KTH ROYAL INSTITUTE
OF TECHNOLOGY

Degree Project in the Field of Technology Electric Power Engineering and the Main Field of Study Electrical Engineering

Second cycle, 30 credits

Communication Interfaces for Mobile Battery Energy Storage Applications

ALESSANDRO BONETTI

Stockholm, Sweden, 2023

Communication Interfaces for Mobile Battery Energy Storage Applications

ALESSANDRO BONETTI

Degree Programme in Electrical Engineering
Date: July 4, 2023

Supervisors: Anton ter Vehn, Oskar Svensson
Examiner: Lars Nordström
School of Electrical Engineering and Computer Science
Host company: Northvolt Systems AB
Swedish title: Kommunikationsgränssnitt för mobila batteri-energi lösningar

Abstract

In the midst of the green energy transition, the need for flexible grid solutions is growing. One of the most desired and suitable flexible solutions are Battery Energy Storage Systems (BESS), in both stationary and mobile applications. The faster response times and flexible service capability of the BESS enables the introduction of variable renewable energy sources, along with replacing the needs for traditionally fossil fuel-powered temporary applications. To take full advantage of BESS and its flexibility, the unit requires integration into the modern interconnected smart grid, where control and monitoring are of great importance to manage and optimize assets within the smart grid.

To ease the control and monitoring aspects, both manufacturers and users must cooperate to understand the common needs and best practices to find a suitable middle ground. Therefore, an interoperable and readily used communication interface shall be agreed upon. Although several attempts at reaching such middle ground have been made over the years, few have gained traction outside of specific use cases. Thus leaving many redundant and complicated proprietary communication solutions, requiring heavy integration work for the manufacturer and user side.

This thesis project, carried out at Northvolt Systems, aims to analyze the existing and readily used communication interfaces for a specific set of mobile BESS applications. The analysis is performed by a literature review of typical mobile BESS applications with the identified corresponding communication interfaces. Among the identified interfaces is the IEC 61850 standard, which shows suitability in smart grid applications, enabling interoperability, vendor-independence, and standardization. To provide a real-life analysis of the IEC 61850 benefits and applicability to mobile BESS, an integration of the standard to a Northvolt mobile BESS was performed.

The results of the analysis and integration work show that the interoperability, vendor-independence, and standardization enabled from the IEC 61850 standard give large benefits for mobile BESS use cases. Furthermore, gaps in the suitability of the standard were identified. Providing clear suggestions on future work and expansion of the standard to better accommodate the mobile use cases.

Keywords

BESS, DER, Smart Grid, IEC 61850, Communication Protocol, Flexible Grid

Sammanfattning

I den gröna energiomställningen växer behovet av flexibla nätlösningar. En av de mest önskade och lämpliga flexibla lösningarna är användningen av Batterienergilagring (BESS), i både stationära och mobila applikationer. Genom de snabbare svarstiderna och flexibla användningsförmågarna möjliggör BESS integreringen av variabla förnybara energikällor i kraftsystemet, även genom att ersätta behoven för traditionellt fossilbränsledrivna tillfälliga applikationer. För att dra full nytta av en BESS och dess flexibilitet kräver enheten interaktioner i det moderna sammankopplade smarta nätet. Där kontroll och övervakning är av stor vikt för att hantera och optimera tillgångarna inom det smarta nätet.

För att underlätta kontroll- och övervakningsaspekterna måste både tillverkare och användare av BESS samarbeta för att förstå de gemensamma behoven och användningarna för att hitta en lämplig mellanväg. Slutligen för att komma överens om ett driftskompatibelt och lättanvänt kommunikationsgränssnitt. Flertalet försök att nå sådana kompromisser har gjorts genom åren, men ytterst få har slagit igenom utanför dess specifika användningsfall. Därmed finns det många redundanta och komplicerade proprietära kommunikationsgränssnitt som kräver tungt integrationsarbete av både tillverkar- och användarsidan.

Detta examensarbete, utfört hos Northvolt Systems, ämnar att analysera de befintliga och använda kommunikationsgränssnitten för mobila BESS-applikationer. Analysen utförs av en litteraturgenomgång av typiska mobila BESS-applikationer för att identifiera motsvarande kommunikationsgränssnitt. Bland de identifierade gränssnitten finns IEC 61850-standarden, som visar lämplighet i smarta nätapplikationer, vilket möjliggör interoperabilitet, leverantörsoberoende och standardisering. För att ge en verklig analys av IEC 61850-fördelarna och tillämplighet hos en mobil BESS utfördes en integration av standarden till ett av Northvolts mobila BESS.

Resultatet av analys- och integrationsarbetet visar att IEC 61850-standarden möjliggör interoperabilitet, leverantörsoberoende och standardisering, vilket ger stora fördelar för de mobila BESS-användningsfallen. Vidare identifierades brister i standardens lämplighet. Därtill ges tydliga förslag på framtida arbete och utvidgning av standarden för att tillgodose de mobila användningsfallens kravställningar.

Nyckelord

BESS, DER, Smarta nät, IEC 61850, Kommunikationsprotokoll, Flexibelt nät

Acknowledgments

I would like to start by giving sincere thanks to my academic supervisor Anton ter Vehn, for his great support and guidance throughout the thesis project. Specially the efforts in reaching out to key industry players to discuss the project scope and get the industry point of view. My thanks also go to my examiner, Lars Nordström, for his great insight and support in the topic researched. Furthermore, I would like to express my gratitude to my company supervisor, Oskar Svensson. Who has helped me multiple times throughout the project to manage my time and workload while balancing my studies and thesis along with the enrolled part-time work tasks at Northvolt.

Next, I would like to give my sincere thanks to the Voltpack Mobile team and Northvolt for providing me this opportunity to conduct this thesis, while managing a part-time position. Many thanks to the support and understanding shown by the entire Voltpack Mobile systems team.

In addition, I want to express my gratitude to the industrial partners who have helped me throughout the project. First, to Jörg Reuter and Mehrdad Kazemtabrizi from Helinks LLC, who enabled my success through the use of the Helinks tool and the support to get started, thanks. Then, I give my sincere appreciation to Karlheinz Schwarz for answering my questions regarding modeling, and maintaining an open blog with comments and thoughts regarding power system automation.

I wish to further give my sincere thanks to Jan-Olov Ankartross and Lukas Gassner at OMICRON Energy for providing me licensing access and support in using the IEDScout tool.

Furthermore, my greatest thanks to the Moxa team, namely Martin Jenkner and Yashar Zeinali, for not only supporting me with the integration work, but also physically delivering an early test unit to get me started with the project.

Finally, I want to express my greatest gratitude to my family for supporting me throughout my studies and thesis enrollment, thanks for always helping me out when I need and having my back. On a more subtle note, I want to thank my Annika for being by my side throughout this work and beyond.

Stockholm, July 2023
Alessandro Bonetti

Contents

List of Figures

List of Tables

Listings

List of acronyms and abbreviations

ACSI	Abstract Communication Service Interface
API	Application Program Interface
BESS	Battery Energy Storage System
BMS	Battery Management System
CAN	Controller Area Network
CDC	Common Data Class
CID	Configured IED Description
CRC	Cyclic Redundacy Check
DA	Data Attribute
DER	Distributed Energy Resource
DNP3	Distributed Network Protocol 3.0
DO	Data Object
DSO	Distribution System Operator
ECP	Electrical Connection Point
EMS	Energy Management System
EV	Electric Vehicle
FCD	Functionally Constrained Data Object
FCDA	Functionally Constrained Data Attribute
GOOSE	Generic Object Oriented System Event
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
ICD	IED Capability Description
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
KTH	KTH Royal Institute of Technology
LAN	Local Area Network

LD	Logical Device
LN	Logical Node
MMS	Manufacturing Messaging Specification
OCPP	Open Charge Point Protocol
OSCP	Open Smart Charging Protocol
OSI	Open Systems Interconnection
PCC	Point of Common Coupling
PCS	Power Conversion System
PLC	Programmable Logic Controller
RES	Renewable Energy Source
SCADA	Supervisory Control and Data Acquisition
SCL	System Configuration description Language
SoC	State of Charge
SV	Sampled Values
TMS	Thermal Management System
TSO	Transmission System Operator
VMS	Voltpack Mobile System

Chapter 1

Introduction

1.1 Background

The project is about the various existing communication interfaces used in industry for mobile energy solutions. Focusing on the electric power areas. In recent times, interest in flexible power grid solutions has increased. These interest are, as an example, flexible grid operation with Battery Energy Storage Systems (BESSs), Electric Vehicle (EV) charging stations, peak shaving to reduce cost, etc. With all these various new applications, Northvolt Systems, with their mobile BESS the Voltpack Mobile System (VMS) [1], are interested to investigate the currently used communication interfaces to determine the most used and best suited interface for each application.

The project aims to perform a thorough analysis of the various communication interfaces applicable to the applications that a mobile BESS can help support, of which, some typical VMS applications are construction sites, festivals, and EV charging stations. For these applications, communication interfaces between various units for monitoring or control are often proprietary, which results in longer and more expensive first-time deployment due to the integration cost for each proprietary communication solution. An example is the commonly used Modbus TCP communication interface, which for each manufacturer and product is proprietary mapped.

The focus of the analysis is on the benefit of using a standardized communication interface for the various applications. This would reduce the integration time and cost of each mobile deployment. The suggested standardized interface is IEC 61850, which is currently heavily used, but not only in substation automation, and is also gaining popularity for other Supervisory Control and Data Acquisition (SCADA) systems also.

After the analysis of the VMS application, an IEC 61850 Manufacturing Messaging Specification (MMS) communication stack is implemented in the VMS, to test its applicability to mobile energy storage. Where a future integration would be to integrate the VMS to a distribution substation for short-time deployment, where a BESS could help with grid congestion and/or voltage support on seasonally strained power grids. Some noted issues are presented in [2], which analyzed the impact of EVs charging congestion in a low voltage distribution network. The notable issues are under-voltage problems due to feeder length and high additional loading due to EV charging.

1.2 Problem definition

With the growing interest in BESS integration into the power system, for flexibility services and other grid supports, the forecast for such installations is set to be prosperous in the coming future. Nevertheless, the mobile BESS applications allow for unprecedented flexibility, as well as lower environmental footprint compared to traditional fossil fuel based mobile solutions. With such application forecast, it's of interest, for both manufacturers and user of such mobile BESS to provide an agreed platform of interoperability, where the systems can easily be integrated into rapid projects and deployments with minimal configuration time. An issue for such scenarios is the non standardization around the communication interfaces used for such applications, where many deployments and project builds on proprietary solutions. Meaning long development effort and resources for complete integrations. Thus, there is a need to understand which platforms and interfaces are currently being used along with their prospected use for future use, comparing them to find similarities and differences along with respective pros and cons. With this onset, a research question was posed for this thesis, as presented in Section 1.2.1.

1.2.1 Research question

Following the problem definition introduced in Section 1.2. Two research questions are formulated for the thesis, namely

- Which are the best suited communication interfaces for control and monitoring of mobile energy storage units?
- How can the IEC 61850 standard be expanded to suit mobile battery energy storage applications?

1.3 Purpose

The purpose of this thesis project is divided into two interests. On the company side, Northvolts purpose is to investigate and learn about the many communication interfaces readily utilized in industrial power applications. This investigation is purposeful to get a good understanding of the current status quo in the industry, along with catching future trends and demands. The latter thesis implementation, of a partial IEC 61850 communication stack, serves as a validation and initial experience in utilizing a standardized interface and its engineering workflow.

For the academic perspective, be it KTH Royal Institute of Technology (KTH) or the overall engineering society, the purpose of the thesis is to investigate the benefits in utilizing a standardized interface and workflow through a real-life implementation and validation. Often, analysis and implementation of the IEC 61850 standard has been done through simulations or HIL (Hardware in the Loop) studies. This thesis aims to provide a basic yet real implementation of the communication stack and workflow to understands its benefits and eventual shortcomings.

1.4 Objectives

To accomplish the purposes presented in Section 1.3. A set of main goals have been formulated for the degree project. Five measurable project objectives are identified, as Objective x (**Ox**), namely

O1 Identify atleast 5 readily used communication interfaces for power/energy applications in industry.

O2 Analyze identified target interfaces.

O3 Study the IEC 61850 Standard regarding BESS applications for power systems.

O4 Implementation of IEC 61850 communication stack within the VMS (Voltpack Mobile System).

O5 Perform a laboratory control test utilizing an IEC 61850 communication protocol to communicate with devices.

For the first objective, **O1**, atleast 5 interfaces are to be found to provide an insightful analysis on multiple perspectives, with pros and cons for each interface and application respectively.

Across all objectives defined above, sets of deliverables and expected results are defined as

O1
- Identification of readily used interfaces in power applications.
- Identification of needs and requirements from a communication perspective for power applications.

O2
- Presentation of interface comparison based on applicability, usability and readiness for each application and interface.
- Classification between interfaces and suggestions of future trends, needs and usage.

O3
- Familiarization with the standard's processes and workflow.
- Deeper understanding of the standard's data model and implementation considerations.

O4
- A basic client-server functionality to investigate supervisory and control applications through the standard's communication protocols.
- Analysis and comparison of implementation workflow against proprietary communication interface, such as Modbus TCP.

O5
- Verification and documentation of integration feasibility in simple SCADA application.
- Novel real-life implementation and execution of communication stack for readily available Distributed Energy Resource (DER).

1.5 Research Methodology

The degree project's main methodologies is comprised of two approaches. Firstly an extensive literature review to gather insight on the various power applications for a typical mobile BESS and the applications typical communication methods or interfaces. The review's focus is to give a general overview of the applications and interfaces, providing a qualitative classification between the various interfaces to each corresponding application. Therefore providing ability to further discuss which areas are of interest for future implementation. To comprise of industry know-how, the literature review is expanded by a quick information gathering from key industry players through

interviews, to provide a nuanced view of the status quo on each application investigated.

Secondly, for the validation part, a part implemented communication stack following IEC 61850 structure is done. The implementation is performed at a real-life stage, in contrast to other simulations or HIL integrations. Such an implementation gives a better view and understanding of the real challenges and opportunities in integrating a standardized communication architecture. Along with concrete description of such real-life integration with its challenges and benefits.

1.6 Delimitations

The degree project is limited to the comprehensive scope of IEC 61850 data modeling and validation. Where data modeling aims to construct a minimal but standard-correct virtualization of the Northvolt mobile BESS. The scope of the modeling is delimited to include the *typical* BESS topology, i.e. a battery storage unit grid connected through a Power Conversion System (PCS) and a power transformer. As the standard allows for great data detail for each physical device, the implemented model will reduce the available data to the minimum needed, as deemed mandatory by the IEC 61850 standard. Another delimitation is in the IEC 61850 communication protocol integration. The project implements the MMS protocol (TCP/IP based). Further IEC 61850 protocols, such as Generic Object Oriented System Event (GOOSE) and Sampled Values (SV), are not implemented. The delimitations are chosen according to the time frame of the degree project while not compromising the scope, to provide an analysis of workflow and integration feasibility. Full integration of additional data points, adaptations, and communication services (protocol) are typical integration projects manufacturers fulfill over months if not years.

1.7 Structure of the thesis

The thesis is structured in six parts. First, a literature review of common BESS applications and which communication interfaces/protocol are commonly used is presented in Chapter 2. Then, the project methodology is presented in Chapter 3. The implemented IEC 61850 compliant BESS data model and virtualization is presented in Chapter 4. The results of the data modeling and validation test cases are presented in Chapter 5 which are then discussed in

Chapter 6. Finally, conclusions and future work is presented in Chapter 7.

Chapter 2

Literature review

This chapter introduces the literature review performed in the scope of the thesis. The review focuses on typical mobile storage applications, to understand which communication interfaces or protocols are commonly used. Firstly, a general introduction to a BESS and the Northvolt mobile equivalent, the VMS is presented in Section 2.1. Then three common mobile applications are covered in Section 2.2, introducing the application and identified interfaces respectively. After, an introduction of the identified interfaces and protocols are presented in Section 2.3, to give a brief overview of the structure and features of the interface or protocol respectively.

2.1 Battery Energy Storage System typical topology

Typically, a BESS is a system purposely used as a mean of intermediate storage of electrical energy. In contrast to the general Energy Storage System (ESS) term, a BESS relies on electro-chemical reactions in the batteries to convert electrical energy into chemical energy, thus with storage capabilities. Thus, the system can be crudely defined into two parts; the energy storage, i.e. the electro-chemical battery often accompanied by a Battery Management System (BMS), whose purpose is to monitor and control the battery system to provide safe operations, such as charge and discharge limits of the entire system. Then, a PCS, whose purpose is to interface the electrical grid connection, and the battery system terminals. Examples are power electronic based converters, which convert three-phase alternating current to direct current, and vice versa depending on the BESS operating status (charging/discharging

etc.). Considering the above two general parts, a general system topology is presented in Figure 2.1. Where the three-phase power system is interfaced by a circuit breaker and, possibly but commonly, a power transformer, providing galvanic isolation of the converters and appropriate voltage levels at the terminals. Then the PCS which interfaces the DC link and battery to the three-phase power system. And finally the battery. This general topology is easily expandable and deployable at various locations of the power grid [3], from low-voltage distribution networks, with smaller scale BESS in the kW range, up to medium-voltage distribution or even high-voltage transmission level BESS in the MW to GW range. Due to this flexibility, the systems fall into the larger term DER. Such systems can operate autonomously with local control or scheduling, along with remote control. Often aggregated by an ESS operator to provide a variety of services, ranging from energy storage to ancillary services, such as frequency support. Further applications focusing on mobile deployment are presented in Section 2.2.

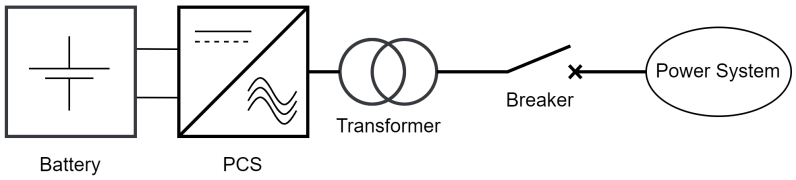


Figure 2.1: Typical single line topology of a BESS.

2.1.1 Voltpack Mobile System

The VMS is a mobile BESS sold by Northvolt. The mobility and flexibility of the system enables novel applications and deployments where BESS previously were unused due to the non-flexible solutions. The system is modular, meaning that the energy storage capacity can be quickly adapted depending on the application case, in contrast to larger and bulkier solutions. The system is built of two main blocks. The PCS building block, responsible for the main control of the mobile BESS. The nominal power rating of the PCS block is 225 kVA, with a maximum peak power in the peak shaving mode of 275 kW [1]. The second block is the modular battery pack. Each pack is rated for 281 kWh, where the system can accommodate up to 5 packs connected together, thus up to 1.405 MWh of energy storage [1]. Four relevant operating modes for this thesis are: *Island* mode, where the system is able to supply an electrical island as a grid forming unit. *Rapid Peak*

Shave mode, where the system provides fast peak shaving capabilities of smaller grid connection, effectively allowing rapid and effective deployments of strong power at locations of limited or weak grid connections, such as construction sites or remote events. *Microgrid* mode, where the system can support a microgrid with customizable droop controls, supporting other grid forming units. And finally, *Grid Boost* mode, where the system runs as a grid following unit, controlling the active and reactive power at its electrical connection point independently. Which is one of the most typical utility BESS use cases, providing setpoints through operator or automatic control as in ancillary services.

2.2 Mobile battery storage applications

The three mobile storage applications presented in this section were identified and chosen through some application criteria. The applications presented focuses mainly on industrial and utility cases. The cases consider applications where storage capacity volumes are higher, such as in hundreds to thousands of kWh. Thus not investigating consumer cases, such as home or residential area storage.

The identified applications are EV charging stations, presented in Section 2.2.1. Off-grid operations in remote ares, such as microgrids, presented in Section 2.2.2. Temporary and mobile utility grid support, such as flexibility services (peak-shaving, frequency regulation, volt-VAR control etc.), presented in Section 2.2.3.

2.2.1 Electrical Vehicle charging stations

As Europe is set to overtake China in the highest rate of EVs by 2030 [4], the inherent need for charging infrastructure and stations is inevitable. In fact, charging stations are set to be a multi billion dollar market, estimated to about 77 billion USD by 2027, with a Compound Annual Growth Rate (CAGR) rate of 44 % from 2022 to 2027 [5]. Thus even if a new infrastructure has to be built, the monetary intention exist. With such growth rate of EVs and respective charging stations, the traditional power grid is set to be on the back foot, where the necessary improvements needed to meet such a demand may take longer than the expected growth. To meet such fast growing demands, novel charging station infrastructure emerge, utilizing energy storage as a mean of power peak shaving, where the station's grid connection is insufficient. These applications may not all be stationary, as

in a charging stations. But also mobile applications, with charging trucks or pop-up events exist, to meet the demand and fast deployment needed for the EVs growth.

A typical charging station electrical topology is showed in Figure 2.2. The topology represents both mobile charging applications, where the grid connection may be intermittent depending on location and power availability, but also more permanent installations. Whether those are retrofits to conventional fueling stations, where the grid connection may not be strong enough, or new charging stations with inadequate grid connections.

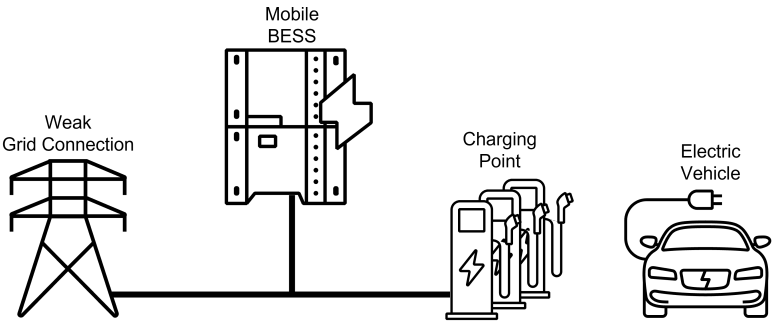


Figure 2.2: Charging Point general topology utilizing mobile BESS.

Several use cases and solutions for such applications exists. Examples include mobile fast charging units, such temporary EV fast charging using Kempower mobile charges, as described in [6]. Allowing for temporary solutions, in case of events or extensions of charging capacity. As the popularity of EVs increases, the need to provide charging solutions at events or remote areas arise, where such applications could use mobile chargers [7], supported by mobile BESS.

As showcased in [8], specific charging stations aided by local BESS can be implemented for peak-shaving purposes. Thus the local BESS can restrain the grid usage, according to the available grid capacity, while maximizing the charging output. This solution enables turnkey integrations of charging stations without the need of grid capacity increase, reducing operating and starting cost, enabling a faster transition to more charging stations.

The uncertainty of peak power and resilience during contingencies from fast charging stations are challenging to the utility power network. As presented in [9], the paper introduces optimization strategies for EV charging stations using local BESS. The optimization algorithm was developed to minimize operational cost, while maintaining resilience to the grid and maximizing the peak-shaving of the station. The algorithm resulted in a 3.9 %

additional peak-shaving and 3.41 % operational cost reduction with the local BESS utilized [9].

Other examples is the mobile EV charging solutions using the Northvolt VMS mobile BESS together with Scania trucks [10]. The solution provided for fast charging solutions (up to 150 kW) in a Swedish ski resort where grid connections not only are limited but often weak. The solution allowed for deployment of charging solutions in the low voltage network in a mobile and flexible way.

2.2.1.1 Identified communication interfaces

An EV related protocol study, conducted by ElaadNL in 2017 shows a thorough analysis of protocols and interfaces used for various EV related applications, such as smart charging, communication between Charging Point Operator (CPO) and central systems (such as Distribution System Operators (DSOs)) [11]. The discussed protocols in the study were; For smart charging, Open Smart Charging Protocol (OSCP), and Open Charge Point Protocol (OCPP), for CPO to central system, OSCP, IEC 61850-90-8, and OpenADR.

OCPP is a protocol mainly aimed between the Electric Vehicle Supply Equipment (EVSE) and charging point [11]. To facilitate smart charging and control over the equipment. Further detail regarding the protocol is presented in Section 2.3.4. OSCP, also commonly used in the EV realm is mainly intended for communications between CPOs and DSOs, providing frameworks for load scheduling and control, further described in Section 2.3.4.

While IEC 61850 was originally developed for substation automation, its been extended over the years to cover further domains. Such as communications between EVSE to CPOs and DSOs (part 90-8) [11]. Further details on the standard is presented in Section 2.3.2.

Another interface identified is OpenADR, which is an automated demand response protocol. As shown in [12], OpenADR was used together with OCPP for managing charging stations. The protocol can be used between the charging station and EVSE to an Energy Management System (EMS) or DSO for demand response applications, such as forecasted load from tariffs, peak-shaving and reducing grid load. Further on the protocol is presented in Section 2.3.5.

Modbus is also another commonly utilized protocol. Although used in various forms, since no enforced standard exist, manufacturers implement own proprietary mappings. The protocol is commonly used between equipment and control systems, such as chargers, BESS and an EMS. Further details on

the protocol are presented in Section 2.3.1.

Summary of the identified interfaces and protocols are listed below

- OCPP & OSCP
- OpenADR
- IEC 61850
- Modbus

2.2.2 Remote off-grid operation

Another typical mobile BESS application is microgrid operations. Which could be at remote locations on or off grid depending on operation and grid availability. Typical usages are at construction sites or event/festival areas where grid connections may be severely inadequate or underdimensioned for the usage needed. In these applications further DERs may be interconnected to form the microgrid. Thus the BESS may take many different operating rules depending on the microgrid topology and grid connection. Such as running in a grid forming mode, forming the microgrid to maintain specific voltage and frequency setpoints. But also to run in grid following mode, assisting droop curves of the microgrid DERs or other services needed (energy shifting).

A general topology of the microgrid is shown in Figure 2.3. The topology visualize a basic microgrid concept, with a single grid connection available at the Point of Common Coupling (PCC). The microgrid side, which for this example is of AC type (examples of DC microgrid exists as well), contains atleast a BESS unit, often accompanied by other DERs units. Which may be gensets (fossil based) for installations with poor grid connections which are temporary, such as construction sites or festivals. Not only fossil based DER may be connected, renewable energy types such as photo-voltaic panels or wind turbines may be present as well. Notably, due to many distributed units that may reside and operate together, communication and control between them is essential. Such control and monitoring can be achieved by both distributed or central logic depending on the philosophy and needs of the microgrid. Nevertheless, a common ground for communication must be met by each respective unit.

Examples of common communication grounds is the study performed by Jun et. al on IEC 61850 based microgrids. The authors presented methods of mapping the IEC 61850 data models and services to IoT protocols, such as XMPP and MQTT [13]. The proposed integration to IoT protocols showed

increased interoperability between the DER units within the micro grid and the utility services (grid operators). The study shows the benefit of standardized data models and services for increased system interoperability and reliability, focusing on microgrid applications.

Further, an overview of the identified communication interfaces for this application is presented in Section 2.2.2.1.

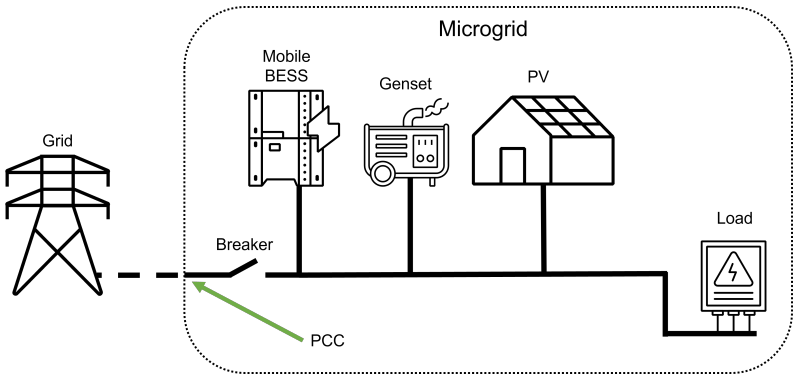


Figure 2.3: Microgrid topology with mobile BESS.

2.2.2.1 Identified communication interfaces

For microgrid topologies, with varying degree of complexity, such as simple genset together with a BESS topology, or more complex systems with metering and local control, a commonly occurring protocol between the systems interconnecting into an EMS is Modbus [14]. Although being a legacy protocol, many examples of such systems and product lines are controllers for gensets and Energy Storage systems, such as a *ASC 150 ESS DEIF Controller* utilizing Modbus as the communication protocol exists [15]. The protocol is further presented in Section 2.3.1.

Other communications interfaces for microgrid applications are Distributed Network Protocol 3.0 (DNP3) and IEC 61850, as discussed in the study of microgrid communications in [14], which highlights both state of the art and future trends, such as IEC 61850. The examples show the usage of the interfaces for SCADA purposes, managing and controlling the microgrid operation in secure and reliable ways.

DNP3 is a communication standard often used in the domain of power engineering. For communications in SCADA systems, such as between system operators and substations, or internally within substations. The standard is further presented in Section 2.3.3.

The original scope of IEC 61850 comes from substation automation. Expanded over the years, the standard also includes specifications allowing for further control. Such as DER managing (part 7-420 [16]), see Section 2.3.2.

Summary of the identified interfaces and protocols are listed below

- Modbus
- DNP3
- IEC 61850

2.2.3 Temporary utility grid support

Following the increase of EVs and general electricity usage, temporary and uncoordinated overload scenarios are becoming more common in distribution grids. These heavy overload scenarios impact on the power quality at the distribution level, as well as overloading the distribution transformer, decreasing their long-term performance [17]. Since these overloads can be temporary and season dependent, increasing transformer sizing may not be economically viable or long term sustainable for future upgrade, thus research shows that usage of strategically placed energy storage can be used to support such grid congestion. Studies such as [18] show that installation of BESS at the secondary side of distribution transformer can provide both technological and economical advantages, by optimizing the storage size.

Furthermore, examples of functions such BESS can partake in are several. As presented in [19], coordinated voltage control strategies for mobile BESS units shows mitigation of voltage violations by coordinated regulatory actions with transformer tap changers, capacitor banks and photo-voltaic generation in a distribution network. Further improvements of BESS placements are presented [20], where strategic placements of BESS can increase the power quality in a distribution grid by supporting voltage and frequency deviations. Power quality issues where BESS support mitigates the issues are; voltage swelling or dipping, both for short spikes and longer scenarios; voltage unbalances, harmonic distortions and frequency support. Moreover, apart from power quality increase, energy storage support functions such as peak-shaving, effectively increasing the physically available power by supporting strained or weak connections, as in the EV application, see Section 2.2.1.

Examples of such coordinations with communication strategies is presented by Albunashee et al. which presents the differences between

centralized control strategies, using Modbus or DNP3 to decentralized control using IEC 61850 [21]. The study implements voltage and reactive power control strategies for DER and capacitor bank coordination. The benefits of decentralized control strategies using the GOOSE protocol is the faster communication capability between the devices.

A generic overview of possible BESS placements for such application is shown in Figure 2.4. The Figure illustrates two separate scenarios, where a BESS is strategically placed within the vicinity of a substation, possibly interacting directly through the station SCADA and upstream control center. Furthermore, similar performances can be obtained by strategic placement of the BESS downstream of the substation, thus not interacting directly with the station but with the control center SCADA. While these two scenarios are electrically near equal (apart from very local voltage capabilities), the communication and security requirements may differ greatly. Namely, the addition of new devices in a substation automation system can pose stricter cybersecurity requirements on the device, these requirements are set by the station operator. While the scenario outside of the station vicinity does not access a station level communication, risks of unauthorized access to critical station functions are reduced.

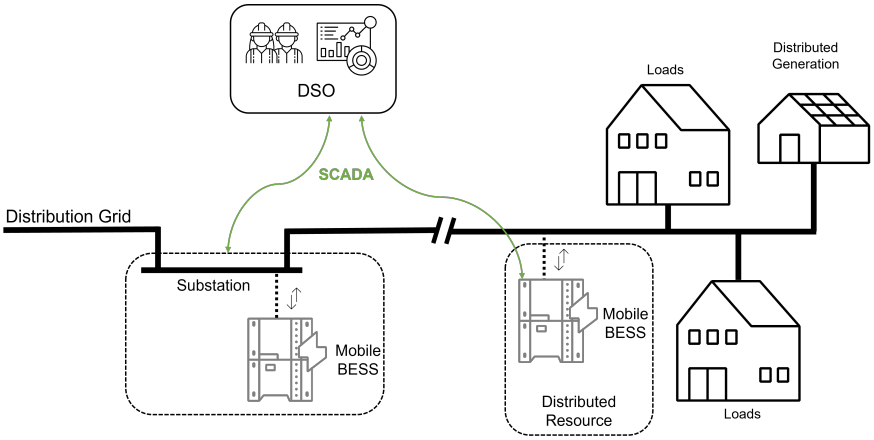


Figure 2.4: Temporary grid support topology. Showing possible locations, either within a substation and its premises, or as a distributed resource outside a station.

2.2.3.1 Identified communication interfaces

Typically, within SCADA systems, where system operators (both DSOs and Transmission System Operators (TSOs)) control centers interact with

substations, both traditional communications interfaces like DNP3 and IEC 60870-5, and modern interfaces like IEC 61850 are used [22, 23]. These interfaces and standards are well utilized and specifically developed for utility applications. Used for monitoring of remote stations and eventual control when needed. The DNP3 standard is presented in Section 2.3.3, while IEC 60870 parts 5-101 and 5-104 are presented together in Section 2.3.6. The IEC 61850 standard is presented in Section 2.3.2.

OpenADR has also been utilized to implement flexibility services towards DSOs. J. Guerrero et. al proposes in [24] the use of OpenADR for communications between distributed nodes, such as DER, and stakeholder by adding monitoring and management services. The papers shows how OpenADR was implemented to a capacity bidding program for control and monitoring of energy consumption. The OpenADR standard is presented in Section 2.3.5.

A summary of the identified interfaces and protocols for this application are listed below

- DNP3
- IEC 60870-5-101/104
- IEC 61850
- OpenADR

2.3 Readily used interfaces

The identified communication interfaces or protocols from Section 2.2 will be introduced in this section respectively. Providing basic information about the interface or protocol, as well as an example of common applications implemented for each.

2.3.1 Modbus

The Modbus protocol is seen as the de facto industrial automation standard protocol since its introduction 1979 [25]. It quickly gained popularity from its simplicity in integrating various devices across multiple networks. Functioning in the application layer, providing client-server based communication. Modbus is a request-response protocol with defined function codes to access or manipulate data. The function codes are essential parts

of the service provided by Modbus and its Protocol Data Units (PDUs). Which are made independent of any underlying communication layers. The Modbus protocol has been expanded throughout its years to meet the industry requirements. Therefore available in several formats. Although their underlying communication layers may differ between the variant, the Modbus PDU is specified equally, although their respective Application Data Unit (ADU) may differ by additional fields dependent on the communication layer.

Several variants of the Modbus protocol exist, an example of the most commons is listed, namely

- *Modbus RTU*, serial communication over different physical layers, such as RS232 or RS485
- *Modbus ASCII*, serial communication using ASCII characters for protocol messaging
- *Modbus TCP/IP*, variant allowing communication over TCP/IP networks. Typically connecting to port 502

Notably, due to its legacy structure where the Modbus PDU was firstly developed for serial line communication, the maximal PDU length is set to 253 bytes [25]. Limiting some operations, such as large data reads.

In general for the Modbus TCP/IP protocol variant, the ADU frame is comprised of a Modbus Application Protocol Header (MBAP) and a PDU. As shown in Figure 2.5. Where the MBAP provide information needed for the TCP/IP communication, an addition compared to Modbus RTU.

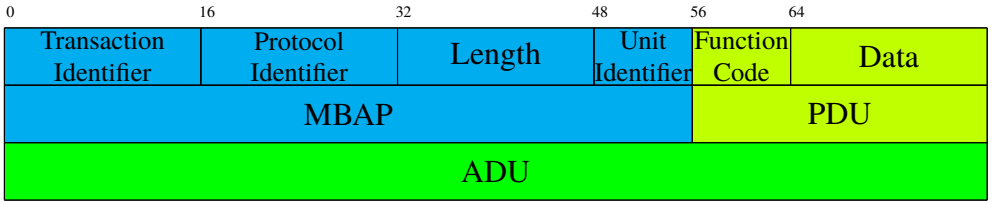


Figure 2.5: Example of a Modbus TCP/IP ADU frame.

2.3.1.1 Typical area of usage

Due to its simplicity in implementation and integration. Modbus across its multiple variants is one of the most common industrially used protocols. With, although its age, a large share of usage, in both field bus applications (RTU) and industrial ethernet applications [26].

The protocol was designed for automation between Programmable Logic Controllers (PLCs) in industrial applications. Whether it's manufacturing processes or other industrial automation's, Modbus has gained a high share of usage. Nevertheless, the standard is used in various power applications as well, providing easy and robust communication interface between various devices therein. An example is the work done in [27], presenting a reconfigurable microgrid using Modbus and Controller Area Network (CAN) bus as the basis for the communication system architecture. Showing a planning basis for future integration of localized power generation and consumption trough introduction of Renewable Energy Sources (RESs) maintaining high reliability in operation.

2.3.1.2 Security concerns

Several security concerns regarding the Modbus protocol are brought up in literature. Amongst these, the authors in [28] list several attack methods which exploits the protocol specification. Such as *baseline response replay* where the attacker may record genuine traffic between the client and server, for later replaying to the server. Others note about the lack of encryption specified in the standard and authentication of communication [29].

Another famous vulnerability is the *Modbus Worm*, as presented in [30]. The *Modbus Worm* exploits the non existing authentication and integrity mechanism in the protocol. By writing arbitrary data to the Modbus server, possibly altering the SCADA system and the process controlled therein.

2.3.2 IEC 61850

The IEC 61850 standard was developed in the early 2000s. Where the first main parts where published between 2002 to 2005. A result of nearly a decade of work within the IEEE on power utility communication [31]. The origins of the standard arises from utility work within protection, control and monitoring of substations. Over the years, the standard has developed to also cover measurements, such as statistical and historical data and power quality. With the concepts of the standard being introduced beyond the initial substation domain, to also include parts for hydropower plants (IEC 61850-7-410), DERs (IEC 61850-7-420), wind turbine modeling according to IEC 61850 in the IEC 61400-25 series and extension to substation to substation communications (IEC 61850-90-1). With planned expansions in areas such as network control centers (IEC 61850-90-2) and feeder automation [31]. Finally, IEC 61850 has gained significant recognition over the years as it has been designated by the

International Electrotechnical Commission (IEC) as one of the fundamental core standards for implementing the smart grid [32].

Fundamentally, the IEC 61850 standard series is based on three methods. **Functional decomposition**, the ability to represent the components of a distributed function using logical relationships. Where the standard introduces Logical Nodes (LNs), describing functions, subfunctions and its interfaces. **Data flow modeling**, the flow of data between communication interfaces supporting exchange of information between distributed functional components and their performance requirements. Lastly **information modelling**, to define the abstract syntax and semantic of the information exchange, based on data object classes, with types, attributes, object methods and relationships between [31].

The main objective of the standard is to provide interoperable, vendor independent frameworks between Intelligent Electronic Devices (IEDs) [31]. To achieve this, the standard defines three main protocols for its information exchange. A client-server protocol for communication between a SCADA client or IED to an IED using MMS, see Section 2.3.2.1. Two peer-to-peer protocols for faster communications between IEDs, the first for transmission of object oriented event reporting called GOOSE, see Section 2.3.2.2. The second for fast streams of measurement data, for example by replacing hardwired connection from instrument transformers to digital values, called SV protocol, see Section 2.3.2.3.

Amongst the most important aspects of the standard is the standardized data models. The basis for the IEC 61850 data model are the so called LNs, which are standardized objects representing either physical or virtual functions and or equipment [33]. Examples of LNs could be functions for protection purposes, metering, control of physical equipment (breaker and switches) and so on. The part IEC 61850-7-4 introduces the basic data models of the standard [33]. Further additions have been done, such as DER logical nodes, defined in part IEC 61850-7-420 [16]. An example of the IEC 61850 data model is shown in Figure 2.6. The basis of the model is the *physical device*, i.e. the IED. Within an IED, multiple *logical devices* may be defined as to serve various purposes of the *physical device*, such as protection, control or metering, defined as Logical Devices (LDs) in the data model. Each *logical device* may contain several standardized *logical nodes* according to the standard namespaces (such as 7-4 and/or 7-420) defined as LNs in the data model. The example figure shows two *logical nodes*, **XCBR1** representing a breaker and **MMXU1** representing electrical measurements. Each *logical node* consists of several Data Objects (DOs), whom themselves are objects of

Common Data Classes (CDCs). The example figure shows the **Pos** DO of the breaker LN (**XCBR1**), which represents the breaker position as a double bit status (stVal), a quality flag (q) and a timestamp of the value (t), all defined as Data Attributes (DAs). Depending on the configuration, the **Pos** DO may also allow for operate control of the breaker position, i.e. opening and closing. Similarly, for the measurement LN (**MMXU1**) the example shows the DO **TotW**, representing the total three-phase power, given as a magnitude (Mag), a quality flag (q) and a timestamp of the value (t).

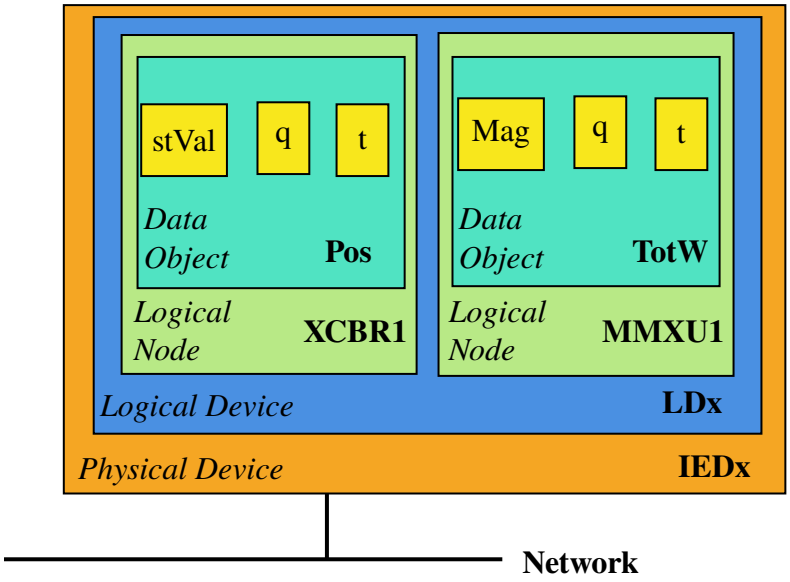


Figure 2.6: Example of an IEC 61850 Data model.

Another key feature of the standard is the ability for configurable reporting. Such as event driven reports, cyclic reports or interrogation reports (requested by clients). The basis for the IEC 61850 reports are made of two parts, the datasets and report control blocks [34]. A dataset is an ordered set of DOs references called Functionally Constrained Data Objects (FCDs) or a set of DAs called Functionally Constrained Data Attributes (FCDAs). The ordered set must be known to the client and the server [34]. The report control blocks are responsible for the configurable reporting mechanism provided by the standard. Two types exist, buffered and unbuffered report control blocks. For buffered report control blocks, the reporting information is kept in memory in case of transmission loss or communication interrupts, such that they can be resent upon communication healing. For the unbuffered ones, the data is lost in case of connection loss [34].

2.3.2.1 MMS protocol

The MMS protocol is based on a client-server topology. The protocol is TCP/IP based, where MMS resides in the application layer, relying on TCP/IP for error detection and recovery. A MMS client sends a request for a specific data item to a MMS Server of an IED, identified by an unique IP address. The server return the requested data in a response message to the client. The protocol also supports a client to send spontaneous notifications, for instance in the occurrence of an event. [35]

2.3.2.2 GOOSE protocol

The GOOSE protocol is used for faster data exchange within an IEC 61850 network. The GOOSE messages are exchanged at the link layer, utilizing the multicast functionality provided by Ethernet. The basis for GOOSE communications resides in event-driven transmission of messages on a publisher-subscriber topology. The messages are sent in a cyclic manner as a heartbeat indication. Upon the occurence of a preconfigured event, the publishing IED immediately sends a new GOOSE message with the values of the variables configured for the event. Since the messages are multicasted, the publisher does not receive acknowledgment of arrival. To overcome any errors in transmission, the messages are retransmitted at a high rate interval, gradually decreasing the intervals. The rate of retransmission is application specific. Since the messages operate at the link layer, they cannot cross over networks, being bounded by the network routers. The messages are identified by the publisher MAC address, along with an identifier of the message. Being a publisher-subscribe protocol, any new message value replaces the former one, instead of queuing. [35]

2.3.2.3 SV protocol

The SV protocol, specified in IEC 61850-9-2, is defined for transmission of analog values, such as current and voltage, from sensors (merging units) to subscribing IED. Like the GOOSE protocol (see Section 2.3.2.2), the protocol resides in the link layer, utilizing the Ethernet multicast functionality in a publisher-subscriber model. The messages are likewise identified by the publisher MAC address and an identifier, where the messages are periodically transmitted at a high rate. Since no retransmission is possible, any lost message is overwritten by the next successful message transmission. The rate of transmission is dependent on the grid frequency, for a 50 Hz grid the standard

specifies a period of 250 μs. [35]

2.3.2.4 Typical area of usage

Being specifically developed for the substation automation domain, the standard is well defined within the power system area. With additions during the years to cover other domains, such as hydroplants and DERs [22]. As listed by Mackiewicz in [36], some of the key features of the standard includes

- **Virtual models**. The virtual models of LDs and LNs directly gives definitions of the data, services and behavior of the devices.
- **Named data**. IEC 61850 data is named with descriptive strings in a power system context describing the data. A feature lacking in legacy protocols where data often is indexed.
- **Self-describing devices**. Clients are able to online download the IED data description, thus not needing any manual configuration to retrieve the data objects.
- **Lower installation cost**. The fast protocols defined in the standard, such as GOOSE is able to quickly exchange data or status over the Local Area Network (LAN) without separate and unique wires for each status or signal. Significantly reducing installation cost due to wire reduction, construction costs (digging of trenches, ducts or conduits).
- **Lower Commissioning Costs**. Reduced configuration and commissioning costs as the manual configuration is minimized. Client applications do not need manual configurations as the data point list can be access directly from the devices or imported. As manual configuration is minimized, the risk of errors and rework is also minimized.
- **Lower Extension Costs**. IEC 61850 devices do not need reconfiguration to expose new data. Thus extending a system by adding devices or applications can be done with minimal system impact.
- **Lower Integration Costs**. Utilizing widely used networking technology within the utility enterprise. Integration cost of new systems and data can be reduced. Instead of costly proprietary solutions for each device, needing manual configuration and maintenance for each data point needed in the SCADA system, IEC 61850 can deliver data without separate communication interfaces or device reconfiguring.

2.3.3 DNP3

The DNP3 protocol standard was initially developed by Westronic Inc. during the early 1990s. The main goal of development was to design an open protocol for the utility industry. Notably, at the time of development, was a need of scalability due to the bandwidth limitations present. The goal was therefore set for a protocol reducing the needed bandwidth and using fewer layers [37]. Further on, the protocol was also designed for reliability, utilizing Cyclic Redundancy Check (CRC) to ensure reliable data transfer. The basis of the protocol is a master to outstation topology. Typically a master initiates a request to an outstation.

Some of the defining features of the protocol are listed below, namely

- Broadcasting. Ability to send a message to multiple recipient devices.
- Select before-operate. Extra reliability when operating an output. Can be enabled or disabled.
- Time-stamped data. Ability to provide a time-stamp for each datapoint.
- Time-synchronization. Ability to provide accurate time-synchronization between master and outstation.
- Quality flags. Flag representations to show whether a data is valid, and why.
- Multiple data formats. Data can be reported amongst various data formats, further described in Table 2.1
- Layer separation. Application functions separated from transport and network layers.
- Report-by-exception. Ability to report only changes in data, in contrast to full data reporting. Reducing bandwidth needed.
- Internal indications. Global set of flags send in each request response. Indicating device health and request results.

As presented in [37], the DNP3 basic message and data flow is performed on a master-outstation model, see Figure 2.7. The master initiates a data transfer through its user layer passing by an application layer to send a request to the outstation. The request contains a function code (which indicates the request function, such as read, write, confirm etc) and eventually a DNP3

Data formats	Data type	Description
Binary Output	boolean	Typically utilized for single status output commands or settings
Analog Output	16-bit integer 32-bit integer 32-bit float 64-bit float	Typically utilized for commands or settings which require more data, such as integers or floats.
Binary Input	boolean	Typically used for statuses such as breaker input, relay logic etc.
Analog Input	16-bit integer 32-bit integer 32-bit float 64-bit float	Typically used for measured values such as electrical quantity measurements like voltage and current
Counter Input	16-bit integer 32-bit integer	Typically used for counter inputs such as pulsating values

Table 2.1: Basic DNP3 data formats [37].

object to specify the data requested. the transport function partitions the request into sized transmission units, feeding further to the data link layer. This layer is responsible for addressing and error detection, appending such information to the request, finally transmitting the packet to the outstation through the physical media. At the outstation the layers are reversed. Firstly the outstation data link layer check for errors during physical media transmission. Upon a successful error check, the address and error detection is removed from the message before feeding the application layer. The application layer will then interpret the requested function codes and possible DNP3 objects to inform the user layer about the request.

The outstation will initiate a response based on the master request, passing back down the DNP3 layer all the way back to master user layer. In DNP3 it's always the master which initiates control commands to various variables or actuators belonging to an outstation. However the protocol also defines reports initiating *unsolicited responses*. Thus the outstation may initiate a response granted its data is deemed notable enough for transmission without an implied master request.

A comparison of the DNP3 model to the general Open Systems Interconnection (OSI) 7 layer model is shown in Figure 2.8. Where the presentation and session layers are non present, including a pseudo transport and network layer instead of separate.

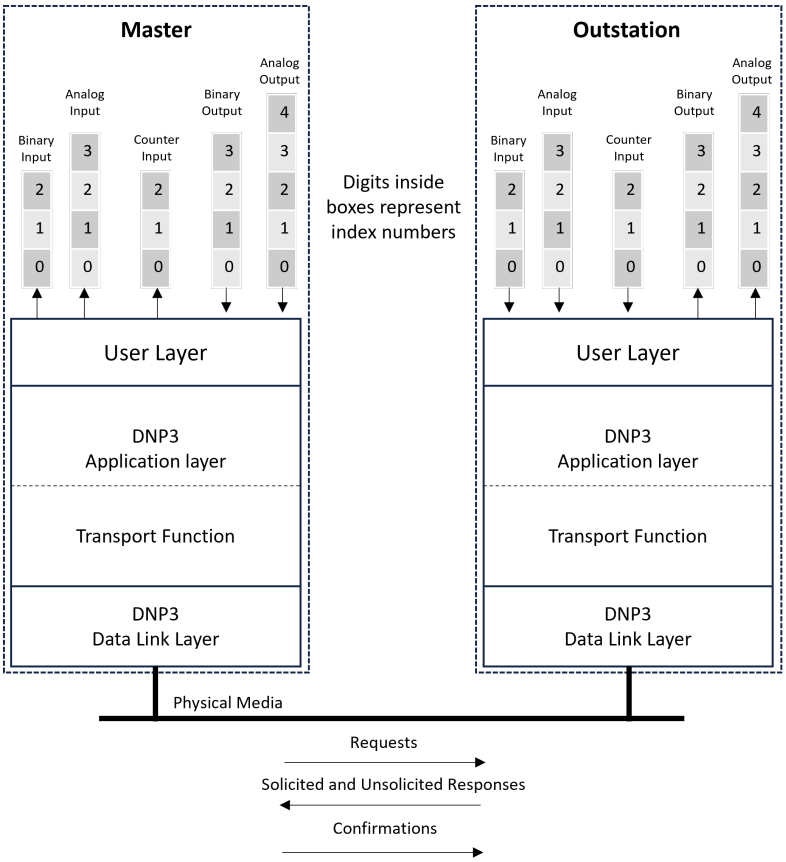


Figure 2.7: A DNP3 master-outstation model as illustrated in [37, Figure 0.1].

In an implementation study, analyzing the usage of DNP3 as a communication protocol for a smart grid, showed that the protocol although being viable for usage, still lacked in performance for more time critical application [38]. The study was performed by integrating DNP3 over TCP/IP for a *Green Hub* distribution level microgrid, including distributed energy storage. Experiments of fault clearing showed that the communication delay for DNP3 event driven modes was sufficiently low for some protection functions, such as fault clearing. But scaling the system to more communication units could be problematic due to the high bandwidth required for the event driven report publishing. The authors then concluded that a priority system could be beneficiary to the standard, to give higher priority to time critical applications such as protection, while *real-time* messages should also maintain higher priority than *low-speed* messages [38].

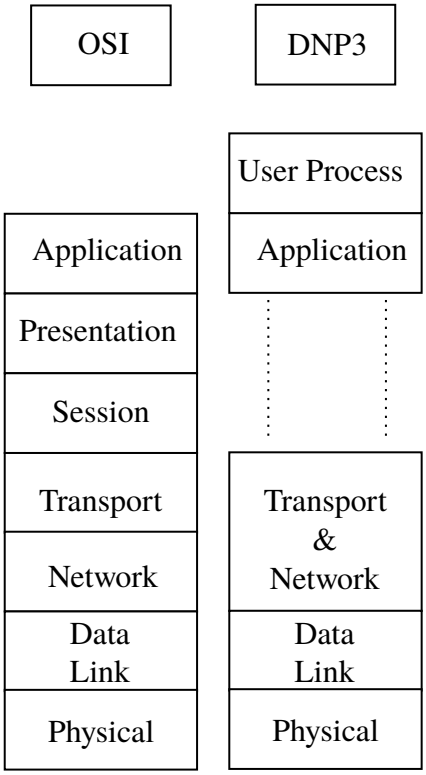


Figure 2.8: DNP3 and OSI model layers.

2.3.3.1 Typical area of usage

DNP3 is a communication protocol specifically designed for power utility automation. It's prominently used in the Americas, Australia, parts of Asia, and Africa [22]. Although initially designed for power utility, the protocol is also seen in other industries, such as, oil and gas, security and water.

It is very similar to the protocol defined in IEC 60870-5, see Section 2.3.6. Although DNP3 is compliant with standard IEC 60870-5-1 and IEC 60870-5-2, it's not with IEC 60870-5-101. Where the application layer differ greatly, thus the two are not interoperable [37].

2.3.3.2 Security concerns

As the DNP3 standard does not implement any encryption or authentication mechanisms it is vulnerable to a large variety of attacks. Although DNP3 uses simple integrity measures by CRCs, a study managed to identify 28 attacks and 91 attack instances to the protocol layers. The effects of the to attack ranged from retrieving network or device configurations to corrupting

outstation devices, gaining control of master units [39].

Further concerns regarding security comes from the function codes that can be used. The function code `0x0D` can reset and reconfigure a DNP3 outstation by forcing a power cycle. While reinitializing, some devices may clear their internal messages queues. Which an attacker can use to their advantage, purposely causing delays in remote outstations before they reconnect and accept genuine requests [40]. The function code `0x13` enables loading new configurations for the outstation, such that an attacker with unauthorized access can alter settings, possibly suppressing critical alarms or outputs [40].

2.3.4 OCPP & OSCP

The OCPP is an open standard developed for two way communications between an electric vehicle charging stations and their respective Electric Vehicle Supply Equipment (EVSE) to the Charging Point Operator (CPO). As the standard is primarily intended for communications between CPOs and EVSE/charging stations, the device models presented in the standard does not include modeling options for communication to non-EV related equipment, such as BESS. Although the standard specifies that exceptions could be done, as to alter the device model by removing the top-level *charging station* in its model. At the moment, the OCPP specification does not provide such use cases, although those could be added in the near future [41].

As specified by the Open Charge Alliance, the overall charge point topology can be simplified as in Figure 2.9 [42]. Where as introduced earlier, OCPP is primarily intended for communications between CPOs and EVSE/Charging points. Another Open Charge Alliance standard is developed for communications between CPOs and DSOs. Notice that the two dashed protocols, between the EV and EVSE are not in the scope of this project, since they're intended for low level wired communication between the charging equipment and vehicle.

OSCP is a standard developed for utilizing flexible energy resources based on their available capacity integrating toward smart charging of EVs. The standard domain model defines four domains. A *Flexible Resource*, which is a physical device that can control its consumed or generated energy in a flexible way. For instance, EVs BESS or heat pumps etc. The flexibility of the resource is respective of time and/or ability to consume or generate energy. The next domain specified is the *Flexibility Provider*, which controls a set of Flexible Resources. It's therefore responsible for requesting the resources to either

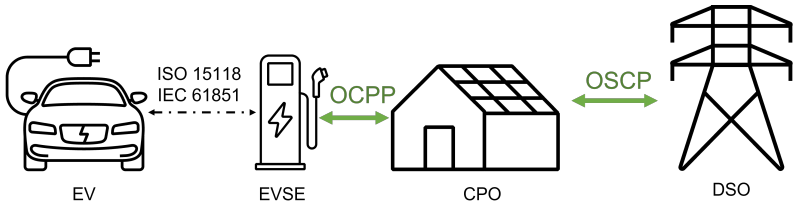


Figure 2.9: General charging point topology and respective protocols for data exchange.

consume or produce energy. Providers could be CPOs or battery operators. A further domain is called *Capacity Provider*, defined as the manager of the grid operation, doing measurements and or imposing boundaries on Flexibility Providers within its grid. The Capacity Provider does not address the resources directly, but interact through the Flexibility Provider. Examples of such Capacity Providers are DSOs, which are responsible for correct grid operation, thus enforcing boundaries on grid capacity available for the Flexibility Provider. The last domain specified is the *Capacity Optimizer*, which can support the Flexibility Provider by optimizing the usage of its resources. This could be done by weather forecasts or historical data (energy tariffs) to determine the optimal operating point. The role of the Capacity Optimizer could however also be taken by either the Capacity Provider or Flexibility Provider by themselves. [43]

The underlying protocol utilized by OSCP is Hypertext Transfer Protocol (HTTP). Where a set of messages are defined. The standard is based on HTTP combined with JSON formatting, fitting well within a RESTful Application Program Interface (API) architecture [43]. The set of messages defined in the standard are presented below, namely

- `Register`
  - Message to be sent before any other message. Provides tokens to register authentication between messages.
- `Handshake`
  - A request to initiate a handshake mechanism, part of connection between the domains.
- `HandshakeAcknowledge`
  - Response sent after a handshake request.

- `Heartbeat`
  - The heartbeat message is sent periodically to notify the sender of the availability of the domain. The interval of heartbeats is determined in the Handshaking mechanism.
- `UpdateGroupCapacityForecast`
  - Message containing a capacity forecast of the available capacity over a creating area over a time period. The message is sent from the Capacity Provider to the Flexibility Provider. It could also be sent from the Flexibility Provider to the Capacity Optimizer to request an optimal forecast in said area.
- `AdjustGroupCapacityForecast`
  - Message sent from the Flexibility Provider to the Capacity Provider if it can't meet the capacity limits provided. Thus requesting an adjustment. The Capacity Provider may then respond with an updated forecast with a `UpdateGroupCapacityForecast` message.
- `GroupCapacityComplianceError`
  - Message send from the Flexibility Provider to the Capacity Provider to inform if it can't comply with the forecast requested.
- `UpdateGroupMeasurements`
  - Message used for the total usage of the aggregated area in control of the Flexibility Provider. The message is provided from the Flexibility Provider to the Capacity Provider.
- `UpdateAssetMeasurements`
  - Message containing metering values sent from the Flexibility Provider to the Capacity Optimizer. The optimizer may use these values to return an optimized forecast profile, which is returned through a `UpdateGroupCapacityForecast` message.

Where the used data types are given in Table 2.2.

Data type	Description
`string`	Unicode characters
`object`	Unordered collection of key:value pairs
`integer`	32-bit signed integer No leading zeros or plus sign allowed
`decimal`	Floating point number with maximal 8 decimal places
`datetime`	Time values formatted according to RFC3339 Decimal places limited to 3.
`AnyType`	Textual data with unspecifed length or format
`boolean`	Digital values which only takes either ”false” or ”true”
`URL`	String of maximal 255 characters as per defined by the URL specification
`null`	Empty data

Table 2.2: Data types defined in OSCP 2.0 [43].

2.3.4.1 Typical area of usage

OCPP is an open standard specifically developed for communications between the CPO and EVSE. Although further expansion is considered by the standard responsibles, such work is not openly available as of the thesis. Nevertheless, the standard is prominently used worldwide at charging stations, quickly gaining traction as installations are increasing following the green energy transition [11].

OSCP is developed for the communication between the CPO and DSO. Used for management of charging stations from the utility owner point of view, to enable flexible usage and grid support through capacity scheduling [44].

2.3.5 OpenADR

The standard OpenADR began in development following an energy crisis in California, USA during 2002. The crisis led to the creation of this demand response standard, which has gained traction as a Smart Grid standard to ensure interoperability for demand response [12]. OpenADR is meant to be an open standard to facilitate two way information exchange on a demand response basis. It standardizes the message format for management of Auto-DR (demand response) and DERs to enable dynamic price and or reliability

information exchange in an interoperable way between utilities, EMSs and control systems [45]. OpenADR was created to simplify the automation of existing demand response and DER systems for the power utility industry, with message signals allowing users to optimize energy efficiency and effectiveness of their power system [45].

Demand response functions define a set of actions that units can take during power system contingencies. Such as reducing their load to help the supply demand of the system or as a reaction to market prices. Automated demand response implies fully automated signaling from system operators (utilities, DSOs etc.) providing automated controlling of their end-customer control system or strategy. OpenADR is meant to act as a foundation for such interoperable information exchange [46]. After the second edition, OpenADR 2.0, the standard was submitted to the IEC, where it is now available as IEC 62746-10-1 [47].

The signalling model of OpenADR defines nodes divided in two groups. Servers which publishes information regarding upcoming events are named Virtual Top Nodes (VTNs) and are considered to be upstream. While the automated clients, which receives the information downstream are named Virtual End Nodes (VENs) [45].

The nodes communicate using two protocols. One protocol is HTTP, using a PUSH request when the VTN initiates communication. Or using a PULL request when the VEN request information from a VTN, thus initiating message exchanges. The standard also defines communication over another transport protocol, XML Messaging and Presence Protocol (XMPP) [45].

The standard defines data models by supplying own schemas defining subsets of DER units. Including, hierarchical element relations, ordering of elements and mandatory cardinality between them.

The signal definitions of the standard consists of 10 base signals. The standard allows for extensions of the signal list, such to meet own requirements, but there is no requirement of compliance between other VENs or VTNs. A summary of the signals are given below, namely

- `SIMPLE`
  - Simple levels.
- `ELECTRICITY_PRICE`
  - Price of electricity, indicated in units currency/kWh.
- `ENERGY_PRICE`

  - Price of energy, indicated in units currency/kWh

- `DEMAND_CHARGE`
  - Demand charge price, indicated in units currency/kW

- `BID_PRICE` /`BID_LOAD` /`BID_ENERGY`
  - Customer bid levels. Used to indicate the bidding price, the amount of load of the bid and amount of energy corresponding.

- `CHARGE_STATE`
  - Used to dispatch storage resources. Such as providing setpoints for charging or discharging the unit.

- `LOAD_DISPATCH`
  - Instructions to set the load values of the unit.

- `LOAD_CONTROL`
  - Instruction used to set the load control values relative to the units output capacity. Therefore not requiring the VTN (or VEN) to know the precise load consumption, but expressed such that the VTN can increase or decrease the load consumption.

The standard also support a variety of reports, which are structured according to a report tree, see Figure 2.10. For compliance to the standards, the VTNs and VENs are not required to support all report types. There's possibility to develop deployment-specific reports as an extension, but it cannot be expected to comply for other VTNs/VENs [45].

The **METADATA** report is used to indicate the VTN/VEN reporting capability. The **METADATA** report may itself contain specifications of more report types, each with its own descriptors and specification [45].

A branch of **DATA REPORTS**, which are non metadata reports are used to report the actual data, either measured or calculated. The core element of any **DATA REPORT** is the *data point*. A *data point* represents certain quantities of the report, either measured or calculated. The *data point* has certain specified attributes, such as units, scaling etc. A **DATA REPORT** may contain several *data points*. For example, the **METADATA** report may contain a report consisting of *data point* sets that can appear in a report, such as a VEN providing reports of both energy and power as separate *data points*.

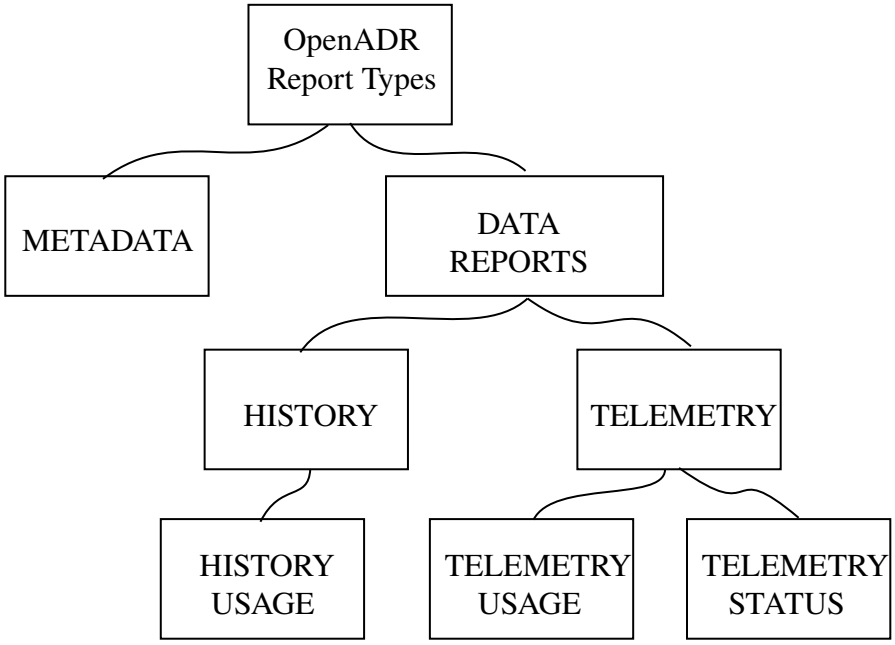


Figure 2.10: OpenADR report types.

Subsets of **DATA REPORTS** exists. Such as **HISTORY**, which is a report type showing the history of *data points* logged. Further subset of **HISTORY** report is a **HISTORY USAGE** type, which stores logs of the usage data.

Another subset is the **TELEMETRY** report type, which refers to periodically real-time reported data. Two subsets exist, namely **TELEMETRY USAGE** and **TELEMETRY STATUS**. The former is a type to show the usage data of the periodic reports. The latter reports the current status of the resource, available as a periodic report from a VEN to a VTN.

2.3.5.1 Typical area of usage

The standard was intentionally developed for the energy and power industry, to provide a standardized automated demand response protocol for utilities. Some use cases of the standard are EVs charging stations turned into demand response units by automating the communication between the CPO and DSO as shown in [12]. Other use cases include the demand response architecture of a virtual power plant. It allowed an interface between a photo-voltaic virtual plant and utility DER management software. Such that the virtual power plant storage systems charged and discharged concerning the utility need (demand) [48].

2.3.6 IEC 60870-5-101/104

The standard IEC 60870 defines various systems utilized for telecontrol applications, such as SCADA systems. Amongst these set, the most commonly used part for electrical power systems is part 5, i.e. IEC 60870-5 [22]. The standard comprises of 7 parts, along with 6 companion standards, namely parts

Telecontrol equipment and systems

- 5-1 Transmission frame formats
- 5-2 Link transmission procedures
- 5-3 General structure of application data
- 5-4 Definition and coding of application information elements
- 5-5 Basic application functions
- 5-6 Guidelines for conformance testing
- 5-7 Transmission protocols - Security extensions

Companion standards for basic telecontrol tasks

- 5-101 Transmission protocols
- 5-102 Transmission of integrated totals
- 5-103 Protection equipment
- 5-104 Network access
- 5-601 Conformance test cases for 5-101
- 5-604 Conformance test cases for 5-104

The protocol structure is based on the three-layer reference model Enhanced Performance Architecture (EPA) defined in IEC 60870-5-3. A basic model of the structure is shown in Figure 2.11. For 5-101, the physical layer utilizes the ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) recommendations, providing symmetric and memoryless binary transmission on a physical medium. Preserving high level data integrity from the defined block encoding methods in the link layer. The link layer consists of multiple transmission procedures called Link Protocol Control Information (LPCI), capable of carrying Application Service Data Units (ASDUs) as link layer user data. This layer uses various frame formats to provided the needed integrity, efficiency and convenience of transmission. The application layer consists of multiple

application functions, which are responsible for transmission of ASDUs from source and its destination. The user process layer, permits a number of basic application functions, defined in IEC 60870-5-5. [49]

For IEC 60870-5-104, the protocol structure is very similar, see Figure 2.11. Notice however that the protocol relies on the TCP/IP structure from the OSI layers 1 to 4 according to RFC 2200 without any needed alteration [50]. The standard defines the usage of a TCP/IP network, for instance a LAN connecting telecontrol equipment and transporting ASDUs according to IEC 60870-5-101.

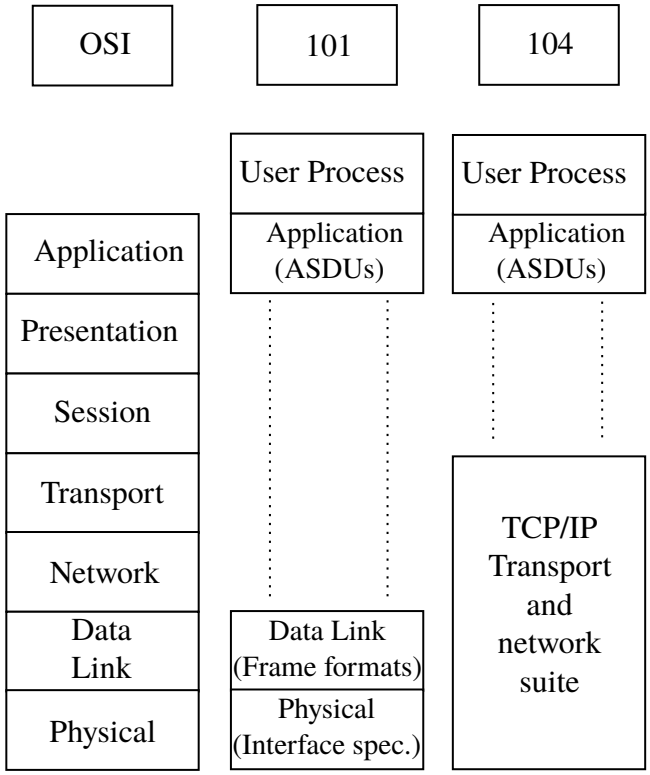


Figure 2.11: IEC 60870-5-101/104 and OSI model layers.

IEC 60870-5-101 defines two frame formats, a fixed length format used for control messages, where an Application Protocol Data Unit (APDU) only consisting of an Application Protocol Control Information (APCI) frame is sent. And a variable length frame, where the APDU includes not only the APCI, but a variable length ASDU, according to the control field for the message [51].

A variety of APDU frames are defined in IEC 60870-5-101, which can be used for some basic application functions such as [51]

- Initialization
- Polling data
- Periodic transfer
- Spontaneous event transfer
- General interrogation
- Time synchronization
- Control command
- Counters
- Parameters loading
- Test command
- File transfer
- Transfer delay measurements

In contrast to 5-101, the transport layer of 5-104 utilizes a stream-oriented interface (TCP/IP), thus not clearly defining start or stop of 5-104 ASDU transmission. Therefore, the standard mandates the usage of some delimiting elements, each APCI includes a start character, a length indication of the ASDU and control fields [50], see Figure 2.12. The standard mandates that only a complete APDU may be transferred.

The start octet, START 68H (hexadecimal value) defines the start point of the data stream. The following octet (length), defines the APDU body length, which encapsulates both the control field octets, and the APDU, this length is limited to 253 octets, since the maximal frame length is 255. The control fields defines control information to ensure protection against loss and duplication of message frames [50].

Although time synchronization is often performed using a specific ASDU defined in IEC 60870-5-101. For IEC 60870-5-104 using the TCP/IP suite, other synchronization protocols are often used, such as SNTP (Simple Network Time Protocol) or NTP (Network Time Protocol). When higher time synchronization is needed, GPS clocks using protocols IRIG-B (Inter-range Instrumentation Group timecode) or PTP (Precision Time Protocol) are used instead [51].

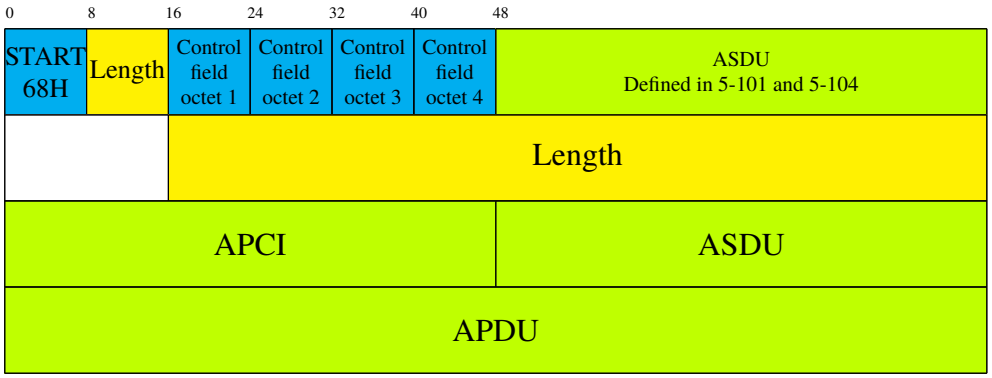


Figure 2.12: Example of an IEC 60870-5-104 APDU frame.

2.3.6.1 Typical area of usage

Being specifically developed for telecontrol applications of power utility services, the protocol is prominently used for such purposes. Being more popular in the European region, but likewise prominent in other regions also [22].

2.3.6.2 Security concerns

Due to the age of the protocols, some security concerns have risen over the years. For instance, the 5-101/104 protocols do not include any authentication of the sent data. Thus being vulnerable by unauthorized connections and/or data message altering from man in the middle attacks. Typically security measure against such attack uses authorized IP-address tables, along with separate private networks and firewalls at the remote stations [51].

A study conducted in 2022 with a hardware in the loop laboratory setup demonstrates some well known attacks and some newly found by the authors considering 5-104 [52]. The experiment showed that the 5-104 protocol can be attacked granted the attacker is informed about the protocol features, such as the master-slave topology model, the ASDU message sets and how protocol communication is configured. The attacks conducted where such as data gathering, operation failure and denial of service attacks. Where the authors found a new attack which resets the TCP connection, arising the possibility of spoofing the communication between master and slave [52].

Chapter 3

Method

This chapter presents the methodology and research process followed in this thesis project. With brief introductions and motivation on the process selection, mostly defined by the objectives stated in Section 1.4. The methodology is presented in four parts. First, the research process of the thesis project is presented in Section 3.1. Then the project environment, detailing the software and hardware utilized in the project is presented in Section 3.2. The evaluation framework, detailing the validation scope and test definitions to validate the project is presented in Section 3.3. Lastly, a presentation of the system documentation, presenting the documentation and notes over the project work is detailed in Section 3.4.

3.1 Research process

The research process followed in this thesis project is directly derived from the five project objectives as presented in Section 1.4. The five objectives are used to define four project (research) stages. A color coded overview of the research process is shown in Figure 3.1. Firstly, as marked in grey in the Figure, a analysis stage of the project is defined. This stage is directly linked to objective **O1**, where the mobile VMS applications are first researched, to identify commonly used and potential communication interfaces (protocols). This outcome is summarized to provide an overview of potential communication interfaces for the VMS. Next stage, marked in yellow in the Figure, research and analysis of the communication interfaces and applications is performed. This stage is directly linked to objective **O2**, further the two above presented stages together results in the detailed literature review as presented in Chapter 2. Next, following the literature review, research and implementation of a IEC

61850 communication stack on the VMS is performed in the green (see Figure 3.1) research stage. The project environment used, based on the identification in the research process, is further introduced in Section 3.2. Further, the IEC 61850 implementation is detailed in Chapter 4, detailing the IEC 61850 data model and modelling process performed in the project. This stage, along with the above mentioned chapters are directly related to objectives **O3** & **O4**. Finally, the final research stage, as shown in purple in the Figure, shows the validation and testing phase of the communication interface integration. This stage provides the novel real-life implementation framework and analysis to validate the use of the proposed interface (IEC 61850) compared to other solutions. This framework is further introduced in Section 3.3. Where the results are presented in Chapter 5, following with a discussion in Chapter 6.

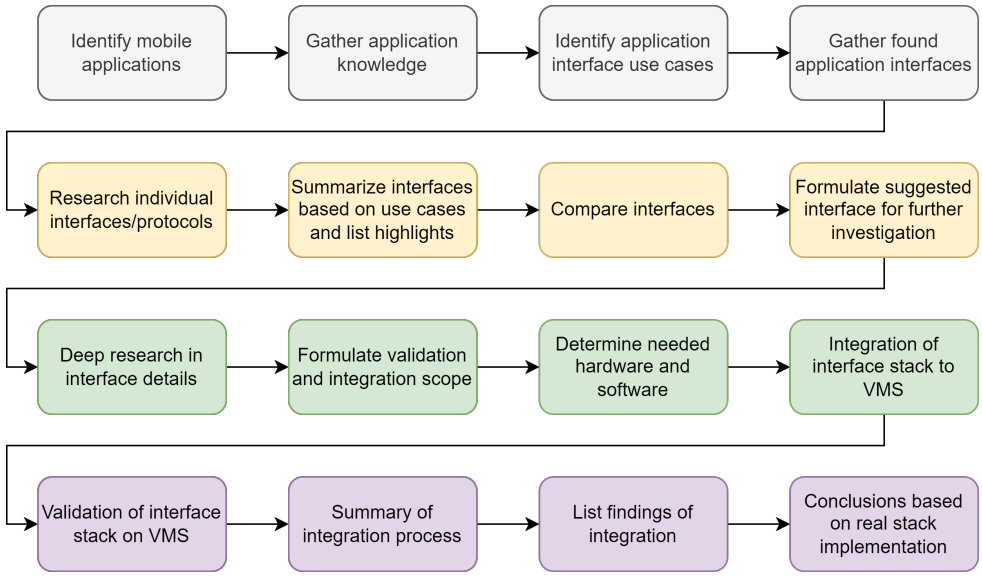


Figure 3.1: Diagram of the research process followed.

3.2 Project environment

This section presents the project environment utilized in this thesis project. The details explained here allows for result reproduction, expansion and future work on the project deliverables. The section details are direct results from the research and modelling process which defines the environment needed according to the evaluation framework specified.

Two parts are described, first the software tools and programs used in the

project work and validation are presented in Section 3.2.1. Then, the hardware used in the project work is presented in Section 3.2.2.

3.2.1 Software used

The basis for the chosen software utilized is firstly based on the need derived from the research process, i.e. what is needed to achieve the goals. Further, since an IEC 61850 interface is to be integrated, compliant and commonly used software within the standard's user base is to be chosen. To give a better neutral perspective on the integration a *vendor independent* IEC 61850 software tool is preferred, since it provides, by definition, a vendor unbiased framework for the integration and use of IEC 61850. Therefore the hardware choice can be done independently of any software vendor limitation.

On this basis, the IEC 61850 data model, and thus main integration scope was done in *Helinks STS System Integrator* tool. STS System Integrator is a vendor independent IEC 61850 multi-functional engineering tool [53]. The software provides tools ranging from data modelling, to system configuration and system specification. The software is mainly used (in this project) for the data model creation (IED Capability Description (ICD) file) and IED configuration (Configured IED Description (CID) file).

For the validation stage in the research process, an IEC 61850 compatible client is needed. Effectively, the client needs to emulate the behavior of an IEC 61850 client within a station environment (IED) or as a control center Human-Machine Interface (HMI). Based on the previous reasoning, its deemed suitable to choose a vendor independent solution for this application as well. To provide an unbiased evaluation of the integration and use scope of the project work. For this, the IEC 61850 client utilized is *IEDScout* by OMICRON [54]. The software tool provides full IEC 61850 client functionality, for both MMS and GOOSE services.

3.2.2 Hardware used

Trivially, since the project objective aims to analyze a real IEC 61850 stack implementation, a fully operational VMS is used. As introduced in Section 2.1.1, the mobile BESS is made of modular blocks. As per the evaluation framework, see Section 3.3, and the modelling scope, see Section 4.1, only two modular blocks are utilized. Namely a Volthub Grid and a Voltpack Mobile, i.e. the PCS block and one battery pack respectively [1].

Further, as presented in Chapter 4, a protocol gateway is used to integrate

the IEC 61850 standard within the VMS. The gateway needs are listed in Section 4.5. Based on those needs, and the modelling process a protocol gateway from Moxa is selected. Namely, MGate 5119-T [55], which is capable of multiple protocol conversions (Modbus, DNP3, and 101/104), and provides the needed IED server capabilities and MMS communication services.

3.3 Evaluation framework

The evaluation framework is designed to answer the research questions posed in Section 1.2.1, as well as the valuation objectives stated in Section 1.4. Furthermore, the framework design follows the process flow as introduced in Section 3.1, see the purple stage in Figure 3.1.

Related to the first research question, namely which communication interface is most suitable for mobile applications, the evaluation is performed from the literature review results. Based on the literature study, investigating several applications and interfaces, suitability of each interface across the applications is done through discussions. Notably, a comparison summary is presented in Section 5.1, further discussed under Chapters 5 & 6.

For the second research question, namely the identified usability and expansion need of the IEC 61850 for the scope of mobile BESS, a real system implementation is carried out. The evaluation is set to construct a basic data model and testing environment to document the integration process, along with any noted shortcomings or needs not covered in the IEC 61850 standard. The testing environment is the divided into two communication methods, *vertical* and *horizontal* communications, reflecting typical capabilities in IEC 61850 systems. Further details on the *vertical* communication framework is presented in Section 3.3.1. *Horizontal* communication evaluation framework is presented in Section 3.3.2.

The evaluation is performed and presented in the results, see Chapter 5. The results are then further discussed in Chapter 6.

3.3.1 Vertical communication

As an evaluation of the typical *vertical* communication performed within substation (Station HMI to IED) or from control center to a remote unit, a test case to verify the communication compatibility of the IED model and the integration work is set to be performed. The *vertical* part considers communications from an IED to the station HMI or control centers, as in the temporary utility grid support application in Section 2.4. Nevertheless, such

communication architecture can also be considered for the other applications, where client-server communication is seen as *vertical*.

This evaluation requires a MMS IEC 61850 client used for communication to the VMS IEC 61850 DER-IED. The evaluation is performed by controlling the VMS on a client-server architecture and show the functionality that an IEC 61850 interface offers compared to other interfaces. This is done by utilizing the specific functionalities offered, such as the configurable report control blocks on the IED and the standardized operating command. Examples of operating commands that reflect this evaluation are

- **Start**: The DER is expected to initialize the start sequence and go to an available to connect state, i.e. the DER shall go to a state where it's ready to connect to the grid and execute on the received setpoint. In this evaluation, the VMS DER is configured to always allow connection (`AuthConn=true`), thus the expected state change is going from state *on but disconnected and not ready* to state *disconnected and authorized*.

- **Connect**: The DER is expected to initialize the connection sequence, by synchronizing itself to the grid connection. Thus the expected state change is going from state *disconnected and authorized* to *synchronizing* and finally (if successful synchronization) to *running* state.

- **WSpt** & **VArSpt**: When the DER is in the *running* state, power setpoint are issued to the storage LN, i.e. **DSTO**, to control the active and reactive power exchanged to the grid connection. These commands represents the typical operating commands issued by a power management system. Although IEC 61850 supports more detailed operating functions, as discussed in Chapter 6, basic operation can be sufficiently achieved by operating directly on the setpoint rather than through a function. The DER is expected to follow these setpoints when running.

- **Disconnect**: The DER is expected to disconnect from the grid. This command is issued when in operating state *running*. Thus it's expected that the state goes from *running* to *disconnected and authorized*.

- **Stop**: The DER is expected to stop the current operation and enter the *stopping* state, after stopping the DER shall go to *on but disconnected and not ready* state. This command may be issued in three states, namely *disconnected and available*, *disconnected and authorized* and *running*.

Further, the developed system is expected to follow the above commands, as well as provide the configured reports as created in Chapter 4. The results of this evaluation are presented in Section 5.2.1.

3.3.2 Horizontal communication

In contrast to the *vertical* communication resembling client-server communication, *horizontal* communication is deemed as publisher-subscriber broadcast communication. Within IEC 61850 systems, typically *horizontal* communication reflects the communication capability IEDs to IEDs, commonly achieved by using the GOOSE protocol on station bus level. This evaluation thus reflects the VMS IEC 661850 DER-IED capability of utilizing the GOOSE protocol.

Use cases for the GOOSE protocol based on the investigated applications are; rapid and reliably protection operations, and coordination through decentralized control. For protection applications, subscribing to GOOSE messages allows faster control on events, such as performing a DER command based on a protection function, such application could be lowering the power output upon a over-current start event. Furthermore, as presented by Albunashe et al. [21], a decentralized DER control scheme using GOOSE protocol for DER coordination is investigated. The results show clear advantages of faster command issuing using the GOOSE for advanced coordination strategies.

The evaluation shall then consider the implemented IEC 61850 IED capability of managing publisher and subscriber capabilities of the GOOSE protocol.

3.4 System documentation

The work documentation of this thesis project consists mainly of the thesis report, i.e. this document. Which contains the work details, motivations, results and evaluations of the project. However, the main work outcome, such as the ICD and CID files are too vast to include as a relevant appendices (XML files of several thousands of lines). Thus, the specific work files and details (mappings, configurations) relevant to the hosting company Northvolt are delivered separately in a documented folder. This folder contains the needed files to use the system as detailed in the thesis, such as the gateway configurations and System Configuration description Language (SCL) files created.

Chapter 4

IEC 61850 BESS data model

This chapter introduces, presents and motivate the modelling approach and data model implemented for validation of the VMS BESS. Specifically, the chapter aims to provide a simplified, yet IEC 61850 compliant modeling approach to show how the standard may be applicable to mobile BESS. First, the modelling scope is presented in Section 4.1. Following, the modelling process is introduced in Section 4.2, introducing the steps needed for data modelling. Then, the outcome from the modelling research process, i.e. the requirements as seen from the standard are introduced in Section 4.3. Following, the initial modelling process, abstracting the physical system and device is presented in Section 4.4. Finally, the data model is finalized with the IEC 61850 LNs and DOs utilized and presented in Section 4.5.

4.1 Modelling scope

The modelling scope of the project is deducted from the evaluation framework as presented in Section 3.3. Thus, the main scope is to evaluate the applicability of the IEC 61850 standard to a mobile BESS, to understand opportunities in the standardized framework, along with challenges and learning's from the integration process. Thus the model case is chosen to a basic frame, comprising of a general BESS usage and topology as introduced in Section 2.1 and 2.1.1. To achieve this, the physical system has to be determined. The setup is chosen as a complete VMS comprising of one PCS block, and one battery pack, allowing for a minimal yet fully operational system. Since the VMS can operate in many different modes and configurations, the model was chosen to utilize the grid connected mode *Grid Boost* as its basis of operation. Therefore, the final scope of the data

model, thus the outcome of the modelling and integration of IEC 61850 is to; describe the capabilities of the VMS in the scope of IEC 61850, namely part 7-420 describing DER systems such as BESS. Identifying what is mandatory and applicable from the standard point of view. Along with the existing control frame of the VMS to not derate any functionality. The model and implementation is therefore to be seen as an extension of the system.

4.2 Modelling process

This section presents the modelling process followed in this thesis. The process presented is applicable for a retrofit style IEC 61850 integration, i.e. that the functioning physical device, in this case the BESS DER, is already designed and functioning. Thus the model is meant to represent the current system and its components, with condition that further customization on the system based on modelling insights should be minimized. For future product development, the process may still be followed, but if applied earlier in the product development stage, modelling requirements and functionalities from the standard may be can be integrated in the product nature.

A visualization of the modelling process is shown in Figure 4.1, where each process block is explained here.

Initially, regardless of the interface scope (be it IEC 61850, DNP3 or 101/104 etc.), it is of utmost importance to understand the system or device that is to be modeled, in this case the VMS, both from the vendor perspective, i.e. the internal systems, components and interactions between them. But also to understand the usability from a user perspective, thus what is interacted with and shown outside of the system scope. Examples of such research and understanding are presented in Section 4.4, where the physical system (VMS) is abstracted to virtual and abstract devices. In parallel to this research, basic understanding of the interface to be modeled has to be met. In this case, the IEC 61850 standard with a DER scope. This research is needed to gather which parts are mandatory for the modelling, and to find any likeliness or differences from the actual system. A summary of the standards found at this stage is presented in Section 4.2.2. While a summary of their requirements on the modelling stage is explained in Section 4.3.

Following the initial research, a decomposition of the physical system has to be made. The intent is to identify and list the subsystems and components of the physical system, in such a way as to be described according to the chosen interface. The level of decomposition is determined by the stages before, since they together form an interface overview of what is needed to be decomposed.

This stage is conducted in Section 4.4.

After the decomposition, an overview of the existing data available from the physical system must be mapped. As the scope of this process is retrofit-based, it is important to note what data are available to be read and what could be altered through write commands.

With the data availability understood, and a system decomposition with function descriptions, the integral data modelling parts can commence. This means formulating the LNs which represents the system decomposition and functionalities of the physical system. Having identified the LNs, their respective DOs must be chosen. Following the standard requirements, the mandatory DOs must be present. This requirement directly identifies if any data is missing from the physical system, such as mandatory data formats. Examples are enumeration types, where the physical system may use one enum type not compatible to the mandatory requirement. This stage is further introduced in Section 4.5.

Formulating the basis of the data model above, a crucial part of the IED model is the network topology and capabilities of the system. Besides the data model, the interface stack of the IED intended to be interfaced has to be chosen. This stage requires thought regarding the IEC 61850 communication protocol that can be used, such as MMS, GOOSE or SV. Further, the interface stack can be evaluated between the options available for the retrofit, such as native stacks, if the system controller can support such functions. Or, if a protocol converter gateway can be used to interface the IEC 61850 protocols to the physical system. These choices affect parts of the data model, such as any eventual proxy indication, communication capabilities (protocol), maximum client connections, reports configurable, datasets available etc. Nonetheless, the LNs and DOs defined before are valid regardless of this configuration. This stage and choice motivation is presented in Section 4.5.

With the above stages determined, the formal data model can be build. This means that the abstracted model and definitions identified have to be formulated in the SCL file used for describing IED capabilities. Namely the ICD file. This serves as a template for the engineering process of IEC 61850 configurations, and is seen as the formal description of the IED, thus the modelled system. This file is constructed by each manufacturer and provided to the users and customers when the component or system is integrated. This file is created by a vendor independent tool as described in Section 4.5.

Finally, although the modelling part is *formally* performed, it's of utmost importance to validate the usability and validity of the model. Thus the ICD file created can be used in an IEC 61850 engineering tool for

configuration. Examples are network information configurations, reports and datasets configured etc. This configured version, i.e the CID file, is then imported to the IED to validate the model and communications. Which can be accomplished by, for instance using a compliant IEC 61850 client, connecting to the IED and accessing the features as described by the model. See the results presented in Chapter 5.

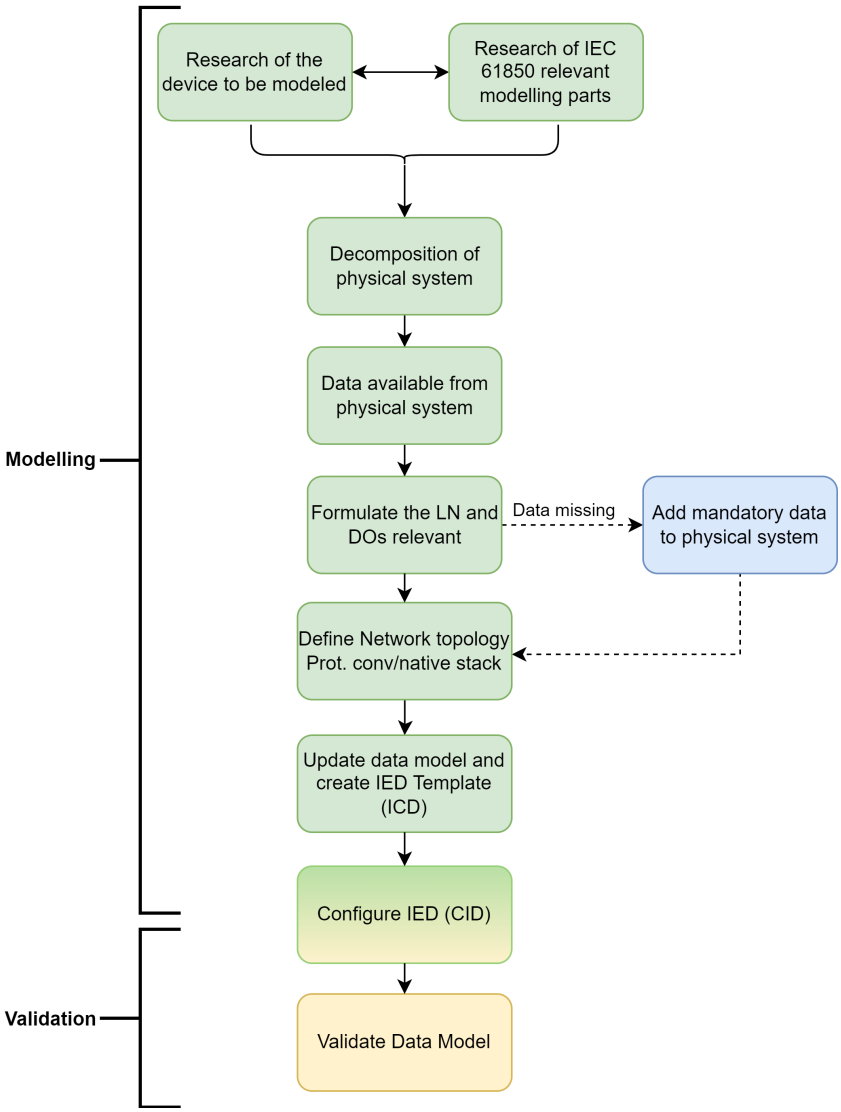


Figure 4.1: Diagram of the modelling process for an IEC 61850 data model.

Further, some examples of data modelling are investigated and studied to grasp the modelling processes and approaches used for a variety of applications, see Section 4.2.1. Following such examples, and as a result of

the IEC 61850 study, a summary of the core modelling parts is presented in Section 4.2.2.

4.2.1 Examples of data modelling

Along with the modelling research process, it's of importance to investigate examples and use cases of data modelling. To understand and identify the common traits and practice of modelling. Therefore, a set of examples of DER modelling and use cases of IEC 61850, specifically part 7-420 are introduced here.

Two examples of modelling approaches are presented. Firstly a IEC 61850 based communication system for a functional architecture and operational management of backup generators is shown in [56]. The authors present an IEC 61850 based communication system for DER management through the modelling according to parts 7-4 and 7-420. Core parts of the article show the process of obtaining the data from the non-IEC 61850 controllers and devices, along with mapping to IEC 61850 as well as to the MMS protocol utilized for IEC 61850 communication in the system. Notably the system shows integration of Modbus based communications through a data feeder also acting as an IED MMS server.

Next, concrete modelling examples of a photo-voltaic DER application modelling is presented in [57]. Where the core IEC 61850 logical node parts 7-4 and 7-420 where used to model the plant topology and functionalities needed for operational management. The data model was developed at a gateway level, such that the system could ensure interoperability of communication between DER to DER, DER to utility operator (DSO or TSO) or DER to energy provider. Concluding that the standardized data modelling methods, i.e. using existing LNs yields simplified integration effort, specifically when adding new DER equipment.

4.2.2 Core modelling standards

Amongst the many parts of the IEC 61850 standard series, the following parts are further studied to conformally produce the data model applicable to IEC 61850, namely

- **IEC 61850-6**. This part describes the SCL used within the IEC 61850 standard. Which is a description language for communication in power utility automation systems, defining the formalities of the various SCL XML files [58].

- **IEC 61850-7-1**. This part briefly introduces the modelling methods, communication principles and information models used in the standards. Providing an overview on the following standards of part 7-X [59].
- **IEC 61850-7-2**. This part introduces the concepts of the Abstract Communication Service Interface (ACSI) as used within the IEC 61850 standards [60].
- **IEC 61850-7-3**. This part introduces and explains the CDCs referred to and used by the LNs as defined in part 7-4, and 7-4XX [61].
- **IEC 61850-7-4**. This parts specifies information models of general devices and functions typically utilized in power system utility automation. Such as information models for substation application, defining the LNs and their DOs needed for communication between IEDs [33].
- **IEC 61850-7-420**. This part specifies the information models for description of DERs and their communication to Distribution Automation (DA) systems. The DER definition includes information models for systems such as distribution-connected generation systems, energy storage systems, and controllable loads, as well as facility DER management systems and other, defining the needed LNs and their DOs needed for communication between the IEDs of the DA system [16].

The above mentioned parts of the IEC 61850 standards provide the definitions and examples needed to understand and correctly define a data model. As well as the requirements and modelling processes deemed necessary as seen by the standard.

4.3 Requirements from Standards

Studying the identified parts of IEC 61850 regarding the data modelling, as stated in Section 4.2.2. A summary of some general requirements, for a compliant data model are summarized in this section. Notably, part IEC 61850-3, which introduces general requirements for IEDs is not considered at this stage. Since part 3 mainly regards construction, design and environmental requirements for communication and automation of IEDs and other systems as plants or substations [62].

Regarding the data model, IEC 61850-7-1 presents examples and general requirements for the modelling procedure, to formulate a correct data model. Specifically the concepts regarding LDs. Although a single physical device, i.e. the IED may contain multiple LDs depending on their respective function. These LDs must contain, at minimum a certain set of LNs. Namely, each LD *must* contain a *logical node zero* **LLN0**. The LN represents the common data of its LD, such as the control mode of the device, thus also representing the control mode of *all* LNs in the same LD [59]. Secondly, atleast one LD, the root device must contain the *physical device* node **LPHD**. This LN represents the data of the physical device hosting the LN, such as model numbers, vendor and location information etc. [59].

Other important requirements are the definitions within the used LNs depending on the physical structure of the system and IED. In the case of a protocol gateway. Where the IEC 61850 gateway definition states that; *Gateways are network interconnection devices that translate protocols to other protocols. For example, gateways may convert non IEC 61850 data into IEC 61850 data.* [59]. If the IED physical structure utilizes a gateway as a proxy for the IEC 61850 communication, it has to be stated in the data model. Thus the proxy status value must indicate such a topology, i.e. `LPHD.Proxy.stVal = "true"` must be stated in the root physical device LN **LPHD** [59].

Further, it's important following the decomposition stage of the modelling, thus when the abstract functions are formulated and the equivalent 61850 LNs found, to utilize the LNs defined in the standard namespaces (such as IEC 61850-7-4) if applicable and deemed fit. When utilizing such LNs, care must be given to follow the *mandatory* (M) DOs that must be present in the LN. If *optional* (O) DOs are useful in the modelling, they can be included in the model granted they follow the namespace [59].

Then, regarding the DER modelling part of the standard, considering IEC 61850-7-420, two mandatory requirements are identified. Along with two optional requirements for further modelling. Namely [16]

- **Mandatorily**, at least one resource inherited from the abstract class *DEResourceLN* has to be present in the data model. Examples of such childrens are instances of the LNs; **DGEN** representing generating capabilities of the DER, **DSTO** representing the storage capabilities of the DER or **DLOD**, representing the load capabilities of the DER.

- **Mandatorily**, at least one Electrical Connection Point (ECP) has to be present in the data model. Examples of ECP LNs are either, **DPCC**

representing the PCC of the DER; general ECP type **DECP** or a virtual connection point **DVER**.

- **Optionally**, operational functions derived from the abstract class *OperationalFunctionLN*. Examples of children's of such class are; **DBAT** representing the operational function and status of a battery within the DER or **DINV** representing the operational functions and statuses of an inverter system within the DER.
- **Optionally**, a single power management function **DPMC**.

4.4 Abstraction of the physical model

Formulating the IEC 61850 data model means creating a virtual model of the device or system that is to be represented by the IED. Following the introduction of the VMS in Section 2.1.1, a simplification and abstraction is presented in this section, along with the assumptions done to fit the model. Any discrepancies or abnormalities in the modeling approach are discussed in Chapter 6. The modeling procedure follows examples given in IEC 61850-7-420 regarding BESS models [16]. Along with other modeling examples, such as Photo-voltaic stations modeled in IEC 61850 as shown in [57].

4.4.1 Abstracted model

Considering the simplified scope of the modeling. The VMS is chosen to be modeled as a *typical* grid connected BESS, thus being able to inject and or consume power from the grid connection, i.e. PCC as per specified to by the operator of the system. This functionality fits well within the operating functions of the VMS with the operating mode *Grid Boost*. The specific applications where such as function is relevant are all the introduced BESS applications in Chapter 2. Although specific thought is made to the application *Temporary utility grid support* which suits well with such functionality, see Chapter 2.2.3.

Therefore, the other VMS functions and physical devices as breakers or connections are not considered in the model, given that they are not used in the scope of *Grid Boost*. The simplification therefore gives an easy Single Line Diagram (SLD) of the BESS topology as shown in Figure 4.2. Starting from the left, the important battery device, which represents the storage capability and technology of the BESS DER. The battery is then DC coupled through

a bus to a PCS, representing inverter capabilities of the DER. The PCS is galvanically isolated from the power system through a transformer, which is considered as a part of the PCS, thus the color coding. A circuit breaker, capable of load breaking capability is placed between the PCS connection and the power system PCC.

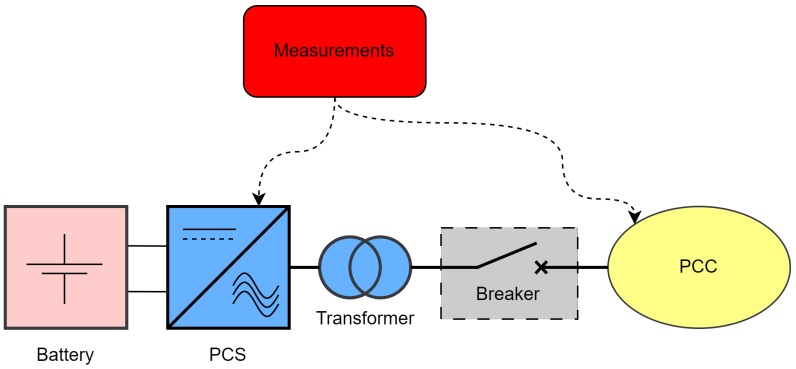


Figure 4.2: Simplified BESS topology color coded for modeling.

After introducing the BESS abstracted model in Figure 4.2, the representative LNs representing the model by virtue of the IEC 61850 standards part 7-4 (for the general nodes) [33] as well as part 7-420 (for the DER specific nodes) [16] are identified by the standards definitions. First by utilizing part 7-4 for the general functions, it is straightforward to model according to the nodes available. As per part 7-4, the LNs used are; **XCBR** representing the breaker capabilities of the device, along with status information, such as the breaker position. **MMXU** representing the three-phase measurement capability that the DER can represent at both the PCC and the PCS (virtue of the lossless SLD). Considering the DER as a single LD, the device characteristics, such as vendor name, model number, locations etc. can be modeled by the *mandatory* LNs **LLN0**, which could hold eventual datasets and reports available to clients and nameplate descriptions, and **LPHD**, which represents the physical information of the device (nameplate information).

Then, to model the DER functionalities and devices, IEC 61850 part 7-420 LNs are chosen as follows; **DSTO** represents the DER storage capability, such as nameplate power and energy capacity ratings, operational state and commands for state control, active and reactive power control etc. Thus effectively representing the DER capability. Since the BESS is, as seen from the power system, able to act as both a load or generator, i.e. consume or inject active and reactive power individually, these capabilities are described respectively in the LNs **DLOD** and **DGEN**. Describing the

energy storage capability is done through the LN **DBAT**, presenting both DC measurements representing the battery, but also nameplate ratings of charge/discharge capability, battery technology kind etc. As per part 7-420, the storage DER is hierarchically represented by **DSTO**, which in turn references its capabilities, such as load (**DLOD**), generation (**DGEN**) and storage technology (**DBAT**). Next, describing the PCS of the BESS, the LN **DINV** represents the inverter-based PCS along with nameplate ratings, isolation details and eventual alarms, such as DC-link loss or AC loss (loss of mains). This LN encapsulates the isolating transformer as a mean of galvanic isolation of the PCS. Finally, the BESS connection point, i.e. the PCC is represented by the **DPCC** LN. Which presents information regarding the connection point, such as measurements references (**MMXU**), equipment references (**XCBR**), phase connection properties, grounding properties (such as grounding configurations, TT, TN-C etc.).

The model is shown with the chosen LNs and their defining IEC 61850 part in **bold**, see Figure 4.3. Further, the model is introduced in detail, with the used DOs of each LN in Section 4.5.

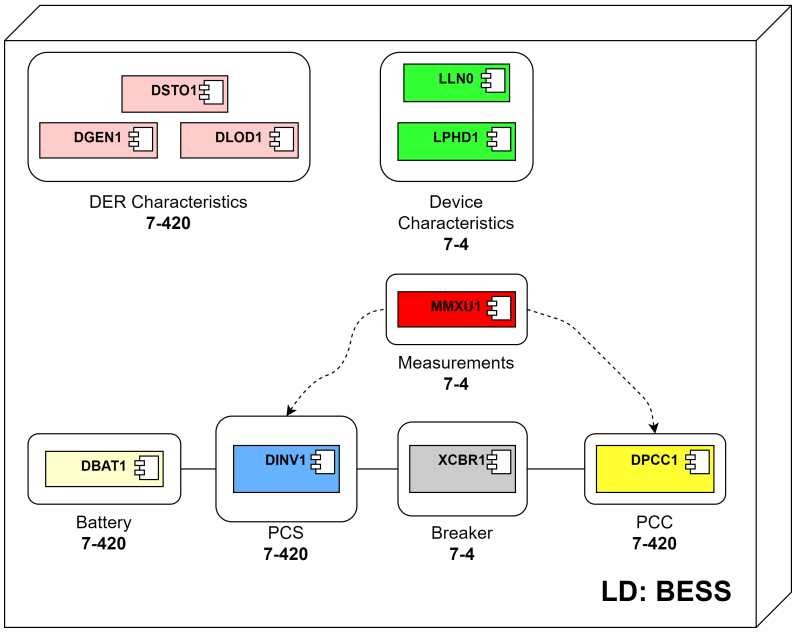


Figure 4.3: IEC 61850 simplified BESS topology. Showing the LNs used along with their respective part in IEC 61850.

4.5 Building the data model

Following the modelling process introduced in Section 4.2, along with the scope definition in Section 4.1. A data model is formulated in completion in this section. The model utilizes the results from the identified requirements in Section 4.3, along with the abstracted model presented in Section 4.4.

As per the modelling process, following the physical device abstraction, the communication topology of the integration has to be set. The scope of the model is to validate the communication interface as per the standard definition, done in such a way to not influence the design choices of the physical system, hence a retro-fit approach. Therefore, it's suitable to utilize the already existing communication interface of the VMS, in this case a proprietary Modbus TCP interface. Exposing an IEC 61850 interface can then be done by using a protocol gateway. Which is responsible of the IED server services, along with the *external* communication interfaces. *Internally*, the gateway communicates to the VMS through the proprietary interface. Such communication topology is shown in Figure 4.4. Notably, some benefits of such topology are

+ Separate communication interfaces exposed to clients or integrators. The proprietary mapping is handled by the vendor integration, while the standardized interface is exposed to the external (IEC 61850) network.

+ Additional layers of communication security, if the *external* network is compromised, the *internal* network and operation can be kept running separately and autonomously. A compromised gateway could be ignored from the physical BESS device, by means of software or physical keys/switches (local control).

+ Hardware requirements on the communication devices is set as a gateway requirement. For instance, compliance to IEC 61850-3 is requested to the gateway device, thus the retrofit physical system (the VMS mobile BESS) does not require such efforts.

+ Distributed logic for IED server needs. Being two separate devices, the gateway and the BESS logic controller, any issues on the BESS side or gateway side can be identified by the IEC 61850 network. If the *internal* communication is lost, quality bits flag for such discrepancies on the affected DOs or the behavior of the LD.

However, some drawbacks of such topology must be considered. Comparing to a native stack integration, where the interface would reside on the physical device (logic controller) itself. Following drawbacks are identified

– Additional communication layers and conversion inherently adds delay in the entire communication stack. Since a gateway must request data from its represented device, the messaging between adds a communication delay and asynchronous behavior between the interfaces.

– Distributed control units results in more update and service time on the vendor perspective. Changes or additions on the physical system (VMS) have to be reflected in the gateway exposing the device. Since they do not share a common deployment platform, vendor integration has to ensure comparability between two physical devices.

– Protocol limitations are determined by the gateway chosen.

With such benefits and drawbacks identified, the protocol gateway for this integration is chosen as the Moxa MGate 5119-T [55], which is capable to run as an IED server, with MMS protocol communication on the IEC 61850 network side. Communication as a Modbus TCP client on the internal VMS network side.

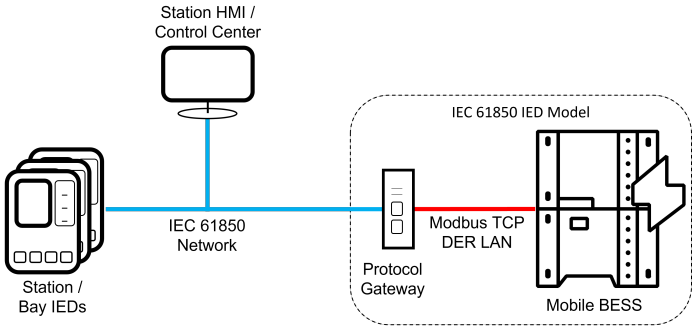


Figure 4.4: BESS communication topology modeled.

With the communication topology, the modelling work is performed in the vendor independent IEC 61850 engineering tool Helinks STS System Integrator [53]. Where the LD structure and LNs chosen were as per the abstracted model in Section 4.4. Following part 7-420 of the IEC 61850 standard [16], along with the VMS topology, it's convenient to *group* the eventual logical nodes needed under one abstract LD.

Further, the DOs of each chosen LN where chosen on two bases. Namely

- Mandatory DOs of the chosen LN must be present as per the IEC 61850 standard.

- Optional DO of the chosen LN which are present in the existing physical system (VMS) are adapted.

With this basis, a UML diagram of the complete VMS data model is shown in Figure 4.5. The diagram depicts the chosen LNs inside the LD. Along with the chosen DOs and their respective CDC. As per IEC 61850-7-420, references to the DER parts are shown as tags between the LNs used. The mandatory DOs as per parts 7-4 and 7-420 are marked in **bold**.

Notably, some of the integration processes are further described in the following sections. Adaptation of the datatypes defined by IEC 61850 where modified according to the allowance of the standard, examples of such procedures is presented in Section 4.5.1. Some DOs were directly determined by the requirements as identified in Section 4.3, such as the proxy indication, i.e. `BESS/LPHD1.Proxy` of type **SPS** (single point status), set to `stVal = true`.

IEC 61850 specifies five control models used for commands and controls of IEDs. The control model available are

- **Status only**

– *Normal security*

  - **Direct control with normal security**
  - **SBO control with normal security**

– *Enhanced security*

  - **Direct control with enhanced security**
  - **SBO control with enhanced security**

Status only disables any client control of the object, but allows reading of the status or measurement value (`stVal` or `mxVal` respectively). Two security levels exits, *normal* or *enhanced security*. The difference is the feedback send after any operate command. Where the *enhanced security* initiates a feedback message after the operate command.

Further, two operate conditions are possible. **Direct control**, where the operate command is issued by the client whenever, or **SBO** (Select Before Operate), where a select command is issued firstly, indicating to any eventual clients who also access the object, that an operation selection is present, thus blocking any contradicting or subsequent commands from other clients. This command is typically used for more crucial objects such as breakers

or disconnecting switch operations. Since the internal breaker **XCBR1** is exclusively operated by the DER state machine (VMS control logic, mapped to `DEROpSt.stVal` for **DSTO1**, **DGEN1** and **DLOD1**), no object of typical SBO type is present. Thus the control mode implemented for all commands and controls in the data model are of type **Direct control with normal security**. Identification of such commands in the UML diagram in Figure 4.5, can be done by the CDC class specified, such as **ENC** (Enum type control), **SPC** (Single Point Control), **DPC** (Double Point Control) or **APC** (Analog Point Control). Where the latter is used for setpoint control of the DER. Such as in **DSTO1** where `WSpt` and `VArSpt` represents the active and reactive power setpoints of the storage DER respectively. Notice how these DOs are present in the referenced DER characteristics **DGEN1** & **DLOD1**. Although these reflect the same feedback setpoint value, i.e. `WSpt.mxVal.f` and `VArSpt.mxVal.f`, the control model is set to **Status only**, since the setpoints shall be issued to the hierarchical storage LN **DSTO1**.

The datamodel implemented presents useful predefined report control blocks and datasets. This functions enables the vendor or manufacturer to distribute predefined reports and datasets as per the system design and typical usability. Although these comes as predefined, they are freely altered or removed by clients, depending on their application and need. As per the IEC 61850 standard and common practice, the datasets and report control blocks are located below the logical node zero of the LD (**BESS**). A total of 5 datasets and report control blocks are constructed, an example of the configuration and motivation is presented in Section 4.5.2, detailing the configured reports.

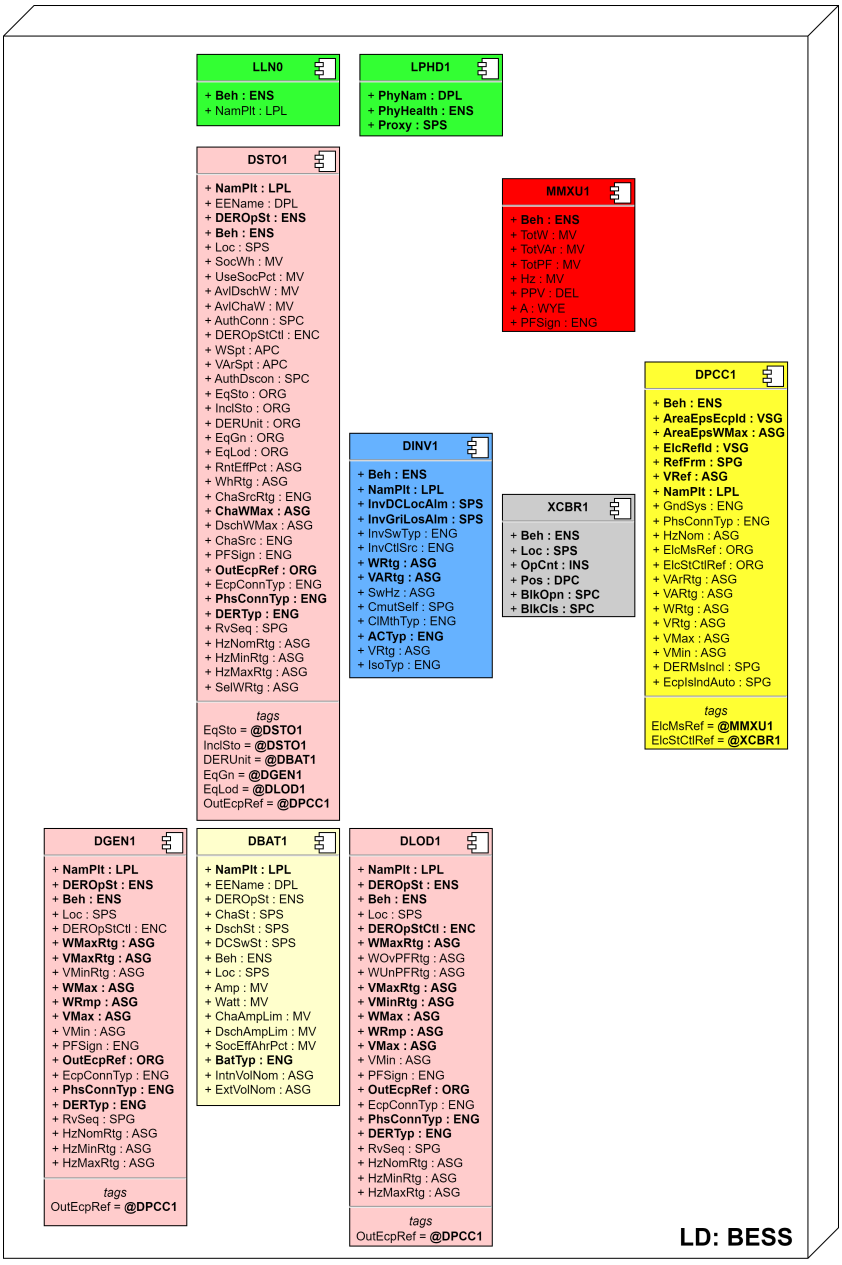


Figure 4.5: UML diagram of the mobile BESS data model. Showing the LNs, DOs & DAs used and eventual tags referring between the LNs. Mandatory DOs are marked in **bold**.

4.5.1 Datatypes

To represent the datamodel according to the data available of the physical device. The datatypes, as defined in the standards IEC 61850-7-4 and IEC 61850-7-420 have to be modified according to the modelling needs. The modification is done considering the semantics of the CDCs as described by the standards. Each LN consists of a set of DOs, who are themselves children's of the generic CDCs. These CDCs are defined in IEC 61850-7-3, where the DAs within each CDC has a flag describing if the data is considered as mandatory or optional by the standard. To model the mobile BESS, the specified DOs within the chosen LNs of the model were modified according to the relevant data to be given, and the capability of the physical device, i.e. the VMS.

An example is the measurement LN **MMXU**, which represents three-phase measurements. Since the physical device only presents the RMS (Root Mean Square) value of both current and voltage, the limitation must be clearly defined in the datamodel. Since the standard allows for current and voltage measurements of both magnitude (thus RMS) and phase angle. Consider the **MMXU** DO representing the phase-phase voltage measurements, i.e. **PPV**. The CDC of the DO is of type *DEL* (delta measurements). Encapsulated in the DO, each phase-phase voltage is given as a structured data, including (among others) the current value (cVal), which mandatorily must give a magnitude (mag) and optionally give an angle (ang), along with a quality indication of the measurement (q), a timestamp of the measurements (t). Units of the measurement, expressed as both the SI-unit (SIUnit), and eventual prefix (multiplier), along with a description of the angular reference (angref). As seen in Figure 4.6, the removed DAs of the datatype are stricken through. Showing only the modeled parts needed to describe the *magnitudial* measurement capability of the phase-phase voltages.

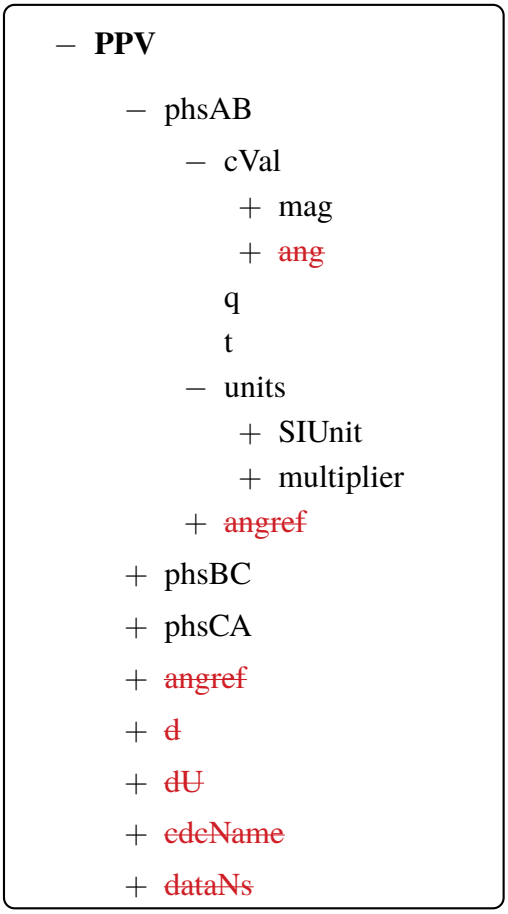


Figure 4.6: Modification of the DO **PPV** to show only RMS values (magnitude) of the phase-phase voltage.

4.5.2 Configured reports

Amongst many other benefits of the IEC 61850 standard, one of the main benefits and specialties are the configurable report control blocks. Where a user at configuration level, or a client at deployment stage can configure a report set to the IED (server). The reports may be through MMS and or GOOSE depending on the client/server capability and application use case. The reports can then be classified in two ways, buffered and unbuffered ones. Where the buffered reports are kept in a buffer in case of communication loss between the client and server, often utilized for digital signals, such as breakers or switch positions. Unbuffered reports are then often used for reports of more monitoring purposes, such as analog values.

Each report must refer to a dataset, which comprises of functionally constrained DAs (FCDA) or DOs (FCDOs). Theses constrains indicate the type of data constraint, such as measurements (MX), statuses (ST) or others.

An example of two implemented datasets are shown in the listing 4.1. Which shows a dataset for the measurements at the PCC, named *PCC_Measurements*. Which consists of five FCDA. All functionally constrained to include only measurements (MX). The five FCDA are, total active power (TotW), total reactive power (TotVAr), frequency (Hz), phase-phase voltages (PPV) and currents (A). Being functionally constrained by *MX*, means that values such as `cVal.mag.f` (magnitude expressed as a float), `q` (quality flag) and `t` (timestamp) are part of the dataset. The other dataset shown is for the breaker status, named *Breaker_Status*. The dataset consists of a single FCDA referring to the breaker position, i.e. `XCBR.Pos`, functionally constrained by statues (ST), i.e. the data values such as `stVal` (status value), `q` (quality flag) and `t` (timestamp).

Listing 4.1: Snippet of the configured datasets available from the IED.

```
<DataSet desc="Preconfigured Dataset" name="PCC_Measurements"
    >
     <FCDA doName="TotW" fc="MX" ldInst="BESS" lnClass="MMXU"
        lnInst="1" prefix=""/>
     <FCDA doName="TotVAr" fc="MX" ldInst="BESS" lnClass="MMXU
        " lnInst="1" prefix=""/>
     <FCDA doName="Hz" fc="MX" ldInst="BESS" lnClass="MMXU"
        lnInst="1" prefix=""/>
     <FCDA doName="PPV" fc="MX" ldInst="BESS" lnClass="MMXU"
        lnInst="1" prefix=""/>
     <FCDA doName="A" fc="MX" ldInst="BESS" lnClass="MMXU"
        lnInst="1" prefix=""/>
</DataSet>
<DataSet desc="Preconfigured Dataset" name="Breaker_Status">
      <FCDA doName="Pos" fc="ST" ldInst="BESS" lnClass="XCBR"
          lnInst="1" prefix=""/>
</DataSet>
```

Further, an example of two report control blocks (RCBs), using MMS communications and referring to the two above dataset are shown in the listing 4.2.

The first RCB, using the PCC measurement dataset, is configured as *unbuffered* reports, since it contains analogue values not crucial for buffering, thus `buffered="false"` and `bufTime="0"`. The RCB is named *PCC_Measurements_poll*, referring to the dataset of the measurements (`datSet="PCC_Measurements`). The purpose of the RCB is to

periodically report the measurements, thus the report *trigger options* are set to allow for General Interrogation, i.e. that the client can request the report whenever it wants (`gi="true"`), and to allow for integrity reports, i.e. that the report is send periodically from server to client (`period="true"`). The integrity period is set to 1000 ms (`intgPrd="1000"`), thus a report is periodically sent each second when enabled. Further, the RCB is configured to send the following data included in the report, the report configuration revision (`configRef="true"`) such that the client knows which kind of configuration is sent, if the model is updated for future releases. The data reference (`dataRef="true"`). The sequence number (`seqNum="true"`) indicating the number of the report, an integer which is continuously increased such that the client can understand if any report has been lost. Finally, the timestamp of the report (`timeStamp="true"`). A further entry specifies the maximum reports enabled by clients, set to 3. This limit is set considering the maximum reporting capability of the IED.

The second RCB, refers to the breaker position. Being a digital values, i.e. the breaker position is given by four states represented by two bits, the report is configured to be a buffered one (`buffered="true"`) with a buffertime of 1000 ms (`bufTime="1000"`). Similarly to the above example, the RCB is configured for various trigger options. Here two specific options are further added. A data change reporting, i.e. when the position changes, the server send a report to indicate such event (`dchg="true"`). Further, the report is also configured to be triggered by a quality change (`qchg="true"`), indicating that the value quality is changed, the client must then take actions if the quality flag is deemed too bad for any further action. Notice that the report is also set to allow integrity periods, for monitoring purposes, but with a higher integrity period of five seconds (`intgPd="5000"`).

Listing 4.2: Snippet of the configured report control blocks of the data model.

```
<ReportControl desc="Measurements of AC quantities from PCC"
    datSet="PCC_Measurements" name="PCC_Measurements_poll"
    intgPd="1000" buffered="false" bufTime="0" confRev="1"
    rptID="VMS1LD0/LLN0.PCC_Measurements">
     <TrgOps gi="true" period="true"/>
     <OptFields bufOvfl="false" configRef="true" dataRef="true
         " dataSet="true" entryID="true" reasonCode="true"
         seqNum="true" timeStamp="true"/>
     <RptEnabled max="3"/>
</ReportControl>
<ReportControl desc="Updates when breaker position changes"
    datSet="Breaker_Status" name="Breaker_Status_Change"
    intgPd="5000" buffered="true" bufTime="1000" confRev="1"
    rptID="VMS1LBESS/LLN0.Breaker_Status">
     <TrgOps dchg="true" gi="true" period="true" qchg="true"/>
     <OptFields configRef="true" dataRef="true" dataSet="true"
          entryID="true" reasonCode="true" seqNum="true"
         timeStamp="true"/>
     <RptEnabled max="3"/>
</ReportControl>
```

Chapter 5

Results

This chapter presents the results of the literature review and the IEC 61850 communication interface integration of the VMS. The chapter follows the evaluation framework proposed in Section 3.3. First, a summary and result of the literature review is presented in Section 5.1. Then, the evaluation of the developed IEC 61850 interface is presented in Section 5.2. Section 5.3 presents the results of the integration work performed in this project, detailing the documented opportunities and challenges of using IEC 61850 in the scope of a mobile BESS. Finally, a result summary is presented in Section 5.4.

5.1 Summary of the literature review

This section presents a short summary of the investigated interfaces/protocols in the literature review, see Chapter 2. The comparison summary is highlighted in a table, see Table 5.1. To provide parameter based comparison and summary of the investigated interfaces/protocols, a parameter set is considered. Namely the parameters

- **Industry**: In which industry is this interface typically used in and tailored to. The parameters highlights typical application usages, but also the intended use from the interface standard maintainer.
- **Usage**: This parameter lists the geographical usage of the interface, i.e. where it's typically utilized. To provide location independent solutions, wide covering is preferred.
- **Security**: A security rating for each interface is determined by the available research present on the individual interface's identified

vulnerabilities. Although the parameter is hard to determine, the general research consensus and vulnerabilities identified can be used to give a comparative non-deterministic ranking amongst the interfaces. Considerations are also taken to the ability to comply to IEC 62443 [63], which is an IEC standard addressing cybersecurity requirements for automation and control systems.

- **Authentication**: This parameters highlights the availability of authentication covered by the interface's standard. Authentication can be a further measure to increase the security within an application, decreasing risk of unauthorized control or access to vulnerable systems.
- **Reports**: This parameter lists the interfaces standard possibility and offering of reports. Providing comparison between the various report structure that may exists. Such as *event driven*, where a report is issued upon an event (such as a state/variable change). *Cyclic* reports represents configured structured data sent periodically, the period can often be configured based on the application need. *Interrogation* reports are not issued directly by the server, but rather a response to a client request, delivering structured report data.
- **Data models**: This parameter indicates if the interface allows for standardized data models. These data models indicate how the device's data semantic and structure shall be to comply to the interface. For an interoperable system and for fast commissioning, clear semantics results in less integration work on system level, since all devices must comply to standardized models.
- **Data types**: This parameter list the available data types supported in each interface/protocol. This parameter is important for considering any eventual implication of available device conversion to suit the protocol capability.
- **Maturity**: A comparative maturity rating parameter is based on the amount of publicly available use-cases and know-how in the industry. Thus generally, older interfaces/standards (which are commonly used) can be considered as more mature.
- **Priority tagging**: This parameter shows the interface/protocol capability to tag data points, such as commands, with priority. Thus if conflicting commands are sent to a device, priority tagging resolves the conflicting issues.

- **Timestamps**: This parameter indicates the interface/protocol capability of individual data point timestamps.
- **Quality flags**: This parameter indicates the interface/protocol capability of providing quality flags on individual data points. The flags shall be specified by the interface/protocol standard. Examples of such flags, could be indications of bad ”quality” in the sense of inconsistent data, overflow of the value, out of range indications etc.
- **Certification**: This parameters indicates if there's any accreditation of compliance to the interface/protocol standard available. Certifications could then be given to the device compliant to the interface.
- **Application identified**: As discussed in each respective interface introduction, the application suitability identified will be repeated in this parameter for the general comparison overview.

Although most parameters are easily determined from the respective introduction, for some protocols, the parameter fit is not as easily determined. One instance is for the Modbus protocol, while the protocol itself, be it TCP, RTU or ASCII, formally does not include data models, some data types and certification, there are readily used *variants* of the Modbus protocol which expand in these areas. An example is Sunspec Modbus. This variant is indeed certifiable by the Sunspec alliance, and is also referenced as an eligible protocol for DER interconnection and interoperability in IEEE 1547-2018, along with DNP3 [64, 65]. Further, the variant also includes standardized DER data models. It's then also important to recognize that while the Modbus protocol does *only* support boolean and integer data types, common workarounds to the limited 16-bit registers is to assign multiple register to map further data types, such as 32-bit (or 64-bit) floats, 32 to 64 bit integers, ASCII characters etc, although such expansions exists, endianness is often differing from device to device. Thus the parameter evaluation is not clearly defined by considering the variant existing.

Parameter	Modbus	IEC 61850	DNP3	OCPP & OSCP	OpenADR	IEC-101/104
Industry	Industrial applications	Power Utility Oil & Gas Water	Power Utility	EV	EV Power Utility	Power Utility
Usage	Worldwide	Worldwide	Americas Asia	Americas Europe	Americas Europe	Asia Europe
Security	Lowest	High	Low	Medium	Medium	Low
Auth.	No	Yes	No	Yes	Yes	No

Parameter	Modbus	IEC 61850	DNP3	OCPP & OSCP	OpenADR	IEC-101/104
Reports	No	Event driven Cyclic Interrogation Buffered Unbuffered	Event driven Cyclic Interrogation	Interrogation	Cyclic Interrogation	Event driven Cyclic Interrogation
Data models	Yes/No	Yes	No	No	Yes	No
Data Types	boolean integer	boolean integer float strings enums	boolean integer float	boolean integer float strings	boolean integer float strings	boolean integer float
Maturity	Good	Medium	Good	Medium	Medium	Good
Priority tagging	No	Yes	No	No	No	Yes
Timestamps	No	Yes	Yes	Optional	Yes	Yes
Quality flags	No	Yes	Yes	No	No	Yes
Certifiable	Yes/No	Yes	Yes	Yes	Yes	Yes
Application identified	EV Microgrid	EV Microgrid Utility Support	Microgrid Utility Support	EV	EV Utility Support	Utility Support

Table 5.1: A summary over the investigated protocols/standards across multiple parameters.

5.1.1 Electrical Vehicle charging stations

As presented in Table 5.1, the four identified readily utilized interfaces for EV charging stations are

- Modbus
- IEC 61850
- OCPP & OSCP
- OpenADR

Comparison between the identified interfaces for the applications shows differences in some of the investigated parameters. Firstly, while two of the interfaces (OCPP & OCPP and OpenADR) are purposely designed for the EV use case, the latter two (Modbus and IEC 61850) cover more use cases and applications. Furthermore, the interfaces differ greatly in the protocol specific parameters such as **reports**, **data models**, **priority tagging**, **timestamps** and **quality flags**.

For the specific use case, as a mean of supporting greater interoperability, flexibility and fast deployment, report availability can give large benefits to the application. Notably, Modbus does not support any protocol specified

reports, thus mandating for proprietary solutions, prone to heavy integration work. Furthermore, while all remaining interfaces offer interrogation based reports, OpenADR and IEC 61850 is capable of offering more advanced reports. Such as cyclic reports in OpenADR; and event driven, cyclic, buffered and unbuffered in IEC 61850.

5.1.2 Remote off-grid operation

Following the summary presented in Table 5.1, three common interfaces for microgrids, or remote off-grid operations are identified, namely

- Modbus
- IEC 61850
- DNP3

While no interface is purposely designed for the application, only DNP3 usage scope is *limited* (altough broad) to power utility use cases. While the latter two are frequent among other use cases. Furthermore, notable parameter differences between the interfaces are; **location usage**, **security** and **data models**.

For the microgrid use case, the unavailability of data models and clear semantics between the interfaces directly impacts the ease-of-use and interoperability between the devices. Where two interfaces, Modbus and DNP3 often come with proprietary data mappings, thus requiring heavier integration work for integration new devices from different vendors. Furthermore, the greatly studied security vulnerabilities of Modbus and DNP3 must be acknowledged, where as presented under each interfaces review (see Section 2.3.1.2 for Modbus, and see Section 2.3.3.2 for DNP3), many critical security vulnerabilities and knows attacks are present. For larger use cases, with more interconnected devices and critical load, the security parameter is of key importance.

5.1.3 Temporary utility grid support

The four interfaces identified for temporary utility support, as presented in Table 5.1 are

- IEC 61850
- DNP3

- OpenADR
- IEC 60870-5-101/104

Notably, some of the key parameter differences between the identified interfaces are; **location usage**, **security**, **data models**, **maturity** and **priority tagging**. On the growing interest in DER for flexibility services, as both stationary or mobile temporary units, interoperability is of key importance. Where some main differences are the data models available in each interface standard, as in IEC 61850 and OpenADR. While the other two lack such standardization, thus driving in proprietary integration heavy solutions.

Furthermore, the maturity parameter is of importance, specifically in industries like power utilities, where high reliability and longevity is important. Thus a maturity in the interface usage is valuable. Although DNP3 and IEC-101/104 are commonly used in their respective regions, several cybersecurity issues have been identified and commonly discussed (see Section 2.3.3.2 for DNP3, and see Section 2.3.6.2 for IEC 60870-5-101/104). Due to the criticality of some power utility assets, gradual increase of usage of IEC 61850 along with modern security measures are preferred.

5.2 Developed IEC 61850 communication interface

The IEC 61850 communication interface was connected to a PC running IEDScout [54] as a IEC 61850 client (HMI). This connection represents the connection of the VMS IED to an IEC 61850 network. The connection sequence is performed as follows. Using IEDScout, by a wired ethernet connection to the IED gateway, connection is performed by the command Discover IED (1), where the IP-address of the IED and OSI parameters are entered. After connection to the IED, the data model is downloaded to the client and visible to the user. Controlling of parameters is done by the Control (2) button, which, depending on the applied control mode, allows for operating commands on the selected DO. See Figure 5.1. As highlighted by the Online indicator, the connection status is indicated after an IED is *discovered*.

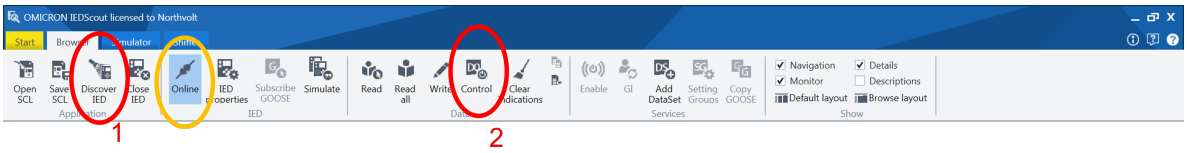


Figure 5.1: Connecting to an IED with IEDScout by OMICRON.

The connection parameters configured in the IEC 61850 client are shown in Figure 5.2. Notably, this is the only client configuration needed.

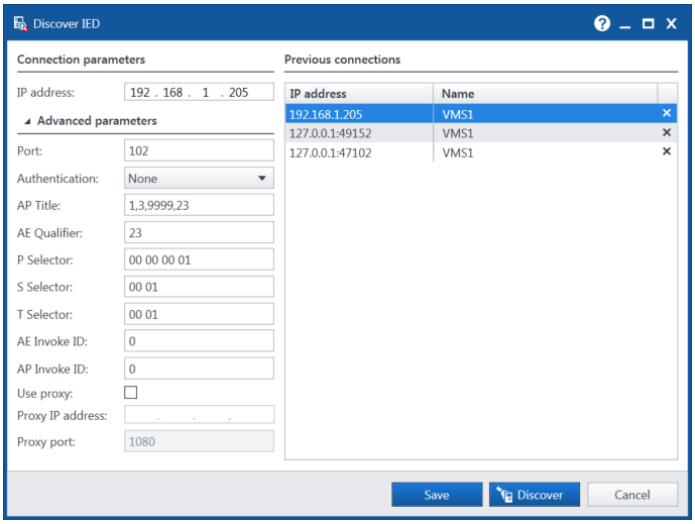


Figure 5.2: IEDScout connection parameters needed for IED connection.

After connection, the validations according to the evaluation framework were followed. First the *vertical communication* is performed, see Section 5.2.1. Then the *horizontal communication* is valuated, see Section 5.2.2.

5.2.1 Vertical communication

As a verification of typical vertical IEC 61850 communications, typically through the MMS protocol, a set of reads and command operations were performed. For all sequences, the configured report control blocks where enabled. The five blocks are

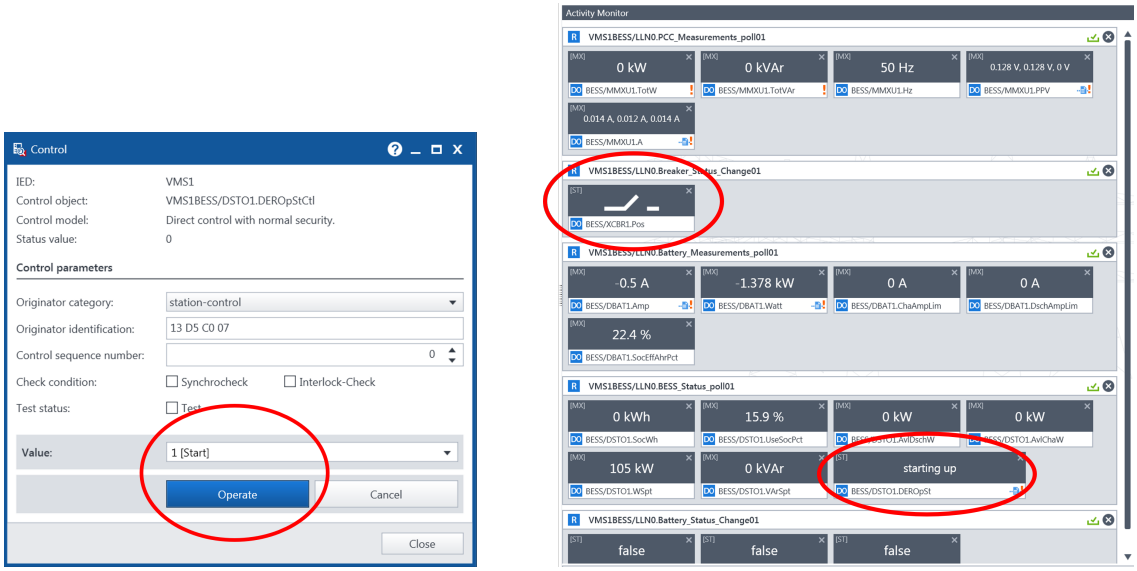
- `VMS1BESS/LLN0.PCC_Measurements_poll01`. Which performs integrity polls of the PCC measurements, coming from the measurement LN **MMXU**.

- `VMS1BESS/LLN0.Breaker_Status_Change01`. Which is a report triggered on data or quality change of the breaker status, i.e. `XCBR1.Pos.stVal`. A integrity period of 5 seconds is also configured for monitoring.
- `VMS1BESS/LLN0.Battery_Measurements_poll01`. Which performs integrity polls of the battery measurements, showing the discharge and charge current limits and instantaneous current and power.
- `VMS1BESS/LLN0.BESS_Status_poll01`. This report provides integrity data on the status of the BESS DER, such as the operating state `DEROpSt`, usable State of Charge `UseSocPct` and energy capacity `SocWh` etc.
- `VMS1BESS/LLN0.Battery_Status_Change01`. This report is triggered by data or quality change of the single point **DBAT** statuses, i.e. charging status `ChaSt`, discharging status `DschSt` and DC switch position `DCSwCls`.

Enabling all reports control blocks shows the performance and integration ease of the IEC 61850 interface, since no manual client configuration was needed except the connection parameters, as shown in Figure 5.2.

After the physical system start-up, the control sequence of the VMS DER was performed using the IEDScout client. After power-up, the systems enter the state (`DEROpSt`) *on but disconnected & not ready*, expecting a start command to proceed in the state machine. The start command issuing is shown in Figure 5.3, where direct control with normal security operate command was issued to the state control DO `VMS1BESS/DSTO1.DEROpStCtl`. The command CDC is of type **ENC** (enumerated control), where the start command has the enum-value 1 (selected from client). After the operate command, the IEDScout activity monitors shown the received reports visualizing the DER behavior, where the operating state (`VMS1BESS/DSTO1.DEROpSt`) represents the initialization state (*starting up*), where the DC-bus (battery contactors) is energized, preparing for connect commands. See Figure 5.3b.

The next command of operation issued to the DER state machine is the connect command. The unit shall then commence the synchronization process to connect the DER terminals to its PCC safely. As seen in Figure 5.4. A direct control with normal security operate command is issued to the DER by the enum-value 2 [Connect]. Analyzing the reports received post commands shows the following; the DER breaker closes



(a) Direct control of **DEROpStCtl** to operate a start command.

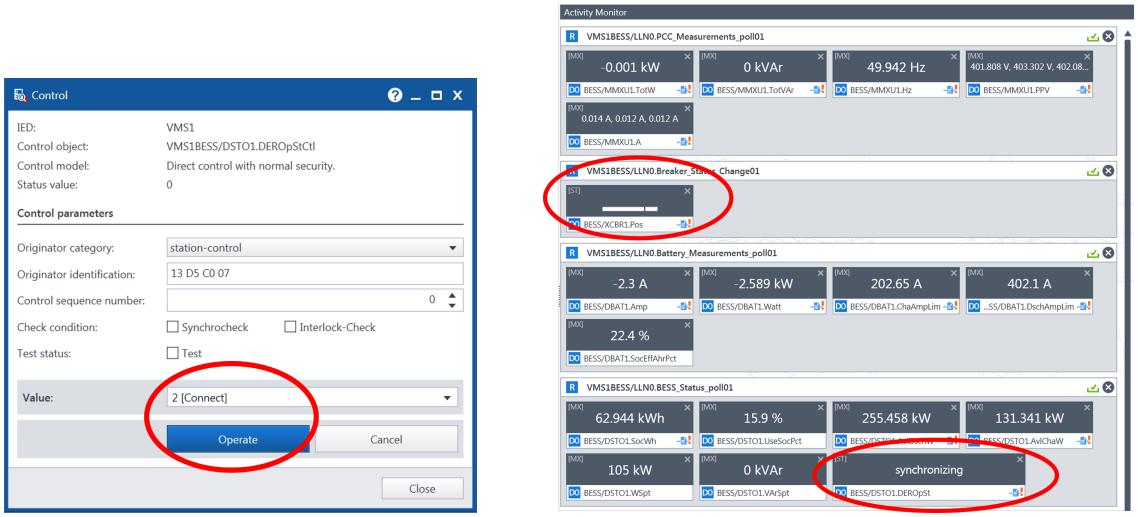
(b) Received integrity reports and data change updated following start command.

Figure 5.3: DER start command request.

(`XCBR.Pos.stVal`) to connect the PCC to the PCS terminals, while the DER enter the synchronization state (`DEROpSt`). The status values are also updated further, showing the current charge and discharge power capacity along with the actual energy capacity, see Figure 5.4b.

While the state control of a DER is of importance, the operations of the unit must be reliable for further commands such as power setpoints. This capability is tested by issuing an active power setpoint to the DER while it's running. As shown in Figure 5.5, a change in active power setpoint (**WSpt**) is operated to the LN **DSTO1**. The change was done from a previous power setpoint of 120 kW to a new 105 kW setpoint. Notice that the reference frame indicated by the DER, as shown in the PCC reference frame DO `DPCC1.RefFrm` (CDC of type **SPG**, Single Point Setting), set to false, i.e. consumer reference frame (positive is load/charging of BESS). As seen by the received reports, the power setpoint is tracked by the PCC measurements. The battery charging power can be seen, along with the setpoint feedback, see Figure 5.5b.

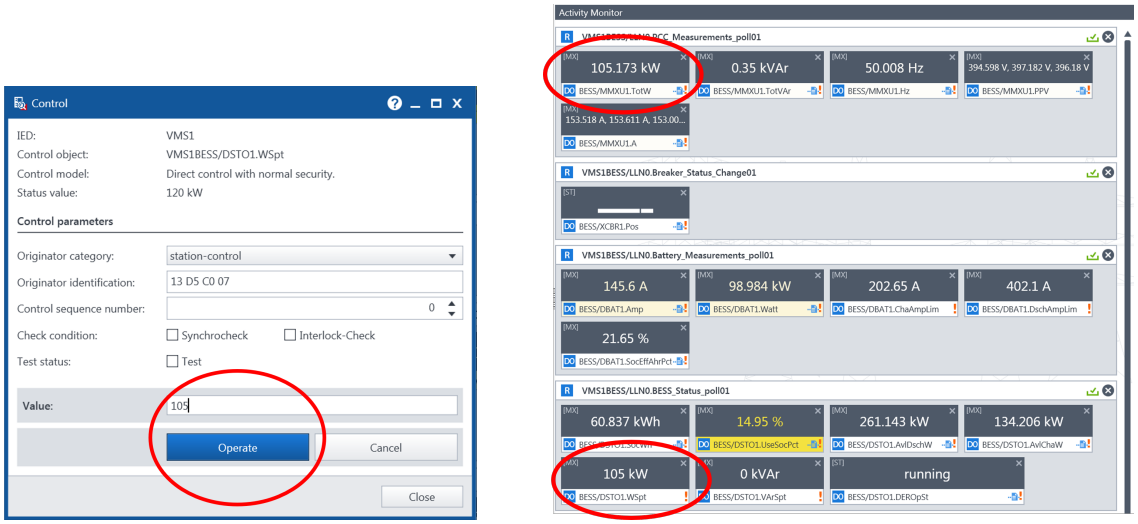
The above sequence shows the operation of the DER IEC 61850 interface created for the VMS by virtue of vertical communication, i.e., using the MMS protocol. The report results along with the correct state and setpoint control show the validity of the operating DER model.



(a) Direct control of **DEROpStCtl** to operate a connect command.

(b) Received integrity reports and data change updated following connect command.

Figure 5.4: DER connect command request.



(a) Direct control of the active power setpoint of the DER, i.e. **WSpt**.

(b) Received integrity reports and data change updated following active power setpoint change.

Figure 5.5: VMS active power setpoint change.

5.2.2 Horizontal communication

Typically, horizontal communication, e.g., from IED to IED is performed by rapid GOOSE messages. Such as the implementation of the DER control in

[21], where GOOSE messages were used for decentralized control of DERs for Volt / Var control strategies.

However, due to the gateway selection, along with the limitation in the project initial scope. The possibility of GOOSE messaging to and from (publisher/subscriber) is not possible at the current implementation stage. This results in the VMS DER inability of faster horizontal communications. Applications of such functionalities could be faster communication requirements within a substation station bus. For example, if a bay signals an opening in the breaker, this fast signal could be configured as an input on the DER side. Whether that could be a change in power setpoint, disconnection from the PCC or islanding operations. Further functionalities linked to protection functions could also be used. As in lowering the power input/output of the DER if an overcurrent protection starts its timer.

Furthermore, the usage of the GOOSE protocol with a gateway network topology may be misleading, as the expectation of fast communication is hindered by the protocol conversions. Although this could be designed for, the gateway could have physical connections (relay switches) that could be physically integrated into the system.

However, while the availability of the protocol can be improved with other solutions, the data model developed is still valid, as demonstrated in Section 5.2.1. Thus, the data model of the VMS DER is considered to be finalized.

5.2.3 Summary

The IEC 61850 datamodel was validated by analyzing two communications scopes of typical usage. First, *vertical communication* is performed using the MMS protocol. Such communication architecture is commonly used for communication between IEDs and station HMI or operator control center. Thus reflecting the proprietary legacy protocol operation of the VMS. The results in Section 5.2.1, show sufficient communication capability for DER operations, such as state control (start, connect etc.), power setpoints. As shown by the easy client connection, the IEC 61580 interface has great benefit in the ease of unit integration, with minimal integration needs, since the data model can be read upon IED connection, exposing the entire data model and DOs configurations. Secondly, analysis of *horizontal communication* is done. This communication architecture is common in rapid IED to IED communications. While this functionality is not existing in the implemented solution, it does not impact the data model validity, since the model is functional regardless of protocol exposure. The server capabilities of the IED

reflects which communication protocols that can be used. Thus the result of the IEC 61850 integration still show the applicability and interoperability that is achieved by the standard and the implemented interface.

5.3 IEC 61850 integration work

This section presents the integration work results of the IEC 61850 interface for the VMS. Details of identified benefits and gaps of the interface will be presented, to give a perspective on the integration work. The perspective of these results are from the manufacturer perspective, how the interface was integrated in a current system, while some minor aspects from the system usability, i.e. from the client perspective is given as a comparison to other interfaces. The main benefits and highlights of the integration work is presented in Section 5.3.1. While the identified gaps and suggested improvements to the interface is presented in Section 5.3.2.

5.3.1 Identified benefits

The benefits listed in the literature review of the IEC 61850 interface, see Section 2.3.2, were seen and validated in this evaluation framework. Namely the benefits of *standardized virtual models*. Where each implemented LN serves a specified purpose in the model, containing mandatory and optional DOs as specified by a standard model. The main benefit is the clear design requirement from the manufacturer perspective, i.e. what data and how it shall be represented. For a customer perspective, it clarifies the expected data from a compliant unit, allowing for interoperability between vendor-independent devices. Compared to the other interfaces who lack this specification, the work needed at engineering level, such as configuration and commissioning is greatly increased. Thus requirements are set from a standard, which mandates some specific DOs and other modelling needs, instead of having these requirements strictly from conflicting customers based on their usage and needs.

Furthermore, another main advantage of the IEC 61850 interface is the *self-describing device*. As shown in Section 5.2, an IEC 61850 client can directly connect to the IED (if authorized) and obtain the entire data model directly, without the need of pre-configuration and manual mapping of data, as common in ”index” based protocols like Modbus or DNP3. Then the client can directly access the *named data* to monitor the device and operate command. While the described operation is performed on-line, i.e. connected to a device,

the developed SCL model (the ICD file) can be used in the engineering process before a system configuration and commissioning, enabling so-called *top-down engineering* workflow, as commonly used in the Helinks tool.

Additionally, the conceptual view of a DER from the IEC 61850 standard shows benefits compared to the current system view for the VMS. Namely, as described by the operational functions available in IEC 61850-7-420, the DER units are consider to be autonomous. That is, they can receive external command and functions to follow, but may also operate by themselves if configured. Examples are scheduling operational functions or curve droop settings, that the DER follows after being enabled, regardless of any needed client connections. Compared to a purely client-server based protocol, like Modbus, such advanced operational functions may often be mapped on the client controller side, constantly polling the server (BESS) for data and writing new setpoint accordingly. With the standard operational functions specified in IEC 61850-7-420, the client enables and sets the needed operational settings, while the server (BESS DER), internally is responsible for the function. Although such functionalities are possible in other interfaces, the specifics of the function, such as the settings needed and when to operate, are up to the manufacturer to decide. A summary of the operational functions deemed interesting for mobile BESS operations are presented and explained below.

- **DAGC**: This operating function, *Automatic Generation Control*, is utilized by the balancing authority to control the DER active power output for managing the asset, mainly for frequency regulation [16]. Typically, commands are issued by direct operate every few seconds.

- **DTCD**: This operational function refers to *coordinated charge and discharge operation to manage the State of Charge (SoC)* of the storage DER [16]. Typically, commands are issued by setting a target SoC (`SocUseTgt` DO) at a specific target time (`DateTgt` DO). Where the DER autonomously charges and discharged to the desired target within the boundaries of the operation.

- **DHFW** & **DLFW**: These operational functions refers to *High/Low Frequency-Active Power* operation of the DER [16]. These functions sets or limits the active power output of the DER for high or low frequency conditions respectively. Typical usage is for frequency support, i.e. as a Frequency Containment Reserve (FCR) providing synthetic/artificial inertia.

- **DWFL**: This operational function represents the *Active Power Following* operation of the DER [16]. This function requests the DER to follow and compensate for active power at a certain ECP. Effectively, such functionality allows for load following and peak-shaving depending on the settings and constraints used. Further, the function can also refer to another DER unit, to act as generation following, to coordinate between the resources.
- **DVVR**: This operational function represents the *Voltage-Reactive Power* operation of the DER [16]. The functions relies on volt-VAr curves used to autonomously control the reactive power output from the DER to follow voltage changes. The curves specify the support level provided by the DER to mitigate the voltage changes.

5.3.2 Identified gaps

During the integration work, some gaps on the mobile BESS point-of-view where identified in the IEC 61850 standard. Notably, these gaps are missing standard LNs and DOs important for mobile applications.

Firstly the missing description and capability to represent a Thermal Management System (TMS) within a DER. Specifically for battery storage systems, monitoring and control of the TMS is important for safe and efficient operations. For a mobile application, this importance is amplified, since the deployments site for a device may vary greatly between the applications and throughout the seasons. A suggestion is therefore made by designing a LN capable of the needs identified, called **DTMS**, further discussed in Section 6.1.3, with a suggested LN proposed in Appendix A.

Secondly, connected to the before mentioned gap, the general state machine for a DER in IEC 61850 is sufficient enough for basic operations, as shown in Section 5.2. However, some notable extensions are identified. Such as, inclusions of detailed ”start” up states, relevant for battery storage DERs. For mobile applications, the unit may be transported to and from sites resulting in longer off-state duration, which depending on the weather conditions may imply non-ideal operating conditions at startup. Requiring mandatory heating or cooling operations, therefore extension of the state machine to include such state would allow for clearer operation of the unit. Nonetheless, further extension of state machine descriptions could also be taken, such as specifying typical state transition times. Such timing specifications would be relevant for synchronization procedures, where typical times can differ greatly (seconds to minutes) based on the DER types (inverter connected versus generator etc.).

Additionally, further details, useful for client operators could be added to the physical device nameplate, i.e. **LPHD** `PhyNam`. The suggested DOs can include data on weight and dimension. Further expanding the usability of the data model as an information source, instead of relying on various manuals or guides.

5.4 Summary

This section provide a summary of the literature investigation in Chapter 2, together with the results of the interface and integration work presented earlier.

Firstly, from the literature review, it is evident that only one interface studied is suitable to cover all three interfaces, the IEC 61850 standard. Nonetheless, the other parameters investigated, such as the worldwide usage and the many data types supported further extend such interfaces choice. It must then be realized that although the IEC 61850 standard can cover all investigated applications, it may not be the most commonly utilized, specifically in the EV charging case, where other protocols, driven by the charging stations are more prevalent. Thus, defining an interface that fits the best, considering actual use-cases, is hard to define. Nonetheless, for strict power utility applications, where BESS installations are constantly growing, along with the usability of mobile versions show clear avenue in integrating the IEC 61850 interface. Which was highlighted further in Section 5.3.1.

Chapter 6

Discussion

This chapter presents discussions on the work performed within the thesis project. Namely, the IEC 61850 interface integration to the VMS, see Section 6.1.

6.1 IEC 61850 Integration

This section presents discussions and reflections on the IEC 61850 integration work performed in this thesis. The discussion includes the data model simplification done at modeling stage, see Section 6.1.1. The choice of using a protocol gateway for the integration work and its implications, see Section 6.1.2. Finally, for a discussion of the recognized gap in part 7-420 for a mobile BESS operation, which are unavailable LNs, see Section 6.1.3.

6.1.1 Data model simplification

The data model and integration performed, as presented in Chapter 4, follows the initial goals drafted at the start of the project. To provide a basic yet fully operational IEC 61850 interface to evaluate its benefit for a mobile BESS, which gave the results as presented in Chapter 5. Nevertheless, some simplifications to reach the results stage were made, such as the minimum VMS topology available for an operating system, i.e., one PCS physical block, and one battery block. Conveniently, this can define the abstracted model into one physical device representing the BESS. Furthermore, since VMS allows modular battery block connections, detailed models should consider such system capability. Thus, an extension of the model would be to incorporate the modular capability of the system by introducing instances of **DBAT** for each

battery block. These LNs may then be expanded to separate LDs, to further expand the system description with details of each battery block separately.

Furthermore, for integration investigation, advanced operational functions, as identified in Section 5.3.1, were not implemented in the data model or system integration. As presented by the benefits of such operational functions, effectively rendering the VMS an autonomous DER. Such model expansion could show an even greater real-life performance increase of the system usability. Specifically, in the sense of complying to standardized operational functions where the operating and communication requirements are clear. Otherwise, such improvements are often driven by user feedback for product development, while these operational functions could be directly considered in the design process of the product development, rather than additions.

6.1.2 Gateway usage

As initially presented in the objectives in Section 1.4, the scope of integration of the IEC 61850 interface was to investigate basic client-server functionality in SCADA applications. Thus, an initial constraint in the integration work was chosen to only consider the MMS protocol, which in turn simplified the search and procurement of reliable protocol gateway for the needs of the work; see Chapter 4. Furthermore, during the integration work, documenting the benefits and gaps identified along with the literature review provided, the great benefit of publisher-subscriber capability of an IED became evident. For example, for the possible evaluation frame of an evaluation of horizontal communication using GOOSE, see Sections 3.3.2 and 5.2.2. Therefore, the initial choice of gateway usage limits future expansion to utilize the many more benefits and capabilities of IEC 61850. Examples of such additional capabilities are fast horizontal communication with other IEDs, participation in applications requiring higher speed communications such as protection applications, and broadcast decentralized coordination of DER. Nevertheless, although limited to one of the IEC 61850 communication services, the easy workflow and detached development from the product side offer great benefits to system integrators and manufacturers in not only investigating IEC 61850 benefits. But also offering its new capabilities.

6.1.3 Missing Logical Nodes from vendor perspective

As briefly covered in Section 5.3.2, an important subsystem of a mobile BESS is not covered in a satisfactory manner under IEC 61850-7-420. Namely a LN

to represent the physical capabilities of a TMS. For a BESS and even more specifically for a mobile unit, the TMS is of great importance for safe and efficient system operations. Although some basic coverage is present in 7-420, such as the DO `ClMthTyp` in the PCS LN **DINV**. `ClMthTyp` only indicates the cooling method as a setting, CDC type ENG (enumerated setting).

Due to the *flexible and mobile* nature of mobile BESS, the environmental conditions can differ greatly for each system depending on the respective mobile deployments. Ranging from high temperatures and high humidity to the inverse during the same season, monitoring and control of the TMS is critical. Specifically for battery-based energy storages, maintaining correct cell temperatures is needed to keep the pack in optimal operating ranges and minimizing performance decreases due to problematic operating conditions.

A proposal of LN to add the required functionality and capability according to the needs of a mobile BESS is presented in Appendix A, where a new LN **DTMS** is with specified DOs and literal kinds to represents a general TMS. The LN is designed to be subsystem independent; thus, the TMS can be modeled to manage the thermals of various LN instances such as **DINV** and **DBAT** separately or together.

In particular for the LN DOs, status information for the operating state of the TMS, `TMSOpSt` , is deemed mandatory. For mobile applications, longer-term storage of a unit can often occur between deployments. Thus at site commissioning stage, i.e. when the mobile unit is deployed and connected at a site, the operating conditions may not be ideal for safe operations (cold battery temperatures during winter, or over-temperature on summer season). Therefore, status information for the TMS state is needed to indicate any heating or cooling needed before operation can commence on site. The suggested TMS operating state literals are presented in Table A.2.

Chapter 7

Conclusions and future work

This chapter presents the conclusions of the thesis project conducted, the limitations and their respective impact on the outcome, and finally the proposed future work. The conclusions of the thesis project are presented in Section 7.1. The limitations of the project work and their respective implications are presented in Section 7.2. Finally, suggested future work for the continuation and expansion of the project is presented in Section 7.3.

7.1 Conclusions

This thesis project investigated the vastly available interfaces and protocol commonly used in power utilities and EV charging solutions. The investigation compares the identified communication interfaces and their respective applicability to a mobile BESS, specifically the VMS. For specific power utility applications, it is clearly noted that the standard IEC 61850 allows clear benefits compared to the other investigated interface. Exploring the standard further, a basic data model and system integration is developed to document the suitability of the standard on a real mobile BESS. The integration work highlights some key benefits of integrating a standardized communication interface compared to the other investigated interfaces. Notably, the self-description of the device, the clear data model requirements, and data type definition facilitate not only the development phase from the manufacturer perspective, but also the interoperability and usability form a customer and client perspective. This interoperability facilitates rapid integrations for customer projects and clear requirements for the manufacturer.

Furthermore, we conclude with the research questions initially posed. To find the best-suited communication protocol for mobile BESS applications,

while the investigations clearly point to the key benefits of IEC 61850, further research on the actual use-cases existing must also be considered to answer the question. Nevertheless, while IEC 61850 is deemed most suitable for power utility applications, other basic applications of mobile BESS often does not require the same strictness and requirements as the IEC 61850 mandates, therefore, for basic applications, the legacy Modbus protocol should not be underestimated. Rather, the main benefit of its ease of use and maturity will keep the protocol in use for basic applications where full SCADA systems are not necessary.

Secondly, regarding the suitability and/or eventual gaps in the IEC 61850 standard for mobile BESS solutions, it is shown that the standard provides sufficient parts for operation of a mobile BESS unit in power utility applications. Furthermore, some gaps where found. Importantly for mobile applications, the lack of LNs for a TMS was identified. A suggestion of LN design is proposed to fill the gaps needed for thorough monitoring and control of the entire mobile system.

7.2 Limitations

Two main limitations where found during the thesis project. First, the research availability for unbiased and quantitative data on the interfaces investigated in the literature review. Then the self-imposed project limitation to integrate a client-server based IEC 61850 architecture, where the gained knowledge during the project shows clear limitation on further expansion using the selected hardware.

A limiting factor in the literature review and analysis is the unavailability of publicly available research on use-cases and quantitative data on installations using a specific protocol/interface in the analyzed application scope. Such unavailability is perhaps reasonable considering the security risks of publicly defining clear use-case and details regarding power utility applications and communication interfaces. Nevertheless, the unavailability of such clear details was circumvented by considering protocol-specific details and capabilities, which are readily available for each protocol/interface. Second, in relation to the literature review, a limitation was made in considering the battery size, together with considering mainly the uses of power utilities and EVs charging stations. Smaller BESS sizes for residential applications, where not considered, thus limiting some prevalent communication protocols in building automation, such as BACnet and KNX, but also home automation such as ZigBee, ZWave, and MQTT.

Furthermore, as recognized in the discussion, although the initial integration scope is achieved in the thesis, a clear outcome following the knowledge gained in the field and development work, shows a limitation in the final interface developed. While the interface is fully capable of client-server communication in a typical *vertical* manner. The current solution is not expandable for further protocol additions, such as GOOSE to achieve publisher-subscriber communications. Nevertheless, the developed interface achieves the set objectives and desired investigation result. However, the identified limitation post-development provides clear future improvements and extension directions. This suggested work is presented in further detail in the future work section; see Section 7.3.

7.3 Future work

Although the goals for this thesis project were met, as discussed in Chapter 6 and in Section 7.2, the main results of the thesis project provide an avenue for further research and development in the field of communications for mobile BESS. Four suggestions for further expansion of the project and investigations to be considered are introduced here. Namely the points,

- Cooperate with utility companies (DSOs) to further validate and develop the IEC 61850 data model and capabilities. An evaluation framework is to install such device in the utility grid, perhaps at the distribution level, for real-life performance analysis of the system.

- Expansion of the basic IEC 61850 data model to include the suggested solution TMS and the modular battery block connections that are possible, integrating multiple instances of **DBAT**. Furthermore, the model can be expanded to include the VMS specific topology, which is more advanced with electrical connections and breakers than the basic BESS model utilized.

- Incorporate the publisher-subscriber protocol GOOSE into the capability of IEC 61850 VMS IED, to further maximize the key benefits of the standard. Accommodating novel and state-of-the-art BESS coordination and protection capabilities. Furthermore, such a coordination scheme could be utilized to effectively connect multiple VMS and other mobile BESS in an effective manner, for an interoperable coordinated mobile system DER.

- Extend the scope of battery size investigation to consider residential use cases. Examples of such protocols/interfaces common in building automation are BACnet and KNX, while for home automation protocols such as ZigBee, ZWave, and MQTT could be investigated.

References

[1] *Voltpack Mobile System*, en, Feb. 2021. [Online]. Available: https://northvolt.com/products/systems/voltpacks/mobile/ (visited on 02/17/2023).

[2] Y. Yu *et al.*, "Data-Driven Study of Low Voltage Distribution Grid Behaviour With Increasing Electric Vehicle Penetration," *IEEE Access*, vol. 10, pp. 6053–6070, 2022, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3140162.

[3] M. T. Lawder *et al.*, "Battery Energy Storage System (BESS) and Battery Management System (BMS) for Grid-Scale Applications," *Proceedings of the IEEE*, vol. 102, no. 6, pp. 1014–1030, Jun. 2014, Conference Name: Proceedings of the IEEE, ISSN: 1558-2256. DOI: 10.1109/JPROC.2014.2317451.

[4] I. Oxborrow, *Europe set to be global leader for electric vehicle use by 2030, report says*, en, Section: Technology, Jan. 2023. [Online]. Available: https://www.thenationalnews.com/business/technology/2023/01/09/europe-set-to-be-global-leader-for-electric-vehicle-use-by-2030-report-says/ (visited on 04/28/2023).

[5] *EV Charging Station Market Size, Share, Forecast, Report, 2030*. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/electric-vehicle-supply-equipment-market-89574213.html (visited on 04/28/2023).

[6] I. Belloni, *Temporary EV fast charging at events – how to organize and what to consider?* en-US, Apr. 2022. [Online]. Available: https://kempower.com/temporary-ev-fast-charging-at-events-how-to-organize-and-what-to-consider/ (visited on 04/28/2023).

[7] I. Belloni, *Proving the case for EV charging at events*, en-US, Sep. 2021. [Online]. Available: https://kempower.com/proving-the-case-for-ev-charging-at-events/ (visited on 04/28/2023).

[8] *Peak Load Shaving With E-vehicle Charging Stations*, en. [Online]. Available: https://www.tesvolt.com/en/projects/peak-shaving-with-electric-vehicle-charging-stations.html (visited on 04/28/2023).

[9] A. Y. Ali, A. Hussain, J.-W. Baek, and H.-M. Kim, "Optimal operation of static energy storage in fast-charging stations considering the trade-off between resilience and peak shaving," en, *Journal of Energy Storage*, vol. 53, p. 105 197, Sep. 2022, ISSN: 2352-152X. DOI: 10.1016/j.est.2022.105197. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352152X22011963 (visited on 04/28/2023).

[10] *Powered by Northvolt: Fast Charging Electric Trucks*, Mar. 2023. [Online]. Available: https://batteriesnews.com/powered-northvolt-fast-charging-electric-trucks/ (visited on 03/14/2023).

[11] P. Klapwijk and L. Driessen, "EV Related Protocol Study," Tech. Rep., May 2017.

[12] A. Hoekstra, A. Wargers, E.-l. Foundation, H. Singh, and P. Voskuilen, "Using OpenADR with OCPP," en,

[13] H.-J. Jun and H.-S. Yang, "Performance of the XMPP and the MQTT Protocols on IEC 61850-Based Micro Grid Communication Architecture," *Energies*, vol. 14, p. 5024, Aug. 2021. DOI: 10.3390/en14165024.

[14] A. Bani-Ahmed, L. Weber, A. Nasiri, and H. Hosseini, "Microgrid communications: State of the art and future trends," en, in *2014 International Conference on Renewable Energy Research and Application (ICRERA)*, Milwaukee, WI, USA: IEEE, Oct. 2014, pp. 780–785, ISBN: 978-1-4799-3795-0. DOI: 10.1109/ICRERA.2014.7016491. [Online]. Available: http://ieeexplore.ieee.org/document/7016491/ (visited on 02/08/2023).

[15] *ASC 150 Storage - Flexible ESS controller*, en. [Online]. Available: https://www.deif.com/products/asc-150-storage/ (visited on 04/27/2023).

[16] "Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources and distribution automation logical nodes," English, French, International Electrotechnical Commission, IEC 61850-7-420:2021, Oct. 2021. [Online]. Available: https://webstore.iec.ch/publication/34384 (visited on 02/03/2023).

[17] D. Cai *et al.*, "Analysis of Heavy Load and Overload Distribution Transformer in Regional Power Grid," in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, Oct. 2018, pp. 1–5. DOI: 10.1109/EI2.2018.8581984.

[18] N. Rodrigues, S. Vyas, and A. Datta, "Two-Stage Battery Energy Storage System Sizing for Distribution Transformer Overload Management," in *2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, ISSN: 2687-7767, Nov. 2019, pp. 1–6. DOI: 10.1109/UPCON47278.2019.8980179.

[19] X. Sun, J. Qiu, Y. Tao, and Y. Yi, "Cost-Effective Coordinated Voltage Control in Active Distribution Networks With Photovoltaics and Mobile Energy Storage Systems," *IEEE Transactions on Sustainable Energy*, vol. PP, pp. 1–1, Oct. 2021. DOI: 10.1109/TSTE.2021.3118404.

[20] C. Das, "Overview of energy storage systems in distribution networks: Placement, sizing, operation, and power quality," *Renewable and Sustainable Energy Reviews*, vol. 91, Aug. 2018. DOI: 10.1016/j.rser.2018.03.068.

[21] H. Albunashee and R. McCann, "DER Coordination Strategy for Volt/VAR Control using IEC61850 GOOSE Protocol," Dec. 2020.

[22] M. S. Thomas and J. D. McDonald, *Power System SCADA and Smart Grids*. London, UNITED KINGDOM: Taylor & Francis Group, 2015, ISBN: 978-1-4822-2675-1. [Online]. Available: http://ebookcentral.proquest.com/lib/kth/detail.action?docID=1829472 (visited on 02/23/2023).

[23] M. Matt, *Make your BESS ready for the Smart Grid*, en-US, Jan. 2022. [Online]. Available: https://www.energy-storage.news/make-your-bess-ready-%20for-the-smart-grid/ (visited on 06/14/2023).

[24] J. Guerrero *et al.*, "Flexibility Services Based on OpenADR Protocol for DSO Level," *Sensors*, vol. 20, p. 6266, Nov. 2020. DOI: 10.3390/s20216266.

[25] *Modbus Specifications and Implementation Guides*. [Online]. Available: https://modbus.org/specs.php (visited on 02/09/2023).

[26] T. Carlsson, *Industrial networks keep growing despite challenging times*, Feb. 2022. [Online]. Available: https://www.hms-networks.com/news-and-insights/news-from-hms/2022/05/02/industrial-networks-keep-growing-despite-challenging-times (visited on 02/10/2023).

[27] S. S. Thale, R. G. Wandhare, and V. Agarwal, "A Novel Reconfigurable Microgrid Architecture With Renewable Energy Sources and Storage," *IEEE Transactions on Industry Applications*, vol. 51, no. 2, pp. 1805–1816, Mar. 2015, Conference Name: IEEE Transactions on Industry Applications, ISSN: 1939-9367. DOI: 10.1109/TIA.2014.2350083.

[28] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the Modbus protocols," en, *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, Dec. 2008, ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2008.08.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187454820800005X (visited on 02/09/2023).

[29] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, Conference Name: IEEE Internet of Things Journal, ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2703172.

[30] I. Nai Fovino, A. Carcano, M. Masera, and A. Trombetta, "An experimental investigation of malware attacks on SCADA systems," en, *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 139–145, Dec. 2009, ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2009.10.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548209000419 (visited on 04/23/2023).

[31] "Communication networks and systems for power utility automation - Part 1: Introduction and overview," English, French, International Electrotechnical Commission, Tech. Rep. IEC TR 61850-1:2013, Mar. 2013. [Online]. Available: https://webstore.iec.ch/publication/6007 (visited on 02/03/2023).

[32] *IEC 61850: Core standards for the smart grid*, en. [Online]. Available: https://www.iec.ch/blog/iec-61850-core-standards-smart-grid (visited on 06/20/2023).

[33] "Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes," English, French, International Electrotechnical Commission, Tech. Rep. IEC 61850-7-4:2010+AMD1:2020 CSV, Feb. 2020. [Online]. Available: https://webstore.iec.ch/publication/66551 (visited on 04/23/2023).

[34] *Datasets and Report control blocks*, en, topic. [Online]. Available: https://www.winccoa.com/documentation/WinCCOA/3.18/en_US/IEC61850/IEC61850_basics/IEC-03.html (visited on 04/24/2023).

[35] "Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines," English, French, International Electrotechnical Commission, Tech. Rep. IEC TR 61850-90-4:2020, May 2020. [Online]. Available: https://webstore.iec.ch/publication/64801 (visited on 04/23/2023).

[36] R. Mackiewicz, "Overview of IEC 61850 and Benefits," in *2006 IEEE PES Power Systems Conference and Exposition*, Oct. 2006, pp. 623–630. DOI: 10.1109/PSCE.2006.296392.

[37] "IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)," *IEEE Std 1815-2010*, pp. 1–775, Jul. 2010, Conference Name: IEEE Std 1815-2010. DOI: 10.1109/IEEESTD.2010.5518537.

[38] X. Lu, W. Wang, and J. Ma, "An Empirical Study of Communication Infrastructures Towards the Smart Grid: Design, Implementation, and Evaluation," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 170–183, Mar. 2013, Conference Name: IEEE Transactions on Smart Grid, ISSN: 1949-3061. DOI: 10.1109/TSG.2012.2225453.

[39] S. East, J. Butts, M. Papa, and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," vol. 311, Mar. 2009, ISBN: 978-3-642-04797-8. DOI: 10.1007/978-3-642-04798-5_5.

[40] B. Zhu, A. Joseph, and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Oct. 2011, pp. 380–388. DOI: 10.1109/iThings/CPSCom.2011.34.

[41] *OCPP 2.0.1, Protocols, Home - Open Charge Alliance*. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/ (visited on 02/09/2023).

[42] *Open Charge Alliance - Global Platform For Open Protocols*. [Online]. Available: https://www.openchargealliance.org/ (visited on 04/22/2023).

[43] *OSCP 2.0, Protocols, Home - Open Charge Alliance*. [Online]. Available: https://www.openchargealliance.org/protocols/oscp-20/ (visited on 04/22/2023).

[44] C. M. Portela, "OSCP - An open protocol for smart charging of Electric Vehicles," en, 2015.

[45] *OpenADR 2.0 Specification*. [Online]. Available: https://www.openadr.org/specification (visited on 02/09/2023).

[46] *About OpenADR*. [Online]. Available: https://openadr.memberclicks.net/overview (visited on 04/23/2023).

[47] "Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response," English, French, International Electrotechnical Commission, Tech. Rep. IEC 62746-10-1:2018, Nov. 2018. [Online]. Available: https://webstore.iec.ch/publication/26267 (visited on 04/23/2023).

[48] *OpenADR Case Study- Distributed Energy Resources Sunpower Virtual Power Plant*. [Online]. Available: https://openadr.memberclicks.net/assets/OpenADR%20Case%20Study%20Sunpower%20Final.pdf.

[49] "Telecontrol equipment and systems - Part 5-101: Transmissionprotocols - Companion standard for basic telecontrol tasks," English, French, International Electrotechnical Commission, Tech. Rep. IEC 60870-5-101:2003+AMD1:2015 CSV, Nov. 2015. [Online]. Available: https://webstore.iec.ch/publication/23822 (visited on 04/14/2023).

[50] "Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standardtransport profiles," English, French, International Electrotechnical Commission, Tech. Rep. IEC 60870-5-104:2006+AMD1:2016 CSV, Jun. 2016. [Online]. Available: https://webstore.iec.ch/publication/25035 (visited on 04/14/2023).

[51] *Introduction to the IEC 60870-5-104 standard – ENSOTEST*, en-US. [Online]. Available: https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard/ (visited on 02/23/2023).

[52] L. Erdődi, P. Kaliyar, H. Siv, A. Akbarzadeh, and A. Waltoft-Olsen, "Attacking Power Grid Substations: An Exper-iment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104," Aug. 2022. DOI: 10.1145/3538969.3544475.

[53] *HELINKS STS System Integrator (V3.8.0.9)*, 2020. [Online]. Available: https://www.helinks.com/products-services/ (visited on 05/23/2023).

[54] *OMICRON IEDScout (V5.12)*, 2022. [Online]. Available: https://www.omicronenergy.com/en/products/iedscout/ (visited on 05/26/2023).

[55] *MGate 5119 Series - Modbus TCP Gateways*, en-us. [Online]. Available: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5119-series (visited on 05/26/2023).

[56] T. Hwang, Y.-S. Yoo, S. Kang, and I. Lee, "Design of an IEC 61850 Based Communication System for DER Management," Nov. 2014.

[57] C.-H. Liu and J.-C. Gu, "Modeling and Integrating PV Stations into IEC 61850 XMPP Intelligent Edge Computing Gateway," *Energies*, vol. 12, p. 1442, Apr. 2019. DOI: 10.3390/en12081442.

[58] "Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in power utility automation systems related to IEDs," English, French, International Electrotechnical Commission, International Standard IEC 61850-6:2009+AMD1:2018 CSV, Jun. 2018. [Online]. Available: https://webstore.iec.ch/publication/63319 (visited on 05/22/2023).

[59] "Communication networks and systems for power utility automation - Part 7-1: Basic communication structure - Principles and models," English, French, International Electrotechnical Commission, Tech. Rep. IEC 61850-7-1:2011+AMD1:2020 CSV, Aug. 2020. [Online]. Available: https://webstore.iec.ch/publication/67536 (visited on 04/26/2023).

[60] "Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)," English, French, International Electrotechnical Commission, Tech. Rep. IEC 61850-7-2:2010+AMD1:2020 CSV, Feb. 2020. [Online]. Available: https://webstore.iec.ch/publication/66525 (visited on 05/22/2023).

[61] "Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes," English, French, International Electrotechnical Commission, Tech. Rep. IEC 61850-7-3:2010+AMD1:2020 CSV, Feb. 2020. [Online]. Available: https://webstore.iec.ch/publication/66526 (visited on 05/22/2023).

[62] "Communication networks and systems for power utility automation - Part 3: General requirements," International Electrotechnical Commission, Tech. Rep. IEC 61850-3:2013, Dec. 2013. [Online]. Available: https://webstore.iec.ch/publication/6010 (visited on 05/22/2023).

[63] *IEC 62443*, en-US. [Online]. Available: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/ (visited on 04/27/2023).

[64] *Specifications - SunSpec Alliance*, en-US, Apr. 2021. [Online]. Available: https://sunspec.org/specifications/ (visited on 04/26/2023).

[65] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, Apr. 2018, Conference Name: IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003). DOI: 10.1109/IEEESTD.2018.8332112.

Appendix A

Additional Logical Node — Thermal Management System

One of the crucial components for a BESS is the TMS. The TMS is responsible for the thermal control within the system. Depending on the components utilized, and their respective cooling method, such system can be responsible for thermal management of components such as; the PCS (the power converters), the power transformer, and the battery system (modules or packs, etc.). For mobile applications, where the deployment area can vary quickly and transportation can occur quite often, the control and monitoring of TMS is of utmost importance. Since the IEC 61850-7-420 standard does not provide a LN for such a system, a proposal is presented here, the LN **DTMS**. A table of the suggested data objects is formulated, see Table A.1.

The suggestion accounts for TMS as used for mobile and flexible solutions. Where the specific devices in such BESS could be physically distant, or in their own enclosures. Like the VMS and its PCS enclosure and modular battery enclosure. Thus, depending on the operations, multiple TMSs can be present in one mobile BESS DER. For example, one for PCS (LN **DINV**), and one for physical battery (LN **DBAT**). Thus, the proposed **DTMS** refers to its connected cooling equipment with a DO `ECoolRef`, of CDC type *ORG*. Other DOs suggested for a TMS are described in the DO table for **DTMS**, see Table A.1. The two new literals (enumeration kinds) proposed are given in a tables, respectively. *TMSStateKind*, representing the operating state of TMS is shown in Table A.2. *TMSControlStrategyKind*, representing the control strategy setting of the TMS, what it is supposed to control based on, is shown in Table A.3.

DTMS				
Data object name	**Common Data Class**	**T**	**Explanation**	**PresCond nd/ds**
Descriptions				
EEName	DPL		(inherited from: ControlEquipmentInterfaceLN) Name plate of external (electrical, mechanical or communication) equipment to which the logical node is associated.	O /F
NamPlt	LPL		(inherited from: DomainLN) Name plate of the logical node.	MONamPlt / MONamPlt
Status information				
CompSt	SPS		Compressor state	O /O
PmpSt	SPS		Pump state	O /O
HeatSt	SPS		Heater state	O /O
TMSOpSt	ENS (TMSStateKind)		Current state of operation of the thermal management system	M /M
ClLoAlm	SPS		Coolant level low alarm	O /O
ClTmpHiAlm	SPS		Coolant high temperature alarm	O /O
ClTmpLoAlm	SPS		Coolant low temperature alarm	O /O
Beh	ENS (Behaviour-ModeKind)		(inherited from: DomainLN) Read-only value, describing the behaviour of a domain logical node. It depends on the current operating mode of the logical node ('DomainLN.Mod'), and the current operating mode of the logical device that contains it ('LLN0.Mod'). Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of 'DomainLN.Beh'.	M /M
Health	ENS (HealthKind)		(inherited from: DomainLN) Reflects the state of the logical node related hardware and software. More detailed information related to the source of the problem may be provided by specific attribute of the logical node.	O /O
Measured and metered values				
VolHVBus	MV		Voltage (DC) between poles	O /O
InClTmp	MV		Intake coolant temperature	O /O
OutClTmp	MV		Outlet coolant temperature	O /O
FanSpdPct	MV		Fan speed	O /O
EnvTmp	MV		Ambient temperature	O /O

DTMS				
Data object name	**Common Data Class**	**T**	**Explanation**	**PresCond nd/ds**
EETmp	MV		External electronics temperature	O /O
WTot	MV		Total power consumption of the thermal management system	O /O
Controls				
ClSpt	APC		Cooling setpoint	O /O
TMSSt	SPC		Thermal management system start operation	M /M
CoolAuth	SPC		Cooling authorization	O /O
HeatAuth	SPC		Heating authorization	O /O
Settings				
ECoolRef	ORG		Reference to the equipment being cooled by the thermal management system, such as DINV, DBAT etc...	Mmulti /F
FanSpdMinPct	ASG		Minimum fan speed	O /O
ClTmpHiAls	ASG		Coolant high temperature alarm threshold	O /O
ClTmpLoAls	ASG		Coolant low temperature alarm threshold	O /O
CntMeth	ENG (TMSControl-StrategyKind)		Thermal management system control strategy	O /O

Table A.1: Data objects of DTMS.

TMSStateKind		
enumeration item	**value**	**description**
initialization	1	Initialization of the TMS controller
standby	2	Standby and ready for operation
pre-heating	3	Pre-heating before operation
running with cooling	4	Operating at normally
shutdown	5	Shutting down operation
Not applicable or not known	98	Not applicable or not known

Table A.2: Literals of TMSStateKind.

TMSControlStrategyKind		
enumeration item	**value**	**description**
Coolant temperature control	1	Controlling based on coolant temperature, valid for the setpoint given
External electronics control	2	Cooling based on temperature measurements of electronics (power electronics, battery cells etc.), valid for setpoint given

Table A.3: Literals of TMSControlStrategyKind.

TRITA-EECS-EX- 2023:586