IEC – International Electrotechnical Commission - Organization

IEC – International Electrotechnical Commission - Organization

IEC – International Electrotechnical Commission - Organization

Globally relevant standards

Expertise and consensus

Thousands of experts participate in IEC standardization work in IEC technical committees and subcommittees (TC/SCs). They are chosen by their National Committee (NC) to share their technical expertise and represent the national requirements of industry, government, test & research laboratories, academia or user groups at the global level in the IEC.

The IEC offers these experts a neutral and independent platform where they can discuss and agree on state-of-the-art technical solutions with global relevance and reach. These are published as voluntary, consensus-based international standards.

Each TC defines its scope and area of activity, which it submits to the IEC Standardization Management Board (SMB) for approval.

A TC can form one or more SCs depending on the extent of its work programme. Each SC defines its scope and reports directly to the parent TC.

The SMB also establishes project committees which prepare individual standards that don't fall within the scope of an existing TC or SC. Project committees are disbanded once the standard has been published.

Facts and figures

TC/SCs

Technical Committees	109
Subcommittees	101
Total	210

WGs

Working Groups	702
Project Teams	189
Maintenance Teams	641
Total	1532

National Committees

Upon admission, every IEC Member – one National Committee per country - promises to fully represent all private and public national interests in the field of electrotechnology at the global level in IEC standardization and conformity assessment activities.

The IEC offers them a neutral, independent international forum where often globally renowned experts from industry, government, academia and user groups can sit together and find consensus on solutions to broad technical challenges.

Facts & figures

IEC National Committees

Full Members	62
Associate Members	27
Total	89

IEC – International Electrotechnical Commission - Organization

What is an international standard

IEC International Standards reflect the global consensus and distilled wisdom of many thousand technical experts who are delegated by their countries to participate in the IEC.

They provide instructions, guidelines, rules or definitions that are then used to design, manufacture, install, test & certify, maintain and repair electrical and electronic devices and systems.

IEC International Standards are essential for quality and risk management; they help researchers understand the value of innovation and allow manufacturers to produce products of consistent quality and performance. IEC International Standards are always used by technical experts; they are always voluntary and based on the international consensus of experts from many countries.

International standards also form the basis for testing and certification.

International standards are also often adopted by countries or regions to become national or regional standards. For example, close to 80% of European electrical and electronic standards are in fact IEC International Standards.

On the other side, regulations are rules or directives that are made and maintained by a national or regional authority. Generally, compliance with regulations is a must.

However, it is quite common for technical regulations to refer to international standards because standards help avoid that the law becomes too detailed or descriptive. This approach allows laws to stay current because standards are regularly reviewed and updated.

Standardization Management Board

The SMB (Standardization Management Board) is responsible for the management and supervision of IEC standardization work. The SMB is a decision-making body which reports to the CB (Council Board).

Read the SMB Communiqué newsletter

Development process

The IEC has a clear, well-established and strictly controlled standards development process. It governs the development and publication of IEC International Standards and other types of publications and includes enough time for comments by all stakeholders at different stages of development.

IEC National Committees (IEC Members), are involved at every stage of the process.

IEC publications are developed in over 200 technical committees and subcommittees (TC/SCs) and hundreds of working groups, each responsible for a specific technology area.

IEC – International Electrotechnical Commission - Organization

7 stages of standard development

	Stages	Action	Documents
1	Preliminary (optional)	Preliminary work item added to the work programme	PWI
2	Proposal	Proposal to start a new project comes from NC, TC, SMB, liaison org.	NP → Vote → RVN
3	Preparatory	Preparation of Working Draft within the working group (WD)	WD Internal to WG, not circulated
4	Committee	Working draft circulated as Committee Draft (CD)	CD → Comments → CC
5	Enquiry	When mature, the CD is circulated as a Committee Draft for Vote (CDV)	CDV → Vote + Comments → RVC
6	Approval	Final Draft International Standard prepared from approved CDV and NCs comments (FDIS)	FDIS → Vote → RVD
7	Publication	IEC publishes International Standard (IS)	IS

IEC Standards

- ISO / IEC 15118
- IEC 63110
- IEC 61850

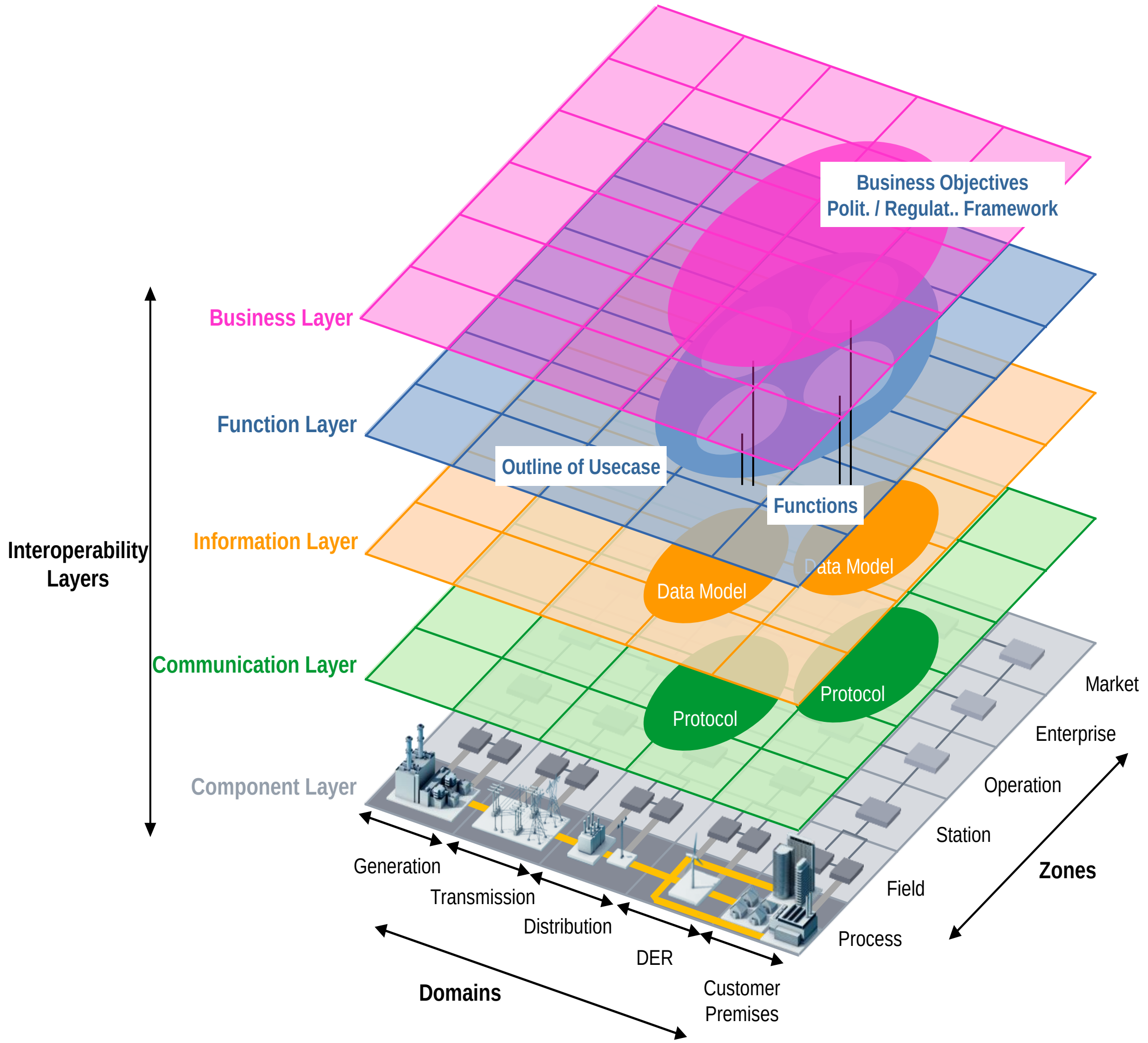
IEC International Technical Committees and Working Groups involved

- IEC TC120 “Electrical Energy Storage Systems”
- IEC TC69 / JWG11 “Management of Electric Vehicles charging discharging infrastructures”
- IEC TC 57 / WG17 “Power system intelligent electronic device communication and associated data models for microgrids, distributed energy resources and distribution automation”

SAE – Society of Automotive Engineers is active is standardization activity of vehicles in North America

- SAE - Hybrid Communication and Interoperability Task Force
  works on Electrical Vehicle standards

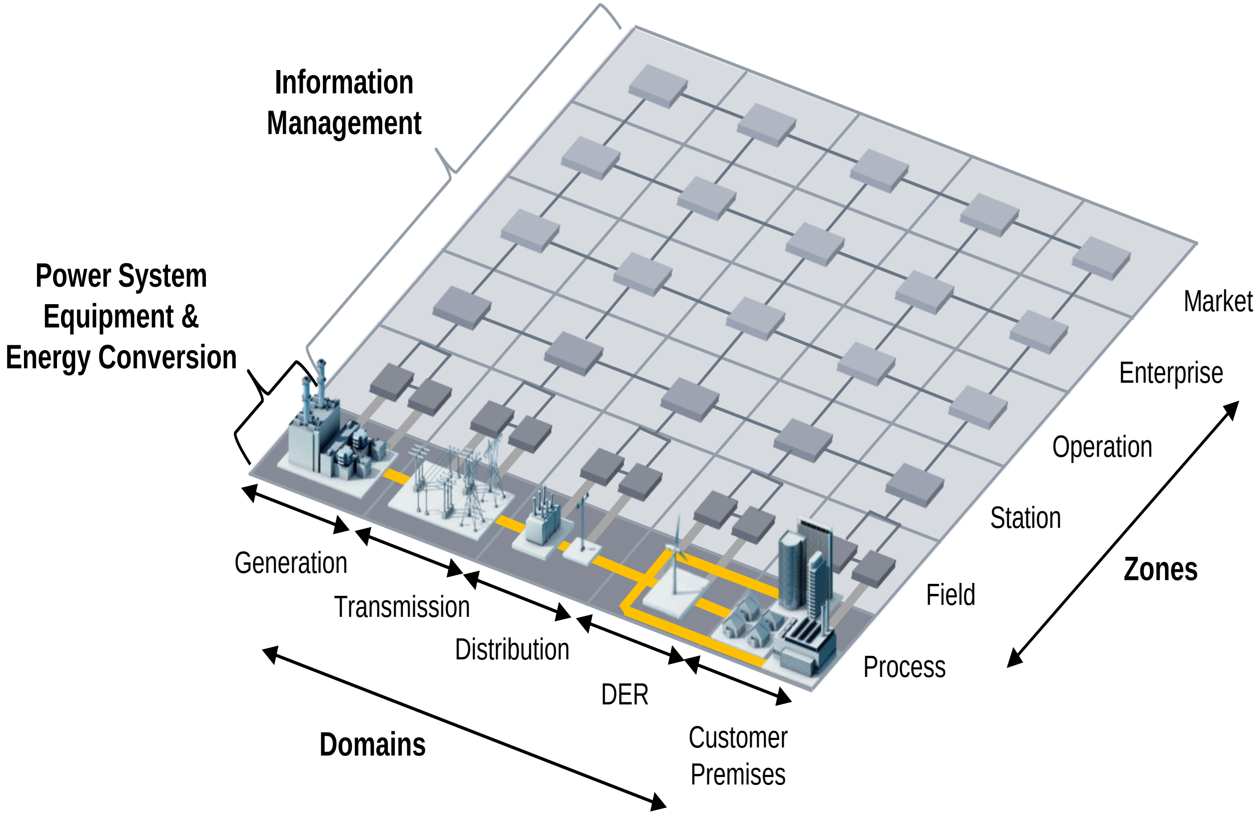
Smart Grid Architecture Model



The **Smart energy Grid Architecture Model** (SGAM) is a three-dimensional architectural framework that can be used to model interactions (mostly exchange of information) between different entities located within the smart energy arena :

- Business axe (domains)
- Architecture axe (zones)
- Interoperability axe (levels)

Smart Grid Architecture Model



SGAM Domain

A set of roles involved in the energy industry, considering that the whole industry is partitioned into 5 business domains:

- Generation
- Transmission
- Distribution
- DER (Distributed Energy Resources)
- Customers' Premises

SGAM Zone

hierarchical level of the system architecture from the energy market places, down to the physical power equipment, considering that the whole chain is partitioned into 6 zones:
Market, Enterprise, Operation,
Station, Field and Process

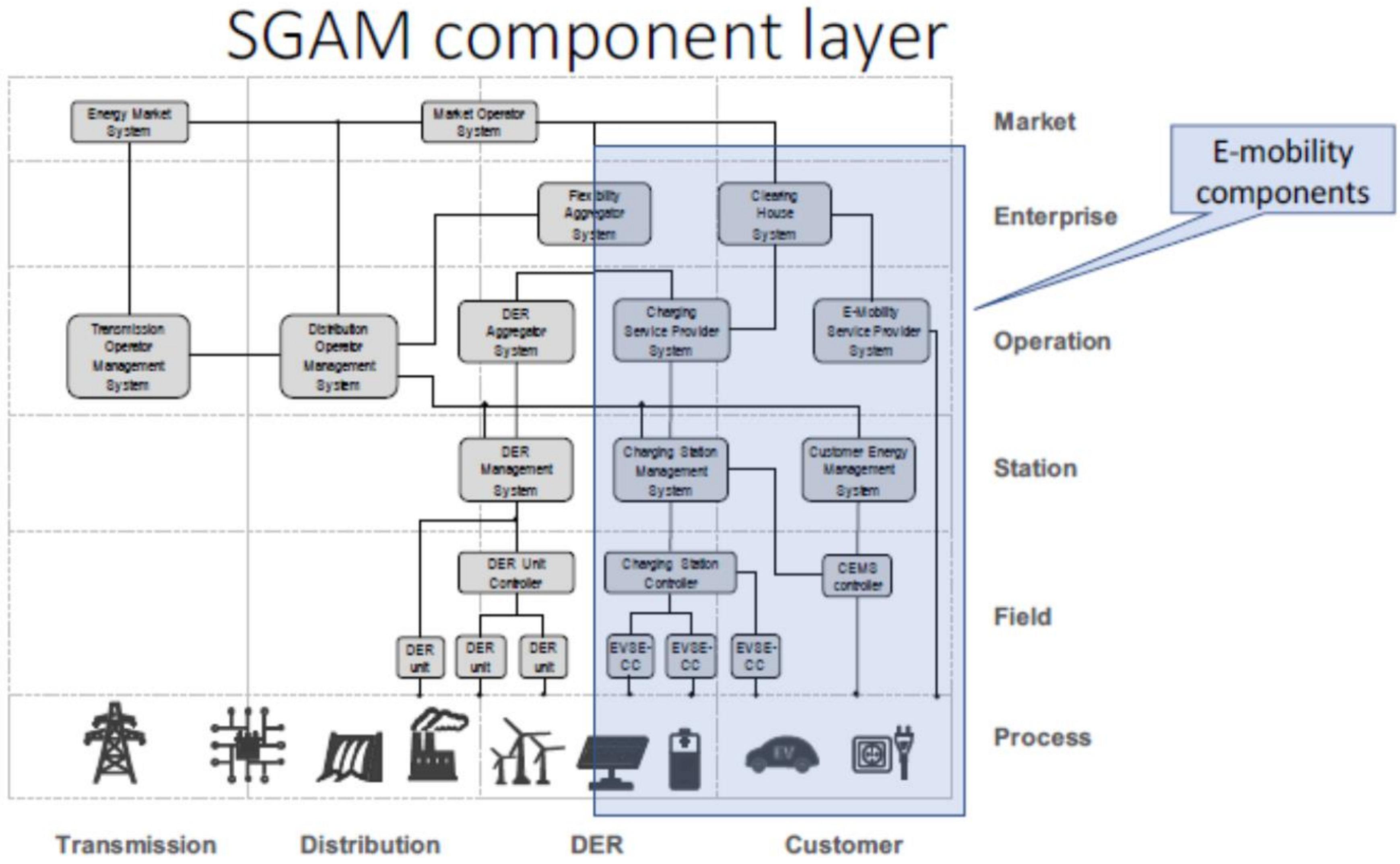
Smart Grid Architecture Model

Domain	Description
(Bulk) Generation	Set of roles representing the generation of electrical energy in bulk quantities typically connected to the transmission system, such as by fossil, nuclear and hydro power plants, off-shore wind farms, large scale solar power plant (i.e. PV, CHP).
Transmission	Set of roles involved in transporting energy over long distances, and/or large quantity of energy with roles in the Distribution domain, and/or in some cases directly with roles in energy intensive customer premises.
Distribution	Set of roles involved in transporting energy to and from DER domain roles and/or customer premises domain roles.
DER	Set of roles connected to actor(s) from the distribution domain and customer premises, defined as the business goal of providing energy services to the grid typically as production and/or storage and/or any types of ancillary services. It includes distributed energy resources directly connected to the distribution grid, applying small-scale power generation and consumption technologies, as well as energy related actors providing services to these one (such as aggregators, VPPs, ..). These distributed electrical resources may be directly or indirectly controlled by different stakeholders for the business goal of providing energy services to the grid, such as TSO, DSO, an aggregator, a customer, a microgrid EMS, or Balance Responsible Party (BRP).
Customer Premises	Set of roles with their primary business goals not directly related to providing energy services to the grid while using the energy grid as one energy source. Examples include home or building facilities, industries (e.g. industrial plants), non-energy-related infrastructures (such as transportation, airports, harbors, shopping centers, campus), EV systems, ... It includes as well the energy related roles providing services to these one such as aggregators, energy retailers, … It may host local energy producer units in form of e.g. photovoltaic generation, electric vehicles storage, batteries, micro turbines.

Smart Grid Architecture Model

Zone	Description
Process	Includes the physical, chemical or spatial transformations of energy (electricity, solar, heat, water, wind …) and the physical equipment directly involved in the flow of energy (e.g. generators, transformers, circuit breakers, overhead lines, cables, electrical loads, any kind of sensors and actuators which are part or directly connected to the process,…).
Field	Includes “intelligent” equipment to directly manage the flow of energy, including to protect, control and monitor the process of the power system, e.g. protection relays, bay controller, any kind of electronic devices which acquire and use process data from the power system.
Station	Includes the area aggregation level for field level participating in the same “application”, e.g. for data concentration, functional aggregation, substation automation, local SCADA systems, industrial workshop controller, local HVAC controller…
Operation	Includes the hosting power system management capabilities in the respective domain, e.g. distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems, Building management system, Industrial plant management system.
Enterprise	Includes the commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders …), e.g. asset management, logistics, work force management, staff training, customer relation management, billing and procurement…
Market (place)	Includes the market operations possible along the energy conversion chain, e.g. wholesale marketplace, retail marketplace.

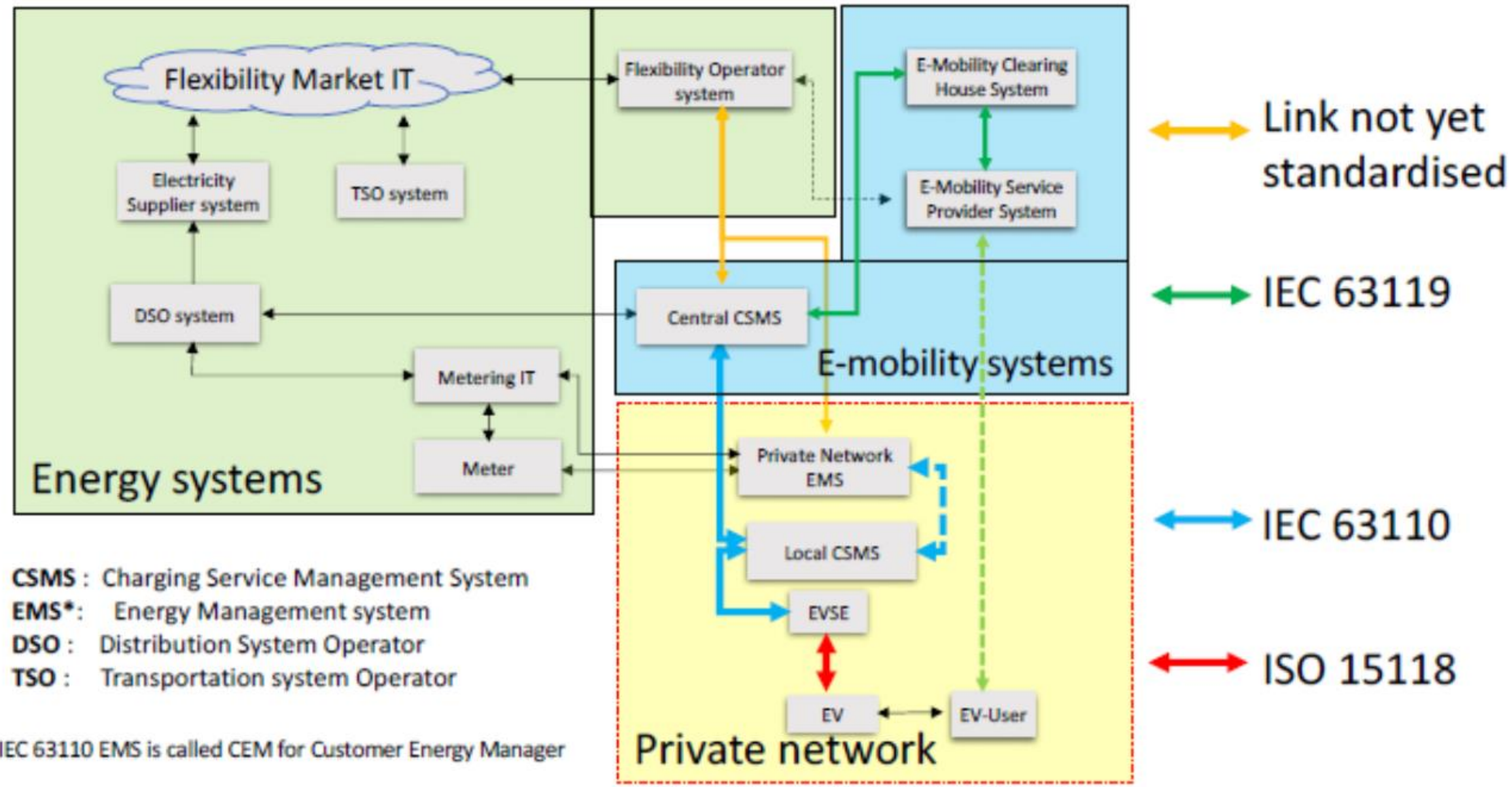
Smart Grid Architecture Model



IEC Standards – E-mobility

IEC 63110 Management of Electric Vehicles charging and discharging infrastructures

Next E-mobility standard landscape



CSMS : Charging Service Management System
EMS*: Energy Management system
DSO : Distribution System Operator
TSO : Transportation system Operator

* In IEC 63110 EMS is called CEM for Customer Energy Manager

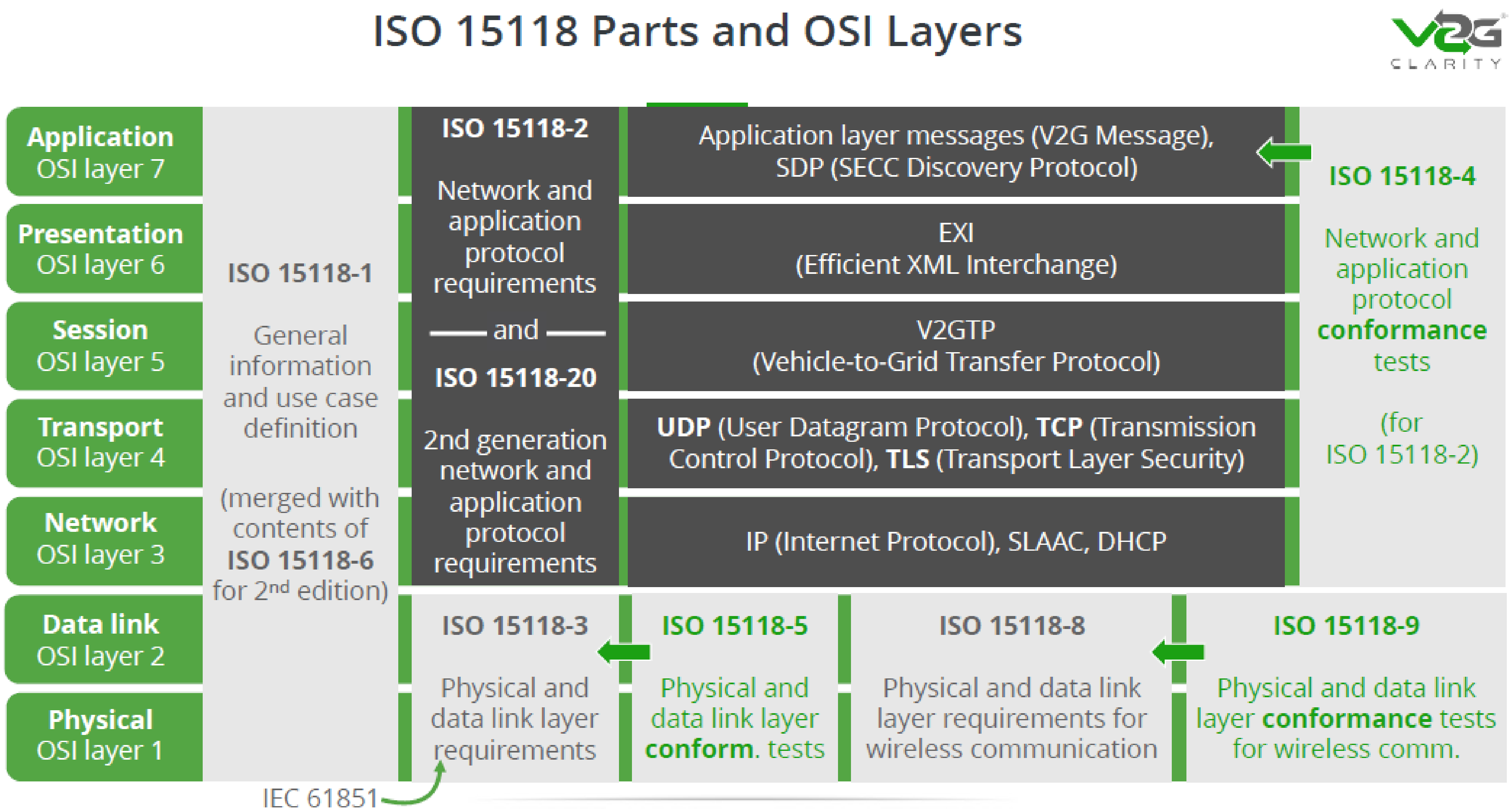
ISO 15118 - Tutorial

ISO 15118 is an international standard that outlines the ***digital communication protocol*** *that an electric vehicle (EV) and charging station should use to recharge the EV's high-voltage battery. As part of the Combined Charging System (CCS), ISO 15118 covers all charging-related use cases across the globe. This includes wired (AC and DC) and wireless charging applications and the pantographs that are used to charge larger vehicles like buses.*
From V2G Clarity, by Marc Mueltin

Contents

ISO 15118 - Overview

ISO 15118 is titled **”Road vehicles – Vehicle to grid communication interface”** and consists of seven parts. Each part covers a different aspect of digital communication between electric vehicles and charging stations.



ISO 15118-1 is titled **”General information and use-case definition”.**
It provides general information and defines terms and use cases.

ISO 15118-2 is titled **”Network and application protocol requirements”.**
Technical specifications of all application layer messages exchanged between the EV and the charging station.

ISO 15118-3 is titled **”Physical and data link layer requirements”**
It defines communication for wired charging on the two lowest layers.
Powerline communication (PLC) according **to HomePlug Green PHY** specification is applied to encode digital signals onto the Control Pilot (CP) pin, to establish the higher-level communication.
It specifies also interaction with IEC 61851.

ISO 15118-4 and -5 include **conformance tests** for the requirements specified in ISO 15118-2 and -3.
The ”systems under test” are the EV and the charging station.

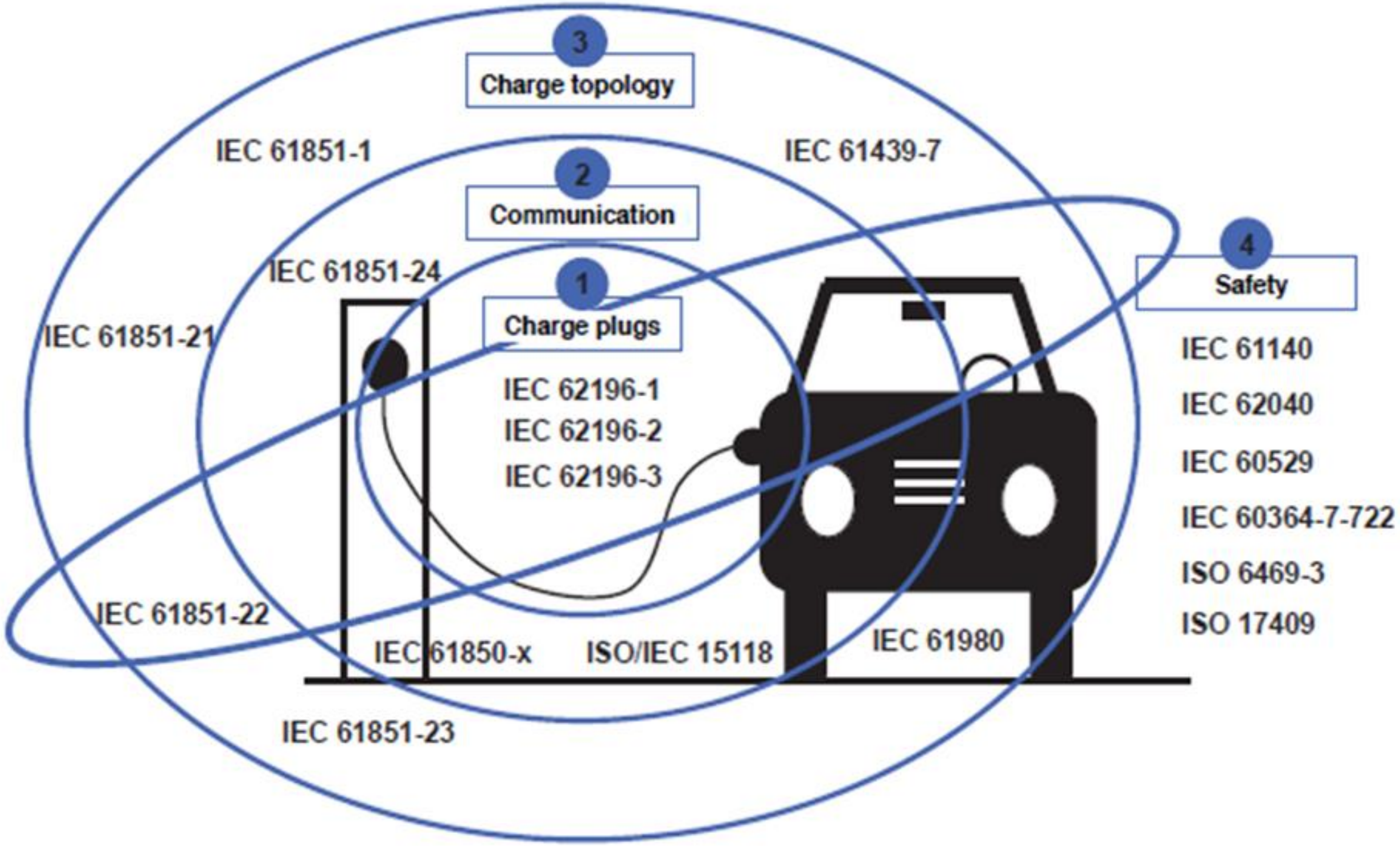
ISO 15118-6 was called **”General information and use-case definition for wireless communication”**
It does not exist any more, it is included in the second edition of ISO 15118-1.

ISO 15118-7 was called **”Network and application protocol requirements for wireless communication”.**
This part has been merged with part two. Requirements about both wired and wireless communication and charging can be found in ISO 15118-20.

ISO 15118-8 is called **”Physical layer and data link layer requirements for wireless communication”.**
It specifies the technical requirements for wireless charging communication on the lowest two layers.

ISO 15118-9 is called **”Physical and data link layer conformance test for wireless communication”.**
It provides conformance tests for part eight and completes the current list of required conformance tests for both wired and wireless communication.

Relationship of ISO 15118 with standards IEC 61851 and IEC 62196

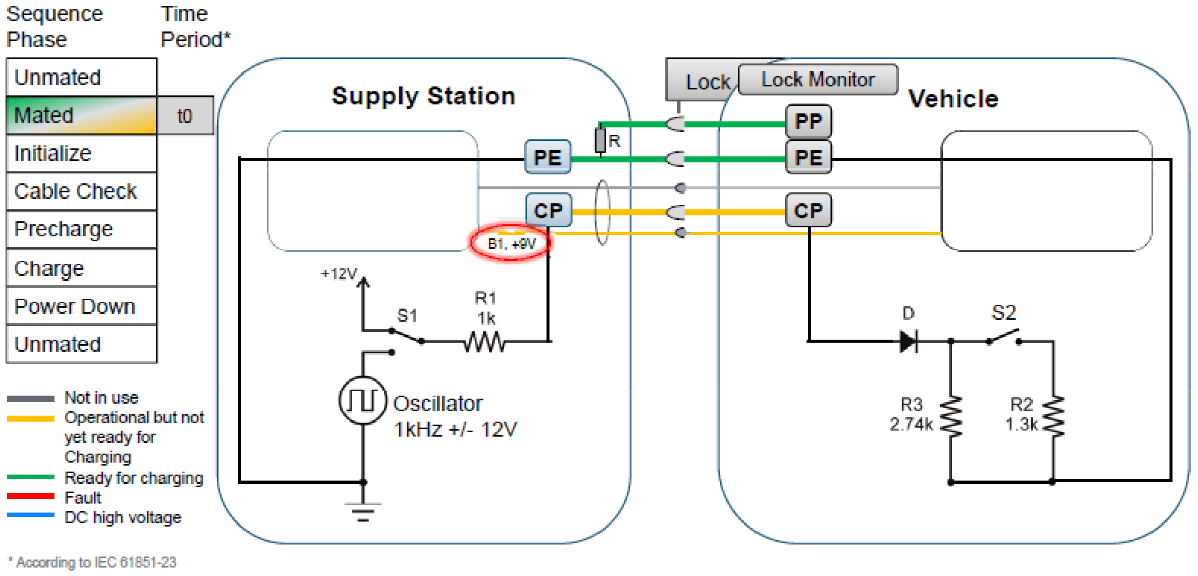


IEC 61851 – safety related standard for EV charging

CONTROL PILOT

It is an electrical signal that is sourced by the EVSE. Control pilot is the primary control conductor and is connected to the equipment ground through control circuitry on the vehicle and performs the following functions:

- Verifies that the vehicle is present and connected
- Permits energization/de-energization of the supply
- Transmits supply equipment current rating to the vehicle
- Monitors the presence of the equipment ground
- Establishes vehicle ventilation requirements
- Serves as medium for Power-Line-Communication (PLC)



➤ CP enters state B1 instantly with mating. This condition is detected by the 9V signal measured at R1. Vehicle is immobilized (PP).

PROXIMITY PILOT

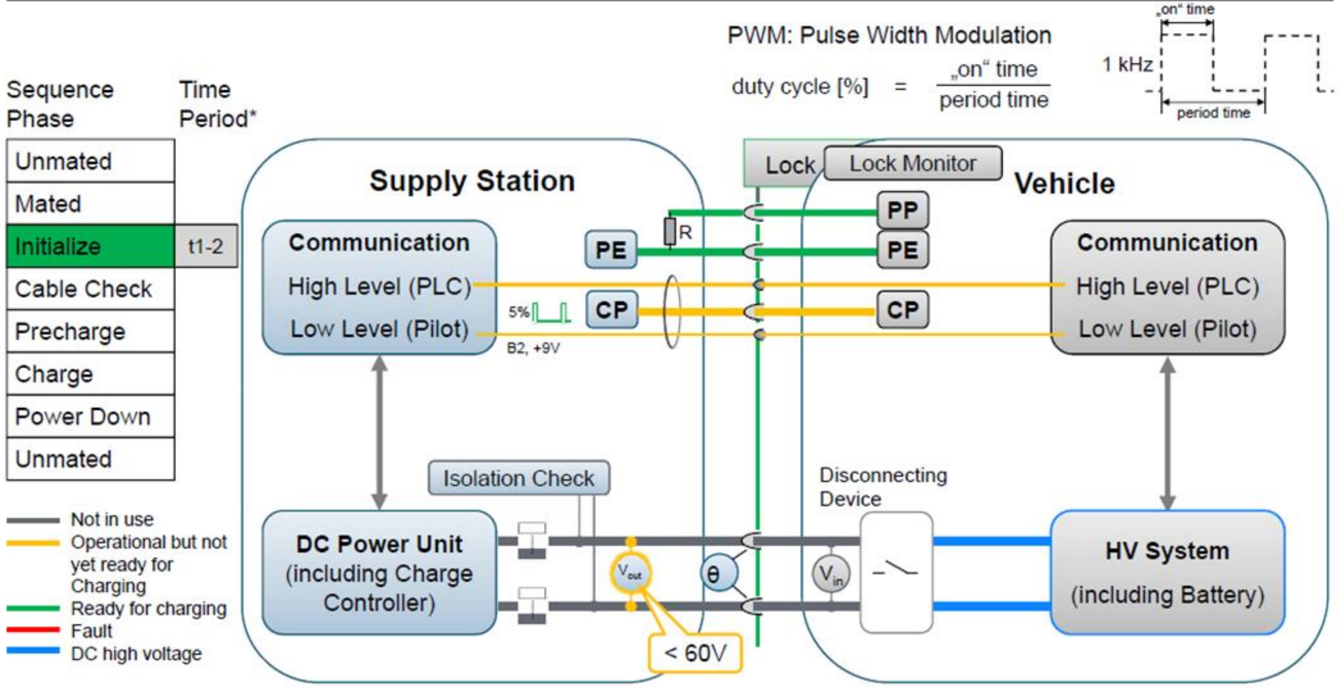
The PP pin transmits a signal which allows the EV to detect when it is plugged in.

PROTECTIVE EARTH

PE is an equipment grounding conductor

IEC 61851 – safety related standard for EV charging

Illustration of charging sequence with a simplified architecture on system level



➢ Establish PLC communication: Exchange operating limits and parameters of charging. Shutdown if d.c. Voltage > 60V or incompatibility of EV and d.c. supply is detected.

Control Pilot System Functions

State	Functions
State A +12V	▪ No coupler engagement
State B +9V	▪ Coupler engagement detected ▪ Vehicle not yet ready ▪ EVSE supply energy: Off
State C +6V	▪ Vehicle ready ▪ EVSE supply energy: On
State D +3V	▪ Vehicle ready ▪ EVSE supply energy: On ▪ Ventilation required
State E +0V	▪ Short of CP to PE (connection lost) ▪ Unlock plug after max. 30ms
State F -12V	▪ EVSE not available.

IEC 61851 – PWM and PLC

PWM signal on CP pin at 1kHz, duty cycle defines value of charging current, amplitude corresponds to State of EV – EVSE coupling. High level communication on PLC according to HomePlug GreenPHY, 2-30 MHz band

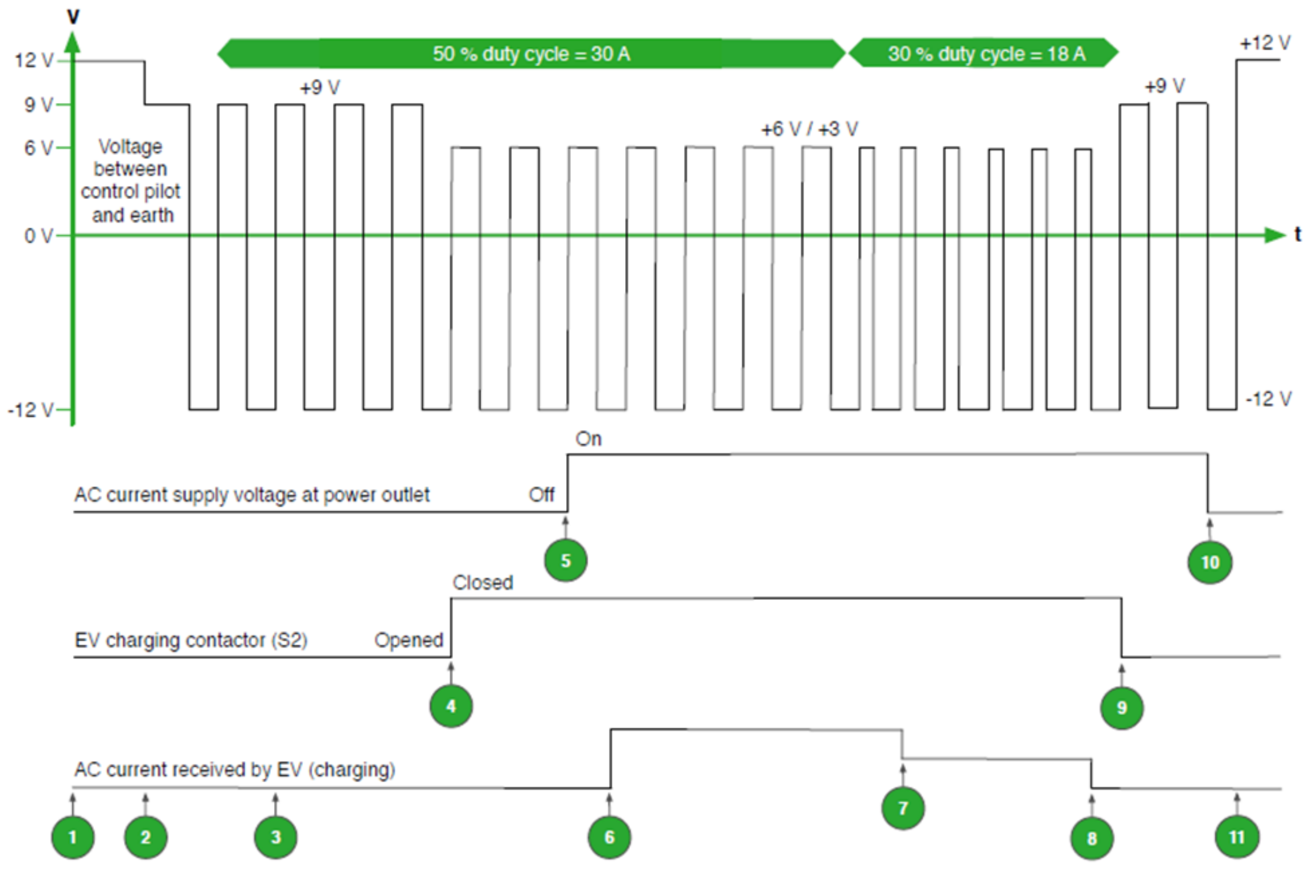


Figure 2.7.: Example of a charging session illustrated by means of a pulse-width modulated signal (inspired by [1], Annex A)

Communication Protocols in ISO 15118

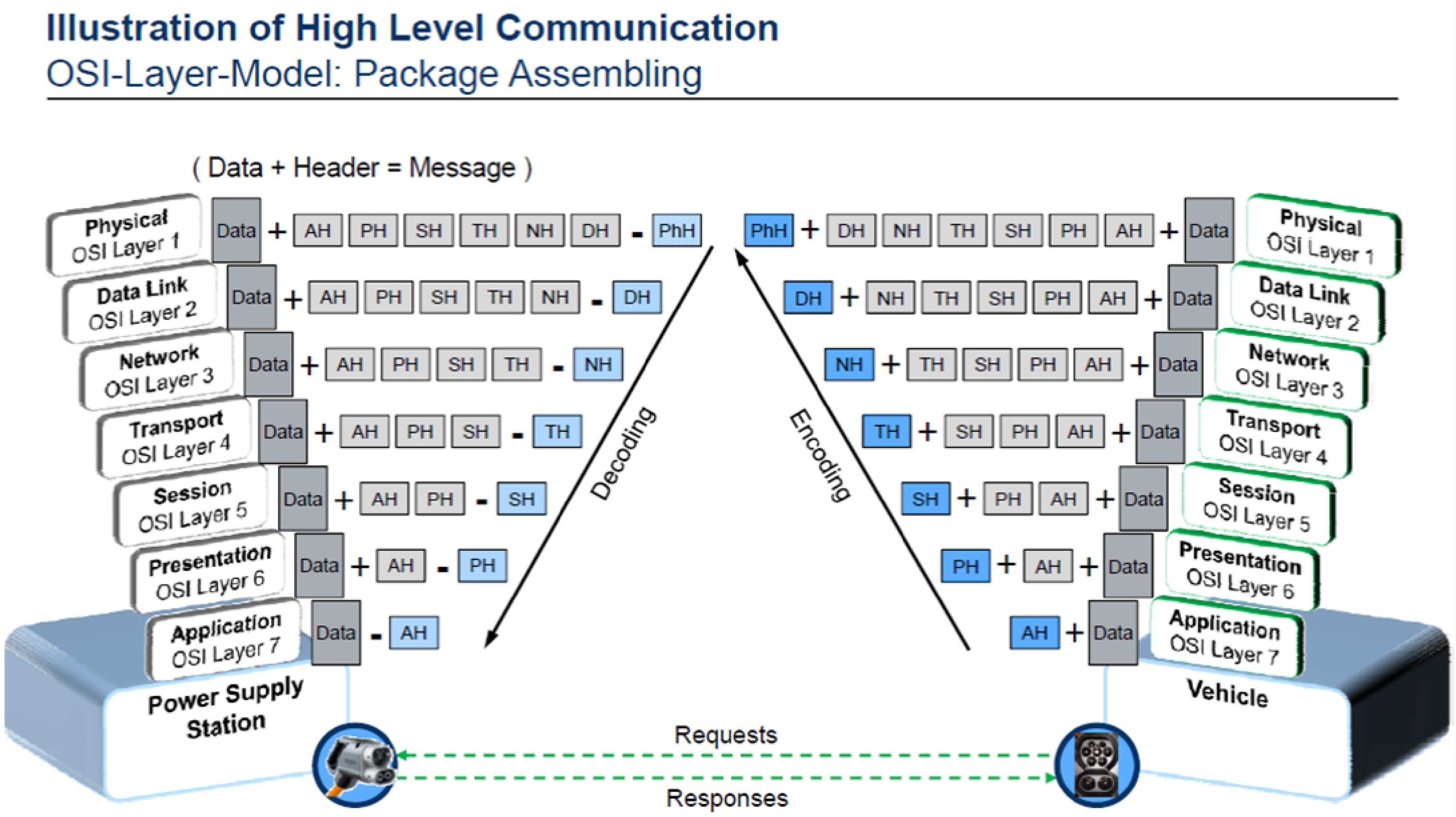
The operating principle of the OSI model is:
communication between two endpoints in a network is divided into seven groups of functions or layers.

The communication between EV and charging station to charge the battery, involves:

- **Electric vehicle communication controller (EVCC)**,
- **Supply equipment communication controller (SECC).**

The EVCC's message will be processed on the EV side by all functional layers, starting with the application layer and all the way down to the physical layer.
Once the message has traversed to the bottom layer, the EV sends the data to the charging station using a physical medium like a charging cable or a WiFi connection.
On the receiving end, the charging station will go through the same steps but in the opposite direction.
The complete data packet traverses from the bottom physical layer up to layer seven – which is called the application layer.

Communication Protocols in ISO 15118



- During the communication process each Layer is encoding (addition) or decoding (subtraction) the layer specific header.

Communication Protocols in ISO 15118
Application Layer

Text from pre-FDIS of ISO 15118-20.

Application layer messages
8.1 General information and definitions
The vehicle to grid application layer message definition describes the **client-server** based message exchange between EVCC and SECCs for the purpose of initializing and configuring the charge process of an EV.
The Message Set is designed to cover the use cases defined in Part 1 of this standard. The messages and the required message flow (i.e. communication protocol) represent the application layer according to the OSI layered architecture model.

A V2G message uses the EXI-based Presentation Layer as described in 7.9.1. The communication between EVCC and SECC at application layer level is based on **client/server architecture**. The EVCC always acts as a **client (service requester)** during the entire charging process, whereas the **SECC always acts as a server (service responder)**. Hence the EVCC always initiates communication by sending a request message to the SECC, then the SECC returns the corresponding response message. All messages exchanged between EVCC and SECC are described with their syntax and their semantics in 8.2, 8.3, 8.4 and 8.5. The entire XML schema definition describing V2G message set is included in Annex A.

Communication Protocols in ISO 15118

Layer 7 – Application Layer

The **application layer** message set defined in ISO 15118-2 is designed to support the energy transfer from an EVSE to an EV.

ISO 15118 defines two types of application messages:
SDP messages and V2G messages.

SDP = SECC Discovery Protocol consists of one request and response message.
The EV and the charging station use this message pair during the communication setup to agree upon a protocol version and they mutually exchange their respective **IP address and port**.

V2G message = Vehicle-to-Grid is used for all other communications, from starting a session and entering a charging loop to terminating a session. It consists of a **header and a body**, the header carries the session ID and a digital signature, while the body carries the message content.

Communication Protocols in ISO 15118 - Application Layer - SDP

7.10.1 SECC discovery protocol

7.10.1.1 General information

An EVCC uses the SECC discover protocol (SDP) to get the IP address and port number of the SECC. The SDP client sends out SECC discovery request messages to the local link (multicast) expecting any SDP server to answer its request with an SECC discovery response message containing this information.

After the EVCC received the IP address and the port number of the SECC, it can establish a transport layer connection to the SECC (refer to 7.3.4).

(Figure and text from preFDIS ISO 15118-20)

They refer to SECC Discovery Protocol (SDP)
The response message sent by SECC identifies its IP Address and Port

[V2G20-154] An SDP server shall send the SECC discovery response message with the payload as defined in Figure 16.

[V2G20-155] An SDP server shall send the payload in the order as shown in Figure 16. A byte with a lower number shall be sent before a byte with a higher number. The payload starts with byte 1 and ends with byte 20.

[V2G20-156] An SDP server shall send the fields "SECC IP address" and "SECC port" in big endian format: The most significant byte is sent first the least significant byte is sent last.

NOTE 1 The mechanism used by the SDP server to determine its own IP address is out of the scope of this standard.

NOTE 2 The source IP address and the source port of a received UDP packet is usually provided by the TCP/IP stack.

Byte No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	SECC IP Address																SECC Port		Security	Transport Protocol

Figure 16 — SECC discovery response message payload

Communication Protocols in ISO 15118

Layer 6 – Presentation layer

The application layer sends the data packet to the **presentation layer,** which translates the application data into a specific format that both the sending and receiving side will understand.

To speed up the transmission, the chosen format compresses the data to reduce the amount of bits and bytes to send.
ISO 15118 uses **Efficient XML Interchange (EXI)** for V2G messages, a binary data representation of data structures that are in the **Extensible Markup Language (XML)** form.

All V2G messages in ISO 15118 are defined in the XML format.
An XML message coming from the EV's application layer is encoded into the EXI format on the presentation layer before being delivered to the session layer beneath. Upon receiving the message, the charging station will then decode EXI into XML again. EXI is not applied for SDP messages.

Layer 5 - Session layer

It handles communication sessions between the EV and charging station.
A dedicated ISO 15118-protocol mechanism, called **Vehicle-to-Grid Transfer Protocol or V2GTP**, is utilized.
The V2GTP header contains important information about the payload type, stating whether it is an EXI encoded V2G type or an SDP message that is being transported.

Communication Protocols in ISO 15118

Efficient XML interchange

(Figure and text from preFDIS ISO 15118-20)

The Efficient XML interchange (EXI) format allows to use and process XML-based messages on a binary level.
Thus, the EXI format increases the processing speed of XML-based data as well as reduces the memory usage.
Basically, EXI is a W3C recommendation. The EXI format uses a relatively simple grammar driven approach that achieves very efficient encodings for a broad range of use cases.
It is not uncommon for EXI messages to be up to 100 times smaller than equivalent XML documents.
The EXI specification describes in a predefined process how schema information has to be transformed into EXI grammar.
(DOM = Document Object Model)

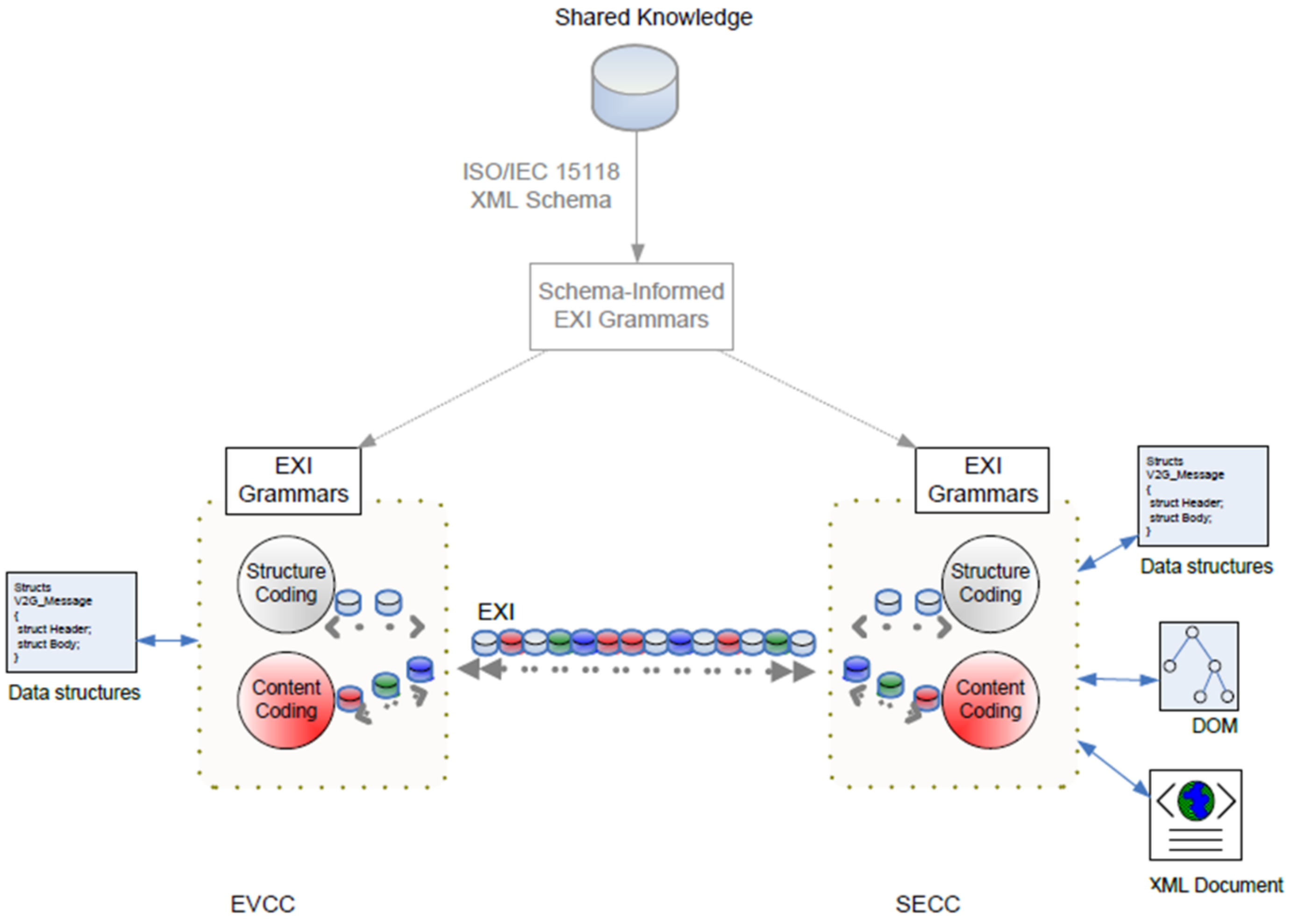


Figure 11 — Basic concept of EXI applied to V2G communication

Communication Protocols in ISO 15118

Layer 4 - Transport layer. Both the EV and the charging station need to establish a **TCP/IP connection** in order to reliably send data packets to each other via the communication link and guarantee error recovery and retransmissions, if needed. All V2G messages are transmitted using TCP.

TLS, the Transport Layer Security protocol, must be selected any time data needs to be secured by encryption.
On the other hand, SDP messages are transmitted using the **User Datagram Protocol (UDP).**

UDP does not focus on reliability of data transmission. Instead, UDP is primarily used for applications that focus on very quick transmission of data packets from point to point in a communication network.

UDP is a connectionless protocol with a minimum of protocol mechanisms.
UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues.
UDP does not provide the reliability and ordering guarantees that TCP does.
Packets may arrive out of order or may be lost without notification of the sender or receiver. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes.
UDP is located on the Transport Layer of the OSI layered architecture model.

Communication Protocols in ISO 15118

Layer 3 – Network layer

TCP makes use of **Internet Protocol (IP)** to assign unique IP addresses for the
EVCC and SECC, needed to route data packets between both entities.
Other protocol mechanisms applied on the network layer include **Stateless Address Autoconfiguration (SLAAC) and Dynamic Host Configuration Protocol (DHCP).**

Layer 2 and 1 – Data link and physical layer

The two lowest layers of the seven layers of communication are the **data link layer and the physical layer.**
On the physical layer, data is transmitted using electric signals such as voltage or radio frequencies.
During wired communication, the EV exchanges data with the directly connected charging
station using digital signals modulated on a wire inside the charging cable, called the **Control Pilot (CP) pin**, when it is plugged into both the EV and charging station.

Security - ISO 15118-1 / Annex B

- **Confidentiality**

is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms, which render data unintelligible.

- **Data integrity**

is a service that addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

- **Authentication**

is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons, this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

Non-repudiation is a service that prevents an entity from denying previous commitments or actions.
Reliability / Availability is the property of a service of being available and working reliably.

Figure from ISO 15118-1

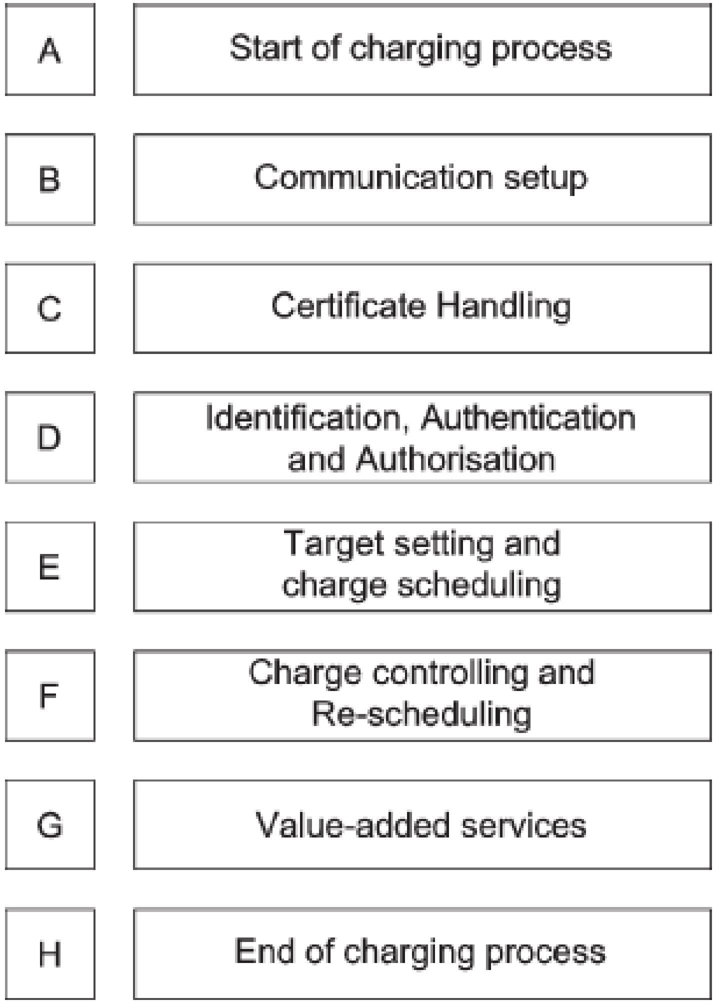


Figure 2 — Use case elements function groups

Message Sequence for an ISO 15118-2 Charging Session

As an example it is shown a sequence of messages being exchanged for an **Alternating Current (AC) charging session** carried out via ISO 15118-2.
The entities that carry out certain actions, such as sending or receiving messages and opening or closing contactors, are illustrated in the boxes at the top.
States A, B, and C relate to certain voltage levels measured by the charging station and are defined in IEC 61851.

ISO 15118 builds and expands on IEC 61851 and enables digital communication between EVCC and SECC, which starts as soon as the duty-cycle of the pulse width modulation (PWM) signal is set to 5%, as defined in IEC 61851.

All the messages illustrated in the next steps are sent as V2G messages, each consisting of a header and a body. The header carries information including the session ID and an optional digital signature, the body holds the actual message content

Communication Protocols in ISO 15118

Figures and text from pre-FDIS of ISO 15118-20.

Protocol Data Unit of V2GTP message PDU consists of Header and Payload

V2G transfer protocol
General information
The V2G transfer protocol (V2GTP) is a compact communication protocol to transfer V2G messages between two V2GTP entities. It mainly consists of a header and payload definition that allow to be separated and process V2G messages efficiently. V2GTP is the standard transfer protocol between the EVCC and SECC but may also be used for communication with other V2G Entities that support the V2GTP protocol.

7.8.3 Protocol data unit

7.8.3.1 Structure

The V2GTP PDU consists of a header and a body section as shown in Figure 8.

Header (8 Bytes)	Payload (0-4294967295 Bytes)

Figure 8 — V2GTP message structure

The payload contains the application data (e.g. a V2G message). The header separates the payloads (i.e. individual V2GTP messages) within a byte stream and gives information for the payload processing.

The V2GTP message header structure is shown in Figure 9 and described in Table 7. The supported payload types are described in Table 8.

Byte No.	1	2	3	4	5	6	7	8
Header Field	Protocol Version	Inverse Protocol Version	Payload Type		Payload Length			

Figure 9 — V2GTP message header structure

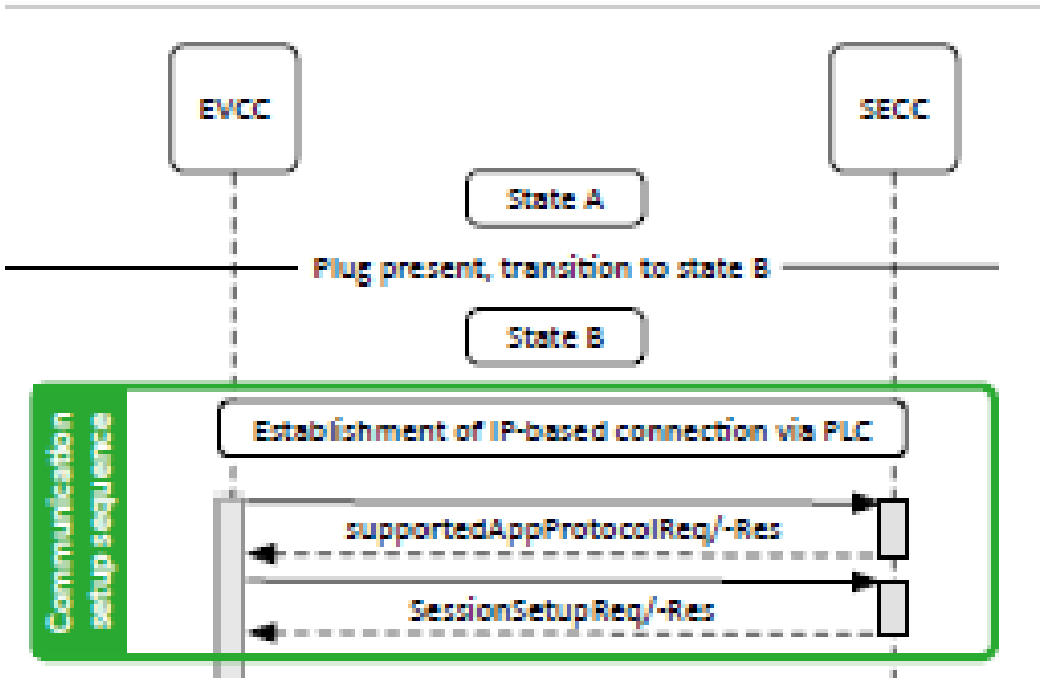
Message Sequence for an ISO 15118 Charging Session

A - Start of charging process
B - Communication setup

The sequence starts with the **supportedAppProtocolRequest.** The EV and charging station use this request-response message pair to agree upon a protocol version.

Next is **SessionSetupRequest** to assign a unique session ID for a communication session.

The session can be paused and resumed at a later time using the same session ID.
In this case, the previously agreed upon charging parameters will be applied again to ensure charging continues as originally intended by the driver.



Message Sequence for an ISO 15118 Charging Session

Figures from pre-FDIS of ISO 15118-20
XML Schema. The message is **supportedAppProtocolRequest.**

8.2.2 Message definition supportedAppProtocolReq and supportedAppProtocolRes

[V2G20-175] The SECC and EVCC shall implement the message elements as defined in Figure 19.

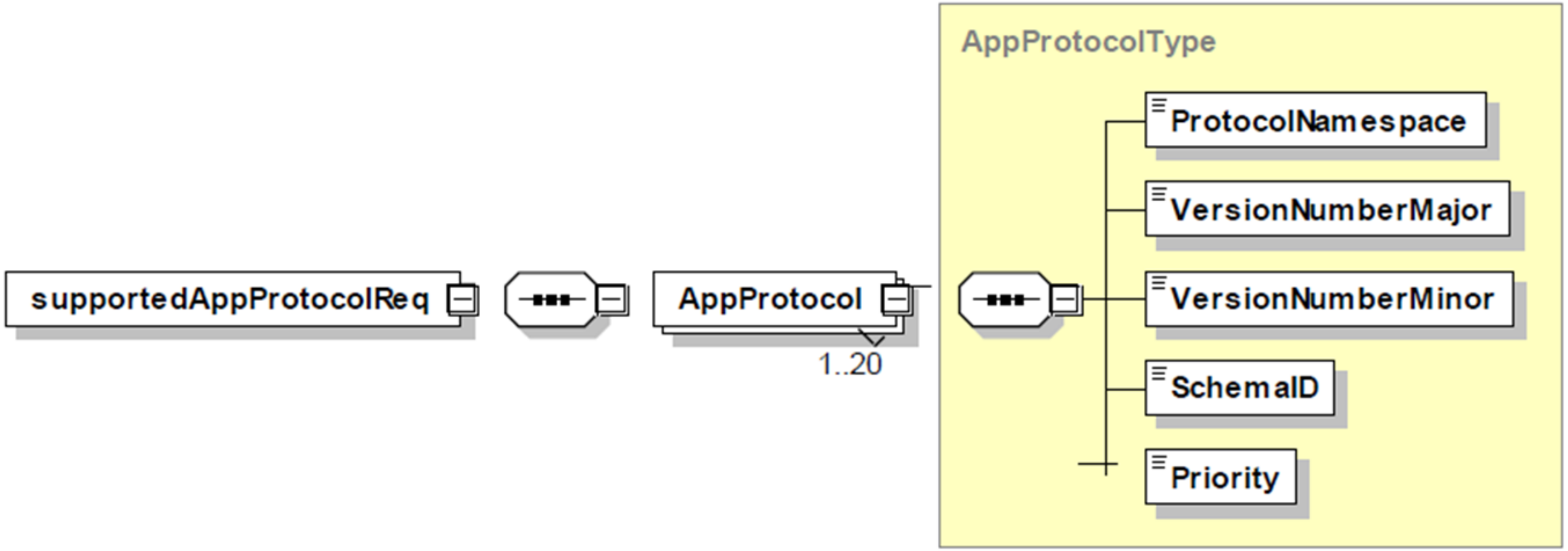


Figure 19 — Schema diagram – supportedAppProtocolReq

Message Sequence for an ISO 15118 Charging Session

Text from pre-FDIS of ISO 15118-20

Example of V2G message, XML language. **supportedAppProtocolRequest.**

The following is V2G message example 1 – supportedAppProtocolReq: protocol prioritization.


```xml
<?xml version="1.0" encoding="UTF-8"?>
<n1:supportedAppProtocolReq xsi:schemaLocation=" urn:iso:std:iso:15118:-20:AppProtocol ../V2G_CI_AppProtocol.xsd"
xmlns:n1="urn:iso:15118:2:2015:AppProtocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
	<AppProtocol>
		<ProtocolNamespace>urn:iso:15118:2:2015:MsgDef</ProtocolNamespace>
		<VersionNumberMajor>3</VersionNumberMajor>
		<VersionNumberMinor>0</VersionNumberMinor>
		<SchemaID>10</SchemaID>
		<Priority>1</Priority>
	</AppProtocol>

	<AppProtocol>
		<ProtocolNamespace>urn:iso:15118:2:2013:MsgDef</ProtocolNamespace>
		<VersionNumberMajor>2</VersionNumberMajor>
		<VersionNumberMinor>0</VersionNumberMinor>
		<SchemaID>20</SchemaID>
		<Priority>2</Priority>
	</AppProtocol>
	<AppProtocol>
		<ProtocolNamespace>urn:iso:15118:2:2010:MsgDef</ProtocolNamespace>
		<VersionNumberMajor>1</VersionNumberMajor>
		<VersionNumberMinor>0</VersionNumberMinor>
		<SchemaID>30</SchemaID>
		<Priority>3</Priority>
	</AppProtocol>
</n1:supportedAppProtocolReq>
```


The following is V2G message example 2 – supportedAppProtocolRes: protocol prioritization.

Message Sequence for an ISO 15118 Charging Session

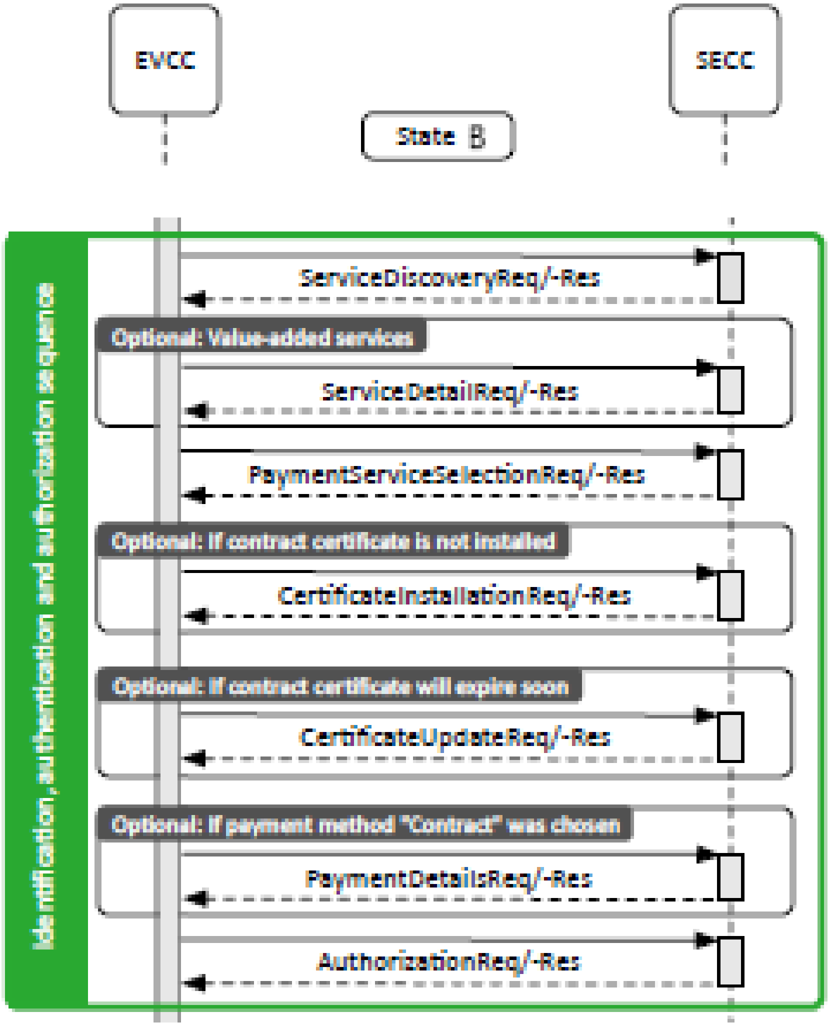
C – Certificate Handling

D - Identification, Authentication and Authorisation

EV will use the **ServiceDiscoveryRequest** to ask the charging station about its offerings.
These services include:
AC single-phase charging or AC three-phase charging,
Variations of Direct Current (DC) charging,
The available identification mechanisms

- **External Identification Means (EIM) or**
- **Plug & Charge**

The EV can request more details for each service by using the optional **ServiceDetailRequest** message.
Once the identification mechanism, charging mode, and optional value-added services to use are clear, the EV then will inform the charging station with the **PaymentServiceSelectionRequest**.
Which is related to the authentication and authorization method.



Service messages

Table from
Pre-FDIS ISO 15118-20

Messages:

ServiceDiscoveryRequest - Res

ServiceDetailRequest - Res

8.6.3 Selection of service and service parameters

8.6.3.1 Overview

This subclause defines the reserved ServiceID ranges and the relevant services. These are exchanged and negotiated between the EVCC and the SECC by exchanging service discovery and service detail request response messages.

[V2G20-1355] The EVCC and the SECC shall implement the ServiceIDs as defined in Table 186.

Table 186 — Definition of ServiceID, ServiceName and ServiceCategory

ServiceID (unsignedshort)	ServiceName	Description
0		reserved by ISO
1	AC	AC Charging, physical layer according to ISO 15118-3/8
2	DC	DC Charging, physical layer according to ISO 15118-3/8
3	WPT	WPT, physical layer according to ISO 15118-8
4	AC_ACD	AC Charging with ACD, physical layer according to ISO 15118-8
5	DC_ACD	DC Charging with ACD, physical layer according to ISO 15118-8
6	WPT_ACD	WPT with ACD, physical layer according to ISO 15118-8
7	AC_BPT	AC Charging with BPT, physical layer according to ISO 15118-3/8
8	DC_BPT	DC Charging with BPT, physical layer according to ISO 15118-3/8

Authentication and authorization in ISO 15118

ISO 15118 provides two ways of authenticating and authorizing a user for a charging session:
External Identification Means (EIM) and Plug & Charge (PnC).

EIM represents any user authentication method that requires additional action by the driver such as presenting an RFID card to the reader at the charging station.
Plug & Charge is a more user-convenient way of charging that also enables <u>security features </u>and ensures data integrity and authenticity <u>through digital certificates and digital signatures.</u>

In case the EV selects Plug & Charge as an identification method, a valid digital contract certificate must be installed in order for the charging station to automatically authenticate and authorize the driver.
If the EV does not yet have this certificate installed or if its existing contract certificate has expired, the EV can use the **CertificateInstallation** message pair to install a new contract certificate from the charging station.

In cases where an EV has a soon-to-be expiring contract certificate installed for Plug & Charge, the EV can be programmed to initiate a **CertificateUpdate** message pair to receive a new contract certificate.
If the EV is programmed to select Plug & Charge as its identification method, the EV will need to present its contract certificate to the charging station in order for the driver to be authenticated and authorized for charging.
This is done using the **PaymentDetailsRequest** message.

Identification for an ISO 15118 Charging Session

Figure from ISO-15118-1

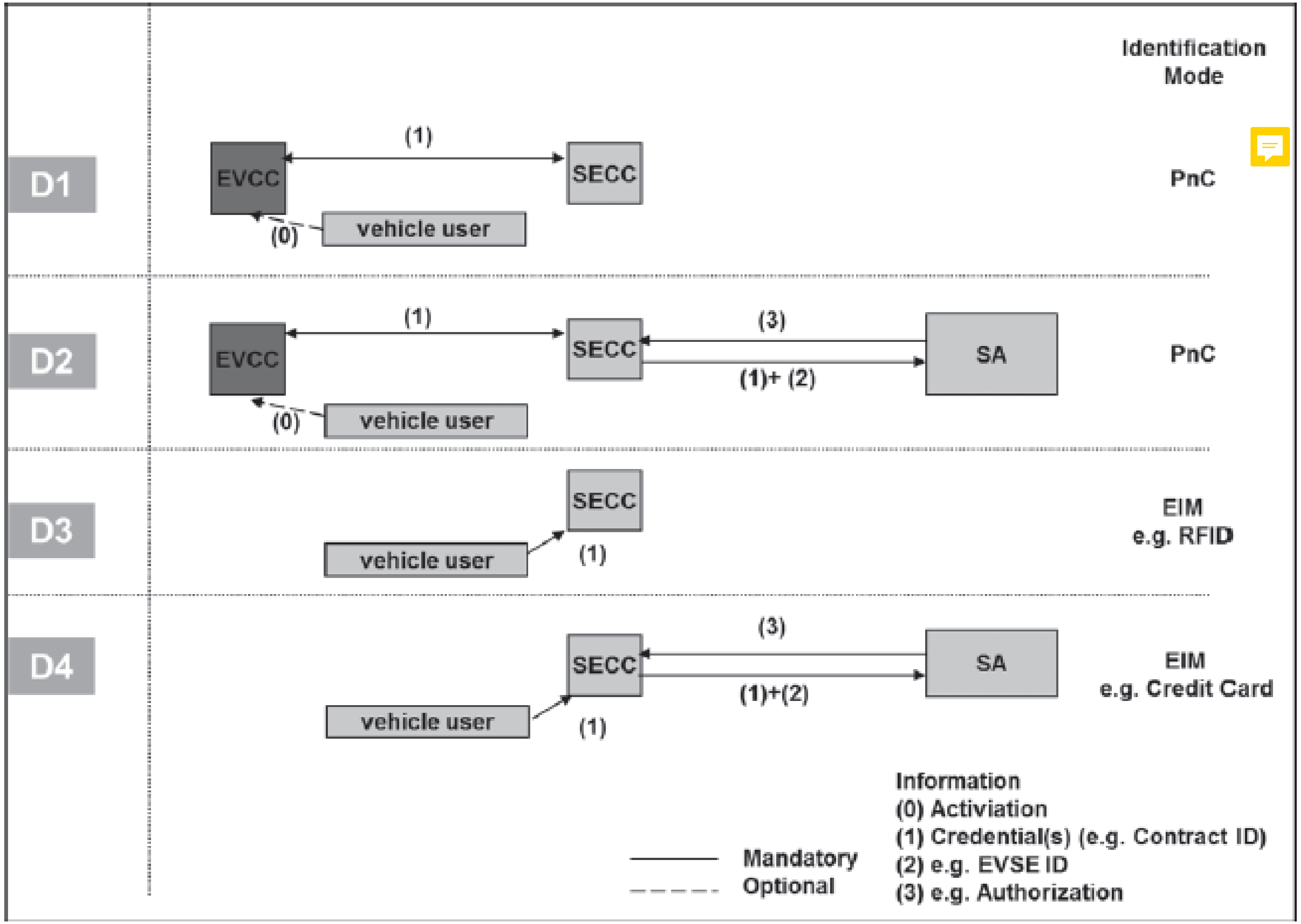
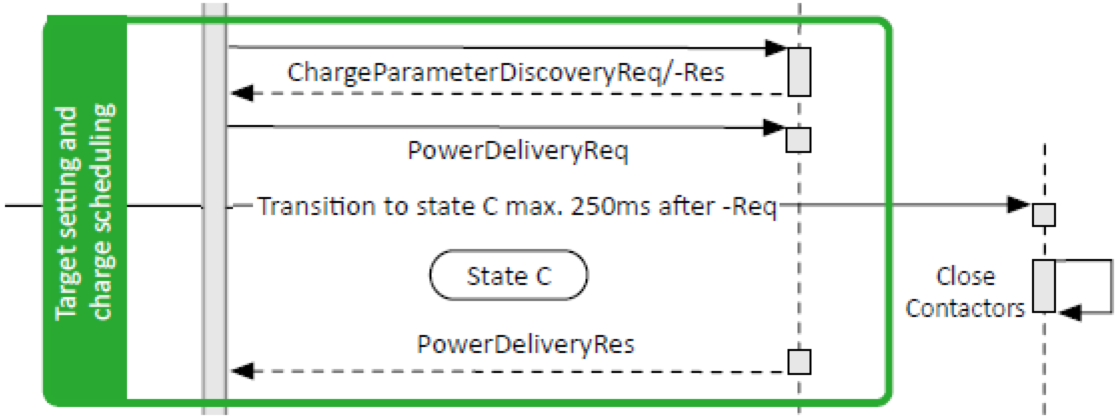


Figure 3 — Graphical overview of scenarios for identification

Message Sequence for an ISO 15118 Charging Session

E – Target setting and charge scheduling



With the **ChargeParameterDiscoveryRequest** and -Response messages, the EV and charging station mutually exchange their respective technical charging limits by communicating their maximum and minimal allowed voltage levels and currents.

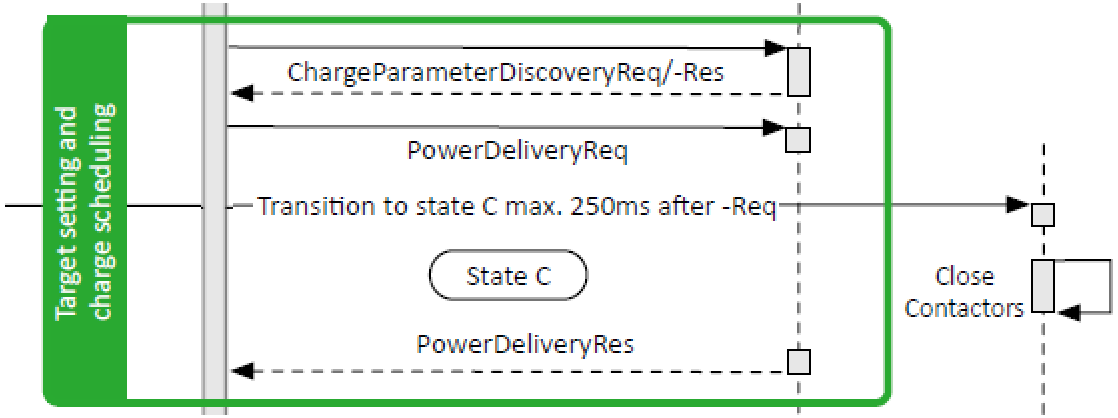
The EV also informs the charging station of the amount of energy needed and the desired departure time indicated by the driver.

The SECC will then calculate a charge schedule to propose to the EV. The proposed schedule will include the maximum power with which the EV is allowed to charge while connected to the charging station as well as an optional **SalesTariff.**

The SalesTariff includes schedules that provide information on cost over time, cost in relation to power demand and amount of energy, or a combination of these, aimed at incentivizing the EV to engage in a certain charging behavior.

Message Sequence for an ISO 15118 Charging Session

E – Target setting and charge scheduling



Once the charging station sends the proposed charging schedule to the EV, the EVCC will calculate a charging schedule of its own. It does so by taking into account several factors like the technical restrictions imposed by the battery management system and financial incentives provided by **ChargeParameterDiscoveryResponse** message. This EV charging schedule must not exceed the upper power limits provided by the charging station. The EVCC then sends its schedule to the SECC via the **PowerDeliveryRequest** message. The EVCC can decide to instantly start charging or to delay the charging process. It indicates this intent by setting the parameter ”ChargeProgress” to either ”Start” or ”Stop”.

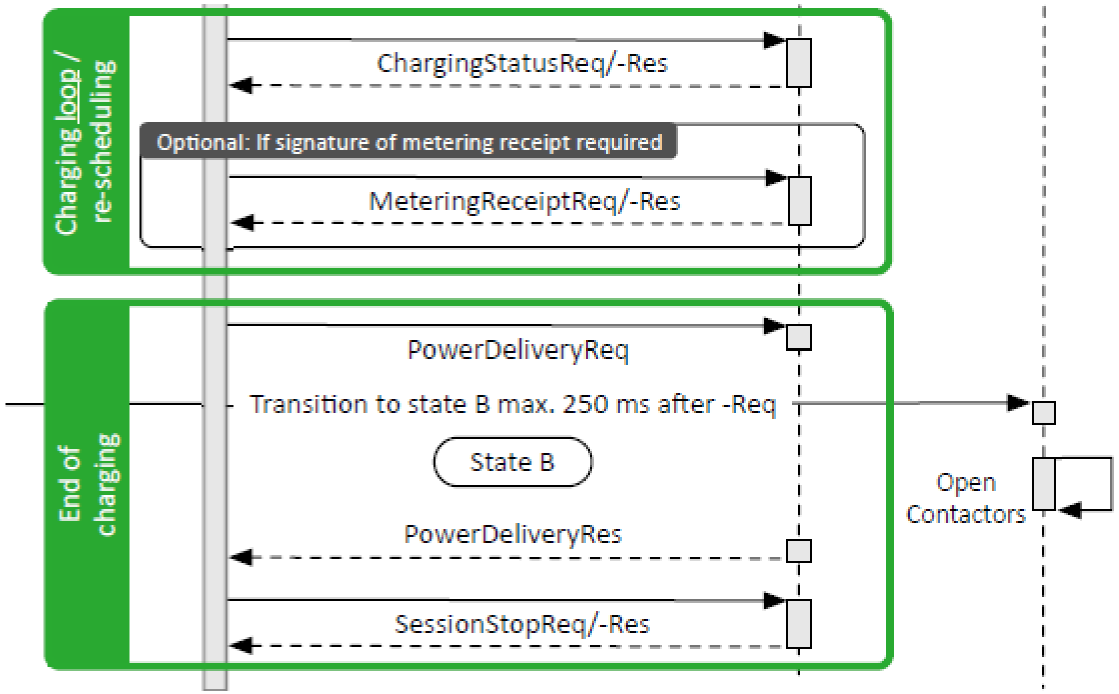
If the parameter is set to ”Start”, the EV will trigger a switch to cause the voltage level to drop from 9 V to 6 V. According to IEC 61851, this will cause a state transition from state B to state C: ”EV detected and ready for charging”. The charging station will then close its contactor to initiate the flow of energy.

Message Sequence for an ISO 15118 Charging Session

F – Charge controlling and Re-scheduling

A charging loop starts. The **ChargingStatusRequest** message pair is used to trigger a response message from the charging station during charging. It enables the charging station to react to any unforeseen situations within the local electrical grid. One such circumstance would occur if several EVs were to suddenly begin charging at the same time and all request to be charged as quickly as possible. If the charging station's local transformer cannot handle this situation, then some EVs will need to be charged at a lower level of power. Depending on the individual circumstance, the charging station can ask the EV to renegotiate its requested charging schedule or even demand the EV instantly stop charging to prevent the grid from a potentially dangerous overload.

The charging station can also request a digital signature from the EV for the current meter values by using the **MeteringReceiptRequest** message. This triggers the EV to send a signature declaring that it has seen the meter values.

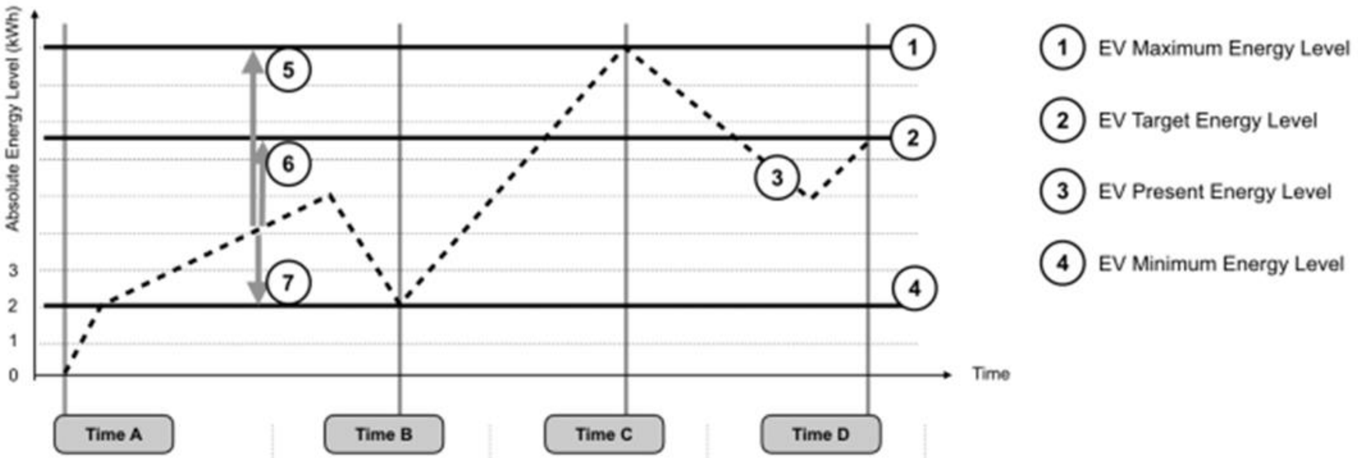


Message Sequence for an ISO 15118 Charging Session

Text and graph from pre-FDIS of ISO 15118-20

8.5.2.6.3 **Rules related to EV Energy Request values**

The EV Energy Request parameters defined below are used by the EV to inform the EVSE of its energy demands and limitations. They are instantaneous values that will change over time during the energy transfer loops. They are calculated, updated and sent during the energy transfer loop by the EV and they are one of the foundations for the Dynamic control mode



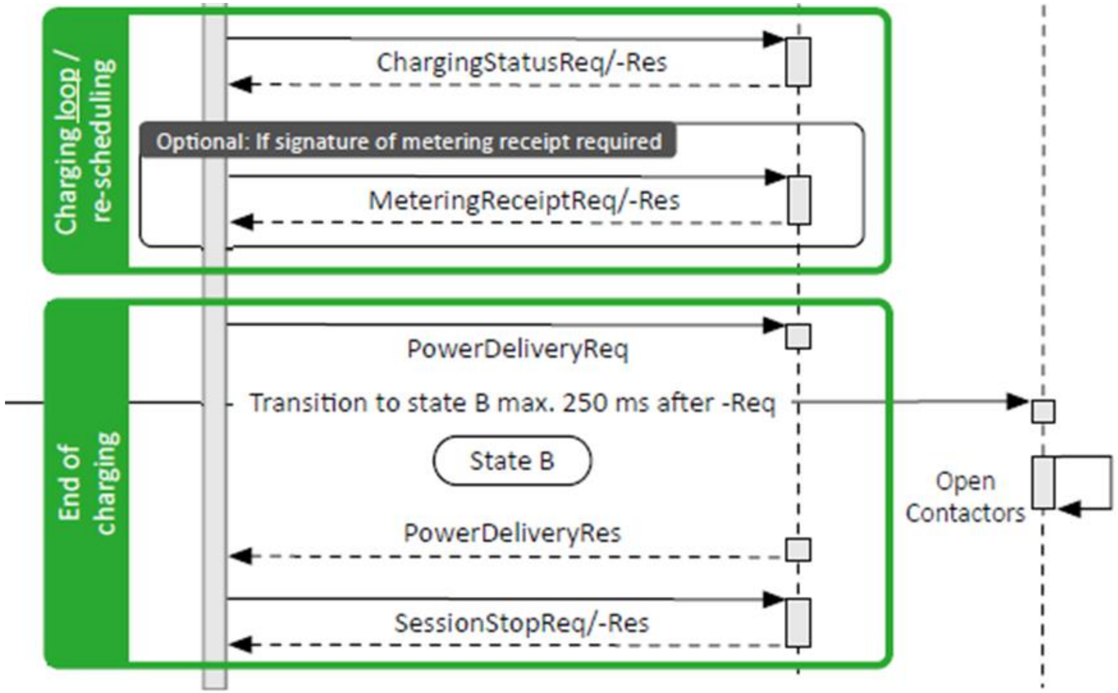
Time A	Time B	Time C	Time D	
9.0	7.0	0.0	2.5	5 **EVMaximumEnergyRequest**
6.5	4.5	-2.5	0.0	6 **EVTargetEnergyRequest**
2.0	0.0	-7.0	-4.5	7 **EVMinimumEnergyRequest**
The session starts with an immediate need to charge in order to reach the EV Minimum Energy Level.	Further discharging is not possible since the EV Minimum Energy Level has been reached.	EV Maximum Energy Level has been reached no further charging is allowed.	The EV Target Energy Level has been reached at departure time.	Comment

Message Sequence for an ISO 15118 Charging Session

H – End of charging process

As soon as the EV intends to pause or end the charging session based on its calculated charging schedule, it will send another **PowerDeliveryRequest** message with its parameter ChargeProgress set to ”Stop”.

The communication concludes with **SessionStopReq/Res** message pair.
The request message’s ChargingSession parameter can be set to either ”Terminate” or ”Pause”.
If the charging session is to be paused, certain parameters, like the agreed-upon charging schedule, are temporarily stored by the charging station so it can apply these values when the charging resumes.



Comparison of standards

	DC	AC	Security	Plug & Charge	Smart Charging	Wireless Power Transfer	Bidirectional power transfer	ACD (Pantograph for busses)
DIN SPEC 70121 (2012 / 2014)	✓							
CHAdeMO[1]	✓						✓	
ISO 15118-2 (2014)	✓	✓	✓	✓	✓			
ISO 15118-20 (2020)	✓	✓	✓	✓	✓	✓	✓	✓

IEC 63110

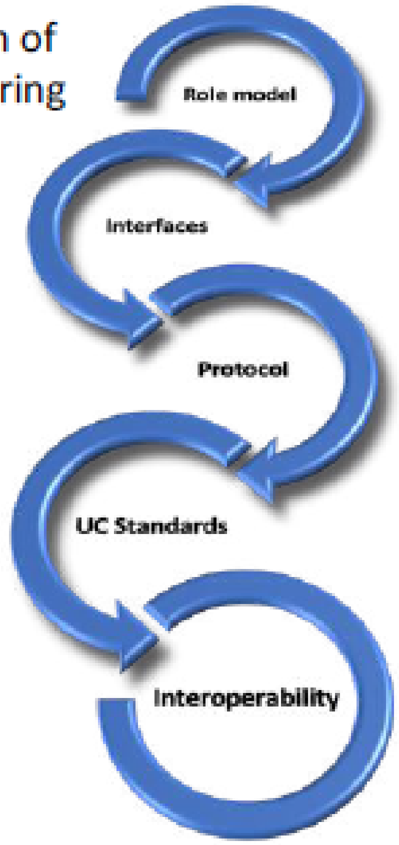
“Management of Electric Vehicles charging discharging infrastructures”

Standard developed by

IEC TC69 / JWG11

Why a role model is so important ?

A role model is a conceptual representation of the interactions between all actors considering the roles they play in a specific market.



Communication protocols allow interactions connecting those roles through interfaces.

Communication standards describe these protocols and their ways to exchange the information captured in the use cases.

The main objective of standards is to ensure interoperability between all the actors through their different roles in their market.

Business use cases and role model

Communication standards are the description of protocols and their way to exchange information between roles in a market model.

To ensure interoperability between roles, the communication standards describe "what" is exchanged (the information) and "how" (the protocol) it is transferred from one interface to another.

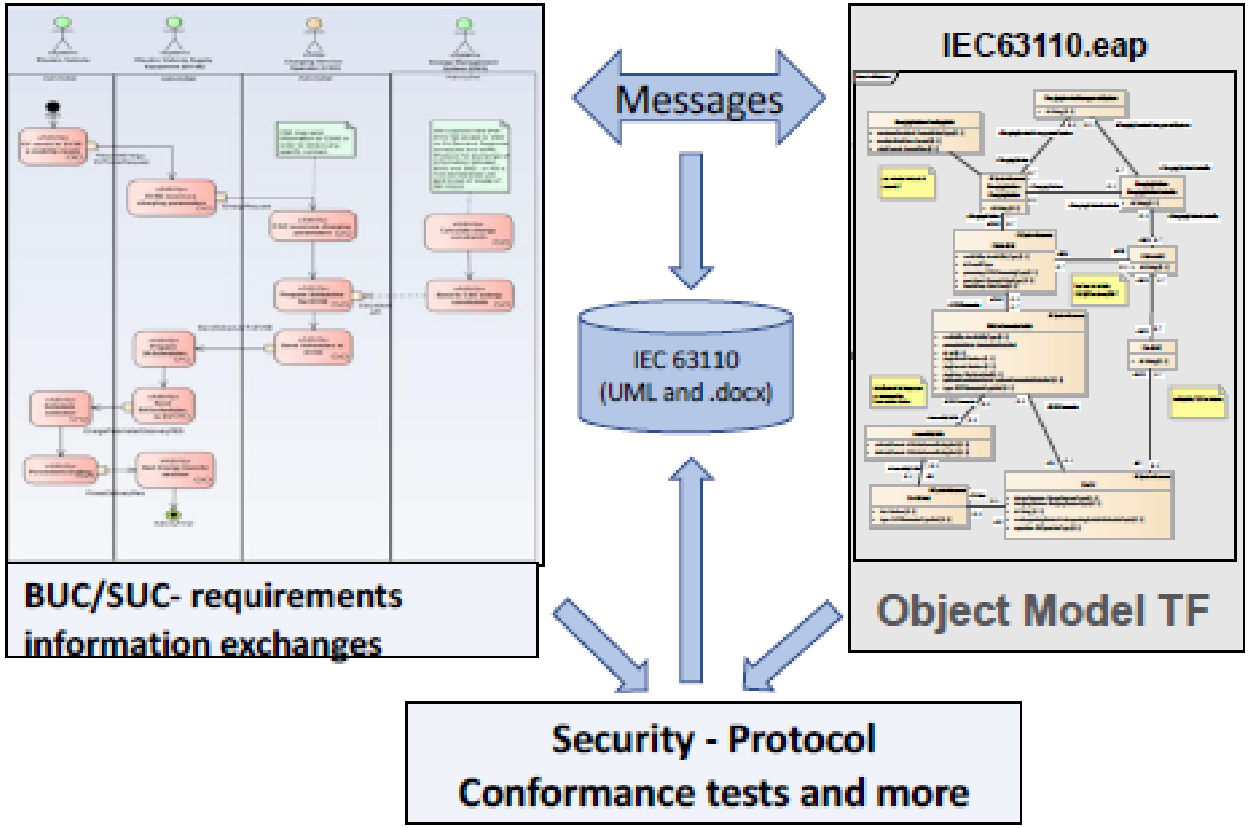
The "what" is described in Business use cases

"How" the "what" is transmitted is described in messages transported by protocols.

Modern communication standards like IEC 63110 has one specific document for Business Use Cases and another one for messages and protocol specification.

Relations between Use cases – Object model - Messages

1. Use cases describe information exchange between systems and roles.
2. The Object model contains Packages describing devices variables and functions.
3. Messages are the way to read/write devices variables of the object model as described in the use cases.
4. Once the use cases and the objects model are in place messages can be automatically derived.



Development methodology based on Enterprise Architect, IEC 62913-1 and IEC 62559

Use cases

- The Business Use cases described in IEC 63110-1 document are at the source of IEC 63110 protocol. They capture the common, repeated, deployed or envisioned usages of the e-mobility environment.
- In IEC 63110-1 document the BUC are divided in 3 domains:
  - Energy Transfer Services
  - E-mobility services
  - Charging Station Management

Each of these 3 domains relies on business use cases that describe situations where business actors realise some objectives. The three domains, although they may exchange information, are relatively independent.

Business use cases developed in IEC 63110-1

Energy Transfer Domain

- Smart charging - discharging
- Demand Response
- CSMS - CEM information exchange
- DSO curtailment
- Dynamic Control mode
- ....

E-mobility service domain

- CS - CSMS information exchange during a Service Session
- Remote authorisation by external means
- Remote authorisation with locally presented credentials
- Reservation of an EVSE
- Contract tariff information
- ISO 15118 contract certificates
- ...

Management of Charging Station

- Migration of a CS to a new CSMS
- CS diagnostics
- Fault code provisioning
- Information display on the EVSE
- Manage CS configuration
- Set log criteria
- CS monitoring
- Update CS and CSMS certificates
- Information deletion triggered by EVU or CSMS
- Firmware updates
- Public tariffs information

Sessions and Transactions
Service Detail Record production

More than 30 use cases have been developed so far !

IEC 63110 – Communication Architecture

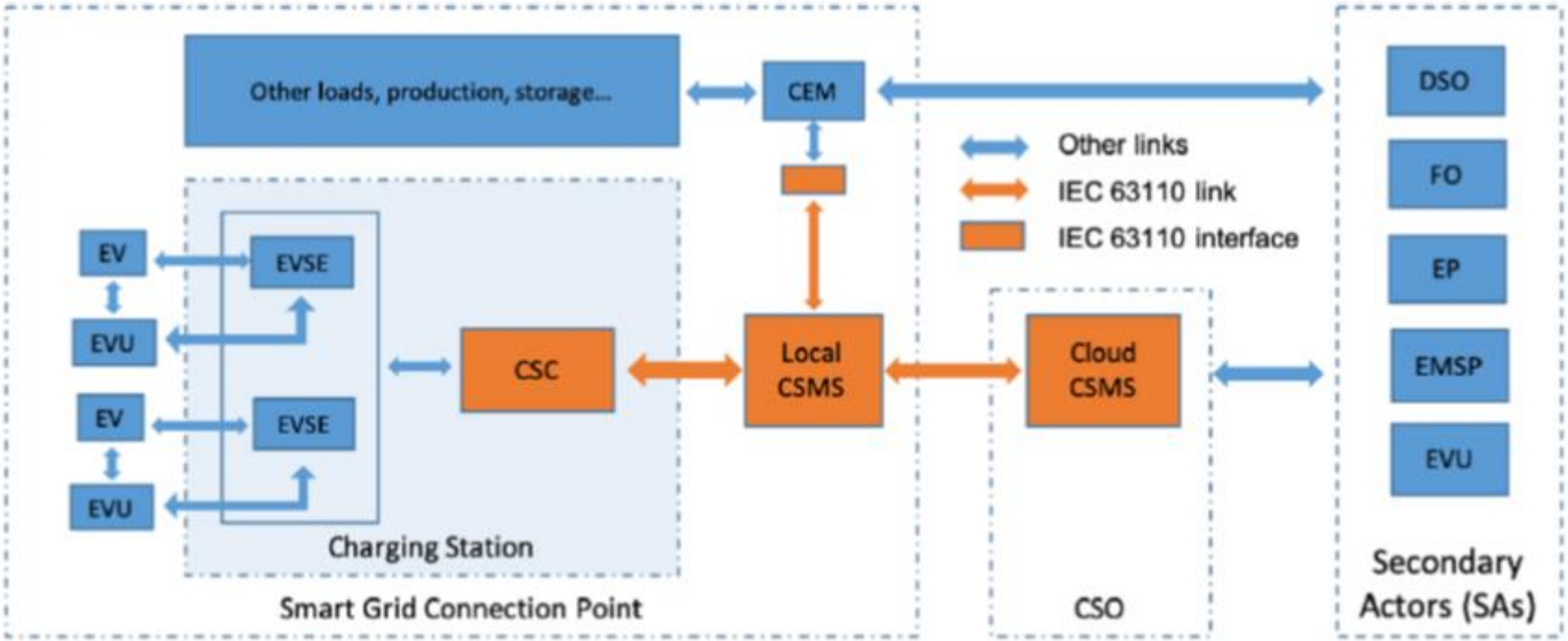
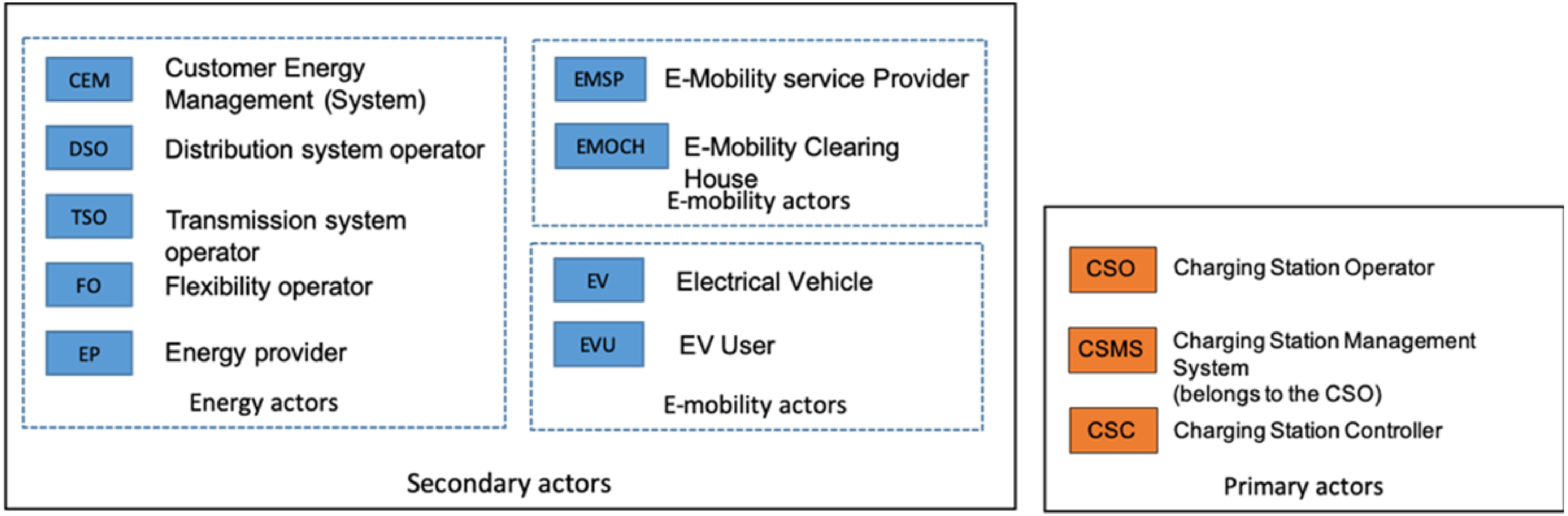
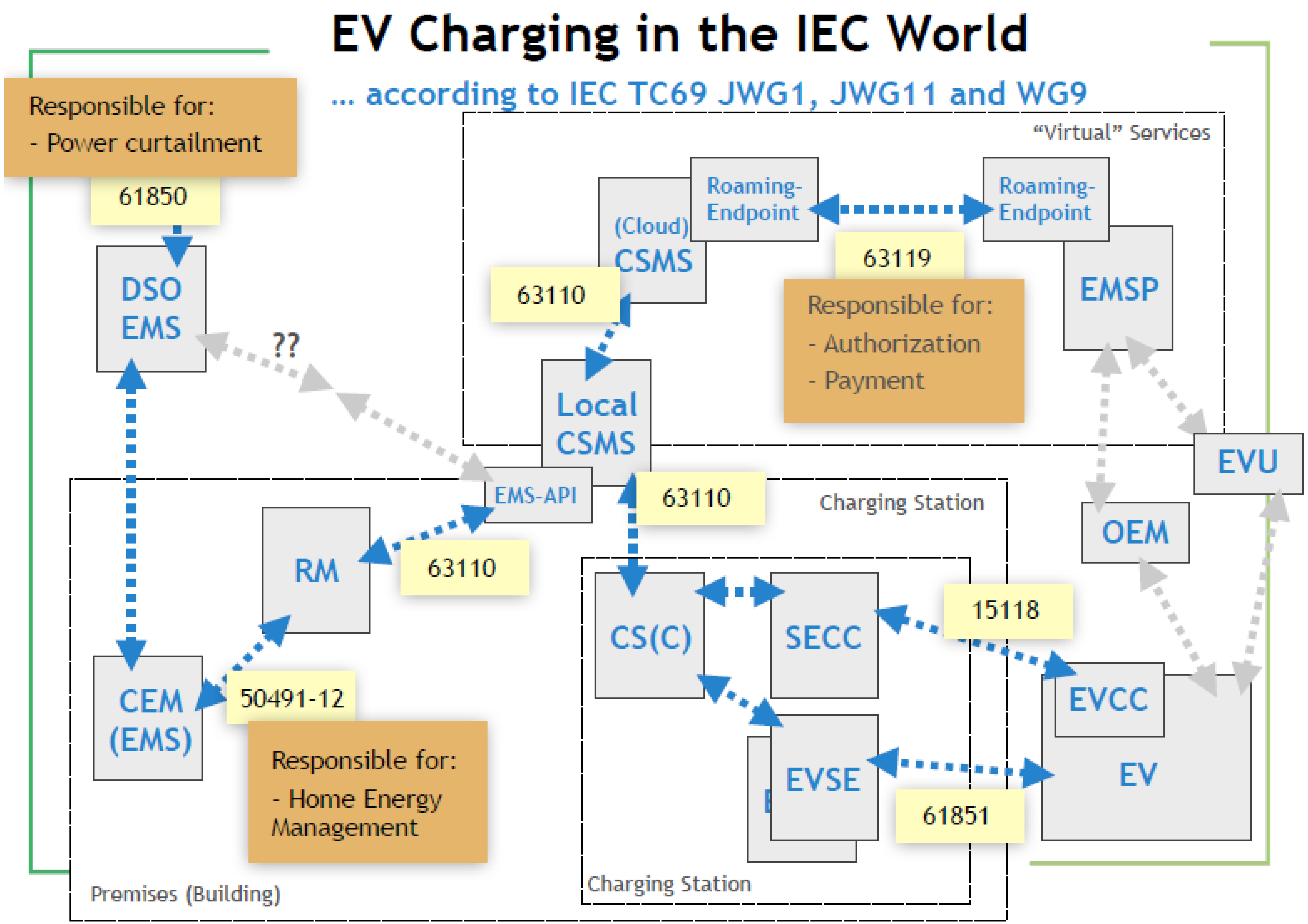


Figure 6 Generic communication architecture- system view

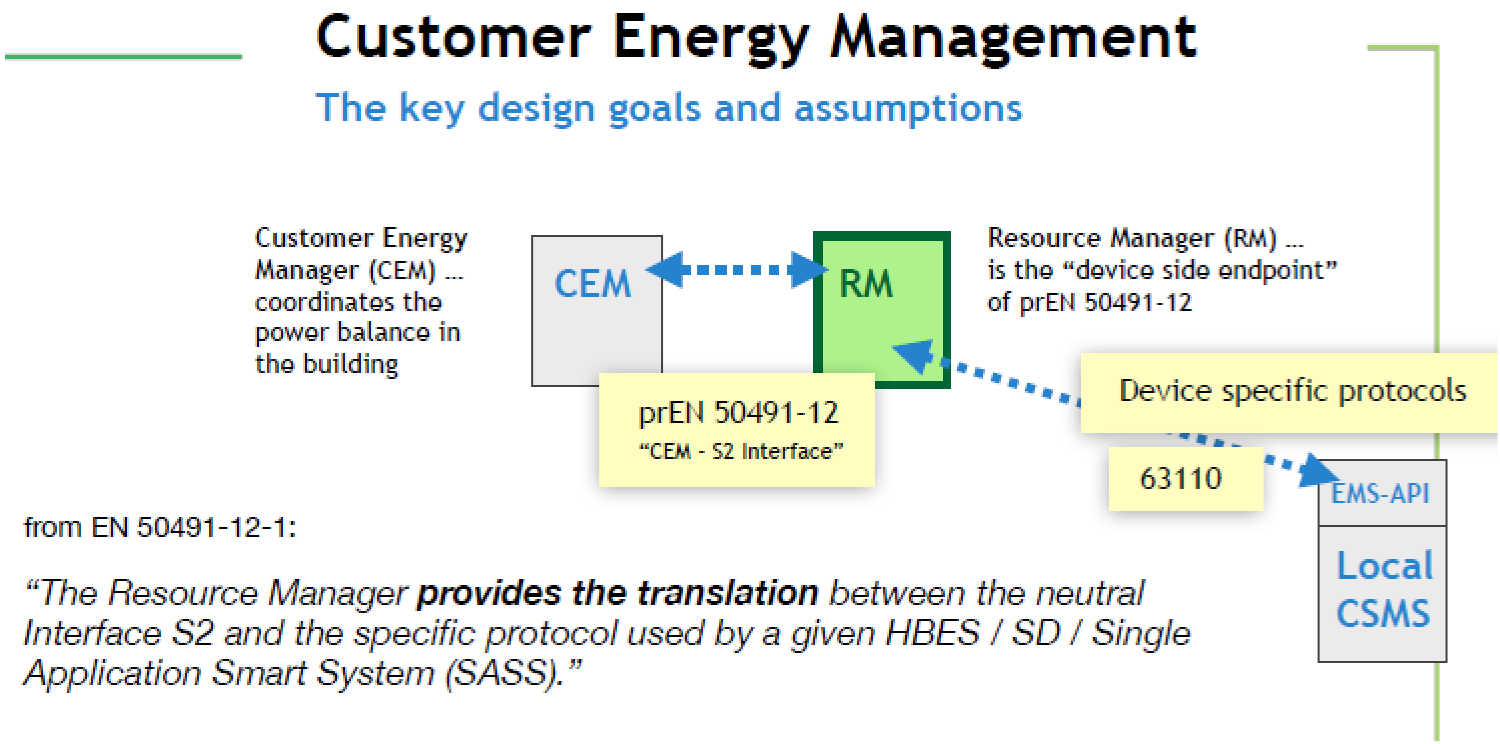
IEC 63110 – Communication Architecture - Actors



IEC 63110 – Communication Architecture



IEC 63110 – Communication Architecture



IEC 63110 – Communication Architecture

Types of things to manage

+ There are two types of things to manage:
  - Physical entities (e.g. Charging stations, servers)
  - Logical entities (e.g. regions, sites)

+ We need to keep this distinction very clear in the 63110-1 document.

Physical entities

+ The complete set of physical entities to manage:
  - Servers (i.e. CSMS)
  - Charging Stations (i.e. CS)
  - EVSE (the equipment used to charge EVs)
  - Power units (PU) (i.e. the units that convert grid power into DC power)

+ In addition, there are physical entities to interact with:
  - Resource Managers (these are the middle-men between CSMS and CEM)

IEC 63110 – Communication Architecture

Logical entities

+ The hierarchy of management entities:
  - Cloud CSMS
  - Regional CSMS
  - Site CSMS
  - Zone CSMS
+ The hierarchy of groupings of physical entities:
  - Root (e.g. top level for the CSO)
  - Region (e.g. Countries or states with distinct laws)
  - Site (a facility with one or more zones)
  - Zone (an area with 1 or more CS or PU)
  - CS (with 1 or more EVSE and 0 or more PU)
  - EVSE (with 1 connector) / PU

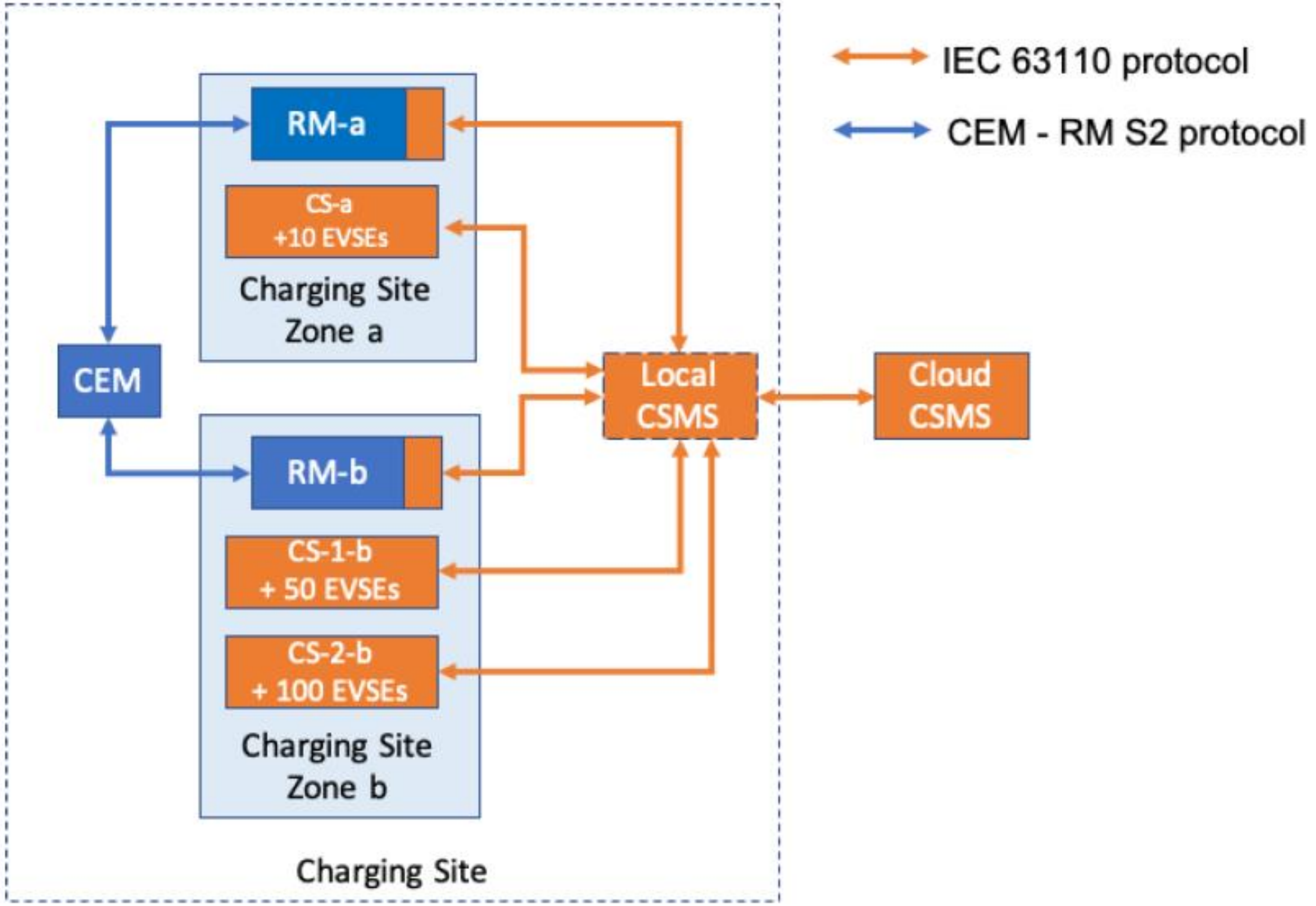


Figure 7 – a Charging Site with two Charging Site Zones controlled by a CSMS (either Local or Cloud)

IEC 63110 – Use Cases

The Use cases have been divided in three domains:

- Energy Domain
- Manage Charging Station Domain
- Deliver e-mobility Services Domain

e-mobility-1	Remote Authorization by External Means	Charging Session
e-mobility-2	Remote Authorization with Locally Presented Credentials	Charging Session
e-mobility-3	Reservation of an EVSE	Charging Session
e-mobility-4	Service Detail Record production	Charging Session
e-mobility-5	Tariff information while Charging	Charging Session
e-mobility-6	ContractCertInstallation	Charging Session
e-mobility-7	Tariff information during Operation	CS Operation
Energy transfer-1	Actors' relations during V2G session	Charging Session
Energy transfer-2	CEM-CSMS information exchange	Charging Session
Energy transfer-3	Charging with demand response	Charging Session
Energy transfer-4	CS-CSMS Dynamic mode infomation exchange	Charging Session
Energy transfer-5	Negotiate a charge plan for smart charging	Charging Session
Energy transfer-6	Power variation triggered by DSO	Charging Session

IEC 63110 – Use Cases

Manage CS-1	Secure boostrapping of CS including migration	CS Installation
Manage CS-10	CA Certificates Installation	CS Installation
Manage CS-11	CS Deregistration by CSMS	CS Operation
Manage CS-12	Fault code Provisioning	CS Operation
Manage CS-13	information deletion triggered by CSMS	CS Operation
Manage CS-14	information deletion triggered by EVU	CS Operation
Manage CS-15	Information display on the EVSE	CS Operation
Manage CS-16	Discover CS configuration	CS Operation
Manage CS-2	Monitor a CS	CS Operation
Manage CS-3	Retrieve logged information from the CS	CS Operation
Manage CS-4	Set log criteria	CS Operation
Manage CS-5	Update the firmware of a CS	CS Operation
Manage CS-6	OCSP response messages	CS Operation
Manage CS-7	Update Certificate On CS with Keypair Created Outside	CS Operation
Manage CS-8	Update Certificate On CS	CS Operation
Manage CS-9	Update local CSMS Certificate	CS Operation

IEC 63110 – DER Functions – New Use Cases

Task Force JWG11 / WG17 - New Use Cases for 63110 – Energy related

DER Functions Potentially Applicable to EVs

Grid Code functions

1. Disconnect/Connect Function
2. Cease to Energize and Return to Service
3. **High/Low Voltage Ride-Through** Operational function
4. **High/Low Frequency Ride-Through**
5. Dynamic Reactive Current Support
6. **Frequency-active power**
7. Volt-Watt
8. Fixed (Constant) Power Factor
9. Fixed (Constant) Reactive Power
10. **Volt-VAr** Control
11. Watt-VAr
12. Watt-PF
13. Set Active Power
14. Limit Active Power Production or Consumption
15. Low Frequency-Watt Emergency function for demand side management (fast load shedding)
16. Low Voltage-Watt Emergency function for demand side management
17. Monitoring Function
18. Scheduling of Power Settings and Operational functions

IEC 63110 – DER Functions – New Use Cases

Non-Grid Code Functions (Market Functions)

19. Peak Power Limiting
20. Load Following
21. Generation Following
22. Dynamic Active Power Smoothing
23. Droop / Frequency-active power Primary Control
24. Automatic Generation Control (AGC)
25. **Operating Reserve (Spinning Reserve)**
26. **Synthetic or artificial inertia Frequency-active power**
27. Coordinated Charge/Discharge Management
28. Frequency-active power Smoothing
29. Power Factor Limiting (Correcting)
30. Delta Power Control Function
31. Power Ramp Rate Control
32. Dynamic Volt-Watt Function

Non-Functional Capabilities

33. Collect and Provide Historical Information
34. Establish Different Ramp Rates for Different Purposes
35. Soft-Start Return to Service

Microgrid Capabilities being Defined in IEC 61850-90-23

36. Microgrid Separation Control (Intentional Islanding)
37. Provide Black Start Capability

IEC 63110 – Use Case Example – V2G Session

8.2.6 Actors relations during V2G session

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

Scope and objectives of use case

Scope and objectives of use case	
Scope	Actors' relations during V2G session
Objective(s)	
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 setup a V2G service. It doesn't describe the necessary steps to operate the service on CS side.
Complete description
Different services are employed by TSO, DSO and flexibility operators to keep the grid stable and operating: frequency reserve, voltage control, demand-response, congestion management. Some services are automatic (e.g. frequency), some are subject to program with days or hours ahead (e.g. DR). Actors involved: – Flexibility operators: they aggregate EVs and offer services to TSO and DSO – DSO: has some requirements for local constraints – CEM: optimises local Power and Energy demand and production based on signal received by DSO, FO – CSMS: receives messages from EMS and control the CS. – CS: controls the EVSEs

← Flexibility
Operators aggregate EVs

IEC 63110 – Use Case Example – V2G Session

Description of the use case:

1. 1 or more EVs are charging in the area controlled by a CS and a CSMS.
2. The CEM receives a message from DSO, FO or from another SA that energy injection into the grid should start.
3. The CEM informs the CSMS of the impact on the current max power allocated to the CS. The impact could influence schedules but could also be that active & reactive power need to be injected into the grid.
4. CSMS gets from the CSO the list of EVs able to inject energy into the Grid and having a valid contract. The way the contract check works is out of scope.
5. Based on the max power allocated by the CEM and on mobility needs, the CSMS sends to CS the new schedules for each EVs listed in schedule mode.
6. Some EVs may need to switch to ISO 15118 dynamic mode in order to react to active and reactive real time setting from a SA. See CS-CSMS Dynamic mode information exchange use case.
7. CS negotiates with the EVs the changes in charging schedule.
8. CS returns to CSMS the result of the negotiation.
9. The CSMS aggregates the new schedules and sends it to the CEM.
10. When the situation returns to normal, the CEM informs the local CSMS that the V2G episode is over and sends to local CSMS a new power allocation.

← ISO 15118 Dynamic mode

IEC 63110 – Use Case Example – V2G Session

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 and their charging 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 EV supply equipment 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 to the local grid code requirements.
6	Contracts: The EVUs participating to the ancillary service have a contract with an FO

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		CSMS, CS	SA, CEM		

IEC 63110 Message and encoding technology

JWG11 has worked since a year and a half on requirements for messaging and encoding technologies.

Four candidate technologies were pre-selected :

XMPP, COAP-TCP, MQTT, DDS

Finally, on October 21st 2019, after a rigorous selection process, XMPP has been chosen by JWG11 experts.

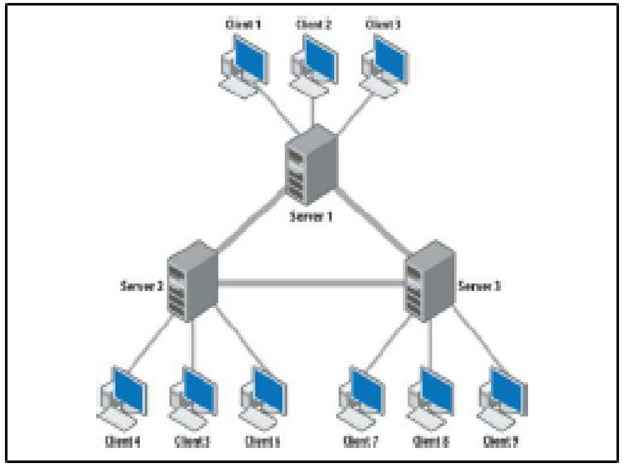
IEC 63110 uses XMPP for transport technology

What is XMPP ?

- XMPP is an **open communication protocol** for message-oriented middleware. It enables fast, secure, scalable, near-real-time exchange of XML data between multiple entities.
- **XMPP is normalized** by IETF (RFC 6120 and RFC 6121). No royalties or granted permissions are required to implement these specifications. Designed to be extensible, the XMPP Standards Foundation (XSF) develops and publishes XEPs extensions through a standard process.
- **XMPP is based on XML**, just like ISO 15118, so there is no need for new encoders in Charging Stations.
- XMPP is used for request/response, publish-subscribe systems, signaling for VoIP, video, file transfer, games, the Internet of Things (IoT) applications such as the Smart Grid, and social networking services.

How XMPP works

- **XMPP uses a decentralized** Client - Server and Server - Server communication architecture.
- This architecture enables **separation of roles**:
  - Clients (CS, CSMS, CEM) can focus on energy budget, charging process, e-mobility services and user experience.
  - Servers can focus on reliability, scalability, cybersecurity and multi-server's federation.
- **XMPP is highly secure**: its core specification natively features encryption (TLS), secure authentication (SASL) and end-to-end security between servers and clients.
- **The decentralized architecture of XMPP**, combined with its addressing schema (similar to email), allow transparent, firewall friendly and seamless integration of Charging Stations and CEM into the IEC 63110 multi-level communication architecture.
- **XMPP has the proven scaling capability** required for the challenging expected e-mobility booming. XMPP is used for example by gaming platforms to securely connect every day millions of players and billions of events per server/day.



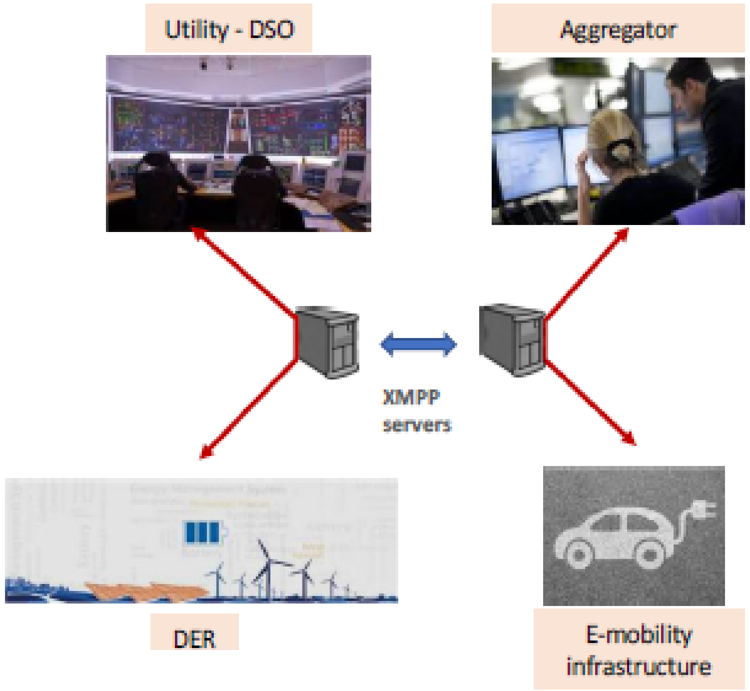
XMPP integration with Smart Grid standards

XMPP is the basis for the DER management standards IEC 61850-8-2 and IEC 63110

With IEC 61850-8-2 multiple Virtual Power Plants belonging to different EV charging stations, local production or storage entities can securely exchange messages through the multi-federation XMPP server's capability.

The last version of OpenADR 2.0 uses XMPP as transport protocol (IEC 62746-10-1) ensuring even more interoperability with flexibility operators.

IEC 63110 with XMPP is a proven solution to ensure the integration of e-mobility infrastructure management into present and future IEC Smart Grid standards.



Relation with existing management solutions

There are many existing specifications for Charging Station management. Some are open, like OCPP, other are industry proprietary developments. Most of them are not able to interoperate (for example transport technology and object model are usually different)

JWG11 mission is to develop a new international open standard ensuring interoperability with all future e-mobility technologies based on experience and contributions of experts from all the world. Interoperability with existing deployed systems is then not a reasonable option.

Among the existing specifications, OCPP claims to be one of the most used. This is why JWG11 has accepted to have an official liaison with OCA. The object of this liaison is to exchange documents and comments from their respective experts.

Many JWG11 experts, either belonging to OCA or using OCCP in their company, bring their experience on protocol and e-mobility issues to solve.

From a strict hardware point of view it is expected that CS and CSMS supporting OCPP 2.x will be able to support IEC 63110 stack.

IEC 61850 - Tutorial

Contents

IEC 61850 is not just another protocol!

IEC 61850 – Overview

IEC 61850 is not just another protocol!

Start of standardization activity in 1995, by IEC TC57

Original title : **Communication networks and systems in substations**
Focus on substation automation to support introduction of IEDs and achieve interoperability

In 2007 change of title and scope
New title: **Communication networks and systems for power utility automation**
Extension to power systems and to DERs

Virtualization → creation of abstract data models which can be mapped to a number of protocols

IEC 61850 – Overview

Part #	Title
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	- Principles and Models
7.2	- Abstract Communication Service Interface (ACSI)
7.3	- Common Data Classes (CDC)
7.4	- Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	- Mappings to MMS (ISO/IEC 9506 – Part 1 and Part 2) and to ISO/IEC 8802-3
9	Specific Communication Service Mapping (SCSM)
9.1	- Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link
9.2	- Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

IEC 61850 provides:

- Information model
- Communication Protocols
- Configuration Language

Information exchange requires specific **data models** for data generated by power system devices (IEDs, DERs)

In addition to the specification of the protocol elements (how bytes are transmitted on the wire), IEC 61850 provides a comprehensive model for how power system devices should organize data in a manner that is consistent across all types and brands of devices, to achieve **interoperability**

IEC 61850 series uses concept of **virtualization** in order to create these abstract data models.

Definitions are created by using an **object model** which decomposes the functionalities of a real device into the smallest possible entities.

IEC 61850 – Overview

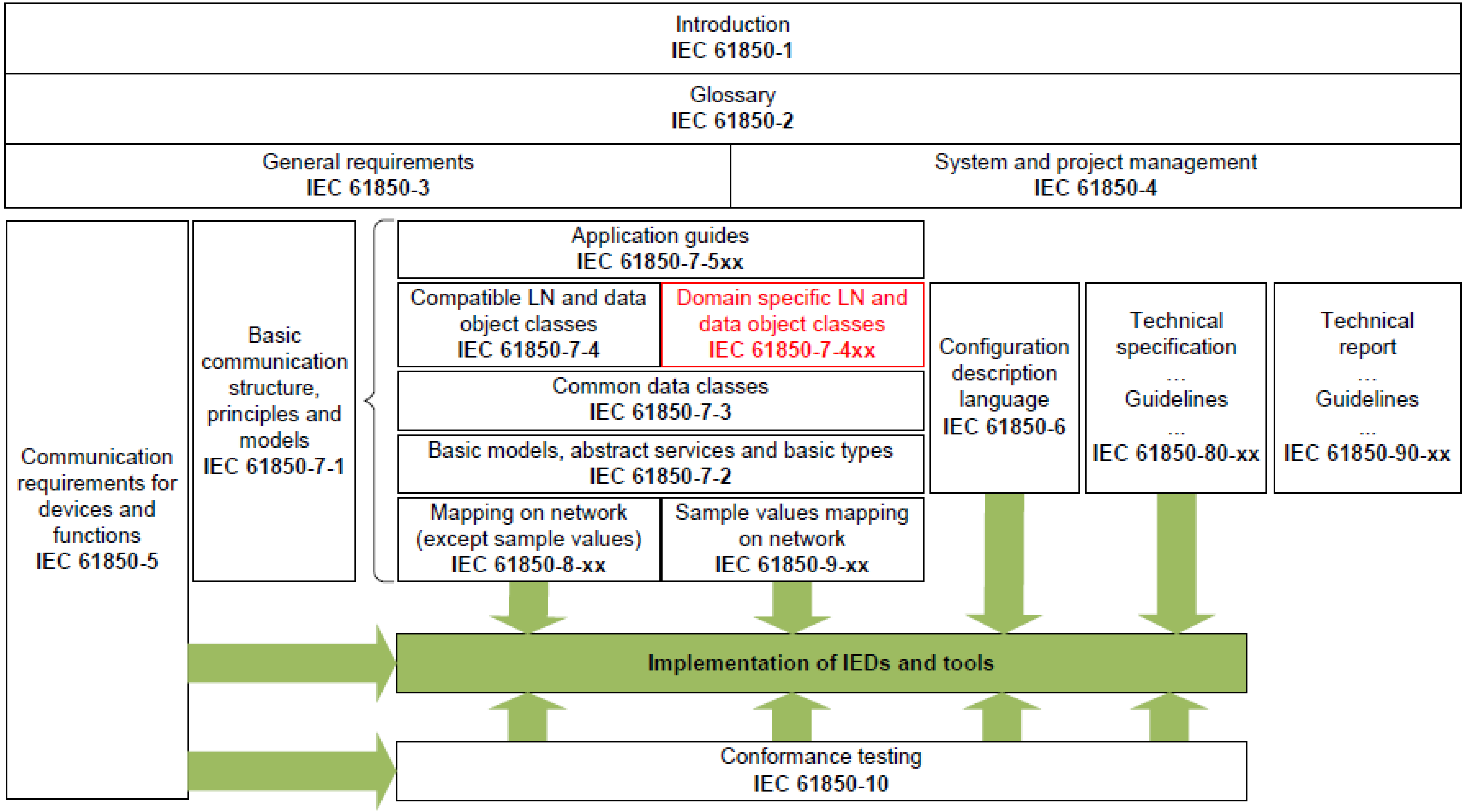


Figure 1: Overall structure of IEC 61850 parts

IEC 61850 – Series of standards - Parts

The general title of the IEC61850 standard is **Communication networks and systems for power utility automation**

The standard consists of the following parts:

IEC61850-1 Introduction and overview

IEC61850-2 Glossary.

Explains terms and abbreviations used throughout the standard

IEC61850-3 General requirements.

Specifies system requirements with emphasis on the quality requirements of the communication network.

IEC61850-4 System and project management.

Specifies system and project management with respect to the engineering process, life cycle of overall system and IEDs and the quality assurance.

IEC61850-5 Communication requirements for function and device models.

Describes all required functions in order to identify communication requirements between technical services and the substation, and between IEDs within the substation. The goal is interoperability for all interactions.

IEC61850-6 Configuration description language

Specifies the SCL file format for describing communication related IED configurations, IED parameters, communication system configurations, function structures, and the relations between them.

IEC 61850 – Series of standards - Parts

IEC61850-7 Basic communication structure for substation and feeder equipment

IEC61850-7-1 Principles and models

Introduces modelling methods, communication principles and information models used in IEC61850-7.

IEC61850-7-2 Abstract communication service interface (ACSI)

Presents the ACSI providing abstract interfaces describing the communications between a client and a remote server, such as interfaces for data access and retrieval, device control, event reporting and logging.

IEC61850-7-3 Common data classes

Specifies common attribute types and common data classes related to substation applications. The common data classes specified, are classes for status information, measured information, controllable status information, controllable analogue set point information, status settings and analogue settings.

IEC61850-7-4 Compatible logical node classes and data classes

Specifies the compatible logical node names and data names for communication between IEDs.

IEC 61850 – Series of standards - Parts

IEC61850-8 Specific communication service mapping (SCSM)
IEC61850-8-1 Mapping to MMS (ISO/IEC 9506 Part 1 and Part 2)
Specifies how time-critical and non-time-critical data may be exchanged through local area networks by mapping ACSI to MMS.
IEC61850-9 Specific communication service mapping (SCSM)
IEC61850-9-1 Serial unidirectional multidrop point to point link
Specifies the specific communication service mappings for the communication between bay and process level and a mapping of the abstract service for the transmission of sampled values.
These are specified on a serial unidirectional multidrop point to point link.
IEC61850-9-2 Mapping on a IEEE 802.3 based process
Defines the SCSM for the transmission of sampled values according to the abstract specification in IEC61850-7-2.
IEC61850-10 Conformance testing
Specifies how a system should be tested to ensure conformance with the IEC61850 standard.

IEC 61850 – Data Model

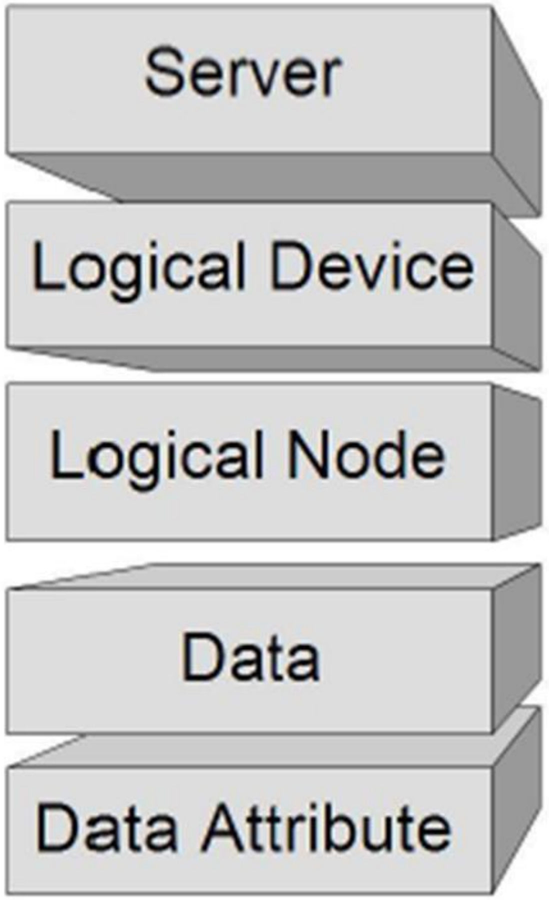
Data Model
Old protocols have typically defined how bytes are transmitted on the wire. However, **they did not specify how data should be organized in devices** in terms of the application.

This approach requires power system engineers to manually configure objects and map them to power system variables and low-level register numbers, I/O modules, etc.

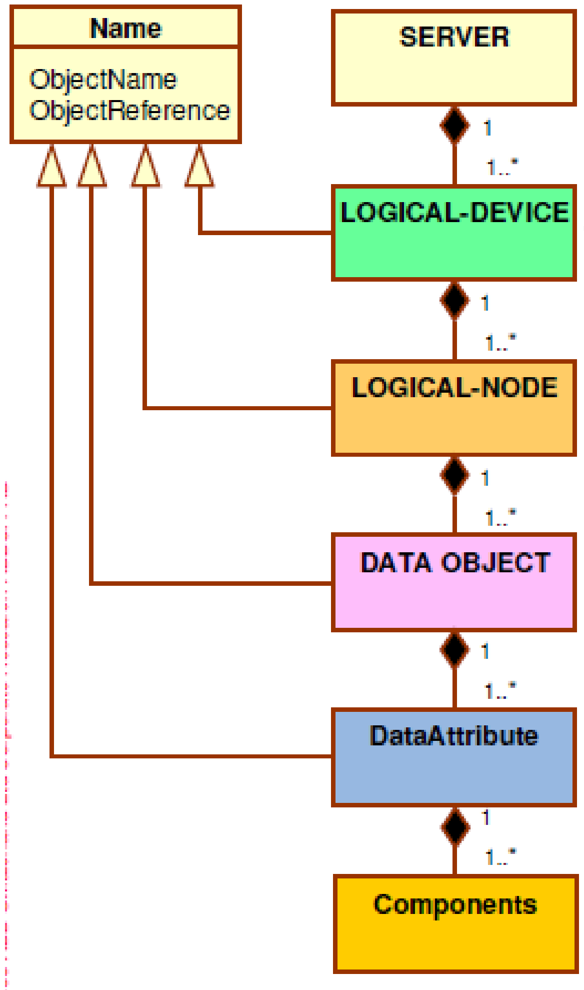
IEC 61850, in addition to the specification of the protocol elements, provides a comprehensive **model for how power system devices should organize data** in a manner that is consistent across all types and brands of devices.

IEC 61850 device model begins with a **physical device (IED)** that connects to the network and is typically defined by its **IP address.**

Note:
IPv4 is a 32 bit IP address → 2^32 addresses is more than 4 billion
IPv6 is a 128 bit IP address



IEC 61850 – Hierarchy of Naming and Data Structure



Physical Device:
access by network address

Aggregates data from multiple devices into a single physical device

Represents the protection and control functions within a device, and the device itself

Variables of a Logical Node represented as a collection of Common Data Classes

Elements of an Common Data Class (value, time-stamp,..) belonging to Functional Constraints

Basic or composite Data Attribute types, e.g. Common Data Attributes

IEC 61850 – Data Model

A physical device (IED) consists of one or several **logical devices (LDs).**
The logical device model allows a single physical device to act as a proxy or gateway for multiple devices thus providing a standard representation of a data concentrator.

Each logical device contains one or more **logical nodes (LN).**
A logical node is a grouping of data and services related to some power system function.
The LN is specified as the <u>smallest entity that can exchange information.</u>

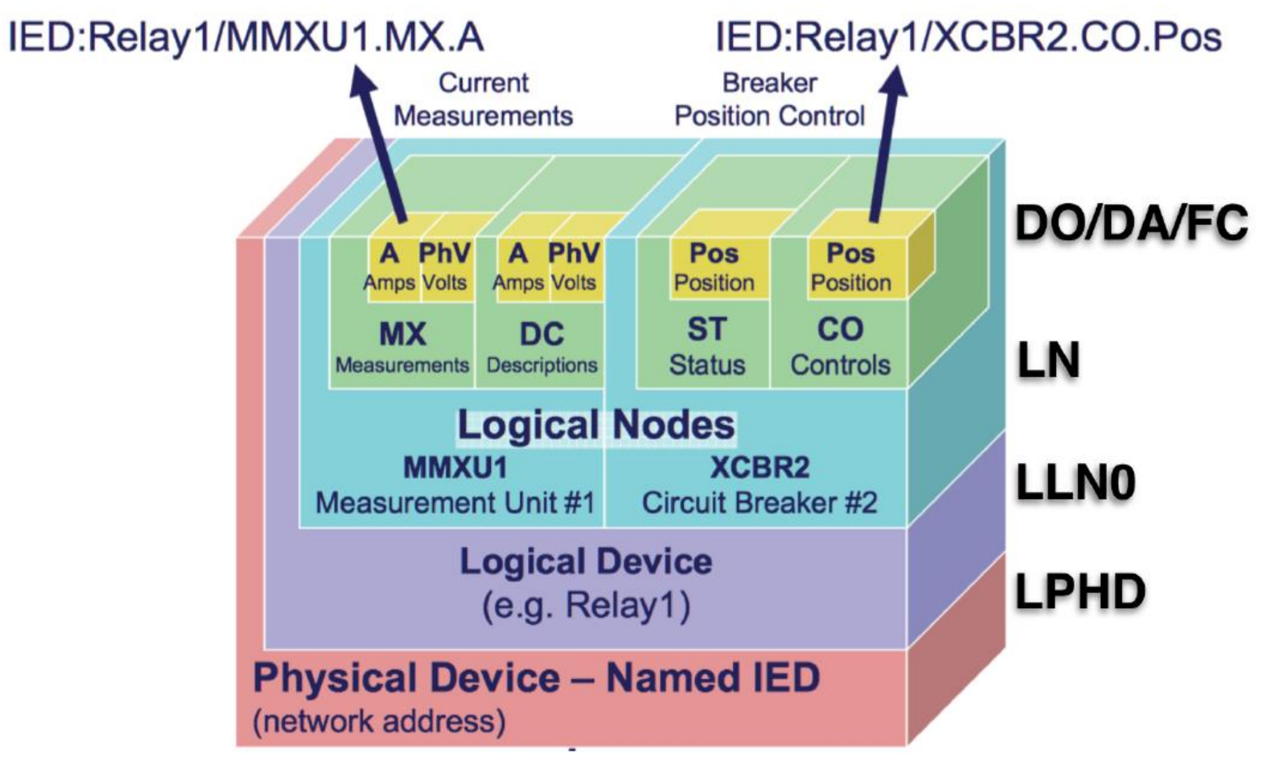


Figure 2: Structural Composition of an IEC 61850 based IED

At least three LNs must be within a LD, namely 2 LNs related to common issues for the LD (**LLN0 and LPHD=LogicalNode for PhysicalDevice**, which describes the common device properties), and at least one LN performing some functionality

Each LN contains one or more elements of data, which are classified as **Data Objects and Data Attributes**
Each Data Object of a logical node belongs to a **Common Data Class** (CDC).

IEC 61850 – Data Model – Logical Node Groups

A complete list of LN is defined in 61850-7-4.
LNs are combined into groups based on their functionality.
These groups and the number of nodes in a group are in **table of LOGICAL NODE GROUPS** .
Table below is not updated, it is shown as an example.

Logical Group	Name	Number of Logical Nodes
L	System LN	2
P	Protection	28
R	Protection related	10
C	Control	5
G	Generic	3
I	Interfacing and archiving	4
A	Automatic control	4
M	Metering and measurement	8
S	Sensor and monitoring	4
X	Switchgear	2
T	Instrument transformers	2
Y	Power transformers	4
Z	Further power system equipment	15

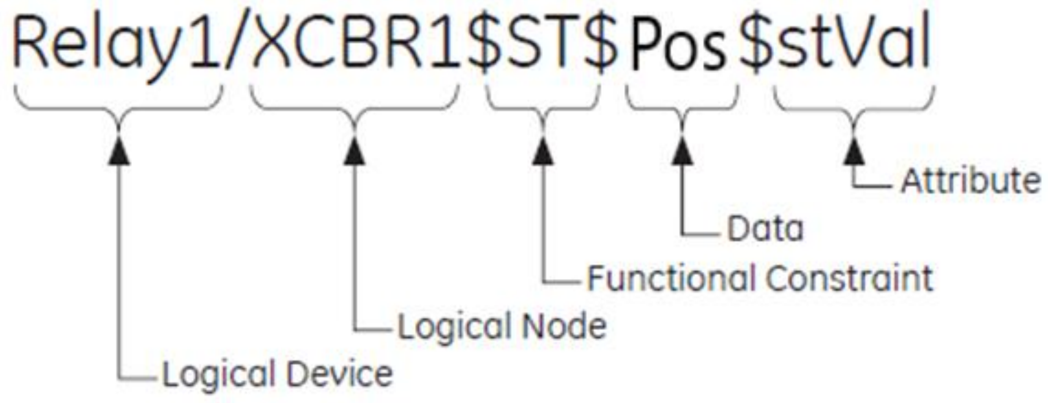
IEC 61850 – Data Model

LNs are the building blocks for IEDs and have standardized names, data structures, abstract service interfaces and behaviour models.

Naming Structure: LNs exchange data by reading and writing values to memory locations referenced to by their data attribute (DA).
The IEC 61850 standard uses a hierarchical naming convention that uniquely identifies each DA in the substation, or power system.
The first letter of the LN name identifies the group to which the LN belongs, and suffixes can be used to identify each instance of the LN in the IED.
An IED name is unique within the substation, and LN name is unique within the IED.

The status value (stVal) of the switch position (Pos) of the circuit breaker Relay1 can be determined by referencing **"Relay1/XCBR1.ST.Pos.stVal".**

Where "1" represents an instance of the circuit breaker LN (XCBR) in "Relay1", "X" identifies its LN group as switchgear, and "ST" represents the functional constraint (FC) for status value.



Anatomy of an IEC 61850-8-1 Object Name

IEC 61850 –Data Model

Data Structure:

To simplify engineering, IEC 61850 has defined standard groups of Data Attributes, called CDC ("Common Data Classes")

Each Data Object of a logical node belongs to a CDC.

The **commmon data class (CDC)** template specifies the data type of each data attribute (DA) allowed for the given data object (DO).

For example, if the CDC specifies that the controllable double point (DPC) template be used for the Relay1/XCBR1.Pos data object, then the data attribute for Relay1/XCBR1.ST.Pos.stVal will have a type with four possible states:
intermediate-state, off, on, bad-state.

The **timestamp** attribute "t" referenced by Relay1/XCBR1.ST.Pos.t will have a data type of either int32 or unsigned int24 based on the chosen time quality.

IEC 61850 – Data Objects and Data Attributes

Object Reference	Type	Remark
`MMXU1`	LN	Measurement LN
`MMXU1.PhV`	DATA	Phase to ground voltages
`MMXU1.PhV.phsA`	DATA	Value of Phase A
`MMXU1.PhV.phsA.cVal`	DataAttribute	Complex Value
`MMXU1.PhV.phsA.cVal.mag`	DataAttribute	Magnitude of complex number
`MMXU1.PhV.phsA.cVal.mag.f`	DataAttribute	Floating point number

Example of types: The logical node MMXU. The recursive structure of types DATA and data attributes is illustrated.

For example a commonly used class in IEC 61850 is "WYE", which provide information about phase to ground related measured values of a three-phase power system apparatus.
Attributes in WYE include phsA, phsB, phsC, neut for phase A, B, C and ground current or voltage measurements.
These attributes are of **type CMV (complex measured value)** and consist of magnitude and phase angle as in any AC measurements.
Attributes of CMV are described in Figure.

7.4.3 Complex measured value (CMV)

Table 31 defines the common data class “complex measured value”.

Table 31 – Complex measured value

CMV class					
Data attribute name	**Type**	**FC**	**TrgOp**	**Value/Value range**	**M/O/C**
DataName	Inherited from GenDataObject Class or from GenSubDataObject Class (see IEC 61850-7-2)				
DataAttribute					
			measured attributes		
instCVal	Vector	MX			O
cVal	Vector	MX	dchg, dupd		M
range	ENUMERATED	MX	dchg	normal|high|low|high-high|low-low	O
rangeAng	ENUMERATED	MX	dchg	normal|high|low|high-high|low-low	O
q	Quality	MX	qchg		M
t	TimeStamp	MX			M

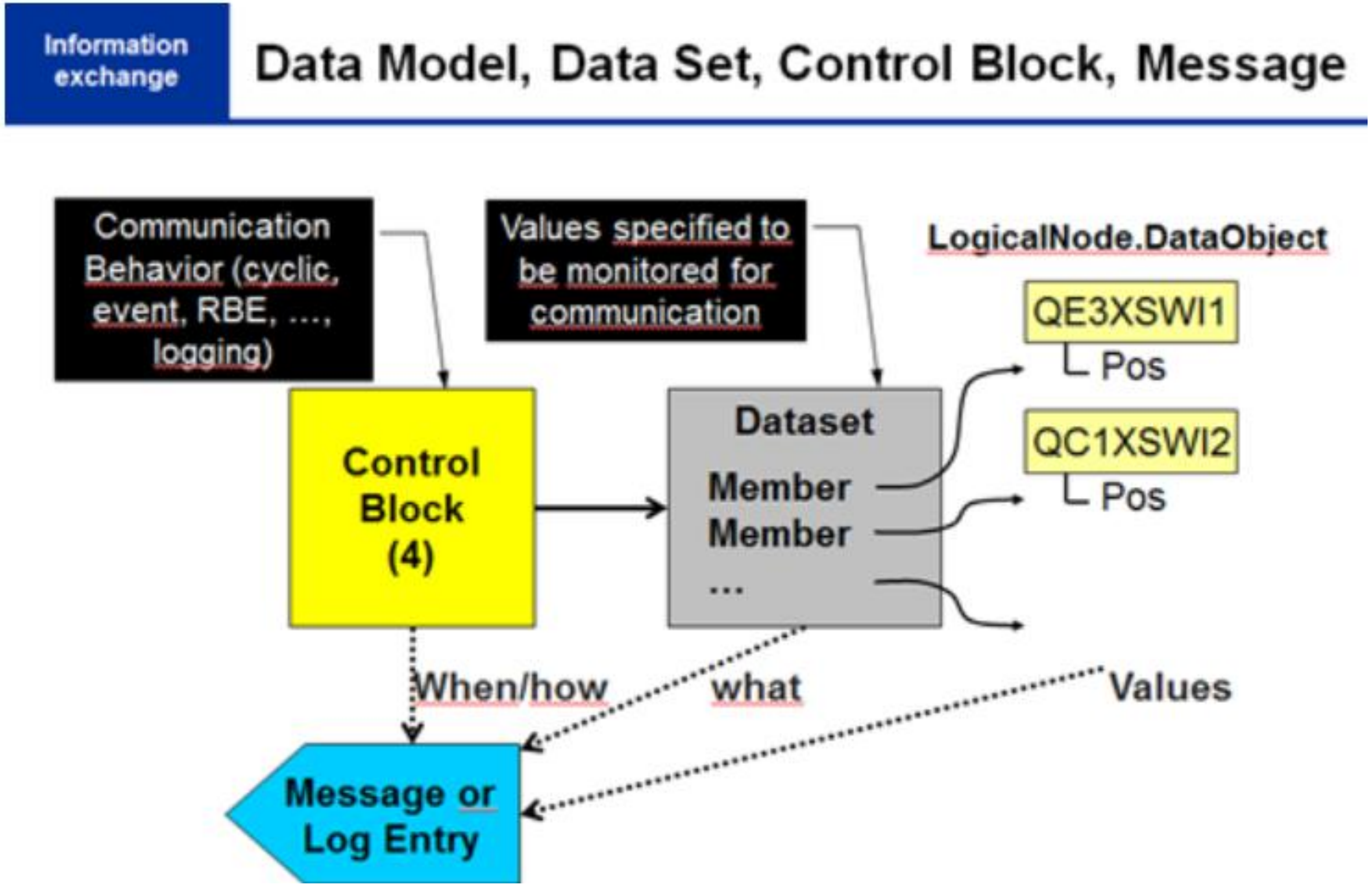
In IEC 61850 standard part 7-3, common data class is defined to describe the data object.

Phase A current is not only index 1 of analog input.
In IEC 61850, attributes of class CMV

“cVal.mag.f” is used for magnitude measurement
“cVal.ang.f” for angle,
“q” for quality and
“t” for timestamp.

Data class SPS (Single point status) is defined for binary data including attribute
“stVal” for a Boolean value,
“q” for quality, and
“t” for timestamp,
and some other attributes.
In fact all data objects in IEC 61850 have at least three attributes: value, quality and timestamp

IEC 61850 – Datasets and Control Blocks



Data Exchange by Messages

Dataset → **WHAT**

Control Block → **WHEN**

Protocol → **HOW**

Naming Structure = PhysDev (IED), LN, Data Attributes
defines IED and specific memory address in it, for any variable

→ **WHERE**

IEC 61850 – Datasets and Control Blocks

Control blocks (CB) define, how and when the data is transferred
Periodically, or driven by event/data change

- Report and Log CBs:

describe conditions for generating reports and logs

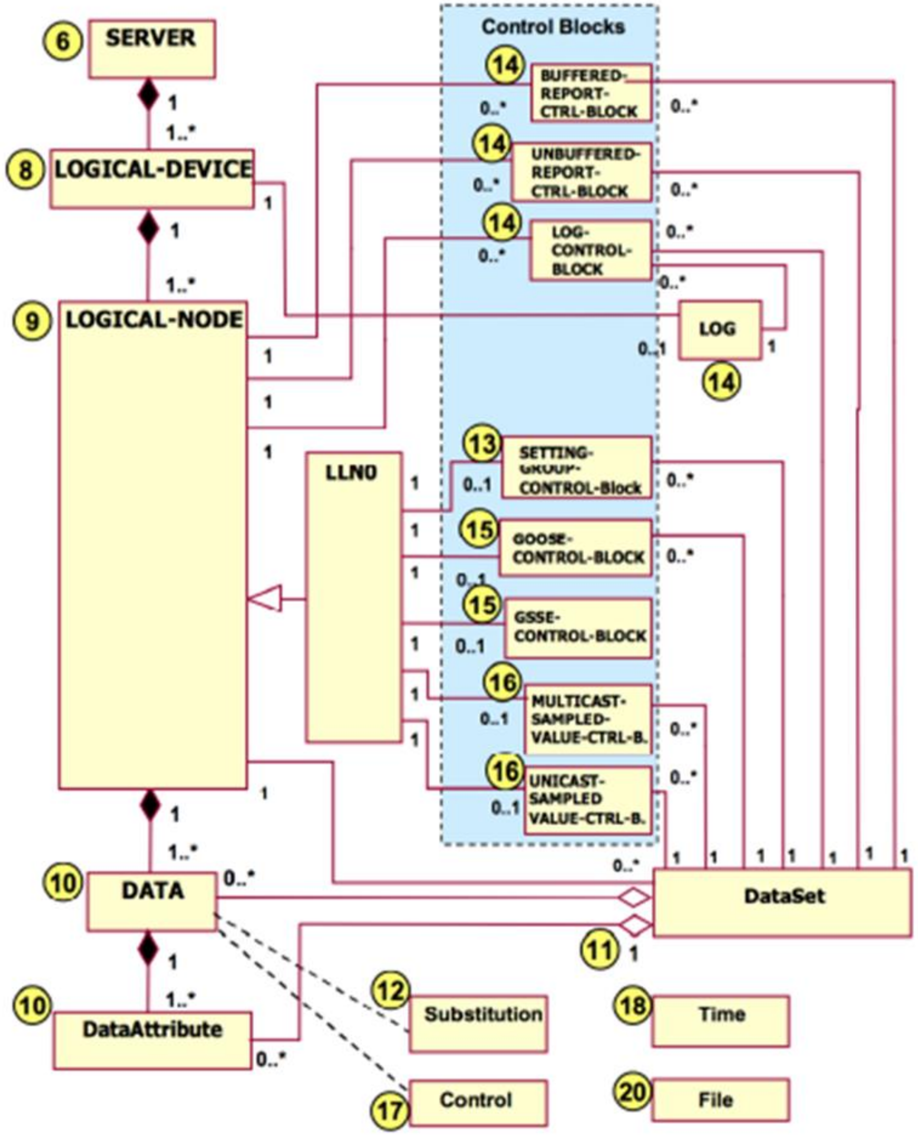
- Generic substation events (GSE) CB:

supports a fast and reliable system-wide distribution of input and output data values.

- Sampled values CB:

fast and cyclic transfer of measurement values (Ex. instrument transformers)

Datasets are lists of data attributes (DA) that are handled as a whole.
A variable is identified within a dataset by its offset and its size.
A dataset is treated as a whole for communication and access.
Variables may be of different types, types can be mixed.
Part 9.1 specifies a pre-configured or **"universal" dataset** as defined in IEC 60044-8.
This dataset includes 3-phase voltage, bus voltage, neutral voltage, 3-phase currents for protection, 3-phase currents for measurement



Conceptual service model of the ACSI

IEC 61850 – Communication Protocols

IEC 61850 series defines communication by **OSI model (Open System Interconnection**) that uses the concept of layering the communication functions.
OSI model does not specify which protocols should be used, nor it restricts to a single set of protocols. IEC 61850, by using OSI model, preserves the possibility to change the chosen protocol if there is a technology development.
Communication can be divided into three separate parts:

- **Data** of the applications
- **Services** for transferring data
- Communication **protocols**

Data of the applications is described in an object model, which decomposes data of substation/power system functions into smallest possible entities, which exchange information.
An object-oriented concept, **Abstract Communication Service Interface (ACSI),** is used for transferring services.
To achieve actual communication the abstract objects and services shall be mapped to real communication protocols. The implementation to real protocols is made by **Specific Communication Service Mappings (SCSM).**

IEC 61850 – Communication Protocols

Communication services/protocols defined by IEC 61850 series:

- **Client-Server** Communication
- Time critical **Sampled Values**
- Time critical **GOOSE** messages

Client-Server communication works where the client requests data from a server which offers it.
Server contains data of the Logical Device, time synchronization and file transfer, visible and accessible from the communication network.

Client-Server communication is used for transferring large amounts of information, **not time-critical**.
For example: transferring configuration data to IEDs.

For **time-critical** information there are two communication services:

- Sampled-values (SV) for metering information
- GOOSE messages for peer-to-peer communication between IEDs

IEC 61850 – Communication Protocols

Communication **Protocol Profiles** used in IEC 61850 are shown in Figure below

Time synchronization provides a reference clock for the entire network. For example it is used to have sampled values in chronological order. It uses **Simple Network Time Protocol (SNTP)**.

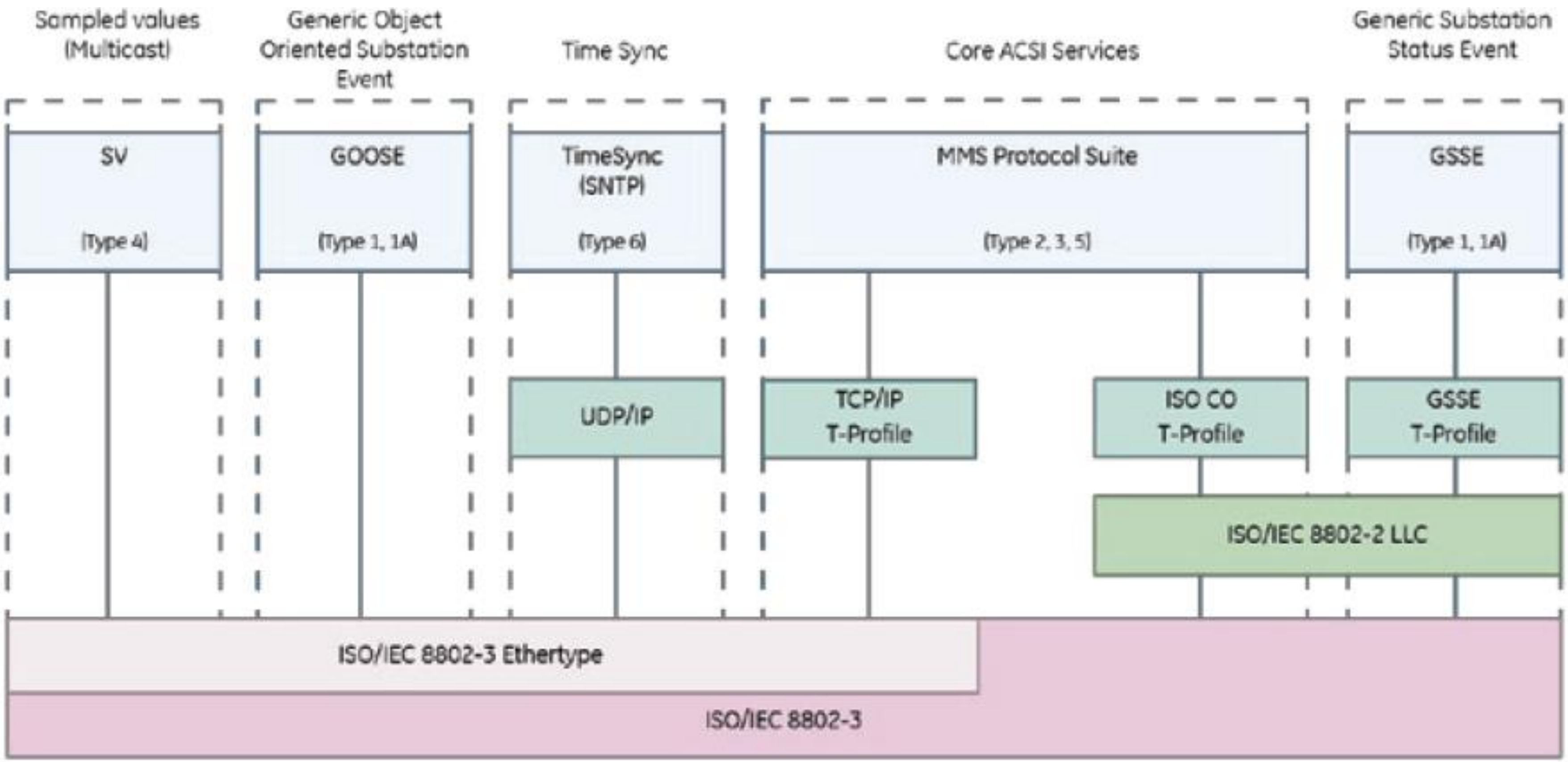


Figure 4.
Overview of IEC 61850 Functionality and Associated Communication Profiles

IEC 61850 – Communication Protocols

Sampled Values are messages related to **instrumentation and measurement**.
They are time critical and need to be in chronological order.
They can be sent as unicast to one receiver or as multi cast to several receivers.

Time critical **GOOSE** messages have been defined for **fast horizontal communication** between IEDs.
They are used to transfer state and control information between IEDs, as trip or locking commands, in order to accomplish **control and protection functions**.

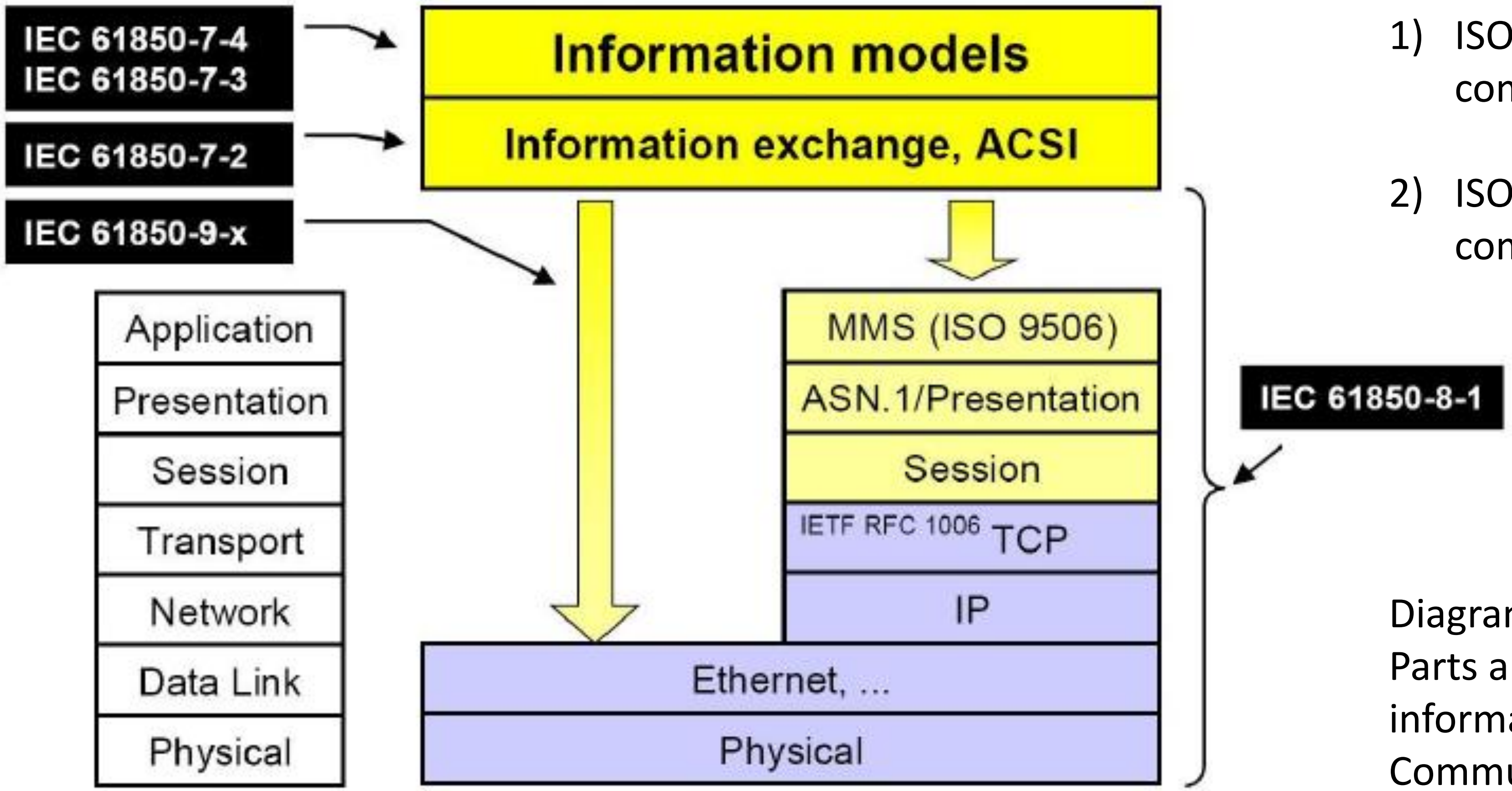
GOOSE messages are transmitted as **multicast over LAN**, from which all IEDs configured to receive the message can subscribe it.
They implement a real-time **Publisher/Subscriber** communication model.

IEC 61850 – Communication Protocols

For **client-server communication MMS** is used. It is an internationally standardized messaging system, for exchanging real-time data and supervisory control information between networked devices.
Originally developed for manufacturing (Manufacturing Messaging Service) it was chosen because it can support the complex naming and service models of IEC 61850.

MMS covers the **application profile of OSI model.**
Transport and network layers are covered either by TCP/IP or ISO.
GOOSE messages are simply sent to the network.
This is needed in order to meet the time critical demand for GOOSE communication.
GOOSE messages are mapped directly into the Ethernet data frame in order to eliminate the processing time of the middle layers.

IEC 61850 – Communication Protocols



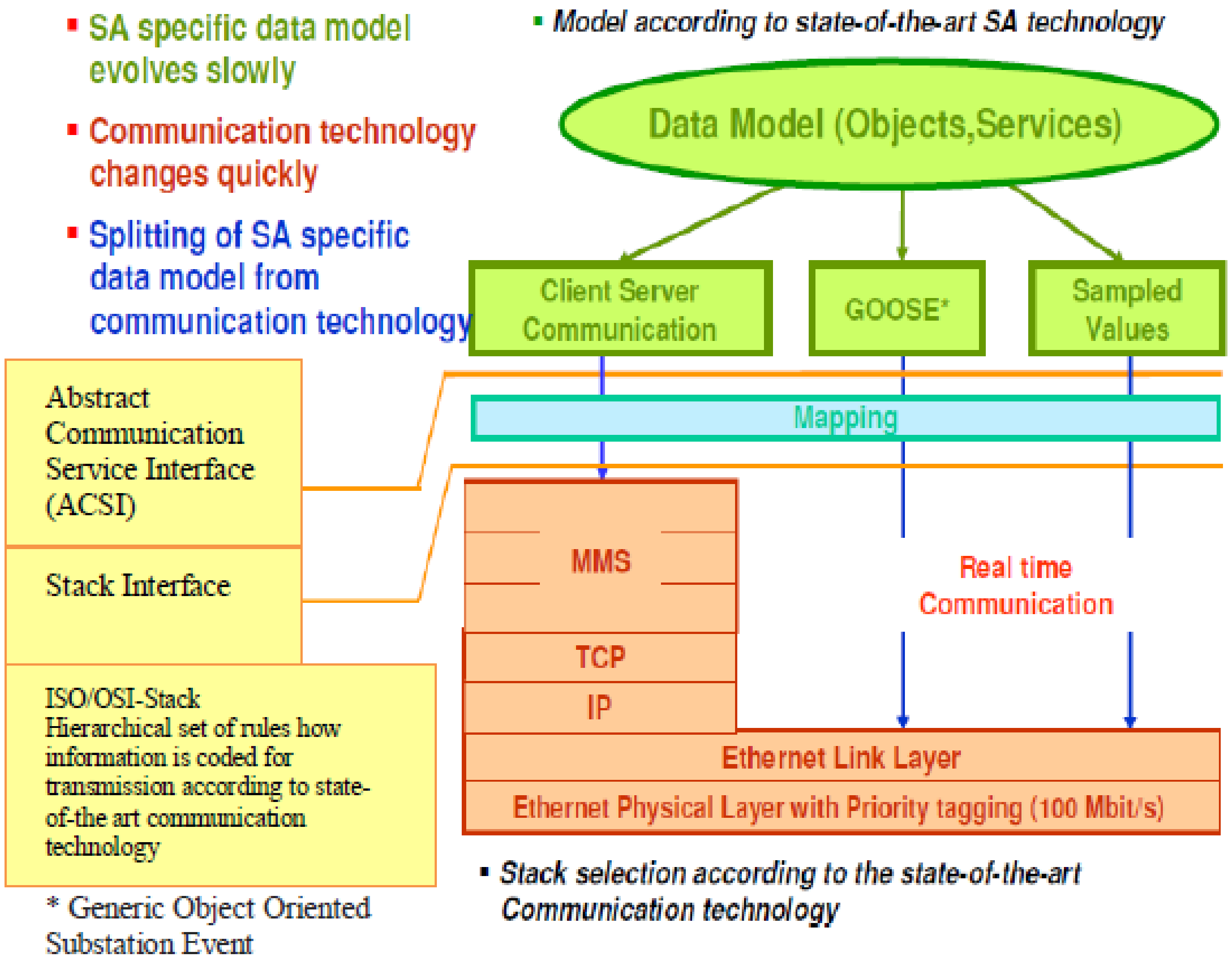
IEC 61850 groups the seven abstract OSI layers into two profiles:

1) ISO application profile **(A-Profile)** composed of the three upper layers,

2) ISO transport profile **(T-Profile)** composed of the four lower layers.

Diagram shows references to IEC 61850 Parts and correspondence to protocols, information models, and Abstract Communication Service Interface (ACSI) for information exchange

IEC 61850 – From Abstract Models to Real Communication Protocols

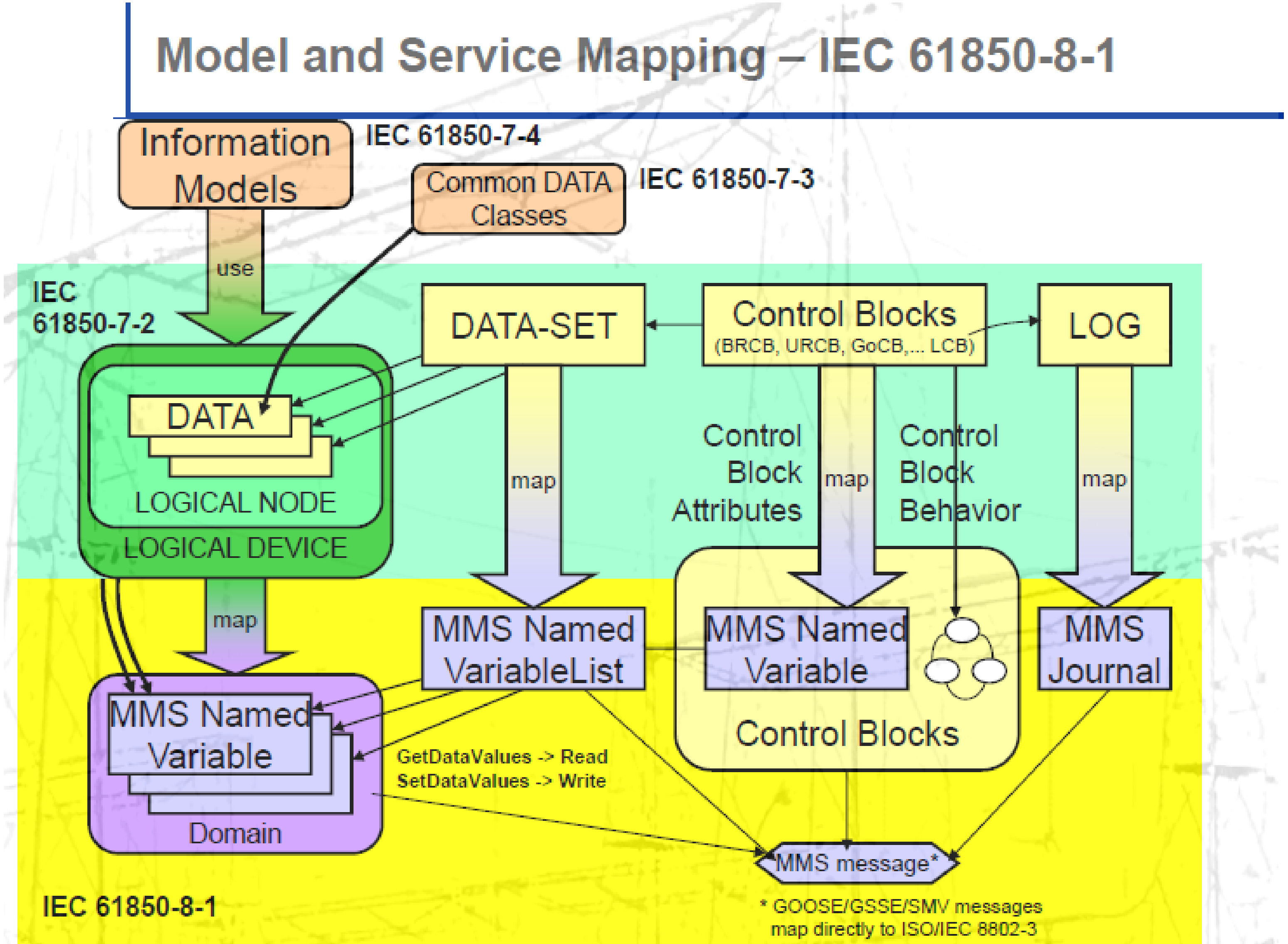


Abstract Communication Service Interface (ACSI)

Specific Communication Service Mapping (SCSM)

SA = Substation Automation

IEC 61850 / Mapping to MMS by Part 8-1 (SCSM)



From Abstract Models to Real Communication Protocols

Abstract Communication Service Interface **(ACSI)**

Specific Communication Service Mapping **(SCSM)**

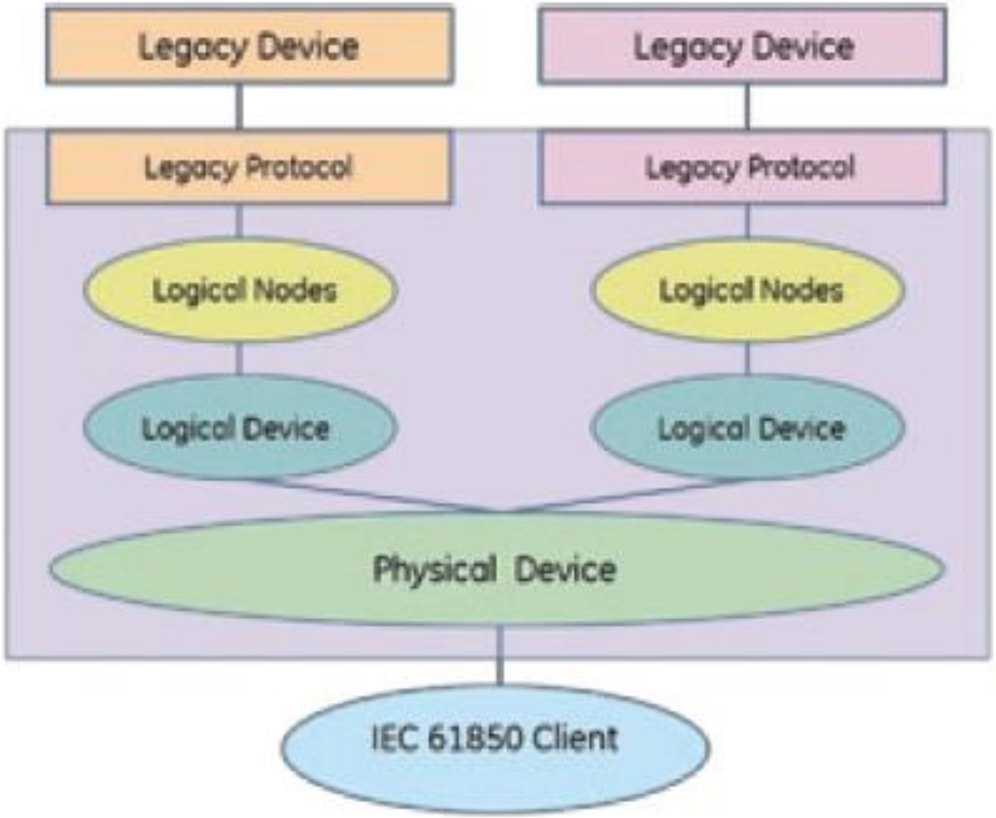
IEC 61850-8-1

IEC 61850 – OPC Data Access

There are SW products capable to support both IEC 61850 communications and OLE for Process Control (OPC) application program interface (API) of the OPC Foundation.
The **OPC Data Access (DA)** specification is an API that enables an OPC Client application, such as a SCADA or Human Machine Interface (HMI) to provide a generic interface to outside data that is independent of any specific protocol.
This enables third parties to develop OPC Servers to interface with a wide variety of protocols, **including IEC 61850**, Modbus, DNP3, and hundreds of other protocols.

Interface with Legacy Protocols

It is possible to accommodate use of legacy IEDs and protocols from the past in an IEC 61850 system. IEC 61850 itself is well suited to accommodate legacy protocols with its logical device model.
The ability to support multiple logical devices within a single physical device allows IEC 61850 to directly support the modelling of a **data concentrator or multi-device gateway** inherently without resorting to techniques outside the scope of the standard.



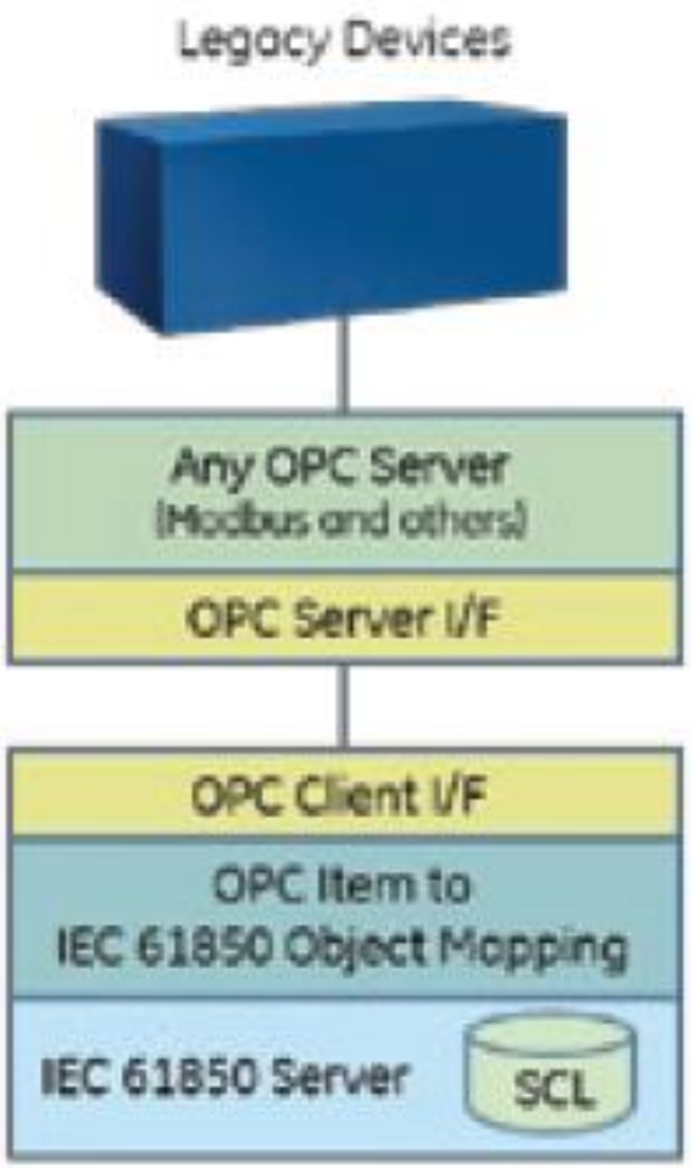
IEC 61850 Data Concentrator Architecture

IEC 61850 – OPC Data Access

In addition to the use of separate data concentrators, OPC technology also offers a way to incorporate simple **gateway functionality** into a substation SCADA system (see Figure).

In this case, the roles of OPC client and server are reversed from the previous example illustrating a substation SCADA application by building an OPC client application on top of an IEC 61850 server.

The OPC client is then mapped to an OPC server supporting any legacy or proprietary protocol.
This enables **data from legacy devices to be accessed as IEC 61850 data** simplifying the client application development by providing a consistent standardized mechanism for data access across the entire substation



IEC 61850 Data Gateway using OPC

IEC 61850 - Substation Configuration Language (SCL)

SCL is a Configuration description language for communication in electrical substations related to IEDs.
It is an **XML based language** that allows a formal description of:

- An automation system and the substation components, including the relation between them
- IED configuration
- Information flow between IEDs and LNs
- Communication network

Some Use Cases of SCL:

- System Design → single line diagram
- System Engineering → system configuration
- IED Development
- IED configuration/parametrization
- Documentation → view of system
- Simulate I/Os of IEDs for testing
- Message interpretation
- Message tracing
- Calculate traffic throughput to check against network infrastructure (for ex 100Mbit/s)

IEC 61850 - Substation Configuration Language (SCL)

SCL specifies a hierarchy of configuration files that enable multiple levels of the system to be described in unambiguous and standardized XML files.
The various SCL files include system specification description (SSD), IED capability description (ICD), substation configuration description (SCD), and configured IED description (CID) files. All these files are constructed in the same methods and format but have different scopes depending on the need

.SSD	**System Specification Description** Data exchange from a system specification tool to the system configurator
.SCD	**Substation Configuration Description** Data exchange from the system configurator to IED configurators
.ICD	**IED Capability Description** Data exchange from the IED configurator to the system configurator
.CID	**Configured IED Description** Data exchange from the IED configurator to the IED *It is an SCD file, possibly **stripped down** to what the concerned IED shall know (restricted view of source IEDs)*
.IID	**Instantiated IED Description** Data exchange from the IED configurator to the system configurator
.SED	**System Exchange Description** Data exchange between system configurators of different projects

IEC 61850 - Substation Configuration Language (SCL)

Use of SCL Files

Single line diagram with standard designation

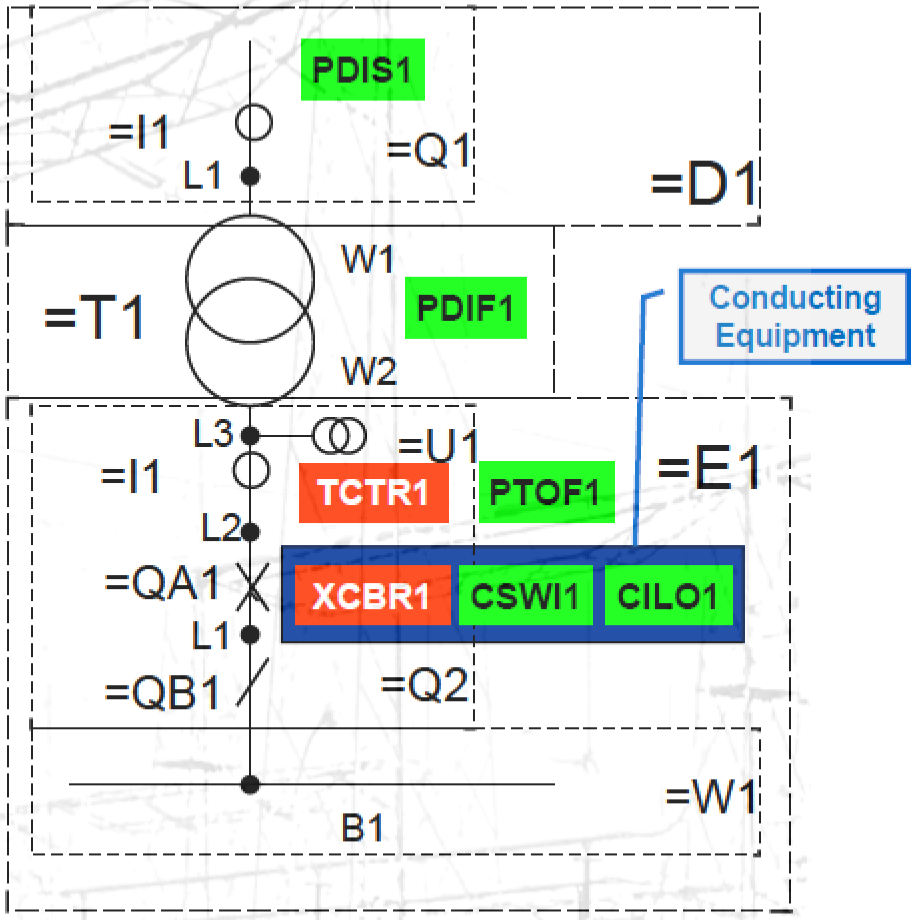
Substation Berlin220_132 with one transformer T1 between voltage levels D1 and E1, and a bay E1Q2.

The transformer T1 has two windings W1 and W2.

Winding W1 is connected to a 220 kV voltage level D1 at bay Q1, connectivity node L1.

Winding W2 is connected to the bay Q2 in 132 kV voltage level E1.

Designation according to IEC 61346 series.



Logical Nodes Names

PDIS = Distance Protection

PDIF = Differential Protection

TCTR = Current Transformer

XCBR = Circuit Breaker

CSWI = Control of Switch

CILO = Interlocking Control

PTOF = Over frequency Protection

IEC 61850 - Substation Configuration Language (SCL)

Use of SCL Files

(1) System Specification „Substation“

```
<?xml version="1.0"?>
<SCL xmlns="http://www.iec.ch/61850/2003/SCL"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="2007" revision="A">
   <Header id="SSD Example"/>
   <Substation name="Berlin220_132">
      <PowerTransformer name="T1" type="PTR">
         <LNode lnInst="1" lnClass="PDIF" ldInst="F1"/>
         <LNode lnInst="1" lnClass="TCTR" ldInst="C1"/>
         <TransformerWinding name="W1" type="PTW">
            <Terminal connectivityNode="baden220_132/D1/Q1/L1"
            substationName="baden220_132" voltageLevelName="D1"
            bayName="Q1" cNodeName="L1"/>
         </TransformerWinding>
         <TransformerWinding name="W2" type="PTW">
            ...
      </PowerTransformer>
      <VoltageLevel name="D1">
         <Voltage multiplier="k" unit="V">220</Voltage>
         <Bay name="Q1">
            <LNode lnInst="1" lnClass="PDIS" ldInst="F1"/>
            <ConductingEquipment name="I1" type="CTR">
            <Terminal connectivityNode="baden220_132/D1/Q1/L1"
            substationName="baden220_132" voltageLevelName="D1" bayName="Q1"
            cNodeName="L1"/>
            </ConductingEquipment>
            <ConnectivityNode name="L1" pathName="berlin220_132/D1/Q1/L1"/>
         </Bay>
      ...
```

IEC 61850 / Distributed Energy Resources (DER)

Standards and drafts

1. IEC 61850-7-4 (General, Basics)	– 491 pages (final Draft, soon IS)
2. IEC 61850-7-420 (DER Specific)	– 378 pages (almost final Draft)
3. IEC 61850-90-6 (Distribution Automation)	– 213 pages (early Draft)
4. IEC 61850-90-7 (Inverter)	– 102 pages (moved to 7-420)
5. IEC 61850-90-8 (EV)	– 71 pages (early Draft)
6. IEC 61850-90-9 (Storage)	– 128 pages (final Draft)
7. IEC 61850-90-10 (Schedules)	– 40 pages (published)
8. IEC 61850-90-15 (DER Management)	– 44 pages (early Draft)
9. IEC 61850-90-16 (Device Management)	– 90 pages (early Draft)

IEC 61850 -7-420 / Distributed Energy Resources (DER)

Title: Part 7-420: basic communication structure
Distributed Energy Resources and distribution automation logical nodes

Text from IEC 61850-7-420 / INTRODUCTION

Increasing numbers of DER (distributed energy resources) systems are being interconnected to electric power systems throughout the world. …..
…. In the past, DER manufacturers developed their own proprietary communication technology. However, as distribution system operators (DSOs), aggregators, and other energy service providers start to manage DER devices which are interconnected with the power system, they are finding that coping with these different communication technologies present major technical difficulties, implementation costs, and maintenance costs. Therefore, DSOs and DER manufacturers recognize the growing need to have **one international standard that defines the communication and control interfaces for all DER devices**. Such standards, along with associated guidelines and uniform procedures would simplify implementation, reduce installation costs, reduce maintenance costs, and improve reliability of power system operations.
…. Communications for DER plants involve not only local communications between DER units and the plant management system, but **also between the DER plant and the operators or aggregators** who manage the DER plant as a virtual source of energy and/or ancillary services

IEC 61850 -7-420 / Distributed Energy Resources (DER)

Text from IEC 61850-7-420 / INTRODUCTION

… In particular, new DER functions are being defined, and in some cases, becoming mandatory. The mandatory “grid codes” have been defined by various groups in terms of power system interconnection and operational requirements. These grid codes have been assessed for the communication requirements which are included in this DER information model.

In basic terms, “communications” can be separated into four parts:

- **information modelling** (the types of data to be exchanged – **nouns**),
- **services modelling** (the read, write, or other actions to take on the data **– verbs**),
- **communication protocols** (mapping the noun and verb models to actual **bits and bytes**),
- **telecommunication media** (fibre optics, radio systems, wireless systems, and other **physical equipment**)

The general technology for information modelling has developed to become well-established as the most effective method for managing information exchanges. In particular, the IEC 61850-7-x information models for the exchange of information within substations have become International Standard. Many of the components of this standard can be reused for information models of other types of devices.

IEC 61850 -7-420 / Distributed Energy Resources (DER)

Title: Part 7-420: basic communication structure
Distributed Energy Resources and distribution automation logical nodes

Text from IEC 61850-7-420 (CDV) / SCOPE - General

This International Standard defines the IEC 61850 information models to be used in the exchange of information with distributed energy resources (DER) and Distribution Automation (DA) systems. DERs include distribution-connected generation systems, energy storage systems, and controllable loads, as well as facility DER management systems, including aggregated DER, such as plant control systems, facility DER energy management systems (EMS), building EMS, campus EMS, community EMS, microgrid EMS, etc. DA equipment includes equipment used to manage distribution circuits, including automated switches, fault indicators, capacitor banks, voltage regulators, and other power management devices.
The IEC 61850 DER information model standard utilizes **existing IEC 61850-7-4 logical nodes where possible**, while defining DER and DA specific logical nodes to provide the necessary data objects for DER and DA functions, including for the **DER interconnection grid codes** specified by various countries and regions.
Although this document explicitly addresses distribution-connected resources, most of the resource capabilities, operational functions, and architectures are also applicable to transmission-connected resources.

NOTE: This means that DSO and TSO are both actors of the information exchange with DERs ruled by Part 7-420

IEC 61850 – 90- 8 / Object Model for E-mobility

INTRODUCTION

This part of IEC 61850-90, which is a technical report, describes how current standardization for Electric Road Vehicles (EV) and the Vehicle-to-Grid Communication Interface can be linked to IEC 61850-7-420, which deals with Distributed Energy Resources (DER).

This technical report provides necessary background information and proposes **an object model for E-Mobility** in order to establish an **EV plugged into the power grid as DER** according to the principles of IEC 61850-7-420. The basic information modeling in IEC 61850 and IEC 61850-7-420 already covers a lot of needs for the E-Mobility domain. **Missing parts can be modeled as new logical nodes and data objects**, which this technical report defines.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-8: Object model for E-mobility

1 Scope

This part of IEC 61850-90, which is a technical report, shows how IEC 61850-7-420 can be used to model the essential parts of the E-Mobility standards related to Electric Vehicles and Electric Vehicle Supply Equipments (IEC 62196, IEC 61851, IEC 15118) and the Power system (IEC 61850-7-420), in order to secure a high level of safety and interoperability.

Text from IEC TR 61850-90-8

IEC 61850 – 90- 8 / Object Model for E-mobility

Figure from IEC TR 61850-90-8

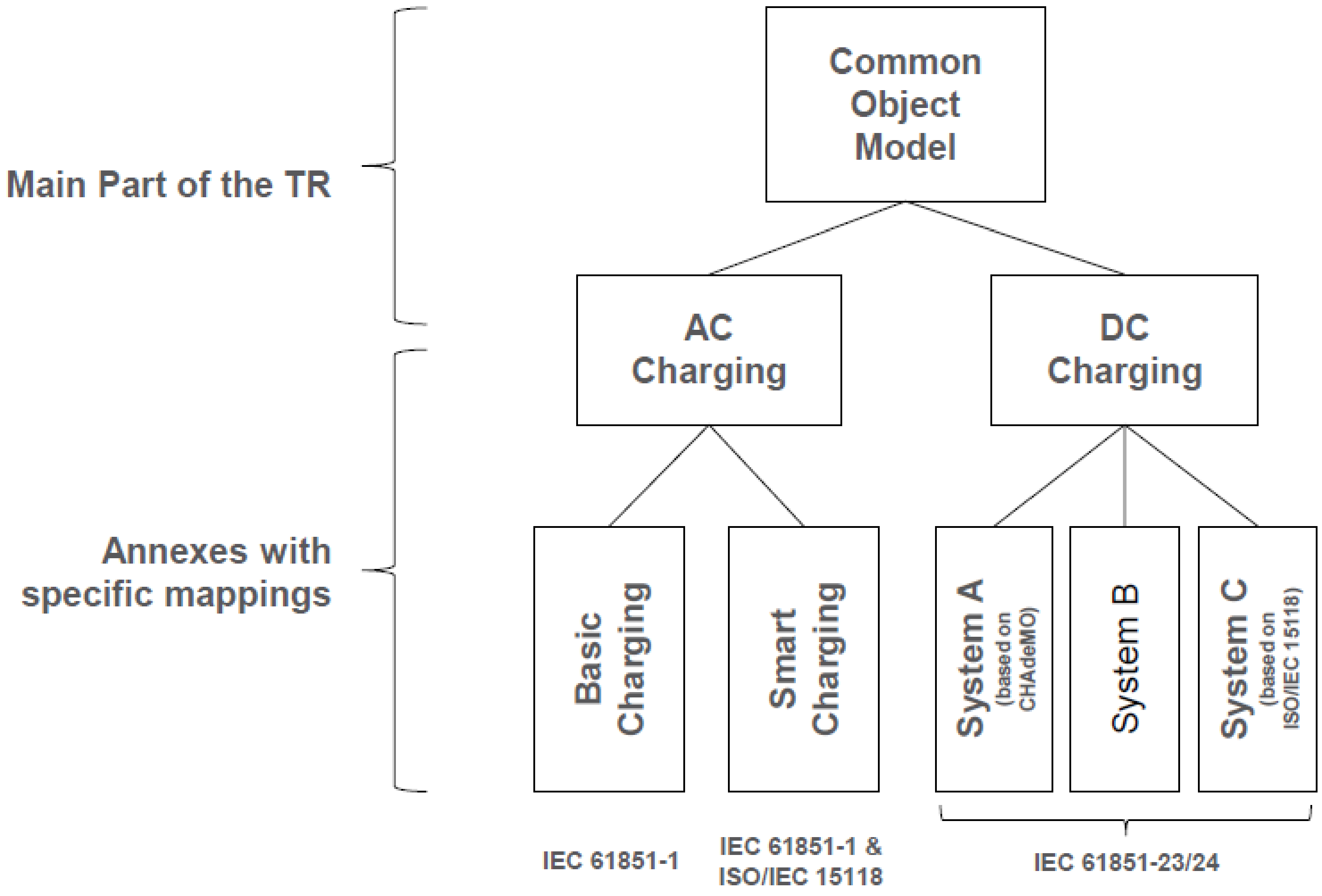


Figure 2: Overview on document structure

IEC 61850 – 90- 8 / Object Model for E-mobility

Text from IEC TR 61850-90-8

CONTENTS

IEC 61850 – 90- 8 / Object Model for E-mobility

Text from IEC TR 61850-90-8

IEC 61850 – 90- 8 / Object Model for E-mobility

Contents

IEC 61850 – 90- 8 / Object Model for E-mobility

Figure from IEC TR 61850-90-8

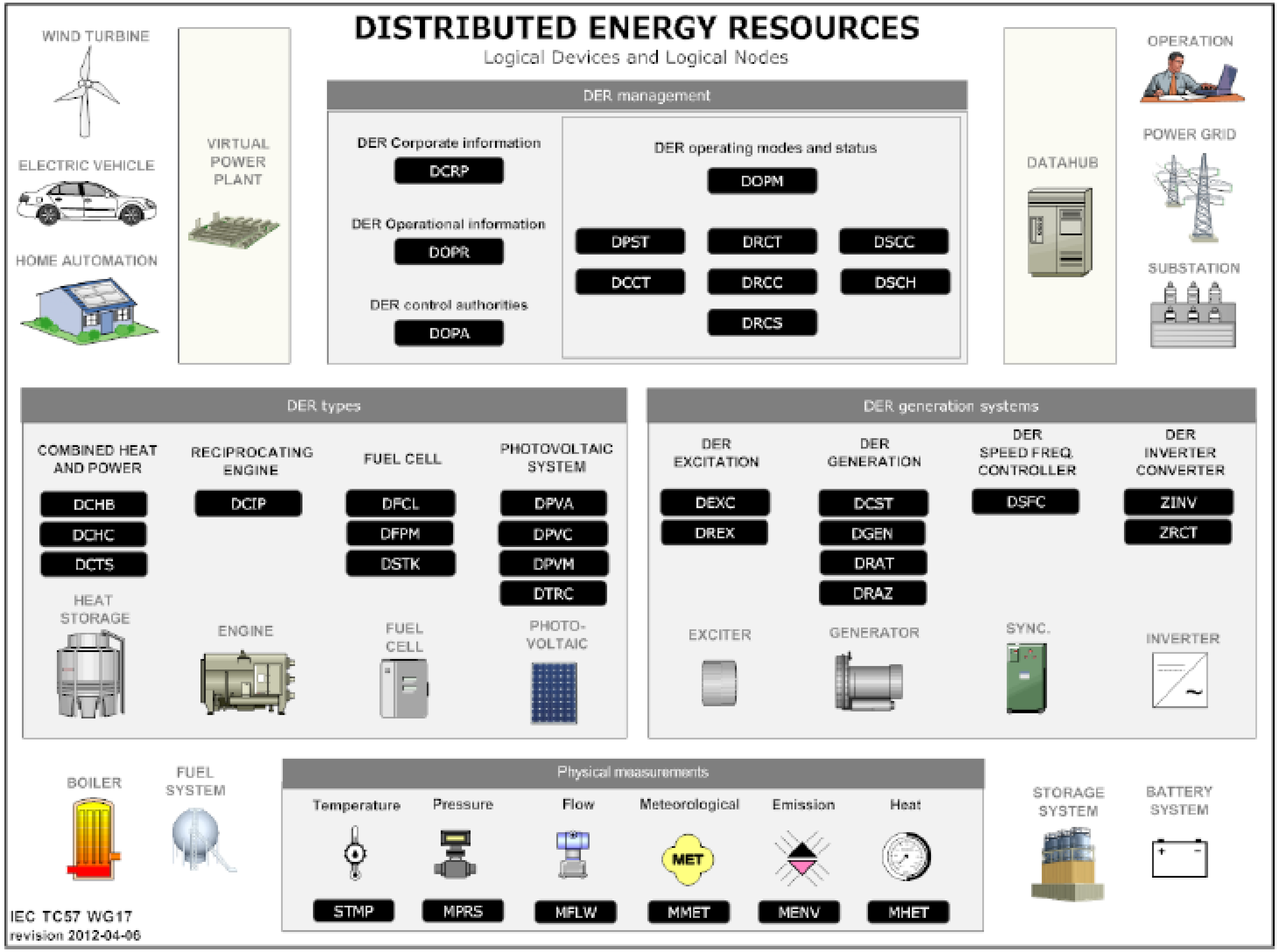


Figure 3: Conceptual organization of Logical Devices and Logical Nodes of DER systems

IEC 61850 – 90- 8 / Object Model for E-mobility

Text from IEC TR 61850-90-8

Table C.22 – Example logical node instances

Logical node instance	Description
DESE1	Models EVSE #1
DEDO1	Models the outlet of EVSE #1
DEEV1	Models the EV connected to the outlet of EVSE #1
DESE2	Models EVSE #2
DEDO2	Models the outlet of EVSE #2
DEEV2	Models the EV connected to the outlet of EVSE #2

IEC 61850 – 90- 8 / Object Model for E-mobility

Figure from IEC TR 61850-90-8

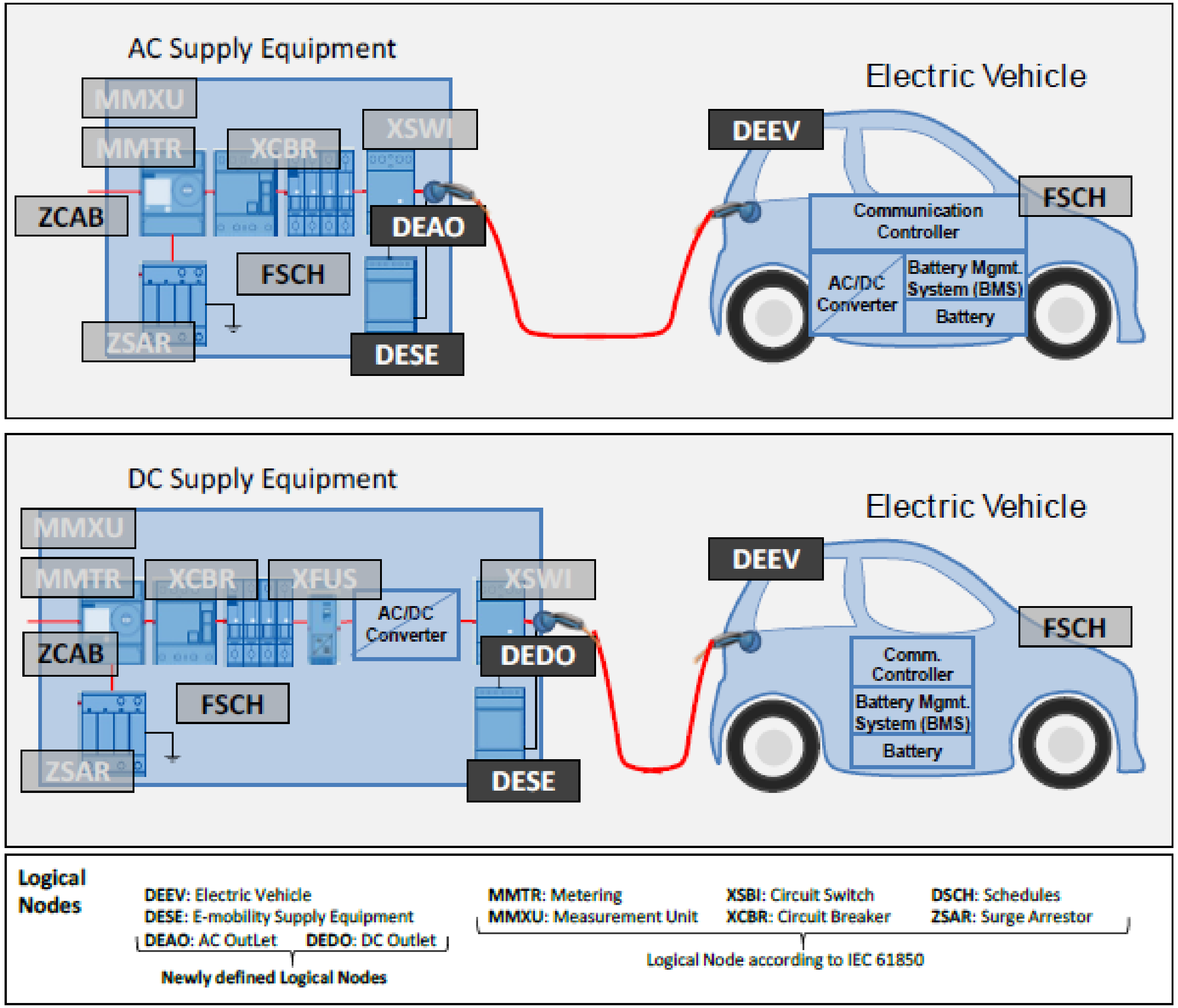


Figure 6: IEC 61850 Logical Nodes overview, based on [IEEE VPPC2012]

IEC 61850 – 90- 8 / Object Model for E-mobility

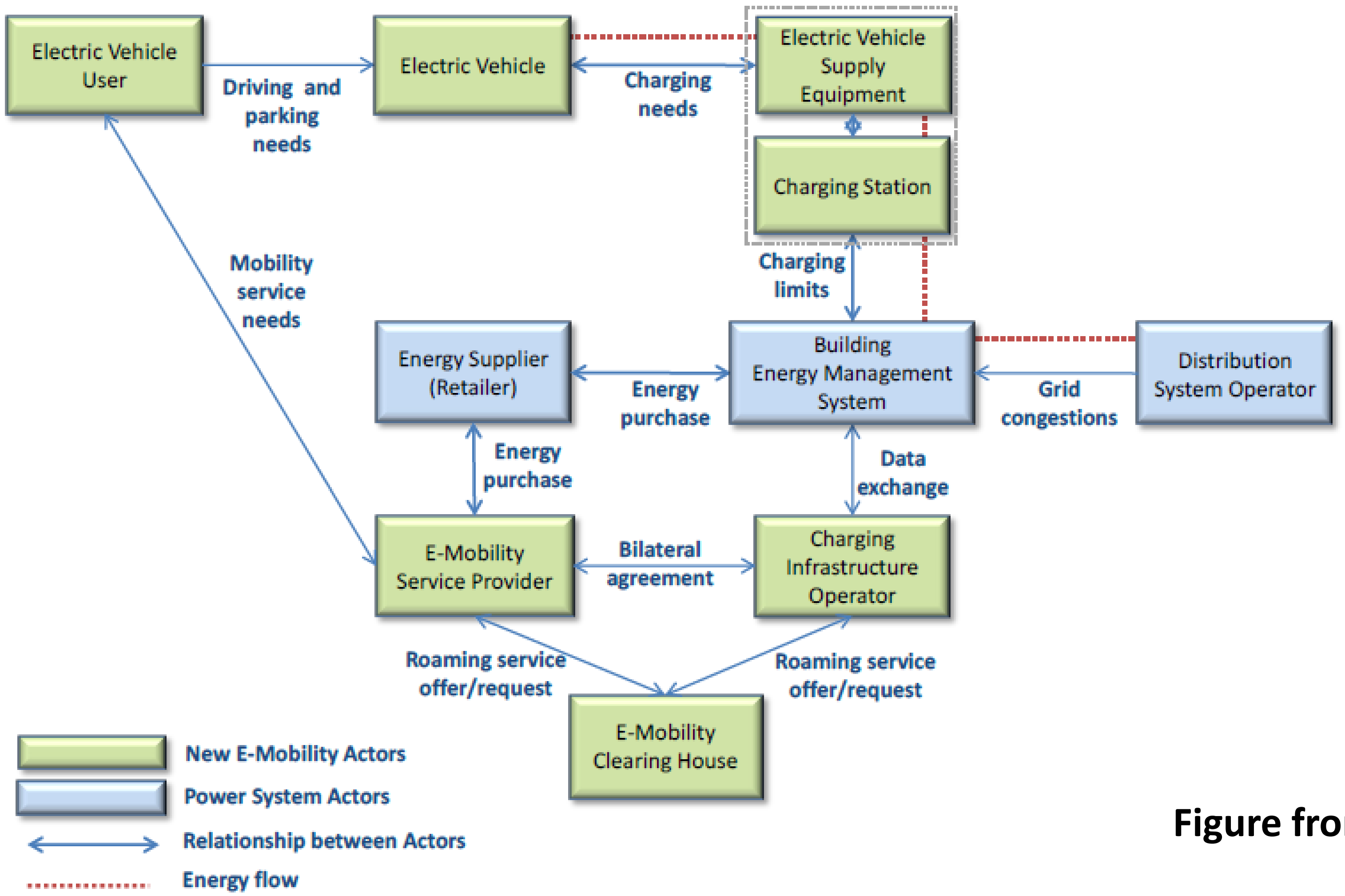


Figure 4: Generic role model of relevant actors for smart charging EVs

Figure from IEC TR 61850-90-8

IEC 61850 – 90- 8 / Object Model for E-mobility

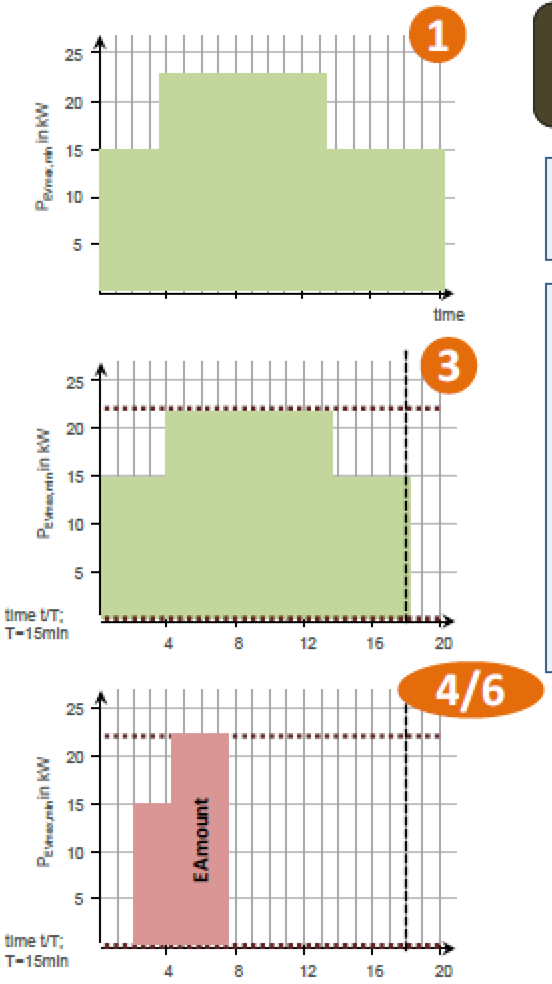
Table 1: Overview of use cases relevant to secondary actors [ISO 15118-1:2013]

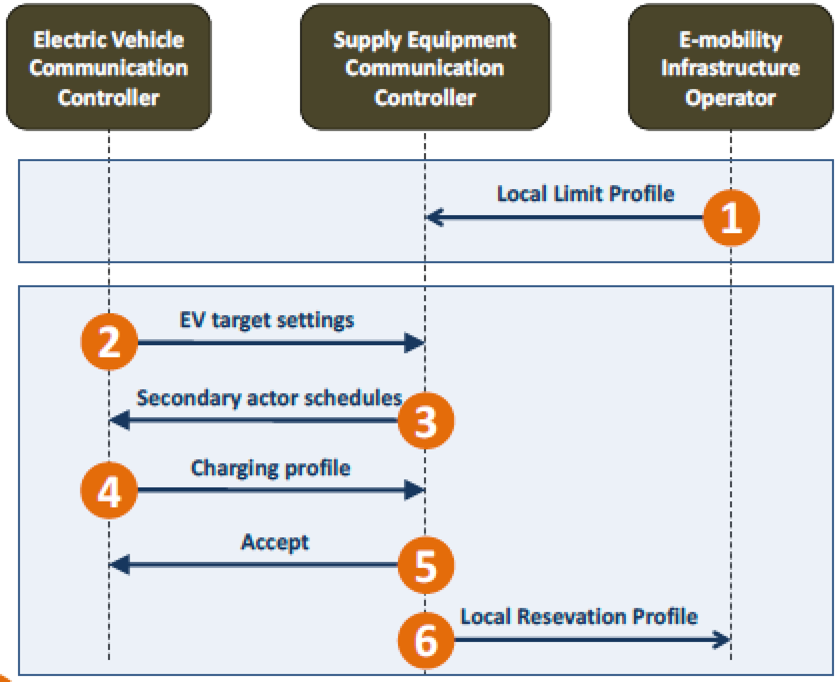
ID	Use case name
C1	Certificate update
C2	Certificate installation
D2	Authentication from EV with Authorisation from secondary actors
D4	Identification at the EVSE with validation from the secondary actor
E2	Optimised charging with scheduling from the secondary actor
E3	Optimised charging with scheduling at EV
F4	Reactive power compensation
F5	Vehicle to grid support
G1	Value-added services
G2	Charging details

Text from IEC TR 61850-90-8

IEC 61850 – 90- 8 / Object Model for E-mobility

Figure from IEC TR 61850-90-8





	Target settings and limits: (2)
EAmount	Amount of energy (EAmount) to be delivered before departure time (DepartureTime)
DepartureTime	Point in time when the user intends to unplug the EV
EVMaxVoltage	Maximum voltage supported by the EV
EVMaxCurrent	Maximum current limits
EVMinCurrent	Minimum current limits

Figure 8: Exemplary exchange of charge schedule information for an EVSE with one outlet, based on [IEEE VPPC2011]

IEC 61850 – 90- 8 / Object Model for E-mobility

Figure from IEC TR 61850-90-8

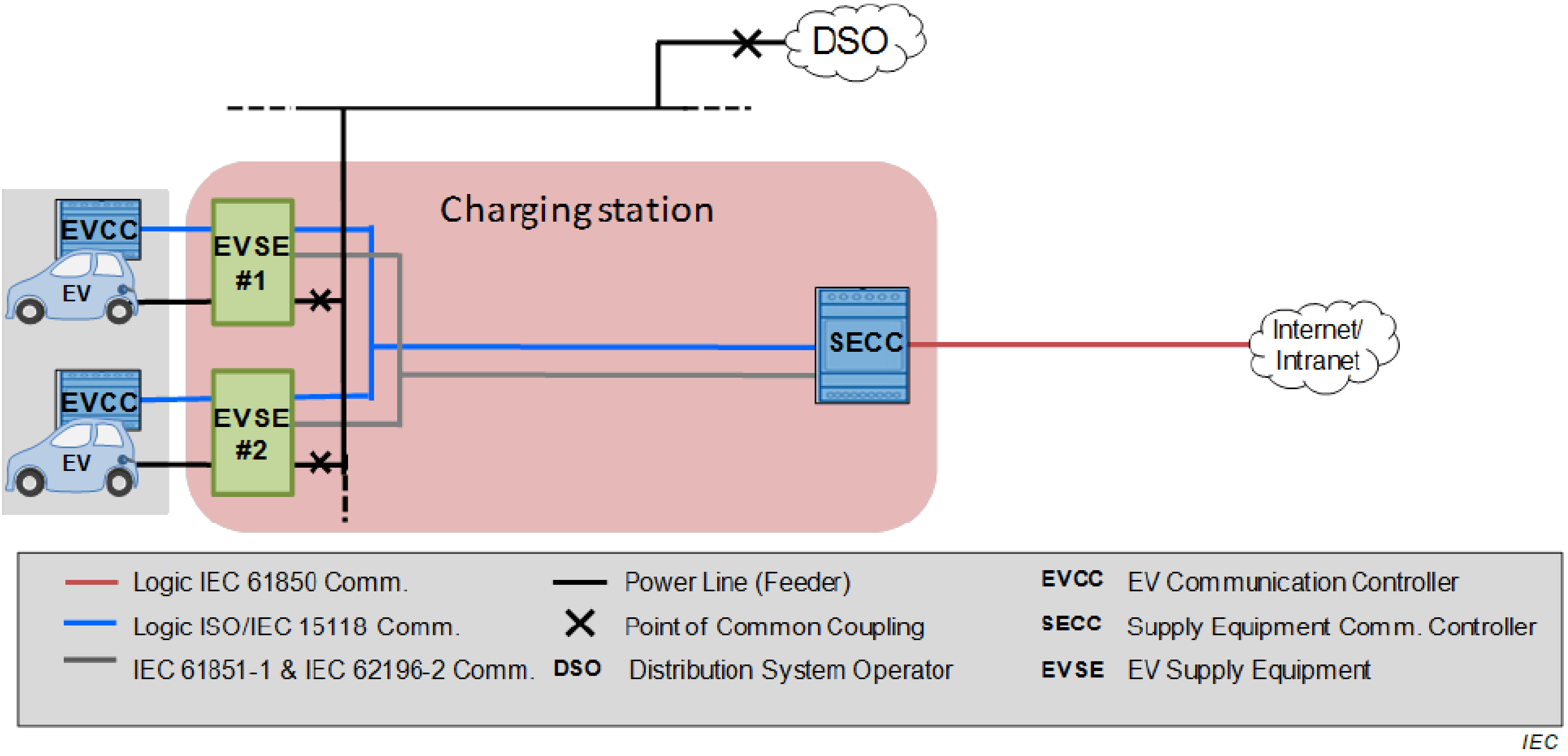


Figure C.1 – Example of an AC charging station

IEC 61850 – 90- 8 / Object Model for E-mobility

Figure from IEC TR 61850-90-8

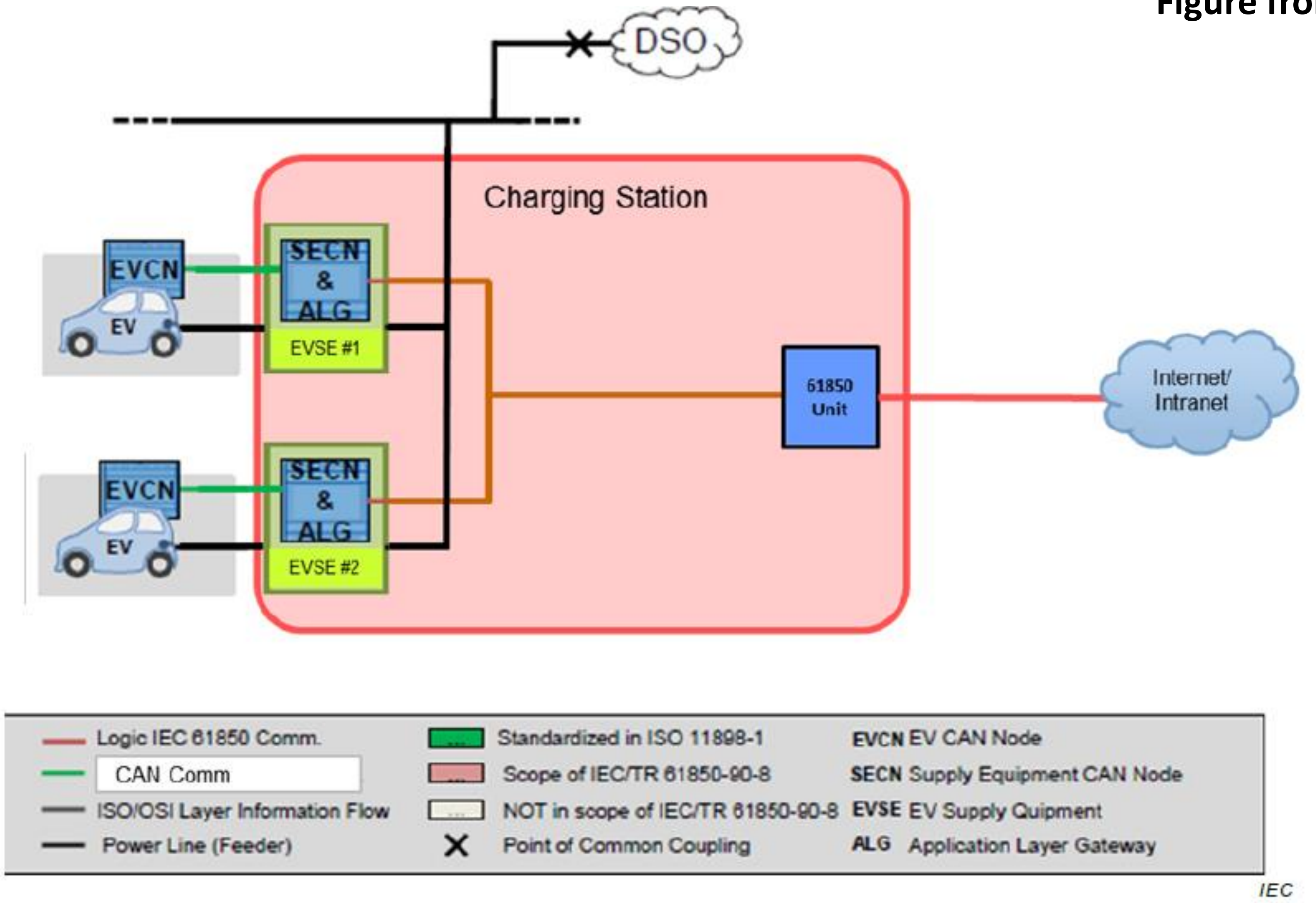


Figure C.2 – Example of a DC charging station

Cyber and Physical Vulnerabilities of IEC 61850 Communication Network

Smart grid incorporates data communication network into existing electrical power systems to provide a more efficient and resilient power grid. IEC 61850 deals with communication networks for automation of substations and modern electrical power systems (Smart Grids)

Cyber and Physical Vulnerabilities

Cyber-Physical systems like smart grid, are vulnerable to both cyber acts and physical events that could critically impact their safe and reliable operation.
High availability, tight coupling of components, and time sensitive communication requirements of power systems make them even more vulnerable.

Physical Vulnerabilities

Attacks on Physical Components – An attacker can physically attack sensors, actuators and other components that may result in faulty measurements causing errors in the system state estimation and control operations

Faults and Failure of Components – Devices may fail during operation. These failures could be caused by some accumulated faults or the device reaching its end of life.

Accidents and Acts of Nature – Severe weather conditions could cause instability in power systems and power disruption.

Cyber and Physical Vulnerabilities of IEC 61850 Communication Network

Cyber Vulnerabilities

Software and Firmware Bugs

IED and Network Misconfiguration – Some of these misconfigurations include:

- Using default settings and default passwords even when the device is operational,
- Poorly maintained security and software patches,
- Using short and guessable passwords,
- Poorly configured firewall

Data Manipulation and Falsification

Data manipulation and falsification attacks affect data integrity.

By altering certain bits of the signal, an attacker alters the meaning of the control signal.

An attacker with knowledge of how the system works can generate packets or replay previously recorded packets to change the correct behaviour of the system.

Data manipulation attacks are countered by proper application of cryptographic controls in the authentication and integrity checks of communicating nodes and data.

Cyber and Physical Vulnerabilities of IEC 61850 Communication Network

Cyber Vulnerabilities (continue)

<u>Malware and Advanced Persistent Threat (APT)</u>

Malware are pieces of software with malicious intent.

Malware could open covert communication channels to the remote attacker so that the attacker can take control of the host, send vital information about the system to a remote attacker, or just perform pre-programmed malicious actions

APTs are unique forms of malware and attacks that use various stealthy techniques to gain remote access while staying undetected on the host system for a long time.

<u>Communication Channel</u>

power systems are distributed and cover multiple locations requiring communication links between the various parts of the system.

This communication network can be wired or wireless, although the wireless connection is most often used. One weakness of wireless communication is that of visibility. Anyone in proximity to the wireless network and operating on the same frequency and channel can see the network traffic. Power systems rely on the timeliness of communication packets to operate (e.g., interlocking and switching functions in power distribution systems) and a delay or loss of packets may yield undesired results.

Typical attacks include signal jamming, wormhole attacks, and signal diversion attacks.

Cyber and Physical Vulnerabilities of IEC 61850 Communication Network

Coordinated Cyber-Physical Attacks

Another possibility is a coordinated cyber-physical attack, exploiting both the physical and cyber vulnerabilities of the power system in a contemporary way to maximize the impact.
This kind of attack could be a collusion between an insider with access to the physical power system components, and a cyber attacker at a remote location with knowledge of the power communication network working together to cause cascading failures and service disruption.

How to secure IEC 61850 Communication by IEC 62351

Information security is a serious concern for power management systems.
IEC 62531 standard is the globally accepted standard for securing power management systems.
IEC 62531 defines information security requirements for the various communication profiles used in substation and power system automation necessary to provide confidentiality, integrity, availability, and non-repudiation.

TCP Profile: IEC 62531-3 specifies the use of transport layer security (TLS) 1.0 or higher to protect TCP/IP profiles and provides protection against:

- eavesdropping through encryption,
- spoofing through Security Certificates (Node Authentication),
- replay through TLS encryption,
- and man-in-the-middle security risk through message authentication.

It mandates digital signature standard (DSS), signature algorithms with RSA key length of 2048 bits and also mandates the support for regular and ephemeral Diffie-Hellman key exchange with a key length of 2048 bits.
For authentication, it mandates the use of the X.509 certificates with support for multiple certificate authority (CA).

MMS Profile: IEC 62531-4 defines the security requirements for all profiles that include MMS. It provides authentication through the use TLS based X.509 certificates
Encryption according to IEC 62531-3.

How to secure IEC 61850 Communication by IEC 62351

GOOSE and SV: IEC 62531-6 defines the security requirements for IEC 61850 communication profiles.
GOOSE and SV profiles use multicast and non-routable messages that run on the substation LAN, and must be transmitted within 4ms.
IEC 62531-6 does not recommend the use of encryption or certificate based authentication as it may increase the transmission time and add more processing overhead.
For GOOSE profile, encryption can be used only if the processing and transmission time is less than 4ms. For message authentication and integrity protection of GOOSE and SV messages, the IEC 61850 supports the use of HMAC digital signatures.

Access Control and Certificate Management:
IEC 62531-8 specifies the use of role-based access control (RBAC) for power systems.
RBAC defines roles and set of rights associated with each role.
Users/Entities are assigned to roles, and they inherit all the rights associated with that role. The IEC 62531-8 standard defines a list of roles and associated rights for power systems

IEC 62351 – Overview

IEC 62351 (Information Security for Power Systems Control Operations)
It is the security standard which defines the end to end cyber security requirements for securing power management networks.
It specifies the security requirements for secure data communication and processing in power systems in regards to data confidentiality, data integrity, authentication, and non-repudiation.
It consists of several parts.

IEC 62351-1: general overview of the standard, information on security, threats and countermeasures.

IEC 62351-2: glossary of terms

IEC 62351-3: security of protocols based on TCP/IP used for automation of electrical power systems.
It prescribes use of Transport Layer Security (TLS) with X.509 certificates.
Purpose is to ensure authenticity and integrity of data on the transport layer, and also confidentiality by using the encryption mechanisms of TLS.
TLS counters also threats such as man-in-the-middle-attacks and replay attacks.
Mutual authentication through certificates (i.e., client and server each present a certificate) is required. Algorithms and some minimum key lengths to be used are prescribed.

IEC 62351 – Overview

IEC 62351-4: security for profiles such as Manufacturing Message Specification (MMS), which is used in IEC 61850 Recommendations for A-Profile and T-Profile based on TCP/IP.
A-Profile: Use of X.509 certificates to authenticate applications,
T-Profile: How to use TLS as a layer between TCP and the ISO Transport Service adopting a different TCP port for secure connections.

IEC 62351-5: security for protocols related to IEC 60870-5 (-101, -103, -104) and derivatives such as DNP-3 (IEEE)
These protocols are message-based, and authentication needs to be done on a per-message basis.
As keys used for authentication and encryption should be changed regularly, it proposes mechanisms to update keys in a device remotely.

IEC 62351-6: security for protocols described in IEC 61850.
For MMS and protocols using TCP/IP, the provisions described in IEC 62351-4 shall apply
Extension to GOOSE and SMV PDUs (protocol data unit), by addition of a field to the PDU containing security-relevant information. The extension is intended to authenticate a PDU by inclusion of a signed hash of the PDU.

IEC 62351 – Overview

IEC 62351-7: Power systems infrastructure makes heavy use of interconnected information systems to manage operations. This information systems infrastructure also needs to be securely managed, which is done using the Simple Network Management Protocol (SNMP)
Part 7 describes data object models to be used that are specific to power systems.

IEC 62351-8: Role-based access control (RBAC) for power systems infrastructure.
It addresses different modes of access, such as direct and remote access, as well as access by human users and automated access by computer agents.
It defines a list of predefined roles (Viewer, Operator, etc.), and of pre-defined rights (View, Read, Control, etc.).

IEC 62351-9: certificate and / or key management.

IEC 62351-10: general guidelines for the security architecture of power systems.

IEC 62351 Security Standard vs IEC TC57 Communication Standards

TC57 has developed Communication standards for power systems, specifically in EC 61850 and IEC 60870-5