TARA INNOVA

IEC 62443 Compliance Guide

How TARA INNOVA and Oasis Map to Industrial Cybersecurity Requirements

What Is IEC 62443

IEC 62443 is the international standard series for cybersecurity in Industrial Automation and Control Systems (IACS). It defines security requirements for asset owners, system integrators, and component suppliers operating in manufacturing, energy, utilities, and critical infrastructure. NIS2 references IEC 62443 as a recognized framework for OT security compliance.

Zone and Conduit Model

IEC 62443 organizes industrial networks into security zones connected by conduits. Each zone has a defined security level. Oasis directly implements this model:

- **Zone enforcement** — Oasis acts as the conduit security layer between IT and OT zones. Device identity, rate control, and payload validation on every crossing
- **Protocol mediation** — Secure bridging between industrial protocols and enterprise systems without exposing either side
- **Conduit monitoring** — Every message tracked. Anomaly detection on data flows between zones. Real-time metrics on inter-zone traffic
- **Security level mapping** — CRP documents achieved security levels per zone with evidence of enforced controls

Key Requirements and Coverage

IEC 62443 Requirement	TARA INNOVA / Oasis Coverage
SR 1.1 — Human user identification and authentication	Quicksand enforces user authentication with session integrity, PoW challenges, and device trust verification
SR 1.2 — Software process and device identification	Oasis validates device identity on every integration route. Certificate-based authentication for machine communication
SR 2.1 — Authorization enforcement	Oasis enforces per-channel access policies. Role-based controls with least privilege per integration route
SR 3.1 — Communication integrity	mTLS on all conduits. Payload schema validation ensures message integrity. Tamper-evident audit logs
SR 3.5 — Input validation	Oasis validates payloads against expected schemas. Quicksand blocks injection patterns and malformed requests
SR 5.1 — Network segmentation	Oasis deployed in gateway mode at zone boundaries. Enforces conduit policies per IEC 62443 zone model
SR 6.1 — Audit log accessibility	CRP provides immutable audit trail across all enforcement points. Regulator-ready evidence packages
SR 6.2 — Continuous monitoring	Real-time metrics on all integration routes. Throughput, rejection rates, latency, and protocol breakdown with anomaly alerting

OT-Specific Deployment

Oasis deploys in modes suited to industrial environments:

- **Gateway mode** — Inline at network boundaries between IT/OT zones. Full protocol inspection and enforcement
- **Agent mode** — Lightweight deployment on constrained edge devices. Minimal footprint with full governance
- **Air-gapped support** — On-premise only deployment with no external dependencies. Full functionality without internet connectivity
- **300+ protocol connectors** — Native support for industrial protocols alongside enterprise and cloud protocols

---