EV-314

Coverage of CRA Annex I requirements by the IEC 62443 requirements for EV charging stations

Version 2026v1.0

11/02/2026

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 and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.

Version History

Date	Version	Description
14/01/2026	EV-314 2026v0.9	Final draft coverage of CRA Annex 1 requirements by the IEC 62443 requirements for EV charging stations
11/02/2026	EV-314 2026v1.0	Final version coverage of CRA Annex 1 requirements by the IEC 62443 requirements for EV charging stations

ENCS

Table of Contents

Version History 3

1 Introduction 5

1.1 Coverage of CRA Annex 1 by EV-311 5

2 Detailed Analysis of CRA Annex 1 Coverage 7

References 12

1 Introduction

In December 2024, the Cyber Resilience Act (CRA) entered into force [1]. Covering all digital products on the European market, the CRA requires manufacturers to meet cybersecurity obligations which will fully apply from 11 December 2027.

Requirements listed in the CRA shall apply to all EV charging stations. As stated in Article 2 of the CRA, any product with digital software or hardware elements on the market directly or indirectly connected to a device or network falls into scope of the regulation. The charging infrastructure consists of various technical layers to maintain physical and logical connectivity, and data communication. Due to this, charging stations fall into scope of the requirements laid out in the CRA.

As the CRA is drafted as a catch-all document to cover all digital products, the requirements in the CRA are quite generic. Hence, there is currently work being done by CEN/CENELEC and ETSI to create a harmonized standard to cover these requirements.

Moreover, EV charging stations will fall, for the time being, into the default product category. This means that no vertical harmonized standard for these types of products is expected in the short term, and manufacturers will be able to self-assess their conformity to the CRA.

To ensure manufacturers have guidelines to comply with the CRA, we have mapped the requirements we have developed for EV charging stations (*EV-311 Security requirements from IEC 62443 for procuring EV charging stations, version 2025v1.0*) [2] to the essential cybersecurity requirements in Part 1 of Annex I of the CRA. This comparison helps us identify whether conforming to EV-311 requirements also means compliance with the CRA and the harmonized standards under development. The main finding is:

- Each requirement under *Annex 1 Part 1* is mapped to at least one EV-311 requirement, except *2(g)*.

Once the horizontal harmonized standards are published by CEN/CENELEC and ETSI, this document can be extended to map those standards to our EV-311 requirements.

1.1 Coverage of CRA Annex 1 by EV-311

All requirements laid out in Part 1 of Annex 1 are applicable to charging stations. For our analysis, we have considered the points listed under *Annex 1 Part 1 (2)*. We found that all CRA Annex 1 requirements have at least one EV-311 requirement that is directly applicable to them, except for requirement *2(g) of Annex 1 Part 1*.

Requirement 2(g) in CRA Annex 1 stipulates the data minimisation requirements for data processing. Where processing should only be limited adequate and relevant data related to the intended purpose of the product.

Our analysis found that there are no EV-311 requirements that directly map to *2(g)*. This is an identified gap that should be addressed. Additional requirements for data minimisation should be added to the list of EV requirements and implemented to strengthen compliance to the CRA and mitigate cybersecurity risks to charging systems.

Next section shows a detailed mapping of EV-311 requirements to the corresponding CRA requirements.

2 Detailed Analysis of CRA Annex 1 Coverage

The table below shows the detailed mapping from Annex 1 requirements of the CRA to the selected IEC 62443-4-2 [3] in EV-311. A description of the coverage is also included in the table below.

It should be noted that not all EV-311 requirements are listed in this table. We have selected only those that are directly relevant to the essential cybersecurity requirements in *Part 1 of Annex I* of the CRA.

Table 1: Coverage of CRA Annex 1 requirements by the selected IEC 62443-4-2 requirements in EV-311.

CRA Annex 1 requirement	EV-311 requirements	Rationale
A. Be made available on the market without known exploitable vulnerabilities	IEC 62443-4-1	Suppliers should fully comply to IEC 62443-4-1 [4], at least level 2 maturity, and level 3 maturity from 2027 onwards, to ensure secure development processes and that there are no known exploitable vulnerabilities at the time of the product release.
B. Be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state	CR 7.6 Network and configuration settings	Components are delivered with the recommended network and security configurations by the manufacturer

C. Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them	EDR 3.10 Support for updates	Software and firmware updates can be performed remotely over the WAN interface and over the local maintenance interface. Sufficient memory and computing power in the charging station shall be ensured to allow for such updates during its lifetime. Performance tests can be done to show compliance with the requirement
D. Ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access	CR 1.1 Human user identification and authentication CR 1.2 Software process and device identification and authentication CR 2.1 RE1 Authorization enforcement for all users CR 2.8 Auditable events EDR 3.11 Physical tamper resistance and detection	Authorised access is ensured through identification and authentication of engineer roles and EV drivers. Roles are separated to implement the principle of least privilege. Identification and authentication are unique for CSMS and electric vehicles. Additionally, access control events are logged for monitoring. Specific access to audit information and audit logs is also restricted to the CSMS and engineers Protection against physical manipulation and tampering such as charging station casing and tamper resistance and detection mechanisms shall be implemented. Additionally, relevant organisational objectives

		from EV-211 OR 2 should also be met
E. Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means	CR 4.1 Information confidentiality	Protecting confidentiality of information in transit shall be done through encryption of all communication on the WAN interface. For information at rest, access control mechanisms and physical protection shall be used.
F. Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions	CR 2.11 RE2 Protection of time source integrity CR 3.1 Communication integrity CR 3.8 Session integrity EDR 3.10 RE1 Update authenticity and integrity	TLS and cryptographic methods are used to protect the integrity and authenticity of communication and information received on the WAN interface. Authenticity and integrity of any software or firmware update is validated by components through a digital signature before installation. The update should be signed by the supplier. Integrity protection mechanisms shall not be bypassed through the recovery process
G. Process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)		*Not covered by EV-311* When using OCPP, the Open Charge Alliance (OCA) determines the data exchanged between CSMS and the charging station, as well as its intended purpose

H. Protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks	CR 2.10 Response to audit process failures CR 7.1 DoS protection	Essential functions such as charging transaction should be maintained in events of denial-of-service (DoS) attack on WAN interface. Audit storage capacity can be maintained through MemoryExhaustion alert. Oldest log entries should be overwritten if the security log is full.
I. Minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	NDR 5.2 Zone boundary protection	An integrated telecom modem acting as firewall to monitor and control communication on WAN interface.
J. Be designed, developed and produced to limit attack surfaces, including external interfaces	CR 7.7 Least functionality IEC 62443-4-1	As suppliers should deliver the products with all unneeded functions disabled. Suppliers should also fully comply to IEC 62443-4-1, at least level 2 maturity, and level 3 maturity from 2027 onwards, to ensure secure development processes.
K. Be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	CR 7.1 DoS protection CR 7.4 Control system recovery and reconstitution EDR 3.2 Protection from malicious code IEC 62443-4-1	Components can be restored from a backed-up configuration by the CPO central system will reduce the degrading impact of an incident Security features from the underlying hardware and operating system hall be enabled when a device is delivered. Components still capable of delivering essential functions

		such as charging transactions in the events of DoS attack on WAN interface. Suppliers should also fully comply to IEC 62443-4-1, at least level 2 maturity to ensure secure development processes.
L. Provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user	CR 2.8 Auditable events CR 6.1 Audit log accessibility EDR 3.11 RE1 Notification of a tampering attempt	The CSMS can collect security events from components. Critical events are sent as notifications, and other events are gathered by reading logs. Logged events include opening charging station casing, access control events, configuration change events, and device boot and shut down.
M. Provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner	CR 4.2 Information persistence	Components should be able to delete any personal information stored on it on request of the CSMS. This includes transaction information and information used for charging authorization.

References

[1] European Commission, "Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)," 2024.

[2] ENCS, "EV-311: Security requirements from IEC 62443 for procuring EV charging stations," 2025.

[3] ISA / IEC, "ISA 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components," 2019.

[4] ISA / IEC, "ISA 62443-4-1 Security for industrial automation and control systems - Part 4-1: Product development requirements for IACS components," 2018.