IEC 63110-1

Edition 1.0 2022-07

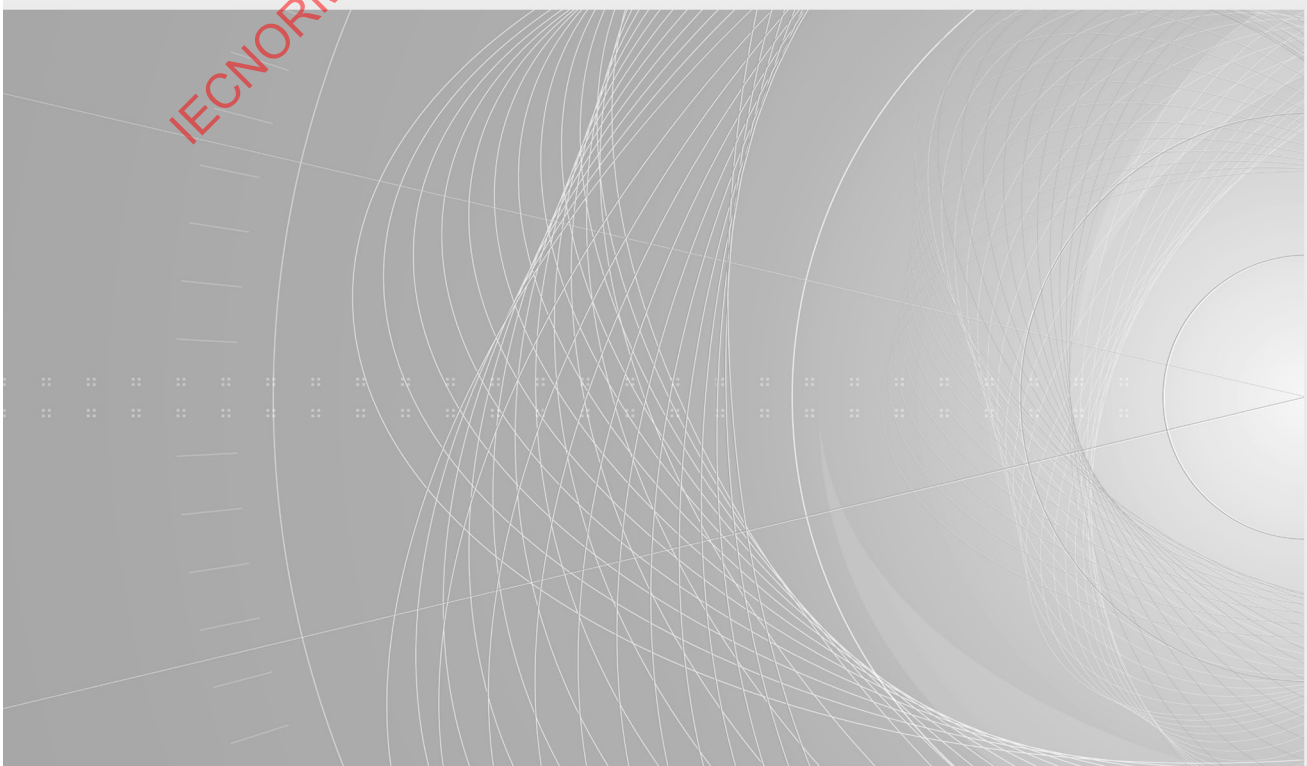
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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



IEC 63110-1:2022-07(en-fr)

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

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

IEC 63110-1

Edition 1.0 2022-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

CONTENTS

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.

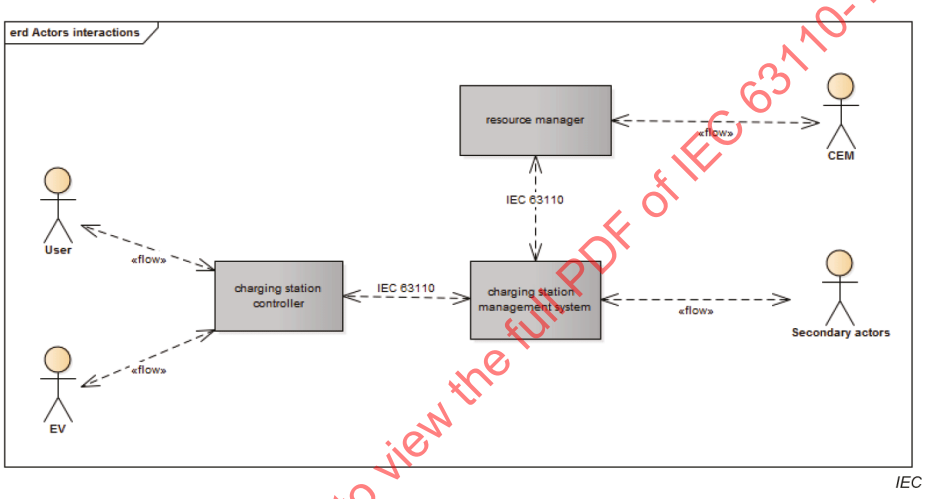


Figure 1 – Actor's interactions

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.

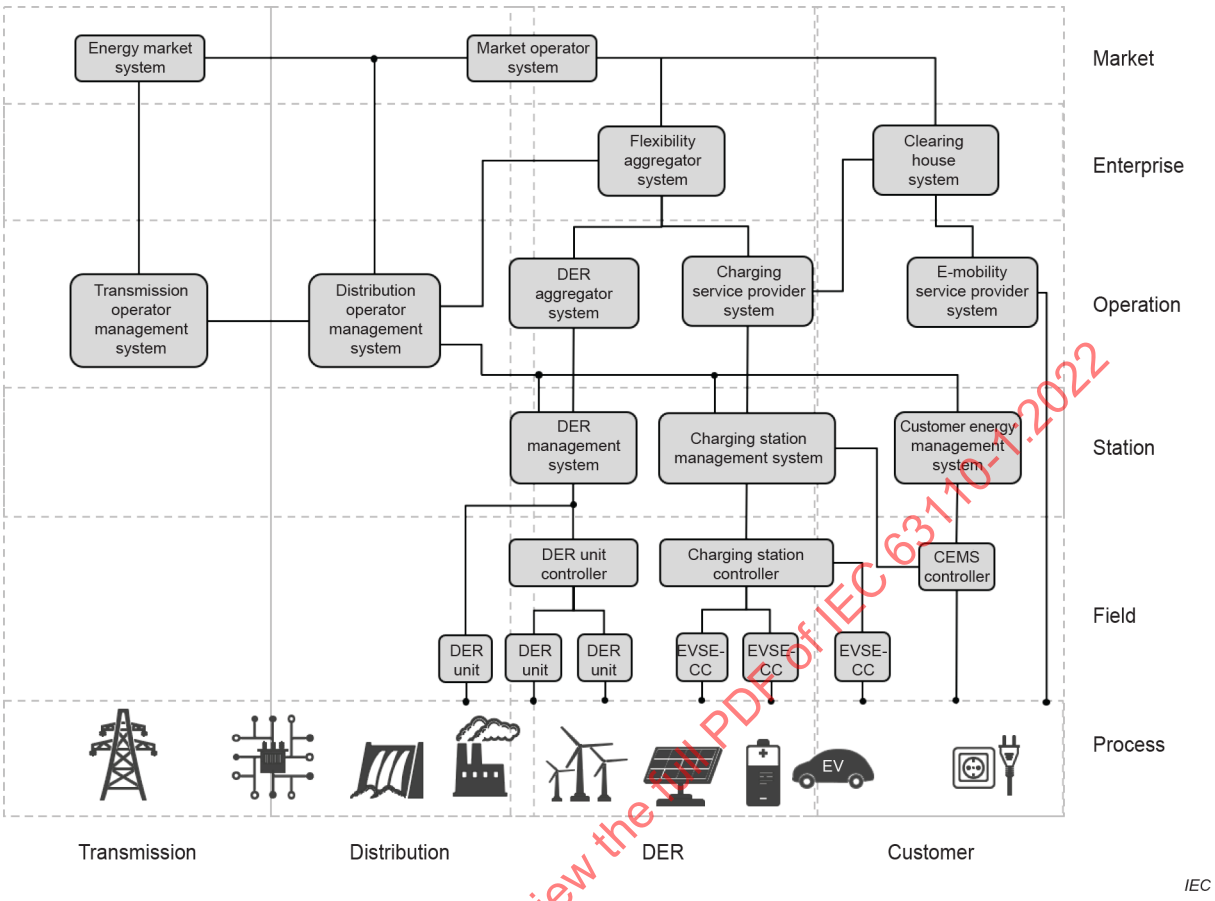


Figure 2 – Architecture model of the component layer

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).

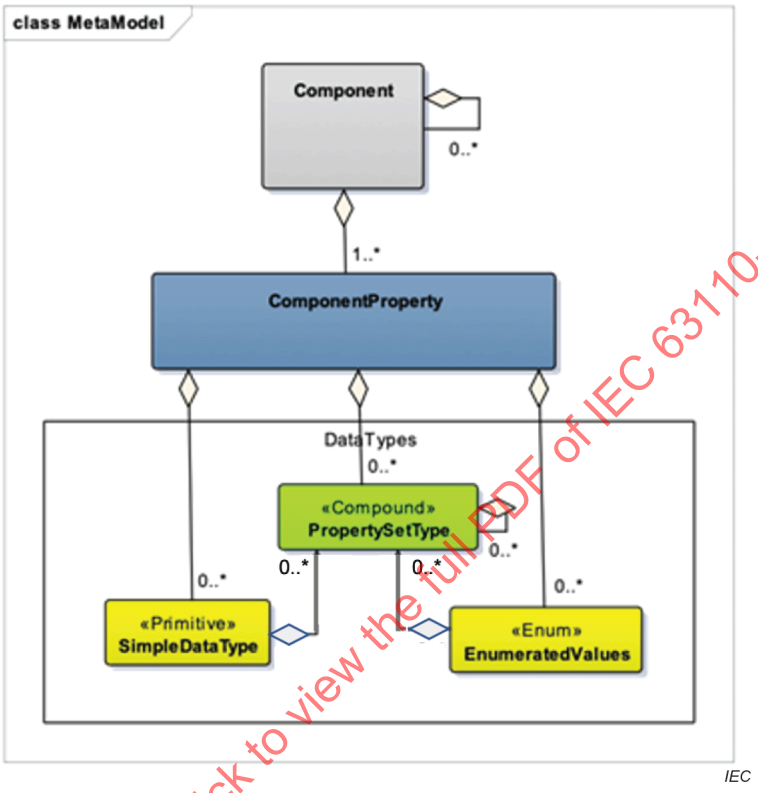


Figure 3 – IEC 63110 metamodel

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.

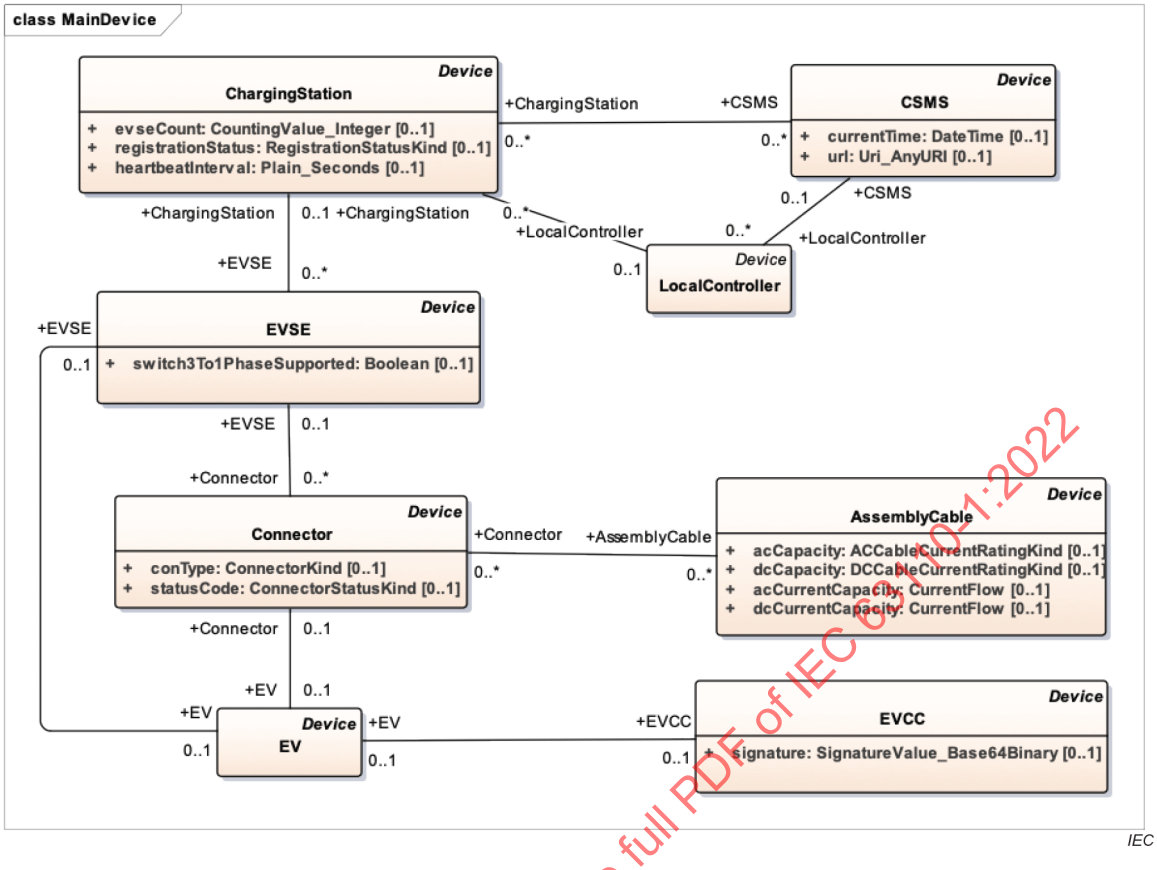


Figure 4 – IEC 63110 top-level architecture

4.4 Actors and system view

Figure 5 shows the different actors interacting in IEC 63110.

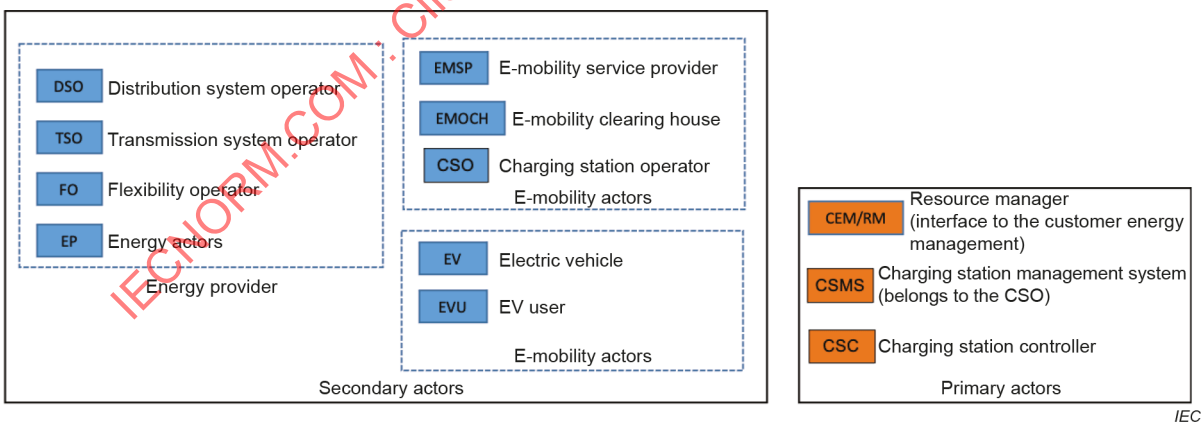


Figure 5 – Actors

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.

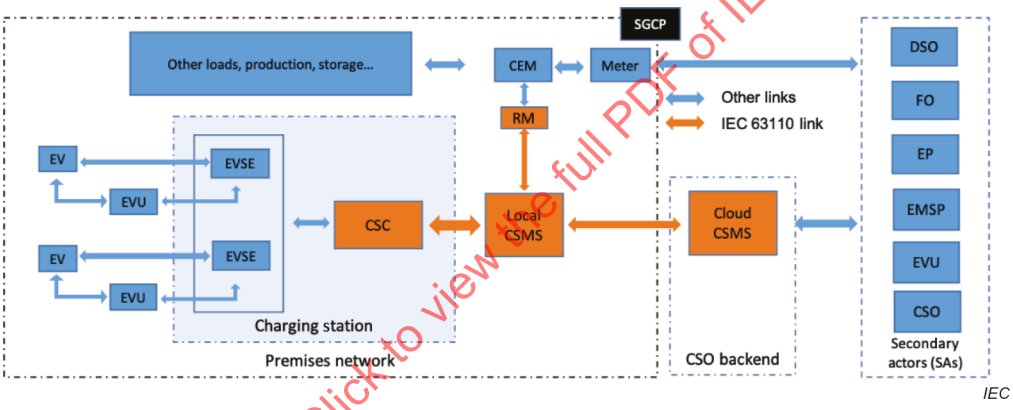


Figure 6 – Generic communication architecture – System view

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.

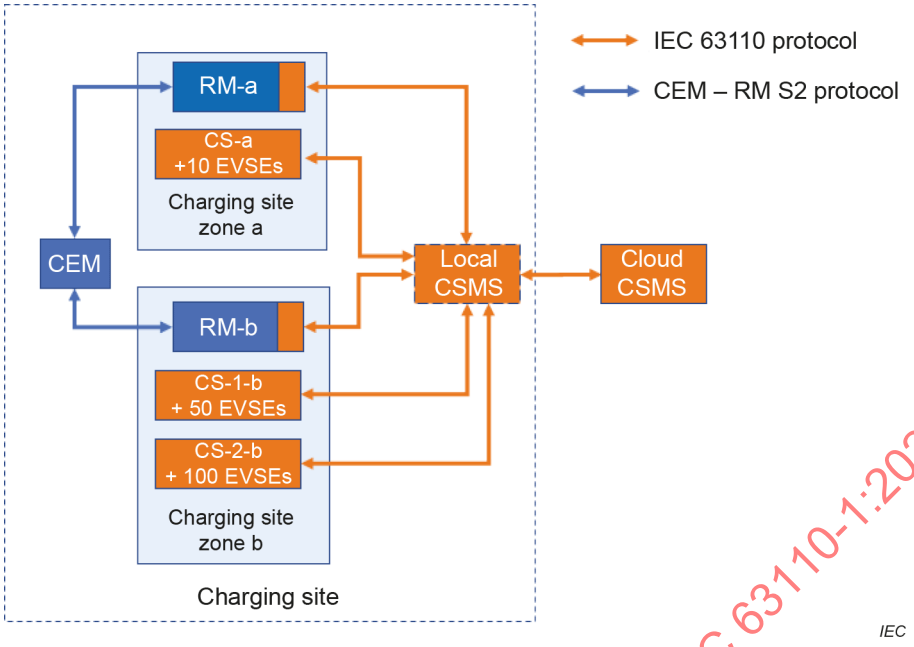


Figure 7 – Charging site with two charging site zones controlled by a CSMS

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 renegotiation, 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.

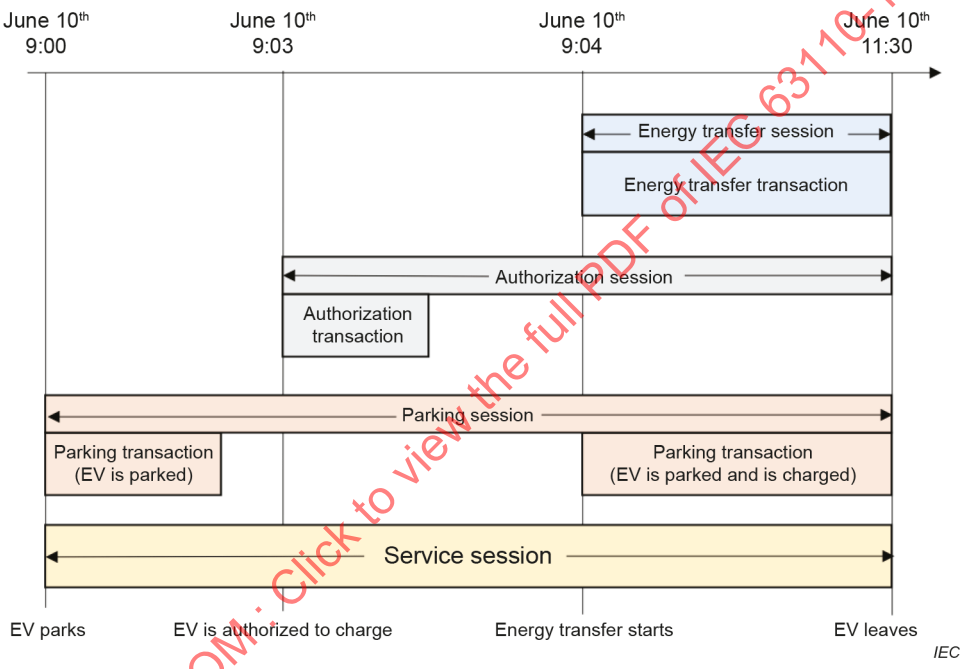


Figure 8 – Example of service session

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.

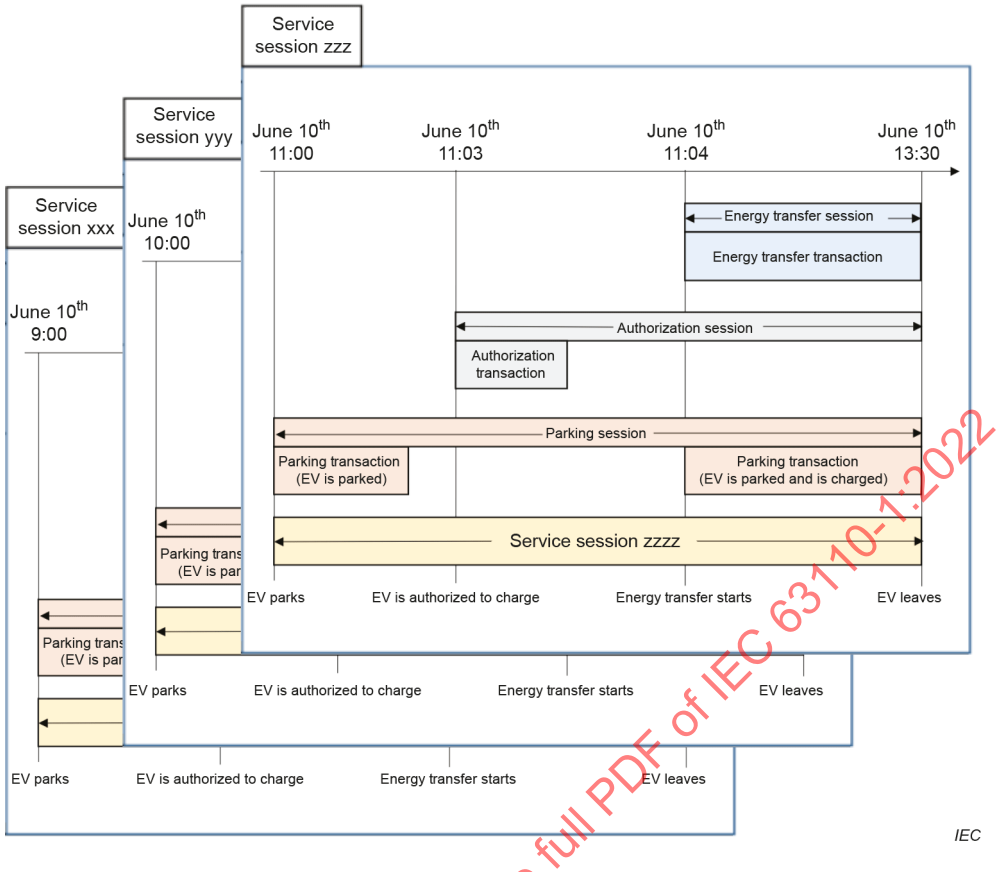


Figure 9 – Example of simultaneous service sessions

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 (message types, information exchange)	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 (message types, information exchange)	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 results 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 61851-23-1[1] 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

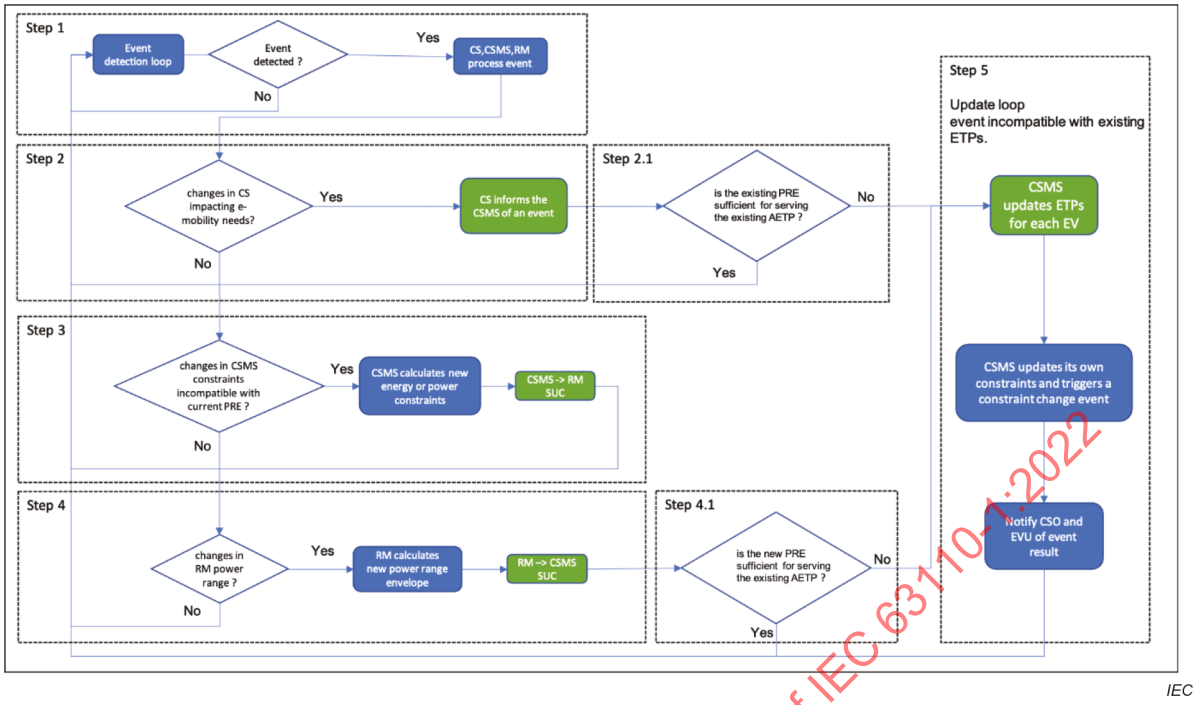


Figure 10 – Smart charging sequence diagram

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, CO_2 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

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	CSMS informs the RM	CSMS shall update the RM with new power and energy constraints whenever their changes impact operation.
Req2	RM obligation	The PRE shall satisfy the latest power and energy constraints communicated.
Req3	CSMS obligations	The aggregated ETP provided by the CSMS shall stay within the PRE received from the RM.
Req4	RM obligations	Whenever the CSMS updated the RM with new power and energy constraints, the RM shall answer by setting a new PRE without undue delay.

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

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
E4	Energy transfer services	RM – CSMS information exchange at the initiative of the RM

Scope and objectives of use case

Scope and objectives of use case	
Scope	Describe the information exchange between the RM and the CSMS (either local or cloud). 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 PRE to the CSMS, via the RM responsible for a charging site zone. The CSMS optimizes e-mobility energy transfers based on e-mobility needs, EVSE characteristics and contracts terms. NOTE This use case describes message initiated from the RM. The use case "CSMS – RM information exchange at the initiative of the CSMS" describes the other way around situation.
Objective(s)	Objective: The CSMS and the RM exchange information about PRE and aggregated ETP. This exchange of information has the objectives of: – for the RM, optimizing the use of energy in the CSZ; – for the CSMS, optimizing e-mobility needs, while considering RM constraints.

Narrative of use case

Narrative of use case
Short description
This SUC describes the information exchange between the RM and the CSMS at the initiative of the RM
Complete description
The CEM and the CSMS maintain an event loop monitoring changes in energy or power conditions in their respective scope. When the RM is instructed by the CEM of an energy or power condition change affecting the effective PRE of its charging site zone (e.g., more or less power is available in the CSZ) then: – the RM sends a new PRE to the CSMS that still satisfies as much as possible the latest power and energy constraints sent by the CSMS. – based on the new PRE, the CSMS calculates new ETPs for each EV impacted and informs the CS (out of scope load balancing algorithms could be used by the CSMS); – the CSMS informs the RM of the new aggregated ETP.

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 RM and CSMS	In case of external event likely to modify the current PRE, the RM sends to the CSMS a new PRE. The CSMS modifies accordingly the ETPs and the AETP. NOTE Thresholds can apply to an event in order to avoid small variations flooding CSMS-RM with frequent messages. See 8.2.3 (smart charging management) for a description of the information exchanged between RM and CSMS.	RM, CSMS	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	RM sends new PRE to CSMS	The RM sends to the CSMS new PRE	RM	CSMS	Info1 – RM sends PRE to CSMS
2	CSMS optimizes ETP for each EV	The CSMS calculates a new ETP for each EVSE impacted by the new PRE and communicates them to the relevant CS(s). See 8.2.3 (smart charging BUC) for steps not related to RM-CSMS communication	CSMS		
3	CSMS calculates the AETP and transfers it to the RM	– The CSMS aggregates the ETPs. – The CSMS updates the corresponding Energy Transfer Transactions. – The CSMS sends to RM, the resulting AETP.	CSMS	RM	Info2 – CSMS sends to RM the AETP.

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	RM sends PRE to CSMS	PRE
Info2	The CSMS sends to RM the resulting AETP	AETP

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	RM sends PRE to CSMS	The RM shall transfer to CSMS a new PRE whenever the energy conditions of the building or of the CSZ are likely to impact operation of the CSMS.
Req2	CSMS obligations	The AETP provided by the CSMS shall stay within the PRE received from the RM

8.2.7 Power variation triggered by DSO

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
E5	Energy transfer services	Power variation triggered by DSO

Scope and objectives of use case

Scope and objectives of use case	
Scope	Power variation triggered by DSO
Objective(s)	Execute without undue delay the curtailment message received from the DSO.
Related business case(s)	Deliver energy services

Narrative of use case

Narrative of use case
Short description
How CSMS applies curtailment message from DSO
Complete description
Different services are employed by TSO, DSO, and FOs to keep the grid stable and operating: frequency reserve, voltage control, demand-response, congestion management, etc. Some services are automatic (e.g., frequency), some are subject to market program with days or hours ahead (e.g., DR) and some may be mandatory like curtailment by DSO. Curtailment occurs when the DSO has local issues in the geographical area of the SGCP. As any such resource, the DSO may have installed a device that is in charge of controlling the power usage in case of emergency. This use case supposes that the said device is able to communicate the DSO curtailment messages to the CEM. The CEM calculates the fraction of the curtailment allocated to the charging site zone and informs the CSMS via the appropriate RM. NOTE 1 It is also technically possible that curtailment messages from DSO may be received by the CSO backend. This situation is not in scope of this use case. Look at the use case "CSMS – RM exchange of information at the initiative of the CSMS" for more information on that situation. NOTE 2 The CSMS keeps track of the curtailment event so it can be reflected in the SDR and the user can be informed. NOTE 3 In normal electrical conditions, the DSO doesn't send curtailment messages. A curtailment message sent by the DSO means that the geographical area is under abnormal electrical conditions. The curtailment message needs to be applied in order to help the grid to return to normal conditions. The CSMS shall handle curtailment messages from DSO following the steps below: 1) The CSMS receives a message from the RM that curtailment of power (increase of production or reduction of consumption) is required, and curtailment needs to start without undue delay. Since the curtailment message comes from a DSO, the RM indicates that the curtailment is mandatory. The curtailment message takes the form of a new PRE. 2) Based on the new PRE reflecting the curtailment objectives, on the actual aggregated power and on mobility needs, the CSMS calculates a new ETP for each EV. 3) The CSMS transfers to the CSC the new ETPs for each EV, indicating that their application is mandatory. 4) The CS shall ensure that the new ETPs are used by applying all possible enforcement to EVSE (e.g., switching off relays if needed). 5) The CSMS sends the AETP to the RM.

Key performance indicators (KPI)

Key performance indicators			
ID	**Name**	**Description**	**Reference to mentioned use case objectives**
1	Fulfilment of the curtailment	Spread in kilowatt hours (kWh) between the curtailment of power budget allocated to the CSMS and the effective power/energy consumed or produced at the CS connection point.	Execute without undue delay the curtailment message received from the DSO.

Use case conditions

Prerequisites	
1	– A CEM is present and is able to receive messages from the DSO. – An RM is present.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Pre-condition	Post-condition
1	Curtailment message reception	The CSMS receives a message from the RM that curtailment of power ((increase or reduction of production, or reduction or increase of consumption) is required and needs to start without undue delay.	CSMS, CS, 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	RM sends a curtailment message to the CSMS	A curtailment message, in the form of a new PRE, is sent by the RM to the CSMS requesting a power variation.	RM	CSMS	Info1 – RM sends a curtailment message to the CSMS
2	CSMS receives and processes a curtailment message	Based on the new PRE, the CSMS calculates ETPs. This activity is out of scope of this document.			
3	CSMS sends to the CSC the new ETPs	The CSMS sends the new ETPs for each EV impacted by the curtailment.	CSMS	CSC	Info2 – CSMS sends the new ETPs to the CSC
4	CSMS calculates the AETP and transfers it to the RM	– The CSMS sends the AETP to the RM. – The CSMS updates the corresponding Energy Transfer Transactions.	CSMS	RM	Info3 – CSMS sends to RM the AETP.

Information exchanged

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	The RM sends a curtailment message to the CSMS	The new PRE to be applicable A parameter indicating that the curtailment came from the DSO	
Info2	CSMS sends energy transfer plans to CSC	ETPs	
Info3	The CSMS sends to RM, the aggregated energy transfer plan	AETP	

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	New ETPs	The CSMS shall allocate ETP to each EV based on PRE, mobility needs, EVSE and EV characteristics.
Req2	Curtailment	The CSMS shall instruct the CS of the mandatory nature of new ETPs.
Req3	Inform RM of curtailment status	The CSMS shall send the new AETP to the RM.

8.2.8 Actors' relations during a V2G session

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
E6	Energy transfer Services	Actors' relations during a V2G session

Scope and objectives of use case

Scope and objectives of use case	
Scope	Actors' relations during a V2G session
Objective(s)	Describe exchange of information between actors involved in a V2G session
Related business case(s)	Deliver energy services

Narrative of use case

Narrative of use case
Short description
This UC only describes relations between actors in order to set up a V2G service. It does not describe the necessary steps to operate the service on CS side.
Complete description
Description of the use case. – The CEM receives a message from DSO, FO or from another SA requesting that energy injection into the grid may start. The request may contain limitations in power, energy, and time. – Based on CEM instruction, the RM sends to the CSMS the new PRE reflecting the injection request (see "CSMS – RM exchange of information at the initiative of the RM" use case) – Based on the new PRE, on mobility needs, on FO's contracts status and other constraints, the CSMS sends to CSC a series of new ETPs directed to the EVs impacted. – Each CS applies the energy transfer plan for all EVs impacted. NOTE 1 The CSMS only sends ETPs for each EV involved, after receiving from the CSO the confirmation of the contract validity of the user regarding energy injection into the grid by a secondary actor. The check is done by the CSO and is out of scope. NOTE 2 There is a need for a pre-configuration of the CS depending on mandatory local rules or a continuous update of the EVSE grid functions according to market rules.

Use case conditions

Prerequisites	
1	EVU agrees to V2G sessions: The EVUs of the EVs able to charge and discharge have expressed their consent to V2G to an SA (e.g., an FO) and their mobility needs (target SOC and time of departure).
2	EVSEs are allowed to operate V2G: EVSEs are certified to discharge energy into the grid.
3	Discharging capabilities of the CS: The CS has the capability to accept discharge energy from the EVSE and has been certified to do so.
4	EVs are able to operate bidirectional energy transfers: All or some EVs are able to charge and discharge.
5	Grid codes: The CS is able to comply with the local grid code requirements.
6	Contracts: The EVUs participating in the V2G service have a valid contract with an FO.
7	For each EV, the CSMS gets from the CSO the operational permission if injecting energy into the grid is possible or not. This might depend on having an appropriate contract, but the way this contract check works is out of scope.

Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Actors' relations during a V2G session	Actors exchange information during a V2G session	CSMS, CS	SA, 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	The CEM receives a V2G trigger	The CEM receives a message from DSO, FO, or other SA that energy injection into the grid may start. The message contains the power and energy conditions and duration of the V2G episode. The CEM sends to the RM the relevant parameters in the corresponding CSZ.	SA	CEM, RM	
2	The RM informs the CSMS of the new PRE	The RM informs the CSMS of a new PRE. The PRE impact could influence energy transfer plans as power need to be injected into the grid.	RM, CSMS	RM, CSMS	See "CSMS – RM exchange of information at the initiative of the RM" use case
3	The CSMS sends to CSC the new ETPs	Based on the new PRE, on mobility needs and on FO's contracts status, the CSMS sends to CSC the new ETPs for each EV listed by the CSO as able to operate V2G.	CSMS	CSC	Info1 – Send ETPS for each EV
4	The CSMS updates grid code in EVSE	If an update of an EVSE grid codes configuration is necessary as a result of step 3, parameters shall be provided to the responsible CS.	CSMS	CSC	See "Monitor a CS" use case

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	Send ETPs to each EV	ETPs for each EV impacted

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Information for SDR	During and at the end of the V2G session, the CSC shall send to the CSMS the necessary energy information in order for the CSO to fill in the SDR elements for each EV involved or not in the V2G episode.

8.2.9 Information exchange required to ensure a dynamic energy transfer control

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
E7	Energy transfer services	Information exchange required to ensure a dynamic energy transfer control

Scope and objectives of use case

Scope and objectives of use case	
Scope	CS-CSMS dynamic energy transfer control information exchange description
Objective(s)	– Allow the CS, the CSMS or a secondary actor to provide an ETP. – Proof of service: The objective for the CSMS is to allow the dynamic mode service and to track the EV engaged in a dynamic mode session in order to collect all the energy transferred to ensure the proof of service required by the secondary actor who triggered the dynamic control mode.

Narrative of use case

Narrative of use case
Short description
This use case describes the information exchange between the CS and the CSMS in case some EVs are engaged in a dynamic energy transfer control. In dynamic energy transfer control, the energy transfer may be controlled by a secondary actor like an FO resulting in an updated ETP, that the EV will follow with a best effort strategy.
Complete description
Dynamic energy transfer control mode can be used to allow a quick response to changes of external conditions. This type of control is useful for grid services but also when fine grain timing control of energy transfer is necessary. Examples of situations where dynamic energy transfer control can be used: – ancillary services (frequency regulation, reactive injection onto the grid, …); – in unpredictable constrained environment where schedule is not optimum; – load balancing within the charging site is easier with dynamic energy transfer control. NOTE 1 The CSMS can control the energy transfer by means of an ETP labelled as dynamic (could be a boolean in the ETP transfer message). NOTE 2 In order to establish the ETP, the CSMS can use inputs from an SA like an FO for example. NOTE 3 In dynamic energy transfer control, an ETP sent by the CSMS will be considered by the EV as a plan of power targets to be reached in a best effort strategy. NOTE 4 Dynamic energy transfer control is not limited to V2G or bidirectional energy transfer. Simple charge can also get the benefit of it. NOTE 5 The way the EVSE is effectively controlled is out of scope. It could be through ISO 15118 dynamic control mode or PWM variation for example. EXAMPLE In home, the CEM could do load balancing by calculating in real-time a PRE allocated to the CSMS in order to keep enough energy for other loads. **Detailed description:** When frequent changes of the power conditions require to switch to dynamic energy transfer control, then the EVs willing to implement dynamic energy transfer control need to receive adapted ETPs. For that the following steps are necessary: – The CSMS can receive a PRE either from RM or constraints via the CSO or generated internally. – The CSMS processes the PRE or constraints received, and sends to CS new ETPs which execute them. – The CSMS configures the CS reporting. The CS can be specifically configured to allow the CSMS to collect the necessary information to ensure the proof of service and user information. See "Monitor a CS" use case.

Narrative of use case
– The CSMS monitors the status of the CS, EVSEs and, if possible, EVs engaged in the dynamic energy transfer. – The CSMS calculates the AETP and sends it to the RM. NOTE 1 The beginning of the energy transfer can mark the start of the power measurements necessary to the proof of service. It also triggers a new energy transfer transaction. NOTE 2 The CSMS can inform the CSO that a dynamic energy transfer control has been engaged with the relevant EVs. NOTE 3 Point 5 needs to be evaluated in term of bandwidth. IEC 63110 needs to avoid communication procedure and operation where micro-management of CS by CSMS would saturate the communication flow. NOTE 4 Dynamic energy transfer control will try to follow the ETP using a best effort strategy.

Use case conditions

Prerequisites	
1	Identification: One or more EV are engaged in service session and may have been authorized for energy transfer.
2	Capability: EV and EVSE support dynamic energy transfer control.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Triggering event
1	Exchange of information during dynamic energy transfer control	The information necessary for a dynamic energy transfer control	CSMS, CS	RM, CSMS or SA

Scenario step by step analysis

Step No.	Name of process/ activity	Description of process/activity	Information producer	Information receiver	Information exchanged
1	The CSMS receives constraints	The CSMS can receive a PRE from RM or constraints via the CSO or generate them internally.	RM or CSO	CSMS	Info1 – CSMS receives a PRE from RM or from CSO
2	The CSMS processes the PRE or constraints received and sends to CSC new ETPs	– For each EV willing to implement dynamic energy transfer control, the CSMS calculates a new ETP based on the previous constraints. – For EVs not engaged in the dynamic energy transfer control, the CSMS may calculate new ETPs compatible with the PRE. – The updated ETPs are sent to the CS. – The CS executes them.	CSMS	CSC	Info2 – CSMS sends ETPs to CS
3	The CSMS configures the CS reporting	The CS can be specifically configured to allow the CSMS to collect the necessary information to ensure proof of service and user information.	CSMS	CSC	See "Monitor a CS" use case.
4	CS sends the status	The CSMS monitors the status of the CS, EVSEs and, if possible, EVs engaged in the dynamic energy transfer.	CSC	CSMS	Info3 – EV status during dynamic energy transfer control
5	CSMS sends the AETP to the RM	CSMS calculates the AETP and sends it to the RM.	CSMS	RM	Info4 – CSMS sends to RM the AETP.

Information exchanged

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	CSMS receives a PRE	PRE	
Info2	CSMS sends ETPs to CS	ETPs for each EVs impacted	
Info3	CS status during dynamic energy transfer control	Based on the configuration of the CS (see "Monitor a CS" use case), the CSMS collects the necessary information for FO, user and for proof of service like metering measurements, battery energy metrics, SOC.	
Info4	CSMS sends to RM the AETP	AETP	

Requirements

Requirements		
Requirement R-ID	**Requirement name**	**Requirement description**
Req1	Traceability	Switch to dynamic energy transfer control of an EV shall trigger a new energy transfer transaction.
Req2	Traceability	The start of a dynamic energy transfer control shall trigger the starting point of specific power measurements on each relevant EVSE, which will be part of the proof of service contained in the SDR.

8.2.10 Providing frequency regulation service by means of decentralized frequency measurements

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
E8	Energy transfer services	Providing frequency regulation service by means of decentralized frequency measurements

Scope and objectives of use case

Scope and objectives of use case	
Scope	This use case describes the information exchange between CS and CSMS to provide frequency regulation services by means of local frequency measurements. In order to do so, the CSMS provides the CS with configuration parameters. The CS reads the frequency locally and regulates its charging/discharging power based on this measurement and on the configuration parameters sent by the CSMS.
Objective(s)	– Describe information exchanges between CSMS and CS in order to enable frequency regulation based on local frequency measurements. – Comply with different TSO and market requirements (including observability).

Narrative of use case

Narrative of use case
Short description
This UC describes the exchange of data between the CSMS and the CS in order to provide frequency regulation services by means of local frequency measurements
Complete description
Providing frequency control by means of decentralized frequency measurements relies on frequency measurements made locally by the CS, as opposed to a centralized measure that is done in one place for the whole country. To operate decentralized frequency control the following steps are necessary: – Grid code configuration The CSMS provides the CS with information regarding the local grid connection requirements the CS shall be compliant with (could be done once during setup and when there are changes). – V2X technical parameters The CS and the CSMS exchange about technical V2X parameters. In particular, the CS will provide the CSMS with its technical limitations (due to both EV and CS limitations) such as (among others) maximum charging and discharging power. – Regulation configuration The CSMS provides the CS with configuration parameters for the decentralized frequency regulation. A non-exhaustive list of these parameters: • power baseline; • power-frequency table. – Provision of frequency regulation service • In real time, the CS reads the frequency locally and adapts its charging/discharging power based on the frequency value and on the configuration parameters sent by the CSMS (among others based on the power baseline and power frequency table which are currently valid). • In real time, the CS sends measurements to the CSMS for observability purposes (among others the AC active power and the frequency measures with good accuracy and short sample time). • In real time, the CSMS may update the CS configuration parameters. – Ending the local frequency regulation session The local frequency control service may be ended both by the CS and the CSMS. Either to end the energy transfer session or to switch to another control mode.

Key performance indicators

Key performance indicators			
ID	**Name**	**Description**	**Reference to mentioned use case objectives**
1	Frequency regulation service	Frequency regulation service KPIs coming from the TSOs, including but not limited to • activation time; • response time; • power response accuracy; • droop control accuracy.	Comply with TSO and market requirements
2	Observability	Provide TSO with relevant observability data	Comply with TSO and market requirements

Use case conditions

Prerequisites	
1	EV and CS are engaged in a V2X energy transfer session (V2X authorized) by using the dynamic energy transfer control.
2	CS and CSMS are engaged in a V2X energy transfer session (V2X authorized).
3	CS and CSMS are engaged in a local decentralized frequency regulation mode.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Triggering event
1	Provision of decentralized frequency control	The information necessary for a decentralized frequency control service	CSMS, CS	SA

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer	Information receiver	Information exchanged
1	The CS receives local grid connection requirements	The CS receives local grid connection requirements from the CSMS. Local grid connection requirements could be provided by different means: the CSMS could either send standard names, or parameter values	CSMS	CSC	Info1 – Local grid connection requirements
2	The CSMS receives V2X charging/ discharging parameters	The CSMS receives V2X charging/ discharging parameters from the CS	CS	CSMS	Info2 – V2X charging/ discharging parameters
3	The CS receives configuration parameters	The CS receives configuration parameters for the local frequency regulation, including (among others): • power baseline; • power-frequency table.	CSMS	CSC	Info3 – frequency regulation configuration parameters
4	Provision of decentralized frequency control service	– In real time, the CS reads the frequency locally and adapts its charging/discharging power based on the frequency value and on the configuration parameters sent by the CSMS. – In real time (around 1 s rate), the CS sends measurements to the CSMS for observability purposes (among others the AC active power with good accuracy and short sample time). – In real time (around 1 min rate), the CSMS may update the CS configuration parameters.	CSMS, CSC	CSMS, CSC	Info3 – frequency regulation configuration parameters Info4 – Starting of frequency control session Info5 – Observability data

Information exchanged

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	Local grid connection requirements	– Standard name; or – Local grid connection parameters.	
Info2	V2X charging/discharging parameters	EV and CS charging/discharging parameters and limitations, possibly including but not limited to: – minimum charging power; – maximum charging power; – minimum discharging power; – maximum discharging power; – minimum charging current; – maximum charging current; – minimum discharging current; – maximum discharging current; – minVoltage; – maxVoltage; – evTargetEnergyRequest; – evMinEnergyRequest; – evMaxEnergyRequest; – minSoC; – maxSoC.	
Info3	Regulation configuration parameters	Configuration parameters for the CS local regulation algorithm, possibly including but not limited to: – power baseline; – power-frequency table.	
Info4	Starting of frequency regulation session	Frequency regulation mode	
Info5	Observability data	Data used by the FO (on behalf of the TSO) to check the provision of the service possibly including but not limited to: – frequency measurements; – AC active power measurements; – EVs actual energy level (kWh); – EVs SoC.	

Requirements

Requirements		
Requirement R-ID	**Requirement name**	**Requirement description**
Req1	Support of dynamic energy transfer control	ISO 15118-20 dynamic control mode or equivalent for another standard shall be supported by CS and CSMS.
Req2	Support of decentralized frequency control mode	Decentralized frequency control mode shall be supported by CS and CSMS.
Req3	Traceability	Changes in energy transfer control mode shall trigger a new energy transfer transaction.
Req4	Observability	The activation of a dynamic control shall trigger the starting point of power and frequency measurements and transmission, either on each EVSE or at CS level that will be part of the observability process.
Req5	Grid connection requirements	CSMS shall inform CS about grid connection requirements.
Req6	Frequency regulation parameters	CSMS shall send the frequency regulation parameters to the CS.

8.3 Manage CS domain use cases

8.3.1 General

The use cases of the manage CS domain are part of the operation life cycle of the CS.

They describe mainly three types of activities:

– initial setup;
– maintenance-diagnostics;
– decommissioning.

Except for maintenance and diagnostics, most of these use cases are executed when the CS is not in operation.

8.3.2 Use case list of the manage CS domain

Table 5 shows the list and a short description of use cases of the manage CS domain.

Table 5 – List of use cases of the manage CS domain

ID	Use case	Brief description	Life cycle / Sequence
M1	Discover CS configuration	The CSMS discovers the configuration of a CS.	Operation / Maintenance
M2	Update a CS component properties	Update a CS component properties	Operation / Maintenance
M3	Monitor a CS	The CSMS monitors some parameters of a particular CS.	Operation / Maintenance
M4	Update the firmware of a CS	The CSMS remotely updates the software/firmware of a CS including elements which are under the control of the CS.	Operation / Maintenance
M5	Reboot a CS	The CSMS sends a reboot request to the CS	Operation / Maintenance

ID	Use case	Brief description	Life cycle / Sequence
M6	The CSMS sets the information to be presented to the user	The CSMS requests the CS to present information at the EVU	Operation / Maintenance
M7	The CSMS sets log criteria	The CSMS requests the CS to set the log criteria that could be retrieved afterwards for analysis.	Operation / Maintenance
M8	Retrieve log information from the CS	The CSMS requests logged information from the CS.	Operation / Maintenance
M9	Fault-code provisioning	In case of failure, the CS sends to the CSMS details about the failure.	Operation / Maintenance
M10	Information deletion triggered to CSMS by an SA	Remove data that was stored in EVSE, CS. The trigger for deletion may come from the CSO, the EVU, or internal housekeeping.	Operation / Maintenance
M11	CS deregistration	Deregistering the CS from the CSMS.	Operation / Decommissioning
M12	Migration of the CS	Migration of the CS to different CSMS within the same CSO	Operation / Initial setup
M13	Onboarding the CS	Onboard an unregistered CS or a CS after major maintenance to the CSMS.	Operation / Initial setup
M14	CA certificate provisioning	The CS can retrieve from CSMS the RootCA certificates and their meta-data used for authenticating EV and CSMS.	Operation / Maintenance
M15	ISO 15118 OCSP response messages	The CS can periodically receive the OCSP response data for the CS's certificate chain from the CSMS.	Operation / Maintenance
M16	Install CS certificate	Update device certificate on CS triggered by CSMS or by itself.	Operation / Maintenance
M17	Install the certificate of the local CSMS	Update device certificate on local CSMS triggered by CSMS or by itself.	Operation / Maintenance
M18	Install CS certificate with key pairs created outside	Update device certificate on CS triggered by CSMS or CA server or by itself.	Operation / Maintenance
M19	Certificate revocation	Handle certificate revocations of primary actors and CAs	Operation / Maintenance

8.3.3 Discover CS configuration

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M1	CS management	Discover CS configuration

Scope and objectives of use case

Scope and objectives of use case	
Scope	The CSMS discovers the configuration of a CS.
Objective(s)	Objective: Discover the configuration of a CS.
Related business case(s)	Manage CS: the CSMS manage the CS.

Narrative of use case

Narrative of use case
Complete description
1) The context of this use case can be: a) a CS is enrolled on a CSMS network for the first time; b) following a known event that may result in some CS parameters changing, such as a technician visit to investigate/repair/upgrade equipment, wiring, etc.; c) elocation of a CS to another site that may have a different parameter set for grid connection; d) the CSMS detects any apparent anomaly in the responses of a CS to other messages, that may indicate an inconsistency between its model of the CS charging topology and the actual hardware. 2) The CSMS sends a configuration discovery request to the CS. There may be parameter options to specify/restrict the capability reporting: a) the scope of the services to be reported; b) the depth of service detail; c) possible and/or actual available capabilities. 3) The CS prepares the report. a) For high function charging stations, the CS's internal controller will introspect its own object model and prepare the corresponding report. b) For basic CSs with little or no configurability, there may be no introspection, and the report may be a fixed pre-prepared message that is always the same (for a given make/model/firmware). 4) The CS sends the configuration report to the CSMS. This is a separate step that should happen asynchronously, because a full introspection process may take some considerable time (e.g., on a large/complex object model).

Use case conditions

Prerequisites	
1	The CS has accepted the authority of the CSMS to change its configuration.
2	The CSMS has registered the CS.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition
1	Discover the list of all parameters with their attributes	The CSMS needs to discover the services that can be (and/or are being) offered by a particular CS.	CS CSMS	The CSO requests the CSMS to get the configuration of a CS.	– The CS is connected to the CSMS. – The CS has been accepted in the network by the CSMS.

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	The CSMS sends a configuration discovery report request to the CS	There may be options to specify/restrict the reporting: • the scope of the services to be reported; • the depth of service detail; • possible and/or actual available parameters.	CSMS	CSC	Info1 – The CSMS requests a configuration discovery to the CSC.
2	The CS sends configuration discovery report to the CSMS	The CS answers back to the CSMS with the status of the report process. The response contains the type of response that will be done: immediate or with delay. – In case of immediate response, the CS sends the prepared report to the CSMS. – In case of delay, the CS informs the CSMS of the progress of the report elaboration	CSC	CSMS	Info2 – The CS sends the discovery report.
3	The CSMS receives the configuration discovery report	This configuration may be maintained in a local CSMS.	CSMS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CSMS requests a configuration discovery to the CS.	There may be parameter options to specify/restrict the reporting: – the scope of the services to be reported; – the depth of service detail; – possible and/or actual available parameters; – destination URI; – encryption keys.
Info2	The CS sends the discovery report.	Immediate or delayed response. The discovery report contains all the object description of the CS.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Basic request	The CS shall accept at least a minimal/basic request from the CSMS to describe its parameters configuration.
Req2	Valid report	The CS shall send a valid configuration report to the CSMS, for any request it accepts, when it is requested to do so.
Req3	Asynchronous messages exchanges	The messages involved in the discovery process shall support asynchronous messages exchanges. The purpose is to make sure that a request leading to a long response and to a large size list is properly handled by CS and CSMS.
Req4	Report reflects CS object model	The configuration report shall correctly reflect the CS object model and actual services that are available and/or active, as requested.
Req5	No interruption of charging service during report preparation and transmission	The CS shall maintain energy transfer during the elaboration of the configuration report.

8.3.4 Update a CS component properties

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M2	Manage charging station	Update a CS component properties

Scope and objectives of use case

Scope and objectives of use case	
Scope	The components of a CS can have properties which allow modifications of their values. This use case defines how to apply such modifications.
Objective(s)	Objective: The CSMS wants to customize the behaviour of a CS by changing some writeable properties of existing components.

Narrative of use case

Narrative of use case
Short description
This UC describes how the CSMS can modify property values of CS components).
Complete description
The CSMS has discovered earlier in the process which components and root level properties a CS is exposing (see UC "Discover CS configuration") The CSMS has identified writeable properties that have values which need to be modified. If multiple values are subject for simultaneous modification they will form an atomic update action, where either all modification will be performed or none of them will be applied. The CSMS sends a request to the CS which will contain the list of key paths which identify the targeted properties as well as the new values. The CS will validate the key paths and the new values against the access rules and value requirements (type, value range, etc.) of the targeted properties. If all changes are valid then the CS will apply the modifications. The CS then sends a response to the CSMS which either confirms the value update or which reports the detected errors as well as related explanations.

Use case conditions

Prerequisites	
1	– The CSMS and the CS have established a trusted communication. – The CSMS has performed the "Discover CS configuration" use case

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	CSMS sends a list of necessary property updates to the CS	CSMS sends a list of necessary property updates to the CS and the CS then applies them or returns an error.	CSMS	End conditions: in case of success: – CS properties are updated to the values. in case of failure: – CS properties still reflect the old values

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 sends update request	The CSMS sends to the CS the list of the key paths for the targeted CS component properties and their new values	CSMS	CS	Info1 – CSMS sends update request
2	CS validates update request	The CS validates the requested modifications against each property's access rules and acceptable value choice options or value ranges. If the entire list of requested updates is valid then all changes will be applied in a consistent atomic way. If the validation failed, then the CS will compile a list of errors and associated descriptions.	CS		
3	CS confirms update request	The CS answers either by sending a success confirmation or with a list of validation errors and associated descriptions which allow the CSMS to identify the affected properties.	CS	CSMS	Info2 – CS confirms update request

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	List of updates	A list containing the key paths for all properties which should be updated as well as the new values for each targeted property. The values can either be of a simple or a complex type.
Info2	Update confirmation	Either "success" is reported or a list of validation errors for each affected property as well as the associated error descriptions. The error descriptions are intended for debugging purposes and should not be restricted to a simple text only. Possible errors are: property not writeable, keyPath does not match any property, new value does not match the required type, new value is outside the allowed range or set of choices, etc.

Requirements

Requirements (optional)		
Requirement R-ID	**Requirement name**	**Requirement description**
Req1	Atomic modification	The CS shall update all properties in a consistent way
Req2	Validation	The CS shall report all validation errors.

8.3.5 Monitor a CS

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M3	CS management	Monitor a CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	The CSMS monitors some parameters of a particular CS.
Objective(s)	The CSMS wants to monitor some parameters of a CS in near real time to obtain information on the CS operation and when there is operating outside normal ranges.
Related business case(s)	

Narrative of use case

Narrative of use case
Short description
The CSMS monitors some parameters values of a CS
Complete description
As EVSE/CSs are deployed in many different locations, it may be useful to have some means to monitor EVSEs with regard to operation and manipulation of EVSEs. In order to monitor a particular EVSE, the CSMS will first parameter conditions (for example thresholds for some values). The CS will then inform the CSMS of all events regarding this particular EVSE. An event is either a periodic fixed set of parameter values or an alert on some parameter values exceeding thresholds. The following steps are a possible way to prepare the monitoring: – the CSMS requests the CS to set or adjust thresholds or intervals for selected parameters; – the CS responds indicating if it is able to monitor the selected parameters and notify CSMS about events; – during normal operation, the CS informs the CSMS if parameter values transition from within to outside the thresholds or vice versa.

Use case conditions

Prerequisites	
1	– The CS is connected when monitoring parameters are set by the CSMS. – The CS is connected when monitoring event messages are sent. – The list of components as described in the object model with the list of parameters are known by the CSMS.

Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Monitor a CS	1) CSMS requests the CS to set or adjust thresholds or intervals for selected parameters. 2) The CS responds indicating if it is able to monitor the selected parameters and notify CSMS about events. 3) During normal operation, the CS informs the CSMS if parameter values transition from within to outside the thresholds or vice versa.	CSMS, CS			End conditions: Success: – Operating limits are set by the CSMS. – The CS will send information to the CSMS when values exceed thresholds. – The CS sends information to the CSMS when values no longer exceed thresholds. – The CSMS is informed about the parameters that can be monitored by the CS and optionally their limits as recommended by the CSM. – The CS takes a snapshot of selected parameters upon request and transmits them to the CSMS. Fail: – Operating limits are not set by the CSMS; the CS will use default limits set by the CSM. – CS is not able to apply the CSMS parameters or limits. CS informs the CSMS of this failing condition with an explicit error description.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	The CSMS requests the CS to adjust parameters limits	The CSMS requests the CS to set or adjust thresholds or intervals for selected parameters.	CSMS	CSC	Info1 – Parameters requested by CSMS for monitoring the CS	
2	The CS acknowledges and notifies	The CS responds indicating if it is able to monitor the selected parameters and notify CSMS about events.	CSC	CSMS	Info2 – list of parameters monitored by the CS	
3	The CS informs the CSMS of a monitoring event	During normal operation, the CS informs the CSMS if parameter values transition from within to outside the thresholds or vice versa.	CSC	CSMS	Info3 – list of CS parameters and values exceeding thresholds	Req1, Req2, Req3, Req4

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
4	Get monitor event	The CSMS receives the monitor event corresponding to a parameter value transitioning from within to outside the thresholds or vice versa.	CSMS			

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	Parameters requested by CSMS for monitoring the CS	Thresholds or intervals for selected parameters
Info2	List of parameters monitored by the CS	List of parameters monitored by the CS
Info3	list of CS parameters and values exceeding thresholds	List of CS parameter values transitioning from within to outside the threshold or vice versa.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Events	The CS shall send events to the CSMS.
Req2	Error or warning	The CS shall send information to the CSMS, issuing a warning or error when a parameter value exceeds the corresponding threshold.
Req3	Error or warning solved	The CS shall send information to the CSMS, indicating that a previous warning or error is resolved when a parameter value returns to within its threshold.
Req4	Periodic state	CS shall send a notification for periodic values every interval.

8.3.6 Update the firmware of a CS

Name of use case

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
M4	CS management	Update the firmware of a CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	Remote software or firmware of an element of the CS
Objective(s)	The CSMS wants to update the software/firmware of a CS including elements which are under the control of the CS (EVSE, internal part of EVSE, communication controller, etc.).
Related business case(s)	Manage CS: The CSMS manages the CS.

Narrative of use case

Narrative of use case
Short description
Update the firmware of a CS or a component of it.
Complete description
– Charging station is informed by CSMS that a new firmware or software update is available for a specific sub-component with a known identifier. The CSMS provides: • the URL to the update package or the update package itself; • conditions to apply the update (e.g., priority, time); • relevant information to enable trust into the delivery mechanism of the update package (certificate for the server host, signature of the update package and credential to be used by the CS, etc.). – In case of out of band delivery, the CS starts software download according to communicated schedule. – Once CS is ready to install the update, it notifies CSMS. – CSMS sends message to charging station: either to start software update process immediately or to start it according to communicated schedule. – CS confirms or not correct reception of the update package. – CSMS requests the CS to install the update. – CS informs the CSMS of the update final status. NOTE Software and firmware update mechanism can be very complicated and can depend on many factors. To name only few: • different charger software complexity (DC fast charging station versus home wallbox) and architecture (OS type, software stack, etc.); • charger SECC hardware platform type (e.g., OS or embedded) and its computational, storage capacity; • charger manufacturer; • modem or communication modules; • others. Therefore, the internal software update mechanism within the CS itself is out of the scope of IEC 63110 (all parts).

Use case conditions

Prerequisites	
1	Update has been verified and approved for installation by the CSO. Verification means: – that the CSO has validated the behaviour of the package with internal tests; – the integrity of the package has been verified and approved for installation.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CSMS informs CS that a new firmware is available for transfer	Charging station is informed by CSMS that a new firmware or software update is available for a specific sub-component with a known identifier. The CSMS also provides installation conditions like priority, time, etc.	CS, CSMS	
2	The CSMS sends the package to the CS	In case of in-band delivery, the CSMS sends the package as part of the payload message.	CS, CSMS	
3	The CS starts software download	In case of out of band delivery, the CS retrieves the firmware package using the URL provided in info1.		
4	The CS informs CSMS that update is ready to install	After checking that the download is finished and is without error, the CS notifies the CSMS that the new firmware/software is ready to be installed.	CS, CSMS	
5	The CSMS requests CS to install update upon specified conditions	Conditions for install update may be: – install immediately; – install update on a particular EVSE only when corresponding service session is over; – start software update process according to communicated schedule.	CS, CSMS	
6	The CS informs the CSMS of the status of the update	CS informs the CSMS if the update is successful or failed. Reasons of the failure are sent to the CSMS.	CS, CSMS	End conditions: – CSMS receives message from CS with software version installed; – CSMS receives message from CS that it is not operational; – CSMS declares CS not operational due to timeout.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	The CSMS informs the CS that a firmware update is available	The message informs the CS of a new firmware availability. Parameters allow CS to know the conditions and the scope of the update.	CSMS	CSC	Info1 – Firmware update available	Req1, Req2
2	The CSMS sends update package to CS	In case of in-band delivery only	CSMS	CSC	Info2 – Send update package	
3	Uploading firmware	The CSMS uploads the firmware package to the link given in step 1	CSMS			
4	Downloading firmware	The CS downloads the firmware package from the link given in step 1	CS			
5	Send update status to CSMS	The CS inform CSMS of the status of the pending update	CSC	CSMS	Info3 – Send update status to CSMS	Req4
6	The CS informs the CSMS of the result of the update	After the update, the CS informs the CSMS if the update failed or not.	CSC	CSMS	Info3 – Send update status to CSMS	Req5, Req6, Req7

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	Firmware update available	– Identifier of the update. – Sub-component subject of the update. – Conditions of the update like priority or time. – The way the update is available: out of band or in-band. – In case of out of band information about package location, certificate for the server host, signature of the update package and credential to be used by the CS are transmitted.
Info2	Send update package	Binary package to be installed by the CS in the sub-element.
Info3	Send update status to CSMS	– Status of update. – Ready for immediate installation. – Ready for installation at a certain point in time or when current service session is finished. – Update rejected because of incompatibility. – Update impossible because of error in transmission.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Authentication of the source	CS shall be able to authenticate the source of the package.
Req2	Role validation	CS shall be able to validate the role of the update message sender (the role shall be authorized to make firmware updates).
Req3	Download shall resume after error	In case communication drops during the firmware download, the CS should be able to resume downloading the missing part.
Req4	Validate update	CS shall check if the integrity of the firmware update and if it is compatible with its current state and if it is necessary (e.g., already installed). If not, the CS shall inform the CSMS of the rejection of the update and the reason of the rejection.
Req5	Fall-back to previous version in case of failure	If some problems occurred during update process and new version was not installed, the system shall be able to roll back to previous version.
Req6	Firmware version	CS shall send to CSMS current version of software after the update process is done successfully or not.
Req7	Irrecoverable error	If some problems have occurred during update process which could not be solved by charging station and remote update server and roll back was not possible, but charging station could still communicate to CSMS, then charging station shall notify CSMS that charging station is not operational with fault-codes and optional description of the error.

8.3.7 Reboot a CS

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M5	CS management	Reboot a CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	The CSMS requests the CS to reboot
Objective(s)	Objective: reboot in order for the CS to perform in a known and predictive state

Narrative of Use Case

Narrative of use case
Short description
The CSMS requests the CS to reboot
Complete description
On some occasion the CSMS needs to request the CS to reboot. Typical reasons are: – Apply a configuration change after a migration – Use new certificates – The CS is still able to communicate but is not working properly. This use case defines 2 types of actions: forced reboot, on-idle reboot. In case of forced reboot – The CSMS sends a forced reboot request to the CS – The reboot will take place at or after some point in time – The CS answers with the identifier of the reboot activity – The CS reboots its system even if there are active service sessions at or after the specified point in time. In case of on-idle reboot – The CSMS sends an on-idle reboot request to the CS – The reboot will take place at or after the time (optionally) provided by the CSMS and when no service sessions are active (e.g. EVs are not transferring energy nor data). – In case there are no EV connected to EVSE • The CS confirms the request with the identifier of the reboot activity • The CS reboots at or after the specified point in time. – In case there are one or more EVs connected to EVSE • The CS answers with the identifier of the reboot activity • The reboot will be performed when there is no more EV connected to EVSE but not before the specified point in time NOTE 1 The CSMS may have an estimation of the duration of this schedule by looking at the relevant ETPs. NOTE 2 This reboot message can be cancelled by the appropriate counter message with the relevant identifier of the reboot activity.

Use case conditions

	Prerequisites
1	The CSMS is aware of which reference clock is using to determine time.

Overview of scenarios

No.	Scenario name	Scenario description	Pre-condition	Post-condition
1	Reboot	The CSMS sends to the CS a request to reboot		

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 sends a reboot to CS	The CSMS requests: Force reboot Or On-idle reboot The CMSMS may provide a point time to apply the reboot	CSMS	CSC	Info1 – reboot
2	CS responds	– If CSMS requests "force reboot" without specifying a point in time, the CS answers "identifier of the reboot activity" to the CSMS and reboots as soon as practical. – If CSMS requests "force reboot" and specifies a point in time, then the CS answers "identifier of the reboot activity" to the CSMS and will reboot at or after the specified point in time. – If CSMS requests "on-idle reboot" without specifying a point in time, then • If no EVs are engaged in an active session, then the CS answers "identifier of the reboot activity" and reboots as soon as practical. • If there are one or more EVs engaged in an active service session then the CS answers "identifier of the reboot activity", and reboots when there are no more active service sessions. – If CSMS requests "on-idle reboot" and specifies a point in time, then: • If no EVs are connected to EVSE, then the CS answers with the identifier of the reboot activity, and will reboot at or after the specified point in time if there are no active service sessions • If there are one or more EVs engaged in an active service session, then the CS answers "identifier of the reboot activity" and reboots when there are no more active service sessions but not before the point in time specified.	CSC	CSMS	Info2 – status of reboot

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	reboot	Type of reboot: can be "forced reboot" or "on-idle reboot" The point in time at or after which the CS will reboot
Info2	status of reboot	identifier of the reboot activity

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	force reboot	When CS receives a force reboot, it shall reboot its system as soon as practical (regardless of active service sessions)

8.3.8 The CSMS sets the information to be presented to the user

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M6	CS management	Information display on EVSE

Scope and objectives of use case

Scope and objectives of use case	
Scope	Information display on the EVSEs.
Objective(s)	CSMS sends to CS user-centric specific information to be delivered (e.g., in a display) to a particular EVSE. In general, the information that will be delivered will not be related to the charging process but only to general information useful for user. For example, traffic in the area, weather forecast, emergency signal, advertising.

Narrative of use case

Narrative of use case
Short description
The CSMS requests the CS to present information to EVU
Complete description
The EV user is expected to read or hear information from the EVSE. Information display can happen before, during or after the use of EVSE. Time, duration and nature of information display is set by CSMS. 1) Rules and content of information to be delivered are set by CSMS. 2) The nature of information to be delivered has an impact on the way the CSMS will send the information (in band or out of band). 3) The CS sends a confirmation to the CSMS that the information has been received and is being presented in the EVSE user interface (display or audio, etc.).

Use case conditions

Prerequisites	
1	The EVSE has a user interface that is described in object model and that can be discovered by the CSMS.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CSMS delivers the information to be presented by the user interface	The way the CS will get the information to be presented depends on how the CSMS will send the information.	CSMS	End conditions: – information is presented in the EVSE; – CS fails to get the information from CSMS; – CS does not support this function.

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	The CSMS requests the CS to present some information to the user	The mechanism to send the information to be presented is like the one used for firmware update (in band or out of band).	CSMS	CSC	Info1 – The CSMS request the CS to get information to be presented to user.
2	The CS gets the information to be presented to the user	The CS answers with the status of the retrieval process.	CSC	CSMS	Info2 – The CS informs the CSMS of the information retrieval process
3	The CSMS gets the status of information retrieval process	The CS informs the CSMS of the status of the retrieval process. The CS informs the CSMS when the information is ready to be presented to the user.	CSMS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CSMS requests the CS to get information to be presented to user.	– List of EVSE impacted (based on object model). – Starting time and end time. – Downloading mechanism. – Information ID providing semantical meaning of the payload – delivery of the payload should be possible either in-band or out-of-band. – Valid period. Language aware payload
Info2	The CS informs the CSMS of the information retrieval process.	– Retrieval process ongoing, finished, failed, etc. – List of EVSEs ready to present information to the user.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Presentation conditions	The CS shall apply the CSMS rules regarding time and duration of the information presentation.
Req2	Retrieval status information	The CS shall inform the CSMS of the outcome of the information transfer and installation in the EVSE.
Req3	Presentation status	The CS shall inform the CSMS that the information is being presented in the EVSE.
Req4	Language aware	All information presented to user shall support language localization based on user preference if available

8.3.9 The CSMS sets log criteria

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M7	CS management	The CSMS sets log criteria CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	The CSMS requests the CS to set log criteria.
Objective(s)	Objective: The CSO wants the CS to set the log criteria that could be retrieved afterwards for analysis (see 8.3.10, "Retrieve log information from the CS" use case).
Related business case(s)	Manage CS: the CSO manages the CS.

Narrative of use case

Narrative of use case
Short description
The CMSM requests the CS to set log criteria.
Complete description
To capture information about the operation of the CS (e.g., with regards to access control, charging sessions, configurations, charging attempts, process, and CS operation), the CSO can set the criteria for capturing events and information that need to be stored. The logging capabilities could be described as a service component listed in a discovery phase. – The CSMS requests the CS to set log criteria. – The CS responds if it is able to log information according to the criteria. – During normal operation, the CS logs all events matching the active criteria, in non-volatile storage. A set of criteria can be grouped and referenced by a criteria identifier. Once a criteria set has been defined it can be activated or de-activated just by referencing the set identifier.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CSMS sets log criteria of the CS	The CSMS sets log criteria of the CS.	CSMS	End conditions: – Success: CS accepts criteria and log entries are added for each matching future event according to the criteria set by the CSMS. – Fail: The CSMS is informed that the CS cannot log some information matching the requested criteria.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	The CSMS sends the log criteria to the CS	When the CSMS sends only the criteria identifier, then the CS switches to the corresponding criteria list. When the CSMS sends the criteria identifier and a list of criteria, then the CS replaces or creates the current criteria list corresponding to the identifier. A set of criteria can be grouped and referenced by a criteria identifier. Once a criteria set has been defined it can be activated or de-activated just by referencing the set identifier. Log criteria are for example referring to access control, charging sessions, configurations, charging attempts, process, and CS operation.	CSMS	CSC	Info1 – The CSMS sends the log criteria to the CS	
2	The CS gets the log criteria	Response is the criteria that could not be set and the possible reason for that fail.	CSC	CSMS	Info2 – The CS returns the criteria status to the CSMS	
3	The CSMS reports to the CSO the state of the log	In case of fail, the CSMS informs the CSO of the failure (this is an out-of-scope message).	CSMS			

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CSMS sends the log criteria to the CS	– The identifier of the log criteria in case of new criteria identification. – Scope of this criteria list. – Duration of the log. – Condition of capture (periodicity, on event, etc.). – List of parameters subject to active criteria.
Info2	The CS returns the criteria status to the CSMS	Either: current active identifier of the log criteria list of parameters where the criteria could be applied, Or error code where the identifier could not be set, reason why.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Minimum set of criteria	Default and minimum set of criteria that shall be applicable anytime.
Req2	Object model	The log criteria shall refer to states of objects described in the CS object model.
Req3	Criteria identifiers	The CSMS shall identify the criteria.
Req4	Number of criteria lists stored in the CS	The CS shall store at least two criteria lists, with their identifiers.
Req5	Switch from one list to another	The CS shall switch from one list to another whenever the CSMS sends a known identifier.
Req6	Sensitive information not stored in logs	The CS shall not log sensitive information like keys or credentials.
Req7	Secure storage	The CS shall contain secure non-volatile memory to store log information.
Req8	Restricted access to logs	The CS shall prevent access to logged information by unauthorized actors.
Req9	Log criteria match	The CS shall log events matching the criteria requested by the CSMS.
Req10	Form of logs	Each log entry shall contain a timestamp, a capture sequence number, and a severity level.

8.3.10 Retrieve log information from the CS

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M8	CS management	Retrieve logged information from the CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	Retrieve logged information from the CS
Objective(s)	Examine logged information: A CSMS wants to retrieve logged information from the CS for detailed analysis of the CS operation.
Related business case(s)	Deliver e-mobility services.

Narrative of use case

Narrative of use case
Short description
The CSMS request the CS to send some logged information
Complete description
A user, or the CSO, may have experienced problems with a CS that cannot be explained by examining the regular messages between CS and CSMS. Detailed information from the CS is necessary to examine its operation and explain the issue. The volume of the payload varies from few kilobytes (kB) to megabytes (MB) depending on the filters. The access to the diagnostic information may be restricted. Steps to follow: 1) The CSMS requests the CS to send diagnostic information. The request may contain optional filters. 2) The CS responds by acknowledging whether it is able to send the information. 3) The CS assembles and transmits the requested information. 4) While collecting and transmitting diagnostic information, the CS may send updates to the CSMS about the process status. The logged information is sent to the CSMS with an in-band communication.

Use case conditions

Prerequisites
– The CS shall implement chunk delivery mechanism.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CSMS requests the CS for log information	Retrieve logged information from the CS	CSMS CS	End conditions: Success: – Diagnostic data has been successfully received. – Matching diagnostic information is available, diagnostic information is sent, CSMS is informed about processing status. Fail: – No matching diagnostic information is available. – Matching diagnostic information available, diagnostic information cannot be sent, CSMS is informed about the failure status. – Communication link dropped out during process.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	The CSMS requests logged information to CS	CSMS requests the CS to send diagnostic information. The request may contain optional filters.	CSMS	CSC	Info1 – CSMS requests logged information to CS	Req1
2	CS acknowledges	The CS responds by acknowledging whether it is able to send the information.	CSC	CSMS	Info2 – CS acknowledges CSMS	Req2
3	CS assembles the requested information	CS assembles the requested information	CS			Req3
4	The CSMS gets status from CS	During collection and transfer of diagnostic information by the CS, the CSMS may receive updates from the CS about the process status.	CSC	CSMS	Info3 – CS transfers status to CSMS	Req4
5	CS processes request	CS transmits information over an in-band communication stream.	CSC	CSMS	Info4 – chunk transmission	

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	CSMS requests logged information to CS	– Optional filters restricting scope like the time interval, severity level, earliest transfer start time, retry information, resume after information settings, etc.
Info2	CS acknowledges CSMS	– acknowledge of the request and whether the CS can perform the requested action
Info3	CS transfers status to CSMS	– Progress of the process. – Estimation of time/ chunk left.
Info4	Chunk transmission	– Current chunk of information requested. – Necessary identification required by the chunking process

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Request message	The CSMS shall send a request message to the CS that contains all information pertinent to filter settings. This may include the time interval, severity level, earliest transfer start time.
Req2	CS acknowledge	The CS shall reply with a message that indicates whether it can comply with the request.
Req3	Filter	If the request includes a filter, the CS shall only send diagnostic information that matches the filter settings.
Req4	Ongoing status	The CS shall inform the CSMS of the processing status (e.g., collecting and transmitting of diagnostic information).

8.3.11 Fault-code provisioning

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M9	CS management	Fault-code provisioning

Scope and objectives of use case

Scope and objectives of use case	
Scope	When a problem occurs with the CS, it is the CSO's role to identify the problem and quickly address the problem if possible or make the CS unavailable until fixed. This use case recognizes that (i) the communication between CS and CSMS should be able to deliver the fault information, and (ii) the fault-code that represents the fault information should be defined such that the code is understood by different CS manufacturers and CSOs.
Objective(s)	When a failure occurs in some of the functionalities of the CS, the CS shall inform the CSMS of the relevant information about the failure such as the component of the CS that failed to perform correctly and the cause of the failure, if identified.

Narrative of use case

Narrative of use case
Short description
Fault-code description
Complete description
In the event of failure, the CS diagnoses, i.e. – identifies the component that failed to operate, – identifies the cause/type of the failure, – determines the corresponding fault-code, and – sends the fault-code and meta-data (e.g., timestamp, unstructured text, etc.). The CSMS receiving the fault-code may request CS for a certain action to resolve the faulty situation. For example, – perform a recovery function such as rebooting with a certain configuration; – display the status on CS's interface; and – run extensive diagnosis for extra report; and/or – stop operation and wait for maintenance. The CSMS updates the availability of the CS accordingly to CSO and EMSP (scope of IEC 63119).

Use case conditions

Prerequisites	
1	The CS can identify the origin and the reason for the problem to determine the fault-code. There should be a fault-code scheme that both CS and CSMS understand.

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	CS diagnoses in case of failure	In the event of failure, the CS diagnoses, i.e. – identifies the component that failed to operate, – identifies the cause/type of the failure, – determines the corresponding fault-code, – sends the fault-code and meta-data (e.g., timestamp, unstructured text, etc.).	CSC	CSMS	Info1 – CS sends a fault-code to CSMS
2	The CSMS updates the availability of the CS	The CSMS updates the availability of the CS accordingly, to CSO and EMSP (scope of IEC 63119).	CSMS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	CS sends a fault-code to CSMS	– Component that failed. – Cause/type of the failure. – Fault-code. – Meta-data (timestamp, unstructured text, etc.).

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	CS's actions in case of failure	In the event of failure: – CS shall diagnose the problem and determine the best-describing fault-code. – CS shall send the fault-code to CSMS as configured. – if requested by the CSMS, CS shall perform the requested actions as directed.
Req2	CSMS's actions in case of failure	In case of CS's failure: – the CSMS may determine the action for the fault-code received from the CS. For example, attempt recovery, display status, run diagnosis and report, or stop operation and wait for maintenance. – CSMS may request the CS to perform the decided action.

8.3.12 Information deletion triggered to CSMS by an SA

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M10	CS management	Information deletion triggered to CSMS by a secondary actor

Scope and objectives of use case

Scope and objectives of use case	
Scope	Information deletion trigger to CSMS by a secondary actor
Objective(s)	Remove data that was stored in EVSE, CS, and CSMS.
Related business case(s)	

Narrative of use case

Narrative of use case
Short description
The CSMS is requested by a secondary actor to delete information
Complete description
During a service session, many data are temporary or permanently stored in EVSE, CS and CSMS. The CSO or other actors may decide to remove a part or all of data stored in EVSE and CS. Possible reasons: the EVU wants their data removed, the EV has been stolen, the customer is inactive or old data clean up, EVU wants data removed, etc. This use case presents the situation where the CSMS is triggered to perform a deletion of data. NOTE 1 The trigger for deletion can come from the CSO, the EVU, or internal housekeeping. NOTE 2 Additional systems (e.g., servers) can also be subject to the deletion but this is out of scope of the IEC 63110 protocol. 1) CSMS is triggered to delete information – The CSMS receives a trigger for deletion from the appropriate actor (CSO, EVU, etc.) to delete all or part of data stored in CS, EVSE. – The CSMS may request confirmation of the deletion before starting the deletion process. – When processing data deletion, the CSMS requires the CS to delete some specific information in the CS and in the EVSE. – The CS informs the CSMS of the deletion status. – The CSMS processes the delete. – CSMS informs the triggering actor of the deletion status. NOTE 3 In some cases, the CSMS could need to backup data before deleting it (e.g., legal, or financial information related to service session). NOTE 4 The words "delete information" mean permanently erase information from memory and permanent storage devices. NOTE 5 The deletion applies to all information including the one stored in the log files. NOTE 6 The deletion can be submitted to conditions like "to be done before a certain date", or "only to the last session". NOTE 7 Data retention time is out of scope and is subject to local applicable law.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	CSMS triggered to delete information	The CSMS is triggered to delete some information in the CS, the EVSE, and the CSMS. The trigger for this deletion may come from the CSO, the EVU, or by its own initiative.	CSMS	End conditions: The expected data is deleted from EVSE, CS, and CSMS. In case the information cannot be deleted, an error status with details will be sent to triggering actor.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	The CSMS receives a trigger to delete specific information	An actor (e.g., CSO, EVU, internal process) requires the CSMS to delete all or a part of the information in the CS, the EVSE, and the CSMS.	CSO, EVU, CSMS housekeeping			
2	The CSMS may confirm the request for information deletion (especially in the case of the EVU wanting to delete their information)	The CSMS asks the triggering actor to confirm the deletion of the data	CSMS			Req1
3	The CSMS requests the CS and EVSE to delete information	The CSMS requires the CS to delete specified data in the CS and in its EVSE(s)	CSMS	CSC	Info1 – CSMS requests CS to delete information	
4	The CS processes the deletion	Deletion affects the CS internal system and EVSE(s).	CS			Req2
5	The CS provides the deletion status to the CSMS	The CS provides the deletion status to the CSMS (e.g., successful, partially successful, failed)	CSC	CSMS	Info2 – CS returns deletion status to CSMS	Req3
6	The CSMS processes the deletion	Deletion affects the CSMS	CSMS			Req4, Req5
7	Deletion status is sent to triggering actor	Deletion status is sent to the triggering actor	CSMS			Req6

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	CSMS requires CS to delete specified data	Deletion scope (may be related to a specific EVU, or may be data older than a certain date, etc.). Execution conditions (e.g., as soon as possible, at a specific hour).
Info2	CS returns deletion status to CSMS	Detail about the deletion status (e.g., success, failed with details on information that could not be deleted and why).

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Confirmation from triggering actor	In some cases, when the CSMS receives the trigger, the CSMS may need to confirm the deletion with the triggering actor.
Req2	Deletion affects the CS internal system and EVSE(s).	The CS shall delete all the specified data.
Req3	CS sends the deletion status to the CSMS	The CS shall inform the CSMS of the deletion status.
Req4	Deletion affects the CSMS	The CSMS shall delete all the specific data.
Req5	Logging	CSMS shall store the deletion trigger and deletion status in the logging system.
Req6	Deletion status is sent to triggering actor	The CSMS shall inform the triggering actor of the deletion status.

8.3.13 CS deregistration

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M11	CS management	CS deregistration

Scope and objectives of use case

Scope and objectives of use case	
Scope	Deregistering the CS by the CSMS
Objective(s)	Objective: Deregister the CS
Related business case(s)	Onboarding and information deletion use cases

Narrative of use case

Narrative of use case
Short description
A CS is deregistered by the CSMS
Complete description
Deregistration can be considered the reverse use case to bootstrapping. If a CS needs to be separated from its connection with a CSMS, the CS needs to be deregistered in the CSMS. A deregistration shall be triggered centrally by the CSO, through the CSMS, or locally with an authorized human intervention. Additionally, the CSMS shall be able to give information about the registration status of each connected charging station. The CSMS will perform the UC "Information deletion triggered to CSMS by an SA" (see 8.3.12) before completing the deregistration. A deregistered charging station shall have the effect that the CS is no longer associated with the CSMS, nor usable by the EVU. Therefore, in the CSMS, the CS shall be set to deregistered/unavailable as well as in the CSO backend (out of scope of IEC 63110) and connected secondary services. Detailed description: – Deregistration triggered by CSMS The CSO requests CSMS that one, more or all EVSEs of a certain CS or the CS itself shall be deregistered. CSMS receives deregistration request and forwards it to CS. – Deregistration triggered by CS (optional) An authorized person (e.g., service engineer) deregisters the CS in a diagnosis session to test if deregistration works or when updating the hardware. This action needs to be performed locally. The CS thereby sends deregistration information to the CSMS which forwards it to SA backend. – Information of registration status The CSMS shall be able to inform upon request if a charging station is registered, not registered, deregistered, registration pending or deregistration pending.

Use case conditions

Prerequisites	
1	– The CS is operative, registered and connected to the CSMS.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	Deregistration required by CSO or CS	– The CSMS is requested to deregister a CS (triggered by local input via CS diagnosis session or centrally by the CSO). – The CSMS performs deregistration and shares new registration status with CSO.	CSMS CS	End conditions: – The CS is deregistered. – CS, CSMS and CSO updated their respective registration status info. – The CS is set to unavailable/ deregistered and therefore no longer usable by an EVU.

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	The CSMS receives a deregistration request from the CS	The CSMS receives a deregistration request. The request can be applied to the whole CS or only to one particular EVSE. NOTE The request can also come from the CS or the CSO (out of scope).	CSC	CSMS	Info1 – The CSMS receives a deregistration request
2	The CSMS is requested (e.g., by the CSO) to deregister a particular CS	The CSMS receives a deregistration request. The request can be applied to the whole CS or only to one particular EVSE.	CSO	CSMS	
3	The CSMS performs the deregistration	With the received parameters: – The CSMS performs the UC Information deletion triggered to CSMS by an SA with a restricted scope to a particular EVSE if required. – The CSMS sends a deregistration command to the CS with a restricted scope to a particular EVSE if required. – The CSMS informs the CSO of the pending deregistration command (out of scope). – if there is a need of a temporary disconnection then the CSMS needs to send a switch off message. This is not part of deregistration.	CSMS	CSC	Info2 – The CSMS requests the CS to deregister
4	The CS performs the deregistration	– The deregistration is performed with the scope received (the whole CS or a particular EVSE). – Deregistration status is sent to the CSMS after deregistration.	CSC	CSMS	Info3 – The CS sends the registration status to the CSMS
5	The CSMS gets the deregistration status	The CSMS will inform the CSO of the deregistration status (out of scope).	CSMS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CSMS receives a deregistration request	The request indicates if it applies to the whole CS or a particular EVSE. In the case of a particular EVSE, the identification of the EVSE shall be supplied by the CS.
Info2	The CSMS requests the CS to deregister	Scope of the deregistration: – whole CS; – a particular EVSE.
Info3	The CS sends the registration status to the CSMS	Info on the registration status: – registered (error occurred); – not registered.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Enable local deregistration	CS deregistration may be triggered by the CS through a local human intervention.
Req2	Enable central deregistration	CS deregistration may be triggered by the CSMS.
Req3	Deregistration scope	It shall be possible to perform deregistration on the CS or at the EVSE level.
Req4	Log	The CSMS shall log the deregistration status and the messages sent by the CS during deregistration.
Req5	Status	The CS shall send a status during and after the deregistration.
Req6	Information deletion	The CSMS shall delete the information stored in the CS (or in the EVSE). The deletion process is described in the "Information deletion triggered to CSMS by an SA" use case (see 8.3.12).

8.3.14 Migration of the CS

Name of use case

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
M12	CS management	Migration of the CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	Migration of the CS to different CSMS within the same CSO
Objective(s)	Objective: Disconnect the CS from the current CSMS and then reconnect it to a new CSMS within the same CSO
Related business case(s)	Onboarding the CS CS deregistration Information deletion triggered to CSMS by an SA

Narrative of use case

Narrative of use case
Short description
A CS migrates from a CSMS to another one
Complete description
A CS under the current CSMS may need to be prepared for migrating to a new CSMS and be reconnected to the new CSMS. Migration procedure takes the following steps: 1) Optionally perform "Information deletion triggered to CSMS by an SA" (see 8.3.12) use case. 2) During this use case, the current CSMS sends the following bootstrapping information to the migrating CS: • connection information to new CSMS; • initial credential information needed for establishing a secure channel. 3) Perform "CS deregistration" use case (see 8.3.13). 4) Perform "Onboarding the CS" use case (see 8.3.15).

Overview of scenarios

No.	Scenario name	Scenario description	Pre-condition	Post-condition
1	Information deletion	If needed, customer information is deleted. Refer to "Information deletion triggered to CSMS" use case (see 8.3.12)	Refer to "Information deletion triggered to CSMS" use case (see 8.3.12)	Refer to "Information deletion triggered to CSMS" use case (see 8.3.12)
2	Preparation of migration	Installing bootstrapping information to the CS	CSO is able to generate bootstrapping information to the CS needed for migration	End conditions: – The CS has successfully stored necessary information for migration
3	CS deregistration	Deregister the CS from the current CSMS. Refer to "CS deregistration" use case (see 8.3.13)	Refer to "CS deregistration" use case (see 8.3.13)	Refer to "CS deregistration" use case (see 8.3.13)
4	Onboarding CS	On board the CS to the new CSMS Refer to "Onboarding the CS" use case (see 8.3.15)	Refer to "Onboarding the CS" use case (see 8.3.15)	Refer to "Onboarding the CS" use case ((see 8.3.15)

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
2.1	CSMS sends bootstrapping information to the CS	The CSMS sends bootstrapping information to the CS so that the CS can use that information to connect to a new CSMS during a bootstrapping phase.	CSMS	CSC	Info1 – Bootstrapping information

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	Bootstrapping information	This information describes how the CS can connect to the new CSMS and what are the credentials to use for establishing a secure channel between CS and the CSMS.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Bootstrapping information	If the CSMS intends to de-register a CS for migrating to another CSMS, the CSMS shall have access to the bootstrapping information that the CS needs to migrate to another CSMS.
Req2	Bootstrapping information delivery	If the CSMS intends to de-register a CS for migrating to another CSMS, the CSMS shall send the bootstrapping information to the CS.

8.3.15 Onboarding the CS

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M13	CS management	Onboarding the CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	Onboarding the CS
Objective(s)	Objective: Onboard an unregistered CS or a CS after major maintenance to the CSMS so that the CS can operate in a CSO network.
Related business case(s)	Install CS certificate Discover CS configuration

Narrative of use case

Narrative of use case
Short description
An unregistered CS is onboarded in a CSMS
Complete description
An unregistered CS or a CS after major maintenance that lost credentials (e.g., certificate expired/revoked or erasure of storage content) needs a well-defined procedure to securely connect and register to the network before operation. Onboarding use case is typically followed by "Discover CS configuration" use case (see 8.3.3). Onboarding use case consists of the following steps in order: 1) Connect the CS with the CSMS by establishing a mutually authenticated, encrypted, and integrity-protected communication channel based on the connection information and initial credentials stored in CS. 2) Optional: CSMS may choose to send new credential to CS after which CS and CSMS establish new secure channel (see Install CS certificate use cases). 3) Perform "Discover CS configuration" use case (see 8.3.3). 4) Register the CS with the CSMS by assigning proper identifiers and provide configuration information necessary for proper operation. NOTE The onboarding process may be implemented by utilizing a bootstrapping server dedicated for expediting the onboarding process by distributing connection information and credentials to the CS.

Overview of scenarios

No.	Scenario name	Scenario description	Pre-condition	Post-condition
1	Secure bootstrapping of the CS	Process of connecting or re-connecting a CS to a CSMS based on the credential initially stored in the CS.	– CSO can generate bootstrap information including credential information to the CS. Such bootstrapping information includes connection information to CSMS and initial credentials. – CSO can install bootstrapping information in the CS. This can happen during production of the CS, factory setup, installation at the site, or during the initial bootup (e.g., input on HMI).	End conditions: – The CS has successfully established a secure channel with the CSMS. – If bootstrapping fails, a major maintenance is called for.
2	Long-term credential installation	Optionally, CSMS may want to replace the initial credential with a long-term credential needed for normal operation. Refer to the use cases "Install CS certificate" (8.3.18) and "Install CS certificate with key pairs created outside" (8.3.20).	Refer to the use cases "Install CS certificate" (8.3.18) and "Install CS certificate with key pairs created outside" (8.3.20).	Refer to the use cases "Install CS certificate" (8.3.18) and "Install CS certificate with key pairs created outside" (8.3.20).
3	Discover CS configuration	Refer to the use case "Discover CS configuration" (8.3.3).	Refer to the use case "Discover CS configuration" (8.3.3).	Refer to the use case "Discover CS configuration" (8.3.3).
4	Registration of CS	Register the CS with the CSMS by assigning proper identifiers and provide configuration information necessary for proper operation	The CSMS identified the CS's hardware and software capabilities in "Discover CS configuration" use case (8.3.3).	The CS is assigned with necessary identifiers and configuration information If registration fails, a major maintenance is called for.

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	The CS establishes a secure communication channel with the CSMS	Establish a secure channel to CSMS based on the bootstrapping information stored in CS, such that CS and CSMS can successfully authenticate each other based on the credential included in the bootstrapping information.	CSC CSMS	CSMS CSC	Depends on the connection method
4	The CSMS sends the registration information to the CS	The CSMS generates/retrieves the registration information of the CS and sends it to the CS.	CSMS	CSC	Info 1: Registration information

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	CS registration information	Registration information includes – SECCID – EVSEID – Supported EMSPs

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Mutual authentication	When the CS connects to the CSMS for bootstrapping, CSMS and CS shall authenticate each other based on the credentials included in the bootstrap information.
Req2	Confidentiality and integrity	When the CS connects to the CSMS for bootstrapping, the resulting communication channel shall be confidential, and integrity protected.
Req3	Registration information in the CS	After the CS connects to the CSMS and the CSMS gathers CS's configuration information, then the CSMS shall send registration information to CS.

8.3.16 CA certificate provisioning

Name of use case

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
M14	CS management	CA certificate provisioning

Scope and objectives of use case

Scope and objectives of use case	
Scope	The CS gets from the CSMS the root CA certificates and their meta-data used for all authenticating purposes.
Objective(s)	The CS can retrieve from CSMS the RootCA certificates and their meta-data used for authenticating EV and CSMS, as well as the cross certificates used for authenticating itself to EVs.
Related business case(s)	

Narrative of use case

Narrative of use case
Short description
The CSMS provides to the CS the root CA certificates
Complete description
This use case is only on RootCA provisioning and not certificate installation. The following steps (from 1 to 5) are not the steps of the scenario but provide a list of possible RootCA purposes. CS needs to store some RootCA certificates (issued for a RootCA, but not necessarily self-signed) and related meta-data for secure operation. 1) (Mandatory) CS needs the RootCA certificate of the CSMS's certificate chain (in short, RootCA certificate of CSMS) to authenticate the CSMS during the establishment of a secure channel with CSMS. This is usually the same with CS's V2G RootCA (and we assume this in the following). 2) (Optional) When an ISO 15118-compliant EV chooses to get authorized by PnC method, and if it is CS's role to validate the contract certificate chain, CS needs to have the RootCA certificate of the EMSP (see "Authorization with locally presented credentials" use case in 8.4.4). 3) (Optional) When CSO supports cross certification to allow the service to an EV that trusts only a V2G RootCA other than the CSO's V2G RootCA, CS needs to have a cross certificate issued by the V2G RootCA trusted by EV for the CSO's V2G RootCA. 4) (Mandatory) To check if EV can trust the CSO's V2G RootCA (for TLS) or the CPS's V2G RootCA (for certificate installation in part20), CS needs to know the meta-data of the available trust anchors. Trust anchors include the CS's V2G RootCAs (including new one for migration) and cross-certifying V2G RootCAs. Meta-data of a certificate include the SHA1 hash (for TLS) and DN/serial number. 5) (Optional) For the migration of V2G RootCA of the CS, if the CSO chooses to use the migration method as defined in RFC 4210, during the migration period CS needs to hold one of two cross certificates: a) OldWithNew: cross certificate signed by new RootCA for old RootCA. CS with old certificate chain needs this for an EV trusting new RootCA; b) NewWithOld: cross certificate signed by old RootCA for new RootCA. CS with new certificate chain needs this for an EV trusting old RootCA. Two cases arise: – Case 1: triggered by CSMS When CSMS has an update on one of the CA certificates/meta-data that needs to be installed in CS, • CSMS sends to one or more CSs a list of updates, • upon receiving the updates from CSMS, CS installs the received certificate or meta-data without undue delay and updates the update-timestamp and stores securely the certificates/meta-data. – Case 2: triggered by CS When CS determines to update any changes on CA certificates (probably in a periodic manner), • CS requests CSMS for updates of CA certificates by sending a) the timestamp of the last successful update (triggered by either), b) (optional) the list of IssuerDN/Serial of CA certificates currently in CS; this information can be useful if some certificates were deleted in CS for any reason, and CSMS will send any missing data. • upon receiving the request, the CSMS sends CA certificates/meta-data that are updated/added after the indicated timestamp (possibly none), as defined in case 1. • upon receiving the response from the CSMS, the CS will securely store the CA certificates/meta-data.

Use case conditions

Prerequisites	
	– The CS and the CSMS have already established a secure communication channel. – The CSMS maintains a database for CA certificate data (certificate, DN, serial, hash) tagged with update/addition timestamp.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CS is aware of certificates updates	The CS determines that an update on CA certificates is necessary (probably in a periodic manner).	CS	
2	The CSMS is aware of some certificates updates to be installed in the CS	The CSMS has received an update on one of the CA certificates/meta-data that needs to be installed in the CS. The updates will be sent to the CS.	CSMS	
3	The CSMS sends to CS a RootCA certificate update	The CSMS sends to CS the update of the CS's RootCA certificates and their meta-data used for authenticating EV and CSMS, as well as the cross certificates used for authenticating CS to EVs.	CSMS	End conditions: – When successful, CS has the up-to-date list of CA certificates. – When failed for certain updates, CS fails to operate with up-to-date CA certificates.

Scenario step by step analysis

The CS is aware of certificates updates.

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
1.1	The CS requests the CSMS for updates of CA certificates	The CS determines that updates on CA certificates are necessary (probably in a periodic manner).	CSC	CSMS	Info1 – The CS request the CSMS for certificates updates
1.2	The CSMS prepares the certificates to be updated	The CSMS transfers the request to the CSO. This is an out-of-scope activity. Eventually, the CSMS will get the certificates updates.	CSMS		

The CSMS sends to CS a RootCA certificate update.

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
3.1	The CSMS sends to the CS a list of updates	This action is triggered when the CSMS receives an update on one of the CA certificates/meta-data that needs to be installed in CS.	CSMS	CSC	Info2 – The CSMS sends to the CS a list of updates of certificates or meta-data
3.2	The CS gets the update	Upon receiving the updates from the CSMS, the CS installs the received certificate or meta-data without undue delay and updates the update-timestamp. The CS will securely store the CA certificates/meta-data.	CS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CS request the CSMS for certificates updates	– Timestamp of the last successful update (triggered by either). – (Optional) List of IssuerDN/Serial of CA certificates currently in the CS. This information can be useful if some certificates were deleted in the CS for any reason, and the CSMS will send any missing data.
Info2	The CSMS sends to the CS a list of updates of certificates or meta-data	Type of update: certificate or meta-data A dash "–" means the field is omitted. – For V2G RootCA of CSO (old or new) • (V2GRootCA, <V2GRootCA certificate>, –) – EMSP RootCA (whether update or newly added EMSP) • (EMSPRootCA, <EMSPRooCA certificate>, –) – OEM RootCA (whether update or newly added OEM) • (OEMRootCA, <OEMRooCA certificate>, –) – Cross certificates (whether update or newly-added cross-cert) • (CrossCert, <Cross certificate>, –) – Cross-certifying V2G RootCA (corresponding to above cross cert) • (CrossRootCA, –, <meta-data>) – OldWithNew cross certificate for migration • (OldWithNew, <OldWithNew certificate>, –) – NewWithOld cross certificate for migration • (NewWithOld, <NewWithOld certificate>, –)

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Installation request	When the CSMS makes an update on the CA certificate database, CSMS shall request the CS to install the update or a collection of updates since the last update.
Req2	Timestamp	When requested by the CSMS, the CS shall install the received updates of CA certificates and set the timestamp to the time of the update.
Req3	Timestamp monitoring	Depending on the policy, the CS shall periodically request the update of CA certificates to the CSMS by providing the timestamp of the last update.
Req4	Updates on timestamp	When requested, the CSMS shall send all the updates in CS certificates that are changed since the timestamp in the request.
Req5	Timestamp information	When the CS requests CA-certificate updates, it indicates the timestamp of the last successful retrieval.
Req6	Certificates information	When the CSMS sends CA-certificate updates, it sends a list of certificate type, certificate, and meta-data, where only meta-data is sent for the cross-certifying V2G RootCA certificates.

8.3.17 ISO 15118 OCSP response messages

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M15	CS management	The CSMS updates the ISO 15118-OCSP response for CS

Scope and objectives of use case

Scope and objectives of use case	
Scope	When ISO 15118-compliant EV attempts a TLS connection with the CS, the CS needs to prove that all the certificates in CS's certificate chain are valid (i.e., not revoked). To do that, the CSMS recurrently (frequently enough to keep the OCSP responses valid) retrieves OCSP responses for the CS certificate chain from the OCSP responder(s) of the CSO PKI and pushes the responses to the CS. The CS needs to store one OCSP response for each certificate in its certificate chain (including SubCA certificates).
Objective(s)	Objective: the CSMS can recurrently provide the CS with the OCSP response data for the CS's certificate chain.
Related business case(s)	

Narrative of use case

Narrative of use case
Short description
The CSMS updates the OCSP response for CS
Complete description
1) When the CSMS decides to update the CS's certificate revocation status through online certificate status protocol (OCSP) responses, for example current ones stored in the CS are about to expire, the CSMS requests the OCSP responder(s) for OCSP retrieval by sending an OCSP request message according to RFC 6960. 2) For each request, the CSMS identifies (e.g., from its certificate database) the following information for each certificate of the CS's certificate chain: – issuer's DN; – issuer's public key; – serial number of the certificate; – OCSP responder's URL. If no URL was found, CSMS may try to retrieve the URL by any other means. If no URL is available at its best, the CSMS will enter a maintenance status. NOTE If unsuccessful, something needs to be done by the CSMS to handle this situation, which is out of scope of this document. 3) Upon successful retrieval of the information in step 2, the CSMS generates the OCSP request message and sends it to the OCSP responder. Upon receiving the OCSP response from the responder, the CSMS sends the responses to the CS. The CSMS also records the responses and the identity of the CS, for example in its database. 4) If one of the retrievals failed, the CSMS indicates which OCSP query failed and why. 5) The CS then stores the received OCSP responses and sends them to the EVs during the TLS connection by OCSP stapling (RFC 6961). 6) For each error, depending on the error type, the CSMS decides whether to retry the retrieval, or enter a maintenance status. 7) If CS cannot accept the OCSP response then CS will indicate that to the CSMS (signature error, memory full, …).

Use case conditions

Prerequisites	
1	– CS and CSMS have already established a secure communication channel. – EV and CS communicate over ISO 15118. – CSMS manages the certificate chain of each CS and the last OCSP responses provided to the CS. – CSMS manages the OCSP responder URL information in case the certificate does not contain the information in the Authority Information Access extension.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CSMS updates the OCSP responses and sends them to the CS	The CSMS recurrently retrieves OCSP responses for the CS certificate chain from the OCSP responder(s) of the CSO PKI and pushes the responses to the CS so that the CS can prove that certificates in its certificate chains are not revoked. This is needed in ISO 15118 for TLC connection with the EV.	CSMS	End conditions: – The CS receives OCSP responses for all the certificates in its certificate chain. – Upon failure on one of the retrievals, CS may try again or would require maintenance.

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	The CSMS retrieves the OCSP responses for the CS from the OCSP responders	When the CSMS decides to update the CS's OCSP responses, for example current ones stored in the CS are about to expire, the CSMS first collects information necessary to generate OCSP request message (issuer's DN and public key, serial number, and the responder's URL) for each certificate in the chain. Then the CSMS requests the OCSP responder(s) for OCSP retrieval by sending an OCSP request message according to RFC 6960.	CSMS/ OCSP responder	OCSP responders/ CSMS	
2	The CSMS sends the received OCSP responses to the CS	Upon receiving the OCSP responses from the responder, the CSMS sends the responses to the CS. The CSMS also keeps track of the responses and the identity of the CS, for example in its database.	CSMS	CSC	Info1 – The CSMS sends OCSP response to the CS
3	The CS stores the responses	The CS then stores the received OCSP responses and sends them to EVs during the TLS connection by OCSP stapling (RFC 6961). For each error, depending on the error type, CS decides whether to retry the retrieval, or enter a maintenance status.	CS	EV	
4	The CS rejects the OCSP responses	If CS cannot accept the OCSP response then CS will indicate that to the CSMS (because of signature error, memory full, etc.). Upon receiving, the CSMS shall enter maintenance status or try to resolve the problem and retry this use case.	CSC	CSMS	Info2 – The CS sends the CSMS for the rejection of the OCSP response

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
Info1	The CSMS sends OCSP response to the CS	For each certificate, the following parameters are sent by the CSMS to the CS: – the OCSP response message;	
Info 2	The CS sends the CSMS for the rejection of the OCSP response	If CS cannot accept the OCSP response then CS will indicate that to the CSMS (because of signature error, memory full, etc.).	

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	RFC 6960	CSMS shall be able to generate an OCSP request message for given certificates in the CS's certificate chain (according to RFC 6960 or any successor).
Req2	Information necessary for OCSP updates	The CSMS shall always maintain the set of valid OCSP responses and certificate information for the CS's current certificate chain.
Req3	Frequency of request	CSMS shall update OCSP responses of each CS frequently enough to keep them valid all the time.
Req4	OCSP retrieval and provision to CS	The CSMS (or the CSO) shall generate and send OCSP request to the corresponding OCSP URL, and the CSMS forwards the OCSP responses to the CS.
Req5	Error handling	Upon any failure, CSMS shall try to retrieve OCSP responses or enter a maintenance status.

8.3.18 Install CS certificate

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M16	CS management	Install CS certificate

Scope and objectives of use case

Scope and objectives of use case	
Scope	Install certificate on CS triggered by CSMS or by itself
Objective(s)	Install a new certificate or replace an old certificate in the CS
Related business case(s)	

Narrative of use case

Narrative of use case
Short description
The CSMS installs a certificate in the CS
Complete description
A CS has multiple certificates for various uses. The CS has capabilities to create a key pair (i.e., private/public key). A PKI including certification authority server is available to manage the certificate life cycle including the life cycle of the trust anchors. The use case covers the following main scenarios. – Replacement of the certificate that was installed during production of the CS/CS controller. – Renewal of a device certificate prior to its expiration date. – Renewal of key material prior to its expiration date. This use case does not cover following scenarios: – Issuer's certificate had been revoked (CA or sub-CA certificate). In this case, it could be also necessary to update trust anchors stored on CS. – The current CS certificate had been revoked. Detailed description: – CSMS may send a request to the CS, or the CS may trigger itself (in case of certificate expiration) to update the CSMS-CS communication certificate on the CS – The CS creates a Certificate Signing Request (CSR) and sends this CSR to the CSMS. – This informative point is out of scope: The CSMS forwards the CSR to the CA server. The CA server checks the parameters of the CSR for plausibility and compliance to rules, creates a new CS certificate, and sends it back to the CSMS. If the plausibility-check failed, the CSR will be rejected leading to maintenance actions. – The CSMS forwards the new certificate or an error notification to the CS. – The CS receives the result of the CSR. If the result was successful, the CS validates the received CS certificate and stores it locally on CS for further processing. If the result was not successful, the CS or the CSMS initiates another attempt. If this last try fails then maintenance is necessary. NOTE The behaviour of the CS without valid certificate needs to be defined by the CSO. – The CS will switch to the new certificate / key material for authentication as soon as the updated certificate becomes valid without undue delay or when the CSMS triggers the switch.

Use case conditions

Prerequisites	
1	The CS can create key pairs

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	A new certificate (chain) is installed in the CS	The installation is requested by the CSMS or by the CS itself	CS CSMS	End conditions: – The CS has a new certificate(chain) installed. – In case of failure during installation and old certificate is still valid, the CS may use old certificate chain if allowed. – If there is no secure communication established, then the behaviour of the CS is a business decision.

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	The CSMS requests the CS to install its certificate	NOTE 1 The CS could be triggered by itself.	CSMS	CSC	Info1 – The CSMS requests the CS to install its certificate
2	The CS executes the installation certificate request	The CS creates a new key pair. The CS creates a certificate signing request (CSR) and sends this CSR to the CSMS.	CSC	CSMS	Info2 – The CS creates a CSR and sends it back to the CSMS
3	The CSMS forwards the new certificate(chain) to the CS	– The CSMS forwards the CSR to the CA server. – The CA server checks the parameters of the CSR for plausibility and compliance to rules, creates a new CS certificate, and sends it back to the CSMS. – If the plausibility-check failed, the CSR will be rejected leading to maintenance actions. – The CSMS forwards the new certificate (chain) or the error code to the CS. NOTE 2 Only the last step is in IEC 63110 scope.	CSMS	CSC	Info3 – The CSMS forwards the new certificate to the CS.
4	The CS gets the result of CSR by the CSMS	Action depends on the CSR result.	CS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CSMS requests the CS to install its certificate	Immediate
Info2	The CS creates a CSR and sends it back to the CSMS	The certificate signing request (CSR)
Info3	The CSMS forwards the new certificate to the CS	The new certificate or the error code

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Secure storage-1	The CS shall store private keys in a secure storage that prevents unauthorized access to the private key.
Req2	Secure storage-2	The CS shall store trust anchors (root certificates) for validation in a secure storage that prevents unauthorized access to the trust anchors.
Req3	CSR	The CS shall be able to create CSRs.
Req4	Mutual authentication	All communication paths shall be based on mutual authentication.
Req5	Sanity check	The CS may do its own local sanity check for the certificate chain.
Req6	Switch to new certificate	The CS shall switch to the new certificate/key material for authentication as soon as the updated certificate becomes valid without undue delay or when the CSMS triggers the switch.

8.3.19 Install the certificate of the local CSMS

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M17	CS management	Install the local CSMS certificate

Scope and objectives of use case

Scope and objectives of use case	
Scope	Install certificate on local CSMS
Objective(s)	Objective: The local CSMS is triggered by itself or by a cloud CSMS to renew its certificate.

Narrative of use case

Narrative of use case
Short description
The cloud CSMS installs the local CSMS certificates
Complete description
The CSMS is using a certificate for authentication during IEC 63110 communication between local CSMS and CS or local CSMS and cloud CSMS. The local CSMS has capabilities to create a key pair (i.e., private/public key). A PKI including certification authority server is available to manage the certificate life cycle including the life cycle of the trust anchors. The use case covers four main scenarios: – replacement of the certificate that was installed during production in factory of the local CSMS; obviously, this is the first step during integration of a new local CSMS in the system of the CSO; – renewal of a local CSMS certificate prior to its expiration date; – the current local CSMS certificate had been revoked; – issuers certificate had been revoked (CA or sub-CA certificate). NOTE In this case, it could be also necessary to update trust anchors stored on local-CSMS. Detailed description: – Optional: local CSMS sends a request to update its system certificate to a cloud CSMS. – The local CSMS creates a new key pair. – The local CSMS creates a certificate signing request (CSR) and sends this CSR to the cloud CSMS. – This informative point is out of scope: The cloud CSMS forwards the CSR to the CA server. The CA server checks the parameters of the CSR for plausibility and compliance to rules, creates a new local CSMS certificate and sends it back to the cloud CSMS. If the plausibility-check failed, the CSR will be rejected leading to maintenance actions. – The cloud CSMS forwards the certificate chain or the result of the CSR to the local CSMS. – The local CSMS receives the result of the CSR. If the result was successful, the local CSMS may do its own local sanity check for the certificate chain and stores it locally for further processing. Authentication on each connection with CS: the LCSMS will use the certificate/key material as soon as valid and practical.

Use case conditions

Prerequisites	
1	The local CSMS can create key pairs

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The local CSMS requests the cloud CSMS to update its system certificate	The local CSMS can be triggered by itself or by the cloud CSMS.	Local CSMS	End condition: In case of success: – The local CSMS will be using the new certificate for all communication. In case of failure during update: – The local CSMS keeps using old certificate chain; if there is no secure communication established, then the behaviour of the CS is a business decision.

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	The local CSMS sends a CSR to the cloud CSMS	The local CSMS creates a new key pair. The local CSMS creates a certificate signing request (CSR)	Local CSMS	Cloud CSMS	Info1 – The local CSMS sends a certificate signing request (CSR) to the cloud CSMS
2	The cloud CSMS processes the CSR	This processing informative point is internal to the local CSMS: – The cloud CSMS forwards the CSR to the CA server. – The CA server checks the parameters of the CSR for plausibility and compliance to rules, creates a new local CSMS certificate and sends it back to the cloud CSMS. – If the plausibility-check failed, the CSR will be rejected leading to maintenance actions. The cloud CSMS forwards the certificate chain or the result of the CSR to the local CSMS.	Local CSMS	Cloud CSMS	Info2 – The CSMS sends the result of the CSR to the local CSMS
3	The local CSMS stores the certificate chain	The local CSMS receives the result of the CSR. – If the result was successful, the local CSMS may do its own local sanity check for the certificate chain and stores it locally for further processing. – Authentication on each connection with CS: the local CSMS will use the certificate/key material as soon as valid and practical.	Local CSMS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The local CSMS sends a certificate signing request (CSR) to the cloud CSMS	The CSR
Info2	The CSMS sends the result of the CSR to the local CSMS	The certificate of the error in case of fail

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Mutual authentication	All certificate-related communication paths shall be based on mutual authentication.
Req2	Integrity protection	All certificate-related messages shall be integrity-protected.
Req3	Key pair creation capability	The local CSMS shall have capabilities to create a key pair for creation of certificates.
Req4	Secure storage-1	The local CSMS shall store private keys in a secure storage that prevents external access to the private key.
Req5	Secure storage-2	The local CSMS shall store trust anchors (root certificates) in a secure storage.
Req6	CSR capabilities	The local CSMS shall have capabilities to create CSRs messages to CA servers.
Req7	Certificate transmission	The cloud CSMS shall forward the certificate from the CS server to the local CSMS.

8.3.20 Install CS certificate with key pairs created outside

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M18	CS management	Install CS certificate with key pairs created outside

Scope and objectives of use case

Scope and objectives of use case	
Scope	Install device certificate on CS triggered by CSMS or CA server or by itself with the key pair created outside the CS.
Objective(s)	Objective: The CS is triggered by the CSMS or by CA server or by itself to renew the CS device certificate.

Narrative of use case

Narrative of use case
Short description
The CSMS installs a certificate in the CS with key pairs created outside
Complete description
The CS has no capabilities to create a key pair (i.e., private/public key). A PKI including certification authority server is available to manage the certificate life cycle including the life cycle of the trust anchors and creates the key pair. The certificate authority server will send both the newly created private key and the new device certificate to the CS (e.g., as a PKCS#12 file defined in RFC 7292). The private key shall be protected by symmetric or asymmetric encryption. The use case covers the following main scenarios. – Installation of a new certificate chain after deployment of the CS/CS controller to the CSO or major maintenance that lost credentials (following the use case "Onboarding the CS" in 8.3.15). – Installation of a new certificate when the current certificate is expiring soon. – Installation of a new certificate chain when any of CA certificates in the chain needs to be updated, including RootCA. This use case does not cover following points. – Issuer's certificate had been revoked (CA or sub-CA certificate). – The current CS certificate had been revoked. – In these cases, it is important not to trust the security of the current channel, and the CS should enter major maintenance phase, after which "Onboarding the CS" use case (8.3.15) is triggered, and all credentials and trust anchors (if necessary) need to be installed thereafter. NOTE CSO can decide to use the same certificate for the secure connection between EV and CS. Management of this certificate is described in a specific use case.

Use case conditions

	Prerequisites
1	– A secured channel between CSMS and CS is already established using a certificate that is still valid. – The CS is able to decrypt the received private key. – The CSO PKI is able to create key pairs and create the certificates according to the current certificate policy for the CS.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	A new certificate (chain) is installed in the CS	The installation is requested by the CSMS or by the CS itself	CS CSMS	End conditions: – The CS has a new certificate (chain) installed. – In case of failure during installation and old certificate is still valid, the CS may use old certificate chain if allowed. – If there is no secure communication established, then the behaviour of the CS is a business decision.

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	The CS sends a request to the CSMS for a certificate installation	The CS sends a regular request not a CSR.	CSC	CSMS	Info1 – The CS sends a request to the CSMS for certificate installation
2	The CSMS processes the request from the CS	This informative point is out of scope: – The CSMS forwards the request to the CSO PKI. The CSO PKI creates a new key pair and a new certificate for the CS. – The CSO PKI sends both private key and certificate to the CSMS. The private key will be encrypted in a way that only CS extracts the private key. – In case of a failure, the CSO PKI will send an error code to CSMS.	CSMS	CSC	Info2 – The CSMS sends to the CS the certificate and the CS private key
3	The CS receives the certificate and the private key	If step 2 was successful, the CS shall verify the received CS certificate. If this verification is ok the CS stores it locally, otherwise an error code is sent in the response of the request. In both cases the CS generates an event of severity audit documenting the verification result. If step 2 is not successful, the CS or the CSMS initiates another attempt. In case of failure during installation, the CS keeps using old certificate while it is valid. The behaviour of the CS without valid certificate is a business decision. The CS will switch to the new certificate/key material for authentication as soon as the installed certificate becomes valid without undue delay or when the CSMS requests the switch. NOTE Switching key material means that the new keys will be used for the next authentication of the CS.	CS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CS sends a request to the CSMS for certificate update	Simple request (not a CSR)
Info2	The CSMS sends to the CS the certificate and the CS private key	– Certificate – Private key encrypted in a way only the CS can extract it – Error code if something failed

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Secure storage	The CS shall store private keys in a secure storage that prevents unauthorized access to the private key.
Req2	Sanity check	The CS shall verify the validity of the received certificate and private key.
Req3	Switch to new certificate	The CS shall switch to the new certificate/key material for authentication as soon as the updated certificate becomes valid without undue delay or when the CSMS requests the switch.

8.3.21 Certificate revocation

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
M19	CS management	Certificate revocation

Scope and objectives of use case

Scope and objectives of use case	
Scope	Handle certificate revocations of primary actors and CAs
Objective(s)	Handle revocations of the certificates issued to primary actors (CS, CSMS, RM) or certificate authorities (subordinate CAs or root CAs)

Narrative of use case

Narrative of use case
Short description
This use case describes certificate revocation
Complete description
A certificate can be revoked when the device of the certificate has been compromised, the certificate's private key is compromised, or the certificate cannot be used for its purpose any more for some reason (e.g., relevant contract is terminated), or the issuing certificate is revoked. It is assumed that the revocation decision is made by the PKI operator and the decision has been communicated to CSO, and the mechanism is out of scope of this use case. It is assumed that the PKI will revoke all the certificates issued under revoked certificates. This use case is triggered when the following certificates are revoked: – entity certificates issued to CS, CSMS, and RM; – subordinate CA (SubCA) certificates in the certificate chain of these entities; – RootCA certificates that issued those SubCA certificates; – any cross certificates issued to RootCA or SubCAs mentioned above. When one or more certificates are revoked, 1) the CSMS will notify all the actors that may interact with the entity whose certificate is revoked, 2) the CSMS will update the CRLs to the actors when applicable. The actors' responses to the revocation notification and the recovery procedure of the device with revoked certificate can vary depending on the security policy of the CSO. Therefore, this document does not define any requirements regarding the revocation handling and recovery. However, this document provides the following guidelines and recommendations that can be selectively adopted by the operators. Their decisions will consider different aspects of their business such as target security level, cost, and service quality. When a certificate is revoked, CSO should consider the following recommendations. 1) It is recommended to terminate all the active communication links that were established using the revoked certificate. If the link was established after the compromise of the key, the link is not trustworthy at all, and immediate termination is strongly recommended. Even if the link was established before compromise, it is likely that either the device is under the control of the attacker or the attacker may be able to derive the session key unless the key exchange protocol used provides perfect forward secrecy (e.g., ECDHE). 2) If a device's certificate is revoked and communication links are terminated, it is necessary for the operator to decide how to recover the status of the device and how to get the device connected again to the network. a) For high level of security, the device with revoked certificate should be considered as a compromised device and it is recommended that a maintenance procedure is needed for the device; for example, a technician needs to visit the site and refresh the device state by re-flashing the system and installing new credentials. b) When an alternative certificate is available in the device, the operator may choose to use that certificate for the device to connect to the network and receive a new certificate that replaces the revoked certificate. However, caution needs to be taken. If the device is compromised, it is likely that the attacker also has access to the alternative certificate and key. In this case, re-connecting with alternative certificate does not solve the security breach. To avoid the interruption of service as much as possible, the alternative certificate may be used temporarily until a technician can reach the site for full examination and initialization of the device. c) The operator may choose to continue the operation of the device by sending over a new certificate (see "Install CS certificate" use case in 8.3.18) to the device over the communication link that was established with the revoked certificate. After delivery of a new certificate, the device will terminate the current connection and re-connect with the new certificate. This approach can maximize the service time of the device even in the event of certificate revocation. However, the operator needs to be aware of the possible adversarial consequences of this choice because the new connection with the new certificate may still be under the attacker's control. If the operator chooses this option, he or she needs to weigh not only the service quality's point of view but also the potential security breach and detrimental consequences if things go wrong. When some of the certificates in the cloud CSMS's certificate chain are revoked, CSMS should enter a maintenance status.

Overview of scenarios

No.	Scenario name	Scenario description	Pre-condition	Post-condition
1	Notification of revocation	CSMS announces the revocation events to all the relevant actors (including the entity with revoked certificate) and delivers updated CRLs if applicable.	PKI notifies the CSO about the revocation and CRLs.	All relevant actors (including the entity with revoked certificate) are notified about the revocation and CRL if applicable.

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	Notification of revocation	CSMS announces the revocation events to all the relevant actors (including the entity with revoked certificate) and delivers updated CRLs if applicable.	CSMS	local CSMS RM, CSC intermediate server	Info 1 – Revocation notification

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	Revocation notification	Revocation notification includes: – a list of certificate identifiers (issuer DN, serial number) and revocation reasons; – a list of updated CRLs.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Revocation notification	Cloud CSMS shall notify all the relevant actors about the revocation of certificates and updated CRLs. Relevant actors include the entity with revoked certificates and actors who need to verify the certificates of the entity with revoked certificates.

8.4 Deliver e-mobility services domain use cases

8.4.1 General

All the use cases in this domain belong to the service operations cycle. They describe the EVU direct or indirect interactions with the CSMS.

During these interactions, the core role of the CSMS is to constantly wait for EVU interactions through an event monitor loop. This event driven activity is distributed in the CS and in the CSMS (either local or cloud). For large configurations with many CSZs and EVSE controlled by one or more CSs, it is recommended that the monitoring loop is handled at the local level. In that case, the messages sent by the CS will be processed directly by a local CSMS without delay.

8.4.2 Use case list for deliver e-mobility service domain

Table 6 shows the list and a short description of use cases of the e-mobility domain.

Table 6 – List of use cases of the e-mobility domain

ID	Identified business use case	Brief description	Life cycle / Sequence
S1	Reservation of an EVSE	How to ensure that EVUs, having reserved an EVSE, get a parking place and an EVSE available when they check in.	Service operations / Event loop
S2	Authorization with locally presented credentials	The EVU presents credentials to be authorized by the CSMS to use the infrastructure.	Service operations / Event loop
S3	Authorization by external means	An EVU triggers a new authorization transaction at a CS, using some authorization process that is managed by the CSMS.	Service operations / Event loop
S4	Inform EVU about tariff during charging session	Inform EVU of their specific tariff information for use of the charging infrastructure.	Service operations / Event loop
S5	Inform EVU about tariff during operation	Inform EVU general tariff information for use of the charging infrastructure without the need for user identification.	Operation / Initial setup
S6	SDR information production	Fill in the required information to produce and send the information necessary to CSO for the SDR.	Service operations / Event loop
S7	ISO 15118 contract certificate installation/update	Installation/update of ISO 15118 contract certificates in EV based on ISO 15118-2 and ISO 15118-20.	Service operations / Event loop

8.4.3 Reservation of an EVSE

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
S1	E-mobility services	Reservation of an EVSE

Scope and objectives of use case

Scope and objectives of use case	
Scope	The CSMS handles a reservation of an EVSE
Objective(s)	Ensure reservation is honoured: Ensure that EVUs having reserved an EVSE get a parking place and an EVSE available when they check in.
Related business case(s)	Deliver e-mobility services

Narrative of use case

Narrative of use case
Short description
The CSMS ensures an EVSE reservation is handled
Complete description
1) The CSMS receives from the CSO a request that an EVU expects to reserve an EVSE at a certain date with some requirements like plug standard and e-mobility needs, credential, or ID elements. 2) The CSMS checks if the reservation is possible: • if the reservation is possible, the CSO informs the entity which issued the request (out of scope) and instructs the CS of the reservation details to indicate the reservation (for example display, status light) and to prevent other EV users from using the reserved resource. • If the reservation is not possible, the CSO sends a negative response to the entity who issued the request. 3) The user approaches the CS and presents the credentials. The credentials are validated by the CSMS. The user starts charging, and subsequently the reservation comes to an end when the EV leaves the parking place.

Use case conditions

	Prerequisites
1	Connection: The CS is connected to the CSMS.
2	CS accepts reservation.
3	The CSMS is able to handle reservations

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	The CSMS receives a reservation request from the CSO	The CSMS receives a request that an EV user expects to reserve an EVSE at a certain date with some requirements like plug standard and e-mobility needs, credential, or ID elements.	CSMS	
2	The CSMS checks the reservation	The CSMS checks if the reservation is possible. Examples of possible reasons for a reservation not to be possible: – power required by EVU is not available; – all EVSE are already reserved at the date of the EVU arrival; – the type of credential the EVU requests is not available (ISO 15118 plug and charge for example).	CSMS	
3	The CSMS informs the CSO of the reservation status	The CSMS sends to CSO information about the reservation status. The CSO will inform the entity which issued the request of the reservation status (possible or not).	CSMS	
4	CSO error handling	The CSO may receive new instruction by the entity which tried the reservation. Action may be taken by the CSMS accordingly.		
5	The CSMS informs the CS of the details of the reservation	The CSMS instructs the CS of the reservation details to indicate the reservation (for example display, status light) and to prevent other EV users from using the reserved resource.	CSMS	End conditions: – an EVSE is reserved; – no EVSE is available; – an EVSE is reserved for the user within limited period of validity; – charging station does not support this function; – no show (linked to a time out).

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
5.1	The CSMS receives reservation instruction from CSO	The CSMS receives a request that an EV user expects to reserve an EVSE at a certain date with some requirements like plug standard and e-mobility needs, credential, or ID elements.	CSO	CSMS	
5.2	The CS transfers to the CSMS the EVU credentials	The EVU approaches the CS and presents the credentials. The credentials are sent to the CSMS. NOTE There could be a long time between EVU arrival and reservation time.	CSC	CSMS	Info1 – Reservation credential
5.3	The CSMS validates the credentials presented by the EVU	The credentials are validated by the CSMS. A reservation transaction is added to the current service session.	CSMS		
5.4	The CSMS instructs the CS of the reservation details	The CSMS instructs the CS of the reservation details to indicate that the EVSE has been reserved (for example display, status light) and to prevent other EV users from using the reserved resource.	CSMS	CSC	Info2 – Reservation details

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	Reservation credential	Credentials defined during the reservation process
Info2	Reservation details	Information to be displayed at the EVSE that has been reserved Information related to EVU identification Information related to reservation reference Time of arrival and departure Information necessary for the CS to allocate an EVSE (like max. power, plug standard, AC or DC type of charge)

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Support of reservation	If a CS supports the function of reservation, it should guarantee parking space for the vehicle, for example using sensors and lockers.
Req2	Minimum local CSMS functionality	The local CSMS shall be able to handle reservation (allocation, credential, or ID elements) in order for the CS to accept reservation.
Req3	Reliable connection	A CS accepting reservation shall have a permanent and reliable connection with the CSMS.
Req4	Reservation information transfer	When a reservation is accepted and if the user reserved a particular EVSE, then the appropriate reservation information shall be transferred from the CSMS to the CS.
Req5	Traceability	All reservation events (acceptation, rejection, confirmation, etc.) shall trigger a reservation transaction by the CSMS.

8.4.4 Authorization with locally presented credentials

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
S2	E-mobility services	Authorization with locally presented credential(s)

Scope and objectives of use case

Scope and objectives of use case	
Scope	The scope of this UC is to describe the procedure to authorize a particular action based on the local presentation of a credential.
Objective(s)	Objective: Enable the CS to request the CSMS to authorize an action based on a credential within the context of a new or existing service session.
Related business case(s)	Deliver e-mobility services.

Narrative of use case

Narrative of use case
Short description
The CS locally receives a credential to authorize to trigger an action at the charging infrastructure level.
Complete description
– The CS requests the CSMS to authorize an action based on credential locally presented. – The credential is received and processed by the CSMS. – The CSMS sends the credential to the CSO. – The CSO receives credential from the CSMS, and requests authorization from an SA. – The CSMS gets authorization status. – The CSMS informs the CS of the authorization status. Examples of actions: The EVU swipes an RFID card to be identified and authorized to charge. The EVU swipes an RFID card to be identified in order to remove the plug. The CS gets the ISO 15118 contract certificate that was sent by the EV to the EVSE.

Use case conditions

Prerequisites	
1	The CS is able to process a credential. This credential has been issued by an EMSP. This credential could have any form (digital or material). Some additional prerequisites may depend on the action's context.

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	The CS requests the CSMS to authorize an action based on local presented credential	The CS received a credential in order for a particular action to be authorized. Possible actions are: – EVU wants to identify in order to use the EVSE; – EVU wants to identify in order to unlock the cable; – other actions.	CSC	CSMS	Info1 – Authorization Request
2	The CSMS sends the credential to CSO	This is a CSO internal process out of scope	CSMS	CSO	
3	The CSO receives credential from CSMS and requests authorization from SA	Authorization may be granted by EMSP	CSO	SA	
4	The CSMS gets authorization status	The CSMS gets the authorization status from the CSO. If this authorization failed, a reason shall be given by the CSO. If the authorization is successful, then authorization session and transactions references shall be transmitted by CSO to the CSMS.	CSO	CSMS	
5	The CSMS informs the CS of the authorization status	CS is informed of the authorization status for further local actions. In case of fail, the reason shall be communicated by the CSMS to the CS.	CSMS	CSC	Info2 – Authorization response

Information exchanged

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	Authorization request	Authorization request contains at least: – the credential presented locally.	
Info2	Authorization response	The authorization response contains at least: – the authorization status (success or fail), – the reason of the failure (error number), – references to authorization session and authorization transaction.	

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	CS information	The CSMS shall inform the CS of the authorization status without undue delay.
Req2	Integrity and confidentiality	Credential transmission shall require integrity and confidentiality.
Req3	Session and transaction	The CSMS shall trigger a new authorization session and transaction.

8.4.5 Authorization by external means

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
S3	E-mobility services	Authorization by external means

Scope and objectives of use case

Scope and objectives of use case	
Scope	Authorization transaction at a CS triggered by EVU.
Objective(s)	Objective: Enable the CSMS to instruct the CS to authorize an action within the context of a new or existing session.
Related business case(s)	Deliver e-mobility services

Narrative of use case

Narrative of use case
Short description
An authorization is given to the EVU through an external means.
Complete description
An EVU wants to trigger a new authorization transaction at a CS, using some authorization process that is managed by, or accessible to, the CSMS. The EVU and CSMS use some external mechanism to identify the specific CS (and connector/charging type) required. The EVU expects a timely indication from the CS that connection has been authorized. NOTE Credential transmission between EVU and authorizing system can require integrity and confidentiality (out of direct scope).

Use case conditions

Prerequisites	
1	Prerequisites depend on the context of the action.

Overview of scenarios

No.	Scenario name	Scenario description	Post-condition
1	Authorization is given to CSMS from EVU by external means	"External means" refers to an authorization that is given by the EVU through means that are out of scope of IEC 63110. It can be: – through mobile phone application, – with phone call to operators, – any other future out of scope ways.	End conditions: – positive authorization with necessary and optional information; – negative authorization with a reason; – other response or error from backend (e.g. backend not available).

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	The CSO receives from SA an authorization status and sends it to CSMS.	The EVU arrives at the CS and asks for authorization using external means. The authorization process is out of band of IEC 63110 but supposes that, during the process, EVU gives information about the location of the CS, his/her identity, and reference to EMSP contract. The result is that the CSO backend receives an authorization status (positive or negative) and sends it to CSMS.	SA	CSO	
2	CSMS receives authorization status and sends it to CS	The authorization status received from CSO is sent to CS. The authorization could be positive or negative. In case it is negative, a reason shall be given to CS.	CSMS	CS	Info1 – Authorization response
3	CS requires EVSE to inform EVU of authorization status	The CS requires the EVSE to instruct the EVU of the authorization status.			

Information exchanged

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	Authorization response	Authorization response contains at least: – the authorization status (success or fail), – the reason of the fail (error number), – references to authorization session and authorization transaction.	

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Information to CS	The CSMS shall inform the CS of the result of the authorization.
Req2	Information to EVU	The CSMS may ask the CS to inform the EVU of the result of the authorization typically within 5 s.
Req3	Fulfil necessary steps after authorization	The CSMS and the CS shall take the necessary steps to fulfil the action (if authorized).
Req4	Update session and authorization transaction	The CSMS shall update the authorization session with the relevant authorization transaction.

8.4.6 Inform EVU about tariff during charging session

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
S4	E-mobility services	Inform EVU about tariff during charging session

Scope and objectives of use case

Scope and objectives of use case	
Scope	Tariff information during charging session
Objective(s)	Objective: Inform the EVUs of their specific tariff information for using the charging infrastructure.
Related business case(s)	Deliver e-mobility services

Narrative of use case

Narrative of use case
Short description
In order to offer contract-based tariff for the authorized EV, the CSMS will request the CSO to ask the EMSP for the tariff information such as tariff currency, type, time, etc. based on EVU identification.
Complete description
When the EVU has a valid contract with the EMSP, the tariff information for using the charging infrastructure might be different from the generic public tariff information. The CSMS and the CS should be able to make user specific tariff information available to the user when requested. In addition to user identity, the user specific tariff information may also be dependent on the time of day, EV capabilities, secondary actor status, etc. CS should be able to obtain the tariff information from CSMS to make it available to the user. The following steps should be followed. – In order to offer contract-based tariff for the authorized EV, the CS will inform the CSMS about the EV capabilities, status, identification, etc. – The CSMS will provide the tariff information such as tariff currency, type, time, etc. to the CS tailored to the CS request. It may include terms related to parking fees and taxes. – The CSMS may send updated tariff information during charging session depending on the other real-time constraints.

Use case conditions

Prerequisites	
1	Online: The CS is online.
2	Valid contract: The EVU has a valid contract with an EMSP.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Post-condition
1	Tariffs information exchange	The CSMS asks the CSO to retrieve EVU tariffs from the EMSP. NOTE The CS can display the tariff elements. If the CSMS is aware of variation in the tariffs, it can send update to the CS.	CSMS	End conditions: Valid user specific tariff information is available for the user.

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	The CSMS sends to the CS the tariffs applicable to the EVU	In order to offer contract-based tariff for the authorized EV, the CSMS is informed about the EV capabilities, status, identification, etc. NOTE The CSMS can be informed by the CS in case of local authorization or by the CSO in case of remote authorization. The CSMS will ask the EMSP the tariff information, such as tariff currency, type, time, based on e-mobility needs expressed by the EVU and its contract with EMSP NOTE The CS can display the tariff elements. If the CSMS is aware of variation in the tariffs, it can send update to the CS.	CSMS	CSC	Info1 – EVU tariffs information
2	The CS gets the tariffs from the CSMS	The CS takes actions to inform the EVU of the tariffs received. Actions may be: – display at EVSEM; – transfer to EV through ISO 15118.	CS		

Information exchange

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	EVU tariffs information	Tariffs coming from the EMSP and related to the contract the EVU has signed. It may depend on the CSO agreement with the EMSP.	

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	CSMS sends tariffs to CS	CSMS shall be able to send tariff information based on the EV capabilities and status to CS, which may be displayed.
Req2	Tariff updates	CSMS shall be able to send updated tariff information during charging session.
Req3	Tariff validity	The validity of the tariff information may be checked.
Req4	Accept/reject	CS may inform the CSMS of acceptance or rejection by the EV/EVVU of the updated tariff information.

8.4.7 Inform EVU about tariff during operation

Name of use case

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
S5	E-mobility services	Inform EVU about tariff during operation.

Scope and objectives of use case

Scope and objectives of use case	
Scope	Tariff information during operation
Objective(s)	– Making general tariff information for using the charging infrastructure available for the user. – Inform EV user of general tariff information for use of the charging infrastructure without the need for user identification
Related business case(s)	Deliver e-mobility services.

Narrative of use case

Narrative of use case
Short description
The CSMS sends a general (public) tariff to the CS
Complete description
General tariff information for the use of the charging infrastructure shall be available to the user both when the CS is online and offline. General tariff information refers to the tariff used for ad hoc charging where the user does not have any contract related identification means. General tariff information also applies when CS is offline and not able to retrieve user-specific contract related tariff. The tariff information should be made available from CSMS to CS. An update may be triggered by the time of day, change in secondary actor status, etc., and may happen at any time. 1) CSMS provides general tariff information to CS when CS is online to support ad hoc charging when EV user does not provide any valid contract or when CS is offline. 2) If CS supports offline charging, CS will store the latest generic tariff information it has obtained from CSMS and make it available for the user. 3) When CS is online, it may obtain generic tariff information and updates for ad hoc charging. 4) The general tariff information may be updated at any time. 5) The general tariff information may contain currency, time of the day, tariff type, etc.

Use case conditions

Prerequisites	
1	The CS can be online or not.
2	The CS is able to display tariff information/make tariff information available for the end user.

Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Inform EVU of tariff information	Make ad hoc tariffs available for the EVU	CSMS CS			End conditions: Valid general tariff information can be displayed on the CS/made available to the end user both when CS is online and offline.

Scenario step by step analysis

Step No.	Name of process/activity	Description of process/activity	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)
1.1	The CSMS sends general tariff information to CS	This tariff general information will be used by EVU for ad hoc charging	CSMS	CSC	Info1 – General tariff information
1.2	The CS receives general tariff information		CS		

Information exchanged

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
Info1	General tariff information	General tariff information for all EVU except tariff negotiated with EMSP	

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Off-line information	If CS supports offline charging, CS shall be able to store the latest generic tariff information obtained when online or by any other means and make the information available for the user.
Req2	Validity	Validity of tariff information may be checked.
Req3	CSMS is able to send tariff to CS	CSMS shall be able to send updated tariff information to CS for display for ad hoc charging.
Req4	CS is able to obtain tariff from CSMS	CS shall be able to obtain tariff information from CSMS for ad hoc charging.

8.4.8 SDR information production

Use case identification		
ID	**Area(s)/Domain(s)/Zone(s)**	**Name of use case**
S6	E-mobility services	SDR information production

Scope and objectives of use case

Scope and objectives of use case	
Scope	Service detail record information production
Objective(s)	Information for SDR: Fill-in the necessary information to produce and send the information necessary to the CSO for the SDR.
Related business case(s)	Deliver e-mobility services

Narrative of use case

Narrative of use case
Short description
The CSMS collects the information necessary to form an SDR to be sent at the end of the service session to EMSP by the CSO.
Complete description
The CSMS collects the information necessary to form an SDR to be sent at the end of the service session to EMSP by the CSO. SDR is used by EMSP for billing and non-repudiation purpose. Primary source of information is CS, EVSE, CEM, EMSP and CSO. The CSMS only collects accessible information and does not form the SDR, this is done by the CSO. NOTE Only transfer of information from CS to CSMS is in IEC 63110 scope. SDR formatting by CSO is out of scope. The CSMS gathers all possible elements necessary to the SDR during the service session. The SDR contains at least the following information: 1) timestamps at beginning and end of every transaction; 2) transaction description; 3) service session ID (unique at the CSO/EMSP level); 4) type of charge AC or DC, single phase or 3 phases, etc.; 5) identification: EV identification, EVSE identification, Smart Grid Delivery Point identification; 6) total active and reactive energy transferred to EV; 7) total active and reactive energy transferred from the EV; 8) contract IDs and actors IDs involved; 9) error codes indicating that the charging session was interrupted; 10) all information necessary to establish the final price (e.g., contract terms, parking time, services fees, energy relevant item like maximum power, flexibility activation and operator reference, grid service activation and operator reference); 11) all element necessary to prove the identity of the EV, CS and EVSE; 12) information signed by the EV proving its acceptance of the charging conditions during session (e.g., metering receipt in ISO 15118); 13) when the EV stops using the charging infrastructure (e.g., the car has left the parking place and the communication session is over), the SDR is finalized and CSMS sends it to CSO; the CSO is responsible for transmitting it securely to EMSP (out of scope). NOTE Points 6 and 7 are derived per energy transfer session and operator influencing the SDR (e.g., flexibility, or mandatory grid codes or other contracts providing charging services).

Use case conditions

Prerequisites	
	– At least one service session has been started. – At least one transaction (parking, energy transfer, etc.) has started. – Contract reference, prices and other required e-mobility data are known by the CSMS.

Overview of scenarios

No.	Scenario name	Scenario description	Post-condition
1	Gathering elements for the SDR	The CSMS gathers all possible elements necessary to the SDR during the service session. This is a process that lasts from the first transaction until the service session is over.	End conditions: – The information for the SDR is produced with all relevant items. – The information for the SDR is sent to the CSO and erased from CSMS memory. – In case connection with the CSO is lost, the information for the SDR is encrypted and ready to be sent to CSO whenever possible.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Collect information	The CSMS shall collect as soon as it is available any information required by the CSO to form the SDR.
Req2	Incremental update	The CSMS shall transfer to CSO all information so the CSO is able to produce an SDR any time during the charging session (in order to avoid consequences of interruption of service or unexpected event).
Req3	Privacy	Information for the SDR contains user private data and shall be treated in consequence by CSMS (e.g., GDPR compliance for Europe).
Req4	Encryption	If the information necessary to the SDR cannot be sent to the CSO (e.g., connection is lost), it shall be encrypted by the CSMS and stored locally until connection is re-established.
Req5	Erase information after transfer	The CSMS shall erase the information for the SDR after successful transfer to CSO.

8.4.9 ISO 15118 contract certificate installation/update

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
S7	E-mobility services	ISO 15118 contract certificate installation/update

Scope and objectives of use case

Scope and objectives of use case	
Scope	Installation/update of ISO 15118 contract certificates in EV based on ISO 15118-2 and ISO 15118-2-20.
Objective(s)	Support ISO 15118 plug and charge: CS and CSMS support the installation/update of ISO 15118 contract certificates in EV based on ISO 15118-2 and ISO 15118-2-20.
Related business case(s)	

Narrative of use case

Narrative of use case
Short description
Support of contract certificate in the EV in the context of ISO 15118
Complete description
When ISO 15118-compliant EV requests an installation or update of contract certificates via CertificateInstallationReq or CertificateUpdateReq message of ISO 15118, CS requests CSMS to retrieve the requested contract certificates and accompanying information needed for secure installation from a secondary actor (CPS or CPP). With ISO 15118-2, only one certificate will be delivered, but with ISO 15118-20, multiple certificates can be delivered. Updates of certificates are only supported by ISO 15118-2. NOTE 1 In this description, CertificateInstallationReq/Res and CertificateUpdateReq/Res messages mean EXI-encoded ISO 15118 messages (and additionally encoded in Base64, if needed) under the respective XML schema of the current session between EV and CS. NOTE 2 In principle, throughout this document, CSMS is deemed unaware of the ISO 15118 stack (ISO 15118 schema and respective EXI layer) for the sake of simplicity and modular approach. 1) When CS receives a CertificateInstallationReq or CertificateUpdateReq message from EV. a) CS verifies the signature of the message using the certificate contained in the message (OEM provisioning certificate for installation and contract certificate for update). b) CS validates the certificate chain (if it has the corresponding RootCA certificate (even if CPS/CCP will do this validation again anyway). c) CS sends the following information to CSMS for the retrieval of contract certificates: i) CertificateInstallationReq or CertificateUpdateReq message (as is); ii) PCID (for installation) or EMAID (for update); iii) ISO 15118 schema version of the message; iv) deadline for retrieval (due to ISO 15118 timeout); v) list of V2G RootCA certificates trusted by the EV (CSMS uses this information to determine CPS/CCP to retrieve contract certificates); vi) for ISO 15118-2, list of certificate hashes obtained from trust_ca_keys received from EV during TLS; vii) for ISO 15118-2, list of DN/Serial pairs obtained from ListOfRootCertificateIDs in CertificateInstallationReq. 2) CSMS then retrieves contract certificates as follows (out of scope). a) CSMS identifies the list of CCP/CPS to contact as follows: i) if a directory service exists, CSMS queries it for the list; ii) if no directory service, CSMS selects candidate CCPs/CPSs, whose RootCA the EV can trust, among a known set of CCPs/CPSs; iii) CSMS then forwards the message from CS (step 1-b) to the chosen CCPs/CPSs in Step 2-a-i or 2-a-ii. b) CSMS then collects available contract certificates from replying CCPs/CPSs. 3) CSMS sends one or more contract certificates to CS as follows. a) If CSMS gets nothing by the deadline indicated in step 1-b, CSMS sends an error code to CS and terminates the use case. Possible error code: NO_CONTRACT_CERTIFICATE_FOUND.

Narrative of use case
b) For ISO 15118-2, CSMS sends the received CertificateInstallationRes or CertificateUpdateRes message to CS. c) For ISO 15118-20, CSMS sends a collection of received CertificateInstallationRes messages (or only partial information of the message) to CS, either immediately after reception or all together at once, indicating the completion of the retrieval. 4) Then, CS sends certificates retrieved from CSMS as follows (out of scope). a) For ISO 15118-2, CS forwards the CertificateInstallationRes or CertificateUpdateRes message with updated SessionID to EV. b) For ISO 15118-20, CS forwards to EV each CertificateInstallationRes message with updated SessionID, EVSEProcessing, RemainingCerts, EVSEStatus, and ResponseCode. When EV indicated a MaxSupportedCerts in CertificateInstallationReq less than the number of available contract certificates, CS sends certificates whose EMAID is in the PrioritizedEMAIDs of CertificateInstallationReq first.

Use case conditions

Prerequisites	
1	Support of ISO 15118 versions requiring certificates.

Overview of scenarios

No.	Scenario name	Scenario description	Primary actor	Pre-condition	Post-condition
1	Install/update contract certificate	The CSMS gets the contract certificate	CSMS	– CS and CSMS have already established a secure communication channel. – The CSMS knows a Directory Service, or the CSMS has a list of known CPSs/CCPs and their V2G RootCA certificates. – EV and CS communicate over ISO 15118 with PnC identification method. – CPS/CCP validates the certificate chain (OEM provisioning certificate chain for installation and contract certificate chain for update)-OOS – CPS/CCP checks the revocation status of the certificate chain (OEM provisioning certificate chain for installation and contract certificate chain for update)-OOS	End condition: This use case ends when CS receives contract certificates successfully. Otherwise, the CS receives an error code from CSMS.

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	The CS receives a CertificateInstallationReq or CertificateUpdateReq message from EV	The way the CS receives the message from the EV through the EVSE is described in ISO 15118.	CSC	CSMS	Info1 – The CS asks the CSMS for an ISO 15118 contract certificate
2	The CSMS retrieves contract certificates	The way the CSMS retrieves the contract certificate is out of scope. See complete description for more information.	CSMS		
3	The CSMS sends one or more contract certificates to CS	CSMS sends one or more contract certificates to CS as follows • If CSMS gets nothing, CSMS sends an error code to possible error code: NO_CONTRACT_CERTIFICATE_FOUND • For ISO 15118-2, CSMS sends the received CertificateInstallationRes or CertificateUpdateRes message to CS. • For ISO 15118-20, CSMS sends a collection of received CertificateInstallationRes messages (or only partial information of the message) to CS, either immediately after reception or all together at once, indicating the completion of the retrieval.	CSMS	CSC	Info2 – The CSMS sends to the CS the contract certificate(s)
4	The CS receives the contract certificate(s) from CSMS and forwards it to the EV	• (ISO 15118-2) CS forwards the CertificateInstallationRes or CertificateUpdateRes message with updated SessionID to EV. • (ISO 15118-20) CS forwards to EV each CertificateInstallationRes message with updated SessionID, EVSEProcessing, RemainingCerts, EVSEStatus, and ResponseCode. When EV indicated a MaxSupportedCerts in CertificateInstallationReq less than the number of available contract certificates, CS sends certificates whose EMAID is in the PrioritizedEMAIDs of CertificateInstallationReq first.	CS		

Information exchanged

Information exchanged, ID	Name of information	Description of information exchanged
Info1	The CS asks the CSMS for an ISO 15118 contract certificate	1) CertificateInstallationReq or CertificateUpdateReq message (as is). 2) PCID (for installation) or EMAID (for update). 3) ISO 15118 schema version of the message. 4) Deadline for retrieval (due to ISO 15118 timeout). 5) List of V2G RootCA certificates trusted by the EV (CSMS uses this information to determine CPS/CCP to retrieve contract certificates). 6) For ISO 15118-2, list of certificate hashes obtained from trust_ca_keys received from EV during TLS. 7) For ISO 15118-20, list of DN/Serial pairs obtained from ListOfRootCertificateIDs in CertificateInstallationReq.
Info2	The CSMS sends to the CS the contract certificate(s)	– For ISO 15118-2: CSMS sends the received CertificateInstallationRes or CertificateUpdateRes message to CS. – For ISO 15118-20: CSMS sends a collection of received CertificateInstallationRes messages (or only partial information of the message) to CS, either immediately after reception or all together at once, indicating the completion of the retrieval.

Requirements

Requirement R-ID	Requirement name	Requirement description
Req1	Check validity	Upon reception, the CS shall verify the signature of the CertificateInstallationReq and CertificateUpdateReq message.
Req2	CSMS sends contract certificate to CS	Upon reception, CSMS shall request contract certificates from secondary actors, and forward the received information back to CS.
Req3	Ongoing information to CS	When multiple contract certificates are received, the CSMS shall indicate the completion of the reception to the CS.
Req4	Error handling	When no contract certificates are received, CSMS shall indicate the error (NO_CONTRACT_CERTIFICATE_FOUND) to CS.

Annex A
(informative)

Implementation examples

A.1 General

Annex A presents informative examples of possible implementations of the general IEC 63110 communication architecture. It is not intended to represent an exhaustive vision of all situations. Refer to communication requirements in 7.3 for normative details.

A.2 A simple home example or a single EVSE at kerbside

The CSMS connects directly to the CSC embedded in the CS. There is no local CSMS. The cloud CSMS connects directly to the CSC. Figure A.1 shows an illustration of this case.

NOTE A simple CEM functionality could also be embedded in the CSC, but this would not scale correctly if another CS exists in the same home.

Secondary actors exchanging messages with the CSO may influence the charging or the behaviour of the CS. Examples of message from SAs: call for flexibility, peak hour, or emergency signal from DSO. The link between the CSC and the DSO will be indirect, for example through the meter control interface or the CEM if there is one.

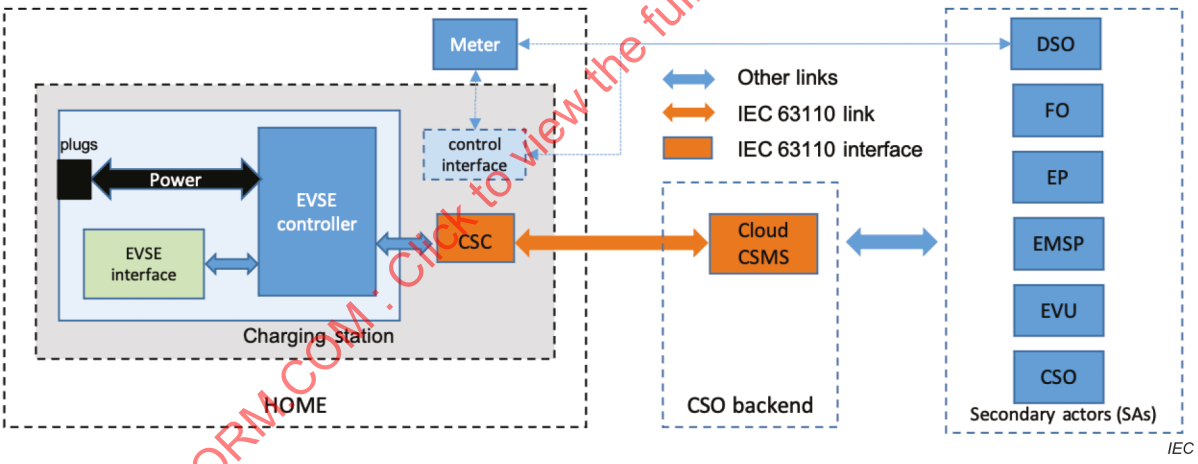


Figure A.1 – A simple home with one CS

A.3 A more complex home with one or more CSs

In a more complex situation, the home owner has installed a CS, a solar panel, battery storage and a CEM. Figure A.2 shows an illustration of this case.

Based on communication requirements in 7.3, CSC only accepts messages exchanges with CSMS (local or cloud); and CEM, via the RM, exchanges messages exclusively with CSMS.

In this example, a local CSMS is installed and is able to communicate locally with the RM and the CSC.

A local CSMS has three functions:

– seamlessly route all messages between CSC and Cloud CSMS;
– interface with the RM and route the messages to Cloud CSMS if necessary;
– take local decisions, for example in case communication with cloud CSMS is broken.

Secondary actors like DSO or FO may exchange messages with the CSO and/or CEM. These messages can influence the charging or the behaviour of the CS.

NOTE The Local CSMS could be embedded in the CSC but this would not scale correctly if another CS exists in the same home.

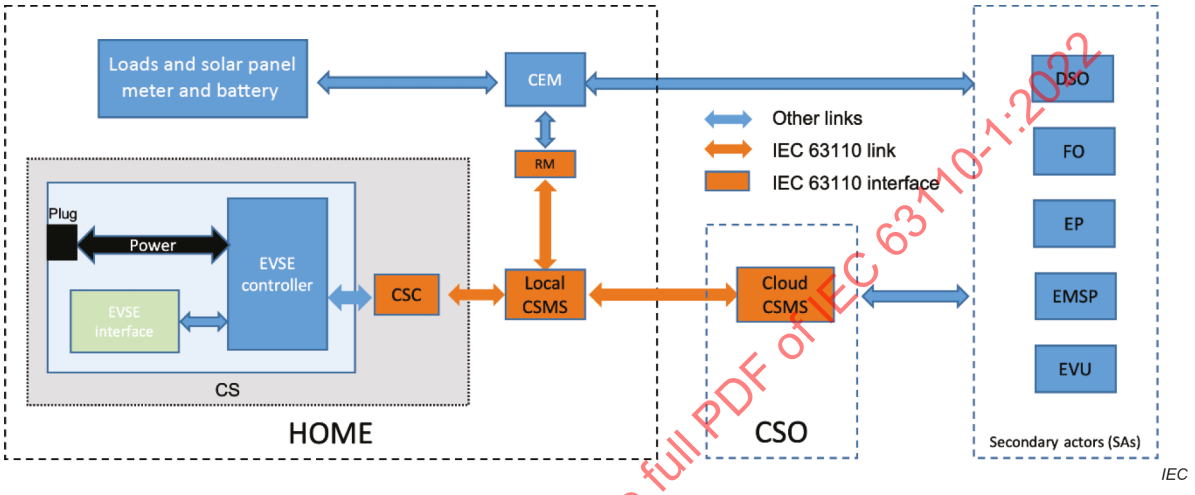


Figure A.2 – Complex home with one CS

A complex situation with two charging stations is showed in Figure A.3. It illustrates a home with two CSs, a solar panel, storage and a CEM and a local CSMS. The RM sends aggregated power profiles or energy related constraints based on production, storage, energy transfer plan or energy tariff variations to the local CSMS. The local CSMS allocates the energy to the EVs according to the CEM constraints and their respective mobility needs. The local CSMS can take decisions on behalf of the CSMS like load balancing between the two CSs.

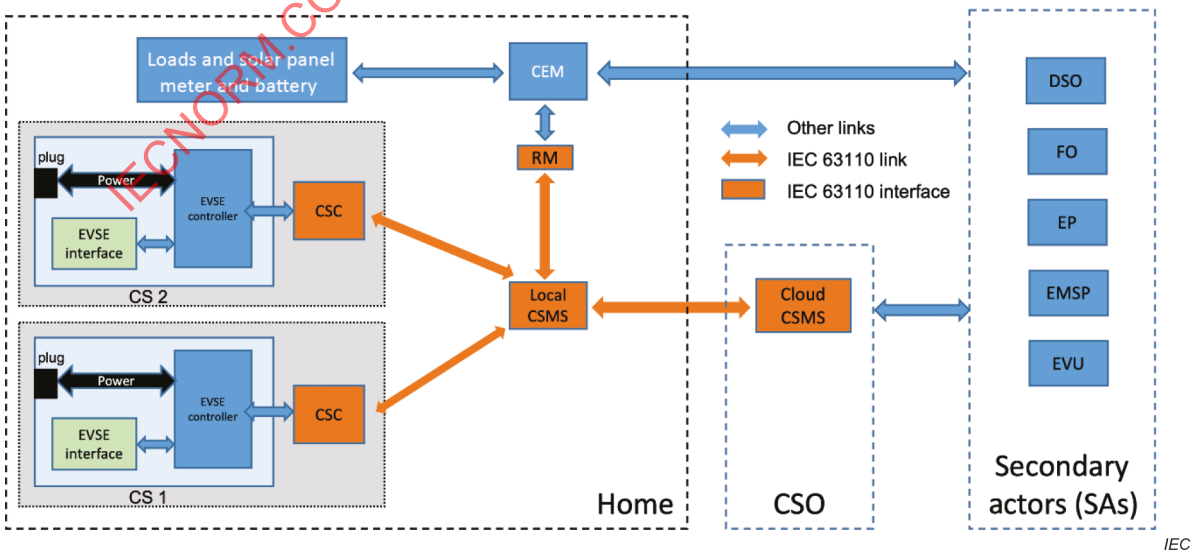


Figure A.3 – Complex home with two charging stations

A.4 Parking lots or high-power CS example

Figure A.4 illustrates the situation of a parking lot or a group of high power EVSEs in a highway with no other loads. The CS is composed of one or more EVSEs controlled by at least one CSC. More than one CSZ and CSs, connected to other EVSEs is also a possible implementation. A local CSMS is present. As the site is only dedicated to charge EVs, for simplification of the design, a CEM functionality is embedded in the local CSMS, but it could be located somewhere else in the site.

The CS manages all EVSEs via a dedicated communication link (out of scope of IEC 63110).

The DSO may have installed an interface able to receive its messages and to communicate them to the local CSMS via the RM. Messages may be related to grid code behaviour (frequency regulation or voltage regulation signals) or emergency. During an emergency situation, the DSO could request that the CS goes down to a low power mode (e.g., 20 % of its maximum power). The message would be sent by the DSO to its interface and transferred to the CEM. Based on mobility needs, the local CSMS starts immediately load balancing actions sending relevant messages to the CSC.

The CSO may also receive messages from other secondary actors, for example FO.

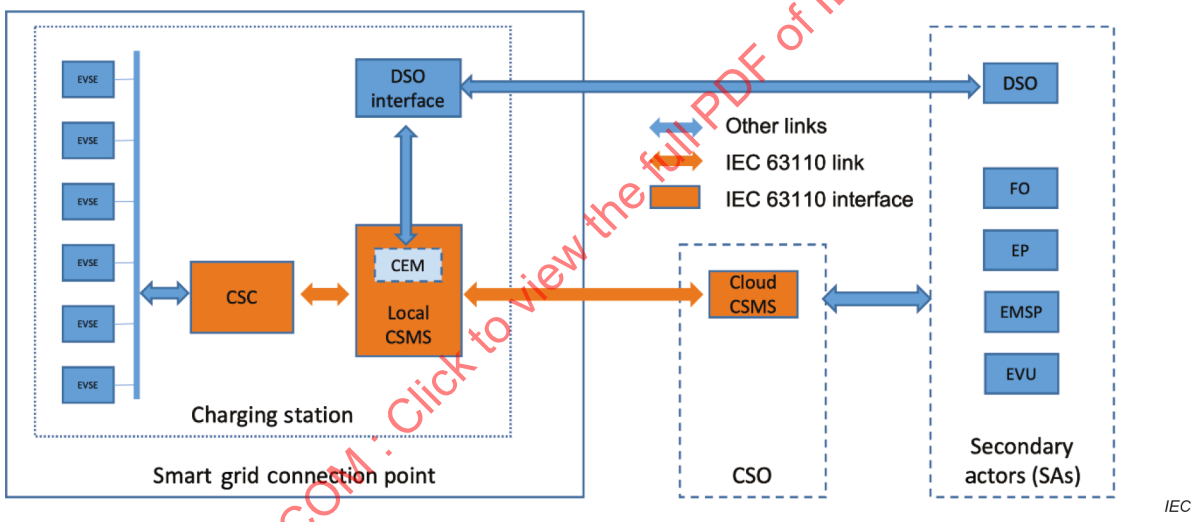


Figure A.4 – Parking lot example

A.5 A CS with local production and storage

Figure A.5 shows the example of a group of EVSEs installed inside a SGCP with local production, battery storage and CEM. The system could be significant in terms of power, for example with high power EVSEs.

The CEM is able to exchange messages with the CSMS (either local or cloud), the storage and production units. The CEM is also able to receive messages from secondary actors like DSO, for example in case of network congestion. The CEM can also exchange information from devices able to measure voltage and frequency and trigger ancillary services.

The CEM exchanges messages, via the RM, with the CSMS in order to optimize global consumption or production based on local conditions or on messages coming from SAs. Based on PRE received from the RM, the CSMS sends ETPs to the CSC to manage energy transfer (charging or discharging) for each EVSE. In case there is a local CSMS, it can transfer the messages to the cloud CSMS if the decision cannot be taken locally.

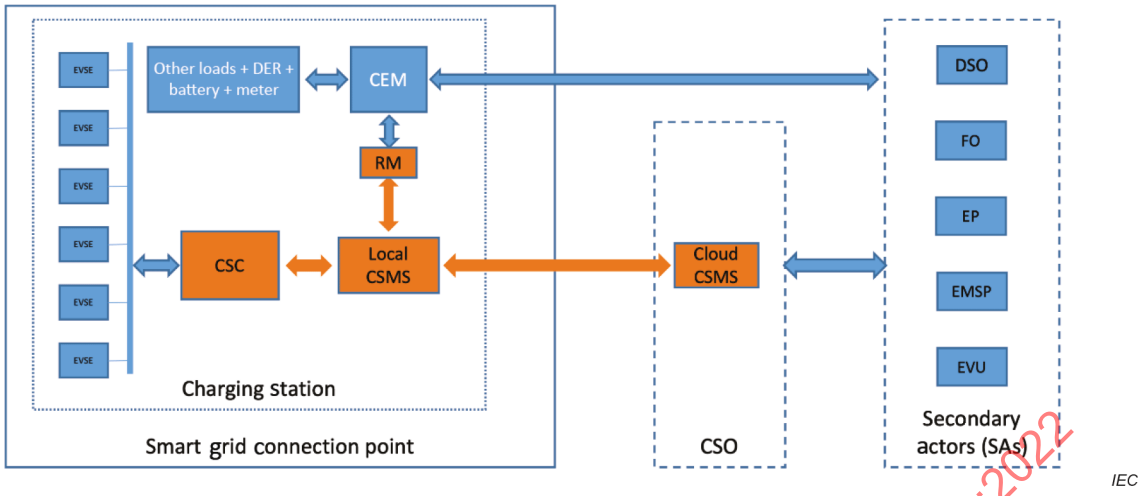


Figure A.5 – CS with local production and battery storage

Annex B
(informative)

Requirements used for selecting the transport technology

B.1 Message specific timeouts shall be supported

Necessary.

The protocol shall be able to define specific timeouts for different interactions (message exchange at the application layer).

Some messages are more critical than others. Some messages demand more (backend) processing than others, which results in (highly) different latencies. So, a uniform reaction time is hard to define and a decision if a message "was lost" and how to react to such an event is hard to capture by one single timeout definition.

For example, ISO 15118 has some timing requirements which might impact the CSO backend communication (certificate update is one example).

B.2 Transport foundation shall be IP based – with IPv4 and IPv6 support

Necessary.

The internet protocol (IP) is non-proprietary and well documented. It is compatible with all operating systems, so it can communicate with any other system, and hardware support is well established.

Today's backbone is IPv4 based but all future evolution (e.g., on wireless networks) will require IPv6 support.

B.3 It shall be possible to transport encrypted and/or signed message payload sub-elements

Necessary.

Privacy and security are a key (legal) requirement. Some data elements (e.g., firmware images, credential update requests) might need to be transferred from, for example, an EV to a CSP without the CSO having the right to "read" or "modify" that data. In those cases, fragments (sub-elements) of the message need to be encrypted or signed independently of the underlying message transport system.

Common solutions:

– In general, this can be achieved with any encoding technology. In most cases, however, it might require custom definitions for the data structures and techniques (signatures, encryption etc.).
– Allow binary payloads in the messages.

B.4 The communication between a CSC and a CSMS shall be encrypted (transport layer)

Necessary.

The communication between a CSC and a CSMS will carry sensitive data. Because "untrusted" communication services (e.g., regular mobile phone networks) will be used in real applications of IEC 63110, this demands that the entire communication stream shall be encrypted.

B.5 Bidirectional communication shall be possible

Necessary.

True bidirectional capabilities are needed, because IEC 63110 needs to cover use cases where activity can originate on both sides of the communication channel.

The IEC 63110 communication pattern is not limited to a simple client-server setup but can also be more of a peer-to-peer nature.

B.6 Long messages shall not block urgent messages

Necessary.

Some of the IEC 63110 use cases will naturally result in very large messages. A common example might be the servicing of charging stations, which includes the firmware upgrade process, which might need to transmit some megabytes of data.

In order to limit the number of parallel channels, and to prevent the channel from getting blocked for a very long time by a single large message, it is necessary to have a strategy from how to multiplex small messages while big bulk messages are being transmitted.

NOTE Depending on the size of largest IEC 63110 messages and the lowest bandwidth of an acceptable communication technology and the priority requirements of critical message, this could force message chunking to meet all those requirements or force the use of out-of-band transmission protocols (e.g., sftp).

B.7 Message payload encoding shall be memory and CPU efficient

Desirable.

In order to support a broad range of possible solutions and to reduce operating costs, the message encoding should not come with unnecessarily demanding requirements during processing (on memory size or CPU cycles). "Bigger" (more inefficient) data representations typically drive hardware and transmission cost up.

B.8 Message priority shall be under the control of the application layer

Desirable.

Especially on very low bandwidth physical networks (e.g., 3G wireless), the application layer might need to have a very precise understanding of and control over the message delivery queue. This will typically be driven by timing requirements for critical messages.

B.9 Asynchronous message transfer shall be supported

Necessary.

Some use cases (simple status updates) do not need messages that satisfy a strict request-response (confirmation) pattern. In those cases, asynchronous messages can reduce the latency and increase the transmission bandwidth within the system.

For increased efficiency, a single communication channel should be able to support sending multiple messages without having to wait for the response. Note that there may be circumstances where the application might want to block.

B.10 Authentication with related session mechanism shall be supported

Necessary.

Different messages might need different levels of authentication or privileges.

Since the authentication (e.g., with certificates) might be compute intensive, a related session concept would be helpful, so that the process does not need to be repeated with every single message.

B.11 Multicast messages should be supported

Necessary.

For some use cases, multicast ("group level targeting") messages might be a helpful capability in order to reduce the necessary transmission bandwidth (e.g., firmware upgrades of a CS) or to increase reaction times (e.g., emergency set-point communication).

NOTE 1 The message is broadcasted, so response is not mandatory.

NOTE 2 It is really about ease of broadcasting to groups and sub-groups and not about reducing network bandwidth.

B.12 Addressing scheme needs to be supported

Necessary.

In order to support "virtual function end-points", "broadcasting" or "pub-sub" style communication patterns, a concept of resource identifiers is needed. This will allow "binding" to a resource or targeting (addressing) a message to a resource or (group of) receiver(s).

If a cloud CSMS wants to address a specific CS which is "behind" a local CSMS, there is a need to know how the information will find its target. TCP/IP will not solve this problem in that case.

B.13 Coordinated time at CS level shall be supported

Desirable.

For many use cases, "time" is a key concept: parking reservations, energy transfer plans, failure statistics, certificate expiration, message timeouts and retransmissions, etc.

By its nature, IEC 63110 is a distributed system where (potentially conflicting) information can originate at different sources. To determine "order" or identify the "truth", timestamps are a key mechanism.

In most cases, it is the application layer that needs to know the "time" (of the system, of message creation, etc.). In some cases, it is the message dispatching part (perhaps in the transport system) that needs to understand "time" (to discard outdated messages, to properly (re)order the message queue, etc.).

B.14 Message encoding shall support non-standard payload elements

Desirable.

Some applications will require custom payload elements in addition to the standardized payload data.

This is common when applying a technology for use cases that have not been fully covered when the standard was defined or during research and the testing of future protocol features.

NOTE There is the possibility for this non-standard payload to be misused, so care is needed when wording the allowance for using of this payload extension.

B.15 Message encoding shall support versioning

Necessary.

In order to support the evolution of a protocol and to enable system migration in real world deployments, the encoded payload should carry a reference to the schema version which was used during the encoding process of the message.

The system needs to allow for evolution of messages and data in order to ensure forward and backward compatibility.

At the system level, message versioning is needed.

NOTE This is "mandatory" for the entire system, but is "optional" at the encoding layer, since it can be solved in different ways.

B.16 Communication shall be delay tolerant

Desirable.

The transfer time may vary from some milliseconds to seconds. The communication protocol needs to be tolerant to such delays.

Transfer time is defined as the overall transfer time from application to application including the coding at the sender side, the delay in the communication network and the decoding at the receiver side.

B.17 The communication technology should have a high reliability in payload delivery

Desirable.

Reliability falls into the following "problem domains":

– confirmation of message delivery (no-ACK, one-way-ACK, two-way-ACK?);
– message (payload) integrity;
– guarantee of "order preserving" message delivery.

B.18 The selected communication technology should not have a single point of failure

Desirable.

There should be no single point of failure all along the communication path between two communicating entities. The maximum recovery delays and failure behaviour should be well documented (and customizable).

B.19 Technology shall have proven implementations

Desirable.

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

These tools may include:

– protocols used by the technical solution: implementations of the main components of the technical solutions);
– simulators: client side or server-side simulators to validate the interoperability;
– protocol analyzer used to analyse the protocol stack on the Ethernet link.

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

B.20 Technology shall not have intellectual property restrictions

Desirable.

Typically, there are many "open" (unrestricted) choices available.

B.21 The communication technology shall be stable

Desirable.

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

Evolutions may be linked in particular to the number of standardization bodies involved, and the associated management rules. There is a strong need for a long-term stable solution since the typical system lifetime is 20 years and longer.

Positive criteria:

– a complete specification is available;
– vibrant community;
– rapid response to known vulnerabilities and limitations (e.g., lack of features).

Negative criteria:

– technology is orphaned, nobody seems to be maintaining it anymore;
– bad track record of maintaining technologies.

B.22 Fine grained authorization shall be supported

Necessary.

Systems shall be capable of simultaneously holding multiple connections to different communication partners with different trust levels.

The goal is to prevent primary actors from accessing the overall system. For example, a CS might be restricted to data only for that CS. A local CSMS may be restricted to the data for the CS at a local site.

For example:

A local CSMS shall only be allowed to control its local CS nodes in a CSZ but not remote CS node of another CSZ.

Communicating with CEM or when receiving message from secondary actors like DSO or FOs.

The following needs to be considered:

– there is a need for connection-based as well as role-based access control;
– for processing efficiency, a related session concept should be available;
– this is tightly related to the requirement of Clause B.10 "Authentication with related session mechanism shall be supported".

B.23 Communication layer shall be supported by at least two operating systems and embedded platforms for CS and CSMS

Desirable.

– The communication layer should not favour a specific operating system/platform.
– The communication layer should support embedded environment that CS will run on.
– Selection should not mandate a certain commercial framework to run.
– This requirement does not necessarily promote a cross-platform solution.

B.24 Interoperability with conventional information models used in power industry

Desirable.

Interoperability between IEC 63110 information model and other power-industry-friendly information models (like IEC 61970 or IEC 61850) is necessary for seamless integration of charging infrastructure with other parts of the grid.

B.25 Communication layer shall support IEC 63110's multi-level architecture for CSMS

Desirable.

The IEC 63110 communication architecture is a multi-level architecture shared between local CSMS and cloud CSMS. The goal of this requirement is to ensure that the chosen communication layer meets all the communication/architectural requirements imposed by this multi-level CSMS ambition.

What are the goals [G] of the hierarchical CSMS architecture?

[G1] Local CSMS acts as a mirror of cloud CSMS that can also deal with local factors by communicating with CEM, for example.

[G2] Local CSMS can handle offline situations.

[G3] Local CSMS acts as an edge computer to lessen the burden of cloud CSMS for better scalability and performance.

Protocol needs to define architectural [A] requirements:

[A1] Every CSC can communicate with a single cloud CSMS through various network configurations.

[A2] Optionally, a local CSMS can reside between CS and cloud CSMS.

[A2'] Optionally, a local CSMS can reside inside the same grid point as the CSC.

[A3] A local CSMS is not necessarily directly connected to the CSC (there could be some switches, bridges, routers in between, even could reside outside the physical facility of the CSC as far as it can do its job and meet the scalability needs).

[A3-1] CS has multiple communication paths to local CSMS.

[A4] A local CSMS can also communicate with other components such as a CEM.

[A5] This architecture is hierarchical in that a cloud CSMS deals with multiple local CSMSs as well as multiple CSs, and a local CSMS deals with multiple CSs.

[A6] Local CSMS and cloud CSMS knows whether itself is local or cloud.

For the communication [C] layer:

[C1] Local CSMS is transparent to CSC in that CSC cannot distinguish the communication with local CSMS from that with cloud CSMS (e.g., CS cannot tell whether a message is from local CSMS or cloud CSMS; CSC knows only one address for CSMS).

[C2] The authentication and key-exchange mechanism should support this architecture: for example, CSC authenticates one CSMS, which implies the authentication of the other, or CSC authenticates both without knowing it deals with two CSMSs.

[C3] A message sent from CSC to CSMS is accessible by either CSMS or both depending on the type of information.

[C3-1] Encrypted messages from CSC should be accessed from local CSMS or cloud CSMS depending on their access right to that particular information (access control mechanism).

[C4] All other requirements can be achieved even if the communication is encrypted.

[C5] CSC should be able to address the abstraction of CSMS so that the CSC does not care which CSMS it is talking to, whereas both the CSMS can recognize which CSC they are dealing with.

[C6] CSC should be able to receive data generated by either CSMS and either CSMS can receive interested information generated by interested CSs.

[C7] It will be a plus for the communication layer if it can handle all the issues about "abstraction of CSMS with concrete CSMSs behind" regardless of the underlying physical network architecture and without the need for a fancy state-of-art technology like SDN (software-defined network).

[C8] There should not be a significant performance degradation due to the realization of CSMS-abstraction layer.

B.26 Efficient support for binary payload

Desirable.

Certain data elements will need to be transmitted via IEC 63110 as binary data. The encoding protocol should allow efficient handling of such payload values.

The data which would fall into this category are:

– signed certificates or SASchedule information for ISO 15118 charging;
– encrypted data;
– firmware images;
– advertisement images;
– etc.

B.27 Communication layer shall support request/response and publish/subscribe patterns

Mandatory.

In the CSMS "multi-hop" architecture, a number of different communication patterns will be needed. The communication layer shall not prohibit their usage or implementation.

Possible patterns:

– request-response (e.g., for targeted command and control interactions);
– publish + subscribe (e.g., for generic status monitoring).

Annex C
(informative)

Example of a complex service session

C.1 Visual representation

Figure C.1 shows an example of a service session including reservation, parking, energy transfer and other services.

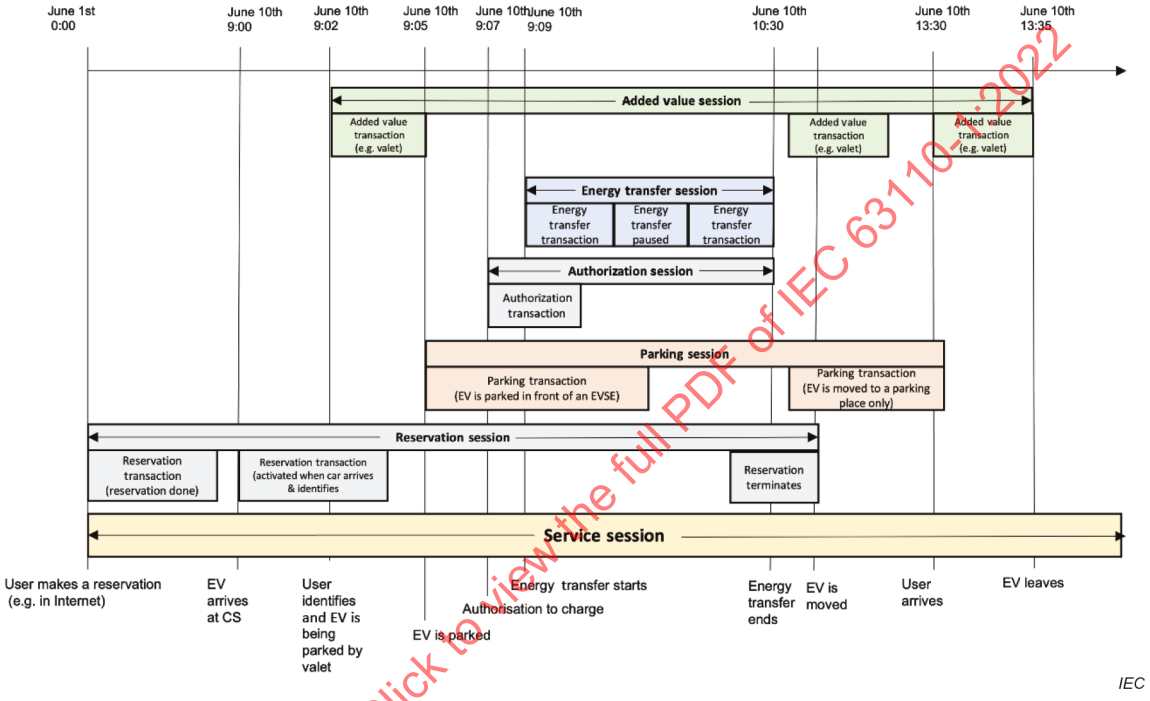


Figure C.1 – Example of a complex service session

C.2 Description

a) On 1 June, the user reserves a place to park and charge an EV in a parking lot with a reservation starting on 10 June at 9:00. The reservation process in itself is out of scope of IEC 63110. A reservation file will eventually arrive at the CSO backend so a charging infrastructure corresponding to the EV characteristics and EVU mobility needs can be allocated to the user (and necessarily also a parking place). The CSO registers this reservation transaction by creating a first entry in a new SDR document. From CSO point of view, this event marks the start of the service session. CSMS and CSO need to share the same SDR and service session references so they can update each other on any event during service session life.

b) On 10 June at 9:00, the EV arrives at the parking lot and the EVU or the EV is identified at 9:02. A reservation transaction event is triggered when there is a match between the reservation reference presented by the EVU and the reference contained in the reservation transaction recorded in the CSO backend. This event triggers a new entry in the SDR corresponding to this new reservation transaction.

c) The EVU then decides not to park and plug the EV but to use the valet service offered by the parking lot. If this valet service is registered in the CSO backend as another session service, then this transaction will create at 9:05 a new entry in the SDR in the clause related to other session.

d) After the EV is parked by the valet and if the parking session is registered in the CSO backend as a service, an entry in the SDR is created for the parking service with the corresponding parking transaction (start of parking).

e) At 09:07, the valet plugs the EV. This event will trigger the start of an authorization session and the related authorization transaction. If the authorization is successful, the energy transfer can start. The detailed sequence of the authorization session depends on the identification technology used. For example, if ISO 15118 plug and charge is used, the CSMS will first need to transfer to CSO the relevant certificate sent by the EV during identification phase and wait for the validation from the EMSP.

f) At 09:09, the energy transfer session starts. The detailed sequence of the energy transfer session depends on the charging technology used. For example, if ISO 15118 plug and charge is used, once authorized the ISO 15118-2 negotiation will start. After that, the CSMS will need to allocate the power profile negotiated. The CSMS informs the CSO of the beginning of the energy transfer session based on the corresponding energy transfer transaction (start of charge). The CSO then creates a new entry in the SDR.

g) Depending on the granularity of the SDR and if the CSMS is informed of any energy event, like the pause in the example or a renegotiation, the CSMS will trigger a new energy transfer transaction that can be sent to CSO in order to update the SDR.

h) At 10:30, if the CS is informed of the end of the energy transfer (with ISO 15118 this could correspond to the end of the V2G session), a last energy transfer transaction is sent to the cloud CSMS. This event will contain the sum of all the active and reactive energies exchanged during all the energy transfer session in order for the SDR to contain all the energy exchanges with their corresponding financial conditions.

i) Optionally, the valet service, informed by the CSO that the energy transfer session is over, can decide to move the EV to a parking zone without EVSE. This could trigger a new parking transaction entry in the SDR with possibly a change of parking tariffs conditions.

j) On 20 June at 13:30, the EVU returns and asks the valet to get the EV. This triggers a new SDR entry in the parking transaction section and the finalization of the parking session at 13:36. When the EVU gets the keys of the EV, the CSO is informed and all pending sessions including the reservation and the service session are closed. The CSO writes the corresponding entry in the SDR.

Some of the steps of this example of a complex service session are not directly in IEC 63110 scope but most of them depend on communication between CSMS, CSC, CSO and parking lot operator.

Annex D
(informative)

Classification of use cases impacts

The following classification offers a view of the use case in terms of impact and risk. Its objective is to help readers and implementers of IEC 63110 to prioritize their development, their reading and implementation.

Use cases do not have similar impact in terms of operation, cybersecurity, latency of message, and time of execution.

To sort the use cases in terms of impact, different criteria have been used. The criteria have different meaning depending on the risk.

– Operation risk levels are qualified as: high, medium, and low. They measure the impact on the operation of the CSO if the use case fails.
– Cybersecurity risk levels are qualified as: high, medium, and low. They measure the impact on the data protection if there is a cybersecurity issue during the use case.
– Communication cost levels are qualified as: high, medium, and low. They measure the bandwidth needed by the use case. Bandwidths are relative and not absolute.
– Timing expectation levels are qualified as: fast, medium, slow, and unknown. They measure at what speed the use case is expected to perform. Timings are relative.
– Frequency operation levels are qualified as: often, sometimes, rare, and unknown. They measure how often the use cases are used in the life of a CS/CSMS. Levels are relative.

Table D.1, Table D.3 and Table D.2 show a classification for all the use cases and for the three domains presented in this document.

Table D.1 presents the classification for the energy domain.

Table D.1 – Use case classification of the energy domain

Use case name	Operation risk level	Cybersecurity risk level	Communication cost level	Timing expectation level	Frequency operation level
Smart charging	High	Medium	Medium	Medium	Unknown
Charging with demand response	Medium	Medium	Low	Medium	Rare
CSMS – RM exchange of information at the initiative of the CSMS	Medium	Medium	Low	Medium	Often
CSMS – RM exchange of information at the initiative of the RM	Medium	Medium	Low	Medium	Rare
Power variation triggered by DSO	Medium	High	Low	Medium	Rare
Actors' relations during a V2G session	Medium	High	High	Fast	Often
Information exchange required to ensure a dynamic energy transfer control	Medium	High	High	Fast	Often
Providing frequency regulation service by means of decentralized frequency measurements	Medium	High	high	Fast	Rare

Table D.2 presents the classification for the manage CS domain.

Table D.2 – Use case classification for the manage CS domain

Use case name	Operation risk level	Cybersecurity Risk level	Communication cost level	Timing expectation level	Frequency operation level
Discover CS configuration	High	Low	High	Medium	Sometimes
Update a CS component properties	High	Low	Medium	Medium	Sometimes
Monitor a CS	High	Low	Medium	Slow	Often
Update the firmware of a CS	High	High	Medium	Slow	Rare
Reboot a CS	High	High	Low	Fast	Rare
The CSMS sets the information to be presented to the user	Low	Low	Medium	Fast	Rare
The CSMS sets log criteria	Medium	Medium	Medium	Slow	Sometimes
Retrieve log information from the CS	Low	Medium	High	Slow	Sometimes
Fault-code provisioning	Medium	Low	Low	Medium	Often
Information deletion triggered to CSMS by an SA	Medium	Medium	Low	Slow	Rare
CS deregistration	Medium	Medium	Low	Slow	Rare
Migration of the CS	Medium	Low	Low	Slow	Rare
Onboarding the CS	Medium	Low	Low	Slow	Rare
CA certificate provisioning	High	High	Medium	Medium	Rare
ISO 15118 OCSP response messages	Medium	High	Medium	Fast	Often
Install CS certificate	High	High	Medium	Medium	Rare
Install the certificate of the local CSMS	High	High	Low	Medium	Rare
Install CS certificate with key pairs created outside	High	High	Medium	Medium	Rare
Certificate revocation	High	High	Low	Fast	Rare

Table D.3 presents the classification for the deliver e-mobility services domain.

Table D.3 – Use case classification of the deliver e-mobility services domain

Use case name	Operation risk level	Cybersecurity Risk level	Communication cost level	Timing expectation level	Frequency operation level
Reservation of an EVSE	High	Low	Low	Slow	Sometimes
Authorization with locally presented credentials	High	High	Medium	Fast	Often
Authorization by external means	High	High	Medium	Fast	Often
Inform EVU about tariff during charging session	High	Medium	Medium	Fast	Often
Inform EVU about tariff during operation	Low	Low	Low	Slow	Sometimes
SDR information production	High	High	Medium	Medium	Often
ISO 15118 contract certificate installation/update	High	High	Medium	Medium	Rare

Annex E
(informative)

Security use case sequence

Figure E.1 presents an example of sequence diagram implementing use cases related to cybersecurity. It gives an illustration of the order that security use cases should follow to ensure the security of the communication.

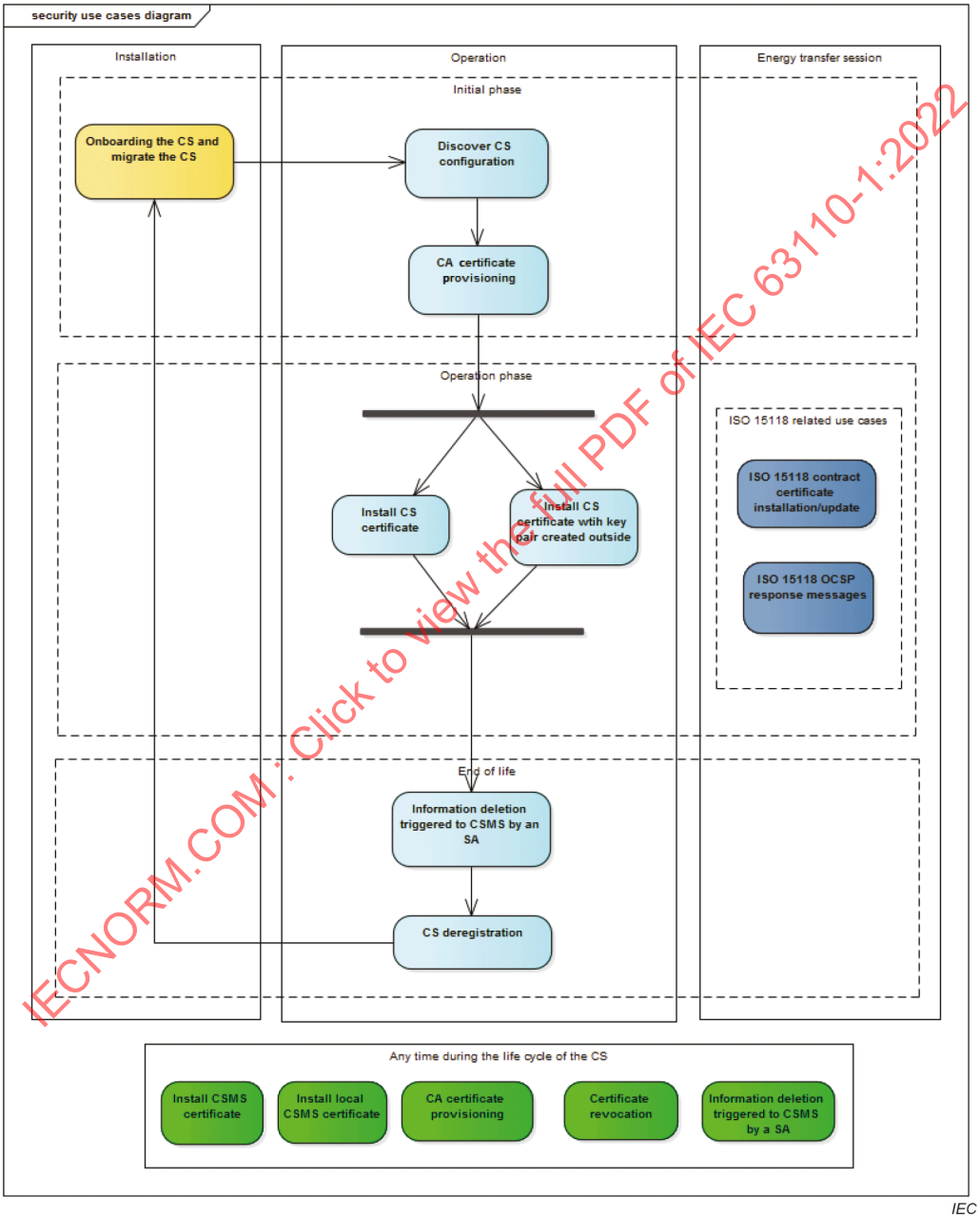


Figure E.1 – Security use case sequence

Bibliography

IEC 61850-7-420, *Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources and distribution automation logical nodes*

IEC TR 61850-80-3:2015, *Communication networks and systems for power utility automation – Part 80-3: Mapping to web protocols – Requirements and technical choices*

IEC 61851-1:2017, *Electric vehicle conductive charging system – Part 1: General requirements*

IEC 61851-23, *Electric vehicle conductive charging system – Part 23: DC electric vehicle charging station*

IEC 61851-23-1, *Electric vehicle conductive charging system – Part 23-1: DC electric vehicle charging station with an automated connection device* [2]

IEC 61851-25, *Electric vehicle conductive charging system – Part 25: DC EV supply equipment where protection relies on electrical separation*

IEC 61970 (all parts), *Energy management system application program interface (EMS-API)*

IEC 62559-2:2015, *Use case methodology – Part 2: Definition of the templates for use cases, actor list and requirements list*

IEC SRD 62913-2-4:2019, *Generic smart grid requirements – Part 2-4: Electric transportation related domain*

IEC 63119 (all parts), *Information exchange for electric vehicle charging roaming service*

ISO 15118-1:2019, *Road vehicles – Vehicle to grid communication interface – Part 1: General information and use-case definition*

ISO 15118-2, *Road vehicles – Vehicle to grid communication interface – Part 2: Network and application protocol requirements*

ISO 15118-20, *Road vehicles – Vehicle to grid communication interface – Part 20: 2nd generation network layer and application layer requirements*

EN 50491-12-1:2018, *General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Smart grid – Application specification – Interface and framework for customer – Part 12-1: Interface between the CEM and Home/Building Resource manager – General Requirements and Architecture*

CEN-CENELEC-ETSI, *Smart Grid Coordination Group, Smart Grid Reference Architecture. November 2012*

SG-CG/M490/E_Smart Grid Use Case Management Process, 2012

EURELECTRIC, *Active Distribution System Management. A key tool for the smooth integration of Distributed Generation*, 2013

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

OCPP 2.0.1 (2020-03-31), *Open Charge Point Protocol*, Open Charge Alliance, Arnhem, NL. Available at: https://www.openchargealliance.org/downloads/

INTERNET ENGINEERING TASK FORCE (IETF). RFC 4210: *Internet X.509 Public Key Infrastructure Certificate Management Protocol* [online]. C. Adams et al. September 2005 [viewed 2022-01-26]. Available at: https://www.ietf.org/rfc/rfc4210.txt

INTERNET ENGINEERING TASK FORCE (IETF). RFC 6961: *The Transport Layer Security (TLS) Multiple Certificate Status Request Extension* [online]. Y. Pettersen. June 2013 [viewed 2022-01-26]. Available at: https://www.ietf.org/rfc/rfc6961.txt

INTERNET ENGINEERING TASK FORCE (IETF). RFC 7292: *PKCS #12: Personal Information Exchange Syntax v1.1* [online]. K. Moriarty et al. July 2014 [viewed 2022-01-26]. Available at: https://www.ietf.org/rfc/rfc7292.txt

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

PROTOCOLE DE GESTION DES INFRASTRUCTURES DE CHARGE ET DE DÉCHARGE DES VÉHICULES ÉLECTRIQUES –

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

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 63110-1 a été établie par le comité d'études 69 de l'IEC: Véhicules électriques destinés à circuler sur la voie publique et chariots de manutention électriques. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
69/837/FDIS	69/843/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 63110, publiées sous le titre général *Protocole de gestion des infrastructures de charge et de décharge des véhicules électriques*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.

INTRODUCTION

Ces dernières années, la nécessité de réduire les émissions de gaz à effet de serre a conduit l'industrie automobile à développer des véhicules propulsés par l'énergie électrique. Parmi eux, le succès des véhicules équipés de batteries électriques rechargeables a marqué le début du déploiement des infrastructures de charge électrique.

Lors des premières années, les solutions de gestion des infrastructures de charge s'appuyaient sur des spécifications d'alliance industrielle ou des protocoles propriétaires. Elles ont dans une très large mesure contribué à la formation et à l'implication des premiers utilisateurs de véhicule électrique. Toutefois, avec le développement de masse de la mobilité électrique exigée par les dernières politiques énergétiques dans la plupart des pays, il s'avère nécessaire de normaliser le protocole de communication entre les infrastructures de charge et les opérateurs de bornes de charge afin d'établir un écosystème de mobilité électrique international, sûr, sécurisé, interopérable et convivial pour le réseau électrique.

Ce protocole normalisé s'avère avantageux pour tous les acteurs de l'environnement de mobilité électrique, notamment les fabricants de véhicules électriques, les fabricants de bornes de charge et les opérateurs de services de recharge, les prestataires de services de mobilité électrique, les opérateurs de réseau partiellement interconnecté, les gestionnaires de réseaux de distribution (GRD), les gestionnaires de réseaux de transport (GRT), les opérateurs de flexibilité (OF), les responsables d'équilibre et bien entendu les utilisateurs de véhicule électrique.

Une attention particulière est accordée à la sécurité et à la traçabilité des transactions par rapport à l'identification et au paiement, mais également aux réglementations relatives à la protection de la vie privée en vigueur dans de nombreux pays afin d'éviter l'utilisation malveillante ou criminelle de la borne de charge.

Les exigences générales et les définitions du présent document forment le cadre fondamental de toutes les descriptions de cas d'utilisation et des documents connexes de l’IEC 63110 (toutes les parties). Le présent document est le fruit d'un large consensus entre tous les acteurs de la mobilité électrique, et il convient de le considérer comme une ligne directrice destinée aux personnes chargées de la mise en œuvre de l'IEC 63110 (toutes les parties).

Les spécifications techniques et les exigences du protocole défini dans l’IEC 63110 seront définies dans une future partie de l’IEC 63110.

PROTOCOLE DE GESTION DES INFRASTRUCTURES DE CHARGE ET DE DÉCHARGE DES VÉHICULES ÉLECTRIQUES –

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

1 Domaine d'application

La présente partie de l'IEC 63110, qui sert de base aux autres parties de l'IEC 63110, couvre les définitions, cas d'utilisation et architectures pour la gestion des infrastructures de charge et de décharge des véhicules électriques.

Elle porte sur les exigences générales relatives à la mise en place d'un écosystème de mobilité électrique et couvre donc les flux de communication entre les différents acteurs de mobilité électrique, ainsi que les flux de données avec le système d'alimentation électrique.

Le présent document couvre les caractéristiques suivantes:

– la gestion du transfert d'énergie (session de charge, par exemple), la consignation, y compris les échanges d'informations relatives à l'énergie exigée, l'utilisation du réseau électrique, les données contractuelles et les données de comptage;

– la gestion des actifs du SAVE, y compris le contrôle, la surveillance, la maintenance, l'approvisionnement, la mise à jour du micrologiciel et la configuration (profils) du SAVE;

– l'authentification/l'autorisation/le paiement des sessions de charge et de décharge, y compris les informations d'itinérance, de tarification et de comptage;

– la fourniture d'autres services de mobilité électrique;

– la cybersécurité.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 15118 (toutes les parties), *Véhicules routiers — Interface de communication entre véhicule et réseau électrique*

INTERNET ENGINEERING TASK FORCE (IETF). RFC 6960: *Infrastructure de clé publique Internet X.509 : protocole d'état de certificat en ligne – OCSP* [en ligne]. S. Santesson et al. juin 2013 [consulté le 2022-01-26]. Disponible à l'adresse: https://www.ietf.org/rfc/rfc6960.txt

3 Termes, définitions et termes abrégés

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1 Termes et définitions

3.1.1
acteur
entité qui communique et interagit

Note 1 à l'article: Ces acteurs peuvent inclure les personnes, applications logicielles, systèmes, bases de données, voire le système d'alimentation lui-même.

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

3.1.2
responsable d'équilibre
BRP
partie qui dispose d'un contrat qui assure la sécurité financière et qui identifie la responsabilité d'équilibre avec le responsable du règlement des déséquilibres de la zone d'équilibre du marché habilitant la partie à opérer sur le marché

Note 1 à l'article: L'abréviation "BRP" est dérivée du terme anglais développé correspondant "balance responsible party".

3.1.3
cas d'utilisation professionnelle
description de la manière dont les rôles métier interagissent pour exécuter un processus métier

Note 1 à l'article: Ces processus sont déduits des services, c'est-à-dire des transactions métier, qui ont déjà été identifiés.

3.1.4
gestionnaire d'énergie client
CEM
fonction d'automatisation interne dédiée à l'optimisation de la consommation et/ou de la production d'énergie dans les locaux selon les préférences du client faisant usage des marges de manœuvre internes et généralement fondée sur des informations externes obtenues par l'intermédiaire du Point de connexion au réseau intelligent et éventuellement d'autres sources de données

Note 1 à l'article: Le gestionnaire d'énergie client fournit les services prévus tout en satisfaisant aux termes du contrat avec le fournisseur d'électricité, le GRD, l'OF ou d'autres opérateurs système.

Note 2 à l'article: L'abréviation "CEM" est dérivée du terme anglais développé correspondant "customer energy manager".

3.1.5
prestataire de service de charge
CSP
rôle qui ne fait pas fonctionner le SAVE, mais qui gère et authentifie les justificatifs d'identité et fournit des services de charge et d'autres services à valeur ajoutée aux utilisateurs de véhicule électrique

Note 1 à l'article: L'abréviation "CSP" est dérivée du terme anglais développé correspondant "charging service provider".

3.1.6
site de charge
CSI
zone géographique qui englobe une ou plusieurs CS

Note 1 à l'article: Il s'agit d'un concept physique.

Note 2 à l'article: L'abréviation "CSI" est dérivée du terme anglais développé correspondant "charging site".

3.1.7
zone du site de charge
CSZ
concept de gestion qui représente un groupe d'une ou de plusieurs bornes de charge sur un site de charge particulier

Note 1 à l'article: Le domaine d'application de la gestion de l'énergie d'un GR est défini par le CSMS dans le contexte d'une zone du site de charge.

Note 2 à l'article: Il s'agit d'un concept logique.

Note 3 à l'article: L'abréviation "CSZ" est dérivée du terme anglais développé correspondant "charging site zone".

3.1.8
système de gestion de borne de charge
CSMS
système responsable de la gestion des infrastructures de charge

Note 1 à l'article: Le CSMS peut être équipé d'instances CSMS et/ou CSMS en nuage locales pour mettre en œuvre le système. Voir la description du système en 4.4.

Note 2 à l'article: Il s'agit d'un concept logique.

Note 3 à l'article: L'abréviation "CSMS" est dérivée du terme anglais développé correspondant "charging station management system".

3.1.9
opérateur de service de charge
OSR
partie responsable de l'approvisionnement et du fonctionnement d'une infrastructure de charge (y compris des sites de charge) et de la gestion de l'électricité afin de fournir les services de transfert d'énergie demandés

3.1.10
borne de charge
CS
équipement physique composé d'un ou de plusieurs CSC et d'un ou de plusieurs SAVE qui gèrent le transfert d'énergie depuis et vers les VE

Note 1 à l'article: L'abréviation "CS" est dérivée du terme anglais développé correspondant "charging station".

3.1.11
contrôleur de charge
CSC
sous-système de CS responsable de la gestion d'un ou de plusieurs SAVE

Note 1 à l'article: Le protocole entre le CSC et le SAVE ne relève pas du domaine d'application de l'IEC 63110 (toutes les parties).

Note 2 à l'article: L'abréviation "CSC" est dérivée du terme anglais développé correspondant "charging station controller".

3.1.12
fabricant de borne de charge
CSM
partie responsable de la fabrication de la borne de charge qui fournit les mises à jour et mises à niveau logicielles du matériel et le support de diagnostic à l'OSR

Note 1 à l'article: L'abréviation "CSM" est dérivée du terme anglais développé correspondant "charging station manufacturer"

3.1.13
CSMS en nuage
instance du CSMS déployée physiquement en un lieu distant du site de charge

Note 1 à l'article: Le CSMS en nuage ne doit pas garantir le même niveau de fiabilité et de latence de communication que celui prévu à partir d'un CSMS local.

Note 2 à l'article: Il s'agit d'un concept physique.

3.1.14 Contraintes

3.1.14.1
contraintes de puissance
plage des limites supérieure et inférieure pour les valeurs de puissance extrêmes dans une période donnée

3.1.14.2
contraintes d'énergie
plage des limites supérieure et inférieure pour la puissance moyenne dans une période donnée

3.1.15
gestionnaire de réseau de distribution
GRD
entité responsable de la planification, du fonctionnement, de la maintenance et du développement dans des zones données du réseau de distribution d'électricité

Note 1 à l'article: Les zones données du réseau de distribution d'électricité peuvent être la basse tension, la moyenne tension et éventuellement haute tension.

Note 2 à l'article: Le GRD fournit la qualité de l'alimentation électrique (livraison de puissance, tension, etc.) et l'accès du client au marché fournisseur d'électricité par l'intermédiaire de son réseau dans des conditions réglementées

Note 3 à l'article: Cette définition a été adaptée sur la base de celle du Tableau 3 de l'IEC SRD 62913-2-4:2019.

3.1.16
chambre de compensation de mobilité électrique
EMOCH
entité qui intervient entre deux partenaires de compensation pour fournir des services de validation pour l'itinérance concernant les contrats de différents PSME

Note 1 à l'article: L'abréviation "EMOCH" est dérivée du terme anglais développé correspondant "e-mobility clearing house".

3.1.17
besoins de mobilité électrique
besoins de mobilité électrique exprimés par l'utilisateur d'un VE en termes d'heure de départ, de demande d'énergie minimale et maximale et d'objectif de demande d'énergie ou d'objectif d'état de charge minimal et maximal

[SOURCE: ISO 15118-1:2019, 3.1.25, modifié – L'expression "ou d'objectif d'état de charge minimal et maximal" a été ajoutée à la définition.]

3.1.18
prestataire de services de mobilité électrique
PSME
partie chargée de fournir un service à forte valeur ajoutée lié à l'utilisation d'un véhicule électrique

Note 1 à l'article: Des exemples de service sont la location d'un véhicule électrique, la réservation d'un service de stationnement, les services de navigation et les services énergétiques qui incluent le fournisseur de borne de charge en relation avec l'OSR.

Note 2 à l'article: Cette définition a été adaptée sur la base de celle du Tableau 3 de l'IEC SRD 62913-2-4:2019.

3.1.19
dispositif de communication de véhicule électrique
EVCC
système intégré au véhicule qui établit la communication entre le véhicule et le SECC afin de prendre en charge des fonctions spécifiques

Note 1 à l'article: L'abréviation "EVCC" est dérivée du terme anglais développé correspondant "electric vehicle communication controller".

[SOURCE: ISO 15118-1:2019, 3.1.31, modifié – La Note 1 à l'article a été supprimée.]

3.1.20
système d'alimentation pour véhicule électrique
SAVE
équipement ou ensemble d'équipements qui assure des fonctions réservées à l'alimentation en énergie électrique à partir d'une installation électrique fixe ou d'un réseau d'alimentation jusqu'au VE pour les besoins de la charge et de la décharge

[SOURCE: IEC 61851-1:2017, 3.1.1, modifié – Les mots "et de la décharge" ont été ajoutés à la définition, et les exemples ont été supprimés.]

3.1.21
utilisateur de véhicule électrique
UVE
personne ou entité légale qui utilise le véhicule et donne des informations relatives à ses besoins

Note 1 à l'article: Cette définition a été adaptée sur la base de celle du Tableau 3 de l'IEC SRD 62913-2-4:2019.

3.1.22
fournisseur d'électricité
FE
entité dont l'activité consiste à acheter de l'électricité en gros et à la revendre directement au client dans le cadre d'un contrat

Note 1 à l'article: Le fournisseur d'électricité peut également proposer des services énergétiques.

Note 2 à l'article: Le fournisseur d'électricité peut générer des marges en modulant les prix de l'électricité (durée d'utilisation, prix de pointe critique, etc.), et ces marges peuvent avoir une valeur sur les marchés de l'énergie et/ou pour l'exploitation du réseau.

3.1.23
identifiant d'authentification de mobilité électrique
EMAID
identifiant utilisé pour l'identification du détenteur du contrat

Note 1 à l'article: L'abréviation "EMAID" est dérivée du terme anglais développé correspondant "e-mobility authentication identifier''.

3.1.24
plan de transfert d'énergie
ETP
prévision de futures activités de transfert d'énergie avec les incertitudes, options de flexibilité et limites dans le temps associées

Note 1 à l'article: Le plan de transfert d'énergie peut prendre en charge toutes les techniques de charge différentes (programme et modes dynamiques définis dans l'ISO 15118, CHAdeMO, etc.).

Note 2 à l'article: L'abréviation "ETP" est dérivée du terme anglais développé correspondant "energy transfer plan''.

3.1.25
flexibilité
élasticité de l'utilisation des ressources (demande, stockage, génération) de modification de la consommation et/ou de génération d'énergie/puissance, à un niveau individuel ou agrégé, en réaction à un signal externe (signal ou demande de prix) afin de fournir un service à l'intérieur du système énergétique

Note 1 à l'article: Cette définition est fondée sur EURELECTRIC, Active Distribution System Management [voir la Bibliographie].

3.1.26
opérateur de flexibilité
OF
partie responsable d'au moins un service comme l'agrégation de la flexibilité de la charge provenant de différents utilisateurs des réseaux électriques basse tension et/ou moyenne tension et l'échange avec d'autres parties telles que le gestionnaire de réseau de transport et/ou le GRD pour fournir des services auxiliaires (mécanisme d'ajustement), ou d'autres marchés de flexibilité (futurs) éventuels, par exemple, optimisation de la facturation des réseaux d'équilibre

Note 1 à l'article: Il peut assurer la charge du véhicule électrique par l'intermédiaire des OSR et commercialiser ses services à d'autres parties.

3.1.27
bloc fonctionnel
FB
représentation logique d'un composant qui contient des informations relatives aux entrées, aux sorties, aux processus, aux exigences, aux fonctions et aux séquences fonctionnelles d'une fonctionnalité donnée

Note 1 à l'article: L'abréviation "FB" est dérivée du terme anglais développé correspondant "functional block''.

3.1.28
limite de puissance dure
HPL
puissance maximale admissible d'une borne de charge due à la conception physique

Note 1 à l'article: L'abréviation "HPL" est dérivée du terme anglais développé correspondant "hard power limit''.

3.1.29
CSMS local
instance du CSMS déployée physiquement en un site de charge spécifique

Note 1 à l'article: Il s'agit d'un concept physique.

3.1.30
limite de puissance
valeur de puissance qui ne peut pas être dépassée

3.1.31
plage de puissance
zone de fonctionnement entre une limite de puissance supérieure et une limite de puissance inférieure

Note 1 à l'article: Les limites de la plage de puissance sont inscrites par le gestionnaire de ressources dans le cadre des contraintes de puissance supérieure et inférieure du CSMS.

Note 2 à l'article: Ces limites sont fondées sur la puissance totale attribuée par le CEM à la CSZ.

Note 3 à l'article: Il convient, par conception, que les limites de puissance se situent toujours dans la plage des HPL de la CSZ.

3.1.32
enveloppe de plages de puissance
PRE
série consécutive de plages de puissance dans la durée

Note 1 à l'article: L'abréviation "PRE" est dérivée du terme anglais développé correspondant "power range envelope''.

3.1.33
protocole de vérification de certificat en ligne
OCSP
protocole de communication utilisé pour déterminer l'état actuel d'un certificat numérique sans exiger des listes de révocation de certificats, telles qu'elles sont définies dans le document RFC 6960

Note 1 à l'article: L'abréviation "OCSP" est dérivée du terme anglais développé correspondant "online certificate status protocol''.

3.1.34
acteur primaire
entité impliquée directement dans le processus IEC 63110

3.1.35
réseau privé
PN
réseau d'électricité (domestique, bâtiment, usine, etc.) en aval d'un point de connexion au réseau intelligent (SGCP)

Note 1 à l'article: Il est géré par l'opérateur de réseau privé, qui assume pleinement leurs responsabilités et la couverture.

Note 2 à l'article: L'abréviation "PN" est dérivée du terme anglais développé correspondant "private network''.

3.1.36
gestionnaire de réseau privé
PNO
partie chargée de gérer l'énergie dans les locaux

Note 1 à l'article: Le PNO peut avoir un contrat avec le GRD et d'autres acteurs du secteur de l'énergie.

Note 2 à l'article: L'abréviation "PNO" est dérivée du terme anglais développé correspondant "private network operator''.

3.1.37
gestionnaire des ressources
GR
composant logique (généralement mis en œuvre dans un logiciel) qui représente exclusivement la flexibilité énergétique d'un groupe de dispositifs ou d'un seul dispositif intelligent vis-à-vis du gestionnaire d'énergie du client des bâtiments et qui est responsable de l'envoi d'instructions connexes à ce groupe de dispositifs ou à ce dispositif unique, en utilisant généralement un protocole spécifique au dispositif

Note 1 à l'article: Dans le contexte du présent document, le gestionnaire des ressources gère la flexibilité énergétique d'une CSZ.

3.1.38
acteur secondaire
SA
entité impliquée indirectement dans l'échange d'informations IEC 63110

Note 1 à l'article: Les acteurs secondaires peuvent échanger des informations entre eux

Note 2 à l'article: Les acteurs secondaires peuvent également être une seule entité.

Note 3 à l'article: L'abréviation "SA" est dérivée du terme anglais développé correspondant "secondary actor''.

3.1.39
relevé de service détaillé
RSD
module de données qui contient toutes les informations nécessaires dans le cadre d'une identification unique nécessaire à la facturation ou l'information d'une/relative à une session de service d'un client particulier

3.1.40 Session

3.1.40.1
session d'autorisation
ensemble de toutes transactions d'autorisation

Note 1 à l'article: Les données sont collectées dans le relevé de service détaillé (RSD).

3.1.40.2
session de transfert d'énergie
ensemble de toutes les transactions de transfert d'énergie

Note 1 à l'article: Les données sont collectées dans le relevé de service détaillé (RSD).

3.1.40.3
autre session
ensemble de toutes les autres transactions supplémentaires éventuellement facturables

Note 1 à l'article: Les données sont collectées dans le relevé de service détaillé (RSD).

3.1.40.4
session de stationnement
ensemble de toutes transactions de stationnement

Note 1 à l'article: Les données sont collectées dans le relevé de service détaillé (RSD).

3.1.40.5
session de réservation
ensemble de toutes transactions de réservation

Note 1 à l'article: Les données sont collectées dans le relevé de service détaillé (RSD).

3.1.40.6
session de service
ensemble de toutes transactions facturables d'un utilisateur à un instant donné

Note 1 à l'article: Les données sont collectées dans le relevé de service détaillé (RSD).

Note 2 à l'article: La session de service peut également représenter une durée au cours de laquelle un service a été fourni. Dans ce cas, une session de service commence lorsque la première transaction facturable commence, et s'achève à la fin de la dernière transaction facturable.

3.1.41 Transaction

3.1.41.1
transaction d'autorisation
événement lié au processus d'autorisation

EXEMPLE Le fait d'autoriser le VE à charger constitue une transaction d'autorisation particulière.

Note 1 à l'article: L'autorisation est donnée par le SA, par exemple: PSME.

Note 2 à l'article: L'autorisation permet d'utiliser un SAVE particulier et en général en public, une CS est nécessaire pour le début de la session de transfert d'énergie.

Note 3 à l'article: Une autorisation négative est également une transaction d'autorisation.

3.1.41.2
transaction de transfert d'énergie
événement lié au processus de transfert d'énergie

EXEMPLE 1 Le début du transfert d'énergie est une transaction de transfert d'énergie particulière.

EXEMPLE 2 La modification de la puissance maximale allouée à un SAVE est une transaction de transfert d'énergie particulière.

3.1.41.3
autre transaction
événement lié à un service supplémentaire

Note 1 à l'article: Un voiturier, un lavage ou tout autre service non nécessairement lié à la mobilité électrique sont des exemples de services supplémentaires.

3.1.41.4
transaction de stationnement
événement lié à un service de stationnement

EXEMPLE Début ou fin des frais de stationnement.

3.1.41.5
transaction de réservation
événement lié à un processus de réservation

EXEMPLE 1 La signature d'un contrat de réservation est généralement la première transaction de réservation.

EXEMPLE 2 La modification du contrat, telle que la modification de l'heure de départ, est une transaction de réservation.

3.1.42
contrôleur de communication de l'infrastructure de recharge
SECC
entité qui établit la communication avec un ou plusieurs EVCC et qui peut être en mesure d'interagir avec des acteurs secondaires

Note 1 à l'article: L'abréviation "SECC" est dérivée du terme anglais développé correspondant "supply equipment communication controller''.

[SOURCE: ISO 15118-1:2019, 3.1.68, modifié – Les Notes à l'article ont été supprimées.]

3.1.43
charge intelligente
SC
processus de transfert d'énergie contrôlé, dont les objectifs consistent à optimiser les besoins de mobilité électrique du client, les tarifs, ainsi que les contraintes de puissance du CSMS et du réseau électrique

Note 1 à l'article: L'abréviation "SC" est dérivée du terme anglais développé correspondant "smart charging".

3.1.44
point de connexion au réseau intelligent
SGCP
limite entre la zone du réseau électrique et les marchés vers le client (ménages, bâtiment, industrie, par exemple)

Note 1 à l'article: L'abréviation "SGCP" est dérivée du terme anglais développé correspondant "smart grid connection point".

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

3.1.45
heure de départ
ToD
heure que l'utilisateur a indiqué à laquelle le VE se déconnecte du SAVE et par la suite à laquelle l'utilisateur est réputé quitter l'emplacement de stationnement

Note 1 à l'article: Ces informations font partie des besoins de mobilité électrique.

Note 2 à l'article: Ces informations sont utilisées par le CSMS pour prévoir l'ETP.

Note 3 à l'article: L'abréviation "ToD" est dérivée du terme anglais développé correspondant "time of departure''.

3.1.46
gestionnaire de réseau de transport
GRT
entité chargée de transporter l'énergie sous forme de courant électrique au niveau national ou régional, au moyen d'infrastructures fixes

3.2 Termes abrégés

AETP aggregated energy transfer plan (plan de transfert d'énergie agrégé)
BRP balance responsible party (responsable d'équilibre)
CEM customer energy manager (gestionnaire d'énergie client)
CS charging station (borne de charge)
CSC charging station controller (contrôleur de borne de charge)
CSMS charging station management system (système de gestion de borne de charge)
OSR opérateur de service de recharge
CSP charge service provider (prestataire de service de charge)
CSZ charging station zone (zone du site de charge)
GRD gestionnaire de réseau de distribution
EMAID e-mobility authentication identifier (identifiant d'authentification de mobilité électrique)
PSME prestataire de services de mobilité électrique
ETP energy transfer plan (plan de transfert d'énergie)
SAVE système d'alimentation pour véhicule électrique

UVE	utilisateur de véhicule électrique
OF	opérateur de flexibilité
OCSP	online certificate status protocol (protocole de vérification de certificat en ligne)
PRE	power range envelope (enveloppe de plages de puissance)
GR	gestionnaire des ressources
SA	secondary actors (acteurs secondaires)
RSD	relevé de service détaillé
SGCP	smart grid connection point (point de connexion au réseau intelligent)
TOD	time of departure (heure de départ)
GRT	gestionnaire de réseau de transport

4 Acteurs et modèle d'architecture

4.1 Acteurs

Il existe trois acteurs primaires qui peuvent déclencher un processus d'échange de données dans le concept de communication de données IEC 63110. La Figure 1 présente leurs interactions.

Un VE ou un utilisateur peut déclencher l'échange de données entre le CSC et le CSMS (lors du branchement ou lors de la demande d'autorisation de charge, par exemple).

Les acteurs primaires impliqués directement dans le processus IEC 63110 sont le CSC, le CSMS et le RM.

Les acteurs secondaires peuvent déclencher l'échange de données avec le CSMS (le gestionnaire de réseau, le fournisseur de service, le PSME,... par exemple). Voir 5.3 pour une liste des acteurs primaires et secondaires.

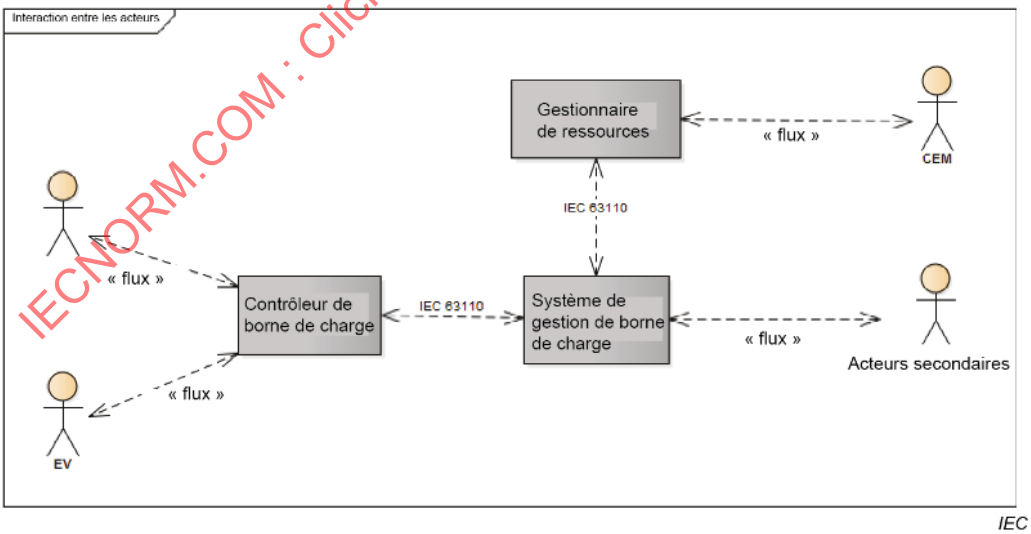


Figure 1 – Interactions entre les acteurs

Le modèle d'architecture représenté à la Figure 2 donne une vue plus détaillée des sous-composants pour le CSC et le CSMS.

4.2 Modèle d'architecture

Un modèle d'architecture est une représentation graphique des composants logiques, des interfaces et de leurs niveaux d'agrégation.

Un modèle d'architecture ne représente pas la mise en œuvre physique, mais il présente les interfaces du point de vue de la communication de données, et la manière dont les composants logiques sont organisés du point de vue d'une agrégation.

Le modèle d'architecture repose sur le modèle de référence du modèle architectural du réseau intelligent, et la Figure 2 est la couche de composant. SG-CG/M490/E [voir la bibliographie] donne des informations plus détaillées sur le modèle architectural du réseau intelligent.

Le présent document porte principalement sur les protocoles de communication de données, les interfaces et l'échange d'informations entre le contrôleur de borne de charge et le système de gestion de borne de charge.

D'autres interfaces sont également définies dans le modèle d'architecture, mais elles sont spécifiées par d'autres normes et sont utilisées en référence selon la dernière version officielle du document normatif.

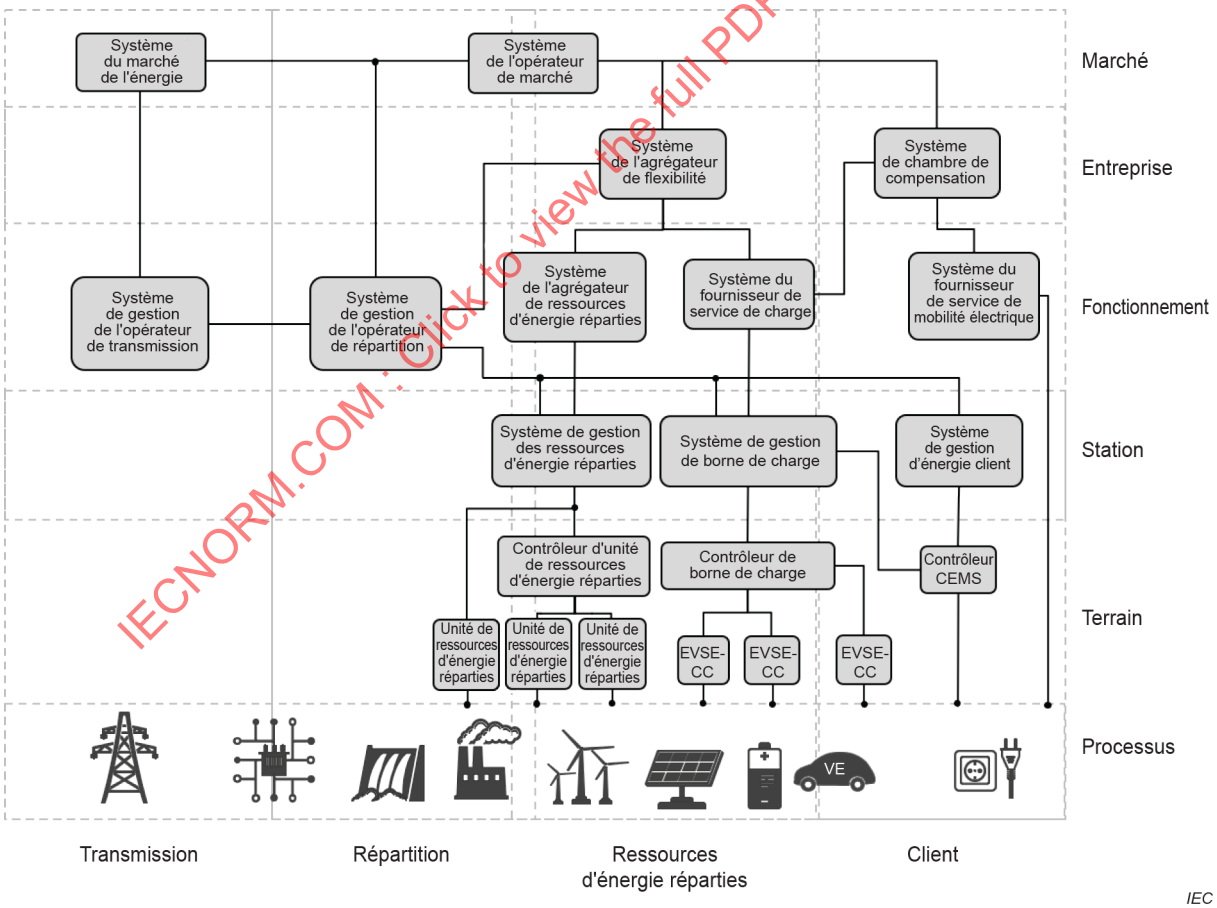


Figure 2 – Modèle d'architecture de la couche de composant

4.3 Métamodèle IEC 63110

Le métamodèle utilisé pour l'IEC 63110 comporte trois niveaux tels qu'ils sont représentés à la Figure 3: niveau du composant, niveau de la propriété et niveau DataType.

Le niveau supérieur est celui du composant. Il modélise les composants du monde physique (les contrôleurs, les commutateurs et les sorties, par exemple). Un composant peut inclure d'autres composants (une borne de charge inclut un ou plusieurs SAVE, par exemple).

Le deuxième niveau est celui de la propriété du composant. Il indique la propriété d'un composant (un nom, un type, un intervalle de temps, par exemple).

Le troisième niveau est le niveau DataType. Il spécifie le type d'informations reflétées par les propriétés de composant. Trois types de DataType sont possibles:

– SimpleDataType sont les types de données les plus fondamentales disponibles dans le modèle (des valeurs de chaînes, entières, booléennes ou à virgule flottante, par exemple). De même, des types de données comme la date et l'heure relèvent également de cette variante.
– EnumeratedDataType reflète les valeurs identifiées par des noms. Par exemple, au lieu d'utiliser les valeurs numériques 0 et 1 pour indiquer si un commutateur est ouvert ou fermé, un type de données énumérées nommé PositionKind peut être utilisé, comportant les valeurs énumérées Closed=0, Open=1, et donc Closed (fermé) et Open (ouvert) peut ainsi être utilisé en lieu et place de 0 et de 1.
– PropertySetTypes décrit des ensembles de propriétés associées couramment réutilisées ensemble. Par exemple:
  - pour refléter un intervalle de date, un type DateInterval (PropertySetType) peut être défini, avec deux propriétés – date de début et de fin de l'intervalle (par exemple, start:Date et end:Date);
  - pour refléter un mesurage de puissance active, un type ActivePower peut être défini, avec trois propriétés – valeur, unité et multiplicateur (par exemple; value:decimal, unit:string, multiplier:string).

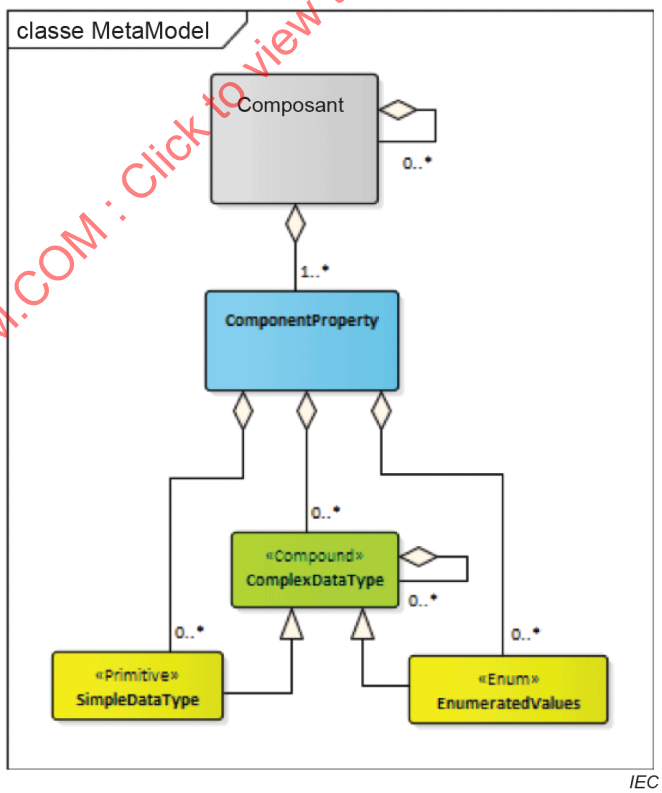


Figure 3 – Métamodèle IEC 63110

Un extrait de l'architecture de niveau supérieur est représenté à la Figure 4.

L'architecture reflète les principaux composants impliqués dans la charge d'un véhicule électrique. Pour l'ensemble de l'image du modèle d'objet de l'IEC 63110, voir le modèle UML de l'IEC 63110 et le document IEC 63110-1-1 connexe qui contient toutes les informations détaillées.

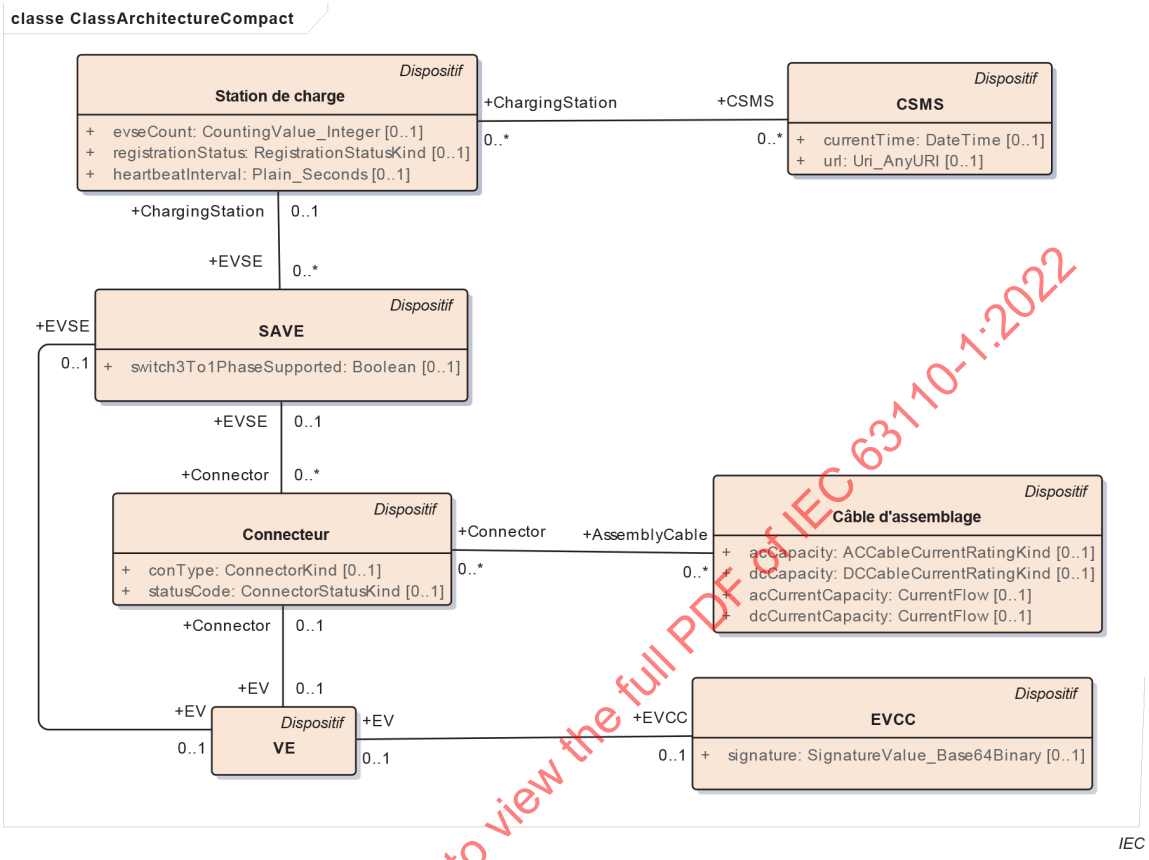


Figure 4 – Architecture de niveau supérieur IEC 63110

4.4 Vue des acteurs et du système

La Figure 5 représente les différents acteurs qui interagissent dans l'IEC 63110.

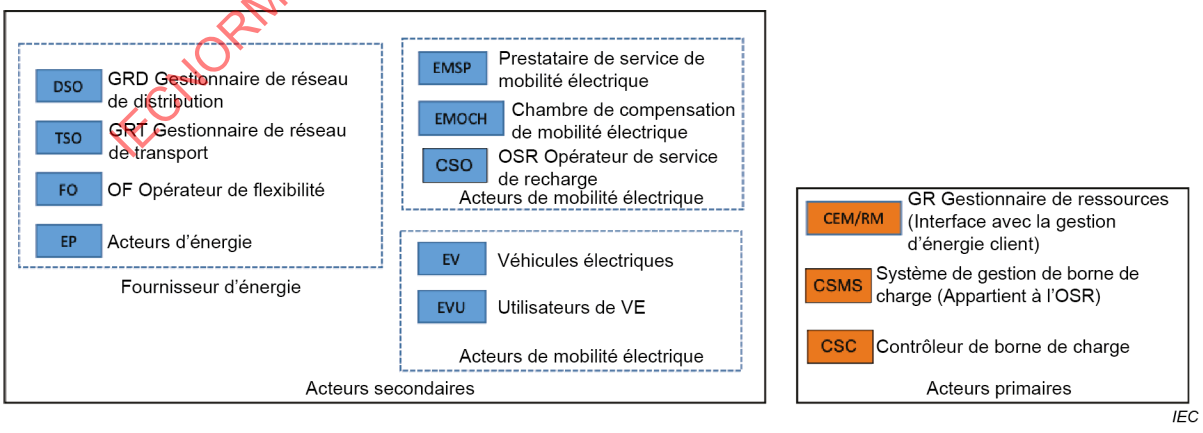


Figure 5 – Acteurs

Les acteurs échangent des messages par l'intermédiaire de systèmes qui mettent en œuvre des protocoles et des interfaces.

Le CSMS est le système spécifié et géré par l'OSR. Le CSMS commande et surveille les bornes de charge par l'intermédiaire d'une communication IEC 63110 avec le contrôleur de borne de charge. Le CSMS et le CSC contiennent des interfaces physiques de communication également compatibles avec l'IEC 63110. Les interfaces IEC 63110 connectent le CSMS au CSC et de manière facultative au GR. Le CSC comporte également d'autres interfaces de communication avec le SAVE à l'intérieur de la borne de charge. En présence d'un CEM, il convient que le CSMS puisse communiquer avec lui par l'intermédiaire du GR. L'OSR peut demander au CSMS local d'assurer cette communication.

Le CSMS (local ou en nuage) reçoit une PRE de la part du GR et attribue les ETP aux CS et à chaque SAVE sur le site de charge Cette attribution peut être calculée en local si un CSMS local est mis en œuvre.

Si la communication entre le CSMS en nuage et le CSMS local est interrompue, il convient que ce dernier soit en mesure de maintenir en local le fonctionnement des CS.

Une tâche du CS consiste à agréger, à commander et à surveiller un ou plusieurs SAVE. La sécurité et le contrôle en temps réel du transfert d'énergie relèvent du domaine d'application du SAVE, et il convient que le CS ne les contrôle pas directement. Une autre tâche du CS consiste à échanger des messages de gestion avec le CSMS.

La Figure 6 représente une vue générique d'une architecture de communication avec une borne de charge installée derrière un SGCP. Un système CEM facultatif est chargé d'optimiser la puissance et l'énergie à l'intérieur du SGCP. Le CEM est capable d'échanger des messages avec le CSMS (local ou en nuage) par l'intermédiaire du GR qui met en œuvre le protocole défini dans l'IEC 63110. Il comporte également des connexions qui ne relèvent pas du domaine d'application avec d'autres systèmes en local ou en fonction des acteurs secondaires. Tous les systèmes d'alimentation pour VE sont connectés au CS par l'intermédiaire de leur propre protocole de communication. Les UVE sont capables d'interagir sur le VE, les SAVE, l'OSR et le PSME par l'intermédiaire d'interfaces adaptées (affichage local ou applications distantes, par exemple). Un même SGCP peut comporter un plus grand nombre de CS contrôlés par un ou plusieurs CSMS locaux. Le ou les CSMS locaux facultatifs peuvent être situés dans différents dispositifs, y compris le CS.

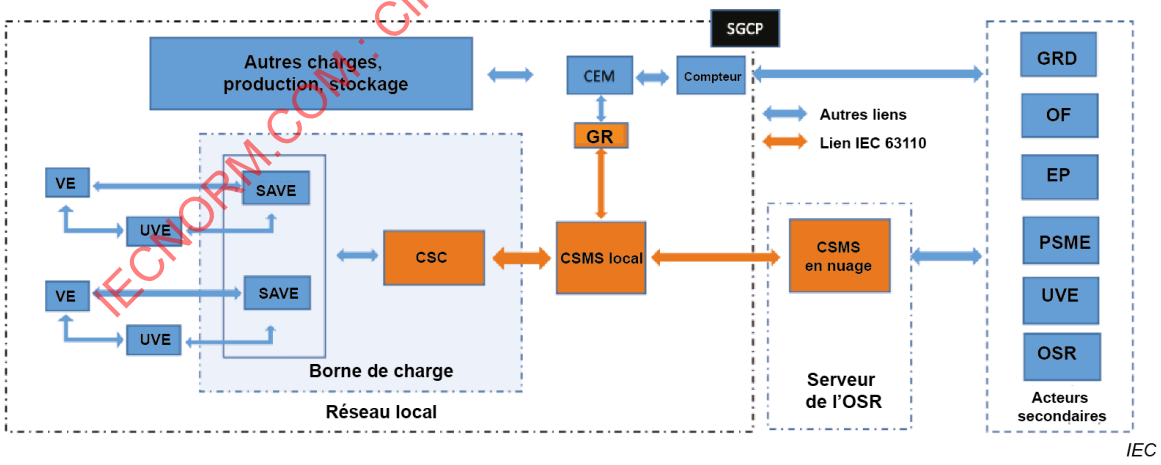


Figure 6 – Architecture de communication générique - vue générale

La Figure 7 représente une situation dans laquelle deux (voire plus) zones du site de charge (a et b) dans le même SGCP sont contrôlées par un CSMS (local ou en nuage). Le CEM est chargé d'optimiser la puissance et l'énergie dans le SGCP et pour chaque CSZ. Pour chaque CSZ, le CEM contrôle un gestionnaire des ressources (GR-a et GR-b) capable d'échanger des messages avec le CSMS (local ou en nuage) par l'intermédiaire du protocole défini dans l'IEC 63110.

NOTE Le gestionnaire de ressources (GR) fait référence au concept S2 décrit dans l'EN 50491-12-1. D'autres normes sont possibles à condition qu'elles offrent une interface avec le protocole défini dans l'IEC 63110.

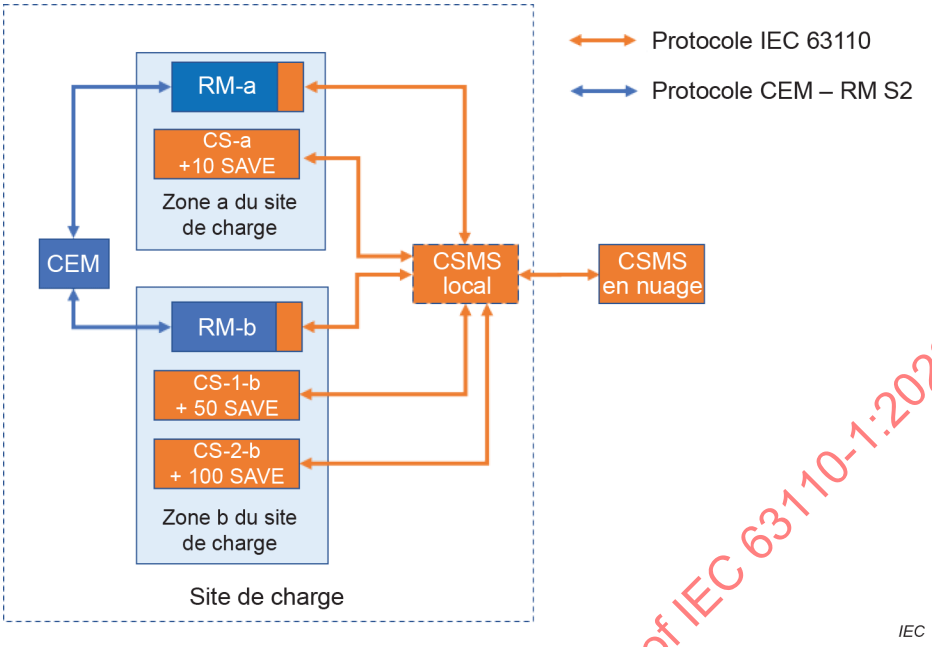


Figure 7 – Site de charges avec deux zones du site de charge contrôlées par un CSMS

NOTE Pour le CSMS, il n'est ni possible ni pertinent de comprendre comment le RM a calculé les informations sur les contraintes de puissance qu'il lui a fournies. L'existence d'un système complet d'automatisation des bâtiments (CEM) ne relève pas du domaine d'application du présent document.

4.5 Exemples de mise en œuvre

Dans la plupart des cas, l'architecture générique représentée à la Figure 6 peut être simplifiée ou adaptée en fonction de la situation. D'une part, dans les maisons, il est nécessaire d'avoir un CS dont les fonctions sont très simples. D'autre part, pour les installations volumineuses (les parcs de stationnement, par exemple), des systèmes complexes sont probablement chargés de la coordination de nombreux CS installés, par exemple, à des étages différents.

L'Annexe A donne des exemples de mise en œuvre à titre informatif. Ces exemples représentent des choix possibles de mise en œuvre donnés à titre d'illustration. Il est nécessaire de comprendre que les situations correspondantes peuvent être mises en œuvre de différentes manières.

5 Descriptions de rôles, des acteurs et des domaines

5.1 Généralités

Afin d'assurer des mises en œuvre interopérables entre les rôles métier et les rôles du système dans un environnement de mobilité électrique, il est nécessaire de décrire des cas d'utilisation exhaustifs en définissant leurs relations et interactions, en vue de satisfaire aux besoins du client final par des services adaptés.

5.2 Descriptions des types de cas d'utilisation

Il existe deux types de cas d'utilisation:

– les cas d'utilisation professionnelle décrivent la manière dont les rôles métier interagissent pour exécuter un processus métier. Ces processus sont déduits des services (des transactions métier, par exemple) qui ont déjà été identifiés;

– les cas d'utilisation de système décrivent la manière dont les rôles du système et/ou les rôles métier d'un système donné interagissent pour exécuter une fonction exigée pour activer/faciliter les processus métier décrits dans les cas d'utilisation professionnelle. Ils ont pour objet de détailler l'exécution de ces processus du point de vue d'un système d'informations.

Étant donné qu'une fonction peut être utilisée pour activer/faciliter plusieurs processus métier, un cas d'utilisation de système peut être associé à plusieurs cas d'utilisation professionnelle.

5.3 Description des rôles métier

Le Tableau 1 répertorie les rôles métier qui résultent d'une analyse métier du domaine de mobilité électrique. Les rôles sont communs à d'autres normes comme l'IEC SRD 62913-2-4, l'IEC 63119 et l'ISO 15118 (toutes les parties).

Tableau 1 – Rôles métiers du domaine de mobilité électrique

Acteurs		
Nom de l'acteur	**Type d'acteur**	**Rôle dans le présent document**
Opérateur de service de charge (OSR)	Rôle métier	Acteur primaire
Gestionnaire de réseau de distribution (GRD)	Rôle métier	Acteur secondaire
Prestataire de services de mobilité électrique (PSME)	Rôle métier	Acteur secondaire
Utilisateur du VE (UVE)	Rôle métier	Acteur secondaire
Opérateur de flexibilité (OF)	Rôle métier	Acteur secondaire

5.4 Description des acteurs du système

Le Tableau 2 répertorie les principaux acteurs du système du domaine de mobilité électrique.

Tableau 2 – Acteurs du système du domaine de mobilité électrique

Acteurs		
Nom de l'acteur	**Type d'acteur**	**Informations supplémentaires spécifiques au présent document**
CSMS	Rôle du système	Système principal d'échange de messages avec le CS
CS	Rôle du système	Système principal d'échange de messages avec le CSMS
GR	Rôle du système	Système principal d'échange de messages avec le CSMS
CEM	Rôle du système	Système secondaire d'échange de messages avec le CSMS par l'intermédiaire du GR
VE	Rôle du système	Système secondaire
SAVE	Rôle du système	Système secondaire
EVCC	Rôle du système	Système secondaire
SECC	Rôle du système	Système secondaire

5.5 Description du domaine

5.5.1 Généralités

Les domaines de cas d'utilisation IEC 63110 sont divisés en trois cas métier:

– offre de services de transfert d'énergie;
– offre de services de mobilité électrique;
– gestion de la CS.

Chacun de ces trois cas métier s'appuie sur des cas d'utilisation professionnelle qui décrivent des situations dans lesquelles les acteurs métier réalisent certains objectifs. Les trois domaines sont relativement indépendants, même s'ils peuvent échanger des informations.

5.5.2 Offre de services de transfert d'énergie

5.5.2.1 Généralités

Ce domaine métier décrit les relations entre les acteurs en mesure d'influencer le transfert d'énergie. Il contient les cas d'utilisation relatifs à la gestion du transfert d'énergie vers un ou plusieurs systèmes d'alimentation pour VE afin de charger ou de décharger la batterie des VE connectés physiquement. Les précédentes phases d'échange d'informations relatives à l'identification et à l'autorisation, etc. ont par hypothèse abouti.

Les acteurs secondaires suivants peuvent influencer le transfert d'énergie:

– le GRD;
– l'OF;
– le CEM;
– l'UVE;
– le VE;
– le SAVE;

Leurs influences sont décrites dans les cas d'utilisation correspondants ("Assurer la charge en réponse à une demande" ou "Négocier un plan de charge pour une charge intelligente", par exemple).

Les acteurs secondaires peuvent influencer le transfert d'énergie à condition d'avoir établi une connexion digne de confiance et sécurisée avec l'OSR ou le CSMS.

5.5.2.2 Influence du GRD

Le GRD est responsable de la qualité de l'alimentation en électricité (livraison de puissance, tension, etc.). Il peut lancer des opérations de délestage en cas d'urgence ou de congestion dans son réseau de distribution.

Selon les différents événements (contraintes du réseau électrique, réglementations locales, contrats, par exemple), le GRD peut demander au CSMS ou exiger qu'il applique des variations de puissance immédiates.

Les messages qui proviennent du GRD peuvent être envoyés aux différents acteurs par l'intermédiaire de communications sécurisées et dignes de confiance:

(GRD à OSR) ou (GRD à l'EMS au CSMS)

5.5.2.3 Influence de l'opérateur de flexibilité

L'OF est une partie qui agrège la flexibilité de la charge provenant de différentes parties qui utilisent le réseau électrique et l'échange avec le gestionnaire de réseau de transport et/ou le GRD pour fournir des services auxiliaires (mécanisme d'ajustement).

À l'inverse des opérations de délestage du GRD, qui sont une réponse à des problèmes techniques locaux, l'OF envoie des messages aux parties en fonction des règles du marché.

Les messages relatifs aux variations de puissance sont directement envoyés par l'intermédiaire d'interfaces de communication propriétaires aux systèmes des parties concernées. Dans le cas de la mobilité électrique, ils peuvent être envoyés à l'OSR ou directement à un VE particulier.

Si les messages sont envoyés à l'OSR, le CSMS les traite et transmet la variation de puissance au CSC.

Si l'OF a envoyé un message directement à un VE particulier, il est nécessaire que le CSC informe le CSMS des variations de puissance lorsque le CS détient les informations.

NOTE La communication entre le FO et le VE ne relève pas du domaine d'application du présent document.

Dans tous les cas, la preuve de service est assurée par l'enregistrement de la transaction de transfert d'énergie correspondante par le CSMS.

5.5.2.4 Influence du CEM

Le CEM est le système responsable de la gestion interne de la consommation et/ou production d'énergie à l'intérieur d'un site. En règle générale, le CEM exécute des algorithmes internes en fonction des contraintes. Le CEM peut être connecté au compteur principal, aux producteurs locaux, aux unités de stockage et aux consommateurs. Le CEM est capable d'échanger des messages sécurisés et dignes de confiance avec le CSMS (local ou en nuage) par l'intermédiaire du GR.

Au cours de son processus d'optimisation normal/de routine, le GR définit une PRE pour le CSMS, fondé sur les contraintes d'énergie et de puissance associées, ainsi que sur les demandes ou configurations du gestionnaire de l'énergie du bâtiment et le bilan énergétique actuel entre production et consommation dans la CSZ appropriée. Le CEM peut également optimiser la puissance par rapport à la stratégie tarifaire en fonction du marché qui peut influer sur les limites de puissance définies par le GR.

L'enveloppe de plages de puissance, qui se présente en général sous la forme de programmes de transfert d'énergie supérieur ou inférieur dans le temps, positifs ou négatifs, constitue la base de la génération de puissance par le CSMS des ETP à chaque VE en fonction des caractéristiques du SAVE, des besoins de mobilité électrique et des contrats avec les PSME.

5.5.2.5 Influence de l'UVE et du VE

Le VE et l'UVE peuvent influencer indirectement le transfert d'énergie par leurs messages, destinés par exemple au SAVE avec négociation ou renégociation ISO 15118 ou à l'OSR par l'intermédiaire de l'application PSME pour l'UVE. L'impact sur l'échange d'informations CS-CSMS dépend des informations spécifiques et est exprimé dans les cas d'utilisation décrits dans le présent document.

5.5.3 Offre de services de mobilité électrique

Ce domaine métier est lié à la gestion des services de mobilité électrique relatifs à l'identification et à l'autorisation de l'UVE, mais également à la réservation et à la production de RSD.

Les cas d'utilisation de ce domaine métier décrivent également les relations avec les acteurs secondaires de mobilité électrique (le PSME et les chambres de compensation, par exemple). Les interfaces d'itinérance nécessaires à la connexion au PSME de l'UVE sont décrites dans l'IEC 63119. Lors du processus d'autorisation, l'IEC 63110 est responsable de la collecte des justificatifs d'identité correspondants et les transmet en général au SA chargé de leur validation. Les cas d'utilisation de ce domaine sont très importants, car ils décrivent les interactions entre l'UVE et l'infrastructure de charge.

5.5.4 Gestion de la borne de charge

Ce domaine métier est lié à la gestion du CS.

Le domaine de gestion CS contient toutes les opérations traitées par l'OSR pour maintenir l'infrastructure de charge dans un état de fonctionnement optimal.

6 Événements, boucles et sessions

6.1 Généralités

L'OSR est responsable de la gestion d'une CS pendant sa durée de vie. Cela inclut les phases suivantes:

– installation physique;
– configuration initiale;
– mise en service;
– surveillance;
– maintenance-diagnostic;
– mise hors service;
– désinstallation physique.

Du point de vue d'un protocole, seules les phases après l'installation physique et avant la désinstallation physique relèvent du domaine d'application du présent document. Toutes ces phases ne sont pas indépendantes et suivent normalement un cycle de vie logique.

Dans le présent document, le cycle de vie d'une CS est décrit avec les phases suivantes:

– installation de la CS;
– fonctionnement de la CS;
– opérations de service.

L'installation de la CS fait référence à la première mise en service d'une CS sur le serveur de l'OSR, par exemple lors de l'installation d'une CS neuve ou de la migration d'une CS vers un nouvel opérateur. Sauf en cas de mises à niveau importantes du matériel ou de remplacement d'éléments essentiels, l'installation de la CS n'a généralement lieu qu'une seule fois dans la durée de vie d'une CS gérée par un OSR particulier.

Le fonctionnement de la CS fait référence à toutes les opérations liées à sa gestion par le CSMS. Par exemple, sa configuration en fonction de caractéristiques du CSMS ou des mises à jour et diagnostics du micrologiciel.

Les opérations de service font référence à toutes les opérations nécessaires à la gestion des interactions de l'UVE avec la CS (la réservation, l'identification, la négociation dans le cadre de plans de transfert d'énergie, les transferts d'énergie et la fermeture finale de la session de service, par exemple).

Les domaines de cas d'utilisation décrits en 5.5 se recoupent avec le cycle de vie. Par exemple, les cas d'utilisation des domaines de services de mobilité électrique et de services de transfert d'énergie appartiennent au cycle d'opérations de service. La plupart des cas d'utilisation des domaines de gestion de la borne de charge appartiennent au cycle de fonctionnement du CS.

Dès que le CS est correctement mis en service et configuré, la plus grande part de l'activité du CSMS a lieu pendant le cycle d'opérations de service. L'efficacité et la qualité de cette partie de l'activité du CSMS sont des éléments essentiels au succès du déploiement massif des millions de CS prévues dans les décennies à venir (voir 7.2 pour les exigences de protocole).

Les activités du cycle d'opérations de service concernent les interactions entre l'UVE ou le VE et la CS. Pour assurer un processus d'interaction sûr, efficace et fiable, le CSMS doit suivre toutes les activités susceptibles d'avoir un impact sur la relation avec l'UVE (les questions financières, techniques ou contractuelles, par exemple).

À cet effet, les concepts de sessions et de transactions sont présentés dans le présent document.

6.2 Description des sessions et des transactions

Comme cela est défini à l'Article 3, l'IEC 63110 utilise les concepts de sessions et de transactions. Dans l'IEC 63110, les sessions ne font pas référence aux sessions de communication, mais aux activités entre le moment auquel un UVE ou un VE entre dans le domaine d'application de l'IEC 63110 et le moment auquel le VE en sort. Les sessions et les transactions sont essentiellement utilisées pour identifier et suivre les services potentiellement facturables déclenchés lors du cycle d'opérations de service, combinés et consignés dans le RSD.

La session de service commence par la première transaction et se termine à la fin de la dernière transaction. En fonction de la situation, la session de service peut contenir plusieurs transactions qui appartiennent à différents types de sessions comme l'autorisation, la réservation, le stationnement, le transfert d'énergie, etc. Certaines transactions au cours d'une session de service peuvent ne pas être déclenchées, bien que les transactions de transfert d'énergie se produisent dans la plupart des sessions de service. Voir les définitions à l'Article 3.

La Figure 8 représente une session de service avec des sessions d'autorisation, de stationnement et de transfert d'énergie.

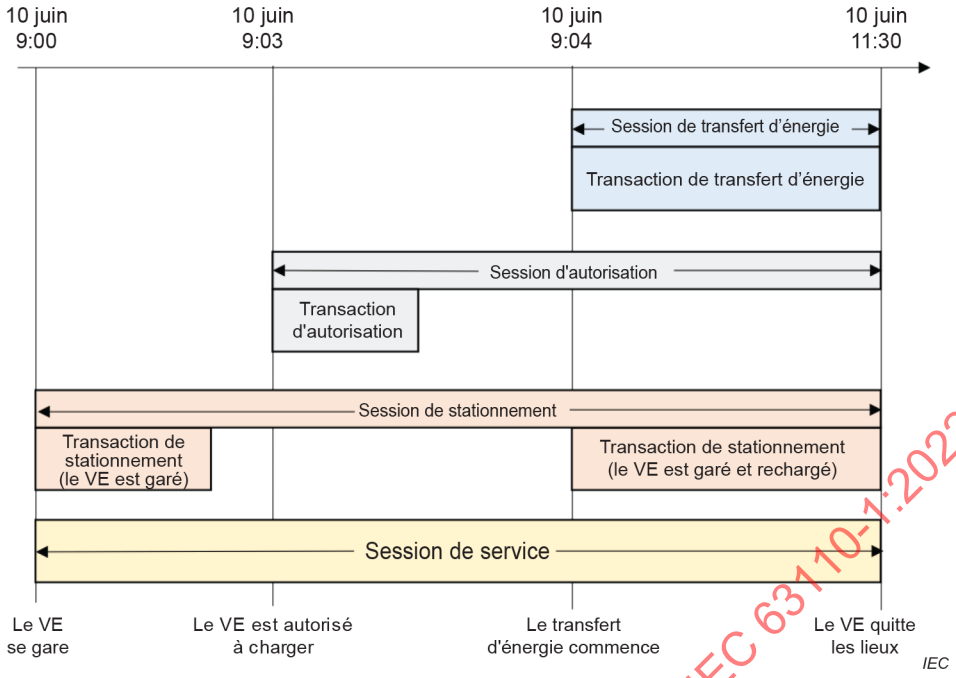


Figure 8 – Exemple de session de service

La session de service commence à 9:00, lorsque le VE est garé, ce qui déclenche une transaction de stationnement. Ensuite, à 9:03, par exemple après que l'utilisateur a branché le véhicule, le VE est autorisé à charger dans le cadre d'une transaction d'autorisation. À 9:04, la session de transfert d'énergie commence et dure jusqu'à 11:30, heure à laquelle le VE quitte les lieux, ce qui met fin aux sessions de stationnement, d'autorisation et de transfert d'énergie.

Toutes les sessions contiennent des transactions associées qui sont consignées par le CSMS ou l'OSR. Certaines d'entre elles sont ajoutées par l'OSR dans le RSD.

Le CSMS maintient plusieurs sessions de service en parallèle correspondant à chaque VE engagé dans une session de service, comme cela est représenté à la Figure 9.

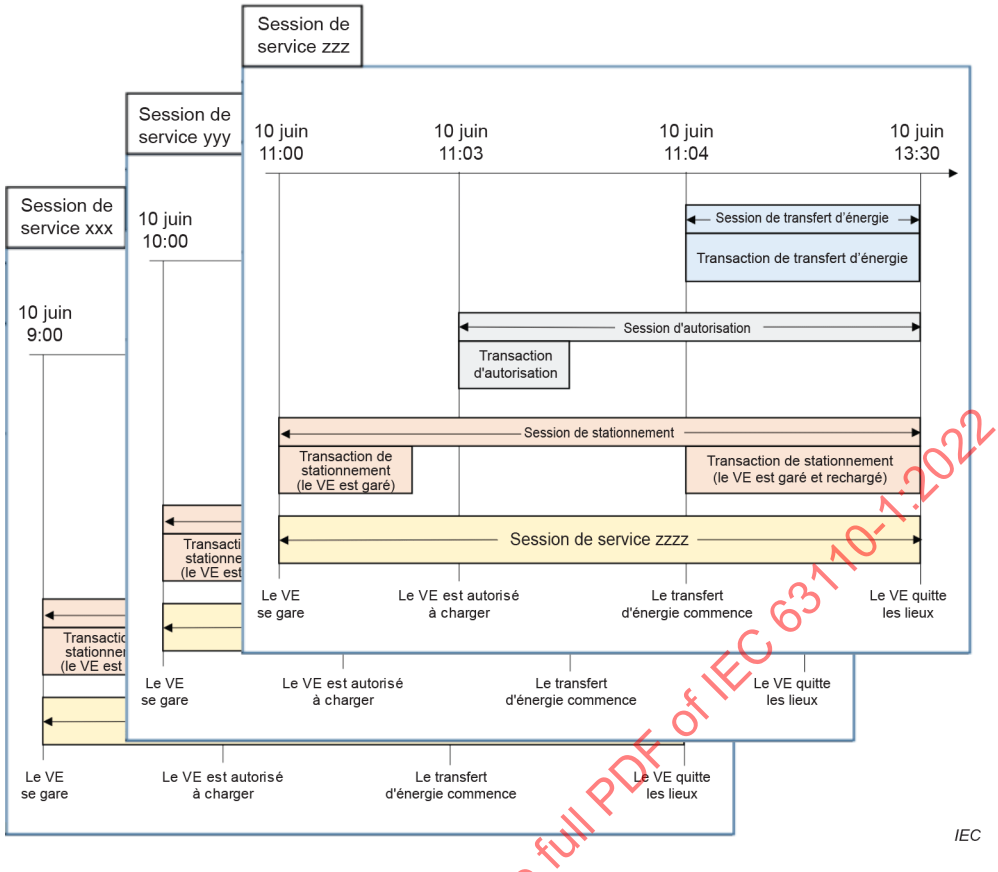


Figure 9 – Exemple de sessions de service simultanées

L'Annexe C donne, à titre d'illustration uniquement, un exemple plus complexe de session de service qui inclut la réservation, le stationnement, le transfert d'énergie et d'autres services.

7 Exigences générales

7.1 Généralités

L'Article 7 présente les exigences générales que les personnes chargées de la mise en œuvre du protocole défini dans l'IEC 63110-2 doivent suivre.

7.2 Exigences de protocole de communication

7.2.1 Généralités

Pour pouvoir charger sans problème les millions de VE qui circulent dans chaque pays dans les années à venir, il est nécessaire de choisir un protocole approprié de transmission de messages capable d'évoluer de manière sécurisée et efficace.

La liste des exigences présentées à l'Annexe B a permis de sélectionner la technologie de transmission de messages. Certaines de ces exigences peuvent être applicables au protocole défini dans l'IEC 63110.

7.2.2 Transfert de données

Pour transférer des données brutes telles que des microprogrammes, des certificats, des vidéos, de gros blocs de données, des informations sur les CS ou des stocks, les acteurs primaires doivent choisir, pour chaque transfert, l'une des deux méthodes suivantes:

– hors bande, fournissant un lien et une méthode de téléchargement des données;

– dans la bande, avec ou sans mécanisme de découpage.

Il convient d'utiliser le mécanisme dans la bande pour des raisons de sécurité le cas échéant.

Se reporter aux cas d'utilisation pertinents pour de plus amples informations concernant l'utilisation des deux méthodes.

7.3 Exigences relatives à l'architecture de communication

L'Article 4 relatif à l'architecture décrit un modèle qui repose sur le modèle de référence du modèle architectural du réseau intelligent (SGAM - *smart grid architecture model*).

Même si la mise en œuvre détaillée des étapes de cas d'utilisation décrites à l'Article 8 est une décision des personnes chargées de la mise en œuvre, l'échange d'informations entre le CSMS et le CSC décrit dans le présent document doit être appliqué.

La CS doit respecter le modèle SGAM et satisfaire en particulier aux exigences suivantes:

– Le CSMS et le CSC doivent communiquer à l'aide du protocole défini dans l'IEC 63110;

– Le CSC doit uniquement communiquer avec le CSMS;

– Le CSMS et le GR doivent échanger des informations à l'aide du protocole défini dans l'IEC 63110.

Outre les exigences susmentionnées, le protocole défini dans l'IEC 63110 doit assurer – si la personne chargée de la mise en œuvre le souhaite – que les messages définis peuvent être utilisés dans des architectures CSMS à plusieurs niveaux dans leur forme native afin de fournir des concepts de basculement de base, une surveillance à plusieurs niveaux, une livraison de données dans la bande à plusieurs sauts et des solutions similaires qui sont intrinsèques aux cas d'utilisation individuels de la communication entre CS et CSMS. Pour de plus amples informations, voir l'Article B.25.

7.4 Exigences spécifiques à l'utilisateur

Même si l'UVE ne relève pas directement du domaine d'application de l'IEC 63110 (toutes les parties), certains paramètres dont il est à l'origine (l'heure de départ, le coût ou les limites énergétiques, par exemple) peuvent être exigés pour certains cas d'utilisation, de manière à pouvoir les communiquer aux acteurs secondaires. Les messages IEC 63110 doivent par conséquent être en mesure de les transmettre.

7.5 Exigences relatives à la mise en œuvre CSMS

Les informations détaillées de mise en œuvre CSMS ne relèvent pas du domaine d'application du présent document. Toutefois, pour assurer l'interopérabilité, la fiabilité, la sécurité et la preuve de service, les personnes chargées de la mise en œuvre doivent appliquer les exigences suivantes.

– Le CSMS doit mettre en œuvre un mécanisme capable de suivre et de consigner en toute sécurité toutes les transactions qui se produisent pendant une session de service d'un VE particulier.

– Les sessions et transactions doivent être stockées en toute sécurité dans le CSMS avant d'envoyer les informations à l'OSR à la clôture de la session de service pour l'établissement du RSD.

– Le CSMS doit accepter les demandes de modification de transaction formulées uniquement par des entités dignes de confiance.
– Le CSMS doit vérifier l'intégrité du message qui demande la mise à jour

7.6 Exigences d'interface entre le CEM, le GR et le CSMS

Les cas d'utilisation sont la base de ces exigences. Dans certains cas d'utilisation, en particulier ceux qui relèvent du domaine de l'énergie, le GR et le CSMS (local ou en nuage) doivent échanger des informations telles que l'enveloppe de plages de puissance, les contraintes et les ETP agrégés.

Le CEM joue un rôle irremplaçable dans le comportement général de l'énergie dans les locaux et, de ce fait, dans l'énergie attribuée à la mobilité électrique. Il est probable que, lorsque des millions de VE vont être amenés à charger au même moment, le CEM va jouer un rôle central pour l'équilibre général du réseau électrique.

Afin d'assurer la sécurité et l'interopérabilité entre les réseaux IEC 63110 et le GR, il est donc nécessaire de décrire la manière dont le CSMS et le GR vont échanger des informations. Étant donné que le protocole défini dans l'IEC 63110 est utilisé pour la communication entre le CSC et le CSMS et qu'il constitue la base de la sécurité de l'échange, il semble naturel et simple que le GR puisse également utiliser le même protocole. Cela simplifie les interfaces CSMS locales et assure une relation de confiance avec le GR.

Par conséquent, le GR et le CSMS (local ou en nuage) doivent utiliser le protocole défini dans l'IEC 63110 pour échanger les informations

7.7 Exigences spécifiques au réseau électrique

Les exigences relatives aux codes de réseau électrique locaux doivent être prises en charge par la mise en œuvre IEC 63110 des CS et CSMS.

7.8 Exigences relatives au GRD

Les exigences relatives au GRD sont liées aux codes de réseau électrique existants.

Les GRD, en tant qu'entités responsables de la qualité de l'électricité et de la stabilité locale du réseau électrique, peuvent envoyer, par exemple, des messages de délestage au CEM afin d'éviter ou de réduire le plus possible la congestion dans la zone des locaux du CEM.

Les demandes de délestage provenant du GRD doivent être appliquées sans délai par le CSMS et la CS.

NOTE 1 Dans certaines régions, les demandes de délestage provenant du GRD sont obligatoires.

NOTE 2 Les messages de délestage peuvent être envoyés à l'OSR ou au CSMS (local ou en nuage). Dans les deux cas, une attention particulière est apportée par tous les acteurs concernés afin d'assurer l'intégrité des messages tout au long de leur transmission. Les messages corrompus ou provenant d'une source non digne de confiance peuvent être catastrophiques pour la stabilité du réseau électrique.

7.9 Exigences de cybersécurité

7.9.1 Généralités

Le paragraphe 7.9 décrit les exigences de sécurité pour la communication entre le CSC et le CSMS. En outre, il explique la justification des exigences qui reposent sur l'approche fondée sur les risques. Le présent document décrit les exigences générales en matière de cybersécurité.

Les problèmes de sécurité ont un impact sur le protocole, mais également sur d'autres parties et systèmes impliqués dans la mobilité électrique (les cartes et lecteurs RFID, par exemple), l'organisme de gestion des certificats et l'intégrité des données, y compris les dispositifs externes (les mobiles multifonctions, par exemple).

La principale recommandation générale du 7.9 réside dans le fait qu'il est nécessaire que le protocole vérifie que les informations du système ne sont pas lisibles ni falsifiées par tout acteur non autorisé.

7.9.2 Considérations relatives à la sécurité des informations

Le Tableau 3 ci-dessous fournit certaines considérations de sécurité concernant la confidentialité, l'intégrité et la disponibilité des informations transmises par l'intermédiaire de l'IEC 63110.

Le Tableau 3 présente le niveau de sécurité exigé pour les informations

Tableau 3 – Considérations relatives à la sécurité des informations

Données/informations (types de messages, échange d'informations)	**Brève description**	**Considérations relatives à la sécurité concernant**		
		Confidentialité (pseudonymat, anonymat)	**Intégrité** (intégrité des données, opportunité, non-répudiation, authenticité)	**Disponibilité** (résilience)
EMAID	L'EMAID est l'identifiant d'authentification de mobilité électrique utilisé pour l'identification du détenteur du contrat. La définition peut être consultée dans le document de modèle d'objet (IEC 63110-1-1).	Identifie une personne (confidentialité des données)	Identifie le conducteur et le contrat entre le conducteur/le propriétaire de la voiture et le MO	Moyen qui permet de lancer une session de charge.
Justificatif d'authentification de l'utilisateur	Le justificatif d'authentification de l'utilisateur est utilisé pour l'identification du détenteur du contrat.	Identifie une personne (confidentialité des données)	Identifie une personne et un contrat et est utilisé pour l'authentification	Moyen qui permet de lancer une session de charge.
Image du micrologiciel	Micrologiciel du contrôleur de point de charge	L'identité du client peut être aspirée et envoyée vers des serveurs externes. Peut donner lieu à une identification de la personne (confidentialité des données)	Les violations accidentelles ou volontaires de l'intégrité du micrologiciel (micrologiciel piraté) peuvent provoquer des préjudices (pertes financières, dommages possibles de l'EVCC, perte de fonction)	La disponibilité du micrologiciel du contrôleur est essentielle pour la disponibilité de ce dernier et le fonctionnement de la borne de charge. Elle est nécessaire à la communication entre le CSMS et le CSC.

Données/informations (types de messages, échange d'informations)	Brève description	Considérations relatives à la sécurité concernant		
		Confidentialité (pseudonymat, anonymat)	Intégrité (intégrité des données, opportunité, non-répudiation, authenticité)	Disponibilité (résilience)
Configuration du contrôleur	Liste des attributs de configuration du contrôleur de SAVE.	Les informations personnelles peuvent faire partie du fichier de configuration du contrôleur	Les violations accidentelles ou volontaires de l'intégrité de la configuration (micrologiciel piraté) peuvent provoquer des préjudices (pertes financières, dommages possibles de l'EVCC, perte de fonction)	Une réduction des services disponibles due à une modification de la configuration du contrôleur peut avoir un impact négatif sur l'activité
Valeurs du compteur de prise de courant	Compteur électrique à l'intérieur d'une borne de charge, qui mesure la consommation de puissance de la prise de courant	Les données du compteur ne sont pas attribuées à une personne physique et ne sont par conséquent pas pertinentes pour la protection/confidentialité des données.	Un mesurage compromis peut donner lieu à une perte de confiance de la part des clients et à une éventuelle perte d'activité. De même, toutes les factures seront fausses, ce qui donne lieu à un problème général au niveau du système	La CS ne doit pas facturer les transactions pendant la défaillance du compteur, ce qui peut donner lieu à une perte d'activité.
Valeurs du compteur de connexion au réseau électrique	Le compteur électrique utilisé pour mesurer la consommation de puissance de la connexion au réseau électrique	Les valeurs énergétiques peuvent être utilisées pour estimer le comportement personnel d'un conducteur.	Un mesurage compromis peut donner lieu à une perte de confiance de la part des clients et à une éventuelle perte d'activité. De même, toutes les factures seront fausses, ce qui donne lieu à un problème général au niveau du système	Il peut s'avérer nécessaire d'arrêter la CS pendant la défaillance du compteur, ce qui donne lieu à une perte d'activité.
Relevé de service détaillé (composé des valeurs de compteur, des horodatages, de l'ID de session, de l'EMAID, etc.)	L'ensemble de données de base utilisé pour la facturation	Le document contient des données privées qui permettent d'identifier une personne ou un contrat	Un document corrompu peut donner lieu à une perte de confiance de la part des clients et à une éventuelle perte d'activité	Le CS ne doit pas facturer les transactions pendant la défaillance du compteur, ce qui peut donner lieu à une perte d'activité.

Données/informations (types de messages, échange d'informations)	Brève description	Considérations relatives à la sécurité concernant		
		Confidentialité (pseudonymat, anonymat)	Intégrité (intégrité des données, opportunité, non-répudiation, authenticité)	Disponibilité (résilience)
Le certificat et la clé privée relatifs au SAVE (ISO 15118)	Certificat d'un contrôleur de communication de l'infrastructure de recharge SECC utilisé pour établir une connexion TLS entre le SECC et l'EVCC par l'intermédiaire de l'ISO 15118	Un certificat exposé n'affiche que l'identité du SECC et les identités d'émission de CA, leurs clés publiques et les périodes de validité.	Un certificat corrompu peut donner lieu à une perte de confiance de la part de tous les acteurs et à une éventuelle perte d'activité.	Lorsque le certificat SECC est corrompu (volé) du fait de l'absence de SECC, le certificat, ou la clé privée, empêche la connexion TLS. Noter qu'une communication qui n'exige pas de TLS est toujours possible. Toutefois, la communication est non cryptée et peut exposer des informations personnelles du client qui facture.
Fichier journal de diagnostic	Fichier journal fourni par un SAVE et qui contient des informations de diagnostic	Un fichier journal devenu lisible peut permettre d'identifier des personnes ou de divulguer des informations sensibles	Un fichier journal corrompu peut donner lieu à une mauvaise interprétation et à des actions réalisées par l'OSR qui peuvent endommager l'EVCC ou être à l'origine d'une perte de fonction	Un fichier journal corrompu n'a que peu voire pas d'influence sur les opérations du SAVE.
Fichier journal d'audit	Fichier journal fourni par un SAVE et qui contient des informations concernant les événements relatifs à la sécurité	Un fichier journal devenu lisible peut permettre d'identifier les événements relatifs à la sécurité et les failles de l'infrastructure de charge, ainsi que les informations contractuelles de l'utilisateur.	En cas de corruption (modification ou falsification) d'un fichier journal de sécurité, les problèmes de sécurité existants ne peuvent pas être reconnus et entraînent des failles de sécurité, ou des problèmes de sécurité inexistants peuvent être notifiés à l'opérateur, entraînant une indisponibilité inutile de l'infrastructure de recharge.	En cas de perte ou de corruption de fichiers journaux de sécurité importants, des failles de sécurité importantes peuvent rester non identifiées, ce qui provoque une corruption non reconnue du système.
Tuple SASchedule (composé du programme Pmax et des prix de vente)	Informations relatives aux restrictions de puissance et aux prix de l'énergie, utilisées pour optimiser la charge du VE	La CS et le SAVE refusent les Tuples SASchedule corrompus.	La CS et le SAVE refusent les Tuples SASchedule corrompus.	Chaque CS qui a reçu un SASchedule corrompu n'est pas en mesure de fournir un service de charge programmé. Il lui est de ce fait nécessaire de revenir à d'autres modes de charge.

Données/informations (types de messages, échange d'informations)	Brève description	Considérations relatives à la sécurité concernant		
		Confidentialité (pseudonymat, anonymat)	Intégrité (intégrité des données, opportunité, non-répudiation, authenticité)	Disponibilité (résilience)
Charge/profil de charge (puissance prévue dans le temps)	Profil de puissance prévue envoyé par le VE après négociation avec le SAVE.	Le profil de charge est calculé par le VE sur la base des besoins de mobilité de l'utilisateur (heure de départ et quantité d'énergie cible/min/maximale à charger), ce qui entraîne des comportements et des situations propres à l'utilisateur.	La modification malveillante du profil de puissance peut entraîner le rejet de la charge par le SAVE en raison de la violation du programme Pmax ou peut empêcher la satisfaction des besoins de mobilité de l'utilisateur, ce qui nuit à la satisfaction de l'utilisateur à l'égard du service de charge. Cette modification peut même endommager le dispositif du VE ou causer des problèmes de sécurité par la violation des limites physiques du VE.	Chaque VE qui envoie des paramètres de charge corrompus/incorrects peut finir par être endommagé par une puissance/un courant trop élevés.
Informations d'état du SAVE	Informations d'état relatives au SAVE (disponible, occupé, réservé, etc.).	N'est pas réputé être associé à des données personnelles.	Des erreurs dans l'état du SAVE ou la non-disponibilité de l'état peuvent causer un dommage mineur (pertes financières liées à l'arrêt de la station, plaintes des clients, etc.).	Un SAVE dont l'état est erroné doit cesser de fonctionner, ce qui entraîne une perte d'activité et une perte des services de charge.
Certificat d'approvisionnement OEM ISO 15118	Certificat à l'intérieur d'un VE, utilisé pour transférer un certificat de contrat d'un acteur secondaire vers le VE	Un certificat exposé de VE n'affiche que l'identité de ce dernier, le PCID et les identités d'émission d'AC, leurs clés publiques et les périodes de validité.	Le remplacement du certificat d'approvisionnement OEM par un autre empêche l'installation des certificats de contrat. La modification délibérée du PCID dans un certificat d'approvisionnement OEM entraîne l'installation d'un certificat de contrat erroné, ce qui peut entraîner des litiges de facturation.	L'absence de certificat d'approvisionnement OEM empêche seulement l'installation ou la mise à jour d'un certificat de contrat. La charge n'est pas affectée si un certificat de contrat valide est déjà installé.

Données/informations (types de messages, échange d'informations)	Brève description	Considérations relatives à la sécurité concernant		
		Confidentialité (pseudonymat, anonymat)	Intégrité (intégrité des données, opportunité, non-répudiation, authenticité)	Disponibilité (résilience)
Certificat de contrat	Certificat délivré à un utilisateur de VE ou à une organisation pour identifier le contrat avec l'EMSP et installé dans le VE.	Identifie une personne (confidentialité des données)	Les modifications apportées au certificat de contrat peuvent entraîner des litiges en matière de facturation, car le certificat indique le compte sur lequel il est nécessaire de facturer la session de charge.	L'autorisation d'installation du certificat de contrat est nécessaire.
Paramètre de charge	Paramètre envoyé par l'EVCC afin d'optimiser le transfert d'énergie, par exemple: courant max/min, tension, énergie exigée, heure de départ	Le paramètre de charge comprend des informations personnelles telles que l'heure de départ, la demande d'énergie cible/min./max., qui peuvent révéler la mobilité et le mode de vie du conducteur.	Un paramètre de charge corrompu peut conduire à une mauvaise compréhension des limites physiques du VE et peut entraîner des problèmes de sécurité, ainsi qu'une interruption de la charge en cas de dépassement de la puissance maximale du SAVE.	Chaque VE qui envoie des paramètres de charge corrompus/incorrects peut finir par être endommagé par une puissance/un courant trop élevés.
Réponses OCSP	État de révocation du certificat SECC fourni au VE lors de l'établissement de liaison TLS	L'exposition de l'état de révocation du certificat SECC ne pose pas de problème.	La manipulation de l'OCSP peut faire en sorte que des certificats révoqués soient acceptés par le VE, ce qui pose des problèmes de confidentialité, ou que des certificats valides soient refusés par le VE, ce qui entraîne une attaque par déni de service.	L'absence de réponses OCSP pour un certain nombre de chargeurs entraîne une attaque massive par déni de service.

7.9.3 Analyse des menaces

7.9.3.1 Généralités

L'analyse des menaces repose sur l'architecture et les cas d'utilisation présentés en 4.2 et à l'Article 8.

Le paragraphe 7.9.3 prend en considération les vecteurs de menace pertinents pour le protocole de communication d'arrière-plan.

7.9.3.2 Usurpation

En règle générale, l'usurpation consiste à prétendre être quelque chose ou quelqu'un d'autre que soi-même. Dans le contexte du protocole de communication d'arrière-plan, il peut s'agir d'un message envoyé au CSC par une personne malveillante qui lui fait croire que le message provient du CSMS. Il peut également s'agir d'un scénario de menace qui fait croire au CSC qu'il communique avec un faux CSMS. Une personne malveillante peut alors hameçonner les justificatifs d'identité (ID utilisateur, mots de passe, codes PIN, etc.).

7.9.3.3 Manipulation frauduleuse

La manipulation frauduleuse consiste à modifier les données dans la mémoire, sur le réseau ou sur le disque. Il est concevable de manipuler les profils de charge, les informations tarifaires ou les informations contractuelles transmises par l'intermédiaire du protocole d'arrière-plan.

7.9.3.4 Répudiation

En règle générale, la répudiation consiste à affirmer qu'une personne revendique qu'elle n'a rien fait ou qu'elle n'est pas responsable de ce qu'il s'est passé. La non-répudiation est essentielle pour une facturation correcte.

7.9.3.5 Accès non autorisé

La divulgation d'informations concerne des entités qui ont accès à des données auxquelles elles ne sont pas autorisées à accéder. En particulier, toutes les informations traitées comme étant confidentielles font souvent l'objet d'attaques et exigent certainement d'être protégées. Toutes les informations qui figurent dans le Tableau 3 et dont la confidentialité est élevée sont affectées.

7.9.3.6 Déni de service

En règle générale, une attaque de déni de service consiste à épuiser une ressource nécessaire pour fournir un service. Dans le contexte de l'IEC 63110, ces ressources peuvent être un réseau, des CPU et la mémoire sur le CSC et le CSMS, ainsi que l'équipement principal sur le CS. Des personnes malveillantes peuvent saturer le réseau ou augmenter la charge sur la CS et le CSMS en répétant des messages.

7.9.3.7 Élévation de privilège

En règle générale, l'élévation de privilèges permet à quelqu'un de faire quelque chose qu'il n'est pas autorisé à faire, par exemple lorsqu'un utilisateur normal peut appliquer des mises à jour de micrologiciel alors que seuls des administrateurs sont autorisés à le faire. De faibles mises en œuvre de contrôles des autorisations (voire de simples défaillances de mise en œuvre) peuvent être utilisées par des personnes malveillantes comme porte dérobée.

7.9.4 Exigences de sécurité

7.9.4.1 Généralités

Le paragraphe 7.9.4 décrit les exigences générales en matière de sécurité afin d'atténuer les menaces décrites en 7.9.3.

7.9.4.2 Authentification sécurisée

Le protocole défini dans l'IEC 63110 doit permettre une authentification sécurisée.

7.9.4.3 Micrologiciel sécurisé

Il est nécessaire que le téléchargement des images du micrologiciel soit sécurisé afin de protéger leur intégrité et d'éviter des images falsifiées.

Pour le chargement du micrologiciel, l'IEC 63110 doit prendre en charge les actions suivantes.

– Le paquet de mises à jour du micrologiciel doit être signé numériquement. Tant les signatures numériques intégrées dans l'image du micrologiciel (fichier) que les signatures externes doivent être prises en charge.
– Le chargement du micrologiciel exige une autorisation.
– Le protocole doit offrir la possibilité d'indiquer si les mises à jour du micrologiciel, l'activation du micrologiciel et les reprises ont abouti ou échoué.
– Le protocole doit offrir la possibilité de revenir à une ancienne version en cas d'échec de l'activation du micrologiciel.

7.9.4.4 Communication sécurisée

Pour la mise en œuvre d'un principe de défense en profondeur, le protocole doit prendre en charge la sécurité dans plusieurs couches. De plus, le protocole doit assurer une sécurité de bout en bout dès que cela est nécessaire, en particulier concernant les architectures à sauts multiples (dans le cas du CSMS local, par exemple). Le chiffrement de bout en bout est important pour les données confidentielles (en particulier les données privées). Le protocole doit offrir des capacités qui permettent de détecter les messages dupliqués (afin de gérer les attaques de déni de service).

Une protection forte et sécurisée de l'intégrité des messages est importante pour éviter les menaces telles que la manipulation frauduleuse, la répudiation, l'usurpation et le déni de service.

7.9.4.5 Contrôle d'accès

Le protocole doit offrir une possibilité de contrôle d'accès à grain fin. Une capacité d'autorisation sécurisée doit être utilisée pour mettre en œuvre un principe de moindre privilège. Des mécanismes d'authentification puissants sont exigés pour éviter la répudiation. Le protocole doit prendre en charge l'accès autorisé uniquement et empêcher l'élévation de privilèges.

7.9.4.6 Consignation des événements relatifs à la sécurité

Une consignation et une alarme suffisantes sont exigées pour empêcher la répudiation et pouvoir aider à détecter les attaques ou les fraudes.

Le protocole doit au moins prendre en charge les événements suivants relatifs à la sécurité:

– tentatives réussies ou avortées d'ouverture de session;
– téléchargements de micrologiciel (réussis, avortés, reprises);
– modifications de la configuration;
– autres types d'attaques;
– faux messages (contrôle d'intégrité).

Le protocole doit prendre en charge les compteurs pour les événements relatifs à la sécurité tels que:

– tentatives de connexion non autorisées;
– tentatives d'ouverture de session avec un mot de passe erroné, de mauvais justificatifs d'identité, des certificats expirés.

Le journal et les alarmes doivent être protégés contre des modifications non autorisées (manipulation frauduleuse) et l'usurpation. Le journal peut contenir des informations utiles pour les personnes malveillantes et ne doit être accessible qu'aux utilisateurs autorisés.

7.9.5 Relation avec les cas d'utilisation

Les exigences de cybersécurité s'appliquent de manière universelle à tous les cas d'utilisation. Toutefois, certains cas d'utilisation particuliers exigent un mécanisme précis afin d'assurer la sécurité des transactions. Par exemple, l'installation des certificats dans le CSMS ou dans la CS est une fonction nécessaire décrite dans les cas d'utilisation.

La Figure E.1 de l'Annexe E représente une séquence informative de cas d'utilisation qui peuvent être utilisés pour assurer la sécurité de l'infrastructure de charge.

7.10 Exigences de sécurité

Les exigences de sécurité sont décrites dans les normes correspondantes. Se reporter à l'IEC 61851-1, l'IEC 61851-23, l'IEC 61851-23-1[1] et l'IEC 61851-25.

L'IEC 63110 n'est pas conçue pour être utilisée pour toutes les fonctions relatives à la sécurité.

Si la CS détecte un problème de sécurité dans un ou plusieurs SAVE et qu'il le signale au CSMS, ce dernier doit prendre les mesures appropriées pour empêcher l'utilisation des SAVE en question avant de procéder à une évaluation de la sécurité.

Si la CS détecte un problème de sécurité dans un SAVE pendant une session de charge, le CSMS doit informer l'OSR afin d'indiquer à l'utilisateur par les moyens appropriés qu'un problème de sécurité a été signalé dans le SAVE en cours d'utilisation et que les besoins de mobilité électrique peuvent ne pas être satisfaits.

8 Cas d'utilisation

8.1 Généralités

Les cas d'utilisation présentés de 8.2 à 0 utilisent la méthodologie présentée dans l'IEC 62559-2. Les cas d'utilisation définis dans l'IEC 63110-1 ont été inspirés par les cas d'utilisation OCPP 2.0.1.

Les cas d'utilisation professionnelle présentés à l'Article 8 capturent les utilisations habituelles, répétées, déployées ou envisagées de l'environnement de mobilité électrique. Ils proposent des scénarii et des séquences qui peuvent être organisés différemment ou dans un ordre différent, mais à la fin, ils mènent au même échange d'informations entre les acteurs primaires du présent document: le CSMS et le CSC. L'Article 8 a pour objet de décrire de manière aussi exhaustive que possible toutes les exigences des acteurs pendant les séquences de mobilité électrique qui relèvent du domaine d'application du présent document.

L'Annexe D propose une classification des cas d'utilisation en matière d'effets de mise en œuvre qui peut aider à prioriser l'élaboration du protocole défini dans l'IEC 63110.

NOTE Dans les cas d'utilisation suivants, le terme CS est générique. En fonction du contexte, il peut faire référence à la borne de charge, mais également au contrôleur de borne de charge.

[1] En cours d'élaboration. Stade au moment de la publication: IEC CDV 61851-23-1:2020.

8.2 Cas d'utilisation du domaine de l'énergie

8.2.1 Généralités

Tous les cas d'utilisation du domaine de l'énergie appartiennent au cycle des opérations de service. Ils décrivent les aspects de la CS relatifs à la gestion de l'énergie. Ils définissent également des scénarii dans lesquels des acteurs secondaires tels que le CEM, l'UVE ou le GRD peuvent influencer le comportement des sessions de charge.

Du point de vue énergétique, le rôle central du CSMS consiste à adapter en permanence la demande ou la production de puissance de la CS en fonction de la PRE fixée par le GR au CSMS et, en même temps, à annoncer en permanence ses contraintes de puissance et d'énergie au GR. Ceci est réalisé par la surveillance constante de tout événement susceptible de modifier la puissance totale agrégée consommée ou produite au niveau de la CS. Cette adaptation constante conduit à l'attribution de l'ETP à chaque SAVE par le CSMS. L'ETP peut être un profil (puissance dans le temps) ou une valeur unique. Il peut être positif ou négatif à un moment donné. L'un des principaux rôles du CSMS est de calculer les ETP en fonction des besoins de mobilité de l'utilisateur du VE, des caractéristiques du VE et du SAVE, ainsi que de la logique métier du CSMS.

Le fait que la somme de tous les ETP soit toujours comprise dans la PRE fixée par le GR permet une meilleure utilisation et un meilleur accès aux ressources par l'UVE, ce qui est optimal du point de vue du CEM et du réseau. En ce sens, le rôle de gestionnaire d'énergie joué par le CSMS consiste essentiellement à mettre en œuvre ladite "charge intelligente".

La mise en œuvre détaillée de cette boucle de réaction principale ne relève pas du domaine d'application, mais une présentation générale est donnée dans le diagramme de séquences de la Figure 10. Le mécanisme de publication/abonnement proposé par le protocole défini dans l'IEC 63110 offre la possibilité de mettre en œuvre en toute transparence cette boucle d'événement.

Cette activité pilotée par un événement est distribuée dans les CS et les CSMS (local ou en nuage). Pour les configurations importantes qui comportent de nombreuses CSZ et de nombreux SAVE commandés par une ou plusieurs CS, la PRE envoyée par le GR pour une CSZ spécifique est traitée directement par le CSMS responsable de cette CSZ. Voir les exemples de mise en œuvre à l'Annexe A pour une présentation exhaustive du rôle du CEM.

Le cas d'utilisation de charge intelligente décrit cette boucle d'événement de manière détaillée. Dans le présent document, il est considéré comme le principal cas d'utilisation pour le domaine de l'énergie. Tous les autres cas d'utilisation sont des sous-cas d'utilisation qui détaillent certains aspects particuliers des échanges d'informations à partir d'autres acteurs.

La Figure 10 décrit une mise en œuvre possible de cette boucle d'événement. Elle est donnée à titre d'illustration. Les activités en vert relèvent directement du domaine d'application du présent document. Chaque activité est associée à un numéro - voir la section "Analyse étape par étape du scénario" en 8.2.3 pour plus d'informations sur les activités.

8.2.2 Liste des cas d'utilisation du domaine de l'énergie

Le Tableau 4 fournit une liste et une brève description des cas d'utilisation du domaine de l'énergie.

Tableau 4 – Liste des cas d'utilisation du domaine de l'énergie

ID	Cas d'utilisation	Brève description	Cycle de vie / Séquence
E1	Gestion de la charge intelligente	Établir les meilleurs ETP possibles pour un groupe de VE.	Opérations de service / Boucle d'événement
E2	Assurer la charge en réponse à une demande	ETP fondés sur les incitations de flexibilité provenant du marché.	Opérations de service / Boucle d'événement
E3	Échange d'informations CSMS – GR à l'initiative du CSMS	Le CSMS et le GR échangent des informations de bilan énergétique et de bilan de puissance.	Opérations de service / Boucle d'événement
E4	Échange d'informations CSMS – GR à l'initiative du GR	Le GR et le CSMS échangent des informations de bilan énergétique et de bilan de puissance.	Opérations de service / Boucle d'événement
E5	Variation de puissance déclenchée par le GRD	Manière dont le CSMS applique le message de délestage provenant du GRD	Opérations de service / Boucle d'événement
E6	Relations entre les acteurs pendant une session V2G	Relations entre les acteurs afin d'établir un service V2G.	Opérations de service / Boucle d'événement
E7	Échange d'informations exigé pour assurer une commande de transfert d'énergie dynamique	Permettre à la CS, au CSMS ou à un acteur secondaire de fournir un ETP	Opérations de service / Boucle d'événement
E8	Offrir un service de régulation de fréquence au moyen de mesurages de fréquence décentralisés	Offrir un service de régulation de fréquence au moyen de mesurages de fréquence décentralisés	Opérations de service / Boucle d'événement

8.2.3 Gestion de la charge intelligente

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E1	Services de transfert d'énergie	Gestion de la charge intelligente

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Ce cas d'utilisation décrit les fonctions réalisées par le CSMS afin d'optimiser l'ETP de chaque VE et d'organiser ce qu'il est généralement appelé "charge intelligente". Pour ce faire, le GR, le CSMS et la CS maintiennent une boucle de réaction principale à tous les événements susceptibles de modifier les contraintes de puissance et d'énergie pour un ou tous les VE concernés par une session de service.
Objectif(s)	– Décrire les échanges d'informations entre le CSMS, le CSC et le GR afin d'optimiser les ETP attribués aux VE. – Améliorer l'expérience utilisateur: vérifier que les UVE sont capables de réaliser une charge qui satisfasse aux besoins de mobilité électrique. – Satisfaire aux contraintes d'énergie: adapter l'ETP pour chaque VE selon la PRE attribuée au CSMS par le GR.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation décrit l'échange de données entre le GR, le CSMS et le CSC afin de satisfaire aux besoins de mobilité électrique des VE tout en optimisant les ETP.
Description complète
Afin que le CSMS puisse optimiser l'ETP et s'adapter à toute variation dans ses propres contraintes d'énergie ou de puissance ou à partir de la PRE définie par le GR, il suivra l'étape suivante. Voir la Figure 10 pour une description graphique: **Boucle de détection d'événements** À tout moment au cours du processus, les contraintes d'énergie et de puissance, ainsi que la PRE, peuvent être mises à jour en raison d'un événement défini. Une liste non exhaustive d'événements est présentée ci-dessous: – un nouveau VE arrive; – un VE fait une pause ou met fin au transfert d'énergie; – la puissance maximale disponible au niveau de la CS a été atteinte; – la PRE calculée par le CEM a été modifiée; – les contraintes d'énergie et de puissance pour le CSMS ont été modifiées; – un ou plusieurs VE souhaitent modifier leur ETP; – les variations de puissance dynamique pour les services auxiliaires peuvent influer sur d'autres ETP pour VE; – réservation immédiate pour un VE qui va arriver ultérieurement; – variations des tarifs; – élément déclencheur interne de CSMS (variation des contraintes...). **Analyser l'événement et s'adapter** Lorsqu'un événement susceptible de modifier les besoins de mobilité électrique, les contraintes d'énergie et de puissance CS ou CSMS, voire la PRE du GR est détecté, le destinataire de l'événement analyse la puissance disponible et l'énergie nécessaire à la nouvelle situation après l'événement. **Dans le cas où l'événement entraîne une modification des besoins de mobilité électrique:** Lorsque la PRE existante n'est pas suffisante pour servir l'AETP existant: aller à la boucle de mise à jour ou revenir à la boucle de détection d'événements **sinon si l'événement conduit à une modification des contraintes d'énergie et de puissance du CSMS incompatible avec la PRE actuelle** alors: le CSMS calcule les nouvelles contraintes d'énergie et de puissance le CSMS déclenche le cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du CSMS" revenir à la boucle de détection d'événements **sinon** revenir à la boucle de détection d'événements **fin** **boucle de mise à jour** Lorsqu'un événement est incompatible avec les ETP existants: alors: le CSMS calcule et met à jour les ETPS pour chaque VE concerné le CSMS met à jour ses propres contraintes d'énergie et de puissance le CSMS déclenche un événement de modification des contraintes CSMS. le CSMS peut notifier à l'OSR d'informer l'utilisateur du résultat de l'événement (ne relève pas du domaine d'application de ce protocole).

Récit du cas d'utilisation
aller à la boucle de détection d'événements NOTE 1 Il est important que la charge intelligente n'empêche pas le CSMS de faire ses meilleurs efforts pour répondre aux besoins de mobilité. NOTE 2 En cas de variations de l'ETP pour un VE particulier, le CSMS informe sans délai l'OSR, afin qu'il puisse le signaler à l'EMSP correspondant. NOTE 3 Il est prévu que le CSMS tente d'optimiser le nouveau ETP sur la base de chaque situation spécifique au VE, comme le contrat, la priorité, les besoins de mobilité, etc.

Indicateurs de performance clés (IPC)

Indicateurs de performance clés			
ID	**Nom**	**Description**	**Référence aux objectifs de cas d'utilisation mentionnés**
1	Expérience utilisateur	Pourcentage d'utilisateurs ayant été en mesure de charger selon leurs besoins de mobilité électrique	Augmenter l'expérience utilisateur
2	Utilisation de la puissance allouée	Satisfaire aux contraintes d'énergie et capacité à gérer les variations de répartition de la puissance	Satisfaire aux contraintes d'énergie

Conditions de cas d'utilisation

Conditions préalables	
1	Les locaux comportent un CEM et un GR est chargé de la CSZ lorsqu'une CS est gérée par un CSMS.

Remarques générales

Remarques générales
Technologie de charge ''agnostique'': ce cas d'utilisation ne dépend d'aucune technologie de charge. Il décrit uniquement l'échange d'informations entre le CSMS, le GR et le CS. Il revient à la CS de gérer en interne les différentes technologies de charge telles que CHAdeMO, ISO 15118, série IEC 61851 ou le transfert de puissance sans fil (technologies inductives).

Présentation des scénarii

Conditions du scénario						
N°	**Nom du scénario**	**Description du scénario**	**Acteur primaire**	**Événement déclencheur**	**Condition préalable**	**Post-condition**
1	Gestion de la charge intelligente	Ce scénario présente les étapes de la gestion de la charge intelligente	CSMS, CS	Un événement		

Analyse étape par étape du scénario

Voir la Figure 10 pour des informations détaillées sur le diagramme de séquences correspondant.

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Détection d'un événement par la CS, le CSMS ou le GR	Nouvel événement susceptible de modifier les besoins de mobilité électrique; détection et traitement de la PRE ou de l'AETP par le destinataire de l'événement.	GR, CS, CSMS		
2	La CS traite une modification qui influe sur les besoins de mobilité électrique	Dans le cas où l'événement peut entraîner une modification des besoins de mobilité électrique, la CSC informe le CSMS de l'existence de l'événement. Par exemple, un nouveau VE tout juste branché.	CS	CSMS	Info1- le CSC transmet l'événement au CSMS
2.1	Traiter une modification des besoins de mobilité électrique	Si la PRE existante ne permet pas de servir l'AETP existant, passer alors à l'étape 1.5; sinon, revenir à la boucle de détection d'événements.	CSMS	CS	Voir étape 5
3	Traiter une modification des contraintes CSMS	Si les nouvelles contraintes CSMS sont incompatibles avec la PRE actuelle, le CSMS demande alors au GR de mettre à jour la PRE. Voir le cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du CSMS". Sinon, revenir à la boucle de détection d'événements.	CSMS, GR	CSMS, GR	Voir Cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du CSMS"
4	Traiter une modification de la PRE	Si l'événement entraîne une modification de la PRE, le GR demande alors au CSMS de mettre à jour les ETP. Voir "Échange d'informations CSMS – GR à l'initiative du GR" UC	GR, CSMS	GR, CSMS	Voir Cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du GR"
4.1	Confronter les ETP mis à jour à l'AETP existant.	Si la nouvelle PRE ne permet pas de servir l'AETP existant, passer alors à l'étape 1.5; sinon, revenir à la boucle de détection d'événements.	CSMS	CS	Voir étape 5
5	Boucle de mise à jour: Traitement d'un événement incompatible avec les ETP existants	L'événement détecté entraîne une situation incompatible avec l'ETPS existant. Le CSMS met à jour l'ETPS pour chaque VE concerné. Le CSMS met à jour ses contraintes d'énergie et de puissance et déclenche un événement qui correspond à une modification des contraintes CSMS. Le CSMS peut notifier à l'OSR de signifier le résultat de l'événement.	CSMS	CS	Info2 – Envoyer un ETPS pour chaque VE

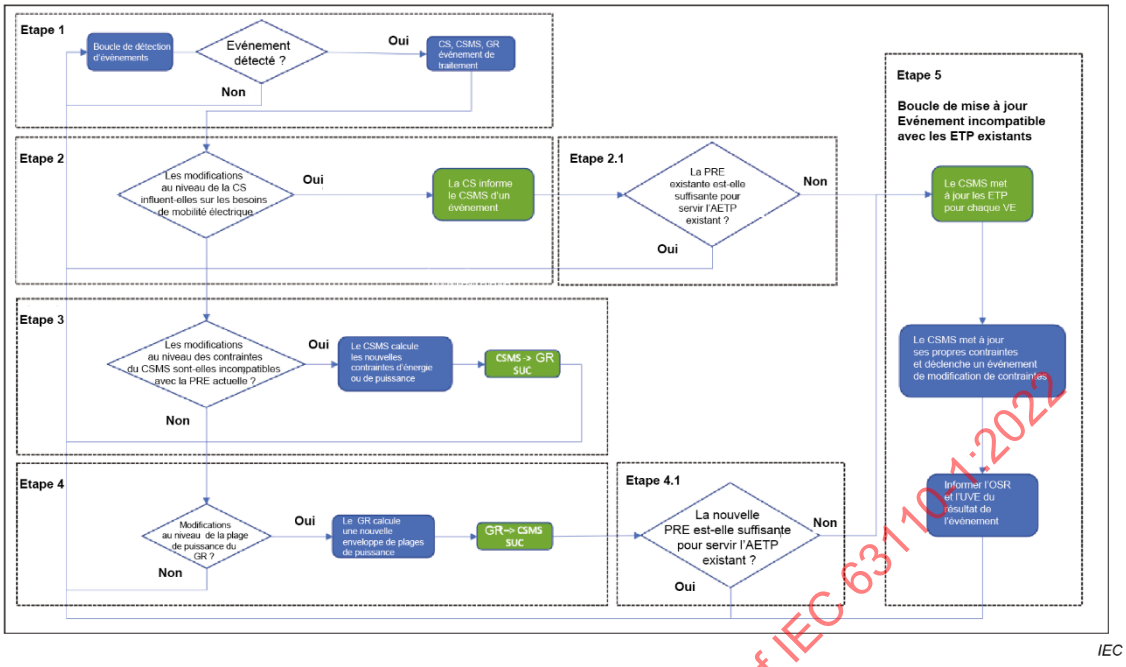


Figure 10 – Diagramme de séquence de charge intelligente

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	La CS transmet l'événement au CSMS	Nature de l'événement. Exemples: – un nouveau VE a été branché; – un VE a été débranché; – un VE a mis à jour son heure de départ.
Info2	Transmettre des ETP à chaque VE	ETP pour chaque VE concerné

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Transmission des ETP au CSC pour chaque VE	En cas de variations de l'ETP pour un VE particulier, le CSMS doit communiquer sans délai le nouveau ETP au CSC approprié
Req2	Traçabilité	Tous les événements qui influent sur les ETP doivent déclencher une transaction de transfert d'énergie

8.2.4 Assurer la charge en réponse à une demande

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E2	Services de transfert d'énergie	Assurer la charge en réponse à une demande

Domaine d’application et objectifs du cas d'utilisation

Domaine d’application et objectifs du cas d'utilisation	
Domaine d'application	Le domaine d'application de ce cas d'utilisation professionnelle consiste à décrire la procédure de charge agrégée du VE en fonction d'une incitation provenant d'acteurs secondaires.
Objectif(s)	Proposer un service de charge conforme aux besoins de mobilité électrique de l'utilisateur. Optimiser la charge en fonction des incitations des acteurs secondaires.
Cas métier connexe(s)	Offre de services énergétiques.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation décrit l'échange d'informations entre la CS et le CSMS nécessaires au fonctionnement d'un programme de réponse à la demande mandaté par un SA.
Description complète
Les programmes de réponse à la demande sont utilisés pour influencer la consommation d'énergie ou la demande d'électricité dans des conditions d'alimentation contraintes. Ces programmes offrent généralement des incitations aux clients sous la forme de tarifs spéciaux, de remboursement, voire de paiement. Les SA intéressés par des programmes de réponse à la demande sont les suivants: GRD, OF et BRP. En fonction des conditions incitatives proposées par les SA, le transfert d'énergie depuis/vers les VE peut commencer immédiatement ou pas. De même, après que le transfert d'énergie a commencé, il peut être modifié ou interrompu pendant une certaine période. Étant donné que le CSMS peut uniquement recevoir des messages provenant du GR, du CSC ou de l'OSR, ce cas d'utilisation ne prend en considération que les messages de réponse à la demande provenant du GR ou de l'OSR. Les messages de réponse à la demande reçus directement par le VE ne relèvent pas du domaine d'application de ce cas d'utilisation. Dans les deux cas, le message est présenté à la CS sous une forme qui reflète les incitations reçues par le CSMS (un nouveau plan de transfert d'énergie, par exemple). L'UVE peut accepter de participer, par exemple reporter ou interrompre la charge en fonction de l'incitation. L'UVE peut également refuser les modifications apportées au plan de charge et aux besoins de mobilité électrique. NOTE 1 Le CSMS consigne l'état de charge (charge en cours normale ou charge sous le contrôle d'un acteur de flexibilité), à quel moment la charge a commencé et à quel moment elle se termine afin de remplir le RSD. La session de transfert d’énergie et les transactions correspondantes sont également mises à jour. NOTE 2 L'application d'un programme de réponse à la demande ne dispense pas le CSMS de faire de son mieux pour répondre aux besoins de mobilité des VE connectés.

Indicateurs de performance clés (IPC)

Indicateurs de performance clés			
ID	**Nom**	**Description**	**Référence aux objectifs de cas d'utilisation mentionnés**
1	Transférer l'énergie dans la batterie du VE	Pourcentage de charge atteint entre la connexion et la déconnexion par l'utilisateur	Proposer un service de charge conforme aux besoins de mobilité électrique de l'utilisateur
2	Profiter des incitations	Pourcentage de messages de réponse à la demande acceptés	Optimiser la charge en fonction des incitations de l’acteur secondaire.

Conditions de cas d'utilisation

Conditions préalables	
1	L'UVE est identifié et autorisé à charger.
2	Le CSMS peut recevoir des messages d'incitation de la part des SA: après la réception des incitations, le CSMS, en fonction de ses paramètres, peut adapter l'incitation à la situation énergétique locale, puis la transmettre à la CS.

Présentation des scénarii

Conditions du scénario						
N°	**Nom du scénario**	**Description du scénario**	**Acteur primaire**	**Événement déclencheur**	**Condition préalable**	**Post-condition**
1	Assurer la charge en réponse à une demande	Ce scénario décrit la procédure de charge du VE en fonction d'une incitation provenant d'acteurs secondaires	CSMS	Incitations reçues		

Analyse étape par étape du scénario

Les étapes 1 et 2 suivantes sont indépendantes et non séquentielles

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le CEM reçoit des incitations de la part du SA et le GR envoie un nouveau plan de transfert d'énergie au CSMS	Le CEM reçoit des incitations qui visent à modifier la demande des locaux Le CEM calcule en interne une nouvelle répartition de la puissance destinée au CSMS fondée sur les conditions des incitations. Par exemple: – si les incitations favorisent une augmentation de la demande due à un excès de production solaire dans le pays, le CEM attribue plus de puissance au CSMS; – si le prix de l'énergie augmente brusquement au cours des deux heures qui suivent, le CEM peut attribuer moins de puissance au CSMS pendant cette période. Ce calcul interne au CEM ne relève pas du domaine d'application. Le nouveau plan de transfert d'énergie du CSMS, calculé par le CEM, peut être envoyé au CSMS par le GR.	SA, CEM, GR	CSMS	Info1 – Le CEM transmet la PRE au CSMS

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
2	Le CSMS envoie le nouveau plan de transfert d'énergie au CSC en raison des incitations reçues de la part du SA	– Les incitations peuvent être reçues de manière asynchrone (tous les jours de la semaine + le week-end, par exemple) ou en temps réel lorsque le CEM ou l'OSR sont mis à jour pas un acteur secondaire. – Le CSMS informe le CSC des incitations. La CS envoie les informations aux SAVE concernés. – Les VE concernés par une session ISO 15118 du mode de programme reçoivent un message de renégociation avec une nouvelle proposition de programme. – Les informations relatives aux incitations peuvent être le tarif, la puissance maximale, les plans de variations du niveau de CO_2 ou simplement un signal indiquant une période de pointe.	CSMS	CSC	Info2 – Envoyer un ETPS pour chaque VE
3	La CS est informée des incitations reçues du CSMS	La CS informe tous les SAVE des incitations en cours. Le VE peut décider ou pas de profiter des incitations.	CS		

Informations échangées

Informations échangées			
Informations échangées, ID	**Nom des informations**	**Description des informations échangées**	**Exigence, R-ID**
Info1	Le GR transmet la PRE au CSMS	PRE	
Info2	Transmettre des ETP à chaque VE	ETP pour chaque VE affecté	

Exigences

Exigences		
R-ID d'exigence	**Nom de l'exigence**	**Description de l'exigence**
Req1	Échange d'informations	À chaque réception d'un message d'incitation provenant d'un SA, le CSMS doit transférer au CSC les informations appropriées afin que la CS informe tous les SAVE de l'incitation.

8.2.5 Échange d'informations CSMS – GR à l'initiative du CSMS

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E3	Services de transfert d'énergie	Échange d'informations CSMS – GR à l'initiative du CSMS

Domaine d’application et objectifs du cas d'utilisation

Domaine d’application et objectifs du cas d'utilisation	
Domaine d'application	Décrire l'échange d'informations entre le CSMS (local ou en nuage) et le GR. Le CEM est responsable de la gestion de l'énergie derrière un SGCP (dans un bâtiment ou une maison, par exemple). Le CSMS est responsable de la gestion d'une ou de nombreuses bornes de charge installées derrière un point de connexion au réseau électrique (dans un bâtiment ou une maison, par exemple). Le CEM optimise l'attribution d'énergie et de puissance entre les ressources (charge, stockage et systèmes de production). L'une des ressources est l'infrastructure de charge gérée par un CSMS. Le CEM définit des limites de puissance pour le CSMS, par l’intermédiaire du GR responsable d’une zone du site de charge. Le CSMS optimise les transferts d’énergie de mobilité électrique sur la base des limites de puissance CEM, des besoins de mobilité électrique, ainsi que des conditions contractuelles et de la logique métier. NOTE Ce cas d'utilisation décrit un échange de messages déclenché par le CSMS. Le cas d'utilisation "Échange d'informations RM – CSMS à l'initiative du GR" décrit la situation inverse.
Objectif(s)	Objectif: Le CSMS et le GR échangent des informations concernant les limites de puissance et les plans de transfert d’énergie agrégés. Cet échange d'informations a pour objet: – pour le CSMS, d'optimiser les besoins de mobilité électrique tout en tenant compte des besoins des acteurs secondaires; – pour le CEM (par l’intermédiaire du GR), d’optimiser l’utilisation de l’énergie dans les locaux compte tenu des contraintes de puissance et d'énergie du CSMS.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d’utilisation décrit l’échange d'informations entre le CSMS et le GR à l’initiative du CSMS
Description complète
Le CEM et le CSMS maintiennent une boucle d'événement qui surveille les modifications apportées aux contraintes d'énergie ou de puissance dans leur domaine d'application respectif. Le CSMS calcule de manière constante l’AETP sur la base des informations qu’il échange avec le CSC (et les SAVE associés). Si cet AETP ne convient pas à la PRE existante définie par le GR, le CSMS calcule alors les nouvelles contraintes de puissance et d’énergie qui permettent l’adaptation du plan de transfert d’énergie, et: 1) le CSMS informe le GR de ses nouvelles contraintes de puissance et d’énergie; 2) le GR répond au CSMS par l’envoi d’une PRE mise à jour qui satisfait à ses contraintes; 3) après communication des ETP appropriés aux SAVE concernés, le CSMS informe le GR de l’existence du nouvel AETP.

Conditions de cas d'utilisation

Conditions préalables	
1	Le CSMS et le GR ont établi une communication digne de confiance.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Échange d'informations entre le CSMS et le GR	Le CSMS et le GR échangent des messages dans le cas d'un événement externe susceptible de modifier le plan de transfert d'énergie agrégé actuel du CSMS. NOTE Des seuils peuvent être appliqués à un événement pour éviter que de petites variations n'envahissent l'échange de messages CSMS - GR avec des messages fréquents. Voir aussi 8.2.3 (cas d'utilisation de charge intelligente) pour une description des informations échangées entre le GR, le CSC et le CSMS.	CSMS, GR, CS	Conditions de fin: en cas de succès: – nouvelle PRE et nouveau AETP en vigueur. en cas d'échec: (peut être dû à des problèmes de communication entre le GR et le CSMS) – le CSMS relance la communication avec le GR.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	le CSMS informe le GR des nouvelles contraintes de puissance et d'énergie	Le CSMS transmet les nouvelles contraintes de puissance et d'énergie au GR.	CSMS	GR	Info1 – Le CSMS transmet les nouvelles contraintes de puissance et d'énergie au GR.
2	Le GR obtient la PRE du CEM	Le CEM détermine la nouvelle PRE et en informe le GR. Il s'agit d'un processus interne du CEM qui ne relève pas du domaine d'application.	CEM, GR		
3	Le GR transmet une nouvelle PRE au CSMS	Le GR transmet au CSMS la nouvelle PRE	GR	CSMS	Info2 – Le GR transmet la PRE au CSMS
4	Le CSMS optimise l'ETP pour chaque VE	Le CSMS calcule un nouveau plan de transfert d'énergie pour chaque SAVE concerné par la nouvelle enveloppe de plages de puissance et le communique au(x) CS concerné(s). Voir 8.2.3 (cas d'utilisation de charge intelligente) pour les étapes non liées à une communication GR-CSMS.	CSMS		
5	Le CSMS calcule l'AETP et le transfère au GR	– Le CSMS agrège les plans de transfert d'énergie. – Le CSMS met à jour les transactions de transfert d'énergie correspondantes. – Le CSMS transmet l'AETP au GR.	CSMS	GR	Info3 - Le CSMS envoie le plan de transfert d'énergie agrégé au GR

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS transmet les contraintes de puissance et d'énergie au GR.	Contraintes de puissance et d'énergie (plage des limites supérieure et inférieure)
Info2	Le GR transmet la PRE au CSMS	PRE
Info3	Le CSMS envoie l'AETP au GR	AETP

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Le CSMS informe le GR	Le CSMS doit mettre à jour le GR avec les nouvelles contraintes de puissance et d'énergie lorsque leurs modifications affectent le fonctionnement.
Req2	Obligation du GR	La PRE doit satisfaire aux toutes dernières contraintes de puissance et d'énergie communiquées.
Req3	Obligations du CSMS	L'ETP agrégé fourni par le CSMS doit demeurer dans la PRE reçue du GR.
Req4	Obligations du GR	À chacune de ses mises à jour par le CSMS, par l'ajout de nouvelles contraintes de puissance et d'énergie, le GR doit répondre par l'établissement d'une nouvelle PRE sans délai.

8.2.6 Échange d'informations CSMS – GR à l'initiative du GR

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E4	Services de transfert d'énergie	Échange d'informations GR – CSMS à l'initiative du GR

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Décrire l'échange d'informations entre le GR et le CSMS (local ou en nuage). Le CEM est responsable de la gestion de l'énergie derrière un SGCP (dans un bâtiment ou une maison, par exemple). Le CSMS est responsable de la gestion d'une ou de nombreuses bornes de charge installées derrière un point de connexion au réseau électrique (dans un bâtiment ou une maison, par exemple). Le CEM optimise l'attribution d'énergie et de puissance entre les ressources (charge, stockage et systèmes de production). L'une des ressources est l'infrastructure de charge gérée par un CSMS. Le CEM définit une PRE pour le CSMS, par l'intermédiaire du GR responsable d'une zone du site de charge. Le CSMS optimise les transferts d'énergie de mobilité électrique sur la base des besoins de mobilité électrique, des caractéristiques du SAVE et des conditions contractuelles. NOTE Ce cas d'utilisation décrit le message déclenché par le GR. Le cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du CSMS" décrit la situation inverse.
Objectif(s)	Objectif: Le CSMS et le GR échangent des informations concernant la PRE et l'ETP agrégé. Cet échange d'informations a pour objet: – pour le GR, d'optimiser l'utilisation de l'énergie dans la CSZ; – pour le CSMS, d'optimiser les besoins de mobilité électrique tout en tenant compte des contraintes du GR.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation particulier décrit l'échange d'informations entre le GR et le CSMS à l'initiative du GR
Description complète
Le CEM et le CSMS maintiennent une boucle d'événement qui surveille les modifications apportées aux conditions d'énergie et de puissance dans leur domaine d'application respectif. Lorsque le CEM informe le GR d'une modification des conditions d'énergie ou de puissance qui affecte la PRE efficace de sa zone du site de charge (par exemple, disponibilité d'une puissance plus ou moins importante dans la CSZ), alors: – le GR transmet une nouvelle PRE au CSMS qui satisfait encore autant que possible aux dernières contraintes de puissance et d'énergie transmises par le CSMS; – sur la base de la nouvelle PRE, le CSMS calcule les nouveaux ETP pour chaque VE concerné et en informe le CS (des algorithmes d'équilibrage des charges qui ne relèvent pas du domaine d'application peuvent être utilisés par le CSMS); – le CSMS informe le GR de l'existence du nouveau ETP agrégé.

Conditions de cas d'utilisation

Conditions préalables	
1	Le CSMS et le GR ont établi une communication digne de confiance.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Échange d'informations entre le GR et le CSMS	Dans le cas d'un événement externe susceptible de modifier la PRE actuelle, le GR transmet une nouvelle PRE au CSMS. Le CSMS modifie les ETP et l'AETP en conséquence. NOTE Des seuils peuvent être appliqués à un événement pour éviter que de petites variations n'envahissent l'échange de messages CSMS - GR avec des messages fréquents. Voir 8.2.3 (gestion de charge intelligente) pour une description des informations échangées entre le GR et le CSMS.	GR, CSMS	Conditions de fin: en cas de succès: – nouvelle PRE et nouveau AETP en vigueur. en cas d'échec: (peut être dû à des problèmes de communication entre le GR et le CSMS) – le CSMS relance la communication avec le GR.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le GR transmet une nouvelle PRE au CSMS	Le GR transmet au CSMS la nouvelle PRE	GR	CSMS	Info1 – Le GR transmet la PRE au CSMS
2	Le CSMS optimise l'ETP pour chaque VE	Le CSMS calcule un nouveau ETP pour chaque SAVE concerné par la nouvelle PRE et le communique au(x) CS concerné(s). Voir 8.2.3 (cas d'utilisation professionnelle de charge intelligente) pour les étapes non liées à une communication GR-CSMS.	CSMS		
3	Le CSMS calcule l'AETP et le transfère au GR	– Le CSMS agrège les ETP. – Le CSMS met à jour les transactions de transfert d'énergie correspondantes. – Le CSMS transmet l'AETP résultant au GR.	CSMS	GR	Info2 – Le CSMS envoie l'AETP au GR

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le GR transmet la PRE au CSMS	PRE
Info2	Le CSMS transmet l'AETP résultant au GR	AETP

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Le GR transmet la PRE au CSMS	Le GR doit transférer une nouvelle PRE au CSMS chaque fois que les conditions énergétiques du bâtiment ou de la CSZ sont susceptibles d'affecter le fonctionnement du CSMS.
Req2	Obligations du CSMS	L'AETP fourni par le CSMS doit demeurer dans la PRE reçue du GR

8.2.7 Variation de puissance déclenchée par le GRD

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E5	Services de transfert d'énergie	Variation de puissance déclenchée par le GRD

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Variation de puissance déclenchée par le GRD
Objectif(s)	Exécuter sans attendre le message de délestage reçu de la part du GRD.
Cas métier connexe(s)	Offre de services énergétiques

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Manière dont le CSMS applique le message de délestage provenant du GRD
Description complète
Différents services sont utilisés par le GRT, le GRD et les OF pour maintenir la stabilité et le fonctionnement du réseau électrique: réserve de fréquence, réglage de tension, demande-réponse, gestion des congestions, etc. Certains services sont automatiques (la fréquence, par exemple), d'autres font l'objet d'un programme de marché avec des jours ou des heures d'avance (DR, par exemple), et d'autres encore peuvent être obligatoires (le délestage par le GRD, par exemple). Un délestage se produit lorsque le GRD a des problèmes locaux dans la zone géographique du SGCP. Comme toutes les ressources de ce type, le GRD peut avoir installé un dispositif chargé de contrôler l'utilisation de la puissance en cas d'urgence. Ce cas d'utilisation prend pour hypothèse que ledit dispositif est capable de communiquer les messages de délestage du GRD au CEM. Le CEM calcule la part du délestage allouée à la zone du site de charge et informe le CSMS par l'intermédiaire du GR approprié. NOTE 1 Il est également techniquement possible que le serveur de l'OSR puisse recevoir les messages de délestage provenant du GRD. Cette situation ne relève pas du domaine d'application de ce cas d'utilisation. Consulter le cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du CSMS" pour de plus amples informations sur cette situation. NOTE 2 Le CSMS garde la trace de l'événement de délestage afin qu'il puisse être reflété dans le RSD et que l'utilisateur puisse être informé. NOTE 3 Dans des conditions électriques normales, le GRD n'envoie pas de messages de délestage. Un message de délestage envoyé par le GRD signifie que la zone géographique relève de conditions électriques anormales. Il est nécessaire d'appliquer le message de délestage afin de permettre au réseau de revenir à des conditions normales. Le CSMS doit gérer les messages de délestage provenant du GRD selon les étapes ci-dessous: 1) le CSMS reçoit un message du GR selon lequel un délestage de puissance (augmentation de la production ou réduction de la consommation) est exigé et selon lequel il est nécessaire que ce délestage commence sans attendre. Étant donné que le message de délestage provient d'un GRD, le GR indique que le délestage est obligatoire. Le message de délestage prend la forme d'une nouvelle PRE; 2) sur la base de la nouvelle PRE qui reflète les objectifs de délestage, de la puissance agrégée réelle et des besoins de mobilité, le CSMS calcule un nouveau ETP pour chaque VE; 3) le CSMS transfère au CSC les nouveaux ETP pour chaque VE, en indiquant que leur application est obligatoire; 4) le CS doit vérifier que les nouveaux ETP sont utilisés en appliquant toutes les contraintes possibles au SAVE (coupure des relais au besoin, par exemple); 5) le CSMS envoie l'AETP au GR.

Indicateurs de performance clés (IPC)

Indicateurs de performance clés			
ID	**Nom**	**Description**	**Référence aux objectifs de cas d'utilisation mentionnés**
1	Exécution du délestage	Propagation en kilowatts-heures (kWh) entre l'énergie du délestage/le bilan de puissance attribué au CSMS et la puissance/énergie efficace consommée ou produite au point de connexion de la CS.	Exécuter sans attendre le message de délestage reçu de la part du GRD.

Conditions de cas d'utilisation

Conditions préalables	
1	– Un CEM est présent et capable de recevoir des messages du GRD. – Un GR est présent.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Condition préalable	Post-condition
1	Réception du message de délestage	Le CSMS reçoit un message du GR selon lequel un délestage de puissance (augmentation ou réduction de la production ou réduction ou augmentation de la consommation) est exigé, et selon lequel il est nécessaire que ce délestage commence sans attendre.	CSMS, CS, GR		

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le GR envoie un message de délestage au CSMS	Un message de délestage, sous la forme d'une nouvelle PRE, est envoyé par le GR au CSMS, demandant une variation de puissance.	GR	CSMS	Info1– Le GR envoie un message de délestage au CSMS
2	Le CSMS reçoit et traite un message de délestage	Sur la base de la nouvelle PRE, le CSMS calcule les ETP. Cette activité ne relève pas du domaine d'application du présent document.			
3	Le CSMS envoie au CSC les nouveaux ETP	Le CSMS envoie les nouveaux ETP pour chaque VE concerné par le délestage.	CSMS	CSC	Info2– le CSMS envoie les nouveaux ETP au CSC
4	Le CSMS calcule l'AETP et le transfère au GR	– Le CSMS envoie l'AETP au GR. – Le CSMS met à jour les transactions de transfert d'énergie correspondantes.	CSMS	GR	Info3 – Le CSMS envoie l'AETP au GR

Informations échangées

Informations échangées			
Informations échangées, ID	**Nom des informations**	**Description des informations échangées**	**Exigence, R-ID**
Info1	Le GR envoie un message de délestage au CSMS	La nouvelle PRE à appliquer Paramètre qui indique que le délestage provient du GRD	
Info2	Le CSMS envoie des plans de transfert d'énergie au CSC	ETP	
Info3	Le CSMS envoie le plan de transfert d'énergie agrégé au GR	AETP	

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Nouveaux ETP	Le CSMS doit allouer un ETP à chaque VE sur la base d'une PRE, des besoins de mobilité et des caractéristiques du SAVE et du VE.
Req2	Délestage	Le CSMS doit informer la CS de la nature obligatoire des nouveaux ETP.
Req3	Informer le GR de l'état du délestage	Le CSMS doit envoyer le nouveau AETP au GR.

8.2.8 Relations entre les acteurs pendant une session V2G

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E6	Services de transfert d'énergie	Relations entre les acteurs pendant une session V2G

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Relations entre les acteurs pendant une session V2G
Objectif(s)	Décrire l'échange d'informations entre les acteurs engagés dans une session V2G
Cas métier connexe(s)	Offre de services énergétiques

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation décrit uniquement les relations entre les acteurs afin de configurer un service V2G. Il ne décrit pas les étapes nécessaires au fonctionnement du service côté CS.
Description complète
Description du cas d'utilisation: – le CEM reçoit un message de la part du GRD, de l'OF ou d'un autre SA qui demande que l'injection de l'énergie dans le réseau électrique puisse commencer. La demande peut contenir des limites en matière de puissance, d'énergie et de durée; – sur la base d'une instruction du CEM, le GR transmet au CSMS la nouvelle PRE qui reflète la demande d'injection (voir le cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du GR"); – sur la base de la nouvelle PRE, des besoins de mobilité, de l'état des contrats de l'OF et d'autres contraintes, le CSMS envoie au CSC une série de nouveaux ETP à l'intention des VE concernés; – chaque CS applique le plan de transfert d'énergie pour tous les VE concernés. NOTE 1 Le CSMS envoie uniquement des ETP pour chaque VE concerné, après réception par l'OSR de la confirmation de la validité du contrat de l'utilisateur concernant l'injection d'énergie dans le réseau électrique par un acteur secondaire. La vérification est assurée par l'OSR et ne relève pas du domaine d'application. NOTE 2 Une pré-configuration de la CS selon les règles locales obligatoires ou une mise à jour continue des fonctions du réseau électrique du SAVE selon les règles du marché est nécessaire.

Conditions de cas d'utilisation

Conditions préalables	
1	L'UVE accepte les sessions V2G: Les UVE des VE qui peuvent charger et décharger ont exprimé leur consentement au V2G à un SA (par exemple, un OF), ainsi que leurs besoins de mobilité (état de charge cible et heure de départ).
2	Les SAVE peuvent utiliser V2G: Les SAVE sont certifiés décharger l'énergie dans le réseau électrique.
3	Capacités de décharge du CS: La CS a la possibilité d'accepter l'énergie de décharge provenant du SAVE et détient des certifications à cet effet.
4	Les VE peuvent utiliser les transferts d'énergie bidirectionnels: Tout ou partie des VE peuvent charger et décharger.
5	Codes de réseau électrique: La CS peut satisfaire aux exigences locales en matière de code de réseau électrique.
6	Contrats: Les UVE qui participent au service V2G ont un contrat valide avec un OF.
7	Pour chaque VE, le CSMS obtient de l'OSR la permission opérationnelle qui indique si l'injection d'énergie dans le réseau électrique est possible ou non. Ce paramètre peut dépendre de la détection d'un contrat approprié, mais le mode de vérification effective du contrat ne relève pas du domaine d'application.

Présentation des scénarii

Conditions du scénario						
N°	**Nom du scénario**	**Description du scénario**	**Acteur primaire**	**Événement déclencheur**	**Condition préalable**	**Post-condition**
1	Relations entre les acteurs pendant une session V2G	Échange d'informations entre les acteurs pendant une session V2G	CSMS, CS	SA, GR		

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le CEM reçoit un déclencheur V2G	Le CEM reçoit un message de la part du GRD, de l'OF ou d'un autre SA selon lequel l'injection d'énergie dans le réseau électrique peut commencer. Le message contient les conditions de puissance et d'énergie, ainsi que la durée de l'épisode V2G. Le CEM envoie au GR les paramètres appropriés dans la CSZ correspondante.	SA	CEM, GR	
2	Le GR informe le CSMS de la nouvelle PRE.	Le GR informe le CSMS d'une nouvelle PRE. L'impact de la PRE peut influencer les plans de transfert d'énergie, car il est nécessaire d'injecter de la puissance dans le réseau électrique.	GR, CSMS	GR, CSMS	Voir le cas d'utilisation "Échange d'informations CSMS – GR à l'initiative du GR".
3	Le CSMS transmet au CSC les nouveaux ETP	Sur la base de la nouvelle PRE, des besoins de mobilité et de l'état des contrats de l'OF, le CSMS transmet au CSC les nouveaux ETP pour chaque VE indiqué par l'OSR comme capable de fonctionner sous V2G.	CSMS	CSC	Info1 – Envoyer un ETPS pour chaque VE
4	Le CSMS met à jour le code de réseau électrique dans le SAVE	Lorsqu'une mise à jour de la configuration des codes de réseau électrique d'un SAVE est nécessaire après l'étape 3, des paramètres doivent être fournis au CS responsable.	CSMS	CSC	Voir le cas d'utilisation "Surveiller une CS".

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Transmettre des ETP à chaque VE	ETP pour chaque VE affecté

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Informations pour le RSD	Pendant et à la fin de la session V2G, le CSC doit envoyer au CSMS les informations d'énergie nécessaires afin que l'OSR renseigne le RSD avec les éléments de chaque VE concerné ou non par l'épisode V2G.

8.2.9 Échange d'informations exigé pour assurer une commande de transfert d'énergie dynamique

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E7	Services de transfert d'énergie	Échange d'informations exigé pour assurer un contrôle de transfert d'énergie dynamique

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Description de l'échange d'informations de commande de transfert d'énergie dynamique CS-CSMS
Objectif(s)	– Permettre à la CS, au CSMS ou à un acteur secondaire de fournir un ETP – Preuve de service: Le CSMS a pour objectif de permettre le service en mode dynamique et de suivre le VE engagé dans une session en mode dynamique afin de collecter toute l'énergie transférée et garantir la preuve de service exigée par l'acteur secondaire qui a déclenché le mode de commande dynamique.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation décrit l'échange d'informations entre la CS et le CSMS lorsque certains VE sont engagés dans une commande de transfert d'énergie dynamique. Dans le cadre d'une commande de transfert d'énergie dynamique, le transfert d'énergie peut être contrôlé par un acteur secondaire comme un OF, ce qui produit un ETP mis à jour que le VE applique avec une stratégie du meilleur effort.
Description complète
Le mode de commande de transfert d'énergie dynamique peut servir à répondre rapidement aux variations des conditions externes. Ce type de commande est utile aux services de réseau électrique, mais également lorsque la maîtrise du rythme à grain fin du transfert d'énergie est nécessaire. Exemples de situations dans lesquelles la commande de transfert d'énergie dynamique peut être utilisée: – services auxiliaires (régulation de fréquences, injection réactive dans le réseau électrique…); – dans un environnement contraint imprévisible dans lequel le programme n'est pas optimal; – la commande de transfert d'énergie dynamique facilite un équilibrage des charges sur le site de charge. NOTE 1 Le CSMS peut commander le transfert d'énergie au moyen d'un ETP qualifié de dynamique (peut être booléen dans le message de transfert ETP). NOTE 2 Pour établir l'ETP, le CSMS peut utiliser les intrants d'un SA comme un OF par exemple. NOTE 3 Dans le cadre d'une commande de transfert d'énergie dynamique, un ETP transmis par le CSMS est considéré par le VE comme un plan d'objectifs de puissance à atteindre dans une stratégie du meilleur effort. NOTE 4 La commande de transfert d'énergie dynamique ne se limite pas au transfert d'énergie V2G ou bidirectionnel. Une simple charge peut également en bénéficier. NOTE 5 Le mode de contrôle effectif du SAVE ne relève pas du domaine d'application. Il peut s'effectuer par le mode de commande dynamique ISO 15118 ou la variation MLI, par exemple. EXEMPLE Dans une maison, le CEM peut procéder à un équilibrage des charges par le calcul en temps réel d'une PRE attribuée au CSMS afin de garder suffisamment d'énergie pour d'autres charges. **Description détaillée:** Lorsque des variations fréquentes des conditions de puissance exigent d'adopter la commande de transfert d'énergie dynamique, il est alors nécessaire que les VE qui souhaitent mettre en œuvre cette commande reçoivent des ETP adaptés.

Récit du cas d'utilisation
Pour ce faire, les étapes suivantes sont nécessaires: – le CSMS peut recevoir une PRE transmise par le GR, ou des contraintes transmises par l'intermédiaire de l'OSR ou générées de manière interne; – le CSMS traite la PRE ou les contraintes reçues et envoie à la CS les nouveaux ETP qui les traitent; – le CSMS configure la consignation de la CS. La CS peut être configurée spécifiquement pour permettre au CSMS de collecter les informations nécessaires pour assurer la preuve de service et les informations de l'utilisateur. Voir le cas d'utilisation "Surveiller une CS"; – le CSMS surveille l'état de la CS, des SAVE et, si possible, des VE engagés dans le transfert d'énergie dynamique; – le CSMS calcule l'AETP et le transfère au GR. NOTE 1 Le début du transfert d'énergie peut marquer le début des mesurages de puissance nécessaires à la preuve de service. Il déclenche également une nouvelle transaction de transfert d'énergie. NOTE 2 Le CSMS peut informer l'OSR de l'exécution d'une commande de transfert d'énergie dynamique avec les VE appropriés. NOTE 3 Il est nécessaire d'évaluer le point 5 en matière de largeur de bande. Il est nécessaire que l'IEC 63110 évite la procédure de communication et le fonctionnement lorsque la microgestion de la CS par le CSMS risque de saturer le flux de communication. NOTE 4 La commande de transfert d'énergie dynamique tente de suivre l'ETP au moyen d'une stratégie du meilleur effort.

Conditions de cas d'utilisation

Conditions préalables	
1	Identification: Un ou plusieurs VE sont engagés dans une session de service et peuvent avoir été autorisés pour le transfert d'énergie.
2	Capacité: Le VE et le SAVE prennent en charge la commande de transfert d'énergie dynamique.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Événement déclencheur
1	Échange d'informations lors de la commande de transfert d'énergie dynamique	Les informations nécessaires à une commande de transfert d'énergie dynamique	CSMS, CS	GR, CSMS ou SA

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations	Destinataire des informations	Informations échangées
1	Le CSMS reçoit les contraintes	Le CSMS peut recevoir une PRE transmise par le GR, ou des contraintes transmises par l'intermédiaire de l'OSR ou les générer de manière interne.	GR ou OSR	CSMS	Info1 – Le CSMS reçoit une PRE en provenance du GR ou de l'OSR
2	Le CSMS traite la PRE ou les contraintes reçues et envoie au CSC les nouveaux ETP.	– Pour chaque VE qui souhaite mettre en œuvre la commande de transfert d'énergie dynamique, le CSMS calcule un nouveau ETP fondé sur les contraintes précédentes. – Pour les VE non engagés dans la commande de transfert d'énergie dynamique, le CSMS peut calculer de nouveaux ETP compatibles avec la PRE. – Les ETP mis à jour sont envoyés à la CS. – La CS les exécute.	CSMS	CSC	Info2 – Le CSMS transmet les ETP à la CS
3	Le CSMS configure la consignation de la CS	La CS peut être configurée spécifiquement pour permettre au CSMS de collecter les informations nécessaires pour assurer la preuve de service et les informations de l'utilisateur.	CSMS	CSC	Voir le cas d'utilisation "Surveiller une CS".
4	La CS transmet l'état	Le CSMS surveille l'état de la CS, des SAVE et, si possible, des VE engagés dans le transfert d'énergie dynamique.	CSC	CSMS	Info3 – État du VE lors de la commande de transfert d'énergie dynamique
5	Le CSMS envoie l'AETP au GR	Le CSMS calcule l'AETP et le transfère au GR	CSMS	GR	Info4 – Le CSMS envoie l'AETP au GR

Informations échangées

Informations échangées			
Informations échangées, ID	**Nom des informations**	**Description des informations échangées**	**Exigence, R-ID**
Info1	Le CSMS reçoit une PRE	PRE	
Info2	Le CSMS transmet les ETP à la CS	ETP pour chaque VE concerné	
Info3	État de la CS lors de la commande de transfert d'énergie dynamique	Sur la base de la configuration de la CS (voir le cas d'utilisation "Surveiller une CS"), le CSMS collecte les informations nécessaires à l'OF, l'utilisateur et pour la preuve de service telles que les mesurages du compteur, la métrique de l'énergie des batteries, SOC.	
Info4	Le CSMS envoie l'AETP au GR	AETP	

Exigences

Exigences		
R-ID d'exigence	**Nom de l'exigence**	**Description de l'exigence**
Req1	Traçabilité	La permutation sur le mode de commande de transfert d'énergie dynamique d'un VE doit déclencher une nouvelle transaction de transfert d'énergie.
Req2	Traçabilité	Le lancement d'une commande de transfert d'énergie dynamique doit déclencher le point de départ de mesurages de puissance spécifiques de chaque SAVE approprié, qui fait partie intégrante de la preuve de service contenue dans le RSD.

8.2.10 Offrir un service de régulation de fréquence au moyen de mesurages de fréquence décentralisés

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
E8	Services de transfert d'énergie	Offrir un service de régulation de fréquence au moyen de mesurages de fréquence décentralisés

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Ce cas d'utilisation décrit l'échange d'informations entre le CSMS et la CS pour fournir des services de régulation de fréquence par des mesurages de fréquence locale. Pour ce faire, le CSMS fournit les paramètres de configuration à la CS. La CS lit la fréquence en local et régule sa puissance de charge/décharge en fonction de ce mesurage et des paramètres de configuration envoyés par le CSMS.
Objectif(s)	– Décrire les échanges d'informations entre le CSMS et la CS afin de permettre une régulation de fréquence fondée sur des mesurages de fréquence locale. – Satisfaire aux différentes exigences du GRT et du marché (y compris l'observabilité).

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation décrit l'échange de données entre la CS et le CSMS pour fournir des services de régulation de fréquence par des mesurages de fréquence locale
Description complète
Prévoir une régulation de fréquence au moyen de mesurages de fréquence décentralisés repose sur des mesurages de fréquence réalisés localement par la CS, par opposition à une mesure centralisée réalisée en un lieu donné pour l'ensemble du pays. Les étapes suivantes sont nécessaires à une régulation de fréquence décentralisée: – configuration du code de réseau électrique Le CSMS fournit à la CS des informations concernant les exigences de connexion au réseau local auxquelles elle doit se conformer (cette opération peut être effectuée une fois lors de l'installation et en cas de modifications); – paramètres techniques V2X La CS et le CSMS échangent des informations concernant les paramètres V2X techniques. Plus particulièrement, la CS fournit au CSMS ses limites techniques (dues à la fois aux limites du VE et de la CS) telles que, entre autres, une puissance de charge et de décharge maximale; – configuration de la régulation Le CSMS fournit à la CS les paramètres de configuration pour la régulation de fréquence décentralisée. Liste non exhaustive de ces paramètres: • référence de puissance; • table de puissance-fréquence; – offre de service de régulation de fréquence : • en temps réel, la CS lit la fréquence en local et adapte sa puissance de charge/décharge en fonction de la valeur de fréquence et des paramètres de configuration envoyés par le CSMS (entre autres fondés sur la référence de puissance et la table de puissance-fréquence actuellement valides); • en temps réel, la CS envoie des mesurages au CSMS à des fins d'observabilité (entre autres, la puissance active en courant alternatif et les mesures de fréquences avec une exactitude correcte et un court temps d'échantillonnage); • en temps réel, le CSMS peut mettre à jour les paramètres de configuration de la CS. – fin de la session de régulation de fréquence locale La CS et le CSMS peuvent mettre fin au service de régulation de fréquence locale. Pour mettre fin à la session de transfert d'énergie ou pour passer à une autre mode de commande.

Indicateurs de performance clés

Indicateurs de performance clés			
ID	**Nom**	**Description**	**Référence aux objectifs de cas d'utilisation mentionnés**
1	Service de régulation de fréquence	IPC du service de régulation de fréquence provenant des GRT, y compris, entre autres: • temps d'activation; • temps de réponse; • Exactitude de la réponse en puissance; • Exactitude de la régulation du statisme.	Satisfaire aux exigences du GRT et du marché
2	Observabilité	Fournir au GRT des données d'observabilité pertinentes	Satisfaire aux exigences du GRT et du marché

Conditions de cas d'utilisation

Conditions préalables	
1	Le VE et la CS sont engagés dans une session de transfert d'énergie V2X (compatible V2X) à l'aide du mode de commande de transfert d'énergie dynamique.
2	La CS et le CSMS sont engagés dans une session de transfert d'énergie V2X (compatible V2X).
3	La CS et le CSMS sont engagés dans un mode de régulation de fréquence décentralisée locale.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Événement déclencheur
1	Offre de régulation de fréquence décentralisée	Les informations nécessaires à un service de régulation de fréquence décentralisée	CSMS, CS	SA

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations	Destinataire des informations	Informations échangées
1	La CS reçoit des exigences de connexion au réseau électrique local	La CS reçoit des exigences de connexion au réseau électrique local de la part du CSMS. Les exigences de connexion au réseau électrique local peuvent être fournies de différentes façons: le CSMS peut envoyer des noms ou des valeurs de paramètres normalisés	CSMS	CSC	Info1 – Exigences de connexion au réseau électrique local
2	Le CSMS reçoit les paramètres de charge/décharge V2X	Le CSMS reçoit les paramètres de charge/décharge V2X de la part de la CS	CS	CSMS	Info2 – Paramètres de charge/décharge V2X
3	La CS reçoit les paramètres de configuration	La CS reçoit les paramètres de configuration de la régulation de fréquence locale, y compris (entre autres): • référence de puissance; • table de puissance-fréquence.	CSMS	CSC	Info3 – Paramètres de configuration de régulation de fréquence
4	Offre de service de régulation de fréquence décentralisée	– En temps réel, la CS lit la fréquence en local et adapte sa puissance de charge/décharge en fonction de la valeur de fréquence et des paramètres de configuration envoyés par le CSMS. – En temps réel (de l'ordre de 1 s) la CS envoie des mesurages au CSMS à des fins d'observabilité (entre autres, la puissance active en courant alternatif avec une exactitude correcte et un court temps d'échantillonnage). – En temps réel (de l'ordre de 1 min), le CSMS peut mettre à jour les paramètres de configuration de la CS.	CSMS, CSC	CSMS, CSC	Info3 – Paramètres de configuration de régulation de fréquence Info4 – Début de la session de régulation de fréquence Info5 – Données d'observabilité

Informations échangées

Informations échangées			
Informations échangées, ID	**Nom des informations**	**Description des informations échangées**	**Exigence, R-ID**
Info1	Exigences de connexion au réseau électrique local	– Soit un nom normalisé – Soit des paramètres de connexion au réseau électrique local.	
Info2	Paramètres de charge/décharge V2X	Paramètres de charge/décharge du VE et de la CS et limitations, comprenant éventuellement, entre autres: – la puissance de charge minimale; – la puissance de charge maximale; – la puissance de décharge minimale; – la puissance de décharge maximale; – le courant de charge minimal; – le courant de charge maximal; – le courant de décharge minimal; – le courant de décharge maximal; – minVoltage; – maxVoltage; – evTargetEnergyRequest; – evMinEnergyRequest; – evMaxEnergyRequest; – minSoC; – maxSoC.	
Info3	Paramètres de configuration de la régulation	Paramètres de configuration de l'algorithme de régulation locale de la CS, comprenant éventuellement, entre autres: – la référence de puissance; – la table de puissance-fréquence.	
Info4	Début de la session de régulation de fréquence	Mode de régulation de fréquence	
Info5	Données d'observabilité	Données utilisées par l'OF (pour le compte du GRT) pour vérifier l'offre de service, comprenant éventuellement, entre autres: – les mesurages de fréquence; – les mesurages de puissance active en courant alternatif; – le niveau d'énergie réel des VE (kWh); – le SoC des VE.	

Exigences

Exigences		
R-ID d'exigence	**Nom de l'exigence**	**Description de l'exigence**
Req1	Prise en charge de la commande de transfert d'énergie dynamique	Le mode de commande dynamique pour l'ISO 15118 ou équivalent pour une autre norme doit être pris en charge par la CS et le CSMS.
Req2	Prise en charge du mode de régulation de fréquence décentralisée	Le mode de régulation de fréquence décentralisée doit être pris en charge par la CS et le CSMS.
Req3	Traçabilité	Les variations du mode de commande de transfert d'énergie doivent déclencher une nouvelle transaction de transfert d'énergie.
Req4	Observabilité	L'activation d'une commande dynamique doit déclencher le point de départ des mesurages et de la transmission de puissance et de fréquence, sur chaque SAVE ou au niveau de la CS, qui fait partie intégrante du processus d'observabilité.
Req5	Exigences de connexion au réseau électrique	Le CSMS doit informer la CS des exigences de connexion au réseau électrique.
Req6	Paramètres de régulation de fréquence	Le CSMS doit envoyer les paramètres de régulation de fréquence à la CS.

8.3 Cas d'utilisation du domaine de gestion de la CS

8.3.1 Généralités

Les cas d'utilisation du domaine de gestion de la CS font partie intégrante du cycle de vie de fonctionnement de la CS.

Ils décrivent principalement trois types d'activité:

– configuration initiale;
– maintenance-diagnostic;
– mise hors service.

À l'exception de la maintenance et des diagnostics, la plupart de ces cas d'utilisation sont exécutés lorsque la CS ne fonctionne pas.

8.3.2 Liste des cas d'utilisation du domaine de gestion de la CS

Le Tableau 5 présente la liste et une brève description des cas d'utilisation du domaine de gestion de la CS.

Tableau 5 – Liste des cas d'utilisation du domaine de gestion de la CS

ID	Cas d'utilisation	Brève description	Cycle de vie / Séquence
M1	Découvrir la configuration de la CS	Le CSMS découvre la configuration d'une CS.	Exploitation / Maintenance
M2	Mettre à jour les propriétés des composants d'une CS	Mettre à jour les propriétés des composants d'une CS	Exploitation / Maintenance
M3	Surveiller une CS	Le CSMS surveille certains paramètres d'une CS particulière.	Exploitation / Maintenance

ID	Cas d'utilisation	Brève description	Cycle de vie / Séquence
M4	Mettre à jour le micrologiciel d'une CS	Le CSMS met à jour à distance le logiciel/micrologiciel d'une CS, y compris les éléments sous le contrôle de cette dernière.	Exploitation / Maintenance
M5	Redémarrer une CS	Le CSMS envoie une demande de réinitialisation à la CS.	Exploitation / Maintenance
M6	Le CSMS définit les informations à présenter à l'utilisateur	Le CSMS demande à la CS de présenter les informations à l'UVE.	Exploitation / Maintenance
M7	Le CSMS définit les critères de journalisation	Le CSMS demande à la CS de définir les critères de journalisation qui peuvent être extraits ultérieurement pour analyse.	Exploitation / Maintenance
M8	Extraire les informations de journalisation de la CS	Le CSMS demande à la CS les informations consignées.	Exploitation / Maintenance
M9	Fourniture d'un code de défaut	En cas de défaillance, la CS envoie au CSMS les informations détaillées relatives à la défaillance.	Exploitation / Maintenance
M10	Suppression des informations déclenchée auprès du CSMS par un SA	Supprimer les données stockées dans le SAVE, le CS. L'OSR, l'UVE ou l'entretien interne peut déclencher la suppression.	Exploitation / Maintenance
M11	Annulation de l'enregistrement de la CS	Annulation de l'enregistrement de la CS dans le CSMS.	Exploitation/Mise hors service
M12	Migration de la CS	Migration de la CS vers différents CSMS dans le même OSR	Exploitation/Configuration initiale
M13	Connexion de la CS	Connecter une nouvelle CS ou une CS après une maintenance majeure du CSMS.	Exploitation/Configuration initiale
M14	Fourniture du certificat d'AC	La CS peut extraire du CSMS les certificats RootCA et leurs métadonnées pour authentifier le VE et le CSMS.	Exploitation / Maintenance
M15	Messages de réponse OCSP ISO 15118	La CS peut régulièrement recevoir les données de réponse OCSP pour la chaîne de certificats de CS de la part du CSMS.	Exploitation / Maintenance
M16	Installation du certificat CS	Mettre à jour le certificat du dispositif sur la CS déclenchée par le CSMS ou par elle-même.	Exploitation / Maintenance
M17	Installer le certificat du CSMS local	Mettre à jour le certificat du dispositif sur le CSMS local déclenché par le CSMS ou par lui-même.	Exploitation / Maintenance
M18	Installation du certificat CS avec des paires de clés créées à l'extérieur	Mettre à jour le certificat du dispositif sur la CS déclenchée par le serveur du CSMS ou de l'AC ou par lui-même.	Exploitation / Maintenance
M19	Révocation du certificat	Gérer les révocations de certificats des acteurs primaires et des AC	Exploitation / Maintenance

8.3.3 Découvrir la configuration de la CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M1	Gestion de la CS	Découvrir la configuration de la CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Le CSMS découvre la configuration d'une CS.
Objectif(s)	Objectif: Découvrir la configuration d'une CS.
Cas métier connexe(s)	Gérer la CS: le CSMS gère la CS.

Récit du cas d'utilisation

Récit du cas d'utilisation
Description complète
1) Le contexte de ce cas d'utilisation peut être le suivant: a) une CS est inscrite sur un réseau CSMS pour la première fois; b) par suite d'un événement connu qui peut être à l'origine de la modification de certains paramètres CS (par exemple, visite d'un technicien pour enquêter/réparer/mettre à niveau l'équipement, le câblage, etc.); c) déplacement d'une CS vers un autre site qui peut avoir un jeu de paramètres différent pour la connexion au réseau; d) le CSMS détecte une anomalie apparente dans les réponses d'une CS à d'autres messages, qui peut indiquer une incohérence entre son modèle de topologie de charge CS et le matériel actuel. 2) Le CSMS envoie une demande de découverte de configuration à la CS. Il peut s'agir d'options de paramètres qui permettent de spécifier/limiter la capacité en consignant: a) le domaine d'application des services à consigner; b) l'intensité des informations détaillées des services; c) les capacités disponibles possibles et/ou réelles. 3) La CS prépare le rapport. a) Pour des bornes de charge de haut niveau, le contrôleur interne de la CS procède à une introspection de son propre modèle d'objet et prépare le rapport correspondant. b) Pour les CS de base qui présentent peu ou pas de configurabilité, il peut ne pas y avoir d'introspection, et le rapport peut être un message fixe déjà établi qui est toujours le même (pour une marque/un modèle/un micrologiciel donnés). 4) La CS envoie le rapport de configuration au CSMS. Il s'agit d'une étape distincte qu'il convient de réaliser de manière asynchrone, car un processus d'introspection complet peut prendre énormément de temps (sur un modèle d'objet important/complexe, par exemple).

Conditions de cas d'utilisation

Conditions préalables	
1	La CS a accepté l'autorité du CSMS pour modifier sa configuration.
2	Le CSMS a enregistré la CS.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Événement déclencheur	Condition préalable
1	Découvrir la liste de tous les paramètres avec leurs attributs	Il est nécessaire que le CSMS découvre les services qui peuvent être (et/ou sont) fournis par un CS particulier.	CS CSMS	L'OSR demande au CSMS d'extraire la configuration d'une CS.	– La CS est reliée au CSMS. – La CS a été acceptée dans le réseau par le CSMS.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le CSMS envoie une demande de rapport de découverte de configuration à la CS	Il peut s'agir d'options qui permettent de spécifier/limiter la consignation: • le domaine d'application des services à consigner; • l'intensité des informations détaillées des services; • les paramètres disponibles possibles et/ou réels.	CSMS	CSC	Info1 – Le CSMS demande une découverte de configuration au CSC
2	La CS envoie le rapport de découverte de configuration au CSMS.	La CS répond au CSMS avec l'état du processus de consignation. La réponse contient le type de réponse formulée (immédiatement ou avec un retard). – En cas de réponse immédiate, la CS envoie le rapport préparé au CSMS. – En cas de retard, la CS informe le CSMS de la progression de l'élaboration du rapport	CSC	CSMS	Info2 – La CS envoie le rapport de découverte.
3	Le CSMS reçoit le rapport de découverte de configuration	Cette configuration peut être conservée dans un CSMS local.	CSMS		

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS demande une découverte de configuration à la CS.	Il peut s'agir d'options de paramètre qui permettent de spécifier/limiter la consignation: – le domaine d'application des services à consigner; – l'intensité des informations détaillées des services; – les paramètres disponibles possibles et/ou réels; – l'URI de destination; – les clés de chiffrement.
Info2	La CS envoie le rapport de découverte.	Réponse immédiate ou différée. Le rapport de découverte contient toute la description d'objet de la CS.

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Demande de base	La CS doit accepter au moins une demande minimale/de base de la part du CSMS pour décrire la configuration de ses paramètres.
Req2	Rapport valide	La CS doit envoyer un rapport de configuration valide au CSMS pour toutes les demandes qu'elle accepte, lorsqu'il lui est demandé de procéder ainsi.
Req3	Échanges de messages asynchrones	Les messages impliqués dans le processus de découverte doivent prendre en charge les échanges de messages asynchrones. Il s'agit de vérifier que la CS et le CSMS traitent correctement une demande qui donne lieu à une longue réponse et à une liste volumineuse.
Req4	Le rapport reflète le modèle d'objet CS	Le rapport de configuration doit correctement refléter le modèle d'objet CS et les services réels disponibles et/ou actifs, selon le cas.
Req5	Aucune interruption du service de charge pendant la préparation et la transmission du rapport	La CS doit maintenir le transfert d'énergie pendant l'élaboration du rapport de configuration.

8.3.4 Mettre à jour les propriétés des composants d'une CS

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M2	Gestion de la borne de charge	Mettre à jour les propriétés des composants d'une CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Les composants d'une CS peuvent avoir des propriétés qui permettent des modifications de leurs valeurs. Ce cas d'utilisation définit comment appliquer ces modifications.
Objectif(s)	Objectif: Le CSMS souhaite personnaliser le comportement d'une CS par la modification de certaines propriétés inscriptibles des composants existants.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Ce cas d'utilisation décrit comment le CSMS peut modifier les valeurs de propriétés des composants de CS.
Description complète
Le CSMS a découvert plus tôt dans le processus les composants et les propriétés de niveau racine qu'une CS expose (voir le cas d'utilisation "Découvrir la configuration de la CS") Le CSMS a identifié les propriétés inscriptibles dont il est nécessaire de modifier les valeurs. Lorsque plusieurs valeurs sont soumises à une modification simultanée, elles forment une action de mise à jour atomique, dans laquelle toutes les modifications sont réalisées, ou aucune d'entre elles n'est appliquée. Le CSMS envoie une demande à la CS qui contient la liste des parcours clés qui identifient les propriétés ciblées, ainsi que les nouvelles valeurs. La CS valide les parcours clés et les nouvelles valeurs par rapport aux règles d'accès et aux exigences de valeurs (type, plage de valeurs, etc.) des propriétés ciblées. Lorsque toutes les modifications sont valides, la CS applique alors les modifications. La CS envoie alors une réponse au CSMS qui soit confirme la mise à jour des valeurs, soit consigne les erreurs détectées, ainsi que les explications associées.

Conditions de cas d'utilisation

Conditions préalables	
1	– Le CSMS et la CS ont établi une communication digne de confiance. – Le CSMS a exécuté le cas d'utilisation "Découvrir la configuration de la CS"

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Le CSMS envoie à la CS une liste des mises à jour de propriétés nécessaires	Le CSMS envoie à la CS une liste des mises à jour de propriétés nécessaires et la CS les applique alors ou renvoie un message d'erreur.	CSMS	Conditions de fin: en cas de succès: – les propriétés de la CS sont mises à jour selon les valeurs. en cas d'échec: – les propriétés de la CS reflètent toujours les anciennes valeurs

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le CSMS envoie une demande de mise à jour	Le CSMS envoie à la CS la liste des parcours clés pour les propriétés des composants de CS ciblées et leurs nouvelles valeurs	CSMS	CS	Info1 – Le CSMS envoie une demande de mise à jour
2	La CS valide une demande de mise à jour	La CS valide les modifications demandées par rapport aux règles d'accès de chaque propriété et aux options de choix de valeurs ou de plages de valeurs acceptables. Lorsque la liste entière des mises à jour demandées est valide, toutes les modifications sont alors appliquées de manière atomique cohérente. En cas d'échec de la validation, la CS compile alors une liste des erreurs et des descriptions associées.	CS		
3	La CS confirme la demande de mise à jour	La CS répond par l'envoi d'une confirmation de succès ou d'une liste des erreurs de validation et des descriptions associées qui permettent au CSMS d'identifier les propriétés concernées.	CS	CSMS	Info2 – La CS confirme la demande de mise à jour

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Liste des mises à jour	Liste qui contient les parcours clés pour toutes les propriétés qu'il convient de mettre à jour, ainsi que les nouvelles valeurs pour chaque propriété ciblée. Les valeurs peuvent être simples ou complexes.
Info2	Confirmation de mise à jour	Consignation de "succès" ou d'une liste d'erreurs de validation pour chaque propriété concernée, ainsi que les descriptions d'erreurs associées. Les descriptions d'erreurs sont réservées au débogage et il convient de ne pas les limiter à un texte simple uniquement. Erreurs possibles: propriété non inscriptible, keyPath ne correspond à aucune propriété, la nouvelle valeur ne correspond pas au type exigé, la nouvelle valeur value se situe en dehors de la plage admise ou de l'ensemble de choix admis, etc.

Exigences

Exigences (facultatives)		
R-ID d'exigence	**Nom de l'exigence**	**Description de l'exigence**
Req1	Modification atomique	La CS doit mettre à jour toutes les propriétés de manière cohérente.
Req2	Validation	La CS doit consigner toutes les erreurs de validation.

8.3.5 Surveiller une CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M3	Gestion de la CS	Surveiller une CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Le CSMS surveille certains paramètres d'une CS particulière.
Objectif(s)	Le CSMS souhaite surveiller certains paramètres d'une CS presque en temps réel afin d'obtenir des informations relatives au fonctionnement de la CS et savoir à quel moment elle fonctionne hors des plages normales.
Cas métier connexe(s)	

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Le CSMS surveille certaines valeurs de paramètres d'une CS
Description complète
Comme les SAVE/CS sont déployés en de nombreux emplacements différents, il peut s'avérer utile de posséder certains moyens qui permettent de surveiller les SAVE en ce qui concerne leur fonctionnement et leur manipulation. Pour surveiller un SAVE particulier, le CSMS paramètre en premier lieu les conditions (par exemple, seuils pour certaines valeurs). La CS informe ensuite le CSMS de tous les événements relatifs à ce SAVE particulier. Un événement est un ensemble fixe périodique de valeurs de paramètre ou une alerte relative à certaines valeurs de paramètres qui dépassent des seuils. Les étapes suivantes constituent un moyen possible de préparer la surveillance: – le CSMS demande à la CS de définir ou d'ajuster des seuils ou intervalles pour les paramètres sélectionnés; – la CS répond en indiquant si elle peut surveiller les paramètres sélectionnés et informer le CSMS des événements; – pendant le fonctionnement normal, la CS informe le CSMS que les valeurs de paramètre se situent dans les limites des seuils ou inversement.

Conditions de cas d'utilisation

Conditions préalables	
1	– La CS est connectée lorsque les paramètres de surveillance sont définis par le CSMS. – La CS est connectée lorsque les messages d'événement de surveillance sont envoyés. – La liste des composants décrits dans le modèle d'objet avec la liste des paramètres sont connues du CSMS.

Présentation des scénarii

Conditions du scénario						
N°	**Nom du scénario**	**Description du scénario**	**Acteur primaire**	**Événement déclencheur**	**Condition préalable**	**Post-condition**
1	Surveiller une CS	1) Le CSMS demande à la CS de définir ou d'ajuster des seuils ou intervalles pour les paramètres sélectionnés. 2) La CS répond en indiquant si elle peut surveiller les paramètres sélectionnés et informer le CSMS des événements. 3) Pendant le fonctionnement normal, la CS informe le CSMS que les valeurs de paramètre se situent dans les limites des seuils ou inversement.	CSMS, CS			Conditions de fin: Succès: – les limites de fonctionnement sont définies par le CSMS; – la CS envoie des informations au CSMS lorsque les valeurs dépassent les seuils; – la CS envoie des informations au CSMS lorsque les valeurs ne dépassent plus les seuils; – le CSMS est informé des paramètres qui peuvent être surveillés par la CS, et éventuellement de leurs limites, telles qu'elles sont recommandées par le CSM; – la CS prend une photo instantanée des paramètres sélectionnés et la transmet sur demande au CSMS. Échec: – les limites de fonctionnement ne sont pas définies par le CSMS; la CS utilise les limites par défaut définies par le CSM; – la CS ne peut pas appliquer les paramètres ou limites du CSMS. La CS informe le CSMS de cette condition défaillante avec une description explicite de l'erreur.

Analyse étape par étape du scénario

N° d'étape	**Nom du processus/de l'activité**	**Description du processus/de l'activité**	**Producteur des informations (acteur)**	**Destinataire des informations (acteur)**	**Informations échangées (ID)**	**Exigence, R-ID**
1	Le CSMS demande à la CS d'ajuster les limites de paramètres	Le CSMS demande à la CS de définir ou d'ajuster des seuils ou intervalles pour les paramètres sélectionnés.	CSMS	CSC	Info1 - Paramètres demandés par le CSMS pour la surveillance de la CS	
2	La CS accuse réception et informe	La CS répond en indiquant si elle peut surveiller les paramètres sélectionnés et informer le CSMS des événements.	CSC	CSMS	Info2 – liste des paramètres surveillés par la CS	

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)	Exigence, R-ID
3	La CS informe le CSMS d'un événement de surveillance	Pendant le fonctionnement normal, la CS informe le CSMS que les valeurs de paramètre se situent dans les limites des seuils ou inversement.	CSC	CSMS	Info3 - Liste des paramètres CS et des valeurs qui dépassent les seuils	Req1, Req2, Req3, Req4
4	Extraire l'événement de surveillance	Le CSMS reçoit l'événement de surveillance correspondant à des valeurs de paramètre qui se situent dans les limites des seuils ou inversement.	CSMS			

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Paramètres demandés par le CSMS pour la surveillance de la CS	Seuils ou intervalles pour les paramètres sélectionnés
Info2	Liste des paramètres surveillés par la CS	Liste des paramètres surveillés par la CS
Info3	Liste des paramètres CS et des valeurs qui dépassent les seuils	Liste des valeurs de paramètre qui se situent dans les limites des seuils ou inversement.

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Événements	La CS doit envoyer les événements au CSMS.
Req2	Erreur ou mise en garde	La CS doit envoyer des informations au CSMS, en émettant une mise en garde ou une erreur lorsqu'une valeur de paramètre dépasse le seuil correspondant.
Req3	Erreur ou mise en garde résolue	La CS doit envoyer des informations au CSMS, en indiquant qu'une précédente mise en garde ou erreur est résolue lorsqu'une valeur de paramètre revient dans les limites de son seuil.
Req4	État périodique	La CS doit envoyer une notification pour chaque intervalle de valeurs périodiques.

8.3.6 Mettre à jour le micrologiciel d'une CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	Zone(s)/Domaine(s)	Nom du cas d'utilisation
M4	Gestion de la CS	Mettre à jour le micrologiciel d'une CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Logiciel ou micrologiciel distant d'un élément de la CS
Objectif(s)	Le CSMS souhaite mettre à jour le logiciel/micrologiciel d'une CS, y compris les éléments qui sont sous le contrôle de la CS (SAVE, partie interne du SAVE, contrôleur de communication, etc.).
Cas métier connexe(s)	Gérer la CS: Le CSMS gère la CS.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Mettre à jour le micrologiciel d'une CS ou un de ses composants.
Description complète
– La borne de charge est informée par le CSMS qu'une nouvelle mise à jour de micrologiciel ou de logiciel est disponible pour un sous-composant spécifique avec un identifiant connu. Le CSMS fournit: • l'URL vers le module de mise à jour ou le module de mise à jour lui-même; • les conditions d'application de la mise à jour (priorité, durée, par exemple); • les informations pertinentes relatives au niveau de confiance dans le mécanisme de livraison du module de mise à jour (certificat pour le serveur hôte, signature du module de mise à jour et justificatifs d'identité à utiliser par la CS, etc.). – En cas de livraison hors bande, la CS commence à télécharger le logiciel en fonction du programme communiqué. – Dès que la CS est prête à installer la mise à jour, elle en informe le CSMS. – Le CSMS envoie un message à la borne de charge pour lui demander de lancer immédiatement le processus de mise à jour du logiciel ou de le commencer selon le programme communiqué. – La CS confirme ou pas la bonne réception du module de mise à jour. – Le CSMS demande à la CS d'installer la mise à jour. – La CS informe le CSMS de l'état final de la mise à jour. NOTE Le mécanisme de mise à jour du logiciel et du micrologiciel peut être très compliqué et peut dépendre de nombreux facteurs. Pour n'en citer que quelques-uns: • complexité différente du logiciel du chargeur (borne de charge rapide en courant continu/borne de charge murale domestique) et architecture différente (type de système d'exploitation, pile de logiciels, etc.); • type de plateforme matérielle SECC du chargeur (système d'exploitation ou intégré, par exemple) et sa capacité de calcul ou de stockage; • fabricant du chargeur; • modem ou modules de communication; • autres. Par conséquent, le mécanisme de mise à jour de logiciel interne à l'intérieur de la CS elle-même ne relève pas du domaine d'application de l'IEC 63110 (toutes les parties).

Conditions de cas d'utilisation

Conditions préalables	
1	La mise à jour a été vérifiée et son installation approuvée par l'OSR. Moyens de vérification: – l'OSR a validé le comportement du module par des essais internes; – l'intégrité du module a été vérifiée et son installation approuvée.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Le CSMS informe la CS qu'un nouveau micrologiciel est disponible pour le transfert	La borne de charge est informée par le CSMS qu'une nouvelle mise à jour de micrologiciel ou de logiciel est disponible pour un sous-composant spécifique avec un identifiant connu. Le CSMS précise également les conditions d'installation, comme la priorité, la durée, etc.	CS, CSMS	
2	Le CSMS envoie le module à la CS	En cas de livraison dans la bande, le CSMS envoie le module comme partie intégrante du message de charge utile.	CS, CSMS	
3	La CS commence à télécharger le logiciel	En cas de livraison hors bande, la CS récupère le module de micrologiciel à l'aide de l'URL fournie dans info1.		
4	La CS informe le CSMS que la mise à jour est prête à être installée	Après avoir vérifié que le téléchargement s'est terminé sans erreur de transmission, la CS informe le CSMS que le nouveau micrologiciel/logiciel est prêt à être installé.	CS, CSMS	
5	Le CSMS demande à la CS d'installer la mise à jour dans les conditions spécifiées	Les conditions d'installation de la mise à jour peuvent être: – installer immédiatement; – installer la mise à jour sur un SAVE particulier uniquement lorsque la session de service correspondante est terminée; – lancer le processus de mise à jour du logiciel selon le programme communiqué.	CS, CSMS	
6	La CS informe le CSMS de l'état de la mise à jour	La CS informe le CSMS de la réussite ou de l'échec de la mise à jour. Les raisons de l'échec sont envoyées au CSMS.	CS, CSMS	Conditions de fin: – Le CSMS reçoit le message de la CS avec la version installée du logiciel; – Le CSMS reçoit le message de la CS selon lequel il n'est pas opérationnel; – Le CSMS déclare la CS non opérationnelle en raison d'une expiration du délai.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)	Exigence, R-ID
1	Le CSMS informe la CS qu'une mise à jour de micrologiciel est disponible.	Le message informe la CS de la disponibilité d'un nouveau micrologiciel. Les paramètres permettent à la CS de connaître les conditions et le domaine d'application de la mise à jour.	CSMS	CSC	Info1 – Mise à jour de micrologiciel disponible	Req1, Req2
2	Le CSMS envoie le module de mise à jour à la CS	Dans le cas d'une livraison dans la bande uniquement	CSMS	CSC	Info2 – Envoi du module de mise à jour	
3	Téléchargement du micrologiciel	Le CSMS télécharge le module de micrologiciel selon le lien donné à l'étape 1	CSMS			
4	Chargement du micrologiciel	La CS charge le module de micrologiciel selon le lien donné à l'étape 1	CS			
5	Envoi de l'état de mise à jour au CSMS	La CS informe le CSMS de l'état de la mise à jour en attente	CSC	CSMS	Info3 – Envoi de l'état de mise à jour au CSMS	Req4
6	La CS informe le CSMS du résultat de la mise à jour	Après la mise à jour, la CS informe le CSMS de la réussite ou de l'échec de la mise à jour.	CSC	CSMS	Info3 – Envoi de l'état de mise à jour au CSMS	Req5, Req6, Req7

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Mise à jour de micrologiciel disponible	– Identifiant de la mise à jour. – Sous-composant objet de la mise à jour. – Conditions de la mise à jour (priorité ou durée, par exemple). – La manière dont la mise à jour est disponible: hors bande ou dans la bande. – En cas d'informations hors bande relatives à l'emplacement du module, le certificat pour le serveur hôte, la signature du module de mise à jour et les justificatifs d'identité à utiliser par la CS sont transmis.
Info2	Envoi du module de mise à jour	Module binaire à installer par la CS dans le sous-élément.
Info3	Envoi de l'état de mise à jour au CSMS	– État de la mise à jour. – Prêt pour l'installation immédiate. – Prêt pour l'installation à un certain moment ou lorsque la session de service en cours est terminée. – Mise à jour rejetée en raison d'une incompatibilité. – Mise à jour impossible en raison d'une erreur de transmission.

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Authentification de la source	La CS doit pouvoir authentifier la source du module.
Req2	Validation du rôle	La CS doit pouvoir valider le rôle de l'émetteur du message de mise à jour (le rôle doit être autorisé à procéder à des mises à jour de micrologiciel).
Req3	Le téléchargement doit reprendre après une erreur	En cas de problème de communication pendant le téléchargement du micrologiciel, il convient que la CS puisse reprendre le téléchargement de la partie manquante.
Req4	Valider la mise à jour	La CS doit vérifier si l'intégrité de la mise à jour du micrologiciel est compatible avec son état en cours et si elle est nécessaire (par exemple, déjà installée). Si ce n'est pas le cas, la CS doit informer le CSMS du rejet de la mise à jour et de la raison de ce rejet.
Req5	Retour à la version précédente en cas d'échec	Si des problèmes se sont produits lors du processus de mise à jour et que la nouvelle version n'a pas été installée, le système doit pouvoir revenir à la version précédente.
Req6	Version du micrologiciel	La CS doit envoyer au CSMS la version actuelle du logiciel à l'issue du processus de mise à jour, réussi ou pas.
Req7	Erreur irrécupérable	Si des problèmes se sont produits lors du processus de mise à jour, qu'ils ne peuvent pas être résolus par la borne de charge et le serveur de mise à jour distant et que le retour à la version précédente est impossible, mais que la borne de charge peut toujours communiquer avec le CSMS, ladite borne doit informer le CSMS qu'elle n'est pas opérationnelle en indiquant les codes de défaut et en donnant une description facultative de l'erreur.

8.3.7 Redémarrer une CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M5	Gestion de la CS	Redémarrer une CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Le CSMS demande à la CS de redémarrer
Objectif(s)	Objectif: redémarrage afin que la CS fonctionne selon un état prévisible connu

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Le CSMS demande à la CS de redémarrer
Description complète
Il est parfois nécessaire que le CSMS demande à la CS de redémarrer. Les raisons types sont les suivantes: – appliquer une modification de configuration après une migration; – utiliser de nouveaux certificats; – la CS est toujours capable de communiquer, mais ne fonctionne pas correctement. Ce cas d'utilisation définit 2 types d'actions: redémarrage forcé, redémarrage au ralenti. En cas de redémarrage forcé – Le CSMS envoie une demande de redémarrage forcé à la CS. – Le redémarrage a lieu à un moment donné ou après ce moment – La CS répond avec l'identifiant de l'activité de redémarrage – La CS redémarre son système même en cas de sessions de services actifs au moment indiqué ou après ce moment. En cas de redémarrage au ralenti – Le CSMS envoie une demande de redémarrage au ralenti à la CS. – Le redémarrage a lieu au moment ou après le moment (éventuellement) indiqué par le CSMS, et lorsqu'aucune session de service n'est active (par exemple, lorsque les VE ne transfèrent ni énergie ni données). – Dans le cas où aucun VE n'est connecté au SAVE • La CS confirme la demande avec l'identifiant de l'activité de redémarrage • La CS redémarre au moment indiqué ou après ce moment. – Dans le cas où un VE ou plus est (sont) connecté(s) au SAVE • La CS répond avec l'identifiant de l'activité de redémarrage • Le redémarrage a lieu lorsque plus aucun VE n'est connecté au SAVE, mais pas avant le moment indiqué NOTE 1 Le CSMS peut avoir une estimation de la durée de ce calendrier en regardant les ETP concernés. NOTE 2 Ce message de redémarrage peut être annulé par le message de compteur approprié avec l'identifiant pertinent de l'activité de redémarrage.

Conditions de cas d'utilisation

Conditions préalables	
1	Le CSMS sait quelle horloge de référence est utilisée pour déterminer le temps.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Condition préalable	Post-condition
1	Redémarrage	Le CSMS envoie à la CS une demande de redémarrage		

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le CSMS envoie une demande de redémarrage à la CS	Le CSMS demande: Redémarrage forcé Ou Redémarrage au ralenti Le CSMS peut fournir un moment ponctuel pour appliquer le redémarrage	CSMS	CSC	Info1 – redémarrage
2	La CS répond	– Si le CSMS demande "redémarrage forcé" sans indiquer de moment précis, la CS répond "identifiant de l'activité de redémarrage" au CSMS et redémarre dès que la pratique le permet. – Si le CSMS demande "redémarrage forcé" et indique un moment précis, la CS répond alors "identifiant de l'activité de redémarrage" au CSMS et redémarre au moment indiqué ou après ce moment. – Si le CSMS demande "redémarrage au ralenti" sans indiquer de moment précis, alors • Si aucun VE n'est engagé dans une session active, la CS répond alors "identifiant de l'activité de redémarrage" et redémarre dès que la pratique le permet. • Lorsqu'un VE ou plus est engagé dans une session de service active, la CS répond alors "identifiant de l'activité de redémarrage", et redémarre lorsque plus aucune session de service n'est active. – Si le CSMS demande "redémarrage au ralenti" et indique un moment précis, alors • Lorsqu'aucun VE n'est connecté au SAVE, la CS répond alors avec l'identifiant de l'activité de redémarrage, et redémarre au moment indiqué ou après ce moment si aucune session de service n'est active • Lorsqu'un VE ou plus est engagé dans une session de service active, la CS répond alors "identifiant de l'activité de redémarrage", et redémarre lorsque plus aucune session de service n'est active, mais pas avant le moment précis indiqué.	CSC	CSMS	Info2 – état de redémarrage

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	redémarrage	Type de redémarrage: il peut s'agir d'un "redémarrage forcé" ou d'un "redémarrage au ralenti" Moment auquel ou après lequel le redémarrage a lieu
Info2	état de redémarrage	identifiant de l'activité de redémarrage

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	redémarrage forcé	Lorsque la CS reçoit une demande de redémarrage forcé, elle doit redémarrer son système dès que la pratique le permet (sans tenir compte des sessions de service actives)

8.3.8 Le CSMS définit les informations à présenter à l'utilisateur

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M6	Gestion de la CS	Les informations s'affichent sur le SAVE

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Les informations s'affichent sur les SAVE.
Objectif(s)	Le CSMS envoie à la CS des informations spécifiques centrées sur l'utilisateur à fournir (sur un écran, par exemple) à un SAVE particulier. En règle générale, les informations fournies ne concernent pas le processus de charge. Il s'agit uniquement d'informations générales utiles pour l'utilisateur. Par exemple, le trafic dans la zone, les prévisions météorologiques, le signal d'urgence, la publicité.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Le CSMS demande à la CS de présenter des informations à l'UVE.
Description complète
L'utilisateur du VE est réputé lire ou écouter les informations provenant du SAVE. Les informations peuvent s'afficher avant, pendant ou après l'utilisation du SAVE. L'heure, la durée et la nature des informations affichées sont définies par le CSMS. 1) Les règles et le contenu des informations à fournir sont définis par le CSMS. 2) La nature des informations à fournir a un impact sur la manière dont le CSMS envoie les informations (dans la bande ou hors bande). 3) La CS envoie une confirmation au CSMS selon laquelle les informations ont été reçues et sont présentées sur l'interface utilisateur du SAVE (visuel ou audio, etc.).

Conditions de cas d'utilisation

Conditions préalables	
1	Le SAVE présente une interface utilisateur qui est décrite dans le modèle d'objet et qui peut être découverte par le CSMS.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Le CSMS fournit les informations à présenter par l'interface utilisateur.	La manière dont la CS obtient les informations à présenter dépend de la manière dont le CSMS envoie les informations.	CSMS	Conditions de fin: – Les informations sont présentées dans le SAVE; – La CS ne parvient pas à extraire les informations du CSMS; – La CS ne prend pas en charge cette fonction.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Le CSMS demande à la CS de présenter certaines informations à l'utilisateur	Le mécanisme d'envoi des informations à présenter s'apparente à celui utilisé pour mettre à jour le micrologiciel (dans la bande ou hors bande).	CSMS	CSC	Info1 - Le CSMS demande à la CS d'extraire les informations à présenter à l'utilisateur.
2	La CS extrait les informations à présenter à l'utilisateur	La CS répond avec l'état du processus d'extraction.	CSC	CSMS	Info2 - La CS informe le CSMS du processus d'extraction des informations
3	Le CSMS extrait l'état du processus d'extraction des informations	La CS informe le CSMS de l'état du processus d'extraction. La CS informe le CSMS lorsque les informations sont prêtes à être présentées à l'utilisateur.	CSMS		

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS demande à la CS d'extraire les informations à présenter à l'utilisateur.	– Liste des SAVE concernés (selon le modèle d'objet). – Heure de début et Heure de fin. – Mécanisme de téléchargement. – ID d'informations qui donne une signification sémantique de la charge utile. – il convient que la charge utile puisse être fournie dans la bande ou hors bande. – Période valide. Charge utile consciente de la langue
Info2	La CS informe le CSMS du processus d'extraction des informations.	– Processus d'extraction en cours, terminé, échoué, etc. – Liste des SAVE prêts à présenter les informations à l'utilisateur.

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Conditions de présentation	La CS doit appliquer les règles du CSMS en ce qui concerne l'heure et la durée de présentation des informations.
Req2	Informations de l'état d'extraction	La CS doit informer le CSMS du résultat du transfert d'informations et de l'installation dans le SAVE.
Req3	État de présentation	La CS doit informer le CSMS que les informations sont présentées dans le SAVE.
Req4	Conscience de la langue	Toutes les informations présentées à l'utilisateur doivent prendre en charge la localisation de la langue en fonction des préférences de l'utilisateur, lorsqu'elles sont disponibles.

8.3.9 Le CSMS définit les critères de journalisation

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M7	Gestion de la CS	Le CSMS définit les critères de journalisation CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Le CSMS demande à la CS de définir les critères de journalisation.
Objectif(s)	Objectif: L'OSR souhaite que la CS définisse les critères de journalisation qui peuvent être extraits par la suite pour l'analyse (voir 0, cas d'utilisation "Extraire les informations de journalisation de la CS").
Cas métier connexe(s)	Gérer la CS: l'OSR gère la CS

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Le CMSM demande à la CS de définir les critères de journalisation.
Description complète
Pour capturer les informations relatives au fonctionnement de la CS (en ce qui concerne le contrôle d'accès, les sessions de charge, les configurations, les tentatives de charge, le processus et le fonctionnement de la CS, par exemple), l'OSR peut définir les critères de capture des événements et des informations qu'il est nécessaire de stocker. Les capacités de journalisation peuvent être décrites comme un service qui figure dans une phase de découverte. – Le CSMS demande à la CS de définir les critères de journalisation. – La CS répond s'il est en mesure de journaliser les informations en fonction des critères. – Pendant le fonctionnement normal, la CS journalise tous les événements qui correspondent aux critères actifs, dans une mémoire non volatile. Un ensemble de critères peut être regroupé et référencé par un identifiant de critères. Après qu'il a été défini, un ensemble de critères peut être activé ou désactivé simplement par référencement de son identifiant.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Le CSMS définit les critères de journalisation de la CS	Le CSMS définit les critères de journalisation de la CS.	CSMS	Conditions de fin: – Succès: La CS accepte les critères et des entrées de journal sont ajoutées pour chaque événement futur correspondant en fonction des critères définis par le CSMS. – Échec: Le CSMS est informé que la CS ne peut pas journaliser certaines informations qui correspondent aux critères demandés.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)	Exigence, R-ID
1	Le CSMS envoie les critères de journalisation à la CS	Lorsque le CSMS n'envoie que l'identifiant des critères, la CS passe alors à la liste des critères correspondante. Lorsque le CSMS envoie l'identifiant de critères et une liste de critères, la CS remplace ou crée alors la liste de critères actuelle correspondant à l'identifiant. Un ensemble de critères peut être regroupé et référencé par un identifiant de critères. Après qu'il a été défini, un ensemble de critères peut être activé ou désactivé simplement par référencement de son identifiant. Les critères de journalisation sont, par exemple, le contrôle d'accès, les sessions de charge, les configurations, les tentatives de charge, le processus et le fonctionnement du CS.	CSMS	CSC	Info1 – Le CSMS envoie les critères de journalisation à la CS	
2	La CS extrait les critères de journalisation	La réponse réside dans les critères qui ne peuvent pas être définis et la possible raison de cet échec.	CSC	CSMS	Info2 – La CS renvoie l'état des critères au CSMS	
3	Le CSMS signale l'état du journal à l'OSR	En cas d'échec, le CSMS en informe l'OSR. (ce message ne relève pas du domaine d'application).	CSMS			

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS envoie les critères de journalisation à la CS	– L'identifiant des critères de journalisation en cas d'identification de nouveaux critères – Domaine d'application de cette liste de critères. – Durée du journal. – Condition de capture (périodicité, en cas d'événement, etc.). – Liste des paramètres soumis aux critères actifs.
Info2	La CS renvoie l'état des critères au CSMS	Soit: l'identifiant actif actuel de la liste des critères de journalisation des paramètres auxquels les critères peuvent être appliqués, Soit le code erreur si l'identifiant ne peut pas être défini, et la raison de cette impossibilité.

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Ensemble minimal de critères	Valeur par défaut et ensemble minimal des critères qui doivent être applicables à tout moment.
Req2	Modèle d'objet	Les critères de journalisation doivent faire référence aux états des objets décrits dans le modèle d'objet de la CS.
Req3	Identifiants de critères	Le CSMS doit identifier les critères.
Req4	Nombre de listes de critères stockées dans la CS	La CS doit stocker au moins deux listes de critères, avec leurs identifiants.
Req5	Passer d'une liste à l'autre	La CS doit passer d'une liste à une autre chaque fois que le CSMS envoie un identifiant connu.
Req6	Les informations sensibles ne sont pas consignées dans les journaux	La CS ne doit pas journaliser les informations sensibles comme les clés ou les justificatifs d'identité.
Req7	Stockage sécurisé	La CS doit contenir une mémoire rémanente sécurisée pour stocker les informations de journal.
Req8	Accès restreint aux journaux	La CS doit empêcher l'accès aux informations journalisées par des acteurs non autorisés.
Req9	Les critères de journalisation correspondent	La CS doit journaliser les événements qui correspondent aux critères demandés par le CSMS.
Req10	Format des journaux	Chaque entrée de journal doit contenir un horodatage, un numéro de séquence de capture et un niveau de sévérité.

8.3.10 Extraire les informations de journalisation de la CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M8	Gestion de la CS	Extraire les informations journalisées de la CS.

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Extraire les informations journalisées de la CS.
Objectif(s)	Examiner les informations journalisées: Un CSMS souhaite extraire les informations consignées auprès de la CS pour procéder à une analyse détaillée du fonctionnement de la CS.
Cas métier connexe(s)	Offre de services de mobilité électrique.

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Le CSMS demande à la CS d'envoyer certaines informations journalisées
Description complète
Un utilisateur ou l'OSR peut avoir été confronté à des problèmes avec une CS, que l'examen des messages réguliers échangés entre la CS et le CSMS ne peut expliquer. Des informations détaillées provenant de la CS sont nécessaires pour examiner son fonctionnement et expliquer le problème. Le volume de la charge utile varie de quelques kilooctets (ko) à plusieurs mégaoctets (Mo) en fonction des filtres. L'accès aux informations de diagnostic peut être restreint. Étapes à suivre: 1) le CSMS demande à la CS d'envoyer des informations de diagnostic. La demande peut contenir des filtres facultatifs; 2) la CS répond en indiquant si elle peut ou pas envoyer les informations; 3) la CS rassemble et transmet les informations demandées; 4) lors de la collecte et de la transmission des informations de diagnostic, la CS peut envoyer des mises à jour au CSMS concernant l'état du processus. Les informations journalisées sont envoyées au CSMS avec une communication dans la bande.

Conditions de cas d'utilisation

Conditions préalables
– La CS doit mettre en œuvre un mécanisme de livraison par découpage.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Le CSMS demande à la CS de journaliser les informations	Extraire les informations journalisées de la CS.	CSMS CS	Conditions de fin: Succès: – Les données de diagnostic ont bien été reçues. – Les informations de diagnostic correspondantes sont disponibles, elles sont envoyées et le CSMS est informé de l'état du processus. Échec: – Aucune information de diagnostic correspondante n'est disponible. – Les informations de diagnostic correspondantes sont disponibles, elles ne peuvent pas être envoyées et le CSMS est informé de l'état de défaillance. – Liaison de communication coupée pendant le processus.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)	Exigence, R-ID
1	Le CSMS demande des informations journalisées à la CS	Le CSMS demande à la CS d'envoyer des informations de diagnostic. La demande peut contenir des filtres facultatifs.	CSMS	CSC	Info1 – Le CSMS demande des informations journalisées à la CS	Req1
2	La CS accuse réception	La CS répond en indiquant si elle peut ou pas envoyer les informations.	CSC	CSMS	Info2 – La CS renvoie au CSMS des informations d'accès au fichier journal	Req2
3	La CS rassemble les informations demandées	La CS rassemble les informations demandées	CS			Req3
4	Le CSMS obtient l'état auprès de la CS.	Lors de la collecte et du transfert des informations de diagnostic par la CS, le CSMS peut recevoir des mises à jour de la part de la CS concernant l'état du processus.	CSC	CSMS	Info3 – La CS transfère l'état au CSMS	Req4
5	La CS traite la demande	La CS transmet les informations dans un flux de communication dans la bande.	CSC	CSMS	Info4 – transmission par découpe	

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS demande des informations journalisées à la CS	– Filtres facultatifs qui limitent le domaine d'application, tels que l'intervalle de temps, le niveau de sévérité, la première heure de début du transfert, les informations sur les tentatives, les paramètres de reprise après informations, etc.
Info2	La CS accuse réception de la demande du CSMS	– réception de la demande. La CS indique si elle peut ou non réaliser l'action demandée
Info3	La CS transfère l'état au CSMS	– Progression du processus. – Estimation du temps / découpage restant.
Info4	Transmission par découpage	– Découpage actuel des informations demandé. – Identification nécessaire exigée par le processus de découpage

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Message de demande	Le CSMS doit envoyer un message de demande à la CS qui contient toutes les informations utiles pour les paramètres de filtre. Il peut s'agir de l'intervalle de temps, du niveau de sévérité, de la première heure de début du transfert.
Req2	La CS accuse réception	La CS doit répondre avec un message qui indique si elle peut satisfaire à la demande.
Req3	Filtre	Si la demande contient un filtre, la CS doit uniquement envoyer des informations de diagnostic qui correspondent aux paramètres de filtre.
Req4	État en cours	La CS doit informer le CSMS de l'état du traitement (collecte et transmission des informations de diagnostic, par exemple).

8.3.11 Fourniture d'un code de défaut

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M9	Gestion de la CS	Fourniture d'un code de défaut

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	En cas de problème avec la CS, le rôle de l'OSR consiste à identifier le problème et à le résoudre rapidement, dans la mesure du possible, ou de rendre la CS indisponible le temps de corriger le problème. Ce cas d'utilisation reconnaît (i) qu'il convient que la communication entre la CS et le CSMS puisse délivrer des informations de défaut, et (ii) qu'il convient que le code de défaut qui représente les informations de défaut soit défini de manière à être compris par différents fabricants CS et différents OSR.
Objectif(s)	En cas de défaillance de certaines fonctionnalités de la CS, cette dernière doit donner au CSMS les informations pertinentes relatives à la défaillance (par exemple, le composant de la CS dont l'exécution n'a pas réussi et la cause de la défaillance, si elle a été identifiée).

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Description d'un code de défaut
Description complète
En cas de défaillance, la CS procède à un diagnostic, c'est-à-dire: – identifie le composant dont le fonctionnement est défaillant; – identifie la cause/le type de défaillance; – détermine le code de défaut correspondant; et – envoie le code de défaut et les métadonnées (par exemple, horodatage, texte non structuré, etc.). Le CSMS qui reçoit le code de défaut peut demander à la CS de mettre en œuvre une action donnée afin de résoudre la situation défaillante. Par exemple, – exécuter une fonction de reprise (par exemple, un réamorçage avec une certaine configuration); – afficher l'état sur l'interface de la CS; et – exécuter un diagnostic précis pour le rapport supplémentaire; et/ou – arrêter le fonctionnement et attendre la maintenance. Le CSMS met à jour la disponibilité de la CS en conséquence, adressée à l'OSR et au PSME (domaine d'application de l'IEC 63119).

Conditions de cas d'utilisation

Conditions préalables	
1	La CS peut identifier l'origine et la raison du problème afin de déterminer le code de défaut. Il convient de disposer d'au moins un schéma de code de défaut que la CS et le CSMS comprennent.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	Diagnostic de la CS en cas de défaillance	En cas de défaillance, la CS procède à un diagnostic, c'est-à-dire: – identifie le composant dont le fonctionnement est défaillant; – identifie la cause/le type de défaillance; – détermine le code de défaut correspondant; – envoie le code de défaut et les métadonnées (par exemple, horodatage, texte non structuré, etc.).	CSC	CSMS	Info1 – La CS envoie un code de défaut au CSMS
2	Le CSMS met à jour la disponibilité de la CS	Le CSMS met à jour la disponibilité de la CS en conséquence, adressée à l'OSR et au PSME (domaine d'application de l'IEC 63119).	CSMS		

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	La CS envoie un code de défaut au CSMS	– Composant dont le fonctionnement est défaillant. – Cause/type de la défaillance. – Code de défaut. – Métadonnées (horodatage, texte non structuré, etc.).

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Actions de la CS en cas de défaillance	En cas de défaillance: – la CS doit diagnostiquer le problème et déterminer le code de défaut le plus descriptif; – la CS doit envoyer le code de défaut au CSMS tel qu'il est configuré; – si le CSMS le demande, la CS doit exécuter les actions demandées selon les directives énoncées.
Req2	Actions du CSMS en cas de défaillance	En cas de défaillance de la CS: – le CSMS peut déterminer l'action correspondant au code de défaut reçu de la part de la CS. Par exemple, tenter une reprise, afficher l'état, exécuter un diagnostic et le consigner dans un rapport, ou arrêter le fonctionnement et attendre la maintenance; – le CSMS peut demander à la CS d'exécuter l'action déterminée.

8.3.12 Suppression des informations déclenchée auprès du CSMS par un SA

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M10	Gestion de la CS	Suppression des informations déclenchée auprès du CSMS par un acteur secondaire

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Suppression des informations déclenchée auprès du CSMS par un acteur secondaire
Objectif(s)	Supprimer les données stockées dans le SAVE, la CS et le CSMS.
Cas métier connexe(s)	

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Un acteur secondaire demande au CSMS de supprimer des informations
Description complète
Lors d'une session de service, de nombreuses données sont temporairement ou définitivement stockées dans le SAVE, la CS et le CSMS. L'OSR ou d'autres acteurs peuvent décider de supprimer tout ou partie des données stockées dans le SAVE et la CS. Raisons possibles: l'UVE souhaite supprimer ses données, le VE a été volé, le client est inactif ou les anciennes données ont été nettoyées, l'UVE souhaite supprimer des données, etc. Ce cas d'utilisation présente la situation dans laquelle le CSMS est déclenché pour procéder à la suppression des données. NOTE 1 L'OSR, l'UVE ou l'entretien interne peut déclencher la suppression. NOTE 2 Des systèmes supplémentaires (serveurs, par exemple) peuvent également être soumis à cette suppression, qui ne relève toutefois pas du domaine d'application du protocole défini dans l'IEC 63110. 1) Le CSMS est déclenché pour supprimer des informations – Le CSMS reçoit un déclencheur de suppression de la part de l'acteur approprié (OSR, UVE, etc.) afin de supprimer tout ou partie des données stockées dans le CS et le SAVE. – Le CSMS peut demander confirmation de la suppression avant de lancer le processus de suppression. – Lors de la suppression des données, le CSMS exige que le CS supprime certaines informations spécifiques dans la CS et le SAVE. – La CS informe le CSMS de l'état de la suppression. – Le CSMS traite la suppression. – Le CSMS signale l'état de la suppression à l'acteur à l'origine du déclenchement. NOTE 3 Dans certains cas, il peut s'avérer nécessaire que le CSMS sauvegarde les données avant de les supprimer (les informations juridiques ou financières relatives à la session de service, par exemple). NOTE 4 L'expression "supprimer des informations" signifie effacer définitivement les informations de la mémoire et des dispositifs de stockage permanent. NOTE 5 La suppression s'applique à toutes les informations, y compris celles stockées dans les fichiers journaux. NOTE 6 La suppression peut être soumise à des conditions telles que "à réaliser avant une certaine date" ou "uniquement sur la dernière session". NOTE 7 Le temps de rétention des données ne relève pas du domaine d'application et fait l'objet des lois locales en vigueur.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	CSMS déclenché pour supprimer des informations	Le CSMS est déclenché pour supprimer des informations dans la CS, le SAVE et le CSMS. L'OSR, l'UVE ou une initiative personnelle peut déclencher la suppression.	CSMS	Conditions de fin: Les données prévues sont supprimées du SAVE, de la CS et du CSMS. Si les informations ne peuvent pas être supprimées, un état d'erreur détaillé est envoyé à l'acteur à l'origine du déclenchement.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)	Exigence, R-ID
1	Le CSMS reçoit un déclencheur pour supprimer des informations spécifiques	Un acteur (l'OSR, l'UVE ou un processus interne, par exemple) exige que le CSMS supprime tout ou partie des informations dans la CS, le SAVE et le CSMS.	Entretien interne de l'OSR, de l'UVE et du CSMS			
2	Le CSMS peut confirmer la demande de suppression des informations (en particulier si l'UVE souhaite supprimer ses informations)	Le CSMS demande à l'acteur à l'origine du déclenchement de confirmer la suppression des données	CSMS			Req1
3	Le CSMS demande à la CS et au SAVE de supprimer les informations	Le CSMS exige que la CS supprime les données spécifiées dans la CS et ses SAVE.	CSMS	CSC	Info1 - Le CSMS demande à la CS de supprimer des informations	
4	La CS traite la suppression	La suppression a un impact sur le système interne de la CS et du ou des SAVE.	CS			Req2
5	La CS fournit l'état de la suppression au CSMS	La CS fournit l'état de la suppression au CSMS (par exemple, succès, succès partiel, échec)	CSC	CSMS	Info2 – La CS renvoie l'état de la suppression au CSMS	Req3
6	La CSMS traite la suppression	La suppression a un impact sur le CSMS	CSMS			Req4, Req5
7	L'état de la suppression est envoyé à l'acteur à l'origine du déclenchement	L'état de la suppression est envoyé à l'acteur à l'origine du déclenchement	CSMS			Req6

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS exige de la CS qu'elle supprime des données spécifiées	Portée de la suppression (peut être liée à un UVE spécifique, ou peut concerner des données antérieures à une certaine date, etc.). Conditions d'exécution (dès que possible, à une heure précise, par exemple).
Info2	La CS renvoie l'état de la suppression au CSMS	Informations détaillées relatives à l'état de la suppression (succès, échec avec les précisions relatives aux informations qui n'ont pas pu être supprimées et les raisons invoquées).

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Confirmation de la part de l'acteur à l'origine du déclenchement	Dans certains cas, lorsque le CSMS reçoit le déclencheur, il peut être nécessaire qu'il confirme la suppression auprès de l'acteur à l'origine du déclenchement.
Req2	La suppression a un impact sur le système interne de la CS et du ou des SAVE.	La CS doit supprimer toutes les données spécifiées.
Req3	La CS envoie l'état de la suppression au CSMS	La CS doit informer le CSMS de l'état de la suppression.
Req4	La suppression a un impact sur le CSMS	Le CSMS doit supprimer toutes les données spécifiques.
Req5	Journalisation	Le CSMS doit stocker le déclencheur de suppression et l'état de la suppression dans le système de journalisation.
Req6	L'état de la suppression est envoyé à l'acteur à l'origine du déclenchement	Le CSMS doit signaler l'état de la suppression à l'acteur à l'origine du déclenchement.

8.3.13 Annulation de l'enregistrement de la CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M11	Gestion de la CS	Annulation de l'enregistrement de la CS

Domaine d'application et objectifs du cas d'utilisation

Domaine d'application et objectifs du cas d'utilisation	
Domaine d'application	Annulation de l'enregistrement de la CS par le CSMS
Objectif(s)	Objectif: Annuler l'enregistrement de la CS
Cas métier connexe(s)	Cas d'utilisation Connexion et suppression des informations

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Le CSMS annule l'enregistrement de la CS
Description complète
L'annulation de l'enregistrement peut être considérée comme le cas d'utilisation inverse de l'amorçage. S'il s'avère nécessaire de séparer une CS de son point de connexion avec un CSMS, il est nécessaire d'annuler l'enregistrement de la CS dans le CSMS. Une annulation d'enregistrement doit être déclenchée de manière centrale par l'OSR, par l'intermédiaire du CSMS ou en local dans le cadre d'une intervention humaine autorisée. De plus, le CSMS doit être en mesure de donner des informations relatives à l'état d'enregistrement de chaque borne de charge connectée. Le CSMS exécute le cas d'utilisation "Suppression des informations déclenchée auprès du CSMS par un SA" (voir 8.3.12) avant d'annuler l'enregistrement. Lorsque l'enregistrement d'une borne de charge a été annulé, le CS ne doit plus être associé au CSMS ni utilisable par l'UVE. Par conséquent, dans le CSMS, la CS doit être définie sur enregistrement annulé/indisponible, ainsi que sur le serveur de l'OSR (hors du domaine d'application de l'IEC 63110) et les services secondaires connectés. Description détaillée: – annulation d'enregistrement déclenchée par le CSMS L'OSR demande au CSMS que l'enregistrement d'un, de plusieurs ou de tous les SAVE d'une certaine CS ou de la CS elle-même doit être annulé. Le CSMS reçoit une demande d'annulation d'enregistrement et la transfère à la CS; – annulation d'enregistrement déclenchée par la CS (facultative) Une personne autorisée (l'ingénieur d'entretien, par exemple) annule l'enregistrement de la CS dans une session de diagnostic pour vérifier par essai l'annulation d'enregistrement ou lors de la mise à jour du matériel. Il est nécessaire de réaliser cette action en local. La CS envoie alors les informations relatives à l'annulation d'enregistrement au CSMS, qui les transfère au serveur du SA; – informations de l'état de l'enregistrement Le CSMS doit pouvoir indiquer sur demande si la borne de charge est enregistrée, non enregistrée, si son enregistrement a été annulé, si son enregistrement est en cours ou si l'annulation de son enregistrement est en cours.

Conditions de cas d'utilisation

Conditions préalables	
1	– La CS est opérationnelle, enregistrée et connectée au CSMS.

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Acteur primaire	Post-condition
1	Annulation d'enregistrement exigée par l'OSR ou la CS	– Il est demandé au CSMS d'annuler l'enregistrement d'une CS (déclenché par entrée locale par l'intermédiaire d'une session de diagnostic de la CS ou de manière centralisée par l'OSR). – Le CSMS procède à l'annulation d'enregistrement et partage le nouvel état d'enregistrement avec l'OSR.	CSMS CS	Conditions de fin: – L'enregistrement de la CS est annulé. – La CS, le CSMS et l'OSR ont mis à jour les informations relatives à leur état d'enregistrement respectif. – La CS est définie sur indisponible/enregistrement annulé et n'est donc plus utilisable par un UVE.

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
1	La CS envoie une demande d'annulation d'enregistrement au CSMS	Le CSMS reçoit une demande d'annulation d'enregistrement. La demande peut être appliquée à l'ensemble de la CS ou uniquement à un SAVE particulier. NOTE La demande peut également provenir de la CS ou de l'OSR (ne relève pas du domaine d'application).	CSC	CSMS	Info1– Le CSMS reçoit une demande d'annulation d'enregistrement
2	Il est demandé au CSMS (par exemple par l'OSR) d'annuler l'enregistrement d'une CS particulière	Le CSMS reçoit une demande d'annulation d'enregistrement. La demande peut être appliquée à l'ensemble de la CS ou uniquement à un SAVE particulier.	OSR	CSMS	
3	Le CSMS procède à l'annulation d'enregistrement	Avec les paramètres reçus: – le CSMS exécute le cas d'utilisation Suppression des informations déclenchée auprès du CSMS par un SA avec un domaine d'application limité à un SAVE particulier, si cela est exigé; – le CSMS envoie une commande d'annulation d'enregistrement à la CS avec un domaine d'application limité à un SAVE particulier, si cela est exigé; – le CSMS informe l'OSR de la commande d'annulation d'enregistrement en attente (ne relève pas du domaine d'application); – si une déconnexion temporaire s'avère nécessaire, il est alors nécessaire que le CSMS envoie un message de mise hors tension. Cette opération ne fait pas partie intégrante de l'annulation d'enregistrement.	CSMS	CSC	Info2 – Le CSMS demande à la CS de procéder à l'annulation d'enregistrement
4	Le CS procède à l'annulation d'enregistrement	– L'annulation d'enregistrement est réalisée avec le domaine d'application reçu (l'ensemble de la CS ou un SAVE particulier). – L'état de l'annulation d'enregistrement est envoyé au CSMS après l'annulation de l'enregistrement.	CSC	CSMS	Info3 – La CS envoie l'état d'enregistrement au CSMS
5	Le CSMS obtient l'état de l'annulation d'enregistrement	Le CSMS informe l'OSR de l'état de l'annulation d'enregistrement (ne relève pas du domaine d'application).	CSMS		

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Le CSMS reçoit une demande d'annulation d'enregistrement	La demande indique si elle s'applique à l'ensemble de la CS ou à un SAVE particulier. Dans le cas d'un SAVE particulier, l'identification du SAVE doit être fournie par la CS.
Info2	Le CSMS demande à la CS d'annuler l'enregistrement	Domaine d'application de l'annulation d'enregistrement: – ensemble de la CS; – un SAVE particulier.
Info3	La CS envoie l'état d'enregistrement au CSMS	Informations relatives à l'état d'enregistrement: – enregistré (erreur effective); – non enregistré.

Exigences

R-ID d'exigence	Nom de l'exigence	Description de l'exigence
Req1	Activer l'annulation d'enregistrement locale	L'annulation d'enregistrement de la CS peut être déclenchée par cette dernière dans le cadre d'une intervention humaine locale.
Req2	Activer l'annulation d'enregistrement centrale	L'annulation d'enregistrement de la CS peut être déclenchée par le CSMS.
Req3	Domaine d'application de l'annulation d'enregistrement	Il doit être possible de procéder à l'annulation d'enregistrement sur la CS ou au niveau du SAVE.
Req4	Journal	Le CSMS doit journaliser l'état de l'annulation d'enregistrement et les messages envoyés par la CS pendant l'annulation d'enregistrement.
Req5	État	La CS doit envoyer un état pendant et après l'annulation d'enregistrement.
Req6	Suppression des informations	Le CSMS doit supprimer les informations stockées dans la CS (ou dans le SAVE). Le processus de suppression est décrit dans le cas d'utilisation "Suppression des informations auprès du CSMS par un SA" (voir 8.3.12).

8.3.14 Migration de la CS

Nom du cas d'utilisation

Identification du cas d'utilisation		
ID	**Zone(s)/Domaine(s)**	**Nom du cas d'utilisation**
M12	Gestion de la CS	Migration de la CS

Domaine d’application et objectifs du cas d'utilisation

Domaine d’application et objectifs du cas d'utilisation	
Domaine d'application	Migration de la CS vers différents CSMS dans le même OSR
Objectif(s)	Objectif: Déconnecter la CS du CSMS actuel, puis la reconnecter à un nouveau CSMS avec le même OSR.
Cas métier connexe(s)	Connexion de la CS Annulation de l'enregistrement de la CS Suppression des informations déclenchée auprès du CSMS par un SA

Récit du cas d'utilisation

Récit du cas d'utilisation
Brève description
Une CS migre d’un CSMS à un autre
Description complète
Il peut être nécessaire de préparer une CS sous le CSMS actuel pour une migration vers un nouveau CSMS et de la reconnecter au nouveau CSMS. La procédure de migration suit les étapes suivantes: 1) exécuter éventuellement le cas d'utilisation "Suppression des informations déclenchée auprès du CSMS par un SA" (voir 8.3.12); 2) lors de cas d'utilisation, le CSMS actuel envoie les informations d’amorçage suivantes à la CS qui migre: • informations de connexion à l’intention du nouveau CSMS; • informations relatives aux justificatifs d'entrée d'origine nécessaires pour établir un canal sécurisé; 3) exécuter le cas d'utilisation "Annulation de l'enregistrement de la CS" (voir 8.3.13); 4) exécuter le cas d'utilisation "Connexion de la CS" (voir 8.3.15).

Présentation des scénarii

N°	Nom du scénario	Description du scénario	Condition préalable	Post-condition
1	Suppression des informations	Au besoin, les informations du client sont supprimées. Se reporter au cas d'utilisation "Suppression des informations déclenchée auprès du CSMS" (voir 8.3.12)	Se reporter au cas d'utilisation "Suppression des informations déclenchée auprès du CSMS" (voir 8.3.12)	Se reporter au cas d'utilisation "Suppression des informations déclenchée auprès du CSMS" (voir 8.3.12)
2	Préparation de la migration	Installation des informations d'amorçage dans la CS	L'OSR est capable de générer des informations d'amorçage à la CS nécessaires à la migration	Conditions de fin: – La CS a enregistré avec succès les informations nécessaires de migration
3	Annulation de l'enregistrement de la CS	Annuler l'enregistrement de la CS du CSMS actuel Se reporter au cas d'utilisation "Annulation de l'enregistrement de la CS" (voir 8.3.13)	Se reporter au cas d'utilisation "Annulation de l'enregistrement de la CS" (voir 8.3.13)	Se reporter au cas d'utilisation "Annulation de l'enregistrement de la CS" (voir 8.3.13)
4	Connexion de la CS	Connecter la CS au nouveau CSMS Se reporter au cas d'utilisation "Connexion de la CS" (voir 8.3.15)	Se reporter au cas d'utilisation "Connexion de la CS" (voir 8.3.15)	Se reporter au cas d'utilisation "Connexion de la CS" ((voir 8.3.15)

Analyse étape par étape du scénario

N° d'étape	Nom du processus/de l'activité	Description du processus/de l'activité	Producteur des informations (acteur)	Destinataire des informations (acteur)	Informations échangées (ID)
2.1	Le CSMS envoie des informations d'amorçage à la CS	Le CSMS envoie des informations d'amorçage à la CS de sorte que cette dernière puisse utiliser ces informations pour se connecter à un nouveau CSMS lors d'une phase d'amorçage.	CSMS	CSC	Info1 – Informations d'amorçage

Informations échangées

Informations échangées, ID	Nom des informations	Description des informations échangées
Info1	Informations d'amorçage	Ces informations décrivent le mode que peut utiliser la CS pour se connecter au nouveau CSMS, ainsi que les justificatifs d'identité à utiliser pour établir un canal sécurisé entre la CS et le CSMS.