Audit report

Technical documentation (CRA Annex VII) - Edge Controller EC-200

Organisation	**Example Machine Works B.V.**
Source snapshot	be4aea5f · 2026-09-16 21:03

Contents

1. General description of the product

Field	Value
Product	Edge Controller EC-200
Type	network-device
CRA classification	important class II
Manufacturer	Example Machine Works B.V.

(a) Intended purpose. Illustrative demo - the machine's network-connected edge controller is a device of the kind listed in CRA Annex III (class II). Reclassify for your own product.

(b) Software versions affecting compliance. 3 release(s) recorded; latest: firmware v2.5.0. The release register lists each version with its security-relevant changes.

(c) Hardware: photographs / illustrations, markings, internal layout. 3 document(s) filed under this point:

- DR-114 Design record EC-200 (v1.2) - Approved, filed at PLM vault / DR-114
- External views EC-200, front and rear (drawing) (rev. 1.0) - Approved, filed at evidence/p-edge-controller-ec-200/techdoc/TD-1/
- Type plate and markings EC-200 (drawing) (rev. 1.0) - Approved, filed at evidence/p-edge-controller-ec-200/techdoc/TD-1/

The files travel with the audit binder under evidence/.

(d) User information and instructions (Annex II). 10 of 10 requirements assessed; 10 in place, 0 partial, 0 open. (Assessment: Products > this product > User information (Annex II).) The customer-facing security datasheet complements this.

2. Design, development, production and vulnerability handling

Design and development documents on file (1):

- Main board component layout EC-200 (drawing) (rev. 1.0) - Approved, filed at evidence/p-edge-controller-ec-200/techdoc/TD-2/

(a) Design and development; system architecture. The component register describes the architecture: 2 component(s)/dependencies recorded (see the audit binder for the full register).

- Secure development lifecycle: 47 of 47 requirements assessed; 46 in place, 0 partial, 0 open. (Assessment: Organisation > Secure development lifecycle.)
- Secure code review: 11 of 11 requirements assessed; 11 in place, 0 partial, 0 open. (Assessment: Organisation > Secure code review checklist.)

(b) Vulnerability handling processes. Required here: the SBOM (see point 8), the coordinated vulnerability disclosure policy, the vulnerability reporting contact, and the secure update distribution.

- Vulnerability handling & disclosure (CVD): 13 of 13 requirements assessed; 12 in place, 1 partial, 0 open. (Assessment: Organisation > Vulnerability handling & disclosure.)
- Incident & vulnerability reporting (Art. 14): 7 of 7 requirements assessed; 7 in place, 0 partial, 0 open. (Assessment: Organisation > Incident & vulnerability reporting.)
- The generated disclosure policy and security.txt (Tools > Disclosure policy & security.txt) document the public CVD channel.

(c) Production and monitoring processes. 10 of 10 requirements assessed; 10 in place, 0 partial, 0 open. (Assessment: Organisation > Placing on market & post-market.)

3. Cybersecurity risk assessment (Art. 13(2)-(3))

Risk	Threat	L	I	Treatment	Status
No public advisory page yet		2	3	mitigate	open
Default administrative credentials shipped with the device		3	5	mitigate	mitigated
Known CVE in a third-party TLS library		4	4	mitigate	closed

Product threat model: 3 threat(s) recorded (Products > this product > Threat model).

How the essential requirements (Annex I Part I) apply: 14 of 14 requirements assessed; 14 in place, 0 partial, 0 open. (Assessment: Products > this product > Essential requirements.) The per-requirement statuses, applicability decisions and evidence are in the CRA product assessment document of the audit report set.

4. Support period (Art. 13(8))

Support period: 10 year(s), security updates until 2036-06-30; expected product lifetime 15 years, following the machine population in the field.

5. Harmonised standards, common specifications and certification schemes

Standards applied (voluntarily - no harmonised standards are cited under the CRA yet, so these give structure and evidence, not a presumption of conformity):

- IEC 62443-4-1
- IEC 62443-4-2
- IEC 62443-3-3
- IEC 62443-2-3
- ISO/IEC 29147
- ISO/IEC 30111

Where a standard is applied in part, the assessment records per control whether it applies; the audit report set carries the per-control detail.

6. Reports of the tests carried out

- Security testing: 12 of 12 requirements assessed; 12 in place, 0 partial, 0 open. (Assessment: Organisation > Security testing checklist.)
- Test evidence (reports, scan output) is attached per control and travels in the audit binder under evidence/.

7. EU declaration of conformity (copy)

The declaration draft for this product is generated under Tools > EU declaration of conformity and is included in the audit binder (products/edge-controller-ec-200/declaration-draft.md). Sign the final declaration and file the signed copy here; the draft is prepared, signing it is the manufacturer's own act.

8. Software bill of materials

SBOM available (CycloneDX), generated with syft (CI job sbom-gen); coverage: full. Component register: 2 component(s) recorded in Crosswalk. 2 SBOM import(s) on record (Products > this product > SBOM imports).

Role	Name	Date	Signature
Compiled by			
Approved by (management)			

> Generated with Crosswalk as a compliance-support aid; it is not legal advice and is not, by itself, proof of compliance. Verify against the official text of Annex VII (OJ L, 2024/2847).