TECHNICAL CYBERSECURITY ASSESSMENT

CRA Technical Evidence Pack

Technical evidence, gap analysis and remediation roadmap for a connected embedded product

PUBLIC DEMONSTRATION SAMPLE

Field	Value
Document	CRA Technical Evidence Pack
Code	SLX-CRA-TEP-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 technical summary

The IG-200 application case starts from a versioned industrial gateway and organizes hardware, firmware, dependencies, exposed interfaces, update/recovery, vulnerability handling and lifecycle evidence into a traceable engineering picture.

Assessment status	Areas	Interpretation

OK	8	Verified/documented controls usable in the agreed technical scope.
PARTIAL	7	Controls or evidence exist but are incomplete or inconsistent.
GAP	5	Material control/process gaps requiring remediation.
NOT VERIFIED	2	No conclusion because evidence or scope is insufficient.

Overall result: the baseline contains useful controls (TLS 1.3, A/B update, roles and factory reset), but release SBOM, recovery trust, debug governance, coordinated disclosure and vulnerability release checks are not yet adequate as a coherent evidence chain.

Top-priority 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

2. Product baseline

Field	Identified configuration
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. Intended use and critical assets

IG-200 is integrated into industrial machinery to collect telemetry, expose local data, receive authorized parameters and publish data to an MQTT broker. Direct Internet exposure is not intended, but field networks, service access and physical access are treated as reasonably foreseeable conditions.

Asset	Security objective	Impact if compromised
Firmware and boot chain	Integrity / authenticity	Unauthorized code execution and persistence
Credentials and keys	Confidentiality / integrity	Unauthorized access and impersonation
Machine configuration	Integrity / availability	Incorrect parameters or service outage
Telemetry	Integrity / context-based confidentiality	Bad decisions or operational-data leakage
Update package	Authenticity / integrity	Installation of altered releases
Security logs	Integrity / availability	Reduced event detection and reconstruction

4. Software inventory and SBOM state

Starting from the preliminary inventory, the assessment reconstructed a CycloneDX snapshot for IGOS 2.4.1. It is not yet generated deterministically by the build pipeline or associated with the distributed A/B image; finding IG200-F-003 therefore remains open.

Component	Version	Origin	Role	Evidence
Gateway Core	3.2.0	Proprietary	Protocol bridge / REST API	Build manifest
U-Boot	2024.01	Open source	Boot, verification, rollback	Repository tag
Linux kernel	6.1.y	Open source	Kernel	Component manifest
BusyBox	1.36.1	Open source	Userland/services	Component manifest
OpenSSL	3.0.13	Open source	TLS / crypto	Component manifest
libmodbus	3.1.10	Open source	Modbus RTU/TCP	Manual inventory

5. Exposed surface

Interface	Exposure	Observed control	State	Action
HTTPS / REST	Plant network	TLS + role login	OK	Keep service/config inventory tied to release
MQTT 5/TLS 1.3	Outbound	Server certificate + device credential	OK	Backend remains outside the assessed boundary
Modbus TCP	Field network	Incomplete command/ACL matrix	PARTIAL	Limit functions and document network assumptions
USB service	Physical	Recovery tool	PARTIAL	Apply equivalent image authentication
JTAG	Physical	Production test pads	GAP	Define protection state and authorized recovery
UART service	Internal	Header not populated	PARTIAL	Formalize production and logging policy

6. Technical cybersecurity risk excerpt

Illustrative method: inherent risk = likelihood (1–5) × impact (1–5). Residual risk only credits verified or documented controls. This is an internal prioritization method, not a CRA-prescribed scale.

Scenario	Asset	L	I	Inherent	Residual
Unauthorized IGOS installation through recovery	Firmware	3	5	15 · High	12 · High
Debug access to a field device	Keys/config	3	4	12 · High	9 · Medium
Compromised Web UI administrator credential	Config/UI	3	4	12 · High	6 · Medium
Manipulation of cloud traffic	Telemetry	2	4	8 · Medium	3 · Low
Undetected vulnerable Linux component	Firmware	3	4	12 · High	8 · Medium
Loss of security-event traceability	Logs	3	3	9 · Medium	6 · Medium

7. Annex I, Part I — working technical mapping

Ref.	Technical area	State	Observation
I.1	Cybersecurity level appropriate to risk	PARTIAL	Risk model exists; security baseline needs formalization.
I.2(a)	No known exploitable vulnerability at market release	NOT VERIFIED	End-to-end release process was not verified.
I.2(b)	Secure by default	PARTIAL	Modbus, REST and service interfaces need review.
I.2(c)	Vulnerabilities addressable through security updates	PARTIAL	Recovery verification is not equivalent.
I.2(d)	Protection from unauthorized access	PARTIAL	Production JTAG/UART is not governed.
I.2(e–g)	Confidentiality, integrity and minimisation	OK/PARTIAL	TLS is verified; recovery/configuration evidence remains incomplete.
I.2(h–i)	Availability and network impact	OK	Watchdog, safe behavior and reconnect backoff reviewed.
I.2(j–l)	Surface, impact mitigation and security logging	GAP/PARTIAL	Service inventory, privilege baseline and event coverage are incomplete.
I.2(m)	Secure removal of data/settings	OK	Factory reset verified on sample.

8. Annex I, Part II — vulnerability handling

Area	Current evidence	State	Target action
Components, vulnerabilities and machine-readable SBOM	Preliminary inventory; reconstructed snapshot	PARTIAL	Automate and tie to the release
Remediation without delay / security updates	Informal internal process	GAP	Define triage, ownership, SLA and release flow
Regular security testing and review	Regression tests; sporadic review	PARTIAL	Define cadence and security gates
Disclosure of corrected vulnerabilities	Generic release notes	GAP	Create advisory workflow and template
Coordinated vulnerability disclosure	No public policy	GAP	Publish policy, scope and reporting channel
Secure update distribution	Signed A/B; different recovery policy	PARTIAL	Unify verification policy

9. Update, rollback and recovery

Path	Package	Verification	Rollback	State
Remote A/B update	Signed bundle	Signature + hash in bootloader	A/B + last-known-good	OK
Local service update	Signed bundle	Signature + hash in bootloader	Manual	OK
USB recovery	Raw service image	Hash only	Recovery-only	GAP
Factory programming	Provisioning image via JTAG	Procedural control	N/A	PARTIAL

IG200-F-001 · HIGH — every path capable of installing persistent firmware should apply equivalent image authentication. Closure requires negative tests for invalid signatures, unauthorized downgrade, corrupted images and interrupted updates.

10. Security test evidence

Test / review	Baseline	Outcome	Evidence ID
Update tamper test	IGOS 2.4.1	Pass on A/B · Fail on recovery	IG200-E-UPD-004
TLS server validation	IGOS 2.4.1	Pass	IG200-E-NET-011
Default credential review	Factory image	Pass	IG200-E-ID-003
Debug access review	HW Rev. B	Readiness fail	IG200-E-HW-007
Factory reset / data erase	IGOS 2.4.1	Pass	IG200-E-DATA-002
Security log coverage	IGOS 2.4.1	Partial	IG200-E-LOG-006

11. Findings register

ID	Area	Finding	State	Priority	Owner
IG200-F-001	Update/recovery	Recovery authentication not equivalent	GAP	HIGH	Firmware
IG200-F-002	HW hardening	Production JTAG/UART policy absent	GAP	HIGH	HW/ Firmware
IG200-F-003	SBOM	No deterministic build-generated release SBOM	GAP	HIGH	Build/ Release
IG200-F-004	Vulnerability handling	CVD policy and security contact absent	GAP	HIGH	Product/ Security
IG200-F-005	Lifecycle	Support-period rationale not documented	PARTIAL	MEDIUM	Product/R&D
IG200-F-006	Logging	Incomplete administrative/security event coverage	PARTIAL	MEDIUM	Firmware
IG200-F-007	Release gate	Known-vulnerability gate absent	GAP	HIGH	Release/ Security
IG200-F-008	Attack surface	Service, privilege and UART inventory incomplete	PARTIAL	MEDIUM	Gateway/ Mfg.
IG200-F-009	Identity	Admin provisioning and lockout incomplete	PARTIAL	MEDIUM	Firmware
IG200-F-010	Decommissioning	User instructions not formalized	PARTIAL	LOW	Product docs

12. Remediation roadmap

Window	Objective	Findings / actions	Verifiable output
0–30 days	Close critical prerequisites	F-001 recovery; F-002 debug; F-003 SBOM; F-004 CVD/contact; F-007 release gate	Recovery tests, JTAG policy, SBOM pipeline, CVD draft and release checklist
30–60 days	Make the release traceable	F-006 logging; F-008 service inventory; F-009 identity hardening	Service inventory, event catalog, negative auth tests and SBOM delta check
60–90 days	Consolidate lifecycle evidence	F-005 rationale; F-010 user/decommission docs; retest	Lifecycle memo, updated instructions and closure evidence
Continuous	Maintain evidence and vulnerabilities	Dependency monitoring, review cadence, advisory/reporting runbook	Recurring process records and dashboard

13. Annex VII evidence map — excerpt

Ref.	Evidence element	Pack location	Coverage
VII.1	General description, intended use, SW versions and user information	Sections 2–3 + product docs	PARTIAL
VII.2(a)	Design/development and system architecture	Section 2 + IG200-E-ARCH-*	OK
VII.2(b)	Vulnerability handling, SBOM, CVD and secure update	Sections 4, 8–9	PARTIAL
VII.2(c)	Production, monitoring and validation	Manufacturing docs	NOT VERIFIED
VII.3	Cybersecurity risk assessment	Sections 6–8	PARTIAL
VII.4	Support-period information	Lifecycle evidence	PARTIAL
VII.6	Security/conformity test reports	Section 10 + evidence index	PARTIAL
VII.7	EU declaration of conformity	Not included	N/A

14. Evidence index

Evidence ID	Description	Type	Level
IG200-E-ARCH-001	IG-200 HW Rev. B system architecture	Diagram/ document	DOCUMENTED
IG200-E-SBOM-002	Reconstructed CycloneDX snapshot for IGOS 2.4.1	JSON	DOCUMENTED
IG200-E-UPD-004	Update tamper negative test	Test report	VERIFIED
IG200-E-HW-007	Debug access inspection	Test note/photo	VERIFIED

IG200-E-NET-011	TLS invalid-certificate test	Test log	VERIFIED
IG200-E-ID-003	Factory credential provisioning note	Manufacturing note	DOCUMENTED
IG200-E-DATA-002	Factory-reset verification	Test report	VERIFIED
IG200-E-LOG-006	Security-event coverage review	Review note	VERIFIED

Appendix A — illustrative SBOM snapshot

Component	Version	Licence	Supplier	Identifier
Gateway Core	3.2.0	Proprietary	Silicon LogiX	pkg:generic/gateway-core@3.2.0
U-Boot	2024.01	GPL-2.0-or-later	DENX / project	pkg:generic/u-boot@2024.01
Linux kernel	6.1.y	GPL-2.0-only	Linux community	pkg:generic/linux@6.1
BusyBox	1.36.1	GPL-2.0-only	BusyBox project	pkg:generic/busybox@1.36.1
OpenSSL	3.0.13	Apache-2.0	OpenSSL project	pkg:generic/openssl@3.0.13
libmodbus	3.1.10	LGPL-2.1-or-later	libmodbus project	pkg:generic/libmodbus@3.1.10

Appendix B — complete finding record example

Field	Value
Finding ID	IG200-F-001
Title	Recovery path: image authenticity is not uniformly verified
Area / state / priority	Update and boot chain · GAP · HIGH
Baseline	HW Rev. B · IGOS 2.4.1 · U-Boot 2024.01
Evidence	IG200-E-UPD-004, IG200-E-ARCH-001
Suggested owner / target	Firmware / Product Security · IGOS 2.5.x
Observation	The standard A/B path verifies signature and digest; USB recovery only verifies integrity by hash.
Technical impact	A local actor could attempt installation of an unauthorized image, weakening the boot/update trust chain.
Recommended action	Use equivalent authentication on A/B, service and recovery; test invalid signature, downgrade, corruption and interruption.
Closure evidence	Negative test report, updated bootloader/recovery baseline, update-chain description and approved closure record.

Remediation support

Silicon LogiX can continue from assessment into firmware/software implementation, update-chain review, SBOM automation and production of closure evidence. Remediation is quoted and baselined separately so changes and retests remain traceable.

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.