2019

Specification of IEC 61850 Information Exchange between DER and Power System Actors, including TSO, DSO and BRP

SPECIFICATION OF IEC 61850 INFORMATION EXCHANGE FOR DER

ENDK-61850-SPEC

Contents

IMPORTANT NOTE:

This specification ENDK-61850-SPEC version 15 is still a working draft.

The sections from page 14 to 70 in this specification is still drafts with comments and only to be used as so.

There cannot be referenced to this specification, until it is to be labelled 'Final version' in the footer.

Introduction

No energy system can work efficiently without information exchange. Energy markets depend on demand and response information. The system and grid operators depend on fast and accurate grid conditional measurements. Energy producers need to monitor and operate the facility and end-users need billing.

Information exchange on many different levels are needed and the demand for more secure information exchange is rising, due to the rising focus on distributed energy resources based on stochastic renewable energy as well as an increasing cyber security threat.

New European regulation for establishing guidelines on electricity system operation are now in place and next step will be for the national operators and regulators to make the technical specifications.

The technologies are ready, and the technical standards are drafted – so now is also the time for the ICT manufactures and system integrations to make the solutions work in the field.

What is the purpose of this specification?

This current draft document is an informative technical specification which can support the nominative SO GL (System Operation Guide Lines 2017/1485) and national directives like NGF 'Nationale Gennemførelses-foranstaltninger'

This specification will focus on the information exchange between the facility of energy producing or consuming units – and the operators outside the facility, basically the 2 sides of the red line in the figure.

The main target audience for this specification will be technical management people, on ether the facility or the operator side – who needs to get an overview of the concept and use of standards within this field.

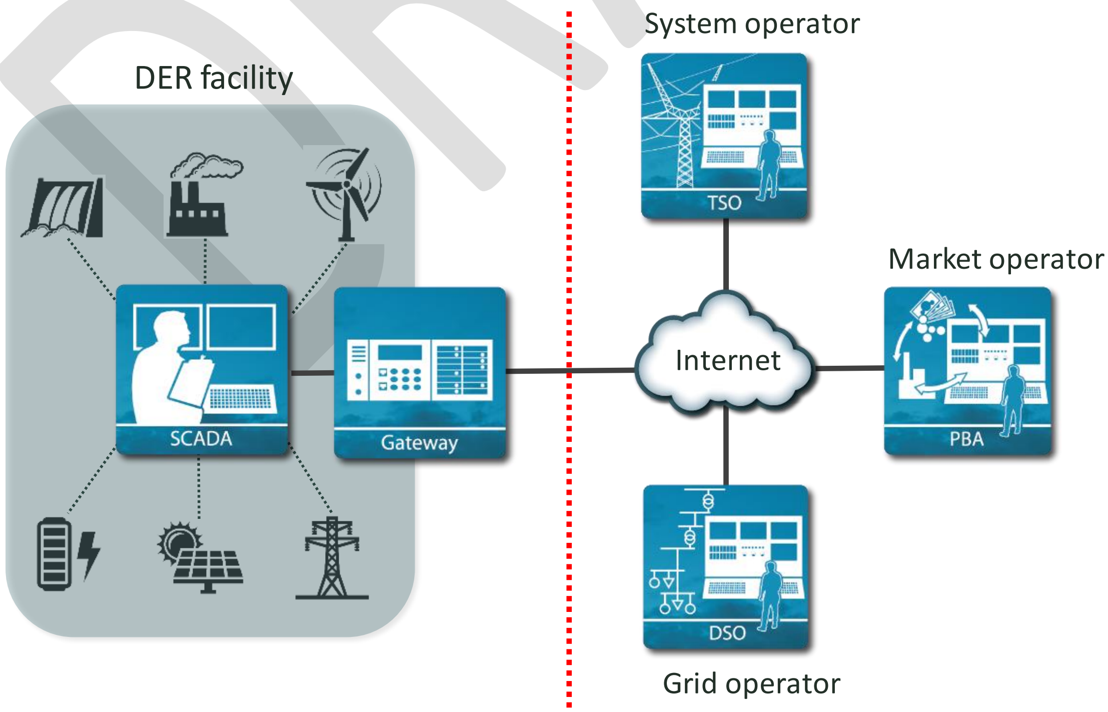


Figure 1 – Interface between DER facility and external actors

Why IEC 61850?

Data communication has been possible for more than 100 years. Many protocols have been developed for many different purposes, ICT platforms and requirements – so Why IEC 61850?

First, we need to look at the challenges?

- The current global expansion of renewable energy resources, like wind-turbines and photovoltage, is a challenge for the power system, regarding energy balance and power losses and power quality.
- Central power production is becoming more distributed and from smaller units.
- Energy markets including ancillary services, are evolving and faster control loops are needed.
- Interconnections between different countries and regions are becoming more important to ensure security-of-supply.
- Cyber security is also targeting 'critical infrastructure'

IEC 61850 is not the solution to all these challenges – but a very important part of the solution as a harmonized data communication system with a high level of interoperability and cyber security.

So, why IEC 61850?

IEC 61850 has been developed over more than 20 years, has a global perspective and includes the following main features:

- Harmonized information model – unique naming convention.
- From 2017 a full digital UML version is available.
- Recognized and recommended by ENTSO-E, EDSO, Eurelectric and many others.
- The IEC organisation has focus on evolving the IEC 61850 (and CIM) standards, while the IEC 60870-5-104 standard will not be further developed.
- The European SmartGrid Taskforce with their M490 mandate points to IEC 61850 as the standard to use for data exchange in the SmartGrid domain.

International perspective

IEC (International Electrotechnical Commission) founded in 1904 and is today the world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies.

IEC TC57 (Technical Committee number 57 out of 104) is the group of technical people working with standards for power system control equipment, distribution automation, energy management, cyber security and more. The only international group within this field of standardization.

What is IEC 61850?

IEC 61850 is an international standard which is designed for secure exchange of information within a power system.

Originally developed for sub-station automation, it is today also covering Distributed Energy Resources (DER) and in addition Information Security – within the same framework under IEC TC57.

IEC 61850 is not just a protocol that can exchange a block of data from A to B – it is also an Information Model, which defines a unique naming convention for all the building blocks inside the power system and DER facility.

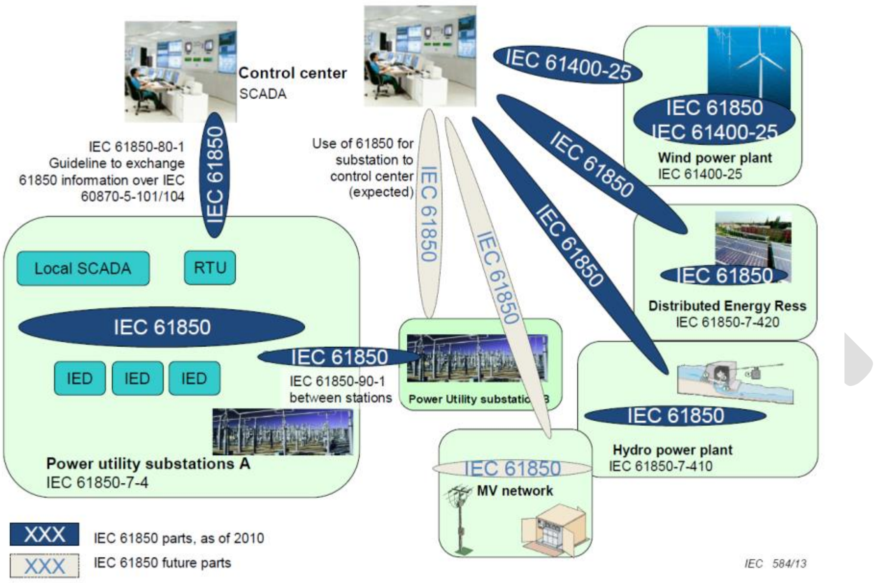


Figure 2 – IEC61850 overview

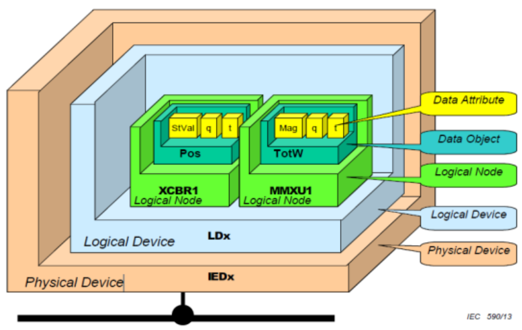
Basic IEC 61850 – information model, protocol and configuration

In IEC 61850 there is basically a Physical view and a Logical view, where the physical view is the actual component, e.g. a voltage measurement inside a power meter at the DER facility – which in IEC 61850 is represented as a Logical Node (LN) called MMXU for measurement.

From a logical point of view, the MMXU is part of a Logical Device (LD) for e.g. a power meter and it contains Data Objects and Data Attributes. So, a measurement is represented as:

FacilityIdentifier_PhysicalDeviceLogicalDevice/LogicalNode.DataObject.DataAttribute.DataAttribute

which, in the real implementation, could look like: **EIC45W0000000000013_HG2GA3/MMXU1.TotW.mag.f**



EIC45W…13	Energy Identification Codes, 45 for DK and 13 for e.g. Skagen
HG2GA3	ISO 81346 naming convention
MMXU1	Measurement unit 1
TotW	Total real power in a three-phase circuit
Mag	Magnitude of analog value
f	Datatype float

Figure 3 – IEC61850 logical topology

IEC61850 protocol and services

The IEC61850 protocol is based on ISO 9605 also called **MMS** (Manufacturing Message Specification) and by adding the newest security extension from IEC 62351-4 - the specification is called **SecureMMS**.

It is a very efficient binary protocol (typical package size app. 400 bytes, for single point polling including security) and on top of it is a set of well-defined services call **ACSI** (Abstract Communication Service Interface).

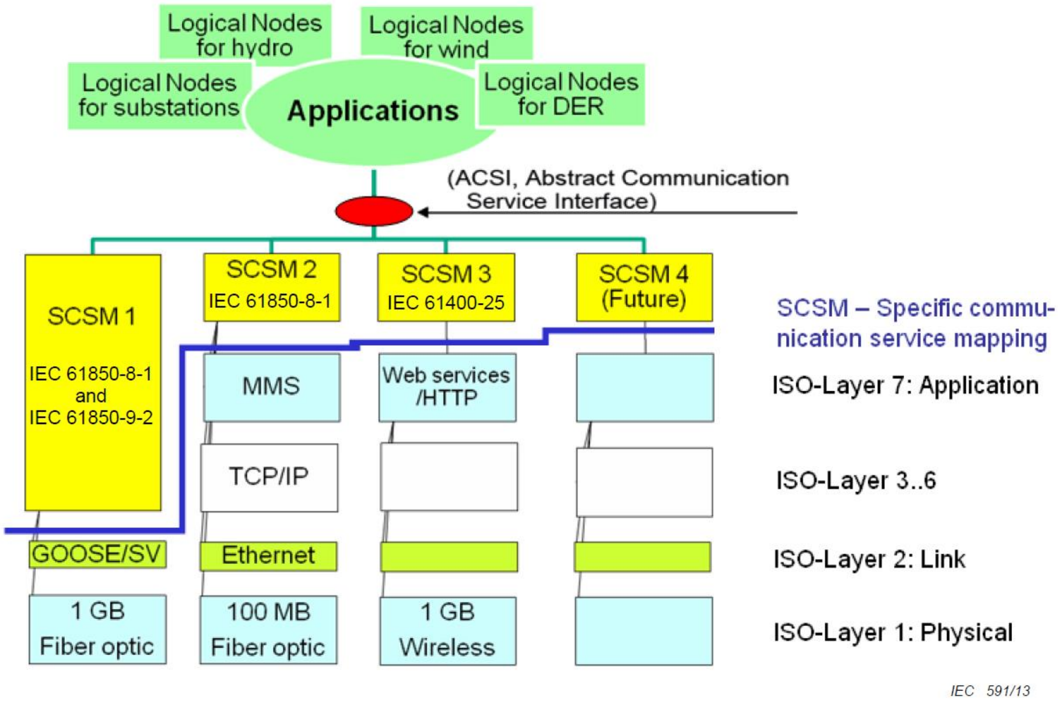


Figure 4 – IEC61850 layers from transport, protocol and services to information layer

Between the transport layer and the information layer is the ACSI services (red marking in figure 3). For examples, please look at the section: *Basic UML use cases for information exchange – examples for inspiration* or the standard document: IEC 61850-7-2

ACSI include services like:

GetLogicalNodeDirectory	An IEC client shall use the service to retrieve a list of all Logical Nodes on a given Logical Device
GetDataValues	An IEC client shall use the service to retrieve data values of a given Data Object
GetDataValues	An IEC client shall use the service to set data values of a given Data Object
DATA-SET	This service is a grouping of elements which can be operated using a single command
REPORT-CONTROL-BLOCK	This is an event-driven service that can automatically send data when triggered from the IEC server

ACSI services are basically 'functionalities' build into the IEC61850 protocol, that can be used as application logic to facilitate the ICT implementation.

SCL for configuration of devices using IEC61850

The System Configuration Description Language (SCL) is part of IEC 61850 and can be used for describing IEC 61850 devices (in IEC 61850 referred to as IED – Intelligent Electronic Device) and how these IEDs are used within a system.

The SCL syntax supports different types of files, each having a specific purpose:

- The ICD (IED Capability Description) file allows a vendor to describe the complete capabilities of a device.
- Provided with the ICD file, the IED engineering can generate an IID (Instantiated IED Description) file, that describes how the capabilities are utilised in the device.
- The IID file can then be used by system engineering to generate a CID (Configured IED Description) or a SCD (System Configuration Description) file.
- The CID file describes the configuration of one IED only, and loaded into an IED, it configures the behaviour of that IED.
- The SCD file describes one or more IEDs with the same details as in the CID, and how they relate to each other and the system. This file can also be loaded into an IED to configure its behaviour.
- System Specification Description (SSD) file: This file contains complete specification of a substation automation system including single line diagram for the substation and its functionalities (logical nodes).

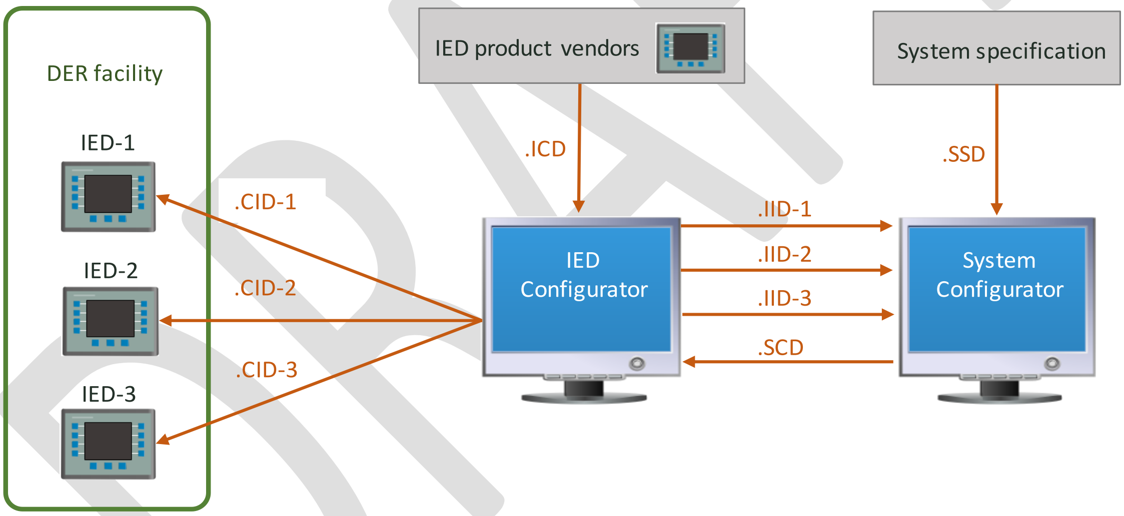


Figure 5 – Use of SCL files and tools for IED configuration

In Figure 5, two configuration tools are being used: the "IED Configurator" and the "System Configurator".

The "IED Configurator" tool is used by an engineer with knowledge about the operation of the individual IED (one or more) in the facility. Use of this tool has two purposes:

1) Based on the IED capabilities (ICD) file provided by the IED vendor, the engineer decides what capabilities to be utilised and based on this defines the information model for the individual IED. The result of this modelling is provided in one or more instantiated IED (IID) files.
2) Based on a system configuration (SCD) file, the configuration for individual IEDs can be generated. This is described in the configured IED (CID) file.

The "System Configurator" tool is used by an engineer with knowledge about the facility in general, e.g. the communication network setup and how devices in the facility are structured. Based on the instantiated IED (IID) files for the individual IEDs in the facility, a system configuration (SCD) file is being generated with information about topology and communication settings.

How to read the standards

If the reader has no previous experience with IEC 61850 and related standards and wants to know more about the standards from an operator and system integrator point of view – it might be a good idea to begin with read the overview document IEC 61850-1 and then take a course. To find 61850 courses do a web-search for '61850 course' and this will give you a good overview.

IEC 61850 is a large series of standard document which consists of the following parts, under the general title **Communication networks and systems for power utility automation**.

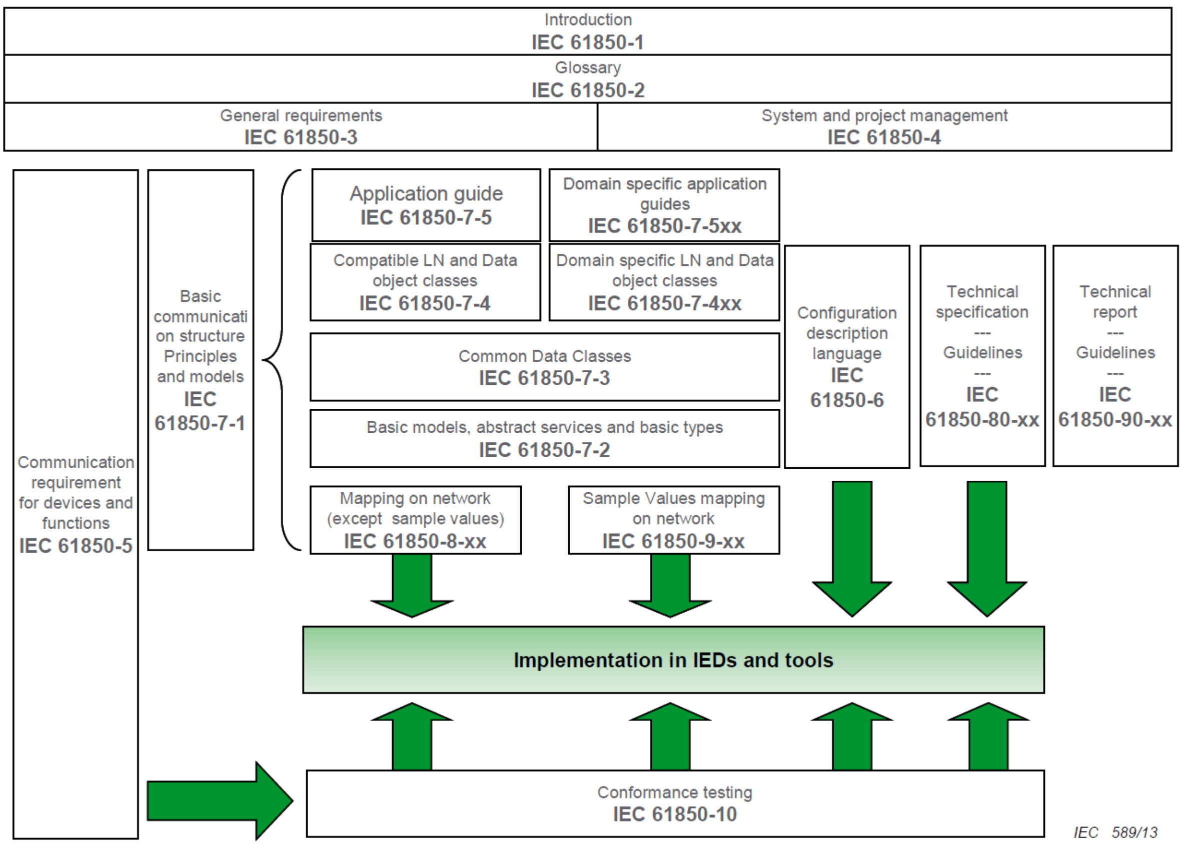


Figure 6 – The IEC 61850 series of standards (IEC 61850:2019 SER)

The IEC 61850 and related standards can be grouped under the following headlines:

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

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 centres

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

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.

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

Conformance testing

IEC 61850 Part 10: Conformance testing

IEC 62351-100-1: Conformance test cases for IEC 62351-5 and companion standards

Cyber security

IEC/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

Please reference ANNEX F for other relevant standards and specifications.

How to get started – practical recommendations

Depending on your purpose for using the IEC 61850 standard, being an operator inside the facility, an operator outside the facility or a system integrator with configuration of IEC 61850 products – there might be different ways for you to get started.

Please have a look at the figure and read the recommendations that will be the best choice for your specific purpose.

Note: These recommendations are only to be used as inspiration for the reader.

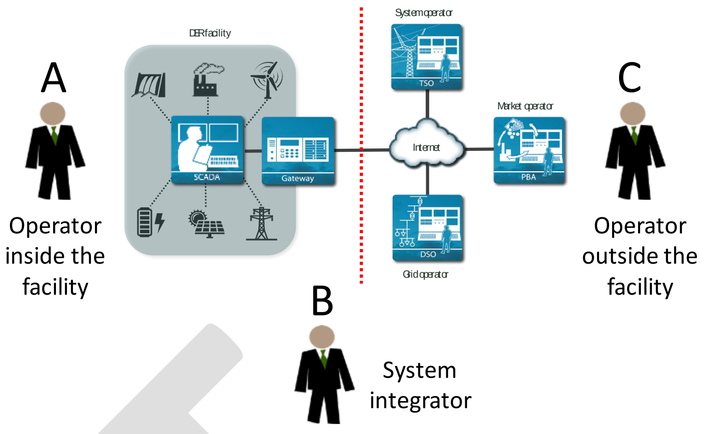


Figure 7 - Actors in focus for this specification

Read this section if you are an Operator inside the DER facility (A)

As owner and operator of a DER facility, the focus will always be on preserving the assets and obtaining optimal production – and secondly interactions with operators outside the facility.

However, being connected to the power system today requires more and more focused on having a close coordination and interaction between the DER facility and power system actors, for the benefit of ancillary services and energy market services.

From a data communication point of view, the DER facility should focus on the following elements:

1. Secure shared access to information managed by the DER facility
2. DER facility as the data source originator and owner of non-aggregated data
3. Point of Communication (PCOM interface) should be based on international and open standards

Also, cases where proprietary technical solutions are the main reason for the DER facility owner to buy services at a given system integrator, should of course be avoided.

Read this section if you are a System integrator (B)

As a system integrator, the focus would be to have a good business based on the DER facility and this also implies to provide the best technical service.

Where this specification focuses on the external PCOM interface, IEC 61850 is also possible to use in other internal system integration processes. Also note the IEC 61850 communication interfaces and elements including information security, should be based on international standards. This will reduce the cost for the DER facility, and it will also benefit the system integrator, because training and recruiting personnel, maintenance of proprietary solutions and reduced cost of components, can in the end benefit the business revenue.

From a data communication point of view, the System integrator should focus on the following elements:

1. Focus on ICT-tools that supports the system integration process
2. Support the international standards and reduce cost on maintenance of proprietary solutions
3. See Information Security services as a mandatory part of your business

Read this section if you are an Operator outside the DER facility (C)

As an Operator outside the DER facility, no matter if you are a System operator, Market operator or Grid Operator, the main point of interest will probable me if the DER facility is a trusted asset - both from a DER resource and security point of view.

- The System operator will focus on 'Security of Supply'
- The Market operator will focus on how to use the DER facility on market terms
- The Aggregator will focus on how reliable and controllable the DER facility is
- The Grid operator will focus on how to use the DER facility in case of power quality management

From a data communication point of view, the Operators should focus on the following elements:

1. Interfacing to a DER facility should be with secure and shared access
2. The operator should be able to communicate with all DER facility, using same standard interface.
3. End-to-end security should be mandatory, based on a common trust framework

Reference architecture

A reference architecture is a conceptual description, in this case a drawing (figure 8), representing the main actors, components and their generic interconnections.

Overview diagram for actors and basic information architecture

The red line is representing the data communication between the DER units, DER controller/gateway, SCADA and network equipment, inside the DER facility.

***DER facility** is the term used for the whole facility, which has a data communication interface called PCOM*

***DER system** is the term used for a functionality that combines several DER units into a system (e.g. several motor-generator sets, PV arrays, electrical storage or wind turbines)*

***DER unit** is the term used for the single DER (e.g. gas turbine, heat pump, electrical boiler, motor-generator set)*

***DER gateway** is the physical component which has an IEC server functionality and can communication to IEC clients outside the DER facility.*

***DER controller** is a physical or virtual component that has functionality that controls and aggregates several DER units for a DER system.*

***PCOM** is the interface between the DER facility and any actor outside the DER facility, in terms of data communication and information exchange.*

***PCC** is the 'Point of Common Coupling' where the DER facility is electrically connected to the public electricity supply grid.*

***ECP** is the 'Electrical Connection Point' where each DER unit is electrically connected to the local facility power grid; groups of DER units (a DER system) have an ECP, where they interconnect to the DER facility power grid; ECP for the DER facility is identical to the PCC.*

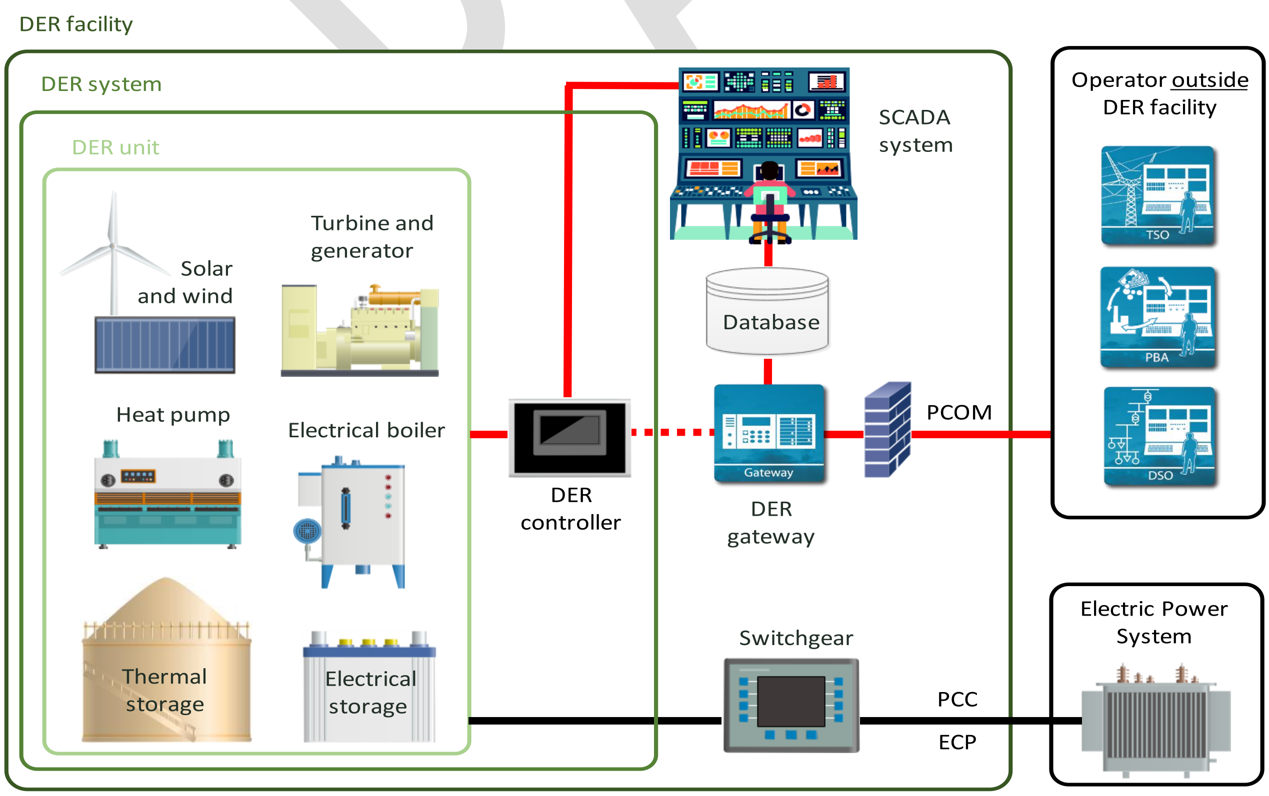


Figure 8 – Reference architecture for this specification

Information model

A very important part of the IEC 61850 standard is the Information model. This is basically a naming convention that defines unique names for all the functionalities and components inside the DER facility. The functionality and components are organised into entities called Logical Nodes (LN).

The information model in IEC 61850-7-420 can be divided into 3 basic groups for LN's, which we in this specification name: **DER facility**, **DER system** and **DER unit**.

In the following, some tables provide information about the available logical nodes within the IEC 61850-7-420 domain, and the basic group they belong to. The tables also have a reference to the package within the IEC 61850 UML model where the logical node is defined. The UML model is described in the "IEC 61850 information model in UML" section in this specification.

The newest version of IEC61850-7-420 from IEC is the edition 1 (IEC61850-7-420:2009) from 2009, but a new edition 2 is currently in 'Preparation of Collected Comments' stage, with a target date of Marts 2020 for the final standard.

Note: This ENDK-61850-SPEC is using the latest draft version from the IEC TC57 WG17 working group, which means that the descriptions in the section of the report about 'Information Model' can change and will be updated until the final standard for IEC61850-7-420 is released by IEC and Dansk Standard.

DER facility Logical Nodes

The main purpose of this group of LNs are to represent the information which is for the whole DER facility, basically the nameplate information of the physical and logical components.

LN Group	UML Package	LN	Title	Description
DER facility	ECP	DCCT	DER economic dispatch parameters	defines the DER economic dispatch parameters. Each DCCT is associated with one or more ECPs
DER facility	ECP	DCRP	DER plant corporate characteristics at the ECP	defines the corporate and contractual characteristics of a DER plant. A DER plant in this context is defined as one DER unit and/or a group of DER units which are connected at an electrical connection point (ECP). The DCRP LN can be associated with each ECP (e.g. with each DER unit and a group of DER units) or just those ECPs where it is appropriate.
DER facility	ECP	DOPA	DER operational authority at the ECP	associated with role based access control (RBAC) and indicates the authorized control actions that are permitted for each "role", including authority to disconnect the ECP from the power system, connect the ECP to the power system, change operating modes, start DER units, and stop DER units. This LN could also be used to indicate what permissions are in effect. One instantiation of this LN should be established for each "role" that could have operational control. The possible types of roles are outside the scope of this standard.
DER facility	GridCodes.ECP	DECP	Electrical Connection Point (ECP)	contains the operational characteristics of the Electrical Connection Point (ECP), including "nameplate" or static information (identity, type), settings (nominal voltage, frequency), and measurements (pointers to MMXU and MMXN data objects)
DER facility	GridCodes.Connect	DCND	Disconnect and connect DER	causes the DER to disconnect which could be cease to energize or could be via a switch to cause galvanic isolation. Connect would initiate the reconnection.
DER facility	GridCodes.Connect	DCTE	Cease to energize	causes the DER to cease to energize
DER facility	GridCodes.RideThrough	DVRT	Voltage high/low ride-through	defines the curves for high/low voltage ride-through events, the status during an event, and a count of events
DER facility	GridCodes.RideThrough	DFRT	Frequency high/low ride-through	defines high/low Frequency ride-through. Each curve defines the boundary between the different zones.
DER facility	GridCodes.FrequencySupport	DFWP	Set active power level based on frequency	provides parameters as the settings for active power based on frequency
DER facility	GridCodes.FrequencySupport	DFWC	Set active power based on frequency	allows more flexibility in defining the frequency-watt function by using curves for both high and low frequencies

LN Group	UML Package	LN	Title	Description
DER facility	GridCodes.VoltageSupport	DVWC	Set active power based on voltage	supports the Volt-Watt mode which establishes volt-watt curves that are used autonomously by the DER to respond to changes in voltage over or under nominal voltage by changing active power as a means to counteract those voltage high or low levels
DER facility	GridCodes.VoltageSupport	DVAR	Set reactive power level	defines the Set Reactive Power mode. The amount of reactive power is set as a percentage of VarMax.
DER facility	GridCodes.VoltageSupport	DVVR	Set reactive power based on voltage	establishes volt-var curves that are used autonomously by the DER to respond to changes in voltage over or under nominal voltage by changing reactive power as a means to counteract those voltage levels
DER facility	GridCodes.ActivePower	DWLM	Mode to cause DER to limit active power	defines the mode that causes the DER to limit active power at the Referenced ECP to the target value
DER facility	GridCodes.ActivePower	DWST	Mode to cause DER to set active power	defines the mode in which the DER's active power at the Referenced ECP is set to the target value
DER facility	GridCodes.ReactivePower	DWPF	Set power factor by feed-in power for WP41	supports the W-PF mode, by setting the power factor based on watts output
DER facility	GridCodes.ReactivePower	DRGS	Provide dynamic reactive current support	provides the settings for dynamic reactive current support functions
DER facility	GridCodes.ReactivePower	DWVR	Set reactive power based on active power	When in the Watt-VAr mode, the DER shall actively control the reactive power output as a function of the active power output following a target real power – reactive power (Watt-Var or P-Q) curve.
DER facility	CHP	DCHC	CHP system controller	supports the CHP controller. The CHP controller provides overall system information from the CHP system to external users, including identification of the types of equipment within the CHP system, usage issues, and constraints affecting the overall CHP system, and other parameters associated with the CHP system as a whole.

DER system Logical Nodes

The main purpose of this group of LN's are to get information about an aggregated functionality.

LN Group	UML Package	LN	Title	Description
DER System	DERController	DRCT	DER maximum and default characteristics	defines the maximum and default capabilities of one DER unit or aggregations of one type of DER device with a single controller.
DER System	DERFunctions	DFWB	Set active power based on frequency	describes the frequency-watt with boundary conditions
DER System	SFC	DSFC	Speed/Frequency controller	defines the characteristics of the speed or frequency controller.

DER unit Logical Nodes

The main purpose of this group of LN's are to get information from and controlling a single DER unit.

LN Group	UML Package	LN	Title	Description
DER Unit	DERGenerator	DRAT	DER generator ratings	defines the DER nameplate ratings for all types of inverter-based and synchronous DER systems, including generators and storage, but excluding controllable load.
DER Unit	DERGenerator	DGEN	DER unit generator	defines the operational state of DER generator
DER Unit	DERGenerator	DRAZ	DER advanced unit ratings	defines the DER advanced ratings. These are established as status objects since they are not expected to be remotely updated except through the use of the system configuration language or other direct intervention.
DER Unit	DERGenerator	DCST	DER unit operational cost	provides the economic information related to DER operating characteristics. In some implementations, it is expected that multiple DCST LNs will be used for different seasons or for different operational conditions.
DER Unit	DERExcitation	DREX	Excitation ratings	defines the DER excitation ratings. These are established as status objects since they are not expected to be remotely updated except through the use of the system configuration language or other direct intervention.
DER Unit	DERExcitation	DEXC	Excitation	provides settings and status of the excitation components of DER devices.
DER Unit	DERInverter	DINV	Inverter	defines the characteristics of the inverter, which converts DC to AC. The DC may be the output of the generator or may be the intermediate energy form after a generator's AC output has been rectified.

DER Unit	DERInverter	DRTF	Rectifier	defines the characteristics of the rectifier, which converts generator output AC to intermediate DC.
DER Unit	DERInverterSpecialPurpose	DGSM	Issue “operational mode control” command	MAY BE DEPRECATED. Control commands to activate each type of mode are issued through LN DGSM. Multiple instances of LN DGSM can be used for managing multiple modes.
DER Unit	DERInverterSpecialPurpose	FMAR	Mode curves and parameters	MAY BE DEPRECATED. defines mode curves and parameters
DER Unit	ReciprocatingEngine	DCIP	Reciprocating engine	supports the reciprocating engine characteristics required for remote monitoring and control of reciprocating engine functions and states
DER Unit	FuelCell	DFCL	Fuel cell controller	provides the fuel cell characteristics required for remote monitoring of critical functions and states of the fuel cell itself.
DER Unit	FuelCell	DSTK	Full cell stack	supports monitoring of the fuel cell stack. Fuel cells are stacked together to provide the desired voltage level
DER Unit	FuelCell	DFPM	Fuel processing module	supports the fuel processing module of the fuel cell. The fuel processing module of the fuel cell is used to extract hydrogen from other types of fuels. The hydrogen can then be used in the fuel cell to make electricity
DER Unit	Photovoltaic	DPVA	Photovoltaics array characteristics	support PV array characteristics. The photovoltaics array characteristics describe the configuration of the PV array. The logical node may be used to provide configuration information on the number of strings and panels or the number of sub-arrays in parallel
DER Unit	Photovoltaic	DPVM	Photovoltaics module ratings	describes the photovoltaic characteristics of a photovoltaic module, including ratings.
DER Unit	Photovoltaic	DPVC	Photovoltaics array controller	supports the photovoltaic array controller and reflects the information required for remote monitoring of critical photovoltaic functions and states. If the strings are individually controlled, one DPVC per string would be required to describe the controls.
DER Unit	Photovoltaic	DTRC	Tracking controller	support the PV tracking system. The tracking controller provides overall information on the tracking system to external users. This LN can still be used for defining array or device orientations even if no active tracking is included.
DER Unit	CHP	DCTS	Thermal storage	describes the characteristics of the CHP thermal storage. This LN applies both to heat storage and to coolant storage, and is used for measurements of heat exchanges
DER Unit	CHP	DCHB	Boiler	describes the characteristics of the CHP boiler system
DER Unit	FuelSystem	DFUL	Fuel supervision	models fuel supervision.
DER Unit	FuelSystem	DFLV	Fuel delivery system	describes the delivery system for the fuel.
DER Unit	Storage	DBTC	Battery charger	The battery charger characteristics covered in the DBTC logical node reflect those required for remote monitoring and control of critical auxiliary battery charger.
DER Unit	DERUnit	DUNI	DER unit (generator or storage)	defines the actual connected and operational state of a DER unit. It does not include controllable load.

Normative signal list from a Danish perspective

This specification uses two types of signal lists, a normative signal list and a reference signal list. The normative signal list refers to the Danish regulations according to the European regulations in RfG and DCC, as well as normative signals for delivering different types of ancillary services. The reference signal list is a common signal list including other signals necessary or of interest for Danish power system actors. The reference signal list is based on experience from the reference signal list developed in the CHPCOM project (see ANNEX C – to be included)

The reference signal list shows signals for the DER facility and specific types of DER systems and DER units, based on which power grid services the facility, system or unit provides or uses. Signals marked with a 'M' are mandatory signals, meaning that they must be present if the power grid service for which they have been marked as mandatory is utilised. Signals without a 'M' are optional and needs only be implemented if they are necessary for operating and monitoring the processes of the DER facility.

The signals are organized based on the purpose of the signal, where the signal originates and the type of signal.

The purpose is one of:

- operational data, that provides information on measurements and status, and means for sending commands and changing settings.
- static data, that contains seldom changed or never changed information (e.g. nameplate details) on the facility, the systems within the facility and the units within the systems.
- statistical data, that provides calculated, measured or manually entered data for statistical purposes.

A signal originates from either the DER facility, a DER system or a DER unit. Please reference the section "Reference Designation System Rules according to ISO/IEC 81346" for information on how to determine where the signal originates based on its IEC 61850 tag.

The type of signal is according to the common data class categories defined in IEC 61850-7-3:2010

- status information shows status of a process or function
- measured and calculated information are analogue values measured from a process or calculated in a function
- commands are signals which can change the state of controls, like start/stop of a diesel genset
- settings are signals which configure a process or function

The IEC 61850 name of the signal is reflected in the "61850 tag" column. Please reference the section "Reference Designation System Rules according to ISO/IEC 81346" for details on how to determine the origin of a signal based on how it is named.

The normative reference signal list is shown in ANNEX D (to be included).

Further, the reference signal list and the required ACSI services are being described as an ICD file, to allow easy adaptation in the configuration tools for a DER gateway. The content of the ICD file is shown in ANNEX .

IEC 61850 information model in UML

The IEC 61850 information model is modelled in UML. This helps in improving the quality of the model, as consistency checks can be done by a tool and mistakes fixed before the information model is released. Besides the documentation, which can be autogenerated, it helps vendors when implementing the model.

The complete UML model is huge and is provided when purchasing the standard. Below is an example on how support for grid codes has been modelled.

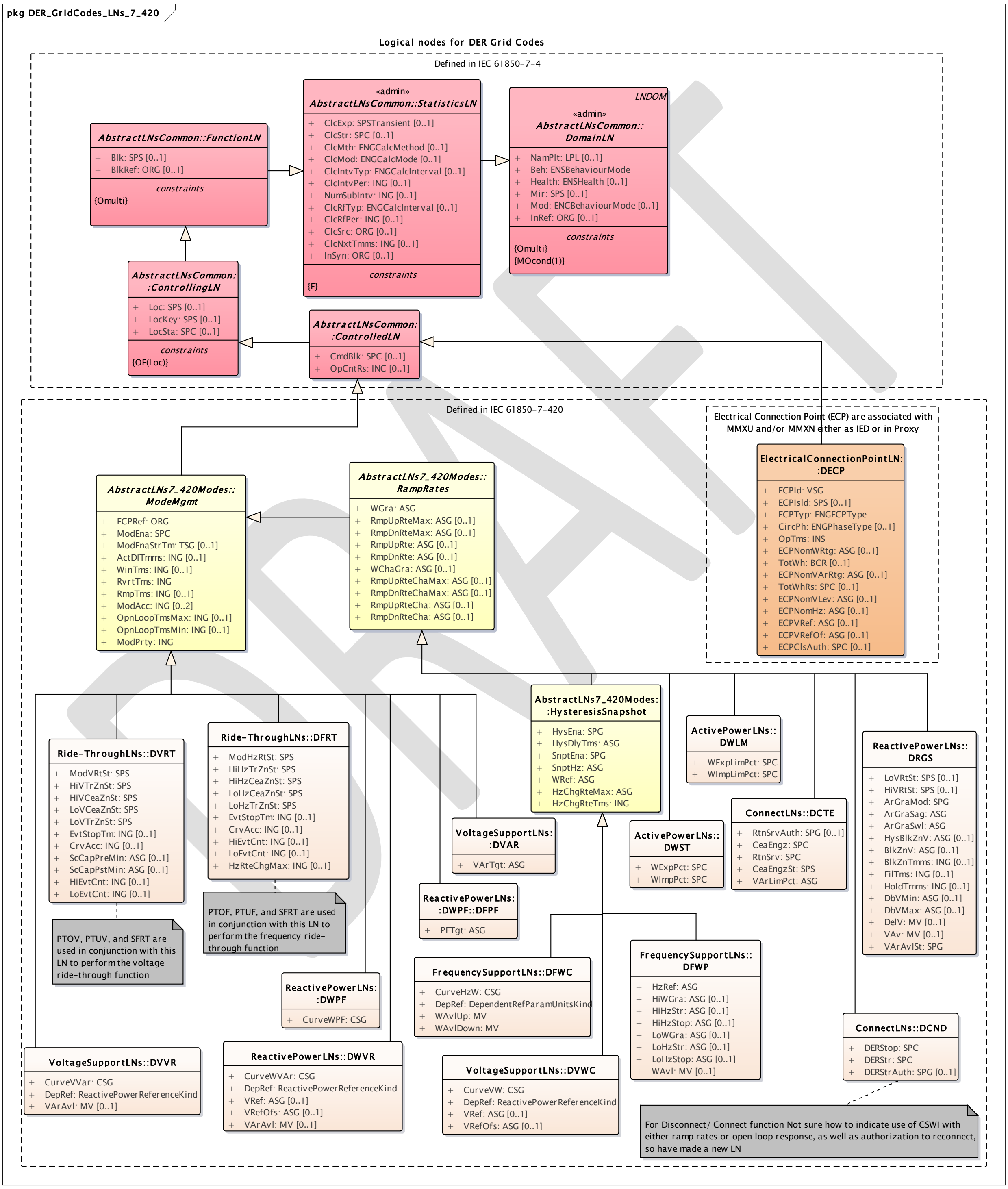


Figure 9 –The IEC 61850-7-420 Grid Codes information model in UML (May 2017)

Reference Designation System Rules according to ISO/IEC 81346

The signals in the reference signal list are named according to the following format:

<Logical Device name>/<Logical Node name>.<Data Object name>.<Data Attribute name>

where the section before the '/' separator follows rules specified by ISO/IEC 81346 and the section after the '/' separator is specified by the structure of the IEC 61850 information model.

ISO/IEC 81346 (also known as RDS – Reference Designation System) specifies classification and structure based on different structure types.

In this specification, the DER facility is the top level and is using a location-type structure (identified by a leading '+' character). The levels below identify the DER systems and DER units and are using a function-type structure (identified by a leading '=' character).

NOTE: In the current edition 2 of IEC 61850-8-1, the MMS protocol does not allow object references to include other characters than a-z, A-Z, 0-9 and '_' (underscore), and the first character must be a letter. As a work around, this specification replaces the leading '+' with the letters "EIC" and the first '=' sign with an underscore. The following unsupported characters are just left out, which is in accordance with the rules of ISO/IEC 81346. E.g. the code "+45W000000000099Y=HG2=GA1=EM" is to be represented in the IEC 61850 tag as "EIC45W000000000099Y_HG2GA1EM".

The ISO/IEC 81346 standard provides some options for naming of the topmost location name (top name). In this specification, the DER facility is named according to the Energy Identification Coding scheme (EIC) codes defined by the ENTSO-E organization and used in the EU transparency platform for identification of actors, sub stations, power plants, etc., in the European public electricity grid

Next to the top location name IEC 81346-2:2019 is used for functional naming of the component to which the information in the IEC 61850-7-x Logical Node refers. See examples in IEC 61850-6 and IEC 61850-7-1.

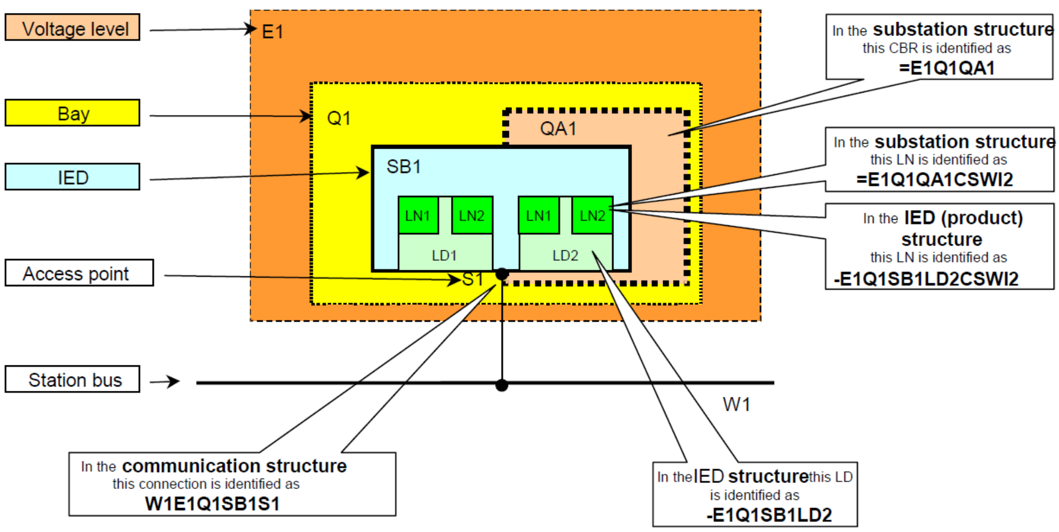


Figure 13 – Names within different structures of the object model

Figure 10 –Names and structure of IEC61850 using IEC81346 topology

This means, the ISO/IEC 81346 logical device name for the logical node follows the information the of the physical device the logical node information represents. E.g. a central controller or can collect information from a circuit breaker and from a generator. In this case the IEC 61850 signal tag for the circuit breaker uses the ISO/IEC 81346 functional name for the circuit breaker and IEC 61850 signal tag for the generator uses the ISO/IEC 81346 functional name for the generator.

Please reference ANNEX E for a list of typical classification codes from ISO/IEC 81346-2:2019 to be used with this specification.

In accordance with ISO/IEC 81346, new classification types can be added to the list in ANNEX E, to identify types of systems and units not covered in the annex.

EIC naming rules

In Denmark, EIC codes are assigned by Energinet.

According to the documentation at http://www.eiccodes.eu, an EIC code is defined using three sections:

- a two-character Local Issuing Office (LIO) code. In Denmark, this is always the number 45.
- a one-character object type code:
    - Y : Areas - Areas for inter System Operator data interchange
    - Z : Measuring Points - Energy Metering points
    - W : Resource objects - Production plants, consumption units, etc.
    - T : Tie-lines - International tie lines between areas
    - V : Location - Physical or logical place where a market participant or IT system is located
    - A : Substations
- 12 characters allocated by the issuing office.
- one check character to ensure the code validity. The algorithm for calculating the check character is described in the EIC Code implementation guide.

Valid characters of an EIC code are A-Z, 0-9 and '-' (minus).

As an example, the power plant at Silkeborg exists as two codes:

- 45V0000000000245 for the location (IT system)
- 45W000000000099Y for the production or consumption resources

Energinet is to be contacted on **eic-administration@energinet.dk** to acquire a EIC code for a plant.

For more information about EIC codes from Energinet: https://energinet.dk/El/Ny-paa-elmarkedet/EIC

Note, only facilities or actors already registered through the relevant TSO or DSO can acquire a EIC code, and only if it has not already been assigned an EIC code. See https://www.entsoe.eu/data/energy-identification-codes-eic/eic-approved-codes/.

Time synchronization and Time stamping rules

Synchronisation of time is critical because every aspect of managing, securing and monitoring operation of resources connected to the power grid involves determining when events happened. For example, when using SecureMMS, all requests are timestamped at client side, and when received at server side, the timestamp is compared to the current time. And, if the time difference is greater than what is deemed secure, the request is rejected.

According to IEC 61850-8-1, SNTP v4 (RFC 4330) shall be used for time synchronisation. This is of great concern, as SNTP lacks advanced features that allows it to calibrate and hence maintain accurate synchronisation. Further, SNTP lacks security features to detect/prevent so called false tickers – i.e. time servers providing wrong time.

So, while SNTP is a viable solution for smaller networks, it is not well suited for synchronising large clusters of clients, such as DER gateways and IEC 61850 clients connected to the public internet.

Instead it is recommended that either NTP (Network Time Protocol) or PTP (Precision Time Protocol) is used for synchronising the system time of a DER gateway.

NTP is a protocol used for the dissemination of accurate time in computer networks, typically in the milliseconds range. It is a client-server-based protocol, where clients request accurate time from a server, and the server responds accordingly.

PTP is like NTP, only it caters for more accurate time stamps, typically in the sub-microseconds range. But to achieve this improved accuracy, the PTP servers must be connected in a network where the switches has been configured as a transparency clock or boundary clock. Otherwise the accuracy is to be expected to be similar to what's achievable from a NTP server.

To be compliant with this specification, a DER gateway acting as time synchronisation client shall comply with the following requirements:

- The client shall support querying time using NTP and/or PTP.
- In case of NTP, the client shall
  - send NTP mode 3 (unicast) requests to the server.
  - accept NTP mode 4 (unicast) responses from the server.
- In case of PTP, the client shall send and accept messages using UDP in compliance with IEEE-1588
- Whether using NTP or PTP, the client must guard against IP spoofing of the time servers used.
  - Using NTP, this can be achieved by using NTP Authentication, which uses non-reversible signatures generated by the server and checked by the clients.
  - Using PTP, identification and authorisation of master clocks can be used. It can be further improved by also authenticating transparent clocks and Announce messages.
- The client shall only use time servers that comply with the server requirements below.
- If using NTP, the client shall guard itself from "false tickers" (servers providing incorrect time information). With four servers, the client is protected against one "false ticker". For protecting against more than one "false ticker", a 2n+1 algorithm is used to calculate required numbers of servers; five servers protect against two "false tickers", seven servers protect against three "false tickers", and so on.

A server used for time synchronisation shall comply with the following requirements:

- For NTP servers, the server shall
  - accept NTP mode 3 (unicast) requests from clients.

    - respond to NTP mode 3 (unicast) requests with a NTP mode 4 reply.
    - run at Stratum level 1 or 2 (the level defines the distance from the reference clock)
        - A Stratum-1 server is directly linked to a reliable source of UTC time, and typically has 10 microseconds accuracy to UTC
        - A Stratum-2 server is connected to a Stratum-1 server using a network connection and typically has 0.5 - 100 millisecond accuracy to UTC
- For PTP servers, the server shall accept and send messages using UDP, in accordance with IEEE-1588

NTP note: The reference clock source that relays the UTC time with no or little delay, is known as a Stratum-0 device. This device is not network connected, but instead directly connected to a computer that then acts as a primary (Stratum-1) time server.

Both the DER gateway and the SCADA system is required to have their system time synchronized with a time server. It is required that they use one or more of the following servers

TODO: list of trusted NTP/PTP servers

The list of trusted time servers is compiled as described below.

For a time server to get on the list, the following requirements, besides those already mentioned, shall be matched:

- stratum 1 server (for getting the best possible accuracy in the provided timestamps)
- stratum 0-time source: GPS, atomic clocks
    - for GPS satellites, consider that some are occasionally being fiddled with (like the US did during the Gulf war)
- authenticated server (makes it harder to tamper with the server, without the clients knowing it)

List of servers for inspiration:

- http://support.ntp.org/bin/view/Servers/ServersAuthenticatedWithAutokey?sortcol=1;table=1;up=2#sorted_table
- http://support.ntp.org/bin/view/Servers/ServersAuthenticatedWithMD5
- https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-authenticated-ntp-service

Note:

Only a few European authenticated NTP servers exists, and none are in the northern parts of Europe.

It therefore should be considered if the European TSOs could setup a network of NTP servers, synchronized across borders.

The only real alternative is to use the pool of servers provided by ntp.org, but these servers are not authenticated, nor are their location known besides the continental zone or country.

Network requirements

The DER facility is required to run separate IT networks for SCADA/61850 and office communication. Traffic on the office network shall not be allowed to enter the technical network, and it is recommended that traffic from the technical network has no path or a firewall restricted and monitored path to the office network.

Wireless hotspots are not allowed on the technical network.

The following table lists the communication ports that a DER gateway uses in its operation. These ports shall be configured as open in the firewall of the DER facility to the DER Gateway.

Direction	Protocol	Port	Description
Inbound	TCP	3782	SecureMMS – exchange of IEC 61850 data using the MMS protocol protected with SSL.
Outbound	TCP	514 (Optional)	Syslog – sending of DER gateway system logs to a remote server, allowing analysis of the operation of the DER gateway. Further, such analysis can provide information supporting security audits in close to real time.
Outbound	TCP/UDP	123 (Optional)	NTP - Network Time Protocol. The DER gateway needs to synchronise its system time with a time server. In case of using NTP and if the server is located outside the facility, this port needs to be open.
Outbound	UDP	319, 320 (Optional)	PTP – Precision Time Protocol. In case the DER gateway synchronises its system time with a PTP server outside the facility, these two ports are needed.

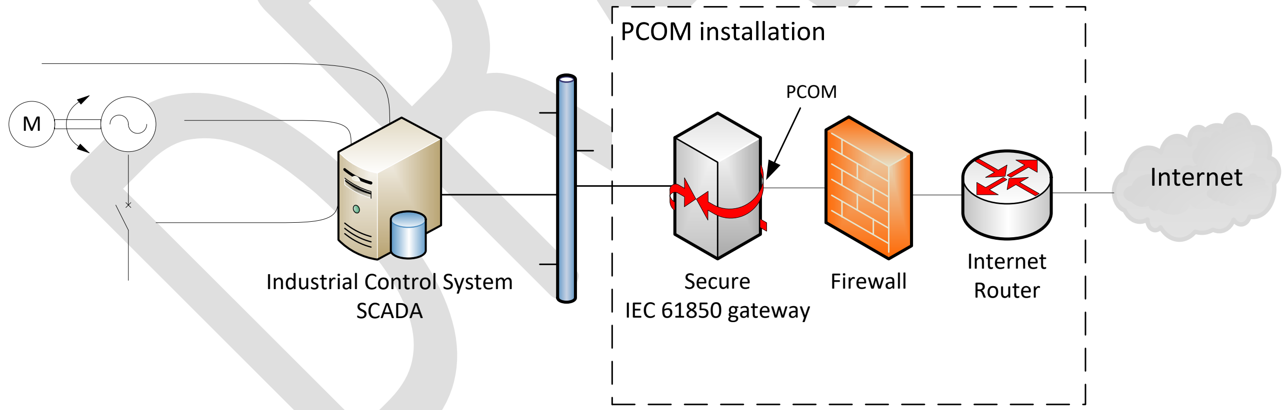


Figure 11 – Components for a secure interface at PCOM

Quality-of-Service

Using IEC 61850 for communication between a DER facility and an actor does not require a lot of bandwidth. The MMS protocol uses an encoding that is quite efficient at limiting the number of bytes, and the IEC 62351 security extension only adds a few percent extra to the byte count. In a real-world setup, typical packet size seen on the wire is 200 bytes for actor (IEC 61850 client) requests and 150-170 bytes for the DER facility (IEC 61850 server) responses.

More importantly is the network latency, i.e. the delays incurred in the processing of network data. Every device involved in the transport of data, adds to the latency.

In Denmark, typical latency in wired broadband networks connected to the internet is below 20ms. For critical facilities it is recommended that the latency end-to-end is kept below 35ms. For non-critical facilities the latency end-to-end should be kept below ?ms.

TODO: investigate trace of a full day schedule with respect to byte count and transfer time.

Investigation of a two days schedule sent from a BRP/AGG to a CHP plant, has provided information as follows. The trace was generated from packets sent between a client and a server on a local 1GB switched network (round trip latency between 0.24 and 0.5 ms), with SSL enabled. The trace includes schedule setup, 576 value updates and schedule enable.

The total time of exchanging the schedule is 2.285 seconds, involving 2350 ethernet frames. Client and server send packets alternately (i.e. client send, server send, client send, server send). The calculated time per byte and throughput is a rough estimate based on totals instead of time per frame, because no details on sent and received timing was available. Hence the time and throughput is nothing but indicative.

Direction	Bytes on wire	Time/byte	Throughput
client -> server	245599	4.65 µs	1.72 Mbit
server -> client	180127	6.34 µs	1.26 Mbit

Basic information security

End-to-End security based on IEC 62351-4:2018

It is required to use different certificates for the application layer and the transport layer. This way, different providers can be selected to reduce the risk of a security breach due to a compromised certificate. For the A-profile application layer, it is recommended to use a NemID FOCES certificate (NemID Funktionssignatur), while for the T-profile transport layer an SSL certificate from one of the trusted certificate providers are to be used.

All certificates used with the DER Gateway shall use at least 2048-bit keys and SHA-256.

For an SSL certificate provider to be present on the list of trusted providers, the following requirements shall be met:

- shall support the SCEP and EST protocols (according to IEC 62351-9:2017)
- shall support retrieval of cert status, using either CRL or OCSP (according to IEC 62351-9:2017)
- shall be a global CA or an RA just below the CA (to have the smallest possible certificate chain)
- provided certificates shall use at least 2K RSA keys and SHA-256 (to achieve a reasonable security level)

Just as an example, the following table provides a list of candidates, selected based on organisation size and reputation. These are then closer examined with respect to the requirements.

Provider	SCEP	EST	CRL	OCSP	Encryption	Hashing	Cert price range
Comodo	yes	yes	no	no	RSA-2048	SHA-256	\$99 - \$249
GeoTrust	no	no					
DigiCert	yes	yes	yes	yes	RSA-2048	SHA-256	\$198 - \$658
GlobalSign	yes	no			RSA-2048	SHA-256	\$249 - \$849
Symantec	yes	no				SHA-256	
Thawte	no	no					
IdenTrust	no	no					
Entrust	yes	yes	no	yes	RSA-2048/3072/4096 ECC	SHA-2	\$174 - \$609
Network Solutions	no	no					
RapidSSL	no	no					

Having examined the candidates, the list of trusted providers would include:

- DigiCert (https://www.digicert.com/)
- Entrust (https://www.entrustdatacard.com/)

The following 12 shows in principle a communication setup between a control center and a plant controller through an intermediate gateway in the control center. During transport layer establishment, the control center acts as a client, and the plant controller acts as a server, while the intermediate gateway acts as a server towards the control center and as a client towards the plant controller.

X.509 certificates are required on both client and server for both the A and T communication profiles. Certificates with the public key are to be distributed to ”the other end”; e.g. of the certificates for the plant controller, the T-profile certificate has to be distributed to the control center gateway, while the A-profile certificate has to be distributed to the control center. Likewise, the A-profile certificate of the control center and the T-profile certificate of the gateway must be distributed to the plant controller.

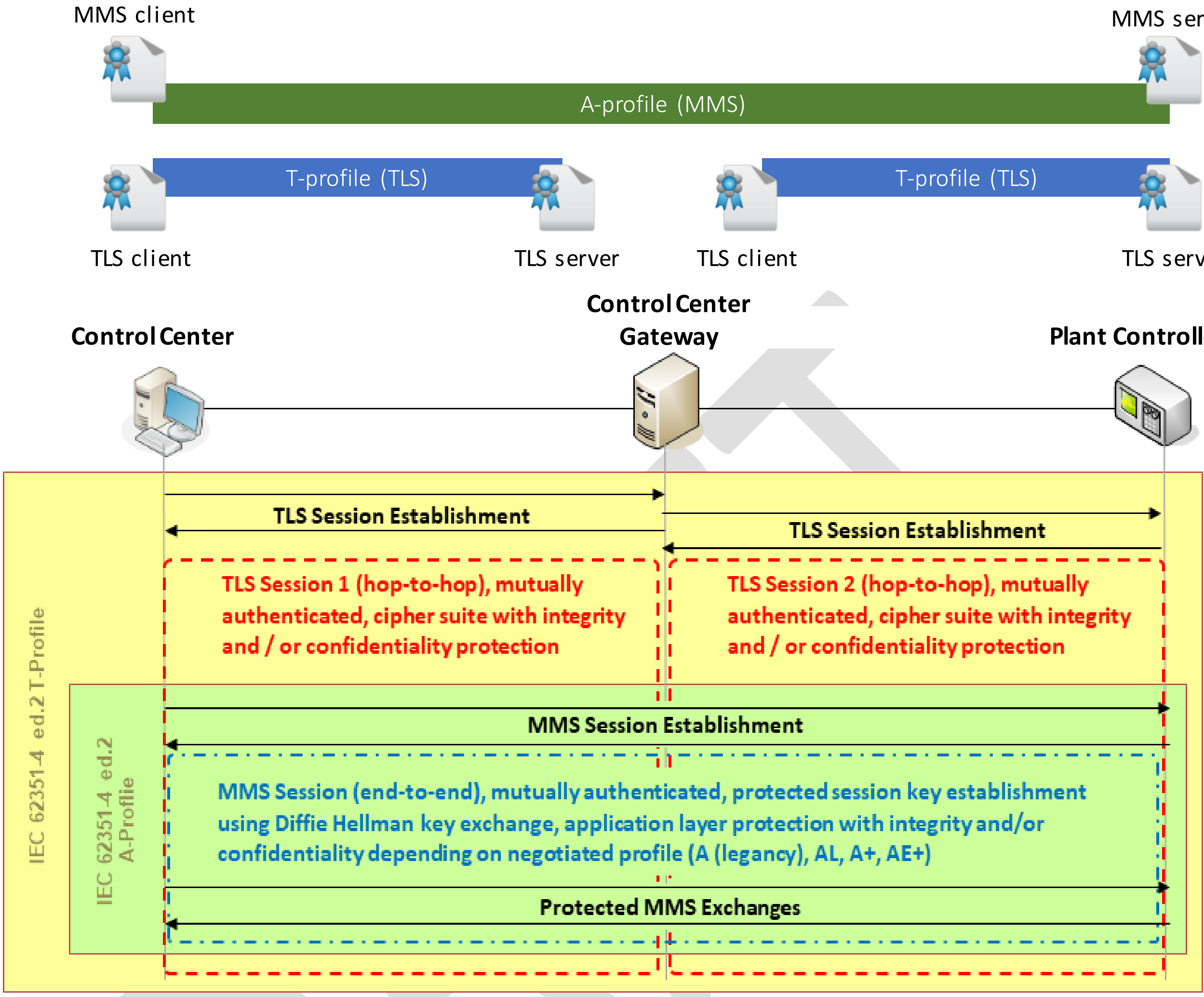


Figure 12 Application and transport layers and the use of certificates

TODO: describe how to check and fetch certificates with the public key at the certificate provider.

Conformance and Interoperability

Why is this important?

In an ideal world a technical standard for data communication would be an international consensus document, which was so generic that it would bridge to all existing implementations in the field, but also so specific that it would not be possible to misunderstand.

International standards are not ‘implementation guidelines’ and there will always be a risk of misinterpretation.

Therefore, it is important to have conformance specifications that specify how a product can be conform to a given standard – and interoperability specification for describing how products from different vendors should test their interoperability.

Definition of Compatibility levels of Interoperability[1]

Interoperability between data communication devices has been specified as different ‘compatible levels’ by IEC TC65. The data communication device has been divided into 7 device features, ranging from the low-level communication profile (protocol and interface) to the more high-level device profile (behavior, functionality, semantic) and with an overlap on the data types and data access.

The definition ‘Device features’ cannot be directly mapped to the different layers in the IEC 61850 series, but it still is a good method for understanding the basic concept of Interoperability.

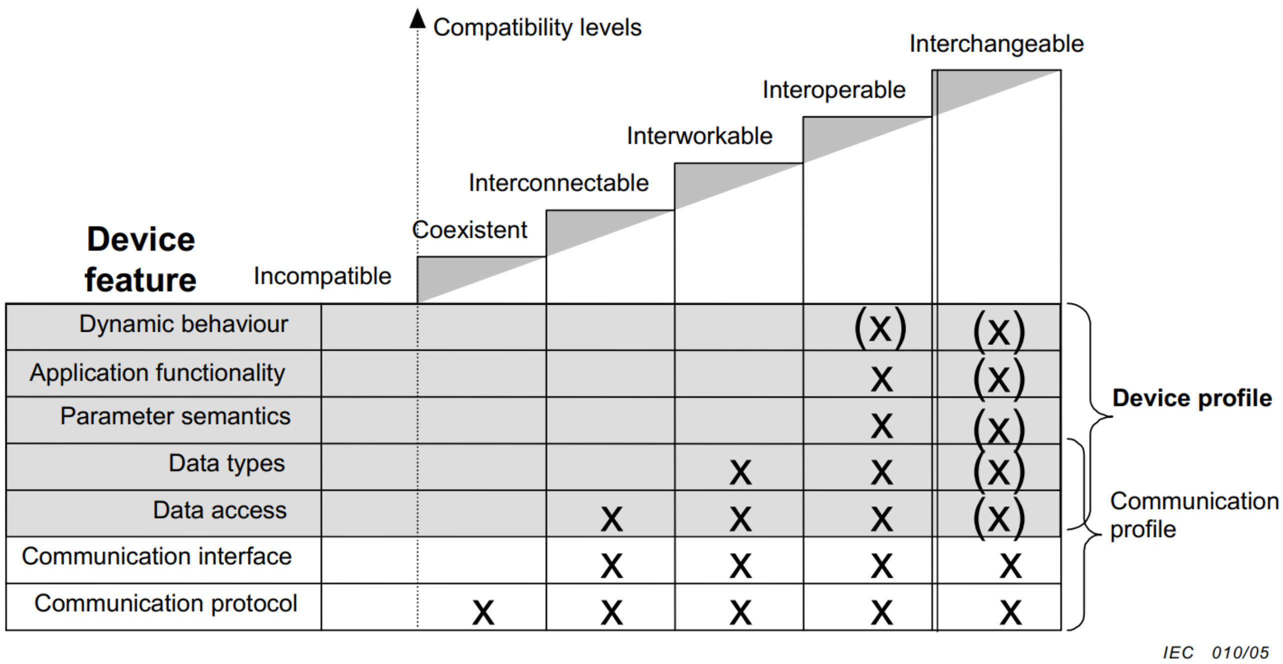


Figure 13 IEC 010/05 figure from IEC TC65 TR 62390

[1] IEC 62930:2005 edition 1.0 Common automation device – Profile guideline

Incompatibility: Two or more devices are incompatible if they cannot exist together in the same distributed system.[2]

Coexistence: Two or more devices coexist on the same communication network if they can operate independently of one another in a physical communication network or can operate together using some or all of the same communication protocols, without interfering with the use of other devices

Interconnectability: Two or more devices are interconnectable if they use the same communication protocols, communication interface and data access.

Interworkability: Two or more devices are interworkable if they can transfer parameters between them, i.e. in addition to the communication protocol, communication interface and data access, the parameter data types are the same.

Interoperability: Two or more devices are interoperable if they can work together to perform a specific role in one or more distributed application programs. The parameters and their application-related functionality fit together both syntactically and semantically. Interoperability is archived when the devices support complementary sets of parameters and functions belonging to the same profile.

Interchangeability: Unlike the other compatible levels (which refer to two or more devices working in the same system) interchangeability refers to the replacement of one device with another. Devices are Interchangeable for a given role in a distributed application system if the new device has the functionality to meet the application requirements.[3]

Different degrees of interchangeability may be applicable for various roles of a device, for example, control, diagnosis, parameterization/configuration. That means that one device can have different degree of interchangeability regarding different interfaces to the system.

Conformance testing of products

Conformance testing for data communication products are typical based on a ’Protocol Implementation Conformance Statement’ (PICS) which is provided by the product manufacturer and defines what mandatory, optional or conditions features of a given standard that is implemented.

The PICS can be extended with extra information for testing ‘Implementation eXtra Information for Testing (IXIT) like administrative settings, test-suite specifications or in case of Protocol information (PIXIT) a service model like the ACSI.

The Model Implementation Conformance Statement (MICS), Technical Issues Implementation Conformance Statement (PICS) and IEC Configuration Description (ICD) in SCL-format are typically also included in the Conformance Statement and testing process, for an IEC 61850 product.

[2] NOTE Incompatibility can result from differences in application functionality, data semantic, data types, communications interface, or even communications protocols used by the affected devices. Incompatible devices may even interfere with or prevent each other’s proper communication or functioning (possibly even destructively), if placed in the same distributed application network.

[3] Full interchangeability regarding the entire device performance is nearly impossible to achieve. However, actual device interchangeability is dependent on the application requirements for the device.

Interoperability testing of PCOM

The Point of Communication (PCOM) interface is the most critical element from an interoperability point of view, for communication between the DER facility and the system operators.

This PCOM interface should be well defined and tested on both sides (red and yellow in the figure) before the end-to-end 'PCOM testing' can take place.

It is out-of-scope for this specification to define and explain testing methods and systems for this 'PCOM testing', but due to the importance of this activity – this should be addressed in upcoming specifications.

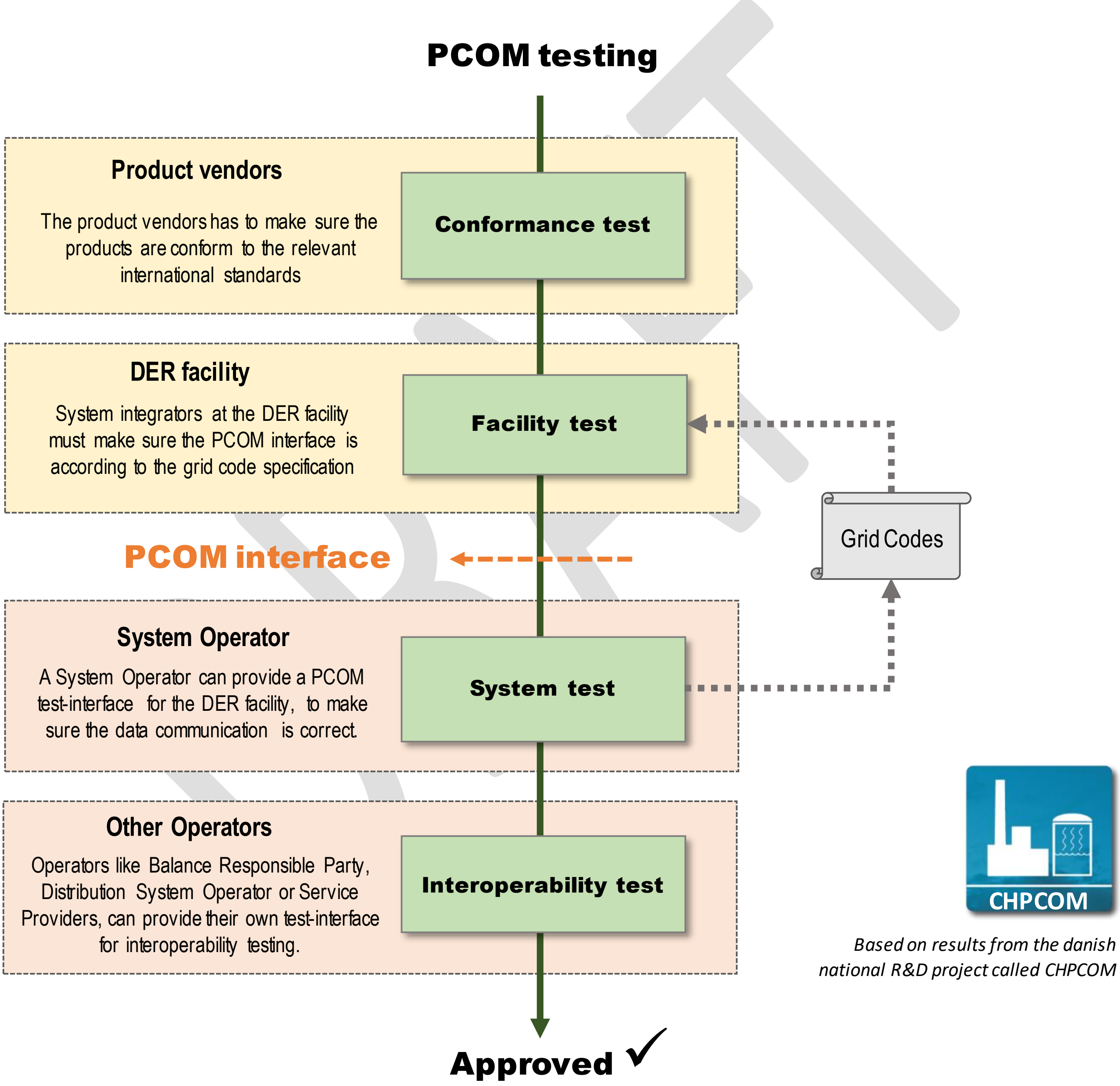


Figure 14 PCOM testing overview from the CHPCOM project

Protocol Implementation Conformance Statement

This specification includes a list of requirements called PICS (Protocol Implementation Conformance Statements) to be implemented in a DER gateway. If all mandatory elements are implemented, the DER gateway implementation will be compliant with the ENDK-61850-SPEC Conformance Statement, including:

- ACSI conformance statement (B11 – B42)
- ACSI models conformance statement (M1 – M17)
- ACSI service Conformance statement (S1 – S60, T1 – T3))

This section states which communication features defined by ACSI (IEC 61850-7-2:2010) is required for a DER gateway to be compliant with this specification.

The conformance statement tables below, uses the same layout as used in the IEC 61850-10 conformance testing document, and the tables can therefore be used when conformance testing a DER gateway in conformance with the procedures described in IEC 61850-10:2012

The following terms are used: Y means "Yes", N means "No", M means "Mandatory / Required", O means "Optional" and a dash means "Not relevant".

ACSI basic conformance statement

The basic conformance statement is defined in Table 1.

Table 1 – ACSI conformance statement

		Client/ Subscriber	Server/ Publisher	Value/ Comments
Client-Server roles				
B11	**Server** side (of TWO-PARTY-APPLICATION-ASSOCIATION)	—	Y/N	
B12	**Client** side of (TWO-PARTY-APPLICATION-ASSOCIATION)	Y/N	—	
SCSMs supported				
B21	**SCSM**: IEC 61850-8-1 used	M	M	
B22	**SCSM**: IEC 61850-9-1 used	O	O	
B23	**SCSM**: IEC 61850-9-2 used	O	O	
Generic substation event model (GSE)				
B31	**Publisher** side	—	O	
B32	**Subscriber** side	O	—	
Transmission of sampled value model (SVC)				
B41	**Publisher** side	—	O	
B42	**Subcriber** side	O	—	

ACSI model conformance statement

The ACSI model's conformance statement is defined in Table 2.

Table 2 – ACSI models conformance statement

		Client/ Subscriber	Server/ Publisher	Value/ Comments
If Server or Client side (B11/12) supported				
M1	**Logical device**	M	M	
M2	**Logical node**	M	M	
M3	**Data**	M	M	
M4	**Data set**	M	M	
M5	**Substitution**	O	O	
M6	**Setting group control**	O	O	
	Reporting			
M7	Buffered report control	O	O	
M7-1	sequence-number	O	O	
M7-2	report-time-stamp	O	O	
M7-3	reason-for-inclusion	O	O	
M7-4	data-set-name	O	O	
M7-5	data-reference	O	O	
M7-6	buffer-overflow	O	O	
M7-7	entryID	O	O	
M7-8	BufTim	O	O	
M7-9	IntgPd	O	O	
M7-10	GI	O	O	
M7-11	conf-revision	O	O	
M8	Unbuffered report control	M	M	
M8-1	sequence-number	M	M	
M8-2	report-time-stamp	O	O	
M8-3	reason-for-inclusion	O	O	
M8-4	data-set-name	M	M	
M8-5	data-reference	O	O	
M8-6	BufTim	O	O	
M8-7	IntgPd	O	O	
M8-8	GI	O	O	
M8-9	conf-revision	O	O	
	Logging	O	O	Required for transfer of statistical data
M9	Log control	O	O	
M9-1	IntgPd	O	O	
M10	Log	O	O	
M11	**Control**	M	M	
If GSE (B31/32) is supported				
M12	GOOSE	O	O	
M13	GSSE	O	O	
If SVC (41/42) is supported				
M14	Multicast SVC	O	O	
M15	Unicast SVC	O	O	
If Server or Client side (B11/12) supported				
M16	Time	O	O	use NTP or PTP

		Client/ Subscriber	Server/ Publisher	Value/ Comments
M17	File Transfer	O	O	

ACSI service conformance statement

The ACSI service conformance statement is defined in Table 3 (depending on the statements in Table 3). In the “AA: TP/MC” column, the acronyms used are AA for “Application Association”, TP for “Two Party” and MC for “Multicast”. The column defines for which type of application association a service is relevant.

Table 3 - ACSI service Conformance statement

	Services	AA: TP/MC	Client (C)	Server (S)	Comments
Server					
S1	ServerDirectory	TP	M	M	
Application association					
S2	Associate		M	M	
S3	Abort		M	M	
S4	Release		M	M	
Logical device					
S5	LogicalDeviceDirectory	TP	M	M	
Logical node					
S6	LogicalNodeDirectory	TP	M	M	
S7	GetAllDataValues	TP	M	M	
Data					
S8	GetDataValues	TP	M	M	
S9	SetDataValues	TP	M	M	
S10	GetDataDirectory	TP	M	M	
S11	GetDataDefinition	TP	O	O	
Data set					
S12	GetDataSetValues	TP	M	M	
S13	SetDataSetValues	TP	M	M	
S14	CreateDataSet	TP	O	O	
S15	DeleteDataSet	TP	O	O	
S16	GetDataSetDirectory	TP	M	M	
Substitution					
S17	SetDataValues	TP	O	O	
Setting group control					
S18	SelectActiveSG	TP	O	O	
S19	SelectEditSG	TP	O	O	
S20	SetSGValues	TP	O	O	
S21	ConfirmEditSGValues	TP	O	O	
S22	GetSGValues	TP	O	O	
S23	GetSGCBValues	TP	O	O	
Reporting (Mandatory for facility type C+D and when delivering system services)					
Buffered report control block (BRCB)					
S24	Report	TP	O	O	
S24-1	data-change (dchg)		O	O	

	Services	AA: TP/MC	Client (C)	Server (S)	Comments
S24-2	qchg-change (qchg)		O	O	
S24-3	data-update (dupd)		O	O	
S25	GetBRCBValues	TP	O	O	
S26	SetBRCBValues	TP	O	O	
Unbuffered report control block (URCB)					
S27	Report	TP	M	M	
S27-1	data-change (dchg)		M	M	
S27-2	qchg-change (qchg)		M	M	
S27-3	data-update (dup)		O	O	
S28	GetURCBValues	TP	M	M	
S29	SetURCBValues	TP	M	M	

Logging (Mandatory for facility type C+D and when delivering system services)					
Log control block					
S30	GetLCBValues	TP	O	O	
S31	SetLCBValues	TP	O	O	
Log					
S32	QueryLogByTime	TP	O	O	
S33	QueryLogByEntry	TP	O	O	
S34	GetLogStatusValues	TP	O	O	

Generic substation event model (GSE)					
GOOSE-CONTROL-BLOCK					
S35	SendGOOSEMessage	MC	O	O	
S36	GetReference	TP	O	O	
S37	GetGOOSEElementNumber	TP	O	O	
S38	GetGoCBValues	TP	O	O	
S39	SetGoCBValues	TP	O	O	
GSSE-CONTROL-BLOCK					
S40	SendGSSEMessage	MC	O	O	
S41	GetReference	TP	O	O	
S42	GetGSSEElementNumber	TP	O	O	
S43	GetGsCBValues	TP	O	O	
S44	SetGsCBValues	TP	O	O	

Transmission of sampled value model (SVC)					
Multicast SVC					
S45	SendMSVMessage	MC	O	O	
S46	GetMSVCBValues	TP	O	O	
S47	SetMSVCBValues	TP	O	O	
Unicast SVC					
S48	SendUSVMessage	TP	O	O	
S49	GetUSVCBValues	TP	O	O	
S50	SetUSVCBValues	TP	O	O	

Control					
S51	Select		O	O	
S52	SelectWithValue	TP	O	O	
S53	Cancel	TP	M	M	
S54	Operate	TP	M	M	
S55	Command-Termination	TP	M	M	
S56	TimeActivated-Operate	TP	O	O	

File transfer

	Services	AA: TP/MC	Client (C)	Server (S)	Comments
S57	GetFile	TP	O	O	
S58	SetFile	TP	O	O	
S59	DeleteFile	TP	O	O	
S60	GetFileAttributeValues	TP	O	O	

Time					
T1	Time resolution of internal clock			10	nearest negative power of 2 in seconds
T2	Time accuracy of internal clock			X	T0
					T1
					T2
					T3
					T4
					T5
T3	Supported TimeStamp resolution	-			nearest negative power of 2 in seconds

Protocol Implementation eXtra Information for Testing (PIXIT)

Please reference ANNEX G for specifications of the PIXIT for each applicable ACSI service mode listed in Table 3.

ACSE authentication for MMS associations

The ACSE authentication is a feature in the MMS protocol, that allows a server to require a password from a connecting client, before a connection is established.

With the use of the security features in SecureMMS, as specified by IEC 62351-7:2017, this simple authentication method is of little value, and hence is not required for compliance with this specification.

Terms and Definitions

The first mandatory task in any standardization and harmonization process, is to agree on common terms and definitions.

In the following table, the most important terms for this specification are defined and with reference to the originator.

Terminology

Term	Term	Definition	Originator
Application Association	AA	An application association provide a mechanism for controlling the access to the instances of a device (access control).	IEC 61850-7-2:2010
Common Data Class	CDC	Common data class that defines the structure of the data object. See IEC 61850-7-3. For common data classes specifically defined for DER logical nodes see clause 8. The literals of enumerated common data classes are described in clause 7.2 (for inherited data objects see their definition in IEC 61850-7-4).	IEC 61850-7-3:2010
Electrical Connection Point	ECP		
DER controller		Physical or virtual component that has functionality that controls and aggregates a number of DER units in a DER system.	
DER facility		Term used for the whole facility (building), which exposes the PCOM data communication interface.	
DER gateway		A physical device that facilitates IEC 61850 communication with clients outside the facility, allowing them to access resources inside the facility.	
DER system		Term used for a functionality that combines several identical or different DER units into a system.	
DER unit		Term used for a single DER device, like a gas turbine or a motor-generator set.	
Logical Device	LD		
Logical Node	LN		
Model Implementation Conformance Statement	MICS	A model implementation conformance statement details the standard data object model elements supported by the system or device.	IEC 61850-10:2012
Manufacturing Message Specification	MMS		
Multicast	MC	Messaging using multicast, e.g. GOOSE and transmission of sampled values.	IEC 61850-7-2:2010
Multicast Application Association	MCAA	Associations for multicast messaging.	IEC 61850-7-2:2010
Point of Common Coupling	PCC	Power delivery point for any grid connected equipment.	
Point of Communication	PCOM	The interface between the DER facility and actors outside the facility, for data communication and information exchange.	
Protocol Implementation Conformance Statement	PICS	A protocol implementation conformance statement is a summary of the communication capabilities of the system or device to be tested.	IEC 61850-10:2012
Protocol Implementation eXtra Information for Testing	PIXIT	The protocol implementation extra information for testing documentation contains system or device specific information regarding the communication capabilities of the system or device to be tested and which are outside the scope of the IEC 61850 series. The PIXIT is not subject to	IEC 61850-10:2012

		standardisation.	
Two Party	TP	Communication between a client and a server.	IEC 61850-7-2:2010
Two Party Application Association	TPAA	Association for two party messaging.	IEC 61850-7-2:2010

Figures

ANNEX A - Basic use cases for information exchange

The best way to explain how IEC 61850 can be used, is to give practical examples of different use cases.

The figure shows seven different use cases, with information exchange between four different actors (system operator, market operator, aggregator and grid operator) and a DER facility (also an actor).

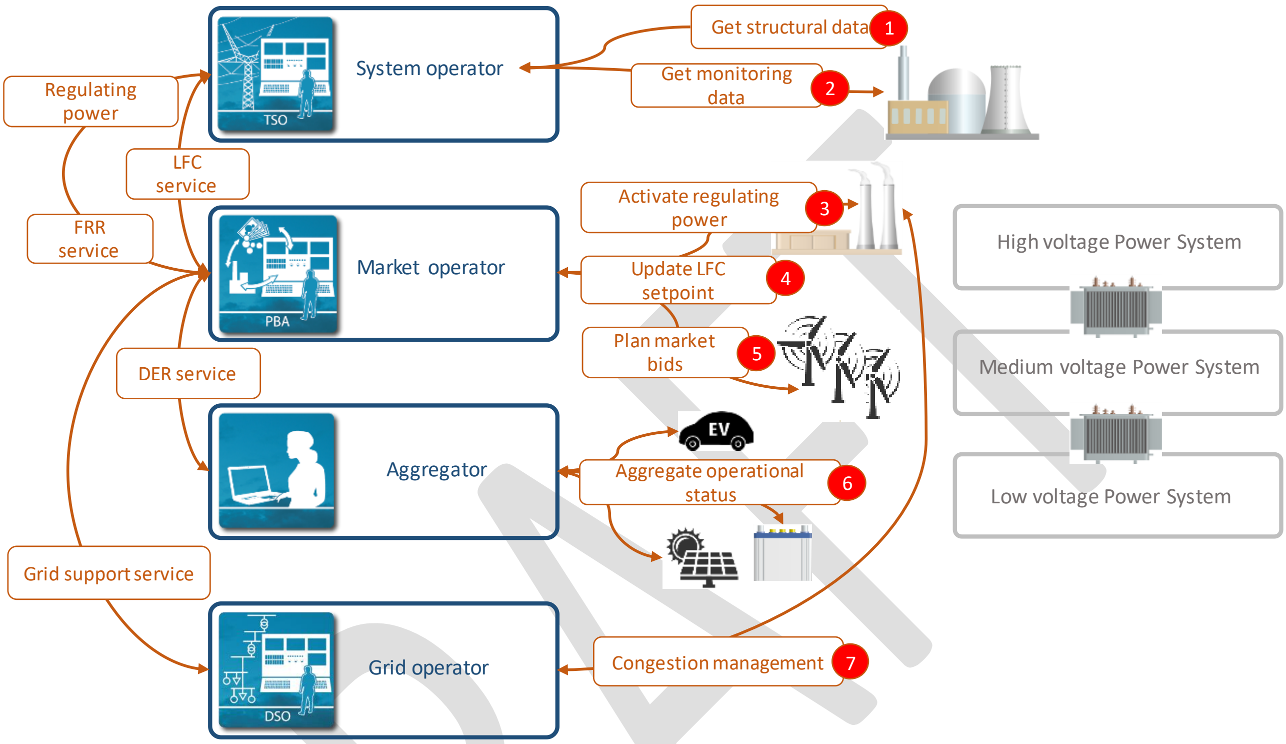


Figure 15 – Overview of use-cases for this specification

The seven use cases are explained on the next pages, using UML use case diagrams and UML sequence diagrams.

The use case diagrams are divided into three levels of use cases: the first level (actor) references the seven use cases from Figure 15 above. The actor use cases include use cases from the second level (function) which describes functions necessary for realising the actor use case. The function use cases include use cases from the third level (61850) that identifies the IEC 61850 services to be used to fulfil the function use case. Use of the IEC 61850 services are shown in sequence diagrams.

For information about how to read the sequence diagrams, please have a look at this link:

https://www.sparxsystems.com.au/resources/uml2_tutorial/uml2_sequencediagram.html

Get structural data (1)

Use case objective:

An actor outside the DER facility wants to update a local copy of information from a DER facility.

The information could be nameplate information about an equipment that has been newly installed or contact information that has changed since the local copy was made.

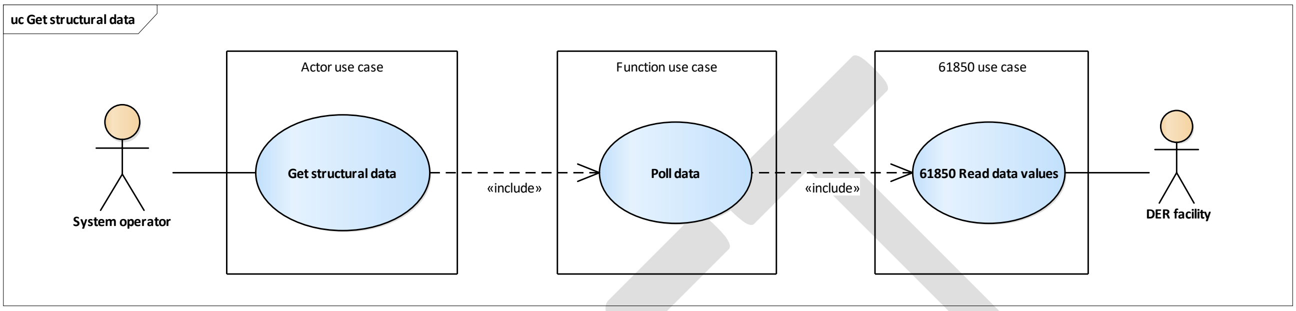


Figure 16 – Use case: Get structural data (1)

The actor 'System Operator' is used as the entity who wants to get the information from the 'DER facility' which is done with a GetDataValues(dataRef) request, resulting in a Response+(dataValues) in case of success or a Response-(serviceError) in case of failure.

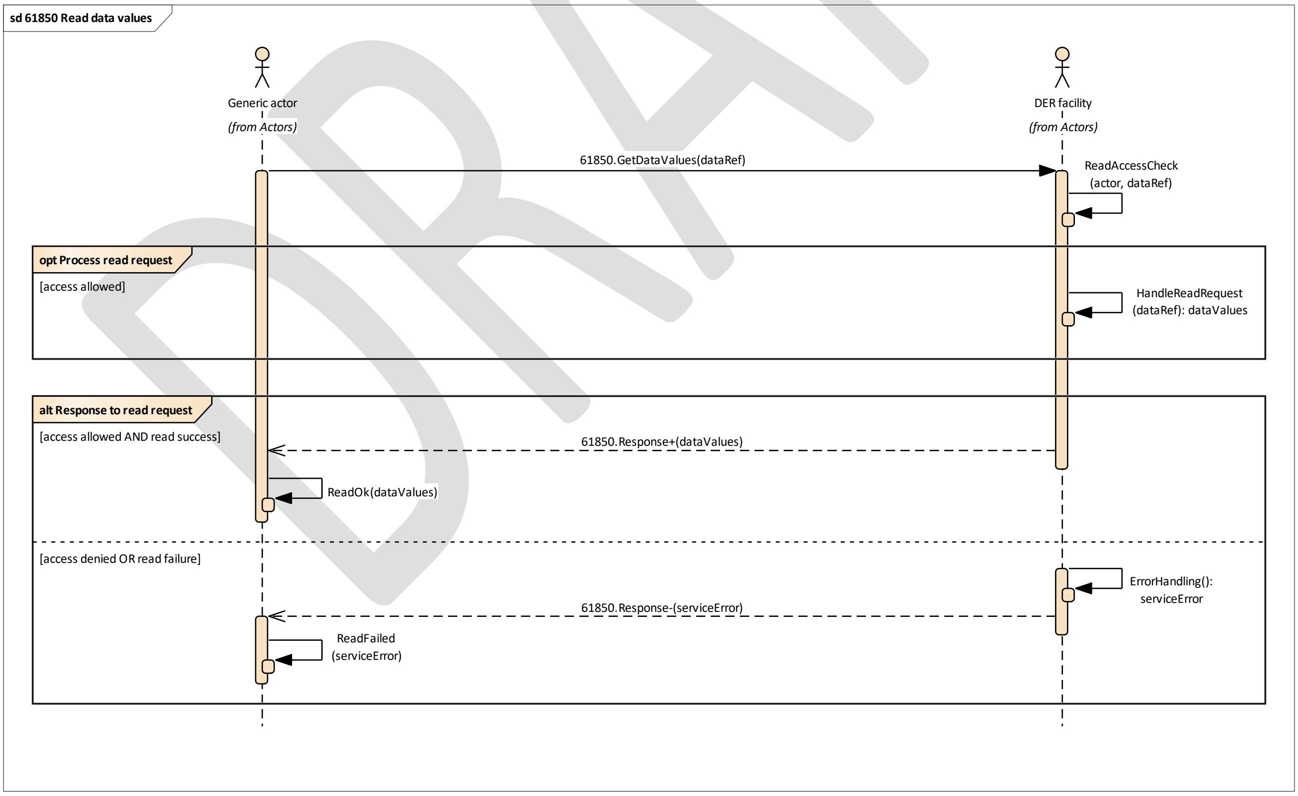


Figure 17 – Use case: 61850 Read data values

Get monitoring data (2)

<u>Use case objective:</u>

An actor outside the DER facility wants to get the latest operational status from a DER facility.

The operational status should be sent automatically, when there is a change in the data values.

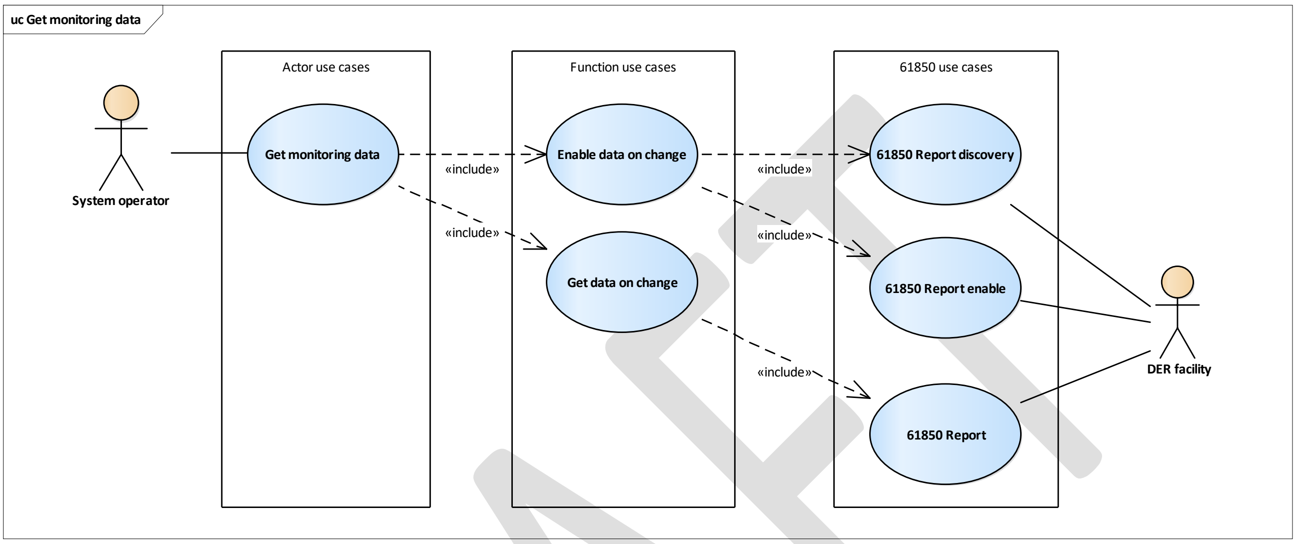


Figure 18 – Use case: Get monitoring data (2)

The concept to be used is called ‘buffered reporting’ and is basically an event driven approach, where information is sent automatically when triggered by an occurrence of an event (e.g. change of one or more data values).

For setting up buffered reporting it is first needed to determine the reports available from the DER facility. This is accomplished in the initial discovery during connection to the DER facility or by reading the system configuration file (SCL file) provided by the facility.

With the knowledge of available reports, each report can be discovered to determine the data values they monitor. This is accomplished by first finding the name of the dataset (GetBRCBValues), then listing the data value references included in the dataset (GetDataSetDirectory).

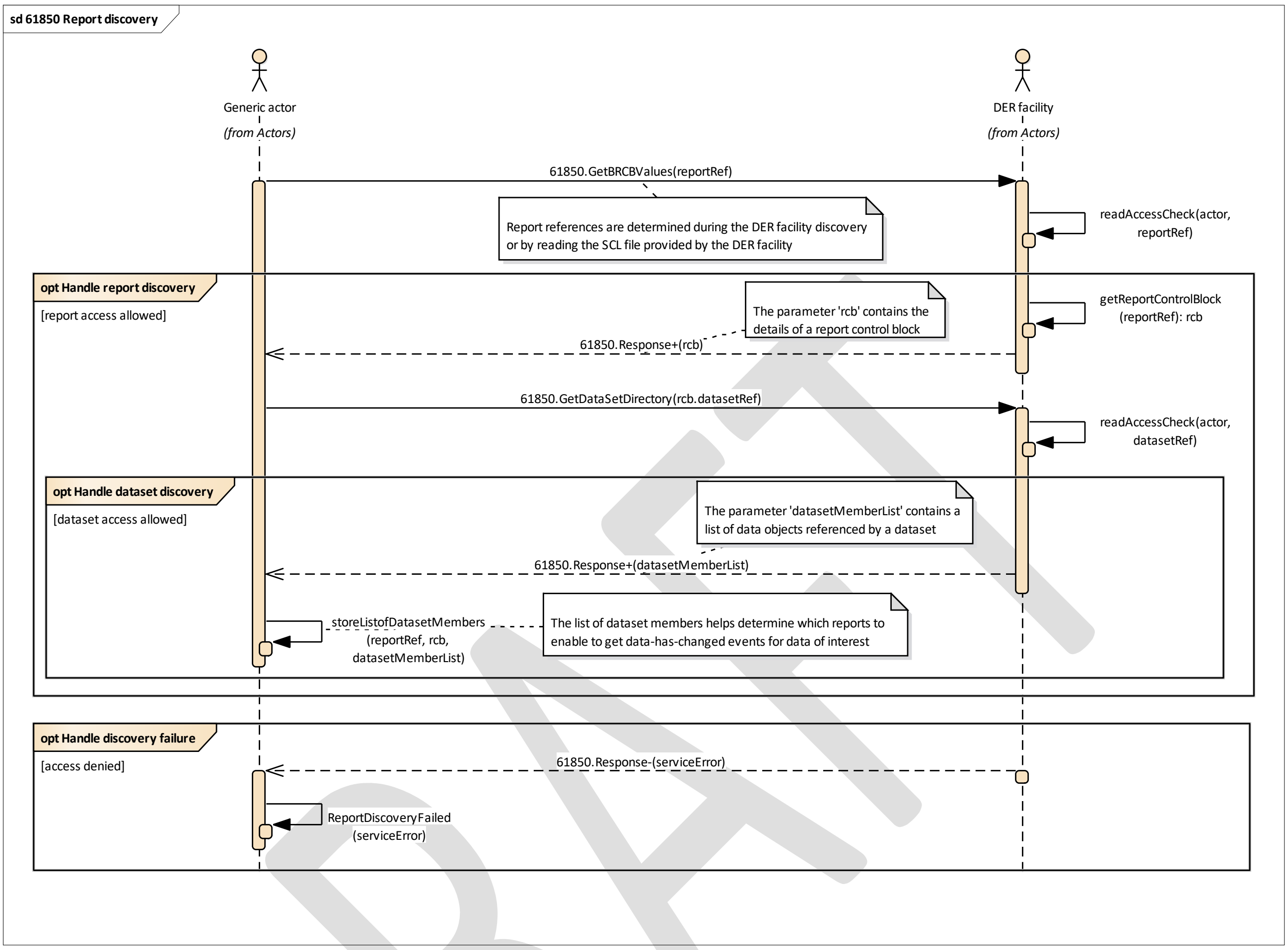


Figure 19 – Use case: 61850 Report discovery

Having determined which report references which data values, the correct report can be enabled (SetBRCBValues).

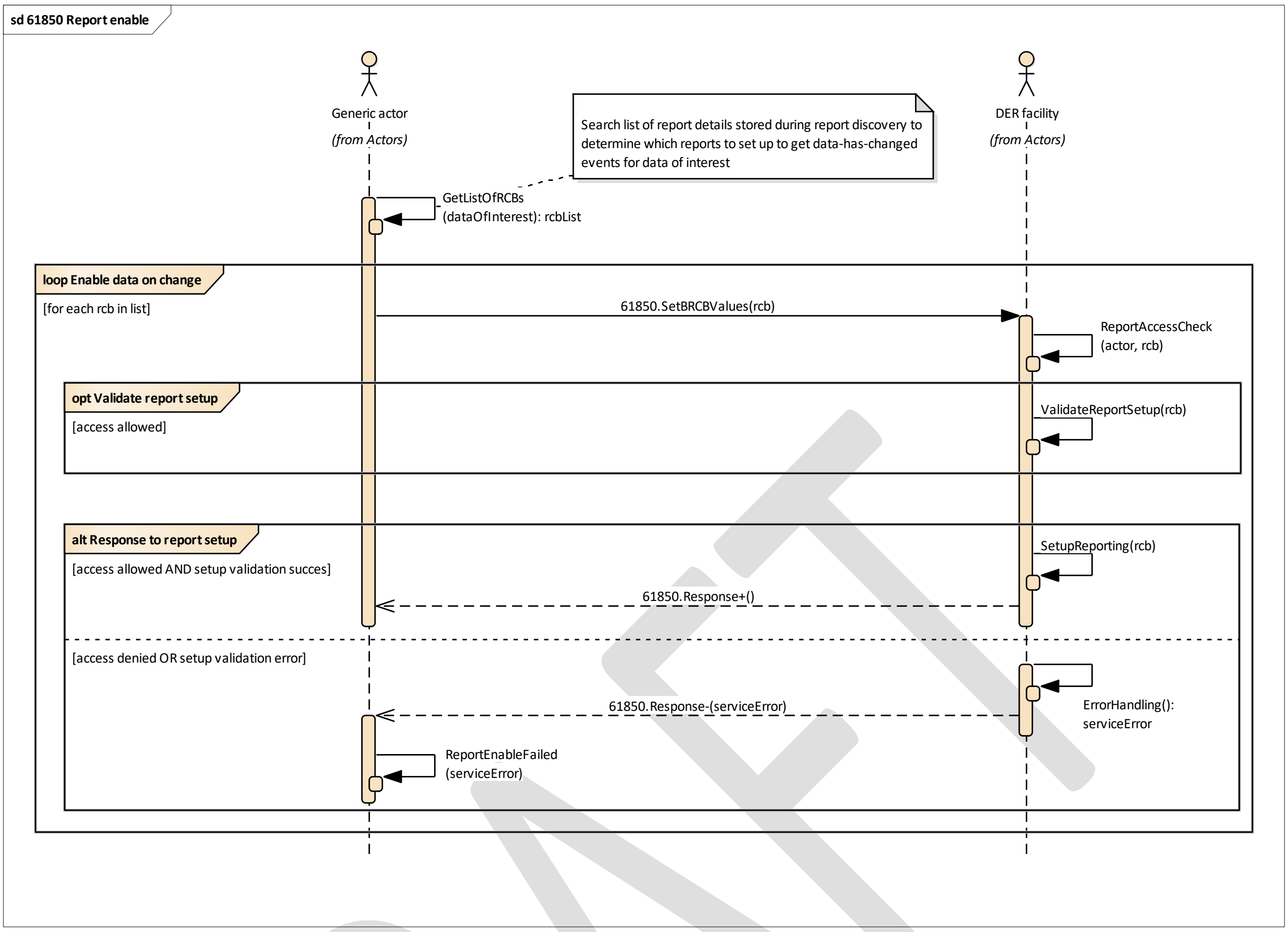


Figure 20 – Use case: 61850 Report enable

With buffered reporting enabled, the data values are sent automatically (Report(dataValues)) when triggered at the DER facility.

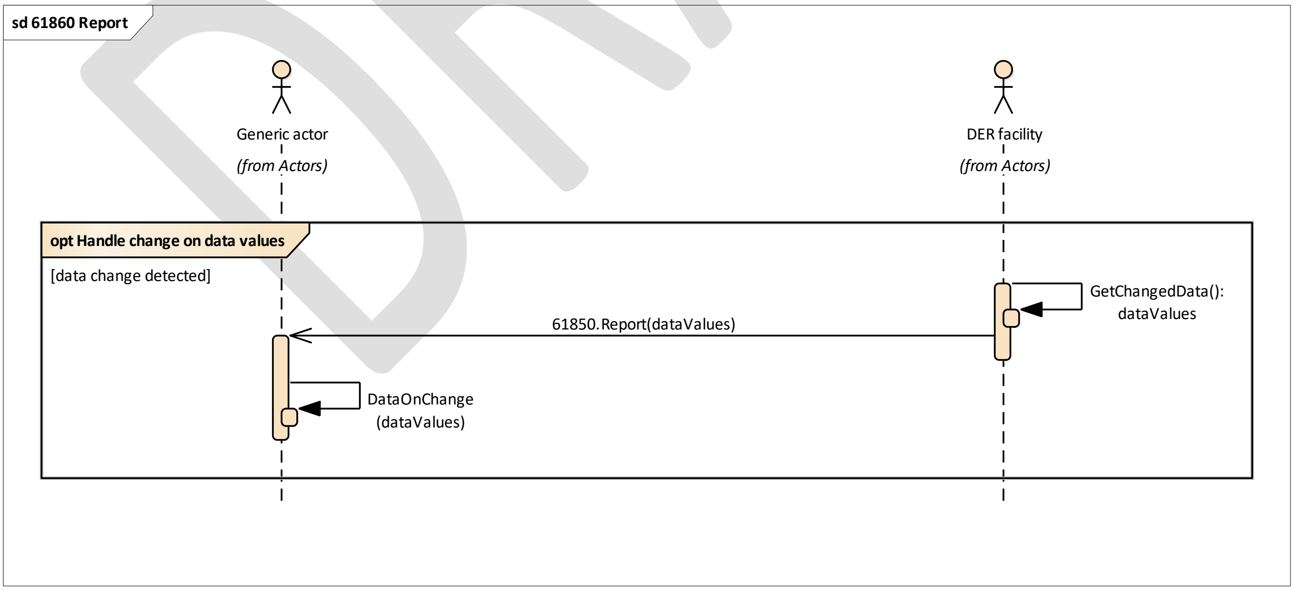


Figure 21 – Use case: 61850 Report

Activate regulating power (3)

<u>Use case objective:</u>

A System Operator has activated a bid send by the Market Operator.

The Market Operator must activate the DER resources at the DER facility.

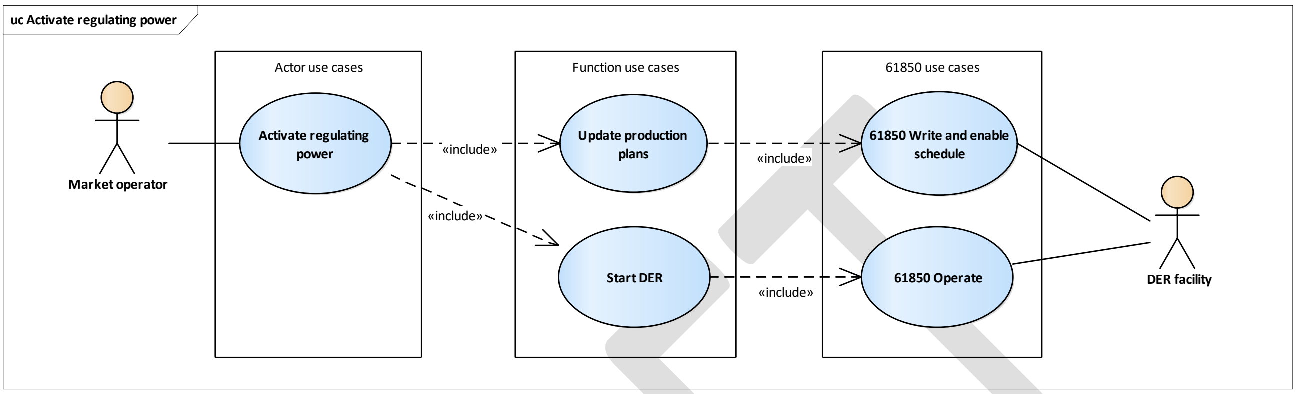


Figure 22 – Use case: Activate regulating power (3)

When the system operator has activated the offered bid, the market operator needs to activate the resources at the DER facility.

This is accomplished by first updating the production plans on the DER facility, which involves writing (SetDataSetValues) and enabling (Operate) a schedule.

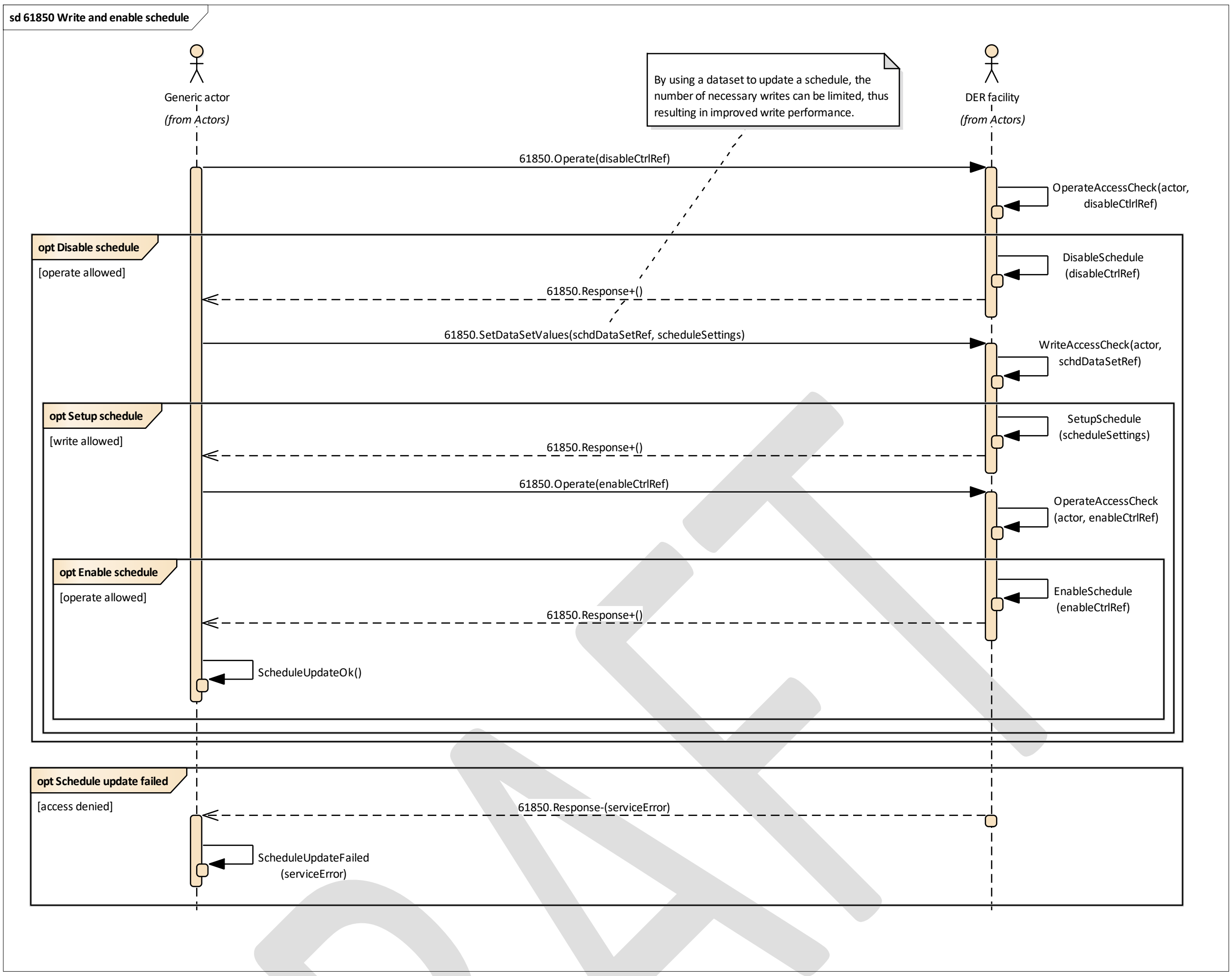


Figure 23 – Use case: 61850 Write and enable schedule

Having updated the production plan, the production units on the DER facility must be started (Operate).

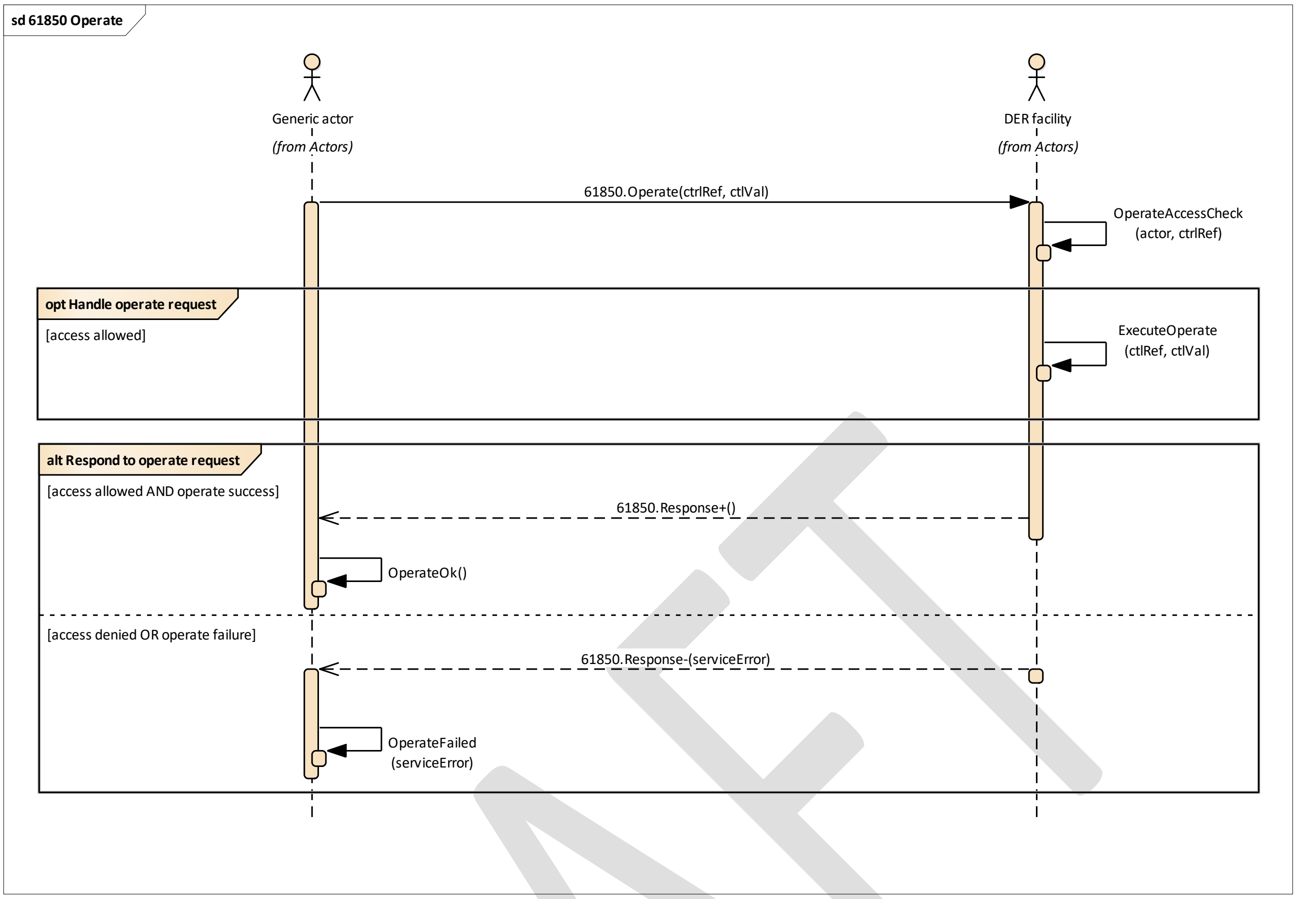


Figure 24 – Use case: 61850 Operate

Update LFC setpoint (4)

Use case objective:

The Market Operator need to make a fast dispatch of the resources available, which fulfils the request from the System Operator.

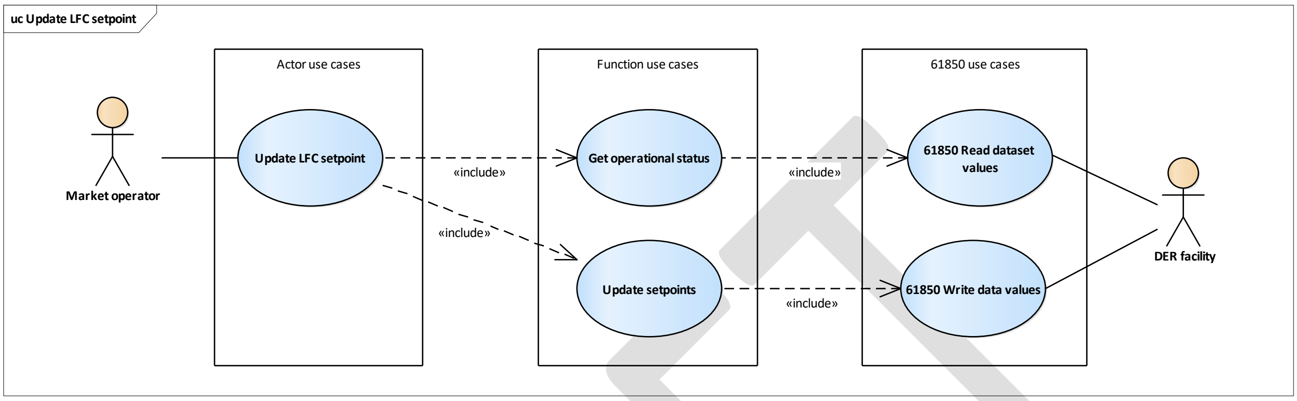


Figure 25 – Use case: Update LFC setpoint (4)

First, the operational status of the DER facilities is determined (GetDataSetValues).

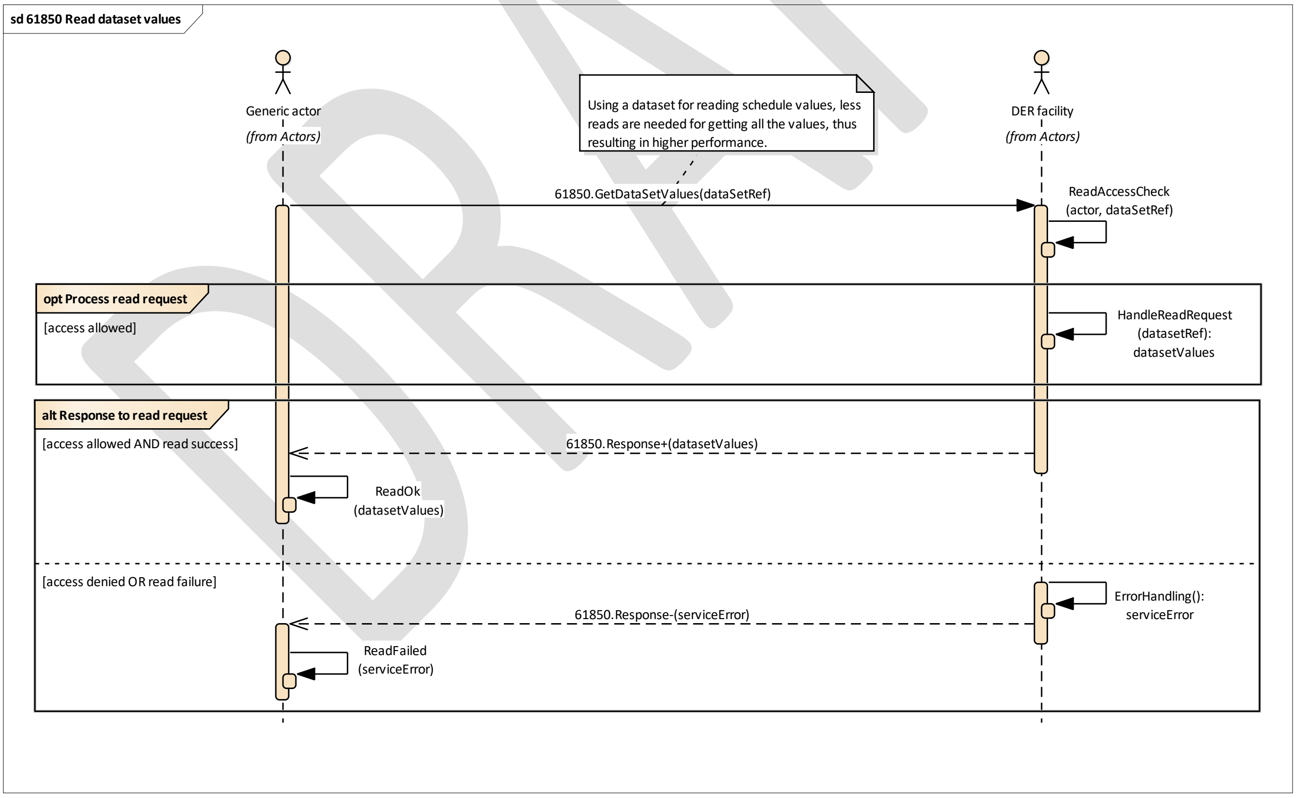


Figure 26 – Use case: 61850 Read dataset values

Next, setpoints are to be updated on the DER facilities (SetDataValues)

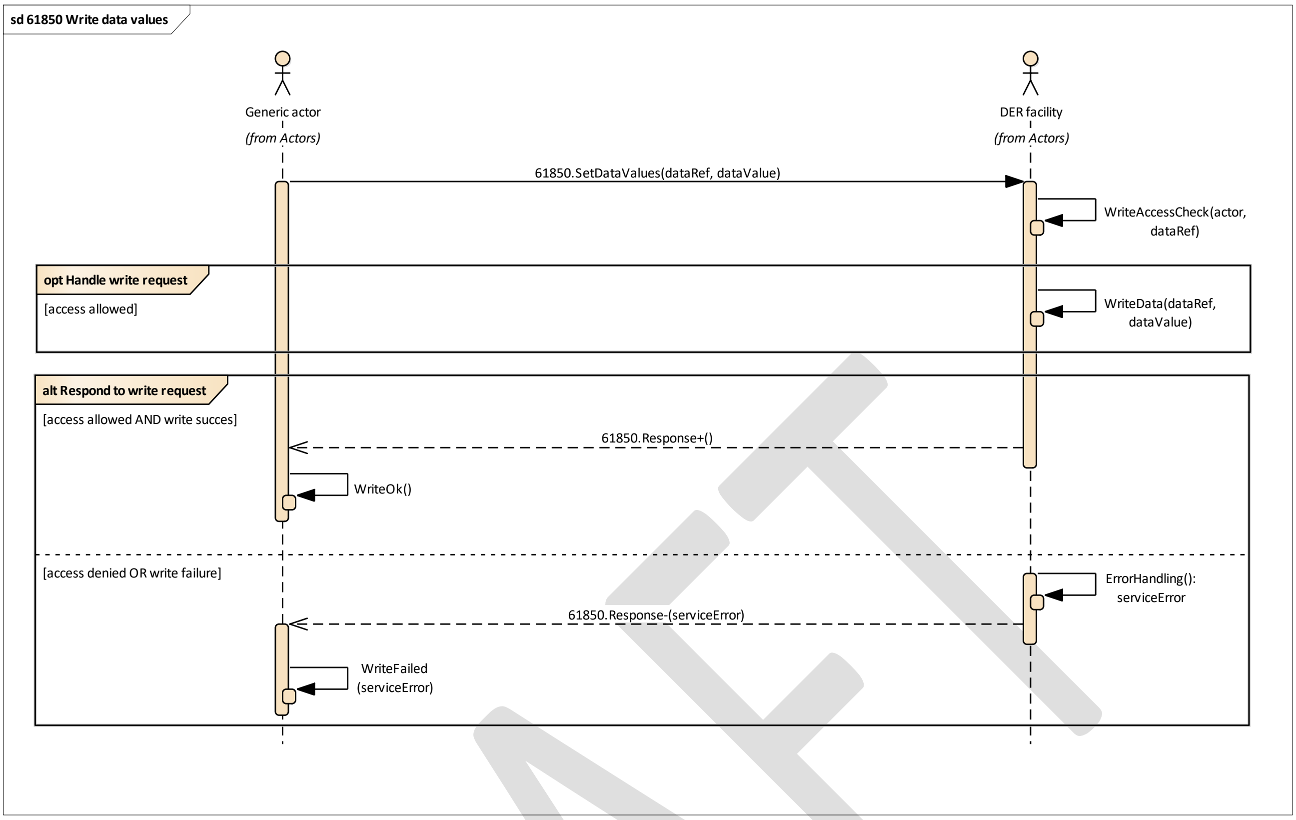


Figure 27 – Use case: 61850 Write data values

Plan market bids (5)

<u>Use case objective:</u>

A System Operator has a contract with a Market Operator for providing Regulating power, LFC or FCC services when needed.

To plan market bids, the Market Operator gets the productions plans from the DER facilities to determine their availability.

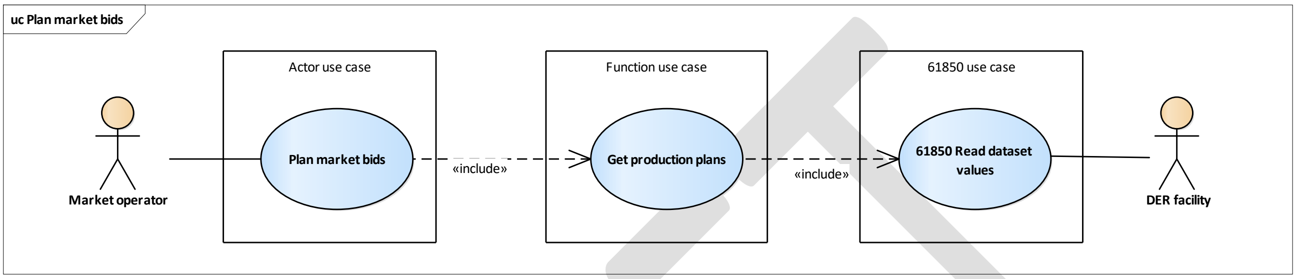


Figure 28 – Use case: Plan marked bids (5)

Please reference Figure 26 – Use case: 61850 Read dataset values for the IEC 61850 details.

Aggregate operational status (6)

<u>Use case objective:</u>

The Aggregator has a large portfolio of smaller DER resources.

The main objective for the Aggregator is to know the exact operational status of the DER resources and to be able to control the DER resources, for providing flexible DER service to the Market Operators.

Note: An Aggregator could be an Electric Vehicle Charging Station Operator who has a very high knowledge about the customers need for charging, or a heat pump service provider, who owns a portfolio of domestic heat pumps and who has a high knowledge about the customer heat demand.

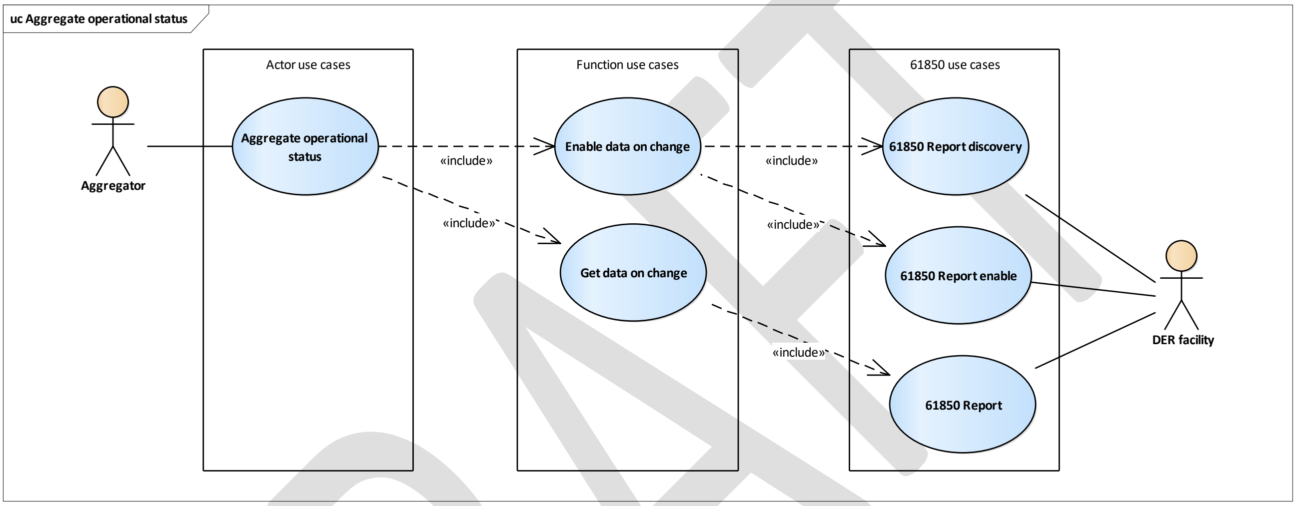


Figure 29 – Use case: Aggregate operational status (6)

Please reference Figure 19 – Use case: 61850 Report discovery, Figure 20 – Use case: 61850 Report enable and Figure 21 – Use case: 61850 Report for the IEC 61850 details.

Congestion management (7)

Use case objective:

The Grid Operator must provide a stable voltage level in the distribution grid.

In case of emergency, the DER facility should use controllable load to support the Grid Operator.

If the voltage is too high, the Grid Operator will send a command to the DER facility for higher load and a status about this to the Market Operator.

If the voltage is too low, the Grid Operator will send a command to the DER facility for lower load and a status about this to the Market Operator.

If the power grid is in "alert" state, the loads are reduced. In "emergency" or "blackout" state, the loads are deactivated.

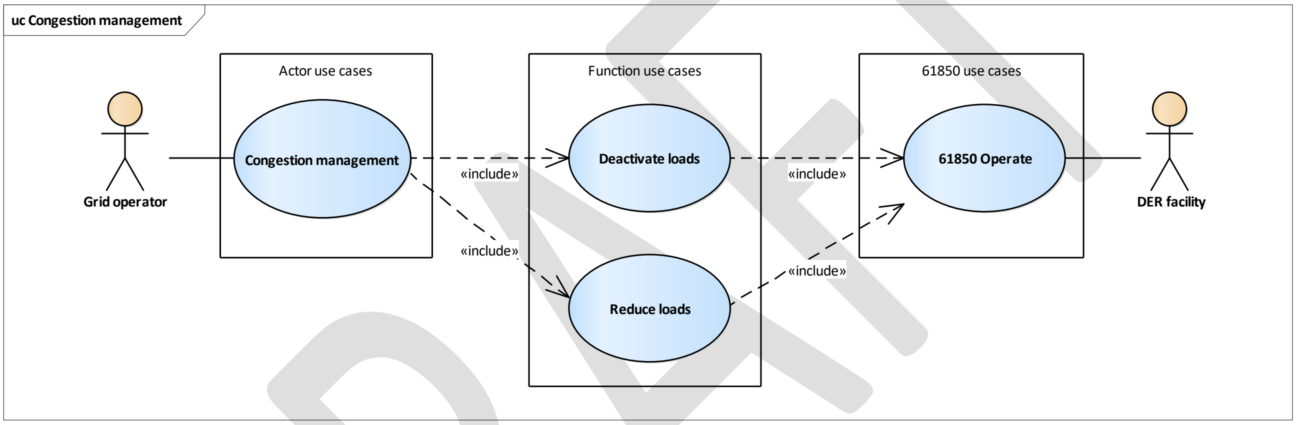


Figure 30 – Use case: Congestion management (7)

Please reference Figure 24 – Use case: 61850 Operate for the IEC 61850 details.

ANNEX B - Information security requirements - Table of compliance

IEEE Std 1686-2013

Vendors/suppliers who are claiming compliance with the IEEE Std 1686 (Standard for Intelligent Electronic Devices Cyber Security Capabilities) shall be required to provide a table of compliance (TOC). The TOC shall list every subclause of Clause 5 of the standard on a separate line. For each subclause, the vendor/supplier shall then indicate the level of compliance for the product in question. The following responses, reflected in the Status column, shall be used:

- Acknowledge: Used as a placeholder when no requirement is presented in the subclause
- Exception: Product fails to meet one or more of the stated requirements of the subclause
- Comply: Product fully meets the stated requirements of the subclause
- Exceed: Product exceeds one or more of the stated requirements of the subclause

A column for comments and explanations may be included to provide additional information the vendor deems useful for clarification of the response.

An example of a TOC is shown below.

Clause number	Clause/subclause title	Status	Comment
5	IED cyber security features	Acknowledge	
5.1	Electronic access control	Comply	
5.1.2	Password defeat mechanisms	Comply	
5.1.3	Number of individual users	Exceed	Product provides for 25 individual ID/password combinations
5.1.4	Password construction	Exception	Upper and lower case letters are interchangeable. Non-alphanumeric characters cannot be used in password
5.1.5	IED access control	Acknowledge	
5.1.5.1	Authorization levels by password	Comply	
5.1.5.2	Authorization using role-based access control (RBAC)	Exceed	Product provides six user-defined roles
5.1.6	IED main security functions	Acknowledge	
5.1.6 a)	View data	Comply	
5.1.6 b)	View configuration settings	Comply	
5.1.6 c)	Force values	Exception	Feature not supported on this product
5.1.6 d)	Configuration change	Comply	
5.1.6 e)	Firmware change	Comply	
5.1.6 f)	ID/password or RBAC management	Comply	
5.1.6 g)	Audit trail	Comply	
5.1.7	Password display	Comply	
5.1.8	Access timeout	Exception	Timeout period is set by a jumper on the main board. Possible selections are 1 min,5 min, 10 min, 30 min, and 60 min
5.2	Audit trail	Comply	
5.2.2	Storage capability	Exceed	Audit trail supports 4096 events before overwriting
5.2.3	Storage record	Comply	
5.2.3 a)	Event record number	Comply	
5.2.3 b)	Time and date	Exceed	User can define the format of the date
5.2.3 c)	User identification	Comply	

Clause number	Clause/subclause title	Status	Comment
5.2.3 d)	Event type	Comply	
5.2.4	Audit trail event types	Comply	
5.2.4 a)	Log in	Comply	
5.2.4 b)	Manual log out	Comply	
5.2.4 c)	Timed log out	Comply	
5.2.4 d)	Value forcing	Comply	
5.2.4 e)	Configuration access	Comply	
5.2.4 f)	Configuration change	Comply	
5.2.4 g)	Firmware change	Exception	Firmware changes are not captured in the audit trail record
5.2.4 h)	ID/password creation or modification	Comply	
5.2.4 i)	Password deletion	Comply	
5.2.4 j)	Audit log access	Comply	
5.2.4 k)	Time/date change	Comply	
5.2.4 l)	Alarm incident	Comply	
5.3	Supervisory monitoring and control	Comply	
5.3.2	Events	Comply	
5.3.3	Alarms	Comply	
5.3.3 a)	Unsuccessful login attempt	Exception	Alarm is set after six unsuccessful attempts within a 5-min period
5.3.3 b)	Reboot	Exception	A specific alarm for a reboot is not available. However, user can deduce that a reboot has taken place by examining the DNP3.0 initialization bit being set followed by a DNP3.0 request for time.
5.3.3 c)	Attempted use of unauthorized configuration software	Comply	
5.3.3 d)	Invalid configuration or firmware download	Comply	
5.3.3 e)	Unauthorized configuration or firmware file	Comply	
5.3.3 f)	Time signal out of tolerance	Comply	
5.3.3 g)	Invalid field hardware changes	Comply	
5.3.4	Alarm point change detect	Comply	
5.3.5	Event and alarm grouping	Exceed	Three groups are provided: “Critical alarms”, “Alarms” and “Events”
5.3.6	Supervisory permissive control	Comply	
5.4	IED cyber security features	Acknowledge	
5.4.1	IED functionality compromise	Comply	Download of configuration will disable all other operations during the period of download
5.4.2	Specific crytographic features	Acknowledge	
5.4.2 a)	Webserver functionality	Comply	Feature not offered in this product
5.4.2 b)	File transfer functionality	Comply	
5.4.2 c)	Text-oriented terminal connections	Comply	
5.4.2 d)	SNMP network management	Exception	SNMPv2 implemented in this product
5.4.2 e)	Network time synchronization	Exception	IEEE Std C37.238 implemented in this product
5.4.2 f)	Secure tunnel functionality	Comply	
5.4.3	Cryptographic techniques	Comply	
5.4.4	Encrypting serial communications	Comply	
5.4.5	Protocol-specific security features	Comply	
5.5	IED configuration software	Acknowledge	
5.5.1	Authentication	Exception	Feature not supported
5.5.2	Digital signature	Comply	
5.5.3	ID/password control	Exception	Passwords can be viewed in the configuration

Clause number	Clause/subclause title	Status	Comment
			by someone with Supervisor Level authority
5.5.4	ID/password-controlled features	Comply	
5.5.4.1	View configuration data	Comply	
5.5.4.2	Change configuration data	Comply	
5.5.4.2 a)	Full access	Comply	
5.5.4.2 b)	Change tracking	Comply	
5.5.4.2 c)	Use monitoring	Comply	
5.5.4.2 d)	Download to IED	Comply	
5.6	Communications port access	Comply	
5.7	Firmware quality control	Comply	

ANNEX C – informative CHPCOM reference signal list

Example of reference signal list from CHPCOM

One of the most important demonstration projects in Denmark regarding use of the IEC 61850 standards for DER, has been the CHPCOM project.

The partners in CHPCOM are all important actors in the Danish power system, like Energinet (TSO), Danish Energy Association (representing DSO and BRP interests) and Danish District Heating Association including Foreningen Danske Kraftvarmeværker (representing the Combined Heat and Power plants).

One of the results from this project was a reference signal list, which represented a large amount of the signals that could be exchanged between a CHP plant and an actor outside the plant.

The reference signal list includes 379 signals which are divided into the three group-types and data-types:

Operational data	**Measurements, status, commands and settings**
Static data	**Nameplate information**
Statistical data	**Calculated and manually typed-in data**

Also, the reference signal list includes a signal explanation, the units (Hz, volt, amp…) and whether the signal is seen as mandatory, optional or conditional – and the '61850 tag name'.

Please contact Energinet (cas@energinet.dk) for a copy of the CHPCOM reference signal list

ANNEX D – Normative reference signal list

Aa part of the work for SO GL ‘System Operation Guide Lines’ and the NGF ‘Nationale gennemførelsesforanstaltninger for informationsudvekslingen’ a normative reference signal list will be established.

Please contact Energinet (cas@energinet.dk) for a copy of the normative reference signal list

ANNEX E – IEC 81346 classification codes

Examples of ISO/IEC 81346 classification codes

DER Facility	DER System	DER Unit	DER Component	Name
Facility				+<EIC code>
	Facility information			=AF
	Power plant system			=HG1
		Boiler-turbine-generator unit		=HG2=GA1
			Boiler	=HG2=GA1=EM
			Turbine	=HG2=GA1=MN
			Generator	=HG2=GA1=GA
		Motor-generator set		=HG3=GA1
			Motor	=HG3=GA1=MS
			Generator	=HG3=GA1=GA
	Heat supply system			=HD4
		Electric boiler unit		=HD4=EB1
		Thermal storage unit		=HD5=CP1
			Electric boiler in thermal storage	=HD6=CP1=EB1
		Boiler unit		=HD7=EM1
		Solar heating unit		=HD8=EVA1
		Heat pump unit		=HD9=EPD1

The numbers identify instances, and as such depends on the count of systems, units and components present on the facility.

E.g. the name “+45W000000000099Y=HG2=GA1=EM” identifies the boiler on the first boiler-turbine-generator unit in the second power plant system at the production resource located in Silkeborg.

ANNEX F – Basic cyber security recommendations and standards

Besides the requirements described in the

Network requirements section, it is also strongly recommended that the following guidelines are followed.

The facility should make sure that only authorised personnel can connect to communication ports (e.g. USB and ethernet) on equipment connected to the technical network.

The facility should implement and enforce a password policy that prevents the use of weak passwords and secures that default passwords are changed to passwords that complies with the rules in the policy.

The facility should implement a contingency plan, that states how to react in case of problems with the IT networks.

The facility should make sure that the software on equipment connected to the technical network is kept up to date to limit any potential security risks.

Below is listed standards that could be relevant when it comes to Cyber Security and information exchange for critical infrastructure:

IEEE 1686:2013 Standard for Intelligent Electronic Devices Cyber Security Capabilities

IEEE Std C37.231 Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control

NERC CIP-002-1: Critical Cyber Asset Identification

NERC CIP-003-1: Security Management Controls

NERC CIP-004-1: Personnel and Training

NERC CIP-005-1: Electronic Security Perimeters

NERC CIP-006-1: Physical Security of Critical Cyber Assets

NERC CIP-007-1: Systems Security Management

NERC CIP-008-1: Incident Reporting and Response Planning

NERC CIP-009-1: Recovery Plans for Critical Cyber Assets

ANNEX G - Protocol Implementation eXtra Information for Testing

This section specifies the PIXIT (Protocol Implementation eXtra Information for Testing) for each applicable ACSI service model as structured in IEC 61850-10. This ACSI model is applicable for all IEDs conformant with this specification.

For each of the use case described in ANNEX A, the following tables includes a column which specifies whether the PIXIT item is mandatory (M) or optional (O) for the use case. Mandatory means that the feature needs to be specified and implemented in the IED.

In the PIXIT tables, the use cases are identified by their number given to them in ANNEX A: Get structural data (1), Get monitoring data (2), Activate regulating power (3), Update LFC setpoint (4), Plan market bids (5), Aggregate operational status (6) and Congestion management (7).

PIXIT for Association model

ID	**Description**	**Clarification**	**Value**	**Use case M/O**						
				1	2	3	4	5	6	7
As1	Maximum number of clients that can set-up an association simultaneously	Depending on type of device	Min 3 Max 10	M	M	M	M	M	M	M
As2	TCP_KEEPALIVE value		1 SECOND	M	M	M	M	M	M	M
As3	Lost connection detection time		20 SECONDS	M	M	M	M	M	M	M
As4	Is authentication supported		O	O	O	O	O	O	O	O
As5	What association parameters are necessary for successful association	Transport selector Session selector Presentation selector AP Title AE Qualifier	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M
As6	If association parameters are necessary for association, describe the correct values e.g.	Transport selector Session selector Presentation selector AP Title AE Qualifier	0001 0001 00000001 <value> <value>	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M	M M M M M
As7	What is the maximum and minimum MMS PDU size	Max MMS PDU size Min MMS PDU size	… …	M M	M M	M M	M M	M M	M M	M M
As8	What is the maximum start up time after a power supply interrupt		300 seconds	M	M	M	M	M	M	M

PIXIT for Server model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Sr1	Which analogue value (MX) quality bits are supported (can be set by server)	Validity:								
		Good		M	M	M	M	M	M	M
		Invalid		M	M	M	M	M	M	M
		Reserved		O	O	O	O	O	O	O
		Questionable		O	O	O	O	O	O	O
		Overflow		O	O	O	O	O	O	O
		OutofRange		M	M	M	M	M	M	M
		BadReference		O	O	O	O	O	O	O
		Oscillatory		O	O	O	O	O	O	O
		Failure		O	O	O	O	O	O	O
		OldData		O	O	O	O	O	O	O
		Inconsistent		O	O	O	O	O	O	O
		Inaccurate		O	O	O	O	O	O	O
		Source:								
		Process		M	M	M	M	M	M	M
		Substituted		M	M	M	M	M	M	M
		Test		M	M	M	M	M	M	M
		OperatorBlocked		M	M	M	M	M	M	M
Sr2	Which status value (ST) quality bits are supported (can be set by server)	Validity:								
		Good		M	M	M	M	M	M	M
		Invalid		M	M	M	M	M	M	M
		Reserved		O	O	O	O	O	O	O
		Questionable		O	O	O	O	O	O	O
		BadReference		O	O	O	O	O	O	O
		Oscillatory		O	O	O	O	O	O	O
		Failure		O	O	O	O	O	O	O
		OldData		O	O	O	O	O	O	O
		Inconsistent		O	O	O	O	O	O	O
		Inaccurate		O	O	O	O	O	O	O
		Source:								
		Process		M	M	M	M	M	M	M
		Substituted		M	M	M	M	M	M	M
		Test		M	M	M	M	M	M	M
		OperatorBlocked		M	M	M	M	M	M	M
Sr5	Which Mode / Behaviour values are supported	On		M	M	M	M	M	M	M
		Blocked		O	O	O	O	O	O	O
		Test		O	O	O	O	O	O	O
		Test/Blocked		O	O	O	O	O	O	O
		Off		O	O	O	O	O	O	O

Note: The mode/behaviour is tied to the group reference, not all logical nodes can be switched off at any time, since it may affect the behaviour of the whole DER facility. The behaviour must be set to ON at start-up of any logical node.

PIXIT for Data set model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Ds1	What is the maximum number of data elements in one data set (compare ICD setting)		User defined	M	M	M	M	M	M	M
Ds2	How many persistent data sets can be created by one or more clients		User defined	M	M	M	M	M	M	M
Ds3	How many non-persistent data sets can be created by one or more clients		User defined	M	M	M	M	M	M	M

PIXIT for Substitution model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Sb1	Are substituted values stored in volatile memory?	Y/N	User defined	O	O	O	O	O	O	O

PIXIT for Setting group control model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Sg1	What is the number of supported setting groups for each logical device (compare NumSG in the SGCB)		User defined	O	O	O	O	O	O	O
Sg2	What is the effect of when and how the non-volatile storage is updated (compare IEC 61850-8-1 $16.2.4)		User defined	O	O	O	O	O	O	O
Sg3	Can multiple clients edit the same setting group		N	O	O	O	O	O	O	O
Sg4	What happens if the association is lost while editing a setting group		Shall revert to the old data	O	O	O	O	O	O	O
Sg5	Is EditSG value 0 allowed?		N	O	O	O	O	O	O	O

PIXIT for Reporting model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Rp1	The supported trigger conditions are (compare PICS)	integrity	M	O	M	O	O	O	M	O
		data change	M	O	M	O	O	O	M	O
		quality change	M	O	M	O	O	O	M	O
		data update	O	O	O	O	O	O	O	O
		general interrogation	M	O	M	O	O	O	M	O
Rp2	The supported optional fields are	sequence-number	M	O	M	O	O	O	M	O
		report-time-stamp	O	O	O	O	O	O	O	O
		reason-for-inclusion	O	O	O	O	O	O	O	O
		data-set-name	M	O	M	O	O	O	M	O
		data-reference	O	O	O	O	O	O	O	O
		buffer-overflow	O	O	O	O	O	O	O	O
		entryID	O	O	O	O	O	O	O	O
		conf-rev	O	O	O	O	O	O	O	O
		segmentation	O	O	O	O	O	O	O	O
Rp3	Can the server send segmented reports		O	O	O	O	O	O	O	O
Rp4	Mechanism on second internal data change notification of the same analogue data value within buffer period (Compare IEC 61850-7-2 $14.2.2.9)	Send report immediately OR Replace analogue value in pending report	Send report immediately	O	M	O	O	O	M	O
Rp5	Multi client URCB approach (compare IEC 61850-7-2 $14.2.1)		Each URCB is visible to all clients	O	O	O	O	O	O	O
Rp6	What is the format of EntryID			O	O	O	O	O	O	O
Rp7	What is the buffer size for each BRCB or how many reports can be buffered	<number of bytes or typical number of dataset members or reports>	User defined	O	M	O	O	O	M	O
Rp9	May the reported data set contain: - structured data objects? - data attributes?		 Y Y	O	M	O	O	O	M	O
Rp10	What is the scan cycle for binary events? Is this fixed, configurable	Fixed	Max 200 ms User defined for each IED	O	M	O	O	O	M	O
Rp11	Does the device support to pre-assign a RCB to a specific client in the SCL		User defined	O	M	O	O	O	M	O

PIXIT for Logging model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Lg1	What is the default value of LogEna (Compare IEC 61850-8-1 $17.3.3.2.1, the default value should be FALSE)		FALSE	O	O	O	O	O	O	O
Lg2	What is the format of EntryID (Compare IEC 61850-8-1 $17.3.3.3.1)	MMS octet string (00000000)	User defined	O	O	O	O	O	O	O
Lg3	If there are multiple Log Control Blocks that specify the Journaling of the same MMS NamedVariable and TrgOps and the Event Condition (Compare IEC 61850-8-1 $17.3.3.3.2)	Single Journal Entry (specify the event condition) or Multiple Journal Entries	User defined	O	O	O	O	O	O	O
Lg4	Pre-configured LCB attributes that cannot be changed online	No restrictions		O	O	O	O	O	O	O

PIXIT for Control model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Ct1	What control models are supported (compare PICS)	status-only	M	O	O	M	O	O	O	M
		direct-with-normal-security	M	O	O	M	O	O	O	M
		sbo-with-normal-security	O	O	O	O	O	O	O	O
		direct-with-enhanced-security	O	O	O	O	O	O	O	O
		sbo-with-enhanced-security	O	O	O	O	O	O	O	O
Ct2	Is the control model fixed, configurable and/or online changeable?		FIXED	O	O	M	O	O	O	M
Ct3	Is TimeActivatedOperate supported		O	O	O	O	O	O	O	O
Ct4	Is “operate-many” supported		NO	O	O	O	O	O	O	O
Ct5	Will the DUT activate the control output when the test attribute is set in the SelectWithValue and/or Operate request (when N test procedure Ctl2 is applicable)		O	O	O	O	O	O	O	O
Ct6	What are the conditions for the time (T) attribute in the SelectWithValue and/or Operate request	e.g. DUT ignores the time value and execute the command as usual	User defined	O	O	M	O	O	O	M
Ct7	Is pulse configuration supported	Y/N	O	O	O	M	O	O	O	M

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Ct8	What is the behaviour of the DUT when the check conditions are set Is this behaviour fixed, configurable, online changeable?	Y/N synchrocheck Y/N interlock-check DUT ignores the check value and always perform the check or DUT uses the check value to perform the check Fixed / Configurable / Online changeable	O, Device dependant	O	O	M	O	O	O	M
Ct9	What additional cause diagnosis are supported	Blocked-by-switching-hierarchy	O	O	O	O	O	O	O	O
		Select-failed	O	O	O	O	O	O	O	O
		Invalid-position	M	O	O	M	O	O	O	M
		Position-reached	M	O	O	M	O	O	O	M
		Parameter-change-in-execution	O	O	O	O	O	O	O	O
		Step-limit	O	O	O	O	O	O	O	O
		BLOCKED-BY-MODE	O NOT REQUIRED FOR FUNCTIONS WITH MANDATORY MODE ON	O	O	M	O	O	O	M
		BLOCKED-BY-PROCESS	O	O	O	O	O	O	O	O
		Blocked-by-interlocking	O	O	O	O	O	O	O	O
		Blocked-by-synchrocheck	O	O	O	O	O	O	O	O
		Command-already-in-execution	M	O	O	M	O	O	O	M
		Blocked-by-health	M	O	O	M	O	O	O	M
		1-of-n-control	O	O	O	O	O	O	O	O
		Abortion-by-cancel	O	O	O	O	O	O	O	O
		Time-limit-over	O	O	O	O	O	O	O	O
		Abortion-by-trip	O	O	O	O	O	O	O	O
Ct10	How to force a “test-not-ok” respond with SelectWithValue request?		User defined	O	O	M	O	O	O	M
Ct11	How to force a “test-not-ok” respond with Select request?		User defined	O	O	M	O	O	O	M
Ct12	How to force a “test-not-ok” respond with Operate request?	DOns: SBOns: DOes: SBOes:	User defined	O	O	M	O	O	O	M

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Ct13	Which origin categories are supported?	All as listed in 7-3, Ed 2, table 10		O	O	M	O	O	O	M
Ct14	What happens if the orCat value is not supported?	DOns: SBOns: DOes: SBOes:	User defined	O	O	M	O	O	O	M
Ct15	Does the IED accept a SelectWithValue/Operate with the same ctlVal as the current status value?	DOns: Y/N SBOns: Y/N DOes: Y/N SBOes: Y/N	Yes Yes Yes Yes	O	O	M	O	O	O	M
Ct16	Does the IED accept a select/operate on the same control object from 2 different clients at the same time?	DOns: Y/N (default Y) SBOns: Y/N (default N) DOes: Y/N (default Y) SBOes: Y/N (default N)	Yes No Yes No	O	O	M	O	O	O	M
Ct17	Does the IED accept a Select/SelectWithValue from the same client when the control object is already selected (tissue 334)	SBOns: Y/N SBOes: Y/N	Yes Yes	O	O	M	O	O	O	M
Ct18	Is for SBOes the internal validation performed during the SelectWithValue and/or Operate step?	SelectWithValue / Operate / SelectWithValue and Operate	As minimum, at Operate	O	O	M	O	O	O	M
Ct20	Does the IED support local / remote operation?	Y/N	User defined, depending on type of IED	O	O	M	O	O	O	M
Ct21	Does the IED send an InformationReport with LastApplError as part of the Operate response- for control with normal security?	SBOns: Y/N DOns: Y/N	Optional	O	O	O	O	O	O	O

PIXIT for Time and time synchronisation model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Tm1	What quality bits are supported (may be set by the IED)	LeapSecondsKnown	O	O	O	O	O	O	O	O
		ClockFailure	O	O	O	O	O	O	O	O
		ClockNotSynchronized	M	M	M	M	M	M	M	M
Tm2	Describe the behaviour when the time synchronization signal/messages are lost	After some time, Clock not synchronised bit is set	User defined	M	M	M	M	M	M	M
Tm3	When is the time quality bit "ClockFailure" set?		User defined	M	M	M	M	M	M	M
Tm4	When is the time quality bit "Clock not synchronised” set?	Loss of signal or clock failure	User defined delay	M	M	M	M	M	M	M
Tm5	Is the timestamp of a binary event adjusted to the configured scan cycle?	Y/N	User defined	M	M	M	M	M	M	M
Tm6	Does the device support time zone and daylight saving?	Y/N	User defined	M	M	M	M	M	M	M
Tm7	Which attributes of the SNTP response packet are validated?	Leap indicator not equal to 3?	User defined	M	M	M	M	M	M	M
		Mode is equal to SERVER	User defined	M	M	M	M	M	M	M
		OriginateTimestamp is equal to value sent by the SNTP client as Transmit Timestamp	User defined	M	M	M	M	M	M	M
		RX/TX timestamp fields are checked for reasonableness	User defined	M	M	M	M	M	M	M
		SNTP version 3 and/or 4	User defined	M	M	M	M	M	M	M

PIXIT for File transfer model

ID	Description	Clarification	Value	Use case M/O						
				1	2	3	4	5	6	7
Ft1	What is structure of files and directories?		User defined	O	O	O	O	O	O	O
Ft2	Directory names are separated from the file name by	“/” or “\”	User defined	O	O	O	O	O	O	O
Ft3	The maximum file name size including path (recommended 64 chars)	… chars	User defined	O	O	O	O	O	O	O
Ft4	Are directory/file name case sensitive		Case sensitive	O	O	O	O	O	O	O
Ft5	Maximum file size		User defined	O	O	O	O	O	O	O
Ft6	Is the requested file path included in the MMS fileDirectory respond file name?	Y/N	User defined	O	O	O	O	O	O	O
Ft7	Is the wild char supported MMS fileDirectory request?	Yes, wild card = *	No	O	O	O	O	O	O	O
Ft8	Is it allowed that 2 clients get a file at the same time?	Y/N	User defined	O	O	O	O	O	O	O

ANNEX H – ICD-file example

In the following is shown an extract of an ICD file that describes the reference signal list and required ACSI services. Only those signals marked as mandatory (M) in the list are included in the ICD.

```xml
<?xml version="1.0" encoding="utf-8"?>
<SCL revision="B" version="2007" xmlns="http://www.iec.ch/61850/2003/SCL"
xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL SCL.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Header version="1" id="DER Gateway" toolID="TMW SCL Navigator V1.0" />
<Communication>
  <SubNetwork name="SubNetworkName">
    <ConnectedAP apName="AP" iedName="TEMPLATE_">
      <Address>
        <P type="OSI-AP-Title">1,1,9999,1</P>
        <P type="OSI-AE-Qualifier">12</P>
        <P type="OSI-PSEL">00000001</P>
        <P type="OSI-SSEL">0001</P>
        <P type="OSI-TSEL">0001</P>
      </Address>
    </ConnectedAP>
  </SubNetwork>
</Communication>
<IED name="TEMPLATE_" manufacturer="EURISCO" configVersion="1.0" originalSclRevision="B"
originalSclVersion="2007">
  <Services>
    <DynAssociation max="10" />
    <ConfLogControl max="10" />
    <GetDirectory />
    <GetDataObjectDefinition />
    <DataObjectDirectory />
    <GetDataSetValue />
    <SetDataSetValue />
    <DataSetDirectory />
    <ConfDataSet modify="true" maxAttributes="50" max="50" />
    <DynDataSet max="100" maxAttributes="50" />
    <ReadWrite />
    <ConfReportControl bufConf="true" bufMode="both" max="50" />
    <GetCBValues />
    <ReportSettings rptID="Dyn" trgOps="Dyn" intgPd="Dyn" optFields="Dyn" cbName="Conf"
datSet="Dyn" bufTime="Dyn" resvTms="true" owner="true" />
    <LogSettings trgOps="Dyn" intgPd="Dyn" datSet="Dyn" logEna="Dyn" />
    <FileHandling />
    <ConfLNs />
    <ConfSigRef max="100" />
  </Services>
  <AccessPoint name="AP">
    <Server>
      <Authentication />
        <LDevice inst="AF" desc="Facility Information">
          <LN lnType="MHET_Prod" lnClass="MHET" inst="1" prefix="" desc="Production of
heat for District Heating" />
        </LDevice>
        <LDevice inst="HG1" desc="Power plant system">
```

```
          <LN lnType="MMXU_VPar" lnClass="MMXU" inst="1" prefix="" />
          <LN lnType="CSWI_BrkInd" lnClass="CSWI" inst="1" prefix="" />
          <LN lnType="DRCC_PSetPt" lnClass="DRCC" inst="1" prefix="" />
        </LDevice>
        <LDevice inst="HG2GA1" desc="Boiler-turbine-generator unit">
          <LN lnType="DRCC_GenStrTm" lnClass="DRCC" inst="1" prefix="" />
          <LN lnType="DRCS_DERUnit" lnClass="DRCS" inst="1" prefix="" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="1" prefix="" desc="Hz regulator
step 1 (primary) active status over" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="2" prefix="" desc="Hz regulator
step 2 (primary) active status under" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="3" prefix="" desc="Hz regulator
step 3 (critical) active status high over" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="4" prefix="" desc="Hz regulator
step 4 (critical) active status low under" />
        </LDevice>
        <LDevice inst="HG3GA1" desc="Motor-generator set">
          <LN lnType="DRCC_GenStrTm" lnClass="DRCC" inst="1" prefix="" />
          <LN lnType="DRCS_DERUnit_Motor" lnClass="DRCS" inst="1" prefix="" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="1" prefix="" desc="Hz regulator
step 1 (primary) active status over" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="2" prefix="" desc="Hz regulator
step 2 (primary) active status under" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="3" prefix="" desc="Hz regulator
step 3 (critical) active status high over" />
          <LN lnType="DSFC_HzRegSt" lnClass="DSFC" inst="4" prefix="" desc="Hz regulator
step 4 (critical) active status low under" />
        </LDevice>
        <LDevice inst="HG2GA1GA" desc="B-t-g unit generator">
          <LN lnType="MMXU_VPar" lnClass="MMXU" inst="1" prefix="" />
          <LN lnType="DGEN_St" lnClass="DGEN" inst="1" prefix="" />
        </LDevice>
        <LDevice inst="HG3GA1GA" desc="M-g set generator">
          <LN lnType="MMXU_VPar" lnClass="MMXU" inst="1" prefix="" />
          <LN lnType="DGEN_St" lnClass="DGEN" inst="1" prefix="" />
        </LDevice>
      </Server>
    </AccessPoint>
  </IED>
  <DataTypeTemplates>
    <LNodeType id="MHET_Prod" lnClass="MHET">
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="HeatOut" type="MV" />
      <DO name="MatTyp" type="ENG_MaterialKind" desc="M-not-used" />
    </LNodeType>
    <LNodeType id="MMXU_VPar" lnClass="MMXU" desc="Voltage_Power-active-reactive">
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="TotW" type="MV0" desc="Active power at PCC" />
      <DO name="TotVAr" type="MV0" desc="Reactive power at PCC" />
      <DO name="PPV" type="DEL0" desc="3 phase voltage at PCC" />
    </LNodeType>
    <LNodeType id="CSWI_BrkInd" lnClass="CSWI">
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="Pos" type="DPC" />
    </LNodeType>
    <LNodeType id="DRCC_PSetPt" lnClass="DRCC">
```

```
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="OutWSet" type="APC0" desc="P Set Point" />
      <DO name="DERStr" type="APC" desc="M-not-used" />
      <DO name="DERStop" type="APC" desc="M-not-used" />
    </LNodeType>
    <LNodeType id="DRCC_GenStrTm" lnClass="DRCC">
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="DERStr" type="APC1" desc="Generator start time" />
      <DO name="DERStop" type="TMW_Generated_APC" desc="M-not-used" />
    </LNodeType>
    <LNodeType id="DRCS_DERUnit" lnClass="DRCS">
      <DO name="RemOpTms" type="INS" desc="Remaining operational run time" />
      <DO name="Beh" type="ENS_BehaviourModeKind" /><DO name="OpTmh" type="INS" desc="M-not-used" />
      <DO name="ECPConn" type="SPS" desc="Breaker status" />
      <DO name="AutoMan" type="SPS" desc="M-not-used" />
      <DO name="ModOnConn" type="SPS" desc="Running and engaged" />
      <DO name="ModOnAval" type="SPS" desc="Running and ready for engaging" />
      <DO name="ModOffAval" type="SPS" desc="Stopped and ready to start" />
      <DO name="ModOffUnav" type="SPS" desc="Stopped but not ready to start" />
      <DO name="Loc" type="SPS" desc="In local-control mode" />
    </LNodeType>
    <LNodeType id="DRCS_DERUnit_Motor" lnClass="DRCS">
      <DO name="RemOpTms" type="INS" desc="Remaining operational run time" />
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="OpTmh" type="INS" desc="M-not-used" />
      <DO name="ECPConn" type="SPS" desc="Breaker status" />
      <DO name="AutoMan" type="SPS" desc="M-not-used" />
      <DO name="ModOnConn" type="SPS" desc="Running and engaged" />
      <DO name="ModOnAval" type="SPS" desc="Running and ready for engaging" />
      <DO name="ModOffAval" type="SPS" desc="Stopped and ready to start" />
      <DO name="ModOffUnav" type="SPS" desc="Stopped but not ready to start" />
      <DO name="ModStr" type="SPS" desc="Motor starting" />
      <DO name="Loc" type="SPS" desc="In local-control mode" />
    </LNodeType>
    <LNodeType id="DSFC_HzRegSt" lnClass="DSFC">
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="Blk" type="SPS" />
      <DO name="ClcExp" type="SPS" />
      <DO name="HzActSt" type="SPS" />
      <DO name="HzPwr" type="MV" />
      <DO name="Droop" type="ASG" />
      <DO name="RefHz" type="ASG" />
      <DO name="RegBndOvHz" type="ASG" />
      <DO name="RegDbOvHz" type="ASG" />
      <DO name="RegBndUnHz" type="ASG" />
      <DO name="RegDbUnHz" type="ASG" />
      <DO name="PwrRsvUnHz" type="ASG" />
    </LNodeType>
    <LNodeType id="DGEN_St" lnClass="DGEN">
      <DO name="Beh" type="ENS_BehaviourModeKind" />
      <DO name="OpTmh" type="INS" desc="M-not-used" />
      <DO name="GnOpSt" type="ENS_DERGeneratorStateKind" desc="M-not-used" />
      <DO name="GenSynSt" type="SPS" desc="Generator sync status" />
      <DO name="OpTmsRs" type="INS" desc="M-not-used" />
      <DO name="TotWh" type="MV" desc="M-not-used" />
```

```
    </LNodeType>
    <!-- DOType's below here -->
    <!-- DAType's below here -->
    <!-- EnumType's below here -->
  </DataTypeTemplates>
</SCL>
```