Cyolo

How Cyolo Helps You Achieve Compliance: ISA/IEC-62443-3-3

Use this guide to discover how Cyolo can help your organization comply with the ISA/IEC 62443-3-3 industrial cybersecurity framework.

INTRODUCTION TO ISA/IEC 62443

ISA/IEC 62443 is an international series of standards for securing operational technology (OT) in industrial automation and control systems (IACS). ISA/IEC 62443 sets cybersecurity benchmarks in all industry sectors that use IACS, including but not limted to manufacturing, oil & gas, electric power generation and distribution, building automation, chemical processing, medical devices, and transportation.

Organizations can use ISA/IEC 62443 to help adopt security as part of their operations lifecycle, to set cybersecurity best practices, to assess their security performance, and to mitigate cyber risks to IACS.

ISA/IEC 62443-3-3 is a section of the standard that defines system security requirements for ensuring an IACS meets the target security level and is protected against cyberthreats and other security risks.

INTRODUCTION TO CYOLO PRO

Cyolo PRO (Privileged Remote Operations) is an advanced, infrastructure-agnostic secure access solution built to mitigate the risks of remote privileged access to IACS and other mission-critical systems. Cyolo PRO's decentralized architecture provides exceptional flexibility and can seamlessly adapt to all environments (cloud-connected, on-premise, and offline) without changing or upgrading the existing infrastructure.

Common challenges Cyolo PRO solves include:

- Securing all access points to mission-critical assets, whether remote or on-prem
- Ensuring rapid, secure, and safe support and maintenance for industrial control systems (ICS) and operational technology (OT) environments
- Safely connecting third-party vendors and technicians to OT environments with no agents or end-user downloads required
- Adding multi-factor authentication (MFA) to legacy systems that do not natively support modern identity authentication
- Implementing segmentation, supervision, session recording, and other requirements of industry and/or regional compliance mandates

CYOLO PRO/ISA 62443-3-3 ALIGNMENT

See how the capabilities of the Cyolo PRO advanced secure remote access solution align to the objectives and principles of ISA/IEC 62443-3-3:

ISA/IEC 62443-3-3 Requirement	Cyolo PRO Support Description
SR 1.1 RE 1-2 – Human user identification and authentication The control system shall provide the capability to identify and authenticate all human users and shall provide the capability to employ Multi-Factor Authentication (MFA) for all human user access to the control system.	Cyolo PRO offers configuration and management of user and groups accounts with granular Role-Based Access Controls (RBAC) and MFA capabilities to help ensure that all users are individually identifiable, auditable, and securely controlled when accessing critical systems, networks or information.
SR 1.2 – Software process and device identification and authentication The control system shall have the capability to identify and authenticate all software processes and devices which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.	Cyolo PRO identifies and authenticates connected components as well as applications and devices accessed via the Cyolo platform.
SR 1.3, 1.4, 1.5 – Account management, identifier management and authenticator management The control system shall provide the capability to support the management of all user accounts including creation, activation, modification, and removal of accounts. The access control system shall protect the credentials from unauthorized disclosure and modification when stored and transmitted.	Cyolo PRO provides granular user and group account management within the platform or the ability to integrate with an existing Identity Access Management (IAM) or Privileged Access Management (PAM) platform. Accounts can be assigned specific role-based permissions and can align with an existing moves, adds, and changes (MAC) process. Encryption is used to protect user credentials from unauthorized disclosure and modification when stored and transmitted.
SR 1.7 RE 1-2 – Strength of password-based authentication Control systems using password- based authentication the system shall provide the capability to enforce configurable passwords based on strength, frequency, length and variety of character types.	When using password-based user authentication, Cyolo PRO offers the capability to configure user passwords based on length, character type, and alphanumeric controls. Once set, password rules around change frequency, reuse, global reset, expiry, and more can be configured by system administrators.

ISA/IEC 62443-3-3 Requirement	Cyolo Support Description
SR 1.8 – Public key infrastructure (PKI) Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.	Cyolo PRO uses PKI and also allows the use of external certificate authorities, enabling users to make use of their own trusted certificate authority when accessing the solution's user interface.
SR 1.9 – Strength of public key infrastructure For control systems utilizing public key authentication, the control system shall provide the capability to: **A.** Validate certificates by checking the validity of the signature **B.** Validate certificates by constructing a certification path to an accepted CA or, in the case of self-signed certificates, by deployment leaf certificates **C.** Validate certificates by checking their revocation status **D.** Establish user control of the corresponding private key **E.** Map the authenticated identity to a user	
SR 1.10 – Authenticator feedback The control system shall provide the capability to obscure feedback of authentication information during the authentication process.	All authentication events within Cyolo PRO are secured and encrypted with the capability to obscure authenticator feedback such as masked characters for password entry.
SR 1.11 – Unsuccessful login attempts The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.	Cyolo PRO offers the ability to disable user logins after a configurable number of unsuccessful login attempts. Additionally, inactive users can be disabled from logging in after a configurable period of time. For networked assets that are monitored by Cyolo PRO, multiple failed login attempts will generate alerts within the platform that can be addressed by users.
SR 1.12 – System use notification The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	Cyolo PRO provides system use notifications and a user agreement on the login screen of the solution prior to authentication. This login message can be customized by system administrators.
SR 1.13, 1.13 RE 1 – Access via untrusted networks and explicit access request approval The control system shall provide the capability to monitor, control, approve or deny all methods of access to the control system via untrusted networks.	Cyolo PRO monitors, controls, and alerts on all network access by users or devices from untrusted networks.
SR 2.1 RE 1-2 – Authorization enforcement for all users and permission mapping to roles On all interfaces, the control system shall provide the capability to enforce access authorizations assigned to all human users for use of the control system to support segregation and mapping of duties, permissions and least privilege.	Cyolo PRO provides configurable and granular segregation of duties via internal RBAC capabilities. These can be broken down into high-level permission tiers including view-only, restricted management, and full management. Additional levels of granularity can be enforced to access specific assets, zones, or sites using the same RBAC profile.

ISA/IEC 62443-3-3 Requirement	Cyolo Support Description
SR 2.1 RE 3-4 – Supervisor override and dual approval The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence. The control system shall also support dual approval where an action can result in serious impact on the industrial process.	Cyolo PRO supports both supervisory override and dual approval for critical change operations such as configuration downloads and changes to OT/ICS assets and resources.
SR 2.1 RE 3-4 – Supervisor override and dual approval The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence. The control system shall also support dual approval where an action can result in serious impact on the industrial process.	Cyolo PRO supports both supervisory override and dual approval for critical change operations such as configuration downloads and changes to OT/ICS assets and resources.
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. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.	Cyolo PRO offers the ability to automatically log out from the system after an idle period. This idle period is configurable by the user.
SR 2.6 – Remote session termination The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.	Cyolo PRO supports the ability for a system administrator/ supervisor to terminate an in-progress remote session at any time.
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 to a configurable number of sessions.	Cyolo PRO supports concurrent session controls for solution access via the graphical user interface (GUI).
SR 2.8 – Auditable events The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	Cyolo PRO offers audit records that provide detailed information for both the solution itself and the networked devices it monitors. System health records from Cyolo PRO include detailed information on system health, alerts, asset changes, system backups and events, updates, and more, in a centralized location. This information can also be exported to a security information and event management (SIEM) tool, security orchestration, automation, and response (SOAR) tool or other centralized collection platform.
SR 2.9 – Audit storage capacity The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	Cyolo PRO provides the capability to configure and allocate sufficient storage capacity for audit logs as well as take snapshots in time for backup.

ISA/IEC 62443-3-3 Requirement	Cyolo Support Description
SR 2.11, 2.11 RE 1-2 – Timestamps and protected time source synchronization The control system shall provide timestamps for use in audit record generation and the capability to synchronize internal system clocks at a configurable frequency with a protected network time source with auditable event notification upon alteration.	Cyolo PRO identifies events in real-time and provides timestamps for all recorded events and provides the capability to connect to an external NTP server through an administrator level process.
SR 2.12 – Non-Repudiation The control system shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Cyolo PRO provides uniquely enumerated event IDs as well as detailed logs of all user, process or device activities that take place within the platform.
SR 3.1 – Communication integrity The control system shall provide the capability to protect the integrity of transmitted information.	Cyolo PRO secures communications between all connected components and checks for errors in the data being transmitted between them.
SR 3.1 RE 1 – Cryptographic integrity protection The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.	Cyolo PRO can help to protect the integrity of transmitted data across the ICS environment by continuously monitoring asset communications for anomalous behavior or deviations from baselines.
SR 3.2 – Malicious code protection The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.	Cyolo PRO can identify if an asset has an antivirus or endpoint detection and response (EDR) solution deployed on it as well as continuously monitor the asset for known threat signatures– helping to detect and protect against the transmission and/or execution of malicious code in the environment. These network signatures can be managed from within the UI of Cyolo PRO, allowing users to edit, enable, or disable the signature for tuning purposes.
SR 3.2 RE 1 – Malicious code protection on entry and exit points The control system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points.	
SR 3.2 RE 2 – Central management and reporting for malicious code The control system shall provide the capability to manage malicious code protection mechanisms.	
SR 3.3 – Security functionality verification The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Cyolo PRO has structured internal processes that are followed for platform functionality testing and security verification during FAT, SAT, and UAT processes. Tools or functions such as pen tests, host and port scans and baseline deviation notifications are best practices that Cyolo uses to ensure proper security functionality during normal operations.
SR 3.3 RE 2 – Security functionality verification during normal operation The control system shall provide the capability to support verification of the intended operation of security functions during normal operations.	

ISA/IEC 62443-3-3 Requirement	Cyolo Support Description
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 at rest.	Cyolo PRO detects, records, and reports when deviations to software or information at rest occur to resources accessed by the platform. These alerts help to protect against unauthorized changes to asset configurations, programs, or functionality. Cyolo PRO provides the capability to automatically send integrity notifications and alerts to an organization's security operations center (SOC) or network operations center (NOC), enabling near real-time security violation mitigation.
SR 3.4 RE 1 – Automated notification about integrity violations The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.	
SR 3.8 – Session integrity The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.	Cyolo PRO generates unique token IDs for every new session and protects session integrity by invalidating token IDs after session termination, either from user logout or the closing of a session window.
SR 3.8 RE 1 – Invalidation of session IDs after session termination The control system shall provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).	
SR 3.8 RE 2 – Unique session ID generation The control system shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid.	
SR 3.8 RE 3 – Randomness of session ID The control system shall provide the capability to generate unique session IDs with commonly accepted sources of randomness.	
SR 3.9 – Protection of audit information The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.	Cyolo PRO helps ensure the protection of all audit and network information with the use of granular user RBAC settings.
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, whether at rest or in transit.	Cyolo PRO provides the capability to provide read only/view only sessions.
SR 4.1 – Information confidentiality SR 4.1 RE 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 an untrusted network.	Cyolo PRO protects the information collected from IACS environments at rest and in-transit with the use of secure shell (SSH) and secure sockets layer (SSL) protocols.
SR 4.1 RE 2 - Protection of confidentiality across zone boundaries The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.	Information traversing the zone boundary through a Cyolo PRO session is protected to ensure confidentiality.

ISA/IEC 62443-3-3 Requirement	Cyolo Support Description
SR 4.3 – Use of cryptography If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.	Cyolo PRO employs the use of Advanced Encryption Standard (AES) for tokens when using the our solution.
SR 5.1 RE 3 – Logical and physical isolation of critical networks The control system shall provide the capability to logically and physically isolate critical control system networks from non- critical control system networks.	
SR 5.2 – Zone boundary protection The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	
SR 5.2 RE 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 (also termed deny all, permit by exception).	
SR 6.1 – Audit log accessibility The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Cyolo PRO's audit logs are available on a read-only basis to an authorized user.
SR 7.1 RE 2 – Limit DoS effects to other systems or networks The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.	Because each Cyolo PRO connection is individualized, the solution can terminate any session that is causing a denial-of-service (DoS) event within an organization's environment.
SR 7.2 – Resource management The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	Cyolo PRO provides internal resource management options for disk / CPU usage within the system health information interface in order to help prevent resource exhaustion that can impact security functions.

ISA/IEC 62443-3-3 Requirement	Cyolo Support Description
SR 7.3 – Control system backup The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.	Cyolo PRO supports ad hoc or scheduled backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations. All backups are capable of integrity validation to ensure the ability to restore or compare, if needed.
SR 7.3 RE 1 – Backup verification The control system shall provide the capability to verify the reliability of backup mechanisms.	
SR 7.3 RE 2 – Backup automation The control system shall provide the capability to automate the backup function based on a configurable frequency.	
SR 7.6 – Network and security configuration settings The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.	Cyolo PRO can be configured to meet control system supplier guidelines for network and security configuration ensuring least privilege access and PAC's and LAC's requirements.
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.	Cyolo PRO provides least functionality requirements by allowing administrators to restrict/prohibit the use of unnecessary functions, services, and ports on the platforms through user configuration and testing.

ABOUT CYOLO

Cyolo, the access company for the digital enterprise, takes a holistic approach to cybersecurity that aligns closely with the ethos of the ISA/IEC 62443 series of standards. The adaptable, infrastructure-agnostic Cyolo PRO solution is purpose-built to secure, monitor, and audit privileged remote connections to IACS and other OT systems.

With Cyolo, organizations like yours can proactively implement the requirements highlighted here with no operational disruptions and no changes needed to your existing infrastructure.

Visit **cyolo.io** or **schedule a demo** to learn more.