safous

ISA/IEC 62443 COMPLIANCE CHECKLIST

Meet ISA/IEC 62443 Compliance Requirements With Safous

The ISA/IEC 62443 series is an international cybersecurity standard for securing operational technology (OT) in industrial automation and control systems (IACS). It outlines the technical security controls organizations must implement to meet target security levels and defend critical assets from cyber threats.

ISA/IEC 62443-3-3 is a section of the standard that defines security requirements to ensure that an IACS meets the target security level for protection against cyber threats and other risks.

Safous makes it easier to align with these requirements by enforcing access governance, identity management, and remote monitoring across IT, OT, and IoT systems – all without disrupting legacy OT environments. For businesses connecting to control systems, Safous provides the cloud-native foundation needed for secure remote operations in complex ICS environments.

This checklist highlights selected ISA/IEC 62443-3-3 requirements that Safous directly supports. Full compliance with this standard requires additional organizational processes, security controls, and system configurations beyond the scope of Safous.

Safous and ISA/IEC 62443-3-3 Alignment

ISA/IEC 62443-3-3 Requirement	How Safous Helps
SR 1.1 RE 1-2 – Human user identification and authentication	Enforces user-specific identity verification and MFA for all access to OT/ICS systems.
SR 1.2 – Software process and device identification and authentication	Authenticates user devices and proxies application access to reduce unauthorized entry points.
SR 1.3-1.5 – Account and credential management	Integrates with identity platforms and supports role-based controls, vaulting, and credential lifecycle enforcement.
SR 1.7 RE 1-2 – Strength of password-based authentication	Enforces custom password policies, expiration, and complexity rules via directory integrations.
SR 1.8–1.9 – PKI and certificate validation	Supports TLS 1.2+ with external CA integration, certificate path validation, and revocation checks.
SR 1.10 – Authenticator feedback	Obscures login credentials (e.g., masked passwords) to prevent side-channel attacks.
SR 1.11 – Unsuccessful login attempts	Detects brute-force attempts and locks accounts after a set number of failed logins.
SR 1.12 – System use notification	Allows admins to display customizable pre-login banners and system use agreements.

ISA/IEC 62443-3-3 Requirement	How Safous Helps
SR 1.13 RE 1 – Access via untrusted networks and explicit access approval	Monitors, filters, and alerts on all remote access from external networks with full session visibility.
SR 2.1 RE 1-2 – Authorization enforcement	Helps enforce least-privilege access via RBAC by mapping access to roles, zones, and application types.
SR 2.1 RE 3–4 – Supervisor override and dual approval	Supports just-in-time access and session approvals for critical actions.
SR 2.5 – Session lock	Automatically locks inactive sessions after a configurable idle period.
SR 2.6 – Remote session termination	Allows admins to manually or automatically terminate privileged sessions in real time.
SR 2.7 – Concurrent session control	Limits concurrent sessions per user with customizable enforcement settings.
SR 2.8 – Auditable events	Captures full session logs, user commands, screen activity, and access events for compliance.
SR 2.9 – Audit storage capacity	Stores session and event logs centrally with configurable retention settings and WORM options.
SR 2.11 RE 1-2 – Timestamps and protected time source	Generates timestamped logs and integrates with trusted NTP sources for accuracy.
SR 2.12 – Non-repudiation	Binds each session to a verified user identity with unalterable activity logs.
SR 3.1 – Communication integrity	Uses encrypted, proxy-based connections to preserve communication integrity and logically isolate application sessions.
SR 3.2 RE 1-2 – Malicious code protection and management	Performs pre-connection posture checks (e.g., AV status, OS patching) to support malicious code protection policies.
SR 3.3 – Security functionality verification	Supports session inspection, change audits, and anomaly detection during normal operations.
SR 3.4 – Software and information integrity	Detects and records unauthorized changes made during remote sessions.
SR 3.8 RE 1-3 – Session integrity	Assigns unique session IDs, terminates expired sessions, and protects against hijacking.
SR 3.9 – Protection of audit information	Helps prevent tampering with session recordings and audit logs using immutable storage options and RBAC.
SR 4.1 – Information confidentiality	Applies end-to-end encryption and application-level session isolation to protect data-in-transit and prevent session-level eavesdropping or lateral exposure.
SR 4.3 – Use of cryptography	Enforces industry-standard cryptographic protocols (TLS 1.2+/1.3) for all communications.

ISA/IEC 62443-3-3 Requirement	How Safous Helps
SR 5.1 – Network segmentation	Limits network exposure by enabling application-level access without direct network access.
SR 5.2 – Zone boundary protection	Helps enforce deny-by-default access policies by allowing traffic only to approved applications.
SR 6.1 – Audit log accessibility	Restricts log access to authorized users through defined roles and permissions.
SR 7.1 – DoS protection	Provides DoS protection at the Safous POP layer and isolates individual app sessions, enabling early traffic filtering and termination of misbehaving sessions to reduce service disruption.
SR 7.2 – Resource management	Applies usage caps to protect system resources from overload and maintain session performance.
SR 7.3 RE 1-2 – Control system backup, verification, and automation	Supports automated backup and export of Safous logs, which can be integrated into the broader IEC 62443-3-3 SR 7.3 control system backup strategy.
SR 7.6 – Network and security configuration settings	Centralizes security and access policies, with support for export and review.
SR 7.7 – Least functionality	Restricts unused protocols and services; limits user actions based on access policy.

Simplify ISA/IEC 62443 Compliance Alignment With Safous

Safous helps you align with ISA/IEC 62443 through a single, cloud-native platform built for critical infrastructure. Gain secure access management, real-time monitoring, and detailed audit trails without adding complexity.

Contact us today to see how Safous can support your compliance roadmap.

EXPLORE SAFOUS

safous