ENCS

EV-111-2022

Security threat analysis for EV charging infrastructure

Version 2022v0.2

30 December 2022

This document was produced in the ENCS program on Security Architectures. This program supports ENCS members in selecting and implementing technical security measures for systems and their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

This document is shared under the Traffic Light Protocol classification:

TLP White – public

The European Network for Cyber Security (ENCS) is a non-profit membership organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure.

Version History

Date	Version	Description
18 July 2022	2022v0.1	First version of the threat analysis for EV charging infrastructure, including context analysis to build profiles.
30 December 2022	2022v0.2	Version to include objectives according to ISO27002:2022 controls

Table of Contents

1 Introduction

This document provides a threat analysis for electrical vehicle charging infrastructure. It analyzes information assets, access control policies and threats to derive security objectives for the infrastructure and its operational environment.

Cyber-attacks on the electric vehicle charging infrastructure are not just a financial and reputational risk to the Charge Point Operators (CPOs) that manage the infrastructure. They are also becoming a large societal risk.

Electric vehicle charging is quickly becoming an essential service to our society. As we are transitioning to electric vehicles, more and more people will rely on charging for their mobility. If the charging infrastructure is not working, people cannot use their cars. So, cyber-attacks on the infrastructure can lead to major societal damage.

Moreover, the EV charging infrastructure could be used to attack the power grid. Large CPOs remotely control hundreds of thousands of charging stations throughout Europe. If attackers gain control of a CPO's infrastructure, they could switch the power of the connected charging stations on and off. The switching could also cause grid imbalances in the supply and demand for electricity. If these imbalances are large enough, they could lead to severe power outages.

Making sure the EV charging infrastructure is secure is, hence, critical. This document analyzes the threats to these systems and defines security objectives to counter these threats. Objectives are defined for both the EV charging infrastructure itself and for the environment in which it operates.

1.1 Relation to other documents

This document is part of a larger series on EV charging infrastructure security as shown in Figure 1.

From the security objectives in this document, security requirements for EV charging infrastructure are defined in [1] based on the IEC 62443-3-3 standard in [3]. CPOs can use these requirements when they procure an EV charging infrastructure from a system integrator, or when they implement the system through an internal department.

This threat analysis allows CPOs to check if the security requirements in [1] apply to their situation. Operators can compare the assets, access control policy, and threats against their own situation. The objectives are organized according to the controls in ISO/IEC 27002:2022 [4], so that CPOs can compare them to the controls that they have selected in an ISO/IEC 27001 based information security management system. If the objectives do not mitigate all their risks, operators can add additional objectives to mitigate their specific risks

Additionally, the objectives to the operational environment give guidance to CPOs on how to securely use an EV charging infrastructure that meets the security requirements. Some threats can only be mitigated in the operational environment. Even when the EV charging infrastructure implements all required measures, it can only be secure if its environment is protected. This document describes the organizational, physical, and telecom measures that CPOs should take for this purpose.

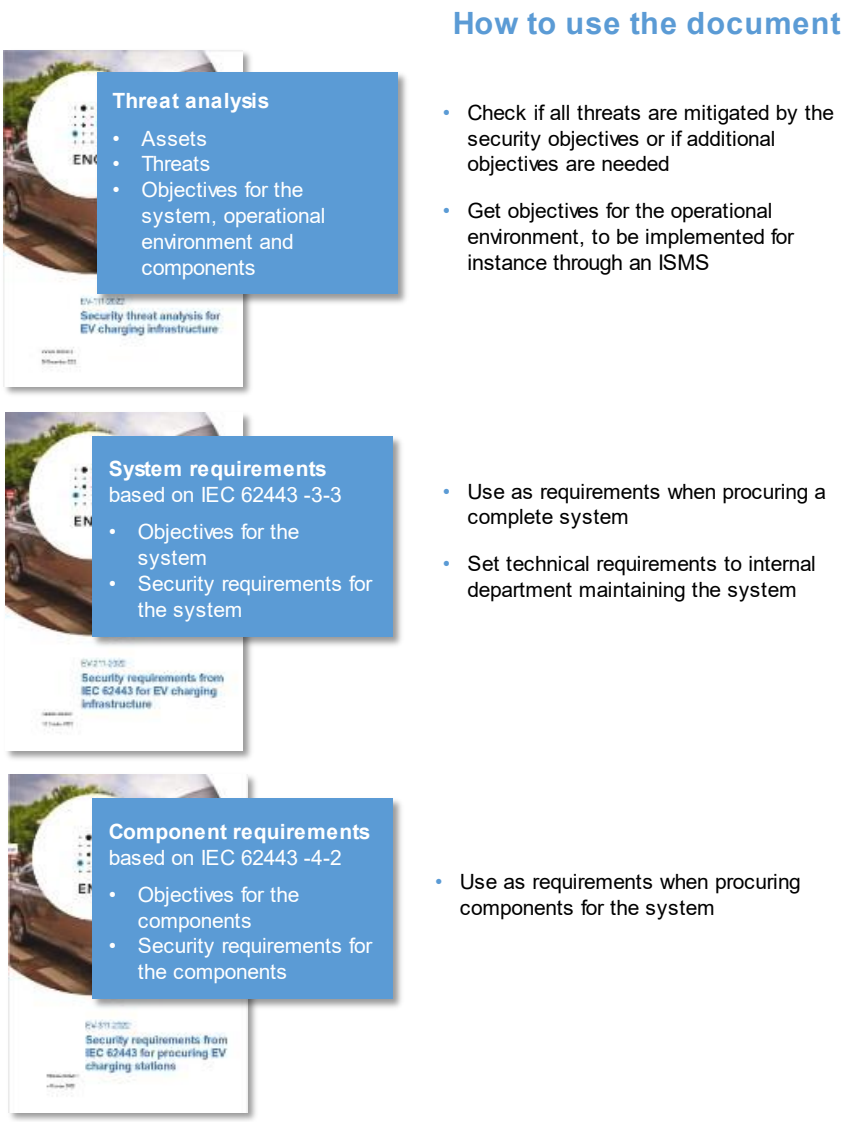

Figure 1: Relation between the different documents on EV charging infrastructure security.

Based on the system objectives, security objectives for EV charging stations are defined in [5] based on IEC 62443-4-2 in [7]. CPOs can use these requirements when procuring charging stations. By deriving the component requirements from the system requirements, the threat analysis ensures a consistent set of requirements for the whole system.

2 System description

To determine the security threats to the EV charging infrastructure, we should first understand how the system works: what its intended use is, in what environment it will be used, and what information assets are processed by it.

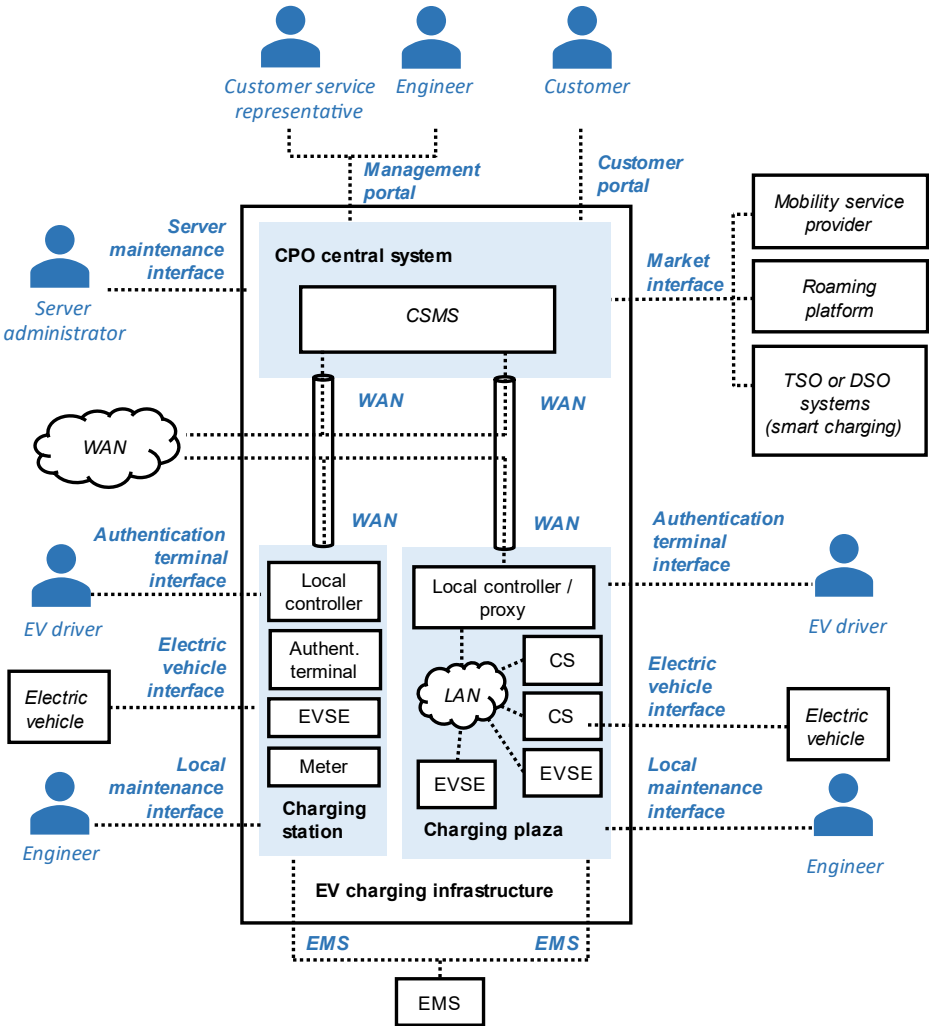

Figure 2: Reference architecture for the EV charging station, showing its users and interfaces.

2.1 Intended use of the system

The EV charging infrastructure consists of the systems used by a Charge Point Operator (CPO) to operate and maintain their charging stations and plazas. This includes the charging stations themselves, and the central systems such as the charging station management system (CSMS).

2.1.1 Components in the system

The CPO central system manages the different charging stations through the charging station management system (CSMS). It contains the servers and workstations used to maintain the CPOs charging stations remotely.

The central system allows to exchange information with mobility service providers and roaming platforms to allow EV drivers to use charging stations operated by different CPOs.

In some cases, the central system also connects to systems of a Transmission System Operator (TSO) or Distribution System Operator (DSO) to allow smart charging. The rate of charging is then adjusted based on the capacity in the electricity grid.

Through the customer portal, customers can retrieve their transaction data and contact customer services, who can access the CPO central system through the management portal, like engineers, to solve issues for the customers.

The charging stations be standalone devices or be in a group forming a charging plaza. The charging stations usually include a local controller and authentication terminal for EV drivers to authenticate to the device, the electric vehicle supply equipment (EVSE) to supply electrical power to the EV vehicles, and a meter, to measure how much power is supplied. The charging station can also be locally maintained by engineers.

2.1.2 Users of the system

The CPO central system is maintained by employees or contractors of the charge point operator. This threat analysis distinguishes between three different groups:

- **Customer service representatives** working for instance at the helpdesk of the CPO. They assist customers with simple problems with the charging stations and have limited access to it.
- **Engineers** that maintain the charging stations. They can make changes to the charging station configuration and update the firmware.
- **Server administrators** that maintain the CPO central system. They are responsible for both the server infrastructure, such as operating systems, virtualization platforms, databases, and the CSMS applications.

The charging stations themselves can be accessed by electric vehicle drivers to start and stop charging. Electric vehicles themselves communicate with the charging station to, for instance, control the charging speed and for stop charging when the vehicle's battery is full.

2.2 Intended operational environment

The intended operational environment of the EV charging infrastructure is shown in the reference architecture Figure 2.

2.2.1 Interfaces

The EV charging infrastructure is connected to the operational environment on the following interfaces.

2.2.1.1 Management portal

Customer service representatives and engineers can access the CPO central system through the management portal to get information on charging stations and change their state or configuration. The management portal is usually a web portal accessed over the internet.

2.2.1.2 Customer portal

Customers can access their customer and billing information through the customer portal. The customer portal can be a web portal on the internet or a smartphone app.

2.2.1.3 Market interface

The central systems are connected to the market parties, such as mobility service providers, roaming platforms, and DSO and TSO systems, over the market interface. The connections are usually over the internet, sometimes through a VPN. Typically web services are used, for instance using the OCPI, OCHP, OSCP and OICP protocols [8].

2.2.1.4 Server maintenance interfaces

Server administrators the server maintenance interface to perform maintenance on the CPO central system servers. The interface is usually accessed over the internet, sometimes through a VPN. Administrators can use any protocol used to administer servers, such as remote desktop protocols or SSH.

2.2.1.5 WAN interface

The charging station is connected to the CPO central system over a wide-area network (WAN). The CPO central collects meter values and transaction data. The other way around, the CPO central system may send charging profiles, set tariffs, or install configurations and updates on the charging station.

The WAN is usually a wireless mobile network, such as a GPRS or LTE network. Network segregation measures such as private APNs are commonly used.

The CSMS often manages the charging stations through the Open Charge Point Protocol (OCPP). This protocol allows to change the setting, perform firmware updates, and collect logs. The reference architecture assumes that all remote maintenance is done through the CSMS central system.

2.2.1.6 Authentication terminal interface

Users authenticate to the charging station through the authentication terminal interface. Some of the most common methods include RFID cards, bank cards, authentication through an application. In the near future, ISO 15118's Plug & Charge will allow authorization by means of certificates [9]. The authentication method used depends on the mobility service provider and often cannot be freely chosen by the CPO. So, only high-level security requirements are included for the terminal.

2.2.1.7 Electrical vehicle interface

The electric vehicle connects to the charging station on the electric vehicle interface, which is the power connection that will charge the car. In Europe, the main EV plug standards are IEC 62196 Type 2 [10] for AC chargers, and CCS Combo 2 [11] for DC chargers. The vehicle can communicate with the charging station to control charging. Now this is usually done through simple electrical signals. But in the future, there will be digital communication over the IEC 15118 protocol.

2.2.1.8 Local maintenance interface

Besides over the WAN through the CPO central system, engineers may also locally maintain the equipment through the local maintenance interface. This interface can be an Ethernet, serial or USB port. Engineers connect an engineering laptop to the local maintenance interface and can configure the equipment using specialized management software or a web interface.

2.2.1.9 EMS interface

An energy management system (EMS) can be used for load balancing by connecting to the charging plazas or charging stations through the EMS interface. The EMS might set charging control limits to prevent overloading connections or due to weather conditions. The communication between the EMS and the charging station can be done through IEE 2030.5 protocol [8]. This interface is found only in certain charging stations, depending on the brand, model, and deployment (e.g., stand-alone or within a charging plaza).

2.2.2 Physical locations

The CPO central system can be located in data centers of the CPO or in a cloud system.

Charging stations can be placed in public parking spaces, in parking garages, or at homes. A charge point operator can operate hundreds of thousands of charging stations

spread over a large area. So, it is not realistic to physically protect them. Engineers only visit charging stations when there are problems or there is scheduled maintenance.

2.3 Information assets

As the primary function of the infrastructure is to enable EV charging, the core information assets are charging transaction information and information to authorize charging. In some cases, the infrastructure will also process charging profiles for smart charging. To allow the infrastructure to be managed, maintenance and security assets are also needed.

2.3.1 Charging transaction information

The main purpose of a charging infrastructure is to charge electric vehicles and process usage information per customer in the CSMS for billing. Therefore, important information assets for the charging infrastructure are those needed for charging transactions:

- Transaction data from EV drivers, such as the ID of the EV driver
- Meter values
- Tariffs

If the integrity of the transaction information is compromised, this could lead to financial damage to the CPO as transactions are not processed correctly. It may also cause problems with charging. A charging station could for instance stop charging before the EV's battery is full. Or it could lock the power plug because it thinks a transaction is not completed. Switching charging on or off at many charging stations could lead to instability in the power grid.

The confidentiality of the transaction information is also important, as it contains personal data. The transactions show for instance where someone's car has been. If such information would leak, it would likely be an incident under the GDPR.

A compromise of availability could also lead to economic losses at CPOs and customers. If for instance the charging stations cannot connect to the central systems, this could mean that EV charging customers cannot charge their vehicles, so that they cannot get where they need to go. But if charging is allowed, it could lead to delays in payment to the CPO or some transactions not being properly registered.

2.3.2 Authorization information

Credit and debit card information or other information for transaction authorization (such as RFID data or PIN codes) is also critical. When its integrity can be compromised, attackers may charge without paying. When for instance credit card information would leak, attackers could steal money from the CPOs customers.

When the availability of processing authorization information is compromised, customers may not be able to charge or CPOs may not be able to get paid, leading to financial damage.

2.3.3 Smart charging information

If the charging station is used for smart charging, the CSMS may send charging profiles to the charging station to set the maximum charging speed.

If smart charging is not available, TSOs and DSOs will need to resolve congestion issues in the grid in another ways. They may be required to forcibly disconnect some users, leading to economic damage. A compromise of the integrity of the profiles could worsen the congestion, possibly requiring TSOs or DSOs to disconnect even more customers.

The load profiles are not highly confidential. They do give information about congestion in the grid, that attackers may use to plan attacks on it.

2.3.4 Maintenance assets

The information assets needed for maintenance are the firmware and the stored configuration, including the communication settings. Additionally, engineers may need the operational logs of the device to analyze and fix problems with the device. If the integrity of the configuration or firmware is compromised, attackers may use it to get to the other information assets. If the confidentiality of maintenance information is compromised, attackers may use the information to prepare attacks.

2.3.5 Security assets

For security, key information assets are the security logs and the keys and passwords. These include the passwords used by engineers to log in and the keys used for authentication and communication security on the WAN. A compromise of the integrity or confidentiality of these assets can again lead to a compromise of the other assets.

3 Threats

Based on the system description we can determine the possible threats. On external interfaces, there are threats of unauthorized access, exploits of software vulnerabilities, and attacks on communication. There are physical threats to the location and supply chain threats to the equipment used. For each normal user group, there are insider threats. And there are threats of what attackers may do to the critical assets after they have gained access.

3.1 Threat actors

The threat analysis considers both external and internal threat actors. Possible external threat actors are:

- Criminals
- Nation state actors
- Terrorists

Criminals can try to make money from the EV charging infrastructure through fraud. Individual EV drivers may try to find ways to charge without paying. Criminal groups may try to offer tools or methods to charge more cheaply. The risk of fraud seems to have been low until now. There are publicly known vulnerabilities in some payment systems. But the financial damages of these vulnerabilities have apparently not been high enough to force CPOs to fix them.

Criminals may also try to make money through ransomware. They could for instance try to make it impossible to charge at the charging stations of a CPO, causing serious financial and reputational damage. They could also threaten to release confidential information about customers.

Nation state actors and terrorists may try to use the EV charging infrastructure to disrupt the electricity grid. By switching the power for many charging stations on or off at the same time, they can cause problems in balancing electricity demand and supply. Such balancing problems could lead to major power outages. If smart charging is used in the future to counter grid congestion, attacking it may also cause damage to transformers and power lines [12] [13].

It is difficult to know the capabilities and goals of nation states. But there are signs that some are developing cyber-attacks to cause power outages. There have been targeted cyber-attacks on grid operators in Ukraine in 2015 and 2016 [14]. Most EU member states have appointed electricity companies as operators of essential services under the NIS directive, so that they are required to take appropriate security measures. But attackers do not have to limit themselves to operators of essential services. Major CPOs may already be big enough to cause balancing issues.

3.2 Unauthorized access threats to the CPO central system

Unauthorized access threats to the CPO central system concern an attacker getting access to the central system as one of the user groups (see Figure 2 in Section 2) using the normal access method on an interface. They may, for instance, compromise a key or password and then log in. Threats are considered per interface (see Figure 2), as usually different measures are taken on each interface.

T-UA1 Unauthorized access as a charging station on the WAN	An attacker gains access to the WAN network and then gains unauthorized access to the CSMS as a charging station. With this access they may stop charging, tamper with transactions and meter values.
T-UA2 Unauthorized access as an engineer or customer service representative on the management portal	An attacker gains access to the management portal interface and then gains unauthorized access to the CSMS as an engineer or customer service representative. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware on all connected charging stations.
T-UA3 Unauthorized access as a server administrator on the server maintenance interface	An attacker gains access to the server maintenance interface and then gains unauthorized access to the CSMS as a server administrator. With this access they may change the server software and configuration, and in this way take full control of the CSMS. With such control, they can stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware on all connected charging stations.
T-UA4 Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface	An attacker gains access to the market interface and then gains unauthorized access to the CSMS. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles.

T-UA5 Unauthorized access as a customer on the customer portal	An attacker gains access to the customer portal and then gains unauthorized access to the CSMS. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles.

3.3 Unauthorized access threats to the charging station

Unauthorized access threats to the charging station concern an attacker getting access to the charging station as one of the user groups (see Figure 2 in Section 2) using the normal access method on an interface. They may, for instance, compromise a key or password and then log in. Threats are considered per interface (see Figure 2), as usually different measures are taken on each interface.

The interface to the EMS is considered as part of the physical threats in Section 3.6, as it is usually not possible to directly access the interface on the EV charging station or plaza without physical tampering.

T-UA5 Unauthorized access as the CSMS	An attacker gains access to the WAN network and then gains unauthorized access to the charging station as the CSMS. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.
T-UA6 Unauthorized access as an EV driver on the authentication terminal interface	An attacker gains access to the authentication terminal interface and then gains unauthorized access to the charging station as an EV driver. With this access they may commit fraud and charge their vehicle without cost.
T-UA7 Unauthorized access as an electric vehicle in the electric vehicle interface	An attacker gains access to the electric vehicle interface and then gains unauthorized access to the charging station as an electric vehicle. With this access they may commit fraud. *Remark:* Committing fraud is only possible if it is possible to pay through EV charging interface (“plug & charge”).

T-UA8 Unauthorized access as an engineer on the local maintenance interface	An attacker gains access to the local maintenance interface and then gains unauthorized access to the charging station as an engineer. With this access they may change the configuration or firmware.

3.4 Exploits of software vulnerability

Exploits of software vulnerabilities concern an attacker exploiting a vulnerability in the EV charging infrastructure to gain access to it. Using a software vulnerability, attackers may gain privileged access to the system, even when users on an interface normally have restricted access, as is for instance the case on the market interface.

T-EX1 Exploit of a software vulnerability on the CPO central system on the WAN	An attacker gains access to the WAN interface and then exploits a software vulnerability to gain access to the CPO central system. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware on all connected charging stations.
T-EX2 Exploit of a software vulnerability on the internet-facing interfaces	An attacker gains access to the management portal, customer portal, and market interface and then exploits a software vulnerability to gain access to the CPO central system. With this access they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware on all connected charging stations.
T-EX3 Exploit of a software vulnerability on the server maintenance interface	An attacker gains access to the server maintenance interface and then exploits a software vulnerability to gain access to the CPO central system. With this access they may take full control of the CSMS. With such control, they can stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware on all connected charging stations.
T-EX4 Exploit of a software vulnerability on the	An attacker gains access to the WAN interface and then exploits a software vulnerability to gain access to

charging station on the WAN	the charging station. With this access they may take full control the charging station, and then stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.
T-EX5 Exploit of a software vulnerability on local interfaces on the charging station	An attacker gains access to the authentication terminal, electric vehicle, local maintenance, or EMS interface on the charging station and then exploits a software vulnerability to gain access to it. With this access they may take full control the charging station, and then stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.

3.5 Communication threats

Communication threats concern compromising the confidentiality, integrity, or availability of the communication on an interface. Separate threats are considered on different interfaces (see Figure 2 in Section 2), as they are protected by different measures.

Attacks on local networks in the field, such as the charging plaza LAN or the network between the EMS and the charging stations or plaza, are not considered here. They are seen as physical threats to the system and treated in Section 3.6.

T-CM1 Data modification on WAN	An attacker gains access to the WAN network and then modifies information sent between the charging station and the CSMS. In this way, stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.
T-CM2 Data disclosure on WAN	An attacker gains access to the WAN network and then eavesdrops on information sent between the charging station and the CSMS. In this way, they may gain confidential information sent between the charging station and CSMS, such as meter values or the configuration of the charge point operator's system.
T-CM3 Network denial-of-service attack on the WAN	An attacker gains access to the WAN interface and disrupts the normal operation of the charging station,

	for instance by sending malformed messages or flooding the device with data. In this way, they may stop charging, prevent transaction data, meter readings, and logs being sent to the CSMS, and charging profiles, configurations, and firmware updates being sent to the charging station.
T-CM4 Data modification on the internet facing interfaces	An attacker modifies information sent or received on the management portal, customer portal, or market interface. In this way, they may stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware.
T-CM5 Data disclosure on internet facing interfaces	An attacker eavesdrops on information sent or received on the management portal, customer portal, or market interfaces. In this way, they may gain confidential information, such as credit and debit card information, charging station keys or passwords, or personal information from customers.
T-CM6 Network denial-of-service attack on the internet-facing interfaces	An attacker disrupts normal communication on the management portal, customer portal, or market portal, for instance by sending malformed messages or flooding the servers with data. In this way, they may prevent transactions from being completed normally, charging profiles to be changed for smart charging by DSOs systems, or configuration changes and firmware updates by engineers and customer service providers.
T-CM7 Data modification on the server maintenance interface	An attacker gains access to the server maintenance interface and then modifies information sent between the server administrator and the CPO central system. In this way, they may change the central system configuration or software.
T-CM8 Data disclosure on the server maintenance interface	An attacker gains access to the server maintenance interface and then eavesdrops on information sent between the server administrator and the CPO central system. In this way, they may gain confidential

	information, such as the configuration of the charge point operator's system.
T-CM9 Network denial-of-service attack on the server maintenance interface	An attacker gains access to the management portal or market interfaces and disrupts the normal operation of the central system, for instance by sending malformed messages or flooding the servers with data. In this way, they may prevent server administrators from performing maintenance on the system, for instance to recover after an incident.

3.6 Physical threats

Physical threats concern an attacker gaining access to the system using physical means. They may try to break into the charging station and then access local interfaces, such as the local maintenance interface, tamper with the hardware, for instance by changing data stored on hard disk or in flash memory, or tamper with the networks, for instance by putting additional devices in them.

They may also try to break into the data centers for the central systems and gain access to the servers.

Of particular concern is the threat of an attacker breaking into one charging station and using their access to get to other charging stations. Such an attack would allow attacker to compromise more than one charging station at the same time, leading to a higher impact.

We only consider physical threats that lead to a compromise of the information assets in Section 2.3. Direct physical sabotage of the charging station itself is not considered.

T-PH1 Unauthorized physical access to the central system centers	An attacker gains physical access to the data center where the CPO central system is hosted and uses the physical access to gain logical access. Attackers may log in on one of the ports or physically tamper with the hardware. With this access they may take full control of the CSMS. With such control, they can stop charging, tamper with transactions and meter values, set incorrect tariffs or charging profiles or change the configuration or firmware on all connected charging stations.

T-PH2 Unauthorized physical access to a charging station	An attacker gains physical access to a charging station and uses the physical access to gain logical access to the EV charging station. Attackers may log in on one of the ports or physically tamper with the hardware. With this access they may commit fraud or change the configuration or firmware.
T-PH3 Unauthorized access to a charging plaza LAN or local controller	An attacker gains physical access to the LAN or local controller of a charging plaza. They use the access to gain logical access to the charging plaza. Attackers may tap into one of the network cables, connect to a router or switch, log in on one of the ports of the controller or physically tamper with the hardware. With this access they may stop charging in the plaza, commit fraud, or change the configuration or firmware.
T-PH4 Unauthorized access as the EMS on the EMS interface	An attacker gains access to the EMS interface, for instance by physically breaking into the interface or the connection between the EMS and the charging station, or by compromising the EMS. The attacker then uses the interface access to gain logical access to the EV charging station or plaza. With this access, they may stop charging or reduce the rate of charging.
T-PH5 Unauthorized access to the EV charging infrastructure from a compromised field location	An attacker gains physical access to a charging station or charging plaza and uses it as an entry point into the EV charging infrastructure to perform further attacks on the CPO central system or other charging stations or plazas.

3.7 Supply chain threats

Supply chain threats concern attacks on the EV charging infrastructure through suppliers. Attackers may compromise the hardware or software used in the infrastructure before it is installed, for instance to put backdoors in it.

The threat of sensitive information leaking through suppliers is not considered here. It can only be countered by organizational measures, not by any technical measures in the EV charging infrastructure.

Threats through staff at suppliers working on the EV charging infrastructure (remotely or locally) are considered part of the insider threats (Section 3.8).

T-SC1 Unauthorized software, firmware, or hardware modification at suppliers	An attacker modifies software, firmware, or hardware at the supplier. This way, attackers may for instance install backdoors or logic bombs in the EV charging infrastructure that would allow them to stop charging, tamper with transactions and meter values, or set incorrect tariffs or charging profiles.
T-SC2 Unauthorized software, firmware or hardware modification between the supplier and installation	An attacker modifies software, firmware, or hardware after it leaves the supplier and before it is installed in the EV charging infrastructure. This way, attackers may, for instance, install backdoors or logic bombs in the charging station that would allow them to stop charging, tamper with transactions and meter values, or set incorrect tariffs or charging profiles. *Remark:* Attackers could, for instance, modify software or firmware in transit from the supplier to the CPO or stored on a server or laptop. They could modify hardware in storage or during transport.

3.8 Insider threats

Insider threats concern threats to the EV charging infrastructure by authorized human users. Different threats are considered for the two user groups: engineers and server administrators (see Figure 2 in Section 2).

T-IN1 Harmful actions by engineers	An engineer with authorized access, incidentally or on purpose, performs actions that are harmful to the EV charging infrastructure. They may, for instance, make incorrect changes to the configuration or install the wrong firmware.
T-IN2 Harmful actions by server administrators	A server administrator with authorized access, incidentally or on purpose, performs actions that are harmful to the EV charging infrastructure. They may, for instance, make incorrect changes to the configuration or install the wrong firmware.

3.9 Post-exploitation threats

The following threats concern steps attackers can take to compromise the EV charging infrastructure information assets after they have gained access to the system. They are considered separately, as they may be combined with any threat that gives an attacker access.

T-PE1 Loss of configurations	The configuration of the charging station is deleted or becomes corrupted through mistakes by engineers or intentional actions from an attacker that has gained access.
T-PE2 Software or firmware corruption	The software or firmware installed in the EV charging infrastructure is corrupted, for instance by placing a backdoor or logic bomb in it, or simply making it unusable.

4 Zoning model

To mitigate the threats, the EV charging infrastructure will be divided into three zones: the CPO central system, charging stations, and charging plazas. Different objectives will be defined for each zone. To define the access control objectives, we also identify the users of each zone.

4.1 Zoning

In the reference architecture, the EV charging infrastructure is divided into three zones:

- The **CPO central system** consists of all servers that are used to manage and maintain the charging stations remotely.
- The **charging station** consists of the all the equipment physically inside the charging station. This can include a local controller, the authentication terminal, the electric vehicle supply equipment (EVSE), and a meter.
- The **charging plaza** consists of all EV charging equipment in a charging plaza connected to the central system through one local controller or proxy. This can include multiple charging stations and EVSE, and a local area network (LAN).

The zoning model allows to set different objectives for the different types of systems in each zone. The CPO central system is a modern IT application, often running in the cloud. The charging station is an embedded system, usually placed in public locations without supervision. The charging plaza consists of multiple embedded systems, connected over a local network in a somewhat supervised location. Different security measures can and should be taken for each type of system.

4.2 Access control policy

To determine what access control measures have to be taken in each zone, we need to know the users of the zone. Table 1 and Table 2 list the users that are authorized to access the CPO central system and the charging station respectively, and the access they require. The last column gives the interfaces on which they access the system (see the reference architecture in Figure 2).

Table 1 User groups on the CPO central system.

User	Required access	Interface
Charging station	• Send transaction data and meter values for billing • Optional: Get charging profiles	WAN

Engineers	• Remote maintenance to charging stations through the central system	Management portal
Customer service representative	• Fix customer problems with charging stations	Management portal
Customers	• See transaction information	Customer portal
Market parties (mobility service provider, roaming platform, TSO, or DSO)	• Exchange transaction data • Enable EV drivers to use charging stations from different CPOs • Provide smart charging schedules	Market interface
Server administrator	• Maintain applications • Maintain network and server infrastructure	Server maintenance interface

The access control model assumes that engineers do not access charging stations directly over the WAN. They always work through the central maintenance system.

Table 2 User groups on the charging station.

User	Required access	Interface
Charging Station Management System (CSMS)	• Collect transaction data and meter values for billing • Set tariffs • Configure the charging station • Restore the charging station from a backed-up configuration • Update the firmware • Monitor operational logs • Optional: Send charging profiles	WAN
Engineer	• Configure the charging station • Restore the charging station from a backed-up configuration	Local maintenance

	• Update the firmware • Analyze the operational logs	
EV driver	• Authenticate for charging • *Optional:* Pay for the charging	Authentication terminal
Electric vehicle	• Control the charging • *Optional:* authenticate for charging	Electric vehicle
Other charging station	• Load balancing within a charging plaza	LAN
Local EMS	• Energy management within the local context (e.g., building)	LAN

5 Security objectives for EV charging infrastructure

We can now define security objectives to mitigate the threats. The zoning model allows to set different objectives based on the scalability of the threats:

- For threats that can affect many charging stations through the central systems or the WAN network, the security objectives provide protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation (security level 3).
- For local threats where the impact is limited to one charging station or small number of charging stations, such as physical attacks, the security objectives provide protection against intentional violation using simple means with low resources, generic skills, and low motivation (security level 2).

Less strict objectives are set for local threats because providing protection against sophisticated attackers would be costly. Charging stations would have to be designed to be much more physically hardened than they are now, and they should be monitored for physical intrusions. The impact of local attacks is usually not large enough to justify such measures.

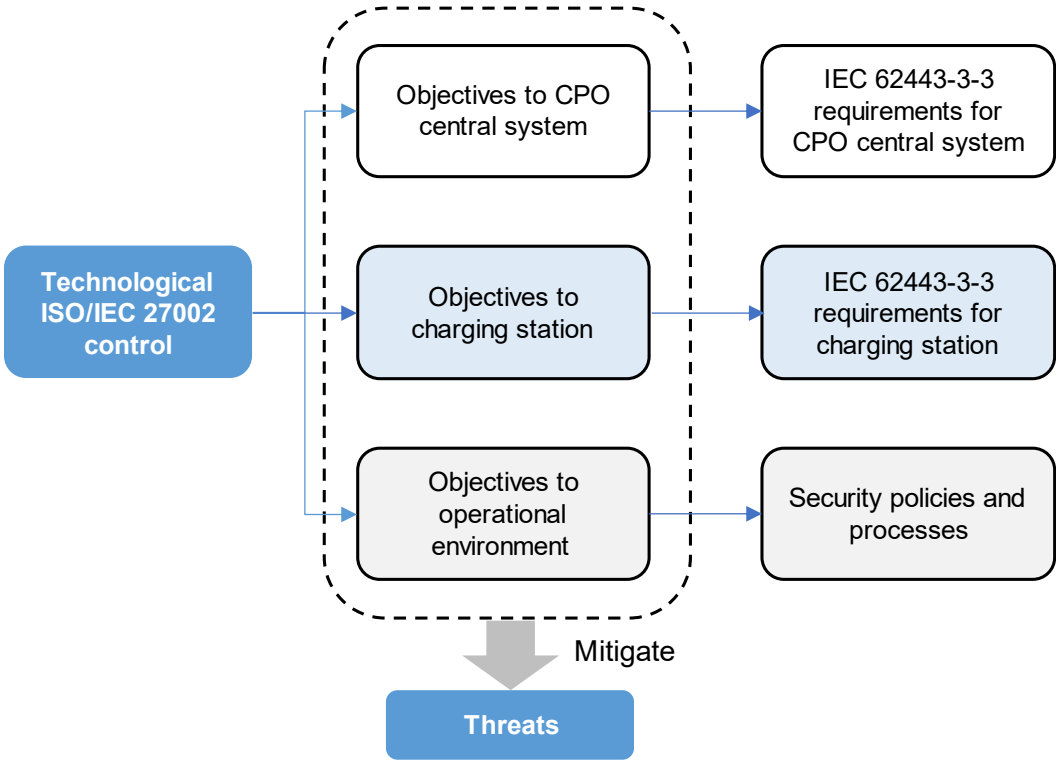

Figure 3: Relation of the security objectives to the ISO/IEC 27001 and IEC 62443 standards.

The objectives are derived from the controls in ISO/IEC 27002:2022 [4]. For the organizational, people, and physical controls, the controls themselves are used as objectives. The technological controls are refined into more detailed objectives for the central system, charging station, and operational environment, as shown in Figure 3, as the aim of this document is in the end to define technical security requirements for EV charging infrastructures in [1].

The objectives to the operational environment are additional organizational and technical measures that the charge point operator should take to securely operate the EV charging infrastructure. These should be addressed in the internal security policies and processes of the operator.

5.1 Organizational controls

At least the following organizational controls from ISO/IEC 27002:2022 are needed to mitigate the threats:

- 5.4 Management responsibilities
- 5.9 Inventory of assets and other information
- 5.15 Access control
- 5.16 Identity management
- 5.18 Access rights
- 5.20 Addressing information security within supplier agreements
- 5.21 Managing information security in the ICT supply chain
- 5.25 Assessment and decision on information security events
- 5.26 Response to information security incidents
- 5.34 Privacy and protection of PII

Implementation guidance on access control (5.15, 5.16, 5.18): objective 8.3-SO3 allows the accounts to be managed centrally.

5.2 People controls

At least the following people controls from ISO/IEC 27002:2022 are needed to mitigate the threats:

- 6.1 Screening
- 6.2 Terms and conditions of employment
- 6.3 Information security awareness, education, and training
- 6.4 Disciplinary process
- 6.5 Responsibilities after termination or change of employment

5.3 Physical controls

The data center housing the central system should be protected following physical security standards for modern data centers. This includes implementing at least the following controls from ISO/IEC 27002:2002:

- 7.1 Physical security perimeters
- 7.2 Physical entry
- 7.3 Securing offices, rooms, and facilities
- 7.4 Physical security monitoring
- 7.8 Equipment siting and protection
- 7.12 Cabling security

Describing appropriate physical security measures for data centers would go too far for this document.

For the charging stations and plazas, the strategy is to limit the impact of a physical break-in to one location (see objective **8.22-SO3** in Section 5.4). By restricting network communications, it can be made very difficult for physical attackers in one charging station to reach other charging stations or central systems.

But is still useful to have physical protection against intentional violation using simple means with low resources, generic skills, and low motivation (security level 2) to discourage fraud and vandalism. Hence, the following objectives should be met by the charging stations and plazas, and their operational environment.

Note that for physical controls, objectives for the charging stations and charging plazas differ. However, for the technological controls defined in section 5.4, objectives for charging stations and charging plazas are the same.

7.4 Physical security monitoring

Charging station	**7.4-SO1 Physical access detection on charging stations:** The charging station sends an alert to the CSMS when any part of its casing is opened. *Implementation guidance:* Alerts for opening the casing are included in the OCPP 2.0 (Appendix 1) standard and the security extension to OCPP 1.6.
Charging plaza	**7.4-SO1 Physical access detection on charging stations:** The cabinets housing the charging plaza equipment (see objective 7.4-SO1) send an alert to the CSMS when they are opened.

Operational environment	**7.4-SO2 Physical access monitoring:** The charge point operator monitors physical security events on the charging stations and plazas and responds to them. *Implementation guidance:* Operators should at least respond to access control events generated according to objective 7.4-SO1, and to reports from users or passers-by on physical damage to charging stations. In most cases an engineer will need to go to the charging station to inspect it. The operator should define a policy on what checks an operator must perform to ensure that the charging station configuration and firmware have not been modified.

7.8 Equipment siting and protection

Charging station	**7.8-SO1 Tamper resistance on charging stations:** The charging station has a casing that protects against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces.
Charging plaza	**7.8-SO2 Tamper protection for charging plaza equipment:** The local controller or proxy, and the networking equipment for a charging plaza will be placed in a locked cabinet. The cabinet protects against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces.

7.12 Cabling security

Charging station	**7.12-SO1 Cabling security for EMS connection:** Network cables connecting a charging station to an EMS are protected against tampering. Attackers without specialist tools cannot physically connect to the EMS interface without leaving visible traces.
Charging plaza	**7.12-SO2 Cabling security for charging plazas:** The network cables of the charging plaza local area network and the connection to an EMS are protected against tampering. Attackers without specialist tools cannot physically connect to the corresponding interfaces without leaving visible traces.

5.4 Technological controls

While for the organizational, people, and physical controls we just use the controls from ISO/IEC 27002:2022, the technological controls are further specified in more detailed objectives for the CPO central system, charging station, and the operational environment (see Figure 3).

For the CPO central system, strong security measures are possible through efficient management. So, there are objectives for strong access control for all users, cryptographically protecting the communication, and monitoring the zone from a SIEM. The central system should be protected from denial-of-service attacks from the WAN and internet-facing interfaces. The functions should also not be disrupted by security updates, so that it is possible to remotely patch vulnerabilities.

For the charging station, strong security measures are possible through automated management. So, there are objectives for strong access control for all users, cryptographically protecting the communication, and monitoring the zone from a SIEM. Charging functions should be protected from denial-of-service attacks from the WAN. The functions should also not be disrupted by security updates, so that it is possible to remotely patch vulnerabilities.

8.3 Information access restriction

CPO central system	**8.3-SO1 Least privileges on the WAN interface:** The CPO central system enforces access control on the WAN, so that users on the interface can only access the functions they need.
	8.3-SO2 Role separation on the market interface: The CPO central system enforces access control on the market interface with separate roles for mobility service providers, roaming platforms, and DSO systems, so that they can only access the functions they need for their role.
	8.3-SO3 Centrally managed, role-based access control for customer service representatives, engineers, and server administrators: The CPO central system enforces role-based access control for customer service representatives, engineers, and server administrators with individual user accounts managed on a central server.
	8.3-SO4 Restrictions on switching commands: The CPO central system does not allow engineers and customer representatives to switch charging on or off on many charging stations at the same time, for instance by limiting the number of switching commands per user per hour.

	8.3-SO5 Individual accounts for customers: The CPO central system support individual accounts for customer and enforces access control so that they can only access the functions they need.
Charging station or plaza	**8.3-SO6 Least privileges on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces:** The charging station or plaza enforces access control on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces, so that user group with access to the interface can only access the functions they need.

8.5 Secure authentication

CPO central system	**8.5-SO1 Mutual authentication for the charging stations, mobility service provider, roaming platform and DSO systems:** The CPO central system enforces mutual authentication with the charging stations, mobility service provider, roaming platform and DSO system. Devices on each side uniquely identify themselves and allow the other side to authenticate them. They only provide access after having authenticated the other side's identity.
	8.5-SO2 Authentication with individual passwords for customers, customer service representatives, engineers, and server administrators: The CPO central system enforces mutual authentication for representatives, engineers, and server administrators. Representatives, engineers, and administrators use individual credentials. The login procedure is protected against known attacks.
	8.5-SO3 Multifactor authentication for server administrators on the server maintenance interface: The CPO central system enforces multifactor authentication for server administrators on the server maintenance interface with a login procedure that is protected against known attacks. *Remark:* The multifactor authentication could for instance be implemented by using a remote access VPN for server administrators with multifactor authentication configured for the user authentication.

Charging station or plaza	**8.5-SO4 Role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations:** The CSMS, electric vehicle, engineers, EMS, and other charging stations identify to the charging station with information that allows the zone to determine its role. The charging station authenticates the system's role and assigns it access rights based on the role. The charging station uniquely identifies itself to CSMS, EV driver, electric vehicle, and other charging stations, and allows the system to authenticate them. *Remark:* Engineers may use shared passwords on the local maintenance interface, although it is recommended to use unique passwords per charging station or centrally managed accounts with individual passwords for the engineers.
	8.5-SO5 Authentication for EV drivers on the authentication terminal: The charging station enforces authentication for EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider.

8.7 Protection against malware

CPO central system	**8.7-SO1 Active malware protection in the CPO central system:** Hosts in the CPO central systems are actively protected against malware through, for instance, anti-virus software or application whitelisting software.

8.8 Management of technical vulnerabilities

CPO central system	**8.8-SO1 Hardening over the local maintenance or server maintenance interface:** Server administrators can harden hosts in the CPO central system over the server maintenance interface or from engineering workstations. They can disable unneeded functions to reduce the likelihood of vulnerabilities and allow to enable security functions available on the hardware and software platforms to reduce their possible impact.

Charging station or plaza	**8.8-SO2 Hardened by default:** The charging stations and charging plaza devices are delivered by the manufacturer in a hardened configuration. Unneeded functions are disabled to reduce the likelihood of vulnerabilities. Security functions on the hardware and software platforms are enabled to reduce the possible impact of vulnerabilities.
Operational environment	**8.8-SO3 Vulnerability management process:** The charge point operator manages vulnerabilities in the system by: • disabling unused ports, services, user accounts and functions to reduce the likelihood of vulnerabilities • monitoring vulnerabilities in the system's software and firmware, assessing the risks of the vulnerabilities, and mitigating the high-risk vulnerabilities, for instance by applying security updates • limiting the impact of vulnerabilities by enabling the security features on the hardware and software platforms used *Implementation guidance:* A clear policy should be defined for when vulnerabilities must be patched, based on their severity. The CVSS score could be used as a severity measure but must usually be complemented with information about the location of the vulnerability in the system.

8.9 Configuration management

CPO central system	**8.9-SO1 Server configuration management:** Server administrators can manage and monitor the configurations of software, services, and networks of the CPO central system from the server maintenance interface.
Charging station or plaza	**8.9-SO2 Automated configuration management:** The charging station can be restored from a backed-up configuration automatically by the CPO central system.

8.13 Information backup

CPO Central system	**8.13-SO1: Automated backups for CPO central system:** The CPO central system supports making automated backups of the configurations and data.
Operational environment	**8.13-SO2 Backup process for charging stations configurations:** The charge point operator has a process to back up the charging station and plaza configurations on the CPO central system. Older versions of the configurations are kept, so that it is possible to revert to them in case of issues.
	8.13-SO3 Backup process for the CPO central system: The charge point operator has an automated process to back up the data and configurations on the CPO central systems (including the charging station and plaza configurations stored there according to 8.13-SO2).

8.15 Logging

CPO central system	**8.15-SO1 Integration with SIEM system:** The servers in the CPO central system log all relevant security events, such as access control events, and changes to the configuration and software. The servers can store the logs locally for forensic analysis. They can send them to a Security Information and Event Management (SIEM) system in a commonly supported format, so that they can be analyzed to detect incidents.
Charging station or plaza	**8.15-SO2 Collecting security events from the charging station through the CPO central system**: The charging station logs all relevant security events locally and sends selected events to the CPO central system, so that they can be analyzed to detect incidents. *Remark:* The CPO central system can then forward the security logs to a SIEM system according to 8.15-SO1.

8.16 Monitoring activities

Operational environment	**8.16-SO1: Security monitoring and incident response:** The charge point operator monitors and responds to security events on the CPO central system and the charging stations and plazas. They gather security logs from the devices centrally, for instance, in a SIEM. They establish procedures, use cases, and rules to find incidents in the logs. And they establish a process for responding to the incidents and minimizing the impact. *Implementation guidance:* Monitoring should try to detect at least: • unauthorized access attempts • unauthorized local access to charging stations • unauthorized changes to security settings (e.g., keys or credentials, authentication settings) • unauthorized installed firmware or software • possible signs of attacks (e.g., physical tamper events, invalid certificates)

8.17 Clock synchronization

CPO Central system	**8.17-SO1 Clock synchronization for the CPO central system:** The CPO central system synchronizes time with a central source to have reliable timestamps for security events.
Charging station or plaza	**8.17-SO2 Clock synchronization for the charging station:** The charging station or plaza synchronizes time with a central source to have reliable timestamps for security events.

8.19 Installation of software on operational systems

CPO central system	**8.19-SO1 Software updates over the server maintenance interface:** Server administrators can update the software and firmware in the CPO central system over the server management interface or from engineering software. Hosts in the CPO central system check the authenticity of firmware or software before installation through digital signatures.

Charging station or plaza	**8.19-SO2 Automated firmware management for local controllers:** The software and firmware on the local controller in the charging station or plaza can be updated through remote access from the CPO central system. The local controller can check the authenticity of firmware before installation through digital signatures. *Remark:* The local controller is the part that communicates with the CPO central system over the WAN. It is not required that other components of the charging station or plaza that are not reachable over the WAN can be remotely updated. It is however recommended to support remote updates for them to allow vulnerabilities in them to be patched more efficiently.

8.20 Network security

CPO central system	**8.20-SO1 Cryptographic protection of communication confidentiality and integrity on the WAN, management portal, market interface, and server maintenance interface:** The CPO central system protects the integrity and confidentiality of communication on the WAN, management portal, market interface, and server maintenance interface using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.
Charging station or plaza	**8.20-SO2 Cryptographic protection of communication confidentiality and integrity on the WAN interface:** The charging station protects the integrity and confidentiality of communication on the WAN interfaces using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks. *Remark:* If wireless communication is used on the local charging station interfaces, such as the authentication terminal, the local maintenance interface, or the EMC interface, it would be recommended to also protect it cryptographically.
	8.20-SO3 Resilience of charging functions against denial-of-service attacks on the WAN: The charging station shields charging functions from denial-of-service attacks on the WAN interface, so that these functions keep working if the device is flooded with data or malformed messages

8.21 Security of network services

Operational environment	**8.21-SO1 Resilience against denial-of-service attacks on the WAN:** The wide-area network (WAN) is resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation (security level 2). The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.
	8.21-SO2 Resilience against denial-of-service attacks on the internet facing interfaces: The internet connections for the management portal and market interfaces are resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation (security level 2). The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.

8.22 Segregation of networks

CPO central system	**8.22-SO1 Network segregation on the WAN, management portal, market interface, and server maintenance interface:** The CPO central system is segregated from other zones on the WAN, management portal, market interface, and server maintenance interface. Only normal connections are allowed through the network perimeter.
Charging station or plaza	**8.22-SO2 Network segregation on the charging station WAN:** The charging station is segregated from other zones on the WAN interface. Only normal connections are allowed through the network perimeter.
Operational environment	**8.22-SO3 No communication between charging stations on the WAN:** There is no direct communication between charging stations on the WAN interface. The charging stations can only communicate with CPO central system. *Implementation guidance:* The restriction on communication can be enforced in architecture of the telecom network.

	The firewall at the central systems should only allow through network services needed for normal communication to the charging stations. The services exposed to the charging stations should be tested for vulnerabilities, assuming that a charging station can be compromised. Charging stations may communicate with each other over a LAN in the same charging plaza. Such communication may be needed for local load balancing. But it should be restricted to local IPs and needed protocols and ports. It is recommended to use a private APN to shield the charging stations from attacks from the internet.

8.24 Use of cryptography

CPO central system	**8.24-SO1 Server key and password management over the server maintenance interface:** Server administrators can manage all passwords and keys used on the CPO central system server efficiently over the server maintenance interface.
Charging station or plaza	**8.24-SO2 Automated key and password management over the WAN:** All passwords and keys used in the charging station can be updated automatically through remote access from the CPO central system.
Operational environment	**8.24-SO3 Key and password management process:** The charge point operator manages the keys and passwords of the devices, so that they are properly protected and can be updated when needed.

6 Rationale for the security objectives

This section explains how the security threats in Section 3 are mitigated by the security objectives in Section 5.

6.1 Protection from unauthorized access threats to the CPO central system

Unauthorized access threats are mitigated by preventing attackers from getting access through authentication, and by limiting access by authorizations, as shown in Table 3.

Table 3: Security objectives to mitigate unauthorized access threats.

Threat	Authentication	Authorization
T-UA1 Unauthorized access as a charging station on the WAN	**8.5-SO1** Mutual authentication for the charging stations, mobility service provider, roaming platform and DSO systems	**8.3-SO1** Least privileges on the WAN interface
T-UA2 Unauthorized access as an engineer or customer service representative on the management portal	**8.5-SO2** Authentication with individual passwords for customers, customer service representatives, engineers, and server administrators	**8.3-SO3** Centrally managed, role-based access control for customer service representatives, engineers, and server administrators **8.3-SO4** Restrictions on switching commands
T-UA3 Unauthorized access as a server administrator on the server maintenance interface	**8.5-SO2** Authentication with individual passwords for customers, customer service representatives, engineers, and server administrators	**8.3-SO3** Centrally managed, role-based access control for customer service representatives, engineers, and server administrators

	8.5-SO3 Multifactor authentication for server administrators on the server maintenance interface	
T-UA4 Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface	**8.5-SO1** Mutual authentication for the charging stations, mobility service provider, roaming platform and DSO systems	**8.3-SO2** Role separation on the market interface
T-UA5 Unauthorized access as a customer on the customer portal	**8.5-SO2** Authentication with individual passwords for customers, customer service representatives, engineers, and server administrators	**8.3-SO5** Individual accounts for customers

To protect against unauthorized access, the goal is to provide protection against sophisticated threats (security level 3) by using strong authentication and applying least privileges on each interface. To ensure that these measures provide the required level of security, the following supporting objectives are required:

- **Key and password management:** to reduce the risk of the authentication measures being bypassed by stolen keys or passwords, these must be updated regularly or after incidents. Server administrators should be able to manage the passwords and keys over the server maintenance interface (**8.24-SO1**). The key and password management process (**8.24-SO3**) makes sure there is a structured process to update them.
- **Account management:** accounts of the engineers should be managed to ensure (**5.16**, **5.18**), for instance, that when an engineer changes jobs their access is revoked. To allow this process to work efficiently, the accounts of customer service representatives, engineers, and administrators in the CPO central system are managed centrally (**8.3-SO3**).
- **Hardening:** the servers in the central systems should be hardened by disabling unused services, so that there are no network services exposed without access control. The server administrator should be able to perform the hardening over the server maintenance interface (**8.8-SO1**). The vulnerability management process (**8.8-SO3**) ensures hardening is performed structurally.
- **Monitoring:** attempts to bypass the access control mechanisms should be monitored. The logging objective (**8.15-SO1**) allows failed and successful login

attempts to be logged and gathered in a SIEM system. Clock synchronization allows to make a reliable timeline of alerts (**8.17-SO1**). Processes should be established to detect and respond to these alerts (**8.16-SO1**).

Additional measures are taken for engineers, customer service representatives and server administrators. These user groups are considered the highest risk, as they have privileged access to the system. For engineer and customer service representatives, restrictions are placed on how many charging stations they can control at the same time (**8.3-SO4**). In this way, incidents in which many charging stations are switched on or off at the same time can be prevented. For server administrators, multifactor authentication (**8.5-SO3**) is required to further reduce the chances of someone gaining unauthorized access.

6.2 Protection from unauthorized access threats to the charging station

The measures to prevent unauthorized access to the charging station are similar to the ones for the CPO central system. Authentication should prevent attackers getting access. Authorization should limit the impact if they do get access.

A simple access control model can be used because each user group accesses a different interface:

- For authentication, role-based authentication (**8.5-SO4**) is used on all interfaces except the authentication terminal. Having users authenticate by role allows to keep account management simple. Charging stations cannot always rely on centralized authentication, as the connection to the central system may sometimes be lost. So, it would be technically challenging to use individual accounts.
- For authorization, least privileges are applied on each interface (**8.3-SO6**). Active access rights management is not required (and is sometimes not possible for the protocols used). It is not needed to set up new users on an interface or change their access rights, as only one user group is using each interface.

The authentication mechanism for EV drivers on the authentication terminal (**8.5-SO5**) is specified by the mobility service provider. A strong authentication mechanism is advisable, as the interface is used for financial transactions. But interoperability is usually the deciding factor, as EV drivers want to be able to charge at different CPOs.

To ensure that the authentication and authorization measures can provide security against sophisticated attackers (security level 3), the following supporting objectives are required:

- **Key and password management:** keys and credentials used for authentication should be regularly updated, to reduce the impact of them being compromised. Automated management over the WAN (**8.24-SO2**) makes is possible to update the keys efficiently. The key and password management process (**8.24-SO3**) makes sure there is a process to update them.
- **Hardening:** the charging station should be hardened by disabling unused services, so that there are no network services exposed without protection. Charging stations should be delivered and installed in a hardened configuration (**8.8-SO2**). The vulnerability management process (**8.8-SO3**) hardening is monitored and improved if needed.
- **Monitoring:** attempts to bypass the access control mechanisms should be monitored. The logging objective (**8.15-SO2**) allows failed and successful login attempts to be logged and collected by the central system. Clock synchronization allows making a reliable timeline of alerts (**8.17-SO2**). Processes should be established to detect and respond to these alerts (**8.16-SO1**).

6.3 Protection from exploits of software vulnerabilities

For all software exploits threats, hardening is used to prevent vulnerabilities. Patching is used to fix vulnerabilities on the CPO central system and the WAN interface on the charging station.

6.3.1 Protection for the CPO central system (T-EX1, T-EX2, T-EX3)

As the internet facing interfaces and server maintenance interface may be directly exposed to external attackers, protection against software exploits should be provided through hardening, patching, and malware protection.

Hardening should reduce the risk of exploits by disabling unused services and enabling security features. The vulnerability management process (**8.8-SO3**) should ensure that unused services are disabled to reduce the attack surface and hence the likelihood of vulnerabilities begin exposed. It should also ensure that security features on the hardware and software platform are enabled to reduce the impact of vulnerabilities. The central system should allow server administrators to perform the hardening (**8.8-SO1**).

If vulnerabilities are still found on the internet facing interfaces, they should be fixed through patching. Server administrators should be able to perform patching through the server maintenance interface (**8.19-SO1**). The vulnerability management process (**8.8-SO3**) ensures there is a structured process for patching.

Malware protection (**8.7-SO1**) should be used to detect and remove any payloads that get through the hardening and patching measures.

6.3.2 Protection on the WAN interface (T-EX4, T-EX5)

Protection against software exploits against the WAN is provided through hardening and patching.

Hardening is effective on the charging station because the functionality needed on each interface is usually simple. Charging stations should be delivered and installed with unneeded network services and functionality disabled and with security functions of the hardware and software platform enabled (**8.8-SO2**). The vulnerability management process (**8.8-SO3**) should monitor that the charging station stays hardened throughout their lifecycle.

Hardening the interfaces should provide security against at least protection against intentional violation using simple means with low resources, generic skills, and low motivation (security level 2). On most interfaces, this is considered sufficient protection, as they can only be accessed locally. So, the impact of an attack will be limited.

On the WAN interface additional security should be provided through patching. Efficient patching is made possible on the charging station through automated firmware management (**8.19-SO2**). Updates are, however, only required for the local controller in the charging station, the part that communicates with the CPO central system. For other parts, it may be only possible to perform firmware updates locally. Vulnerabilities on other interfaces may hence be difficult to patch. The vulnerability management process (**8.8-SO3**) ensures there is a process to perform security updates.

6.4 Protection from communication threats

The confidentiality and integrity of information on all untrusted networks is protected through cryptographic measures, both for the CPO central system (**8.20-SO1**) and for the charging station (**8.20-SO2**).

Communication is not required to be cryptographically protected on the local interfaces on the charging station (authentication terminal, electric vehicle, local maintenance, and EMS). An attacker would usually have to be physically present at these interfaces to compromise the communication. Communication on the charging plaza LAN and the connection to the EMS should be protected through tamper detection measures (**7.12-SO1** and **7.12-SO2**).

The availability of communication is protected by network segregation and resilience of the underlying network. Network segregation through firewalls is used on all interfaces of the CPO central system (**8.22-SO1**) and the WAN interface of the charging station (**8.22-SO2**), so that they are protected against denial-of-service attacks. Additionally, it is

assumed that the networks connected to the WAN, management portal, and market interfaces are sufficiently resilient (**8.21-SO1**, **8.21-SO2**), and that the charging functions can continue even when network communication is unavailable (**8.20-SO3**).

6.5 Protection from physical threats

Physical threats to the CPO central system are countered through data center security. For charging stations and plazas, tamper detection is provided against fraud, while the impact is limited through network segregation.

6.5.1 Physical threats to the CPO central systems (T-PH1)

Physical threats to the CPO central systems are countered by protecting the data center in which it is hosted using the physical security controls (**7.1**, **7.2**, **7.3**, **7.4**, **7.8**, **7.12**), see Section 5.3. If properly implemented, these controls should provide protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation (security level 3).

6.5.2 Physical threats to the charging station (T-PH2, T-PH3, T-PH4, T-PH5)

For the charging station, tamper detection allows to detect fraud. The impact of a physical compromises is limited through network measures.

Tamper protection should be provided first passively through the casing of the charging station or the cabinets in which charging plaza equipment is placed (**7.8-SO1, 7.8-SO2**). Cables to the EMS or within the charging station LAN should also be protected (**7.12-SO1**, **7.12-SO2**). Active detection should be provided by creating alarms for physical access to the casing or cabinets (**7.4-SO1, 7.4-SO1).** For detection to be effective the CPO must of course also have a process to react to the alarms (**7.4-SO2**).

Together the active and passive measures should counter the main physical threats (**T-PH2**, **T-PH3**, **T-PH4**) and provide protection against intentional violation using simple means with low resources, generic skills, and low motivation (security level 2).

This security level is acceptable as long as the threats only affect the charging stations that are physically attacked. To ensure that the rest of the EV charging infrastructure is not affected (**T-PH5**), network segregation is used to limit the impact (**8.22-SO3**).

6.6 Protection from supply chain threats

To prevent the firmware or software from being modified at the supplier (**T-SC1**), the developers and manufacturers of the EV charging infrastructure must protect their assets (**5.25**).

To prevent the firmware or software from being modified between the supplier and installation (**T-SC2**), the server software updates on the central systems and the automated firmware updates on the charging station are protected with a digital signature (**8.19-SO1, 8.19-SO2**).

Network segregation between the central system and the outside (**8.22-SO1**) and between the charging station and the central system (**8.22-SO2**) make it difficult for an attacker to reach the backdoor, even if they succeed in putting it into the firmware.

6.7 Protection from insider threats

Protection against insider threats is provided through access control, people control, and monitoring.

The risks of insider threats can be significantly reduced by separating roles through role-based access control for representatives, engineers, and server administrators (**8.3-SO3**). The largest group of insiders would be customer representatives. These only need limited access. They should for instance not be allowed to update the firmware or change security settings on a charging station. Engineers must have some more access, but they should not be allowed to change the centrals system software or settings. Switching commands should be limited to both user groups (**8.3-SO4)** to make sure that they cannot cause problems in the power grid. With these measures, only a small group of server administrators need privileged access to the central system. An account management process (**5.16**, **5.18**) is required to keep the access rights up to date when engineers and operators change roles or organizations.

People controls (**6.1**, **6.2**, **6.3**, **6.4**), such as screening and training, are important to prevent users misusing or abusing their privileges they have.

Monitoring and incident response process should be used to detect misuse or abuse and respond to it (**8.16-SO1**). Some unusual behavior by engineers, representatives, and server administrators may be detected with monitoring. And if there is an incident the security logs should allow to find out the cause, so that corrective measures can be taken.

To technically support the monitoring and incident response process, security events are logged locally and gathered in a SIEM system (**8.15-SO1, 8.15-SO2**). Clocks are synchronized to allow making a timeline of an incident (**8.17-SO1**, **8.17-SO2**). Engineers and administrators log in with individual user accounts (**8.5-SO2, 8.5-SO3**), so that actions can be traced to them. Requiring centralized access control on the local maintenance interface is not considered feasible yet. So, additional organizational requirements may be needed to monitor who has accessed it.

6.8 Protection from post exploitation threats

Protection against the post exploitation threats is provided through backups, monitoring, firmware and software signing, and network segregation.

6.8.1 Protection against loss of configuration (T-PE1)

The main measure to protect against loss of configurations (**T-PE1**) in the central system is to make backups of this system (**8.13-SO1**) following a backup process **(8.13-SO3)** and then restore the working configuration through server configuration management (**8.9-SO1**).

For the charging station to restore the configuration, it must be possible to restore a working configuration via automated configuration management (**8.9-SO2**). These technological controls must be enabled by a backup process (**8.13-SO2**)

6.8.2 Protection against software or firmware corruption (T-PE2)

To protect against software or firmware corruption (**T-PE2**), changes to the firmware are logged and can be sent to the SIEM system (**8.15-SO1**, **8.15-SO2** with **8.17-SO1**, **8.17-SO2** for clock synchronization), so that operators can detect unauthorized modifications (**8.16-SO1**). The software and firmware are moreover digitally signed (**8.19-SO1, 8.19-SO2**).

If an attacker would install a backdoor, it would be hard to reach because of the network segregation between the central systems and the outside (**8.22-SO1**) and between the central system and the charging station (**8.22-SO2**).

Annex A: Mapping of objectives to threats

To show that all technological security objectives in Section 5.4 are indeed needed to counter the threats, this annex maps them to the threats (Section 3) they are countering according to the rationale in Section 6.

A.1 Objectives for the CPO central system

The table below shows which threats the objectives for the CPO central system mitigate.

Objective	*Threats countered*
8.3-SO1 Least privileges on the WAN interface: The CPO central system enforces access control on the WAN, so that users on the interface can only access the functions they need.	• **T-UA1** Unauthorized access as a charging station on the WAN
8.3-SO2 Role separation on the market interface: The CPO central system enforces access control on the market interface with separate roles for mobility service providers, roaming platforms, and DSO systems, so that they can only access the functions they need for their role.	• **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface
8.3-SO3 Centrally managed, role-based access control for customer service representatives, engineers, and server administrators: The CPO central system enforces role-based access control for customer service representatives, engineers, and server administrators with individual user accounts managed on a central server.	• **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by server administrator

8.3-SO4 Restrictions on switching commands: The CPO central system does not allow engineers and customer representatives to switch charging on or off on many charging stations at the same time, for instance by limiting the number of switching commands per user per hour.	• **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal
8.3-SO5 Individual accounts for customers: The CPO central system support individual accounts for customer and enforces access control so that they can only access the functions they need.	• **T-UA5** Unauthorized access as a customer on the customer portal
8.5-SO1 Mutual authentication for the charging stations, mobility service provider, roaming platform and DSO systems: The CPO central system enforces mutual authentication with the charging stations, mobility service provider, roaming platform and DSO system. Devices on each side uniquely identify themselves and allow the other side to authenticate them. They only provide access after having authenticated the other side's identity	• **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface
8.5-SO2 Authentication with individual passwords for customers, customer service representatives, engineers, and server administrators: The CPO central system enforces mutual authentication for representatives, engineers, and server administrators. Representatives, engineers, and administrators use individual credentials. The login procedure is protected against known attacks.	• **T-UA3** Unauthorized access as a server administrator on the server maintenance interface
8.5-SO3 Multifactor authentication for server administrators on the server maintenance interface: The CPO central system enforces multifactor authentication	• **T-UA3** Unauthorized access as a server administrator on the server maintenance interface

for server administrators on the server maintenance interface with a login procedure that is protected against known attacks.	
8.7-SO1 Active malware protection in the CPO central system: Hosts in the CPO central system are actively protected against malware through, for instance, anti-virus software or application whitelisting software.	• **T-EX1** Exploit of a software vulnerability on the CPO central system on the WAN • **T-EX2** Exploit of a software vulnerability on the internet-facing interfaces • **T-EX3** Exploit of a software vulnerability on the server maintenance interface
8.8-SO1 Hardening over the local maintenance or server maintenance interface: Server administrators can harden hosts in the CPO central system over the server maintenance interface or from engineering workstations. They can disable unneeded functions to reduce the likelihood of vulnerabilities and allow to enable security functions available on the hardware and software platforms to reduce their possible impact.	• **T-UA1** Unauthorized access as a charging station on the WAN • **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface • **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface • **T-EX1** Exploit of a software vulnerability on the CPO central system on the WAN • **T-EX2** Exploit of a software vulnerability on the internet-facing interfaces • **T-EX3** Exploit of a software vulnerability on the server maintenance interface

8.9-SO1 Server configuration management: Server administrators can manage and monitor the configurations of software, services and networks of the CPO central system from the server maintenance interface.	• **T-PE1** Loss of configurations
8.13-SO1: Automated backups for CPO central system: The CPO central system supports making automated backups of the configurations and data.	• **T-PE1** Loss of configurations
8.15-SO1 Integration with SIEM system: The servers in the CPO central system log all relevant security events, such as access control events, and changes to the configuration and software. The servers can store the logs locally for forensic analysis. They can send them to a Security Information and Event Management (SIEM) system in a commonly supported format, so that they can be analyzed to detect incidents.	• **T-UA1** Unauthorized access as a charging station on the WAN • **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface • **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by server administrator • **T-PE2** Software or firmware corruption
8.17-SO1 Clock synchronization for the CPO central system: The CPO central system synchronizes time with a central source to have reliable timestamps for security events.	• **T-UA1** Unauthorized access as a charging station on the WAN • **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface

	• **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by server administrator • **T-PE2** Software or firmware corruption
8.19-SO1 Software updates over the server maintenance interface: Server administrators can update the software and firmware in the CPO central system over the server management interface or from engineering software. Hosts in the CPO central system check the authenticity of firmware or software before installation through digital signatures.	• **T-EX1** Exploit of a software vulnerability on the CPO central system on the WAN • **T-EX2** Exploit of a software vulnerability on the internet-facing interfaces • **T-EX3** Exploit of a software vulnerability on the server maintenance interface • **T-SC1** Software or firmware modification before installation • **T-PE2** Software or firmware corruption
8.20-SO1 Cryptographic protection of communication confidentiality and integrity on the WAN, management portal, market interface, and server maintenance interface: The CPO central system protects the integrity and confidentiality of communication on the WAN, management portal, market interface, and server maintenance interface using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.	• **T-CM1** Data modification on WAN • **T-CM2** Data disclosure on WAN • **T-CM4** Data modification on the internet facing interfaces • **T-CM5** Data disclosure on internet facing interfaces • **T-CM7** Data modification on the server maintenance interface • **T-CM8** Data disclosure on the server maintenance interface
8.22-SO1 Network segregation on the WAN, management portal, market interface, and server maintenance	• **T-SC1** Software or firmware modification before installation

interface: The CPO central system is segregated from other zones on the WAN, management portal, market interface, and server maintenance interface. Only normal connections are allowed through the network perimeter.	• **T-SC2** Hardware modification before installation • **T-CM3** Network denial-of-service attack on the WAN • **T-CM6** Network denial-of-service attack on the internet-facing interfaces • **T-CM9** Network denial-of-service attack on the server maintenance interface • **T-PE2** Software or firmware corruption
8.24-SO1 Server key and password management over the server maintenance interface: Server administrators can manage all passwords and keys used on the CPO central system server efficiently over the server maintenance interface.	• **T-UA1** Unauthorized access as a charging station on the WAN • **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface • **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface

A.2 Objectives for the charging station

The table below shows which threats the objectives for the charging station mitigate.

Objective	***Threats countered***
8.3-SO6 Least privileges on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces: The charging station or plaza enforces access control on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces, so	• **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface

that user group with access to the interface can only access the functions they need.	• **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface
8.5-SO4 Role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations: The CSMS, electric vehicle, engineers, EMS, and other charging stations identify to the charging station with information that allows the zone to determine its role. The zone authenticates the system's role and assigns it access rights based on the role. The charging station uniquely identifies itself to CSMS, EV driver, electric vehicle, and other charging stations, and allows the system to authenticate them.	• **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface
8.5-SO5 Authentication for EV drivers on the authentication terminal: The charging station enforces authentication for EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider.	• **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface
8.8-SO2 Hardened by default: The charging stations and charging plaza devices are delivered by the manufacturer in a hardened configuration. Unneeded functions are disabled to reduce the likelihood of vulnerabilities. Security functions on the hardware and software platforms are enabled to reduce the possible impact of vulnerabilities.	• **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface • **T-EX4** Exploit of a software vulnerability on the charging station on the WAN

	• **T-EX5** Exploit of a software vulnerability on local interfaces on the charging station • **T-PH2** Unauthorized physical access to a charging station • **T-PH3** Unauthorized access to a charging plaza LAN or local controller • **T-PH4** Unauthorized access as the EMS on the EMS interface • **T-PH5** Unauthorized access to the EV charging infrastructure from a compromised field location
8.9-SO2 Automated configuration management: The charging station can be restored from a backed-up configuration automatically by the CPO central system.	• **T-PE1** Loss of configurations
8.15-SO2 Collecting security events from the charging station through the CPO central system: The charging station logs all relevant security events locally and sends selected events to the CPO central system, so that they can be analyzed to detect incidents.	• **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by server administrator • **T-PE2** Software or firmware corruption
8.17-SO2 Clock synchronization for the charging station: The charging station or plaza synchronizes time with a central source	• **T-UA5** Unauthorized access as the CSMS

to have reliable timestamps for security events.	• **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by server administrator • **T-PE2** Software or firmware corruption
8.19-SO2 Automated firmware management for local controllers: The software and firmware on the local controller in the charging station or plaza can be updated through remote access from the CPO central system. The local controller can check the authenticity of firmware through digital signatures.	• **T-SC1** Software or firmware modification before installation • **T-PE2** Software or firmware corruption
8.20-SO2 Cryptographic protection of communication confidentiality and integrity on the WAN interface: The charging station protects the integrity and confidentiality of communication on the WAN interfaces using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.	• **T-CM1** Data modification on WAN • **T-CM2** Data disclosure on WAN
8.20-SO3 Resilience of charging functions against denial-of-service attacks on the WAN: The charging station shields charging functions from denial-of-service attacks on the WAN interface, so that these functions	• **T-CM3** Network denial-of-service attack on the WAN

keep working if the device is flooded with data or malformed messages	
8.22-SO2 Network segregation on the charging station WAN: The charging station is segregated from other zones on the WAN interface. Only normal connections are allowed through the network perimeter.	• **T-CM3** Network denial-of-service attack on the WAN • **T-SC1** Software or firmware modification before installation • **T-SC2** Hardware modification before installation • **T-PE2** Software or firmware corruption
8.24-SO2 Automated key and password management over the WAN: All passwords and keys used in the charging station can be updated automatically through remote access from the CPO central system.	• **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface

A.3 Objectives for the operational environment

The table below shows which threats the objectives for the operational environment mitigate.

Objective	***Threats countered***
8.8-SO3 Vulnerability management process: The charge point operator manages vulnerabilities in the system by: • disabling unused ports, services, user accounts and functions to reduce the likelihood of vulnerabilities • monitoring vulnerabilities in the system's software and firmware, assessing the risks of the	• **T-UA1** Unauthorized access as a charging station on the WAN • **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface

vulnerabilities, and mitigating the high-risk vulnerabilities, for instance by applying security updates • limiting the impact of vulnerabilities by enabling the security features on the hardware and software platforms used	• **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface • **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface • **T-EX1** Exploit of a software vulnerability on the CPO central system on the WAN • **T-EX2** Exploit of a software vulnerability on the internet-facing interfaces • **T-EX3** Exploit of a software vulnerability on the server maintenance interface • **T-EX4** Exploit of a software vulnerability on the charging station on the WAN • **T-EX5** Exploit of a software vulnerability on local interfaces on the charging station
8.13-SO2 Backup process for charging stations configurations: The charge point operator has a process to back up the charging station and plaza configurations on the CPO central system. Older versions of the configurations are kept, so that it is possible to revert to them in case of issues.	• **T-PE1** Loss of configurations

8.13-SO3 Backup process for the CPO central system: The charge point operator has an automated process to back up the data and configurations on the CPO central systems (including the charging station and plaza configurations stored there according to 8.13-SO2).	• **T-PE1** Loss of configurations
8.16-SO1: Security monitoring and incident response: The charge point operator monitors and responds to security events on the CPO central system and the charging stations and plazas. They gather security logs from the devices centrally, for instance, in a SIEM. They establish procedures, use cases, and rules to find incidents in the logs. And they establish a process for responding to the incidents and minimizing the impact.	• **T-UA1** Unauthorized access as a charging station on the WAN • **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface • **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface • **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by server administrator • **T-PE2** Software or firmware corruption

8.21-SO1 Resilience against denial-of-service attacks on the WAN: The wide-area network (WAN) is resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation (security level 2). The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.	• **T-CM3** Network denial-of-service attack on the WAN interface
8.21-SO2 Resilience against denial-of-service attacks on the internet facing interfaces: The internet connections for the management portal and market interfaces are resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation (security level 2). The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.	• **T-CM6** Network denial-of-service attack on the internet-facing interfaces
8.22-SO3 No communication between charging stations on the WAN: There is no direct communication between charging stations on the WAN interface. The charging stations can only communicate with CPO central system.	• **T-PH2** Unauthorized physical access to a charging station • **T-PH3** Unauthorized access to a charging plaza LAN or local controller • **T-PH4** Unauthorized access as the EMS on the EMS interface • **T-PH5** Unauthorized access to the EV charging infrastructure from a compromised field location
8.24-SO3 Key and password management process: The charge point operator manages the keys and passwords of the devices, so	• **T-UA1** Unauthorized access as a charging station on the WAN

that they are properly protected and can be updated when needed.	• **T-UA2** Unauthorized access as an engineer or customer service representative on the management portal • **T-UA3** Unauthorized access as a server administrator on the server maintenance interface • **T-UA4** Unauthorized access as a DSO system, roaming platform or mobility service provider on the market interface • **T-UA5** Unauthorized access as the CSMS • **T-UA6** Unauthorized access as an EV driver on the authentication terminal interface • **T-UA7** Unauthorized access as an electric vehicle in the electric vehicle interface • **T-UA8** Unauthorized access as an engineer on the local maintenance interface

Glossary

AC	Alternating Current
APN	Access Point Name
CPO	Charge Point Operator
CSMS	Charging Station Management System
CVSS	Common Vulnerability Scoring System
DC	Direct Current
DSO	Distribution System Operator
EMS	Energy Management System
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
IACS	Industrial Automation and Control System
LAN	Local Area Network
LTE	Long-Term Evolution
SIEM	Security Incident and Event Management
SSH	Secure Shell Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
VPN	Virtual Private Network
WAN	Wide Area Network

References

[1] ENCS, EV-211-2022: IEC 62443 security requirements for EV charging infrastructure, 2022.

[2] ENCS, EV-201-2022: Security architecture for EV charging infrastructure, 2022.

[3] ISA/IEC, "IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels".

[4] ISO / IEC, "ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls," 2022.

[5] ENCS, EV-311-2022: IEC 62443 requirements for EV charging stations, 2022.

[6] ENCS, EV-301-2022: Security requirements for procuring EV charging stations, 2022.

[7] ISA / IEC, "ISA 62443-4-2 Security for industrial automation and control systems - Technical security requirements for IACS components, Draft 3, Edit 4," January 12 ,2017.

[8] Elaad NL, EV Related Protocol Study, 2016.

[9] Elaad NL, Public Key Infrastructure for ISO 15118 - Freedom of choice for consumers & an open access market, 2022.

[10] IEC, IEC 62196-2:2022 Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility requirements for AC pin and contact-tube accessories, 2022.

[11] IEC, IEC 62196-3:2022 Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 3: Dimensional compatibility requirements for DC and AC/DC pin and contact-tube vehicle couplers.

[12] M. A. Sayed, M. Ghafouri, M. Debbabi and C. Assi, "Dynamic Load Altering EV Attacks Against Power Grid Frequency Control," *IEEE Power & Energy Society General Meeting (PESGM),* pp. 1-5, 2022.

[13] S. Soltan, P. Mittal and H. V. Poor, "BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid," *27th USENIX Security Symposium (USENIX Security 18),* pp. 15-32, 2018.

[14] SANS and E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case," 2016.