Technical Documentation

EX-GW-4200-TD-2026-001 · Annex VII, Regulation (EU) 2024/2847 (Cyber Resilience Act)

Product	Gateway firmware v2.4 — EX-GW-4200 Industrial IoT Gateway
Firmware version	2.4.1 (build 2.4.1-rc0)
Manufacturer	Example Industries GmbH, Musterstrasse 12, 80331 Munich, Germany
Placed on the market	September 2026
Product class	Default (self-assessment)
Document date	16 August 2026

This technical file follows the contents required by Annex VII. Each section below maps to one Annex VII element. Data shown is a fictional example for demonstration.

1. General description of the product

Intended purpose. An industrial edge gateway that aggregates data from field devices and forwards it to cloud services. It performs protocol translation (Modbus RTU/TCP, OPC UA to MQTT) and local buffering.

Versions. Hardware revision C; firmware 2.4.1 (build 2.4.1-rc0). This documentation covers the 2.4.x firmware line.

Attribute	Value
Type / model	EX-GW-4200 Industrial IoT Gateway
Processor	ARM Cortex-A53, 1.2 GHz quad-core
Interfaces	2x Ethernet, RS-485, USB-C (service), optional LTE
Connectivity	MQTT over TLS 1.3, HTTPS, OPC UA
Update mechanism	Signed over-the-air (A/B partitions, rollback)

2. Design, development, production and vulnerability handling

Development process. Source control with mandatory peer review; reproducible builds; static analysis and dependency scanning in CI. Release firmware is signed; keys held in an HSM.

Production. Firmware provisioned in a controlled facility; secure boot fuses set; per-device identity injected.

Vulnerability handling process. The SBOM (section 8) is monitored daily against vulnerability databases. Findings are triaged (fix now / planned fix / not applicable / accepted risk) and recorded. A public contact (compliance@example-industries.example) receives disclosures. Security updates are issued free of charge for the support period (until 11 December 2031). Actively exploited vulnerabilities trigger the 24-hour early-warning report to ENISA.

3. Cybersecurity risk assessment

Risks were assessed against the essential requirements of Annex I. Summary of principal risks and mitigations:

Risk	Assessment	Mitigation
Unauthorised remote access	High impact, medium likelihood	No default passwords, TLS 1.3, role-based access, maintenance SSH bound to local interface
Tampered firmware update	High impact, low likelihood	Signed OTA, secure boot, A/B rollback
Vulnerable third-party component	Medium impact, medium likelihood	SBOM monitoring, scheduled patching, support-period updates
Data exposure in transit	Medium impact, low likelihood	TLS 1.3 for all external traffic; AES-256 at rest
Denial of service / instability	Medium impact, medium likelihood	Watchdog, resource limits, rollback recovery

4. Essential requirements (Annex I) and how they are met

Requirement	How it is addressed
Secure by default	Shipped with no default passwords; first-boot forces a unique credential. Only required network services are enabled.
Protection of data	Configuration and telemetry encrypted at rest (AES-256); all external communication over TLS 1.3.
Access control	Role-based access with per-account credentials; SSH restricted to the local maintenance interface.
Resilience / availability	Watchdog and A/B partition recovery; a failed update rolls back to the last-known-good image.
Minimise attack surface	Unused interfaces and services disabled in the production build; debug console removed.
Security updates	Signed over-the-air updates; security fixes provided free of charge for the support period.
Vulnerability handling	Documented process, public security contact, and SBOM-based monitoring (see technical documentation, section 2 and 8).

5. Harmonised standards applied

Standard	Title
EN 18031-1:2024	Common security requirements for radio equipment and products with digital elements
ETSI EN 303 645 V2.1.1	Cyber security for consumer Internet of Things: baseline requirements
IEC 62443-4-2:2019	Technical security requirements for IACS components
EN ISO/IEC 27001:2023	Information security management systems

6. Reports of tests performed

Test	Method	Result
Authenticated vulnerability scan	Internal, automated (release 2.4.1)	Pass — no open critical/high findings
TLS configuration review	Protocol/cipher audit	Pass — TLS 1.3 only, strong ciphers
Secure boot / signed update	Tampered-image rejection test	Pass — unsigned image rejected, rollback verified
Default credential check	First-boot provisioning test	Pass — unique credential enforced
Fuzzing of MQTT/OPC UA parsers	Interface fuzzing, 24h	Pass — no crashes or memory faults

7. EU Declaration of Conformity

A signed EU Declaration of Conformity (EX-GW-4200-DoC-2026-001) is issued for this product and held with this technical file.

8. Software Bill of Materials (SBOM)

Top-level components of firmware 2.4.1 (build 2.4.1-rc0). The complete machine-readable SBOM is maintained in CycloneDX format and updated on every release.

Component	Version	Licence	Role	Vulnerability status
Linux kernel	6.6.30	GPL-2.0-only	Operating system kernel	Monitored — no known exploited vulnerabilities
BusyBox	1.36.1	GPL-2.0-only	Core userland utilities	Monitored — no open critical findings
OpenSSL	3.0.13	Apache-2.0	TLS and cryptography	Monitored — patched to 3.0.13
Mbed TLS	3.6.0	Apache-2.0	TLS for constrained services	Monitored — no open findings
lwIP	2.2.0	BSD-3-Clause	TCP/IP stack	Monitored — no known exploited vulnerabilities
Eclipse Mosquitto	2.0.18	EPL-2.0	MQTT broker	Monitored — no open critical findings
Dropbear SSH	2022.83	MIT	SSH server for maintenance	Monitored — planned update to 2024.85
curl	8.7.1	curl (MIT-like)	HTTPS client for updates	Monitored — no open findings
zlib	1.3.1	Zlib	Compression library	Monitored — no open findings
Wolfson OTA agent	1.2.0	Proprietary (in-house)	Signed over-the-air update client	Maintained in-house

This is an illustrative sample populated with fictional data for demonstration. It is not a valid technical file and must not be submitted to any authority or customer.