Vaasan yliopisto
UNIVERSITY OF VAASA

Technical Report TR 3.1
IEC 61850 communication Solution for Digital Energy Systems and Beyond
10th June 2021

Mike Mekkanen

Vaasa 2021

Programme for Sustainable Growth and Jobs
Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Contents

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Executive Summary[TV1]

The advancement of technology and standards that merge to power system operation has a significant impact on utility performance and design. For example, IEC 61850 standard, which is still relatively new and at the initial stages of implementation, provides practical advances in terms of more measured and calculated real-time data for power system control and operation purposes. According to the IEC 61850 standard, this real-time data is available and may be utilized in different subscriber IEDs located in various levels/areas. IEC 61850 is an essential enabler of solutions such as harmonized data communication, a high-interoperability framework, and network cyber security.

The topic of standardization of energy system communication is addressed in this report, with a focus on smart grid. The primary goal of this work is to introduce a comprehensive guideline that compiles all the necessary energy system standardization (IEC 61850 standard) concepts and practices in one place, thereby assisting professionals from both industry and academia in the energy sector in implementing various levels of communication network. The report focuses primarily on three perspectives: standardization of all energy system entities and functions, building various levels of IEC 61850 data model and finally interfacing these different data models based on predefined protocols and optimized topology. The report begins with the introduction, fundamentals of standardization, then concludes with the IEC 61850 communication interface/protocols and best practices for adding value to modern energy system operation.

Furthermore, due to the complexity of starting with the IEC 61850 standard, it may be a clever idea to study the IEC standards outline documents first and then move on to more advanced topics based on your needs, as the IEC 61850 standards cover a wide range of topics. As a result, standards with relevant themes are listed in this report to address standard issues and improve learning effectiveness.

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

1 Introduction

Today's power system infrastructure lacks coordination among various operational entities, while being based on the needs of the traditional power industry several decades ago. The existing infrastructure separates various subsystems, data and information sharing is limited i.e., resulting in high-cost operation, more losses and slow/delayed supply restoration. At this point, for any subsequent system activity, exchanging real-time information becomes a primary duty. Real-time information needs to be exchanged quickly and precisely between e.g., substation IEDs and even with other substations, which necessitated the integration and consolidation of IEDs in substations/systems. This endeavor necessitates the use of a communication standard to standardize the communication language between IEDs based on syntax and semantics to assure the interoperability between multivendor IEDs and make the IEDs integration/interfaces more user-friendly. The conventional power system communication solutions are even so simple that they could not handle/support fully the smart electrical system operation functionality or they have reached their technical limits.

1.1 Motivation [TV2]

This report is an instructive specialized on details which can help maintaining the nominative framework operation guidelines. It will emphasis the information interchange among the facility of energy system producing or consuming units, as well as along with the operators outside the facility in standardized way. Figure 1 illustrates the separated areas by the red line based on inter/intra communication interfaces among the energy system entities. This report's primary audience will be technical personnel from either the academia or industry who need an overview of the concept and use of standards in this industry.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

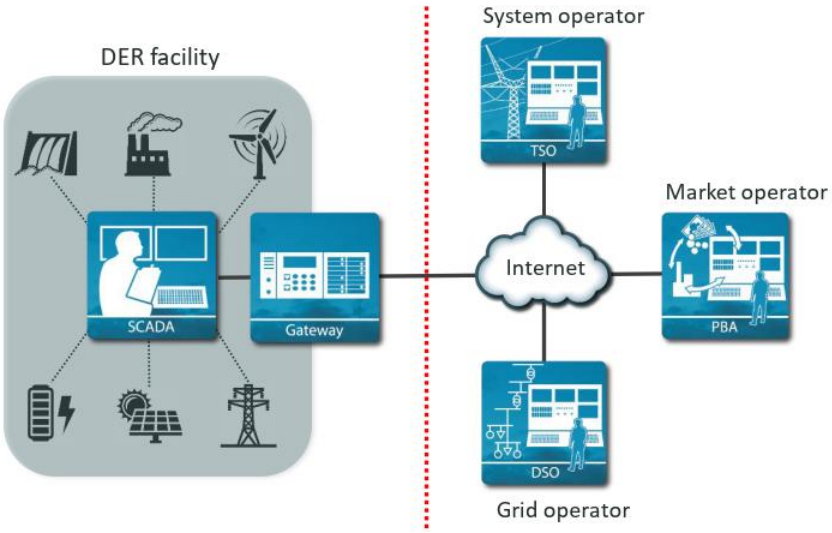

Figure 1. Inter and intra communication interfaces among energy system entities (facilities and operators).

1.2 The Need of Standard and Why IEC 61850?

For more than a century, data communication has been available. Many protocols have been established for a variety of applications, Thus the question that might arise is why IEC 61850? To start with let us have a look at the challenges,

- In terms of energy balance, power losses, and power quality, the current global increase of renewable energy resources e.g., wind turbines, photovoltaics etc., poses a challenge for the power system.
- Power production from centralized sources is while the amount of distributed generation from smaller units is increasing.
- Energy markets are deregulating, adding new services/features such as ancillary services, and requiring faster control loops.
- Power import/export across borders between countries and regions becoming increasingly crucial in ensuring supply security.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

- Power system is a critical infrastructure becoming more interesting target for cyber threats.

Even though IEC 61850 does not have a solution for all these challenges, it is an important part of the solutions providing a harmonized data exchange, framework with a high degree of interoperability, and network cyber security.

Subsequently to keep addressing the starting inquiry why IEC 61850, it fosters a remarkable unique naming for data information model, given in a full UML format, has been accepted/suggested by driving companies, utilities, and other organizations internationally, and supports in a future proof way all the power system operation/maintenance issues. Even the European SmartGrid Taskforce with their M490 mandate focuses to IEC 61850 as the standard to utilize for information exchange in the Smart Grid area. A more detailed description of the IEC 61850 is given in the following chapter.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

2 IEC 61850 Standard

IEC 61850 is an international standard for the secure data transfer inside a power system and beyond.

Originally intended for substation automation within the first version, while currently it encompasses Distributed Energy Resources (DER) as well as Information Security — all under the same IEC TC57 framework as illustrated in Figure 2.

IEC 61850 is an Information Model that establishes a unique naming standard for all the building pieces inside the power system and DER facility. It is more than just a protocol for sending a block of data between two places. It is a cyber-information system that enables with all areas of energy system operation and protection.

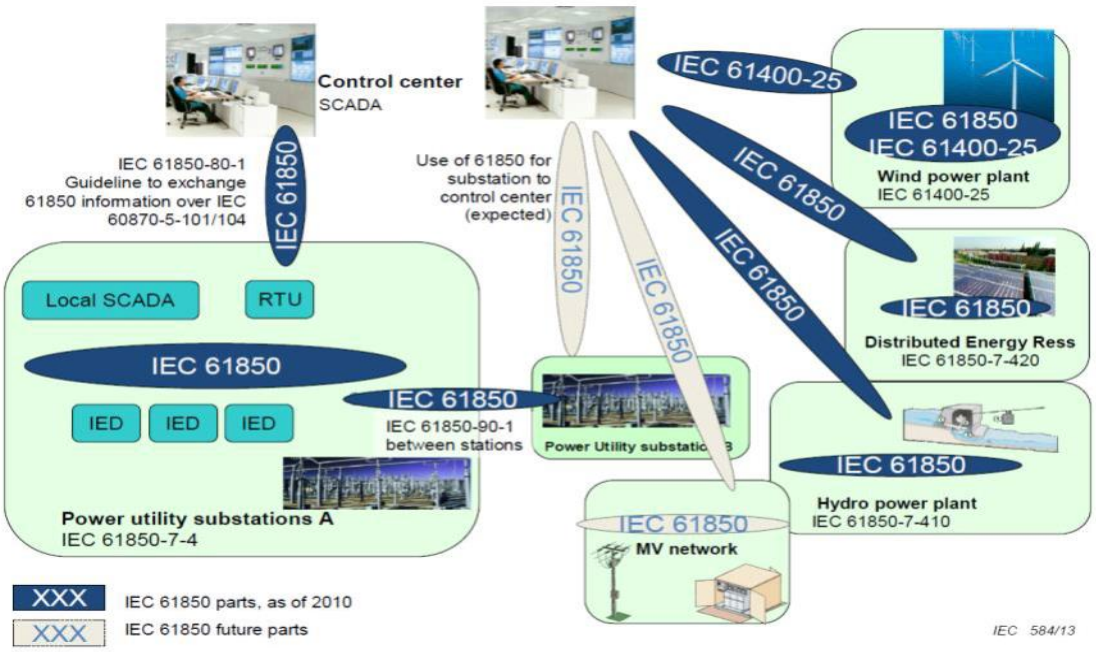

Figure 2. IEC 61850 Scope

2.1 IEC 61850 Standard History

IEC 61850 has been developed over more than 20 years and has been widely accepted worldwide. In the beginning, the Utility Communication Architecture UCA concept had been raised by the Electrical Power Research Institute EPRI and IEEE at early 1990s. The

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

idea behind this work was to identify the requirements, structure and specific communication technologies that can be used to implement the standardization scheme. This standardization approach for electrical system communication might support/suitable for modern electrical system operation functionality and their future extending. The first version was concentrated on vertical communication, interfaces between substation entities to the control center. as well as among the upper levels different control centers.

Next phase of UCA was UCA 2.0, which was released in 1994. The main approach was to define the substation's communication bus. The UCA architecture comprised of data object on the top layer application layer. Service interface was the middle layer in which provided basic tasks such as defining, retrieving, and logging of process data. In the bottom there was the communication profile's layer.

On the other hand, in 1996 Technical Committee 57 of the IEC starts its work on IEC 61850 for the same concept. The two groups agreed to merge their works and work together to define the IEC 61850 standard as the common international standard in 1997. Resulting the harmonization process the current IEC61850 standard specifications was provided as illustrated in Figure 3.

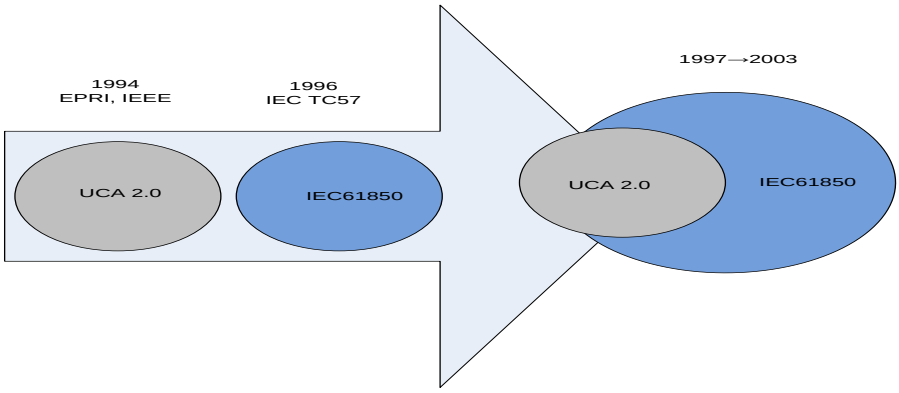

Figure 3. Two groups merge their works.

The IEC 61850 standard is a superset of the UCA 2.0 beside offering additional features that support/handle the modern digital electrical system operation functionality. The first version of the IEC 61850 standard had been published as an international standard in 2003. Figure 4 illustrates the release of the first version and the following IEC 61850 drafts that cover the electrical system operation/communication issues.

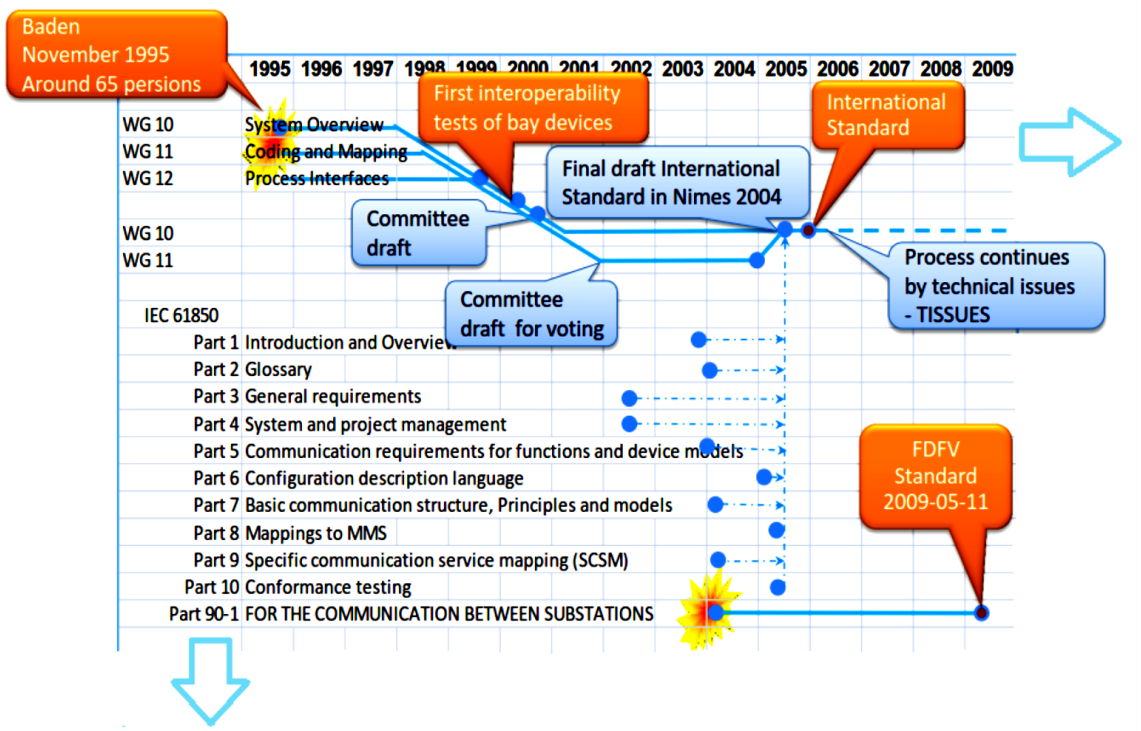

Figure 4. IEC 61850 standard

2.2 IEC 61850 Overview and Basic Concept

Today, the IEC61850 standard has emerged as one of the most promising and strong solutions to the current power industry's restrictions, and it is expected to aid in the growth of power systems. However, the IEC61850 standard's initial focus was on substation automation and protection. The main aspect is that it establishes a consistent structure for all associated system levels. IEC61850 considers all the common components of a substation site, including data models, communication solutions, engineering, and conformity testing. Legacy protocols, on the other hand, focus on how data is conveyed through the channel while organizing the data in terms of applications by means of syntax and semantics within the devices is left without consideration.

The major feature of the IEC61850 is that its "abstracts" data object specification and services based on its architectural design. Creating data objects and services that support a full set of substation functions and provide robust services to facilitate substation communication is independent of any underlying protocol. Because IEC61850 did not

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

specify any communication protocol, the abstract definitions of the data object allow it to be mapped to any protocol that can match the optimal data and service needs. IEC 61850 focuses on three significant areas as listed in the following:

- Standardizes the available information (data object model), substation functions (functional model) and equipment's name.
- Defines diverse ways of the accessing scheme to the available data (communication service modeling) and specifies the mapping scheme to the communication services and to several protocols.
- Defines a language (XML) implemented to describe all the configuration information exchanged between IEDs, network and power system.

2.3 IEC 61850 First Vison and Scope

The scope of the IEC61850 is composed of 10 major parts that together define the various aspects and all the requirements that must be fulfilled by substation automation systems. The main goal is to achieve interoperability between IEDs within the substation as illustrated in Figure 2.

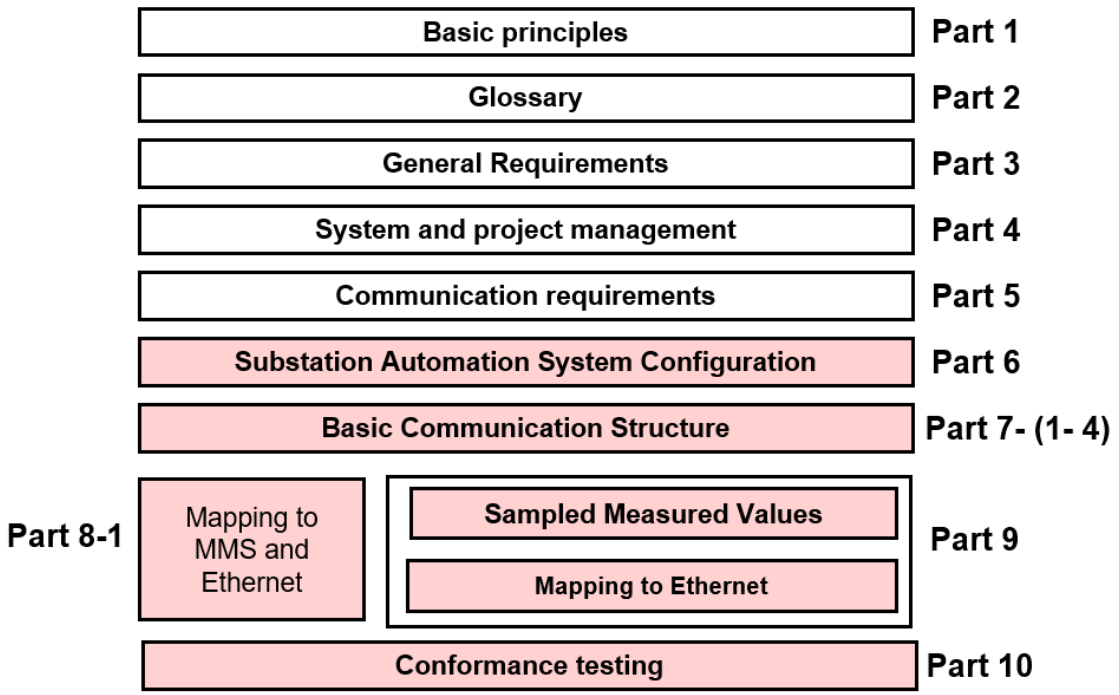

Figure 5. IEC 61850 standard Structure

The first parts from 1 to 5 are the introduction, glossary, general requirements, project management and some of the communication requirements. While, for the digital substation, the most important parts of the standard series are parts 6, 7, 8 and 9 related to telecommunication-based communication as illustrated in Figure 5. At this point the report will outline the content of these sections as they are relevant to the scope of this report.

- **IEC 61850-6** deals with the configuration of a substation automation system so that devices from different venders operate in the same manner within system. To this end, the standard defines the file formats in which IED device configurations, parameters, telecommunication system configurations, switching device functions and the connections between them can be presented. The format created is Extensible Markup Language (XML) based System Configuration description Language (SCL).
- **IEC 61850-7** with its sub-parts defines the architecture for communication between substation devices such as protection relays and circuit breakers. It defines the communication and information model principles also mapping scheme. To this end, the Abstract Communication Service Interface (ASCI), Common Data Classes (CDC) data classes and their corresponding logical nodes are defined to model device properties. It also specifies the data classes regarding syntax and semantics.
- **IEC 61850-8** describes the communication mapping for the entire system which specify how the models and services specified in IEC 61850-7-x series are to be transmitted via the communication network in accordance with the generic object-oriented substation event GOOSE and Manufacturing Message Specification MMS protocols.
- **IEC 61850-9** describe the point-to-point unidirectional communication mapping services. Also, it introduces the Sampled Values (SV) protocol used in the process bus, for example, the measurement data of substation measuring transformers

can be transferred via process bus to the IED devices. SV traffic is configured according to the ISO / IEC 8802-3 Ethernet standard. In addition, the section introduces SCSM, which determines how SV traffic travels according to the IEC 61850-7-2 specification. However, the standard set too loose frames for the devices themselves, which use the SV protocol for communication, resulting in devices from different vendor not working together as desired. To this end, the UCA International Users Group published the Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2, more commonly known as IEC 61850-9-2LE (Light Edition). IEC 61850-9-2LE specifies how devices that communicate according to the IEC 61850-9-2 SV protocol should be specified, for example, in a situation where the standard provided alternatives to device manufacturers. The purpose is to ensure that devices from different manufacturers work together. In addition, it specifies the time synchronization requirements according to the IEC 61588 standard.

- **IEC 61850-10** it specifies the implementations conformance testing techniques and the declaring performance parameters measurements techniques.

2.4 The Best Way to Read the Standard

If the end-user has no related knowledge with IEC 61850 and related standards and needs to get some knowledge concerning the IEC 61850 from an administrator and system integrator point of view – it might be a brilliant idea in any case read the IEC 61850 standard outline at first and later make a forward steps for more advance topics, consequently to handle the difficulties of the standard and make the perusing more helpful, archive of the standard parts on relevant subject gatherings is more than required. From this point of view the IEC 61850 and related standards are grouped together under the suitable headings in the following.

1- General information including basic terms and definition
    - IEC 61850 Part 1: Introduction and overview
    - IEC 61850 Part 2: Glossary
    - IEC 61850 Part 3: General requirements
    - IEC 61850 Part 4: System and project management

- IEC 61850 Part 5: Communication requirements for functions and device models
- IEC/TS 62351-1: Introduction
- IEC/TS 62351-2: Glossary of Terms
- IEC/TR 62351-12: Resilience and Security Recommendations for Power Systems with DER

2- Configuration and guidelines

- IEC 61850 Part 6: Configuration description language for communication in electrical substations related to IEDs
- IEC 61850 Part 90-1: Use of IEC 61850 for the communication between substations
- IEC 61850 Part 90-2: Using IEC 61850 for the communication between substations and control centers
- IEC 61850 Part 90-3: Using IEC 61850 for condition monitoring
- IEC 61850 Part 90-4: Network Engineering Guidelines - Technical report
- IEC 61850 Part 90-5: Using IEC 61850 to transmit synchro phasor information according to IEEE C37.118
- IEC/TR 62351-13: Guidelines on What Security Topics Should Be Covered in Standards and Specifications
- IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles

3- Information model

- IEC 61850 Part 7-1: Basic communication structure – Principles and models
- IEC 61850 Part 7-3: Basic communication structure – Common data classes
- IEC 61850 Part 7-4: Basic communication structure – Compatible logical node classes and data classes
- IEC 61850 Part 7-410: Hydroelectric power plants – Communication for monitoring and control

- IEC 61850 Part 7-420: Basic communication structure – Distributed energy resources logical nodes
- IEC 61850 Part 7-5: IEC 61850 – Modelling concepts
- IEC 61850 Part 7-500: Use of logical nodes to model functions of a substation automation system
- IEC 61850 Part 7-510: Use of logical nodes to model functions of a hydro power plant
- IEC 61850 Part 7-520: Use of logical nodes to model functions of distributed energy resources
- IEC 61850 Part 90-7: Object models for power converters in distributed energy resources systems
- IEC 61850 Part 90-8: Object Model for E-Mobility – now a joint activity (JWG11) with IEC TC69
- IEC 61400-25-4: Basic communication structure for Wind Turbines as, Wind turbines – Communications for monitoring and control of wind power plants

4- Protocols and services

- IEC 61850 Part 7-2: Basic communication structure – Abstract communication service interface (ACSI)
- IEC 61850 Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
- IEC 61850 Part 8-2: Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping
- to Extensible Messaging Presence Protocol (XMPP)
- IEC 61850 Part 80-1: Guideline to exchange information from a CDC based data model using IEC 60870-5-101/104
- IEC 61850 Part 80-4: Translation from COSEM object model (IEC 62056) to the IEC 61850 data model

- IEC 61850 Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3

5- Conformance testing

- IEC 61850 Part 10: Conformance testing
- IEC 62351-100-1: Conformance test cases for IEC 62351-5 and companion standards

6- Cyber security

- EC/TS 62351-3: Security for profiles including TCP/IP
- IEC/TS 62351-4: Security for profiles including MMS
- IEC/TS 62351-6: Security for IEC 61850 profiles
- IEC/TS 62351-7: Objects for Network Management
- IEC/TS 62351-8: Role-Based Access Control
- IEC/TS 62351-9: Key Management
- IEC/TS 62351-10: Security Architecture
- IEC 62351-14 Security Event Logging and Reporting
- IEC/TR 62351-90-2 Deep Packet Inspection

Note: This report is using the latest information about the IEC 61850 standards draft versions from the IEC 61850 available drafts and webpage, which means that the descriptions in the section of the report about IEC 61850 standards can change since the IEC 61850 draft standards are subject to be withdrawn, mandate or updated.

2.5 Practical Tips on How to Get Started

There may be numerous methods to begin depending on your motive for using the IEC 61850 standard, whether you are a project requirements/operator engineer inside facility or project design engineer outside facility or IED parameterizing-system integrator engineer. Depending on your role peruse the suggestions that will be the most ideal choice for particular purpose. Figure 6. shows a simplified allocation of the distinct roles based on the tasks-oriented specification.

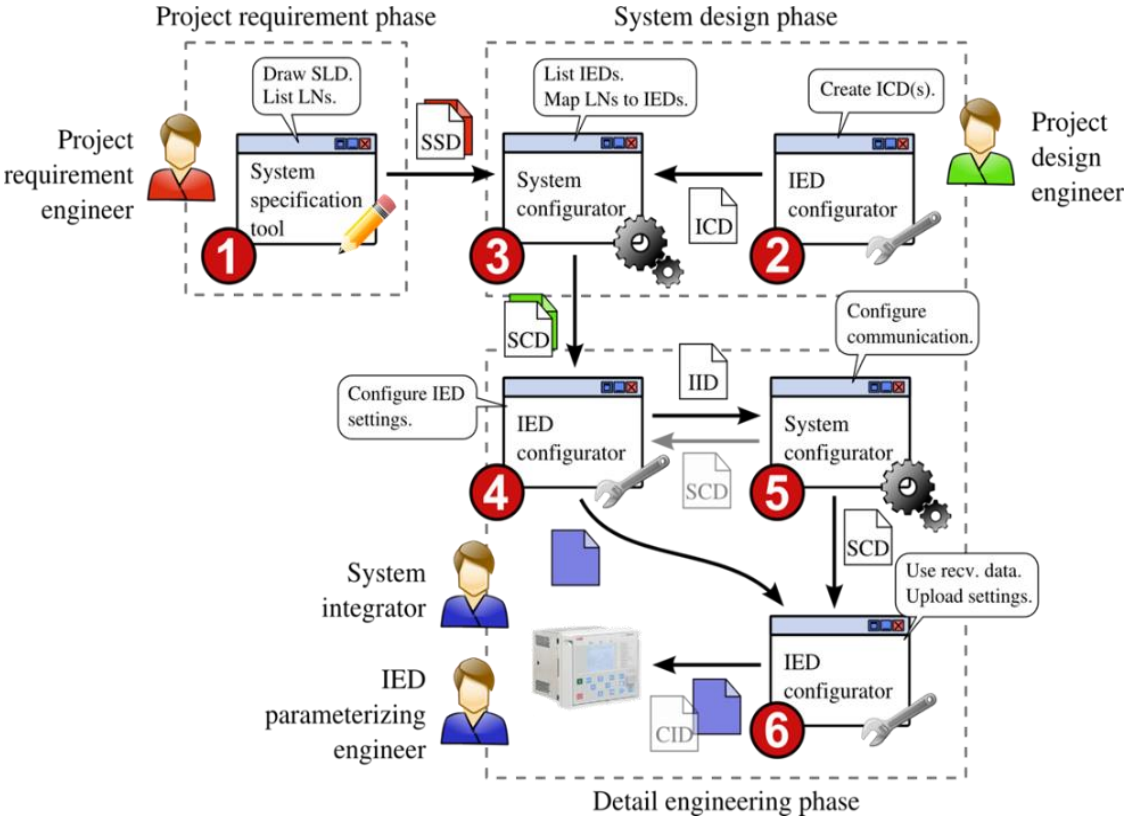

Figure 6. End-user roles allocation at System and IEDs Design, Configuration, and Integrations (DEMVE project materials)

Thus, if you are a project requirements/operator engineer inside facility, the key role will consistently be on operating/protecting the assets and providing optimal production as well as associations with other facilities for more collaboration and get benefit from the add-on services and the developed energy market. In particular and based on the data transfer point view, secure/shared access to information is one from the most critical issue that may require more consideration and oversaw by the specialist inside facility as the facility is the data originator and owner.

While if you are IED parameterizing-system integrator engineer, the key role will consistently be on having a good overview and knowledge for the other systems that need to be integrated, avoiding proprietary solutions, and following the most common solution that should be based on the international standard e.g., IEC 61850. This will reduce cost and tackle the difficulties of the integration task. Also recruiting-training personal for one solution is more beneficial and cost-efficient benefitting at the end the business revenue.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Consequently, if you are project design engineer outside facility, regardless of whether you are from system operator, grid operator or even market operator the normal issue divided between them is if the DER facility is a confided as a resource both from a DER asset and security perspective. Were the system operator will consider the security supply issues, market operator will consider the collaboration of DER facilities in market terms. Aggregator will consider the controllability issues of different DER facilities and the grid operator will consider power quality management by using different DER facilities to balance between power generation and load consumption in a way to improve grid stability while keeping in mind that end-to-end security should be mandatory within the different association levels.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

3 IEC 61850 Technical Specifications

In this part of the report, general IEC 61850 technical specification will be presented, regarding IEC 61850 standard information model construction, communication protocols specifications, different power system topologies, synchronization, redundancy, and design-configuration for utility communication-automation IEDs and systems in power grid environment.

3.1 IEC 61850 Standard Information Model Specifications

Information model is a critical part of the IEC 61850 standard. This is a naming standard that specifies unique names for all the power system entities functionalities and components. The IEC61850 information model is hierarchically arranged, with logical nodes serving as the model's most essential elements. To allow for flexible configuration amongst IEDs within the substation, modeling is done in a consistent manner. It virtualizes physical devices in a substation to a logical device LD. This LD host, collect and group different logical nodes LNs based on its role. A distributed function is a single function that can be separated into many LNs that are placed in separate physical devices. On this end, LN can be defined as a small software that could exchange data.

To conduct the application in the substation, the hierarchical information modeling can be classified into five levels. There is an inheritable link between the levels. One or more physical devices can be defined in a substation, each of which can have zero or many servers, but usually at least one. According to the hierarchical data model, the server object is situated at the top, as shown in Figure 7, and may have one or more access points.

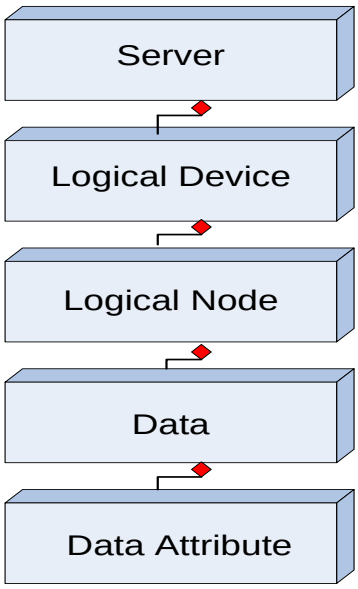

Figure 7. Hierarchy of IEC641850 data model

Characterizing LD and server are openly up to the producers or IEDs parametrizing engineer (see part 2.5) of the substations. While the LNs are predefined within the standard the fact that creates LNs the foremost vital point of the information model. Based on this confinement interoperability between IEDs from deferent producer can be achieved. Subsequently, the information entities within the substation are classified into different distinctive groupings of data. Concurring to this classification all the substation information can be doled out to one of these groups e.g., the metering measurements data information gather in group start with “M” and protection data grouped is begun with “P” etc. In addition, the LNs which are named based on its associated services that are logically related to functions in substation/DERs. LNs can be defined into diverse types. For instance, “Switchgear” function group which started with “X” comprises two different LNs “XCBR” and “XSWI.” Each LN is constructed by seven categories of data classes such as status information, measured information etc. Each one from the data classes consist of several data attributes, as we have many different data attributes that has a defined name, defined type and specific purpose as illustrated in Figure 8.

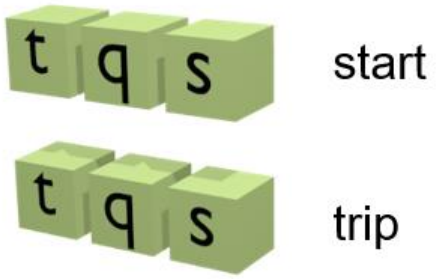

Figure 8. IEC641850 data model start and trip data attributes

Browsing to individual objects may be easy based on this model from the fact that the data object is named by means of its place and path in the information tree. For instance, as in Figure 9., from the left to the right the first name is the device name, the second part represents the LN. The third part is a functional constrains which is used to group the individual attribute that has predefined function based on its functionality, as in our example "ST" stand for status attributes. Last "stVal" contains the value of the status.

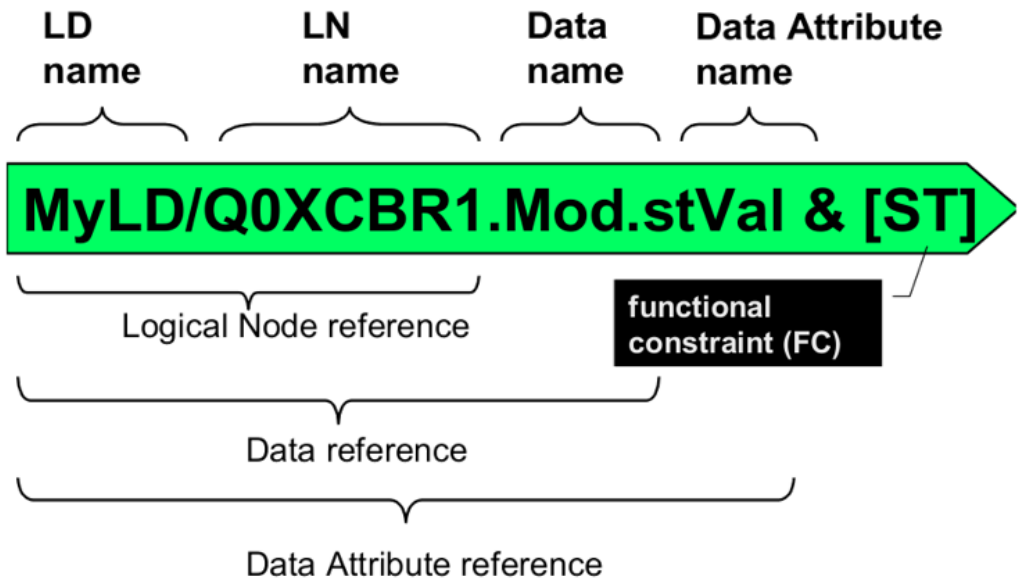

Figure 9. IEC61850 Object Name Structure.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

3.1.1 Logical Nodes, Logical Devices and Physical Devices Concepts

The IEC61850 standard defines the LN concept that can be considered as having a significant role in the standard. This role is achieved through a virtualization concept. The virtualization concept allows the standard to virtualize whole power system actual IEDs and functions into the related information model.

This information model comprises of various LNs that by a sensible conveyed portion can fabricate the consistent LD. The coherent LD is regularly executed in one actual physical device that cannot be distributed. Explicit function in power system that is regularly performed by various actual physical IEDs is called distributed function and the IEDs are called distributed IEDs. To carry out the appropriated function effectively the exchanging of data is needed between these IEDs. The interfaces are performed dependent on the IEC61850 standard correspondence rule as indicated by the clear-cut principles and the mentioned execution. These rules/guidelines permit interoperability between IEDS/systems from various vendors. Figure 10 illustrates the virtualization concept.

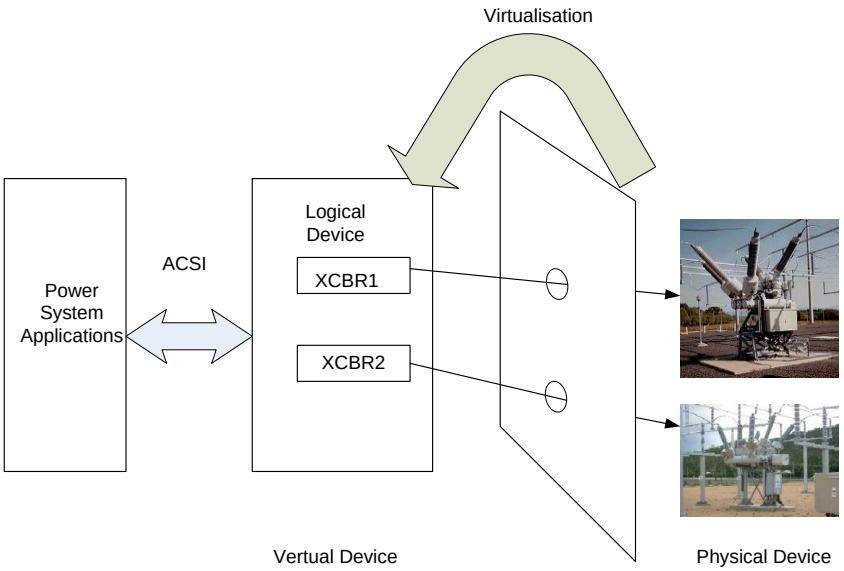

Figure 10. IEC61850 Object virtualization process.

To explain the concept of virtualizations the real physical substation devices in the right side from Figure 10., are modeled into a virtual model in the middle, where the virtual

model contains the LDs that host the LNs which encapsulate the real device and services. The data model and services with associated information are mapped to a network communication protocol such as MMS, TCP/IP, Ethernet etc.

3.1.2 LN Data Model Structure

The LNs according to their designed functionality may consist of a list of data with dedicated data attributes. The data have a predefined structure compliance with the IEC 61850 standard specifications (syntax and semantic). The LNs and the contained data are crucial for the description and information exchange in the substation automation system. Figure 11 illustrates more clearly the concepts of the LD, LNs, classes and data attributes mapped to the real world. It is start with container the physical device, which is containing one or more LDs, each one may contain one or more LNs that contain a set of data classes. The data classes may contain a set of data attribute.

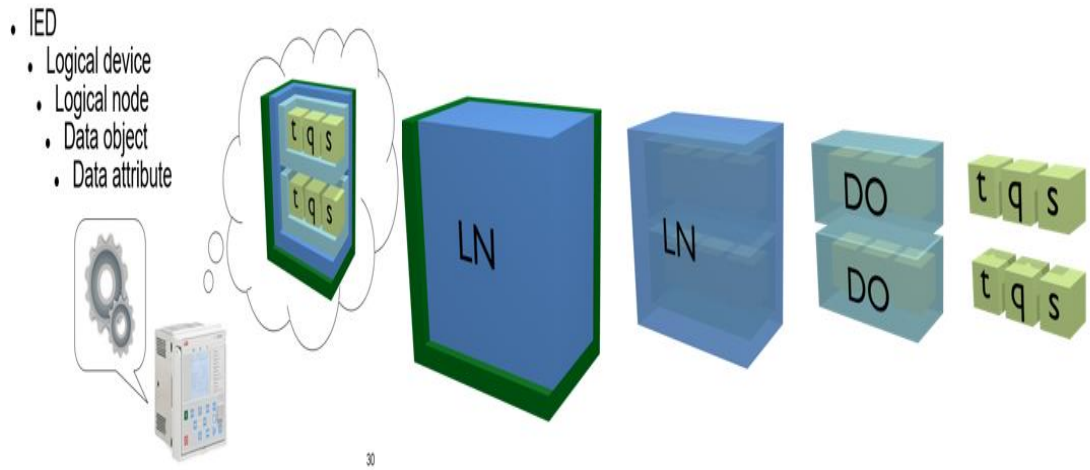

Figure 11. IEC61850 Data model grouping

The terms LD, LN and data object are all virtual which represents real data that been used for communication between physical devices. This data is hidden and

cannot access directly where this approach has advantages that the information modeling and the exchanging data are defined independently from the programing software, operating system, and storage devices.

3.2 IEC 61850 description Language (SCL)

According to IEC61850-6-1, a substation configuration language SCL is defined, which is based on eXtensible Markup Language XML. Before starting to work with a system configuration, a system integrator may need to setup the system devices, as well as add new devices to the system. Based on standardized XML files, the SCL specifies a hierarchy of configuration files that permits unambiguous definition of various levels of the system. It is a standardized way of describing the system's setup as well as the relationship between the system and the functions assigned to it. As a result, the SCL file format makes it possible to define communication and function related device capabilities, device parameters, communication system configuration, and system device allocation in a standardized manner. To build up the automation system, these descriptions files for the complete system and its devices can be transferred between devices, engineering tools, and different system engineering tools.

To achieve standardized system integration and configuration, such as in a substation, using the IEC61850 data model. SCL developed an object model that explains the communication connection and allocation of the IEDs, as well as how this object model may be published in a SCL file and communicated with system engineering tools. There are four different SCL file data formats described, and these files are exchanged across tools according to their requirements. They are built in the same way and with the same format, but their scope and extension are different.

All necessary information, such as substation network topology, IEDs description, communication system description, and data type templates, can be obtained from these files. Below is list of these file formats as well as their content,

- ICD: IED Capability Description. Describe the capabilities of an IED, IED allocation, IED communication description

- IID: Instantiated IED Description. Describe the configuration for an IED, standard parts of a configuration for an IED.
- SCD: System Configuration Description. Standard parts of a configuration for a substation, specify all IEDs, communication configuration and substation description, most complete, and most important file type.
- SSD: System Specification Description, describe the SAS and the required LNs for single-line diagrams
- CID: Configured IED Description-final configuration that can be used for writing configuration to IED.
- SED: System Exchange Description, describe the exchanging configuration between substations, set up data streams between substations.

For more information about these different SCL files in practical implementation at power system design, configuration and integration please see section 2.5. There is a figure showing steps how different SCL files could be exchanged between different system/IEDs configuration tools at different system integration phases.

3.3 IEC 61850 Digital Substation Levels

Digital substation classification could be divided into three hierarchical levels as illustrated in Figure 12. A substation's primary equipment, such as circuit breakers, power transformers, switchgears, etc., and their link elements, such as instrument CTs, VT transformers, circuit breakers, etc., represent the level one process level. Bay-level were IEDs allocated on this level, all the substation functionality, e.g., local operation, macro commands, centralized automatic functions, and incident recording, are performed. Further, for HMI with the SCADA center and with the managing engineering center of the utility, bay devices at this level may be represented as station level.

The communication system and logical interfaces defined by the IEC 61850 standard play a vital role in exchanging information and facilitates the implementation of substation functions. Further it can be considered as the glue that binds the substation levels to-

gether, creates interfaces inside and between substation levels. Communications networks may determine and define the performance, dependability, speed, and supported functionality of all systems, next more information about these logical interfaces.

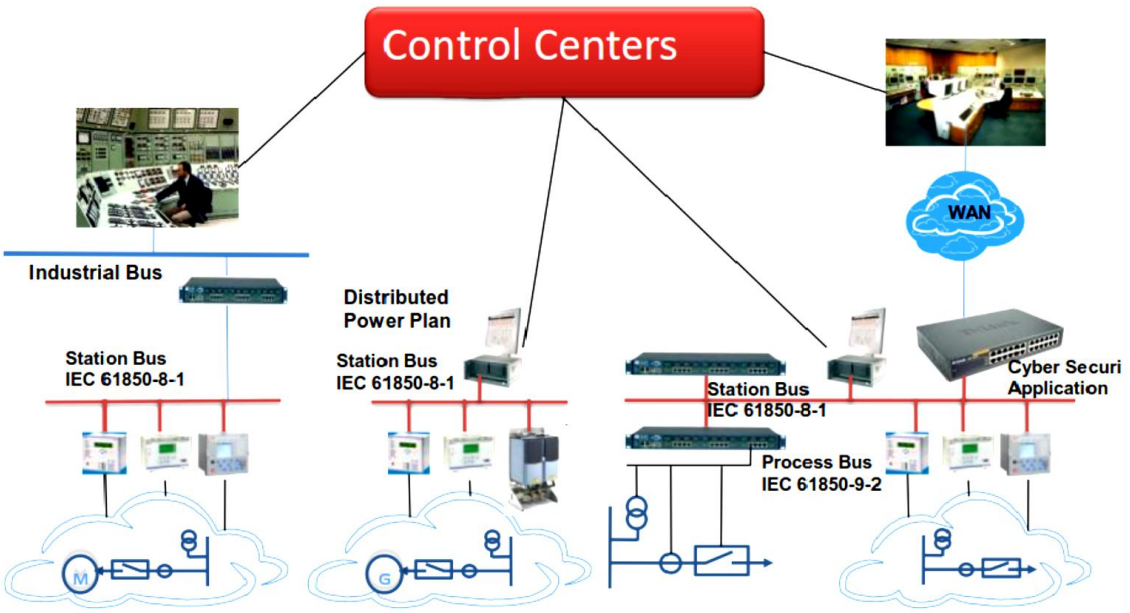

Figure 12. IEC 61850 standard implementation areas

3.4 IEC 61850 Substation Automation System SAS Logical Interfaces.

The three SAS architecture levels, although they are separated as mentioned above, are nonetheless highly interconnected based on several logical interfaces defined by the IEC 61850 standard. From bottom to top, Figure 13 depicts the three levels, as well as the associated logical interfaces numbers. Interfaces number four and five connect the process level to the bay level. These logical interfaces allow control commands and information data to be exchanged. The principal apparatuses, such as circuit breakers, transformers, switchgears, and so on, are usually found at the process level, which may also include IEDs like intelligent sensors and actuators. These apparatuses' input and output messages mostly comprise of analogue signal formatted information, such as transformer voltage and current values, and binary signal formatted control directives from the bay relays. A so-called "merging unit" (MU) is used to convert analogue signals into digitalized standard packets. The MU could be placed in the yard near to or integrated

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

with the instrument transformer, and it should include the voltage and current transformers to feed the LNs (TVTR, TCTR) with the voltages and currents measurements. This conversion offers several benefits, including improving the reliability of the protection and automation systems in terms of broadcasting data and making it available to the entire system. Additionally, by minimizing the use of copper wires, it lowers total SAS costs. This can be accomplished by using logic interfaces instead of electrical lines to connect them. The output packet stream sample values SV that the MU may transfer over the point-to-point-type connection to any IED are broadcasted over the local area network (LAN) in compliance with the IEC 61850-9-2LE.

IEDs such as protection and control units provide protective functions at the bay-level by implementing the functions' output signals initiated on one bay, allowing them to act on the principal apparatus of the primary level. The SAS functions can be arbitrarily or logically distributed across IEDs, according to the IEC 61850 standard. Nowadays, state-of-the-art IEDs may provide multiple functions such as monitoring, protection, and control within an individual IED. On the other hand, distinct functions within an individual bay unit could share data, as illustrated by interface number three.

Various bays within the SAS might communicate to each other through interface number eight in terms of horizontal communication GOOSE messages.

The connectivity between the bay level and the process level is depicted in interfaces four and five. Whereas the connection between the bay level and the station level is presented by interfaces one and six. Were within the station level equipment, such as HMI, station workplace, alarm unit, remote control center, database, etc., communicates with the bay level within interface one to exchange protection data, while interface six is used to exchange control data. Further, interface nine presents the sharing data within the station level. Interfaces seven and ten present the sharing data outside the local station operator. These tasks have been carried out using the second version of standard IEC 61850-7-420 that will be considered later in this report.

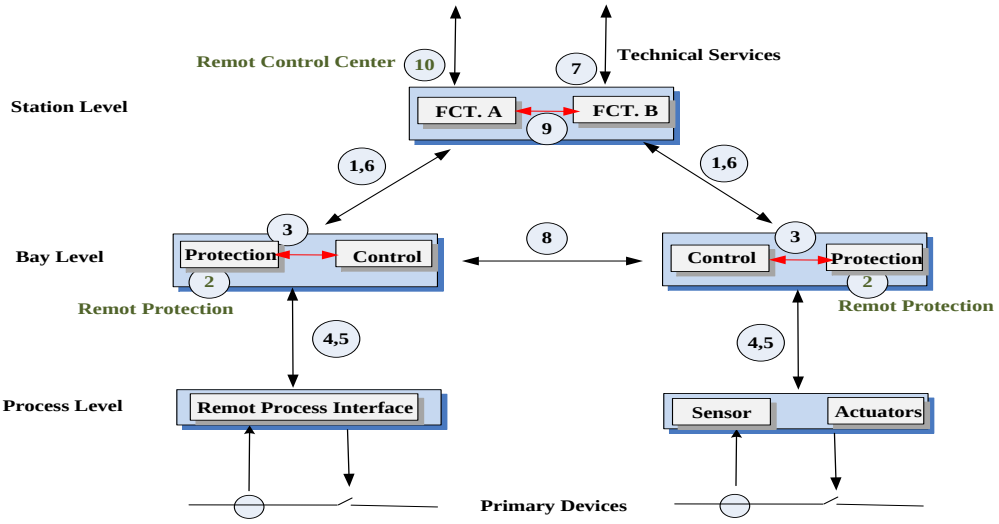

Figure 13. IEC 61850 standard interfaces

3.5 IEC 61850 Standard Communication Entities for Substation Automation

The data object model, together with its accompanying data and services, is isolated from the underneath communication ISO/OSI layers stack, which is the IEC 61850's strongest point. This strategy allows the most innovative communication technologies to be implemented. Next communication elements based on the IEC 61850 standard (protocols, services, mechanisms etc.,) specifications will be presented.

3.5.1 IEC61850 Communication Mechanism and Protocols

The communication scheme that has been used over the ISO/OSI reference model is the mainstream technology. As shown in Figure 14, the ISO/OSI stack is based on the concept of layering communication functionality, which consists of seven layers. The Ethernet physical and link layers are layers one and two, the TCP/IP layer is layers three and four, and the MMS layer is layers six and seven.

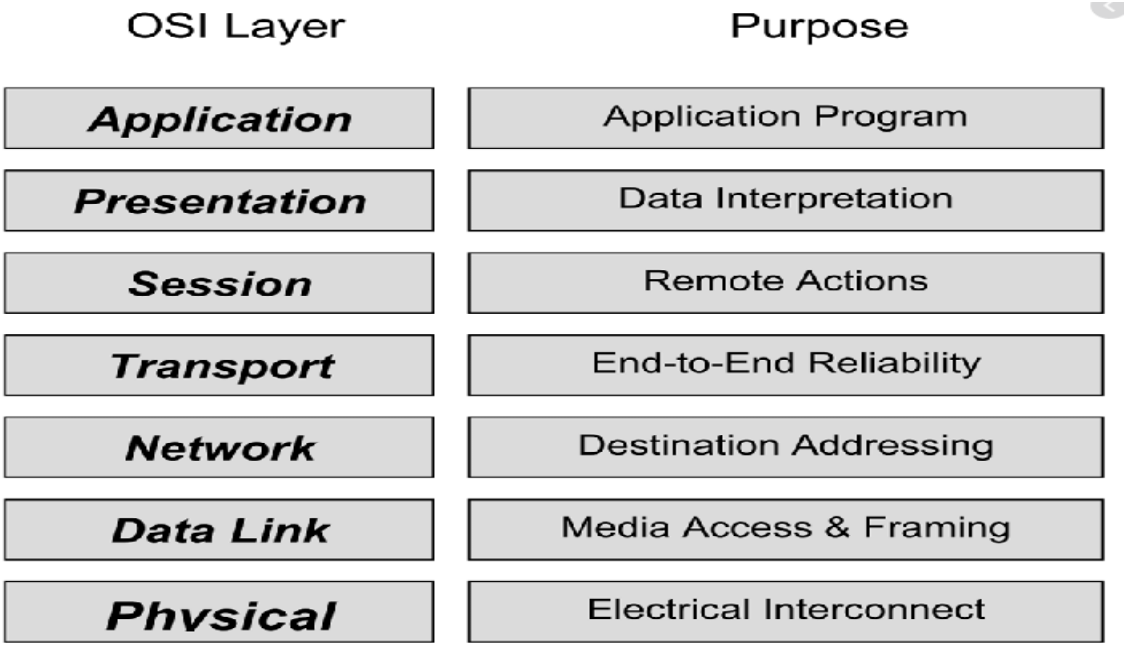

Figure 14. ISO/SOI stack

The object model based on Client/Server services ACSI is mapped to the 5-7 MMS layers. Whereas the time critical messages such as sampled analogue measured values SV, the status indications blocking and trips commands by GOOSE are mapped directly to the Ethernet link layer. In the next three sections we describe the ASCI, MMS, GSSE, GOOSE and SV in more details.

3.5.2 Abstract Communication Service Interface (ACSI)

The IEDs are depicted by the standardized strategy that characterized by the abstract data and object models of IEC61850. This strategy permits all IEDs to exchange information by implies identical structure that compliance with the IEC61850 standard specifications and their related functions. From the network behavior point of view the ACSI gives the determination of the essential for the definition of the substation-specific data models. Moreover, it specifies a set of information exchange service model and the response to those services that allows all IEDs to behave in an identical manner. The abstraction procedure that had been embraced by IEC61850 is one of the foremost critical highlights in which that isolated the substation automation system application from the

undelaying communication protocols and technologies. Figure 15 illustrates the IEC 61850 abstract and mapping concepts.

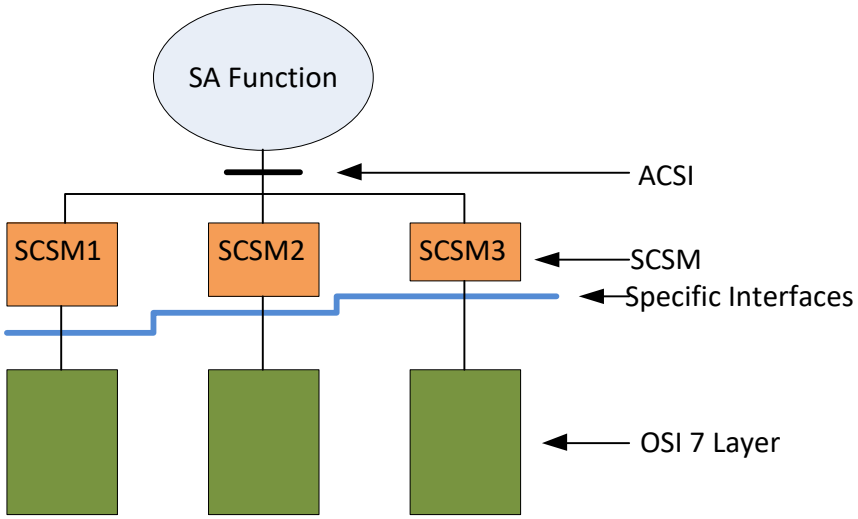

Figure 15. IEC 61850 Abstract and Mapping Concepts

In addition, abstraction in ACSI concepts has two meanings.

- From the information model point view, so that only aspects of real devices or real functions that are visible and accessible over the network are modeled, resulting to hieratical class models such as LOGICAL-DEVICE, LOGICAL-NODE, DATA and DataAttribute.
- From the exchange service model point view, the abstraction of how the devices exchange information means that the definition focuses on aspects on what the services are indented, instead of describing how the services are built. In a real implementation the basic information model and services model are mapped into an existing communication stack. The mapping scheme is realized in the Specific Communication Service Mapping SCSM. In IEC61850 two mapping scheme are specified for the transmission of the sampled value and IEC61850-8 for the transmission of wide station events and all other communication services.

The ACSI provides abstract interfaces, that describe communication between a client and server. This type of interfaces is defined for real-time data access and retrieval, device

control, event reporting and logging, publisher/subscriber, self-description of device, data typing and discovery of data types and for file transfer. Second, that describes communication between applications in one device as a publisher to many applications in different devices as a subscriber for fast and reliable system-wide events distribution such as GOOSE, GSE and SV. The ACSI interfaces which are defined above allows the client to observe the data model, to read and write data, to access datasets, to log etc. by means of calling method such as GetDataValues and SetDataValues. These methods in programing language are reasonable in traditional methods with input arguments and return values.

The ACSI model defines, in addition to a set of services and the response to those services, the concept of application associations that provide a mechanism for controlling the access to the object of a device (access control). To restrict devices visibility different access control schemes can be used.

3.5.3 IEC 61850 GSE and GOOSE

One of the key aspects of IEC61850 is the Generic Substation Events GSE service model, which allows for a quick and reliable system-wide distribution of input and output data values. The autonomous decentralization principle underpins the GSE service model. It employs multicast/broadcast services based on an efficient mechanism for distributing the same GSE event information to several IEDs at the same time. Peer-to-peer and client/server communication methods are supported by the generic substation event distributions. IEC61850-7-2 established two control classes and two message structures, such as,

- Generic Substation State Events GSSE, support only status change information events, fixed structure binary event, bit pairs.
- Generic Object-Oriented Substation Events GOOSE, support of a wide range of a possible common data such as analog, binary and integer value data type organized by a Dataset.

As a result, the primary distinction between the GOOSE and GSSE services is the way information is exchanged. All new systems that transmit a wide range of messages, binary and analogue data use the versatile GOOSE concept. GSSE, on the other hand, is an older binary-only message type.

The GOOSE model's classes and services are depicted in Figure 16. The message is exchanged using the publisher/subscriber mechanism. From the standpoint of implementation, values are written in the local buffer on the publisher's side, and subscribers read the values from the local buffer on the receiving side. The communication system updates the subscribers' local buffers, and the method is controlled by the GSE control class in the publisher.

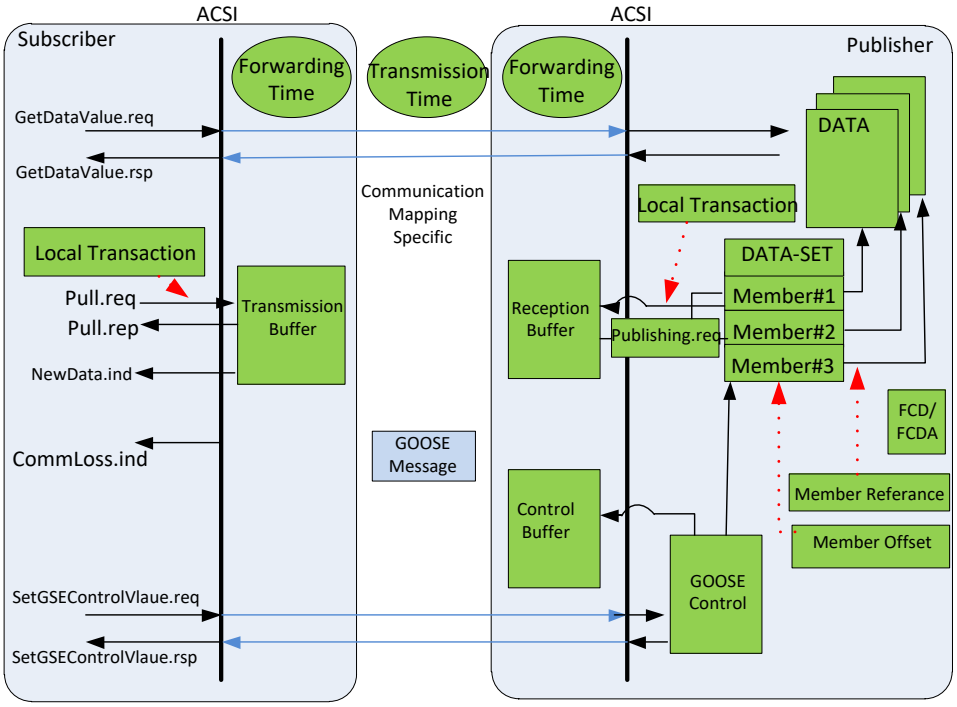

Figure 16. IEC 61850 GOOSE

By receiving the GOOSE messages, which contain all necessary information, the IEDs in the substation are aware that the status has changed and the time of the last status change. In addition, the subscriber's local timer can be configured based on the time of the most up-to-date status change event. Because the GOOSE message transmission time is critical, it is mapped directly to the Ethernet layer to satisfy real-time operation requirements. Traditional protection events such as trip, interlock, and status indication

are regarded as high priority services, with transmission times about a quarter of a cycle or less. As a result, for the 50 Hz cycle frequency system, the message transmission time is defined as 4ms.

Furthermore, because the GOOSE messages are directly mapped over the Ethernet layer, the delivery of services is not guaranteed. To ensure that messages sent via multicast transmission are received, the retransmission technique should be employed. At this point we can see that the GOOSE message is a versatile tool, since it can serve a variety of applications with varying performance needs and data formats.

3.5.4 IEC 61850 Sampled Values SV

The sampled values are peer-to-peer messages that are used to transfer measured values from the switchyard to the bay IEDs in a digital format within the SAS. The measured values at one point based on metering or protection can be distributed to any number of subscribers via a multicast message within the process bus communication network. Individual targets may require a different sample rate, which can be chosen at will based on their requirements. For example, one set of samples can be sent in a single SV packet frame every 250 seconds (about 4 minutes) for a protection application with a sample rate of 4 kHz/s for 50Hz frequency, and eight sets of samples can be sent in a single SV packet frame every 78,125 seconds for a metering application with a sample rate of 4 kHz/s for 50Hz frequency. Within the SV packet frame, these sample values are stored in the application service data unit (ASDU), where the application protocol data unit (APDA) may be made up of one or more ASDUs.

According to the IEC 61850-9-2-LE ASDU consists of a sequence of bits that may translate to the related information such as the “tag”, “Length” and “Values” that may represent the actual information for instance svID which is the unique SV identity, and it is important for the receiver node to subscribe to the needed SV messages. Also, smpCnt is the SV counter that count from 0-3999 for 4 kHz sample/s, and the confRve in which its value increases one very time that the SV parameters is reconfigured or updated. Sample synchronization flag (smpSynch) represent the synchronization status of the SV packet frame as illustrated in Figure 17.

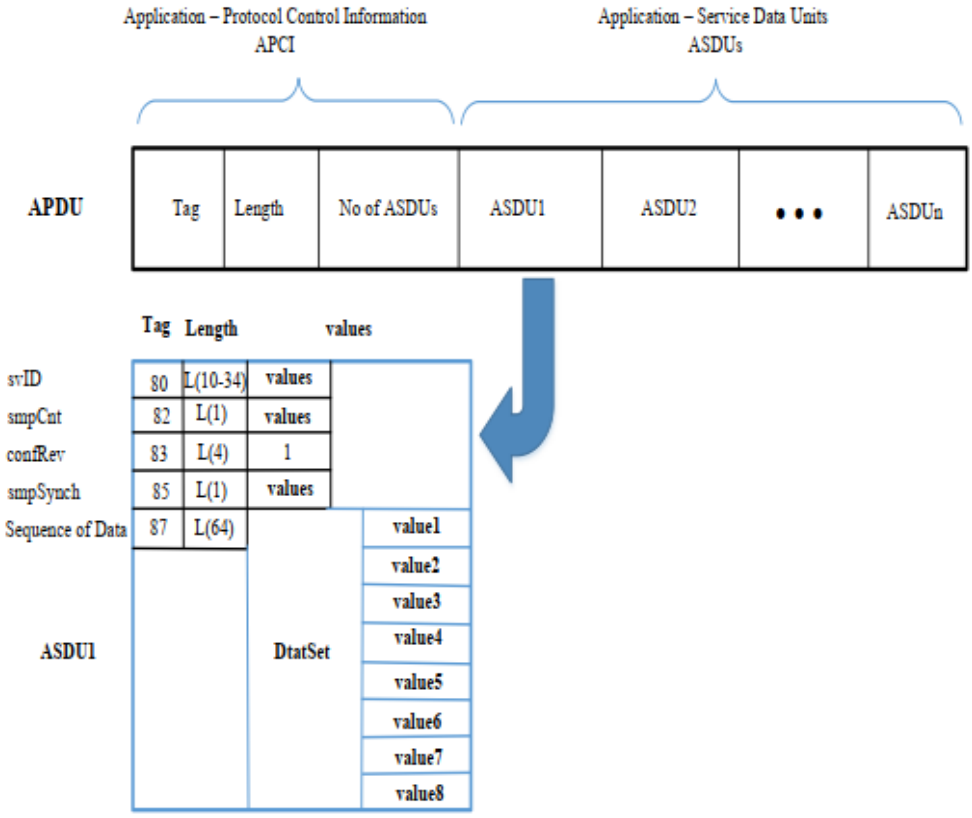

Figure 17. IEC 61850 SV frame

The Sequence of Data represents the actual data set where the InnATCTR1.Amp.instmag.i and InnATCTR1.Amp.q in Figure 18 represent the magnitude of the instantaneous measured value of the current and the data quality respectively for phase one. The same structure is used for the voltage data set.

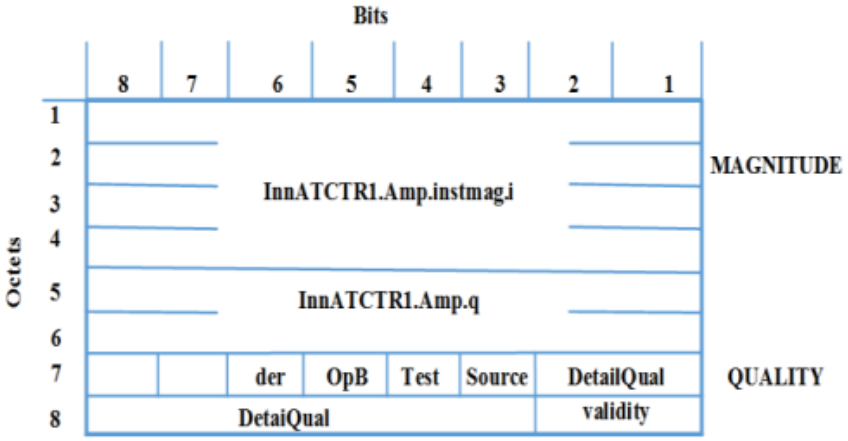

Figure 18. IEC 61850 SV frame Octets allocation

Later in this report comparison between the SV and GOOSE protocol transmission mechanism will be presented and discussed.

3.5.5 IEC 61850 Manufacturing Messaging Specification (MMS) Protocol

The IEC61850-7-x standard object model and service that are pre-specified are mapped over the MMS application layer full OSI/ISO stack (layer seven), which is a part of ACSI that does not handle time critical messages. MMS is a standardized messaging system (ISO 9506) that allows network devices to share real-time data and services. The MMS is an international standardized messaging system (ISO 9506) that been used to exchange real-time data and services among network devices. The mean feature of the MMS it is independent of the application function being performed and the device, software manufacturer. In addition, based on the highly generic nature of the messages services provided by MMS, it is appropriate for diverse types of function, devices, and industries. For example, based on ACSI implementation criteria, MMS' information modeling and services precisely satisfy the requirements. When evaluating the benefits of installing MMS messaging services, three primary factors that lead to cost reduction which can be considered:

- Interoperability that allows two or more network applications to exchange real-time information without the needs to create the information environments
- Independency that provides interoperability independently from the developer of the application, network connectivity and functions based on provide common communication services.
- Data access that facilitates application to provide useful functions by obtaining the information that is required through the network application

The object of the ACSI server class is mapped one-to-one by SCSM to an MMS virtual manufacturing device VMD object from the standpoint of MMS messaging services implementation. The VMD is a crucial aspect of the MMS message services that specifies

how the server behaves in relation to the client application. It also denotes the part of an application task that offers monitoring and control services via a set of resources and capabilities linked to one or more devices. In general, the VMD defined the objects that make up the server. Also included are the services that let a client to access and manipulate these objects by assigning one or more communication addresses, resulting in the service access point SAPs where MMS services can be transferred. The VMD concept is depicted in Figure 19.

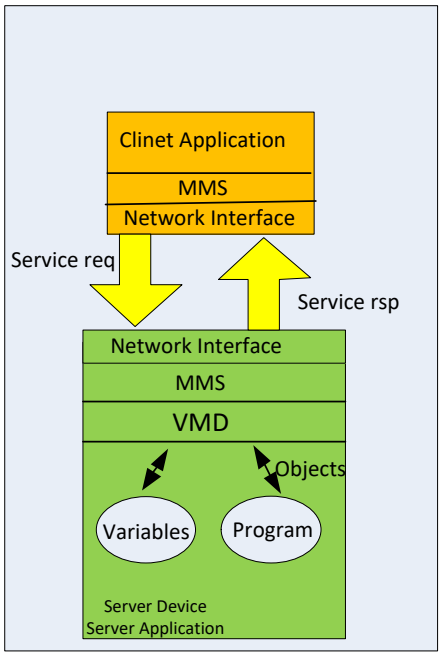

Figure 19. The virtual manufacturing device model VMD.

3.5.6 IEC 61850 Time Synchronization Specification

Substation digitalization framework as proposed in IEC61850 as a digitization environment with strict execution makes it necessary that all IEDs in substation ought to be precisely synchronized for time stamping of exchanged information and control. When a few IEDs are associated together the foremost critical issue to address is how exact time synchronization is arranged with endless of data that is accessible in a quick rate.
Furthermore, most substation functions, such as distance functions that require voltage and current to be synchronized, synchrony-check functions that require two compared voltages to have a common reference, and so on, would not function properly if their

events were not organized in such a way that the accruing order is the same as the published order.

Time reference is a simple method that involves designating one IED as a time reference to which all other IEDs must synchronize. However, with a small LAN, this technique works well since the IED time lags the time reference by the amount of time it takes to travel from the time reference to their destination.

According to IEC61850, the TS model is required to supply a synchronized Coordinate Universal Time CUT to all IEDs in the LAN using the Simple Network Time Protocol SNTP, which has an accuracy of 1ms. TS requirements must be completed regardless of whether SNTP or another protocol is utilized. Figure 20 depicts the TS model, which includes an externally synced timeserver with an external resource, such as a Global Positioning System GPS receiver.

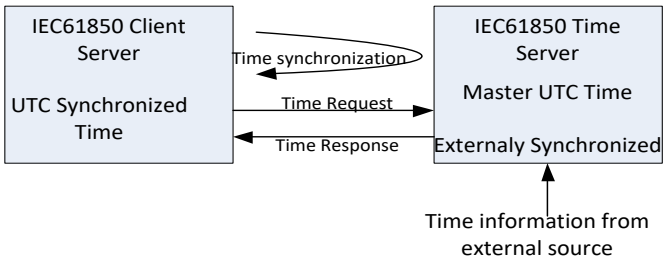

Figure 20. Time synchronization model.

All IEDs in substation are synchronized with the timeserver which represents the source for the substation internal TS and time stamping.

Different classes of TS accuracy have been defined by the IEC61850 standard that illustrates in table 1. The first two times performance classes (T1,T2) are defined for normal events that are not time-critical events. Whereas the rest (T3,T4,T5) is defined for the critical time events such as protection and metering.

Table 1. Performance requirements

Performance Class	Accuracy	Application
T1	± 1ms	Events
T2	± 0.1ms	Synchrocheck

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

T3	± 25μs	Sampled Values
T4	± 4μs	Sampled Values
T5	± 1μs	Sampled Values

As regards, the TS protocol that chosen to use and the performance of the underlying hardware plays a critical role on the accuracy of the TS model. Therefore, the accuracy that provided by the conventional solution, 1ms, does not meet the requirements for the raw data sampled values and for MU. Alternatively, one solution is to use Inter-Range Instrumentation Group time code B (IRIG-B) which is not a time source itself. It provides accuracy of 5μs that requires an external time source such as for instance GPS. Another solution is to use Precision Time Control PTP that has been defined in IEEE 1588. It is a standard controlled mechanism for insuring interoperability between IEDs while meeting the best individual application requirements by providing accuracy of 0.5μs. The PTP has been considered as network core synchronization with a minimum hardware assist and software-based implementation.

To provide a robust and safe solution, two TS models should be defined in the system and not required to be synchronized to switch-over when one of them is in fail state.

3.5.7 IEC 61850 Retransmission Deterministic Approach

According to the first IEC 61850 version, the GOOSE message is routable message that is sent to a network address rather than a device address via a multicast technique. Thus, the network address is a mail group address rather than a device address, the GOOSE messages are routed within a LAN rather than across the internet. The multicast system causes technological challenges for the delivery of messages within the LAN.

When a substation event is sent by an IED within a LAN, other IED receive the message and replicate its response to the same LAN, there is a risk of data collisions and transmission delays. As a result of the LAN's unpredictability, each IED oversees handling message loss, duplication delays, out-of-order delivery, and outages. The Ethernet network is built on CSMA/CD, a non-deterministic protocol that scans the channel and identifies

other transmission signals if data collisions are avoided. This principle is applied in the existing Ethernet network, which includes a queuing method that adds a non-deterministic element to latency. Furthermore, predicting the size of data in the network might be problematic. As the number of devices connected to the LAN grows, the likelihood of a data collision grows exponentially. To improve real-time deterministic performance suitable for SAS, modern Ethernet switching, token ring and token bus, retransmission method, and priority tagging are employed.

IEC61850-8-1 defined the retransmission scheme to achieve a proper level of reliability as illustrated in Figure 21.

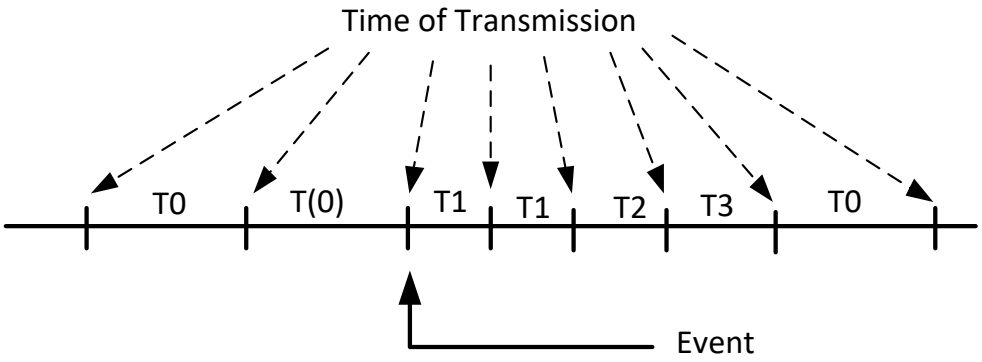

Figure 21. IEC 61850-8-1 retransmission concept.

GOOSE messages are constantly published referred to substation events that invoke a SendGoose service which contains a set of data that consist of binary and analogue data elements. In substation configuration processes each GOOSE message is given a parameter max time (mt) as a waiting time between the first GOOSE message publication and the retransmission event in a stable condition as T0. Next retransmission of the GOOSE message happened when the data element is changed or the max time expired. In this case of data element changed the time of transmission (tot) between messages is noticeably short (4ms), which is (T1) to increase the probability of receiving GOOSE messages by all the clients. After few retransmissions, the (tot) will increase gradually until reach the assigned max time parameter. For each message in the retransmission process the publisher assigned a time to live (ttl) which is used to calculate the time to wait (ttw) by the subscriber. When the (ttw) interval is expired and the message not received by the subscriber it indicates that the association is lost. This feature is also one of the most

IEC 61850 enhancing methods in a way that it allows monitoring controller to have the overall system healthiness status by monitoring the heartbeat GOOSE messages and always see the status of all system associations, allowing the SAS to operate more efficiently and reducing power system outages.

3.5.8 Reliability Criteria and Redundancy

Redundancy has been highlighted as a crucial enabler of SAS reliability, as it prevents the entire system from being brought down by a single failure. The IEC61850 parts, on the other hand, do not address the issue of architecture required to attain a prominent level of reliability. As a result, more effort needs to be done to make this idea a reality and deliver a fault-tolerant system. As a result, redundancy in devices and communication routes should be established at each substation level to provide an elevated level of system tolerance. The level of redundancy supplied is determined by the substation's size; for example, large high-voltage substations frequently include two parallel communication paths and redundant protective IEDs. While no parallel communication channels are employed in tiny substations with lower voltage, redundant IEDs may be deployed. The redundancy system is a method of boosting reliability. On the other side, it increases system complexity in terms of hardware and software, as well as cost. As a result, it requires more careful and practical execution.

Duplicating relays or IEDs can give redundancy on a single device level. For example, a high voltage transmission line may require duplicated main protection with duplicate HMI for operational reasons or redundancy. Both duplicated HMIs can switch over in the case of a failure. Another option is to utilize a contemporary Ethernet switch to provide redundancy in the communication line. An Ethernet switch is a multi-port IED that may require configuration depending on its operating system, firmware, and power supply. By connecting one port to an IED or HMI, a simple small network segment can be created, obviating the need for a sharing medium and increasing channel bandwidth. This feature of the Ethernet switch enables true full-duplex communication between the operator and the process level, with a high data rate, low collision rate, and excellent dependability.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Two redundancy protocols are available High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) that are suitable for Ethernet network.

HSR is an Ethernet network protocol that allows for seamless failover in the event of a network component failure. In HSR network each IED has two Ethernet ports to create a redundant network communication as illustrated in Figure 22. Here we can observe that every IED has two separate connection ports for each signal path in which that provide an alternative association at the bay level in case of failure.

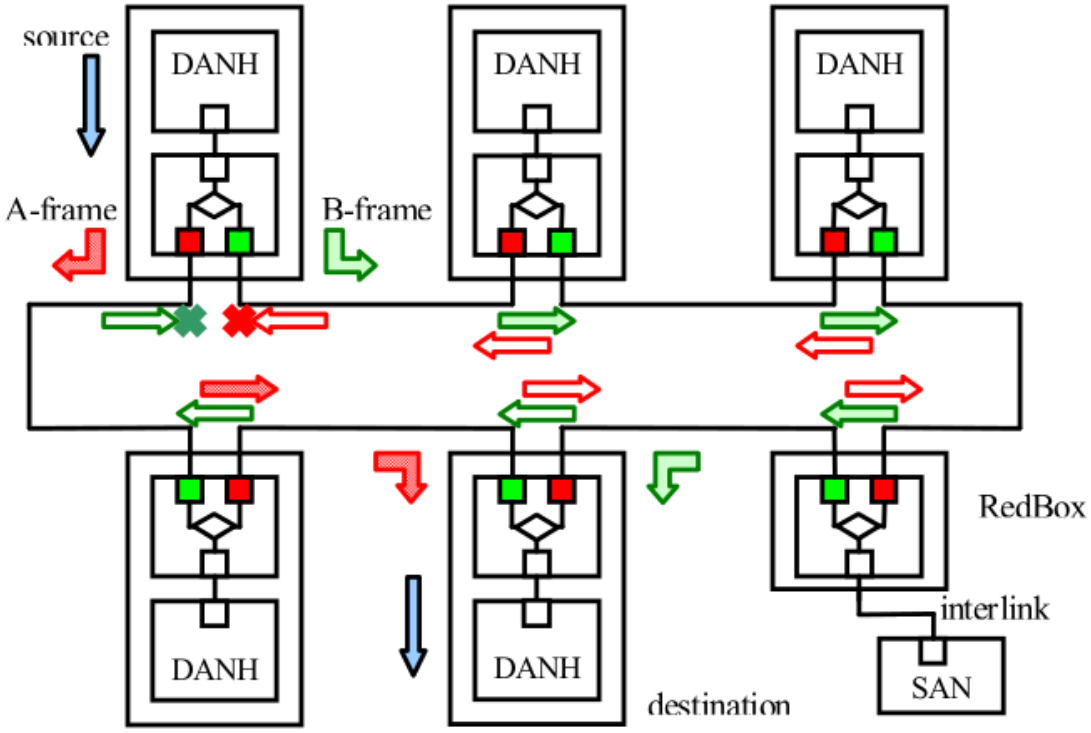

Figure 22. HSR redundancy protocol (DEMVE project materials)

In PRP The IEDs have two separated ports and are linked to two separated Ethernet networks of similar topology as illustrated in Figure 23. In both protocols the IED will receive two messages, one is the original message, and the other is the copy of the original one. As a result, the IED will process one of them (the first receiving message) and discard the second one.

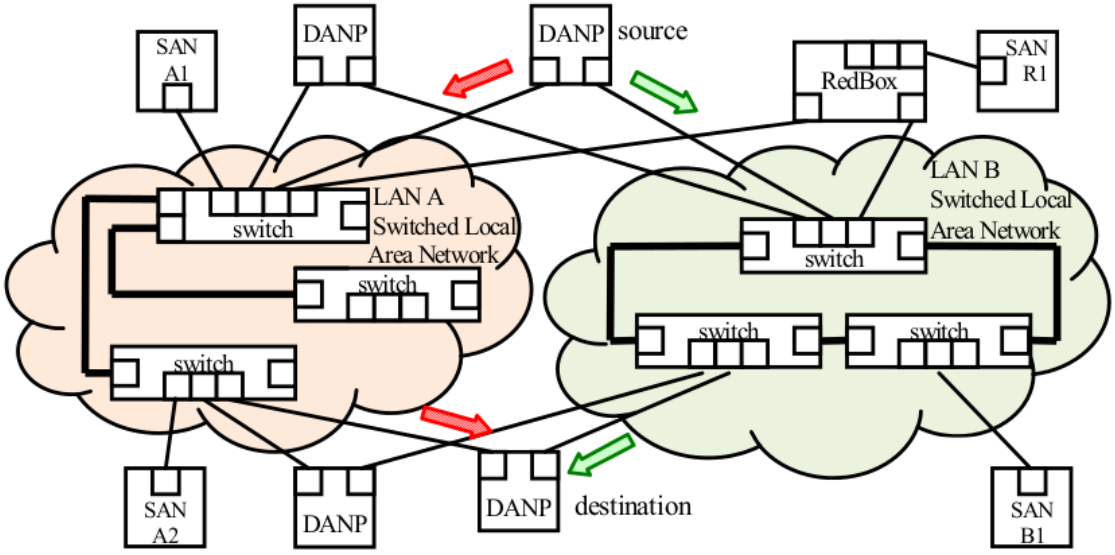

Figure 23. PRP redundancy protocol (DEMVE project materials)

In addition, a mixed solution (PRP+HSR) is also specified to furthermore improve the reliability of the IEC 61850 protocols as illustrated in Figure 24. In this solution we must separate networks (parallel networks LAN A and LAN B) at upper level, and two paths that allows the signal to reach its destination via two IED separated ports.

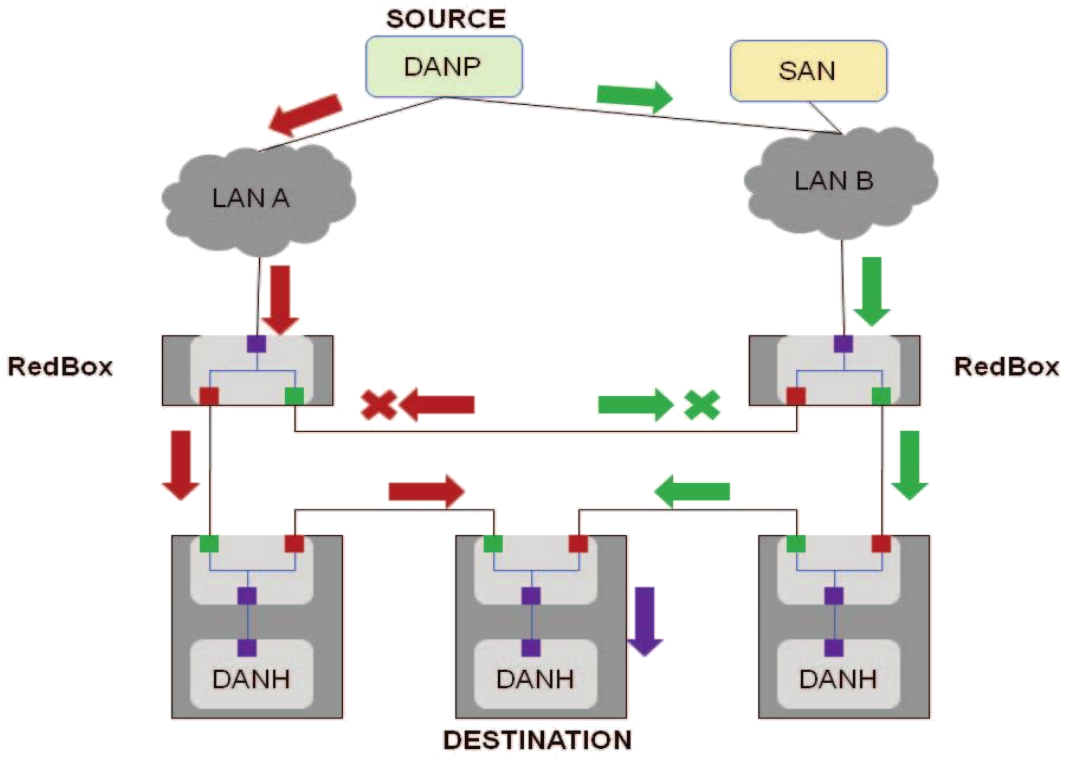

Figure 24. PRP+HSR combined redundancy solution (DEMVE project materials)

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

On the other hand, basing on communication performance requirements as mentioned before the fast GOOSE messages have a strict performance requirement that the messages should be delivered in less than 4ms. Therefore, in any communication protocol, solution etc. that we need to implement we should consider the latency to be no more than the specified IEC 61850 protocols requirements.

To this end, a virtual Local-area Network VLAN is a one of the technical solutions that attenuates the effect of the broadcast/multicast phenomenon in LAN. This can be done by dividing the physically connected network in separate VLANs where traffic flow reduced by restricting it into a single individual VLAN.

3.5.9 Cyber Security Standards and Information Security Management

Organizations Cyber Security standards/state-of-the-art and Information security management knowledge/experience was analyzed/evaluated in Questions from (17-22). The general knowledge/experience of the existing security/communication standards that published from different groups e.g. ISO, IEC, NIST, NERC, CIP etc. which are risk-based, process-based or compliance-based, and energy system communication based are equally-likely/or more, acquired by the Questionnaire contributors as indicated from the answers of the questions e.g. (Q17: 50% and Q18: 63%) this high percentage indicates that the Questionnaire contributors are familiar with the IEC series of standards, however, the relatively newest version of the IEC Cyber Security standard based energy system communication e.g. IEC 6235X and the state-of-the-art simulating/emulating testing tools, there is a lack of knowledge/experience e.g. (Q19: 62% not familiar with the IEC 6235X, Q22: 69% not familiar with the CPS based real-time simulator). According to these highest percentages of unfamiliarity, it would indicate that there is big gap on these topics of and there are areas of improvement that need to be addresses.

Lastly, we recommend that it is the time indeed for the Organizations to really start looking/implementing these CPS standards/guidelines and testing them, in a way that we

can see where the system vulnerabilities might lay and practically do real-time measuring/evaluating to fill the standards/guidelines knowledge gaps, increase the CPS awareness and measure/improve the energy system resiliency, reduce security threats and costs, and especially weaken cyber attackers' strength.

3.6 IEC 61850 Cyber Security Scope

IEC61850 standard does not provide a security solution which it is outside the scope of the standard within the first version, since the IEC 61850 standard was firstly designed to operate within secure network, individual substation connected to Local Area Network (LAN). However, as far as wide area network (WAN) where the client is situated outside of the secured LAN and is attempting to link to the SAS capabilities is this situation the information security is a critical issue. In this respect diverse control access plans like secure association, verification/authentication and encryption ought to be thought of. This the case after IEC 61850 introduced the concept of routed-GOOSE (R-GOOSE) and routed SV (R-SV) within the IEC 61850-90-X standard to support the wide area monitoring protection and control (WAMPAC) application. Please see section 3.7.2 for more information about the IEC 61850-90-X standard.

The access control model in IEC61850-7-2 handles the data security element. The access control model allows you to limit the accessing process to a single server's class instance, class instance attribute, and ACSI acting on. While a set of instances is visible (and hence available) to a client, the restriction process, the server's access control specification and the client's identification play a critical role. A virtual access view is a collection of restrictions. The virtual access view provides also the capability to restrict supported services besides the restriction of the visibility of the instances to a specific client. Figure 25 illustrates the virtual access view concept in IEC61850 standard.

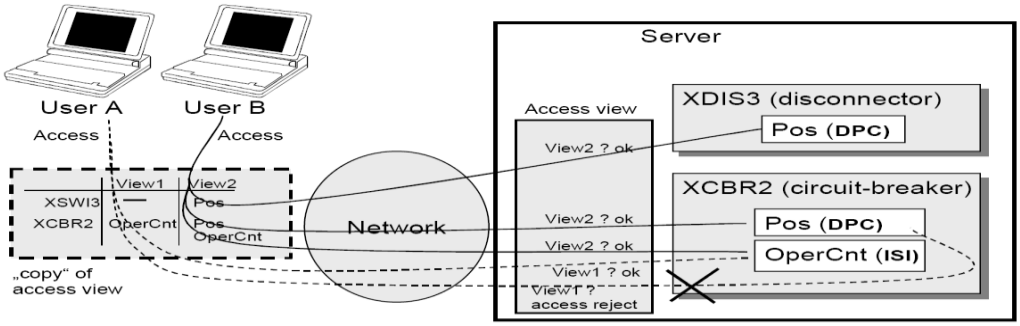

Figure 25. Virtual access view In IEC61850 standard.

IEC61850 based on its implementation point view which relies on the state-of-the-art communication protocols and devices that provide some kinds of security from malicious intruder from the WAN. This security is accomplished through deployment of cyber protection technologies and mechanisms. Beside techniques such as IP-routing, firewall, virtual private network VPN and intrusion detection system IDS, also authentication, authorization and encryption mechanisms are needed to provide a secure operation within and outside the substation. The implementations of these techniques should be applied carefully since IEC 61850 standard assigned strict requirements for its real-time operations. More details about the IEC 61850 security dependent on the IEC 62351 security standard will be examined inside the subsequent specialized report TR 3.2.

3.7 IEC 61850 Extended Version

3.7.1 IEC 61850-7-420

The global incoming booming of the DERs that need to be integrate to the energy grid, and their impacts on the distribution power systems turn into raising challenges. These challenges' stimuli the Utilities and DER manufacturers to announce the concept of growing need to define and standardize the communication outside the individual SAS that may include various DER IEDs.

As a result, the standard IEC 61850-7-420 was published in 2009 as an extension of the IEC 61850 standard and to address these issues. The IEC 61850-7-420 specify several types of LNs and information modeling that applicable for the various DERs e.g., fuel cell

systems, photo-voltaic (PV), combined heat and power (CHP), etc. That information modeling and new LNs facilitate the communication and the integration of the DERs into the utilities protection and automation systems. Utilities and DER manufacturers are expected to achieve benefits from utilizing the IEC 61850-7-420 in terms of reducing the installation, maintenance costs. Further, offering standardization of all DERs data models that will improve the interoperability among distributed automation system (DAS) and DERs and increase the reliability of the energy grid as illustrated in Figure 26.

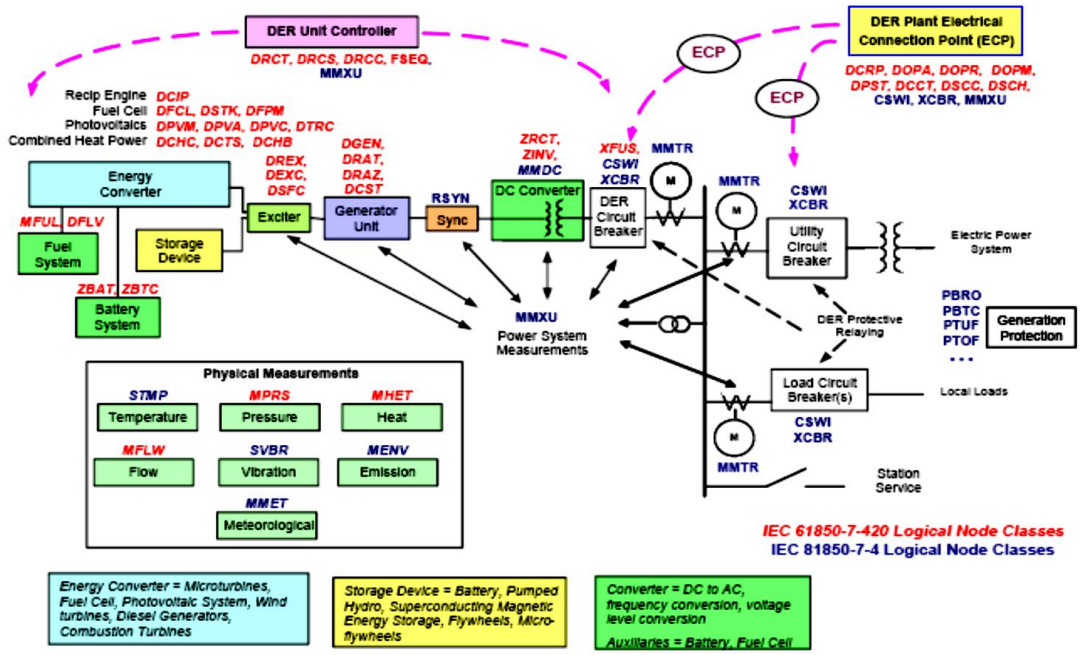

Figure 26. DERs logical devices and logical nodes concepts.

From Figure 26 the consideration has been raised that this IEC 91850-7-420 standard address the information modelling for various DERs, whereas other IEC 61850 implementation aspects such as the services modeling, assigned system configuration language (SCL) and the mapping schemes over the defined protocols had been covered within the previous IEC 61850 10 parts first version. These DERs information modeling defined by IEC 61850-7-420 standard involve not only for the local communication among the local DERs and the local management service systems but may support the sharing information with the main grids operators or aggregators who manage the whole electrical grid operation.

The defined DERs LNs based on IEC 61850-7-420 have been grouped into four groups upon their operation characteristic (node classes and common data classes (CDC)). These DERs LNs groups are logical nodes for DER management systems, logical nodes for DER generation systems, logical nodes for specific types of DER and logical nodes for auxiliary systems. These defined DERs LNs represents all the DERs operation aspects parameters such as for instance, connecting status, availability status, economic dispatch parameters, start/stop time, operating mode etc.

At this end let us consider the DER LNs DPST. It provides the real-time ECPs status and measurements. The ECPs are usually associated with each DER, load, lines, buses etc. that need to connect to the local power system, group of DERs that need to interconnect to the Utility energy system etc. The DRCS LN defines the control status of individual DER or group of the same type of the DERs that controlled within individual controller. Contributors from distinct perspective may also add other LNs that support different power system critical function that are not covered by both IEC 61850 standard.

3.7.2 IEC 61850-90 Series

The scope of IEC 61850 is no longer limited to substations. When the first version of the IEC 61850 when was prepared, it was intended to exchange information among the devices within the SAS. However, the global incoming booming of the DERs that needs to be integrating to the power grid though the micro-grid concept, and their impacts on the distribution power systems turned out new challenges. These issues have prompted utilities and DER manufacturers to declare the increasing need to define and standardize communication outside of individual SASs, which may comprise several SASs/micro-grids, connected over the communications network.

As a result, a series of IEC/TR 61850-90-x since 2010 have been published as an extension of the IEC 61850 standard and to address these issues. To acquire a better understanding of the IEC 61850-90-x standard, see the list of the standards below that are might relevant to our consideration.

- IEC/TR 61850-90-1:2010 specifies the communication among various SASs and provides a comprehensive overview of different issues that related to the inter-

SASs using the IEC 61850 implementation aspects that had been covered within the previous IEC 61850 10 parts first version as given above. It adds the interfaces (IF2, IF11) share the same characteristic of data exchange between substations upon protection, automation and control distributed functions as illustrated in Figure 27

- IEC/TR 61850-90-2 report, which is under preparation, considers the communication between the substations and the control centers.
- IEC/TR 61850-90-3:2013 considers the communication networks and systems for power utility automation using IEC 61850 for condition monitoring diagnosis and analysis.
- IEC/TR 61850-90-4:2013 provides the engineering guideline for communication considering the local area network limited to the requirements of IEC 61850 based SAS.
- IEC/TR 61850-90-5:2012 provides the ability to exchange digital status and synchronous phasor measurements over a wide area monitoring protection and control (WAMPAC) among different phasor measurement units PMUs and control center. The synchronous phasor measurements data content and use is defined by the IEEE C37.118, while the exchanging concept is compliant with the IEC 61850 definitions
- IEC/TR 61850-90-12, that had been published in 2015, provides definitions, guidelines and recommendations upon the existing standards and protocols for the WAN communication engineers. It considers the inter substation communications, substation-to-control center and inter control center communications. Moreover, different issues related to Utilities communication over WAN such as topology, redundancy, jitter and QoS have been addressed, which may facilitate understanding the technologies, and integrating of different selected components through the conducted testing.

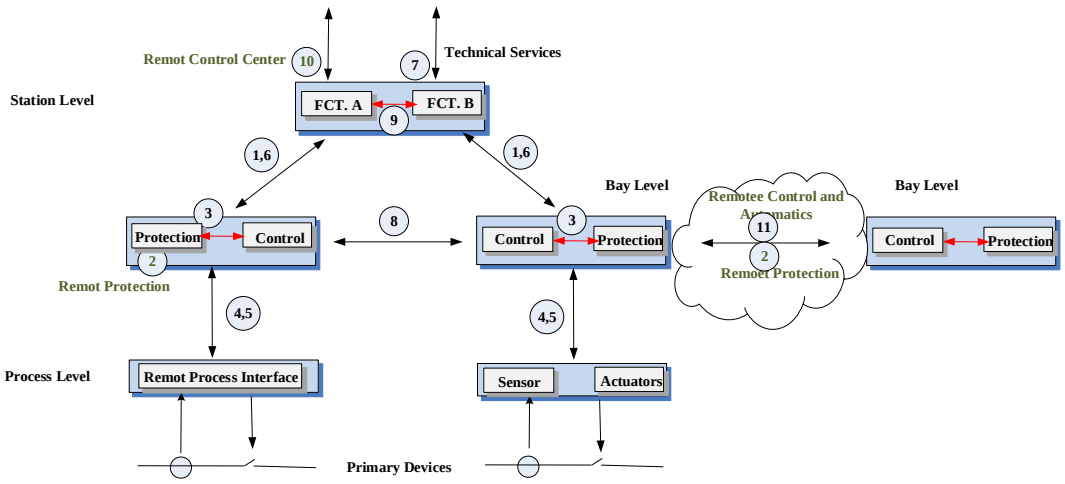

Figure 27. Logical interfaces between substation A and substation B.

We may explore the IEC/TR 61850-90-5 further as it defines a new routable method through the new routable control block for the GOOSE and SV, which are R-GOOSE and R-SV. The mapped data by R-GOOSE and R-SV control blocks are encapsulated in a session protocol data unit (SPDU), which includes data sets and may contain information other than just the synchro-phasors measurements. The encapsulated data is transmitted via the multicast UDP/IP services that improve the delivery priority through implementing the Differential Service Control Protocol (DSCP).

The DSCP limits the probability of delivery packets lost upon the router congestion, by adding the priority tagging to the delivered packets. Consequently, according to the IEC/TR 61850-90-5 specifications, “source filtering” through the Internet Group Management Protocol Version 3 (IGMPv3) was specified. The IGMPv3 enables the subscriber hosts to register on a router and assign which group they want to receive multicast traffic from. As a result, the router does not need to deliver the packets over all the available paths, however, it determines the appropriate dedicated paths upon the registered subscriber hosts that improve the multicast delivery mechanism. IEC/TR 61850-90-5 security is provided through the “perfect forward” security upon the encrypted key rotation between the publisher and the subscriber. The subscriber announce beforehand about the next key rotation and the subscriber needs to detect the synchronization status with the current key.

4 Summary

The evolution of technology and standards that merge to the power system functionality, has a significant impact on the feasibility and utility performance and designs. The relatively new IEC 61850 substation automation standard gives practical improvements in terms of more measured and calculated real-time information on substation operation. This real-time data is easily accessible thanks to the IEC 61850 standard, and it may be used to troubleshoot substation incidents by operating, maintenance, and engineering. Nonetheless, IEC 61850 does not address all these issues, it is a key component of solutions such as harmonized data correspondence, a framework with high interoperability, and network cyber security. Another issue is the difficulty to start with the IEC 61850 standard particularly with the end-user who has no prior experience on power system communication network protocols/standard and related principles. It very well may be a smart thought to read the outline archive for the IEC standards and afterwards take a forward step with more advance documents. Thus, to tackle the difficulties of the standard and make the reading handier, the standard drafts with relevant topics are archived and listed.

On the other hand, certain issues may arise because of the new power system design that compliance with the IEC 61850 specification such as interoperability issues within the multivendor environments since the standard gives more freedom for the providers to implement with. This issue could be addressed by putting IEDs to the test in multivendor environments, as several pilot projects have been set up around the world for this reason, e.g., “Development of the Education Services of IEC 61850 in Multi-Vendor Environment". (DEMVE) at the University of Vaasa.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

References

[1] IEC61850-1Introduction and Overview

[2] IEC61850-2 **Glossary**

[3] IEC61850-3 **General Requirements**

[4] IEC61850-4 **System and project management**

[5] IEC61850-5 **Communication Requirements for Functions and devices Models**

[6] IEC61850-6 **Configuration Description language for communication in Electrical**

[7] IEC61850-7-1: Communication Network and System in Substation-part 7-1:

[8] IEC61850-7-2: Communication Network and System in Substation-part 7-2:

[9] IEC61850-7-3: Communication Network and System in Substation-part 7-3

[10] IEC61850-7-4: Communication Network and System in Substation-part 7-4

[11] IEC61850-5: Communication Network and System in Substation-part 5

[12] IEC61850-8 **Specific Communication Service Mapping (MCSM)**

[12] IEC61850-8-1: Communication Network and System in Substation-part 8-1

[13] IEC61850-9-1 **Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link**

[14] IEC61850-9-2 Sampled values over ISO/IEC 8802-3:

[15] IEC61850-10 Conformance testing:

[16] IEC 61850 Part 7-420: Basic communication structure – Distributed energy resources logical nodes

[17] IEC 61850 Part 90-1: Use of IEC 61850 for the communication between substations

[18] IEC 61850 Part 90-2: Using IEC 61850 for the communication between substations and control centers

[19] IEC 61850 Part 90-3: Using IEC 61850 for condition monitoring

[20] IEC 61850 Part 90-4: Network Engineering Guidelines - Technical report

[21] IEC 61850 Part 90-5: Using IEC 61850 to transmit synchro phasor information according to IEEE C37.118

[22] International Electro technical Commission IEC webpage available online https://webstore.iec.ch/home

[23] IEC Just Published Just Published | IEC Webstore

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund