modibus

CYBERSECURITY WHITEPAPER

Aligned with IEC 62443.

How the Modibus MB-213 platform — hardware, ModiOS, and MDS Cloud — is designed against the IEC 62443-4-2 component requirements and the IEC 62443-4-1 secure development lifecycle.

CERTIFICATIONS & CONFORMANCE

CE	ISO 9001	IEC 62443-1	ISO 27001	ISO 27017
EUROPEAN CONFORMITY	QUALITY MANAGEMENT	INDUSTRIAL CYBERSECURITY	INFORMATION SECURITY	CLOUD SECURITY

SEVEN FOUNDATIONAL REQUIREMENTS COVERED

FR1	FR2	FR3	FR4	FR5	FR6	FR7
Identification & Authentication	Use Control	System Integrity	Data Confidentiality	Restricted Data Flow	Timely Event Response	Resource Availability

HARDWARE

Secure boot · A/B partitions · Signed firmware

PROCESS

SBOM · SAST/DAST · Coordinated disclosure

Written for security architects, OT cyber leads, and integrator security teams.

Twelve pages of substance — not marketing claims.

security@modibus.com

EXECUTIVE SUMMARY

A Plain Statement of How We Approach Security

Industrial remote access has become one of the most attacked surfaces in operational technology. A gateway sitting between the public internet and a customer's PLCs is a prime target — and a prime liability if the vendor treats security as a marketing slide. This document is the **opposite** of a marketing slide: a structured, IEC 62443-aligned account of how the Modibus MB-213 platform is built, hardened, and operated.

IN SCOPE

- **Hardware — MB-213 + CM-series modules.** Bill of materials, supply-chain integrity, secure-boot chain, hardware-backed key storage where supported.
- **ModiOS firmware.** Hardened embedded OS with A/B partitions, signed updates, and rollback protection.
- **MDS Cloud platform.** Multi-tenant remote-access service: identity, RBAC, audit, integration APIs.
- **Vendor process.** Secure development lifecycle, vulnerability disclosure, customer notification.

COMPLIANCE POSTURE (MAY 2026)

STANDARD / PROGRAMME	STATUS	SCOPE / NOTES
CE	Certified	European Conformity (EMC, RoHS, RED) for the MB-213 product family
ISO 9001	Certified	Quality Management System — product development & manufacturing
IEC 62443-1	Certified	Industrial cybersecurity framework conformance
ISO 27001	Certified	Information Security Management System — corporate & cloud
ISO 27017	Certified	Cloud security controls — MDS Cloud platform
SBOM (SPDX 2.3)	Active	Shipped with every firmware release
Coordinated Vulnerability Disclosure	Active	security@modibus.com / PGP key on website

FIVE DESIGN PRINCIPLES

1. **Defense in depth.** Hardware, firmware, network, application, and cloud layers each enforce security independently.
2. **Secure by default.** Out-of-the-box configuration is the secure configuration — no permissive defaults to remember to disable.
3. **Least privilege.** Every user, every device, every service runs with the minimum permissions required.
4. **Outbound-only architecture.** No inbound listening services on the customer's network — ever.
5. **Transparent operations.** Every session, every config change, every cert renewal is audit-logged and exportable to the customer's SIEM.

★ **Disclosure-first stance:** Modibus operates a coordinated vulnerability disclosure programme with published response SLAs. We will tell customers about a vulnerability before it's public — even when it's embarrassing. Trust is built on what we tell you when things go wrong, not on what we claim when everything looks fine.

SECTION 1 · THREAT LANDSCAPE

Why Remote Access Got Dangerous

The convenience that makes industrial remote access valuable — one tunnel from anywhere to a PLC at the edge of a critical process — is exactly what makes it attractive to attackers. The historical record is unkind to vendors who treated this surface casually.

A DECADE OF INDUSTRIAL INCIDENTS

YEAR	INCIDENT	LESSON FOR REMOTE-ACCESS VENDORS
2010	**Stuxnet** · Iranian uranium centrifuges	Air-gaps fail; supply-chain firmware integrity matters as much as network defense.
2017	**Triton / Trisis** · Saudi petrochemical SIS	Attackers will target the safety layer specifically. Privileged engineering access is the prize.
2020	**SolarWinds** · supply-chain compromise	Signed updates from a trusted vendor are the new attack vector. Build pipeline security is non-optional.
2021	**Colonial Pipeline** · legacy VPN credential	One stale VPN account, no MFA, took down the East Coast fuel supply for a week.
2021	**Oldsmar water** · treatment-plant takeover	Shared TeamViewer credentials on a remote-access workstation; sodium hydroxide level changed remotely.
2024	**Ivanti / Pulse Secure** · VPN concentrator zero-days	Inbound-listening VPN appliances are a high-value attack target. Outbound-only changes the attack economics.

COMMON ATTACK VECTORS AGAINST INDUSTRIAL REMOTE ACCESS

- **Credential stuffing & credential reuse.** Operator passwords from unrelated breaches sprayed against the vendor portal. Without MFA, this works depressingly often.
- **Compromised inbound-listening VPN appliances.** Pulse Secure, Citrix ADC, and Ivanti Connect Secure all shipped zero-days exploited in the wild against industrial customers.
- **Supply-chain firmware compromise.** A signed update from a trusted vendor — trojaned in the build pipeline — bypasses every network control.
- **Default or weak credentials.** Field devices reachable from the internet because the gateway forwarded a port and nobody changed `admin / admin`.
- **Pivoting through the gateway.** An attacker in the IT network uses the gateway's legitimate trust relationship to reach the OT segment.
- **Legacy protocols on the wire.** Modbus, DNP3, S7comm in cleartext, with no authentication, exposed to a flat network.

MODIBUS POSITION

The MB-213 platform is designed against this exact threat list. **Outbound-only architecture** eliminates inbound attack surface. **Mandatory 2FA + per-device certificates** defeat credential stuffing. **Signed firmware with hardware root-of-trust** closes the supply-chain vector. **Network segmentation via CM-216** contains pivot range. The control set is detailed across the next sections, mapped to IEC 62443 foundational requirements.

SECTION 2 · STANDARDS

IEC 62443 in 60 Seconds

IEC 62443 is the international family of standards for cybersecurity in industrial automation and control systems (IACS). It is structured by **audience** — what the asset owner has to do, what the system integrator has to do, what the component vendor has to do — and graded by **security level**.

THE FOUR SERIES

SERIES	AUDIENCE	WHAT IT COVERS
62443-1-x	General	Concepts, models, terminology. Foundational reading for everyone.
62443-2-x	Asset owner / operator	Security programme requirements for the organisation running the IACS. Includes patch management policy, segmentation, training.
62443-3-x	System integrator	System-level security: zones, conduits, the security capability of an integrated solution.
62443-4-x	**Component vendor**	**This is where MB-213 lives.** 4-1 covers the secure development process; 4-2 covers technical requirements for the component itself.

SECURITY LEVELS (SL) AT A GLANCE

SL 0	SL 1	**SL 2**	SL 3	SL 4
No specific requirements	Casual or coincidental violation	Intentional violation, simple means, low resources	Sophisticated means, moderate resources	Sophisticated means, extended resources, IACS-specific skills

The MB-213 platform **implements technical controls aligned with SL 2 capabilities** across the seven foundational requirements. The architecture supports a path to SL 3 on selected requirements where the customer's deployment context warrants it — primarily in cryptographic key handling and physical tamper resistance.

THE SEVEN FOUNDATIONAL REQUIREMENTS (FR)

FR 1 · IAC
Identification & Authentication Control
Who is allowed in, and how do we prove it?

FR 2 · UC
Use Control
What are they allowed to do once in?

FR 3 · SI
System Integrity
Is the system in the state we expect?

FR 4 · DC
Data Confidentiality
Is sensitive data protected at rest and in transit?

FR 5 · RDF
Restricted Data Flow
Are zones and conduits enforced?

FR 6 · TRE
Timely Response to Events
Do we see attacks as they happen?

FR 7 · RA
Resource Availability
Can we keep operating under attack or fault?

Sections 4–6 of this whitepaper map every Modibus control to one or more of these seven FRs.

SECTION 3 · ARCHITECTURE

Defense in Depth, Layer by Layer

The MB-213 platform applies independent security controls at five layers. A single failure at any one layer does not collapse the whole stack. The diagram below shows each layer and the principal mechanisms that operate there.

L0 **Physical & Hardware** `silicon`
Tamper-evident enclosure · secure-element-backed key storage (where SKU supports) · physical security boot pin · supply-chain integrity attestation per board serial.

L1 **Boot Chain** `verified boot`
First-stage bootloader signed by Modibus root key → U-Boot verified → Linux kernel signature verified → root filesystem integrity checked via dm-verity. Any broken link halts boot.

L2 **ModiOS Operating System** `hardened`
Minimal package surface · A/B partitions with rollback protection · signed firmware images · AppArmor / capability-based isolation · read-only rootfs option.

L3 **Network Plane** `outbound-only`
No listening services on WAN interface · outbound TLS 1.3 to MDS Cloud · OpenVPN / IPsec for tunnels · CM-216 enforced segmentation between WAN and OT zones · per-device X.509 mutual auth.

L4 **Application & API** `least privilege`
Per-user RBAC with scoped device access · mandatory 2FA on cloud login · SAML SSO support · signed REST API tokens with rotation · webhook payload signing.

L5 **MDS Cloud Platform** `zero trust`
Multi-tenant isolation enforced at every API call · comprehensive audit log · SOC 2 Type II in progress · SIEM-friendly syslog export · webhook-driven incident pipelines.

WHY OUTBOUND-ONLY MATTERS

Inbound-listening services on a customer's WAN — TLS ports accepting client connections, VPN concentrators on UDP/500, web management UIs on TCP/443 — are high-value zero-day targets. The historical incident record (Pulse Secure, Citrix ADC, Ivanti Connect Secure) shows what happens when a zero-day ships against an architecture pattern that exposes services to the public internet.

The MB-213 has **zero listening services on its WAN interface**. All connectivity is initiated outbound by the device to MDS Cloud, multiplexed over a single TLS 1.3 control channel. From the outside the device is invisible — there is no port to scan, no service to fingerprint, no admin UI to brute-force. A remote engineer reaches the customer's PLC by connecting to MDS Cloud, which relays through the pre-established outbound tunnel. The customer's firewall never sees an inbound connection it didn't expect.

FOUNDATIONAL REQUIREMENTS 1 & 2

Identification, Authentication, Use Control

Every connection to the MB-213 platform — whether initiated by a device, a user, an integration, or an OEM-vendor service technician — is identified, authenticated, and constrained by an explicit authorisation policy. There is no anonymous mode, no default account, no shared credential.

USER AUTHENTICATION (FR 1)

- **Mandatory 2FA on MDS Cloud.** TOTP via authenticator app or hardware token (FIDO2 / WebAuthn). New accounts must enrol 2FA before first use; this cannot be disabled at the user level.
- **SAML 2.0 / OIDC SSO.** Enterprise tenants integrate with Azure AD, Okta, Google Workspace, or any standard IdP. Modibus does not store the customer's primary credential.
- **SCIM 2.0 user provisioning.** User lifecycle (joiner / mover / leaver) flows from the customer's IdP automatically. Offboarding revokes session and certificates within 60 seconds.
- **Session policies.** Configurable timeouts (idle and absolute), IP allow-listing, time-of-day restrictions, geo-fencing optional.

DEVICE AUTHENTICATION (FR 1)

- **X.509 device certificates.** Each MB-213 is provisioned with a unique device certificate at manufacture, anchored to the Modibus device PKI. Revocation is enforced via OCSP on every connection.
- **Mutual TLS to MDS Cloud.** The device authenticates the cloud service; the cloud authenticates the device. No anonymous server certificates, no self-signed shortcuts.
- **Hardware-backed key storage.** On SKUs equipped with secure elements, the device private key never leaves the chip. Cloning a device requires physical possession *and* hardware extraction — raising the bar to SL 3 territory.

USE CONTROL (FR 2)

Authentication answers *who*; authorisation answers *what*. Use Control on the Modibus platform is implemented through a **scoped RBAC model**:

ROLE	GRANTED PERMISSIONS	TYPICAL USE
Tenant Admin	Manage users, roles, devices, integrations, audit log retention.	Customer security/IT lead.
Engineer	Open remote sessions to assigned devices; view telemetry; download logs.	OT/automation engineer.
Operator	View dashboards, acknowledge alerts. **No** remote-session capability.	24/7 control room.
Read-Only	View only. No control, no session initiation, no exports of bulk data.	Auditor, contractor.
OEM Vendor	Time-bounded session to a **specific machine only**; auto-expires.	Third-party machine support.

- **Scoped device access.** Engineers see only the devices their role allows. There is no "Engineer who can access all devices" default.
- **Time-bounded vendor access.** OEM-vendor sessions can be configured with explicit start/end timestamps and auto-revoke.
- **Per-session audit.** Every session start, end, file transfer, and command issued is logged with user identity, device identity, source IP, and duration. The audit trail is immutable and exportable to the customer's SIEM.

FOUNDATIONAL REQUIREMENTS 3 & 4

System Integrity & Data Confidentiality

A gateway is only as trustworthy as the firmware running on it. The MB-213 boots into known-good state every time, refuses to run unsigned code, and protects its data both in transit and at rest with industry-standard cryptography — using current algorithms only.

VERIFIED BOOT CHAIN (FR 3)

The boot process is a chain of cryptographic verifications. Every stage validates the next before handing over execution; any failure halts the boot and reports a tamper event to MDS Cloud.

STEP	STAGE	VERIFICATION
1	**SoC ROM → FSBL**	Hardware root-of-trust; first-stage bootloader signed by Modibus root key, hash burned into one-time-programmable fuses.
2	**FSBL → U-Boot**	FSBL verifies U-Boot image signature against a key chained from the root.
3	**U-Boot → Kernel**	FIT image verification: Linux kernel + device tree + initramfs all signature-verified.
4	**Kernel → Rootfs**	dm-verity hash tree validates every block of the root filesystem on read.
5	**Runtime measurement**	Critical processes attested via IMA / EVM; deviations reported to MDS Cloud.

A/B PARTITIONS & UPDATE INTEGRITY (FR 3)

- **Two firmware slots.** The active slot runs; the inactive slot receives the next update. No corruption-during-flash failure mode.
- **Anti-rollback protection.** Each release carries a monotonically increasing version counter; the bootloader refuses to boot images older than the last known-good version.
- **Signed update images.** Updates are PKCS#7-signed by the Modibus build infrastructure. Signing keys live in HSMs with multi-person access controls.
- **Atomic switchover.** An update either succeeds completely or rolls back automatically — no partial-update bricking, ever.
- **Build-pipeline integrity.** Source → CI → signing follows SLSA-style provenance attestation; build reproducibility verified on independent infrastructure.

DATA CONFIDENTIALITY — IN TRANSIT (FR 4)

- **TLS 1.3 only** on the device-to-cloud control channel. No fallback to TLS 1.2 unless the customer explicitly requests it for compatibility with a legacy MITM proxy.
- **Cipher suites.** AEAD only — `TLS_AES_256_GCM_SHA384`, `TLS_CHACHA20_POLY1305_SHA256`. No RSA key transport, no CBC modes.
- **Perfect forward secrecy.** Ephemeral key exchange (ECDHE / X25519) on every session. A compromise of the device or server long-term key does not retroactively decrypt past traffic.
- **Certificate pinning.** The MB-213 ships with the MDS Cloud root pinned; foreign-CA MITM attempts fail closed.
- **VPN tunnels.** OpenVPN with AES-256-GCM and ECDH; IPsec via StrongSwan with IKEv2 + AES-256-GCM.

DATA CONFIDENTIALITY — AT REST (FR 4)

- **MDS Cloud customer data:** encrypted at rest with AES-256, customer-scoped key hierarchy, KMS-backed.
- **Local secrets on device:** private keys protected via hardware-backed key storage (where SKU supports); fallback to filesystem-encrypted partition with TPM-sealed key.
- **Audit log immutability:** log records are append-only, hash-chained, and exported daily to a write-once archive store.

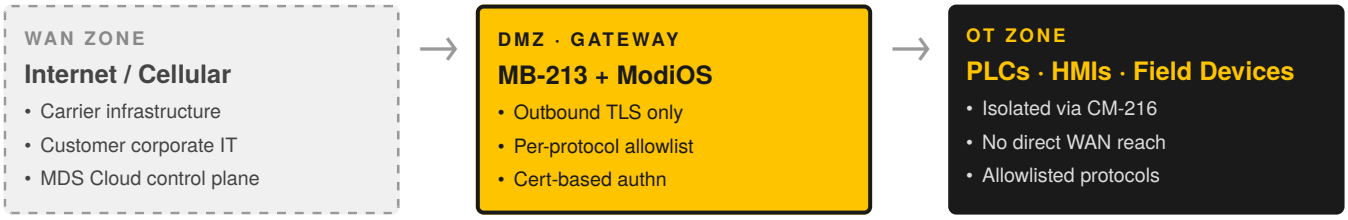
FOUNDATIONAL REQUIREMENTS 5, 6 & 7

Segmentation, Visibility, Availability

Three FRs about what happens once an attacker is past the perimeter: stop them spreading, see them moving, and keep operating. The MB-213 implements zone-and-conduit segmentation in hardware, comprehensive event logging, and resource-availability protections in firmware.

RESTRICTED DATA FLOW — ZONE & CONDUIT MODEL (FR 5)

IEC 62443 expresses network segmentation as **zones** (groups of assets at the same trust level) and **conduits** (controlled communication paths between zones). The MB-213 + CM-216 enforces this model in hardware, not as a firewall rule the customer is expected to remember to configure.



With a **CM-216** module installed, the OT zone is on a physically separate Ethernet switch fabric from the WAN zone. The gateway is the only path between them, and traffic flows are explicit: operator A is permitted to reach PLC 1 over Modbus TCP via the outbound-relay session; operator B is not. The conduit policy is a list, not a hope.

TIMELY RESPONSE TO EVENTS (FR 6)

- **Comprehensive structured logs.** Every authentication, session, configuration change, certificate event, and policy decision emits a structured log line with correlation IDs.
- **Syslog forwarding (RFC 5424).** Native export to the customer's SIEM (Splunk, Sentinel, QRadar, Elastic). TLS-protected, mutually authenticated.
- **Webhook alerting.** Real-time delivery of high-severity events to PagerDuty, Slack, MS Teams, or any HTTPS endpoint — signed payloads with rotating shared secret.
- **Retention.** 13-month default in MDS Cloud; configurable; raw logs available for forensic timelines on request.
- **Health attestation.** Devices report runtime integrity measurements (process list, mounted filesystems, listening sockets) at intervals; deviations trigger alerts.

RESOURCE AVAILABILITY (FR 7)

- **Connection rate limiting.** Per-source IP and per-account limits prevent connection-exhaustion attacks against MDS Cloud.
- **Watchdog timer.** Hardware watchdog automatically reboots the device on kernel hang; recovery time bounded.
- **Process supervision.** Critical services run under systemd with restart policies and resource quotas (CPU / memory cgroups).
- **Fail-closed networking.** Loss of MDS Cloud connectivity does **not** open a wider attack surface; the device remains in its constrained state until tunnels re-establish.
- **MDS Cloud SLA.** 99.9% target; multi-region failover; status page at `status.modibus.com`.

SECTION 4 · IEC 62443-4-1

Secure Development Lifecycle

A secure product is the output of a secure process. IEC 62443-4-1 specifies the practices a component vendor must follow during development, maintenance, and disposal. Modibus aligns with all eight practice areas of the standard; the principal mechanisms are summarised below.

THREAT MODELING

- **Per-feature threat models.** Every feature with a network or trust boundary gets a STRIDE-based threat model before design freeze.
- **Architecture-level reviews** on every major release line. Output: documented assets, trust boundaries, threats, and mitigations — archived in the engineering knowledge base.

CODE-LEVEL CONTROLS

- **SAST in CI.** Static analysis on every pull request: `Semgrep`, language-specific analyzers, custom rule packs for known-bad patterns.
- **DAST in nightly builds.** Dynamic security testing including authenticated and unauthenticated fuzzing of network protocol surfaces.
- **Dependency scanning.** `Trivy` + `Grype` running daily against the live SBOM; new CVEs in dependencies generate tracked tickets within 24 hours.
- **Mandatory peer review.** All security-sensitive changes (auth, crypto, parsers, trust boundaries) require sign-off from a second engineer flagged as a security reviewer.
- **Supply-chain hardening.** Pinned dependency versions with hash verification; vendored third-party crypto with audit logs of upgrades.

SOFTWARE BILL OF MATERIALS (SBOM)

- **SPDX 2.3 format.** Machine-readable, regenerated on every release.
- **Shipped with the product.** Available via the customer portal, the device API, and embedded in the firmware update package.
- **Component-to-CVE crosswalk.** Each shipped SBOM is correlated against NVD; the customer portal shows current CVE status for the customer's installed firmware.

EXTERNAL VALIDATION

ACTIVITY	CADENCE	PROVIDER / NOTES
External penetration test	Annual + on major releases	Accredited testing lab; full report under NDA on request
Internal red-team exercise	Quarterly	Modibus security team; output drives backlog
Continuous fuzzing	Always-on	Network protocol parsers; AFL++ + libFuzzer
IEC 62443-4-1 audit	Annual once certified	Target initial certification Q1 2027

★ **In practice:** every code change touches threat model, peer review, SAST/DAST, fuzz testing, and an updated SBOM. Every step is logged; the audit trail is available to customers on request.

SECTION 5 · CVD

Coordinated Vulnerability Disclosure

Trust is built on what a vendor tells you when something goes wrong. Modibus operates a published coordinated vulnerability disclosure (CVD) programme aligned with ISO/IEC 29147 and 30111. The process below is the same whether the report comes from an external researcher, a customer, an integrator, or our own internal red team.

HOW TO REPORT

CHANNEL	DETAIL
Email	`security@modibus.com` — encrypted via PGP key published on the website and major keyservers.
Web form	`modibus.com/security/report` — for researchers without PGP tooling; uses TLS-only intake with end-to-end encrypted forwarding.
Customers	Through your account team; treated identically — same SLAs, same advisory timelines.
Coordinated disclosure	CERT/CC, NCSC, MITRE: Modibus is a registered CVE Numbering Authority (CNA) candidate.

RESPONSE SLAS

STAGE	CRITICAL	HIGH	MEDIUM	LOW
Acknowledgment	2 business days	3 business days	5 business days	5 business days
Triage & CVSS scoring	5 days	7 days	14 days	30 days
Patch development	30 days	60 days	90 days	Next minor
Public advisory	90 days*	120 days*	120 days*	Aligned to release

** Public advisory may be expedited if the vulnerability is being actively exploited or has been disclosed independently. Customers receive embargo-period notification before public release.*

WHAT CUSTOMERS GET

- **Pre-public notification.** All affected customers receive details and remediation guidance through the customer portal and email *before* public advisory release.
- **Public security advisories.** Catalogued at `modibus.com/security/advisories` with CVSS, affected versions, fixed versions, and detection guidance.
- **CVE assignment.** Each verified vulnerability receives a CVE ID through coordination with MITRE.
- **Patch availability.** Fixes ship as A/B firmware updates; customers can roll forward via MDS Cloud or air-gapped USB.
- **SBOM diff.** Each release ships an SBOM diff highlighting changed dependencies and the CVEs addressed.

RESEARCHER ACKNOWLEDGMENT

Modibus credits security researchers in the published advisory unless they request otherwise. A formal bug bounty programme is on the roadmap (target Q4 2026); until then, we operate a private Hall-of-Fame and provide swag, written acknowledgment, and reference letters. We do not pursue legal action against good-faith security research conducted in line with our published rules of engagement.

SECTION 6 · COMPLIANCE

Certifications & Continuous Security Programs

The certifications, conformance statements, and continuous security programmes that back the technical controls described in this whitepaper. Every entry below is currently in force as of May 2026; certificate copies are available to customers under NDA.

CURRENT CERTIFICATIONS

STANDARD	SCOPE	EVIDENCE AVAILABLE TO CUSTOMERS
CE	European Conformity — EMC, RoHS, RED for the MB-213 platform	Declaration of Conformity (DoC) on request
ISO 9001	Quality Management System — product development & manufacturing operations	Certificate + scope statement
IEC 62443-1	Industrial cybersecurity framework conformance — concepts & terminology applied to MB-213 + MDS Cloud	Conformance statement + control mapping
ISO 27001	Information Security Management System — corporate & cloud operations in scope	Certificate + Statement of Applicability under NDA
ISO 27017	Cloud security controls — MDS Cloud platform in scope	Certificate + scope statement

CONTINUOUS SECURITY PROGRAMMES

PROGRAMME	STATUS	DETAIL
SBOM (SPDX 2.3)	**Active**	Shipped with every firmware release; available via portal & device API
Coordinated Vulnerability Disclosure	**Active**	Public policy; PGP key on keyservers; published response SLAs
Annual external penetration test	**Active**	Accredited testing lab; executive summary public; full report under NDA
Secure development lifecycle	**Active**	Threat modelling, SAST/DAST, peer review, signed builds, SBOM — under ISO 27001 ISMS
CIS Critical Security Controls v8 mapping	**Active**	Control mapping document for compliance teams

REGIONAL & SECTOR-SPECIFIC APPLICABILITY

- **EU CRA (Cyber Resilience Act).** The MB-213 platform meets the “important product” classification requirements: SBOM, vulnerability handling process, and update lifecycle obligations are all in place under the existing ISO 27001 / IEC 62443-1 conformance regime.
- **NIS2 Directive.** Modibus operates as a digital service provider for MDS Cloud under NIS2 scope; incident reporting workflows align with national CSIRT timelines under the ISO 27001 ISMS.
- **NERC CIP.** Customers in scope can request the CIP-013 supply-chain risk attestation pack — backed by the ISO 9001 manufacturing controls and IEC 62443-1 conformance.
- **FDA 21 CFR Part 11.** For F&B and pharma customers: audit-log immutability and electronic-signature workflows in MDS Cloud align with Part 11 requirements; gap analysis & control mapping available.

SECTION 7 · SHARED RESPONSIBILITY

Who Does What — Cleanly Drawn

Cybersecurity for industrial remote access is shared between the vendor, the customer, and (where relevant) the integrator. The matrix below sets the boundaries explicitly, so nothing falls into the gap.

ACTIVITY	MODIBUS	CUSTOMER	SHARED
Hardware & supply-chain integrity Sourcing, manufacturing, secure provisioning	✓	—	—
Firmware development & signing SDL, SAST/DAST, signing infra, SBOM	✓	—	—
Firmware update deployment Decision to install, maintenance window scheduling	—	✓	advisory
MDS Cloud platform operation Patching, monitoring, multi-tenant isolation, SLA	✓	—	—
User account lifecycle Joiner / mover / leaver, role assignment, offboarding	—	✓	—
Network policy at customer site Firewall config, VLAN design, OT segmentation strategy	—	✓	guidance
PLC / endpoint security Hardening connected field devices; default-credential removal	—	✓	—
Vulnerability disclosure Reporting, triage, patch, advisory	✓	—	notification
Incident response Detection, containment, forensics, post-mortem	—	—	✓
Audit-log retention & review Storage, periodic review, SIEM ingest	platform	review	✓
Compliance evidence (audits) Vendor-side documentation, control mapping	✓	—	—

★ **How to read this matrix:** a ✓ in a column means that party owns the activity end-to-end. *guidance* / *advisory* means Modibus provides documentation and recommendations but does not execute the activity. *shared* means the activity requires both parties — typically the customer triggers, Modibus supports.

Take this whitepaper to your security architect.

Request the underlying control-mapping spreadsheet, the SBOM, the latest pentest executive summary, or a 60-minute architecture review with the Modibus security team.

security@modibus.com
sales@modibus.com
modibus.com/security