

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Protocol for management of electric vehicles charging and discharging
infrastructures –**

Part 1: Basic definitions, use cases and architectures

**Protocole de gestion des infrastructures de charge et de décharge des
véhicules électriques –**

Partie 1: Définitions de base, cas d'utilisation et architectures



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Protocol for management of electric vehicles charging and discharging
infrastructures –**

Part 1: Basic definitions, use cases and architectures

**Protocole de gestion des infrastructures de charge et de décharge des
véhicules électriques –**

Partie 1: Définitions de base, cas d'utilisation et architectures

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.70; 43.120

ISBN 978-2-8322-3868-4

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

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions, and abbreviated terms	10
3.1 Terms and definitions.....	10
3.1.14 Constraints	11
3.1.40 Session	15
3.1.41 Transaction	16
3.2 Abbreviated terms.....	17
4 Actors and architecture model	18
4.1 Actors	18
4.2 Architecture model.....	18
4.3 IEC 63110 metamodel.....	19
4.4 Actors and system view	21
4.5 Implementation examples	23
5 Roles, actors, domains descriptions	23
5.1 General.....	23
5.2 Uses cases type descriptions	23
5.3 Description of the business roles	24
5.4 Description of the system actors	24
5.5 Domain description	24
5.5.1 General	24
5.5.2 Deliver energy transfer services	25
5.5.3 Deliver e-mobility services	26
5.5.4 Manage charging station.....	26
6 Events, loops and sessions	27
6.1 General.....	27
6.2 Sessions and transactions description	28
7 General requirements	29
7.1 Generalities	29
7.2 Communication protocol requirements	29
7.2.1 General	29
7.2.2 Data transfer	29
7.3 Communication architecture requirements	30
7.4 User specific requirements.....	30
7.5 CSMS implementation requirements	30
7.6 Interface requirements between CEM, RM and CSMS.....	30
7.7 Grid specific requirements	31
7.8 DSO requirements	31
7.9 Cybersecurity requirements	31
7.9.1 General	31
7.9.2 Security considerations for information	31
7.9.3 Threat analysis	35
7.9.4 Security requirements.....	36
7.9.5 Relation with use cases	36

7.10	Safety requirements	37
8	Use cases	37
8.1	Generalities	37
8.2	Energy domain use cases	38
8.2.1	General	38
8.2.2	Use case list of the energy domain	38
8.2.3	Smart charging management	39
8.2.4	Charging with demand response	43
8.2.5	CSMS – RM exchange of information at the initiative of the CSMS	46
8.2.6	CSMS – RM exchange of information at the initiative of the RM	49
8.2.7	Power variation triggered by DSO	51
8.2.8	Actors' relations during a V2G session	54
8.2.9	Information exchange required to ensure a dynamic energy transfer control	56
8.2.10	Providing frequency regulation service by means of decentralized frequency measurements	58
8.3	Manage CS domain use cases	62
8.3.1	General	62
8.3.2	Use case list of the manage CS domain	62
8.3.3	Discover CS configuration	63
8.3.4	Update a CS component properties	66
8.3.5	Monitor a CS	69
8.3.6	Update the firmware of a CS	71
8.3.7	Reboot a CS	75
8.3.8	The CSMS sets the information to be presented to the user	78
8.3.9	The CSMS sets log criteria	80
8.3.10	Retrieve log information from the CS	82
8.3.11	Fault-code provisioning	85
8.3.12	Information deletion triggered to CSMS by an SA	87
8.3.13	CS deregistration	90
8.3.14	Migration of the CS	93
8.3.15	Onboarding the CS	95
8.3.16	CA certificate provisioning	97
8.3.17	ISO 15118 OCSP response messages	101
8.3.18	Install CS certificate	104
8.3.19	Install the certificate of the local CSMS	107
8.3.20	Install CS certificate with key pairs created outside	110
8.3.21	Certificate revocation	113
8.4	Deliver e-mobility services domain use cases	115
8.4.1	General	115
8.4.2	Use case list for deliver e-mobility service domain	116
8.4.3	Reservation of an EVSE	116
8.4.4	Authorization with locally presented credentials	120
8.4.5	Authorization by external means	122
8.4.6	Inform EVU about tariff during charging session	124
8.4.7	Inform EVU about tariff during operation	126
8.4.8	SDR information production	128
8.4.9	ISO 15118 contract certificate installation/update	129
Annex A (informative)	Implementation examples	134

A.1	General.....	134
A.2	A simple home example or a single EVSE at kerbside.....	134
A.3	A more complex home with one or more CSs	134
A.4	Parking lots or high-power CS example.....	136
A.5	A CS with local production and storage.....	136
Annex B	(informative) Requirements used for selecting the transport technology	138
B.1	Message specific timeouts shall be supported.....	138
B.2	Transport foundation shall be IP based – with IPv4 and IPv6 support.....	138
B.3	It shall be possible to transport encrypted and/or signed message payload sub-elements	138
B.4	The communication between a CSC and a CSMS shall be encrypted (transport layer)	139
B.5	Bidirectional communication shall be possible.....	139
B.6	Long messages shall not block urgent messages.....	139
B.7	Message payload encoding shall be memory and CPU efficient	139
B.8	Message priority shall be under the control of the application layer	139
B.9	Asynchronous message transfer shall be supported.....	140
B.10	Authentication with related session mechanism shall be supported	140
B.11	Multicast messages should be supported	140
B.12	Addressing scheme needs to be supported	140
B.13	Coordinated time at CS level shall be supported	140
B.14	Message encoding shall support non-standard payload elements	141
B.15	Message encoding shall support versioning	141
B.16	Communication shall be delay tolerant.....	141
B.17	The communication technology should have a high reliability in payload delivery.....	141
B.18	The selected communication technology should not have a single point of failure	142
B.19	Technology shall have proven implementations	142
B.20	Technology shall not have intellectual property restrictions	142
B.21	The communication technology shall be stable	142
B.22	Fine grained authorization shall be supported	143
B.23	Communication layer shall be supported by at least two operating systems and embedded platforms for CS and CSMS	143
B.24	Interoperability with conventional information models used in power industry.....	143
B.25	Communication layer shall support IEC 63110's multi-level architecture for CSMS	144
B.26	Efficient support for binary payload.....	145
B.27	Communication layer shall support request/response and publish/subscribe patterns	145
Annex C	(informative) Example of a complex service session	146
C.1	Visual representation	146
C.2	Description	146
Annex D	(informative) Classification of use cases impacts	148
Annex E	(informative) Security use case sequence	150
Bibliography		151

Figure 1 – Actor's interactions..... 18

Figure 2 – Architecture model of the component layer..... 19

Figure 3 – IEC 63110 metamodel.....	20
Figure 4 – IEC 63110 top-level architecture	21
Figure 5 – Actors	21
Figure 6 – Generic communication architecture – System view	22
Figure 7 – Charging site with two charging site zones controlled by a CSMS	23
Figure 8 – Example of service session	28
Figure 9 – Example of simultaneous service sessions.....	29
Figure 10 – Smart charging sequence diagram	43
Figure A.1 – A simple home with one CS	134
Figure A.2 – Complex home with one CS	135
Figure A.3 – Complex home with two charging stations.....	135
Figure A.4 – Parking lot example	136
Figure A.5 – CS with local production and battery storage	137
Figure C.1 – Example of a complex service session.....	146
Figure E.1 – Security use case sequence	150
Table 1 – Business roles of the e-mobility domain	24
Table 2 – System actors of the e-mobility domain	24
Table 3 – Security considerations by information	32
Table 4 – List of use cases of the energy domain	39
Table 5 – List of use cases of the manage CS domain	62
Table 6 – List of use cases of the e-mobility domain	116
Table D.1 – Use case classification of the energy domain.....	148
Table D.2 – Use case classification for the manage CS domain	149
Table D.3 – Use case classification of the deliver e-mobility services domain	149

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**PROTOCOL FOR MANAGEMENT OF ELECTRIC VEHICLES
CHARGING AND DISCHARGING INFRASTRUCTURES –****Part 1: Basic definitions, use cases and architectures**

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.

IEC 63110-1 has been prepared by IEC technical committee 69: Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
69/837/FDIS	69/843/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 63110 series, published under the general title *Protocol for management of electric vehicles charging and discharging infrastructures*, can be found on the IEC website.

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

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

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

In recent years, the necessity of reducing greenhouse gas emissions has led the automotive industry to develop vehicles propelled by electric energy. Among them, the success of vehicles with electric rechargeable batteries has marked the beginning of the deployment of electric charging infrastructures.

During the first years, solutions for management of charging infrastructures were based on industry alliance specifications or proprietary protocols. They greatly contributed to education and involvement of early EV adopters. However, with the coming mass development of e-mobility required by the latest energy policies in most countries, it is necessary to standardize the communication protocol between charging infrastructures and charging stations operators in order to establish an international, safe, secure, interoperable and grid friendly e-mobility eco-system.

This standardized protocol is beneficial to all actors belonging to the e-mobility environment such as EV manufacturers, charging station manufacturers and operators, e-mobility service providers, grid network operators, distribution system operators (DSO) and transmission system operators (TSO), flexibility operators (FO), balance responsible parties and of course the EV users.

Special attention is paid to the security and traceability of the transactions with respect to identification and payment, but also to privacy regulations in force in many countries in order to avoid malicious or criminal use of the charging station.

The general requirements and definitions of this document form the basic framework for all use case descriptions and related documents in IEC 63110 (all parts). This document is the result of a large consensus among all the actors of e-mobility and should be considered as a guideline for implementers of IEC 63110 (all parts).

Technical specifications and requirements of the IEC 63110 protocol will be defined in a future part of IEC 63110.

PROTOCOL FOR MANAGEMENT OF ELECTRIC VEHICLES CHARGING AND DISCHARGING INFRASTRUCTURES –

Part 1: Basic definitions, use cases and architectures

1 Scope

This part of IEC 63110, as a basis for the other parts of IEC 63110, covers the definitions, use cases and architecture for the management of electric vehicle charging and discharging infrastructures.

It addresses the general requirements for the establishment of an e-mobility eco-system, therefore covering the communication flows between different e-mobility actors as well as data flows with the electric power system.

This document covers the following features:

- management of energy transfer (e.g., charging session), reporting, including information exchanges related to the required energy, grid usage, contractual data, and metering data;
- asset management of EVSE, including controlling, monitoring, maintaining, provisioning, firmware update and configuration (profiles) of EVSE;
- authentication/authorization/payment of charging and discharging sessions, including roaming, pricing, and metering information;
- the provision of other e-mobility services;
- cybersecurity.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 15118 (all parts), *Road vehicles – Vehicle to grid communication interface*

INTERNET ENGINEERING TASK FORCE (IETF). RFC 6960: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* [online]. S. Santesson et al. June 2013 [viewed 2022-01-26]. Available at: <https://www.ietf.org/rfc/rfc6960.txt>

3 Terms, definitions, and abbreviated terms

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1 Terms and definitions

3.1.1

actor

entity that communicates and interacts

Note 1 to entry: These actors can include people, software applications, systems, databases and even the power system itself.

[SOURCE: IEC 62559-2:2015, 3.2]

3.1.2

balance responsible party

BRP

party that has a contract providing financial security and identifying balance responsibility with the imbalance settlement responsible of the market balance area entitling the party to operate in the market

3.1.3

business use case

description of how business roles interact to execute a business process

Note 1 to entry: These processes are derived from services, i.e., business transactions, which have previously been identified.

3.1.4

customer energy manager

CEM

internal automation function for optimizing the energy consumption and/or production within the premises according to the preferences of the customer using internal flexibilities and typically based on external information received through the Smart Grid Connection Point and possibly other data sources

Note 1 to entry: It provides the expected services while fulfilling contracted conditions with the Electricity Supplier, the DSO, the FO, or any other system operators.

3.1.5

charging service provider

CSP

role which does not operate EVSE but manages and authenticates EV user's credentials and provides charging and other value-added services for EV users

3.1.6

charging site

CSI

geographical area that encloses one or more CSs

Note 1 to entry: This is a physical concept.

3.1.7 charging site zone CSZ

management concept representing a group of one or more charging stations at a particular charging site

Note 1 to entry: The energy management scope of a RM is defined by the CSMS in the context of a charging site zone.

Note 2 to entry: This is a logical concept.

3.1.8 charging station management system CSMS system responsible for managing charging infrastructures

Note 1 to entry: CSMS can have local CSMS and/or cloud CSMS instances to implement the system. See system description in 4.4.

Note 2 to entry: This is a logical concept.

3.1.9 charging station operator CSO

party responsible for the provisioning and operation of a charging infrastructure (including charging sites), and managing electricity to provide requested energy transfer services

3.1.10 charging station CS

physical equipment consisting of one or more CSCs and one or more EVSEs managing the energy transfer to and from EVs

3.1.11 charging station controller CSC

sub-system of CS responsible for managing one or more EVSEs

Note 1 to entry: The protocol between the CSC and the EVSE is out of scope of IEC 63110 (all parts).

3.1.12 charging station manufacturer CSM

party responsible for manufacturing charging station providing software updates, upgrades of the hardware and diagnostics support to the CSO

3.1.13 cloud CSMS

CSMS instance physically deployed at a distant place from the charging site

Note 1 to entry: The cloud CSMS does not have to guarantee the same level of reliability and communication latency that is expected from a local CSMS.

Note 2 to entry: This is a physical concept.

3.1.14 Constraints

3.1.14.1 power constraints

range for upper and lower limits for extreme power values within a period of time

3.1.14.2

energy constraints

range for upper and lower limits for average power within a period of time

3.1.15

distribution system operator

DSO

entity responsible for the planning, operation, maintenance, and the development in given areas of the electricity distribution network

Note 1 to entry: The given areas of the electricity distribution network can be low voltage, medium voltage, and potentially high voltage.

Note 2 to entry: The DSO provides the quality of electricity supply (power delivery, voltage, etc.) and customer access to electricity provider market through its system under regulated conditions.

Note 3 to entry: This definition has been adapted from the one in IEC SRD 62913-2-4:2019, Table 3.

3.1.16

e-mobility clearing house

EMOCH

entity mediating between two clearing partners to provide validation services for roaming regarding contracts of different EMSPs

3.1.17

e-mobility needs

mobility needs expressed by the EV user in terms of departure time, minimum and maximum energy request and target energy request or minimum and maximum target state of charge

[SOURCE: ISO 15118-1:2019, 3.1.25, modified – The words "or minimum and maximum target state of charge" have been added to the definition.]

3.1.18

e-mobility service provider

EMSP

party responsible for providing high-value service related to the use of an EV

Note 1 to entry: Examples of service are renting an EV, reservation of parking service, navigation services, energy services which include charging station provider in relation with CSO.

Note 2 to entry: This definition has been adapted from the one in IEC SRD 62913-2-4:2019, Table 3.

3.1.19

electric vehicle communication controller

EVCC

embedded system, within the vehicle, that implements the communication between the vehicle and the SECC in order to support specific functions

[SOURCE: ISO 15118-1:2019, 3.1.31, modified – Note 1 to entry has been removed.]

3.1.20

electric vehicle supply equipment

EVSE

equipment or a combination of equipment, providing dedicated functions to supply electric energy from a fixed electrical installation or supply network to an EV for the purpose of charging and discharging

[SOURCE: IEC 61851-1:2017, 3.1.1, modified – The words "and discharging" have been added to the definition, and the examples have been removed.]

3.1.21**electric vehicle user****EVU**

person or legal entity using the vehicle and providing information about its needs

Note 1 to entry: This definition has been adapted from the one in IEC SRD 62913-2-4:2019, Table 3.

3.1.22**electricity provider****EP**

entity whose activity is the wholesale purchase of electricity and the subsequent direct resale to client through a contract

Note 1 to entry: The electricity provider may also deliver energy related-services.

Note 2 to entry: The electricity provider can generate flexibilities through modulation of electricity prices (time-of-use, critical peak prices, etc.) which can have value on energy markets and/or for network operations.

3.1.23**e-mobility authentication identifier****EMAID**

identifier used for identification of the contract holder

3.1.24**energy transfer plan****ETP**

forecast of future energy transfer activities with associated uncertainties, flexibility options and limits over time

Note 1 to entry: The energy transfer plan is able to support all different charging techniques (ISO 15118 schedule and dynamic modes, CHAdeMO, etc.).

3.1.25**flexibility**

elasticity of resource use (demand, storage, generation), modification of consumption and/or generation of energy/power, on an individual or aggregated level, in reaction to an external signal (price signal or request) in order to provide a service within the energy system

Note 1 to entry: This definition is based on EURELECTRIC, Active Distribution System Management [see Bibliography].

3.1.26**flexibility operator****FO**

party that is responsible for at least one of services like aggregating load flexibility from different users of low voltage and/or medium voltage grids, and trading it with other parties like the TSO and/or the DSO in order to provide ancillary services (adjustment mechanism), or any other (future) flexibility markets, e.g., optimization of balancing grid billing

Note 1 to entry: It may address EV charging through CSOs and may trade its service to other parties.

3.1.27**functional block****FB**

logical representation of a component which contains information about the inputs, outputs, processes, requirements, functions, and functional sequences of a given functionality

3.1.28**hard power limit****HPL**

maximum permissible power of a charging station due to physical design

3.1.29

local CSMS

CSMS instance physically deployed at a specific charging site

Note 1 to entry: This is a physical concept.

3.1.30

power limit

power value that cannot be exceeded

3.1.31

power range

operating area between an upper power limit and a lower power limit

Note 1 to entry: The limits of the power range are placed by the RM within the upper and lower power constraints of the CSMS.

Note 2 to entry: These limits are based on the total power allocated to the CSZ by the CEM.

Note 3 to entry: The power limits should by design always be within the range of the HPLs of the CSZ.

3.1.32

power range envelope

PRE

consecutive series of power ranges over time

3.1.33

online certificate status protocol

OCSP

communication protocol used to determine the current status of a digital certificate without requiring Certificate Revocation Lists, as defined in RFC 6960

3.1.34

primary actor

entity involved directly in an IEC 63110 process

3.1.35

private network

PN

electricity network (home, building, factory, etc.) downstream of a smart grid connection point (SGCP)

Note 1 to entry: It is handled by the private network operator, who assumes the full responsibilities and coverage.

3.1.36

private network operator

PNO

party in charge of managing the energy of the premises

Note 1 to entry: The PNO may have a contract with the DSO and other energy actors.

3.1.37

resource manager

RM

logical component (typically implemented in software) that exclusively represents the energy flexibility of a group of devices or a single smart device towards the buildings customer energy manager and is responsible for sending related instructions to that group of devices or that single device, typically using a device-specific protocol

Note 1 to entry: In the context of this document, the resource manager manages the energy flexibility of a CSZ.

3.1.38
secondary actor
SA

entity indirectly involved in IEC 63110 exchange of information

Note 1 to entry: Secondary actors may exchange information between each other.

Note 2 to entry: Secondary actors could also be a single entity.

3.1.39
service detail record
SDR

data package containing all necessary information within one unique identification which is needed for billing or informing of/about a service session of a specific customer

3.1.40 Session**3.1.40.1**
authorization session
collection of all authorization transactions

Note 1 to entry: Data is collected in the service detail record (SDR).

3.1.40.2
energy transfer session
collection of all energy transfer transactions

Note 1 to entry: Data is collected in the service detail record (SDR).

3.1.40.3
other session
collection of any additional other transactions potentially billable

Note 1 to entry: Data is collected in the service detail record (SDR).

3.1.40.4
parking session
collection of all parking transactions

Note 1 to entry: Data is collected in the service detail record (SDR).

3.1.40.5
reservation session
collection of all reservation transactions

Note 1 to entry: Data is collected in the service detail record (SDR).

3.1.40.6
service session
collection of all billable transactions of one user at a specific time

Note 1 to entry: Data is collected in the service detail record (SDR).

Note 2 to entry: The service session can also represent a time period during which a service was provided. In this case, a service session starts when the first billable transaction starts and ends when the last billable transaction ends.

3.1.41 Transaction

3.1.41.1

authorization transaction

event linked to the authorization process

EXAMPLE When the EV is authorized to charge constitutes a particular authorization transaction.

Note 1 to entry: Authorization is given by SA, for example: EMSP.

Note 2 to entry: Authorization allows usage of a particular EVSE and usually in public CS is necessary for the beginning of the energy transfer session.

Note 3 to entry: A negative authorization is also an authorization transaction.

3.1.41.2

energy transfer transaction

event linked to the energy transfer process

EXAMPLE 1 The start of energy transfer is a particular energy transfer transaction.

EXAMPLE 2 The modification of the maximum power allocated to an EVSE is a particular energy transfer transaction.

3.1.41.3

other transaction

event linked to an additional service

Note 1 to entry: Additional services could be valet, washing or any other service not necessarily related to e-mobility.

3.1.41.4

parking transaction

event linked to a parking service

EXAMPLE When parking fee starts or ends.

3.1.41.5

reservation transaction

event linked to a reservation process

EXAMPLE 1 Reservation contract signature is usually the first reservation transaction.

EXAMPLE 2 Modification in the contract like time of departure change is a reservation transaction.

3.1.42

supply equipment communication controller

SECC

entity which implements the communication to one or multiple EVCCs and which may be able to interact with secondary actors

[SOURCE: ISO 15118-1:2019, 3.1.68, modified – The notes to entry have been removed.]

3.1.43

smart charging

SC

controlled energy transfer process with objectives to optimize customer e-mobility needs, tariffs and energy or power constraints for CSMS and grid

3.1.44**smart grid connection point****SGCP**

borderline between the area of grid and markets towards the role customer (e.g., households, building, industry)

[SOURCE: SG-CG/M490/E_Smart Grid Use Case Management Process, 2012]

3.1.45**time of departure****ToD**

time the user has indicated when the EV will disconnect from the EVSE, and subsequently the user is supposed to leave the parking place

Note 1 to entry: This information is part of the e-mobility needs.

Note 2 to entry: This information is used by the CSMS to predict the ETP.

3.1.46**transmission system operator****TSO**

entity entrusted with transporting energy in the form of electrical power on a national or regional level, using fixed infrastructure

3.2 Abbreviated terms

AETP	aggregated energy transfer plan
BRP	balance responsible party
CEM	customer energy manager
CS	charging station
CSC	charging station controller
CSMS	charging station management system
CSO	charging station operator
CSP	charge service provider
CSZ	charging station zone
DSO	distribution system operator
EMAID	e-mobility authentication identifier
EMSP	e-mobility service provider
ETP	energy transfer plan
EVSE	electric vehicle supply equipment
EVU	electric vehicle user
FO	flexibility operator
OCSP	online certificate status protocol
PRE	power range envelope
RM	resource manager
SA	secondary actors
SDR	service detail record
SGCP	smart grid connection point
TOD	time of departure
TSO	transmission system operator

4 Actors and architecture model

4.1 Actors

There are three primary actors which can initiate a data exchange process in the IEC 63110 data communication concept. Figure 1 presents their interactions.

An EV or user can initiate data exchange through the CSC to the CSMS (e.g., when plugging in or when asking for an authorization to charge).

The primary actors involved directly in the IEC 63110 process are the CSC, the CSMS and the RM.

Secondary actors can initiate data exchange with the CSMS (e.g., grid operator, service provider, EMSP, ...). See 5.3 for a list of primary and secondary actors.

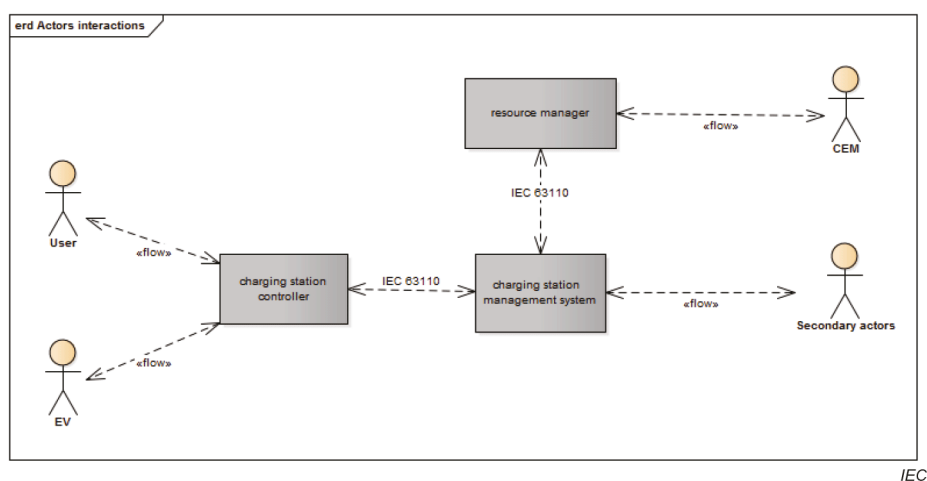


Figure 1 – Actor's interactions

The architecture model depicted in Figure 2 gives a more detailed view of the sub-components for both CSC and CSMS.

4.2 Architecture model

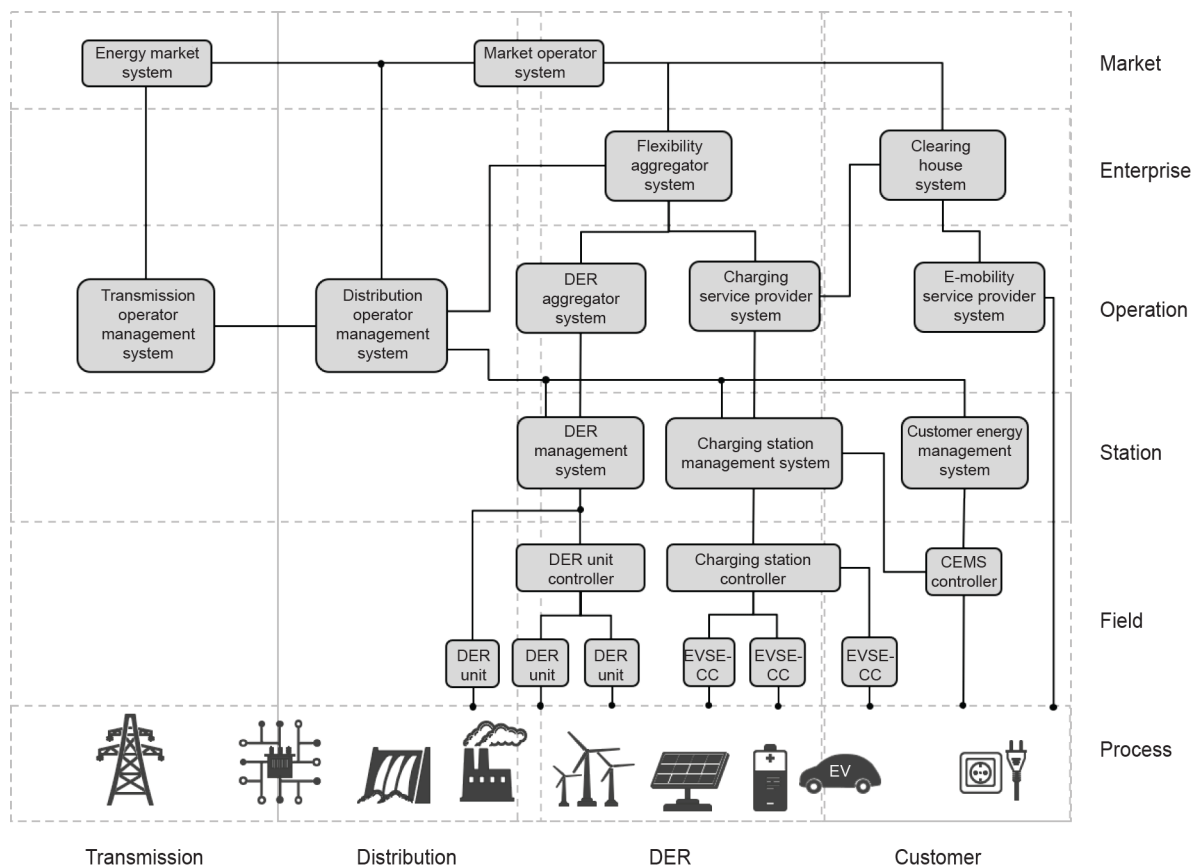
An architecture model is a graphical representation of the logical components, interfaces, and their aggregation levels.

An architecture model does not represent the physical implementation but shows the interfaces from a data communication point of view and how the logical components are organized from an aggregation point of view.

The architecture model is based on the reference model of the smart grid architecture model and Figure 2 is the component layer. SG-CG/M490/E [see bibliography] gives more details on the smart grid architecture model.

The focus of this document is the data communication protocols, interfaces and information exchange between the charging station controller and the charging station management system.

Other interfaces are also defined in the architecture model, but they are specified by other standards and will be used as reference according to the latest official version of the standard document.



IEC

Figure 2 – Architecture model of the component layer

4.3 IEC 63110 metamodel

The metamodel used for IEC 63110 has three levels as shown in Figure 3: component level, property level and DataType level.

The top level is the component level, and it models components in the physical world, like controllers, switches, and outlets. A component may include other components, for example a charging station includes one or more EVSEs.

The second level is the component property level. It gives the property of a component, for example a name, a kind, a time interval.

The third level is the DataType level. It specifies the type of the information reflected by the component properties. Three kinds of Datatype are possible:

- SimpleDataTypes are the most basic data types available in the model, such as string, integer, boolean and float values. Also, data types like date and time belongs to this variant too.
- EnumeratedDataType reflects values identified by names. For example, instead of using the numeric values 0 and 1 for reflecting whether a switch is open or closed, one could use an enumerated data type named PositionKind, having the enumerated values Closed=0, Open=1, and hence use Closed and Open instead of 0 and 1.

- PropertySetTypes describe sets of related properties that are commonly reused together. For example:
 - to reflect a date interval, one could define a DateInterval type (PropertySetType), with two properties – start and end date of the interval (e.g., start:Date and end:Date);
 - to reflect an active power measurement, one could define an ActivePower type, with three properties – value, unit, and multiplier (e.g., value:decimal, unit:string, multiplier:string).

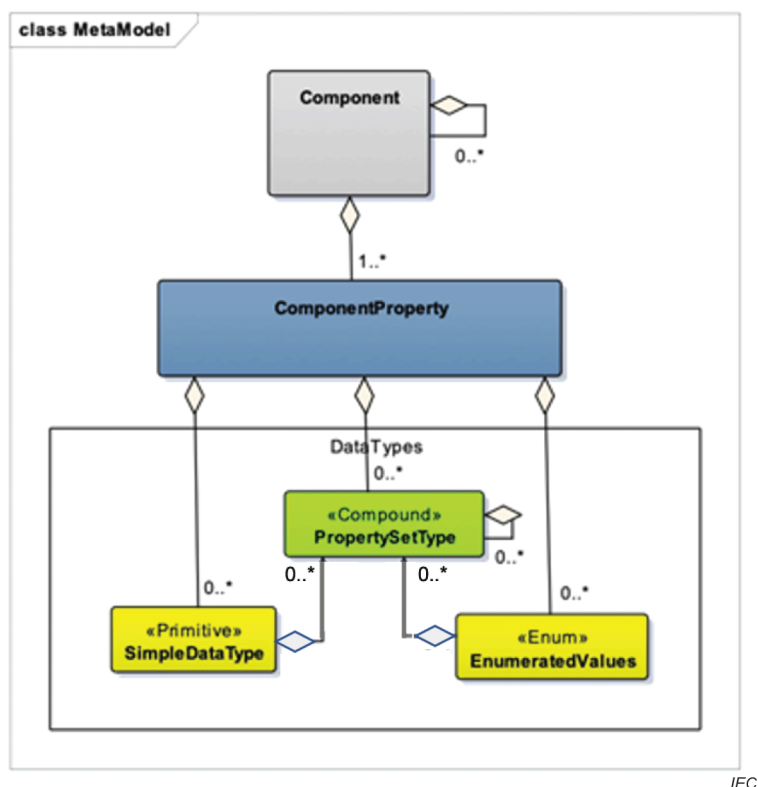


Figure 3 – IEC 63110 metamodel

An extract of the top-level architecture is illustrated in Figure 4.

The architecture reflects the main components involved in charging an electric vehicle. For the full picture of the IEC 63110 object model, see the IEC 63110 UML model and the related IEC 63110-1-1, which has all the details.

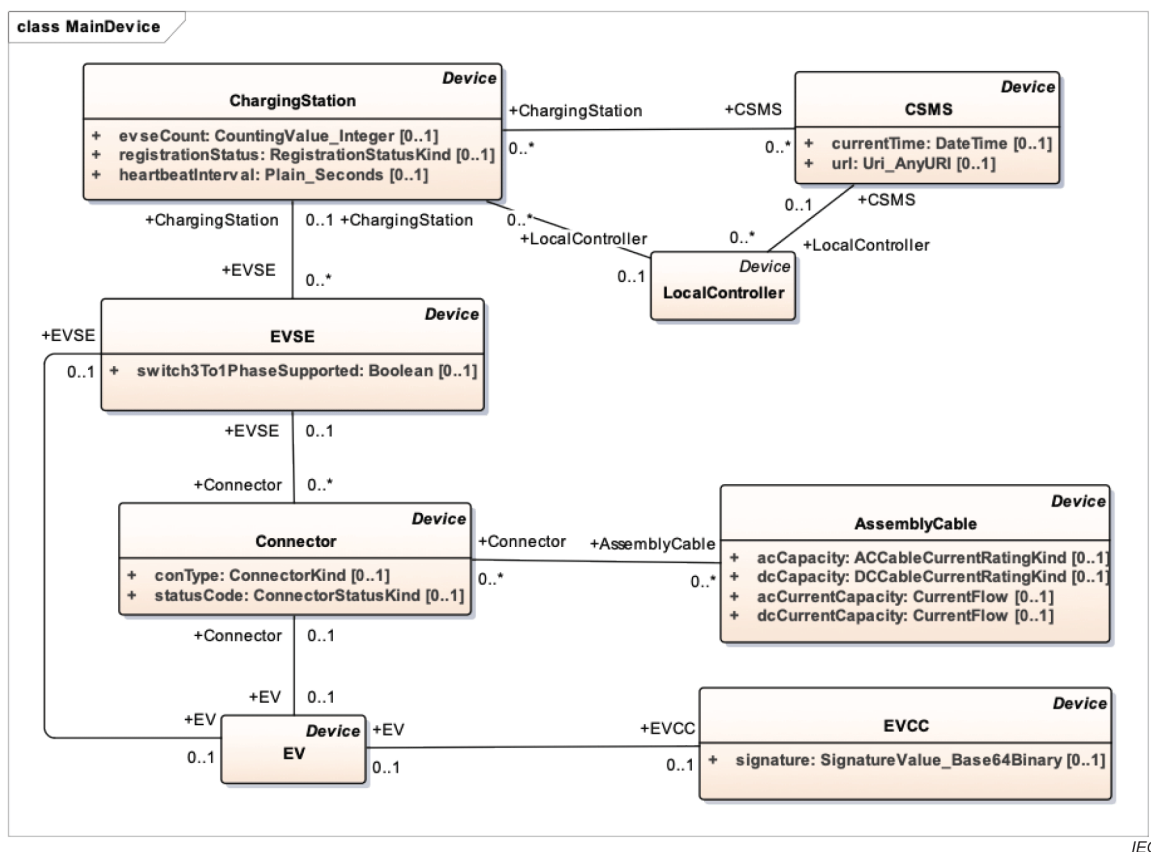


Figure 4 – IEC 63110 top-level architecture

4.4 Actors and system view

Figure 5 shows the different actors interacting in IEC 63110.

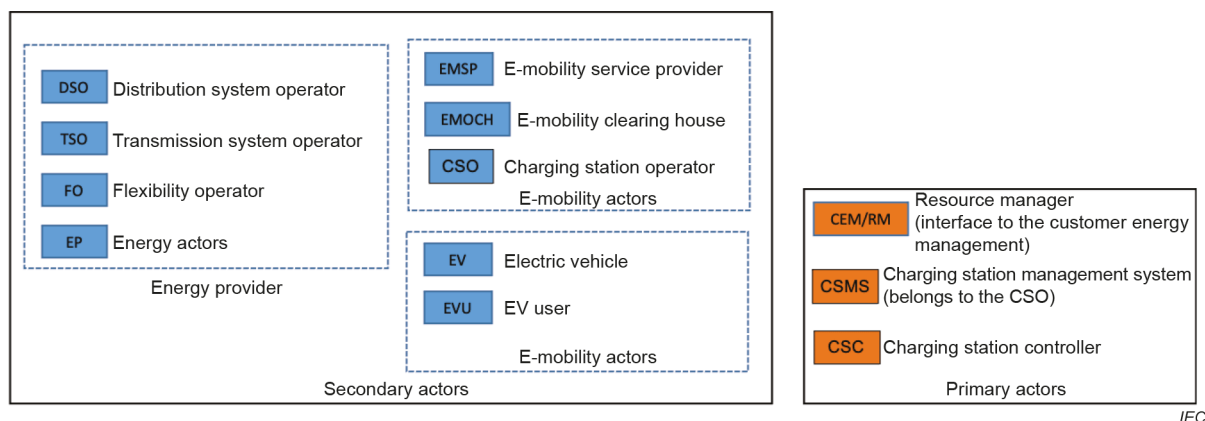


Figure 5 – Actors

Actors exchange messages through systems implementing protocols and interfaces.

The CSMS is the system specified and managed by the CSO. The CSMS controls and monitors charging stations through IEC 63110 communication with the charging station controller. The CSMS and the CSC contain communication physical interfaces also compatible with IEC 63110. IEC 63110 interfaces connect the CSMS to the CSC and optionally with the RM. The CSC has also other interfaces to communicate with the EVSE inside the charging station. When a CEM is present, the CSMS should be able to communicate with this CEM via the RM. The CSO may decide to have a local CSMS performing this communication.

The CSMS (either local or cloud) receives a PRE from the RM and allocates ETPs to the CSs and to each EVSE in the charging site. This allocation can be calculated locally if a local CSMS is implemented.

In case the communication between the cloud CSMS and the local CSMS is broken, the local CSMS should be able to locally maintain CSs operation.

One task of the CS is to aggregate, control and monitor one or more EVSEs. Safety and real-time control of the energy transfer belong to EVSE scope and should not be in direct control of the CS. Another task of the CS is to exchange management messages with CSMS.

Figure 6 presents a generic system view of a communication architecture with one charging station installed behind a SGCP. An optional CEM system is responsible for optimizing power and energy within the SGCP. The CEM is able to exchange messages with the CSMS (either cloud or local) via the RM that implements the IEC 63110 protocol. It has also out of scope connections with other systems either local or depending on secondary actors. All EVSEs are connected to the CS through their own communication protocol. EVU are able to interact on EV, EVSEs, CSO and EMSP through adapted interfaces (e.g., local display or remote apps). There could be more CSs within the same SGCP controlled by one or more local CSMS. The optional local CSMS could be located in different devices, including in the CS.

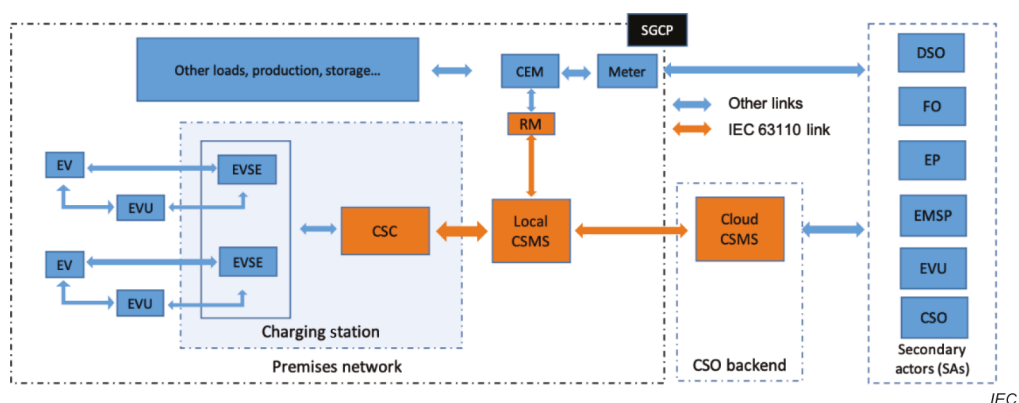
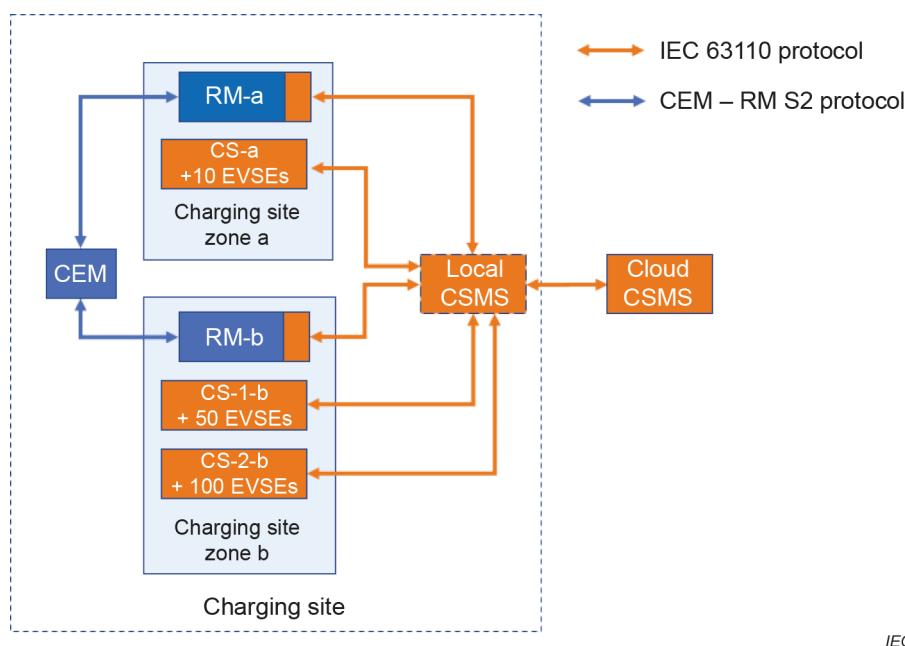


Figure 6 – Generic communication architecture – System view

Figure 7 presents a situation with two (could be more) charging site zones (a and b) within the same SGCP controlled by a CSMS (either local or cloud). The CEM is responsible for optimizing power and energy within the SGCP and for every CSZ. For each CSZ, the CEM controls a resource manager (RM-a and RM-b) able to exchange messages with the CSMS (either cloud or local) through the IEC 63110 protocol.

NOTE RM refers to the S2 concept described in EN 50491-12-1. Other standards are possibly provided, they may offer an interface with the IEC 63110 protocol.



IEC

Figure 7 – Charging site with two charging site zones controlled by a CSMS

NOTE For the CSMS it is not possible and not relevant to understand how the RM has calculated the power constraints information that it has provided to the CSMS. The existence of a full featured building automation (CEM) is out of scope of this document.

4.5 Implementation examples

In most of the cases, the generic architecture presented in Figure 6 can be simplified or adapted depending on the situation. On one hand, in homes it is necessary to have a CS with very simple features; on the other hand, for large installations like parking lots, there will probably be complex systems in charge of coordinating many CSs installed for example on different floors.

Annex A presents some informational implementation examples. Those examples are possible choices of implementation given for illustration purposes. It needs to be understood that the corresponding situations can be implemented in different ways.

5 Roles, actors, domains descriptions

5.1 General

In order to ensure interoperable implementations between business and system roles in the e-mobility environment, it is necessary to describe comprehensive use cases defining their relationships and interactions, in view of satisfying needs of the final customers by adequate service provisions.

5.2 Uses cases type descriptions

There are two types of use cases.

- Business use cases describe how business roles interact to execute a business process. These processes are derived from services, for example business transactions, which have previously been identified.
- System use cases describe how system and/or business roles of a given system interact to perform a function required to enable/facilitate the business processes described in business use cases. Their purpose is to detail the execution of those processes from an information system perspective.

Since a function can be used to enable/facilitate more than one business process, a system use case can be linked to more than one business use case.

5.3 Description of the business roles

Table 1 lists the business roles resulting from a business analysis of the e-mobility domain. The roles are common to other standards like IEC SRD 62913-2-4, IEC 63119 and ISO 15118 (all parts).

Table 1 – Business roles of the e-mobility domain

Actors		
Actor name	Actor type	Role in this document
Charging station operator (CSO)	Business role	Primary actor
Distribution system operator (DSO)	Business role	Secondary actor
E-mobility service provider (EMSP)	Business role	Secondary actor
EV-user (EVU)	Business role	Secondary actor
Flexibility operator (FO)	Business role	Secondary actor

5.4 Description of the system actors

Table 2 lists the principal system actors of the e-mobility domain.

Table 2 – System actors of the e-mobility domain

Actors		
Actor name	Actor type	Further information specific to this document
CSMS	System role	Primary system exchanging messages with CS
CS	System role	Primary system exchanging messages with CSMS
RM	System role	Primary system exchanging messages with CSMS
CEM	System role	Secondary system exchanging messages with the CSMS via the RM
EV	System role	Secondary system
EVSE	System role	Secondary system
EVCC	System role	Secondary system
SECC	System role	Secondary system

5.5 Domain description

5.5.1 General

IEC 63110 use cases domains are divided into three business cases:

- deliver energy transfer service;
- deliver e-mobility services;
- manage CS.

Each of these three business cases relies on business use cases that describe situations where business actors realize some objectives. The three domains, although they may exchange information, are relatively independent.

5.5.2 Deliver energy transfer services

5.5.2.1 General

This business domain describes relations between actors able to influence the energy transfer. It contains use cases related to the management of the energy transfer to one or more EVSEs in order to charge or discharge the battery of the physically connected EVs. Previous exchanges of information phases related to identification, authorization, etc. are presumed to be successful.

The following secondary actors can influence the energy transfer:

- the DSO;
- the FO;
- the CEM;
- the EVU;
- the EV;
- the EVSE;

Their influences are described in the relevant use cases such as in "Provide charging with demand response" or in "Negotiate a charge plan for smart charging".

Secondary actors can influence the energy transfer provided they have established a trusted and secure connection with the CSO or the CSMS.

5.5.2.2 DSO influence

The DSO is responsible for the quality of electricity supply (power delivery, voltage, etc.). It may start curtailment actions in case of emergency or congestions in its distribution network.

In case of various events (e.g., grid constraints, local regulations, contracts), the DSO can request or requires the CSMS to apply immediate power variations.

The messages from the DSO can be sent through secure and trusted communications to different actors:

(DSO to CSO) or (DSO to EMS to CSMS)

5.5.2.3 Flexibility operator influence

The FO is a party that aggregates load flexibility from different parties using the grid and trades it with the transmission system operator and/or the DSO in order to provide ancillary services (adjustment mechanism).

Unlike DSO curtailments, which are a response to local technical issues, FO sends messages to the parties based on market rules.

Messages related to power variations are sent directly through proprietary communication interfaces to the systems of the targeted parties. In the case of e-mobility, they can be sent to the CSO or directly to a particular EV.

If the messages are sent to the CSO, the CSMS processes the message and transmits the power variation to the CSC.

If the FO has sent a message directly to a particular EV, the CSMS will need to be informed of the power variations by the CSC if the information is available to the CS.

NOTE Communication between FO and EV is not in the scope of this document.

In all cases, the proof of service is ensured by the corresponding energy transfer transaction recording by the CSMS.

5.5.2.4 CEM influence

The CEM is the system responsible for the internal management of energy consumption and or production inside a site. Usually, the CEM runs internal algorithms based on constraints. The CEM can be connected to the main meter, local producers, storage units and consumers. The CEM is able to exchange secure and trusted messages with the CSMS (either local or cloud) via the RM.

During its regular/routine optimization process, the RM sets a PRE to the CSMS, based on CSMS energy and power constraints, building energy manager requests or setups and current energy balance between production and consumption, in the relevant CSZ. The CEM may also optimize power against prices strategy depending on market that may have influences in the power limits set by the RM.

The power range envelope, usually in the form of upper and lower power schedules over time, positive or negative, are the basis of the generation by the CSMS of ETPs to each EV based on EVSE characteristics, e-mobility needs and contracts with EMSPs.

5.5.2.5 EVU and EV influence

EV and EVU can influence the energy transfer indirectly through their messages, for example to the EVSE with ISO 15118 negotiation or re-negotiation, or to the CSO via EMSP application for the EVU. The impact on CS-CSMS information exchange depends on the specific information and is expressed in the use cases described in this document.

5.5.3 Deliver e-mobility services

This business domain is related to the management of e-mobility services related to EVU identification and authorization but also reservation and SDR production.

The use cases of this business domain also describe relations with e-mobility secondary actors like EMSP and clearing houses. Roaming interfaces necessary to connect with the EMSP of the EVU are described in IEC 63119. During the authorization process, IEC 63110 is in charge of collecting the corresponding credentials and usually transmits them to the SA in charge of their validation. The use cases of this domain are very important as they are describing EVU interactions with the charging infrastructure.

5.5.4 Manage charging station

This business domain is related to the CS management.

CS management domain contains all operations handled by the CSO to maintain the charging infrastructure in an optimal state of operation.

6 Events, loops and sessions

6.1 General

The CSO is responsible for the management of a CS during its life. This includes the following phases:

- physical installation;
- initial setup;
- commissioning;
- monitoring;
- maintenance-diagnostic;
- decommissioning;
- physical de-installation.

From a protocol perspective, only the phases after physical installation and before physical de-installation are in the scope of this document. All these phases are not independent and normally follow a logical life cycle.

In this document, the life cycle of a CS is described with the following phases:

- CS installation;
- CS operation;
- service operations.

CS installation refers to the first commissioning of a CS into CSO backend, for example during brand new CS installation or during a migration of a CS to a new operator. Except during major hardware upgrades or core parts replacement, CS installation occurs usually only once in the life of a CS managed by a particular CSO.

CS operation refers to all the operations related to its management by the CSMS. For example, its configuration according to the CSMS features or the firmware updates and diagnostics.

Service operations refers to all operations necessary to the handling of EVU interactions with CS like reservation, identification, negotiation for ETPs, energy transfers, and final closure of the service session.

Use cases domains described in 5.5 overlap with life cycle. For example, E-mobility services and energy transfer services domain use cases belong to service operation cycle. Most of manage charging station domains use cases belong to the CS operation cycle.

Once the CS is correctly commissioned and set up, most of the activity of the CSMS occurs during the service operations cycle. The efficiency and quality of this part of the CSMS activity is a key factor for the success of the massive deployment of the millions of CSs planned for the coming decades (see 7.2 for protocol requirements).

Service operations cycle activities are related to EVU or EV interactions with the CS. In order to provide a secure, efficient, and reliable interaction process, the CSMS shall track all activities likely to influence relation with the EVU (for example financial, technical, or contractual matters).

For that purpose, the concepts of sessions and transactions are introduced in this document.

6.2 Sessions and transactions description

As defined in Clause 3, IEC 63110 uses the concept of sessions and transactions. The sessions in IEC 63110 do not refer to communication session but to activities between the instants when an EVU or an EV enters into IEC 63110 scope and when the EV leaves it. Sessions and transactions are mainly used to identify and track potentially billable services triggered during service operations cycle that will be combined and reported in the SDR.

The service session starts with the first transaction and finishes at the end of the last transaction. Depending on the situation, the service session may contain multiple transactions belonging to different types of sessions like authorization, reservation, parking, energy transfer and other. Some transactions during a service session may not be triggered, although energy transfer transactions will occur in most service sessions. See definitions in Clause 3.

Figure 8 shows a service session with authorization, parking and energy transfer sessions.

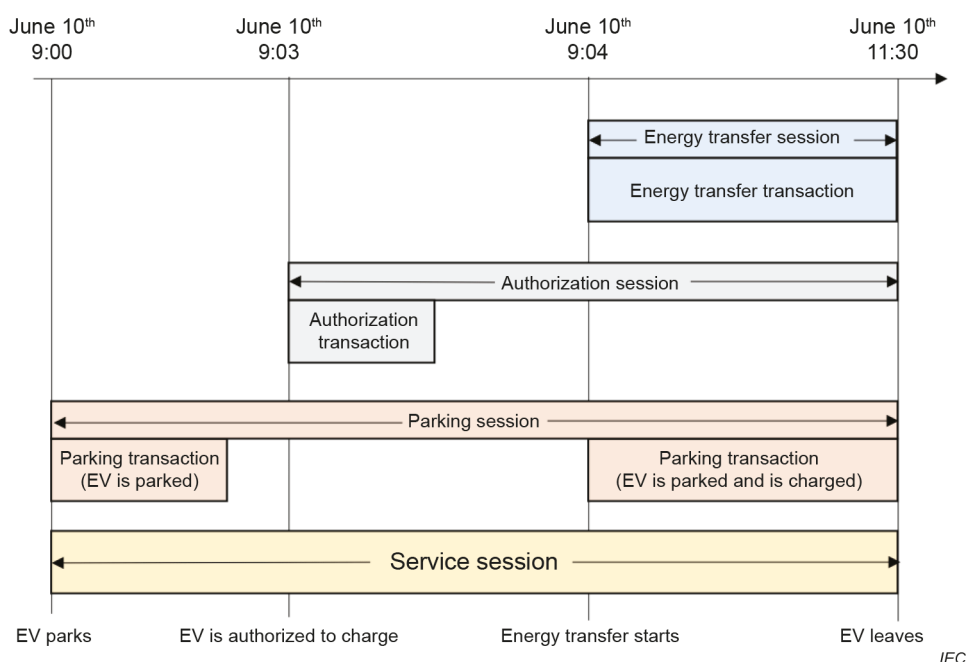


Figure 8 – Example of service session

The service session starts at 9:00 when the EV is parked triggering a parking transaction. Then, at 9:03, for example after the user has plugged, the EV is authorized to charge through an authorization transaction. At 9:04, the energy transfer session starts until 11:30 when the EV leaves, thus terminating the parking, the authorization and the energy transfer sessions.

All the sessions contain related transactions that will be recorded by the CSMS or the CSO. Some of them will be added to the SDR by the CSO.

The CSMS will maintain multiple parallel service sessions corresponding to each EV engaged in a service session as shown in Figure 9.

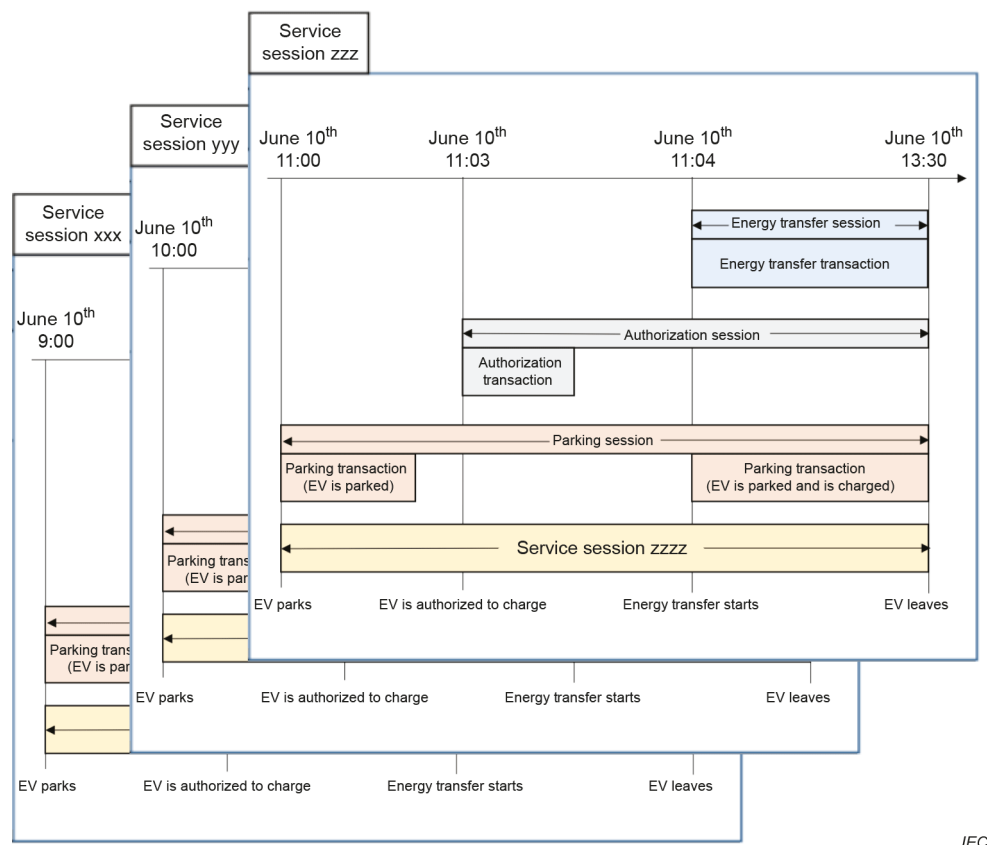


Figure 9 – Example of simultaneous service sessions

Annex C presents, for illustration purposes only, a more complex example of service session including reservation, parking, energy transfer and other services.

7 General requirements

7.1 Generalities

Clause 7 presents the general requirements that implementers of the IEC 63110 protocol shall follow.

7.2 Communication protocol requirements

7.2.1 General

In order to be able to allow the millions of EVs circulating to charge seamlessly in every country in the coming years, it is necessary to choose an appropriate protocol for message transmission that will be able to scale in a secure and efficient way.

The list of requirements presented in Annex B was used to select the message transmission technology. Some of those requirements may be applicable to the IEC 63110 protocol.

7.2.2 Data transfer

In order to transfer raw data like firmware package, certificates, video, large block of data, CS information or inventory, the primary actors shall select, for each transfer, one of the following two methods:

- out-of-band, providing link and method to download the data;
- in-band with or without chunking mechanism.

In-band mechanism should be used for security reasons when appropriate.

Refer to relevant use cases for more information about using the two methods.

7.3 Communication architecture requirements

Clause 4 on architecture describes a model based on the reference model of the SGAM.

Although the detailed implementation of use case steps described in Clause 8 is a decision of implementers, the information exchange between CSMS and CSC as described in this document shall be applied.

CS shall follow the SGAM model and especially the following requirements:

- CSMS and CSC shall communicate using the IEC 63110 protocol;
- CSC shall only communicate with CSMS;
- CSMS and RM shall exchange information using the IEC 63110 protocol.

In addition to the above requirements, the IEC 63110 protocol shall ensure that – if the implementer of the CSMS desires to do so – the defined messages can be used within multi-tiered CSMS architectures in their native form in order to provide basic failover concepts, tiered monitoring, multi-hop in-band data delivery, and similar solutions which are intrinsic to the individual use cases of the CS to CSMS communication. For further details see Clause B.25.

7.4 User specific requirements

Although EVU is not directly in the scope of IEC 63110 (all parts), some parameters originating from the EVU like time of departure or cost or energy limits may be required for some use cases so that they may be communicated to secondary actors, and in consequence IEC 63110 messages shall be capable of transmitting them.

7.5 CSMS implementation requirements

CSMS implementation details are out of scope of this document. However, to ensure interoperability, reliability, security and proof of service, implementers shall apply the following requirements.

- The CSMS shall implement a mechanism able to track and record securely all transactions occurring during a service session of a particular EV.
- Sessions and transactions shall be securely stored in the CSMS before sending the information to CSO at the closure of the service session for SDR establishment.
- The CSMS shall accept transaction change request only by trusted entities.
- The CSMS shall check the integrity of the message requesting the update.

7.6 Interface requirements between CEM, RM and CSMS

Use cases are the basis for these requirements. In some of these use cases, especially those belonging to the energy domain, the RM and the CSMS (either local or cloud) shall exchange information like power range envelope, constraints and aggregated ETPs.

The CEM has an irreplaceable role in the general behaviour of energy in premises and by consequence in the energy allocated to e-mobility. It is likely that, when millions of EVs will be charging in a same period of time, the CEM role in the future will become central to participate in the general balance of the grid.

In order to ensure security and interoperability between IEC 63110 systems and RM, it is then necessary to describe how the CSMS and RM will exchange information. As the IEC 63110 protocol is used for communication between CSC and CSMS and is the basis for the security of the exchange, it appears natural and simple that the RM could also use the same protocol. This will simplify local CSMS interfaces and ensure trusted relations with RM.

Therefore, the RM and CSMS (either local or cloud) shall use the IEC 63110 protocol to exchange information.

7.7 Grid specific requirements

Local grid codes requirements shall be supported by IEC 63110 CS and CSMS implementation.

7.8 DSO requirements

DSO requirements are linked to the existing grid codes.

DSOs, as entities responsible for the quality of electricity and local stability of the grid, may send for example curtailment messages to the CEM in order to avoid or minimize congestion in the area of the CEM premises.

Curtailment requests from DSO shall be applied without undue delay by CSMS and CS.

NOTE 1 In some regions, curtailment requests from DSO are mandatory.

NOTE 2 Curtailment messages can be sent to CSO or to CSMS (either cloud or local). In both cases, a particular attention will be paid by all relevant actors to ensure message integrity all along their transmission. Impact of messages either compromised or originating from a non-trusted source might be catastrophic for the grid stability.

7.9 Cybersecurity requirements

7.9.1 General

7.9 describes security requirements for communication between CSC and CSMS. Further, it explains the rationale of the requirements based on a risk-based approach. This document describes general cybersecurity requirements.

Security concerns impact the protocol, but also other parts and systems involved in the e-mobility environment like RFID cards and readers, certificate management organization, and data integrity including external devices, for example smart phones.

The main general guidance of 7.9 is that the protocol needs to ensure that information in the system will not be readable nor tampered with, by any unauthorized actor.

7.9.2 Security considerations for information

The Table 3 below provides some security considerations regarding confidentiality, integrity and availability for any information that will be transmitted via IEC 63110.

Table 3 shows the security level required by information.

Table 3 – Security considerations by information

Data/information (message types, information exchange)	Brief description	Security considerations regarding		
		Confidentiality (pseudonymity, anonymity)	Integrity (data integrity, timeliness, non-repudiation, authenticity)	Availability (resilience)
EMAID	The EMAID is the e-mobility authentication identifier, used for identification of the contract holder. The definition can be found in the object model document (IEC 63110-1-1).	It identifies a person (data privacy).	It identifies the driver and the contract between driver/car owner and MO.	It is one means to initiate a charging session.
User authentication credential	The user authentication credential is used for identification of the contract holder.	It identifies a person (data privacy).	It identifies a person and a contract and is used for authentication.	It is one means for initiating a charging session.
Firmware image	Firmware of charge point controller	Identity of customer could be sniffed and sent out to external servers. May result in identification of person (data privacy).	Violations of the firmware integrity by accident or by intent (hacked firmware) can cause damage (financial losses, possibly damage of the EVCC, loss of function).	The availability of the controller firmware is essential for the availability of the controller and operation of the charging station. It is necessary for communication between CSMS and CSC.
Controller configuration	List of configuration attributes of EVSE controller	Personal information can be part of the configuration file of the controller.	Violations of the configuration integrity by accident or by intent (hacked firmware) can cause damage (financial losses, possibly damage of the EVCC, loss of function).	A reduction of available services due to a modification of the controller configuration can have a negative business impact.
Power outlet meter values	Electricity meter inside a charging station, which measures the power consumption of the power outlet	The meter data is not assigned to a natural person and is therefore not relevant for data protection/data privacy,	A compromised measurement could lead to a loss of trust from the customers and eventually to a loss of business. Also, all invoices would be wrong leading to a general problem at system level.	CS shall not bill for transactions during meter failure which may lead to business loss.
Grid connection meter values	Electricity meter which is used to measure the power consumption of the grid connection	Energy values could be used to estimate personal behaviour of a driver.	A compromised measurement could lead to a loss of trust from the customers and eventually to a loss of business. Also, all invoices would be wrong leading to a general problem at system level.	CS may need to be stopped during meter failure leading to business loss.

Data/information	Brief description	Security considerations regarding		
		Confidentiality (pseudonymity, anonymity)	Integrity (data integrity, timeliness, non-repudiation, authenticity)	Availability (resilience)
Service detail record (consists of meter values, TimeStamps, session ID, EMAID, etc.)	Data record which is used for billing	The document contains private data that allow identification of a person and a contract.	A compromised document could lead to a loss of trust from the customers and eventually to a loss of business.	CS shall not bill for transactions during meter failure which may lead to business loss.
ISO 15118 EVSE certificate and private key	Certificate on a Supply Equipment Communication Controller (SECC) which is used to establish TLS connection between SECC and EVCC via ISO 15118	Exposed certificate only exposes the identity of the SECC and the identities of issuing CAs, their public keys, and validity periods.	A compromised certificate could lead to a loss of trust from all the actors and eventually to a loss of business.	Where SECC certificate is compromised (stolen) by lack of SECC certificate, or private key prevents the TLS connection. Note that communication that does not require TLS is still possible. However, the communication is unencrypted and may expose personal information of the charging customer.
Diagnostic Logfile	A logfile provided by an EVSE containing diagnostic information	A logfile becoming readable may lead to identification of persons or disclosure of sensitive information.	A compromised logfile may lead to misinterpretation and actions by the CSO that could lead to damage of the EVCC, or loss of function.	A corrupted logfile has little to no impact on EVSE operations.
Audit Logfile	A logfile provided by an EVSE containing information about security relevant events	A logfile becoming readable may lead to identification of security-related events and vulnerabilities of the charging infrastructure as well as contract information of the user.	When a security logfile is compromised (modified or forged) the existing security problems cannot be recognized leaving security holes, or non-existing security problems can be notified to the operator, leading to unnecessary unavailability of the charging infrastructure.	If important security logfiles are lost or corrupted, serious security holes can remain unidentified, causing unrecognized compromise of the system.
SASchedule Tuple (consists of Pmax schedule and sales tariff)	Information about power restrictions and energy prices used to optimize charging the EV	Corrupted SASchedule Tuples will be rejected by the CS and EVSE.	Corrupted SASchedule Tuples will be rejected by the CS and EVSE.	Each CS that received a corrupted SASchedule would not be able to provide a scheduled charging service and would need to fall back to other charging modes.

Data/information (message types, information exchange)	Brief description	Security considerations regarding		
		Confidentiality (pseudonymity, anonymity)	Integrity (data integrity, timeliness, non-repudiation, authenticity)	Availability (resilience)
Charging/Load profile (predicted power over time)	Predicted power profile which is sent by the EV after negotiation with EVSE	Charging profile is calculated by EV based on the user's mobility needs (departure time and target/min/max amount of energy to charge), which leads the user's behaviour patterns and situations.	Maliciously modified power profile can lead to the rejection of charging from EVSE for violating Pmax schedule or can lead to the failure of satisfying the mobility needs of the user, damaging the user satisfaction for the charging service. It can even damage the EV device or cause safety problems by violating the physical limitations of the EV.	Each EV that sends corrupted/incorrect charge parameters might end up damaged from too much power/current.
EVSE status information	Status information about the EVSE like available, occupied, reserved, etc.	It is not known to be related to personal data.	Errors in the EVSE status or non-availability of the status can cause a minor damage (financial losses to station outage, customer complaints, etc.).	An EVSE with error in its status shall stop operation leading to a loss of business and a loss of charging services.
ISO 15118 OEM provisioning certificate	Certificate inside an EV which is used to transfer a contract certificate from a secondary actor to the EV	Exposed certificate of EV only exposes the identity of the EV, PCID, and the identities of issuing CAs, their public keys, and validity periods.	Replacing OEM provisioning certificate with another will prevent the installation of contract certificates. Deliberate change of PCID in an OEM provisioning certificate will cause the installation of a wrong contract certificate, causing possible billing disputes.	Lack of OEM provisioning certificate will only prevent the installation or update of a contract certificate. It won't affect charging if a valid contract certificate is already installed.
Contract certificate	Certificate issued to an EV user or an organization to identify the contract with EMSP and installed in EV	It identifies a person (data privacy).	Changes in contract certificate can cause billing disputes as the certificate indicates which account the charging session needs to be billed to.	It is necessary to allow for installation of contract certificate.
Charge parameter	Parameter sent by the EVCC to optimize the energy transfer, e.g., max./min. current, voltage, required energy, departure time	Charge parameter includes personal information such as departure time, target/min./max. energy request, which can expose the driver's mobility and living pattern	Corrupted charge parameter may lead to misunderstanding of the EV's physical limitations and may cause safety problems and a charge interruption if the EVSE maximum power is exceeded.	Each EV that sends corrupted/incorrect charge parameters might end up damaged from too much power/current.

Data/information	Brief description	Security considerations regarding		
		Confidentiality (pseudonymity, anonymity)	Integrity (data integrity, timeliness, non-repudiation, authenticity)	Availability (resilience)
OCSP responses	Revocation status of the SECC certificate provided to the EV during TLS handshake	Exposing the revocation status of the SECC's certificate does not cause any problems.	Manipulated OCSP can cause revoked certificates to be accepted by EV resulting in privacy issues, or valid certificates to be refused by EV resulting in a denial-of-service attack.	Lack of OCSP responses for a number of chargers will result in a massive denial-of-service attacks.

7.9.3 Threat analysis

7.9.3.1 General

The analysis of threats is based on the architecture and the use cases explained in 4.2 and Clause 8.

7.9.3 considers threat vectors relevant for backend communication protocol.

7.9.3.2 Spoofing

In general, spoofing is pretending to be something or someone other than yourself. In the context of the backend communication protocol, that could be a message that is sent by an attacker to the CSC making them believe the message is from the CSMS. The other way around might also be a threat scenario, to make the CSC believe it is communicating with a fake CSMS. This could be used by an attacker for phishing of credentials (user ID, passwords, PIN codes, etc.).

7.9.3.3 Tampering

Tampering is the modification of data in memory, on network or on disk. It would be conceivable to tamper with load profiles, price information or contract information that is transmitted via the backend protocol.

7.9.3.4 Repudiation

In general, repudiation is to claim that someone claims he or she did not do something or is not responsible for something that happened. Non-repudiation is essential for correct billing.

7.9.3.5 Unauthorized access

Information disclosure relates to entities getting access to data they are not authorized to access. Especially, all information treated as confidential is often subject to attack and certainly requires protection. All information listed in Table 3 marked with high for confidentiality is affected.

7.9.3.6 Denial of service

In general, a denial-of-service attack is used to exhaust a resource that is needed to provide a service. In context of IEC 63110, such resources could be network, CPUs and memory on CSC and CSMS, and the primary equipment on CS as well. Attackers can replay messages in order to flood the network or increase the load on CS and CSMS.

7.9.3.7 Elevation of privilege

In general, elevation of privilege allows someone to do something that he or she is not authorized to do, for example if a normal user is able to apply firmware updates that are normally only authorized to administrators. Typically, weak implementations of authorization checks (or even simple implementation failures) can be used by attackers as a backdoor.

7.9.4 Security requirements

7.9.4.1 General

7.9.4 describes general security-related requirements to mitigate the threats described in 7.9.3.

7.9.4.2 Secure authentication

The IEC 63110 protocol shall provide capability for secure authentication.

7.9.4.3 Secure firmware

The download of firmware images needs to be done in a secure and protected fashion in order to protect the integrity of the firmware images and to avoid tampered firmware images.

For firmware download, IEC 63110 shall support the following.

- The firmware update package shall be digitally signed. Both digital signatures embedded in the firmware image (file) and external signatures shall be supported.
- Firmware download requires authorization.
- The protocol shall provide capability to indicate successful and failed firmware updates, firmware activation and rollbacks.
- The protocol shall provide capability to fall back to an older version in case of failed firmware activation.

7.9.4.4 Secure communication

For implementation of a defence in depth principle, the protocol shall support security in multiple layers. Furthermore, the protocol shall provide end-to-end security wherever it is needed, especially under consideration of multi-hop architectures, for example in case of local CSMS. End-to-end encryption is important for confidential data (especially privacy data). The protocol shall provide capabilities that allow the detection of duplicated messages (in order to manage denial of service attacks).

Strong and secure integrity protection for messages is important to avoid threats like tampering, repudiation, spoofing and denial of service.

7.9.4.5 Access control

The protocol shall provide a capability for fine grained access control. A secure authorization capability shall be used in order to implement a least privilege principle. Strong authentication mechanisms are required to avoid repudiation. The protocol shall support authorized access only and prevent elevation of privileges.

7.9.4.6 Logging of security relevant events

Sufficient logging and alarming are required for prevention of repudiation and can help to detect attacks or frauds.

The protocol shall support at least the following security relevant events:

- successful and failed login attempts;
- firmware uploads (successful, failed, fall back);
- configuration changes;
- other kind of attacks;
- faulty messages (integrity check).

The protocol shall support counters for the security relevant events such as:

- unauthorized attempts to establish a connection;
- login attempts with wrong password, wrong credentials, expired certificates.

The log and alarms shall be protected from unauthorized modifications (tampering) and spoofing. Access to the log may contain useful information for attacker and shall be only accessible for authorized users.

7.9.5 Relation with use cases

Cybersecurity requirements apply universally to all use cases. However, there are specific system use cases that require a precise mechanism in order to ensure the security of the transactions. For example, installation of certificates in the CSMS or in the CS are necessary features described in uses cases.

Figure E.1 in Annex E presents an informative sequence of use cases that could be used to ensure the security of the charging infrastructure.

7.10 Safety requirements

Safety requirements are described in the relevant standards. Refer to IEC 61851-1, IEC 61851-23, IEC 61851-23-1¹ and IEC 61851-25.

IEC 63110 is not designed to be used for any safety relevant features.

In case a safety issue is detected by the CS in one or more EVSEs and reported to the CSMS, the CSMS shall take appropriate measures in order to prevent users from using such EVSEs before a safety assessment is done.

In case a safety issue is detected by the CS in an EVSE during a charging session, the CSMS shall inform the CSO in order to inform the user with the appropriate means that a safety issue has been reported in the EVSE in use and that the e-mobility needs may not be achieved.

8 Use cases

8.1 Generalities

The use cases presented in 8.2 to 8.4 use the methodology presented in IEC 62559-2. The IEC 63110-1 use cases have been inspired by the OCPP 2.0.1 use cases.

¹ Under preparation. Stage at the time of publication: IEC CDV 61851-23-1:2020.

The business use cases presented in Clause 8 capture the common, repeated, deployed or envisioned usages of the e-mobility environment. They propose scenarios and sequences that could be organized differently or with different orders but at the end that will lead to the same information exchange between the primary actors of this document: the CSMS and the CSC. It is the goal of Clause 8 to describe as much exhaustively as possible all actors' requirements during any e-mobility sequences in the scope of this document.

Annex D proposes a classification of the use cases in terms of implementation impacts that can help prioritizing the development of the IEC 63110 protocol.

NOTE In the following use cases, the terms CS is generic, it could refer to the charging station and also to the charging station controller depending on the context.

8.2 Energy domain use cases

8.2.1 General

All the energy domain use cases belong to the service operations cycle. They describe the energy management aspect of the CS. They also define scenarios where secondary actors like CEM, EVU or DSO may influence the charging sessions' behaviour.

From the energy point of view, the core role of the CSMS is to constantly adapt the power demand or production of the CS based on the PRE set by the RM to the CSMS and, at the same time, to continuously announce its power and energy constraints to the RM. This is realized by constantly monitoring any event likely to modify the total aggregated power consumed or produced at the CS level. This constant adaptation is leading to allocation of ETP to each EVSE by the CSMS. ETP could be a profile (power over time) or a single value, it may be positive or negative at some point in time. It is one main role of the CSMS to calculate ETPs based on mobility needs of the EV user, EV and EVSE characteristics and CSMS business logic.

The fact that the sum of all ETPs is always within the PRE set by the RM allows better usage and access to the resources by the EVU and is optimum from the CEM point of view and for the grid. In that sense, the energy management role of the CSMS is mainly to implement what is called "smart charging".

Detailed implementation of the monitoring loop is out of scope, but a general illustration is given in the sequence diagram showed in Figure 10. The Pub/Sub mechanism provided by the IEC 63110 protocol offers the possibility to seamlessly implement this event loop.

This event driven activity is distributed in the CSs and in the CSMS (either local or cloud). For large configurations with many CSZs and EVSEs controlled by one or more CSs, the PRE sent by the RM for a specific CSZ will be processed directly by the CSMS in charge of this CSZ. See implementation examples in Annex A for a comprehensive illustration of the role of the CEM.

The smart charging use case describes this event loop in detail. In this document, it is considered as the main use case for the energy domain. All other use cases are sub-use cases detailing some particular aspects of the exchanges of information from other actors.

Figure 10 describes a possible implementation of this event loop. It is given for illustration purposes. The activities in green are directly within the scope of this document. Each activity has a number attached – see "Scenario step by step analysis" in 8.2.3 for more information about the activities.

8.2.2 Use case list of the energy domain

Table 4 provides a list and a short description of the energy domain use cases.

Table 4 – List of use cases of the energy domain

ID	Use case	Brief description	Life cycle / Sequence
E1	Smart charging management	Settle the best possible ETPs for a group of EVs.	Service operations / Event loop
E2	Charging with demand response	ETPs based on flexibility incentives coming from the market.	Service operations / Event loop
E3	CSMS – RM exchange of information at the initiative of the CSMS	The CSMS and the RM exchange information of energy and power budget.	Service operations / Event loop
E4	CSMS – RM exchange of information at the initiative of the RM	The RM and the CSMS exchange information of energy and power budget.	Service operations / Event loop
E5	Power variation triggered by DSO	How CSMS applies curtailment message from DSO.	Service operations / Event loop
E6	Actors' relations during a V2G session	Relations between actors in order to set up a V2G service.	Service operations / Event loop
E7	Information exchange required to ensure a dynamic energy transfer control	Allow the CS, the CSMS or a secondary actor to provide an ETP	Service operations / Event loop
E8	Providing frequency regulation service by means of decentralized frequency measurements	Providing frequency control service by means of decentralized frequency measurements.	Service operations / Event loop

8.2.3 Smart charging management

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
E1	Energy transfer services	Smart charging management

Scope and objectives of use case

Scope and objectives of use case	
Scope	This use case describes the functions operated by the CSMS to optimize the ETP of each EV and to organize what is usually called "smart charging". In order to realize it, the RM, the CSMS and the CS maintain a monitoring loop of all the events likely to change the power and energy constraints for one or all of the EVs engaged in a service session.
Objective(s)	– Describe information exchanges between CSMS, CSC and RM in order to optimize the ETPs allocated to EVs. – Improve user experience: make sure the EVUs will be able to charge satisfying their e-mobility needs. – Comply with energy constraints: adapt the ETP for each EV according to the PRE allocated to the CSMS by the RM.

Narrative of use case

Narrative of use case
Short description This UC describes the exchange of data between the RM, the CSMS and the CSC in order to fulfil the e-mobility needs of EVs while optimizing the ETPs.
Complete description In order for the CSMS to optimize the ETP and to adapt to any changes in its own energy or power constraints or from the PRE set by the RM, the CSMS will follow the following step, See Figure 10 for a graphic description: Event detection loop At any time during the process, the energy and power constraints and the PRE may be updated due to some event. A non-exhaustive list of events is: – a new EV comes; – an EV pauses or finishes energy transfer; – the maximum power available at CS level has been reached; – the PRE calculated by the CEM has changed; – the energy and power constraints for the CSMS have changed; – one or more EVs want to change their ETP; – dynamic power variations for ancillary services may influence other EV ETPs; – immediate reservation for an EV that will come later; – tariff changes; – internal CSMS trigger (constraints change, ...). Analyse the event and adapt When an event likely to modify e-mobility needs, CS or CSMS energy and power constraints, or RM PRE is detected, the recipient of the event analyses the available power and the energy needed for the new situation after the event. If the event leads to a change in e-mobility needs: in case the existing PRE is not sufficient for serving the existing AETP: go to update loop otherwise return to event detection loop else if the event leads to a change in CSMS energy and power constraints incompatible with current PRE then: the CSMS calculates new energy and power constraints the CSMS triggers the "CSMS – RM information exchange at the initiative of the CSMS" use case return to event detection loop else return to event detection loop end update loop In case of an event is incompatible with existing ETPs: then: the CSMS calculates and updates ETPs for each EV impacted the CSMS updates its own energy and power constraints the CSMS triggers a CSMS constraints change event. the CSMS may notify the CSO to inform user of the event result (this is out of scope of this protocol). go to event detection loop NOTE 1 It is important that smart charging does not prevent the CSMS from making its best efforts to comply with mobility needs.

Narrative of use case	
NOTE 2 In case of ETP changes for a particular EV, the CSMS will without undue delay inform the CSO so it can notify the corresponding EMSP.	
NOTE 3 It is expected that the CSMS will attempt to optimize the new ETP based on every EV specific situation like contract, priority, mobility needs, etc.	

Key performance indicators (KPI)

Key performance indicators			
ID	Name	Description	Reference to mentioned use case objectives
1	User experience	Percentage of users having been able to charge according to their e-mobility needs	Increase user experience
2	Allocated power usage	Comply with energy constraints and ability to handle changing power allocations	Comply with energy constraints

Use case conditions

Prerequisites	
1	There is a CEM in the premises and an RM responsible for the CSZ where there is a CS managed by a CSMS.

General remarks

General remarks
Charging technology agnostic: this use case is not dependent on any charging technology. It only describes the information exchange between CSMS, RM and CS. It is up to the CS to internally handle different charging technologies like CHAdeMO, ISO 15118, IEC 61851 series or wireless power transfer (induction).

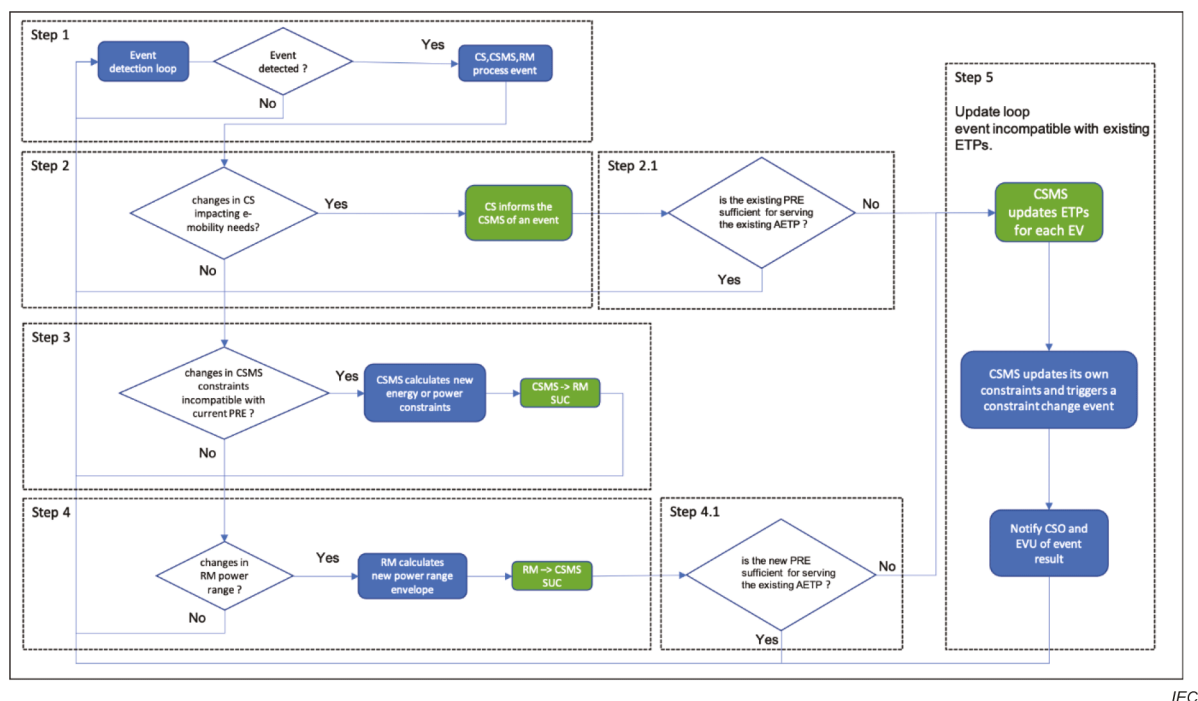
Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition
1	Smart charging management	This scenario presents the steps to manage the smart charging	CSMS, CS	An event		

Scenario step by step analysis

See Figure 10 for details on the corresponding sequence diagram.

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
1	CS, CSMS or RM detected an event	A new event that is likely to change e-mobility needs, the PRE or the AETP is detected and processed by the recipient of the event.	RM, CS, CSMS		
2	CS processes a change impacting e-mobility needs	In case the event could lead to a change in e-mobility needs, the CSC informs the CSMS of the event. For example, a new EV just plugged.	CS	CSMS	Info1- CSC sends the event to the CSMS
2.1	process a change in e-mobility needs	If the existing PRE is not sufficient for serving the existing AETP then branch to step 1.5, otherwise go back to event detection loop.	CSMS	CS	See step 5
3	process a change in CSMS constraints	If the new CSMS constraints are incompatible with the current PRE then the CSMS requests the RM to update the PRE. See "CSMS – RM exchange of information at the initiative of the CSMS" use case. Otherwise go back to event detection loop.	CSMS, RM	CSMS, RM	See "CSMS – RM exchange of information at the initiative of the CSMS" use case
4	process a change in PRE	If the event leads to a change in the PRE, then the RM requests the CSMS to update the ETPs. See "CSMS – RM exchange of information at the initiative of the RM" UC.	RM, CSMS	RM, CSMS	See "CSMS – RM exchange of information at the initiative of the RM" use case
4.1	confront the updated ETPs with the existing AETP	If the new PRE is not sufficient to serve the existing AETP then branch to step 1.5, otherwise go back to event detection loop.	CSMS	CS	See step 5
5	Update loop: process an event incompatible with existing ETPs	The event detected is leading to a situation incompatible with existing ETPs. The CSMS updates the ETPs for each EV impacted. The CSMS updates its energy and power constraints and triggers an event corresponding to a change in CSMS constraints. The CSMS may notify the CSO to instruct of the event result.	CSMS	CS	Info2 – Send ETPs for each EV



IEC

Figure 10 – Smart charging sequence diagram

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	CS sends event to the CSMS	Nature of the event. Examples: – a new EV has been plugged; – an EV has been unplugged; – an EV has updated its departure time.
Info2	Send ETPs to each EV	ETPs for each EV impacted

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	ETPs transmission to CSC for each EV	In case of ETP changes for a particular EV, the CSMS shall without undue delay communicate to the appropriate CSC the new ETP
Req2	Traceability	All events having an impact on ETPs shall trigger an energy transfer transaction

8.2.4 Charging with demand response

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
E2	Energy transfer services	Provide charging with demand response

Scope and objectives of use case

Scope and objectives of use case	
Scope	The scope of this BUC is to describe the procedure of aggregated EV charging based on incentive from secondary actors.
Objective(s)	Deliver a charge service complying with user e-mobility needs. Optimize charging based on secondary actor's incentives.
Related business case(s)	Deliver energy services.

Narrative of use case

Narrative of use case
Short description
This UC describes the exchange of information between CS and CSMS needed to operate a demand response program mandated by a SA.
Complete description
Demand response programs are used to influence energy consumption or electricity demand during constrained supply conditions. Such a program usually offers incentives to customers in the form of special tariffs, reimbursement or even payment. SAs interested in demand response programs are DSO, FO, BRP. Depending on the incentive conditions proposed by SAs, the energy transfer to or from the EVs can start immediately or not. Also, after the energy transfer has started, it could be altered or paused for a certain period of time. As the CSMS can only receive messages from RM, CSC or CSO, this use case considers only demand response messages coming from either the RM or the CSO. Demand response messages received directly by the EV are not in the scope of this use case. In both cases, the message will be presented to the CS in the form reflecting the incentives received by the CSMS (e.g., a new energy transfer plan). EVU may accept to participate, for example delaying or pausing the charge based on incentive. EVU may also refuse any changes in the charging plan and e-mobility needs. NOTE 1 The CSMS will record the status of charge (normal ongoing charging or charge under control of a flexibility actor), when it started and when it finished in order to fill in the SDR. The corresponding energy transfer session and transactions will be also updated. NOTE 2 The application of any demand response program does not prevent the CSMS to do its best effort to fulfil the mobility needs of the EVs connected.

Key performance indicators (KPI)

Key performance indicators			
ID	Name	Description	Reference to mentioned use case objectives
1	Transfer energy into the EV battery	Percentage of the charge reached between connection and disconnection by the user	Deliver a charge service complying with user e-mobility needs
2	Get benefit of the incentives	Percentage of demand response messages accepted	Optimize charging based on secondary actor's incentives.

Use case conditions

Prerequisites	
1	The EVU is identified and authorized to charge.
2	The CSMS can receive incentive messages from SAs: after reception of the incentives, the CSMS, based on its parameters, can adapt the incentive to the local energy situation and then transmit it to the CS.

Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition
1	Charge with demand response	This scenario describes the procedure of EV charging based on incentive from secondary actors	CSMS	Incentives received		

Scenario step by step analysis

The following steps 1 and 2 are independent, and not sequential

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
1	The CEM receives incentives from SA and RM sends a new energy transfer plan to the CSMS	The CEM receives incentives to modify the demand of the premises The CEM internally calculates a new power allocation to the CSMS based on the terms of the incentives. For example: – in case the incentives are favouring an increase of the demand due to excess of solar production in the country, the CEM will allocate more power to the CSMS; – in case the price of energy suddenly increases during the next two hours, the CEM may allocate less power to the CSMS during those two hours. This CEM internal calculation is out of scope. The new CSMS energy transfer plan, calculated by the CEM, can be sent to the CSMS by the RM.	SA, CEM, RM	CSMS	Info1 – CEM sends PRE to CSMS

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
2	CSMS sends the new ETP to CSC due to incentives received from SA	– Incentives can be received asynchronously (e.g., every week day + weekend days) or in real time when the CEM or CSO is updated by a secondary actor. – CSMS informs CSC of the incentives. CS will send the information to the impacted EVSEs. – The EVs being engaged in a schedule mode ISO 15118 session will receive a renegotiation message with a new proposal of schedule. – Information about incentives can be tariff, max power, CO₂ level variations schedules or just a simple signal indicating a peak hour.	CSMS	CSC	Info2 – Send ETPs for each EV
3	CS is informed of incentives received from CSMS	The CS informs all EVSEs of the current incentives. EV may decide or not to get benefit of the incentives.	CS		

Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
Info1	RM send PRE to CSMS	PRE	
Info2	Send ETPs to each EV	ETPs for each EV impacted	

Requirements

Requirements		
Requirement R-ID	Requirement name	Requirement description
Req1	Information exchange	Whenever receiving an incentive message from an SA, the CSMS shall transfer to CSC the appropriate information in order for the CS to inform all EVSEs of the incentive.

8.2.5 CSMS – RM exchange of information at the initiative of the CSMS

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
E3	Energy transfer services	CSMS – RM information exchange at the initiative of the CSMS

Scope and objectives of use case

Scope and objectives of use case	
Scope	Describe the information exchange between the CSMS (either local or cloud) and RM. The CEM is responsible for the management of the energy behind a SGCP (e.g., in a building or in a home). The CSMS is responsible for management of one or many charging stations installed behind a grid connection point (e.g., in a building or in a home). The CEM optimizes energy and power allocation between resources (load, storage and production systems). One of the resources is the charging infrastructure managed by a CSMS. The CEM sets power limits to the CSMS, via the RM responsible for a charging site zone. The CSMS optimizes e-mobility energy transfers based on CEM power limits, e-mobility needs and contracts terms and business logic. NOTE This use case describes an exchange of messages initiated by the CSMS. The use case "RM – CSMS information exchange at the initiative of the RM" describes the other way around situation.
Objective(s)	Objective: The CSMS and the RM exchange information about power limits and aggregated energy transfer plans. This exchange of information has the objectives of: – for the CSMS, optimizing e-mobility needs, while considering secondary actors' needs; – for the CEM (via the RM), optimizing the use of energy in the premises taking in account CSMS power and energy constraints.

Narrative of use case

Narrative of use case	
Short description	
This UC describes the information exchange between the CSMS and the RM at the initiative of the CSMS	
Complete description	
The CEM and the CSMS maintain an event loop monitoring changes in energy or power constraints in their respective scope. The CSMS constantly calculates the AETP based on the information it exchanges with the CSC (and associated EVSEs). If that AETP does not fit into the existing PRE set by the RM, then the CSMS calculates new power and energy constraints that would allow the energy transfer plan to fit, then: 1) the CSMS informs the RM of its new power and energy constraints; 2) the RM replies to the CSMS with an updated PRE which satisfies the CSMS's constraints; 3) after communicating the relevant ETPs to the impacted EVSEs, the CSMS informs the RM of the new AETP.	

Use case conditions

Prerequisites	
1	The CSMS and the RM have established a trusted communication.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	Exchange of information between CSMS and RM	CSMS and RM exchange messages in case of external event likely to modify the current aggregated energy transfer plan of the CSMS. NOTE Thresholds can apply to an event in order to avoid small variations flooding CSMS-RM with frequent messages. See also 8.2.3 (smart charging use case) for a description of the information exchanged between RM, CSC and CSMS.	CSMS, RM, CS	End conditions: in case of success: – new PRE and AETP are in effect. in case of failure: (can be due to communication issues between the RM and the CSMS) – CSMS retries communication with RM.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
1	CSMS informs the RM about the new power and energy constraints	The CSMS sends the new power and energy constraints to the RM.	CSMS	RM	Info1 – CSMS sends power and energy constraints to RM
2	RM gets PRE from the CEM	CEM decides and instructs the RM with new PRE. This is an out-of-scope internal process in the CEM.	CEM RM		
3	RM sends a new PRE to CSMS	The RM sends to the CSMS the new PRE.	RM	CSMS	Info2 – RM sends PRE to CSMS
4	CSMS optimizes ETP for each EV	The CSMS calculate a new energy transfer plan for each EVSE impacted by the new power ranges envelope and communicates them to the relevant CS(s). See 8.2.3 (smart charging use case) for steps not related to RM-CSMS communication.	CSMS		
5	CSMS calculates the AETP and transfers it to the RM	– The CSMS aggregates the energy transfer plans. – The CSMS updates the corresponding Energy Transfer Transactions. – The CSMS sends to RM, the AETP.	CSMS	RM	Info3 – CSMS sends to RM the aggregated energy transfer plan

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	CSMS sends power and energy constraints to RM	power and energy constraints (range of upper and lower limits)
Info2	RM send PRE to CSMS	PRE
Info3	The CSMS sends to RM, the AETP	AETP