EV-211-2022

Security requirements from IEC 62443 for EV charging infrastructure

Version 2022v0.1

3 January 2023

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 components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/resources/security-requirements/):

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	Versions	Description
3 January 2023	2022v0.1	Initial draft based on the security architecture EV-111-2022 with ISO 27002:2022 objectives

Table of Contents

Version history 3

1 Introduction 5

1.1 Relation to other documents 6

2 System description 7

2.1 Intended use of the system 7

2.1.1 Components in the system 8

2.1.2 Users of the system 8

2.2 Intended operational environment 9

2.2.1 Interfaces 9

2.2.2 Physical locations 11

2.3 Zoning model 11

2.4 Access control policy 11

3 Security requirements for the CPO central system 14

3.1 Requirements selected from IEC 62443-3-3 19

3.2 Rationale for the requirements 27

4 Security requirements for charging stations and charging plazas 31

4.1 Requirements selected from IEC 62443-3-3 35

4.2 Rationale for the requirements 41

References 44

1 Introduction

This document gives security requirements that Charge Point Operators (CPO) can use when procuring new EV charging infrastructures from a system integrator, or internally when designing and implementing an EV charging infrastructure. The requirements are based on the IEC 62443-3-3 standard [1].

Charge Point Operators (CPOs) are controlling increasingly more electrical load. To support the rapid growth in electric vehicles (EVs), hundreds of thousands of charging stations are being placed throughout Europe, most of them being remotely controlled by CPOs. In this way, larger CPOs are already controlling hundreds of megawatts of demand, comparable to a large gas power plant. And the controlled load will only grow in the future.

But this also means that CPOs are a target for cyber-attacks. If attackers gain control of a CPO's infrastructure, they could switch the power on the connected charging stations. Such an attack would not only hurt the CPOs themselves. The switching could also cause grid imbalances in the supply and demand for electricity and, possibly, power outages. If smart charging is used, attackers may force charging stations to use more power than assigned to them, which could damage transformers and power lines.

Making sure the EV charging infrastructure is secure is, hence, critical. This document provides a recommended set of security requirements at system level that allows the major security threats to be mitigated with current technology. It provides guidance on what technical measures to take to secure EV charging infrastructures.

The requirements are based on the IEC 62443 standard. They have been selected from *IEC 62443-3-3: System security requirements and security* [1].

The requirements have been designed to allow certification based on the new certification schemes being developed for IEC 62443. Together with the threat analysis for EV charging infrastructure in [2] they form a profile for IEC 62443 (following the rules in [3]).

When charge point operators use the technical requirements in this document, it is recommended to also require that any software supplier complies full to **IEC 62443-4-1** [4] and any system integrator complies fully with **IEC 62443-2-4** [5] both at **maturity level at least 3**. Doing so ensures that the supplier has secure development processes, so that it can correctly and consistently implement the requirements.

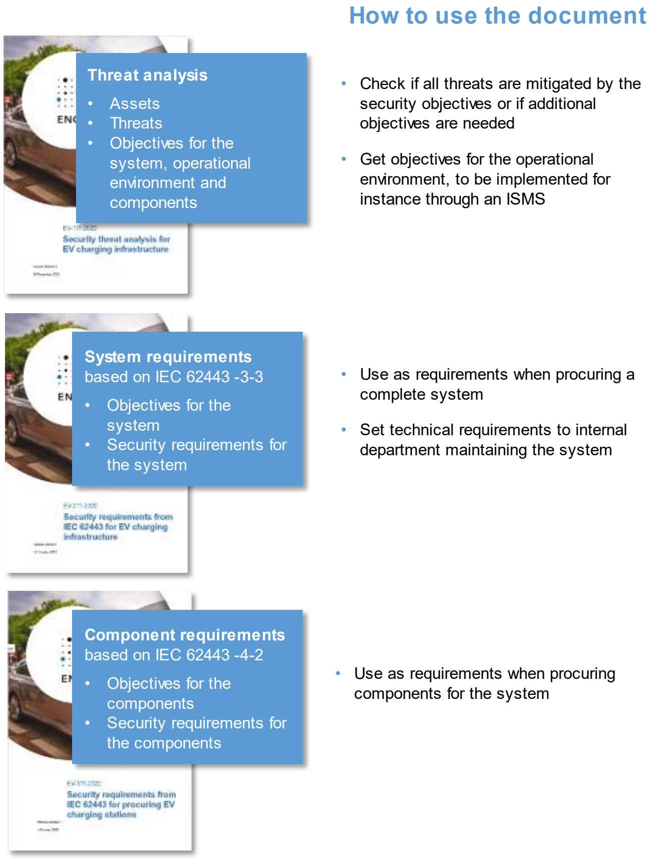
The scope of application of the standards should cover the software developed for the charging infrastructure and all systems the supplier is responsible for.

1.1 Relation to other documents

This document is part of a larger series on EV charging infrastructure security, as shown in Figure 1. The series starts with a threat analysis [2] that determines security objectives to counter the threats posed to the assets in a typical EV charging infrastructure. The objectives are split into objectives for the system and operational environment. The objectives for the system are the basis for the security requirements in this document.

The objectives for the operational environment should be implemented by CPOs outside of the system to operate it securely. Many CPOs will meet these security objectives through their information security management system. Hence, the objectives are linked to controls from the ISO/IEC 27002:2022 standard [6]. They include organizational, people, physical, and technological objectives.

From the security objectives for the system, the component requirements document [7] derives security objectives for charging stations. The objectives are chosen so that a charging station meeting the component objectives can be easily integrated into a system meeting the system objectives. Based on these component objectives, it selects security requirements for charging stations from the IEC 62443-4-2 standards.



How to use the document

Threat analysis
- Assets
- Threats
- Objectives for the system, operational environment and components

- Check if all threats are mitigated by the security objectives or if additional objectives are needed
- Get objectives for the operational environment, to be implemented for instance through an ISMS

System requirements based on IEC 62443 -3-3
- Objectives for the system
- Security requirements for the system

- Use as requirements when procuring a complete system
- Set technical requirements to internal department maintaining the system

Component requirements based on IEC 62443 -4-2
- Objectives for the components
- Security requirements for the components

- Use as requirements when procuring components for the system

Security threat analysis for EV charging infrastructure
Security requirements from IEC 62443 for EV charging infrastructure
Security requirements from IEC 62443 for procuring EV charging stations

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

2 System description

To effectively use the security requirements, it is important to know the assumptions they make about how the EV charging infrastructure works. This includes the intended use of the system, its operational environment, and the zoning model and access control model used in the threat analysis [2] to set security objectives.

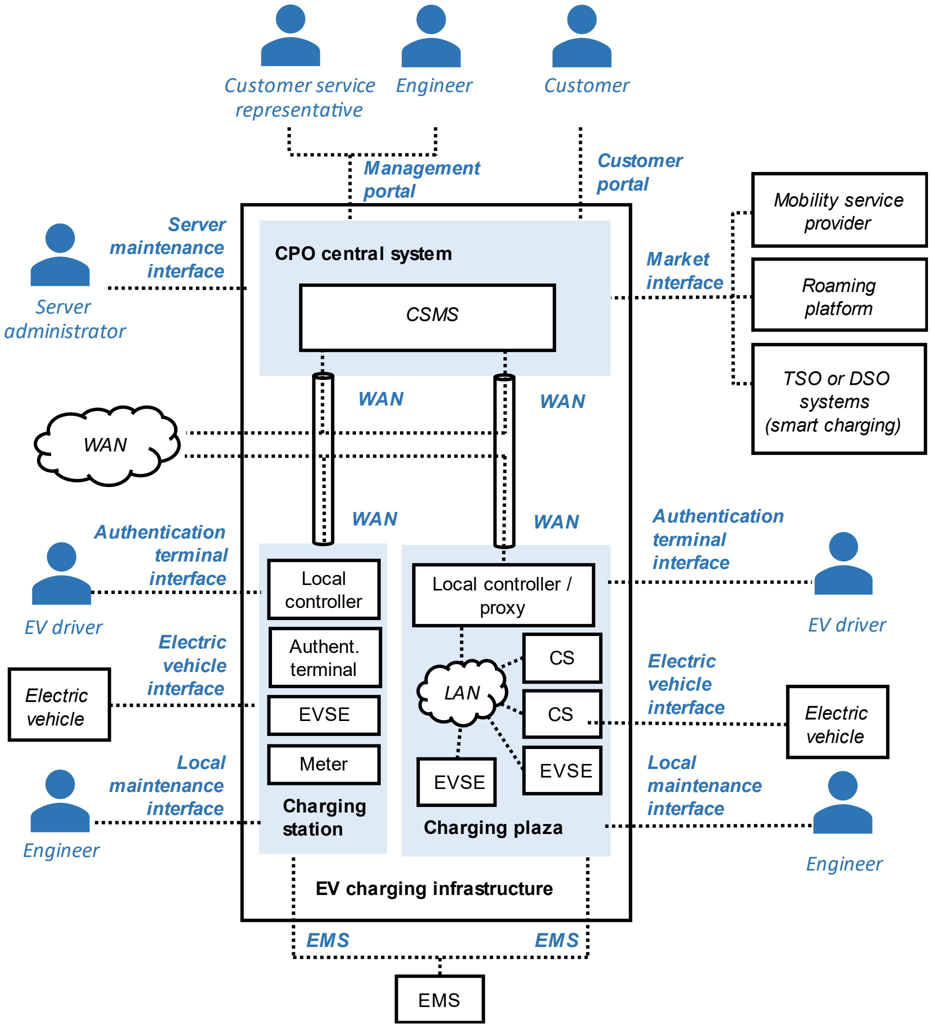


Figure 2: Reference architecture for the EV charging infrastructure, showing its users and interfaces.

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 can 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 the central system.
- **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 to 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 Zoning model

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.

2.4 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	WAN

	• Optional: Get charging profiles	
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 • Update the firmware • Analyze the operational logs	Local maintenance
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

3 Security requirements for the CPO central system

The threat analysis [2] sets security objectives to mitigate the threats to the EV charging infrastructure previously described. These objectives refine the technological security controls in ISO/IEC 27002:2022 [6]. We now break down the objectives into more detailed requirements from IEC 62443-3-3 [1] that a system integrator or department building or maintaining an EV charging infrastructure can follow.

This section gives the security requirements for the **CPO central system**. Table 3 gives for each security objective the requirements selected to cover them. Section 3.1 gives the full list of requirements with domain-specific adaptations and additional guidance. Section 3.2 gives the rationale for selecting them. Requirements for charging stations and charging plazas are given in Section 4.

As mentioned in the introduction, it is recommended that besides the technological requirements selected here, charge point operators also require that any software supplier complies full to **IEC 62443-4-1** [4] and any system integrator complies fully with **IEC 62443-2-4** [5] both at **maturity level at least 2**. From 2024 onwards, it is recommended to require maturity level at least 3 for IEC 62443-4-1.

For IEC 62443-2-4 a system integrator can only reach security level 3 if it performs projects following all requirements in the standard. CPOs can hence ask for security level 3 when they do a second project with a supplier. But it may not always be feasible for a first project.

Table 3: Selection of security requirements from IEC 62443-3-3 to meet the security objectives for the CPO central system.

Security Objective	***IEC 62443-3-3 requirements***
8.3 Information access restriction	
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.	• SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)
8.3-SO2 Role separation on the market interface: The CPO central system enforces	• SR2.1 Authorization enforcement

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.	• SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)
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.	• SR1.3 Account management • SR1.3 RE1 Unified account management • SR1.4 Identifier management • SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • SR2.1 RE2 Permission mapping to roles
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.	• SR2.1 Authorization enforcement
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.	• SR1.3 Account management • SR1.4 Identifier management • SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)
8.5 Secure authentication	
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	• SR1.2 Software process and device identification and authentication • SR1.9 Strength of public key authentication • SR2.6 Remote session termination

side uniquely identify themselves and allow the other side to authenticate them. They only provide access after having authenticated the other side's identity.	• SR4.3 Use of cryptography
8.5-SO2 Authentication with individual passwords for 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.	• SR1.1 Human user identification and authentication • SR1.1 RE1 Unique identification and authentication • SR1.7 Strength of password-based authentication • SR1.7 RE1 Password generation and lifetime restriction for human users • SR1.9 Strength of public key authentication • SR1.10 Authenticator feedback • SR1.11 Unsuccessful login attempts • SR2.5 Session lock • SR2.6 Remote session termination • SR4.3 Use of cryptography
8.5-SO3 Multifactor authentication for server administrators on 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.	• SR1.1 RE2 Multifactor authentication for untrusted networks
8.7 Protection against malware	
8.7-SO1 Active malware protection in the CPO central system: Hosts in the CPO central system, are actively protected against malware, for instance through anti-virus software or application whitelisting software.	• SR3.2 Malicious code protection

8.8 Management of technical vulnerabilities	
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.	• SR 3.2 Malicious code protection • SR7.7 Least functionality
8.9 Configuration management	
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.	• SR7.3 Control system backup • SR7.4 Control system recovery and reconstitution
8.13 Information backup	
8.13-SO1: Automated backups for the CPO central system: The CPO central system supports making automated backups of the configurations and data.	• SR7.3 RE2 Backup automation
8.15 Logging	
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)	• SR2.8 Auditable events • SR2.8 RE1 Centrally managed, system-wide audit trail • SR2.9 Audit storage capacity • SR2.10 Response to audit processing failures • SR3.9 Protection of audit information

system in a commonly supported format, so that they can be analyzed to detect incidents.	• SR6.1 Audit log accessibility • SR6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
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.	• SR2.11 Timestamps • SR2.11 RE1 Internal time synchronization • SR2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
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.	• SR1.8 Strength of public key authentication • SR1.9 Strength of public key authentication • SR3.4 Software and information integrity • SR4.3 Use of cryptography
8.20 Network security	
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.	• SR1.9 Strength of public key authentication • SR3.1 Communication integrity • SR 3.1 RE1 Cryptographic integrity protection • SR3.8 Session integrity • SR4.1 Information confidentiality • SR4.1 RE1 Protection of confidentiality at rest or in transit via untrusted networks

8.22 Segregation of networks	
8.22-SO1 Logical 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. The communication load can be controlled at the perimeter.	• SR5.1 Network segmentation • SR5.2 Zone boundary protection • SR5.2 RE1 Deny by default, allow by exception • SR 7.1 Denial of service protection • SR 7.1 RE1 Manage communication loads
8.24 Use of cryptography	
8.24-SO1 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.	• SR1.5 Authenticator management • SR1.8 Public key infrastructure certificates • SR1.9 Strength of public key authentication • SR4.3 Use of cryptography

3.1 Requirements selected from IEC 62443-3-3

Table 4 below lists all requirements from the IEC 62443-3-3 standard on *System security requirements and security levels* [1] that were selected for the CPO central system in Table 3.

Some of the requirements have been adapted to the specific application domain of EV charging to be able to meet the security objectives. The adaptations are prescriptive. To be compliant with the requirements in this document all adaptations must be followed.

The adaptations should be read as a specification of the original requirement. The original requirement remains in force. The adaptation limits the options for meeting the requirements to ensure that the implementation meets the security objectives.

Besides the adaptations, supplemental guidance is included for some requirements. The guidance is non-binding. It clarifies the requirements, gives examples, or provides recommendations on implementing the requirement. For some requirements, it provides a link to the IEC 62351 standard.

Following the convention in IEC 62443-3-3, the adaptations and supplemental guidance use the term *'control system'* for the CPO central system zone.

Table 4: Full list of requirements selected from IEC 62443-3-3 for the CPO central system.

IEC identifier	Name	Objective
SR1.1	**Human user identification and authentication**	8.5-SO2
SR1.1 RE 1	**Unique identification and authentication**	8.5-SO2
SR1.1 RE2	**Multifactor authentication for untrusted networks** *Adaptation:* The control system shall provide multifactor authentication for server administrators on the server maintenance interface.	8.5-SO3
SR1.2	**Software process and device identification and authentication** *Adaptation:* The control system shall provide the capability to identify and authenticate the role of the charging stations, mobility service provider, roaming platform, and DSO systems. This capability shall enforce such identification and authentication on all interfaces which provide access to the components to support least privilege in accordance with applicable security policies and procedures. Devices in the control system uniquely identify themselves to the CPO central system and allow the system to authenticate them. *Supplemental guidance:* When validating a certificate, the role of the user can be checked through the subject name, common name, or distinguished name.	8.5-SO1
SR1.3	**Account management**	8.3-SO3 8.3-SO5
SR1.3 RE1	**Unified account management**	8.3-SO3

IEC identifier	Name	Objective
	Adaptation: The control system shall provide the capability to be integrated into a central system for managing the accounts for engineers. The component shall assign an account to a role based on information from the central system. *Supplemental guidance:* The central system can check a representative's, server administrator's or engineer's access rights using different technologies. CPOs should choose a method that works with their existing systems.	
SR1.4	**Identifier management**	8.3-SO3 8.3-SO5
SR1.5	**Authenticator management** *Adaptation:* The control system shall provide the capability to update all authenticators from the central maintenance system over the WAN interface. It shall be possible to update them without support from the supplier. The confidentiality and integrity of the authenticators shall be protected during changes. The control system shall at least provide the capability to protect passwords from unauthorized disclosure by storing them salted and hashed. *Supplemental guidance:* The adaptation only concerns point c) and part of point d) of the original requirement. The rest of the requirement stays in force without adaptation. For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.	8.5-SO2 8.24-SO1
SR1.7	**Strength of password-based authentication**	8.5-SO2

IEC identifier	Name	Objective
SR1.7 RE1	**Password generation and lifetime restriction for human users**	8.5-SO2
SR1.8	**Public key infrastructure certificates**	8.19-SO1 8.24-SO1
SR1.9	**Strength of public key authentication**	8.5-SO1 8.5-SO2 8.19-SO1 8.20-SO1 8.24-SO1
SR1.10	**Authenticator feedback**	8.5-SO2
SR1.11	**Unsuccessful login attempts**	8.5-SO2
SR2.1	**Authorization enforcement** *Adaptation:* The control system shall be able to restrict how many charging stations a user can control in a time period. *Supplemental guidance:* The restrictions should at least ensure that users cannot switch charging on or off on many charging stations at the same time. The control system should limit to how many charging stations a switching command can be sent and how many commands can be sent per hour.	8.3-SO1 8.3-SO2 8.3-SO3 8.3-SO4 8.3-SO5
SR2.1 RE1	**Authorization enforcement for all users** *Adaptation:* The control system shall provide the capability to implement the access control policy described in Table 1 in Section 2.4.	8.3-SO1 8.3-SO2 8.3-SO3 8.3-SO5

IEC identifier	Name	Objective
SR2.1 RE2	**Permission mapping to roles**	8.3-SO3
SR2.5	**Session lock**	8.5-SO2
SR2.6	**Remote session termination**	8.5-SO1 8.5-SO2
SR2.8	**Auditable events**	8.15-SO1
SR2.8 RE 1	**Centrally managed, system-wide audit trail**	8.15-SO1
SR2.9	**Audit storage capacity**	8.15-SO1
SR2.10	**Response to audit processing failures**	8.15-SO1
SR2.11	**Timestamps**	8.17-SO1
SR2.11 RE1	**Internal time synchronization**	8.17-SO1
SR2.11 RE2	**Protection of time source integrity**	8.17-SO1
SR3.1	**Communication integrity**	8.20-SO1
SR3.1 RE1	**Cryptographic integrity protection** *Adaptation:* The control system shall provide the capability to verify the authenticity of information received on the WAN, management portal, market interface, and server maintenance interfaces using cryptographic methods.	8.20-SO1
SR3.2	**Malicious code protection** *Adaptation:* Hosts running commercial off-the-shelf operating systems shall have the capability to actively detect and respond to malware.	8.7-SO1 8.8-SO1

IEC identifier	Name	Objective
	All hosts shall allow security features available on the hardware and software platforms to be enabled. Server administrators shall be able to manage malware detection and response and the security features from the server maintenance interface. *Supplemental guidance:* Detection and response to malware may for instance be provided through anti-virus software, endpoint protection, or application whitelisting. It is recommended to use the following hardware features when they are supported: • *No-Execute (NX) / Write-xor-execute (W^R):* A Memory Protection Unit (MPU) or Memory Management Unit (MMU) shall be used to mark code regions as read-only and data sections as non-executable. • *Address Space Layout Randomization (ASLR):* A Memory Management Unit (MMU) shall be used to load data and code at different memory addresses every time an application is run. The software running on the device must be compiled to use the hardware features. The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR. At the operating system layer, user's access to filesystems should be minimized, and processes should be run with minimum privileges. Host-based firewalls should be enabled.	
SR 3.4	**Software and information integrity**	8.19-SO1
SR 3.8	**Session integrity**	8.20-SO1

IEC identifier	Name	Objective
SR 3.9	**Protection of audit information**	8.15-SO1
SR 4.1	**Information confidentiality**	8.20-SO1
SR 4.1 RE1	**Protection of confidentiality at rest or in transit via untrusted networks** *Adaptation:* Components shall support the protection of the confidentiality of information in transit on the WAN, management portal, market interface, and server maintenance interfaces using encryption. Information at rest may be protected by access control mechanisms and physical protection. Cryptographic protection is not required for the information at rest.	8.20-SO1
SR 4.1 RE2	**Protection of confidentiality across zone boundaries**	8.20-SO1
SR 4.3	**Use of cryptography** *Supplemental guidance:* Guidance on cryptographic algorithms and key lengths is given in: • the ANSSI selection guide for cryptographic algorithms [12] and rules and recommendations on the choice and parameters of cryptographic algorithms [13] • the BSI technical guideline *Cryptographic Mechanisms: Recommendations and Key Lengths* [14] • the ECRYPT – *Algorithms, Key Size, and Protocols Report* [15] • the NIST *Recommendation for key management* [16]	8.5-SO1 8.5-SO2 8.19-SO1 8.24-SO1

IEC identifier	Name	Objective
	The latest version of these reports should be followed. Algorithms and key sizes should be used that are recommended for new systems at the time of deployment, and preferably also for the full lifetime of the product. A dedicated cryptographic (pseudo-)random number generator should be used to generate random numbers for all security functions.	
SR5.1	**Network segmentation**	8.22-SO1
SR 5.2	**Zone boundary protection**	8.22-SO1
SR 5.2 RE 1	**Deny by default, allow by exception**	8.22-SO1
SR 6.1	**Audit log accessibility**	8.15-SO1
SR 6.1 RE 1	**Programmatic access to audit logs** *Supplemental guidance:* The control system shall provide the capability to send the audit records using the syslog communication protocol in a commonly used format, so that they can be easily imported into a SIEM system without the need for a customized parser.	8.15-SO1
SR 7.1	**Denial of service protection**	8.22-SO1
SR 7.1 RE1	**Manage communication loads**	8.22-SO1
SR 7.3	**Control system backup** *Adaptation:* The control system supports making automated backups of all configurations and data on the system.	8.9-SO1

IEC identifier	Name	Objective
SR7.3 RE2	**Backup automation**	8.13-SO1
SR 7.4	**Control system recovery and reconstitution**	8.9-SO1
SR 7.7	**Least functionality**	8.8-SO1

3.2 Rationale for the requirements

Below a rationale is provided for the requirements selected in Section 3.1 by showing that they cover the security objectives for the CPO central system (As mentioned in the introduction, it is recommended that besides the technological requirements selected here, charge point operators also require that any software supplier complies full to **IEC 62443-4-1** and any system integrator complies fully with **IEC 62443-2-4** both at **maturity level at least 2**. From 2024 onwards, it is recommended to require maturity level at least 3 for IEC 62443-4-1.

For IEC 62443-2-4 a system integrator can only reach security level 3 if it performs projects following all requirements in the standard. CPOs can hence ask for security level 3 when they do a second project with a supplier. But it may not always be feasible for a first project.).

8.3-SO1 Least privileges on the WAN interface

Authorization for all users is covered by *SR2.1, SR2.1 RE1*. Requirement *SR 2.1 RE1* is adapted to reference the access control policy in Section 0.

8.3-SO2 Role separation on the market interface

General authorization for software process users is covered by *SR 2.1* and *SR 2.1 RE1.* Requirement *SR 2.1 RE1* is adapted to reference the access control policy in Section 0.

No requirements on account management are included, as there may not be a clear account associated with the access if, for instance, a VPN is used.

8.3-SO3 Centrally managed, role-based access control for customer service representatives, engineers, and server administrators

Authorization is covered by *SR 2.1* and *SR 2.1 RE1*. Requirement *SR 2.1 RE1* is adapted to reference the access control policy in Section 0. Requirement *SR 2.1 RE2* is included to allow role-based access control

Central account management is covered by requirements *SR 1.3, SR 1.3 RE1* and *SR 1.4*. The requirement *SR 1.3 RE1* is adapted to clarify how unified account management should be implemented to meet the objective. In particular, it is specified that roles are assigned to users on the central system, not on the device itself. Managing roles on the device would create a significant administrative burden. Also, a requirement for a fallback system is included in case the central system cannot be reached.

8.3-SO4 Restrictions on switching commands

Through authorization enforcement (*SR2.1*), it is ensured that engineers are not authorized to switch many charging stations at the same time.

8.3-SO5 Individual accounts for customers

The individual accounts requirement is covered by account and identification management (*SR1.3, SR1.4*). Authorization for all users is covered by *SR2.1, SR2.1 RE1*.

8.5-SO1 Mutual authentication for the charging stations, mobility service provider, roaming platform and DSO systems

Authentication is covered by requirement *SR1.2*. The requirement is adapted to include role-based authentication for the charging stations, mobility service provider, roaming platform, and DSO systems. Requirement *SR 1.2* asks that the identification and authentication is done in accordance with applicable security policies and procedures.

Strong cryptographic keys and algorithms for the authentication are ensured by requirements *SR1.9* and *SR4.3*. Remote session termination is (*SR 2.6*.) is included to reduce the risk that authentication is bypassed by compromising a session.

8.5-SO2 Authentication with individual passwords for representatives, engineers, and server administrators

Authentication with individual user accounts and passwords is ensured by requirements *SR1.1* and *SR1.1 RE1*.

The login procedure is protected against known attacks as follows. Against brute-force attempts, requirement *SR1.11* ensures access can be blocked after several unsuccessful login attempts and requirement *SR1.10* ensures no information is leaked during the authentication process, while *SR1.7* and *SR1.7 RE1* allow enforcing secure passwords. Requirement *SR1.7 RE1* protects against passwords leaking by allowing to limit their lifetime. Requirements *SR2.5* and *SR2.6* protect against hijacking a user's session. And requirements *SR1.9*, *SR4.3* protect against cryptographic attacks.

Requirement *SR 1.5* protects against attackers getting passwords from a compromised device. The requirement is adapted to require passwords to be stored salted and hashed. Salting and hashing provide an effective method to still protect the passwords.

8.5-SO3 Multifactor authentication for server administrators on server maintenance interface

On top of the requirements defined for objective 8.5-SO2, multifactor authentication is enforced through requirement *SR1.1 RE2*.

8.7-SO1 Active malware protection in the CPO central system

Requirement *SR3.2* ensures the protection against malicious code. The requirement is adapted to clarify that active malware protection must be included in this protection.

8.8-SO1 Hardening over the local maintenance or server maintenance interface

Disabling unneeded functions is covered by requirement *SR 7.7.*

Enabling security functions on the hardware and software platforms is covered by requirement *SR 3.2* on malicious code protection. The requirement is adapted to clarify the measures against malicious code that are at least required.

8.9-SO1 Server configuration management

Restoration from a backed-up configuration is covered by requirement *SR 7.3*, *SR 7.4.*

8.13-SO1: Automated backups for CPO central system

Automated backups are covered by the requirement *SR7.3 RE2.*

8.15-SO1 Integration with SIEM system

Logging security events is covered by requirement *SR2.8* and *SR2.8 RE1* covers the central management of the logs. Sending the logs to the SIEM system is covered by requirements *SR6.1* and *SR6.1 RE1*. The addition to *SR6.1 RE1* is included to ensure that the logs can be sent using syslog in a format supported by most SIEM systems.

Protection of the security logs is covered by requirements *SR2.10* and *SR3.9*. Requirement *SR2.9* ensures that there is enough storage capacity on the device for the logs.

8.17-SO1 Clock synchronization for the CPO central system

Time synchronization is covered by requirements *SR2.11* and *SR2.11 RE1*. Requirement *CR2.11 RE2* ensures that the integrity of the time source is protected.

8.19-SO1 Software updates over the server maintenance interface

No requirements are included to explicitly allow remote software updates. These are requirements for components rather than for the system. Hence, they are not part of IEC 62443-3-3.

Integrity of software and firmware are covered by *SR 3.4*. Requirement *SR 1.8* ensures that the system can be integrated into a PKI for the certificates needed to verify the signature. Requirements *SR 1.9* and *SR 4.3* ensure the strength of the cryptography used for the signatures.

8.20-SO1 Cryptographic protection of communication confidentiality and integrity on the WAN, management portal, market interface, and server maintenance interface

Protecting the confidentiality of the information is covered by requirement *SR 4.1* and *SR 4.1 RE1*. The integrity of the communication is covered by *SR 3.1*, *SR 3.1 RE1*, and *SR 3.8*. Requirements *SR 1.9* ensures that strong cryptography is used to protect communication.

8.22-SO1 Logical network segregation on the WAN, management portal, market interface, and server maintenance interface

Network segregation is ensured by requirement *SR5.1*.

Requirements *SR5.2* and *SR5.2 RE1* ensure that there is protection between different security zones, and only allowed traffic can go through.

Protection against denial-of-service attacks on the WAN is achieved by requirements *SR 7.1* and *SR 7.1 RE1*.

8.24-SO1 Key and password management over the server maintenance interface

Remote updates of keys and credentials are covered by requirements *SR 1.5.* The requirement is adapted to ask for remote key updates.

Requirement *SR1.8* allows a root certificate from the CPO to be installed, so that it can be integrated in their PKI. Requirements *SR1.9* and *SR4.3* ensure the strength of the cryptography used for the certificates.

4 Security requirements for charging stations and charging plazas

After the requirements for the CPO central system, we now select requirements from IEC 62443-3-3 [1] to meet the security objectives for the **charging stations and charging plazas**, as set in the threat analysis [2]. The approach is the same as for the CPO central system in Section 3. We give the list of requirements from IEC 62443-3-3 in Section 4.1, and then a rationale for selecting the requirements in Section 4.2.

The requirements only cover the security objectives derived from technological controls in Section 5.4 of the threat analysis [2]. It does not cover the physical security objectives in Section 5.3 of the analysis, as no physical security requirements are available in IEC 62443 to cover these objectives.

As mentioned in the introduction, it is recommended that besides the technological requirements selected here, charge point operators also require that any software supplier complies full to **IEC 62443-4-1** [4] and any system integrator complies fully with **IEC 62443-2-4** [5] both at **maturity level at least 2**. From 2024 onwards, it is recommended to require maturity level at least 3 for IEC 62443-4-1.

For IEC 62443-2-4 a system integrator can only reach security level 3 if it performs projects following all requirements in the standard. CPOs can hence ask for security level 3 when they do a second project with a supplier. But it may not always be feasible for a first project.

Table 5: Selection of security requirements from IEC 62443-3-3 to meet the security objectives for the charging station. Additional requirements not in IEC 62443-3-3 are given in italic.

Objective	***IEC 62443-3-3 requirements***
8.3 Information access restriction	
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.	• SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)

8.5 Secure authentication	
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. *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.	• SR1.1 Human user identification and authentication • SR 1.2 Software process and device identification and authentication • SR 1.9 Strength of public key authentication • SR 2.6 Remote session termination • SR 4.3 Use of cryptography
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.	• SR1.1 Human user identification and authentication
8.8 Management of technical vulnerabilities	
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.	• SR 3.2 Malicious code protection • SR7.7 Least functionality

8.9 Configuration management	
8.9-SO2 Automated configuration management: The charging station can be restored from a backed-up configuration automatically by the CPO central system.	• SR7.3 Control system backup • SR7.4 Control system recovery and reconstitution
8.15 Logging	
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.	• SR2.8 Auditable events • SR2.9 Audit storage capacity • SR2.10 Response to audit processing failures • SR3.9 Protection of audit information • SR6.1 Audit log accessibility • SR6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
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.	• SR2.11 Timestamps • SR2.11 RE1 Internal time synchronization • SR2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
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.	• SR1.8 Public key infrastructure certificates • SR1.9 Strength of public key-based authentication • SR 3.4 Software and information integrity • SR4.3 Use of cryptography

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 place, 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	
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.	• SR 1.9 Strength of public key-based authentication • SR3.1 Communication integrity • SR3.1 RE1 Communication authentication • SR 3.8 Session integrity • SR4.1 Information confidentiality • SR4.1 RE1 Protection of confidentiality at rest or in transit via untrusted networks
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	• SR7.1 Denial-of-service protection
8.22 Segregation of networks	
8.22-SO2 Logical network segregation on the charging station WAN: The charging	• SR5.1 Network segmentation • SR5.2 Zone boundary protection

station is segregated from other zones on the WAN interface. Only normal connections are allowed through the network perimeter. The communication load can be controlled at the perimeter.	• SR5.2 RE1 Deny by default, allow by exception • SR 7.1 Denial of service protection • SR 7.1 RE1 Manage communication loads
8.24 Use of cryptography	
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.	• SR1.5 Authenticator management • SR1.8 Public key infrastructure certificates • SR1.9 Strength of public key authentication • SR4.3 Use of cryptography

4.1 Requirements selected from IEC 62443-3-3

Table 6 below lists the requirements from the IEC 62443-3-3 standard on *System security requirements and security levels* [1] that were selected for charging stations and charging plazas in Table 5.

Some of the requirements have been adapted to the specific application domain of EV charging to be able to meet the security objectives. The adaptations are prescriptive. To be compliant with the requirements in this document all adaptations must be followed.

The adaptations should be read as a specification of the original requirement. The original requirement remains in force. The adaptation limits the options for meeting the requirements to ensure that the implementation meets the security objectives.

Besides the adaptations, supplemental guidance is included for some requirements. The guidance is non-binding. It clarifies the requirements, gives examples, or provides recommendations on implementing the requirement. For some requirements, it provides a link to the IEC 62351 standard.

Following the convention in IEC 62443-3-3, the adaptations and supplemental guidance will use the term *'control system'* for the field equipment zone.

Table 6: Full list of requirements selected from IEC 62443-3-3 for charging stations and charging plazas.

IEC identifier	Name	Objective
SR1.1	**Human user identification and authentication** *Adaptation:* The control system shall provide the capability to identify and authenticate the role of human users. The system shall identify and authenticate EV drivers on the authentication terminal using a mechanism chosen by the mobility service provider	8.5-SO4 8.5-SO5
SR 1.2	**Software process and device identification and authentication** *Adaptation:* The control system shall provide the capability to identify and authenticate the role of the CSMS, electric vehicle, engineers, EMS, and other charging stations.	8.5-SO4
SR1.3	**Account management**	8.5-SO4
SR1.5	**Authenticator management** *Adaptation:* The control system shall provide the capability to automatically update all authenticators from the central maintenance system over the WAN interface. It shall be possible to update them without support from the supplier. The confidentiality and integrity of the authenticators shall be protected during changes. The control system shall at least provide the capability to protect passwords from unauthorized disclosure by storing them salted and hashed. *Supplemental guidance:* The adaptation only concerns point c) and part of point d) of the original requirement. The rest of the requirement stays in force without adaptation. It is allowed that keys or credentials cannot be updated if they are only used for device internal purposes, such	8.24-SO2

IEC identifier	Name	Objective
	as encrypting local storage or setting up secure communication between processors on the same device. Allowing authenticators to be only updated through firmware updates does not meet the requirement, as preparing the firmware update would require support from the supplier. For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.	
SR1.8	**Public key infrastructure certificates**	8.24-SO2
SR1.9	**Strength of public key authentication**	8.5-SO4 8.19-SO2 8.20-SO2 8.24-SO2
SR2.1	**Authorization enforcement**	8.3-SO6
SR2.1 RE1	**Authorization enforcement for all users** *Adaptation:* The control system shall provide the capability to implement the access control policy described in **Error! Reference source not found.** in Section 0.	8.3-SO6
SR2.6	**Remote session termination**	8.5-SO4
SR2.8	**Auditable events**	8.15-SO2
SR2.9	**Audit storage capacity**	8.15-SO2

IEC identifier	Name	Objective
SR2.10	**Response to audit processing failures**	8.15-SO2
SR2.11	**Timestamps**	8.17-SO2
SR2.11 RE1	**Internal time synchronization**	8.17-SO2
SR2.11 RE2	**Protection of time source integrity**	8.17-SO2
SR 3.2	**Malicious code protection** *Adaptation:* All hosts shall allow security features available on the hardware and software platforms to be enabled. Infrastructure shall be able to manage the security features from the local maintenance interface or over the WAN interface through the CPO central system. *Supplemental guidance:* It is recommended to use the following hardware features when they are supported: • *No-Execute (NX) / Write-xor-execute (W^R):* A Memory Protection Unit (MPU) or Memory Management Unit (MMU) shall be used to mark code regions as read-only and data sections as non-executable. • *Address Space Layout Randomization (ASLR):* A Memory Management Unit (MMU) shall be used to load data and code at different memory addresses every time an application is run. The software running on the device must be compiled to use the hardware features. The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR. At the operating system layer, user’s access to filesystems should be minimized, and processes should	8.8-SO2

IEC identifier	Name	Objective
	be run with minimum privileges. Host-based firewalls should be enabled.	
SR 3.4	**Software and information integrity** *Adaptation:* Equipment in the control systems shall validate the authenticity and integrity of any software or firmware update by validating a digital signature before installing it. The update shall be signed by the supplier. The signature shall protect the entire update. *Supplemental guidance:* It is not required that the integrity or authenticity of the firmware or software is validated during boot ("secure boot").	8.19-SO2
SR 3.9	**Protection of audit information**	8.15-SO2
SR 4.1	**Information confidentiality**	8.20-SO2
SR 4.1 RE1	**Protection of confidentiality at rest or in transit via untrusted networks**	8.20-SO2
SR 4.1 RE2	**Protection of confidentiality across zone boundaries**	8.20-SO2
SR 4.3	**Use of cryptography** *Supplemental guidance:* Guidance on cryptographic algorithms and key lengths is given in: • the ANSSI selection guide for cryptographic algorithms [12] and rules and recommendations on the choice and parameters of cryptographic algorithms [13] • the BSI technical guideline *Cryptographic Mechanisms: Recommendations and Key Lengths* [14]	8.5-SO4 8.19-SO2 8.24-SO2

IEC identifier	Name	Objective
	- the ECRYPT – *Algorithms, Key Size, and Protocols Report* [15] - the NIST *Recommendation for key management* [16] The latest version of these reports should be followed. Algorithms and key sizes should be used that are recommended for new systems at the time of deployment, and preferably also for the full lifetime of the product. A dedicated cryptographic (pseudo-)random number generator should be used to generate random numbers for all security functions.	
SR5.1	**Network segmentation**	8.22-SO2
SR 5.2	**Zone boundary protection** *Supplemental guidance:* The zone boundary protection may be applied by a firewall, router, glass fiber modem, layer 3 switch or any other network device with the necessary capabilities.	8.22-SO2
SR 5.2 RE1	**Deny by default, allow by exception**	8.22-SO2
SR 6.1	**Audit log accessibility**	8.15-SO2
SR 6.1 RE1	**Programmatic access to audit logs**	8.15-SO2
SR 7.1	**Denial of service protection** *Supplemental guidance:* In the degraded mode, at least the charging functions should continue to work properly.	8.20-SO3 8.22-SO1
SR 7.1 RE1	**Manage communication loads**	8.20-SO3

IEC identifier	Name	Objective
		8.22-SO1
SR 7.3	**Control system backup**	8.9-SO2
SR 7.4	**Control system recovery and reconstitution**	8.9-SO2
SR 7.7	**Least functionality** *Adaptation*: The control system shall be delivered with all unneeded functions disabled. In particular, they shall be delivered with: • all unused user accounts removed • all unused network services disabled • all unused hardware interfaces disabled • all debug, diagnostic, or test interfaces disabled Hardware, debug, diagnostic, and test interface shall be disabled through one-time programmable memory (OTP) or muxing. The control system shall be delivered with the security features from the underlying hardware and operating system enabled whenever possible.	7.8-SO1 8.8-SO2

4.2 Rationale for the requirements

Below a rationale is provided for the requirements selected in Sections 4.1 by showing that they cover the security objectives for the charging station (Table 5).

8.3-SO6 Least privileges on the WAN, authentication terminal, electric vehicle, local maintenance, LAN, and EMS interfaces

Authorization for all users is covered by *SR2.1, SR2.1 RE1*. Requirement *SR 2.1 RE1* is adapted to reference the access control policy in Section 0.

8.5-SO4 Role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations

The objective concerns both human users and software process users.

Authentication for human users is covered by requirement *SR1.1*.

Authentication for software process users is covered by requirement *SR1.2*. The requirement is adapted to include role-based authentication for the CSMS, electric vehicle, engineers, EMS, and other charging stations, as called for in the objective.

Strong cryptographic keys and algorithms for the authentication are ensured by requirements *SR1.9* and *SR4.3*. Remote session termination (*SR2.6*) is included to reduce the risk that authentication is bypassed by compromising a session.

8.5-SO5 Authentication for EV drivers on the authentication terminal

Authentication for human users is covered by requirement *SR1.1*. The adaptation ensures that the charging station supports the authentication mechanism specified by the mobility service provider.

8.8-SO2 Hardened by default

Disabling unneeded functions is covered by requirement *SR 7.7*.

Enabling security functions on the hardware and software platforms is covered by requirement *SR 3.2* on malicious code protection. The requirement is adapted to clarify the measures against malicious code that are at least required.

8.9-SO2 Automated configuration management

Restoration from a backed-up configuration is covered by requirements *SR 7.3* and *SR 7.4*.

8.15-SO2 Collecting security events from the charging station through the CPO central system

Logging security events is covered by requirement *SR2.8*. Sending the logs to the CPO central system is covered by requirements *SR6.1* and *SR6.1 RE1*.

Protection of the security logs is covered by requirements *SR2.10* and *SR3.9*. Requirement *SR2.9* ensures that there is enough storage capacity on the device for the logs.

8.17-SO2 Clock synchronization for the charging station

Time synchronization is covered by requirements *SR2.11* and *SR2.11 RE1*. Requirement *CR2.11 RE2* ensures that the integrity of the time source is protected.

8.19-SO3 Automated firmware management for local controllers

No requirements are included to explicitly allow remote software updates. These are requirements for components rather than for the system. Hence, they are not part of IEC 62443-3-3. They are included in the requirements for charging stations [7].

Integrity of software and firmware are covered by *SR 3.4*. Requirement *SR 1.8* ensures that the system can be integrated into a PKI for the certificates needed to verify the signature. Requirements *SR 1.9* and *SR 4.3* ensure the strength of the cryptography used for the signatures

8.20-SO2 Cryptographic protection of communication confidentiality and integrity on the WAN interface

Protecting the confidentiality of the information is covered by requirement *SR 4.1* and *SR 4.1 RE1*. The integrity of the communication is covered by *SR 3.1*, *SR 3.1 RE1*, and *SR 3.8*. Requirements *SR 1.9* ensures that strong cryptography is used to protect communication.

8.20-SO3 Resilience of charging functions against denial-of-service attacks on the WAN

Protection against denial-of-service attacks on the WAN is achieved by requirement *SR7.1*. The requirement is adapted to specify that in a degraded mode, the charging functions should continue to work.

8.22-SO2 Logical network segregation on the charging station WAN

Network segregations is ensured by requirement *SR5.1*.

Requirements *SR5.2* and *SR5.2 RE1* ensure that there is protection between different security zones, and only allowed traffic can go through.

Protection against denial-of-service attacks on the WAN is achieved by requirements *SR 7.1* and *SR 7.1 RE1*.

8.24-SO2 Automated key and password management over the WAN

Remote updates of keys and credentials are covered by requirements *SR 1.5.* The requirement is adapted to ask for automated key updates.

Requirement *SR 1.8* allows a root certificate from the CPO to be installed, so that it can be integrated in their PKI. Requirements *SR 1.9* and *SR 4.3* ensure the strength of the cryptography used for the certificates.

References

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

[2] ENCS, EV-111-2022 Threat analysis for EV charging infrastructure, 2022.

[3] IEC, "IEC 62443-1-5: Rules for IEC 62443 profiles," 2022.

[4] IEC, IEC 62443-4-1: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, 2018.

[5] IEC/ISA, IEC 62443-2-4: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers, 2017.

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

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

[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] ANSSI, "ANSSI-PA-079: Guide de Sélection d'algorithmes cryptographiques," 2021.

[13] ANSSI, "ANSSI-PG-083: Guide de mécanismes cryptographiques: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques," 2020.

[14] Federal Office for Information Security, "BSI - Technical Guideline TR-02101-1: Cryptographic Mechanisms: Recommendations and Key Lengths," 2022.

[15] ECRYPT-CSA, "Algorithms, Key Size and Protocols Report," 2018.

[16] National Institute for Standards and Technology, "NIST Special Publication 800-57 Part 1 Revision 5: Recommendation for Key Management: Part 1 - General," 2020.