positive technologies

PT Industrial Security Incident Manager

White Paper:
Implementing ISA/IEC 62443-3-3 Requirements with PT ISIM

Table of Contents

1. About this Document and its Target Audience

This White Paper provides an analytical overview and practical guide on implementing the system security requirements outlined in the international standard ISA/IEC 62443-3-3, using the industrial cybersecurity solution PT Industrial Security Incident Manager (PT ISIM) by Positive Technologies.

Target Audience

- Chief Information Security Officers (CISOs) and heads of industrial cybersecurity departments.
- Security Operations Center (SOC) analysts and security engineers.
- Industrial Control System (ICS/OT) architects and network infrastructure specialists.
- Integrators of industrial automation systems and IT solutions.
- Decision-makers responsible for ensuring technological process continuity and protecting critical information infrastructure (CII).

2. Extended Overview: Purpose and Structure of ISA/IEC 62443-3-3

The **ISA/IEC 62443** standard is the world's leading framework of rules and recommendations for ensuring the cybersecurity of Industrial Automation and Control Systems (IACS).

Part **ISA/IEC 62443-3-3 ("System security requirements and security levels")** is central to the technical block of the standard. Its primary purpose is to define specific technical requirements for control systems necessary to achieve designated target Security Levels (SL).

General Structure

The document is based on seven Foundational Requirements (FR) that form the bedrock of industrial cyber defense:

1. **FR 1: Identification and Authentication Control (IAC)** — Verifying the identity of users, devices, and processes.
2. **FR 2: Use Control (UC)** — Enforcing authorization policies, controlling sessions and mobile code, and maintaining audit logs.
3. **FR 3: System Integrity (SI)** — Protecting data and communication channels from unauthorized changes, and defending against malicious code.
4. **FR 4: Data Confidentiality (DC)** — Preventing data leaks at rest or in transit.
5. **FR 5: Restricted Data Flow (RDF)** — Network segmentation, zone isolation, and network boundary management.
6. **FR 6: Timely Response to Events (TRE)** — Monitoring, accessing audit logs, and detecting violations.
7. **FR 7: Resource Availability (RA)** — Protecting against DoS attacks, managing configurations, and data backup.

Each Foundational Requirement is broken down into System Requirements (SR) and Requirement Enhancements (RE), the applicability of which depends on the required Security Level (SL-1 to SL-4) for a specific production zone.

3. General Information about PT ISIM, its Purpose, and Capabilities

PT Industrial Security Incident Manager (PT ISIM) is an advanced system for ensuring the cyber resilience of industrial infrastructures, developed by Positive Technologies.

Purpose:

The product is designed for continuous, deep analysis of technological network traffic, IACS asset inventory, and proactive threat hunting. PT ISIM allows for the early detection of cyberattacks, misconfigurations, and unauthorized actions by personnel or contractors without interfering with the production process.

Key Capabilities and Features:

- **Passive Monitoring and Complete Safety for IACS:** PT ISIM receives a copy of the traffic via SPAN ports or TAP devices, operating in a passive mode that eliminates any negative impact on the technological process.
- **Deep Inventory and Network Visibility:** Automatic discovery of equipment, network mapping, and profiling of network interactions. The system collects data using both agentless methods and agents (PT ISIM Endpoint Agent), as well as active scanning.
- **Threat Detection (PT ISTI):** Utilizing a unique, constantly updated database of industrial threat indicators (PT Industrial Security Threat Indicators), it detects vulnerability exploitation, malware activity (including a built-in antivirus module), anomalies, and dangerous commands transmitted via industrial protocols.
- **Centralized Management and Scalability:** The solution's architecture — comprising sensors (PT ISIM View Sensor / netView Sensor), collectors (PT ISIM Collector), host-based software agents (PT ISIM Endpoint Agents), management center (PT ISIM Overview Center) — enables the creation of distributed Industrial Security Operations Centers (Industrial SOCs) for companies of any size.

4. Coverage Matrix: Implementing ISA/IEC 62443-3-3 Requirements with PT ISIM

The table below maps the standard's requirements to the functional capabilities of PT ISIM (Note: this table includes only the fully applicable and populated rows derived from the source data):

Requirement ID	62443 3-3 Requirement	62443 3-3 Requirement Content	PT ISIM Functionality Coverage	Applicable PT ISIM Component
SR 1.2	Software process and device identification and authentication	The control system shall provide the capability to identify and authenticate all software processes and devices.	PT ISIM allows identifying devices, software, and processes of control system components through network node inventory, network traffic analysis, and network scanning.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 1.2 (1)	Unique identification and authentication	The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.	PT ISIM allows uniquely identifying devices, software, and processes of control system components through network node inventory, traffic analysis, and scanning.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 1.13	Access via untrusted networks	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.	PT ISIM implements monitoring and control of network access via untrusted networks by analyzing control system traffic as well as monitoring events and access attempts on endpoints.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.2	Wireless use control	The control system shall provide the capability to authorize, monitor, and enforce usage restrictions for wireless connectivity to the control system.	PT ISIM allows identifying and reporting all unauthorized network devices interacting with control system components, and performs response/restriction functions at the host level.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.2 (1)	Identify and report unauthorized wireless devices	The control system shall provide the capability to identify and report unauthorized wireless devices communicating within the physical environment of the control system.	PT ISIM allows identifying and reporting all unauthorized network devices executing network interactions with control system components.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.5	Session lock	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation.	PT ISIM allows restricting network sessions on individual network nodes, including the ability to fully isolate a node.	PT ISIM Endpoint Agent

Requirement ID	62443 3-3 Requirement	62443 3-3 Requirement Content	PT ISIM Functionality Coverage	Applicable PT ISIM Component
SR 2.6	Remote session termination	The control system shall provide the capability to terminate a remote session automatically after a configurable time period of inactivity or manually.	PT ISIM allows restricting network sessions, including remote ones on individual nodes, providing the ability for full node isolation.	PT ISIM Endpoint Agent
SR 2.7	Concurrent session control	The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user.	PT ISIM allows restricting network sessions, including concurrent sessions for any users on specific network nodes, up to full isolation.	PT ISIM Endpoint Agent
SR 2.8	Auditable events	The control system shall provide the capability to generate audit records relevant to security (access control, errors, system events, etc.).	PT ISIM ensures the collection, processing, and analysis of events and audit logs from operating systems, application software, PLCs, and network devices.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.8 (1)	Centralized management of audit logs	The control system shall provide the capability to centrally manage audit events and collect audit records from multiple components into a single log.	When used within a control system, PT ISIM allows organizing centralized collection, storage, processing, and access to security events and audit data.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.9	Audit storage capacity	The control system shall allocate sufficient audit record storage capacity and provide mechanisms to reduce the likelihood of exceeding capacity.	PT ISIM provides tools for flexible configuration of audit record storage depth depending on the volume of processed data.	PT ISIM View Sensor
SR 2.9 (1)	Warn when audit record storage capacity threshold reached	The control system shall provide the capability to issue a warning when the audit record storage volume reaches a configurable threshold.	Upon reaching storage capacity thresholds, PT ISIM informs users and issues a warning in the interface.	PT ISIM View Sensor
SR 2.10	Response to audit processing failures	The control system shall provide the capability to alert personnel and prevent the loss of essential services in the event of an audit processing failure.	As a centralized system for storing and processing audit data, PT ISIM gives users access to a self-diagnostic system that monitors services and can alert on audit processing failures.	PT ISIM View Sensor
SR 2.11	Timestamps	The control system shall provide timestamps for use in audit record generation.	PT ISIM can process audit records with timestamps, and can also apply its own timestamps automatically.	PT ISIM View Sensor
SR 2.11 (2)	Protection of time source integrity	The time source shall be protected from unauthorized alteration and shall trigger an audit event upon alteration.	PT ISIM allows processing audit events upon unauthorized modification of time source configuration settings and informs the user in the interface.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Requirement ID	62443 3-3 Requirement	62443 3-3 Requirement Content	PT ISIM Functionality Coverage	Applicable PT ISIM Component
SR 2.12	Non-repudiation	The control system shall provide the capability to determine whether a given user performed a specific action.	PT ISIM provides centralized collection and analysis of user action logs, allowing the determination of specific actions or operations performed by a specific user.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.12 (1)	Non-repudiation for all users	The control system shall provide the capability to determine whether a given user (human, software process, or device) performed a specific action.	PT ISIM ensures centralized collection and analysis of event logs for all components and users, allowing the precise identification of actions executed by specific entities.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.1	Communication integrity	The control system shall provide the capability to protect the integrity of transmitted information.	PT ISIM detects integrity violations of transmitted information within network traffic and on control system endpoints.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.2	Protection from malicious code	The control system shall provide the capability to use protection mechanisms to prevent, detect, report, and mitigate the effects of malicious code.	PT ISIM includes fully functional malicious code detection and protection tools.	PT ISIM Endpoint Agent
SR 3.2 (1)	Protection from malicious code on entry and exit points	The control system shall provide the capability to use malicious code protection mechanisms at all entry and exit points.	PT ISIM provides malware protection mechanisms both at entry/exit points and at the network interaction level.	PT ISIM Endpoint Agent
SR 3.2 (2)	Central management and reporting for malicious code protection	The control system shall provide the capability to centrally manage malicious code protection mechanisms.	PT ISIM provides the capability for centralized management of malicious code protection mechanisms.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.3	Security functionality verification	The control system shall provide the capability to support the verification of the intended operation of security functions (FAT, SAT, scheduled maintenance).	When used as a built-in security solution, PT ISIM supports verifying security functions at all stages of the system lifecycle (FAT, SAT, maintenance).	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.3 (1)	Automated mechanisms for security functionality verification	The control system shall provide the capability to use automated mechanisms to support security verification management.	PT ISIM includes functionality for automated security posture verification.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.3 (2)	Security functionality verification during normal operation	The control system shall provide the capability to support the verification of security functions during normal operation.	PT ISIM can be used alongside other Positive Technologies products to perform security function verification during normal operation.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Requirement ID	62443 3-3 Requirement	62443 3-3 Requirement Content	PT ISIM Functionality Coverage	Applicable PT ISIM Component
SR 3.4	Software and information integrity	The control system shall provide the capability to detect, record, report, and protect against unauthorized changes to software and information.	PT ISIM detects unauthorized modifications to software or information, as well as attempts to perform such operations by internal or external users.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.4 (1)	Automated notification of integrity violations	The control system shall provide the capability to use automated tools to notify personnel when integrity discrepancies are detected.	PT ISIM automatically informs users when violations of software or information integrity are detected.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.6	Deterministic output	The control system shall provide the capability to set outputs to a predetermined state under attack conditions.	PT ISIM allows setting and applying automatic response rules for endpoints, bringing them to a required state upon detecting an attack.	PT ISIM Endpoint Agent
SR 3.8	Session integrity	The control system shall protect the integrity of sessions and reject invalid session IDs.	PT ISIM allows setting and applying whitelists for network connections at the network and host levels.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.8 (2)	Unique session ID generation	The control system shall provide the capability to generate a unique session ID for each session.	PT ISIM assigns a unique identifier to every monitored network connection.	PT ISIM View Sensor, PT ISIM Collector
SR 3.9	Protection of audit information	The control system shall protect audit information and audit tools from unauthorized access, modification, and deletion.	Audit info and built-in tools can be protected from unauthorized access/modification via the Endpoint Detection and Response component included in PT ISIM.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 4.1	Information confidentiality	The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported (at rest or in transit).	PT ISIM detects confidentiality breaches performed through unauthorized read/write operations during storage at network nodes (at rest) or during transmission (in transit).	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 4.1 (1)	Protection of confidentiality at rest or in transit via untrusted networks	The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing untrusted networks.	PT ISIM detects confidentiality breaches via unauthorized read/write operations during storage or transmission over remote access channels passing through external untrusted networks.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 4.1 (2)	Protection of confidentiality across zone boundaries	The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.	PT ISIM detects confidentiality breaches via unauthorized read/write operations during transmission across control system network boundaries.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Requirement ID	62443 3-3 Requirement	62443 3-3 Requirement Content	PT ISIM Functionality Coverage	Applicable PT ISIM Component
SR 5.2	Zone boundary protection	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce compartmentalization based on risks.	PT ISIM monitors network communications within and at the boundaries of network segments, and can be flexibly configured to detect zoning violations and cross-segment interactions.	PT ISIM View Sensor, PT ISIM Collector
SR 5.2 (1)	Deny by default, allow by exception	The control system shall provide the capability to deny network traffic by default and allow network traffic by exception.	PT ISIM allows restricting network traffic in accordance with required security policies at the network node level.	PT ISIM Endpoint Agent
SR 5.3	General interpersonal communication restrictions	The control system shall provide the capability to prevent the receipt of general interpersonal communication messages from external users or systems.	PT ISIM allows restricting the transmission and receipt of network communication messages from external networks in accordance with node-level security policies.	PT ISIM Endpoint Agent
SR 5.3 (1)	Prohibit all general interpersonal communication	The control system shall provide the capability to prevent both the transmission and receipt of general interpersonal communication messages.	PT ISIM allows restricting the transmission and receipt of general network communications within the control system between users based on endpoint security policies.	PT ISIM Endpoint Agent
SR 6.1	Audit log accessibility	The control system shall provide the capability for authorized personnel and/or tools to access audit logs on a read-only basis.	PT ISIM supports interfaces and protocols for read-only access to component audit logs and enables centralized log access for users or other systems.	PT ISIM View Sensor
SR 7.7	Least functionality	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols, and/or services.	PT ISIM allows restricting the use of redundant or unused functions, ports, protocols, or services according to endpoint security policies.	PT ISIM Endpoint Agent
SR 7.8	Control system component inventory	The control system shall provide the capability to report the current list of installed components and their associated properties.	PT ISIM ensures deep, comprehensive inventory of software and hardware resources, providing an up-to-date list of all components, properties, operation logs, users, and traffic profiles.	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

5. Conclusion

Implementing the provisions of the ISA/IEC 62443 standard is of **critical importance for ensuring the cyber resilience** of industrial automation systems and Operational Technology (OT) infrastructures. In the current threat landscape, where attacks on industrial facilities are becoming increasingly sophisticated and destructive, basic security measures (such as standard firewalls) are no longer sufficient. Industries require specialized solutions capable of protecting IACS from the "inside" while strictly observing technological process continuity.

Positive Technologies created and continues to actively develop **PT ISIM** precisely to provide industrial enterprises with a reliable, flexible, and fully functional tool. By leveraging advanced deep packet inspection (DPI), asset inventory, and incident detection technologies, PT ISIM enables organizations not only to meet strict technical and procedural requirements (including IEC 62443-3-3) but also to ensure real, practical protection of their critical infrastructure against modern cyber threats.

positive technologies

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage.

Positive Technologies is the first and only cybersecurity company in Russia on the Moscow Exchange (MOEX: POSI), with 220,000 shareholders and counting.