TECHNICAL CYBERSECURITY ASSESSMENT

CRA Technical Assessment Scope

Scope, method, required inputs and acceptance criteria for the technical assessment

PUBLIC DEMONSTRATION SAMPLE

Field	Value
Document	CRA Technical Assessment Scope
Code	SLX-CRA-SCOPE-001-EN
Version	1.0
Date	16 August 2026
Customer / Project	Application case — IG-200 Industrial Edge Gateway
Classification	Public demonstration sample

> This public sample illustrates structure, terminology and level of detail. Customer data, product data and findings are illustrative and the file must not be represented as a real assessment, certification or CRA conformity evidence.

How to use this document

“CRA Technical Evidence Pack” is the Silicon LogiX commercial name for this engineering service; it is not the name of a document prescribed by Regulation (EU) 2024/2847. The Pack organizes technical evidence, gaps and actions that can support the manufacturer’s technical documentation and conformity path.

> It does not replace the manufacturer’s responsibility, legal advice, an EU declaration of conformity, CE marking or any conformity assessment that may require a notified body.

1. Engagement objective

Assess the product’s technical readiness for the cybersecurity aspects relevant to a Cyber Resilience Act path by reconstructing the product baseline, software components, exposed surface, update mechanisms, vulnerability handling and availability of technical evidence.

- Establish a repeatable hardware, firmware/software and connected-service baseline.
- Identify available, missing and unverified evidence.

- Produce or normalize the software inventory and SBOM for the agreed release where material allows.
- Connect technical findings to relevant Annex I areas and Annex VII documentation elements.
- Prioritize engineering work for the customer team or a separate Silicon LogiX remediation engagement.

2. Product and assessment boundary

Field	Agreed baseline
Product	IG-200 Industrial Edge Gateway
Hardware	Rev. B · ARM Cortex-A53 · 1 GB RAM · 8 GB eMMC · 2× GbE · isolated RS-485 · USB service · UART/JTAG
Software	IGOS 2.4.1 · U-Boot 2024.01 · Linux 6.1 LTS · Gateway Core 3.2.0 · Web UI 1.8.2
Connectivity	HTTPS Web UI/REST · MQTT 5/TLS 1.3 outbound · Modbus RTU/TCP
Update	Signed A/B images distributed by the release service; local USB recovery
Support period	5 years from placing on the market — rationale to be completed
Boundary	Product HW/SW baseline, interfaces and update path; unrelated corporate infrastructure and legal assessment excluded

Baseline rule: every conclusion is tied to an identifiable product configuration. Later HW/SW changes can invalidate evidence and require a delta assessment.

3. Material requested from the product team

Category	Requested evidence	Baseline need
Product	One or two samples or controlled remote access; serial number and HW revision	Required
Firmware / software	Binaries, release notes, build configuration and source repositories when in scope	Required
Architecture	Block diagram, interfaces, trust boundaries and main data/control flows	Required
Dependencies	Manifests, package locks, licences, third-party and open-source components	Preferred
Update	A/B, service and recovery procedures; signing, verification, rollback and distribution	Required
Security controls	Credentials, roles, provisioning, secure boot/debug policy and logging	Required
Vulnerability handling	CVD, reporting contact, triage, advisories and CVE/component tracking	Preferred
Lifecycle	Support-period rationale, cadence, EOL/EOS and decommissioning	Preferred

4. Assessment activities

1. Technical kick-off and baseline freeze: product, variants, intended use, owners and boundaries.
2. Product inventory and architecture reconstruction: components, flows, dependencies and trust boundaries.
3. SBOM and dependency review: top-level and transitive components where technically available; agreed machine-readable format.
4. Attack-surface review: physical and logical interfaces, services, protocols, roles, credentials, maintenance and debug.
5. Security-control review: defaults, access control, integrity/confidentiality, logging, hardening and risk-based mitigations.
6. Update and recovery review: authenticity, integrity, distribution, rollback, failure handling and recovery.
7. Vulnerability-handling review: component monitoring, intake, triage, remediation, advisories and support-period operation.
8. Evidence mapping, findings, priorities, owners, remediation targets and closure criteria.

5. Evidence and readiness classification

Level	Meaning
VERIFIED	Observed on the device, configuration, source or a repeatable test.
DOCUMENTED	Supported by traceable documentation/version, but not repeated in the assessment.
DECLARED	Provided by the team without sufficient evidence at assessment time.
NOT VERIFIED	Material unavailable, component outside scope or check not planned.

Status	Use in the report
OK	Evidence is coherent with the reviewed criterion in the agreed scope; this is not certification.
PARTIAL	A control/evidence exists but is incomplete, inconsistent or insufficiently traceable.
GAP	A relevant control/process is missing or evidence is absent with material readiness impact.
N/A	Not applicable to the baseline, with a rationale to be validated in the conformity path.
NOT VERIFIED	No conclusion can be made.

6. Outputs and acceptance

Output	Purpose
Management Summary	Decision view: top findings, ownership and 30/60/90-day path.
CRA Technical Evidence Pack	Baseline, architecture, SBOM summary, attack surface, technical risk, mapping, findings and remediation.
SBOM snapshot / inventory	Release-tied component traceability in an agreed format when technically reconstructible.
Findings register and evidence index	IDs, evidence, impact, priority, owner, status, target release and closure records.

7. Exclusions and responsibility

- Legal opinion, binding CRA scope determination, certification, CE marking or EU declaration of conformity.
- Full penetration test, red team, accredited laboratory, safety or EMC assessment unless separately agreed.
- Cloud, mobile apps or customer infrastructure not expressly included.
- A guarantee that the product has no vulnerabilities or continuous monitoring after delivery.
- The manufacturer retains responsibility for product classification, technical-document completeness and the chosen conformity procedure.

8. Operational phases and change control

Phase	Output	Gate
A · Baseline and discovery	Confirmed scope, evidence request, product map	Baseline frozen
B · Technical assessment	SBOM, surface, control review and risk evidence	Technical review
C · Reporting	Pack, summary, register and roadmap	Delivery and comment cycle
D · Remediation (optional)	Product changes, hardening, tooling and closure evidence	New release + delta verification

New variants, components, services or releases found after the baseline freeze are recorded as a change request or open point so evidence from different products is not mixed.

Official references

Regulation (EU) 2024/2847 — official text

European Commission — Cyber Resilience Act

European Commission guidance C(2026) 5252, published 27 July 2026

Verified on 16 August 2026. The Commission guidance is non-binding. Later implementing acts, harmonised standards, common specifications and guidance must be reviewed before any real engagement.