Realtime **Interface**
System Operator - DER

Dutch implementation of RfG interface requirements
Technical Specification Document

Netbeheer Nederland

01-07-2025 version 1.1

Contents

Document management and distribution

Document management

Version	Date	Changes	Author
1.0 final	February 20th 2024	Changes from Field tests, see attached Change Log	Technical specification WG
1.1 beta 1	May 1st 2025	TLS security added, Minor changes	Technical specification WG
1.1 final	July 1st 2025	Review remarks processed	Technical specification WG

Distribution

Version	Distribution date	Receivers	Comments
1.0 final	February 20th 2024	Public available via website	Final version for roll-out
1.1 beta 1	May 1st 2025	Product development and all other relevant stakeholders	Product development version
1.1 final	July 1st 2025	Public available via website	

1. Introduction

This document, together with the Protocol Implementation Document and SCL-file, forms the specification of the Realtime Interface (version 1.1). Whenever referred to the specification, the reference is to the set of these three documents. Realtime Interface version 1.1 is a minor update of Realtime Interface version 1.0.

1.1. Background

For the positioning and scope of the RTI, see [POS_DOC[1]], which includes more information on the background, scope and positioning. The Positioning Document furthermore briefly describes the applicable regulatory framework.

1.2. Goal of document

The goal of this document is to standardize the interface between System Operators and Power Generating Facility Owners, with regards to an RTI. To this end, the technical specifications for an RTI in the Dutch power system are defined. This document describes the technical specification and architecture of the NBNL RTI version 1.1. However, this specification is developed such that it can also be applied for connections with a mix of power generation and consumption as well as for larger connections[1].

[1] The position document is not published at the moment of releasing this document

1.3. Outline

This section gives an outline of each chapter and helps to better understand the document. The document has been organized in the following normative chapters:

Chapter 3 introduces the functional, non-functional and cyber security requirements on the Customer Endpoint.

Chapter 4 elaborates on the expected behaviour of the Customer Endpoint by introducing high-level process descriptions.

Chapter 5 introduces the architecture, data model, and functional behaviour.

Chapter 6 elaborates on ownership and demarcation.

Chapter 7 briefly discusses implementation and compliance verification**.**

The document concludes with several appendices with references, attachment and examples.

2.Smart Grid Architectural Model - SGAM

2.1. Introduction to SGAM

Smart grid related projects often have relatively complicated architecture models, due to the wide diversity of topics that need to be covered (e.g. physical infrastructure, information technology infrastructure, interfacing with different partners). To provide a uniform representation of the high-level architecture over the various topics, the Smart Grid Architectural Model (SGAM) has been developed.

SGAM utilizes a three-dimensional model, with a two-dimensional base. This base plane covers the different domains and zones of the power system. On the horizontal axis the five domains are covering the electrical energy conversion chain (bulk generation, transmission, distribution, DER, and Customer premises), and on the vertical axis zones are representing the hierarchical levels for management of the power system (process, field, station, operation, enterprise, and market) [CEN2012].

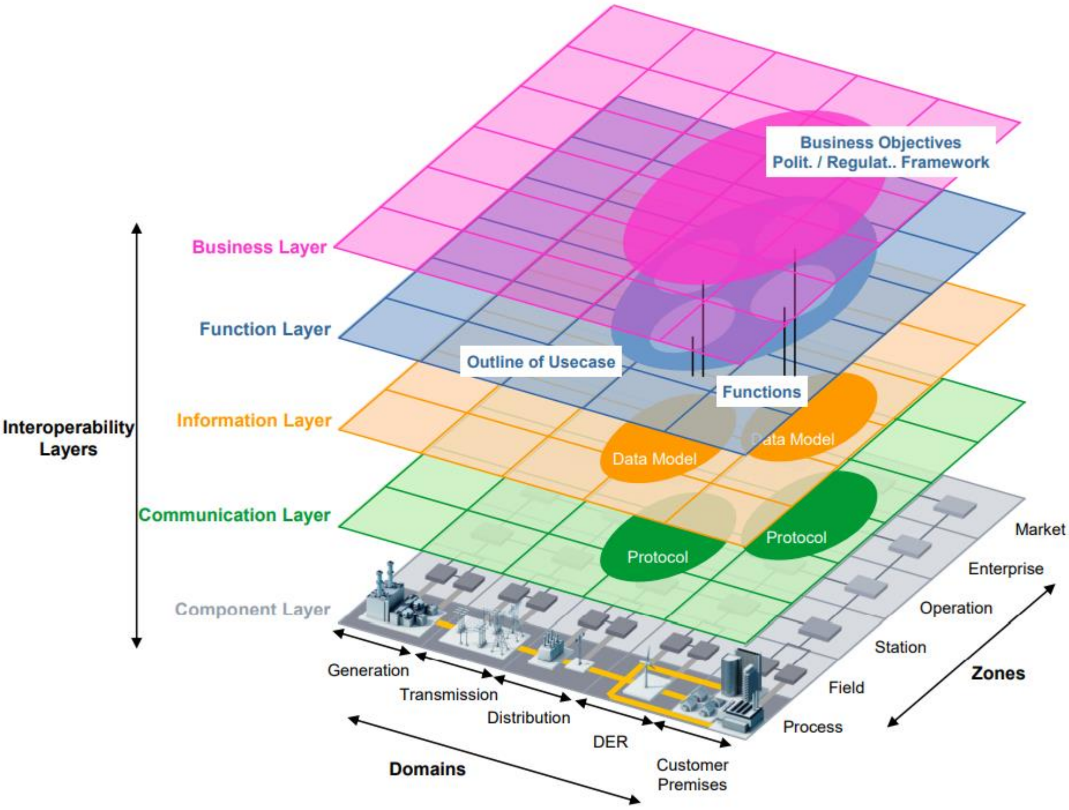


Figure 2: CEN-CENELEC-ETSI Example SGAM

The third dimension is created by adding various layers, describing the aspects of a smart grid. The bottom field provides the physical infrastructure of the smart grid (component layer), the remaining layers are covering the communication protocols, information exchange, main functions of clusters of infrastructure, and the business opportunities of the smart grid [CEN2012].

The main target audiences of the SGAM reference architecture are technical standardization committees, as the reference architecture provides a methodology on the different aspects of a technical standard. The technical specifications and architectural design of the Realtime Interface (RTI) described in this document can be seen as a national standard among Dutch (transmission and distribution) System Operators.

2.2. Description of the SGAM elements

This section briefly explains the different domains, zones, and layers in the SGAM, using the reference architecture [CEN2012] as input.

2.2.1. Domains

The domain-axis of the SGAM consists of the following domains:

- *Bulk generation*: representing large-scale generators (e.g. fossil fuel power plants).
- *Transmission*: representing the infrastructure for the transport of electricity.
- *Distribution*: representing the infrastructure for the distribution of electricity.
- *DER*: representing distributed energy resources (DERs) directly connected to the distribution network.
- *Customer premises*: hosting both producers and consumers of electricity. In this document, customers are typically referred to as Grid Connection Owners.

2.2.2. Zones

The zones-axis of the SGAM consists of the following zones:

- *Process*: includes the physical equipment directly involved in the process of moving energy (both primary and secondary components).
- *Field*: includes equipment to protect, control and monitor the process (intelligent electronic devices which obtain and/or use process data).
- *Station*: areal aggregation level for (e.g.) data concentration, function aggregation, substation automation.
- *Operation*: hosting power system control operations in its respective domain. For example, distribution management systems (DMSs) or EV fleet charge management systems.
- *Enterprise*: commercial and organisational processes, services and infrastructure.
- *Market*: possible market operations along the energy conversion chain (e.g. trading markets).

2.2.3. Layers

The SGAM consists of the following five layers:

- *Business*: business processes, services and organisations (including interactions) related to a use case.
- *Function*: functionality derived from use cases.
- *Information*: data model / information exchanged between systems and/or actors.
- *Communication*: means of communication between systems and/or actors.
- *Component*: devices, applications, persons and organisations and their interactions.

2.3. Introduction to IEC 61850

IEC 61850 is a set of standards that deals with communication networks and systems for power utility automation. It is developed in the late nineties, when the market was dominated by several proprietary standards. The objective was to have an interoperable communication standard and data model. IEC 61850 contains several different parts. The applicable parts are being listed in Attachment [A].

The choice of IEC 61850 for application in the RTI has been made in close collaboration with the different stakeholders. The big advantage of IEC 61850 is the sophisticated data model, as visualised in Figure 3. This data model supports the modelling of the complete chain: from a Physical Device up to detailed Data Attributes. All data which is being exchanged can be related to the asset / Physical Device it belongs to.

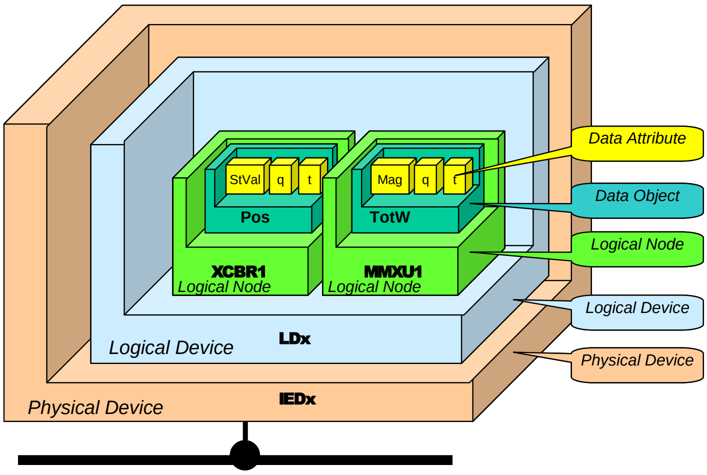


Figure 3: IEC 61850 data model structure, source: IEC 61850-1-1

In October 2021, the latest version of the data model regarding DER has been published, as result of common effort between System Operators, consultants and vendors. This data model is used in the RTI. The fact that it is an IEC standard furthermore helps in applying security measures. See also www.iec.ch.

2.4. Introduction to TLS

Transport Layer Security (TLS) is a cryptographic protocol that can be used to encrypt and authenticate data between a server and a client. It is a widely used protocol to secure web traffic, email and other data transmissions.

The protocol has evolved over time, with TLS 1.3 being the latest version, offering improved security and performance compared to its predecessors. TLS 1.2 is also considered secure if used with the right settings.

Integrating TLS with IEC 61850 plays a crucial role in protecting the communication between the devices in the RTI setup. The IEC 62351 series of standards has been introduced to provide implementation guidelines on TLS implementation in combination with IEC communication protocols in the Power System domain.

In the use case of the RTI, TLS is used for mutual authentication. This measure is needed to enable Customer Endpoints to effectively authenticate SO Endpoints in case the dedicated cabled connection is breached.

3.Requirements Customer Endpoint

This chapter describes the requirements that are applicable for the RTI. They are divided in different parts, starting with functional requirements, followed by the non-functional requirements, and concludes with the security requirements. The Grid Connection Owner has the freedom to realize the Customer Endpoint in different ways, as long as it meets the requirements described in this specification.

3.1. Functional Requirements

The functional behaviour of the RTI is described by the requirements below[2]. The IDs of the requirements are derived from a requirement database. Note that all sign conventions (e.g. the meaning of a plus or minus sign) shall be based on the definitions within the applicable IEC 61850 standard. For an implementation example of the P and Q signs, see IEC 61850-7-420 Ed. 2, figure 33. For more detailed implementation information, see the attached Protocol Implementation Document (Appendix A) and SCL file (Appendix B).

ID	[Setpoint-1]
Requirement	Receive a setpoint for the upper limit of generated active power P as a percentage [%] of the maximum capacity
Source	System Operator
Logical Node	DWMX
Description	
Setpoint-1 is the maximum allowed generated active power at the PoCC. The Setpoint is defined as a percentage of the accumulative "Maximum Capacity (MW)" in the PGMD form(s).	

ID	[Setpoint-2]
Requirement	Receive a setpoint for the upper limit of generated active power P in [MW]
Source	System Operator
Logical Node	DWMX
Description	
Setpoint-2 is the maximum allowed generated active power at the PoCC.	

[2] Note that the requirements presented in this specification all have unique IDs and represent a subset of all current, past, and future requirements in a master database. Therefore the numbering might not appear to be consistent. See also www.netbeheernederland.nl/dossiers/realtimeinterface

ID	[Setpoint-3]
Requirement	Receive a setpoint for the upper limit of consumed active power P in [MW]
Source	System Operator
Logical Node	DWMX
Description	
Setpoint-3 is the maximum allowed consumed (load) active power at the PoCC.	

ID	[Setpoint-8]
Requirement	Receive a reason why a setpoint for active power is sent by the System Operator
Source	System Operator
Logical Node	Nested within DWMX
Description	
Setpoint-8 reflects the reason for which use case a setpoint is sent by the System Operator. The reason is represented by an integer value. This requirement is only applicable for [Setpoint-1], [Setpoint-2] and [Setpoint-3]. For more detailed information see chapter 5.3.3.1.	

ID	[Measurements-1]
Requirement	Sent actual active power measurement on PoCC in [MW]
Source	Customer Endpoint
Logical Node	MMXU
Description	
Measurements-1 is the measurement of the actual active power on the PoCC in MW. The value is the total power of all three phases.	

ID	[Measurements-2]
Requirement	Sent actual reactive power measurement on PoCC in [MVAr]
Source	Customer Endpoint
Logical Node	MMXU
Description	
Measurements-2 is the measurement of the actual reactive power on the PoCC in MVAr. The value is the total reactive power of all three phases.	

ID	[Measurements-4]
Requirement	Sent actual current measurement on PoCC in [A]
Source	Customer Endpoint
Logical Node	MMXU
Description	
Measurements-4 is the measurement of the actual current on the PoCC for all the three phases in A. The values of the currents are always absolute values. This applies for all three phases individually.	

ID	[Measurements-7]
Requirement	Sent actual phase-neutral on PoCC in [kV]
Source	Customer Endpoint
Logical Node	MMXU
Description	
Measurements-7 is the measurement of the actual phase-neutral voltages on the PoCC for all the three phases in kV. This applies for all three phases individually.	

ID	[Measurements-8]
Requirement	Sent phase-phase measurements on PoCC in [kV]
Source	Customer Endpoint
Logical Node	MMXU
Description	
Measurements-8 is the measurement of the phase-phase voltages on the PoCC for all the three phases in kV. This applies for all three phases individually.	

ID	[Safe-Mode-1]
Requirement	In case of lost communication for a duration of a configurable time, restrict the generated active power P configurable level in percentage [%] or absolute values [MW]
Source	n/a
Logical Node	DWMX
Description	
Safe-Mode-1 restricts the amount of generated active power in case of a communication interruption on the RTI. The Customer Endpoint falls back to a predefined setpoint. The configurable generation power shall be configured using either the WMaxSetPct or WMaxSet Data Objects. The configurable time shall be exchanged by the WMaxFto Data Object. For more information, see chapter 4.1.	

ID	[Safe-Mode-2]
Requirement	Retrieve safe mode setpoint in either percentage [%] of the maximum capacity or in absolute values [MW]
Source	Customer Endpoint
Logical Node	DWMX
Description	
Safe-Mode-2 is the setpoint to which the Customer Endpoint has to fall back in case of a communication interruption on the RTI. The System Operator should be able to retrieve the actual setpoint value from the Customer Endpoint.	

ID	[Safe-Mode-3]
Requirement	Set safe mode setpoint in either percentage [%] of the maximum capacity or in absolute values [MW] remotely
Source	System Operator
Logical Node	DWMX
Description	
Safe-Mode-3 means the System Operator is able to set the setpoint for the safe mode at the Customer Endpoint through the RTI. The configurable generation power shall be configured using either the WMaxSetPct (percentage) or WMaxSet (absolute value) Data Objects.	

ID	[Safe-Mode-5]
Requirement	After restoring communication, buffered 15 minutes average active power measurements [MW] for the past 8 hours should be pushed to the System Operator ('buffered reporting')
Source	Customer Endpoint
Logical Node	MMXU
Description	
Safe-Mode-5 allows the System Operator to receive measurement values for a period where there was no communication with the Customer Endpoint through the RTI. The measurement values should be presented as 15 minutes average values of the ‘TotW’ data object, with a maximum time span of 8 hours. The average value should be calculated over the period of 15 minutes prior to the timestamp of the data set.	

ID	[Safe-Mode-6]
Requirement	After restoring communication, buffered 15 minutes maximum active power measurements [MW] for the past 8 hours should be pushed to the System Operator ('buffered reporting')
Source	Customer Endpoint
Logical Node	MMXU
Description	
Safe-Mode-6 allows the System Operator to receive measurement values for a period where there was no communication with the Customer Endpoint through the RTI. The measurement values should be presented as 15 minutes maximum values of the 'TotW' data object, with a maximum time span of 8 hours. The maximum value is the highest measurement in the data set in the 15 minutes prior to the timestamp. The timestamp of the measurement value shall be equal to the time of occurrence.	

ID	[Safe-Mode-7]
Requirement	After restoring communication, buffered 15 minutes minimum active power measurements [MW] for the past 8 hours should be pushed to the System Operator ('buffered reporting')
Source	Customer Endpoint
Logical Node	MMXU
Description	
Safe-Mode-7 allows the System Operator to receive measurement values for a period where there was no communication with the Customer Endpoint through the RTI. The measurement values should be presented as 15 minutes minimum values of the 'TotW' data object, with a maximum time span of 8 hours. The minimum value is the lowest measurement in the data set in the 15 minutes prior to the timestamp of. The timestamp of the measurement value shall be equal to the time of occurrence.	

ID	[Customer-Configuration-1]
Requirement	Retrieve state of Customers installation
Source	Customer Endpoint
Logical Node	DGEN
Description	
Customer-Configuration-1 is the possibility for the System Operator to retrieve the actual state of the Customer Endpoint. In case of communication loss, changes in the past 8 hours should be pushed to the System Operator ('buffered reporting')	

ID	[Customer-Configuration-7]
Requirement	Retrieve RTI version information of Customers Endpoint
Source	Customer Endpoint
Logical Node	LLN0
Description	
Customer-Configuration-7 is the possibility for the System Operator to retrieve the RTI version information of the Customer Endpoint. See chapter 5.3.2.1.	

ID	[Customer-Updates-1]
Requirement	The operating system at the Customer Endpoint has to be able to perform updates and/or patches.
Source	Customer Endpoint
Logical Node	n/a
Description	
During the technical life time of the Customer Endpoint, new functionalities may have to be added or security risks may need to be addressed. Therefore, the Customer Endpoint has to be able to perform updates and patches to for example gain new functionalities. See also related requirement ID [Contract-Updates-1].	

3.2. Non-Functional Requirements

The following non-functional requirements[3] have to be implemented.

ID	[Availability-1]
Requirement	IEC 60870-4 class A1: 99,00%
Source	RTI
Logical Node	n/a
Description	
Availability of communication from System Operator Endpoint to Customer Endpoint, based on a time period of at least 6 months, in line with the referred standard chapter 3.2.1.	

[3] Note that the requirements presented in this specification all have unique IDs and represent a subset of all current, past, and future requirements in a master database. Therefore the numbering might not appear to be consistent.

ID	[Accuracy-1]
Requirement	Class 1, as described in the IEC 61869 set of standards
Source	Customer Endpoint
Logical Node	MMXU
Description	
Accuracy of measurements, referenced to the measurement values on the PoCC. Note that these values can be measured directly on the PoCC, or can be obtained on another location behind the PoCC. The accuracy always shall be within the stated requirement.	

ID	[Accuracy-2]
Requirement	Maximum deviation with UTC-time of 10 seconds
Source	Customer Endpoint
Logical Node	n/a
Description	
Accuracy of time synchronization. Reference is UTC.	

ID	[Accuracy-3]
Requirement	Maximum deviation with UTC-time of 10 seconds
Source	System Operator
Logical Node	n/a
Description	
Accuracy of time synchronization. Reference is UTC.	

ID	[Bandwith-1]
Requirement	Local interface is standard Ethernet (10/100/1000Mbit)
Source	RTI
Logical Node	n/a
Description	
Required bandwidth on the Realtime Interface.	

ID	[Response-Time-1]
Requirement	< 4 seconds
Source	RTI
Logical Node	n/a
Description	
Response time communication interface (acknowledge) between System Operator Endpoint and Customer Endpoint (communication line).	

ID	[Response-Time-2]
Requirement	Depends on the agreed use case framework
Source	Customer Endpoint
Logical Node	n/a
Description	
Response time electrotechnical (asset) response at Customer side. Time from receiving setpoint from System Operator to achieving the desired setpoint.	

ID	[Response-Time-3]
Requirement	< 3 minutes
Source	System Operator
Logical Node	n/a
Description	
In case of a power failure: Time to restore communications after energizing the power system.	

ID	[Response-Time-5]
Requirement	< 3 minutes
Source	Customer Endpoint
Logical Node	n/a
Description	
In case of a power failure: Time to restore communications after energizing the power system.	

ID	[Response-Time-6]
Requirement	< 3 minutes
Source	System Operator
Logical Node	n/a
Description	
Time needed to restore communications after a restart of the System Operator Endpoint.	

ID	[Response-Time-8]
Requirement	< 3 minutes
Source	Customer Endpoint
Logical Node	n/a
Description	
Time needed to restore communications after a restart of the Customer Endpoint.	

3.3. Functional Cyber Security Requirements

The following functional security related requirements are applicable.

ID	[TLS-Customer-Standards-1]
Requirement	Support for TLS 1.2 as described in IEC 62351-3 and -4
Source	Customer Endpoint
Description	The Endpoint shall support protecting IEC 61850 MMS communication with TLS 1.2 as described in IEC 62351-3:2023 and in IEC 62351-4:2018+AMD1:2020 CSV for Transport Security in the native mode of operation. Where IEC 62351-3:2023 updates the content of IEC 62351-4:2018+AMD1:2020 CSV, such as in the case of supported cipher suites and cryptographic algorithms, the newer IEC 62351-3:2023 shall be followed.

ID	[TLS-Customer-Standards-2]
Requirement	Support for TLS 1.3 as described in IEC 62351-3
Source	Customer Endpoint
Description	The endpoint shall support protecting IEC 61850 MMS communication with TLS 1.3 as described in IEC 62351-3:2023.

ID	[TLS-Customer-Standards-3]
Requirement	Compliance with IEC 62351-9 as required by -3 and -4
Source	Customer Endpoint
Description	The Endpoint shall comply at least partially with other standards in the IEC 62351 series, such as IEC 62351-9:2023, as required to comply with IEC 62351-3:2023 and IEC 62351-4:2018+AMD1:2020 CSV.

ID	[TLS-Customer-Ciphers-1]
Requirement	Support for cipher suites: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_RSA_WITH_NULL_SHA256
Source	Customer Endpoint
Description	TLS 1.2 shall support the following cipher suites: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_RSA_WITH_NULL_SHA256 (in addition to the mandatory cipher suites in IEC 62351-3:2023).

ID	[TLS-Customer-Ciphers-2]
Requirement	Support for cipher suite TLS_AES_256_GCM_SHA384 and TLS_SHA384_SHA384
Source	Customer Endpoint
Description	TLS 1.3 shall support the following cipher suites: - TLS_AES_256_GCM_SHA384 - TLS_SHA384_SHA384 (in addition to the mandatory cipher suites in IEC 62351-3:2023).

ID	[TLS-Customer-Ciphers-3]
Requirement	Enable only the needed TLS version and cipher suites
Source	Customer Endpoint
Description	Only the TLS version and cipher suites specifically agreed with the system operator shall be enabled. The other TLS version and other cipher suites, even of the enabled version, shall be disabled.

ID	[TLS-Customer-Cert-1]
Requirement	Support for setting certificate fields to selected values
Source	Customer Endpoint
Description	It shall be possible to limit the use of the certificate to the intended scope by setting the certificate fields to selected values as follows: • Validity = Determined by each SO. A longer period is advised, which should be a maximum of 15 years • Key usage = digital signature, key encipherment (key encipherment might be needed if a cipher suite using RSA is used) • Extended key usage = TLS WWW Server Authentication (OID.1.3.6.1.5.5.7.3.1)

ID	[TLS-Customer-Cert-2]
Requirement	Support for exporting certificates
Source	Customer Endpoint
Description	The Endpoint shall support exporting certificates.

ID	[TLS-Customer-Cert-3]
Requirement	Do not export private keys
Source	Customer Endpoint
Description	Do not export private keys. Exported certificates for this context shall only have public keys. The corresponding private keys shall not leave the endpoint.

ID	[TLS-Customer-Cert-4]
Requirement	Do not import private keys
Source	Customer Endpoint
Description	Do not import private keys. Private keys shall be generated inside the endpoint. The endpoint shall not allow importing certificates with the corresponding private keys.

ID	[TLS-Customer-Mon-1]
Requirement	Log certificate management events
Source	Customer Endpoint
Description	The Endpoint shall enable monitoring of the certificate management events related with, e.g.: • Generation • Trusted certification authorities (adding or removing individual root certificates) • Validation • Expiration • Revocation • Renewal Implementation guidance: The events are related with the own certificates and the certificates of the other Endpoint. Events related with expiration are logged before the certificates expire and when it happens. For the events logged before the certificates expire, it is possible to configure the number of days before the event when the events are logged.

ID	[TLS-Customer-Mon-2]
Requirement	Support for RFC 5424 syslog message format
Source	Customer Endpoint
Description	It shall be possible to extract the certificate management events to make the events readable at least for troubleshooting and forensics, which might involve the SO. This shall be done in the syslog message format described in RFC 5424. Implementation guidance: If the original format does not follow this RFC, then at least the needed information to create a message according to this RFC must be recorded so that it can be used when exporting.

ID	[TLS-Customer-Auth-1]
Requirement	Authenticate Customer Endpoints
Source	Customer Endpoint
Description	The Endpoint shall authenticate an SO Endpoint trying to connect by validating the received certificate and verifying that the SO Endpoint has the corresponding private key.

ID	[TLS-Customer-Auth-2]
Requirement	Only complete connections to authenticated Customer Endpoints
Source	Customer Endpoint
Description	The Endpoint shall only complete a connection if the SO Endpoint is successfully authenticated.

ID	[TLS-Customer-Auth-3]
Requirement	Validate certificates based on date of expiration, certification chain and revocation
Source	Customer Endpoint
Description	Certificate validation can only give a positive result if: • the received certificate has not expired, and • its certificate chain is positively verified, and • the certificate is not revoked.

ID	[TLS-Customer-Auth-4]
Requirement	Ignore eventual IP address mismatches
Source	Customer Endpoint
Description	An eventual mismatch between the IP address in the SO endpoint certificate and the IP address of the SO endpoint presented in the network shall not influence the establishment of a connection, i.e., a connection shall still be established if all remaining validations succeeded with positive results. The mismatch shall still be visible in the security events of the customer endpoint.

ID	[TLS-Customer-Chain-1]
Requirement	Support for updating the list of root certificates
Source	Customer Endpoint
Description	It shall be possible to add or remove individual root certificates from the endpoint. Implementation guidance: Add or remove individual root certificates from the endpoint through firmware or software update or through user configuration.

ID	[TLS-Customer-Revo-1]
Requirement	Validate the revocation status of certificates
Source	Customer Endpoint
Description	The Endpoint shall be able to validate the revocation status of a certificate even without connecting to a central system. Implementation guidance: A CRL can be manually imported or a local list of revoked certificates can be maintained through firmware or software update or through user configuration.

3.4. Non-functional Cyber Security Requirements

In addition to the functional Cyber Security Requirements described in chapter 3.3, the following requirements must be implemented to protect the communication between the System Operator Endpoint and the Customer Endpoint of the RTI. They also protect any devices of the System Operator installed in the Grid Connection Owner premises.

ID	[Network-Segmentation-1]
Requirement	The System Operator Endpoint and the Customer Endpoint shall communicate through a dedicated cabled connection provided by the Customer
Description	
Any equipment used for converting between fibre and ethernet can only be used for the purpose of this connection. At the Customer side, the termination cable shall connect to a network interface of the (e.g. park- or energy management) controller and not to a network device. Under no circumstance shall this cable be disconnected (and connected to a network). This ensures that the System Operator Endpoint and the Customer Endpoint are the only two hosts in the communication channel. Further, it prevents connections with high risk profile networks, such as wi-fi networks or the Internet.	

ID	[Physical-Security-1]
Requirement	If there must be System Operator equipment in the Grid Connection Owner premises, then the Grid Connection Owner shall provide a separate secure area to place this equipment that only the System Operator can access
Description	
The System Operator should already have a room where they have medium voltage equipment in the Grid Connection Owner location. Where this room exists, it should be used to place the System Operator equipment for the Realtime Interface.	

A compromised Customer Endpoint can be used to compromise the Realtime Interface, the electricity grid or the System Operator Endpoint. Therefore, the following minimum set of measures for the Customer side will be included in the Contract.

ID	[Contract-Segmentation-1]
Requirement	The Customer Endpoint shall not be directly accessible from the Internet on any interface, but only through a secure solution such as a VPN or jump server
Description	
The Requirement Network-Segmentation-1 applies to the Realtime Interface between the System Operator Endpoint and the Customer Endpoint. Feasible and effective solutions must be identified for the other interfaces. For instance, a virtual private network can be used to encrypt and protect the integrity of communications with remote systems or human users over the Internet, and a jump server can force remote human users to use a specific application in the middle of the communication path. These solutions can be used together and/or in combination with other solutions. Further, the overall solution should require multi-factor authentication, restrict the users' access according with their authorizations and allow monitoring of user related activity.	

ID	[Contract-Hardening-1]
Requirement	The administrator of the Customer Endpoint shall replace all default passwords with unique and strong passwords
Description	
This applies at least to the Endpoint itself and to all other devices in the same local area network. Strong passwords can be created with effective complexity, length and randomness based on Section 5 of the NIST SP 800-63B. They should be unique for each function in each device.	

ID	[Contract-Updates-1]
Requirement	The administrator of the Customer Endpoint shall have a patching process by which vulnerabilities are solved and updates are applied at least once a year
Description	
This applies at least to the Endpoint itself and to all other devices in the same local area network. This requires monitoring vulnerability lists, vendor advisories and new release notes. Ideally, patches and updates should be applied right after they are tested for compatibility issues.	

ID	[Contract-Training-1]
Requirement	The administrator of the Customer Endpoint shall have basic security training and awareness
Description	
A video covering the importance of these measures, how to implement them on a general level and how to test the implementation is available on the website of Netbeheer Nederland.	

The Grid Connection Owner should take complementary measures not directly related with the Realtime Interface scope based on a risk assessment and existing security standards such as ISO 27001 or IEC 62443 to further protect its Endpoint and any systems connected to it.

These complementary measures can be based on the requirement sets of European Network for Cyber Security (ENCS) and security advice from WindEurope and SolarPower Europe (see *encs.eu*, *windeurope.org* and *solarpowereurope.org*).

4. Process description

This chapter provides a high-level process description of the expected operational behaviour of the Customer Endpoint. The operational behaviour of the Realtime Interface is defined by two types of processes, which are described in this chapter:

- Core process, responsible for handling setpoints, settings and measurements. This process provides the core functionality of the RTI during a normal operational mode, when the IEC 61850 connection is available. The expectation is the Customer Endpoint will operate within this process most of the time.
- Overall process, responsible for handling different operational modes. To ensure secure operation of the overall power system, the behaviour of individual Customer Endpoints during abnormal operation is described. Abnormal operation includes boot periods, reboot periods and periods during which the IEC 61850 connection is unavailable. The overall process furthermore describes its relationship with the core process.

On critical locations in both processes, a predefined state is set. These states are represented by an enumerated value. The predefined state enumerations are derived from the IEC 61850 standard, but applied in the context of the RTI. The states provide the SO information about the current operational state of the RTI. Not all states have a direct link with the DER status. For a detailed description of the predefined states, see chapter 5.3.3.3.

4.1. Core process Realtime Interface

The core processes of the Realtime Interface consists of three main tasks (see Figure 4).

- Receive new reasons, (safe mode) setpoints and safe mode time-out values and act accordingly on them.
- Periodically send reports (including measurements and settings) to inform the SO Endpoint.
- Monitor and report on DER (partial) unavailability. As a result, the Endpoint can have different states within the core process,

For the monitoring on DER (partial) unavailability, a differentiation between full availability and (partial) unavailability of the connected DER is made. (Partial) unavailability, is defined as one or multiple connected DERs is unable to process the operational setpoints. A practical example could be the case of multiple turbines or inverters behind a PoCC.

As long as the RTI is in the operational mode and the IEC 61850 connection is available, the Customer Endpoint remains within the core process (see chapter 4.1).

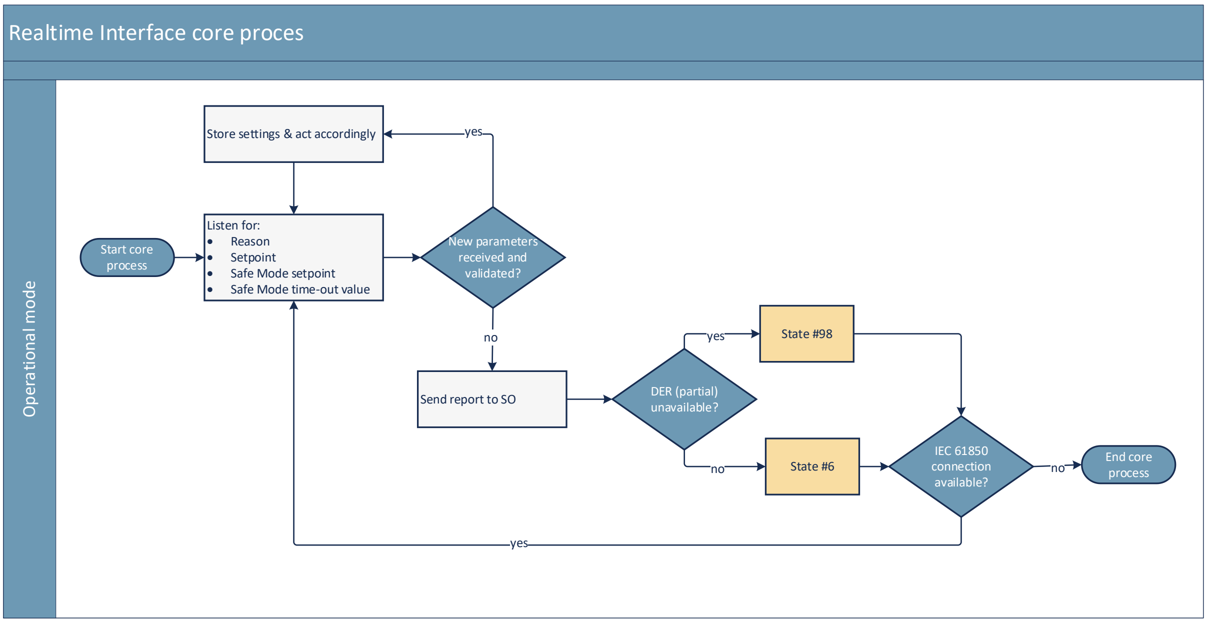

Realtime Interface core proces
Operational mode
Start core process
Store settings & act accordingly
yes
Listen for:
• Reason
• Setpoint
• Safe Mode setpoint
• Safe Mode time-out value
New parameters received and validated?
no
Send report to SO
DER (partial) unavailable?
yes
State #98
no
State #6
IEC 61850 connection available?
no
End core process
yes

Figure 4: Process description of the core processes of the RTI

4.2. Overall process for controlling operational modes

In the overall process (see Figure 5), the expected behaviour of the Customer perspective is visualised, including its relation to the core process (see chapter 4.1). In principle, the RTI is a transparent connection to exchange signals. Nevertheless, some autonomous behaviour needs to be in place to guarantee safe and efficient operation, during a boot or reboot period, and in case the Customer Endpoint loses its IEC 61850 connection.

The overall process distinguishes four swim lanes, describing four operational modes. The four operational modes are:

- Initial boot mode
- Operational mode
- Safe operating mode
- Reboot mode

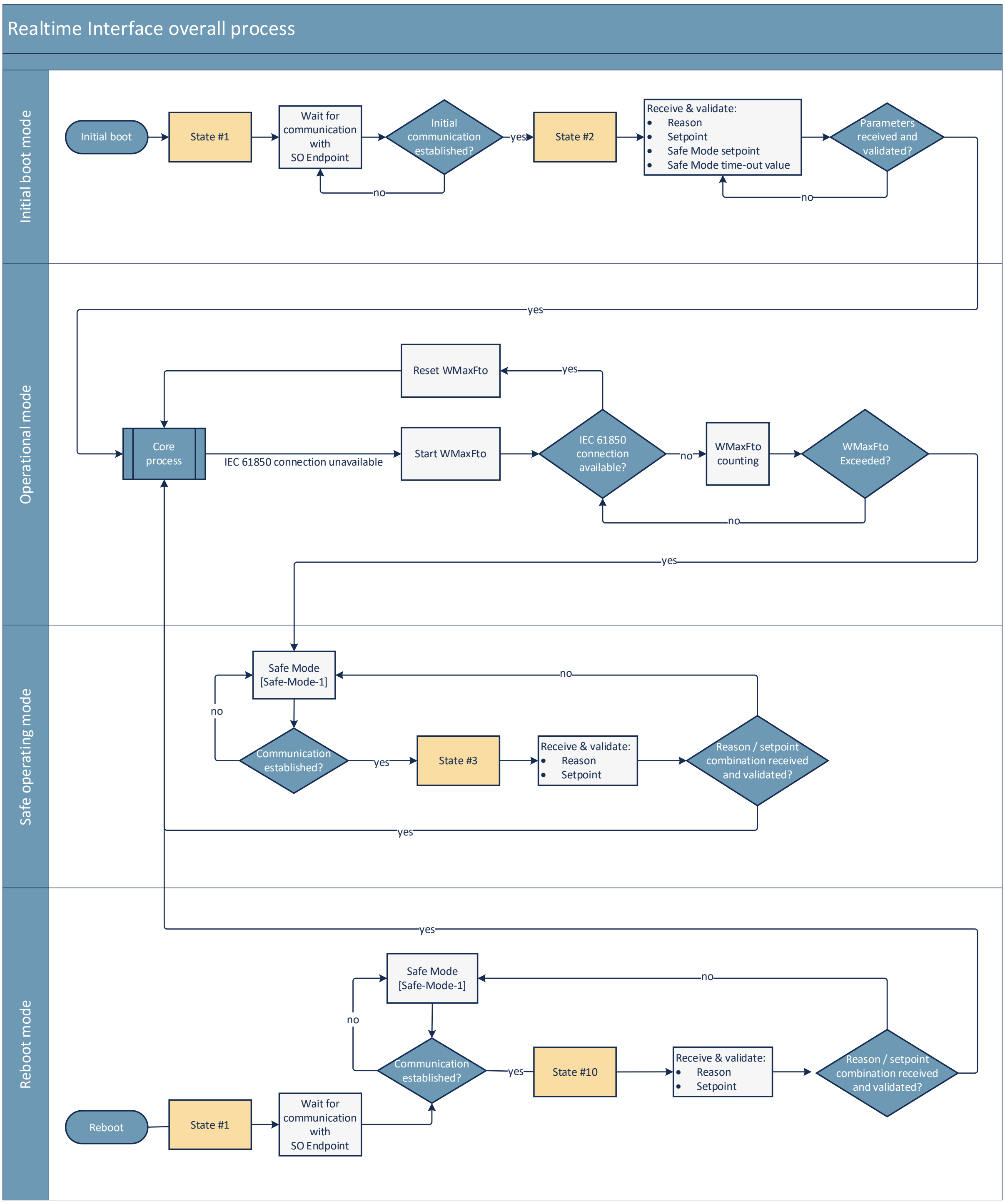

Realtime Interface overall process
Initial boot mode
Initial boot
State #1
Wait for communication with SO Endpoint
Initial communication established?
yes
no
State #2
Receive & validate:
• Reason
• Setpoint
• Safe Mode setpoint
• Safe Mode time-out value
Parameters received and validated?
no
Operational mode
yes
Reset WMaxFto
yes
Core process
IEC 61850 connection unavailable
Start WMaxFto
IEC 61850 connection available?
no
WMaxFto counting
WMaxFto Exceeded?
no
yes
Safe operating mode
Safe Mode [Safe-Mode-1]
no
no
Communication established?
yes
State #3
Receive & validate:
• Reason
• Setpoint
Reason / setpoint combination received and validated?
yes
Reboot mode
yes
Safe Mode [Safe-Mode-1]
no
no
Communication established?
yes
State #10
Receive & validate:
• Reason
• Setpoint
Reason / setpoint combination received and validated?
Reboot
State #1
Wait for communication with SO Endpoint

Figure 5: Overall process description of expected behaviour in the four operational modes of the RTI and its relationship with the core process.

4.2.1. Initial boot mode

Initial boot mode describes the starting behaviour of the Customer Endpoint in case no previous safe mode settings are available. The Power Generating Facility Owner may not deliver any power to the System Operator until all the following criteria are fulfilled:

- an active IEC 61850 connection with the Endpoint of the System Operator is established
- a valid reason and setpoint from the System Operator are received, see chapter 5.3.3.1
- a safe mode setpoint and fallback time setting from the System Operator are received

4.2.2. Operational mode

Operational mode means that the core process for handling setpoints, settings and reports (see chapter 4.1 for the core process) is running. Before entering the operational mode, the Customer Endpoint received the initial operational parameters from the System Operator. The initial operational parameters are:

- Reason
- Setpoint
- Safe Mode setpoint
- Safe Mode time-out value

The operational mode swimlane describes the process related to monitoring the (un)availability the IEC 61850 connection.
The RTI connection is being supervised by the Customer Endpoint. In case the IEC 61850 connection has been lost, the WMaxFto timer shall start. While the connection is lost and the duration of the lost connection is within the parameterized time (LN DWMX, Data Object WMaxFto), the RTI will stay in the operational mode. If and when the parameterized time is exceeded, the Customer Endpoint will change to Safe operating mode.

4.2.3. Safe operating mode

Safe operating mode is reached when the Customer Endpoint has no connection with the System Operator Endpoint for more than a parameterized time (LN DWMX, Data Object WMaxFto), as described in the section about the operational mode. This triggers the safe mode functionality, forcing the Customer Endpoint to the predefined Safe mode setpoint (see chapter 5.3.3.1).

4.2.4. Reboot mode

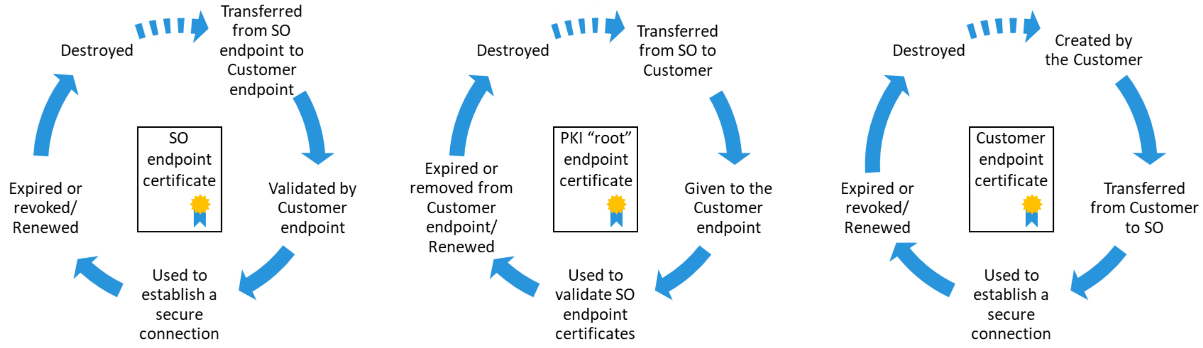
Reboot mode is only applicable in case the Customer Endpoint starts up with the safe mode settings still available (e.g. stored in non-volatile memory). In case no safe mode settings are available, initial boot mode is applicable.

Reboot mode can for example be a result of an outage, a restart of the operating system or a firmware upgrade. To prevent damage to the power system, the Customer Endpoint will follow a predefined Safe Mode setpoint (see chapter 5.3.3.1). This Safe Mode setpoint should be followed until the connection with the System Operator Endpoint is re-established and a valid reason / setpoint combination is received from the System Operator.

4.3. TLS certificate management processes

The functional cyber security requirements of Section 3.3 refer to three types of certificates: SO Endpoint certificates, PKI “root” certificates and Customer Endpoint certificates. PKI “root” certificates are used to validate SO Endpoint certificates.

To make sure that secure TLS connections can be successfully established and that TLS as a security measure has the needed effectiveness, these certificates must be managed through secure processes. The process steps associated with the lifecycle of each type of certificate are represented in Figure 6. Each step is detailed in the sections below.



Destroyed
Transferred from SO endpoint to Customer endpoint
SO endpoint certificate
Validated by Customer endpoint
Used to establish a secure connection
Expired or revoked/ Renewed
Destroyed
Transferred from SO to Customer
PKI “root” endpoint certificate
Given to the Customer endpoint
Used to validate SO endpoint certificates
Expired or removed from Customer endpoint/ Renewed
Destroyed
Created by the Customer
Customer endpoint certificate
Transferred from Customer to SO
Used to establish a secure connection
Expired or revoked/ Renewed

Figure 6: Certificate lifecycles

4.3.1. Initial setup of certificates

It is assumed that the Customer has a secure process in place to create a keypair and a certificate with the public key for the Customer Endpoint that adheres to the technical specifications. The process of certificate generation is out of scope for this document.

The Customer provides the certificate of the Customer Endpoint to the SO through a secure channel, provided by the SO. The Customer Endpoint certificate will be pinned to the SO Endpoint by the SO. The Customer will use the keypair linked to this certificate to communicate with the SO Endpoint.

The PKI “root” certificate of the SO will be provided to the Customer Endpoint through a secure channel. This certificate must be configured on the Customer Endpoint to be used in the validation of the SO Endpoint certificate. The mentioned process flows are depicted in Figure 7.

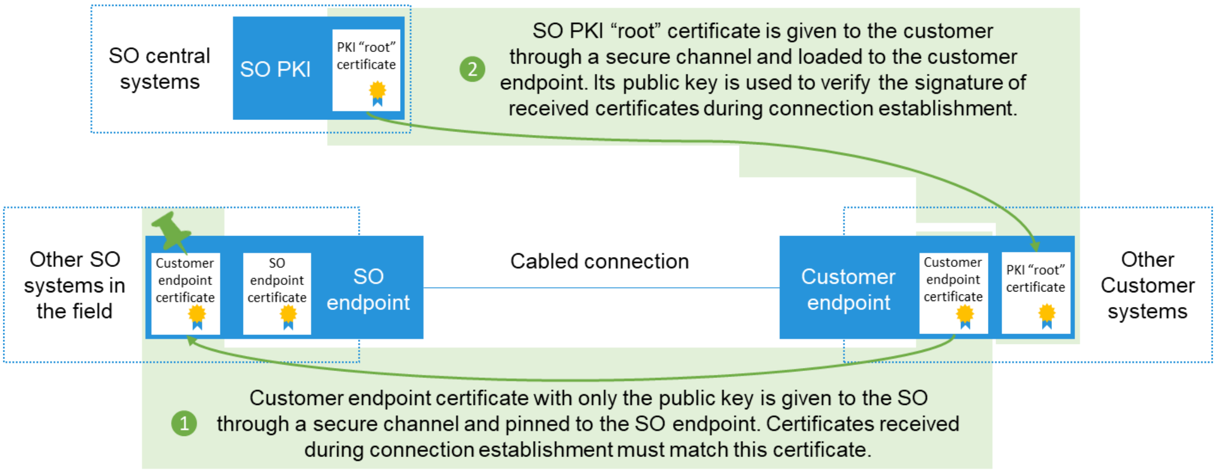

SO central systems
SO PKI
PKI “root” certificate
2
SO PKI “root” certificate is given to the customer through a secure channel and loaded to the customer endpoint. Its public key is used to verify the signature of received certificates during connection establishment.
Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Customer endpoint
Customer endpoint certificate
PKI “root” certificate
Other Customer systems
1
Customer endpoint certificate with only the public key is given to the SO through a secure channel and pinned to the SO endpoint. Certificates received during connection establishment must match this certificate.

Figure 7: Initial setup of certificates

4.3.2. Renewal of SO Endpoint certificate

Before the SO Endpoint certificate expires, the renewal process of the SO Endpoint certificate will start. This has no impact on the setup and no action is required on the Customer Endpoint. The Customer Endpoint will validate the new SO Endpoint certificate successfully because it will be issued by the same SO PKI of which the ”root” certificate is configured on the Customer Endpoint. The mentioned process flows are depicted in Figure 8.

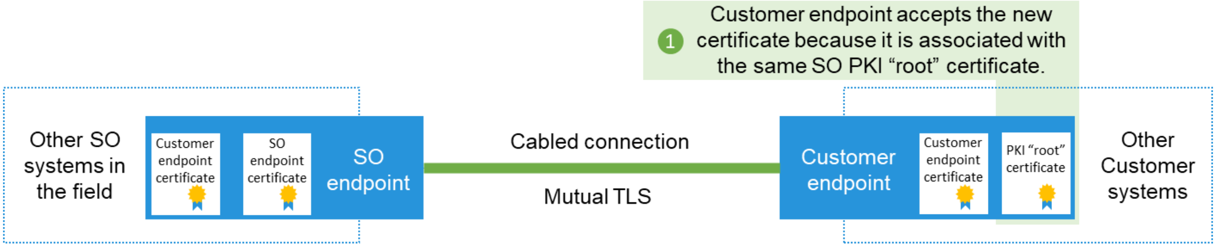

1
Customer endpoint accepts the new certificate because it is associated with the same SO PKI “root” certificate.
Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Mutual TLS
Customer endpoint
Customer endpoint certificate
PKI “root” certificate
Other Customer systems

Figure 8: Renewal of SO Endpoint certificate

4.3.3. Renewal of SO PKI "root" certificate

Before the SO PKI root certificate expires, the renewal process of the SO PKI "root" certificate will start. The new SO PKI "root" certificate is provided to the Customer through a secure channel and loaded to the Customer Endpoint. Its public key is used to verify the signature of received certificates during connection establishment.

The old SO PKI "root" certificate must be removed from the Customer Endpoint. The mentioned process flows are depicted in Figure 9.

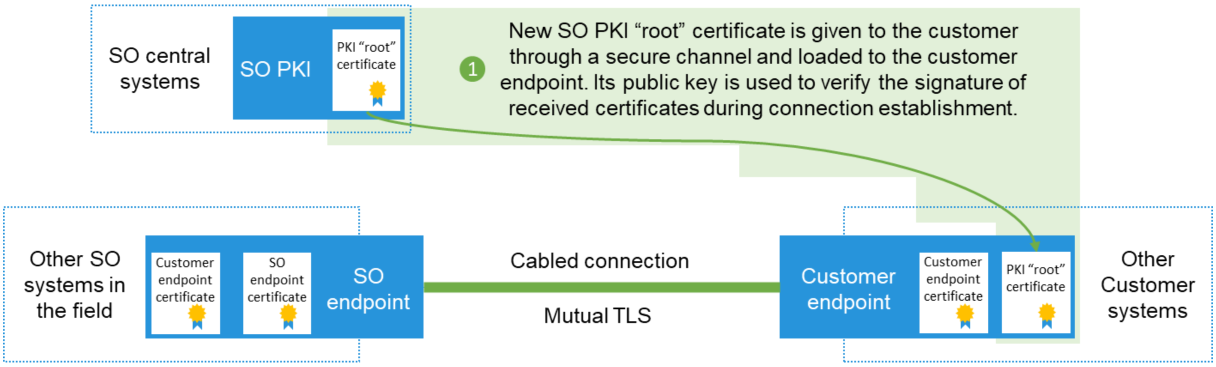

SO central systems
SO PKI
PKI "root" certificate
1
New SO PKI "root" certificate is given to the customer through a secure channel and loaded to the customer endpoint. Its public key is used to verify the signature of received certificates during connection establishment.
Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Mutual TLS
Customer endpoint
Customer endpoint certificate
PKI "root" certificate
Other Customer systems

Figure 9: Renewal of SO PKI "root" certificate

4.3.4. Renewal of Customer Endpoint certificate

Before the Customer certificate expires, the renewal process of the Customer Endpoint certificate is started by the Customer. A new certificate will be created adhering to the technical specifications and is given to the SO through a secure channel. After confirmation that the SO has configured the new certificate, the Customer will use the keypair linked to the new certificate to communicate with the SO Endpoint. The mentioned process flows are depicted in Figure 10.

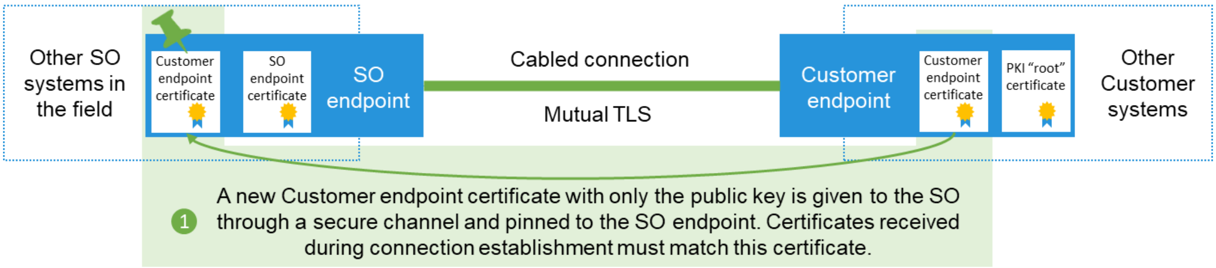

Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Mutual TLS
Customer endpoint
Customer endpoint certificate
PKI "root" certificate
Other Customer systems
1
A new Customer endpoint certificate with only the public key is given to the SO through a secure channel and pinned to the SO endpoint. Certificates received during connection establishment must match this certificate.

Figure 10: Renewal of Customer Endpoint certificate

4.3.5. Revocation and renewal of SO Endpoint certificate

Would there be a sign that the private key of the SO Endpoint was compromised coming from the SO or the Customer, the SO Endpoint certificate will be revoked. Each party will provide a point of contact that can be used to notify them of such compromise. Either party will notify the other through a secure channel. The Customer makes the Endpoint not trust the revoked SO Endpoint certificate.

The SO will create a new SO Endpoint certificate. The Customer Endpoint will validate communication with the new SO Endpoint certificate successfully because it is issued by the same SO Endpoint root PKI of which the "root" certificate is configured on the Customer Endpoint. The mentioned process flows are depicted in Figure 11.

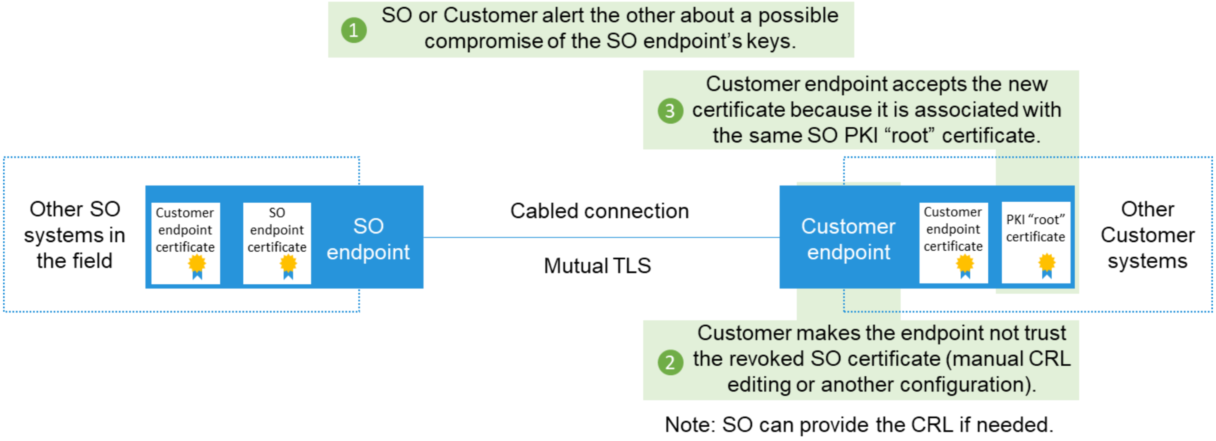

1 SO or Customer alert the other about a possible compromise of the SO endpoint's keys.
3 Customer endpoint accepts the new certificate because it is associated with the same SO PKI "root" certificate.
Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Mutual TLS
Customer endpoint
Customer endpoint certificate
PKI "root" certificate
Other Customer systems
2 Customer makes the endpoint not trust the revoked SO certificate (manual CRL editing or another configuration).
Note: SO can provide the CRL if needed.

Figure 11: Revocation and renewal of SO Endpoint certificate

4.3.6. Revocation and renewal of SO PKI "root" certificate

Would there be a sign that the private key of the SO PKI was compromised coming from the SO or the Customer, the SO PKI "root" certificate will be revoked. Each party will provide a point of contact that can be used to notify them of such compromise.

Either party will notify the other through a secure channel. The Customer makes the Endpoint not trust the revoked PKI root certificate (and SO Endpoint certificate if this is not done automatically).

The new SO PKI "root" certificate is provided to the customer through a secure channel and loaded to the Customer Endpoint. Its public key is used to verify the signature of received certificates during connection establishment.

The old SO PKI "root" certificate must be removed from the Customer Endpoint.
The mentioned process flows are depicted in Figure 12.

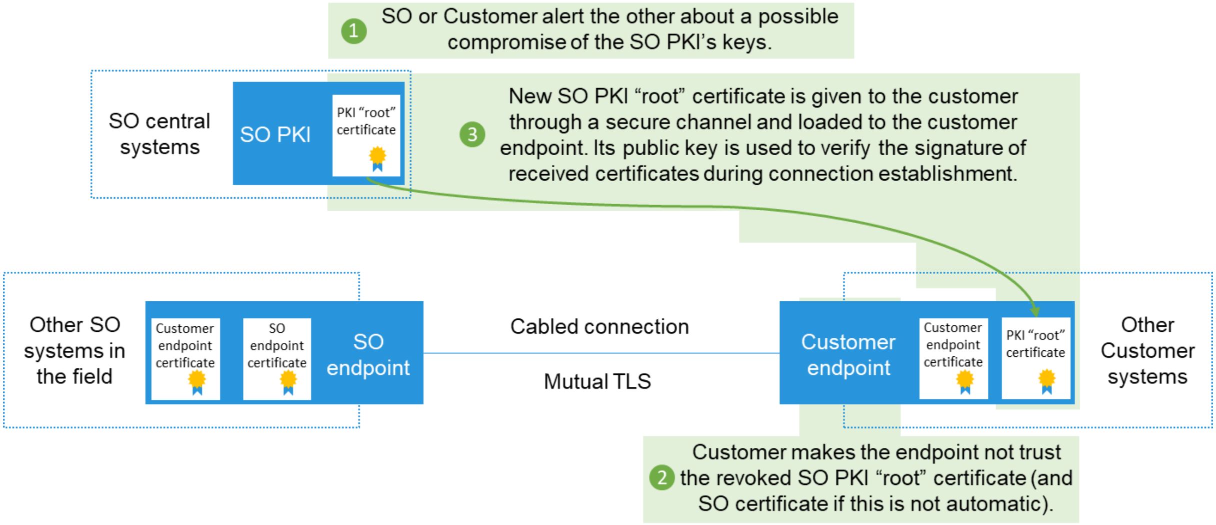

1 SO or Customer alert the other about a possible compromise of the SO PKI's keys.
SO central systems
SO PKI
PKI "root" certificate
3 New SO PKI "root" certificate is given to the customer through a secure channel and loaded to the customer endpoint. Its public key is used to verify the signature of received certificates during connection establishment.
Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Mutual TLS
Customer endpoint
Customer endpoint certificate
PKI "root" certificate
Other Customer systems
2 Customer makes the endpoint not trust the revoked SO PKI "root" certificate (and SO certificate if this is not automatic).

Figure 12: Revocation and renewal of SO PKI "root" certificate

4.3.7. Revocation and renewal of Customer Endpoint certificate

Would there be a sign that the private key of the Customer Endpoint was compromised coming from the SO or the Customer, the Customer Endpoint certificate must be revoked (and unpinned from the SO Endpoint). Each party will provide a point of contact that can be used to notify them of such compromise.

Either party will notify the other trough a secure channel. After generating a new certificate, the Customer provides the certificate of the Customer Endpoint to the SO through a secure channel, which will be pinned to the SO Endpoint by the SO. The Customer will use the keypair linked to this certificate to communicate with the SO Endpoint. The mentioned process flows are depicted in Figure 13.

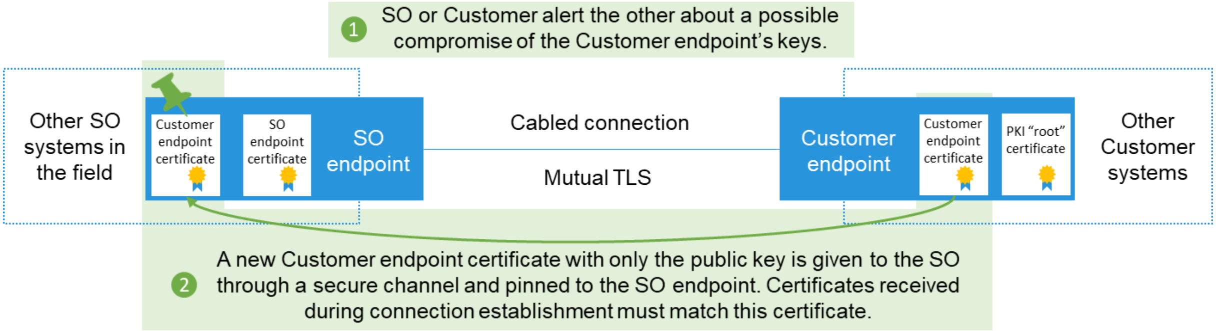

1 SO or Customer alert the other about a possible compromise of the Customer endpoint's keys.
Other SO systems in the field
Customer endpoint certificate
SO endpoint certificate
SO endpoint
Cabled connection
Mutual TLS
Customer endpoint
Customer endpoint certificate
PKI "root" certificate
Other Customer systems
2 A new Customer endpoint certificate with only the public key is given to the SO through a secure channel and pinned to the SO endpoint. Certificates received during connection establishment must match this certificate.

Figure 13: Revocation and renewal of Customer Endpoint certificate

4.3.8. Decommissioning

When the lifetime of the physical Customer Endpoint is reached, it must be securely decommissioned. The customer must revoke all certificates that are configured on the Customer Endpoint and destroy all associated key material.

The Customer must have a process in place to securely dispose the device after it is taken out of use.

5. Architecture

This chapter describes the RTI's architecture using SGAM and elaborates on the applicable IEC 61850 logical nodes. SGAM is followed top-down: in order business layer, function layer, information layer, communication layer and component layer.

5.1. Business Layer

The Business Layer describes the different parties involved with the RTI and the curtailment of generators.

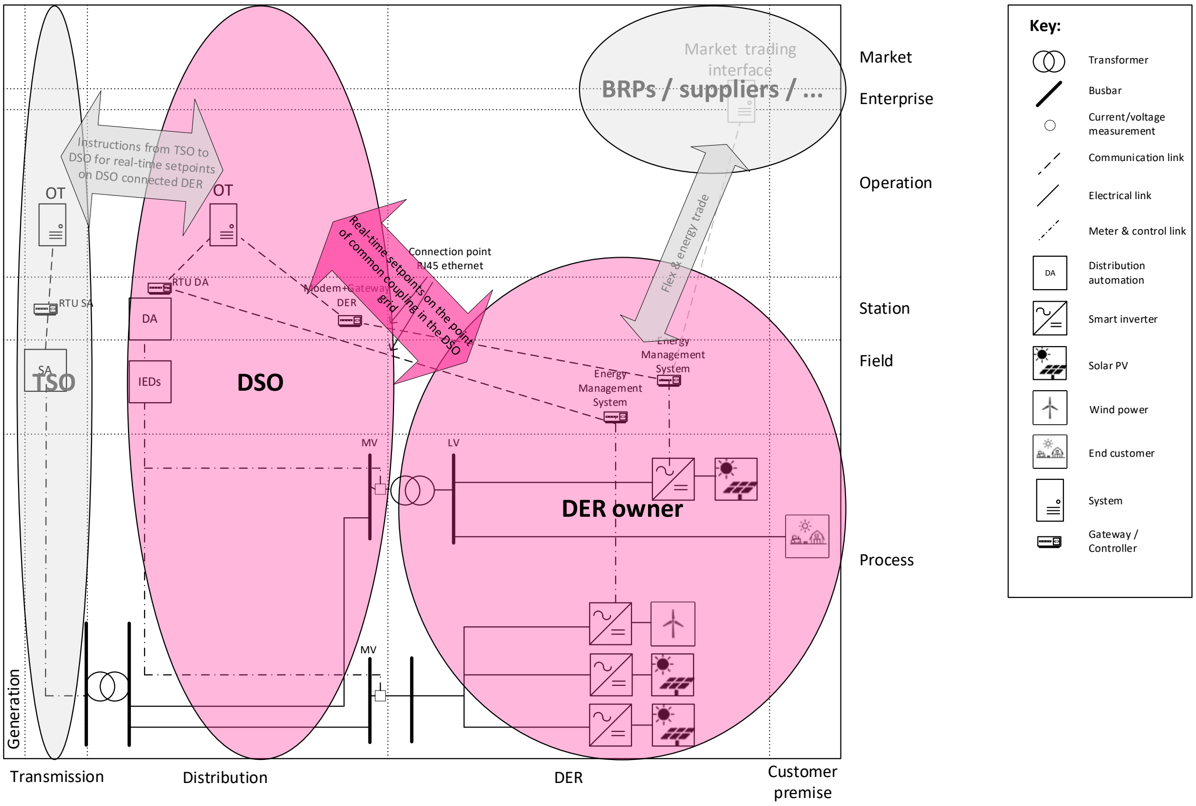


Figure 14: SGAM Business Layer RTI

5.2. Function Layer

The Function Layer describes the function and the interaction of the individual components concerned with the RTI.

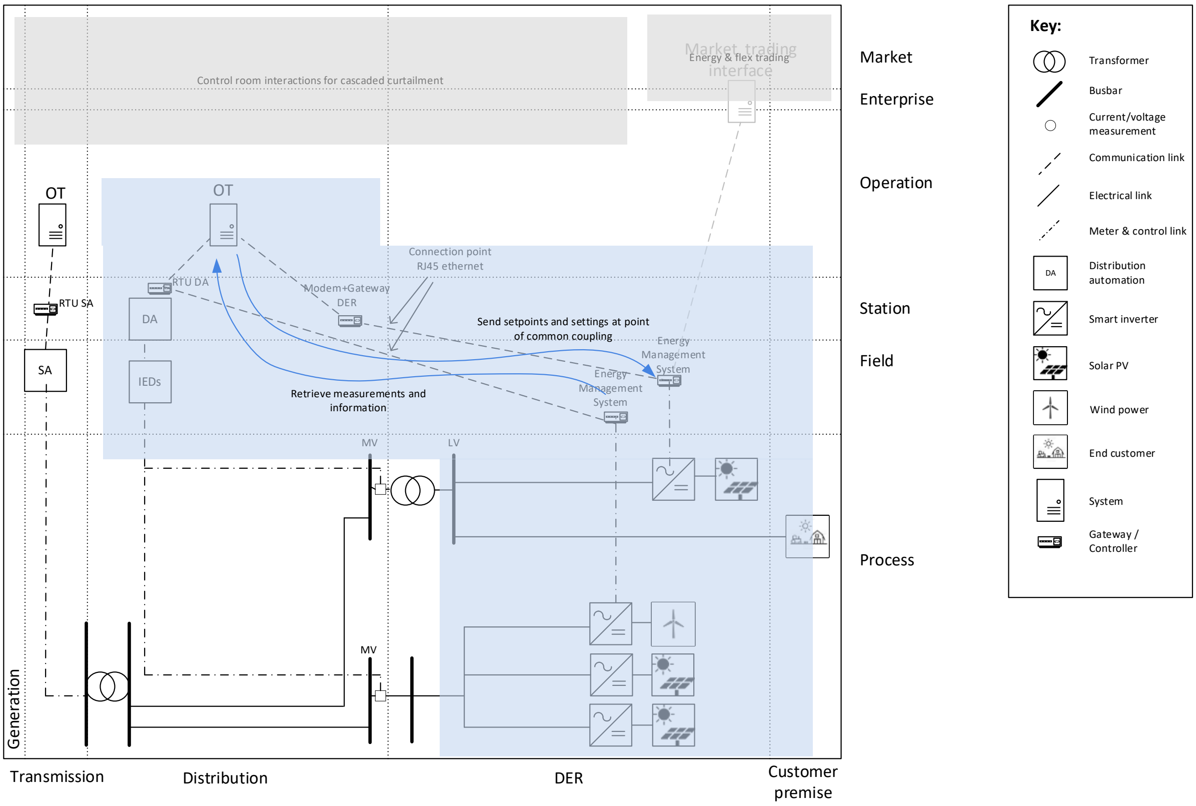


Figure 15: SGAM Function Layer with two different example implementations (blue lines) of the RTI

The Transmission- and Distribution System Operators (TSO & DSO respectively) are responsible for managing the power system. When they foresee that curtailment of a DER is necessary to ensure safe operation of the power system, they send a setpoint through the Realtime Interface towards the DER. When the TSO needs to restrict a Grid Connection Owner in the DSO's grid, the TSO will contact the respective DSO’s operations centre, to relay a curtailment request on behalf of the TSO.

The DER will limit the production of energy on the PoCC, based on the received setpoint of the DSO. The DER shall send measurement values related to the PoCC back towards the DSO.

A DER can also have a connection with market parties like Balance Responsible Parties or energy suppliers to facilitate (flex) energy trading. This function is out of scope of the RTI.

5.3. Information Layer

IEC 61850 is selected as the basis of the data model for the RTI. The signals that are exchanged on the RTI belong to a logical node that is described in the IEC 61850-7-4 Ed 2 and IEC 61850-7-420 Ed 2. The following chapter describes the logical nodes that are being used.

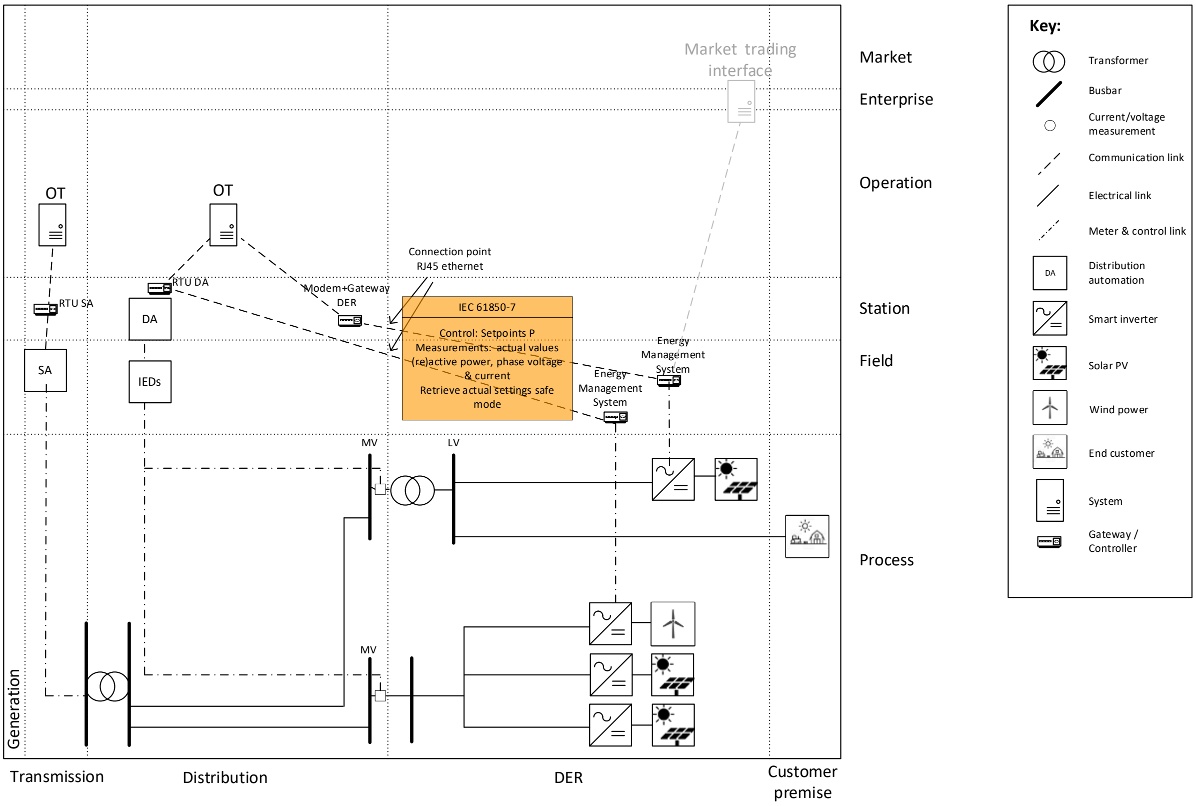


Figure 16: SGAM Information Layer

Note: only the main Data Objects (DOs), related to the core functionality of the Realtime Interface, are described in this chapter. The complete list of Data Objects is being described in the attached IEC 61850 Substation Configuration Language (SCL) file. The SCL file, which is based on the XML file format, hierarchically modelled, should be used for implementing the RTI on both System Operator and Customer Endpoints.

5.3.1. Physical device

5.3.1.1. LPHD: Physical device information

This logical node models common issues and information for physical devices. The selected Data Objects identify the physical devices at the Customer Endpoint and represent its current health status.

Data Object Name	Common Data Class	Explanation
PhyNam	DPL	Physical device name plate
PhyHealth	ENS	Physical device health
Proxy	SPS	Indicates if this LN is a proxy
PwrUp	SPS	Power-up detected

5.3.2. Logical device

5.3.2.1. LLN0: Logical node zero

This logical node models common issues and information for logical devices. The selected Data Objects identify the logical devices at the Customer Endpoint and represent its current health status.

Data Object Name	Common Data Class	Explanation
NamPlt	LPL	Name plate. The configRev attribute reflects the RTI version which is implemented, as required in [Customer-Configuraton-7]. The version shall be named using the following convention: ”major.minor.patch", i.e. RTI v1.1 shall be named as “1.1.0”. The swRev attribute shall reflect the firmware version of the Customer Endpoint and shall be updated in line with applied (security) patches and/or firmware
Beh	ENS	Behaviour
Health	ENS	Health

5.3.3. Logical nodes

5.3.3.1. DWMX: Limit Maximum Active Power operational function

This logical node shall be used to limit the maximum active power at the Grid Connection Owner side. If the setpoint value is negative, consumption (load) is limited. If the setpoint value is positive, the generation is limited. The active power can be given as a percentage or as an absolute value in MW. Percentage values are only supported to limit positive setpoints (limiting the generation). The System Operator shall be able to validate/get the current setpoint value at the Customer side.

Note that only one setpoint to limit the operational active power can be active. E.g. it is not possible to send a negative (limiting consumption) and positive (limiting generation) setpoint together.

The RTI foresees the possibility to receive a setpoint value for limiting the active power as a percentage or absolute value for the operational setpoints - [Setpoint-1], [Setpoint-2], [Setpoint-3] - and safe mode setpoints - [Safemode-2], [Safemode-3].

The Customer Endpoint should internally match the operational setpoints and safe mode setpoints in accordance to the following guidelines, to guarantee consistency in the operational data:

- In case a percentage setpoint is sent, the absolute setpoint is matched accordingly
- In case a positive absolute setpoint (limiting generation) is sent, the percentage setpoint is matched accordingly
- In case a negative absolute setpoint (limiting consumption) is sent, the percentage setpoint is set at 100% (no restriction on the generation side).

Data Objects related to Safe mode (see chapter 4.2.3) are derived from IEC 61850-7-420:2021 Annex F.4. Appendix IV is a RTI specific implementation example of the Safe mode. This Appendix shows that after the fallback time out (WMaxFto) the WMaxSpt(Pct).mxVal shall be set equal to the WMaxSet(Pct).setVal in the Customer Endpoint.

Data Object Name	Common Data Class	Explanation
WMaxSptPct	APC	Setpoint reflecting the maximum of active power as a percentage, as defined in [Setpoint-1]. Its mxVal attribute reflects the value of the setpoint that is requested. Note: The RTI only supports positive values of this Data Object (limiting generation).
WMaxSpt	APC	Setpoint reflecting the maximum limit of active power. Its mxVal attribute reflects the value of the setpoint that is requested. If the value is negative, power consumption is limited. If the value is positive, power generation is limited.
WMaxFto	ING	A fallback timeout delay after which the fallback behaviour should apply. The Customer Endpoint should fallback to WMaxSetPct or WMaxSet.
WMaxSetPct	ASG	Setpoint reflecting the maximum of active power as a percentage, as defined in [Safemode-3]. Its mxVal attribute reflects the value of the setpoint that is requested. Note: The RTI only supports positive values of this Data Object (limiting generation).
WMaxSet	ASG	Setpoint reflecting the maximum limit of active power when the Customer Endpoint is in safe mode. If the value is negative, power consumption is limited. If the value is positive, power generation is limited.
SptReas	INC	Integer which represents the reason for which use case a setpoint is sent by the System Operator

As described in requirement [Setpoint-8], only operational setpoints need a reason. Therefore, a reason code is only applicable to the following data objects: WMaxSpt and WMaxSptPct. Reasons are represented by a specific and unique integer value.

When a setpoint is being sent for the reason of frequency stability, the desired setpoint can only be reached by directly controlling the power generating modules. For this specific setpoint reason, it is not allowed to achieve the desired setpoint at the PoCC by increasing the consumption. For all other setpoint reasons, increasing consumption to reduce net generation on PoCC is allowed.

To properly link a reason to a specific setpoint, the following rules apply:

a) It is only allowed to send a setpoint with a reason.
b) It is not allowed to send multiple reasons applying to one setpoint.
c) Reason and setpoint are sent as separate messages.
d) The reason always has to be sent first.
e) The setpoint shall only be accepted if received within a time window of 10 seconds after receiving the reason.
f) If multiple reasons are received before receiving a setpoint, only the last received reason is valid. Previous reasons are disregarded.
g) A valid reason is an integer number in the range of 0000-9999. Any reason out of this range shall be disregarded.
h) A reason can only be used in combination with one setpoint: For a new setpoint, a new reason has to be sent first.

- Positive scenario: When a reason-setpoint combination complies with the rules specified in a) up to and including h), the setpoint shall be effectuated by the Customer Endpoint. This results in a change of the mxVal. See Appendix III.
- Negative scenario: When a reason-setpoint combination does not comply with the rules specified in a) up to and including h), the setpoint is disregarded by the Customer Endpoint. This does not result in a change of the mxVal. See Appendix III.

The explanation of the different reasons can be found on the Netbeheer Nederland website: www.netbeheernederland.nl/realtimeinterface

Appendix III shows different situations in figures.

☞ Note: Version 1.1 of the RTI only supports reasons for limiting active power.

5.3.3.2. MMXU: Measurement

This logical node shall define all the values that have to be measured on the PoCC. In line with the IEC 61850 standard conventions, a positive sign means that the DER unit is generating power. Measurements should be performed at the same voltage level as the utility meters of the metering company. For example: if the utility meters are measuring voltage on MV level, the voltage measurement values on the RTI should also be on MV. Instantaneous measurement values should be updated and shared with an interval of maximum 5 seconds.

Data Object Name	Common Data Class	Explanation
TotW	MV	Total active power (total P)
TotVAr	MV	Total reactive power (total Q)
PhV	WYE	Phase to ground voltages (VL1ER, …)
PPV	DEL	Phase to phase voltages (VL1VL2, …)
A	WYE	Phase currents (IL1, IL2, IL3)
AvWPhs	MV	Arithmetic average of the total active power (TotW) in MW value over a period of 15 minutes prior to the timestamp of the measurement
MaxWPhs	MV	Maximum magnitude of the total active power (TotW) in MW value over a period of 15 minutes prior to the timestamp of the measurement
MinWPhs	MV	Minimum magnitude of the total active power (TotW) in MW value over a period of 15 minutes prior to the timestamp of the measurement

The quality bits will be set to invalid if the measurements are not valid or non-existent, e.g. the connection to the measurement sensors is lost/broken or the connection to the measurement source is lost. The only allowed quality bit values are good and invalid.

5.3.3.3. DGEN: DER generating unit

This logical node describes the connected and operational state of the DER and should be implemented only once for the RTI.

Data Object Name	Common Data Class	Explanation
DEROpSt	ENS	Current state of operation of the distributed energy resource.

The following states (a subset of table 11 from IEC 61850-7-420:2021) are used in the context of the RTI as described:

Value	Meaning in RTI context
1	Initial state to define a starting status. Goal of defining this state is to enable observing state changes from this point on.
2	IEC 61850 communication between System Operator Endpoint and Customer Endpoint is established after an initial boot. Communication is available. This state is the trigger for the SO to send: • Reason • Setpoint • Safe Mode setpoint • Safe Mode time-out value
3	IEC 61850 communication between System Operator Endpoint and Customer Endpoint is established within a safe operating mode. Communication is available. This state is the trigger for the SO to send: • Reason • Setpoint
6	Full availability to comply with all possible operational setpoints.
10	IEC 61850 communication between System Operator Endpoint and Customer Endpoint is established after a reboot. Communication is available. This state is the trigger for the SO to send: • Reason • Setpoint
98	(Partial) unavailable. One or multiple connected DERs are unable to process the operational setpoints.

When communicating the DER state through the RTI, literals 4, 5, 7, 8 , 9, 11 are not used. The SO can send a control signal when receiving states 3, 6, 10 and 98. Note that the enumerated items, which corresponds with the Values, are described in the

SCL file conform the IEC 61850-7-420 standard. These enumerations do not correspond with the RTI specific context.

The introduction of these different states is a detailed implementation of the [Customer-Configuration-1] requirement. As a result, all users of the RTI have a common understanding of the current state of the Customer Endpoint. All changes of the state of the Customer Endpoint shall be reported using a data change trigger option.

Note that a state is defined on the PoCC, while the state of individual DERs may differ. Therefore, it is important to realize that the state on the PoCC might not represent the state of all individual DERs.

5.3.4. Common Data Classes

The following Common Data Classes (CDC) are supported on the RTI.

Common Data Class	Description
APC	Controllable Analogue Process Value
DEL	Phase to phase measured values for 3-phase system
DPL	Device name plate
ENS	Enumerated status
INC	Controllable integer status
ING	Integer status setting
INS	Integer status
LPL	Logical node name plate
MV	Measured Value
SPS	Single point status
WYE	Phase to ground measured values for 3-phase system

The CDCs are also described in a computer readable format, the attached IEC 61850 SCL file, see Appendix [B].

5.4. Communication Layer

IEC 61850 MMS is selected as the communication protocol for the RTI. More information about IEC 61850 can be found in chapter 2.3.

Chapter 3.3 and 3.4 describes the implementation requirements of mutual Transport Layer Security (mTLS) as defined in IEC 62351 series of standards.

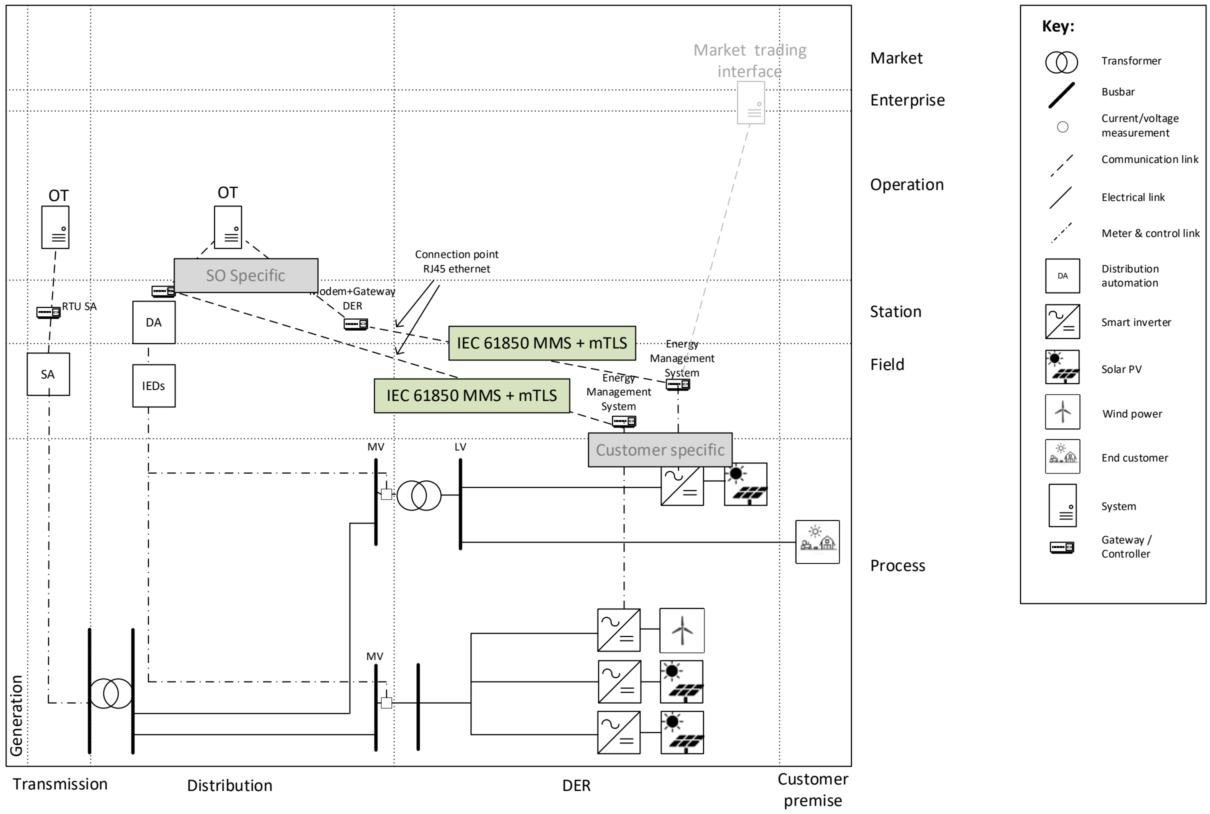


Figure 17: SGAM Communication Layer RTI

IEC 61850 MMS is only being used as protocol for the RTI between the System Operator Endpoint and the Customer Endpoint. The System Operator can specify its own protocol to communicate from the Endpoint towards its central operating systems and likewise, the Grid Connection Owner can specify its own protocol to communicate with the rest of the installation at the Grid Connection Owner's side of the PoCC.

The SO will provide the required TCP/IP connections information for setting up communication between the SO Endpoint and Customer Endpoint. The information will consist of IP-address, subnet configuration and IP-address gateway which needs to be configured on the Customer Endpoint. In case multiple gateway addresses are used the one provided by the SO will be prioritised.

5.5. Component Layer

The Component Layer describes the individual components concerned with the RTI.

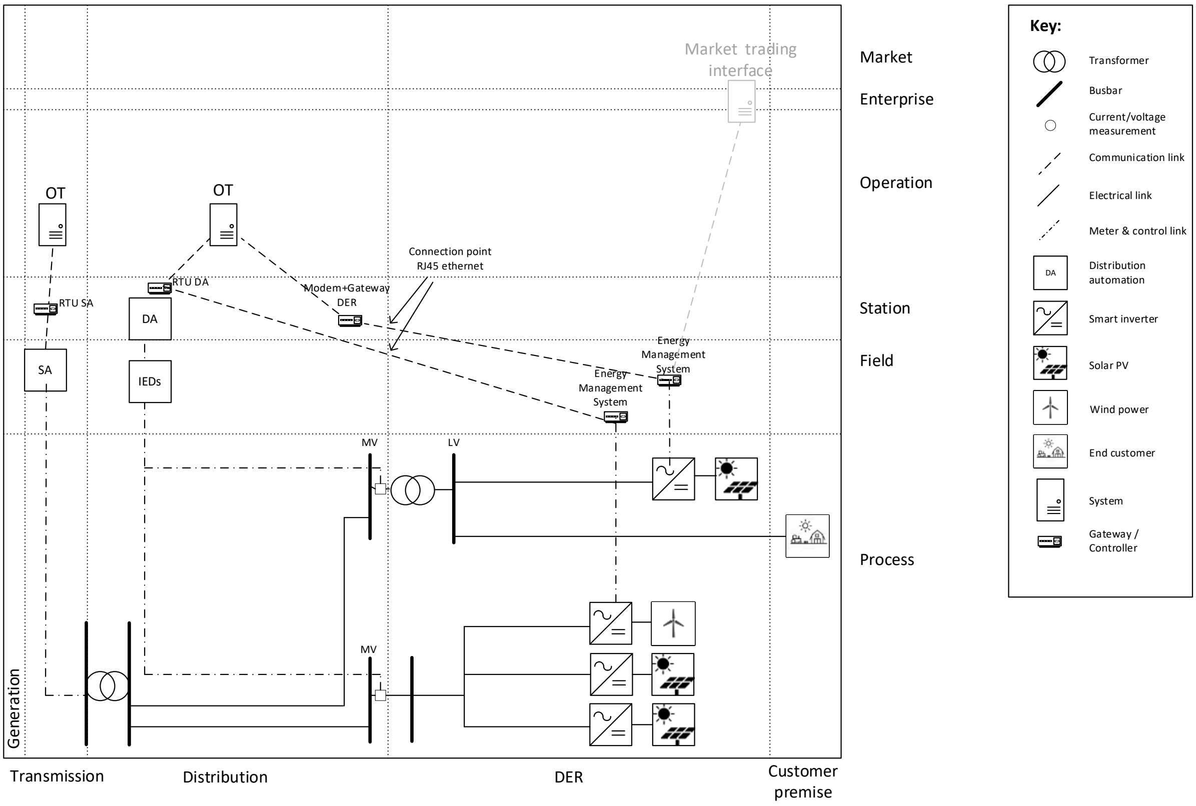


Figure 18: SGAM Component Layer with two different example implementations of the RTI

For version 1.0 of the RTI, the System Operator will place hardware in the MV compartment of the substation at the Customers premises, which is dedicated to the System Operator. The hardware contains an RJ-45 connector where the communication cable (connecting the System Operator Endpoint and Customer Endpoint) has to be connected. The RJ-45 connector at System Operator Endpoint forms the demarcation point between the equipment of the System Operator and the Grid Connection Owner. The Grid Connection Owner has to provide the communication cable between the two Endpoints.

In Figure 18, the System Operator's Endpoint or Remote Terminal Unit (RTU) is visualized in different ways, as different implementations are possible on the System Operator's side. The same applies for the Grid Connection Owner's side; the Endpoint can be implemented in a Park Controller, Energy Management system, a separate box or a different architecture. Two variants are visualized: communicating through the same RTU as is used for Distribution Automation (DA), or using a dedicated RTU.

6.Ownership demarcation

The ownership demarcation point is where the System Operator owned and maintained equipment ends and the Grid Connection Owner equipment (including Customer Endpoint) begins. The System Operator is responsible for maintaining and repairing equipment up to this ownership demarcation point.

The positioning document [POS_DOC] introduces demarcation points in the business, communication and power system domain (Figure 19). In the communication layer, the demarcation point of Realtime Interface version 1.1 is set at D2. The SO is responsible for communication up to this point, after which the responsibility is of the Connected Party.

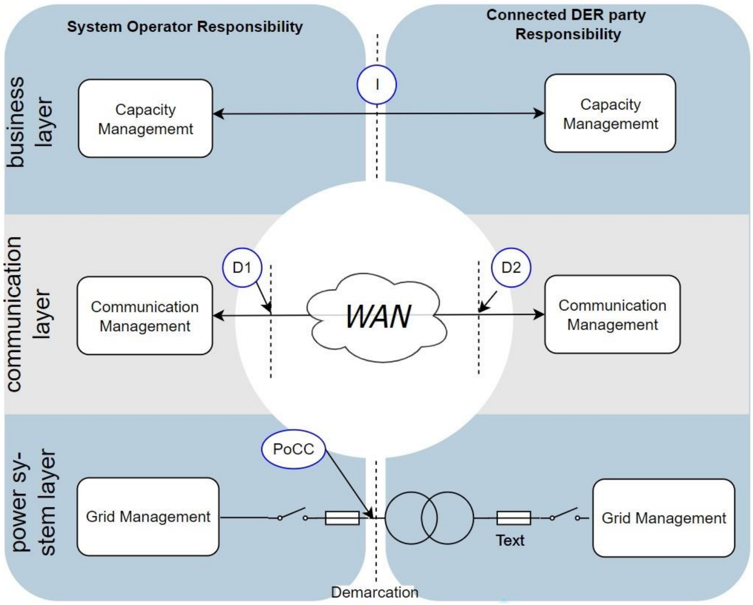


Figure 19: Abstract representation of demarcation points [POS_DOC]

Figure 20 illustrates an abstracted overview of the (relevant) physical components at a Grid Connection Owner's connection with the RTI, including a clarification of demarcation point D2. The colours explain the responsibilities. In general, it can be said that the Grid Connection Owner is responsible for the needed space and the connections. The dashed line represents the physical compartments of the SO and the Grid Connection Owner in the secondary substation. The Customer Endpoint can be located in the secondary substation, but can also be located outside the secondary substation. This is why the Customer Endpoint is visualised on the border of the secondary substation.

In practice, the Grid Connection Owner should provide space for the SO Endpoint, the RJ-45 connection to the SO Endpoint and a power supply for the SO Endpoint. Occasionally, it can be necessary for the SO to apply an external antenna. In that case additional modifications have to be made in the secondary substation.

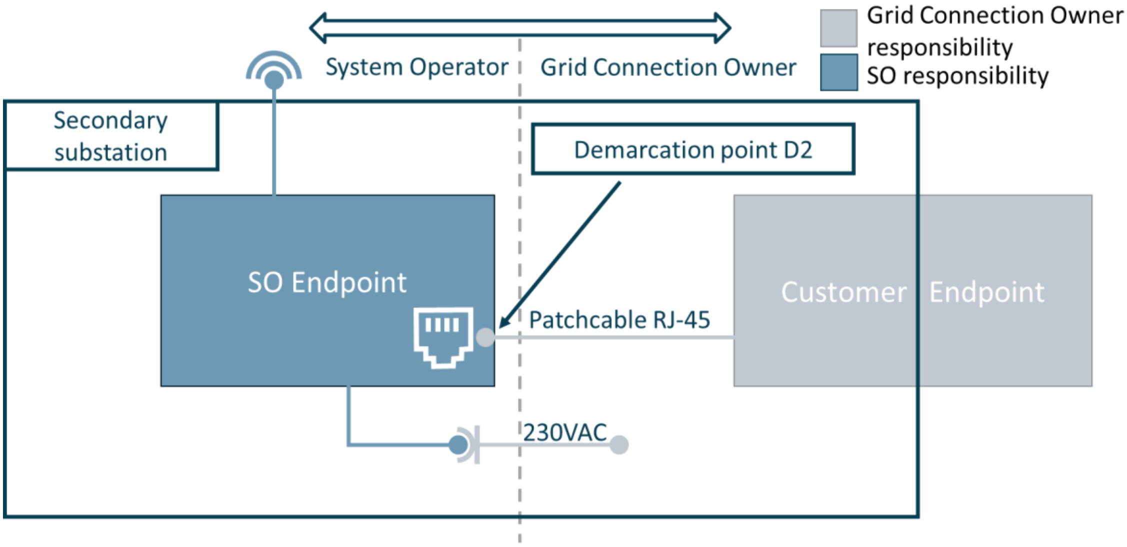


Figure 20: Ownership demarcation and responsibility overview

7. Implementation & compliance verification

The implementation of the RTI can slightly differ from one System Operator to another. The RTI itself is standardized but the physical appearance of the Endpoint and the application process can be different. Basically, it starts with the contract request of a Grid Connection Owner. The System Operator will decide if the RTI is applicable and under which conditions.

The first implementation of the RTI with a new product should be compliance tested before being applied. This has to be done via a product conformance test of the Protocol Implementation Document (PID) and IEC 62351. In addition, the System Operator can require a commissioning test. The compliance verification process is described in a separate document available at the following website: https://www.netbeheernederland.nl/dossiers/realtimeinterface.

Note that after a compliance verification certificate has been obtained, it may be necessary to follow the process again, when changes to the Customer Endpoint have been made that may influence the behaviour of the Endpoint on the RTI.

In case of a modification that impacts the Realtime Interface functionality, a retest should always be performed. An example of a change is a firmware or software update.

Appendix I Attachments

[A] IEC 61850 Protocol Implementation Document (PID) version 1.1

[B] IEC 61850 Data Model (SCL file) version 1.1

[C] Compliance Verification Document version 1.1

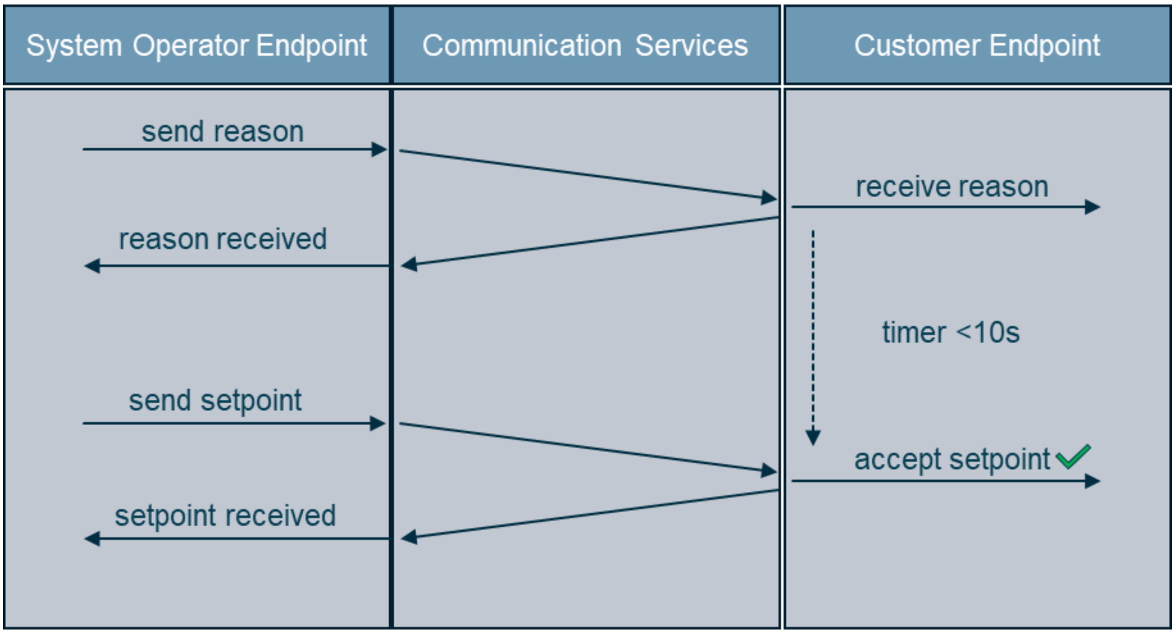
Appendix II Abbreviations

ACM	Autoriteit Consument en Markt
ATO	Aansluit- en Transportovereenkomst / Connection and Transportation Agreement
BRP	Balance Responsible Party
BSP	Balance Service Provider
CDC	Common Data Class
CRL	Certificate Revocation List
CSP	Congestion Service Provider
CSR	Certificate Signing Request
DA	Distribution Automation
DCC	Demand Connection Code (EU-Netwerkcode) Verordening (EU) 2016/1388
DER	Distributed Energy Resource
DMS	Distribution Management System
DO	Data Object
DSO	Distribution System Operator
ECP	Electric Connection Point
EMS	Energy Management System
ENCS	European Network for Cyber Security
EV	Electric Vehicle
GOPACS	Grid Operators Platform for Congestion Solutions
HVDC	High Voltage Direct Current
ID	Intraday
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
kVA	Kilo Volt-Ampère
kVAr	Kilo Volt-Ampère reactief
kW	Kilowatt
kWh	Kilowatthour
LV	Low Voltage
MMS	Manufacturing Message Specification
mTLS	Mutual Transport Layer Security
MV	Medium Voltage
MVA	Mega Volt-Ampère
MVAr	Mega Volt-Ampère reactief
MW	MegaWatt
NBNL	Netbeheer Nederland
OT	Operational Technology
PoCC	Point of Common Coupling
PGMD	Power Generating Module Document

PKI	Public Key Infrastructure
PID	Protocol Implementation Document
PV	Photovoltaic
RfG	Requirements for Generators (EU-Netwerkcode) Verordening (EU) 2016/631
RT	Real-time
RTI	Realtime Interface
RTU	Remote Terminal Unit
SA	Substation Automation
SCL	Substation Configuration Language
SGAM	Smart Grid Architectural Model
SO	System Operator
TLS	Transport Layer Security
TSO	Transmission System Operator
UTC	Coordinated Universal Time
XML	Extended Markup Language

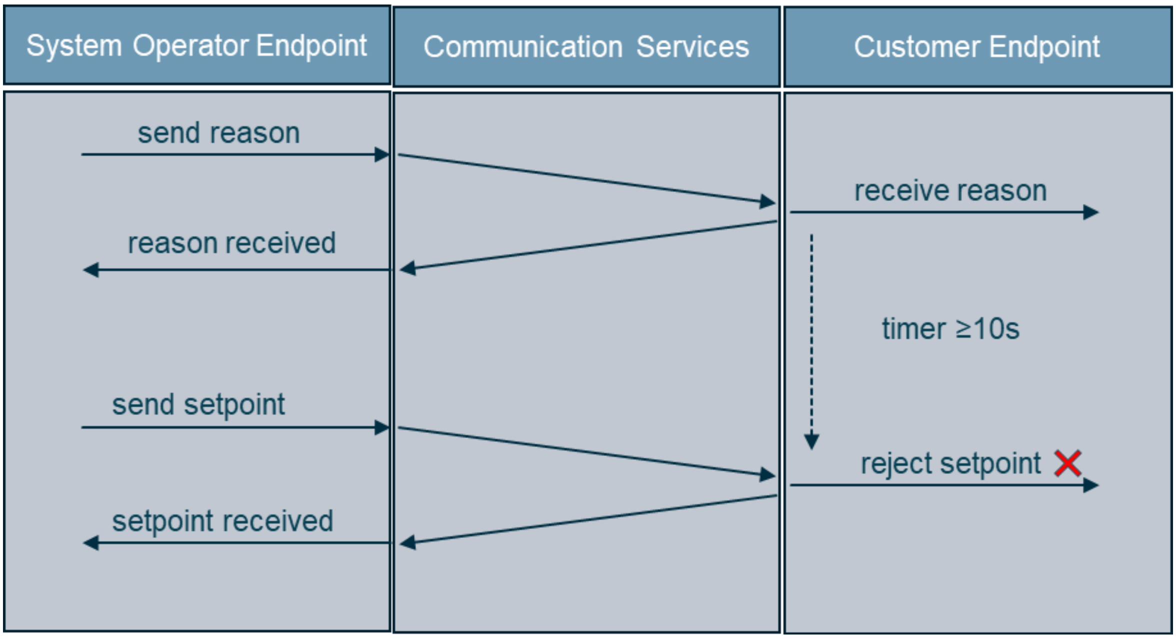
Appendix III Setpoint reasons

Scenario 1: Accept setpoint within the reason valid time.



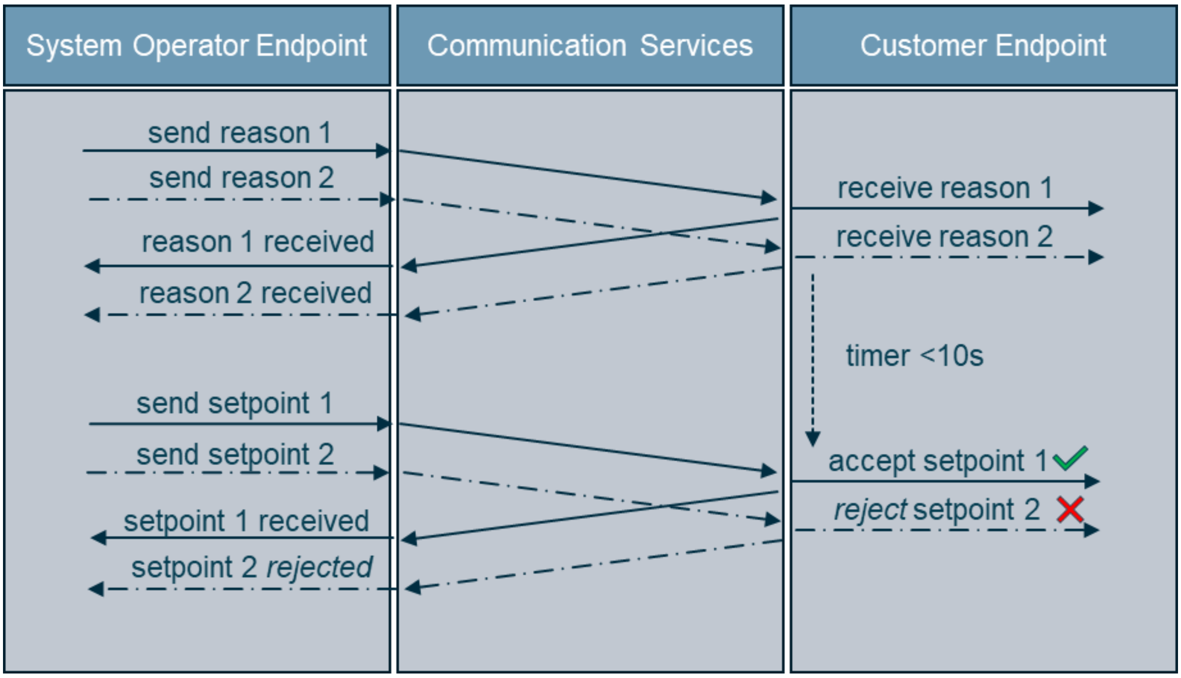
A valid reason is sent by the System Operator Endpoint and received by the Customer Endpoint. The Customer Endpoint also receives a valid setpoint within 10 seconds. The setpoint will be accepted by the Customer Endpoint.

Scenario 2: Exceeding the defined reason time window.



A valid reason is sent by the System Operator Endpoint and received by the Customer Endpoint. The Customer Endpoint also receives a valid setpoint after 10 seconds. The setpoint will be rejected by the Customer Endpoint.

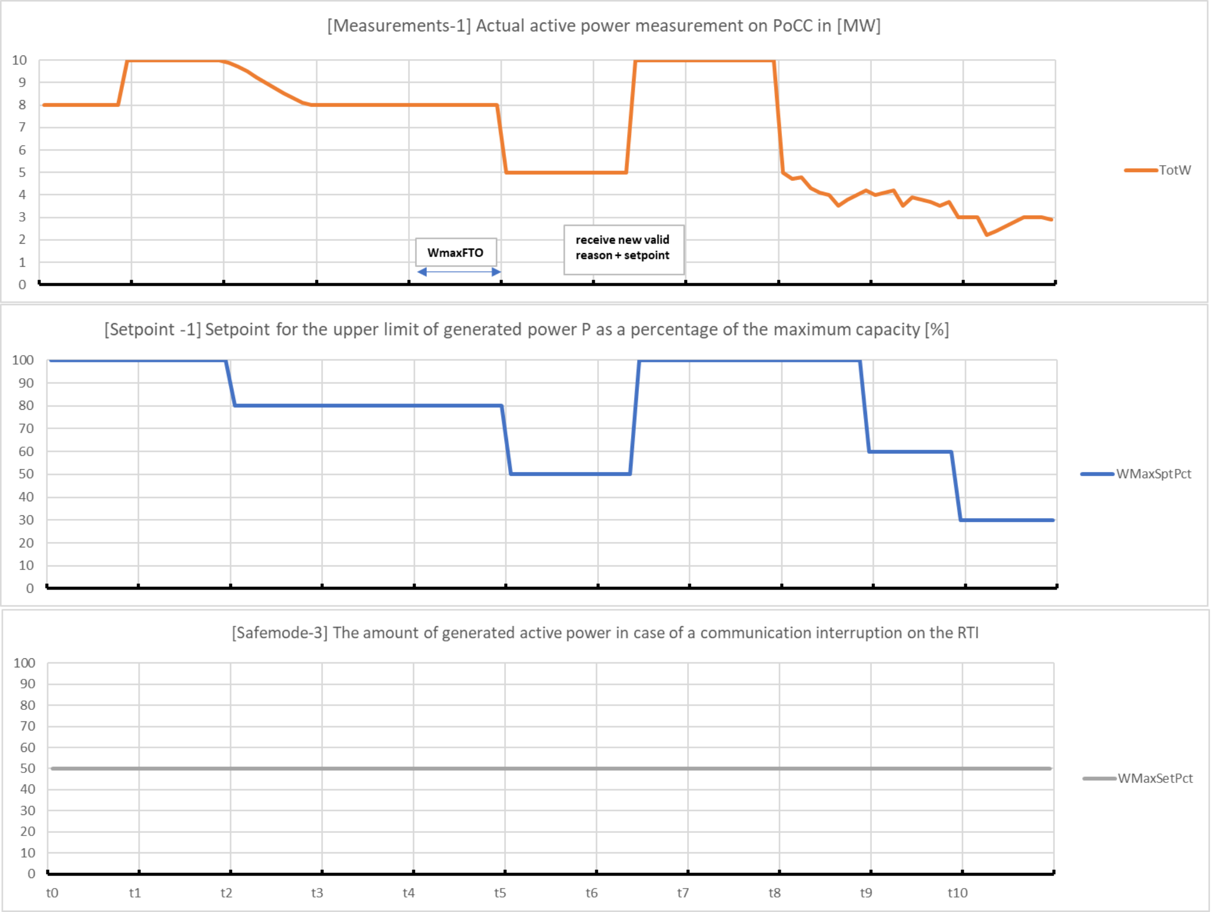
Scenario 3: Match setpoint with multiple received reasons.



Two valid reasons are sent by the System Operator Endpoint and received by the Customer Endpoint. The Customer Endpoint also receives two valid setpoints within 10 seconds. Reason 2 and setpoint 1 forms a valid combination and is accepted by the Customer Endpoint. Reason 1 is overwritten by reason 2, because reason 2 is received before a valid setpoint is received. Setpoint 2 is rejected because every setpoint has to be proceeded by an individual reason.

Appendix IV Customer Endpoint control example

In this appendix, an example is given to clarify the sequence of the expected behaviour of Customer Endpoint, based on signals specified in this technical specification.



[Measurements-1] Actual active power measurement on PoCC in [MW]

[Setpoint -1] Setpoint for the upper limit of generated power P as a percentage of the maximum capacity [%]

[Safemode-3] The amount of generated active power in case of a communication interruption on the RTI

Events at given time indicators:

t0-t1	Power change, no control
t2	Setpoint 80%; WMaxSptPct =80%; some time needed for DER to react (TotW)
t3	Setpoint reached
t4	RTI connection lost: WMaxFto (t5-t4) activate safemode
t5	Safe mode active, reduction to WMaxSptPct 50% After fall back time out the WMaxSpt(Pct).mxVal is the WMaxSet(Pct).setVal
t6	Connection restored after "Receive new valid setpoint + reason" go back to operational mode
t7	No control
t8	Production reduces
t9	Setpoint 60 %; WMaxSptPct = 60%; No effect on production power because actual power is lower than setpoint (TotW)
t10	Setpoint 30%; WMaxSptPct = 30%; Limitation possible (production power close to limiting setpoint)

Appendix V References

[ACM2021] ACM, “System Operators must use congestion management more often”, August 2021, https://www.acm.nl/en/publications/acm-system-operators-must-use-congestion-management-more-often

[CEN2012] CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids, “CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture,” 2012.

[DCC2016] ENTSO-E, “Demand Connection Code”, August 2016, https://www.entsoe.eu/network_codes/dcc/

[ENTSOE2020] ENTSO-E/EFET/ebIX, “The Harmonised Electricity Market Role Model (version 2020-01)”, 2020

[RfG2016] ENTSO-E, “Requirements for Generators”, April 2016, https://www.entsoe.eu/network_codes/rfg/

[CIRED2025] Paper 991: SECURING THE REALTIME DER INTERFACE FOR THE NETHERLANDS: KEY TAKEAWAYS FROM PROTECTING IEC 61850 MMS WITH IEC 62351

[POS_DOC] Document: *Positioning of the Dutch realtime-interface* https://www.netbeheernederland.nl/rti

Appendix VI Changelog

This section contains the main changes from the *previous version* of the specifications.

nr.	Document	Chapter/ Paragraph	Modification
138	SCL file version 1.0		1: Set DCHG to true for all data attributes in a data change report. 2: Gave configRev a value in the SCL. 3: Put units/ctlModel in the correct sequence for APC. 4: Removed LF energy reference 5: Added a BRCB to be able to store all changes to the DER operating state (DEROpSt) in case of communication loss. 6: Changed the name of the RCB's to clarify is they are buffered or unbuffered
139	Compliance Verification Plan version 1.0	Safe-Mode 5-6-7	Added an addition to test case "Safe-Mode 5-6-7", to verify that purging of the buffer is only done on a change of a data attribute value.
140	Technical specification version 1.0	4.1	Added a clarification on how fast instantaneous measurement values should be updated and shared.
141	Technical specification version 1.0	4.1	Added a clarification on which voltage level measurements should be performed.
142	Technical specification version 1.0 and Compliance Verification Plan version 1.0	4.1	Added clarification that the SO Operator should be able to request the IP address and other relevant parameters to be set in a specific range.
145	PID version 1.0	6.2 and 6.3	Changed number of minimal supported data sets and RCB to 4.
146	PID version 1.0 final and Compliance Verification Plan version 1.0		Removed references to deprecated requirement R.7
147	Technical specification version 1.0	4.1	Added clarification on how min, max, avg values should be calculated.
148	Technical specification version 1.0	2 & 6	RTI positioning document published; chapter 2 obsolete and removed from the specification. Chapter 6 updated. Reference made.
149	Technical specification version 1.0	2	Removed passages about the positioning of RTI within the eco-system. Positioning of the RTI is not related to a specific RTI version. A separate positioning paper will be published.
150	Technical specification version 1.0		IEC 62351 TLS requirements added
151	Compliance Verification Plan version 1.0		IEC 62351 TLS test cases added
152	PID version 1.0		IEC 62351 TLS requirements added
153	Technical specification version 1.1 beta1	3.3	Functional security requirements updated and clarified: TLS-CUSTOMER-STANDARDS-2 TLS-CUSTOMER-CIPHERS-3 TLS-CUSTOMER-CERT-3 TLS-CUSTOMER-CERT-4 TLS-CUSTOMER-MON-2 TLS-CUSTOMER-AUTH-4 TLS-CUSTOMER-CHAIN-1
154	Technical specification version 1.1 beta1		Several typos solved and pictures improved
155	Technical specification version 1.1 beta1	3.1	Requirement Measurement-3 is split into Measurement-7 and Measurement-8
156	Compliance Verification Plan version 1.1 beta1		Test scripts updated according to updated technical requirements

RealtimeInterface