IEC TR 61850-80-3

Edition 1.0 2015-11

TECHNICAL REPORT

colour inside

Communication networks and systems for power utility automation – Part 80-3: Mapping to web protocols – Requirements and technical choices

IEC TR 61850-80-3:2015-11(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TR 61850-80-3

Edition 1.0 2015-11

TECHNICAL REPORT

colour
inside

Communication networks and systems for power utility automation – Part 80-3: Mapping to web protocols – Requirements and technical choices

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200 ISBN 978-2-8322-2999-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 80-3: Mapping to web protocols – Requirements and technical choices

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 61850-80-3, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1584/DTR	57/1624/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61850 series, published under the general title *Communication networks and systems for power utility automation*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The usage of the IEC 61850 communication standard is largely spreading over all the domains connected to the smart grid, pushing the usage of technologies adapted to the connection of a very large number of applications and devices across the intra/internet (see related use cases in Annex A). The involved domains typically use already well-established protocols for exchanging data with IT level applications like resource planning, asset and maintenance management, etc. Therefore, it becomes imperative to provide an integration strategy that allows the integration of IEC 61850 into these various disparate protocols and information.

In this context, Web Protocols are considered the most appropriate technology for communication with backend systems and possibly field devices.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 80-3: Mapping to web protocols – Requirements and technical choices

1 Scope

This part of IEC 61850, which is a technical report, describes the requirements and gives an overview of the technical solution for using Web Protocols as a new communication mapping (SCSM) for the IEC 61850 standard.

NOTE The notion of Web Protocols covers here the Web Services technologies, extended by other well deployed technologies based on standards used in the IT domain (IETF, ISO, W3C, OASIS, etc.). The advantage is that due to a lot of professional knowledge and practical experiences in the IT world the risk of non-interoperable solutions in the smart grid domain will decrease.

The structure of this part of IEC 61850 illustrates a two-step approach:

- Collection of the use cases and requirements based upon emerging Smart Grid architectural considerations, taking into account the new extended scope of IEC 61850. Clause 6 proposes a synthesis of the global requirements, while the use cases of the various domains are described in Annex A. The considered domains are:
  - PV-inverters
  - Hydro and thermal generation
  - Wind power plants
  - Combined Heat and Power (CHP)
  - Smart customers
  - E-Mobility
  - Virtual Power Plants (VPP) and micro grids
  - Feeder automation
- Evaluation and selection of technologies in order to build a consistent SCSM. Clause 7 presents the future SCSM 8-2, including an overview of the main selected technology: XMPP. The following goals have been particularly considered for the definition of this SCSM:
  - Identify a single profile supporting all the services required by the domains and defined today in ACSI.
  - Cover the full life cycle of a IEC 61850 system, in collaboration with the System Management work in WG10 (from configuration, through conformance testing, down to maintenance). For this purpose, this part of IEC 61850 may recommend some changes to other parts of the IEC 61850 series such as Parts 6 and 10, etc.
  - Deploy cyber-security to ensure a secure environment (in compliance with the IEC 62351 series).
  - Propose rules for cohabitation with other mappings such as IEC 61850-8-1 and IEC 61850-9-2, and possibly recommend communication profiles depending on specific application context (pole-top equipment, inside DER, connection of DER, etc.).
  - Only the A-Profile is addressed here. Nevertheless, support of TCP/IP and UDP/IP is required for the T-Profiles.

What is not included in the study:

- Modification of objects specified in IEC 61850-7-3 and IEC 61850-7-4
- Introduction of several competing web protocols profiles

The namespace of this document is: “(Tr)IEC 61850-80-3:2015”

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-5, *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models*

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-7-4, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-8-1:2011, *Communication networks and systems for power utility automation – 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 62351 (all parts), *Power systems management and associated information exchange – Data and communications security*

ISO 9506 (all parts), *Industrial automation systems – Manufacturing Message Specification*

ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN. 1): Specification of basic notation*

ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 8825-4:2008, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

RFC 4330, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, IETF, available at http://www.ietf.org*

RFC 6120, *Extensible Messaging and Presence Protocol (XMPP): Core*

RFC 6121, *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*

RFC 6122, *Extensible Messaging and Presence Protocol (XMPP): Address Format*

XEP-0198, Stream Management[1]

XEP-0199, XMPP Ping[2]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
electrical connection point
ECP
point of electrical connection between the DER source of energy (generation or storage) and any electric power system (EPS)

Note 1 to entry: Each DER (generation or storage) unit has an ECP connecting it to its local power system; groups of DER units have an ECP where they interconnect to the power system at a specific site or plant; a group of DER units plus local loads have an ECP where they are interconnected to the utility power system.

Note 2 to entry: For those ECPs between a utility EPS and a plant or site EPS, this point is identical to the point of common coupling (PCC) in IEEE 1547, *Standard for Interconnecting Distributed Resources with Electric Power Systems*.

3.2
electric power system
EPS
all installations and plant provided for the purpose of generating, transmitting and distributing electricity; particular installations, substations, lines or cables for the transmission and distribution of electricity

[SOURCE: IEC 60050-601:1985, 601-01-01, 601-01-02, modified (removal of Note to entry)]

3.3
electrical network
grid
particular installations, substations, lines or cables for the transmission and distribution of electricity

Note 1 to entry: IEC 61850 also uses the following terms:

Utility Grid or Utility electrical network – this corresponds to the area EPS as defined in IEEE.

Facility Grid or Facility electrical network – this corresponds to the local EPS as defined in IEEE.

[SOURCE: IEC 60050-601:1985, 601-01-02, modified (modification of Note 1 to entry)]

3.4
point of common coupling
PCC
ECP between a utility electrical network and facility electrical network

Note 1 to entry: ECP and PCC are related to the physical connectivity of the electrical network only and are independent from application functions.

Note 2 to entry: Other terms used are POC, PUC and PGC with sometimes similar meanings. These are not further considered within IEC 61850, since ECP and PCC are sufficient.

[1] This specification defines an XMPP protocol extension for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption.

[2] This specification defines an XMPP protocol extension for sending application-level pings over XML streams. Such pings can be sent from a client to a server, from one server to another, or end-to-end.

3.5
private network
network used by a unique entity mastering all the data flows, the performance seen by which is guaranteed in terms of bandwidth, throughput, transmission delay, availability, etc.

Note 1 to entry: A private network may be based on a public or shared infrastructure, as soon as the level of services can be guaranteed.

3.6
public network
network not used by a unique entity mastering all the data flows or if the performance seen by the entity using the network is not guaranteed in terms of bandwidth, throughput, transmission delay, availability, etc.

3.7
smart grid
electric power system which uses communication networks for coordinating the actions of the generators and consumers connected to it in order to efficiently deliver sustainable, economic and secure electricity supplies

4 Abbreviated terms

CHP	Combined heat and power
DDEMS	DSO DER Energy Management System
DER	Distributed Energy Resource
DMS	Distribution Management System
DR	Demand Response
DSO	Distribution system operator
ECP	Electrical Connection Point
ENTSO-E	European network of transmission system operators for electricity
EPS	Electric Power System
PCC	Point of Common Coupling
SO	System operator
TSO	Transmission system operator
VPP	Virtual power plant
WAN	Wide Area Network

5 Main involved sub-systems and stakeholders

Figure 1 presents an overview of the main involved sub-systems and indicates for which interactions the new IEC 61850-8-2 web protocols mapping is intended. The sub-systems mentioned in the picture are then described in Table 1 together with other systems and stakeholders considered in this document.

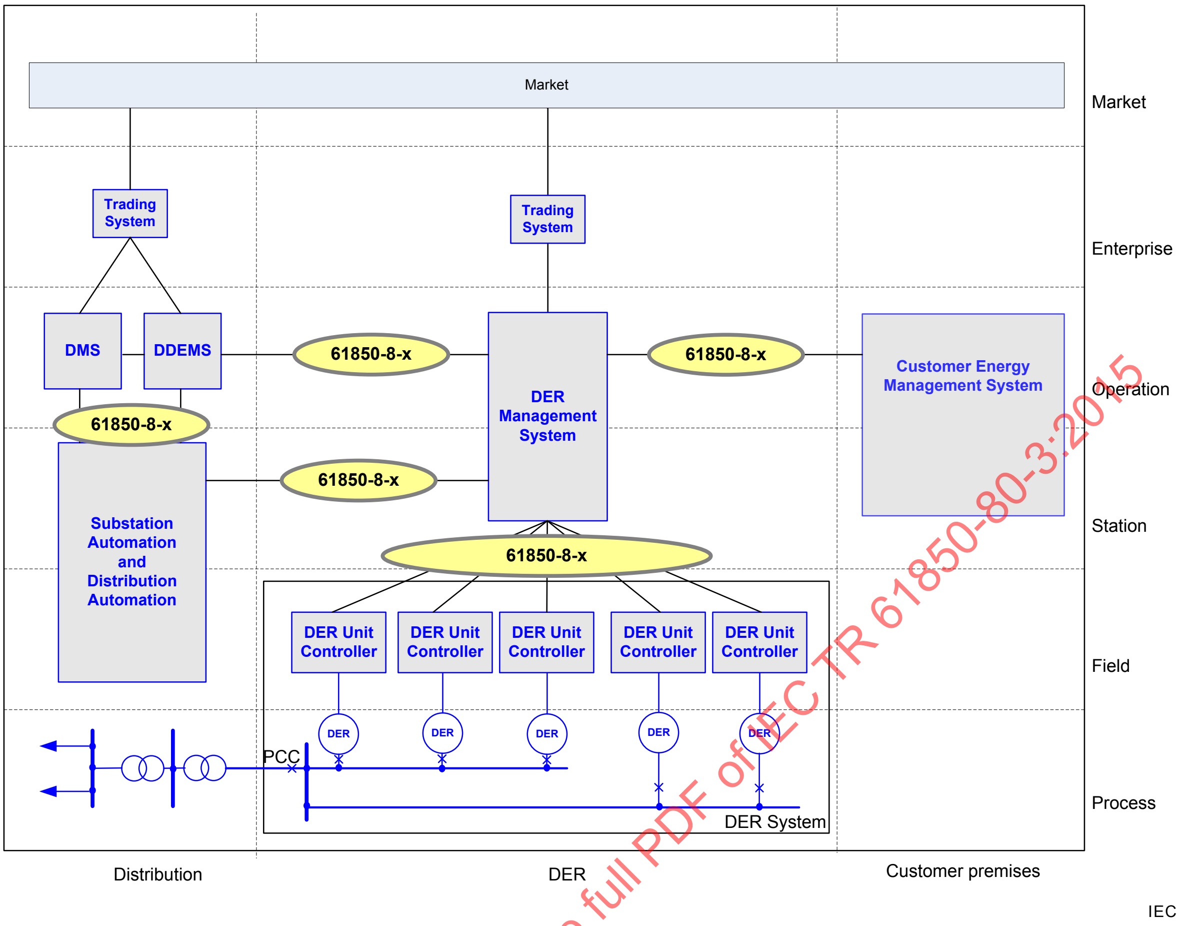


Figure 1 – Architecture overview

Table 1 – Main involved sub-systems and stakeholders

Type	Name	Description
Role	**Aggregator**	Offers services to aggregate energy production, storage capability and energy consumption. Acts towards the grid as one entity, including local aggregation of demand (Demand Response management) and supply (generation management). In cases where the aggregator is not a supplier, it maintains a contract with the supplier
Role	**Balance responsible party**	A party that has a contract proving financial security and identifying balance responsibility with the imbalance settlement responsible of the market balance area entitling the party to operate in the market. This is the only role allowing a party to buy or sell energy on a wholesale level
System	**DER unit controller**	Local controller for the DER unit. May control several DER local servers
System	**DER local server**	A processing unit interacting directly with the DER process by using proprietary communications means. Act as a communication server for the higher level systems
System	**DER management system**	Control Center of the VPP or Microgrid, used for monitoring and controlling the various sub-systems that are registered as participant in the VPP. Provides ancillary and balancing services to DSO
Role	**DER operator**	Any natural or legal person operating a DER plant (often this is either the plant owner or the DSO)
Role	**DER owner**	Any natural or legal entity owning a power generating facility like e.g. CHP plants, Wind power plants, PV plants
Role	**DER manufacturer**	Entity in charge of designing, producing and selling DER Units. May be also in charge of the maintenance
System	**DER unit**	One or several devices at process level that are controlled by the same system at field level. All included devices have the same type (e.g. PV) and can be for generation purpose as well as for storage

Type	Name	Description
Role	**DSO**	According to the Article 2.6 of the Electricity Directive 2009/72/EC: "a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity". Moreover, the DSO is responsible for regional grid access and grid stability, integration of renewables at the distribution level and regional load balancing
Role	**Energy retailer**	Entity selling electrical energy to consumers – could also be a grid user who has a grid connection and access contract with the TSO or DSO. In addition, multiple combinations of different grid user groups (e.g. those grid users that do both consume and produce electricity) exist
Role	**Market operator**	The unique power exchange of trades for the actual delivery of energy that receives the bids from the Balance Responsible Parties that have a contract to bid. The market operator determines the market energy price for the market balance area after applying technical constraints from the system operator. It may also establish the price for the reconciliation within a metering grid area
Role	**Meter operator**	A party responsible for installing, maintaining, testing, certifying and decommissioning physical meters
Role	**Plant maintenance**	Facility or service provider that monitors equipment in DER plants of one or more companies and dispatches maintainers if needed
Role	**Smart customer**	Industry sites, buildings or homes that contribute to and profit from demand response. May be consumers and / or producers of electrical energy
System	**Trading system**	A System with application(s) which are used to trade energy in corresponding markets, supports the dispatch in the decision to buy, sell or to self-produce energy and also provides facilities to exchange the necessary information with the Energy Market Platform.
Role	**TSO**	According to Article 2.4 of the Electricity Directive 2009/72/EC: "a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity". Moreover, the TSO is responsible for connection of all grid users at the transmission level and connection of the DSOs within the TSO control area
Role	**VPP/Microgrid operator**	Any natural or legal person responsible for aggregating DERs to Virtual Power Plants

6 Requirements description

6.1 General

This clause describes the requirements used during the process for selecting a technical solution.

The first fourteen requirements (6.3.1 to 6.3.14) have been analyzed domain by domain, so that what is presented here is a synthesis of a detailed analysis of each domain.

The last five requirements (6.3.15 to 6.3.19) are general requirements relevant for rating technical solutions but which do not depend especially on the considered domains.

6.2 Scope of this clause

6.2.1 ACSI classes to be mapped

The usage of the various ACSI classes defined in IEC 61850-7-2 has been studied for each domain. The synthesis presented in Table A.14 shows that all the classes using the client/server model need to be mapped, as well as the configuration services for the classes using a peer-to-peer model (i.e. GOOSE and SMV).

Regarding the peer-to-peer model, the requirements expressed in Table A.15 for peer-to-peer messages in terms of transfer time is currently not compliant with the performances expected from web protocols. When required for a specific use case, an existing mapping like the one defined for example in IEC 61850-90-5 may be used. Nevertheless, usage of web protocols for implementing one-to-many interactions, even with lower performances, may be studied in the future.

6.2.2 Network type

The analysis of the different use cases listed in Annex A has shown that for most domains, the communication infrastructure may be either private or public networks (see definitions for private/public networks in 3.5 and 3.6). This is an important driver for the choice of the technical solution, in particular because the proposed cyber-security mechanisms will have to comply with the communication over public networks.

6.3 Requirements list

6.3.1 Transfer time

The transfer time is defined as the overall transfer time from application to application including the coding at the sender side, the delay in the communication network and the decoding at the receiver side (see complete description in IEC 61850-5).

For the client /server services considered here, the required transfer time may vary from some seconds to a minimum of 100 ms (see Table A.15).

6.3.2 Throughput

This requirement describes the most demanding scenario in terms of data transfer. A scenario coming from the VPP domain and involving a high number of DERs is probably the most relevant to establish such a throughput requirement. A first assessment is a system with around 100 000 connection points exchanging 1 to 5 kbytes messages every 5 minutes with a transfer time of 1 to 3 seconds.

6.3.3 Data integrity (error probability)

Usual requirements like in the substation automation domain (see IEC 61850-5).

Data integrity means here that the transmission errors shall remain below an acceptable limit for a given background noise. It is then slightly different from the Integrity requirement generally mentioned in a cyber-security context. Only errors that really flow up to the application level and that cannot be recovered shall be taken into account.

6.3.4 Reliability

Usual requirements like in the substation automation domain (see IEC 61850-5).

This requirement is twofold. The Security criteria express the probability for an IED to receive an unwanted command while the Dependability criteria express the probability that a command normally required in a given context may be missing.

These criteria are described in IEC 61850-5. For each of them several classes of IEDs are defined depending on the kind of application.

6.3.5 Availability

The selected communication technology shall support network redundancy as well as device redundancy:

- Network redundancy means here that there should be no single point of failure all along the communication path between two communicating entities.

- Device redundancy can be rather managed at the applicative level, so that there should be no constraint on the communication technology.

In any case, the maximum recovery delay is around 5 minutes.

6.3.6 Interoperability

Interoperability between systems and IEDs implementing the new web protocol communication mapping is a general and obvious requirement. It is expected additionally that:

- Future extensions will not break the communication with older implementations of the same communication mapping.
- The same IED or system should be able to simultaneously host the new web protocol mapping and other already defined communication mappings. This may apply to client and server applications, as well as to gateways making a bridge between several kinds of mappings.

6.3.7 Cyber security

The technical solution shall comply with the following requirements, which include both general security requirements as well as more detailed technical requirements. The applicable standard for cyber-security in this domain is IEC 62351. Each time this is relevant, the requirements below refer to this standard:

- Support of end-to-end security
- Require confidentiality, integrity, availability and non-repudiation
  – In particular, communications over the internet shall be encrypted
- Support secure connections with TLS, insuring data integrity, authentication and confidentiality between two entities directly connected through TLS, as defined in IEC 62351-3
- Devices or controllers shall support a role based security model which defines access down to parameter or message type level
  – Support authorization with an access token at application layer level as defined in IEC 62351-8
- Shall be compliant with a key management as defined in IEC 62351-9, in particular:
  – Devices shall be configured with credentials that enable them to make authenticated and encrypted connections to a trusted communication infrastructure
  – There shall be a mechanism to update credentials, e.g. certificate revocation
- Devices will only make outbound transport level connections to the communication infrastructure using their credentials
- Devices or controllers shall be capable to simultaneously hold multiple connections to different communication partners with different trust levels. For example, Figure 2 presents an architecture where DER System or Unit Controllers must interact with several network domains, potentially with different trust levels

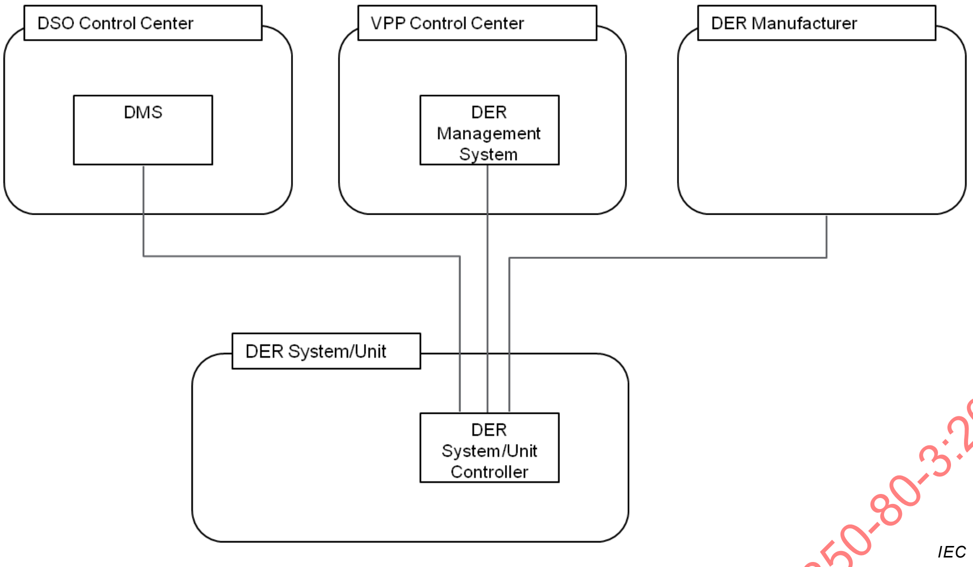


Figure 2 – Device communicating with different trust levels

6.3.8 Device size

Device size is not considered as a limiting factor. The functionality is the more important and the device size should be designed accordingly.

6.3.9 Dynamic extension of the system

After initial commissioning a system evolves all along its life-cycle. The changes may be limited to the upgrade of some components or may include the addition of complete sub-systems. Some communication technologies cannot support easily such extensions, some others are really done for that by providing for example auto discovery features for devices and data.

Dynamic extension of the system is required in particular for the scenarios involving a high number of DER, where registration and discovery functions are required.

6.3.10 Sensitivity to cost of bandwidth

The communication mapping may be used over pay per volume connections (e.g. GPRS) so that the size of the message is an important factor because it has an impact on the overall costs. For this reason, protocols using a more compact encoding or a smaller message structure for the same information will be preferred.

6.3.11 Availability of commercial and open source tools

Some technologies are already well deployed while others are just emerging. The existing tools for these technologies may be also open source or commercial.

These tools may include:

- Protocols used by the technical solution: implementations of the main components of the technical solutions (e.g. WS-* specifications)
- Simulators: client side or server side simulators to validate the interoperability
- Protocol analyzer used to analyze the protocol stack on the Ethernet link

The availability of such tools is in general not a critical requirement. Depending on the domains and the size of the plants, commercial or open source implementations are preferred.

6.3.12 Intellectual property

Any IP restriction related to the communication technology is strictly not acceptable.

6.3.13 Perenniality / Stability of the solution

This criterion means that the domain is sensitive to frequent evolutions of the technical solution.

Evolutions may be linked in particular to the number of standardization bodies involved, and the associated management rules.

There is a strong need for a long-term stable solution, since the typical system lifetime is 20 years and longer.

6.3.14 Request for additional resources and engineering

This criterion means that the cost of the communication solution is an important aspect that might be crucial for the decision of using IEC 61850 for DERs. For this requirement, the point of view of an end user or an installer using the products for building a system like for example a DER plant is considered.

The usage of well known IT technologies is considered as a factor that would limit this cost.

This requirement is particularly important for small plants.

6.3.15 Simplicity and easy implementation of the communication solution

This requirement concerns more the development of the communication technology. However simplicity and easy implementation of the SCSM are also important criteria for customers when deciding to use it for their DERs, because complexity may affect the communication solution in many of its aspects: usability, efficiency, reusability, maintainability, portability and testability.

6.3.16 Ability to become a SCSM / Difficulty in filling the gap

The technologies used for the SCSM shall support the following features:

- Ability to map ACSI services and behaviour, as they are defined in IEC 61850-7-2
- Support the solicited message exchange pattern
- Support the unsolicited message exchange pattern
- Support of basic data types (e.g. support of new CDC without changing the SCSM specification)
- Support for structured data model (e.g. support of mandatory/optional/extended components like DO of LNs)
- Ability to express unambiguously and completely the semantic contained in IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-4xx

6.3.17 One single solution for all smart grid applications

The selected technologies shall be compliant with the other standards applicable for the smart grid, either existing or in progress within the IEC.

6.3.18 Products' time-to-market

The ability to design products and make them available on the market as soon as possible is an important factor for the success of the new SCSM.

6.3.19 Minimize standardization effort

All the technical solutions are not equivalent concerning the effort required to achieve a complete standardization. This includes not only the international standard describing the SCSM but also other aspects, for example compliance testing.

This effort depends mainly on the complexity of the technical solution and whether it is based or not on already standardized technologies which can be referred to.

7 SCSM technical description

7.1 Technology assessment and choice

Six different technologies have been evaluated as possible candidates for the web protocol mapping:

- IEC 62541 (OPC UA)
- IEC 61400-25-4:2008, Annex A (Web services profile for wind power)
- DPWS (Devices Profile for Web Services)
- RESTful Web Services
- XML messaging over Websocket
- XMPP (Extensible Messaging and Presence Protocol)

Among these six candidates XMPP has been selected in particular because it provides the following key benefits. Note that these advantages are also true compared to the SCSM 8-1:

- Cyber-security: XMPP enables devices to make only outbound connections (with additionally a well-known port) to the communication infrastructure, thus limiting the burden and the risk to configure the fire-walls on device side and allowing these devices to be hidden behind a NAT. The core specifications of XMPP include standard security mechanisms like TLS or SASL, supporting a large number of use cases.
- IPv6: XMPP supports a progressive transition to IPv6, as IEC 61850 applications using IPv4 and other ones using IPv6 may interoperate provided that they are connected to an XMPP server presenting dual interfaces IPv4 and IPv6.
- Presence monitoring brings new opportunities for managing scenarios where the integration of DER is dynamic or where communications are intermittent.
- Convergence with smart grid standards, while XMPP is used by other standards, either existing or in progress (e.g. IEC 62746-10-1).

Then, for defining the XML messages transported over XMPP, the usage of the MMS / XER encoding described below has been preferred to a solution using a custom XML schema, establishing a one-to-one correspondence between the request/response parameters as described by IEC 61850-7-2 and the XML payload (with this second solution, the XML payload is similar to the body of the SOAP messages defined by IEC 61400-25-4:2008, Annex A).

The MMS / XER encoding will benefit in particular of a strong synergy with the existing IEC 61850-8-1 mapping, both for the standardization work and for the development of products, leading to an optimized time-to-market (see 7.8).

Figure 3 illustrates the three main choices on which the SCSM is built:

- Choice of MMS XER for the definition of the XML payloads
- Choice of XMPP as a transport technology, allowing the transport of these XML payloads

- Choice of cyber-security technologies: XMPP already provides some security features. Additionally in order to ensure end-to-end security the MMS secure session mechanism defined in next version of IEC 62351-4 will be used (see 7.6).

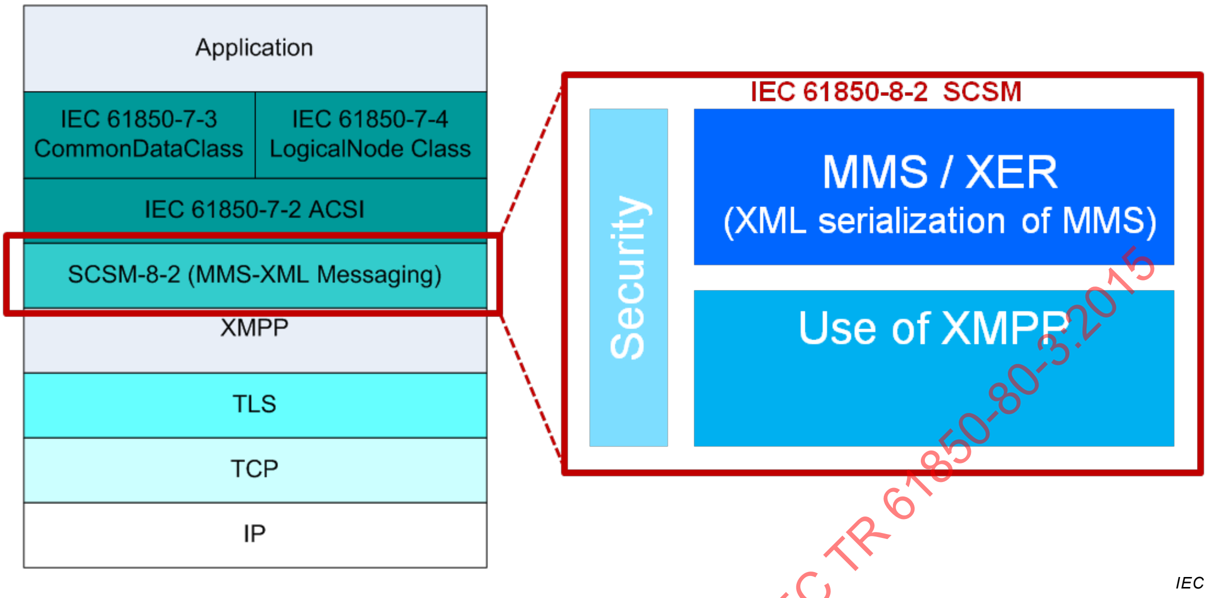

Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
SCSM-8-2 (MMS-XML Messaging)
XMPP
TLS
TCP
IP
IEC 61850-8-2 SCSM
Security
MMS / XER
(XML serialization of MMS)
Use of XMPP
IEC

Figure 3 – Architecture main choices

7.2 XMPP overview

7.2.1 Principles

XMPP is a communication protocol enabling two entities (XMPP clients) to exchange pieces of XML data, called stanzas. The XMPP clients are not directly connected together. They are instead connected to one or several intermediary entities (XMPP servers) making the routing of the stanzas.

As presented in Figure 4, several servers can connect together in order to enable inter-domain communications between XMPP clients. The principle is that each client initiates a connection to its XMPP server (with TCP by default) and creates a logical channel called a stream. Servers connect together in a similar way so that a stanza sent by an XMPP client can flow through the server(s) up to the recipient XMPP client.

For each XMPP client, the permanent and implicitly outgoing connection consists of:

- Creating a TCP connection with the XMPP server (TLS may be used additionally)
- Authenticating through SASL
- Opening two XMPP streams, one for upstream communication to the XMPP server, one for the downstream communication from the XMPP server
- Binding of a resource to the stream

Then, three kinds of stanzas can flow within a stream:

- “iq” dedicated for request / response exchanges – i.e. solicited services: <iq/>
- “message” dedicated for push exchanges – i.e. unsolicited services: <message/>
- “presence” dedicated for presence announcement: <presence/>

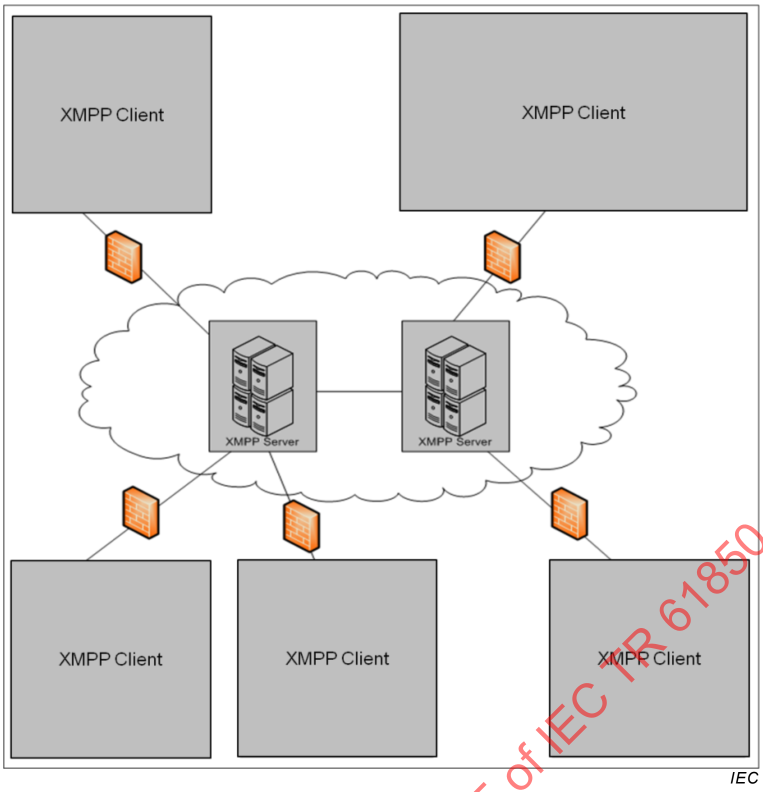


Figure 4 – XMPP architecture overview

7.2.2 Address scheme

Each XMPP entity needs a unique address, called a JID.

JIDs for entities look like email addresses – entity@domain.tld.

Every JID contains a domain portion and each entity that is foreseen to connect to a XMPP server will have a JID with a domain identifier that corresponds to the domain to which the XMPP server belongs. Static configuration or a DNS Service can be used by the XMPP entities to resolve the IP address of the XMPP server they are expected to connect to.

When an XMPP client is connected to a server it needs additionally to define a resource identifier for this connection. This can be the name of a device or software used on the client side to establish the connection or anything else. Then the full JID entity@domain.tld/resource identifies a given connection of an XMPP client.

7.2.3 Scalability and redundancy

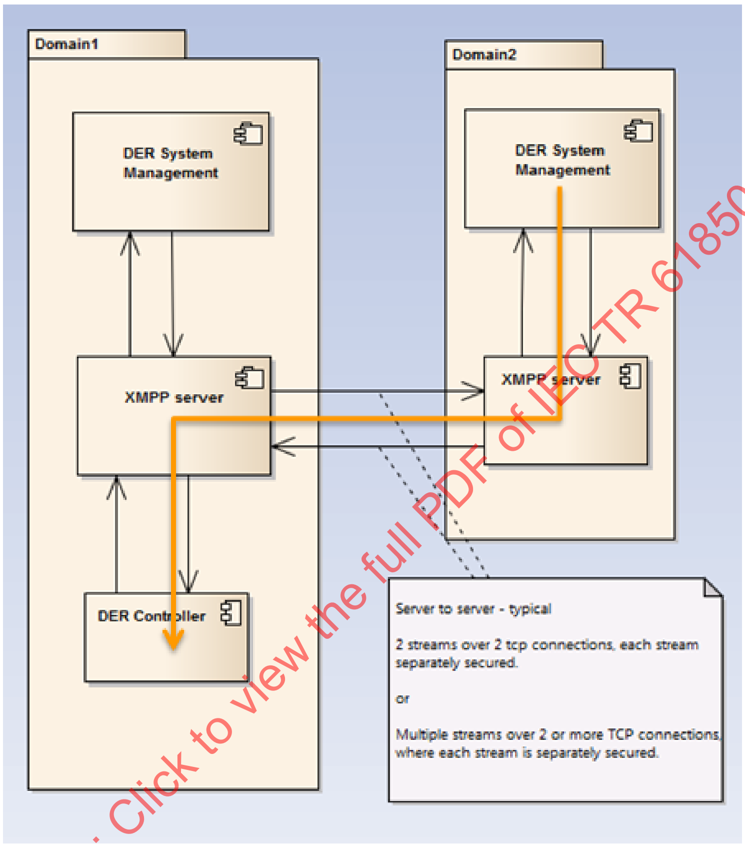
In domains with huge number of members (i.e. XMPP clients), the XMPP server deployment can include a so called clustering, i.e. use of different physical devices to which the TCP connection requests will be initiated by the XMPP clients. In case of clustering, using DNS SRV records allows to balance the load of the different machines, as a weighted list of IP addresses of the connection managers (cluster) that can be involved. A weighted list can also be useful for managing path redundancy: in case the path between an XMPP client and its connection manager is interrupted, a connection to another connection manager, using therefore another path in the WAN, can be initiated by the XMPP client on its own initiative.

NOTE Performance tests show that the transfer time between XMPP clients is by far less than the required 100ms (see 6.3.1, Transfer time) when the XMPP server is not overloaded. It is expected that this performance level can be reached for a very large number of connected clients by adapting the number of servers, typically by clustering.

7.2.4 Server federation

Once two XMPP clients have established an XMPP stream to their XMPP server, the communication can occur through the XMPP stanzas.

In case the two XMPP clients are located in different domains, the XMPP servers of the two domains will establish a communication channel – called XMPP federation – in order to route the information between domains. Figure 5 illustrates the case of an IEC 61850 Client – DER System Management of “domain2.net” that needs to associate to the IEC 61850 Server – DER Controller, member of “domain1.org”.



Server to server - typical

2 streams over 2 tcp connections, each stream separately secured.

or

Multiple streams over 2 or more TCP connections, where each stream is separately secured.

IEC

Figure 5 – XMPP Federation

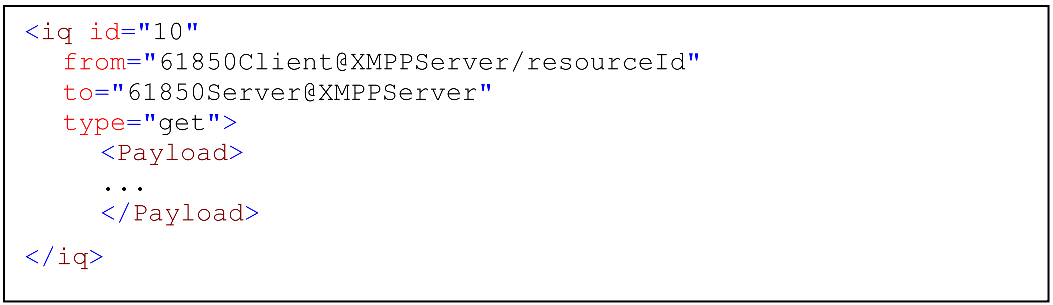
Area of trust over several domains shall be considered in order to allow a secured federation, i.e. an authenticated communication stream between both XMPP servers.

7.2.5 Stanza example

Figure 6 illustrates the XMPP stanza format. The stanza used is <iq/>, i.e. dedicated for request / response. Its type is “get”, therewith, this telegram expect a get response eventually.

The attribute “from” contains the JID of the sender, including the resource identifier used for sending it.

The attribute “to” contains the JID of the sink the stanza is to send to. Here, both from and to belong to the domain “XMPPServer”, therefore the telegram will transit from “61850Client” to ”61850Server” over/via “XMPPServer”.



```
<iq id="10"
   from="61850Client@XMPPServer/resourceId"
   to="61850Server@XMPPServer"
   type="get">
      <Payload>
      ...
      </Payload>
</iq>
```

Figure 6 – Example of a XMPP telegram

7.2.6 Presence monitoring

Presence monitoring is a distinctive feature of XMPP. It enables connected entities to know which entities are also connected. The mechanism is based on the <presence/> stanzas mentioned above as well as on the “rosters” which are contact lists managed by the XMPP servers on behalf of each entity. An XMPP Client can typically:

- Send a presence telegram to another XMPP client via its XMPP server
- Request a presence information from another XMPP client via its XMPP server
- Subscribe to a presence information from another XMPP client via its XMPP server
- Allow its XMPP server to forward/notify presence information to subscribed XMPP clients

7.3 Communication stack overview

Figure 7 presents an overview of the SCSM structure, mentioning the standard specifications and protocols used within the stack.

Regarding the lower layers specified here, note that:

- Layers below the Internet Protocol layer are beyond the scope of the SCSM.
- Usage of XMPP with other transport protocols than TCP is possible (e.g. BOSH or Websocket). However only TCP will be standardized.
- IP is written without any version (IPv4 or IPv6). The mandatory version is IPv4, but IPv6 may be used additionally to IPv4. In general, the clauses of the documents describing the SCSM will be valid for both IP versions. If a mechanism is depending on the IP version, an explanation will be given for both versions.

  In the future, it must be noted that XMPP may enable a smooth migration to IPv6, as XMPP clients using IPv4 and XMPP clients using IPv6 may interoperate, provided that they are connected to an XMPP server presenting the appropriate interfaces IPv4 and IPv6.

The cyber-security aspect is not completely covered in this figure, while the mechanism proposed by XMPP and TLS does not address the requirement for end-to-end security. This aspect is discussed in 7.6.

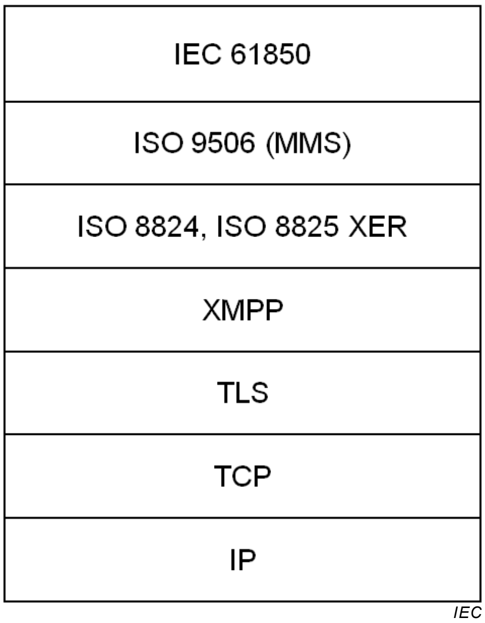


Figure 7 – Simplified communication stack

Table 2 lists which objects and services defined in IEC 61850-7-2 need to be mapped in the SCSM. This corresponds in fact to all the client/server services.

Table 2 – ACSI services to be mapped

Class model	IEC 61850-7-2 Services
Server	GetServerDirectory
Application association	Associate
	Abort
	Release
Logical device	GetLogicalDeviceDirectory
Logical node	GetLogicalNodeDirectory
	GetAllDataValues
Data	GetDataValue
	SetDataValue
	GetDataDefinition
	GetDataDirectory
Data set	GetDataSetValues
	SetDataSetValues
	CreateDataSet
	DeleteDataSet
	GetDataSetDirectory
Setting group control	SelectActiveSG
	SelectEditSG
	SetEditSGValue
	ConfirmEditSGValues
	GetEditSGValue
	GetSGCBValues
Reporting (buffered/unbuffered)	Report
	GetBRCBValues
	SetBRCBValues
	GetURCBValues
	SetURCBValues

Class model	IEC 61850-7-2 Services
Logging	GetLCBValues
	SetLCBValues
	QueryLogByTime
	QueryLogAfter
	GetLogStatusValues
GOOSE	GetGoCBValues
	SetGoCBValues
Sampled Values (multicast/unicast)	Get(M/U)SVCBValues
	Set(M/U)SVCBValues
Control	Select
	SelectWithValue
	Cancel
	Operate
	CommandTermination
	TimeActivatedOperate
Time and time synchronisation	TimeSynchronization
File transfer	GetFile
	SetFile
	DeleteFile
	GetFileAttributeValues

7.4 Definition of the XML payload

The principle is to reuse the definitions of IEC 61850-8-1 regarding the mapping of the ACSI objects and services over the corresponding concepts of MMS. Then, instead of using the BER encoding defined by ISO/IEC 8825-1:2008 for creating the PDUs like in IEC 61850-8-1, the new IEC 61850-8-2 SCSM will use another ASN.1 encoding: the XML Encoding Rules (XER), defined by ISO/IEC 8825-4:2008 (see Figure 8).

The definitions that can be reused from IEC 61850-8-1 include how the objects of the IEC 61850 can be mapped globally over the objects of MMS and more in the details, how each IEC 61850 service is mapped on the MMS services. Table 3, copied from IEC 61850-8-1, shows the MMS objects and services that shall be used for mapping respectively the IEC 61850 objects and services. The detail of the mapping is described in IEC 61850-8-1:2011, Clause 7 for the object mapping and Clauses 9 to 23 for the services. The mapping of the BasicTypes and CommonACSITypes is also the same as the mapping described in IEC 61850-8-1:2011, Clause 8.

NOTE Like the present document, the future IEC 61850-8-2 will make reference to IEC 61850-8-1 rather than duplicating the definitions.

Table 3 – MMS objects and services in use within this SCSM

MMS Object	IEC 61850 Object	MMS Services in Use
Application Process VMD	Server	Initiate Conclude Abort Reject Cancel Identify[a]

MMS Object	IEC 61850 Object	MMS Services in Use
Named Variable Objects	Logical Nodes and Data	Read Write InformationReport GetVariableAccessAttribute GetNameList
Named Variable List Objects	Data Sets	GetNamedVariableListAttributes GetNameList DefineNamedVariableList DeleteNamedVariableList Read Write InformationReport
Journal Objects	Logs	ReadJournal InitializeJournal GetNameList
Domain Objects	Logical Devices	GetNameList GetDomainAttributes StoreDomainContents
Files	Files	FileOpen FileRead ObtainFile FileClose FileDirectory FileDelete

[a] Required by ISO 9506 for conformance.

Concerning the description of the network messages, both the IEC 61850-8-1 and IEC 61850-8-2 profiles will use the same abstract grammar of MMS (see extract in Figure 9), which is based on the ASN.1 BNF grammar defined by ISO/IEC 8824-1.

The difference is that the SCSM 8-2 will use the XML encoding defined by ISO 8825 XER rather than the binary encoding defined by ISO 8825 BER. Figure 10 presents an example of such an XML message corresponding to a GetDataValues service. In order to achieve a good level of interoperability the XML messages shall be validated against a standard “ACSI XML Message” schema (see extract in Figure 11).

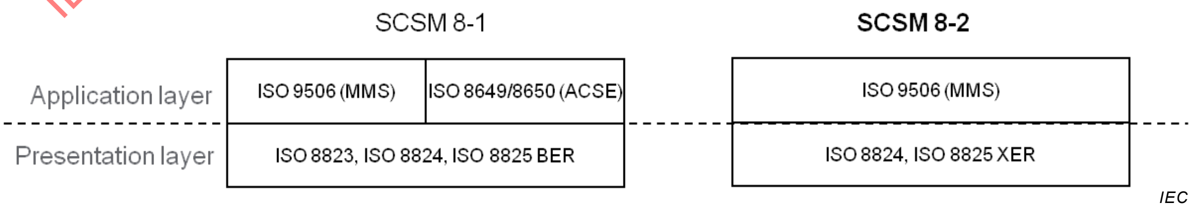
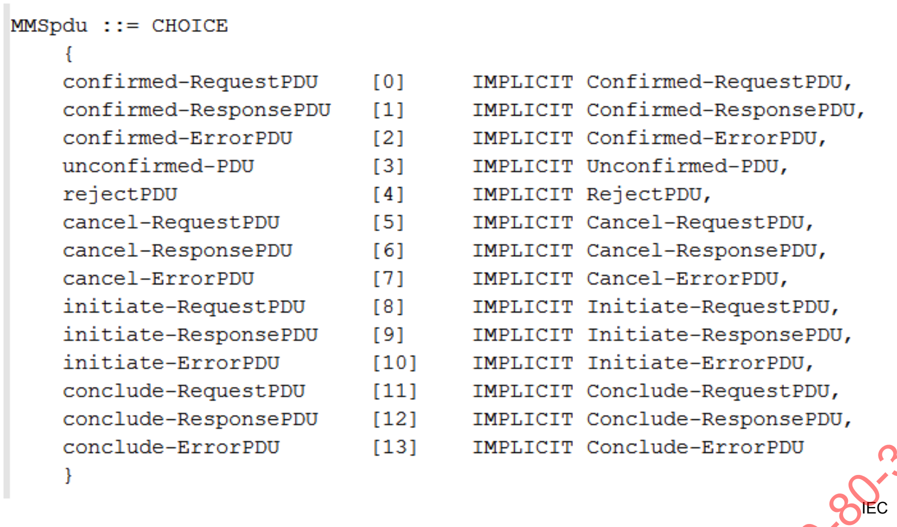


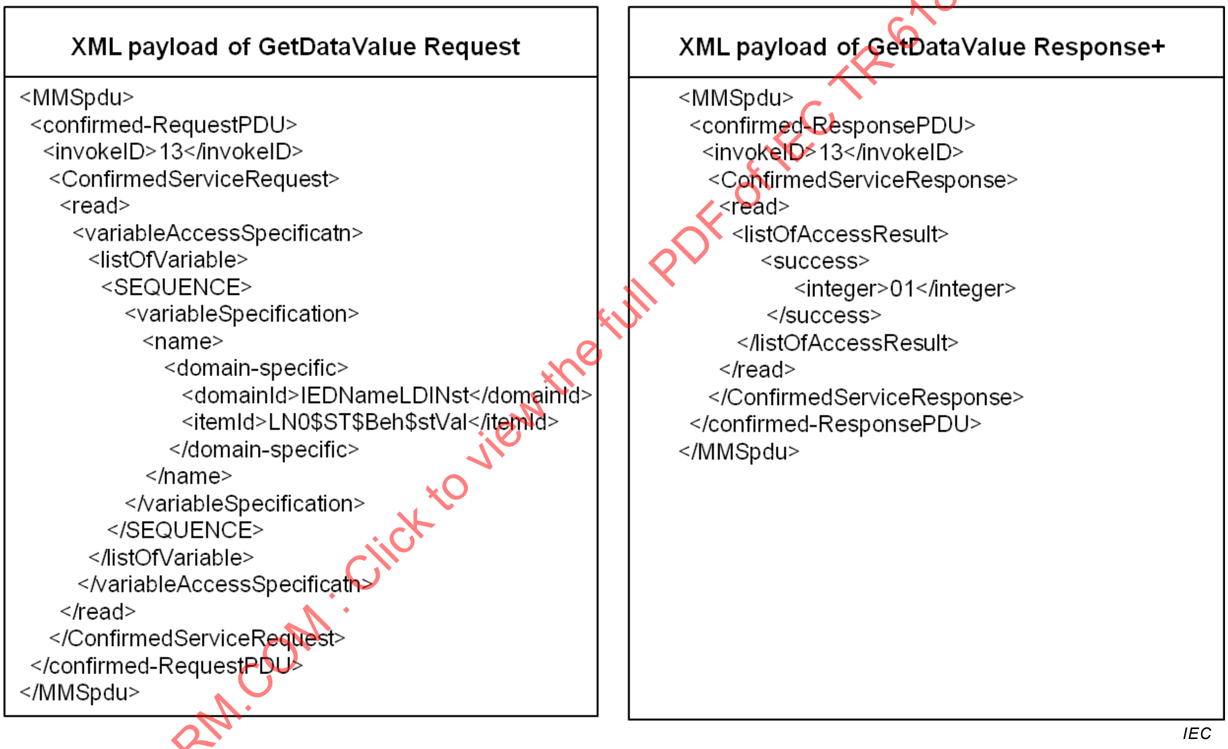
Figure 8 – XER encoding vs BER encoding



```
MMSpdu ::= CHOICE
    {
    confirmed-RequestPDU     [0]     IMPLICIT Confirmed-RequestPDU,
    confirmed-ResponsePDU    [1]     IMPLICIT Confirmed-ResponsePDU,
    confirmed-ErrorPDU       [2]     IMPLICIT Confirmed-ErrorPDU,
    unconfirmed-PDU          [3]     IMPLICIT Unconfirmed-PDU,
    rejectPDU                [4]     IMPLICIT RejectPDU,
    cancel-RequestPDU        [5]     IMPLICIT Cancel-RequestPDU,
    cancel-ResponsePDU       [6]     IMPLICIT Cancel-ResponsePDU,
    cancel-ErrorPDU          [7]     IMPLICIT Cancel-ErrorPDU,
    initiate-RequestPDU      [8]     IMPLICIT Initiate-RequestPDU,
    initiate-ResponsePDU     [9]     IMPLICIT Initiate-ResponsePDU,
    initiate-ErrorPDU        [10]    IMPLICIT Initiate-ErrorPDU,
    conclude-RequestPDU      [11]    IMPLICIT Conclude-RequestPDU,
    conclude-ResponsePDU     [12]    IMPLICIT Conclude-ResponsePDU,
    conclude-ErrorPDU        [13]    IMPLICIT Conclude-ErrorPDU
    }
```

IEC

Figure 9 – ASN.1 abstract definition of MMS PDUs (extract)



XML payload of GetDataValue Request

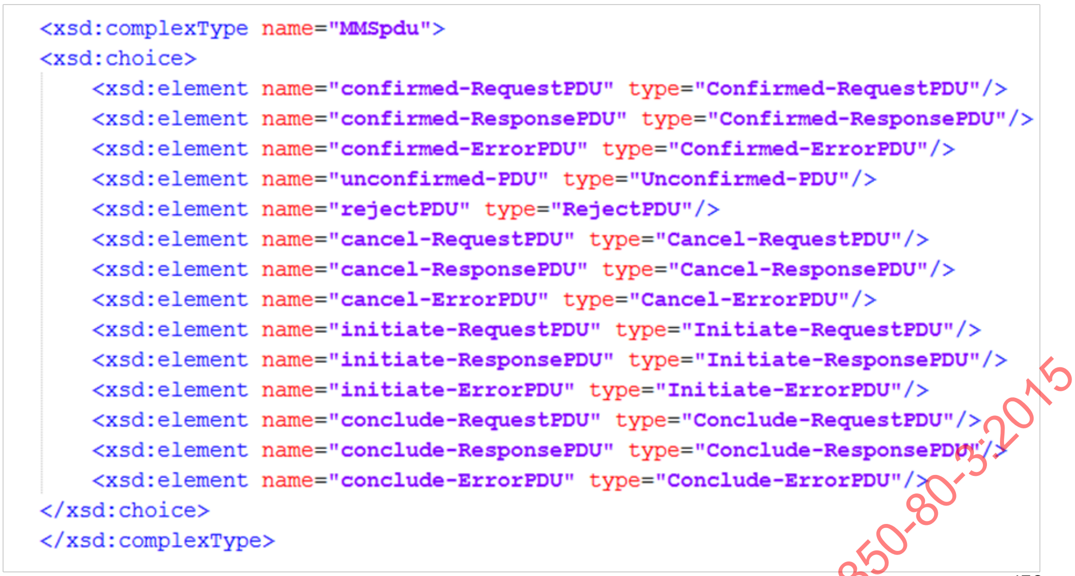
```
<MMSpdu>
 <confirmed-RequestPDU>
  <invokeID>13</invokeID>
   <ConfirmedServiceRequest>
    <read>
     <variableAccessSpecificatn>
      <listOfVariable>
       <SEQUENCE>
        <variableSpecification>
         <name>
          <domain-specific>
           <domainId>IEDNameLDINst</domainId>
           <itemId>LN0$ST$Beh$stVal</itemId>
          </domain-specific>
         </name>
        </variableSpecification>
       </SEQUENCE>
      </listOfVariable>
     </variableAccessSpecificatn>
    </read>
   </ConfirmedServiceRequest>
 </confirmed-RequestPDU>
</MMSpdu>
```

XML payload of GetDataValue Response+

```
<MMSpdu>
 <confirmed-ResponsePDU>
  <invokeID>13</invokeID>
   <ConfirmedServiceResponse>
    <read>
     <listOfAccessResult>
       <success>
          <integer>01</integer>
       </success>
     </listOfAccessResult>
    </read>
   </ConfirmedServiceResponse>
 </confirmed-ResponsePDU>
</MMSpdu>
```

IEC

Figure 10 – Example of XER payloads



```
<xsd:complexType name="MMSpdu">
<xsd:choice>
    <xsd:element name="confirmed-RequestPDU" type="Confirmed-RequestPDU"/>
    <xsd:element name="confirmed-ResponsePDU" type="Confirmed-ResponsePDU"/>
    <xsd:element name="confirmed-ErrorPDU" type="Confirmed-ErrorPDU"/>
    <xsd:element name="unconfirmed-PDU" type="Unconfirmed-PDU"/>
    <xsd:element name="rejectPDU" type="RejectPDU"/>
    <xsd:element name="cancel-RequestPDU" type="Cancel-RequestPDU"/>
    <xsd:element name="cancel-ResponsePDU" type="Cancel-ResponsePDU"/>
    <xsd:element name="cancel-ErrorPDU" type="Cancel-ErrorPDU"/>
    <xsd:element name="initiate-RequestPDU" type="Initiate-RequestPDU"/>
    <xsd:element name="initiate-ResponsePDU" type="Initiate-ResponsePDU"/>
    <xsd:element name="initiate-ErrorPDU" type="Initiate-ErrorPDU"/>
    <xsd:element name="conclude-RequestPDU" type="Conclude-RequestPDU"/>
    <xsd:element name="conclude-ResponsePDU" type="Conclude-ResponsePDU"/>
    <xsd:element name="conclude-ErrorPDU" type="Conclude-ErrorPDU"/>
</xsd:choice>
</xsd:complexType>
```

IEC

Figure 11 – ACSI XML Message schema for XER payload (extract)

NOTE The XML schema defining the MMS XER messages is a straightforward translation of the ASN.1 notation used by MMS. The task of writing a normative XML schema defining the XER messages can be automated by existing tools: starting from the BNF ASN.1 notation that represents the subset of MMS used by IEC 61850, such tools are able to generate the corresponding XSD definitions.

7.5 Transport of XML payloads over XMPP

7.5.1 Mapping over XMPP overview

From an XMPP point of view, all IEC 61850 applications (client or server) are XMPP clients. The architecture (see Figure 12) is based on a tier entity, the XMPP server, on which both IEC 61850 client and server applications are connecting. In this way, no incoming connection is required on IEC 61850 entities (client and server) so that security issues such as firewall parameterization are mostly delegated to the tier server.

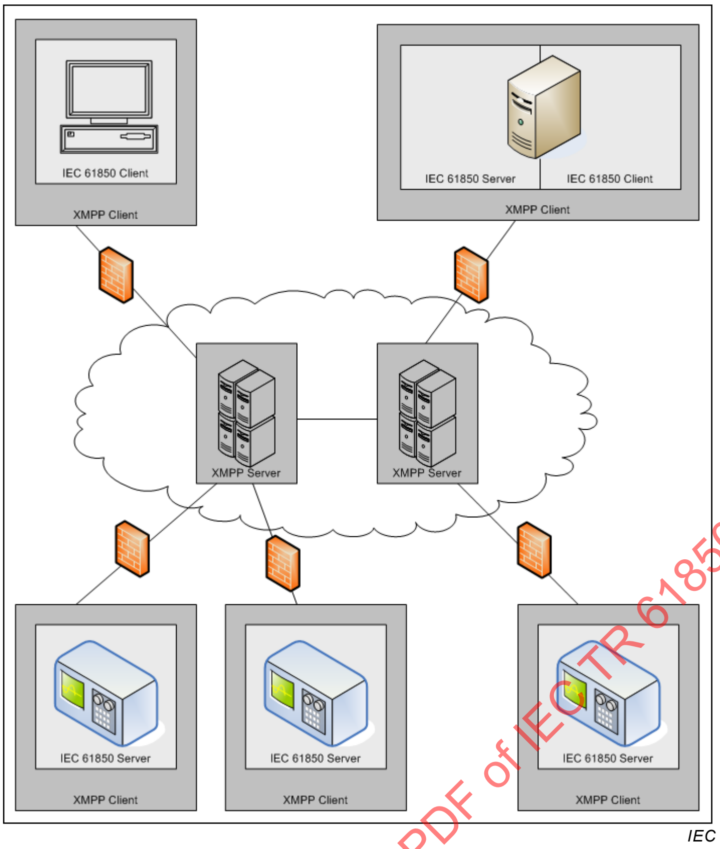


Figure 12 – XMPP architecture for IEC 61850

The following XMPP features are used for the ACSI mapping:

- “iq” stanzas are dedicated to “Request/Reply” message exchange pattern, allowing the implementation of solicited services between an IEC 61850 client application and an IEC 61850 server application.
- “message” stanzas are dedicated to “push” message exchange pattern, well suited for unsolicited services between an IEC 61850 server application and an IEC 61850 client application.

7.5.2 Rules for mapping solicited services

Most of the client/server services are solicited services defined by three elements: the Request, the positive Response and the negative Response.

Parameter name
Request
<request parameters>
Response+
<response parameters>
Response-
<service errors>

All solicited services are implemented by IQ stanzas. The request message is implemented by an IQ stanza of type ‘set’ or ‘get’ and the response message is implemented by a ‘result’ IQ stanza. The direct child element of the IQ stanza, AssociationContext, represents the association established between the client and the server and it contains a MMSpdu element which is the payload of the message as defined in 7.4. The following example presents the IQ stanzas for the GetDataValues service (see also example for a GetLogicalNodeDirectory in

B.2). The element <Security tbd> in this example means that some information dedicated to the end-to-end security will in fact encapsulate the MMSpdu (to be defined in the next edition of IEC 62351-4 and IEC 61850-8-2):

- GetDatavalue Request:

```
<iq id="10"
    from="61850app@XMPPServer/resourceId"
    to="61850server@XMPPServer"
    type="get">
  <AssociationContext id=“32”>
    <Security tbd>
      …
      <MMSpdu xmlns="http://www.iec.ch/61850/2015/SCSM_8_2">
        <Confirmed-RequestPDU>
          <invokeID>13</invokeID>
          <ConfirmedServiceRequest>
            <read>
              …
            </read>
          </ConfirmedServiceRequest>
        </confirmed-RequestPDU>
      </MMSpdu>
      …
    </Security tbd>
   </AssociationContext>
</iq>
```

- GetDatavalue Response+:

```
<iq id="10"
    from= "61850server@XMPPServer"
    to="61850app@XMPPServer/resourceId"
    type="result">
  <AssociationContext id=“32”>
    <Security tbd>
      …
      <MMSpdu xmlns="http://www.iec.ch/61850/2015/SCSM_8_2"
        <confirmed-ResponsePDU>
          <invokeID>13</invokeID>
          <ConfirmedServiceResponse>
            <read>
              …
            </read>
          </ConfirmedServiceResponse>
        </confirmed-ResponsePDU>
      </MMSpdu>
      …
    <Security tbd/>
  </AssociationContext>
</iq>
```

Errors occurring during the IQ stanza transmission or processing, are indicated by an IQ stanza of type=“error” containing an <error/> child element, qualified by the namespace urn:ietf:params:xml:ns:xmpp-stanzas. This namespace as well as the full list of error conditions are specified in RFC 6120.

Errors occurring on IEC 61850 application or mapping layers should be transmitted by a normal IQ response, i.e. with type=“result” and the appropriate MMS error code, encoded in XML.

7.5.3 Mapping of unsolicited services

With XMPP, the typical mechanism used to push information is the “message” stanza. So the unsolicited services are implemented as message stanzas. The direct child element of the stanza, AssociationContext, represents the association established between the client and the server and it contains a MMSpdu element which is the XML payload of the message. The following example shows a message stanza for the Report service (see also example in B.3):

```
<message
    from="server@XMPPServer"
    to="61850app@XMPPServer/ResourceId"
    type="chat">
  <AssociationContext id=“32“>
    <Security tbd>
      …
      <MMSpdu xmlns="http://www.iec.ch/61850/2015/SCSM_8_2">
        <unconfirmed-PDU>
          <UnconfirmedService>
            <informationReport>
              …
            </informationReport>
          </UnconfirmedService>
        </unconfirmed-PDU>
      </MMSpdu>
      …
    </Security tbd>
  </AssociationContext>
</message>
```

7.5.4 Usage of presence monitoring

The XMPP architecture based on a XMPP server where IEC 61850 clients and servers are connecting brings some constraints but also some opportunities if the presence monitoring is used. This clause recommends that the future SCSM 8-2 should use the presence monitoring for the implementation of the ACSI services as they are defined in IEC 61850-7-2.

There are indeed several reasons why presence monitoring is useful in a DER deployment system:

- As the IEC 61850 servers and clients are not connected to each other, the monitoring of the IEC 61850 association cannot occur by using the TCP keep alive. It could use instead a periodic GetNamedList or the XEP-0199: XMPP Ping. However both would have the limitation of detecting the disconnection, cyclically rather than on event.
- Disconnection of XMPP Client peer may not be detected unless a monitoring of a “silent” connection occurs.
- Within the scope of grid integration, being aware of the presence of DER controllers allows system management to better predict the actual available resources, and therefore to better react in emergency situation.
- DER controller may or may not be connected 24/7.
- Dial-up scenario can be solved by using the presence monitoring of device with limited connectivity – i.e. inform one or several System Management(s) that a resource is ready for an IEC 61850 association.
- It allows the System Management responsible for a schedule exchange with a device to be notified that a DER controller / DER system is online.

The detailed usage of the presence monitoring will be defined in the future 61850-8-2 SCSM.

7.6 Cyber security

7.6.1 Security with XMPP

Clause 13, *Security Considerations* of the RFC 6120 specifies the usage of TLS and SASL:

- TLS can be used between XMPP Clients and the XMPP server as illustrated in Figure 13.The specific threats countered at the transport layers level, as long as the XMPP server is a trusted hop, include:
  - Unauthorized access to information through message level authentication and encryption of the messages
  - Unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages
- An additional simple authentication mechanism allows the XMPP server to guarantee the identity of the connected XMPP client – see SASL in Figure 13.

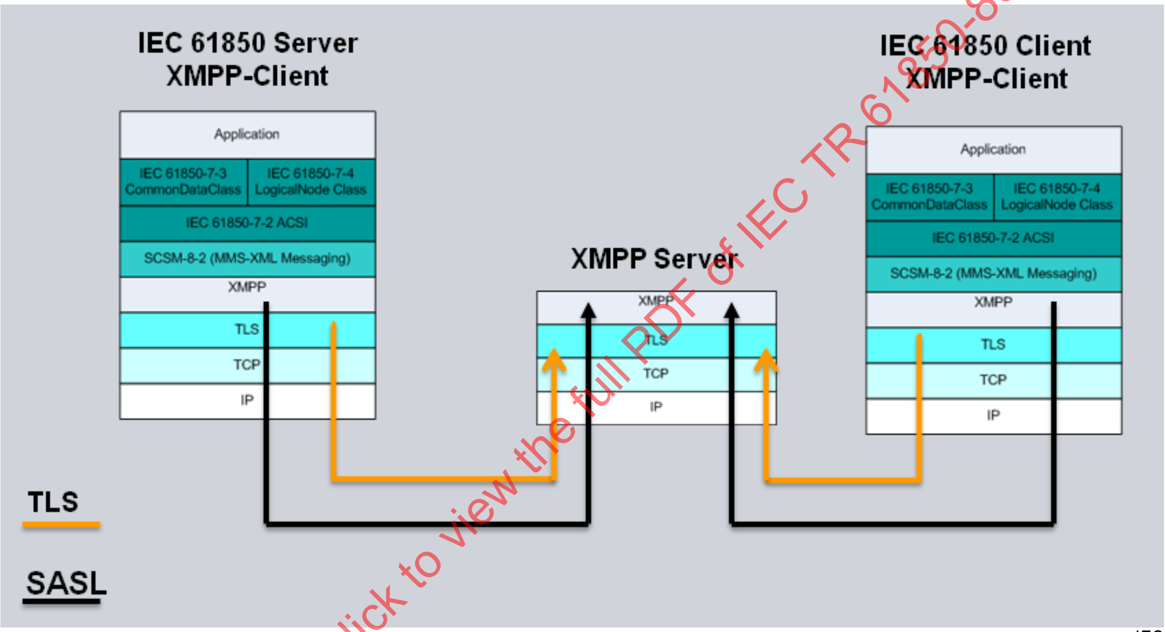

IEC 61850 Server
XMPP-Client
Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
SCSM-8-2 (MMS-XML Messaging)
XMPP
TLS
TCP
IP
XMPP Server
XMPP
TLS
TCP
IP
IEC 61850 Client
XMPP-Client
Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
SCSM-8-2 (MMS-XML Messaging)
XMPP
TLS
TCP
IP
TLS
SASL
IEC

Figure 13 – XMPP using TLS and Simple Authentication and Security Layer (SASL)

It appears that end-to-end security is not guaranteed by XMPP core specifications. A true end-to-end security, as displayed in Figure 14, should additionally allow measures to guarantee:

- The authentication of the IEC 61850 communication entities
- The confidentiality of message content between both IEC 61850 communication entities

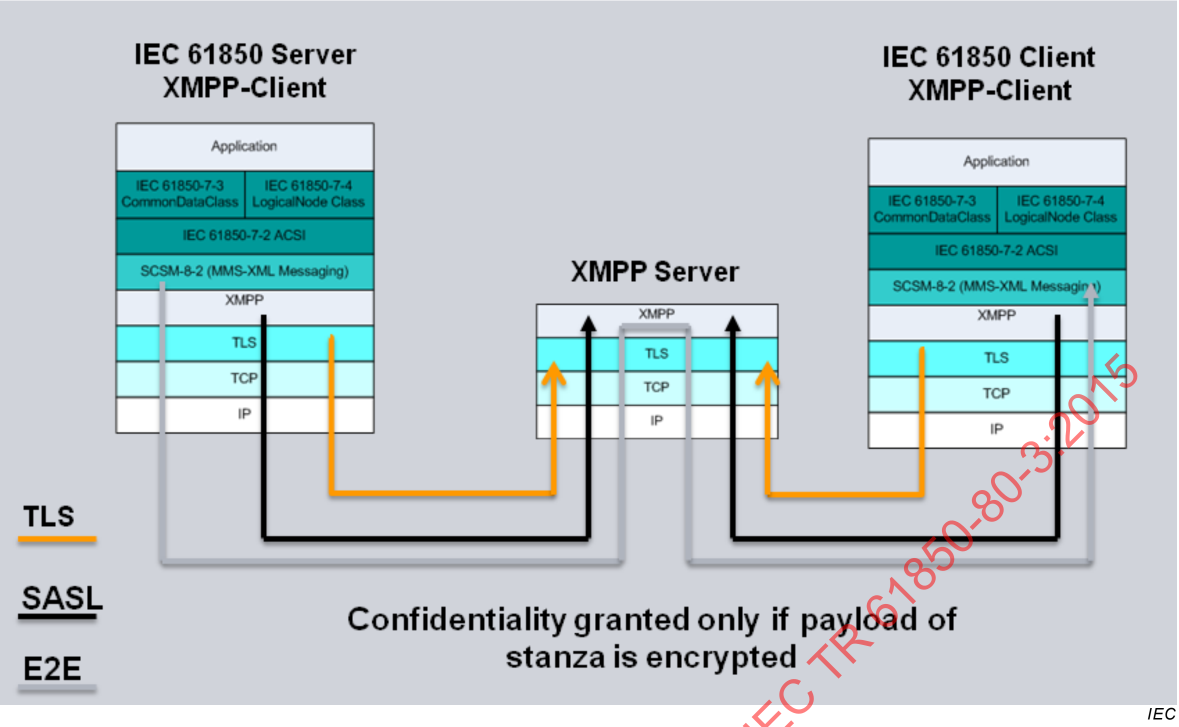

IEC 61850 Server
XMPP-Client
Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
SCSM-8-2 (MMS-XML Messaging)
XMPP
TLS
TCP
IP
XMPP Server
XMPP
TLS
TCP
IP
IEC 61850 Client
XMPP-Client
Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
SCSM-8-2 (MMS-XML Messaging)
XMPP
TLS
TCP
IP
TLS
SASL
E2E
Confidentiality granted only if payload of stanza is encrypted
IEC

Figure 14 – End to end security over XMPP

7.6.2 Choice of technical solutions for security

For mutual authentication, session integrity and confidentiality of XMPP client – server or server – server communication the present SCSM will use TLS as specified in RFC 6120 (XMPP Core) with TLS settings compliant with IEC 62351-3.

End-to-end authentication, integrity, and confidentiality will be achieved by applying the MMS secure session concept defined in the next edition of IEC 62351-4.

7.7 Mapping synthesis

Compared to the simplified Figure 7, Figure 15 brings additional details for the SCSM 8-2 structure:

- Regarding the IEC 61850 standards, the SCSM 8-2 is by definition a mapping of IEC 61850-7-2 and supports all the data defined in IEC 61850-7-3 and IEC 61850-7-4. Additionally, the SCSM 8-2 will use the mapping of IEC 61850-7-2 over MMS which has already been defined by IEC 61850-8-1.
- XMPP is in fact defined by a set of core RFC and extensions called XEP. Among the three core RFC (6120, 6121 and 6122), the RFC 6120 and 6122 specify the low level mechanisms used to transport the XER payload, while the presence monitoring features proposed by RFC 6121, together with the XEP 0198 and XEP 0199 are proposing more advanced features.
- The context, Data and Abort service and protocol layer will be used to:
  - – Forward services signal to ISO 9506 (MMS) – for example to map the ABORT service
  - – Provide an association identifier to the MMS PDU, to allow multiple IEC 61850 Associations between an IEC 61850 Server and an IEC 61850 Client
  - – Store security information – still to be defined depending on the next edition of IEC 62351-4

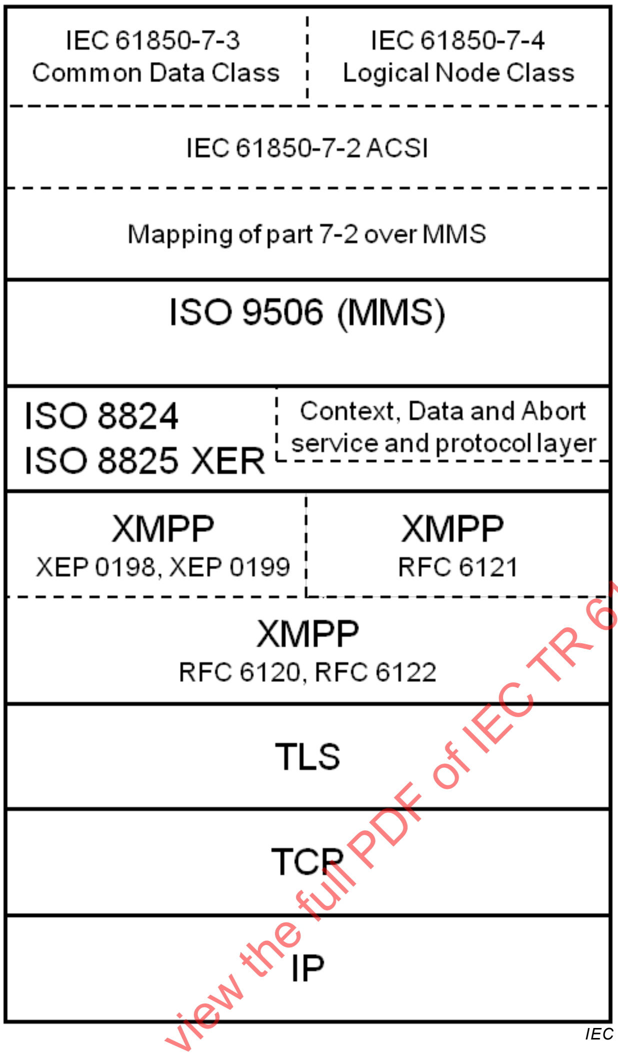


Figure 15 – Synthesis of SCSM 8-2 structure

The incomplete Table 4 illustrates the two levels involved in the mapping. For each ACSI service of the first column, the second column gives the XML definitions resulting from the MMS/XER mapping and the third column shows how the messages are transported over XMPP. The future IEC 61850-8-2 will include the complete table for all ACSI services.

Table 4 – Mapping synthesis

Service	MMSpdu XML messaging definitions	Type of stanza	Comment
Associate	Initiate-RequestPDU Initiate-ResponsePDU	IQ type=set IQ type=result	
Release	Conclude Conclude	IQ type=set IQ type=result	
GetDataValues	Read Read	IQ type=get IQ type=result	
SetDataValues	Write Write	IQ type=set IQ type=result	
Report	informationReport	Message	
GetFile	fileDirectory fileDirectory	IQ type=get IQ type=result	
		Presence	Presence monitoring

7.8 Synergy with existing 8-1 mapping

Figure 16 illustrates the common parts between the SCSM defined respectively by IEC 61850-8-1 and IEC 61850-8-2.

The use of common layers simplifies a dual environment implementation:

- For example, Figure 17 illustrates the use of a dual stack in the Control Center implementation, i.e. an IEC 61850 client connected to IEC 61850-8-1 devices located for instance in Substation via a private network, and to IEC 61850-8-2 devices like DERs components located in a public network (note that the XMPP server is not shown on the IEC 61850-8-2 path).
- Another example is an IEC 61850-8-1 / IEC 61850-8-2 Gateway implementation, as illustrated in Figure 18.

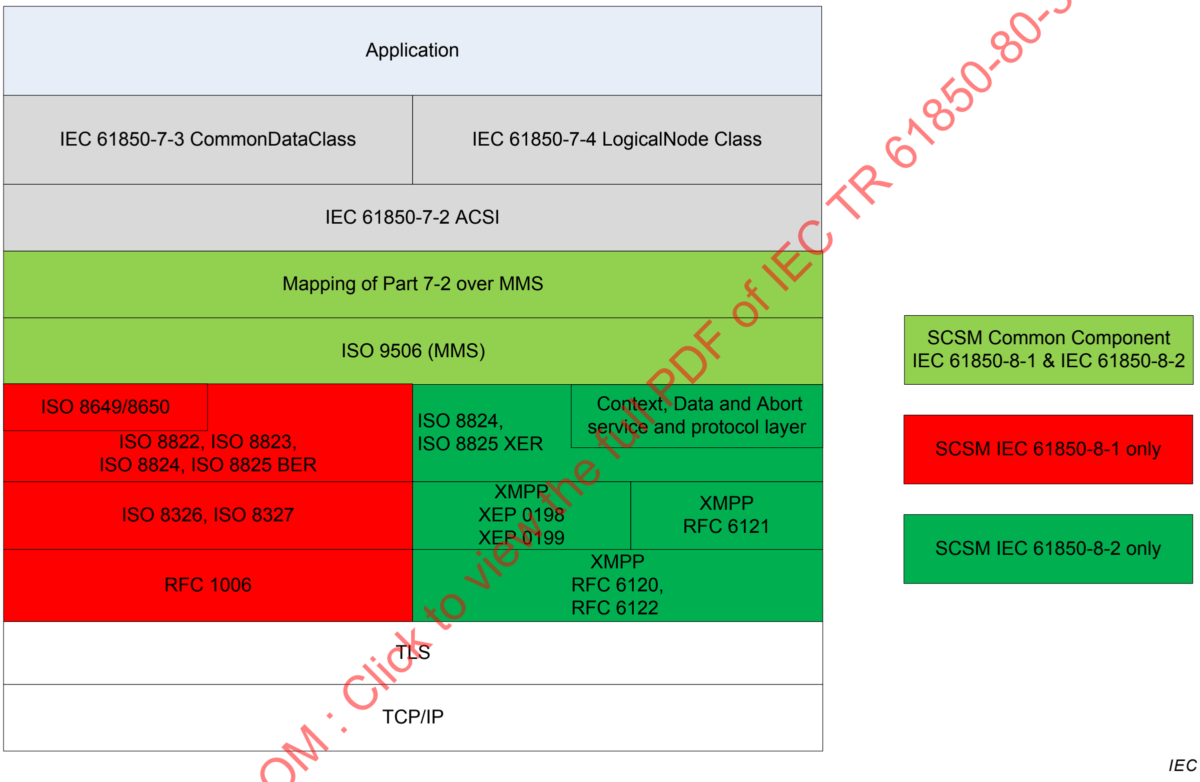

Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
Mapping of Part 7-2 over MMS
ISO 9506 (MMS)
ISO 8649/8650
ISO 8822, ISO 8823, ISO 8824, ISO 8825 BER
ISO 8824, ISO 8825 XER
Context, Data and Abort service and protocol layer
ISO 8326, ISO 8327
XMPP XEP 0198 XEP 0199
XMPP RFC 6121
RFC 1006
XMPP RFC 6120, RFC 6122
TLS
TCP/IP
SCSM Common Component IEC 61850-8-1 & IEC 61850-8-2
SCSM IEC 61850-8-1 only
SCSM IEC 61850-8-2 only
IEC

Figure 16 – SCSM 8-1 and 8-2 synergy

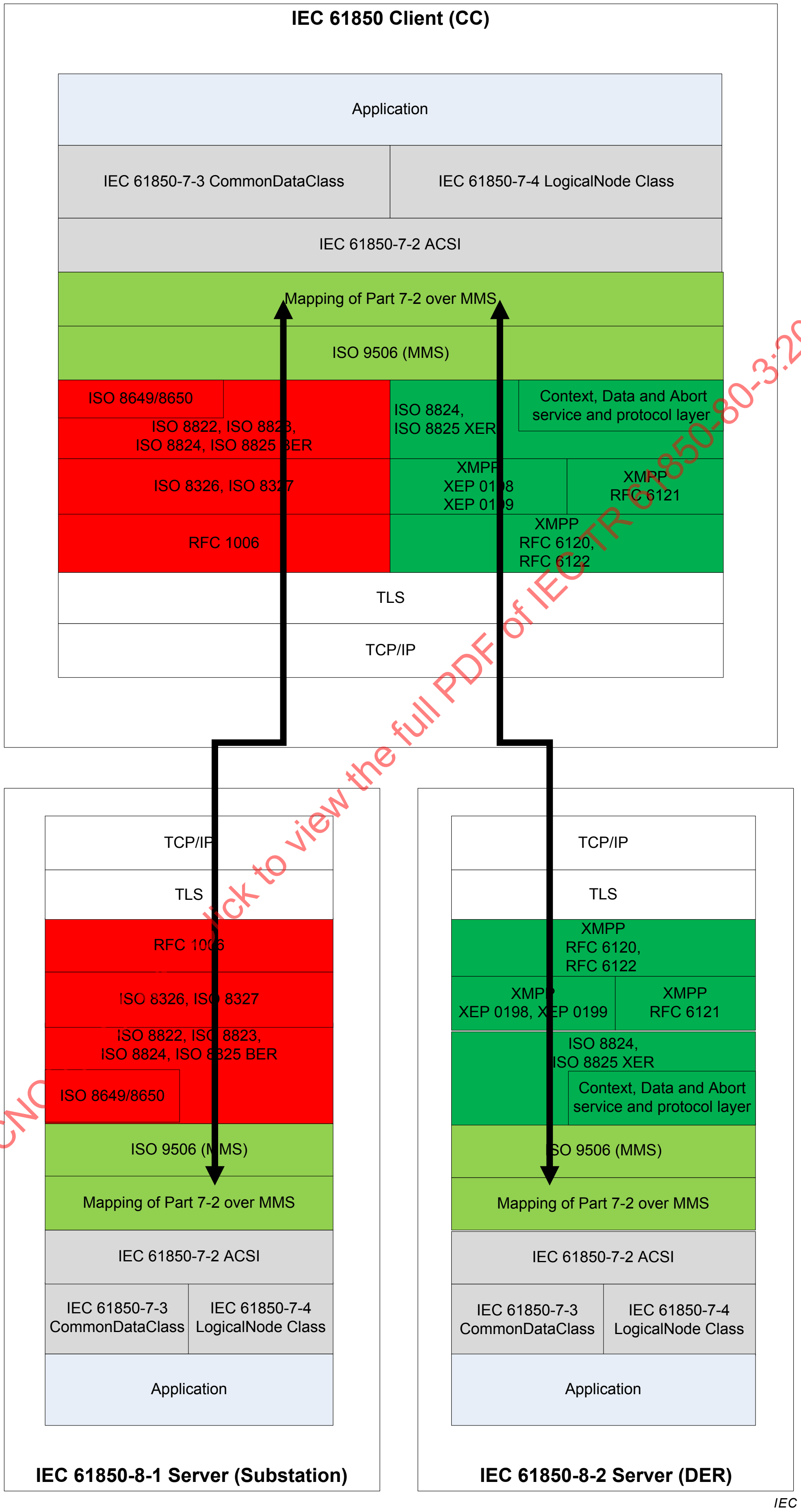

IEC 61850 Client (CC)
Application
IEC 61850-7-3 CommonDataClass
IEC 61850-7-4 LogicalNode Class
IEC 61850-7-2 ACSI
Mapping of Part 7-2 over MMS
ISO 9506 (MMS)
ISO 8649/8650
ISO 8822, ISO 8823, ISO 8824, ISO 8825 BER
ISO 8824, ISO 8825 XER
Context, Data and Abort service and protocol layer
ISO 8326, ISO 8327
XMPP XEP 0198 XEP 0199
XMPP RFC 6121
RFC 1006
XMPP RFC 6120, RFC 6122
TLS
TCP/IP
IEC 61850-8-1 Server (Substation)
IEC 61850-8-2 Server (DER)
XMPP XEP 0198, XEP 0199
IEC

Figure 17 – Control center with dual stack SCSM 8-1 / SCSM 8-2

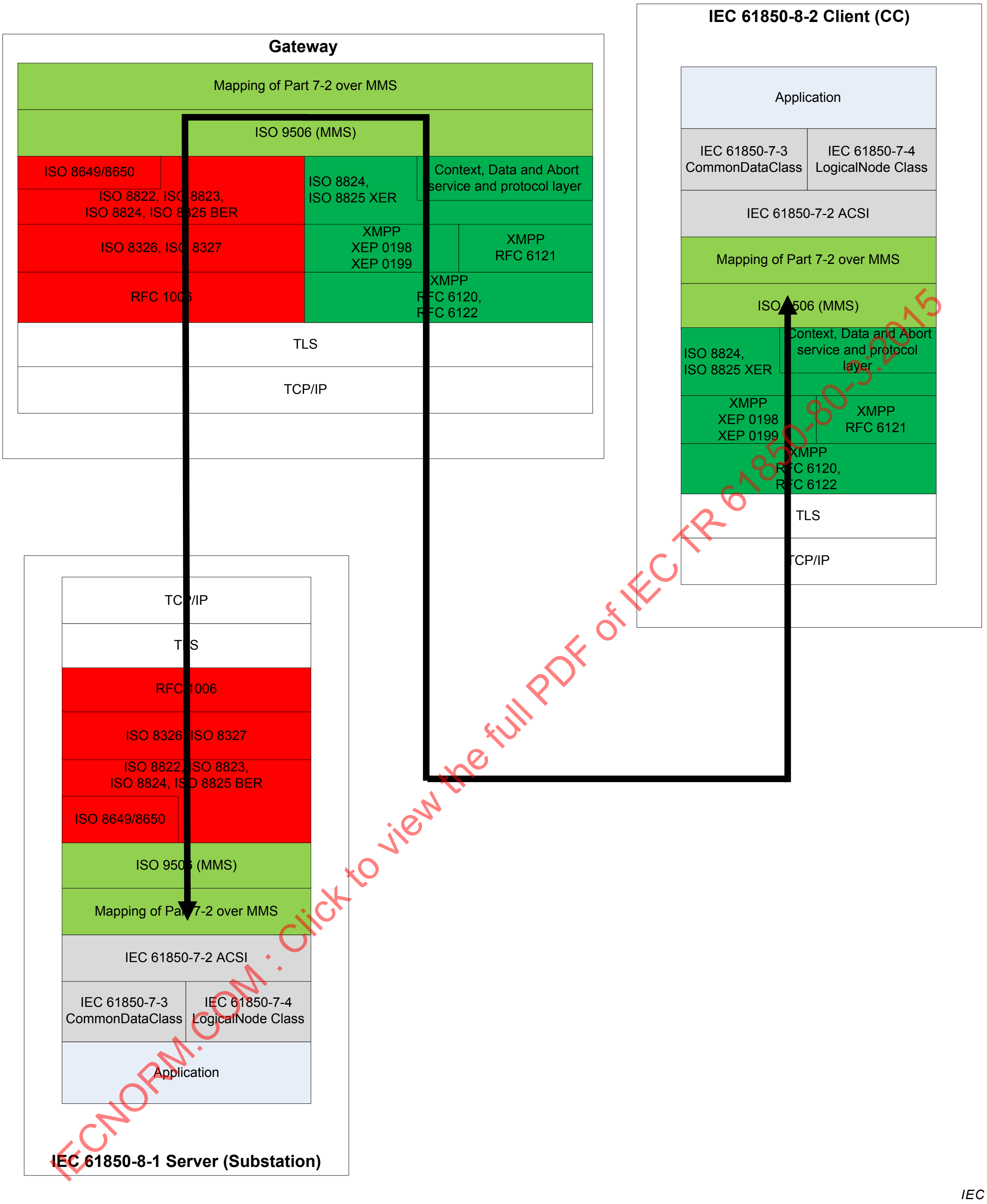


Figure 18 – Gateway between SCSM 8-1 and SCSM 8-2

Annex A
(informative)

Use cases and requirements for each domain

A.1 Use cases for PV-inverters

A.1.1 Scope of this clause

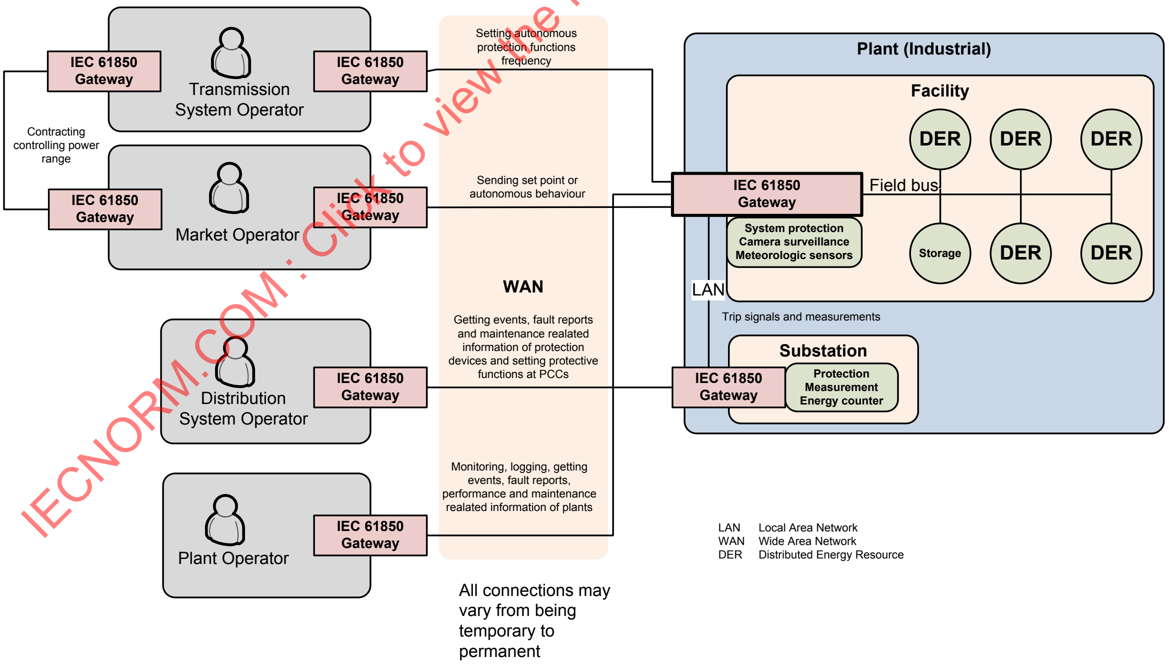
This clause covers the services required for PV-Plants of all sizes: Industrial, Commercial, Residential driven plants. The plants typically have one central point of communication coupling and consist of one to several thousand of devices, which are capable to communicate.

A.1.2 Architecture overview

The system contains protective switches, inverters, data loggers, meteorological sensors, energy counters and other auxiliary devices. Architecture overviews for respectively an industrial and a residential plant are shown in Figure A.1 and Figure A.2.

Scalability:

- About 15 different Logical Nodes per PV plant (up to 40)
- Up to 4 actors at the same time (see A.1.3)
- Further aggregation in actor application or by aggregator (see VPP in Clause A.7)


IEC 61850 Gateway
Transmission System Operator
IEC 61850 Gateway
Contracting controlling power range
IEC 61850 Gateway
Market Operator
IEC 61850 Gateway
Distribution System Operator
IEC 61850 Gateway
Plant Operator
IEC 61850 Gateway
Setting autonomous protection functions frequency
Sending set point or autonomous behaviour
WAN
Getting events, fault reports and maintenance realated information of protection devices and setting protective functions at PCCs
Monitoring, logging, getting events, fault reports, performance and maintenance realated information of plants
All connections may vary from being temporary to permanent
Plant (Industrial)
Facility
DER
DER
DER
IEC 61850 Gateway
Field bus
System protection Camera surveillance Meteorologic sensors
Storage
DER
DER
LAN
Trip signals and measurements
Substation
IEC 61850 Gateway
Protection Measurement Energy counter
LAN Local Area Network
WAN Wide Area Network
DER Distributed Energy Resource

IEC

Figure A.1 – PV – Architecture overview for data connections to an industrial plant

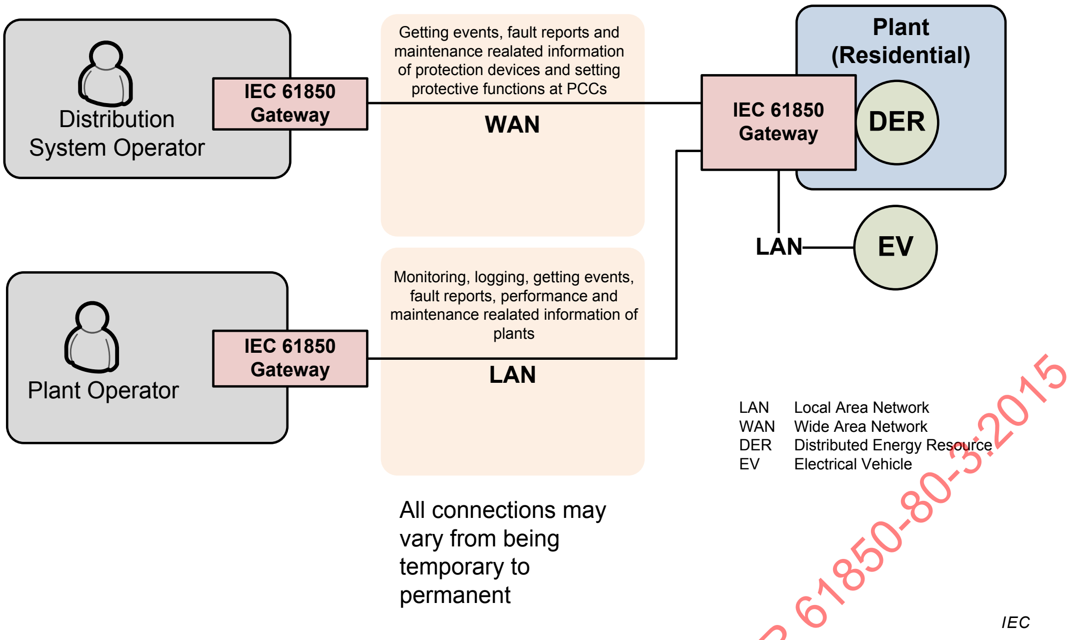

Distribution System Operator
IEC 61850 Gateway
Getting events, fault reports and maintenance realated information of protection devices and setting protective functions at PCCs
WAN
Plant (Residential)
IEC 61850 Gateway
DER
LAN
EV
Plant Operator
IEC 61850 Gateway
Monitoring, logging, getting events, fault reports, performance and maintenance realated information of plants
LAN
LAN Local Area Network
WAN Wide Area Network
DER Distributed Energy Resource
EV Electrical Vehicle
All connections may vary from being temporary to permanent
IEC

Figure A.2 – PV – Architecture overview for data connections to a residential plant

A.1.3 Use cases

The most relevant actors are:

- Plant operator
- Generation asset management
- Distribution system operator
- Transmission system operator
- Market operator

Table A.1 gives a use case list for PV plants.

Table A.1 – Use case list

#	Use case name	Description	Actors
1	Performance and maintenance management	• Measurement and status data points • Provided services	Plant operator
2	Monitoring and logging	• Measurement and status data points • Provided services • Events and fault reports	Generation asset management
3	Voltage stability and system protection	• Direct control by set points or indirect control by schedules • Parameterization of grid integration functions for autonomous behaviors • Parameterization of protection devices/functions • Pre-knowledge of energy flows by forecasts • The grid code CEI 0-21 (from Italy) requires a disconnection within 50 ms through a send disconnection command	Distribution system operator

#	Use case name	Description	Actors
4	Frequency stability, Power Output Adjustment, VAr management, Storage Management and black-start capabilities (not on scope yet)	• Direct control by set points or indirect control by schedules • Parameterization of grid integration functions for autonomous behaviors	Transmission system operator
5	Manipulation of energy flow of plants (consumption/production) due to energy market	• Direct control by set points or indirect control by schedules • Pre-knowledge of energy flows by forecasts	Market operator

A.2 Use cases for hydro and thermal generation

A.2.1 Scope of this clause

This clause covers the communica tion requirements to fulfill the needs of the following type of large power generating plants:

- Hydro electric power plants (all systems)
- Hydro pump-turbine storage (all systems)
- Power plants with steam prime movers (power evacuation only)
- Power plants with gas turbine prime movers or combined cycle power plants (power evacuation only)

A.2.2 Architecture overview

Figure A.3 shows the network architecture between the principal actors for large power generating plants.

The following actors have been identified for the use cases listed in A.2.3 and are roughly described (see also Table 1):

- Transmission system operator – means a natural or legal entity responsible for ensuring the stability of the grid.
- Plant operator – means any natural or legal person operating a power plant.
- Market operator– means any natural or legal entity responsible for ensure the energy reserves to honor the power output obligations.
- Plant Maintenance – means any natural or legal entity responsible to ensure the performance and the reliability of the power plant.

Figure A.4 describes the relationship between the different actors.

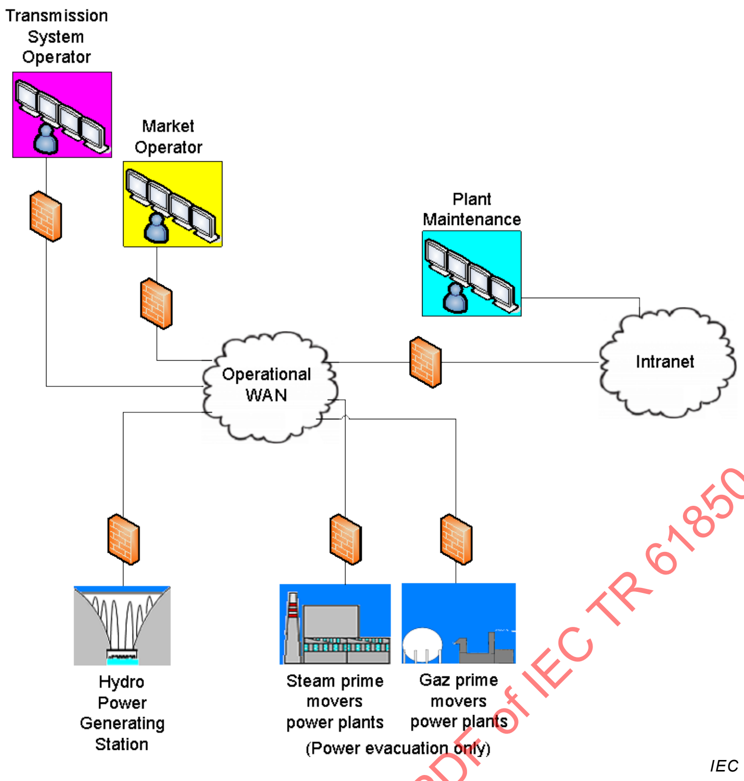

Transmission System Operator
Market Operator
Plant Maintenance
Operational WAN
Intranet
Hydro Power Generating Station
Steam prime movers power plants
Gaz prime movers power plants
(Power evacuation only)
IEC

Figure A.3 – Power plants – Typical power operator network architecture

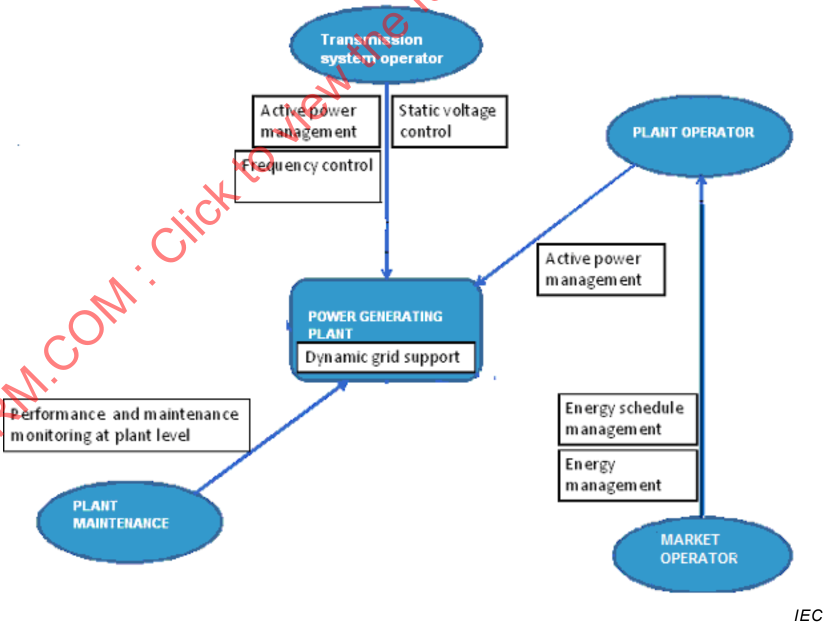


Figure A.4 – Power plants – Relationship between the actors

A.2.3 Use cases

Table A.2 gives a use case list for power plants.

Table A.2 – Power plants – Use case list

	Use case name	Description	Actors
1	Connection to the energy management system	Large power plants have to bridge power related information to the bulk markets. This information is normally confidential but real time. The subscribers of this type of information are basically market operators (power brokers Energy planers and operators of the Bulk market). Remote user access to any power plant IED should not permitted.	Market operator, Plant operator
2	Connection to the corporate equipment & plant maintenance system	Large power plants have to bridge the following type of information to the enterprise layer: • Power related information • Events and fault reports • Maintenance related information (operational counters) The internet layer is basically in the corporate layer. The information is used for building maintenance statistics or issue work orders. The information is normally differed in time and it is not confidential. Remote user access to any power plant IED should not permitted.	Plant maintenance, Plant operator
3	Connection to the transmission system operator	Large power plants have to bridge the following type of information: • Power related information • Events and fault reports • Performance and maintenance related information • Energy storage information • Operational alarms • Status information Large power plants have to receive the following type of information: • Start-stop orders • Operational set points (W, Var, Lev, Flw) The information exchange is required to ensure the stability of the electric grid. This information, within the operational WAN, is real time and may be confidential. Since Grid operators use telecom services that egresses a firewall protected physical security perimeter, internet key exchanges shall be used to ensure that the data was not tampered. The operator shall additionally be authenticated.	Transmission system operator
4	Power station maintenance	Power station maintenance team is required to be linked to the following information: • Energy related information (MW, Water level, etc.) • Events and fault reports • Performance and maintenance related information • Energy storage information • Operational alarms • Status information The information exchange is required to ensure the stability of the electric grid. This information, within the operational WAN may be confidential. User access to any power plant IED is permitted without authentication service, when within a physically secured perimeter.	Plant maintenance

	Use case name	Description	Actors
5	Power plant operations	Power station Operations requires the operator to be linked to the following type of information: • Operational alarms • Energy related information (MW, Water level, etc.) The operator is entitled to send the following orders: • Start-stop orders • Operational set points (W, Var, Lev, Flw) The information exchange is required to ensure the stability of the electric grid. This information, within the operational WAN may be confidential. User access to any power plant IED is permitted without authentication service, when within a physically secured perimeter.	Plant operator

A.3 Use cases for wind power

A.3.1 Scope of this clause

The domain includes communications for monitoring, control and evaluation of wind plants, their components, and their interconnection to the grid.

A.3.2 Architecture overview

The electrical architecture of a wind power plant consists of wind turbines and their associated equipment (transformer, breaker, switch, etc.) connected by wind plant collectors to a substation or substations that interface the plant to the grid. There may also be other components in the plant such as for providing Var compensation if needed because of the turbines having induction generators. The elements of this architecture include:

- Wind turbine and its local components
- Wind plant collectors
- Wind plant substation(s) interconnecting to the grid
- Other wind plant components:
  1) Meteorological tower and sensors
  2) Facilities serving the overall plant for various purposes
  3) Wind plant control facility (local SCADA)
  4) Wind plant communications to the transmission operator or other relevant facility

Other relevant facilities include:

- Transmission operator (TSO)
- Maintenance center
- Weather forecasting facility
- Multiple SCADAs or control centers that receive and can respond to alarms and must coordinate their responses

IEC 61400-25 requires and supports a multi-level control hierarchy with no constraint on topology. This architecture is illustrated in Figures A.5 to A.8 (from a User Group presentation):

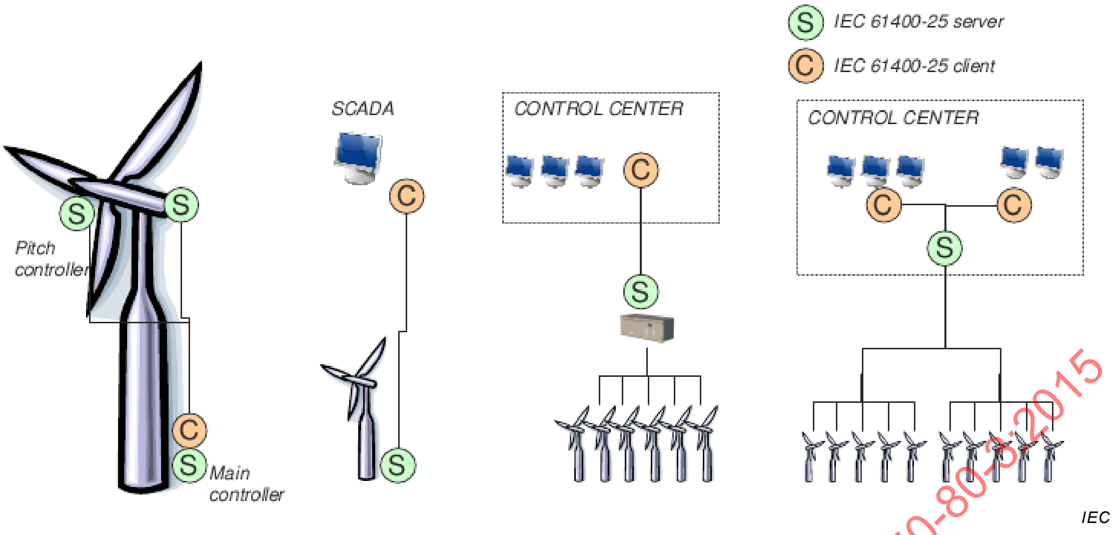


Figure A.5 – Examples of the variety of topologies required/supported for wind power

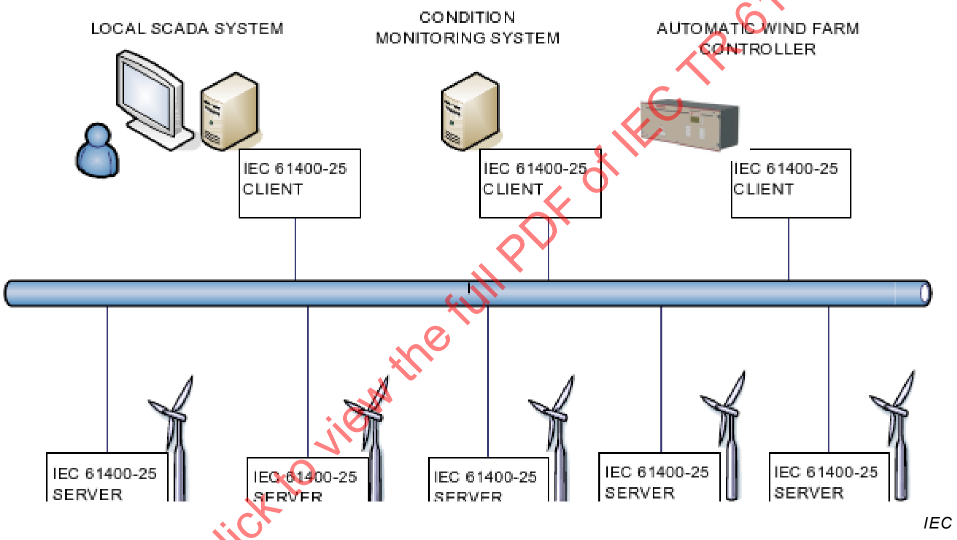


Figure A.6 – Example of use within the wind plant

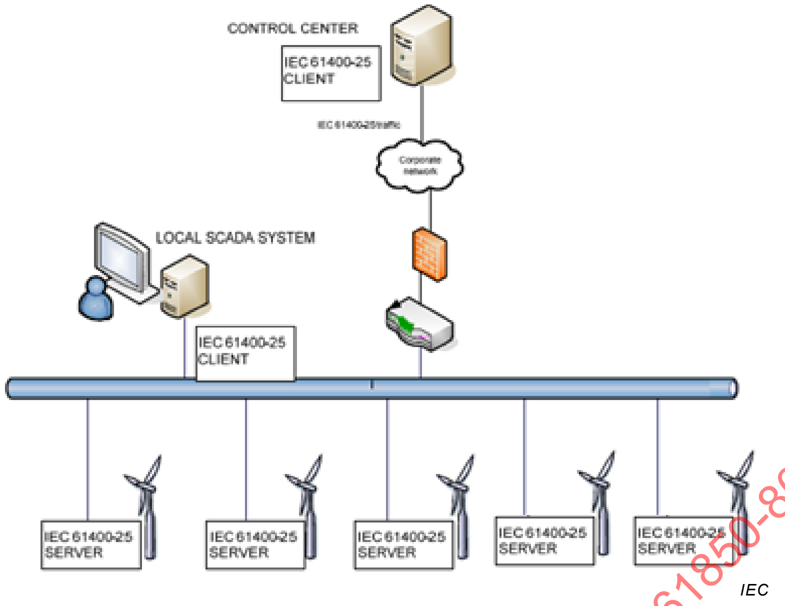


Figure A.7 – Example of use between the wind plant and a control center

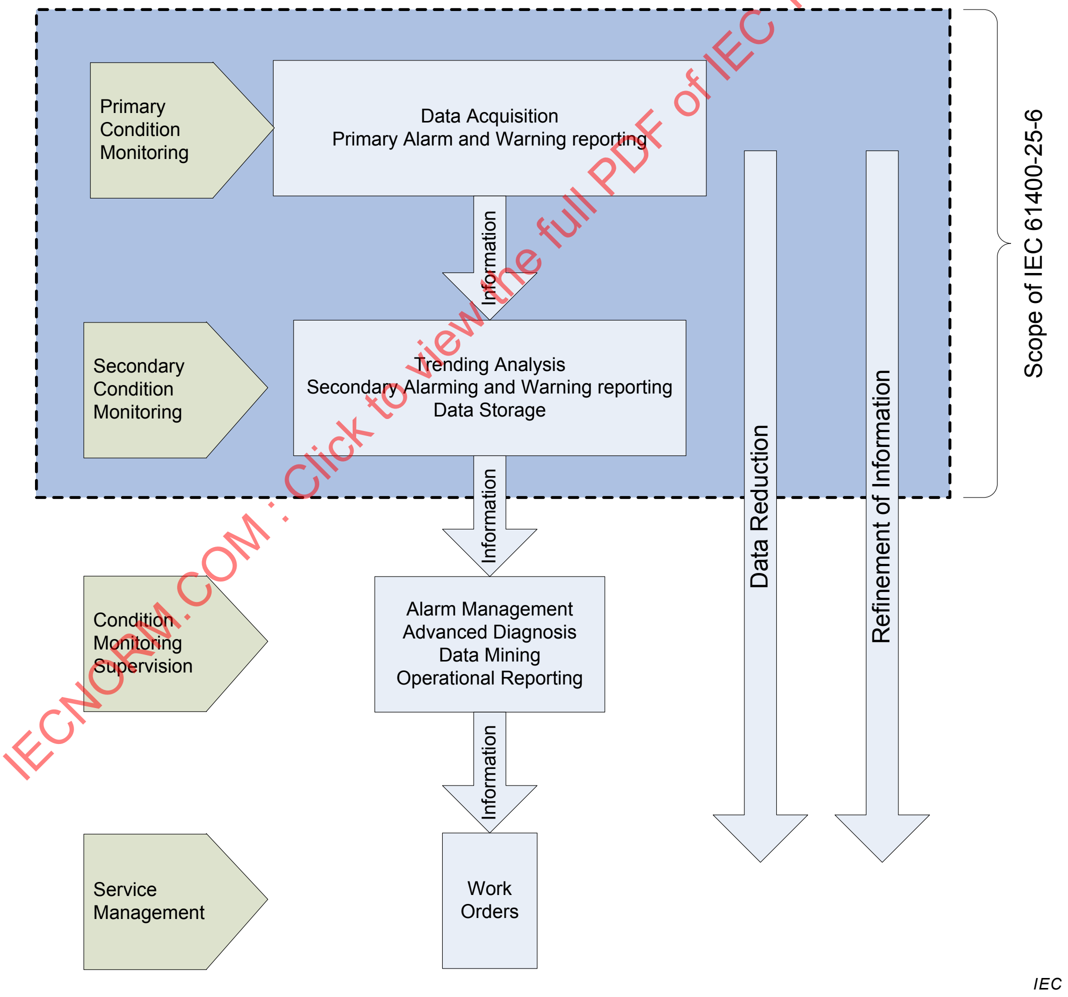


Figure A.8 – Diagram of data use hierarchy levels in condition monitoring

A.3.3 Use cases

The use cases definition presented in Table A.4 requires the identification of typical actors. Elements described in Table A.3 are examples of actors from the 61400-25 communication viewpoint.

Table A.3 – Wind – List of actors

Actor name	Description	Client	Server
Local device server (see DER Local Server in Table 1)	A processing and control unit able to communicate as a 61400-25 server. For example: Turbine controller, Pitch controller, Meteorological sensor		X
Local controller (see DER Unit control in Table 1)	A processing and control unit able to communicate as a 61400-25 client to lower level devices and a server to higher level systems. Examples: controller for a turbine and its associated equipment, controller for a wind plant collector..	X	X
Local SCADA system	A SCADA system for the wind plant. Can act as a client for servers in the wind plant and a server for higher level systems	X	X
Company control center (see DER Management System in Table 1)	A control center for wind plants owned or managed by a company. This control center may interface with the grid operations control center.	X	X
Grid operations control center (see TSO in Table 1)	The control center of the grid operator.	X	
Primary Condition Monitoring system	Sensing devices for collecting condition monitoring information		X
Secondary Condition Monitoring system	Processing devices that receive primary condition monitoring information, perform processing of the information, and pass the results to higher levels	X	X
Condition monitoring center	A facility that receives information from the secondary condition monitoring level, performs further analysis, and determines if action needs to be taken.	X	X
Maintenance center (see Plant maintenance in Table 1)	A facility that monitors equipment in wind plants of one or more companies and dispatches maintainers if needed.	X	X
Business/market administrator (see Market operator in Table 1)	An entity that receives requirements from grid operations, conducts market operations to satisfy those requirements, receives reports on the satisfaction of market commitments, and supports means for related financial settlement.	X	X
Engineering planning and analysis facility	Facility that performs engineering planning and post-disturbance analysis	X	
Software maintenance facility	Facility that maintains software for wind plants	X	X
Weather forecast facility	Facility that receives meteorological data and provides weather forecasts	X	
Company cybersecurity management facility	Manages access control and cybersecurity reporting parameters. Receives reports. Takes action where required	X	

Table A.4 – Wind – Use case list

	Use case name	Description	Actors
1	Wind plant local monitoring and control	Local SCADA communicates with wind plant devices (turbines, turbine-associated equipment, collector-associated equipment, etc.), possibly through intermediate hierarchical actors, for local control.	Local device server Local controller Local SCADA system
2	Wind plant condition monitoring and alarming	Multi-level flow of information in which primary condition monitoring functions provide data to secondary condition monitoring functions that perform analyses and provide results to condition monitoring supervisory functions that perform higher-level analyses, manage maintenance, and provide reports to relevant corporate and grid control/management facilities	Primary Condition Monitoring system Secondary Condition Monitoring system Condition monitoring center Maintenance center Grid operations control center
3	Wind plant organizational monitoring and control	Organizational control center communicates with one or more wind plants owned/controlled by organization. Information exchanged and managed is as determined by organization. Control center may serve as interface to grid control and grid business/market functions.	Local device server Local controller Local SCADA system Company control center
4	Grid control of wind plants	Transmission and/or distribution operator communicates with wind plants in its service territory to perform such functions as may be assigned for technical and reliability purposes.	Local SCADA system Company control center Grid operations control center
5	Business/market administration of wind plant production	Business/market administrator communicates with either wind plant local control or wind plant organizational control to exchange information regarding wind plant production, prospective market activities, and settlement for past market activities.	Business/market administrator Company control center Local SCADA system
6	Weather forecasting	Meteorological tower at wind plant provides sensor data to weather forecaster(s). Forecasts are provided to wind plant local control or wind plant organizational control to assist in determinations regarding wind plant production, market activity, and safety/reliability considerations.	Weather forecast facility Local device server Local controller Local SCADA system Company control center Grid operations control center
7	Event, report, alarm, and log management	Events are captured at devices based on pre-defined criteria. They then become reports, alarms, or logs. They may be received and summarized at a higher level and made available in an aggregated form to yet higher levels.	Local device server Local controller Local SCADA system Company control center Grid operations control center Primary Condition Monitoring system Secondary Condition Monitoring system Condition monitoring center Maintenance center

	Use case name	Description	Actors
8	Post-disturbance analysis	Following a disturbance, a high level actor retrieves relevant information and performs analyses to reconstruct the sequence of events and determine any necessary maintenance or system changes.	Local device server Local controller Local SCADA system Company control center Grid operations control center Primary condition monitoring system Secondary condition monitoring system Condition monitoring center Maintenance center Engineering planning and analysis facility
9	Settings and configuration management	Perform process to determine settings of devices and other equipment/systems. Install settings in devices, equipment, and systems. Check to ensure that correct settings are installed.	Local device server Local controller Local SCADA system Company control center Maintenance center Company cybersecurity management facility
10	Cybersecurity management	Perform process to determine access controls and other cybersecurity parameters. Establish and configure access controls and other cybersecurity parameters. Receive reports on cybersecurity events/conditions and take appropriate actions.	Company cybersecurity management facility Local device server Local controller Local SCADA system Company control center Maintenance center
11	System planning	Perform analyses and simulations to prepare operational plans, determine changes in design of wind plants and other related facilities, and perform other engineering planning functions. Use information from system operation and event logs to aid in performing planning activities.	Engineering planning and analysis facility Local SCADA system Company control center Maintenance center Condition monitoring center
12	Communications network management	Manage the communications network supporting wind plant communications and the other use cases.	Local SCADA system Company control center Maintenance center Condition monitoring center
13	Time synchronization management	Manage clocks that support time stamps for operational data and reports/logs/alarms.	Local device server Local controller Local SCADA system Company control center Maintenance center

	Use case name	Description	Actors
14	Equipment and system test and maintenance	Perform tests and checks on operation of equipment and systems. Manage maintenance of equipment and systems. Use information from condition monitoring, and system operation and event logs to aid in performing maintenance activities.	Local device server Local controller Local SCADA system Company control center Condition monitoring center Maintenance center Engineering planning and analysis facility
15	Software management	Includes software maintenance, receiving and testing changes, software configuration management, and software installation.	Local device server Local controller Local SCADA system Company control center Maintenance center Software maintenance facility

A.4 Use cases for CHP

A.4.1 Scope of this clause

This clause addresses the requirements of distributed combined heat and power (CHP) units in terms of a Web based communication.

Figure A.9 presents the types of CHP plants that are considered in this document. They differ in their power generation technology which leads to distinct plant characteristics concerning electrical power, efficiency, start-up time, etc.

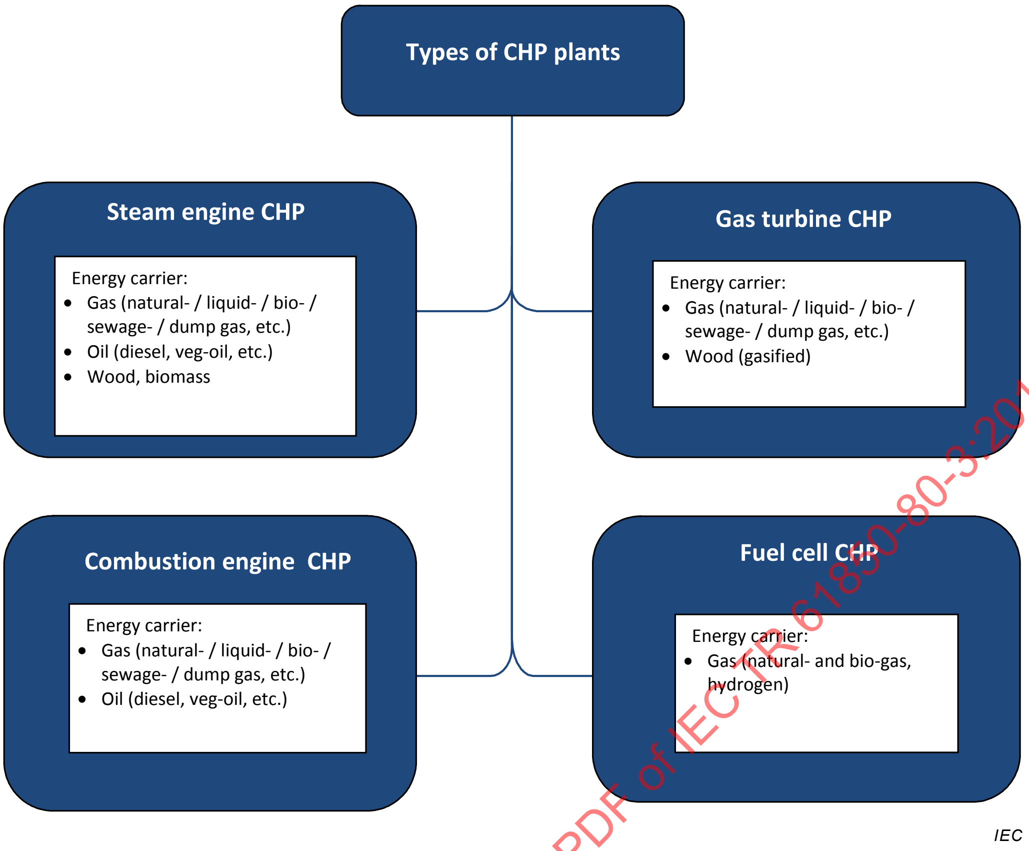

Types of CHP plants
Steam engine CHP
Energy carrier:
Gas (natural- / liquid- / bio- / sewage- / dump gas, etc.)
Oil (diesel, veg-oil, etc.)
Wood, biomass
Gas turbine CHP
Energy carrier:
Gas (natural- / liquid- / bio- / sewage- / dump gas, etc.)
Wood (gasified)
Combustion engine CHP
Energy carrier:
Gas (natural- / liquid- / bio- / sewage- / dump gas, etc.)
Oil (diesel, veg-oil, etc.)
Fuel cell CHP
Energy carrier:
Gas (natural- and bio-gas, hydrogen)
IEC

Figure A.9 – Types of CHP plants

A.4.2 Architecture overview

Figure A.10 shows an example of a system architecture. It should be noted that smaller CHPs are directly connected to the low-voltage grid instead of being connected via a transformer to a higher voltage grid level.

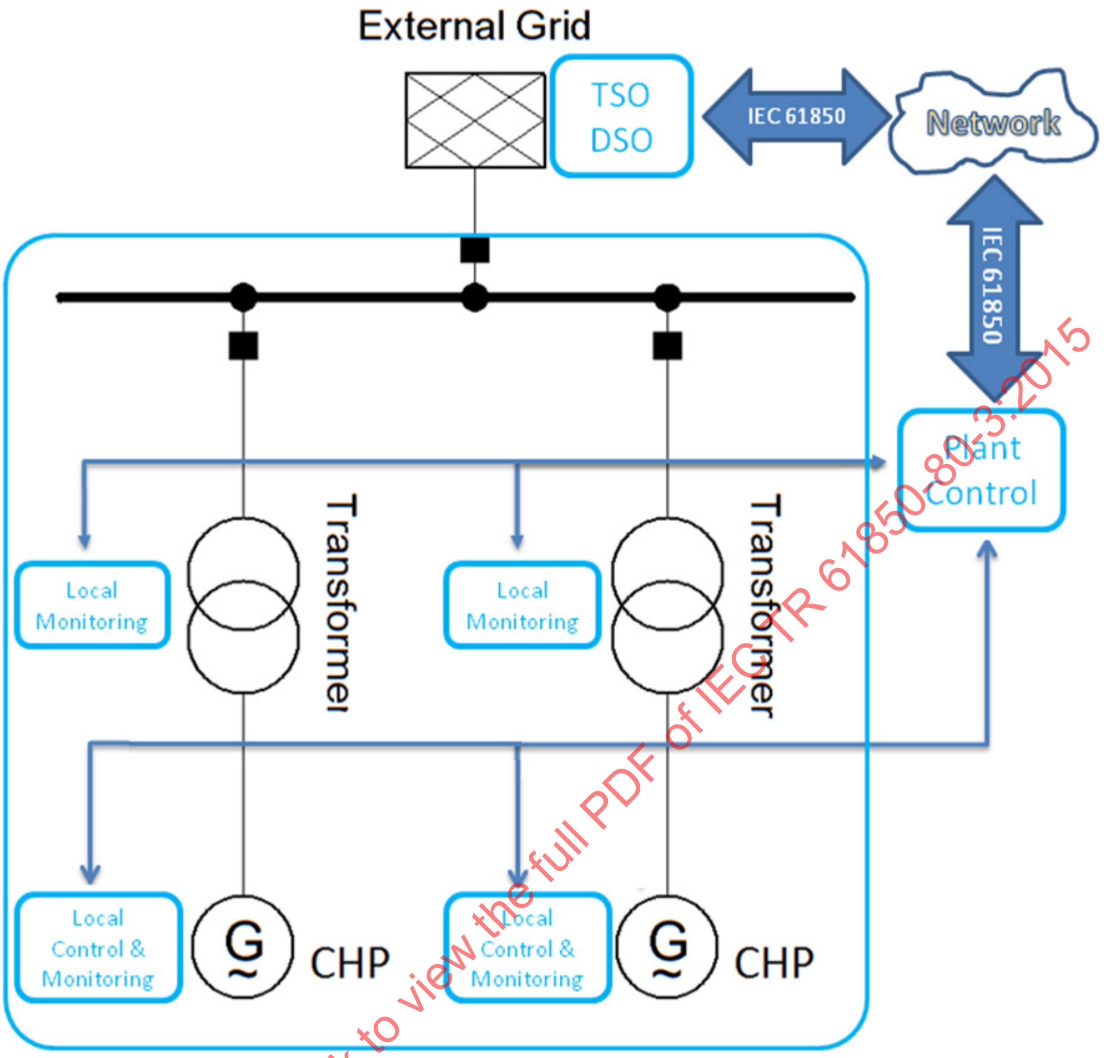


Figure A.10 – CHP – Example of a system architecture

Elements involved in the use cases

Figure A.12 shows the CHP actors and the use cases they are involved in. In the center the Combined Heat and Power (CHP) plant **with its standardized interface** is located and the actors accessing **the standardized interface of** the CHP plant are grouped around.

It should be noted, however, that there are CHP concepts and operational states for which an external control is not possible or reasonable and for which consequently the actors shown in Figure A.12 do not have access to the standardized interface of the CHP plant. If for example a CHP is heat-production driven it is not available for the electricity market.

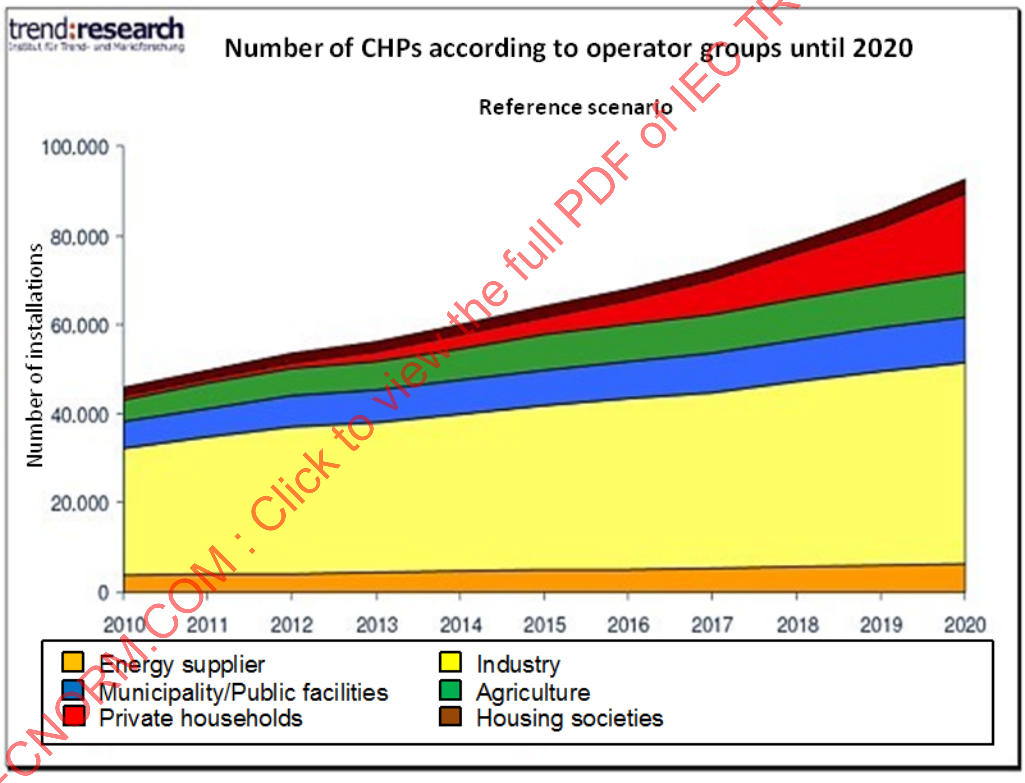
The following actors have been identified for the use cases listed in A.4.3 and are roughly described:

- System operator (SO) – means either a distribution system operator (DSO) or a transmission system operator (TSO).
- Virtual Power Plant (VPP) aggregator – means any natural or legal person responsible for aggregating DERs to Virtual Power Plants. In some cases the VPP aggregator might be identical with the CHP plant operator.

- CHP plant manufacturer – means the manufacturer of the CHP plant.
- CHP plant operator – means any natural or legal person operating a CHP plant (often this is either the CHP plant owner or the SO).
- CHP plant owner – means any natural or legal entity owning a CHP plant as a power generating facility.
- CHP service provider (or Plant maintenance, see Table 1) – means any natural or legal person responsible for the maintenance of the CHP. Often this service is provided by the CHP manufacturer but it could also be another entity such as a maintenance provider, e.g. a heating installer.

Scalability and dynamic extension of the system

In medium-voltage and low-voltage systems a large number of CHP plants is already integrated. In future, the number of CHP plants is expected to rise significantly. For example, in 2010 about 6 000 CHP modules were produced for the German market [Energie&Management]. A German study [trend:research] showed that the number of CHPs on the German market is expected to grow from roughly 45 000 CHP plants in 2010 to over 80 000 CHP plants in 2020 (see Figure A.11).



Source: trend:research

Figure A.11 – Number of CHPs in Germany

For dynamic extension of the system a “Registry” is suggested. The Registry is used by distributed energy resources (DER) in order to register and deregister and by the VPP aggregator to obtain a list of URIs of those DERs that are connected to the grid and are principally available for monitoring and control.

As the Registry does not act on its own it is not depicted as an actor in Figure A.12.

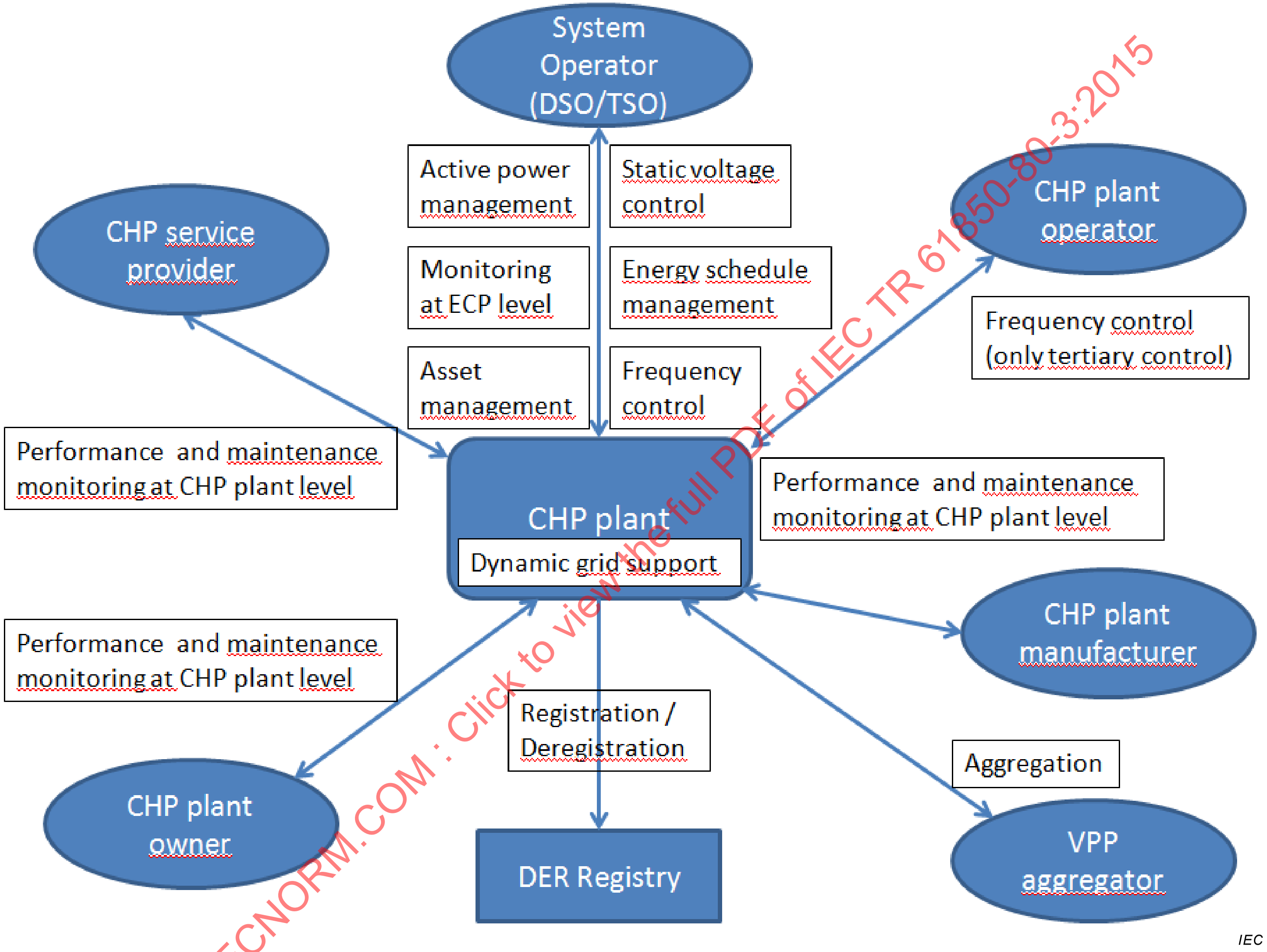

System Operator (DSO/TSO)
Active power management
Static voltage control
Monitoring at ECP level
Energy schedule management
Asset management
Frequency control
CHP service provider
CHP plant operator
Frequency control (only tertiary control)
Performance and maintenance monitoring at CHP plant level
CHP plant
Dynamic grid support
Performance and maintenance monitoring at CHP plant level
Performance and maintenance monitoring at CHP plant level
CHP plant manufacturer
Registration / Deregistration
Aggregation
CHP plant owner
DER Registry
VPP aggregator
IEC

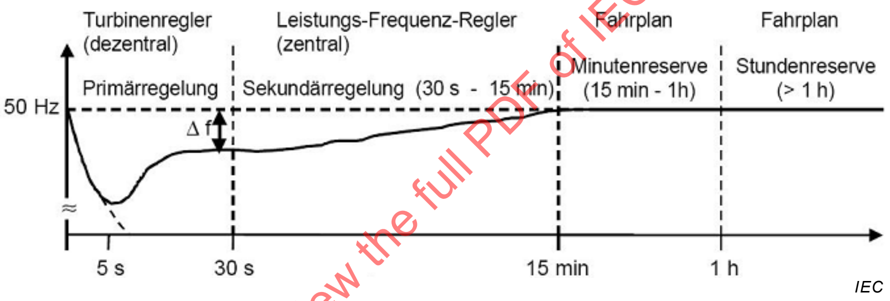
Figure A.12 – CHP use cases and involved actors

A.4.3 Use cases

NOTE In Tables A.5 and A.6, the references to ENTSO-E or country specific requirements are only examples. They do not restrict the general description of the use cases.

Table A.5 – CHP – Use case list

#	Use case name	Description	Actors
1	Voltage control (reactive power management)	Power generating units shall be able to participate in voltage control both in static voltage control and in dynamic grid support. Static voltage control: Static voltage control means voltage control in the MV power system ***under normal operation*** with the aim of keeping slow voltage changes within agreeable limits. Power generating plants shall be able to participate in static voltage control, that is they shall be able to provide reactive power in each operating point according to a given displacement factor cosφ at the electrical connection point. During active power output the **system operator (SO)** sets a fixed reactive power set point or sets a reactive power set point adjustable by a remote control system. The set point may be either a fixed displacement factor cosφ, a variable displacement factor cosφ(P), a fixed reactive power value in MVar or a reactive power-/voltage-characteristic Q(U). If the system operator provides a characteristic, each value of this characteristic has to be automatically set within a given time (e.g. 10 seconds for the cosφ(P)-characteristic and within 10 seconds to 1 minute for the Q(U)-characteristic). The set point can be carried out by agreement of a value / schedule or by online set point setting Dynamic grid support: Dynamic grid support describes the necessity of voltage stability during voltage drops in the overlaying high-and extra-high voltage system – that is ***in fault situations*** – in order to prevent unintentional switch-offs of high energy supplies and with it system collapses. Dynamic grid support is often referred to as Fault-Ride-Through (FRT). Due to an increasing penetration of decentralized energy generators in the MV- and LV-grid, it becomes necessary that these plants participate in dynamic grid support. Therefore, in case of short circuits, power generating plants shall be able • to stay connected during a fault, • to support the voltage by providing reactive power during a fault and • not to consume more inductive reactive power after the fault clearance than before **Dynamic grid support is a feature that is incorporated within the CHP plant controller. No communication between the CHP plant and an external actor is required.**	System Operator (DSO/TSO)

#	Use case name	Description	Actors
2	Frequency control	Frequency control means the provision of reserve energy and balancing power in the case of **frequency violations**. It comprises primary energy control, secondary energy control and tertiary energy control and is described in more detail in the following example reflecting the frequency control measures of ENTSO-E (see also Figure A.13 and Figure A.14). a) System failure b) Primary control c) Secondary control d) Tertiary control **Figure A.13 – CHP – Graphical presentation of frequency control within the European power system**  **Figure A.14 – CHP – Frequency control time characteristic** Primary control: The aim of primary control is to reconstitute the balance between generated and consumed power with the help of the turbine speed controller. Failures cause a frequency deviation upon which the primary control reacts and keeps it within defined secure limits. In Europe, all **system operators (SO)** participate in primary control according to a participation coefficient defined by ENTSO-E. DERs providing primary control energy shall meet the conditions defined. E.g. in Germany the following conditions are defined according to the Transmission Code [Transmission Code 2007]: • At least ± 2 % of the rated power shall be available within 30 s; • the power shall be provided up to 15 minutes for frequency deviations of at least ± 200 mHz; • the frequency-energy efficiency ratio defined by the grid operator shall be adjustable.	System Operator (DSO/TSO), CHP operator
		Power stations participating in primary control ***automatically*** provide their primary control energy when the internal control unit detects a frequency drop. Up to now, **no communication between the CHP plant and an external actor is required. It might become necessary in future, though, considering islanded networks in which one DER is assigned the role of a primary controller in case of frequency violations.** Due to their quick-start capability CHPs are suited for providing reserve- or balancing energy. Although CHPs are built for powers lower than those necessary for participating in primary control (in Germany: 100 MWel) CHP modules or CHPs aggregated within Virtual Power Plants (VPP) can very well be used for primary control.	

#	Use case name	Description	Actors
		Secondary control: After a failure and a successful frequency stabilization of the primary control there is still a frequency deviation. This imbalance is eliminated by the application of secondary control. Secondary control both reduces the frequency to its nominal value and replaces the primary control. The power that has been provided by other SOs during primary control is replaced with the secondary control power provided by power plants within the faulty control area so that the power provided by SOs outside the faulty control area is again available for primary control. Each **SO** has a central controller that triggers the secondary control power at the various suppliers. Secondary control energy shall be provided within a time interval of 30 s to 15 min. Tertiary control: Tertiary control is applied when secondary control power is not sufficient to eliminate the failure when a longer failure is existent. In order to balance load imbalances the power stations shall be able to temporary change their power with a gradient of at least 2 % of their nominal power per minute. Tertiary control energy shall be provided within a time interval (e.g. in Germany: 15 min to 1 h).	
3	Active power manage-ment (Active power reduction)	The generating plant shall be able to be operated with *reduced active power output* [ENTSO-E DNC], [BDEW MVG]. In the following cases the **system operator (SO)** is allowed to temporarily limit the feed-in power or to switch-off the plant: • Potential risk of unsafe system operation, • bottlenecks resp. risk of overload in the system operator's system, • risk of unwanted islanding, • risk of static or dynamic system instability, • system-endangering frequency rise, • maintenance resp. building activities and • in the context of production management, feed-in management and system security management. Generating plants shall be capable of reducing their active power in reduction steps of a defined percentage (e.g. in Germany: 10 %) of the agreed connection power P_{AV}. This power reduction shall be possible in any operational state and from any operating point to a *set point given by the system operator*. This set point usually is set *at the electrical connection point* and corresponds to a value in percent related to the agreed connection power P_{AV}. The reduction of the active power output to the given set point shall not necessarily happen immediately but at least within a given time frame (e.g. in Germany: 1 minute). All operating generating units have to reduce their current active power output when the system frequency exceeds a defined deviation from the nominal system frequency (e.g. in Germany: 50,2 Hz). The active power has to be reduced with a defined gradient (e.g. in Germany: 40 %/Hz) of the instantaneously available power. The active power is only allowed to be increased again when the frequency reaches a defined value (e.g. in Germany:f ≤ 50,05 Hz). Above certain frequency limits and below certain frequency limits (e.g. in Germany: above 51,5 Hz and below 47,5 Hz) the plant has to disconnect. E.g. according to § 6 of the German EEG 2009 – a law for renewable energy resources – DER operators with DER powers higher than 100 kW are obliged to allow for the following facilities accessible for the **system operator**: • a remote-controlled reduction of the fed-in power (with a velocity of 10 % of the nominal power per minute for DERs in the MV system and a complete switch-off of DERs in the LV system) and • retrieval of the actual feed-in power value.	System Operator (DSO/TSO)

#	Use case name	Description	Actors
4	Energy schedule management (Demand Response)	Based on forecasts the **system operator (SO)** issues for example generating unit schedules with the aim of balancing generation and consumption. For the energy schedule management, the system operator (SO) provides a schedule to a CHP, indicating the points in time when a defined amount of power needs to be fed in. Issuing energy schedules is usually done every 15 minutes, on an hourly basis or a daily basis. The Plant Operator and/or VPP Aggregator controls the scheduling of associated generating units, e.g. in order to enable the trading of the generated energy or to meet demands of control energy. In these cases, these actors plan ahead the energy generation of a set of generating units and require means to allocate schedules to individual units. These schedules are expected to originate from ICT-Systems and are then forwarded to the generating units. Based on the scheduled profile of an energy schedule requested by a SO or a VPP aggregator the CHP can either send back the actual profile of the energy schedule to the SO or the VPP operator the SO or VPP aggregator can request the actual energy schedule from the CHP. By means of energy schedules active power management as well as the reactive power management required by national guidelines and laws can be realized.	System Operator (DSO/TSO), CHP operator, VPP Aggregator
5	Asset management	System operators conduct asset management in order to • minimize their total cost while guaranteeing an adequate quality of supply and • deduce optimal strategies for maintenance, reinvestment and fault clearance • have a detailed description of the assets (e.g. GIS data and system characteristics). Indispensible for asset management is access to the data of the assets, in this case the CHP plants, e.g. in order to monitor their performance and being able to detect critical CHP states (based on warnings or alarms issued on basis of predefined criteria). In the case of critical CHP states the asset manager can take measures for apt maintenance strategies in time in order to avoid severe damage of the CHP plant.	System Operator (DSO/TSO)
6	Monitoring power system relevant parameters at the ECP	Monitoring relevant power system parameters (e.g. fed-in energy, mode of operation, authorization details) at the ECP is essential for the relevant **system operator** in order to enable a safe and secure operation of the network. E.g. system operators in their control centers might be interested in monitoring potential system restoration of CHP plants after a black-out.	System Operator (DSO/TSO)
7	Performance and maintenance monitoring (including operational alarms)	Both the **CHP owner and the CHP operator** might be interested in monitoring the performance of their CHP unit while not being physically available at the CHP plant site. For example, in the case of incoming warnings or alarms the CHP owner / operator can notify a maintenance company. Also the **CHP service provider** should be able to monitor CHP plant data in order to provide the necessary maintenance service. A CHP service provider shall be able recognize if a maintenance activity can be performed. For example, when a VPP ask a CHP to participate in tertiary control no maintenance activities are allowed. In contrast to UC 5 (Asset Management) this UC also implies monitoring of non-electrical data, such as data of assets related to thermal energy generation (e.g. pumps).	CHP owner, CHP operator, CHP service provider, CHP plant manufacturer

#	Use case name	Description	Actors
8	System restoration	System restoration comprises black start capability, the capability of taking part in Island Operation and quick re-synchronization capability [ENTSO-E DNC]. a) Black Start Capability Black start capability means that a CHP is capable of black start within its own system and that it is able to synchronize with the superposed system when it is back to normal operation. A CHP with black start capability shall be able to start from shut down within a timeframe decided by the relevant **system operator** in coordination with the relevant TSO without any external energy supply. The CHP shall be able to energize part of the network upon instruction from the relevant system operator and shall be able to synchronize with the grid within defined frequency limits and voltage limits. That is, in case of a black-out the system shall be capable to provide a sequence of steps in order to restore system capability. The voltage regulation shall be enabled to ensure that load connections causing dips of voltage are automatically regulated. b) Capability of taking part in Island Operation If required by the relevant system operator in coordination with the relevant TSO it shall be possible for the CHP to take part in Island Operation within the frequency limits defined and the voltage limits decided by the relevant system operator. Besides, the CHP should be able to operate in FSM (Frequency Sensitive Mode). In case of a power surplus, it shall be possible to reduce the loading of the CHP plant from its previous operating point preventing the disconnection of the CHP plant from the island due to overfrequency. c) Quick re-synchronization capability This feature is required in case of disconnection of the CHP plant from the network in line with the protection strategy usually agreed between the relevant system operator and the CHP owner in the event of disturbances to the system. **Most of this feature is incorporated within the CHP plant. Depending on the system requirements, communication between the CHP plant and an external actor might be required or not. A case requiring communication between the CHP and the system operator is when the system operator needs to selectively switch on a CHP.**	System Operator (DSO/TSO)

Table A.6 – CHP – Other use cases not feasible with existing ACSI

Use case name	Description	Actors
Registration / Deregistration	CHPs register themselves with their URI or IP-address at a **registry** as soon as they are up and running. Then they can automatically be detected by interested energy market participants such as DER aggregators and be accessed via their URI or IP-address for detailed DER information. A CHP deregisters itself only when it is completely taken out of the power system, e.g. because it is replaced by a bigger CHP. In case of maintenance the CHP keeps being registered in the registry as for an aggregator it is not only interesting to see operating CHPs but all CHPs connected to the grid. E.g. a CHP currently being in maintenance might be available some hours later and then be available for aggregation and control, which is a worthful information for an aggregator obliged to fulfill energy schedules for a given time frame.	DER Registry
Aggregation	While a single CHP usually cannot participate in the energy market as it does not meet the requirements in terms of minimum power defined for DERs participating in the energy market, an aggregation of CHPs in contrast can do so. Therefore, a virtual power plant aggregator (**VPP aggregator**) shall be able to communicate with CHPs in order to set up a virtual power plant out of locally distributed CHPs. E.g. negative control energy (e.g. in case of rising frequency) can be provided by collectively switching off CHP units aggregated within a virtual power plant. Especially CHPs which need not continuously provide thermal energy are apt for this scenario. NOTE See also A.7, *Use cases for VPP and Microgrid*	VPP Aggregator

A.4.4 References for CHP domain

[BDEW MVG] BDEW: Technical Guideline for generating units in the medium-voltage system (Technische Richtlinie Erzeugungsanlagen am Mittelspannungsnetz), June 2008

[ENTSO-E DNC] ENTSO-E Draft Network Code for Requirements for Grid Connection applicable to all Generators

[MS Stadler] Stefanie Stadler: Master Thesis “Integration of decentralized generating units and storages in a Smart Grid using the standard IEC 61850” conducted at FGH e.V. in 2012

[Energie&Management] Energie & Management Magazine, 15 November 2011, p. 17 – 21

[TransmissionCode 2007] TransmissionCode 2007 – Grid and System guidelines of the German TSOs, Version 1.1, August 2007

[trend:research] http://www.energie-und-technik.de/erneuerbare-energien/produkte/alternative-energien/article/79902/0/BHKW-Markt_waechst_um_15_Prozent/

A.5 Use cases of domain Smart Customer (DR)

A.5.1 Scope of this clause

The smart customer domain describes the interaction of customers with the grid operator and one or more energy retailer (trader, energy service provider, etc.). Figure A.15 shows the main actors of this domain.

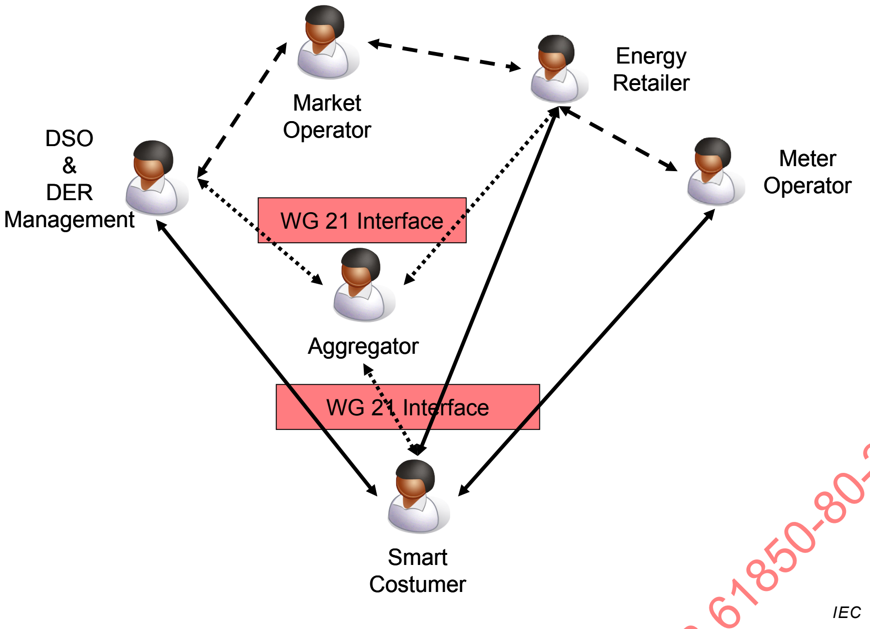


Figure A.15 – Smart customer – Main actors

The smart customer dynamically acts upon incentives and contracts with the grid operator and one or many energy retailers according his needs. His target is to optimize his own processes and financials.

Smart customers are connected to the market and to grid operators to contribute to and profit from demand response. The customers may be consumers and / or producers of electrical energy.

There may be also an indirect integration of smart customers via aggregators.

Connecting industry premises, buildings and homes there will be millions of customers.

The customers may be connected to one or more partner (e.g. DSO, energy retailer).

A.5.2 Architecture overview

Figure A.16 shows the main elements of the Smart Customer domain in the SG reference architecture model.

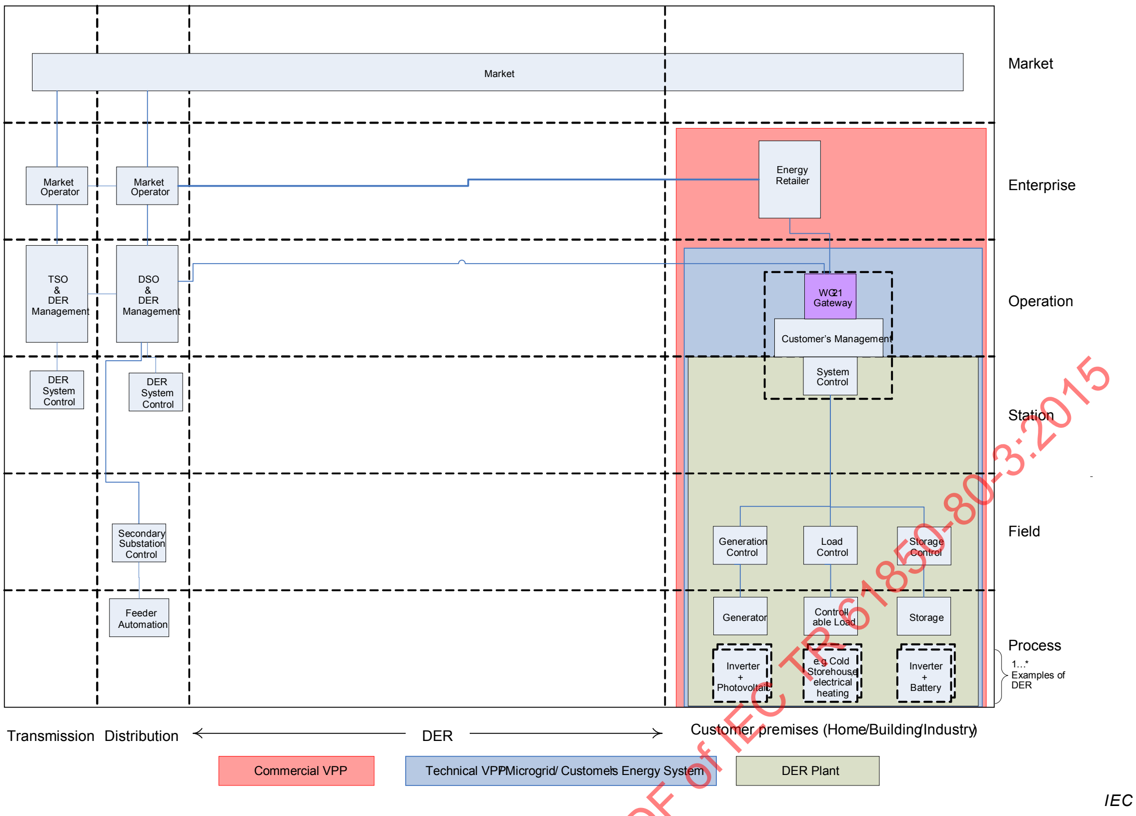


Figure A.16 – Smart customer – Main elements of the smart customer domain (right column)

Figure A.17 shows a high level abstraction of the customer premises as seen from the grid. How much is visible to the grid depends on the contracts between the smart costumer and the other participants.

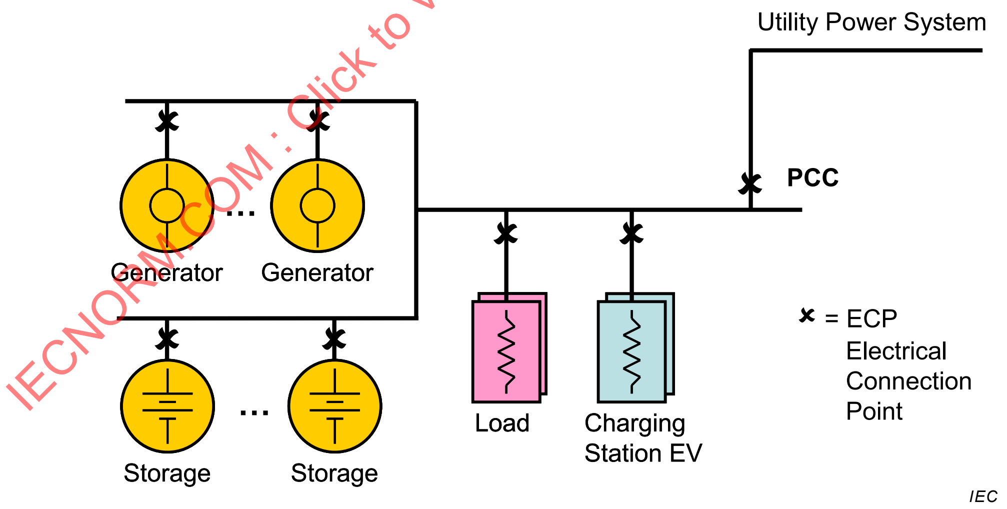


Figure A.17 – Smart customer – Logical model for customer premises communications

The communication relationships are hierarchical. The characteristics are:

- Internet-based communications:
  - Utility/Market to customer
  - Utility/market to service provider/aggregator
  - Aggregator to customer

- Support for ‘push’ communications
- Security is key:
  - Need to avoid opening customer firewalls to allow for inbound connections
  - Need trusted identities for devices

Relationship between actors

- For the purposes of DR markets, it also must be recognized that there may be multiple ‘tiers’, as in the case of wholesale and retail markets
- Some participants may play in more than one market or have other business relationships, as might be the case between aggregators
- Fundamentally, the roles and relationships are hierarchical

Figure A.18 shows the communication relationships between actors.

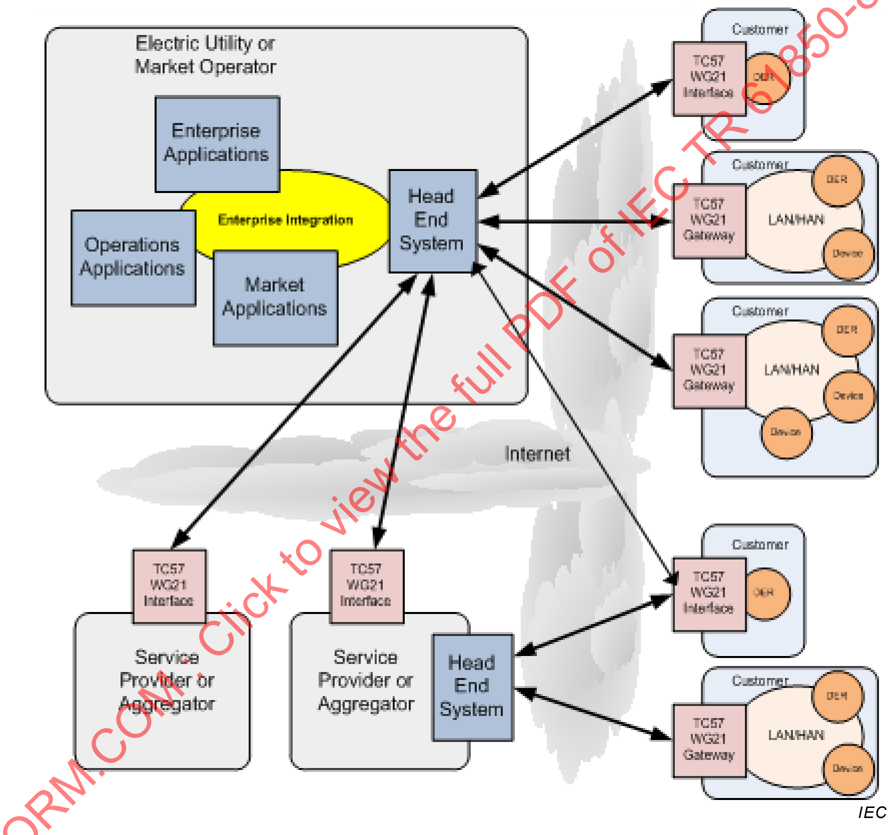


Figure A.18 – Smart customer – Communication relationships

A.5.3 Use cases

In order to show the use cases it is necessary to know which actors are in. The most relevant actors are listed as follows:

- (Smart) customer
- Retailer, Energy Service Provider (ESP) incl. EV charging, supplier, aggregator
- Grid operator, Distribution System Operator (DSO)
- Market operator
- Meter operator

Table A.7 and Table A.8 describe the main use cases of the smart customer domain.

Table A.7 – Smart customer – Use case list

#	Use case name	Description	Actors
1	Configuration/Capability status report	The smart customer reports which features or devices are available or disabled. This includes generation or storage or load capabilities, e.g. operations reserve, Volt-VAr, storage capacity etc.	Customer, Retailer, Grid operator
2	Validation of contracts	The grid operator and / or retailer validates the published features of the smart customer against the contracts	Customer, Retailer, Grid operator
3	The smart customer acts on tariffs	Under agreed commercial conditions, the smart customer receives a schedule for tariffs from the retailer and acts according his own optimization	Customer, Retailer
4	The smart customer acts on schedule for ancillary services	Under agreed commercial conditions, the smart customer receives a schedule for ancillary services from the grid operator and acts according to the contract and his own optimization	Customer, Grid operator
5	Load shedding	The smart customer receives signals from the grid operator and acts according to the given contracts	Customer, Grid operator
6	Emergency signal	The smart customer brings his processes in a safe state to minimize the damage in case of black out	Customer, Grid operator
7	Status check of smart customer	The grid operator and / or retailer verify that the smart customer can be contacted and is active	Customer, Retailer, Grid operator
8	Changing business models / contracts	The grid operator and / or retailer validate that the smart customer can fulfill changed contracts	Customer, Retailer, Grid operator
9	Providing forecasts	The smart customer sends forecasts to the grid operator and / or retailer	Customer, Retailer, Grid operator
10	Smart customer gets history	The smart customer gets historical data from the grid operator and / or retailer	Customer, Retailer, Grid operator
11	Smart customer provides history	The smart customer sends historical data to the grid operator and / or retailer	Customer, Retailer, Grid operator

Table A.8 – Smart customer – Other use cases not feasible with existing ACSI

Use case name	Description
Certificate update	The certificate of the smart customer is updated
Certificate installation	The certificate of the smart customer is installed
Authentication with Authorization from secondary actors	Authentication is done with an additional authorization from a third party (e-car loading station)
Identification with validation from the secondary actor	Identification is done with an additional authorization from a third party (e-car loading station)
Preserving communication security	The smart customer initiates the communication to avoid opening ports to the WAN.
Update of registration certificate	The smart customer updates his reference to the registration server
Withdraw certificate	The smart customer deletes certificates from his trust list
Change of retailer	The smart customer changes to one or more other retailers
EV charging station	An eCar is charged at the EV charging station in the smart customer premises. The third party is identified. The charging is authorized and booked.
Publication of customer premises	The smart customer publishes its features to a registration server.
Subscription of grid operator or retailer	The grid operator or retailer subscribes to a service published by a smart customer. The customer grants access based on the role and on contracts.

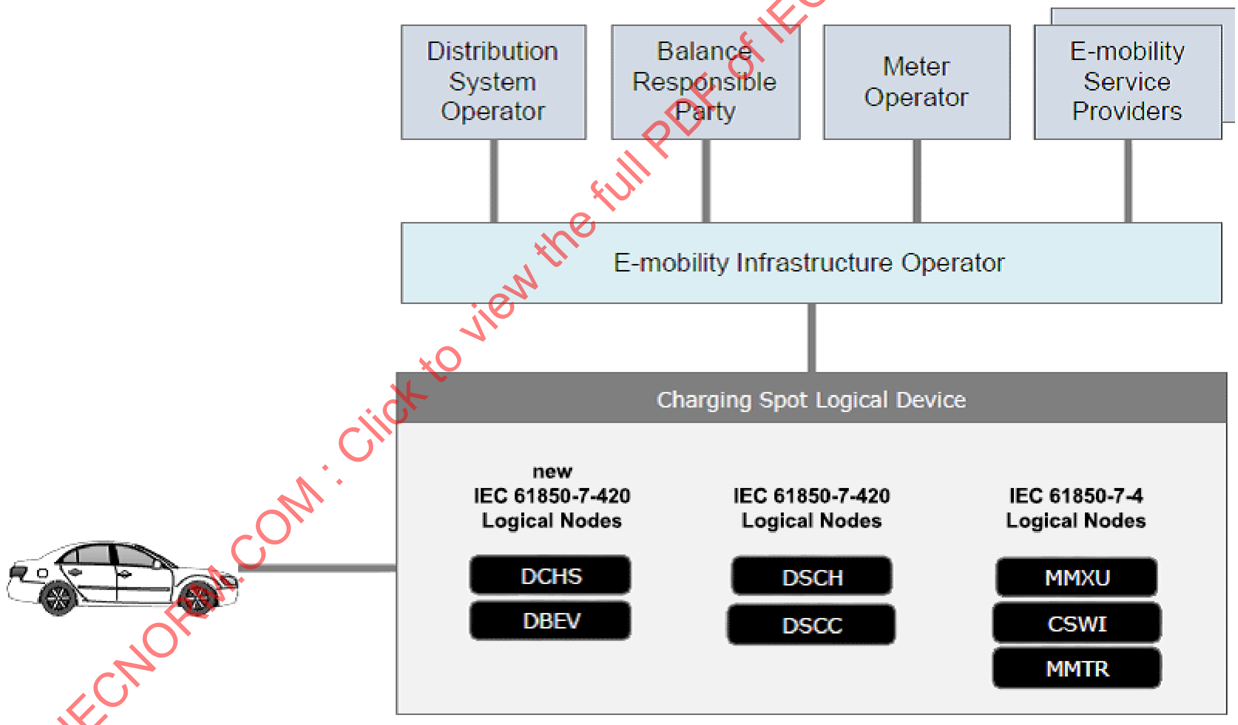
Use case name	Description
Identification of smart customer	The smart customer identifies himself to the grid operator or retailer including credentials
Change of published information	The smart customer updates the features which were published
Replacement of faulty device	A faulty device is replaced at the smart customer site including update of credentials and identification code
Update of smart customer interface or devices at customer site	The smart customer interface or devices are updated, e.g. firmware, by a management authority

A.6 Use cases for E-Mobility

A.6.1 Scope of this clause

E-mobility domain concerns the Electric Vehicle and the Supply Equipment for delivering energy to the vehicle and for other interactions between the EV (Electric Vehicle), EVSE (Electric Vehicle Supply Equipment) and Secondary Actors (DSO, BRP, MO, Service provider). See Figure A.19.

A.6.2 Architecture overview


Distribution System Operator
Balance Responsible Party
Meter Operator
E-mobility Service Providers
E-mobility Infrastructure Operator
Charging Spot Logical Device
new IEC 61850-7-420 Logical Nodes
DCHS
DBEV
IEC 61850-7-420 Logical Nodes
DSCH
DSCC
IEC 61850-7-4 Logical Nodes
MMXU
CSWI
MMTR

IEC

Figure A.19 – E-Mobility – Architecture overview

A.6.3 Use cases

The uses cases listed below are a sub-set of the use cases from ISO/IEC DIS 15118-1, which has an information exchange with Secondary actors.

ID	Use case name
C1	Certificate update
C2	Certificate installation
D2	Authentication from EV with Authorization from secondary actors
D4	Identification at the EVSE with validation from the secondary actor

ID	Use case name
E2	Optimized charging with scheduling from the secondary actor
E3	Optimized charging with scheduling at EV
F4	Reactive power compensation
F5	Vehicle to grid support
G1	Value-added services
G2	Charging details

A detailed description of the E-mobility uses cases is given in Table A.9:

Table A.9 – E-Mobility – Use case list

ID	Use case name	Description	Actors
C1	Certificate update	This use case covers the update of an expired certificate in the EV. Therefore, the EVCC is initiating a certificate update process using the established high-level communication with the SECC to retrieve a new certificate from the issuing secondary actor. NOTE 1 There may be alternative communication paths to do a certificate update. However, these are outside the scope of this standard. NOTE 2 If a certificate has already expired, Use case Element C2 might apply. The certificate update process from SECC to secondary actor and back is outside the scope of this standard. Scenario description: • EVCC requests a certificate update by SECC, providing information about the secondary actor who has issued the certificate. • SECC enables a communication link to the secondary actor or provide the certificates to be updated as a local copy. • SECC requests a certificate update for EVCC from secondary actor containing EVCC specific information. • Issuing entity provides a new certificate to the requesting SECC. SECC forwards the new certificate to EVCC.	Primary actors: EVCC, SECC. Secondary actors: EMOCH, FO, E-Mobility Infrastructure Operator

ID	Use case name	Description	Actors
C2	Certificate installation	This use case covers the installation of a certificate (Contract Certificate) into the EV if no such certificate is available yet / has expired / is invalid. Therefore, the EVCC is initiating a certificate installation process using the established high-level communication with the SECC to retrieve a certificate from the issuing secondary actor. The EV is identified by using a certificate (Bootstrap Certificate) that was installed by the OEM earlier (e.g. at EV production). NOTE There may be alternative communication paths for doing a certificate installation. However, these are outside the scope of this standard. The certificate installation / transfer process from SECC to the secondary actor and back is outside the scope of this standard. Scenario description: • EVCC requests a certificate installation by SECC. • SECC enables a communication link to the secondary actor or provides the certificates to be installed as local copy. For this purpose, the SECC has to identify the secondary actor which has a contract with the owner of the EV. Therefore, it has to send the Bootstrap Certificate (or its ID) to the clearing house / all known clearing houses. The corresponding contract may be identified by the secondary actor, for instance, via the certificate ID of the Bootstrap Certificate. This ID is transferred from the customer to the secondary actor at contract creation. (First, the OEM has to transfer this ID to the customer e.g. at EV delivery). • SECC requests a certificate installation for EVCC from the secondary actor found containing EVCC specific information (Bootstrap Certificate). • Issuing entity shall provide a certificate and the corresponding private key to the requesting SECC. At least the private key has to be encrypted using the old EVCC Bootstrap Certificate. SECC shall forward the new certificate and the corresponding (encrypted) private key to EVCC.	Primary actors: EVCC, SECC. Secondary actors: EMOCH, FO, E-Mobility Operator
D2	Authentication from EV with Authorization from secondary actors	This use case covers the authentication process from the EV. The identification should be made with an ID as stipulated in ISO/IEC 15118-2. Scenario Description: • USER connects the car to the station and activates the service offering the ID. This could also be done automatically. • SECC and EVCC exchange their IDs (e.g. Contract ID). Those are forwarded to the secondary actor for validation. • The secondary actor replies with an agreement or non-agreement Service starts after successful authorization of the IDs	Primary actors: EV, EVCC, EVSE, SECC, HMI Secondary actors: EMOCH, E-Mobility Operator
D4	Identification at the EVSE with validation from the secondary actor	This use case covers the process of how identification should be validated by a secondary actor. User identifies himself at the EVSE by using one of the identification methods offered. NOTE Depending on the identification type, the EVSE operator may not have the possibility to authenticate the ID and therefore might not authorize the service. Scenario description: • SECC forwards the IDs (Spot Operator ID, Power Outlet ID, provider ID and Contract ID) to the secondary actor for validation. • The secondary actor replies with an agreement or non-agreement. Service Starts after successful verification of the IDs.	Primary actors: USER, EVSE, SECC, HMI. Secondary actors: EMOCH, E-Mobility Operator.

ID	Use case name	Description	Actors
E2	Optimized charging with scheduling from the secondary actor	This use case covers the AC charging process with information about local installation, grid schedule and sales tariff table. With this, the EVSE can dynamically react to changes in the supply chain to reduce peak demand or oversupply situations. Additionally, the behavior of the vehicle while charging becomes transparent to secondary actors in order to enhance electricity supply scheduling. The secondary actor needs to propose a charging schedule to the SECC, based on actual information about the local installation, grid schedule and sales tariff table. It is necessary that EVCC, SECC and secondary actor have each the possibility to trigger a re-scheduling of the charging profile. Scenario descriptions: • USER inputs "Target set" at EV" • EV calculates the required amount of energy needed for the charging (Wh) and the departure time to meet the target. • EVCC sends the calculated value and the charging capability of EV to the SECC, which might forward it to a secondary actor. • A secondary actor collects "Demand and prognosis". (e.g. Local physical limits from EVSE, grid schedule from DCH, Sales tariff table from EP or e- • Mobility Operator) • Note: This action might be performed prior to the charging event and could therefore been sent to the SECC. • A secondary actor or the SECC executes "Level selector" to provide input for charging schedule • A secondary actor or the SECC calculates "Charging schedule" • EVSE picks up the current limitation of "Charging schedule" for "Charging Control". • SECC send the current limitation to "EVCC". EV will start charging according to the current limitation	Primary actors: EV, EVCC EVSE, SECC Secondary actors: DCH, E-Mobility Operator

ID	Use case name	Description	Actors
E3	Optimized charging with scheduling at EV	This use case covers the AC charging process with information about local installation, grid schedule and sales tariff table. With this the EV can react on changes in the supply chain to reduce peak demand or oversupply situations. Additionally the behavior of the vehicle while charging becomes transparent to secondary actors in order to enhance electricity supply scheduling. The secondary actor needs to provide a grid schedule and sales tariff table to the SECC. The SECC forwards this information, together with the local limitations, to the EVCC. It is necessary that the EVCC, SECC and secondary actor each have the possibility to trigger a re-scheduling of the charging profile. Scenario descriptions: • USER inputs “Target set” at EV”. • EV calculates the required amount of energy required for the charging (Wh) and the departure time to meet the target. • EVCC sends the calculated value and the charging capability of EV to the SECC, which might forward it to a secondary actor. • A secondary actor collects “Demand and prognosis”. (e.g. grid schedule from DCH, Sales tariff table from EP or e-Mobility Operator) and forwards this information to the SECC. Note: This action might be performed prior to the charging event and could therefore be sent to the SECC. • The SECC provides grid schedule, sales tariff table and local physical limits to the EVCC. • The EV executes “Level selector” to provide input for the charging schedule. • The EV calculates “Charging schedule” and shall send the schedule to the SECC for commitment. • EV picks up the current limitation of “Charging Schedule” for “Charging Control”. EV will start charging according to the current limitation.	Primary actors: EV, EVCC EVSE, SECC. Secondary actors: DCH, E-Mobility Operator.
F4	Reactive power compensation	This use case element covers the exchange of information regarding the possibility of reactive power compensation from the EV side and the demanded reactive power compensation from the EVSE or grid side. Scenario description: • EVCC is indicating that reactive power compensation is possible. • EVCC provides information as to what kind of reactive power compensation can be supported. • SECC requests reactive power compensation with an appropriate reactive power compensation value. • EVCC confirms the adjusted reactive power compensation value. The following information needs to be exchanged between the actors: From EVCC to SECC: Flag indicating that reactive power compensation is supported, supported reactive power compensation values, actual used reactive power compensation value. From SECC to EVCC: flag indicating that reactive power compensation is necessary, necessary reactive power compensation value.	Primary actors: EV, EVCC EVSE, SECC.

ID	Use case name	Description	Actors
F5	Vehicle to grid support	This use case element covers the exchange of information regarding the principle and actual possibility of supporting vehicle to grid energy flow. Therefore, the EV needs the possibility to indicate that it can technically support vehicle to grid energy flow. Additionally, it needs the possibility to provide information as to how much energy is available for vehicle to grid operation, and with which power this operation can be supported. Scenario description: • EVCC shall indicate that it can support vehicle to grid operation from a technical point of view. • EVCC shall provide information at which power vehicle to grid operation can be supported. • EVCC shall provide information as to how much energy is available for vehicle to grid operation, therefore the vehicle takes into account that the user goal of a charged vehicle at a given time can still be reached. • SECC shall indicate that it supports vehicle to grid operation. • SECC shall provide grid schedule together with sales tariff table information or a proposed charging schedule, including a vehicle to grid tariff / segment, to indicate that the EP, EMOCH requests vehicle to grid operation. • EV shall use / reject the offered vehicle to grid tariff / segment according to use case element E3. The following information needs to be exchanged between the actors: From the EVCC to SECC: Flag indicating that vehicle to grid operation is technically possible from the EV side, maximum supported vehicle to grid power value, available vehicle to grid energy or maximum duration of vehicle to grid energy flow at maximum power value. From the SECC to EVCC: Flag indicating that vehicle to grid operation is technically possible from the SECC side.	Primary actors: EV, EVCC EVSE, SECC. Secondary actors: EP, EMOCH.
G1	Value-added services	Optional services that may connect to the local network domain (EVSE) or the internet using optional protocols. Protocols on different communication layers may be used e.g. DHCP, HTTP, SOAP, HTML” Scenario description: • OEM or user requests VAS. • SECC requests service from the EVCC. SECC routes information.	Primary actors: EVCC EVSE, SECC. Secondary actors?

ID	Use case name	Description	Actors
G2	Charging details	This use case covers the exchange of information regarding the current charging process to the SECC. Parameters like battery status and state of charging could be provided for the SECC. The SECC or secondary actor, aware of the status of its charging process, delivers information to the vehicle user. Scenario Description: • Service detail record requested. • SECC requests record from EVCC. • EVCC sends record to SECC after request is accepted. • SECC provides information for the secondary actor or HMI. The following information needs to be exchanged between the actors: From the EVCC to SECC: EV charging details according to the requested list. It needs to be indicated if the requested information is not available from the EV side. From the SECC to EVCC: Authorization to request charging details, list of requested charging details.	Primary actors: EV, EVCC EVSE, SECC, HMI.

A.7 Use cases for VPP and Microgrid

A.7.1 Scope of this clause

The requirements of microgrid will be discussed together with the ones of VPP because they both aggregate the capacity of DER.

VPP:

- “A Virtual Power Plant (VPP) aggregates the capacity of many diverse Distributed Energy Resources (DER), it creates a single operating profile from a composite of the parameters characterizing each DER and can incorporate the impact of the network on aggregate DER output.” (Source: FENIX research project)
- A CVPP (Commercial VPP) has an aggregated profile and output which represents the cost and operating characteristics for the DER portfolio. The impact on the distribution network is not considered in the aggregated CVPP profile. Services/functions from a CVPP include trading in the wholesale energy market, balancing of trading portfolios and provision of services (through submission of bids and offers) to the system operator. The operator of a CVPP can be any third party aggregator or a Balancing Responsible Party (BRP) with market access; e.g. an energy retailer.
- A TVPP (Technical VPP) consists of DER placed in the same distribution network region. The TVPP includes the real-time influence of the local network on DER aggregated profile as well as representing the cost and operating characteristics of the portfolio. Services and functions from a TVPP include local system management for Distribution System Operator (DSO), as well as providing Transmission System Operator (TSO) system balancing and ancillary services.

Microgrid:

A Microgrid is generally intended to balance supply and demand. It always contains a distribution network which has to be managed. Furthermore, an important difference is the ability of the Microgrid to run autonomously in island mode.

There are several operational modes of the microgrid or transitions from one to another:

- Island mode
- Parallel mode

- Transition from parallel to islanding mode
  - In emergency/fault situation of the external utility network
  - In cases of a strategically request (military microgrid)
- Transition from island to parallel mode
  - Always on request
- Black-start of the microgrid eventually including connection to the grid
- Shutdown of the microgrid

A.7.2 Architecture overview

A.7.2.1 Architecture overview for Microgrid

Scalability:

- Up to 500 directly connected DER
- Up to 100.000 indirectly (aggregated) connected DER

Dynamic extension (estimations):

- For industrial / commercial microgrid – monthly
- For campus / institutional microgrid – between monthly to yearly
- Military MG – small dynamic extension (from daily to yearly)
- For community / municipal utility microgrid – hourly to daily

As an example in Figure A.20 a conceptual structure of a microgrid is given.

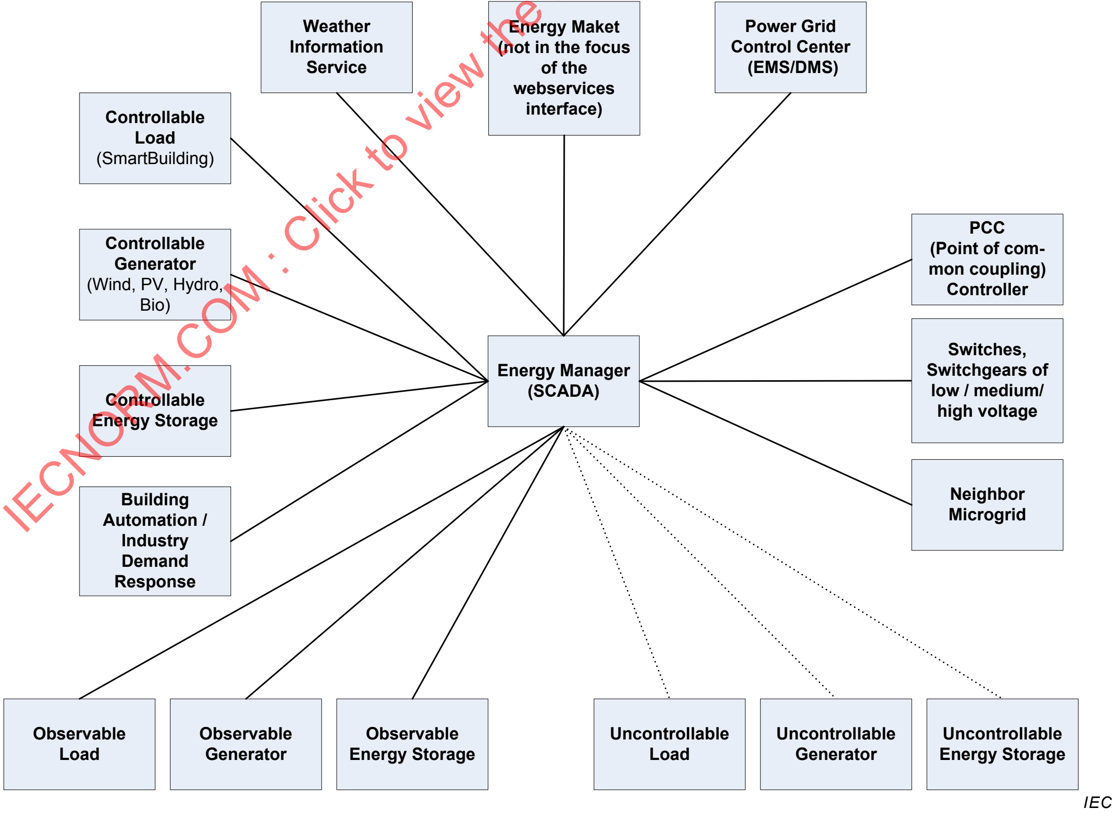

Weather Information Service
Energy Maket (not in the focus of the webservices interface)
Power Grid Control Center (EMS/DMS)
Controllable Load (SmartBuilding)
Controllable Generator (Wind, PV, Hydro, Bio)
Controllable Energy Storage
Building Automation / Industry Demand Response
Energy Manager (SCADA)
PCC (Point of com-mon coupling) Controller
Switches, Switchgears of low / medium/ high voltage
Neighbor Microgrid
Observable Load
Observable Generator
Observable Energy Storage
Uncontrollable Load
Uncontrollable Generator
Uncontrollable Energy Storage
IEC

Figure A.20 – Architectural picture of a microgrid

A.7.2.2 Architecture overview for VPP

Scalability:

- Up to 1 000 directly connected DER
- Up to 1 000 000 indirectly (aggregated) connected DER

Dynamic extension (estimations):

- CVPP / TVPP – hourly to daily

Figure A.21 gives a conceptual structure of a VPP.

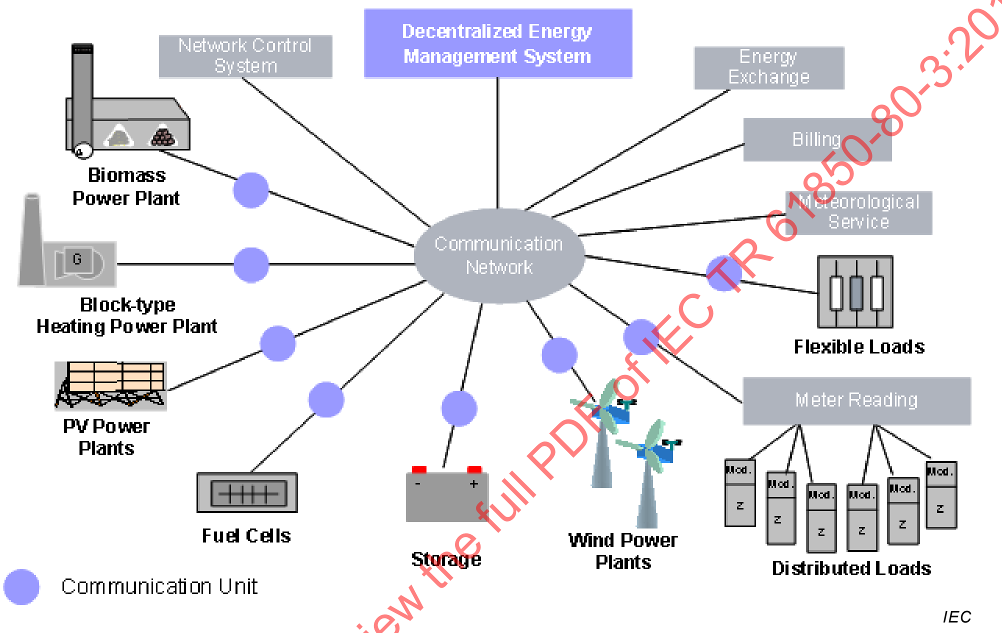


Figure A.21 – Architectural picture of a VPP

A.7.3 Use cases

Table A.10 and Table A.11 give the use cases of the VPP/Microgrid domain.

Table A.10 – VPP/Microgrid – Use case list

#	Use case name	Description	Actors
1	Monitoring/SCADA of the TVPP/microgrid – Status of DER – Measurements forecast /history	The servers provide their information to a VPP/microgrid DER Management in a spontaneous / cyclic mode and per request (see “DER Management“ in Table 1).	VPP Operator
2	Exchange of schedules for operation	Exchange schedules of energy generation to the grid,	DSO
3	Changing of parameters		VPP Operator
4	Ancillary network and balancing services	Microgrid provides by the performance of its DER ancillary and balancing services to DSO.	DSO
5	Monitoring of power quality information	Acc. the regional regulation power quality should be monitored for responsibility.	
6	Direct control in microgrid	It should be possible to control switches, modes analog set-points etc. directly.	DSO

#	Use case name	Description	Actors
7	State transitions (island / parallel)	Islanding decisions may be given from the operator or may come from the PCC device. Paralleling decisions are given by the operator. The microgrid can automatically implement the decision i.e. execute steps like voltage, frequency and phase adaptation and give a signal to the PCC device to close the breaker when all necessary conditions are met.	VPP Operator, PCC device
8	Microgrid: Black-start	In black-start use case the microgrid can started from the scratch. Two functions are needed: local black start of the microgrid (leading to island operation) and reconnection to main grid	

Table A.11 – VPP/Microgrid – Other use cases not feasible with existing ACSI

Use case name	Description	Actors
Autoconfiguration	When new devices (e.g. DER or intelligent appliances) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the VPP/Microgrid they automatically configure itself (also frequently denoted as Plug & Play). The VPP/Microgrid operator can access the devices in a secure and trusted manner. Based on the ownership different access rights control the access of the VPP/Microgrid Operator to the device. The devices can describe their capabilities to the VPP/Microgrid operator and specify their services for monitoring and control. Auto-configuration is needed for different devices and systems, e.g. Plug & Play of Smart Appliances in house, registration of devices owned by the VPP/Microgrid Operator at the VPP/Microgrid DER Management, registration of DER owned by the DER owner at the VPP/Microgrid DER Management or registration of a Building/Home Energy System at the VPP/Microgrid DER Management.	DER Unit, VPP DER Management,
Registration of DER owned by the DER owner at the Microgrid DER Management	The DER owner likes to offer the services of his DER unit (e.g. supplying energy) to a VPP or Microgrid Operator. Before doing so the DER unit has to be registered at the registry of the VPP/Microgrid DER Management. In the registry the technical profile of the DER (performance, characteristics, forecast) will be provided. Furthermore, access rights are defined based on contractual agreements which define the level of monitoring and control of the DER unit from the VPP/Microgrid DER Management system.	DER unit, VPP DER Management
Deregistering	If the DER doesn't want to be registered in the DER Management Registry. It stops to provide its services to this VPP.	DER unit, VPP DER Management
Discovery of DER controller for auto-configuration	After registration the VPP/Microgrid operator can access to the DER Management registry to search and then to communicate to the devices in a secure and trusted manner.	DER unit, VPP operator, VPP DER Management
Discovery of DER in DER Management registry	The devices can describe their capabilities to the VPP/Microgrid DER Management and specify their services (performance and power characteristics).	DER unit, VPP DER Management