PD IEC/TR 61850-80-3:2015

BSI Standards Publication

Communication networks and systems for power utility automation

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

Documents
Document Sharing Hub

Full document details: PD IEC/TR 61850-80-3:2015

National foreword

This Published Document is the UK implementation of IEC/TR 61850-80-3:2015.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 89105 2
ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 August 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD IEC/TR 61850-80-3:2015

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

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: PD IEC/TR 61850-80-3:2015

CONTENTS

FOREWORD ... 6
INTRODUCTION ... 8
1 Scope ... 9
2 Normative references ... 10
3 Terms and definitions ... 11
4 Abbreviated terms ... 12
5 Main involved sub-systems and stakeholders ... 12
6 Requirements description ... 14
6.1 General ... 14
6.2 Scope of this clause ... 14
6.2.1 ACSI classes to be mapped ... 14
6.2.2 Network type ... 15
6.3 Requirements list ... 15
6.3.1 Transfer time ... 15
6.3.2 Throughput ... 15
6.3.3 Data integrity (error probability) ... 15
6.3.4 Reliability ... 15
6.3.5 Availability ... 15
6.3.6 Interoperability ... 16
6.3.7 Cyber security ... 16
6.3.8 Device size ... 17
6.3.9 Dynamic extension of the system ... 17
6.3.10 Sensitivity to cost of bandwidth ... 17
6.3.11 Availability of commercial and open source tools ... 17
6.3.12 Intellectual property ... 18
6.3.13 Perenniality / Stability of the solution ... 18
6.3.14 Request for additional resources and engineering ... 18
6.3.15 Simplicity and easy implementation of the communication solution ... 18
6.3.16 Ability to become a SCSM / Difficulty in filling the gap ... 18
6.3.17 One single solution for all smart grid applications ... 18
6.3.18 Products' time-to-market ... 18
6.3.19 Minimize standardization effort ... 19
7 SCSM technical description ... 19
7.1 Technology assessment and choice ... 19
7.2 XMPP overview ... 20
7.2.1 Principles ... 20
7.2.2 Address scheme ... 21
7.2.3 Scalability and redundancy ... 21
7.2.4 Server federation ... 22
7.2.5 Stanza example ... 22
7.2.6 Presence monitoring ... 23
7.3 Communication stack overview ... 23
7.4 Definition of the XML payload ... 25
7.5 Transport of XML payloads over XMPP ... 28
7.5.1 Mapping over XMPP overview ... 28

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

7.5.2 Rules for mapping solicited services ... 29
7.5.3 Mapping of unsolicited services ... 31
7.5.4 Usage of presence monitoring ... 31
7.6 Cyber security ... 32
7.6.1 Security with XMPP ... 32
7.6.2 Choice of technical solutions for security ... 33
7.7 Mapping synthesis ... 33
7.8 Synergy with existing 8-1 mapping ... 35
Annex A (informative) Use cases and requirements for each domain ... 38
A.1 Use cases for PV-inverters ... 38
A.1.1 Scope of this clause ... 38
A.1.2 Architecture overview ... 38
A.1.3 Use cases ... 39
A.2 Use cases for hydro and thermal generation ... 40
A.2.1 Scope of this clause ... 40
A.2.2 Architecture overview ... 40
A.2.3 Use cases ... 41
A.3 Use cases for wind power ... 43
A.3.1 Scope of this clause ... 43
A.3.2 Architecture overview ... 43
A.3.3 Use cases ... 46
A.4 Use cases for CHP ... 49
A.4.1 Scope of this clause ... 49
A.4.2 Architecture overview ... 50
A.4.3 Use cases ... 54
A.4.4 References for CHP domain ... 59
A.5 Use cases of domain Smart Customer (DR) ... 59
A.5.1 Scope of this clause ... 59
A.5.2 Architecture overview ... 60
A.5.3 Use cases ... 62
A.6 Use cases for E-Mobility ... 64
A.6.1 Scope of this clause ... 64
A.6.2 Architecture overview ... 64
A.6.3 Use cases ... 64
A.7 Use cases for VPP and Microgrid ... 70
A.7.1 Scope of this clause ... 70
A.7.2 Architecture overview ... 71
A.7.3 Use cases ... 72
A.8 Use cases for feeder automation ... 74
A.8.1 Scope of this clause ... 74
A.8.2 Architecture overview ... 74
A.8.3 Use cases ... 78
A.9 Required services and performances ... 79
Annex B (informative) Examples of MMS XER payloads ... 82
B.1 General ... 82
B.2 GetLogicalNodeDirectory ... 82
B.3 Report ... 88

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

Figure 1 – Architecture overview 13
Figure 2 – Device communicating with different trust levels 17
Figure 3 – Architecture main choices 20
Figure 4 – XMPP architecture overview 21
Figure 5 – XMPP Federation 22
Figure 6 – Example of a XMPP telegram 23
Figure 7 – Simplified communication stack 24
Figure 8 – XER encoding vs BER encoding 26
Figure 9 – ASN.1 abstract definition of MMS PDUs (extract) 27
Figure 10 – Example of XER payloads 27
Figure 11 – ACSI XML Message schema for XER payload (extract) 28
Figure 12 – XMPP architecture for IEC 61850 29
Figure 13 – XMPP using TLS and Simple Authentication and Security Layer (SASL) 32
Figure 14 – End to end security over XMPP 33
Figure 15 – Synthesis of SCSM 8-2 structure 34
Figure 16 – SCSM 8-1 and 8-2 synergy 35
Figure 17 – Control center with dual stack SCSM 8-1 / SCSM 8-2 36
Figure 18 – Gateway between SCSM 8-1 and SCSM 8-2 37
Figure A.1 – PV – Architecture overview for data connections to an industrial plant 38
Figure A.2 – PV – Architecture overview for data connections to a residential plant 39
Figure A.3 – Power plants – Typical power operator network architecture 41
Figure A.4 – Power plants – Relationship between the actors 41
Figure A.5 – Examples of the variety of topologies required/supported for wind power 44
Figure A.6 – Example of use within the wind plant 44
Figure A.7 – Example of use between the wind plant and a control center 45
Figure A.8 – Diagram of data use hierarchy levels in condition monitoring 45
Figure A.9 – Types of CHP plants 50
Figure A.10 – CHP – Example of a system architecture 51
Figure A.11 – Number of CHPs in Germany 52
Figure A.12 – CHP use cases and involved actors 53
Figure A.13 – CHP – Graphical presentation of frequency control within the European power system 55
Figure A.14 – CHP – Frequency control time characteristic 55
Figure A.15 – Smart customer – Main actors 60
Figure A.16 – Smart customer – Main elements of the smart customer domain (right column) 61
Figure A.17 – Smart customer – Logical model for customer premises communications 61
Figure A.18 – Smart customer – Communication relationships 62
Figure A.19 – E-Mobility – Architecture overview 64
Figure A.20 – Architectural picture of a microgrid 71
Figure A.21 – Architectural picture of a VPP 72
Figure A.22 – FA – Distributed architecture of a feeder automation system 75
Figure A.23 – FA – Semi-centralized architecture of a feeder automation system 76
Figure A.24 – FA – Centralized architecture of a feeder automation system 77

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

Table 1 – Main involved sub-systems and stakeholders 13
Table 2 – ACSI services to be mapped 24
Table 3 – MMS objects and services in use within this SCSM 25
Table 4 – Mapping synthesis 34
Table A.1 – Use case list 39
Table A.2 – Power plants – Use case list 42
Table A.3 – Wind – List of actors 46
Table A.4 – Wind – Use case list 47
Table A.5 – CHP – Use case list 54
Table A.6 – CHP – Other use cases not feasible with existing ACSI 59
Table A.7 – Smart customer – Use case list 63
Table A.8 – Smart customer – Other use cases not feasible with existing ACSI 63
Table A.9 – E-Mobility – Use case list 65
Table A.10 – VPP/Microgrid – Use case list 72
Table A.11 – VPP/Microgrid – Other use cases not feasible with existing ACSI 73
Table A.12 – FA – Use case list 78
Table A.13 – FA – Other use cases not feasible with existing ACSI 79
Table A.14 – Synthesis – Usage of modeling classes 79
Table A.15 – Synthesis of transfer times 80
Table A.16 – Synthesis – New proposed functions 81

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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.

Documents
Document Sharing Hub

Full document details: PD IEC/TR 61850-80-3:2015

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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:

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

- 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*

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

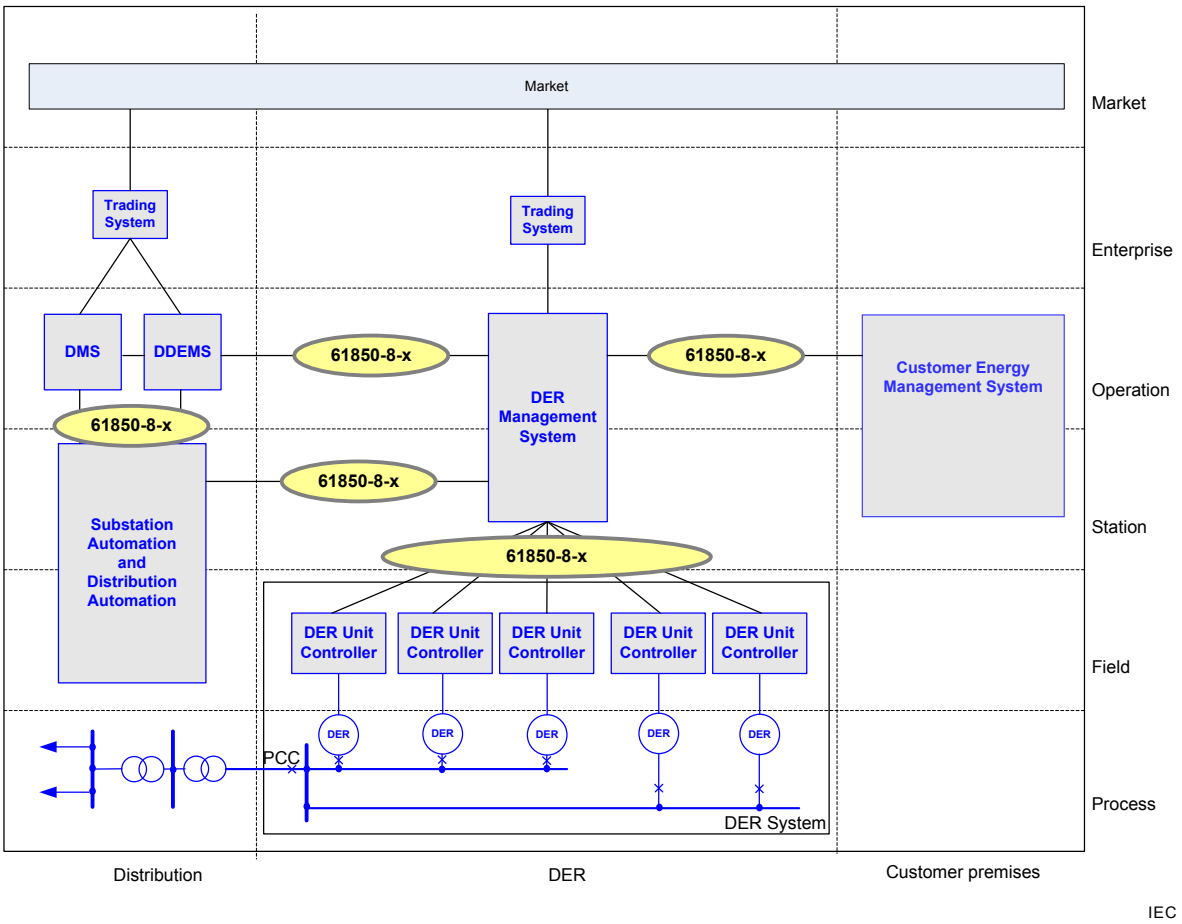


Figure 1 – Architecture overview

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

- 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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

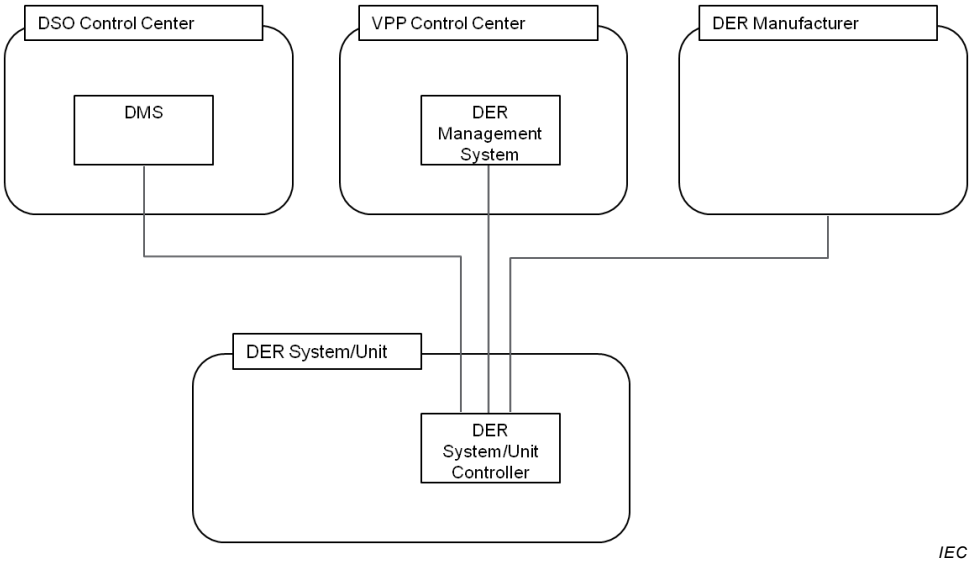


Figure 2 – Device communicating with different trust levels

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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.

AVA Documents
Document Sharing Hub

Full document details: PD IEC/TR 61850-80-3:2015

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

- 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).

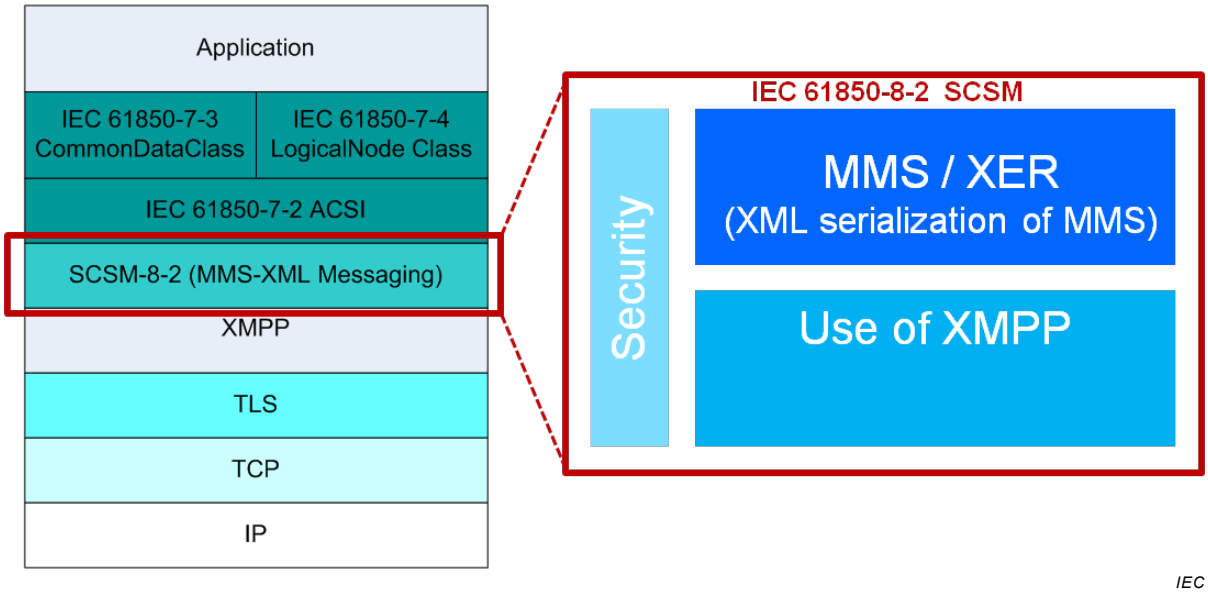


Figure 3 – Architecture main choices

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/>

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

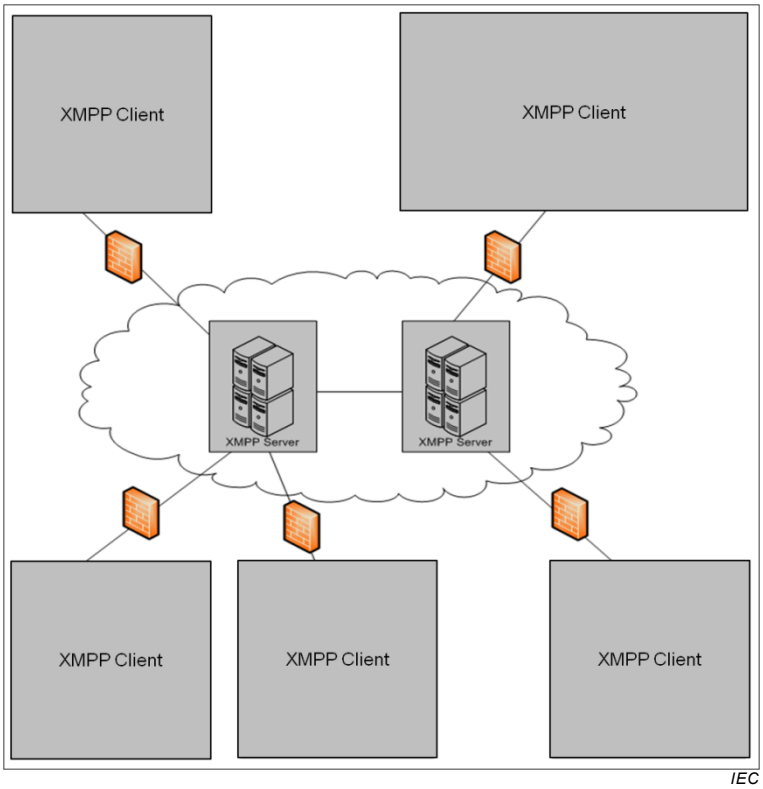


Figure 4 – XMPP architecture overview

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.

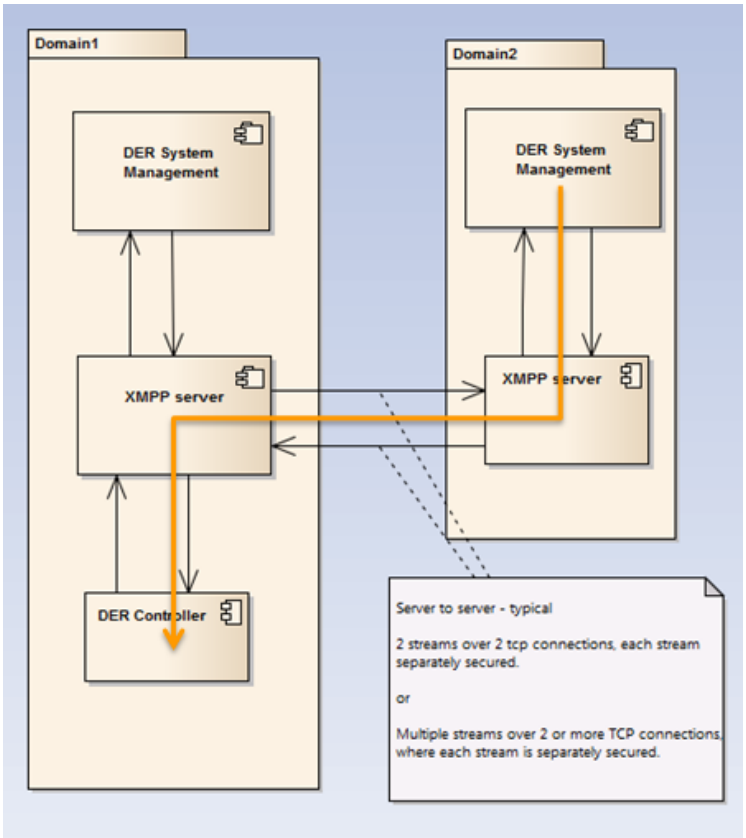
NOTE Performance tests show that the transfer time between XMPP clients is by far less than the required 100ms (see 6.3.1, Transfer time) when the XMPP server is not overloaded. It is expected that this performance level can be reached for a very large number of connected clients by adapting the number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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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”.



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”.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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

IEC

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

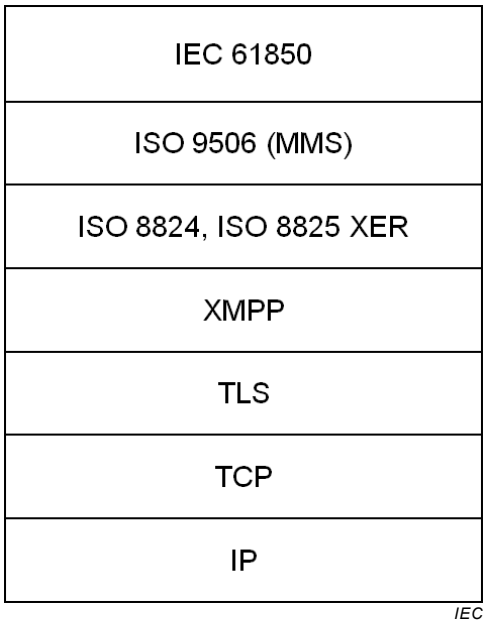


Figure 7 – Simplified communication stack

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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]

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

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).

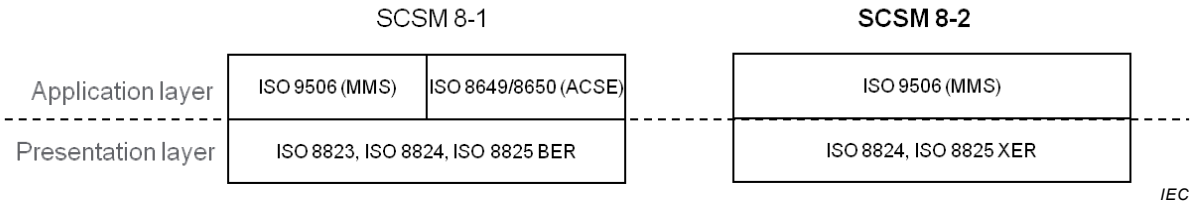


Figure 8 – XER encoding vs BER encoding

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015

```
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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 61850-80-3:2015