EV-201-2019

Security architecture for electric vehicle charging infrastructure

Version 1.0

24 December 2019

This document was produced by ElaadNL and ENCS as part of a program to improve the security of the electric vehicle charging infrastructure. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	DA-301-2019: Security requirements for procuring smart meters and data concentrators
Distribution automation	DA-101-2019: Security risk assessment for distribution automation systems DA-201-2019: Security architecture for distribution automation systems DA-301-2019: Security requirements for procuring distribution automation RTUs DA-390-2019: Market survey on distribution automation RTU security DA-401-2019: Security test plan for distribution automation RTUs
Substation automation	DA-101-2019: Security risk assessment for substation automation systems DA-201-2019: Security architecture for substation automation systems DA-301-2019: Security requirements for procuring substation gateways DA-302-2019: Security requirements for procuring IEDs DA-303-2019: Security requirements for procuring HMI software
Electric vehicles	EV-101-2019: Security risk assessment for EC charging infrastructure EV-201-2019: Security architecture for EV charging infrastructure EV-301-2019: Security requirements for procuring EV charging stations EV-401-2019: Security test plan for EV charging stations

This document is shared under the Traffic Light Protocol classification:

TLP White – public

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

Version History

Date	Version	Description
9 September 2019	0.1	Initial draft shared with ENCS members.
22 October 2019	0.2	Minor changes after risk assessment: • Added measure PH3 on physical access to the local maintenance interface
24 December 2019	1.0	Final version from member project on procuring secure equipment

ENCS

Table of Contents

1 Introduction

This document provides a recommended security architecture for EV charging infrastructures. It gives a set of technical security measures that CPOs can use to mitigate the risks of cyber-attacks.

Charge Point Operators (CPOs) are controlling more and 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.

The cyber-attacks on Ukrainian grid operators [1] have shown that there are hackers that have the skills and motivation to disrupt the power grid. 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.

To mitigate these risks, grid operators as members of ENCS and ElaadNL have asked these organizations to develop this security architecture. The architecture consists of a set of recommended technical security measures that CPOs can use to prevent and detect sabotage and fraud attacks on the EV charging infrastructure.

The architecture is intended to be used together with an information security management system. It is aligned with the ISO/IEC 27001:2013 [2] standard. Each subsection gives technical security measures to meet an objective of ISO/IEC 27001 Annex A. The objective number is given in square brackets.

1.1 Objective

The security architecture provides guidance on what technical measures CPOs can take to secure their EV charging infrastructure systems.

The architecture can also be used by organizations procuring EV charging services, such as provinces and municipalities, to put security requirements to CPOs. The architecture can be used directly in procurement documents.

1.2 Scope

The architecture covers the following topics from ISO/IEC 27001:2013 [2]:

- Access control (A.9)
- Cryptography (A.10)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communication security (A.13)
- Information security aspects of business continuity (A.17)

The architecture covers the CPO central system and the connected charging stations. Figure 1 shows a reference architecture with the interfaces of the EV charging infrastructure and the users on these interfaces.

Some interfaces are found only in certain charging stations, depending on the brand, model and deployment (e.g., stand-alone or within a charging plaza). Not all charging stations will for instance have interfaces to a local energy management system (EMS).

The architecture does not consider the internal working of the charging stations or CSMS and makes no assumptions on it.

1.3 Risks mitigated

The architecture protects the EV charging infrastructure against large-scale fraud and attempts to sabotage the electricity grid. It protects against advanced attackers, that is attackers with the capabilities of a professional criminal group willing to spend several months on a targeted attack.

The architecture leaves open how EV drivers authenticate to a charging station to start charging. The authentication method used depends on the mobility service provider and often cannot be freely chosen by the CPO. If a weak method is used, there is still a serious risk of fraud, for instance by cloning or forging access tokens.

The architecture is designed to limit the impact of physical attacks. It is accepted that advanced attackers can physically compromise a charging station or plaza. But the architecture aims to limit the impact to one station or plaza.

The architecture mitigates the risk of insider threats through logging and monitoring. Security events on charging stations can however not be linked to individual users, because of technical limitations in current charging stations.

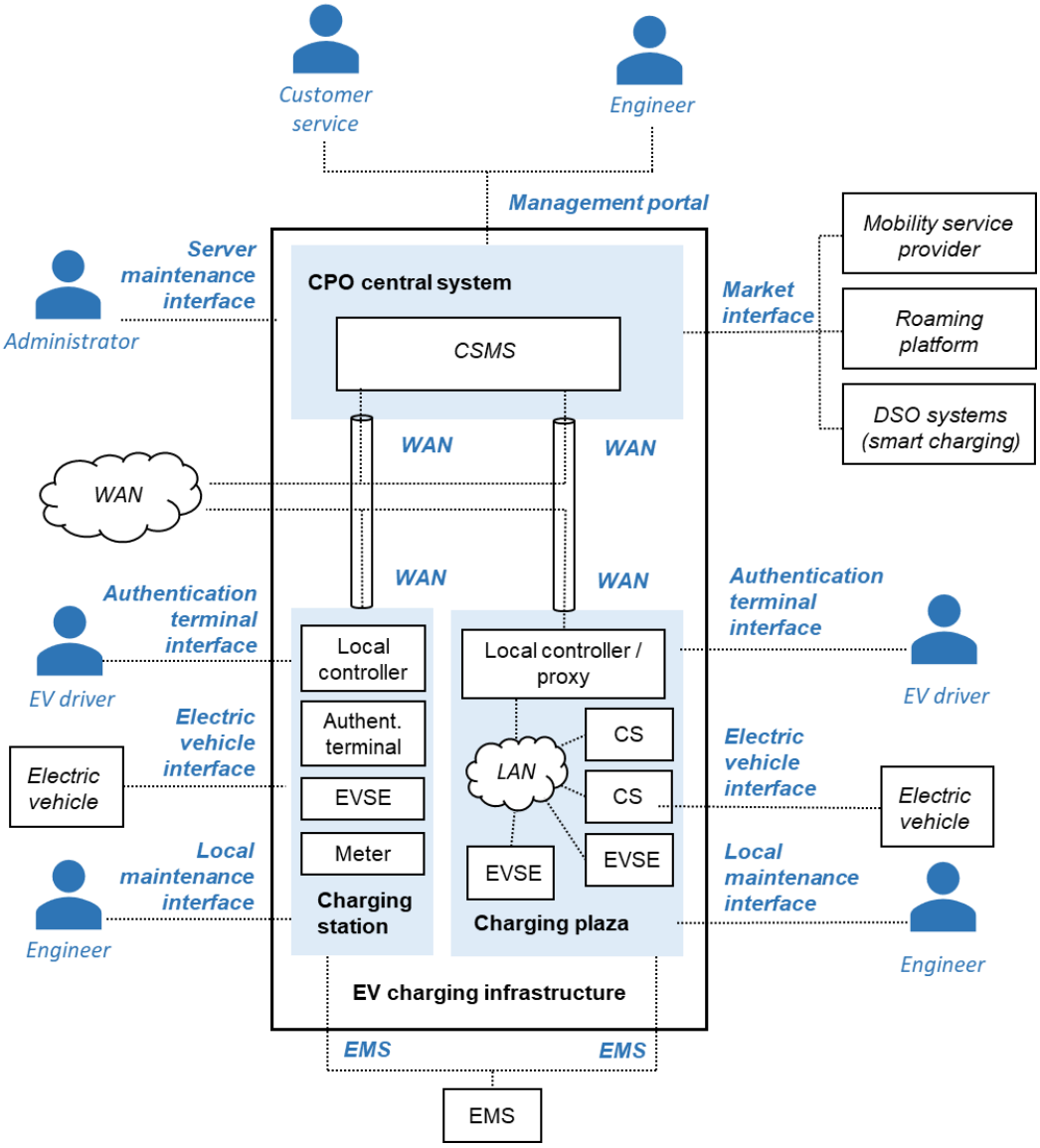

Figure 1: Reference architecture for the EV charging station, showing its users and interfaces.

Using the architecture

The security architecture is part of a larger approach to creating secure systems, both when building new systems or when updating existing systems. It consists of the following steps:

1. Perform a **security risk assessment** to understand the threats to the system and the impact these can have. A risk assessment for a typical EV infrastructure is available in [3].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures are chosen for the entire system, as this is usually more effective than choosing measures per component. The architecture can act as a blueprint for system integrators and the departments maintaining the system. The current document gives a recommended security architecture for EV infrastructure.
3. Derive **security requirements for components** from the security architecture that can be used to develop or procure the components. Security requirements for charging stations are available in [4].
4. **Test the components** to check that they meet the security requirements. In a procurement process, such tests should be a part of the selection phase. A test plan for charging stations is available in [5].
5. **Test the system** once it is deployed to check that it is implemented according to the architecture and mitigates the risks. The implementation of the device and network configuration can be checked using a technical audit. Mitigation of the risks can be checked using penetration and red team tests simulating threats.

These steps ensure that a secure system is delivered. But after that it still needs to be operated securely. Processes and procedures should be set up to securely maintain the system, manage keys and passwords, and respond to incidents.

To ensure the quality of the processes and procedures, it is recommended to use an information security management system, for instance based on the ISO/IEC 27001 [2]. To support this, the architecture is organized by the security objectives in ISO/IEC 27001 [2] Annex A.

2 Access control

To support access control, the security architecture provides a way to manage access rights and to implement authentication for all user groups.

2.1 CPO central system

The CPO central system enforces access control for the user groups in Table 1. Both human users and other systems accessing the charging station are considered users.

Table 1: User groups on the CPO central system.

User	Required access	Interface
Engineers	• Remote maintenance to charging stations through the central system	Management portal
Customer service representative	• Fix customer problems with charging stations	Management 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
Administrator	• Maintain applications • Maintain network and server infrastructure	Server maintenance interface

2.1.1 User access management [A.9.2]

The CPO central system manages access rights in such a way that the CPO can implement the principle of least privileges. For human users, the system uses centrally managed role-based access control to allow the CPO to keep up with personnel changes, giving users only the privileges they need.

AC1: Centrally managed role-based access control for customer service representatives, engineers and administrators

The CPO central system enforces role-based access control for customer representatives, engineers and administrators:

- Users log in with individual accounts;
- A central access control server determines their role;
- The endpoint accessed enforces the access rights of that role.

Administrators manage accounts and roles; and enforce policies on password length and lifetime on the central access control server. The endpoints allow to change the access rights or add new roles.

AC2: 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.

Remark: DSOs may switch larger numbers of charging stations if that is required for smart charging. Their access rights are governed by requirement AC3.

AC3: Least privileges for market parties

The CPO central system restricts the access privileges of market parties based on their market role, so that they can access only the functions and data they need.

Remarks: There are no requirements on how the privileges are managed. They may be static and only be changeable through software updates. Often, the communication protocol already limits access rights. Nonetheless, care should be taken to ensure that no unneeded protocols or functions can be accessed.

2.1.2 System and application access control [A.9.3]

The CPO central system enforces authentication for all its users. It uses individual passwords for every customer service representative and engineer. For market parties, it uses machine-to-machine authentication. For administrators, it uses two-factor authentication.

AC4: Authentication using individual passwords for customer service representatives and engineers

The CPO central system requires customer service representatives and engineers to log in with individual passwords. The log in procedure is protected by:

- not displaying the password when it is being entered;

- not indicating if an account exists after a failed login attempt;
- blocking access after several failed login attempts;
- automatically closing a session when it is inactive for more than an administratively configurable maximum time period.

Users can change their own passwords. Passwords are stored salted and hashed.

Remarks: It is recommended to use a password hashing function that is resistant against GPU cracking attacks, such as Argon2 or PBKDF2.

AC5: Machine-to-machine authentication for market parties

The CPO central system uses mutual authentication with passwords or keys for market parties. The administrators can change the passwords or keys. They protect against compromises of the keys and passwords by:

- using unique passwords or keys for all endpoints;
- generating them randomly with enough entropy to resist brute-force attacks.

Remark: Authentication using TLS with client-side certificates is allowed. TLS with passwords is also allowed, if the passwords are randomly generated and sufficiently long.

AC6: Two-factor authentication for administrators

The CPO central system requires administrators to log in on individual accounts using two-factor authentication.

Remark: The two-factor authentication can be implemented in different ways. If administrators log in remotely, a VPN with two-factor authentication can be used. If administrators log in locally in a data center, the physical access controls to the data center can act as a second factor, apart from the server passwords.

2.2 Charging station

The charging station supports access control for the user groups in Table 2. Both human users and other systems accessing the charging station are considered users.

Table 2: User groups on the charging station.

User	Required access	Interface
Charging Station Management System (CSMS)	• Gather information • Manage configuration • Update firmware	WAN

Engineer	• Manage configuration • Update firmware • Gather information for fault analysis	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

2.2.1 User access management [A.9.2]

The charging station manages access rights in such a way that the CPO can implement the principle of least privileges.

AC7: Least privileges for the CSMS, EV drivers, electric vehicles, other charging stations, and the local EMS

The charging station restricts the privileges of the CSMS, EV drivers, electric vehicles, other charging stations and the local EMS, so that they can access only the services, functions and data they need.

Remark: There are no requirements on how the privileges are managed. They may be static and only be changeable through software updates. Often the privileges are already restricted by the protocol that is used.

AC8: Local accounts for engineers

The charging station supports access control for engineers with local accounts. The charging station enforces the corresponding access rights.

Remark: For charging stations that can maintain a reliable connection with the central systems, it is recommended to use centrally managed, role-based access control. User accounts and roles can then be managed by administrators through the CPO central system.

Different methods can be used for centralized access control, for instance using RADIUS, LDAP, or Active Directory. Charge point operators should choose a method that works with their existing systems.

2.2.2 System and application access control [A.9.3]

The charging station implements authentication for all users. For the CSMS, other charging stations, the local EMS, and electric vehicles (if needed), it uses machine-to-machine authentication. For engineers, it uses passwords. For EV drivers, the authentication mechanism is determined by the mobility service provider.

AC9: Machine-to-machine authentication for the CSMS, other charging stations and the local EMS

The charging uses mutual authentication with passwords or keys for the CSMS, other charging stations, and the local EMS. It protects against compromises of the keys and passwords, as described in AC5.

Remarks: Unique credentials are used for each charging station as described in AC5. Passwords and keys are updated according to measure CR2.

The architecture assumes that the engineers have remote access to the charging stations only through the CSMS. They do not log in directly on the charging stations themselves. Consequently, only the CSMS needs to authenticate to the charging stations on the WAN interface.

AC10: Authentication using passwords for engineers

The charging station requires engineers to log in with a password. The charging station supports passwords that are strong enough to resist brute-force attacks.

Remark: To limit the impact of passwords leaking, it is recommended to use either a unique password for each charging station or centrally managed access control with individual password for all engineers.

AC11: Authentication for EV drivers

The charging station requires EV drivers to authenticate on the authentication terminal interface using a mechanism chosen by the mobility service provider.

Remark: Different mobility service providers use different mechanisms, such as tokens, RFID cards or mobile apps. It is strongly recommended to choose an authentication mechanism that is resistant to known attacks. Some current mechanisms are vulnerable to attacks such as cloning. To allow these to be changed in the future, the charging stations should support replacing the authentication terminal (see measure OP1 in Section 5.1).

AC12: Machine-to-machine authentication for electric vehicles

If the electric vehicle interface allows functions more advanced than controlling the charging, the charging station should use mutual authentication with passwords or keys for the electric vehicles. It should protect against compromises of the keys and passwords as described in AC5.

Remarks: Passwords and keys are updated according to measure CR2. More advanced functions are usually accessed through the IEC 15118 protocol. This protocol defines a certificated-based authentication mechanism [6].

3 Cryptography

The security architecture uses cryptography for several measures:

- Machine-to-machine authentication for various users (Section 2);
- Hashing passwords used by human users (Section 2);
- Digitally signing the firmware (Section 5.4);
- Protecting the confidentiality and integrity of communication (Section 6.1).

Measures need to be taken to make these cryptographic techniques effective.

3.1 Cryptographic controls [A.10.1]

Strong cryptographic keys and algorithms are used to protect against attacks on the cryptography itself. Remote key updates from the central systems are used to allow keys to be updated on possibly thousands of charging stations.

CR1: Strong cryptographic keys and algorithms

The EV charging infrastructure applies cryptography according to regulations and modern guidelines:

- Algorithms and protocols are selected according to expert recommendations, such as those from the ECRYPT project [7];
- Key lengths and other parameter are chosen to resist attacks over the infrastructure's lifetime;
- Random numbers used for security are generated with a cryptographic pseudo-random number generator, following the requirements in Section 3.2.3 of the ECRYPT report [7];
- When certificates are used for authentication, the validity of the certificate is checked, and the provided identity is used to determine authorizations.

CR2: Remote password and key updates

The CPO central system can update all passwords and keys used on the charging stations with a process that meets the following requirements:

- New keys are automatically equipped with a cryptographic random number generator;
- The confidentiality and integrity of passwords and keys is cryptographically protected during transport;
- If public-key cryptography is used, the system can use certificates issued by the CPO's public key infrastructure (PKI).

Remark: The certificate used to verify firmware updates (OP9) is issued by the vendor. So, for this certificate charging stations does not need to be able to use certificates from the CPO’s PKI.

4 Physical and environmental security

Security against physical attacks is provided by the perimeter protection of data centers and by tamper detection on the charging plaza and stations.

4.1 Secure areas [A.11.1]

The data center that houses the CPO central system is protected against advanced threats. Equipment placed in a charging plaza has tamper detection to allow fraud to be detected.

PH1: Physical security of the data center

The servers of the CPO central system are placed in a data center that is protected against advanced physical attacks.

Remark: If cloud services are used, then the policies, security measures and SLAs of the providers must ensure the required protection.

PH2: Physical security of the charging plaza

EV charging equipment in a charging plaza allows physical tampering to be detected by:

- being placed in casings that protects against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces;
- creating a log event whenever any part of the casings is opened.

4.2 Equipment [A.11.2]

The charging station has a tamper resistant casing to counter fraud.

PH3: Tamper detection on the charging station

The charging station allows physical tampering to be detected by:

- having a casing that protects against physical manipulation, so that attackers without specialist tools cannot reach its internal components without leaving visible traces;
- creating a log event whenever any part of its casing is opened.

Remarks: Additional measures can be taken in the hardware, firmware and software to strengthen the protection, such as using a trusted platform module (TPM), secure boot and read-only memory.

PH4: Physical access to the local maintenance interface only possible from casing

The local maintenance interface can only be accessed after opening the charging station casing.

Remark: Because of measure PH2, a log event shall be created whenever an engineer opens the casing to access the local maintenance interface.

Engineers may access the charging stations through local area network (LAN) in a charging plaza or through a wireless network to avoid the need to open their casing. Wireless access should only be enabled during maintenance (see measure CM5 in Section 6.1). If the equipment has wireless capabilities, then those can be enabled and used. Otherwise, a wireless access point can be used.

5 Operations security

The security architecture supports the operational processes and procedures needed to keep the EV charging infrastructure secure throughout its lifetime.

5.1 Operational procedures and responsibilities [A.12.1]

To support capacity management, charging stations need to have enough memory and computing power reserves for security updates, as they will stay in the field for a long period of time.

OP1: Future-proof hardware

The charging stations have enough reserves in memory and computing power to allow updates to security functions during their lifetime.

Remark: Each CPO can further detail this requirement according to their needs, for instance, defining minimum thresholds. More precise requirements are included in the security requirements for procuring charging stations [4].

5.2 Backup [A.12.3]

To support backup and recovery processes, an automated back-up process is used for servers. Charging stations can be reset to factory defaults in case of problems, as they do not store business critical information.

OP2: Automated backups for CPO central system servers

An automated backup process is used for the CPO central system servers.

Remark: The process must include testing the integrity of the backups and the robustness of the recovery procedures.

OP3: Reset to factory defaults for charging stations

The charging stations provide a secure method for the CPO to reset them to factory default settings, including the security settings, in case of problems.

Remark: The method must be consistent with the CPOs incident response plan and recovery procedures.

The security logs must be retrieved, if possible and in case they were not timely sent to the central systems, for further investigation and incident reporting.

5.3 Logging and monitoring [A.12.4]

To support detection and response to security incidents, the EV charging infrastructure needs to log relevant security events and gather them for analysis. Because the security logs are important for security, they also need to be protected themselves.

OP4: Security events

The EV charging infrastructure system logs all events relevant to security in local logs, including:

- Access control events (e.g. successful and failed authentication);
- Changes to security settings (e.g. keys or credentials, authentication settings);
- Changes to software or firmware (e.g. firmware updates);
- Possible signs of attacks (e.g. physical tamper events, invalid certificates).

The log entries for security events include a timestamp, an event description and the user, role or process causing the event.

OP5: Collecting security events

The EV charging infrastructure allows all security events to be read out locally and gathered centrally for analysis.

A label linking the event to its origin endpoint is added to each log entry either at the endpoint or at an aggregation point, allowing to identify its source. The events allow parsing (i.e., easy interpretation), avoiding the need to develop a dedicated parser.

Time is synchronized between endpoints to ensure that a consistent timeline can be created.

Remarks: Not all events need to be gathered. Instead, it is recommended to define detection use cases based on risks and only gather events needed for those.

OP6: Protecting security logs

The EV charging infrastructure protects security logs by:

- Restricting access by only allowing authorized users to access them;
- Having enough storage capacity for the security logs;
- Implementing a rolling security log, in which the entries with the oldest timestamp are discarded first if log storage is full.

Remark: Normally on the system and root users should be allowed to modify the logs, and only specific user groups should be authorized to read them.

The charging station should have at least enough storage capacity to store security events for one week if communications with the central system are interrupted, assuming normal operating conditions.

5.4 Control of operational software [A.12.5]

To support patching, the EV infrastructure has efficient update mechanisms for both the CPO central system and the charging stations. The authenticity of the charging station's firmware is verified using a digital signature.

OP7: Support for secure server software updates

The administrators can efficiently update the operating system and application software in all the servers of the CPO central system, so that security updates can be applied immediately. The update process verifies the authenticity of the installed software.

Remarks: If the servers are managed by an external party, for instance because the system is running in the cloud, updates should be arranged in SLAs.

To allow for efficient updates, it is most convenient to connect them to update servers. Updates can be installed by transferring them manually through USB drives. But for larger systems this takes a lot of work, so that servers might not receive timely updates.

It should be possible to update all parts of the central system, including network equipment.

OP8: Batched, remote firmware updates

The CPO central system can update the charging stations remotely, so that it is possible to apply security updates as they become available.

Remark: With batched, remote updates, charging stations can be kept at the latest firmware version to fix vulnerabilities. Notifications from the vendor on firmware updates should be monitored. After testing and approval from the CPO, the new firmware should be rolled out.

OP9: Verification of firmware signatures before installation

The charging station's firmware is digitally signed by the vendor using his private key in a secure environment at their premises. The charging station checks the signature with the vendor's public key before installation to verify the firmware's authenticity.

5.5 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the EV infrastructure is hardened, avoids known vulnerabilities and applies input validation.

OP10: Hardening

The EV charging infrastructure is hardened by disabling unneeded functions, in particular:

- unused network services are closed;
- unused user accounts are removed;
- unused, externally accessible hardware ports on the charging station are disabled.

Remark: Internal hardware ports on the charging station do not need to be disabled, although this can help hardening the system even further.

OP11: Known vulnerabilities

The EV charging infrastructure uses only applications, libraries and communication protocols without known security vulnerabilities.

OP12: Input validation

The EV charging infrastructure applies input validation to all data it receives.

Remarks: The EV infrastructure developers should make sure their code checks the validity of all received data, including validating if the input values are within the permitted ranges. They should regularly check that there are no input validations vulnerabilities in third-party libraries and applications. They should use code reviews and robustness tests for code they develop in-house, such as web interfaces or the implementation of domain-specific protocols, such as OCPP [8].

OP13: Hardware assisted measures against exploits

The EV charging infrastructure uses hardware assisted measures, such as No Execute (NH) and Address Space Layout Randomization (ASLR), to make exploits more difficult.

6 Communication security

6.1 Network security management [A.13.1]

The EV infrastructure cryptographically protects the integrity and confidentiality of communication over untrusted networks. It restricts network access by:

- blocking communication between charging stations;
- placing firewalls on network boundaries;
- restricting wireless access to charging stations.

The charging stations are protected against denial-of-service (DoS) attacks, as they sometimes may be reached directly from untrusted networks.

CM1: Cryptographic protection of communication confidentiality and integrity

Cryptographic measures are used to protect the integrity and confidentiality of communication on:

- the management portal;
- the market interface;
- the server maintenance interface;
- the WAN interface.

These measures allow to verify the source of messages and protect against replay attacks.

Remark: Communication can for instance be protected through a VPN, through TLS or through application layer measures.

Further measures can be taken to protect communications in the LAN interface to complement the physical protection provided by PH2 and PH3.

CM2: No direct communication between charging stations on the WAN

Direct communication between different charging stations over the WAN is blocked through the cryptographic measures specified in CM1.

Remark: Apart from through cryptographic measures, communication between charging stations on the WAN may be blocked on the telecom layer.

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.

CM3: Network perimeter protection

Firewalls are placed to control the network traffic across all network boundaries by:

- only allowing through communication needed for normal operations;
- limiting traffic in case of a denial-of-service attack through flooding.

Remark: If the firewalls support more advanced protection, for instance by using signatures or deep-packet inspection, this should also be turned on whenever possible.

Measures should also be taken to detect and respond to denial-of-service attacks in the WAN network. If an external telecom provider is used, the steps the provider must take should be part of the contractual agreements. A private access point name (APN) network or similar should be used to restrict who can get access to the network.

CM4: Restriction on wireless communications for local maintenance

If engineers use wireless communication to maintain charging stations, a strong password is used to restrict access to the wireless network.

Remark: Wireless communication may be used for standalone charging stations or in a charging plaza. It is recommended to only turn on the wireless access during the maintenance work.

CM5: Resilience against denial-of-service attacks

The charging stations are resilient against denial-of-service attacks. They do not become unavailable for long periods of time when network interfaces are flooded with data or when malformed messages are received.

Remark: Charging stations are particularly vulnerable to denial-of-service attacks because they are directly connected to WAN network without a firewall in front of them.

The charging stations may become slower when flooded or when dealing with malformed packets, but they should not crash, reboot or become unreachable.

7 Information security aspects of business continuity management

7.1 Information security continuity [A.17.1]

To ensure that the security of the EV infrastructure is not compromised during disruptions, it is designed to fail securely.

BC1: Fail-secure design

The EV charging infrastructure is designed to fail in a manner that limits the security impact. During a failure, the infrastructure:

- does not leak confidential information, such as keys or credentials;
- protects the integrity of critical data;
- does not allow access controls to be bypassed;
- restores availability as soon as possible.

Remarks: Examples of failure are hardware malfunctions, corruption of stored or received data and software crashes. A watchdog can be used to monitor the infrastructure components and to automatically initiate steps to restore availability.

Glossary

ACL: access control list.

AD: active directory.

APN: access point name.

CPO: charge point operator.

CSMS: charging station management system

DOS: denial-of-service.

EMS: energy management system.

EV: electric vehicle.

LAN: local area network.

PKI: public key infrastructure.

RADIUS: remote access dial-in user service.

TLS: transport layer security.

TPM: trusted platform module.

VPN: virtual private network.

WAN: wide area network.

References

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

[2] ISO/IEC, "ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements," 2013.

[3] ENCS, "Security risk assessment for EV charging infrastrucure," 2019.

[4] ENCS, "Security requirements for procuring charing stations," 2019.

[5] ENCS, "Security test plan for charging stations," 2019.

[6] ISO, "ISO 15118-1:2019: Road vehicles - Vehicle to grid communication interface - Part 1: General information and use-case definition," 2019.

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

[8] O. C. Alliance, "Open Charge Point Protocol 2.0," [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-20/. [Accessed 2019].