COMPLIANCE GUIDE

How Zero Networks Helps with ISA/IEC 62443

The ISA/IEC 62443 family of standards provides a globally recognized framework for securing Industrial Automation and Control Systems (IACS), with Part 3-3 focusing on system-level cybersecurity requirements.

Zero Networks enables organizations to implement a zero trust model in OT environments by combining automated microsegmentation, identity-based access control, and just-in-time remote access. Zero Networks directly supports compliance with ISA/IEC 62443-3-3 through practical implementation of foundational security requirements, including least privilege, secure remote access, network segmentation, and logging.

Introduction to ISA/IEC 62443-3-3

ISA/IEC 62443-3-3 defines system-level security requirements for industrial environments and is structured around 13 foundational requirements (FRs). These foundational requirements are further divided into 47 detailed system requirements (SRs) that cover access control, system integrity, restricted data flow, and more.

The framework's goal is to help asset owners and integrators build defensible architectures with layered protections, aligned with risk levels defined by target security levels (SL-T).

Key Capabilities Aligned with ISA/IEC 62443-3-3

3.1. Least Privilege Access

ISA/IEC 62443 SRs Addressed: SR 2.2 (Privilege Restriction), SR 2.3 (User Access Restriction), SR 5.1 (Network Segmentation)

Zero Networks automatically applies least privilege policies at the host level by learning real-time communication pattern and permitting only essential traffic.

- Default deny posture for all access
- Policies built per asset, identity, port, protocol

This aligns with ISA/IEC 62443's core principle of minimizing attack surfaces and access privileges across all system components.

3.2. Secure Remote Access (JIT + MFA)

ISA/IEC 62443 SRs Addressed: SR 1.1 (Human Authentication), SR 2.1 (Authorization Enforcement), SR 6.1 (Audit Log Generation)

Zero Networks enables secure remote access through Just-in-Time (JIT) elevation, where users request time-limited access to a resource. All access is protected by MFA and is tightly controlled and monitored.

- No always-on VPN required
- MFA enforced even for legacy systems
- Access logs are generated for each JIT session

This ensures only verified users can access specific assets — and only when necessary.

3.3. Segmentation and Network Isolation

ISA/IEC 62443 SRs Addressed: SR 5.1 (Zone Segmentation), SR 5.2 (Boundary Protection), SR 5.3 (Enforcing Unidirectional Flows)

Zero Networks applies host-based microsegmentation across OT and IT environments. This means:

- No communication between assets unless explicitly allowed
- Enforcement is identity-aware — based on the authenticated user or service
- Traffic directionality (e.g., allow HMI → PLC, but not reverse) can be enforced

Unlike traditional segmentation via VLANs or firewalls, this model works natively within flat or legacy networks common in OT environments.

3.4. Access Logging and SIEM Integration

ISA/IEC 62443 SRs Addressed: SR 6.1 (Log Generation), SR 6.2 (Log Review), SR 6.3 (Log Protection)

Zero Networks maintains a comprehensive log of:

- All access requests (granted, denied, or expired)
- JIT session approvals and MFA challenges
- Policy creation or modification events

These logs can be forwarded to SIEM platforms like Splunk, Sentinel, etc for real-time analysis and compliance auditing — helping organizations meet continuous monitoring expectations in 62443.

4. Control Mapping Summary

Foundational Requirement	System Requirement	Zero Networks Capability
FR 1: Identification & Authentication	SR 1.1, SR 1.5	Enforces user authentication with MFA; identity-aware rules
FR 2: Use Control	SR 2.1, SR 2.2, SR 2.3	Applies least privilege and use-based access at host level
FR 3: System Integrity	SR 3.2	Prevents unauthorized software execution by restricting communication to known-good systems
FR 4: Data Confidentiality	SR 4.1	Indirectly protects data via enforced trusted communication paths
FR 5: Restricted Data Flow	SR 5.1, SR 5.2, SR 5.3	Enforces microsegmentation and one-way policies between zones
FR 6: Timely Response to Events	SR 6.1, SR 6.2, SR 6.3	Generates detailed audit logs; forwards logs to SIEM
FR 7: Resource Availability	SR 7.1	Reduces attack surface, minimizing DDoS and lateral threat potential

Connect with the Zero team to discover how you can streamline your ISA/IEC alignment with automated microsegmentation.

Request a demo

ZERO. Networks