



TECHNICAL CYBERSECURITY ASSESSMENT

CRA Technical Assessment — Management Summary

Decision summary for management, product owners and R&D leads

PUBLIC DEMONSTRATION SAMPLE

Field	Value
Document	CRA Technical Assessment — Management Summary
Code	SLX-CRA-MGMT-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. Executive snapshot

Readiness conclusion: IG-200 already implements useful controls, but technical preparation should not be considered complete. Five high-priority gaps require action in SBOM/build provenance, update/recovery, production debug and vulnerability handling.

Domain	Status	Management message
--------	--------	--------------------

Architecture and baseline	OK	Product, release and trust boundaries are identifiable.
SBOM and dependencies	GAP	A reconstructed snapshot exists; a deterministic build-generated release SBOM is missing.
Update and recovery	GAP	Recovery does not apply the same authentication as the standard A/B path.
Access and hardening	PARTIAL	Web identity needs completion; JTAG/UART and production configuration need governance.
Vulnerability handling	GAP	CVD, a security contact and release gate must be formalized.
Lifecycle evidence	PARTIAL	The support period is declared but not yet technically justified.

Decision requested: authorize technical remediation in two tranches — critical prerequisites for the next release, then evidence automation and lifecycle consolidation within 90 days.

2. Product and scope

Field	Scope
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

Reference architecture and assessment boundary

OT / field assets	IG-200 product baseline	IT / operational services
PLCs, sensors and I/O Modbus RTU/TCP RS-485 / Ethernet	HW Rev. B · ARM Cortex-A53 IGOS 2.4.1 · Linux 6.1 LTS Gateway Core · Web UI/API U-Boot · A/B update · UART/JTAG	MQTT broker · REST API Device inventory Release repository

Trust boundaries considered: field network, local maintenance, device identity and credentials, outbound MQTT/TLS channel, release service, physical debug and USB recovery.

3. Top five findings

ID	Area	Finding	State	Priority
IG200-F-001	Update / recovery	Recovery image does not receive the same authenticity verification as the standard A/B path.	GAP	HIGH
IG200-F-002	Hardware hardening	Production JTAG/UART access is not governed by a documented protection policy.	GAP	HIGH
IG200-F-003	SBOM / release	A reconstructed CycloneDX snapshot exists, but no deterministic build-generated release SBOM is available.	GAP	HIGH
IG200-F-004	Vulnerability handling	No public CVD policy and no dedicated security reporting contact.	GAP	HIGH
IG200-F-007	Release gate	No formal gate for known-vulnerability review before product release.	GAP	HIGH

4. 30 / 60 / 90-day roadmap

Window	Objective	Actions	Closure indicator
0–30 days	Reduce high-priority risk	Align recovery verification; start SBOM pipeline; define debug policy, CVD/contact and vulnerability release gate.	Negative update tests pass; policies approved; release checklist active.
30–60 days	Make evidence repeatable	Automated SBOM, service inventory, security logging and authentication hardening.	SBOM tied to IGOS; socket/service inventory; event coverage and account tests.
60–90 days	Consolidate lifecycle	Support-period rationale, decommissioning instructions, retest and closure report.	Lifecycle memo; updated docs; findings closed against evidence IDs.

5. Decisions and ownership

Decision	Suggested owner	Target
Confirm HW Rev. B and IGOS 2.4.1 as the remediation baseline.	Product + R&D	Remediation kick-off
Approve the A/B update and recovery-chain change.	Firmware lead	Before IGOS 2.5.x
Define the production debug/provisioning policy.	HW + Manufacturing	Before the next production batch
Appoint the vulnerability-handling owner and security contact.	Management + Product	Before the reporting runbook is exercised

Approve the support-period rationale and maintenance ownership.	Product + Management	Lifecycle consolidation
---	----------------------	-------------------------

6. Commercial next step

The assessment converts a broad regulatory topic into an assignable backlog: product/version, finding, owner, priority, required evidence and target release. Silicon LogiX can then implement firmware/software remediation under a separately scoped baseline and verify closure on the next product release.

Assessment → evidence → gap → remediation → retest → improved product baseline

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.

DEMONSTRATION SAMPLE - NOT VALID FOR CONFORMITY EVIDENCE