspberry PI OS (64-bit) with OpenMUC framework deployment configured in the practical part of this thesis.

Appendix C - Wireshark decoding

```

Length: 12
Padding: 3
▼ servicesSupportedCalled: ee0800000402000001fc18
1... .... = status: True
.1... .... = getNamelist: True
..1... .... = identify: True
...0... .... = rename: False
...1... = read: True
...1... = write: True
...1... = getVariableAccessAttributes: True
...0... = defineNamedVariable: False
0... .... = defineScatteredAccess: False
.0... .... = getScatteredAccessAttributes: False
..0... .... = deleteVariableAccess: False
...0... = defineNamedVariableList: False
...1... = getNamedVariableListAttributes: True
...0... = deleteNamedVariableList: False
...0... = defineNamedType: False
...0... = getNamedTypeAttributes: False
0... .... = deleteNamedType: False
..0... = input: False
..0... = output: False
...0... = takeControl: False
...0... = relinquishControl: False
...0... = defineSemaphore: False
...0... = deleteSemaphore: False
0... .... = reportSemaphoreStatus: False
.0... .... = reportSemaphoreEntryStatus: False
..0... = initiateDownloadSequence: False
...0... = downloadSegment: False
...0... = terminateDownloadSequence: False
...0... = initiateUploadSequence: False
...0... = uploadSegment: False
...0... = terminateUploadSequence: False

0... .... = requestDomainDownload: False
.0... .... = requestDomainUpload: False
..0... = loadDomainContent: False
...0... = storeDomainContent: False
...0... = deleteDomain: False
...1... = getDomainAttributes: True
...0... = createProgramInvocation: False
...0... = deleteProgramInvocation: False
0... .... = start: False
.0... .... = stop: False
..0... = resume: False
...0... = reset: False
...0... = kill: False
...0... = getProgramInvocationAttributes: False
...1... = obtainFile: True
...0... = defineEventCondition: False
0... .... = deleteEventCondition: False
.0... .... = getEventConditionAttributes: False
..0... = reportEventConditionStatus: False
...0... = alterEventConditionMonitoring: False
...0... = triggerEvent: False
...0... = defineEventAction: False
...0... = deleteEventAction: False
...0... = getEventActionAttributes: False
0... .... = reportActionStatus: False
.0... = defineEventEnrollment: False
..0... = deleteEventEnrollment: False
...0... = alterEventEnrollment: False
...0... = reportEventEnrollmentStatus: False
...0... = getEventEnrollmentAttributes: False
...0... = acknowledgeEventNotification: False
...0... = getAlarmSummary: False

0... .... = getAlarmEnrollmentSummary: False
.0... .... = readJournal: False
..0... = writeJournal: False
...0... = initializeJournal: False
...0... = reportJournalStatus: False
...0... = createJournal: False
...0... = deleteJournal: False
...1... = getCapabilityList: True
1... .... = fileOpen: True
..1... = fileRead: True
...1... = fileClose: True
...1... = rename: True
...1... = delete: True
...1... = fileDirectory: True
...0... = unsolicitedStatus: False
...0... = informationReport: False
0... .... = eventNotification: False
.0... .... = attachToEventCondition: False
..0... = attachToSemaphore: False
...1... = conclude: True
...1... = cancel: True

```