Audit report

Product Edge Controller EC-200 - Cyber Resilience Act (EU) 2024/2847

Organisation	**Example Machine Works B.V.**
Generated	2026-09-16
Subject	Edge Controller EC-200
Legal basis	Cyber Resilience Act (EU) 2024/2847
Assessed against	IEC 62443-4-2, IEC 62443-3-3 (clause references; official standard texts not included)
Source snapshot	be4aea5f · 2026-09-16 21:03

Contents

Scope and context

This document records the compliance position of Edge Controller EC-200 for Cyber Resilience Act (EU) 2024/2847: the assessed control sets, the recorded implementation and evidence, the open gaps and the recommended actions. It is generated from the live assessment data and is intended for the QMS or the compliance archive.

Compliance status

Essential requirements (CRA Annex I Part I)

Status	Count
In place	14
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	14

Control	Requirement	Status	Evidence recorded
ER-1	Risk-based cybersecurity	In place	yes
ER-b	Secure-by-default configuration	In place	yes
ER-j	Limited attack surface	In place	yes
ER-k	Exploitation mitigation	In place	yes
ER-d	Protection from unauthorised access	In place	yes
ER-e	Confidentiality of data	In place	yes
ER-f	Integrity of data, commands & configuration	In place	yes
ER-g	Data minimisation	In place	yes
ER-a	No known exploitable vulnerabilities at release	In place	yes
ER-c	Security updates	In place	yes
ER-h	Availability & DoS resilience	In place	yes
ER-i	No negative impact on other services	In place	yes
ER-l	Security logging & monitoring	In place	yes
ER-m	Secure data & settings removal	In place	yes

Recorded implementation and evidence

ER-1 - Risk-based cybersecurity — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "ER-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

ER-b - Secure-by-default configuration

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Security test report STR-2026-04, secure-by-default verification (17 Apr 2026) - Documentation index, attached excerpt "STR-2026-04 (excerpt).md"; CI run #4812 passed.

ER-j - Limited attack surface

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "ER-j" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

ER-k - Exploitation mitigation

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Configuration audit pack SCR-ER-k + controller audit-log excerpt (5 Jun 2026) - evidence/scr-ER-k/, cross-checked against hardening baseline HB-2.

ER-d - Protection from unauthorised access

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Release checklist RC-2.1, gate "ER-d" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

ER-e - Confidentiality of data

In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

ER-f - Integrity of data, commands & configuration

In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "ER-f verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

ER-g - Data minimisation

In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

ER-a - No known exploitable vulnerabilities at release

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "ER-a" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

ER-c - Security updates

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Configuration audit pack SCR-ER-c + controller audit-log excerpt (5 Jun 2026) - evidence/scr-ER-c/, cross-checked against hardening baseline HB-2.

ER-h - Availability & DoS resilience

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Release checklist RC-2.1, gate "ER-h" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

ER-i - No negative impact on other services

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

ER-l - Security logging & monitoring

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "ER-l verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

ER-m - Secure data & settings removal

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

Component security (IEC 62443-4-2) (IEC 62443-4-2)

Status	Count
In place	141
In place, evidence missing	0
Partially implemented	0
Planned	1
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	142

Control	Requirement	Status	Evidence recorded
CR-1.1	Human user identification and authentication	In place	yes
CR-1.1-RE-1	Unique identification and authentication	In place	yes
CR-1.1-RE-2	Multifactor authentication for all interfaces	In place	yes
CR-1.2	Software process and device identification and authentication	In place	yes
CR-1.2-RE-1	Unique identification and authentication	In place	yes
CR-1.3	Account management	In place	yes
CR-1.4	Identifier management	In place	yes
CR-1.5	Authenticator management	In place	yes
CR-1.5-RE-1	Hardware security for authenticators	In place	yes
CR-1.5a	Authenticator management	In place	yes
CR-1.5b	Authenticator management	In place	yes
CR-1.5c	Authenticator management	In place	yes
CR-1.5d	Authenticator management	In place	yes
CR-1.7	Strength of password-based authentication	In place	yes

Control	Requirement	Status	Evidence recorded
CR-1.7-RE-1	Password generation and lifetime restrictions for human users	**In place**	yes
CR-1.8	Public key infrastructure certificates	**In place**	yes
CR-1.9	Strength of public key-based authentication	**In place**	yes
CR-1.9-RE-1	Hardware security for public key authentication	**In place**	yes
CR-1.10	Authenticator feedback	**In place**	yes
CR-1.11	Unsuccessful login attempts	**In place**	yes
CR-1.12	System use notification	**In place**	yes
CR-1.14	Strength of symmetric key-based authentication	**In place**	yes
CR-1.14-RE-1	Hardware security for symmetric key-based authentication	**In place**	yes
NDR-1.6	Wireless access management	**In place**	yes
NDR-1.6-RE-1	Unique identification and authentication	**In place**	yes
NDR-1.13	Access via untrusted networks	**In place**	yes
NDR-1.13-RE-1	Explicit access request approval	**In place**	yes
CR-2.1	Authorization enforcement	**In place**	yes
CR-2.1-RE-1	Authorization enforcement for all users (humans, software processes and devices)	**In place**	yes
CR-2.1-RE-2	Permission mapping to roles	**In place**	yes
CR-2.1-RE-3	Supervisor override	**In place**	yes
CR-2.1-RE-4	Dual approval	**In place**	yes
CR-2.2	Wireless use control	**In place**	yes
CR-2.3	Use control for portable and mobile devices	**In place**	yes
CR-2.5	Session lock	**In place**	yes
CR-2.6	Remote session termination	**In place**	yes
CR-2.7	Concurrent session control	**In place**	yes
CR-2.8	Auditable events	**In place**	yes
CR-2.9	Audit storage capacity	**In place**	yes
CR-2.9-RE-1	Warn when audit record storage capacity threshold reached	**In place**	yes
CR-2.10	Response to audit processing failures	**In place**	yes
CR-2.11	Timestamps	**In place**	yes
CR-2.11-RE-1	Time synchronization	**In place**	yes
CR-2.12	Non-repudiation	**In place**	yes
EDR-2.4	Mobile code	**In place**	yes
EDR-2.4-RE-1	Mobile code authenticity check	**In place**	yes
EDR-2.13	Use of physical diagnostic and test interfaces	**In place**	yes
EDR-2.13-RE-1	Active monitoring	**In place**	yes
HDR-2.4a	Mobile code	**In place**	yes
HDR-2.4b	Mobile code	**In place**	yes
HDR-2.4c	Mobile code	**In place**	yes
HDR-2.13	Use of physical diagnostic and test interfaces	**In place**	yes
NDR-2.4	Mobile code	**In place**	yes
NDR-2.4-RE-1	Mobile code authenticity check	**In place**	yes
NDR-2.13	Use of physical diagnostic and test interfaces	**In place**	yes

Control	Requirement	Status	Evidence recorded
NDR-2.13-RE-1	Active monitoring	**In place**	yes
SAR-2.4	Mobile code	**In place**	yes
SAR-2.4-RE-1	Mobile code authenticity check	**In place**	yes
CR-3.1	Communication integrity	**In place**	yes
CR-3.1-RE-1	Communication authentication	**In place**	yes
CR-3.3	Security functionality verification	**In place**	yes
CR-3.3-RE-1	Security functionality verification during normal operation	**In place**	yes
CR-3.4	Software and information integrity	**In place**	yes
CR-3.4-RE-1a	Authenticity of software and information	**In place**	yes
CR-3.4-RE-1b	Authenticity of software and information	**In place**	yes
CR-3.4-RE-1c	Authenticity of software and information	**In place**	yes
CR-3.4-RE-1d	Authenticity of software and information	**In place**	yes
CR-3.4-RE-1e	Authenticity of software and information	**In place**	yes
CR-3.4-RE-1f	Authenticity of software and information	**In place**	yes
CR-3.4-RE-2	Automated notification of integrity violations	**In place**	yes
CR-3.4a	Software and information integrity	**In place**	yes
CR-3.4b	Software and information integrity	**In place**	yes
CR-3.4c	Software and information integrity	**In place**	yes
CR-3.4d	Software and information integrity	**In place**	yes
CR-3.4e	Software and information integrity	**In place**	yes
CR-3.4f	Software and information integrity	**In place**	yes
CR-3.5	Input validation	**In place**	yes
CR-3.6	Deterministic output	**In place**	yes
CR-3.7	Error handling	**In place**	yes
CR-3.8	Session integrity	**In place**	yes
CR-3.8a	Session Integrity	**In place**	yes
CR-3.8b	Session Integrity	**In place**	yes
CR-3.8c	Session Integrity	**In place**	yes
CR-3.9	Protection of audit information	**In place**	yes
EDR-3.2	Protection from malicious code	**In place**	yes
EDR-3.10	Support for updates	**In place**	yes
EDR-3.10-RE-1	Update authenticity and integrity	**In place**	yes
EDR-3.11	Physical tamper resistance and detection	**In place**	yes
EDR-3.11-RE-1	Notification of a tampering attempt	**In place**	yes
EDR-3.12	Provisioning product supplier roots of trust	**In place**	yes
EDR-3.13	Provisioning asset owner roots of trust	**In place**	yes
EDR-3.14	Integrity of the boot process	**In place**	yes
EDR-3.14-RE-1	Authenticity of the boot process	**In place**	yes
HDR-3.2	Protection from malicious code	**In place**	yes
HDR-3.10	Support for updates	**In place**	yes
HDR-3.11	Physical tamper resistance and detection	**In place**	yes
HDR-3.12	Provisioning product supplier roots of trust	**In place**	yes
HDR-3.13a	Provisioning asset owner roots of trust	**In place**	yes

Control	Requirement	Status	Evidence recorded
HDR-3.13b	Provisioning asset owner roots of trust	In place	yes
HDR-3.14a	Integrity of the boot process	In place	yes
HDR-3.14b	Integrity of the boot process	In place	yes
HDR-3.14c	Integrity of the boot process	In place	yes
NDR-3.2	Protection from malicious code	In place	yes
NDR-3.10	Support for updates	In place	yes
NDR-3.10-RE-1	Update authenticity and integrity	In place	yes
NDR-3.11	Physical tamper resistance and detection	In place	yes
NDR-3.11-RE-1	Notification of a tampering attempt	In place	yes
NDR-3.12	Provisioning product supplier roots of trust	In place	yes
NDR-3.13	Provisioning asset owner roots of trust	In place	yes
NDR-3.14	Integrity of the boot process	In place	yes
NDR-3.14-RE-1	Authenticity of the boot process	In place	yes
SAR-3.2	Protection from malicious code	In place	yes
CR-4.1	Information confidentiality	In place	yes
CR-4.1a	Information confidentiality	In place	yes
CR-4.1b	Information confidentiality	In place	yes
CR-4.2	Information persistence	In place	yes
CR-4.2-RE-1	Erase of shared memory resources	In place	yes
CR-4.2-RE-2	Erase verification	In place	yes
CR-4.3	Use of cryptography	In place	yes
CR-5.1	Network segmentation	In place	yes
NDR-5.2	Zone boundary protection	In place	yes
NDR-5.2-RE-1	Deny all, permit by exception	In place	yes
NDR-5.2-RE-2	Island mode	In place	yes
NDR-5.2-RE-3	Fail close	In place	yes
NDR-5.3	General purpose, person-to-person communication restrictions	In place	yes
CR-6.1	Audit log accessibility	In place	yes
CR-6.1-RE-1	Programmatic access to audit logs	In place	yes
CR-6.2	Continuous monitoring	In place	yes
CR-7.1	Denial of service protection	In place	yes
CR-7.1-RE-1	Manage communication load from component	In place	yes
CR-7.2	Resource management	In place	yes
CR-7.3	Control system backup	Planned	yes
CR-7.3-RE-1	Backup integrity verification	In place	yes
CR-7.4	Control system recovery and reconstitution	In place	yes
CR-7.6	Network and security configuration settings	In place	yes
CR-7.6-RE-1	Machine-readable reporting of current security settings	In place	yes
CR-7.6a	Network and security configuration settings	In place	yes
CR-7.6b	Network and security configuration settings	In place	yes
CR-7.7	Least functionality	In place	yes
CR-7.8	Control system component inventory	In place	yes
CR-7.8-RE-1	Active monitoring	In place	yes

Control	Requirement	Status	Evidence recorded
CR-7.8-RE-3	Fail close	In place	yes

Recorded implementation and evidence

CR-1.1 - Human user identification and authentication

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-CR-1.1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-1.1/, cross-checked against hardening baseline HB-2.

CR-1.1-RE-1 - Unique identification and authentication

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "CR-1.1-RE-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-1.1-RE-2 - Multifactor authentication for all interfaces

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-1.2 - Software process and device identification and authentication

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-1.2 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-1.2-RE-1 - Unique identification and authentication

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-1.3 - Account management

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-1.3" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-1.4 - Identifier management

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Configuration audit pack SCR-CR-1.4 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-1.4/, cross-checked against hardening baseline HB-2.

CR-1.5 - Authenticator management

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Release checklist RC-2.1, gate "CR-1.5" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-1.5-RE-1 - Hardware security for authenticators — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-1.5a - Authenticator management — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-1.5a verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-1.5b - Authenticator management — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-1.5c - Authenticator management — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-1.5c" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-1.5d - Authenticator management — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Configuration audit pack SCR-CR-1.5d + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-1.5d/, cross-checked against hardening baseline HB-2.

CR-1.7 - Strength of password-based authentication — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "CR-1.7" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-1.7-RE-1 - Password generation and lifetime restrictions for human users — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-1.8 - Public key infrastructure certificates — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-1.8 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-1.9 - Strength of public key-based authentication — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-1.9-RE-1 - Hardware security for public key authentication

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-1.9-RE-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-1.10 - Authenticator feedback

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Configuration audit pack SCR-CR-1.10 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-1.10/, cross-checked against hardening baseline HB-2.

CR-1.11 - Unsuccessful login attempts

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Release checklist RC-2.1, gate "CR-1.11" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-1.12 - System use notification

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-1.14 - Strength of symmetric key-based authentication

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "CR-1.14 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-1.14-RE-1 - Hardware security for symmetric key-based authentication

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

NDR-1.6 - Wireless access management

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "NDR-1.6" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

NDR-1.6-RE-1 - Unique identification and authentication

In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Configuration audit pack SCR-NDR-1.6-RE-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-NDR-1.6-RE-1/, cross-checked against hardening baseline HB-2.

NDR-1.13 - Access via untrusted networks

In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	Release checklist RC-2.1, gate "NDR-1.13" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

NDR-1.13-RE-1 - Explicit access request approval

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-2.1 - Authorization enforcement

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-2.1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-2.1-RE-1 - Authorization enforcement for all users (humans, software processes and devices)

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-2.1-RE-2 - Permission mapping to roles

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-2.1-RE-2" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-2.1-RE-3 - Supervisor override

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-CR-2.1-RE-3 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-2.1-RE-3/, cross-checked against hardening baseline HB-2.

CR-2.1-RE-4 - Dual approval

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "CR-2.1-RE-4" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-2.2 - Wireless use control

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-2.3 - Use control for portable and mobile devices

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-2.3 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-2.5 - Session lock

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-2.6 - Remote session termination

In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-2.6" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-2.7 - Concurrent session control

In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Configuration audit pack SCR-CR-2.7 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-2.7/, cross-checked against hardening baseline HB-2.

CR-2.8 - Auditable events

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Release checklist RC-2.1, gate "CR-2.8" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-2.9 - Audit storage capacity

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-2.9-RE-1 - Warn when audit record storage capacity threshold reached

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "CR-2.9-RE-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-2.10 - Response to audit processing failures

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-2.11 - Timestamps

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-2.11" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-2.11-RE-1 - Time synchronization

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Configuration audit pack SCR-CR-2.11-RE-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-2.11-RE-1/, cross-checked against hardening baseline HB-2.

CR-2.12 - Non-repudiation

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Release checklist RC-2.1, gate "CR-2.12" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

EDR-2.4 - Mobile code

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

EDR-2.4-RE-1 - Mobile code authenticity check

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "EDR-2.4-RE-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

EDR-2.13 - Use of physical diagnostic and test interfaces

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

EDR-2.13-RE-1 - Active monitoring

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "EDR-2.13-RE-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

HDR-2.4a - Mobile code

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Configuration audit pack SCR-HDR-2.4a + controller audit-log excerpt (5 Jun 2026) - evidence/scr-HDR-2.4a/, cross-checked against hardening baseline HB-2.

HDR-2.4b - Mobile code

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Release checklist RC-2.1, gate "HDR-2.4b" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

HDR-2.4c - Mobile code

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

HDR-2.13 - Use of physical diagnostic and test interfaces

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence FAT/SAT acceptance report FAT-2026-11, case "HDR-2.13 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

NDR-2.4 - Mobile code

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

NDR-2.4-RE-1 - Mobile code authenticity check

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "NDR-2.4-RE-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

NDR-2.13 - Use of physical diagnostic and test interfaces

In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Configuration audit pack SCR-NDR-2.13 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-NDR-2.13/, cross-checked against hardening baseline HB-2.

NDR-2.13-RE-1 - Active monitoring

In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	Release checklist RC-2.1, gate "NDR-2.13-RE-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SAR-2.4 - Mobile code

In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SAR-2.4-RE-1 - Mobile code authenticity check

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "SAR-2.4-RE-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-3.1 - Communication integrity

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-3.1-RE-1 - Communication authentication

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-3.1-RE-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-3.3 - Security functionality verification

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Configuration audit pack SCR-CR-3.3 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-3.3/, cross-checked against hardening baseline HB-2.

CR-3.3-RE-1 - Security functionality verification during normal operation

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	Release checklist RC-2.1, gate "CR-3.3-RE-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-3.4 - Software and information integrity

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-3.4-RE-1a - Authenticity of software and information

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-3.4-RE-1a verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-3.4-RE-1b - Authenticity of software and information

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-3.4-RE-1c - Authenticity of software and information

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-3.4-RE-1c" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-3.4-RE-1d - Authenticity of software and information

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Configuration audit pack SCR-CR-3.4-RE-1d + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-3.4-RE-1d/, cross-checked against hardening baseline HB-2.

CR-3.4-RE-1e - Authenticity of software and information

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Release checklist RC-2.1, gate "CR-3.4-RE-1e" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-3.4-RE-1f - Authenticity of software and information

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-3.4-RE-2 - Automated notification of integrity violations

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-3.4-RE-2 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-3.4a - Software and information integrity

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-3.4b - Software and information integrity

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-3.4b" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-3.4c - Software and information integrity

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Configuration audit pack SCR-CR-3.4c + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-3.4c/, cross-checked against hardening baseline HB-2.

CR-3.4d - Software and information integrity

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Release checklist RC-2.1, gate "CR-3.4d" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-3.4e - Software and information integrity

In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-3.4f - Software and information integrity

In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "CR-3.4f verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-3.5 - Input validation

In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-3.6 - Deterministic output

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-3.6" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-3.7 - Error handling

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Configuration audit pack SCR-CR-3.7 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-3.7/, cross-checked against hardening baseline HB-2.

CR-3.8 - Session integrity

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Release checklist RC-2.1, gate "CR-3.8" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-3.8a - Session Integrity

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-3.8b - Session Integrity

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-3.8b verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-3.8c - Session Integrity

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-3.9 - Protection of audit information

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-3.9" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

EDR-3.2 - Protection from malicious code

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Configuration audit pack SCR-EDR-3.2 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-EDR-3.2/, cross-checked against hardening baseline HB-2.

EDR-3.10 - Support for updates

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Release checklist RC-2.1, gate "EDR-3.10" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

EDR-3.10-RE-1 - Update authenticity and integrity

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

EDR-3.11 - Physical tamper resistance and detection

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "EDR-3.11 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

EDR-3.11-RE-1 - Notification of a tampering attempt

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

EDR-3.12 - Provisioning product supplier roots of trust

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "EDR-3.12" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

EDR-3.13 - Provisioning asset owner roots of trust

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-EDR-3.13 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-EDR-3.13/, cross-checked against hardening baseline HB-2.

EDR-3.14 - Integrity of the boot process

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "EDR-3.14" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

EDR-3.14-RE-1 - Authenticity of the boot process

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

HDR-3.2 - Protection from malicious code

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "HDR-3.2 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

HDR-3.10 - Support for updates

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

HDR-3.11 - Physical tamper resistance and detection

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "HDR-3.11" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

HDR-3.12 - Provisioning product supplier roots of trust

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Configuration audit pack SCR-HDR-3.12 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-HDR-3.12/, cross-checked against hardening baseline HB-2.

HDR-3.13a - Provisioning asset owner roots of trust

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Release checklist RC-2.1, gate "HDR-3.13a" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

HDR-3.13b - Provisioning asset owner roots of trust

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

HDR-3.14a - Integrity of the boot process

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "HDR-3.14a verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

HDR-3.14b - Integrity of the boot process

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

HDR-3.14c - Integrity of the boot process

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "HDR-3.14c" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

NDR-3.2 - Protection from malicious code

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Configuration audit pack SCR-NDR-3.2 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-NDR-3.2/, cross-checked against hardening baseline HB-2.

NDR-3.10 - Support for updates

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "NDR-3.10" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

NDR-3.10-RE-1 - Update authenticity and integrity

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

NDR-3.11 - Physical tamper resistance and detection

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "NDR-3.11 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

NDR-3.11-RE-1 - Notification of a tampering attempt

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

NDR-3.12 - Provisioning product supplier roots of trust

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "NDR-3.12" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

NDR-3.13 - Provisioning asset owner roots of trust

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Configuration audit pack SCR-NDR-3.13 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-NDR-3.13/, cross-checked against hardening baseline HB-2.

NDR-3.14 - Integrity of the boot process

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Release checklist RC-2.1, gate "NDR-3.14" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

NDR-3.14-RE-1 - Authenticity of the boot process

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SAR-3.2 - Protection from malicious code

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "SAR-3.2 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-4.1 - Information confidentiality

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-4.1a - Information confidentiality

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-4.1a" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-4.1b - Information confidentiality

In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Configuration audit pack SCR-CR-4.1b + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-4.1b/, cross-checked against hardening baseline HB-2.

CR-4.2 - Information persistence

In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	Release checklist RC-2.1, gate "CR-4.2" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-4.2-RE-1 - Erase of shared memory resources

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-4.2-RE-2 - Erase verification

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-4.2-RE-2 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-4.3 - Use of cryptography

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-5.1 - Network segmentation

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-5.1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

NDR-5.2 - Zone boundary protection

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-NDR-5.2 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-NDR-5.2/, cross-checked against hardening baseline HB-2.

NDR-5.2-RE-1 - Deny all, permit by exception

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "NDR-5.2-RE-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

NDR-5.2-RE-2 - Island mode

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

NDR-5.2-RE-3 - Fail close

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "NDR-5.2-RE-3 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

NDR-5.3 - General purpose, person-to-person communication restrictions

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-6.1 - Audit log accessibility — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-6.1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-6.1-RE-1 - Programmatic access to audit logs — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Configuration audit pack SCR-CR-6.1-RE-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-6.1-RE-1/, cross-checked against hardening baseline HB-2.

CR-6.2 - Continuous monitoring — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Release checklist RC-2.1, gate "CR-6.2" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-7.1 - Denial of service protection — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-7.1-RE-1 - Manage communication load from component — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CR-7.1-RE-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-7.2 - Resource management — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-7.3 - Control system backup — Planned

Implementation Configuration backup/restore for the EC-200 is scheduled for firmware v2.5.0 (roadmap ROAD-95, owner @mark, target Nov 2026). Until then recovery relies on re-commissioning from the machine project file.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-7.3" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-7.3-RE-1 - Backup integrity verification — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Configuration audit pack SCR-CR-7.3-RE-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-7.3-RE-1/, cross-checked against hardening baseline HB-2.

CR-7.4 - Control system recovery and reconstitution — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "CR-7.4" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-7.6 - Network and security configuration settings — In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-7.6-RE-1 - Machine-readable reporting of current security settings — In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "CR-7.6-RE-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CR-7.6a - Network and security configuration settings — In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CR-7.6b - Network and security configuration settings — In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CR-7.6b" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CR-7.7 - Least functionality — In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Configuration audit pack SCR-CR-7.7 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CR-7.7/, cross-checked against hardening baseline HB-2.

CR-7.8 - Control system component inventory — In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Release checklist RC-2.1, gate "CR-7.8" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CR-7.8-RE-1 - Active monitoring — In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CR-7.8-RE-3 - Fail close — In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "CR-7.8-RE-3 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

System security (IEC 62443-3-3) (IEC 62443-3-3)

Status	Count
In place	0
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0

Status	Count
Not yet assessed	0
Not applicable	100
Applicable total	0

Control	Requirement	Status	Evidence recorded
SR-1.1	Human user identification and authentication	Not applicable	-
SR-1.1-RE-1	Unique identification and authentication	Not applicable	-
SR-1.1-RE-2	Multifactor authentication for untrusted networks	Not applicable	-
SR-1.1-RE-3	Multifactor authentication for all networks	Not applicable	-
SR-1.2	Software process and device identification and authentication	Not applicable	-
SR-1.2-RE-1	Unique identification and authentication	Not applicable	-
SR-1.3	Account management	Not applicable	-
SR-1.3-RE-1	Unified account management	Not applicable	-
SR-1.4	Identifier management	Not applicable	-
SR-1.5	Authenticator management	Not applicable	-
SR-1.5-RE-1	Hardware security for software process identity credentials	Not applicable	-
SR-1.6	Wireless access management	Not applicable	-
SR-1.6-RE-1	Unique identification and authentication	Not applicable	-
SR-1.7	Strength of password-based authentication	Not applicable	-
SR-1.7-RE-1	Password generation and lifetime restrictions for human users	Not applicable	-
SR-1.7-RE-2	Password lifetime restrictions for all users	Not applicable	-
SR-1.8	Public key infrastructure (PKI) certificates	Not applicable	-
SR-1.9	Strength of public key authentication	Not applicable	-
SR-1.9-RE-1	Hardware security for public key authentication	Not applicable	-
SR-1.10	Authenticator feedback	Not applicable	-
SR-1.11	Unsuccessful login attempts	Not applicable	-
SR-1.12	System use notification	Not applicable	-
SR-1.13	Access via untrusted networks	Not applicable	-
SR-1.13-RE-1	Explicit access request approval	Not applicable	-
SR-2.1	Authorization enforcement	Not applicable	-
SR-2.1-RE-1	Authorization enforcement for all users	Not applicable	-
SR-2.1-RE-2	Permission mapping to roles	Not applicable	-
SR-2.1-RE-3	Supervisor override	Not applicable	-
SR-2.1-RE-4	Dual approval	Not applicable	-
SR-2.2	Wireless use control	Not applicable	-
SR-2.2-RE-1	Identify and report unauthorized wireless devices	Not applicable	-
SR-2.3	Use control for portable and mobile devices	Not applicable	-
SR-2.3-RE-1	Enforcement of security status of portable and mobile devices	Not applicable	-
SR-2.4	Mobile code	Not applicable	-
SR-2.4-RE-1	Mobile code integrity check	Not applicable	-
SR-2.5	Session lock	Not applicable	-
SR-2.6	Remote session termination	Not applicable	-

Control	Requirement	Status	Evidence recorded
SR-2.7	Concurrent session control	Not applicable	-
SR-2.8	Auditable events	Not applicable	-
SR-2.8-RE-1	Centrally managed, system-wide audit trail	Not applicable	-
SR-2.9	Audit storage capacity	Not applicable	-
SR-2.9-RE-1	Warn when audit record storage capacity threshold reached	Not applicable	-
SR-2.10	Response to audit processing failures	Not applicable	-
SR-2.11	Timestamps	Not applicable	-
SR-2.11-RE-1	Internal time synchronization	Not applicable	-
SR-2.11-RE-2	Protection of time source integrity	Not applicable	-
SR-2.12	Non-repudiation	Not applicable	-
SR-2.12-RE-1	Non-repudiation for all users	Not applicable	-
SR-3.1	Communication integrity	Not applicable	-
SR-3.1-RE-1	Cryptographic integrity protection	Not applicable	-
SR-3.2	Malicious code protection	Not applicable	-
SR-3.2-RE-1	Malicious code protection on entry and exit points	Not applicable	-
SR-3.2-RE-2	Central management and reporting for malicious code protection	Not applicable	-
SR-3.3	Security functionality verification	Not applicable	-
SR-3.3-RE-1	Automated mechanisms for security functionality verification	Not applicable	-
SR-3.3-RE-2	Security functionality verification during normal operation	Not applicable	-
SR-3.4	Software and information integrity	Not applicable	-
SR-3.4-RE-1	Automated notification about integrity violations	Not applicable	-
SR-3.5	Input validation	Not applicable	-
SR-3.6	Deterministic output	Not applicable	-
SR-3.7	Error handling	Not applicable	-
SR-3.8	Session integrity	Not applicable	-
SR-3.8-RE-1	Invalidation of session IDs after session termination	Not applicable	-
SR-3.8-RE-2	Unique session ID generation	Not applicable	-
SR-3.8-RE-3	Randomness of session IDs	Not applicable	-
SR-3.9	Protection of audit information	Not applicable	-
SR-3.9-RE-1	Audit records on write-once media	Not applicable	-
SR-4.1	Information confidentiality	Not applicable	-
SR-4.1-RE-1	Protection of confidentiality at rest or in transit via untrusted networks	Not applicable	-
SR-4.1-RE-2	Protection of confidentiality across zone boundaries	Not applicable	-
SR-4.2	Information persistence	Not applicable	-
SR-4.2-RE-1	Purging of shared memory resources	Not applicable	-
SR-4.3	Use of cryptography	Not applicable	-
SR-5.1	Network segmentation	Not applicable	-
SR-5.1-RE-1	Physical network segmentation	Not applicable	-
SR-5.1-RE-2	Independence from non-control system networks	Not applicable	-

Control	Requirement	Status	Evidence recorded
SR-5.1-RE-3	Logical and physical isolation of critical networks	Not applicable	-
SR-5.2	Zone boundary protection	Not applicable	-
SR-5.2-RE-1	Deny by default, allow by exception	Not applicable	-
SR-5.2-RE-2	Island mode	Not applicable	-
SR-5.2-RE-3	Fail close	Not applicable	-
SR-5.3	General purpose person-to-person communication restrictions	Not applicable	-
SR-5.3-RE-1	Prohibit all general purpose person-to-person communications	Not applicable	-
SR-5.4	Application partitioning	Not applicable	-
SR-6.1	Audit log accessibility	Not applicable	-
SR-6.1-RE-1	Programmatic access to audit logs	Not applicable	-
SR-6.2	Continuous monitoring	Not applicable	-
SR-7.1	Denial of service protection	Not applicable	-
SR-7.1-RE-1	Manage communication loads	Not applicable	-
SR-7.1-RE-2	Limit DoS effects to other systems or networks	Not applicable	-
SR-7.2	Resource management	Not applicable	-
SR-7.3	Control system backup	Not applicable	-
SR-7.3-RE-1	Backup verification	Not applicable	-
SR-7.3-RE-2	Backup automation	Not applicable	-
SR-7.4	Control system recovery and reconstitution	Not applicable	-
SR-7.5	Emergency power	Not applicable	-
SR-7.6	Network and security configuration settings	Not applicable	-
SR-7.6-RE-1	Machine-readable reporting of current security settings	Not applicable	-
SR-7.7	Least functionality	Not applicable	-
SR-7.8	Control system component inventory	Not applicable	-

Recorded implementation and evidence

SR-1.1 - Human user identification and authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.1-RE-1 - Unique identification and authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.1-RE-2 - Multifactor authentication for untrusted networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.1-RE-3 - Multifactor authentication for all networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.2 - Software process and device identification and authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.2-RE-1 - Unique identification and authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.3 - Account management

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.3-RE-1 - Unified account management

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.4 - Identifier management

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.5 - Authenticator management

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.5-RE-1 - Hardware security for software process identity credentials

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.6 - Wireless access management

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.6-RE-1 - Unique identification and authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.7 - Strength of password-based authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.7-RE-1 - Password generation and lifetime restrictions for human users

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.7-RE-2 - Password lifetime restrictions for all users

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.8 - Public key infrastructure (PKI) certificates

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.9 - Strength of public key authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.9-RE-1 - Hardware security for public key authentication

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.10 - Authenticator feedback

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.11 - Unsuccessful login attempts

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.12 - System use notification

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.13 - Access via untrusted networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-1.13-RE-1 - Explicit access request approval

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.1 - Authorization enforcement

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.1-RE-1 - Authorization enforcement for all users

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.1-RE-2 - Permission mapping to roles

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.1-RE-3 - Supervisor override

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.1-RE-4 - Dual approval

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.2 - Wireless use control

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.2-RE-1 - Identify and report unauthorized wireless devices

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.3 - Use control for portable and mobile devices

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.3-RE-1 - Enforcement of security status of portable and mobile devices

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.4 - Mobile code

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.4-RE-1 - Mobile code integrity check

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.5 - Session lock

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.6 - Remote session termination

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.7 - Concurrent session control

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.8 - Auditable events

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.8-RE-1 - Centrally managed, system-wide audit trail

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.9 - Audit storage capacity

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.9-RE-1 - Warn when audit record storage capacity threshold reached

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.10 - Response to audit processing failures

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.11 - Timestamps

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.11-RE-1 - Internal time synchronization

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.11-RE-2 - Protection of time source integrity

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.12 - Non-repudiation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-2.12-RE-1 - Non-repudiation for all users

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.1 - Communication integrity

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.1-RE-1 - Cryptographic integrity protection

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.2 - Malicious code protection

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.2-RE-1 - Malicious code protection on entry and exit points

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.2-RE-2 - Central management and reporting for malicious code protection

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.3 - Security functionality verification

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.3-RE-1 - Automated mechanisms for security functionality verification

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.3-RE-2 - Security functionality verification during normal operation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.4 - Software and information integrity

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.4-RE-1 - Automated notification about integrity violations

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.5 - Input validation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.6 - Deterministic output

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.7 - Error handling

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.8 - Session integrity

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.8-RE-1 - Invalidation of session IDs after session termination

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.8-RE-2 - Unique session ID generation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.8-RE-3 - Randomness of session IDs

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.9 - Protection of audit information

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-3.9-RE-1 - Audit records on write-once media

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-4.1 - Information confidentiality

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-4.1-RE-1 - Protection of confidentiality at rest or in transit via untrusted networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-4.1-RE-2 - Protection of confidentiality across zone boundaries

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-4.2 - Information persistence

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-4.2-RE-1 - Purging of shared memory resources

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-4.3 - Use of cryptography

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.1 - Network segmentation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.1-RE-1 - Physical network segmentation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.1-RE-2 - Independence from non-control system networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.1-RE-3 - Logical and physical isolation of critical networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.2 - Zone boundary protection

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.2-RE-1 - Deny by default, allow by exception

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.2-RE-2 - Island mode

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.2-RE-3 - Fail close

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.3 - General purpose person-to-person communication restrictions

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.3-RE-1 - Prohibit all general purpose person-to-person communications

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-5.4 - Application partitioning

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-6.1 - Audit log accessibility

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-6.1-RE-1 - Programmatic access to audit logs

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-6.2 - Continuous monitoring

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.1 - Denial of service protection

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.1-RE-1 - Manage communication loads

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.1-RE-2 - Limit DoS effects to other systems or networks

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.2 - Resource management

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.3 - Control system backup

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.3-RE-1 - Backup verification

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.3-RE-2 - Backup automation

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.4 - Control system recovery and reconstitution

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.5 - Emergency power

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.6 - Network and security configuration settings

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.6-RE-1 - Machine-readable reporting of current security settings

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.7 - Least functionality

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

SR-7.8 - Control system component inventory

Not applicable

Implementation Assessed at system level: the EC-200 is a component inside the MX-540 machine, so the IEC 62443-3-3 system security requirements are recorded on the CNC Machining Center MX-540. Decision recorded 12 Feb 2026 (SEC-741).

Technical documentation (CRA Annex VII)

Status	Count
In place	8
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	8

Control	Requirement	Status	Evidence recorded
TD-1	General description of the product	In place	yes
TD-2	Design, development, production & vulnerability handling	In place	yes
TD-3	Cybersecurity risk assessment	In place	yes

Control	Requirement	Status	Evidence recorded
TD-4	Support-period determination	**In place**	yes
TD-5	Standards applied (or solutions adopted)	**In place**	yes
TD-6	Test reports	**In place**	yes
TD-7	Copy of the EU declaration of conformity	**In place**	yes
TD-8	SBOM available on request	**In place**	yes

Recorded implementation and evidence

TD-1 - General description of the product — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "TD-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

TD-2 - Design, development, production & vulnerability handling — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

TD-3 - Cybersecurity risk assessment — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "TD-3 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

TD-4 - Support-period determination — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

TD-5 - Standards applied (or solutions adopted) — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "TD-5" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

TD-6 - Test reports — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Configuration audit pack SCR-TD-6 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-TD-6/, cross-checked against hardening baseline HB-2.

TD-7 - Copy of the EU declaration of conformity — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Release checklist RC-2.1, gate "TD-7" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

TD-8 - SBOM available on request — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

User information (CRA Annex II)

Status	Count
In place	10
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	10

Control	Requirement	Status	Evidence recorded
UI-1	Manufacturer identity & contact	In place	yes
UI-2	Vulnerability reporting contact & CVD policy	In place	yes
UI-3	Product identification	In place	yes
UI-6	EU declaration of conformity location	In place	yes
UI-4	Intended purpose & security properties	In place	yes
UI-5	Foreseeable-misuse cybersecurity risks	In place	yes
UI-7	Support type & end-of-support date	In place	yes
UI-8	Detailed secure-use instructions	In place	yes
UI-9	SBOM availability to users	In place	yes
UI-10	Keep the user information current and available (Art. 13(18))	In place	yes

Recorded implementation and evidence

UI-1 - Manufacturer identity & contact — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-UI-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-UI-1/, cross-checked against hardening baseline HB-2.

UI-2 - Vulnerability reporting contact & CVD policy — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "UI-2" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

UI-3 - Product identification — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

UI-6 - EU declaration of conformity location — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "UI-6 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

UI-4 - Intended purpose & security properties — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

UI-5 - Foreseeable-misuse cybersecurity risks — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "UI-5" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

UI-7 - Support type & end-of-support date — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Configuration audit pack SCR-UI-7 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-UI-7/, cross-checked against hardening baseline HB-2.

UI-8 - Detailed secure-use instructions — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Release checklist RC-2.1, gate "UI-8" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

UI-9 - SBOM availability to users — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

UI-10 - Keep the user information current and available (Art. 13(18)) — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "UI-10 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

Compliance documentation (CRA Art. 28/30/31)

Status	Count
In place	9
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	9

Control	Requirement	Status	Evidence recorded
CD-1	EU declaration of conformity	In place	yes
CD-2	Conformity assessment completed	In place	yes
CD-3	CE marking	In place	yes
CD-9	Provide the EU DoC (or simplified DoC) with the product (Art. 13(20))	In place	yes

Control	Requirement	Status	Evidence recorded
CD-4	Technical documentation (Annex VII)	**In place**	yes
CD-5	User information & instructions (Annex II)	**In place**	yes
CD-6	Support-period record	**In place**	yes
CD-7	Software bill of materials	**In place**	yes
CD-8	Authorised representative - written mandate (Art. 18)	**In place**	yes

Recorded implementation and evidence

CD-1 - EU declaration of conformity — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CD-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CD-2 - Conformity assessment completed — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CD-3 - CE marking — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CD-3" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CD-9 - Provide the EU DoC (or simplified DoC) with the product (Art. 13(20)) — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Configuration audit pack SCR-CD-9 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CD-9/, cross-checked against hardening baseline HB-2.

CD-4 - Technical documentation (Annex VII) — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "CD-4" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CD-5 - User information & instructions (Annex II) — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CD-6 - Support-period record — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CD-6 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CD-7 - Software bill of materials — **In place**

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CD-8 - Authorised representative - written mandate (Art. 18) — **In place**

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CD-8" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

Gap analysis

1 open item(s) across 1 control set(s).

Component security (IEC 62443-4-2)

- CR-7.3 Control system backup - Planned

Recommendations

Priority: Planned

1. Execute the plan for CR-7.3 (Control system backup) - Component security (IEC 62443-4-2).

Evidence and attachments

183 of 283 requirement(s) carry recorded evidence; it is printed with each requirement under "Recorded implementation and evidence".

File attachments per requirement are kept in the project folder under evidence/ and travel with the audit binder export, in the same control-by-control structure.

Review and sign-off

Role	Name	Date	Signature
Prepared by			
Reviewed by			
Approved by (management)			