Specifications and IT Use-Case definition for V2X services

Project Deliverable 2.2

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101056874.

WWW.SCALE-HORIZON.EU

1 Deliverable administrative information

Deliverable number	D2.2
Deliverable title	Specifications and IT Use-Case definition for V2X Services
Dissemination level	Public
Submission deadline	30/06/2023
Version number	V1.0
Authors	Jordan Sautreau (Trialog) Jelle Mersmans (Enervalis)
Internal reviewers	Yannick Huc (Trialog) Guillaume Mockly (Trialog) Eric Smets (Enervalis)
Document approval	Baerte de Brey (ElaadNL)

1.1 Legal Disclaimer

SCALE is funded by the European Union's Horizon Europe Research and Innovation program under Grant Agreement No 101056874. The views represented in this document only reflect the views of the authors and not the views of the European Commission. The dissemination of this document reflects only the author's view, and the European Commission is not responsible for any use that may be made of the information it contains.

2 Project Executive Summary

SCALE (Smart Charging Alignment for Europe) is a three-year Horizon Europe project that explores and tests smart charging solutions for electric vehicles. It aims to advance smart charging and Vehicle-2-Grid (V2G) ecosystems to shape a new energy system wherein the flexibility of EV batteries' is harnessed. The project will test and validate a variety of smart charging and V2X solutions and services in 13 use cases in real-life demonstrations in 7 European contexts: Oslo (NO), Rotterdam/Utrecht (NL), Eindhoven (NL), Toulouse (FR), Greater Munich Area (GER), Budapest/Debrecen (HU) and Gothenburg (SE). Going further, project results, best practices, and lessons learned will be shared across EU cities, regions, and relevant e-mobility stakeholders. SCALE aims to create a system blueprint for user-centric smart charging and V2X for European cities and regions.

3 SCALE partners

List of participating cities:

- Oslo (NO)
- Rotterdam & Utrecht (NL)
- Eindhoven (NL)
- Toulouse (FR)
- Greater Munich Area (GER)
- Budapest & Debrecen (HU)
- Gothenburg (SE)

List of partners:

- (Coordinator) STICHTING ELAAD NL
- POLIS - PROMOTION OF OPERATIONAL LINKS WITH INTEGRATED SERVICES, ASSOCIATION INTERNATIONALE POLIS BE
- GoodMoovs NL
- Rupprecht Consult – Forschung & Beratung GmbH RC DE
- Trialog FR
- WE DRIVE SOLAR NL BV NL
- UNIVERSITEIT UTRECHT NL
- LEW Verteilnetz GmbH DE
- BAYERN INNOVATIV - BAYERISCHE GESELLSCHAFT FUR INNOVATION UND WISSENSTRANSFER MBH DE
- ABB BV NL
- Enervalis BE
- GEMEENTE UTRECHT NL
- Equigy B.V. NL
- SONO MOTORS GMBH DE

- Meshcrafts As (Current) NO
- Research Institutes of Sweden AB SE
- ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH) GR
- FIER Automotive FIER NL
- Emobility Solutions Kft. HU
- Serviced Office Belbuda Kft HU
- Enedis FR
- L'ASSOCIATION EUROPEENNE DE LA MOBILITE ELECTRIQUE (AVERE) BE
- Norsk elbilforening NO
- VDL ENABLING TRANSPORT SOLUTIONS BV NL
- Urban Electric Mobility Initiative UEMI DE
- Renault FR
- Chalmers University SE
- Polestar SE
- Hyundai NL NL

Social Links:


twitter.com/scaleproject_


www.linkedin.com/company/ scale-project-smart-charging-alignment-for-europe


www.youtube.com/channel/UC1HVFu5uJPCNSV96b3l_rcg

For further information please visit **WWW.SCALE-HORIZON.EU**

4 Deliverable executive summary

4.1 Key words

Electric vehicles, smart charging, bidirectional charging, V2X, interoperability, flexibility, congestion

4.2 Summary

To be able to deliver energy services through charging session optimization, new actors in the ecosystems or data consumers require access to correct and timely data from different data sources. These data needs can relate from data required to compute an optimum charging schedule by a Flexibility Service Provider (FSP) to real-time measurements required by a TSO to verify and validate the correct delivery of a balancing service.

Through expert interviews and workshops, a bottom-up data requirement analysis applied to different behind-the-meter (BTM) and front-of-the-meter (FTM) services was performed to discover what would be required and desired from a data consumer perspective with respect to what data needs to be available at what quality.

This analysis shows that from the different data categories covered being site, EV, Charging Station and User related data, the availability of site related data imposes the biggest barriers to consumer- and grid-centric adoption of the different energy services through smart and bidirectional charging.

Particularly the availability of contractual related data such as the applicable electricity tariff components for BTM services or unique identifiers for the grid connection or active BRP for FTM TSO services create barriers for wide scale adoption. While availability of data can be solved through institutional or protocol interventions, achieving the desired data quality could be more challenging to solve as this impacts the enabling IoT infrastructure of different actors in the eco-system.

To solve these challenges, different insights and recommendations are provided in paragraph 8.4 such as delta monitoring on dynamic data to reduce the amount of data traffic between actors or event streaming architectures to reduce the data latency in the eco-system.

This output and collected insights of chapter 8 will be further used as a basis for Task 2.3 in which proposals will be defined for new protocol updates to make sure the required data could be made available within the right timeframe.

The V2X services does not only generate positive impacts on grid management but could also generate some negative side effects as described under chapter 9. Particularly, BTM services like dynamic time-of-use could generate adverse effects on voltage magnitude and rate of change thereby impacting the DSO. These impacts need to be anticipated in order to prepare Europe for the mass scale-up of smart and bidirectional charging. However, as recommended in paragraph 9.2, these impacts could be mitigated if proper requirements were included in the anticipated amendments to the network code for demand connections and generators for smart and bidirectional charging respectively.

Collecting data on EV users by the different actors of the ecosystem also implies data privacy and cybersecurity requirements. Chapter 10 therefore addresses the data privacy and cybersecurity concerns for each actor in terms of governance, threat detection and responses.

Cybersecurity is a major concern for the successful implementation of smart charging and Vehicle-to-Grid (V2G) services. As the automotive industry embraces the integration of electric vehicles (EVs) into the power grid, ensuring the protection of critical infrastructure and sensitive data becomes essential. This connectivity exposes the system to potential cyber threats, including unauthorized access, data breaches, and vehicle manipulation.

Imagine a scenario where a cybercriminal gains unauthorized access to the charging system and intentionally alters the charging schedules of a large fleet of electric vehicles connected to the grid. By strategically manipulating the charging patterns, they overload specific grid sections, causing localized power outages or compromising grid stability. This not only disrupts the reliable delivery of electricity but also poses safety risks for consumers and may result in significant economic losses. Such a compelling example underscores the critical importance of robust cybersecurity measures in protecting bidirectional charging systems and preventing potential malicious activities that can have far-reaching consequences.

This report aims to contribute to both the understanding of what is required from a data perspective to achieve mass-scale uptake of smart and bidirectional charging services as well as create general awareness around the potential impacts that a massive uptake could have and provide recommendations on how they could be mitigated.

5 Table of content

6 List of abbreviations and acronyms

Acronym	Meaning
aFRR	automatic Frequency Restoration Reserve
BPT	Bidirectional Power Transfer
BRP	Balance Responsible Parties
BTM	Behind-the-meter
CPO	Charge Point Operator
DSO	Distribution Grid Operator
EMS	Energy Management System
eMSP	e-Mobility Service Provider
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FCR	Frequency Containment Reserves
FRR	Frequency Restoration Reserves
FSP	Flexibility Service Provider
FTM	Front-of-the-meter
GDPR	General Data Protection Regulation
HEMS	Home Energy Management System
OEM	Original Equipment Manufacturer
SCALE	Smart Charging Alignment for Europe
SCSP	Smart Charging Service Provider
SoC	State of Charge
TSO	Transmission System Operator
V2B	Vehicle-to-Building

V2G	Vehicle-to-Grid
V2H	Vehicle-to-Home
V2X	Vehicle-to-Everything

7 Purpose of the deliverable

7.1 Attainment of the objectives and explanation of deviations

The objectives related to this deliverable have been achieved in full and as scheduled.

7.2 Intended audience

7.2.1 SCALE Consortium partners

The primary audience for this deliverable is the project partners involved in the development and implementation of V2X services. They can utilize the deliverable to perform data integration and optimization by comparing the data they can share with the expected data. Then the deliverable's cybersecurity requirements section will guide project partners in implementing robust security measures to safeguard the V2X ecosystem against cyber threats.

7.2.2 E-mobility actors

The report benefits e-mobility actors by providing them with the knowledge and insights necessary to develop V2X-ready products, optimize charging infrastructure, align with industry standards, and stay ahead in the rapidly evolving e-mobility market. By embracing V2X services and adhering to cybersecurity best practices, e-mobility actors can enhance their offerings, expand their market reach, and contribute to the growth of sustainable and intelligent transportation systems.

7.2.3 Grid operators

The report offers grid operators a comprehensive understanding of the impact of V2X services on their operations. It empowers them to make informed decisions, improve grid stability, enhance efficiency, and build resilient infrastructure while proactively collaborating with other stakeholders in the e-mobility sector. Ultimately, the benefits gained from this report contribute to a successful integration of V2X services into the power grid, promoting sustainable and intelligent energy management.

7.2.4 Standardization bodies

The insights provided in the deliverable can contribute to the development of regulatory frameworks and standards related to V2X data exchange, grid impact mitigation, and cybersecurity measures. The list of required data to enable V2X services can be used to extend existing protocols to handle them. The data requirements section can help standardization bodies to maximize the interoperability that ensure seamless communication between diverse systems. This will enhance compatibility and collaboration among various stakeholders in the e-mobility sector.

8 Structure of the deliverable & link with other work packages

To identify the gaps in protocol coverage across the e-mobility ecosystem, this report provides a list of minimum data with related quality requirements that need to be covered by e-mobility related protocols.

In our desired future scenario, electric vehicles will be transformed to energy storage assets of which its flexibility could be used in the energy system where it is valued the most in time and space while ensuring the mobility needs of the driver are always covered. The prerequisite is therefore that all energy services must be able to be delivered according to the principles of the system architecture.

To optimally deliver these different energy services by modulating the charging or discharging power in real-time, new types of actors or data consumers arise that require input data to for example optimally compute a charging schedule or in the case of the TSO, high quality, and timely measurement data to validate and settle the delivery of a balancing service.

This task will therefore analyze what these different needs are with respect to the specific data input requirements are from these data consumers for both the different behind-the-meter as well as front-of-meter services.

As input data required by a data consumer can always be traced back to a data source, the data source is also identified. This can be a specific device such as an EV or charging station, a DSO who centrally manages (access to) certain grid or energy consumer information or mobility needs parameters tied to the user.

The output of the bottom-up analysis for each energy service done under chapter 8 will serve as direct input for the protocol definition of Task 2.3.

This task will identify the different interoperability gaps for the different protocols that would be used to transport the different required data with their respective data quality requirements from the data source to the data consumer, such as the Energy Management System (EMS), TSO or Smart Charging Service Provider.

Secondly, the delivery of these energy services could also create an undesired negative impact to other electricity system-side market actors. Delivering balancing services for example impacts the BRP, requiring portfolio corrections and sourcing cost settlement. Chapter 9 focusses specifically on identifying these specific impacts for the BRP, DSO and TSO respectively and provides some recommendations on how they could be mitigated.

As these new data needs could be privacy or security sensitive, the impact on GDPR and cyber-security of these data requirements will be further investigated in chapter 10.

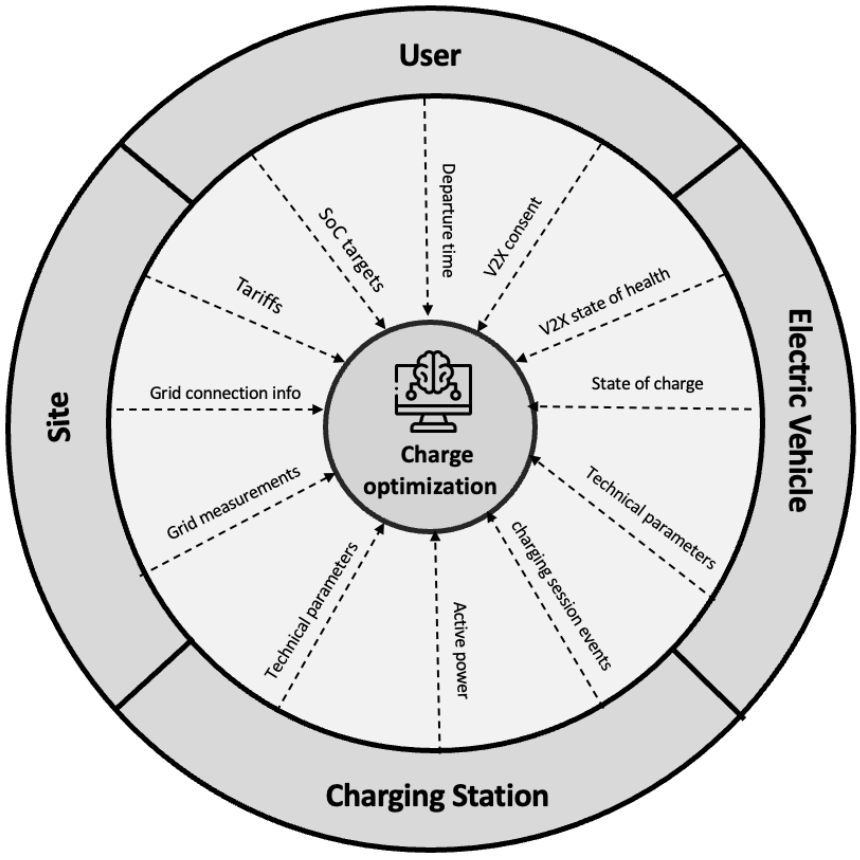
9 Data requirements for energy services

9.1 Introduction

The current dominant protocols and their versions adopted by the e-mobility ecosystem were primarily designed for providing a seamless charging experience to the EV driver with the aim to allow them to charge as fast as possible at every charging station, not necessarily to provide smart or bidirectional charging services with the same level of customer experience.

As depicted in the figure below, the delivery of these energy services through charge optimization are creating new data requirements for the ecosystem to exchange data not previously exchanged, exchange data at a higher data quality or provide data to an actor that previously did not have access to that data.

This results in interoperability issues for actors actively involved in the energy service delivery for smart or bidirectional charging.



This chapter aims to investigate the different data requirements for the different energy services through a bottom-up data analysis and is divided into 2 parts: one that concentrates on behind-the-meter (BTM) services and another that focuses on front-of-the-meter (FTM) services.

This split is based on various factors which are explained below.

- **Actors involved**

Compared to FTM services, the delivery of BTM services requires the active involvement of a more limited set of actors. As the main beneficiary of FTM services is always an energy-system side actor like a TSO, DSO or BRP, this energy-system side actor also acts as data-consumer with regards to such FTM services for example service delivery validation purposes. These energy-system side actors are not actively involved in the delivery of BTM services, in which the flexibility service provider is considered the only data consumer for the delivery of the smart or bidirectional charging service.

- **Customer attractiveness**

The tangible and direct benefits to consumer electricity bills make BTM services more appealing and easier to comprehend from a consumer's point of view compared to FTM services. By examining these factors and distinguishing between BTM and FTM services, the analysis can provide insights into the different dynamics, stakeholders, and quality considerations with each category of energy services.

- **Data quality requirements**

The specific needs and expectations of customers differ when it comes to services installed on their premises (BTM) versus services provided by utility companies on the grid side of the meter (FTM). Each type of service may have unique considerations regarding performance, reliability, and customization to suit individual customer requirements.

For each energy service, the different data objects that are required as input for the data consumers were analyzed based on three aspects, detailed in the following chapters.

9.1.1 Charging Process

Regardless of the specific energy service targeted with smart or bidirectional charging, its delivery can be abstracted into processes. For this data requirement analysis, a distinction was made between the onboarding process and the charging session lifecycle processes (start of a charging session, updates during a charging session and end of a charging session).

These different processes are explained in the table below.

Process	Description
Onboarding	Data objects linked to the onboarding process cover data that can be required by a grid operator for registering a site or asset for a specific balancing service like FCR or aFRR. More broadly, it covers all static data required to compute an optimal charging schedule for a particular energy service within the physical limits of the site and assets while ensuring the mobility needs of the user are covered. This is to make sure that this data is available to be exchanged once a first smart or bidirectional charging session will need to be executed on behalf of the user. As this concerns static data only, no specific data quality requirements will be applicable.
Start of a charging session	At the start of a charging session, the flexibility service provider requires different data so that it can compute an optimal charging schedule with regards to the energy service it aims to deliver on behalf of the user. In addition to static data that was collected during the onboarding phase, required input data can also encompass more dynamic data such as real-time grid measurements.
Updates during a charging session	To optimally deliver a smart or bidirectional charging service throughout an active charging session, one needs to react to changes in the environment by adjusting the charging schedule to it. Examples of such changes could be changes in mobility needs like departure times, building electricity consumption, availability of excess solar energy, …
End of a charging session	For user insights purposes, different data requirements exist at the end of the charging session compared to at the start or during the charging session. Examples of such requirements could be linked to charging costs, cost savings insights, total amount of kWhs discharged…

9.1.2 Data quality criteria

Depending on the charging session lifecycle process, the data quality requirements from the data consumer for the different data objects can be different. These requirements for the different energy services will be assessed based on the following aspects: timeliness, sampling rate and accuracy.

Criteria	Description
Timeliness	Relates to the time difference between the measurement and the time at which the data reaches its destination. Data timeliness is determined by the ability of the data chain and the actors involved to transfer the generated data, process it, and make it available to the data consumer.
Sampling rate	Relates to the frequency at which data is collected or measured over a given period. A higher sampling rate results in higher data transfer, processing, and storage costs. For specific data, a period is provided due to roles constraints. Otherwise, the rate is qualified with high, low, or once if the data value does not change.
Accuracy	Refers to the correctness, precision, and reliability of the data. It indicates how closely the data represents the actual values or measurements it is intended to capture. Accuracy is crucial for making informed decisions, conducting analyses, and ensuring the reliability of downstream processes that rely on the data.
Unit	Refers to the unit of the data. Some data corresponds to specific data structures, so the concept of unit is not applicable (NA).

9.1.3 Data Categories

Data categories in this analysis represent a logical clustering of data objects traced back to a system component, being the site, the electric vehicle, charging station and user. This additional data classification step helps to expose the data source from the different data objects and will provide valuable input for Task 2.3 in which the interoperability gaps regarding the different protocols will be covered.

Data Category	Description
Site	Data linked to a site, represented by a unique identifier. This includes for example data related to applicable electricity tariffs, grid measurements or other technical parameters related to the grid connection. Typically, this data is stored in a central register managed by the Distribution System Operator (DSO), making the DSO the data source for site-linked data objects.
Electric vehicle (EV)	Data linked to the electric vehicle (EV) of the user ranging from state-of-charge measurements to technical information such as minimum or maximum charging power.

Charging Station (CS)	While charging stations act as local sensing networks collecting data from the EV or local grid, this data category includes information exclusively linked to the charging station itself. Examples include active charging profiles and technical parameters like maximum and minimum charging power.
User	Data linked to the user, such as mobility needs (departure time, etc.) or their assigned flexibility service provider

9.2 Service delivery

There are different types of services that are being delivered to the electricity market, these are divided into two main categories. Behind the meter services are local services giving an optimization for the site or the end user and these service implementations are less complex than the in front of the meter services. This last type of service is delivering to the electricity system on a more global scale. All the services in the different categories are defined separately but some of them can be combined, the different combinates are not described but will be implemented in some of the use cases of SCALE.

All the services for the electricity market do need a common set of parameters, data coming from this ecosystem. Before defining the specific needs (on data requirement and data quality) the common data description for all the services is defined in this section.

Data category	Data object	Description	Reason	Data Source	Data Consumer	On boarding	Start	During	End	V2X Specific
Site	Consumption Retail Tariff	Volumetric electricity retail tariff applicable for a given period.	Required as cost input related to time-of-use BTM energy services as well as to compute cost savings for all BTM energy services	User	FSP					No
	Grid connection capacity	The physical capacity at grid connection point level	Required for dynamic load balancing. it assumes that the charger manages this by itself through local load balancing. Required for maximizing the charging speed without blowing the main fuse	User	Charging Station					No

	Local frequency	The local grid frequency at grid connection level	Required for grid code compliance in case of bidirectional charging	Grid meter	Charging Station					Yes
	Local Voltage	The active voltage measured at grid connection level	Required for grid code compliance in case of bidirectional charging	Grid meter	Charging Station					Yes
	Active grid power	The active power measured at the grid connection level	Required to know how power is being consumed from or injection into the grid in real-time	Grid meter	Charging Station					No
CS	Grid Code Coordinates	Coordinates of the different grid code requirements that define how a generator should behave within certain grid operating conditions (volt & Var)	Ensure compliance with local grid codes based on local grid measurements (Volt & Freq) can be provided in case of V2G. The coordinates are used by the charging station to construct grid code curves and compute reactive or active power commands for the vehicle based the local grid measurements	DSO	EVSE					Yes
	EVSE ID	The unique identifier of the connector (=	In order to link EVSE constraints (ex. max charging power) to the proper	CPO	FSP					No

		EVSE) from the charging station	connector and charging session							
	Maximum charging power	The maximum charging power on EVSE level	To provide insights to the user related to charging speed insights	EVSE	FSP					No
	Active Power	The measured active power at a given point in time	To know how much power is sent to the EV	EVSE	User					No
	Session ID	The unique ID for the active charging session generated by the charger (OCPP 2.0+) or CPO (OCPP 1.6)	To be able to link a charging schedule to an active charging transaction	EVSE	FSP					No
	Composite Active Charging profile	The resulting charging profile as computed by the charging station considering all received charging profiles and local grid limitations	To get insights into the resulting charging schedule considering all charging hardware and grid constraints	EVSE	FSP					No

	Charged Energy	Amount of energy supplied by the charger used for charging the vehicle over a charging session. These are the total kWh's as counted by the charger for both charging and discharging minus 2x kWh's for discharging	So that only the kWh's used for charging the EV are used for reimbursement purposes	EVSE	User, OEM, FSP					No
	Discharged Energy	Amount of energy discharged by the EV	So that insights can be provided to the user on how much discharging is or has taken place	EVSE	User, OEM, FSP					Yes
EV	Maximum Charging Power	Maximum charging power on AC	Adapt the power delivered by the CS according to the maximum charging power supported by the vehicle	OEM	FSP, EVSE					No
	Minimum Charging Power	Minimum power consumed by the EV	Adapt the power delivered by the CS according to the	OEM	FSP, EVSE					No

			minimum charging power supported by the vehicle							
	Maximum Discharging Power	Maximum discharging power supported by the EV	Adapt the power asked by the grid according to the maximum discharging power supported by the vehicle	OEM	FSP, EVSE					Yes
	Minimum Discharging Power	Minimum discharging power supported by the EV	Adapt the power asked by the grid according to the minimum discharging power supported by the vehicle	OEM	FSP, EVSE					Yes
	Present SoC	The actual state of charge of the EV	Know what the actual state of charge is of the vehicle so that it can also be displayed in a GUI different from the OEM	OEM	FSP, MSP, user					No
	Minimum Energy Request	The amount of energy required to be charged to reach the minimum SoC	Know how much energy needs to be charged as soon as possible. No smart or bidirectional charging can happen as long as this value is more than 0 kWh	EV	FSP					No
	Target Energy Request	The amount of energy required to be charged to reach the target SoC	Know how much energy needs to be charged to achieve the desired range by a given departure time, also accounting for additional energy needs from the EV	EV	FSP					No

			such as for preconditioning needs							
	Maximum Energy Request	The amount of energy required to be charged to reach the maximum SoC	Know how much energy could be put into the EV	EV	FSP					No
	V2X Warranty Constraints	Absolute discharging limitations over time imposed by the OEM	Data required to plan an optimal V2X strategy and energy service prioritization. Exceeding these would result in losing EV warranty and block the usage of V2X by the OEM	OEM	FSP, User					Yes
	V2X State of health	The remaining budget from the V2X warranty constraints	To have information related to the remaining budget from the absolute V2X warranty constraints so that they can be included in the optimization problem (beginning of the session) and to provide feedback to the user at the end of the charging session	OEM	FSP, user					Yes
	Round Trip Efficiency	Round trip efficiency of the onboard inverter	Avoiding injection can result in low charging power whereby the round-trip efficiency of the	OEM	FSP					No

		at different charging and discharging power rates	on-board inverter could be low. This could result in situations where it would be better not to charge on available excess solar energy when a cost objective applies							
	Discharging capable	Indicates whether the vehicle supports bidirectional charging	The EV is technically capable of discharging	OEM	FSP, User					Yes
User	User ID	Unique identifier of the EV driver under roaming (if controlled through CPO-back-end)	Link charging session data to the correct driver	EMSP User	FSP					No
	Departure Time	Departure time applicable for the active charging session	When the EV should be sufficiently charged to ensure that user mobility needs are covered	User	FSP, EVSE					No
	Minimum State of Charge	The minimum state of charge to guarantee an available range	User setting to ensure that a minimum range can be guaranteed to the driver	User	OEM					No

		for emergency leaves								
	Target State of Charge	The state of charge that must be reached at the end of the charging session	User setting to ensure that a certain range can be guaranteed by the end of the charging session	User	OEM					No
	Maximum State of Charge	The state of charge that cannot be exceeded to avoid battery degradation	User setting that allows to limit the total amount of energy that can be charged to avoid battery degradation	User	OEM					No
	Discharging allowed	Indicate whether the driver allows discharging to happen on its EV	Support bidirectional charging through explicit user consent. The default value should therefore reflect an opt-in	User	FSP, EVSE					Yes
	Priority charging	Parameter to indicate whether the driver wants to charge as fast as possible for the active charging session	A user setting that would allow the driver to overrule smart of bidirectional charging at any time and switch to the maximum charging speed directly	User	FSP					No

9.3 Behind the meter services

Behind-the-meter services refer to energy-related products and services that are installed and managed on the customer's side of the utility meter. In other words, these services are located on the consumer's premises, behind the utility meter that measures the amount of electricity consumed. They are typically implemented to help consumers optimize energy usage and reduce costs.

Behind-the-meter services allow customers to take greater control over their energy consumption, reduce costs, and contribute to sustainability efforts. They enable greater flexibility, resilience, and efficiency in the energy system by leveraging localized energy resources and demand response capabilities.

From a DSO perspective, behind-the-meter services help to manage peak demand on distribution networks and to stabilize the grid. By raising price signals, the DSO invites the customers to reduce their energy usage during peak hours to alleviate strain on the grid. They also enable frequency regulation, voltage support or grid balancing based on local energy storage systems.

To deliver effective BTM services, it is crucial to identify and collect the necessary data that drives these offerings. In this section, we will explore the required data for behind-the-meter services, delving into the various types of information that are required in enabling users to make informed decisions about their energy usage, implement energy efficiency measures, and needed by services providers to operate smoothly and efficiently. Understanding the data requirements of BTM services is essential for service providers, energy companies, and consumers alike, as it sets the foundation for unlocking the full potential of decentralized energy management. Within this analysis, we will only consider the flexibility service provider (FSP) which could be the EMS, CPO, or SCSP.

The different services BTM are defined with a short description of their specific data and data quality needs.

9.3.1 Common data

9.3.2 Solar self-consumption

Solar self-consumption optimizes the charging on solar energy and tries to minimize the feed-in of energy of the solar energy.

9.3.2.1 *Data objects unique to the service*

Data category	Data object	Description	Reason	Data Source	Data Consumer	On boarding	Start	During	End	V2X Specific
Site	Location	GPS coordinates of the location	Generate production forecasts based on location related weather information	User, DSO or CS	FSP					No
	Feed-in/injection tariff	Tariff received by the site for injection into the grid	Compute cost savings for the user or when combined with other use cases to optimize the user cost reduction objective	User	FSP					No
User	Minimum Green Level	The minimum percentage of local green energy that the user wants for charging to take place at any point in time.	To provide the user with an option to indicate what the maximum % of local green electricity is that is allowed to go into the EV at any point in time so that local electricity can be complemented with grid electricity to arrive at the minimum charging power of the EV	User	FSP					No

9.3.2.2 *Data quality requirements*

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Feed-in/injection tariff	High	Low	€/kWh	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required
Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required
Maximum Charging Power	Low	Low	kW	High	Required
Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	**kWh?**	Low	Required

Round Trip Efficiency	Low	Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	High	Required
V2X state of Health	High	Once	**kWh**	Low	Required
Grid code coordinates	Low	Once	NA	High	Required
EVSE ID	High	Once	NA	High	Required
Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required

User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	Once	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired
Discharging allowed	High	Once	Boolean	High	Required

9.3.3 Peak Shaving

This service adapts the usage charging/discharging of EVs to be below a maximum power capacity depending on time and capacity configured.

9.3.3.1 Data objects unique to the service

Data category	Data object	Description	Reason	Data Source	Data Consumer	On boarding	Start	During	End	V2X Specific
Site	Contracted power	Yearly contracted capacity for the grid connection (if applicable)	Define the maximum grid capacity of the connection and do not transgress this limit	DSO, User	FSP					No
	Capacity tariff	Tariff of capacity for the site	Compute cost optimalisation	DSO, User	FSP					No
	Capacity Period	Period over which the highest peak power is measured for capacity tariff billing purposes	Compute cost optimalisation per period	DSO	FSP					No
	Highest measured peak consumption	The highest measured peak consumption on a capacity tariff ISP level for the active period	Compute cost optimalisation per period	User	FSP					No

User	Capacity tariff overrule	Possibility to overrule the tariff calculation	Overrule cost algorithm	User	FSP					No

9.3.3.2 Data quality requirements

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Contracted power	Low	Once	kW	High	Required
Contracted power costs	Low	Low	KW/year; kW/month	High	Required
Highest measured peak consumption	Low	Low	kW	High	Required
Capacity periodicity	Low	Low	Days, Months, Years	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required

Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required
Maximum Charging Power	Low	Low	kW	High	Required
Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	kWh	Low	Required
Round Trip Efficiency	Low	Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	Low	Required
V2X state of Health	High	Once	kWh	High	Required

Grid code coordinates	Low	Once	NA	High	Required
EVSE ID	High	Once	NA	High	Required
Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Charging Schedule	High	High	NA	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required
User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	High	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired

Discharging allowed	High	Once	Boolean	High	Required

9.3.4 Static Time to Use Shifting

The charging and discharging are optimized on a static price component which is configured on site level. No changes or only user entered changes are taken into account.

9.3.4.1 Data objects unique to the service

No data unique to the service : all the data needed is described in the common data section.

9.3.4.2 Data quality requirements

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Feed-in/injection tariff	High	Once	€/kWh	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required
Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required

Maximum Charging Power	Low	Low	kW	High	Required
Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	kWh	Low	Required
Round Trip Efficiency		Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	Low	Required
V2X state of Health	High	Once	kWh	High	Required
Grid code coordinates	Low	Once	NA	High	Required

EVSE ID	High	Once	NA	High	Required
Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required
User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	High	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired
Discharging allowed	High	Once	Boolean	High	Required

9.3.5 Dynamic Time to Use Shifting

The charging and discharging are optimized on a dynamic price component. This price component is received from the energy supplier, or the price component is derived from a known market (for example EPEX prices).

9.3.5.1 Data objects unique to the service

No data unique to the service : all the data needed is described in the common data section.

9.3.5.2 Data quality requirements

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Feed-in/injection tariff	High	Once	€/kWh	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required
Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required
Maximum Charging Power	Low	Low	kW	High	Required

Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	kWh	Low	Required
Round Trip Efficiency	Low	Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	Low	Required
V2X state of Health	High	Once	kWh	High	Required
Grid code coordinates	Low	Once	NA	High	Required
EVSE ID	High	Once	NA	High	Required

Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required
User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	High	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired
Discharging allowed	High	Once	Boolean	High	Required

9.4 Front of the meter services

Front of the meter services, also known as utility-scale services, refer to energy-related activities and services provided by utility companies or grid operators on the grid side of the utility meter. Front of the meter services play a crucial role in maintaining grid reliability, managing electricity supply and demand, and ensuring a stable and secure energy system. They focus on the large-scale aspects of energy generation, transmission, and distribution that enable the delivery of electricity to end-users.

From a DSO perspective, behind-the-meter services help to manage peak demand on distribution networks and to stabilize the grid. By raising price signals, the DSO invites the customers to reduce their energy usage during peak hours to alleviate strain on the grid. They also enable frequency regulation, voltage support or grid balancing based on local energy storage systems.

9.4.1 Frequency Containment Reserves (FCR)

This service delivers FCR to the TSO, local measurements with high resolutions are needed in order to fulfill the service requirements.

9.4.1.1 Data objects unique to the service

Data category	Data object	Description	Reason	Data Source	Data Consumer	On boarding	Start	During	End	V2X Specific
Site	Site EAN	Unique identifier of the grid connection point	Required by the TSO for site/asset registration purposes in the context of DSO prequalification	User, DSO	TSO					No
	BSP ID (EAN)	Unique identifier of the Balance Supplier Party	DSO (or the party that manages the central register) can facilitate BSP switching processes	TSO	DSO					No

9.4.1.2 *Data quality requirements*

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Feed-in/injection tariff	High	Once	€/kWh	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required
Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required
Maximum Charging Power	Low	Low	kW	High	Required
Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	kWh	Low	Required

Round Trip Efficiency	Low	Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	Low	Required
V2X state of Health	High	Once	kWh	High	Required
Grid code coordinates	Low	Once	NA	High	Required
EVSE ID	High	Once	NA	High	Required
Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required

User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	High	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired
Discharging allowed	High	Once	Boolean	High	Required
BSP ID	High	Once	NA	High	Required

9.4.2 Automatic Frequency Restoration Reserve

This service delivers AFRR to the TSO, local measurements with high resolutions are needed in order to fulfill the service requirements.

9.4.2.1 Data objects unique to the service

Data category	Data object	Description	Reason	Data Source	Data Consumer	On boarding	Start	During	End	V2X Specific
Site	Site EAN	Unique identifier of the grid connection point	Required by the TSO for site/asset registration purposes in the context of DSO prequalification	User, DSO	TSO					No
	BSP ID (EAN)	Unique identifier of the Balance Supplier Party	DSO (or the party that manages the central register) can facilitate BSP switching processes	DSO	TSO					No
	BRP ID (EAN)	Unique identifier of the Balance Responsible Party	DSO (or the party that manages the central register) can facilitate BSP switching processes	DSO	TSO					No

9.4.2.2 *Data quality requirements*

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Feed-in/injection tariff	High	Once	€/kWh	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required
Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required
Maximum Charging Power	Low	Low	kW	High	Required
Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	kWh	Low	Required

Round Trip Efficiency	Low	Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	Low	Required
V2X state of Health	High	Once	kWh	High	Required
Grid code coordinates	Low	Once	NA	High	Required
EVSE ID	High	Once	NA	High	Required
Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required

User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	High	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired
Discharging allowed	High	Once	Boolean	High	Required
BSP ID	High	Once	NA	High	Required
BRP ID	High	Once	NA	High	Required

9.4.3 Congestion Avoidance

This service asks for reduction/increasing of consumption in a specific period, allowing local DSO to prevent and resolve congestion. A prognosis of the energy consumption per period is needed.

9.4.3.1 *Data objects unique to the service*

Data category	Data object	Description	Reason	Data Source	Data Consumer	On boarding	Start	During	End	V2X Specific
Site	Site EAN	Unique identifier of the grid connection point	Required by the TSO for site/asset registration purposes in the context of DSO prequalification	User, DSO	TSO					No
	BSP ID (EAN)	Unique identifier of the Balance Supplier Party	DSO (or the party that manages the central register) can facilitate BSP switching processes	DSO	TSO					No
	BRP ID (EAN)	Unique identifier of the Balance Responsible Party	DSO (or the party that manages the central register) can facilitate BSP switching processes	DSO	TSO					No

9.4.3.2 *Data quality requirements*

Data object	Timeliness	Sampling rate	Unit	Accuracy	Data Need
Location	Low	Once	Latitude, Longitude	High	Required
Grid Connection capacity	Low	High	kVA	High	Required
Feed-in/injection tariff	High	Once	€/kWh	High	Required
Consumption retail tariff	High	Low	€/kWh	High	Required
Local Frequency	High	High	Hz	High	Required
Active Voltage	High	High	V	High	Required
Active Grid Power	Real-Time	30s	kW	Low	Required
Maximum Charging Power	Low	Low	kW	High	Required
Minimum Charging Power	Low	Low	kW	High	Required
Maximum Discharging Power	Low	Low	kW	High	Required
Minimum Discharging Power	Low	Low	kW	High	Required
V2X Warranty Constraints	Low	Once	kWh	Low	Required

Round Trip Efficiency	Low	Once	%	High	Desired
Present State of Charge	High	High	%	High	Required
Minimum Energy Request	High	Low	kWh	High	Required
Target Energy Request	High	High	kWh	High	Required
Maximum Energy Request	High	Low	kWh	High	Required
Discharging capable	High	Once	Boolean	Low	Required
V2X state of Health	High	Once	kWh	High	Required
Grid code coordinates	Low	Once	NA	High	Required
EVSE ID	High	Once	NA	High	Required
Session ID	High	Once	NA	High	Required
Active power	Real-Time	4s	kW	High	Required
Composite active charging profile	High	High	NA	High	Required
Charged Energy	High	High	kWh	High	Required
Discharged Energy	High	High	kWh	High	Required

User ID	High	Once	NA	High	Required
Departure time	High	High	Timestamp UTC	High	Required
Minimum State of Charge	High	High	%	High	Required
Target State of Charge	High	High	%	High	Required
Maximum State of Charge	High	High	%	High	Required
Minimum Green Level	Low	Once	%	Low	Desired
Discharging allowed	High	Once	Boolean	High	Required
BRP ID	High	Once	NA	High	Required

9.5 Insights & Impact

This analysis shows that ensuring that the correct data is delivered at the right time at the right place by the eco-mobility ecosystem required for delivering and validating smart or bidirectional charging energy services creates several challenges related to the availability of data as well as its required or desired data quality.

While making data available is a pure protocol concern, achieving this exchange with the desired data quality impacts the underlying IoT infrastructure of several actors in the e-mobility eco-system and can therefore be more challenging to achieve. These different aspects are evaluated further in the following paragraphs.

9.5.1 Data availability

9.5.1.1 Site data availability

To optimally deliver the desired charging cost and electricity bill reduction objectives through smart and bidirectional charging, having access to accurate and up-to-date electricity tariff information is a prerequisite for all energy services to be optimally delivered on behalf of the driver. Whereas charging tariffs are already exchanged between the different actors in the e-mobility ecosystem, the underlying electricity tariffs with their different tariff components are not.

If the user interacts directly through a user interface, the flexibility service provider would be able to collect this required information directly from the user, but in a system architecture where this would not be the case, this data will need to be exchanged over possibly different protocols.

This important interoperability gap will therefore need to be tackled in Task 2.3.

For FTM services specifically, additional data tied to the electricity contract is required such as the unique identifier of the site as well as from the BRP and/or BSP. Particularly for aFRR, the BRP ID is not known to the user nor it is publicly accessible information.

As this data is required for registering a site and asset towards the TSO in order to be allowed to participate in Frequency Restoration Services, not having access to this data creates a very critical interoperability gap. Even when all interoperability gaps applicable to the charging lifecycle would be resolved, this interoperability gap would lead the fact that the energy stored in electricity will not be able to be used for restoring the balance in the electricity grid for the TSO.

Lastly, having access to real-time active grid power measurements is key for BTM bidirectional charging services as well as most other energy services. Consequently, this measurement will need to be exchanged to the flexibility service provider and will therefore, depending on the applicable control topology, need to be supported by the impacted protocols.

9.5.1.2 EV data availability

Having access to accurate information on how much kWhs will need to be charged by when is key to ensure that the mobility needs of the driver are not impacted through smart or bidirectional charging. Luckily, ISO 15118-20 already provides for this data, even accounting for potential additional energy expected to be consumed by for example, preconditioning of the EV.

Secondly, ISO 15118-20 provides also for the data linked to the technical charging and discharging power constraints that the EV has so that the FSP can take it into account when computing optimal charging schedules for a particular or combination of different energy services.

Particularly for bidirectional charging, some specific additional data is ideally required. To ensure for example that discharging happens in an energy efficient way, access to round-trip efficiency data would be desired. Also, to avoid that discharging would impact the EV warranty, access to V2X warranty limits and its state of health are required as such could potentially impact the optimal discharging strategy and frequency.

These interoperability gaps will be further investigated and tackled under Task 2.3.

9.5.1.3 Charging Station data availability

The charging station can be considered as the key infrastructure of which its technical capabilities influence to a great extent what can be achieved in terms of charging and discharging power. As local grid constraints could affect the execution of a charging schedule, it is important that the FSP is informed about any deviations that result from such local limits, particularly in the case of a balancing service delivery.

Luckily, the availability of these required data from the charging station is already made possible through OCPP.

9.5.1.4 User data availability

This analysis shows that all data tied to the user required from the FSP are all user preference related. The exchange of mobility needs related preferences such as departure time and SoC limits need to ensure that smart and bidirectional charging can be executed while ensuring that the driver is guaranteed a desired range by a given time or be overruled when his mobility needs would change throughout a charging session.

When the number of mobile apps a user needs to use to satisfy his charging & mobility needs anywhere and anytime, it is important that this data can be exchanged over the different protocols so that no additional user interface would be required for smart or bidirectional charging.

Mapping the different data related to user preferences from this analysis to the different protocols will therefore be executed under Task 2.3.

9.5.2 Data quality requirements

The data requirement analysis of the different energy services has exposed that access to timely and accurate data is of paramount importance. Achieving these requirements often is mostly beyond the scope of the impacted protocols and are rather focused on measures to be taken on the enabling underlying IoT infrastructure. 4 different key recommendations are provided below that would together enable the data quality requirements from the data consumers to be achieved jointly by the e-mobility eco-system.

9.5.2.1 Delta monitoring at the data source (sensor) level

Compared to uncontrolled charging, optimized charging or discharging increases significantly the variety, velocity, and volume of data to be exchanged when the FSP would need to determine themself whether an update to a charging schedule is needed based on changes in the environment (sensor, user actions…).

Ideally, such events should be triggered as close to the data source as possible. This would effectively replace the responsibility from the data consumer to the data source to drastically reduce the amount of data traffic and minimize the data processing and storage costs across the eco-system.

To be able to cater to the needs of the different energy services, an industry consensus with potential differences for BTM and FTM services should be targeted with regards to desirable delta values for the

different time series data. This allows to recommend suitable default limits for the different actors and respective measurements.

9.5.2.2 Adoption of event streaming architectures by the different actors

To make sure that actionable data arrives in time at the right location, legacy IoT architectures which process data in batch and publish it in a scheduled way or on request to a data consumer fall short. Compared to batch processing, event driven architectures publish events that applications and services can consume, using these events to perform actions. Such architectures encompass both event producers, event consumers as well as event channels. These events can be generated from users interacting with a user interface to update their mobility needs or be originated from a change in a sensor measurement like a grid measurement.

From an e-mobility ecosystem perspective, event driven architectures are needed to achieve the data quality requirements from BTM and FTM energy services as they often require a near real-time response to user actions, security threats or sensor events.

9.5.2.3 Harmonize data models & formats across protocols

While the same type of data is often being exchanged across different protocols, they sometimes lack compatibility with regards to syntax, format, …. This requires additional processing steps for the actor to transport the event from one protocol to another, thereby leading to a data latency increase. Therefore, striving for full data harmonization across protocols will lead to a more responsive and thereby resilient electricity grid.

9.5.2.4 Define the FSP role

To get the data at its proper location, its destination needs to be known. When making use of event stream architectures, the required data needs to be published so for example, the respective FSP assigned by the driver (or site) to optimize its charging. Dependent on the control topology, this could be a different actor such as an EMS, CPO... thereby impacting the protocols to be used to get the data to the

As the SCALE system architecture aims to support different control topologies while making switching FSPs as seamless as possible for customers, the FSP role should be separated from the existing roles known to the e-mobility eco-system.

Secondly, other reasons like the uninventable collection of GDPR related data and the possible negative impacts it could have on grid stability also do justify the need to clearly define this role within the context of the e-mobility and electricity ecosystem.

10 TSO & DSO impact from energy services execution

10.1 Introduction

While the concerns on the impact of EV charging on the electricity grid have been mainly focused on uncontrolled EV charging, controlled smart or bidirectional charging could potentially also create unintended negative impacts on the operation of the electricity grid when consumer adoption would be significant. This chapter therefore explores the impact that these energy services could have on key responsibilities of the Transmission and Distribution Grid Operators and defines possible mitigation strategies on how to deal with them in the conclusions.

10.1.1 TSO challenges

TSOs are required to maintain a continuous second-by-second balance between electricity supply from generation and demand from customers so that electricity at 50Hz can be delivered to load centers. To ensure that changes in frequency due to mismatches between supply and demand can be contained and restored, they procure balancing services provided through third parties, being Balance Service Providers (BSPs).

Historically, these balancing services have been predominantly provided by centralized fossil fueled thermal power plants and therefore will need to be substituted by new sources of flexibility such as smart and bidirectional charging.

Next to balancing the electricity system in real-time, they are responsible for ensuring the long-term ability of the supply-side system to meet customer's energy needs at all hours for a certain period. To this respect, they are tasked by government to perform resource adequacy assessments to analyze whether the expected demand can be covered by the available generation capacity. When expected available generation capacity would be insufficient to meet the total demand, proposals are made to the government on how much additional generation capacity would be required and whether additional supporting mechanisms would be required in case that current energy-only markets would not provide sufficient stimulus by itself for the needed investments leading to additional costs for society.

Applying certain energy services through smart or bidirectional charging will impact the shape of system demand profiles pushing potentially demand out of the system peak but could on the other hand also have negative impacts on real-time balancing needs or available flexible power capacity from EV charging sessions therefore inducing costs elsewhere in the system.

This chapter will therefore investigate the positive and negative impacts of applying these energy services on resource adequacy and system balancing.

10.1.2 DSO challenges

DSOs ensure that electricity is delivered to end-users in a secure, reliable, and efficient manner. In the same way as the TSO manages the system frequency, the DSO uses network assets and consumer owned assets to keep the voltage within statutory limits as governed by the European EN 50160 standard that regulates the minimum power quality requirements for medium and low voltage customers. This standard covers requirement related to voltage magnitude, rapid voltage changes, harmonic voltages, supply voltage dips and interruptions of the supply voltage.

The traditional unidirectional model of energy distribution from high-voltage transmission networks to consumption points is being stressed by the integration of renewable energy sources and electrification of other energy end-use vectors such as transport and heating.

As a significant amount of renewable energy sources is connected in the form of rooftop solar and onshore windmills on the distribution grid while the electrification of these other energy end-use vectors is mainly happening at the same distribution grid, the distribution grid operator is at the center of the energy transition.

This increased penetration of renewable energy and the increased electricity demand of uncontrolled EV charging and heat pumps will clearly lead to power quality issues and congestion on the distribution grid over the long run.

As customers become more active in the energy transition by reacting to price signals or participating in demand response services to for example balance the electricity grid, the execution of these energy services could also have unintended negative consequences such as leading to power quality issues or causing congestion and thereby impacting the operation of the distribution grid.

This chapter will therefore investigate what the positive and negative impacts on voltage quality and congestion could be from delivery of such energy services if they would happen at large scale. These insights will serve to formulate mitigation strategies as conclusion of this chapter.

Although the focus of this analysis is on the impact of smart and bidirectional charging, the same insights could also be transposed to the impact of heat pumps or other considerable flexible electrical loads.

10.2 Energy services impact assessment

10.2.1 Solar self-consumption

10.2.1.1 Impact on TSO

Reduction of system imbalances caused by solar generation

The solar self-consumption energy service has the advantage that charging sessions will follow the actual generation profile of the solar production and therefore absorb any excess solar energy generated at customer sites.

When more renewable energy is generated than expected due to more favorable weather conditions than forecasted and the Intraday market is not capable of matching this excess renewable supply with demand, the TSO will have to activate downward Frequency Restoration Reserves (FRR) to maintain the system balance.

The solar self-consumption energy service has the advantage that charging sessions will follow the actual generation profile of the solar production and therefore absorb any excess solar energy generated at customer sites. This will therefore avoid downward FRR capacity to be activated by the TSO and reduce imbalance costs for BRPs.

10.2.1.2 Impact on DSO

Reduced congestion risk

Increasing self-consumption through smart charging in local distribution networks has a double positive effect on avoiding congestion. On the one hand, congestion caused within the local distribution grid from too much local generation will be mitigated by consuming that available excess generation locally. On the other hand, as (some of) the electricity needed to charge the electric vehicle has been covered by renewable energy during the day, the congestion in the evening caused from uncontrolled EV charging will be more limited.

It should be noted that these positive effects will only manifest themselves on sunny days and less so during the winter months when solar generation is limited.

Avoidance of overvoltage and voltage flickering

With penetration of solar generation in the local grid, availability of excess generation that cannot be met with local consumption can lead to voltage increasing. Such effects are more pronounced on sites further away from the transformer and when solar generation is highest. Self-consumption control reduces the risk of over-voltage by avoiding injection.

Secondly, sudden increases or decreases in solar generation due to clouds passing by can also cause the voltage to rise so quickly that this leads to flickering lights.

As charging on excess solar allows to adapt the charging speed instantaneously to the availability of solar energy, the causes leading to sudden voltage fluctuations will be mitigated.

10.2.2 Demand charge reduction

10.2.2.1 Impact on TSO

Decrease in system peak load

For demand charge reduction to provide value for the site owner, peak consumption must at all times be lower than with uncontrolled charging. When demand charges are applied to residential sites, the peak consumption will be limited in coincidence with the system peak, being at evening periods. This impacts the required available generation capacity and transmission grid infrastructure to meet the total system demand, therefore leading to a more cost-efficient electricity grid.

Lower or higher cost FRR capacity from smart or bidirectional charging

Depending on when demand charges apply, the available balancing capacity from DERs offered by BSP's in Frequency Restoration Reserve (FRR) markets could be substantially impacted.

When for example system imbalances are created by too much wind energy in the electricity system, increasing consumption of EV charging would allow to restore the system balance without having to curtail wind mills. When the demand charge would be determined based on the highest measured 15min peak load at a given site for a given time period, BSP's will be reluctant to make use of the total available flexibility to restore the frequency as this would potentially lead to a higher demand charge and therefore higher electricity bills for the customer.

This requires that the potential gains from providing FRR services should outweigh the increased demand charges, leading to more expensive FRR capacity for the TSO. This effect could be mitigated by making

demand charges time dependent so that the price signals from demand charges only apply when congestion is expected.

10.2.2.2 Impact on DSO

Avoiding congestion caused by consumption

Demand charges can be applied to lower consumption at system peak events (ex. Critical Peak Pricing) but are mainly applied to provide a price incentive to limit peak consumption thereby avoiding congestion in the distribution grid. This DSO impact is therefore considered the main target outcome of demand charges.

10.2.3 Static Time-of-Use

10.2.3.1 Impact on TSO

Decrease system peak

When EV charging takes place based on a static time-of-use rate, the load impact from EV charging will shift more away from the classic peak moment in the evening. As the coincidence of EV consumption with household peak consumption decreases, as a result, the system peak will decrease as well.

When a static time-of-use tariff would apply for which the price differences would be big enough to justify the energy losses due to lower round-trip efficiencies at low discharging power, through bidirectional charging the electricity stored in the EV battery could also be used to supply the household with cheaper electricity compared to the peak tariff.

This would further reduce the system peak resulting in a more cost-effective electricity grid.

Increased imbalance at start of off-peak period

Because the off-peak hours within a static time-of-use tariff are fixed over a certain time period and are often the same for every consumer, the charging sessions will therefore all start charging at full power at the same time. If this occurs on a large scale, this sudden increase in consumption will create a large imbalance in the electricity system as thermal generation capacity will not necessarily be able or required to ramp up as quickly. The result will be a frequency dip that will be restored first by FCR power and then with aFRR capacity.

However, the described effect could be mitigated if the ramp-up rate of EV charging in response to such off-peak hours would be limited.

10.2.3.2 Impact on DSO

Shift of congestion peak

Peak moments in the low voltage distribution network traditionally take place in the evening when household activity is the highest. Shifting the charging times to off-peak hours will mitigate the impact of EV consumption in the current evening peak.

With bidirectional charging, significant cost differences between peak and off-peak hours could also be sufficient to save money to offset residual household consumption to further reduce the impact on congestion caused by consumption.

However, in areas where both EV penetration as well as static time-of-use tariff uptake would be high, the issue related to congestion could be shifted to off-peak hours.

Undervoltage and voltage flickering

As already indicated, without proper requirements on maximum ramp-up rates, all charging sessions optimized on a static time-of-use tariff will start charging instantaneous at maximum power at the start of the off-peak period. In such a situation, a significant sudden increase in consumption could lead to voltage drops and potentially even voltage flickering due to the high rate of voltage change.

10.2.4 Dynamic Time-of-Use

10.2.4.1 Impact on TSO

Increased imbalances at start and end-off the cheapest hours

To make optimal use of the cheapest hours, the flexibility service provider is incentivized to charge as much energy as possible during the cheapest hours and avoid charging at other hours. Similar to the effect that a static time-of-use tariff has for the TSO, the delivery of this energy service mainly results in an increase in system imbalance at the start and end of the cheapest price blocks. Because it may not be possible to charge all kWh for a charging session in the same price block, the effect will not only manifest itself at the beginning but as well at end of the cheapest hours. Consequently, the frequency of such events compared to static time-of-use will also be higher.

Depending on the success of dynamic time-of-use tariff structures, the impact could become significant over time. For example, if 50,000 charging sessions started charging simultaneously at 11kW, an almost instantaneous increase and decrease of 550MW would occur within the 1h time period.

Improved resource adequacy through V2G

When a dynamic time-of-use tariff would also apply to the injection of electricity from a load center, the electricity stored within the EV battery could also be used to sell electricity back to the grid at high price moments. This would reduce the residual load within the system that has to be supplied by conventional thermal generating plants, reducing our reliance on fossil fuels, improving our energy independence, and reducing the overall costs of the electricity system.

10.2.4.2 Impact on DSO

Voltage magnitude and voltage flickering

The same effect as described when applying smart charging to a static time-of-use will occur when applying smart charging to dynamic prices. However, the frequency of these effects will be higher because the cheapest price moments are not necessarily consecutive, therefore resulting in both rapid increases and decreases of the voltage. This could potentially lead to voltage magnitude and voltage flickering issues.

As frequency and voltage requirements for operations in steady and transient states for generators and demand connections are governed by grid codes, a solution could be to incorporate voltage quality requirements in these grid codes that could avoid these unintended negative consequences.

10.2.5 FCR

10.2.5.1 Impact on DSO

Reduced congestion risk

As contracted FCR capacity requires that the capacity is available in both directions, participation in such services through smart and/or bidirectional charging will result in charging sessions happening at lower charging speeds as compared to uncontrolled charging. Although this would in theory reduce the congestion risk in the distribution grid, it is assumed that this effect is going to be marginal as the total FCR capacity to be procured by the TSO is too limited to have profound effects.

10.2.6 FRR

10.2.6.1 Impact on DSO

Increase of congestion

In a market situation in which the total imbalance in a TSO area is high and a significant amount of available FRR capacity is covered by EVs or other types of DERs, the activation of that flexibility could also lead to potential congestion within the local distribution grid.

In the future, it is foreseeable that the sum of the available capacity at connection level potentially used for grid balancing services will exceed the available capacity in the local distribution grid.

10.3 Conclusions

Today, a lot of the effort within the research community and regulatory environment is focused on assessing the impact of uncontrolled EV charging and coming up with policy proposals to mitigate the adverse effects of massive EV uptake. As the negative impacts of uncontrolled charging on system adequacy, congestion and power quality are generally accepted within the research & policy area, achieving large scale consumer uptake of smart and bidirectional charging is widely regarded as a key objective to mitigate these impacts.

The analysis performed in this chapter shows that achieving uptake in smart and bidirectional charging will not necessarily avoid all these issues, depending on the energy services that are applied.

Large scale uptake of dynamic time-of-use particularly could lead to several unintended negative side effects on both the distribution and transmission grid.

As this FTM service aims to provide direct electricity bill reductions for the end-consumer, the flexibility service provider is incentivized to charge as much as possible during the cheapest hours and avoid charging outside of these hours. As a result, and in the absence of any other imposed technical restrictions on, for example, maximum ramp rates, the change in charging current will be instantaneously.

On the DSO-side, this could lead to several power quality issues such as under- and overvoltage as well as flickering due to rapid changes in voltage while for the TSO, this could lead to instantaneous imbalances between supply and demand at the beginning and end of the cheapest hours. Preparing Europe for mass-scale roll-out of smart and bidirectional charging also requires that the correct measures are taken so that these potential negative impacts can be contained.

To ensure that generation and demand units contribute to the safe and stable operation of the electricity system and do not cause any additional disturbances, network codes apply to them. Currently, only demand

units connected to the distribution system that provide demand response services to an energy system actor are in scope of the current Network Code for Demand Connections. This means that smart charging through BTM services such as dynamic time-of-use are currently not in scope.

With the current regulatory push towards dynamic time-of-use pricing as well as the on-going assessment by ACER on the scope and applicable technical requirements amendment proposals with regards to the network code for demand connection and network code for generators, some recommendations derived from these insights can be made.

While bidirectional charging will be covered In the Network Code for Generators based on the current draft proposal thereby adhering to the similar technical requirements as PV-inverters, the network code for demand connections currently does not cover the proper requirements to mitigate and contain the power quality impact that large scale uptake of automated control on dynamic time-of-use tariffs could have.

Therefore, requirements related to under- and overvoltage events, underfrequency events or voltage rate of change should be assessed and further evaluated for targeted inclusion. When such events occur with the charging station having to respond, feedback will need to be provided to the flexibility service provider so that they can be informed of the reason why a certain instructed charging schedule cannot be executed. Secondly, when the charging session is actively delivering a TSO balancing service, this event information could also be provided to the DSO as the flexibility service provider cannot be held responsible for non-compliant delivery of that charging session due to power quality or congestion issues in the local distribution grid.

As already covered in D1.5 deliverable on the software and hardware requirements, OCPP 2.1 targets inclusion of the required functionalities for grid code compliance for bidirectional charging. These same functionalities could also be applied to ensure grid code compliance for smart charging if these additional technical requirements would be included in the revised Network Code for Demand Connections, thereby mitigating, and containing the negative impacts of smart and bidirectional charging on power quality.

11 Cybersecurity and data governance

This section focuses on cybersecurity management and data governance. Cybersecurity refers to the measures taken to protect the digital systems, networks, and data associated with electric vehicles and their supporting infrastructure. It involves safeguarding against unauthorized access, data breaches, malicious activities, and cyber threats that could compromise the safety, reliability, and privacy of electromobility systems.
Data governance, on the other hand, refers to the framework and processes that ensure the availability, integrity, and confidentiality of data. In the context of electromobility, it involves the responsible and ethical management of data collected from electric vehicles, charging stations, and other connected devices. Effective data governance ensures that sensitive information is protected, regulatory requirements are met, and data is utilized in a manner that benefits users, operators, and society.

Cyber-attacks on charging stations, smart grids, or communication networks could disrupt the charging infrastructure, causing inconvenience and potential grid instabilities. A compromised charging network might result in denial of service, financial losses for operators, and inconvenience for EV owners.

The cybersecurity analysis and data governance in this document should stay at a high level primarily because the system architecture is not yet finalized. Since cybersecurity and data governance strategies are intricately tied to the system architecture, we choose a high-level approach which allows for a broader understanding of the potential risks and requirements while avoiding overly specific recommendations that may become outdated as the architecture evolves. By focusing on high-level considerations, the different roles can still identify key security and governance principles that should be incorporated into the future system. These principles may include concepts such as defense-in-depth, data privacy by design, access controls, secure communication protocols, and robust incident response procedures.

11.1 Data governance

Data governance refers to the overall management, protection, and oversight of an organization's data assets. It encompasses the processes, policies, and frameworks that ensure data quality, integrity, privacy, and security throughout its lifecycle. Data collected by all the actors holds immense potential for insights, decision-making, and innovation. However, without proper governance, data can become a liability, leading to issues such as data breaches, inaccuracies, inconsistent interpretations, and regulatory non-compliance. Data governance encompasses different processes to manage data quality, data classification, access controls, data lifecycle, and privacy and security measures.

Data governance also plays a vital role in data privacy and security. With the increasing focus on data protection and privacy regulations, organizations must establish controls and mechanisms to safeguard sensitive data, prevent unauthorized access, and comply with relevant laws and regulations, such as the General Data Protection Regulation (GDPR).

Based on the data listed in this document, we will extract the data that can be labeled as personal data. For each of them, the actors that need to store or only to process them will be highlighted so they can apply the appropriate rules according to GDPR. This document will not define requirements on data privacy.

11.1.1 Methodology

In order to address privacy concerns and ensure the security of personal data, it is essential to follow a systematic approach.

Firstly, it is crucial to identify the personal data involved in each context or scenario. This includes understanding the specific types of information that are considered personal data, such as names, addresses, contact details, financial information, or any other data that can directly or indirectly identify an individual.
Secondly, it is important to establish the links between the actors involved in processing or handling the personal data. This includes identifying the data controllers, data processors, and any third parties with whom the data is shared. Once the actors are identified, it is necessary to list the data exchanged between them. This involves documenting the elements of personal data that are transferred from one actor to another. Lastly, it is essential to document the data stored by each actor. This includes identifying the personal data that is retained by each party, along with the purposes for which the data is stored and the duration of retention. By following this systematic approach, organizations can gain a clear understanding of the personal data lifecycle, enabling them to implement appropriate safeguards and ensure compliance with privacy regulations.

11.1.2 Personal Data

For each data identified as a personal data, we associate a threat defined in LINDDUN [1] framework. Seven categories are defined:

- Linking: Associating data items or user actions to learn more about an individual or a group.
- Identifying: Learning the identity of an individual.
- Non repudiation: Being able to attribute a claim, i.e., to know, having done, having said something, to an individual.
- Detecting: Deducing the involvement of an individual by observing.
- Data disclosure: Excessively collecting, storing, processing, or sharing personal data.
- Unawareness and Unintervenability: Insufficiently informing, involving, or empowering individuals in the processing of personal data.
- Noncompliance: The system deviates from security and data management best practices, standards, and legislation

The following data is considered as personal data:

Data object	Threat	Reason
User ID	Identifying	Identify directly the EV Driver.
Departure Time	Linking Data disclosure	Track the EV Driver trips. Combined the EVSE location it can be used to identify the user.
Active Voltage	Linking	Can deduce the activity on site: is the user present, number of devices connected, ...

[1] See https://linddun.org/

Active Grid Power	Linking	Can deduce the activity on site: is the user present, number of devices connected, ...
Location	Linking, Identifying	Identify users going to a specific location by linking with other data.
BRP ID	Noncompliance	Identify the BRP responsible of a site which can be a confidential information.
BSP ID	Noncompliance	Identify the BSP responsible of a site which can be a confidential information.
Contracted power costs	Noncompliance	Costs are a contractual data and shall be confidential.
Priority Charging	Identifying Data Disclosure	Users with priority charging are a subset of users. Having this information helps identifying a user when it is linked to other information.

11.1.3 Impact on architecture

When two roles need to exchange personal data, they shall use a secured link that guarantees confidentiality, integrity, and authenticity. The data analysis listed for each data the source and the consumer. As these data are exchanged between the roles, it means that the end-to-end communication between the source and the consumer shall be secured. If one link of the chain is unsecure, the exchanged data can be accessed. These data are also stored by some roles. At least the following data shall be encrypted according to data regulations:

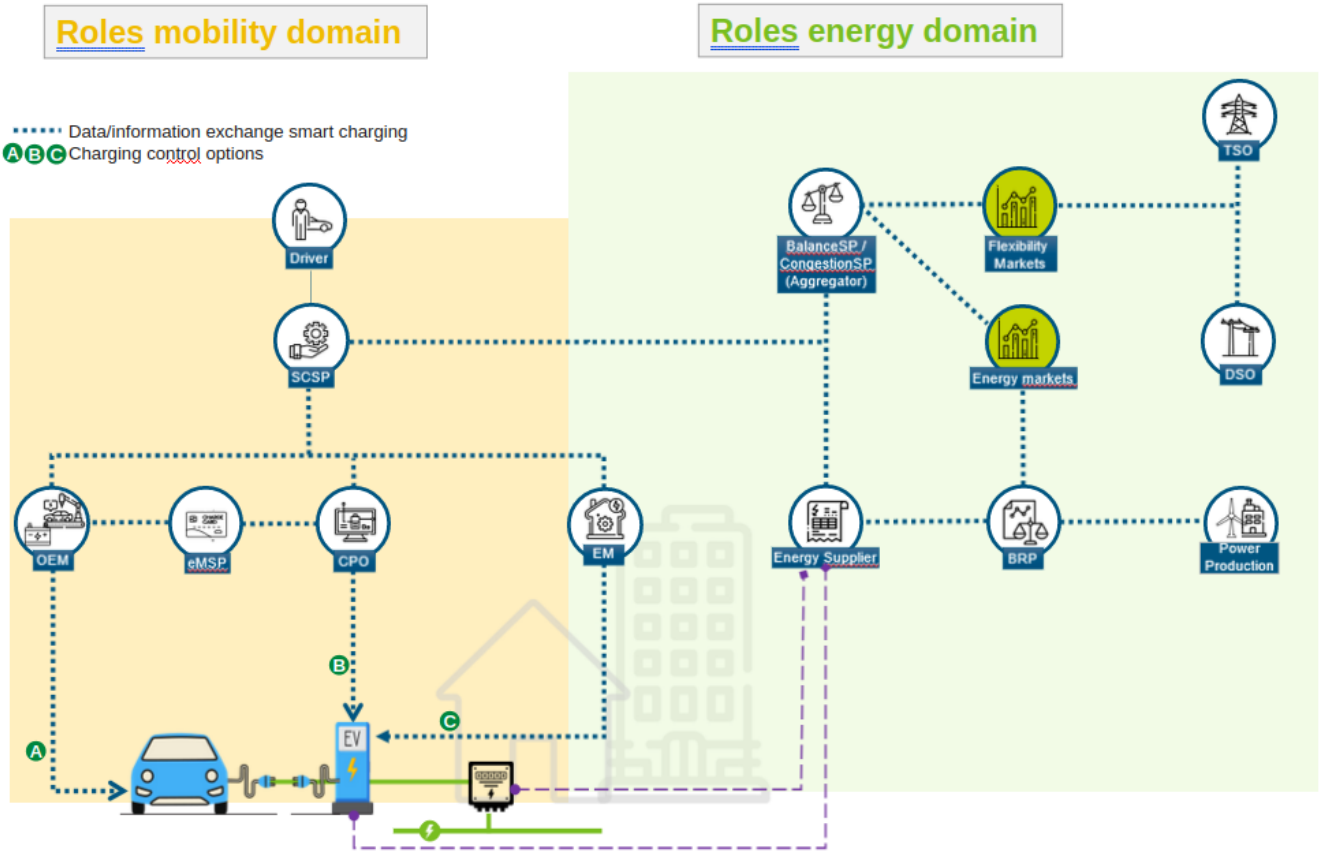
Data object	Source	Consumer
User ID	Driver	OEM eMSP
Departure Time	User	FSP
Active Voltage	Meter	FSP
Active Grid Power	Meter	FSP
Location	User EVSE DSO	FSP
BRP ID	DSO	DSO

BSP ID	TSO	TSO
Contracted power costs	DSO	FSP
Priority Charging	User	FSP

11.2 Threat identification and associated mitigation strategies

To perform a threat detection strategy, the scope and boundaries of the system under analysis shall be clearly established. The system shall be identified (software application, physical device, …) and its interfaces listed. The external dependencies shall also be considered as they are a source of potential threats. Such an analysis can be performed on each role defined in the project architecture. In this document, we will make a general threat detection analysis as the project architecture is not finalized and has specific elements for each use case.

For this analysis, the following general architecture has been considered.



11.2.1 Attackers profile

Cybersecurity attacks can be perpetrated by various types of attackers, each with their own motivations, skill levels, and resources. While it is challenging to provide an exhaustive list, here are some generic attacker profiles commonly encountered in cybersecurity:

- **Cybercriminals**: Attackers are mainly motivated by financial gain. They engage in various activities such as identity theft, credit card fraud, ransomware attacks, or creating and selling hacking tools and stolen data on underground markets. They may operate individually or as part of organized crime syndicates. This is the most common attacker profile. Their resources are limited and their skills are variable.
- **State affiliated groups**: Attackers are supported or sponsored by nation-states to conduct cyber espionage, sabotage, or disruption. State-sponsored actors typically possess advanced technical skills, extensive resources, and sophisticated tools. Their targets can range from government agencies and critical infrastructure to corporations and research institutions. They have important resources and skills to perform various types of attacks.
- **Hacktivists**: Hacktivists are politically or socially motivated attackers who target organizations or individuals to promote their ideological or social causes. They may deface websites, leak sensitive information, or disrupt services to raise awareness or protest specific issues. They have important resources and skills to perform various types of attacks.
- **Insiders**: Insiders are individuals who have authorized access to an organization's systems, networks, or sensitive information. They may be disgruntled employees, contractors, or partners who abuse their privileges for personal gain, revenge, or to sell confidential data to external parties. The resources are limited but their inside knowledge enhances the risk.
- **Script Kiddies**: These are individuals with limited technical skills who use pre-existing tools and scripts to launch basic attacks. Script kiddies often target low-hanging fruit, such as poorly secured systems, with the intention of causing disruption or gaining recognition among their peers. Many global incidents were initiated by script kiddies who acted alone and without specific intent. Their resources and skills are limited.

It is important to understand that these profiles are not mutually exclusive, the attackers can have multiple roles or work with others to achieve their objectives.

11.2.1.1 Attackers' motivation

By mapping these profiles and motivation, we realize that the systems deployed in SCALE are exposed to all the profiles listed above for different motivations:

- **Cybercriminals:** Financial gain**.** They might attempt to exploit vulnerabilities in the charging infrastructure to gain unauthorized access, compromise user data, or engage in ransomware attacks. They may also steal charging data or payment information for fraudulent purposes.
- **State affiliated groups:** Intelligence and political motivation. It could be for intelligence gathering purposes, to monitor energy consumption patterns, or to gain control over critical infrastructure for potential future disruptions or sabotage.
- **Hacktivists**: cause confusion, influence public opinion or create polarization. By disrupting charging operations or gaining unauthorized access to charging systems, they may aim to highlight vulnerabilities in the infrastructure or advocate for alternative energy solutions.
- **Insiders**: Personal gain or revenge. This could involve manipulating charging data, tampering with energy flow, or intentionally disrupting charging operations. Insiders may have financial or personal motives, or they may be coerced or bribed by external parties.

- **Script Kiddies:** Recognition among their peers. They may exploit vulnerabilities in the charging station's software or network to disrupt charging operations, manipulate charging parameters, or cause malfunctions.

Understanding these motivations helps to anticipate potential threats and implement appropriate security measures to the overall charging infrastructure.

11.2.2 System Threats

With the increasing reliance on digital systems and networks, organizations and individuals face numerous cybersecurity threats that can expose sensitive information, disrupt operations, and lead to significant financial and reputational damages. Cybersecurity threats refer to weaknesses or flaws in computer systems, software, networks, and applications that can be exploited by malicious actors. These threats can range from simple coding errors to complex design flaws, and they create opportunities for cybercriminals to gain unauthorized access, manipulate data, or launch destructive attacks.

We can use the STRIDE[2] model to categorize the threats. The electromobility ecosystem is exposed to the following threats:

- **Elevation of privilege**: Use remote access protocols to gain unauthorized access. For example, attackers may attempt to brute-force login credentials, use social engineering to trick employees into revealing passwords, or exploit known vulnerabilities in remote access software. The possible attackers' profiles are: insiders, state affiliated groups.
- **Information disclosure**: Unauthorized access, exposure, or leakage of sensitive or confidential information. Attackers may exploit vulnerabilities to gain access to protected data, such as personal or financial information, trade secrets, or classified documents. The possible attackers' profiles are: insiders, state affiliated groups, hacktivists, and cybercriminals.
- **Denial of service**: Disrupt or degrade the availability of services, systems, or networks. Attackers overwhelm target resources, such as bandwidth, processing power, or memory, making them inaccessible to legitimate users or causing severe performance degradation. The possible attackers' profiles are: script kiddies, state affiliated groups, hacktivists.
- **Spoofing**: Impersonate a legitimate entity to gain unauthorized access or deceive users. It can include activities like IP or email spoofing, where the attacker presents false information to bypass security measures or gain user trust. The possible attackers' profiles are: insiders, state affiliated groups, hacktivists, and script kiddies.
- **Tampering**: Unauthorized modification or alteration of data or systems. Attackers may manipulate data in transit, modify software or hardware components, or tamper with system configurations to compromise integrity, confidentiality, or availability. The possible attackers' profiles are: insiders, state affiliated groups, hacktivists, and script kiddies.
- **Repudiation**: Ability of an attacker to deny their actions or transactions. It includes scenarios where an attacker can alter or remove evidence of their activities, making it difficult to attribute malicious actions to a specific entity. The possible attackers' profiles are: insiders, hacktivists, and script kiddies.

[2] See https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

11.2.3 Possible threats consequences

Within SCALE project, the impact of an attack depends on the pilot's size. On the one hand, large systems often have more resources available to invest in cybersecurity measures so they can build stronger defenses. In the meantime, larger systems are more complex with numerous interconnected components and users. This complexity introduces more vulnerabilities and potential weaknesses. Finally, when a large system is successfully breached the potential impact can be significant. The repercussions of a security breach in a large system can be felt on a larger scale, affecting more individuals, and organizations.

On the other hand, small systems have fewer resources available for cybersecurity. While these systems may have weaker security measures and be more susceptible to attacks, the potential impact of a successful breach is often limited due to the scale and scope of the system. For example, an attack on pilot B4 in Gothenburg impacts few users and charging stations.

Therefore, it is essential to recognize that smaller systems are not immune to cyber threats, and the impact of a breach can still be significant, depending on the nature of the system and the specific circumstances. Regardless of the system's size, implementing appropriate security measures, conducting regular risk assessments, and fostering a security-conscious culture are crucial for mitigating cyber risks and protecting sensitive information.

11.2.4 Threats consequences assessment

Assessing the consequences of cybersecurity threats is a crucial aspect of understanding the potential impact of a security incident. Here are some key steps and considerations in assessing the consequences.

First identify the assets that are at risk from the cybersecurity vulnerability. This can include sensitive data, critical systems, intellectual property, infrastructure, financial resources, reputation, and customer trust. Categorize these assets based on their importance and potential impact if compromised. Then evaluate the potential threats to understand the potential threats that could exploit the vulnerability. Consider different threat actors, their motivations, capabilities, and the likelihood of an attack. This includes assessing the nature of the vulnerability, its exposure to the external environment, and the level of difficulty for an attacker to exploit it. For each listed potential threat, develop scenarios that outline the potential consequences of a successful attack. Consider both direct and indirect impacts. Direct impacts may include data breaches, service disruptions, financial losses, or physical damage. Indirect impacts could involve reputational damage, legal and regulatory consequences, loss of customer trust, or operational disruptions.

In an ecosystem, the systems are interconnected so cascading effects shall be considered. The compromise of one asset or system could impact others in the network or infrastructure.

Finally, legal and regulatory implication shall be considered. Understand the legal and regulatory implications of a cybersecurity vulnerability and evaluate the potential consequences of non-compliance with applicable laws and regulations. Consider factors such as data protection regulations, industry-specific compliance requirements, and the potential for legal actions and penalties.

By conducting a comprehensive assessment of the consequences of cybersecurity vulnerabilities, organizations can make informed decisions about risk mitigation strategies, prioritize resources effectively, and develop robust incident response plans. This proactive approach helps to minimize the potential impact of security incidents and enhance the overall cybersecurity posture.

11.2.5 Mitigation strategies

Mitigation strategies play a crucial role in safeguarding against cybersecurity threats and vulnerabilities. Organizations and individuals must implement proactive measures to mitigate potential risks and minimize the impact of security incidents. Mitigation strategies involve a range of preventive, detective, and responsive actions aimed at reducing vulnerabilities, enhancing resilience, and protecting critical assets. By understanding and implementing effective mitigation strategies, actors can minimize the potential consequences of cybersecurity incidents.

- **Access Control:** Implement access control mechanisms, such as multi-factor authentication, password policies, and user permissions, to prevent unauthorized access to critical systems and data.
- **Encryption**: Encrypt sensitive data, both in streams with other systems and on storage, to protect against data theft or unauthorized access.
- **Firewalls**: Deploy firewalls and other network security devices to prevent unauthorized access to networks and systems. These devices can detect and block malicious traffic and protect against known vulnerabilities.
- **Intrusion Detection and Prevention:** Implement intrusion detection and prevention systems (IDS/IPS) to detect and block unauthorized access attempts or malware infections.
- **Security Auditing and Testing:** Regular security auditing and testing to identify vulnerabilities and potential security gaps. Penetration testing, vulnerability scanning, and security audits can help discover weaknesses before attackers can exploit them.
- **Backup and Recovery:** Maintain regular backups of critical systems and data to mitigate the damage caused by a cyber-attack. Regular testing of backup and recovery procedures is also essential to ensure that backups are reliable and can be restored quickly.
- **Employee Training and Awareness:** Educate employees about cybersecurity best practices, such as avoiding phishing scams and using strong passwords, to prevent attacks caused by human error. This could include conducting regular cybersecurity training sessions and awareness campaigns.

This report lists possible mitigation strategies that can be implemented. Not all the actors can implement all the strategies but they shall consider all of them and implement as much as they can to enhance global security.

11.3 Threats possible consequences

We saw in the previous sections that cyber threats in electromobility encompass a range of malicious activities, including unauthorized access, data breaches, system manipulations, and more. Understanding and addressing these potential consequences is crucial to ensuring the secure and reliable operation of the electromobility ecosystem. In this section, we will explore some of the possible concrete consequences of cyber threats in electromobility and the possible proactive measures to mitigate these risks.

11.3.1 Disruption of charging infrastructure

Attackers may target the charging infrastructure, such as the control systems to disrupt or disable the charging process. To disrupt the infrastructure, attackers can directly target charging stations to make them unavailable for drivers or disconnect from their CPO so the charge cannot be controlled or authorized. They can also target CPOs to impact several charging stations at the same time. Finally, eMSP can also be attacked to block the charging sessions authorization.

This can result in the inability to charge EVs, inconveniencing EV drivers and potentially impacting their daily operations or travel plans. CS and CPO are always impacted as they must find the source of the problem and recover. DSO and BRP might be concerned if the number of unavailable CS is too high so it has an impact on grid stability.

Main target roles	**CS, CPO, eMSP**
Impacted roles	Drivers, CS, CPO, BRP, eMSP, DSO
Types of attack	Elevation of privilege, Denial of service, Spoofing, Tampering
Mitigation Strategies	Access control, Intrusion Detection and Prevention, Firewalls, Backup and Recovery

11.3.2 Privacy breaches

A cyber-attack can compromise sensitive data such as personal information, or payment details, handled by the different roles. This leads to privacy breaches. All the roles are impacted and can be targeted by this issue. This may lead to financial loss for the driver and breaks its confidence into the system. The data can be used to track a driver by using location data and deduce travel patterns. To mitigate the consequences, the collaboration between industry stakeholders, government bodies, and cybersecurity experts is crucial to establish comprehensive frameworks for safeguarding personal information.

Main target roles	**Driver, CS, CPO, eMSP, DSO, TSO, BRP, SCSP**
Impacted roles	Driver, CS, CPO, eMSP, DSO, TSO, BRP, SCSP
Types of attack	Information disclosure, Elevation of privilege, Spoofing

Mitigation Strategies	Access control, Employee Training and Awareness, Encryption

11.3.3 Financial loses

The downtime caused by the attack can result in revenue losses as charging services are disrupted. Additionally, the costs associated with investigating and remediating the attack, restoring system functionality, and implementing improved security measures can add up significantly. All the roles of the ecosystem are concerned by this attack.

Main target roles	**Driver, CS, CPO, BRP, TSO, DSO, eMSP, SCSP**
Impacted roles	Driver, CS, CPO, BRP, TSO, DSO, eMSP, SCSP
Types of attack	Denial of service, Elevation of privilege, Information disclosure, Spoofing, Tampering
Mitigation Strategies	Backup and recovery, Security Audit and Testing, Access control

11.3.4 Compromise vehicle control

As EV are directly connected to charging stations, attackers can exploit vulnerabilities to compromise connected vehicles by gaining unauthorized access to the charging station's systems. This can enable them to manipulate vehicle functions, steal sensitive data from the vehicle's systems, or potentially even take control of the vehicle remotely.

Main target roles	**Driver, OEM, CS**
Impacted roles	Drivers, CS, CPO, BRP, eMSP
Types of attack	Elevation of privilege, denial of service, Spoofing, Tampering
Mitigation Strategies	Backup and recovery, Security Audit and Testing, Access control

11.3.5 Impact public perception

Attackers can erode public trust in the services and their security. Concerns about safety, privacy, and reliability may slow down the adoption of EVs, related infrastructure and services.

Main target roles	**Driver, OEM, CS, CPO, BRP, eMSP, SCSP, EMS**

Impacted roles	OEM, CS, CPO, BRP, eMSP, SCSP
Types of attack	Denial of service, Elevation of privilege, Information disclosure, Spoofing, Tampering, Repudiation
Mitigation Strategies	Security Audit, Access control, Intrusion detection

11.3.6 Grid instability

Attacks can target the electromobility infrastructure to disturb the grid. By gaining control on numerous charging stations, an attacker can overload or imbalance the grid by stopping the ongoing charging sessions, or increase the power delivered by the charging stations. They can also manipulate the power flow to cause voltage fluctuations and impact other devices connected to the grid.

Main target roles	**CPO, BRP, CS, SCSP**
Impacted roles	TSO, DSO, Driver
Types of attack	Denial of service, Elevation of privilege, Spoofing, Tampering
Mitigation Strategies	Security Audit and Testing, Access control, Firewalls

11.3.7 Safety risks

An attack on a charging station can pose safety risks. For instance, attackers may tamper with the charging infrastructure, leading to malfunctioning or overheating of charging equipment. This can potentially cause physical damage, electrical hazards, or even fires, endangering the safety of users, vehicles, and the surrounding environment.

An attack on an EV may compromise control over essential vehicle systems can result in accidents or safety hazards. For example, an attacker manipulating the braking system could cause sudden stops or failure to apply brakes when necessary, leading to collisions or loss of control. Such incidents can result in injuries or fatalities to the occupants of the vehicle or others in its vicinity.

Main target roles	**OEM, CS**
Impacted roles	Driver
Types of attack	Tampering, Spoofing, Elevation of privilege
Mitigation Strategies	Security Audit and Testing, Access control, Firewalls

11.4 Cybersecurity Requirements

This chapter lists all the general cybersecurity requirements that have been identified following the analysis that has been carried.

11.4.1 General requirements

ID	FR.01
Title	Link encryption
Description	Implement end-to-end encryption to protect the confidentiality of data exchanged between system A and system B.

ID	FR.02
Title	Data integrity
Description	Implement mechanisms to validate the integrity of data exchanged between two systems, such as digital signatures or checksums.

ID	FR.03
Title	Entity Authentication
Description	An authentication mechanism must be deployed to ensure that the entity contacted for a specific role is correct.

ID	FR.04
Title	Access Control
Description	Enforce strict access controls to limit access to sensitive information only to authorized personnel or systems

ID	FR.05
Title	Secure Development Practices
Description	Adhere to secure development practices, such as secure coding guidelines and code reviews, to minimize the introduction of security vulnerabilities during system development and maintenance.

ID	FR.06
Title	Patch Management
Description	Regularly apply security patches and updates system to address known vulnerabilities and protect against emerging threats

11.4.2 Data links requirements

ID	FR.DL.01
Title	Encrypt the link between the OEM and the Driver
Roles involved	OEM, Driver
Description	The link between the OEM and the Driver shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.02
Title	Encrypt the link between the OEM and the eMSP
Roles involved	OEM, eMSP
Description	The link between the OEM and the eMSP shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.03
Title	Encrypt the link between the OEM and the CS
Roles involved	OEM, CS
Description	The link between the CS and the Driver shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.04
Title	Encrypt the link between the CPO and the CS
Roles involved	CPO, CS
Description	The link between the CPO and the Driver shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.05
Title	Encrypt the link between the SCSP and the CPO
Roles involved	CPO, SCSP
Description	The link between the CPO and the SCSP shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.06
Title	Secure link between eMSP and Driver
Roles involved	Driver, eMSP
Description	The link between the eMSP and the Driver shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.07
Title	Secure link between BSP and SCSP
Roles involved	BSP, SCSP
Description	The link between the BSP and the SCSP shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.08
Title	Secure link between Driver and SCSP
Roles involved	BSP, SCSP
Description	The link between the Driver and the SCSP shall be secured as described in FR.01.
Connected to other requirements	FR.01

ID	FR.DL.09
Title	Validate the integrity of data exchanged between the OEM and the Driver
Roles involved	OEM, Driver
Description	The link between the OEM and the Driver shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.10
Title	Validate the integrity of data exchanged between the OEM and the eMSP
Roles involved	OEM, eMSP
Description	The link between the OEM and the eMSP shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.11
Title	Validate the integrity of data exchanged between the OEM and the CS
Roles involved	OEM, CS
Description	The link between the CS and the Driver shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.12
Title	Validate the integrity of data exchanged between the CPO and the CS
Roles involved	CPO, CS
Description	The link between the CPO and the Driver shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.13
Title	Validate the integrity of data exchanged between the SCSP and the CPO
Roles involved	CPO, SCSP
Description	The link between the CPO and the SCSP shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.14
Title	Validate the integrity of data exchanged between eMSP and Driver
Roles involved	Driver, eMSP
Description	The link between the eMSP and the Driver shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.15
Title	Validate the integrity of data exchanged between BSP and SCSP
Roles involved	BSP, SCSP
Description	The link between the BSP and the SCSP shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

ID	FR.DL.16
Title	Validate the integrity of data exchanged between Driver and SCSP
Roles involved	Driver, SCSP
Description	The link between the Driver and the SCSP shall guarantee the integrity of the data as described in FR.02.
Connected to other requirements	FR.02

11.4.3 Common requirement for roles

ID	FR.CR.01
Title	Control access to the systems handled by a role
Roles involved	OEM, CS, CPO, Driver, SCSP, BRP, eMSP, Driver
Description	The access to sensitive information shall be restricted authorized personnel or systems as described in FR.04.
Connected to other requirements	FR.04

ID	FR.CR.02
Title	Application of Secure Development Practices
Roles involved	OEM, CS, CPO, Driver, SCSP, BRP, eMSP, Driver
Description	The roles shall apply secure development practices as described in FR.05.
Connected to other requirements	FR.05

ID	FR.CR.03
Title	Implementation of patch management
Roles involved	OEM, CS, CPO, Driver, SCSP, BRP, eMSP, Driver
Description	The roles shall be able to apply security patches and updated as described in FR.06.
Connected to other requirements	FR.06

ID	FR.CR.04
Title	Implementation of personal data storage GDPR requirements
Roles involved	OEM, CS, CPO, Driver, SCSP, BRP, eMSP, Driver
Description	The roles shall apply the requirements related to personal data storage defined in GDPR.
Connected to other requirements	NA

ID	FR.CR.05
Title	Implementation of personal data processing GDPR requirements
Roles involved	OEM, CS, CPO, Driver, SCSP, BRP, eMSP, Driver
Description	The roles shall apply the requirements related to personal data processing defined in GDPR.
Connected to other requirements	NA

ID	FR.CR.06
Title	Implementation of an authentication mechanism
Roles involved	OEM, CS, CPO, Driver, SCSP, BRP, eMSP, Driver
Description	The roles shall implement an authentication mechanism that allows a connected entity to check the role identity as described in FR.03.
Connected to other requirements	FR.03

11.5 Conclusion

It is crucial for charging station manufacturers, operators, and stakeholders to prioritize cybersecurity. This includes implementing robust security measures such as secure authentication, encryption, intrusion detection systems, and regular security updates. Conducting rigorous penetration testing and vulnerability assessments can help identify and remediate potential weaknesses. Collaboration between industry stakeholders, cybersecurity experts, and government entities is essential to establish industry-wide standards and best practices for securing charging station infrastructure. By recognizing and addressing cybersecurity vulnerabilities in charging stations, we can ensure the integrity, reliability, and safety of electric vehicle charging infrastructure, promoting the widespread adoption of electric vehicles while safeguarding against potential cyber threats.

12 Conclusions

In conclusion, this document has successfully outlined the crucial data requirements for enabling V2X services, setting forth quality and availability expectations, and addressing the impact of these services on grid operators. Furthermore, it has provided a comprehensive analysis of the cybersecurity measures necessary to ensure the secure and reliable integration of V2X technologies.

As we move towards a future of intelligent mobility, it becomes evident that collaboration among all stakeholders is paramount. The successful implementation of V2X services hinges on the collective efforts of Original Equipment Manufacturers (OEMs), charging station manufacturers, Charging Point Operators (CPOs), grid operators, and standardization bodies. Collaboration among these actors is essential to facilitate the seamless exchange of data and enable the efficient functioning of V2X services.

Moreover, standardization processes play a pivotal role in shaping the future of V2X services. Establishing uniform guidelines, protocols, and data formats ensures interoperability among diverse V2X systems and promotes a harmonized approach within the e-mobility ecosystem. By adhering to agreed-upon standards, e-mobility actors can unlock the full potential of V2X services, enhancing user experience and maximizing the benefits for all stakeholders.

For grid operators, embracing V2X services presents both opportunities and challenges. As V2X-enabled vehicles become prevalent, Distribution System Operators (DSOs) and Transmission System Operators (TSOs) must proactively adapt their infrastructure and operations. By embracing the bidirectional flow of energy and optimizing grid management in response to V2X services, grid operators can achieve enhanced grid stability, energy efficiency, and load balancing.

The findings of this report will furthermore serve as input for future SCALE topics such as existing protocols analysis, system developments to prepare the project pilots, business case development, and standardization of smart charging and V2X.

In conclusion, the successful implementation of V2X services requires collective action, open data exchange, and standardized practices. It is essential for all stakeholders to collaborate and work in tandem to drive the adoption of V2X technologies and unlock the myriad benefits they offer. By embracing V2X services and proactively preparing their infrastructure, grid operators can pave the way for a greener, more sustainable, and interconnected future of e-mobility and smart grid management.