General Security

Threat model · Cryptographic infrastructure

Identity · PKI · Audit · Compliance

GST-0010-00 2.2 en-US
ENGLISH

This document is written for the information-security, network-engineering, and IT-governance functions on the customer side. It is a technical-evidence document, not a marketing brochure. Implementation specifics that fall under the platform's hardening profile are deliberately omitted; what is presented here is the externally observable architectural posture and the standards-aligned controls that procurement and audit reviews ultimately depend on.

General Security Documentation: Threat model · Cryptographic infrastructure · Identity · PKI · Audit · Compliance
CISO · IT / OT Architects · Network Administrators · Compliance Officers

1.3 Security Documentation

This section consolidates, in a form intended for direct use during information-security review, the technical evidence that the Modibus platform places on record for prospective and existing customers. It is structured around the six dimensions that govern most contemporary procurement and audit reviews of cloud-mediated industrial remote-access platforms: the threat model and the architectural philosophy that addresses it; the cryptographic infrastructure that protects data both at rest and in transit; the identity and access-control model that governs who may do what; the public-key infrastructure and device-identity discipline that prevents unauthorised devices from joining the platform's ecosystem; the logging and audit framework that supports incident reconstruction and regulatory disclosure; and the explicit mapping of these properties onto the controls that ISO/IEC 27001 and the IEC 62443 standard family require.

The level of description in this section is deliberately calibrated. Architectural intent, externally observable behaviour, and standards-aligned controls are described in full. Implementation specifics — the internal hardening profile, version-pinned cryptographic primitives, syscall-allow-lists, internal service identifiers, and similar artefacts — are not, by design. Where appropriate, the relevant artefact is named together with the certification body or audit instrument under which it is reviewed; reviewers with a documented need for additional detail can request it under non-disclosure through ModibusTech's standard customer-onboarding process.

Throughout this document, the brand name 'Modibus' refers to the platform and to the gateway product family (MB213 industrial gateway, WR-401 cellular variant, WR-402 wireless variant) supplied by ModibusTech OÜ, registered in Tallinn, Estonia. References to 'Modbus TCP' are to the open industrial-protocol specification of that name, which is one of several southbound protocols that the Modibus gateway interoperates with.

1.3.1 Threat Model and Zero-Trust Architecture

Industrial threat surface

The threat surface that an industrial remote-access platform must rebut is well documented in the published literature on incidents affecting operational technology over the last decade. Five attack patterns dominate, and the platform's architecture is calibrated to address each of them at multiple layers rather than at a single point.

Man-in-the-middle (MITM) attacks attempt to interpose between an engineer's workstation and the remote field device, either to passively eavesdrop on engineering commands or to actively modify them in flight. The platform rebuts this category through mandatory mutual authentication and authenticated encryption at the transport layer (see §1.3.2): a session that does not present a valid certificate on both ends is closed at the handshake stage, before any application data is exchanged.

Denial-of-service (DoS / DDoS) attacks aim to exhaust the gateway's or the cloud broker's capacity to serve legitimate requests, denying operators access to remediate failing equipment at the moment they need it most. The architectural response is twofold: the gateway never exposes an inbound network surface to the public Internet, removing the primary target that conventional industrial concentrators present; and the cloud broker enforces per-tenant rate-limiting and quota controls so that abusive traffic from one tenant cannot deplete the resources available to another.

Unauthorised-access attempts leverage stolen credentials, weak password practices, or session-token theft to obtain privileges that the holder is not entitled to. The platform's response is to bind every session to a verified human or machine identity (see §1.3.3), to require multi-factor authentication for human users, and to evaluate every access decision against contextual conditions in addition to identity, so that even a fully-stolen credential does not, on its own, produce a successful session if the remaining contextual signals do not corroborate it.

Lateral-movement attempts exploit a foothold in the customer's information-technology environment to reach the operational-technology segment via the legitimate remote-access channel. The architectural response is segmentation: the gateway is itself a security boundary between the IT and OT zones, the broker mediates every interaction between them, and the policy engine enforces that no IT-side identity is implicitly trusted to reach into the OT side without an explicit, logged authorisation.

Rogue-device insertion attempts to enrol an attacker-controlled gateway into the operator's tenant, exploiting any environment in which an enrolled gateway is implicitly trusted as a legitimate publisher of telemetry or as a recipient of operator commands. The platform's response is the dual-identity device-onboarding model described in §1.3.4: the cloud broker accepts a connection only when both the manufacturer-issued device identity and the operator-issued device identity validate.

Zero-Trust as the request-time discipline

The platform's posture toward these threats follows the Zero-Trust architecture principles published by the U.S. National Institute of Standards and Technology in NIST SP 800-207 (Rose et al., 2020). Every engineering session, every telemetry publication, and every administrative action is authenticated, authorised, and contextually evaluated at the moment it occurs, against a centrally-held policy expressed in declarative form. There is no implicit trust by virtue of network location: an engineer connected from inside the corporate network is subject to the same identity, device-posture, and policy checks as one connected from a public Internet endpoint. Network reachability is treated as a necessary but never sufficient precondition; the request must additionally pass the identity, posture, and policy gates before it is honoured.

A consequence of this posture that has direct operational consequences is that revocation is fast and granular. When an employee leaves the customer's organisation, when a device is suspected of compromise, or when a policy is updated to restrict access during a maintenance window, the change takes effect at the next request rather than at the expiry of a long-lived session token. The platform's

session-management architecture enforces re-evaluation against the current policy at well-defined cadences and on attribute change.

Defense-in-Depth as the layered-failure discipline

Zero-Trust is complemented by a Defense-in-Depth posture aligned with the layered-control philosophy of IEC 62443. Seven distinct control planes — physical security, network perimeter, segmentation, transport, identity, application and workload, and asset hardening — each act independently. An adversary who defeats one layer encounters another, and the platform is engineered so that a single-layer failure cannot, on its own, produce a compromise of the end-to-end session. Defeating the layered model requires the simultaneous failure of independent controls, an event that fault-tree analysis treats as several orders of magnitude less probable than the failure of any individual control. The two postures are complementary rather than alternative: Zero-Trust governs the request-time decision flow, Defense-in-Depth governs the resilience of the system to the failure of any single control.

1.3.2 Cryptographic Infrastructure

Data at rest

Confidentiality and integrity guarantees apply to data in two distinct states. Data at rest — on the gateway and on the cloud — is protected by AES-256 in an authenticated mode of operation (AES-GCM), which simultaneously provides confidentiality and integrity in a single primitive and which is the symmetric standard endorsed by NIST FIPS 197 and recommended for new deployments by virtually every contemporary information-security guideline. Encryption keys are not held alongside the encrypted data; they are protected by a hardware-backed key store anchored in the gateway's verified-boot chain, and they never leave that key store in plaintext form. A gateway that is physically removed from its installation site therefore yields no usable plaintext to an adversary who comes into physical possession of it. On the cloud side, customer data is partitioned by tenant, encrypted with tenant-specific AES-256 keys held in a managed key-vault service, and subject to access-control policies that distinguish between operator-readable, auditor-readable, and ModibusTech-readable scopes. Cross-tenant access is prevented by construction rather than by policy alone.

Data in transit — TLS 1.3 with mutual authentication

Data in transit is carried exclusively over Transport Layer Security version 1.3, defined by IETF RFC 8446 (Rescorla, 2018). TLS 1.3 was selected on the basis of four properties that are directly relevant to information-security review. First, all key exchanges are forward-secret by specification — typically achieved through ephemeral elliptic-curve Diffie-Hellman (ECDHE) key agreement — so the future compromise of any long-term key does not retroactively expose past sessions. Second, the legacy ciphersuite families that suffered cryptographic regressions in earlier TLS versions (CBC-mode constructions, RSA key transport, static Diffie-Hellman) are removed by specification rather than merely

discouraged, eliminating downgrade-to-weak-cipher attack patterns by construction. Third, the handshake is reduced from two round-trips to one, materially improving the user experience on high-latency cellular paths. Fourth, the encrypted-SNI extension prevents trivial classification of session destinations by intermediate observers.

Mutual TLS authentication (mTLS) is mandatory for every session: a connection that does not present a valid X.509 client certificate is closed at the handshake stage and recorded in the audit log. Bulk traffic is protected by AES-256 in an AEAD mode (AES-256-GCM) or by ChaCha20-Poly1305 on platforms where the latter delivers better performance, both of which are TLS 1.3 ciphersuites that the IETF recommends for new deployments. Certificate signatures use ECDSA over NIST-standard elliptic curves, and key derivation uses HKDF with SHA-2 family hash functions (SHA-256 or SHA-384). The detailed ciphersuite ordering, key-share preferences, and exact certificate-signature algorithm in use at any given moment are part of the platform's cryptographic-agility schedule and are revised on the cadence dictated by the prevailing certification regime; this is a deliberate property of the design, since the alternative — a hard-coded ciphersuite policy — would impede the orderly retirement of primitives that the cryptographic-research community marks as deprecated.

Outbound-only session model and the firewall consequence

A property of the in-transit design that has immediate consequences for the customer's network architecture is the outbound-only session model. The gateway never accepts an inbound connection from the public Internet. Instead, it originates an outbound TLS session to the cloud rendezvous broker on a standard HTTPS-class port. From the perspective of the customer's perimeter firewall, the gateway is indistinguishable from any other HTTPS client.

The practical consequence for IT operations is the elimination of three classes of network exception that legacy industrial-VPN deployments require: **no inbound port-forwarding rule** is needed on the customer's perimeter firewall; **no demilitarised-zone entry** is needed for the gateway to be reachable from an outside network; and **no exception to the corporate egress policy** is needed beyond permitting outbound HTTPS to the broker's published address. The reverse path — engineer-to-device — is constructed by the broker performing session pairing rather than by direct routing, so the architectural elimination of inbound exposure does not entail a loss of remote-access functionality.

This single property removes the most-exploited attack surface of legacy industrial-VPN deployments — the publicly-reachable concentrator — and is the single most consequential reason that information-security reviews tend to clear Modibus deployments substantially faster than the legacy alternatives that the platform is most often asked to replace.

Cryptographic agility

Cryptographic primitives are not static; the orderly retirement of weakening primitives is itself a control that the platform supports by design. The platform's cryptographic-agility schedule covers ciphersuite

revision, key-length progression, and migration plans for the post-quantum primitives that NIST has begun to standardise — notably ML-KEM (FIPS 203) for key encapsulation and ML-DSA (FIPS 204) for digital signatures — over the coming decade. Customers who require evidence of the platform's intended progression can obtain the cryptographic-agility schedule under non-disclosure as part of the standard onboarding pack.

1.3.3 Authentication and Access Control

Identity federation with the customer's identity provider

Identity is the foundation of every authorisation decision and is treated as such. Modibus integrates with the customer's existing identity provider through industry-standard federation protocols — SAML 2.0 and OpenID Connect (OIDC) — so that human users do not maintain separate Modibus credentials. Password-policy enforcement, account-lifecycle management, role provisioning and de-provisioning, and offboarding workflows remain governed by the customer's directory of record. This integration discharges several recurring audit concerns at one stroke: there is no shadow user-database to enumerate, password rotation is governed by corporate policy rather than by the platform, and a terminated employee loses access to Modibus at the same moment they lose access to the corporate identity directory. For customers without an existing modern identity provider, the platform supports a managed-tenant identity service that satisfies the same audit properties.

Role-based access control

Authorisation is expressed in two complementary layers, the first of which is role-based access control (RBAC). The platform exposes a small, audit-friendly role inventory — typically Administrator, Operator, Auditor, and Read-only — to which the customer's identity provider maps its own group memberships. RBAC supports the coarse-grained access-control vocabulary with which IT governance is already familiar, and it satisfies the common audit requirement that role assignments be derivable from a single source of truth in the customer's identity directory. Custom roles can be defined where the standard role inventory does not reflect the customer's organisational structure.

Attribute-based access control as the contextual overlay

Role assignment, in isolation, is rarely sufficient for an industrial-control environment in which the consequences of a compromised session can extend beyond the digital domain. The platform therefore overlays role assignment with attribute-based access control (ABAC), in which an authorisation decision is conditioned not only on the requestor's role but also on contextual attributes evaluated at the moment of the request. Time-of-day windows, source-IP geolocation, device-posture attestations, and explicit change-control ticket numbers are typical inputs to the ABAC decision. The combination supports policies of the form 'a user with the Operator role may invoke action X on asset Y, but only between defined working hours, only from a corporate-managed endpoint, and only when an open,

approved change-control ticket is in scope.' Authorisation decisions are evaluated at every request, not only at session establishment, so that a contextual attribute changing during a long-running session — for example, the requestor's geolocation departing the policy-permitted range — produces a re-evaluation rather than a continued grant.

Multi-factor authentication

Multi-factor authentication (MFA) is mandatory for every human user. The platform supports the contemporary factor families that information-security policy typically requires: time-based one-time passwords (TOTP, IETF RFC 6238), push-based authenticator applications, hardware security keys conformant to FIDO2 / WebAuthn, and PKI-based smart cards conformant to PIV (NIST SP 800-73). The choice among these factor families is a customer-policy decision; the platform enforces whichever factors the customer's identity provider asserts. Single-factor sign-in for human users is not supported, even where a customer's identity-provider configuration permits it, in order to ensure that the platform's MFA posture cannot be silently weakened from outside the platform.

Service accounts — the non-human identities used by manufacturing-execution systems, business-intelligence pipelines, and similar machine-to-machine consumers of platform telemetry — authenticate with cryptographic keys and the OAuth 2.0 client-credentials grant (RFC 6749) rather than with passwords, with short-lived bearer tokens issued as JSON Web Tokens (JWT, RFC 7519). Service-account credentials carry their own bounded validity and are subject to the same logging and revocation lifecycle as human credentials.

Decision logging for governance

Every authorisation decision — both allow and deny outcomes — is recorded with the subject identity, the asset identity, the action requested, the timestamp, the policy version that resolved the decision, and a hash of the contextual signal that informed it. A denied request is recorded with the same metadata as an approved request. This symmetric logging supports the defensible reconstruction of 'what was attempted and not permitted' during post-incident review, which is frequently more informative than the record of what was permitted.

1.3.4 Public Key Infrastructure and Certificate Management

Hierarchy and least-privilege segregation

The platform's public-key infrastructure (PKI) serves two complementary purposes: it provides the mutual-authentication anchor for transport security, and it provides a tamper-resistant device-identity proof that prevents rogue gateways from joining a customer's tenant. The hierarchy is structured for least privilege. A Root Certificate Authority is held offline in a hardware security module (HSM) certified to a tier of FIPS 140-2 / FIPS 140-3 appropriate to its custodial role, in a physically secured facility, and is brought online only for the limited operations required to refresh the Intermediate CAs. Two segregated

Intermediate CAs operate online: one dedicated to devices and one dedicated to cloud services. This segregation ensures that a compromise of the cloud-services Intermediate cannot, in itself, mint a certificate that a Modibus gateway will accept as a peer device, and conversely that a compromise of the devices Intermediate cannot mint a certificate that a Modibus cloud service will accept. Leaf certificates for individual gateways and individual cloud services are issued from the appropriate Intermediate, with bounded validity periods reviewed on the cadence dictated by the cryptographic-agility requirements of the prevailing certification regime.

Hardware root of trust and Secure Boot

The platform's PKI is anchored in the silicon of the gateway itself rather than in software alone. At every power-on, a verified-boot sequence — commonly described as 'Secure Boot' in IT-security literature — executes in which each stage cryptographically authenticates the next before executing it. The chain begins in immutable on-die memory, whose contents cannot be altered after the gateway leaves the factory, and extends without interruption through the bootloader, the operating-system image, the platform runtime, and the workloads that the runtime launches. A signature mismatch at any stage halts the boot and surfaces the anomaly through an out-of-band recovery channel rather than continuing into a partially-compromised state. The externally-observable property is unambiguous: no unsigned code executes on the gateway under any condition.

This hardware root of trust is the foundation on which every other security property of the gateway is layered. The cryptographic identity of the gateway, the integrity of its firmware, and the audit guarantees described later in this document all derive their assurance from the fact that the gateway will not boot into a compromised state. Information-security reviewers commonly describe this property as the 'security floor' of the device, and the platform is designed so that no software-level configuration error can lower it.

Birth certificates and operator-issued device identities

Every Modibus gateway is provisioned at manufacturing time with a hardware-bound 'birth certificate' — a non-revocable cryptographic identity that is bound to the gateway's secure element at the moment of fabrication and that travels with the device for its operational life. This identity is conceptually aligned with the device-identity framework defined by IEEE 802.1AR-2018 and serves as the cryptographic equivalent of a verified manufacturer's mark. A counterfeit gateway, even one whose physical appearance and external interfaces faithfully imitate a Modibus device, cannot present a valid birth certificate; the cloud broker rejects its connection at the handshake stage.

Once a gateway is enrolled to a customer tenant — through a controlled enrolment process supervised by the customer's administrative role — it additionally receives an operator-issued device identity that carries the customer-specific organisational binding. The cloud broker accepts a connection only when both identities validate. This dual-identity discipline produces two-key cryptographic protection against two distinct categories of failure: the birth certificate prevents supply-chain substitution attacks, in

which a counterfeit device imitates a legitimate one; and the operator-issued identity prevents customer-side mis-enrolment errors, in which a legitimate device is accidentally bound to the wrong tenant. The combined effect, in plain terms, is that a rogue device cannot join the customer's ecosystem either by counterfeiting the manufacturer's mark or by exploiting the customer's onboarding workflow.

Lifecycle automation

Manual certificate management has historically been a leading cause of avoidable outage in industrial deployments; the failure mode is invariably the same — a leaf certificate expires unobserved, and a service that depended on it stops at an inconvenient hour. Modibus automates the entire certificate lifecycle. Hardware-protected key generation, certificate signing requests (CSR), issuance, deployment, monitored use, well-before-expiry renewal, and revocation through the Online Certificate Status Protocol (OCSP, RFC 6960) and Certificate Revocation List (CRL, RFC 5280) channels all proceed without human intervention. Certificate Transparency (CT) logs (RFC 6962) are continuously monitored to detect any rogue issuance attempted against the platform's domain names. Customers do not maintain, schedule, or operate certificate-renewal procedures; they are notified of lifecycle events through the platform's audit log and through the SIEM integration described in §1.3.5.

1.3.5 Logging, Traceability and Audit

Three layers of evidentiary record

Forensic defensibility requires that an incident, weeks after it occurred, can be reconstructed from records whose integrity has not been disturbed. Modibus produces such records at three layers and retains them in tamper-evident form. The three layers are deliberately distinct so that the question being investigated — 'who did what?', 'what did the policy permit?', or 'what did the platform itself do?' — can be answered against the appropriate record without conflation.

The session layer records every interactive engineering session: the authenticated subject, the asset accessed, the wall-clock interval (start time, end time, total duration) of the session, the application-layer commands or tool dialogues issued during the session, and a cryptographic digest of any payloads exchanged. These records are produced at the broker, where they are unforgeable by either endpoint of the session.

The authorisation layer records every (subject, action, asset) decision evaluated by the policy engine — both allow and deny outcomes. This is the layer that answers the audit question of what was attempted and what the policy permitted or refused. Decision records carry the policy version that resolved them, allowing post-hoc reconstruction not only of what was attempted but of the rules in force at the moment of the attempt.

The system layer records platform-internal events: certificate issuance and revocation, configuration changes, firmware updates, role assignments and revocations, and security-relevant exceptions

detected by the runtime. These are operationally distinct from the session and authorisation layers but are joined by correlation identifiers, so that an investigator following a trail across all three layers can reconstruct the full causal chain of an incident from a single starting point.

Tamper-evident integrity

All three layers of record are tamper-evident: each day's accumulated records are sealed with a Merkle-tree construction over SHA-256 digests, and the resulting Merkle root is anchored to an external write-once witness, which means that a modification to a historical record — whether by an external attacker, by a malicious insider, or by accident — is cryptographically detectable. The platform does not claim that historical records cannot be altered; that claim would be technically untenable for any system. It claims only that any alteration produces a detectable inconsistency between the stored records and their committed digest, and it provides the mechanism by which an auditor can verify the integrity of the record at any point in the future.

Capture of who, when, what, and how long

For the specific audit questions that information-security reviewers routinely ask about a remote-access platform — who connected, when, to what asset, with what privileges, and for how long — the session-layer record is the canonical source. Every active engineering session is associated with an authenticated identity, a precise start and end time, a wall-clock duration, the asset or assets it accessed, the role under which the access was authorised, and the contextual signals that informed the authorisation. A query against the session-layer record can therefore answer questions such as 'list every session that engineer Z held against asset Y in the previous quarter, with start time, end time, and total duration', or 'list every action invoked under the Administrator role on assets in tenant T over the previous month', without requiring inspection of any internal Modibus telemetry beyond the audit log.

SIEM and Syslog integration

The platform's audit records are exported, in real time, to the customer's existing security-information and event-management (SIEM) infrastructure. Three forwarding formats are supported at the customer's choice: Syslog conformant to IETF RFC 5424, the Common Event Format (CEF) widely consumed by enterprise SIEMs, and a structured JSON format suitable for cloud-native log-pipeline tools. Multiple destinations may be configured simultaneously, which materially simplifies the dual-tenant arrangements common in regulated industries — for example, where the operator's internal SOC and a contracted external SOC both ingest the same audit stream — without requiring custom integration on the platform side.

Forwarding occurs over an authenticated, integrity-protected channel; the customer's SIEM authenticates the platform's forwarding identity rather than implicitly accepting any traffic that arrives on the configured port. Retention periods on the platform side are configurable per data category and per regulatory regime; the default profile aligns with ISO/IEC 27001 control A.8.15 (logging) and with the

twelve-month minimum that European operating practice typically requires under the General Data Protection Regulation.

Operational consequence for incident response

The cumulative effect of the three layers of record, the tamper-evident sealing, and the SIEM forwarding is that a customer's incident-response team is able to reconstruct any past event involving the Modibus platform from records that are either present in the customer's own SIEM or independently retrievable from the platform's audit archive. The platform does not introduce a new opaque component into the customer's logging architecture; it contributes records that integrate with the architecture the customer already operates.

1.3.6 Compliance Mapping

The architectural choices documented in §§1.3.1 through 1.3.5 are not merely technically defensible; they map directly onto the controls that the prevailing international standards require an operator to demonstrate during procurement review and ongoing audit. This subsection summarises the mapping for the two standards most consequential to industrial remote-access procurement: ISO/IEC 27001:2022, which governs the information-security management system that the operator must maintain, and the IEC 62443 family, which governs the security of industrial automation and control systems specifically. The platform's full statement of applicability and the certification artefacts that substantiate each row of the mapping table are available under non-disclosure to qualified reviewers as part of ModibusTech's standard onboarding pack.

ISO/IEC 27001:2022 — Information Security Management System

ISO/IEC 27001:2022 specifies the requirements for establishing, implementing, maintaining, and continually improving an information-security management system (ISMS). Its 2022 revision restructured Annex A into 93 controls organised under four themes (organisational, people, physical, and technological) and introduced eleven new controls, several of which are directly relevant to industrial gateway platforms. The platform's architecture addresses, among others, controls A.5.7 (threat intelligence), A.5.23 (information security for use of cloud services), A.8.5 (secure authentication), A.8.9 (configuration management), A.8.15 (logging), A.8.16 (monitoring activities), A.8.20 (network security), A.8.24 (use of cryptography), A.8.26 (application-security requirements), and A.8.28 (secure coding).

The platform's ISMS scope explicitly includes the cloud-resident multi-tenant infrastructure on which Modibus operates, closing the audit-of-shared-responsibility gap that frequently appears in cloud-mediated industrial offerings. The ISMS materialises as a documented asset inventory covering every gateway, certificate, and operational privilege; a cryptographic-asset register satisfying A.8.24; a threat-intelligence feed integrated with the SIEM; an incident-response plan with measured-quarter exercises;

and a continual-improvement loop in which post-incident root-cause analyses produce binding corrective actions, the closure of which is verified by an independent internal-audit function.

IEC 62443 — Industrial Automation and Control System Security

IEC 62443 is the only international standard family written specifically for the security of industrial automation and control systems, and it underpins regulatory frameworks worldwide, including the European NIS-2 directive's implementing acts. The Modibus platform aligns with three parts of the family. IEC 62443-1-1 establishes the foundational vocabulary and the zone-and-conduit segmentation model: the platform expresses each of the OT field zone, the gateway management zone, the cloud control zone, and the customer-engineer zone as a 62443 zone, with the encrypted authenticated sessions between them documented as conduits. IEC 62443-3-3:2013 defines seven foundational requirements (FR1 through FR7) at the system level; the controls described in this Security Documentation satisfy each of them, with the gateway product family targeting Security Level 2 (SL-2) in default configuration and an SL-3 deployment template available for high-assurance customers. IEC 62443-4-2:2019 defines component-level requirements for embedded devices, host devices, network devices, and software applications; the gateway product family is independently audited against these requirements during the platform's annual certification cycle.

In plain operational terms, the IEC 62443 alignment ensures that the platform's contribution to a customer's own zone-and-conduit architecture is explicit and documented: a customer drawing the conduits into and out of the gateway can do so against a published characterisation of the gateway's security level rather than against a marketing claim.

Mapping table

The compact mapping table that follows is intended for procurement-review use. Each row identifies a standard or control reference, the architectural property of the Modibus platform that addresses it, and the section of this Security Documentation in which the relevant evidence is described.

Standard / Control	Modibus architectural property	Evidence
ISO/IEC 27001 A.5.7	Continuous threat-intelligence integration with audit-log correlation	*§1.3.1*
ISO/IEC 27001 A.5.23	Documented cloud-services security and shared-responsibility allocation	*§§1.3.1, 1.3.6*
ISO/IEC 27001 A.8.5	SAML 2.0 / OIDC federation; TOTP / FIDO2 MFA; no shadow accounts	*§1.3.3*
ISO/IEC 27001 A.8.9	Configuration management with signed firmware and dual-bank update	*§1.3.4*
ISO/IEC 27001 A.8.15	Tamper-evident SHA-256 Merkle audit log; Syslog / CEF / JSON SIEM forwarding	*§1.3.5*

ISO/IEC 27001 A.8.16	Real-time monitoring; allow and deny decisions both recorded	*§§1.3.3, 1.3.5*
ISO/IEC 27001 A.8.20	Outbound-only TLS 1.3 transport; zero inbound exposure on customer perimeter	*§1.3.2*
ISO/IEC 27001 A.8.24	AES-256 at rest; TLS 1.3 mTLS in transit; HSM-backed PKI; agility schedule	*§§1.3.2, 1.3.4*
ISO/IEC 27001 A.8.26	Workload-isolation envelope; signed and verified workload images	*§1.3.4*
IEC 62443-1-1	Zones and conduits formally identified across IT / OT / cloud domains	*§§1.3.1, 1.3.6*
IEC 62443-3-3 FR1	Identification and authentication: federated identity + MFA + mTLS	*§§1.3.3, 1.3.4*
IEC 62443-3-3 FR2	Use control: RBAC + ABAC; per-request authorisation; full decision log	*§§1.3.3, 1.3.5*
IEC 62443-3-3 FR3	System integrity: Secure Boot, signed firmware, hardware root of trust	*§1.3.4*
IEC 62443-3-3 FR4	Data confidentiality: TLS 1.3 in transit, AES-256-GCM at rest, tenant-scoped keys	*§1.3.2*
IEC 62443-3-3 FR5	Restricted data flow: outbound-only sessions, broker-mediated pairing	*§1.3.2*
IEC 62443-3-3 FR6	Timely response: real-time SIEM forwarding; revocation effective at next request	*§§1.3.1, 1.3.5*
IEC 62443-3-3 FR7	Resource availability: per-tenant rate-limiting; quotas; no inbound DoS surface	*§§1.3.1, 1.3.2*
IEC 62443-4-2	Component-level requirements (EDR / HDR / NDR / SAR) independently audited annually	*§1.3.6*

This mapping is condensed for review-cycle use. The full statement of applicability — including the additional ISO/IEC 27000-series sector standards (27017, 27018, 27011), ISO/IEC 27701 for privacy information management, and the complete IEC 62443-3-3 and 62443-4-2 requirement-by-requirement allocations — is available to qualified reviewers under non-disclosure. The certification artefacts referenced in the table are produced by independent third-party assessors and are reviewed during the platform's annual certification cycle.

End of section 1.3.