CLAROTY

SOLUTION OVERVIEW

CLAROTY & ISA/IEC-62443-3-3

Supporting Compliance with Claroty Industrial Solutions

CLAROTY

TABLE OF CONTENTS

Overview

Protecting critical infrastructure, manufacturing processes, and the cyber-physical systems within them from cyber threats is increasingly important as threats against these organizations grow more prevalent each year. Industrial environments and their underlying operational technology networks are complex, making the establishment of strong cybersecurity measures challenging. This complexity is due to factors like geography, a mix of old and new systems across sites, a wide variety of specialized assets, and the knowledge gaps that exist between traditional IT security practices and operational considerations.

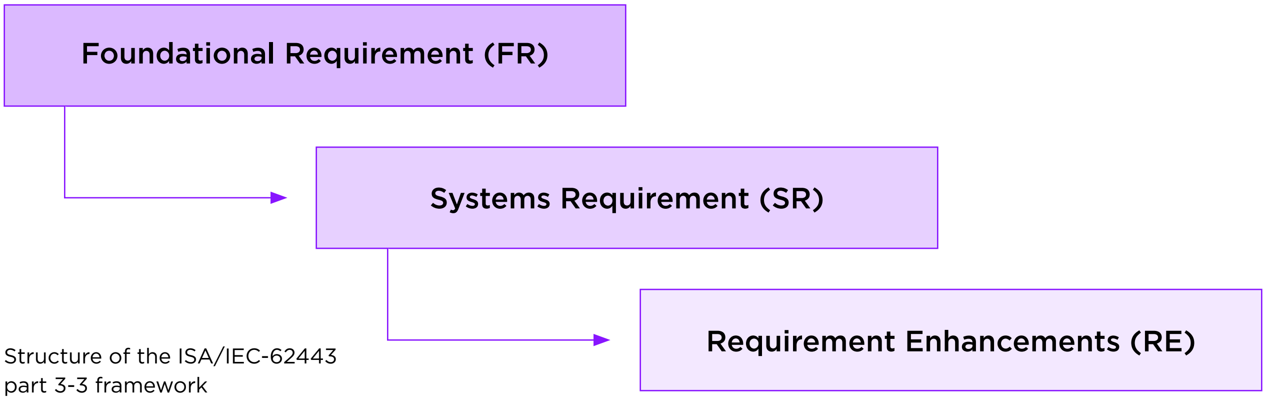
To address these challenges, organizations around the globe collaborate to create cybersecurity standards like ISA/IEC-62443, developed by the International Society of Automation and published by the International Electrotechnical Commission. It provides a comprehensive framework for securing industrial automation and control systems, covering both technical and procedural aspects of cybersecurity.

Having long supported critical infrastructure and manufacturing owners/operators in their efforts to secure complex IACS environments, Claroty is uniquely suited to help these enterprises align with many of the framework's requirements. Our comprehensive industrial cybersecurity solutions, including Claroty xDome, Continuous Threat Detection (CTD), and Secure Remote Access (SRA), were designed for the unique challenges and needs of OT networks. This document outlines how Claroty industrial solutions help to align industrial organizations with the ISA/IEC-62443-3-3 framework.

ISA/IEC-62443-3-3 Structure

The ISA/IEC-62443 framework is arranged into four groups that are applicable to the variety of audiences or focuses within the IACS which they apply. ISA/IEC-62443 part 3-3 defines system security requirements and capability levels to build an IACS that meet a target security level and provides ways for which users can evaluate their security practices.

The framework is broken down into seven Foundational Requirements (FR), each with a series of System Requirements (SR) and Requirement Enhancements (RE) that can be used to reach one of the five target Security Levels (SL). The below diagram lays out the hierarchy of the framework:



Structure of the ISA/IEC-62443 part 3-3 framework

The five Security Levels of the framework indicate their resistance against different magnitudes of attackers. These security levels are:

- **Security Level 0:** No special requirement or protection required.
- **Security Level 1:** Protection against unintentional or accidental misuse.
- **Security Level 2:** Protection against intentional misuse by simple means with few resources, general skills and low motivation.
- **Security Level 3:** Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation.
- **Security Level 4:** Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation.

How this document is structured

This document identifies areas where Claroty solutions (Claroty xDome, CTD, and SRA) provide either **solution support** or **environmental support** for the guidelines set forth by ISA/IEC-62443-3-3.

- **Solution Support:** The System Requirement (SR) is met by the deployed Claroty solution itself as an appliance/software in the IACS environment.
- **Environment Support:** The System Requirement (SR) is supported throughout the IACS environment by the deployed Claroty solution, helping ensure site-wide compliance.

Foundational Requirements & Claroty

This section of the document introduces the seven Foundational Requirements (FR) of ISA/IEC-62443-3-3 and their system requirements and enhancements, as well as how Claroty Industrial Solutions support each. System Requirements (SR) that are not applicable to Claroty solutions have not been included in this section.

FR1 - Identification & Authentication Control

The development of a comprehensive list of all users, including humans, software processes, and devices, for each control system component is crucial in ensuring the necessary level of FR1 - Identification & Authentication Control protections. This process is a fundamental aspect for safeguarding IACS. By verifying the identity of any user before granting access, FR1 System Requirements play a pivotal role in preventing unauthorized access and potential security breaches. Additionally, it is essential to tailor the FR1 mechanisms to the specific needs of different components within the system. While some components might necessitate robust authentication methods, others might not, underscoring the need for versatile and adaptable strategies to meet FR1 System Requirements. This approach not only enhances security but also ensures efficient and effective operation of control systems in various environments.

Description	Claroty Solution Coverage	Claroty Support Description
SR 1.1 – Human User Identification and Authentication. The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Solution Support (xDome, CTD, and SRA)	Claroty solutions offer configuration and management of user accounts and groups of users with granular role-based access controls (RBAC) – including specific functionalities, view-only permissions, full administration, and more. User identification can be performed locally or via LDAP over SSL connection for Active Directory or SAML methods, with support for multi-factor authentication. These granular access controls help to ensure that the vast array of sensitive network and device data within Claroty solutions is not only secure, but helps to streamline the user experience based on their role in the organization.
SR 1.1 RE 1 – Unique Identification and Authentication The control system shall provide the capability to uniquely identify and authenticate all human users.	Solution Support (xDome, CTD, and SRA)	
SR 1.1 RE 2 – Multifactor Authentication for Untrusted Networks The control system shall provide the capability to employ multi-factor authentication for all human user access to the control system.	Solution Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.	Solution Support (xDome, CTD, and SRA)	Claroty solutions identify and authenticate their connected components (Sensors, CTD servers, CTD Enterprise Management Console, xDome collectors) as well as all internal software processes. The status and health of these components is visible within each solution to help ensure solution uptime and direct troubleshooting activities.
SR 1.3 – Account management The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	Solution Support (xDome, CTD, and SRA)	Claroty solutions provide granular user account management and integrations with services like Active Directory. User accounts can be added to groups, modified by assigning specific permissions, or deleted by system administrators. Additionally, all user activity is tracked within our solutions and can be exported or forwarded to syslog for audit and/or review.
SR 1.4 – Identifier management The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.	Solution Support (xDome, CTD, and SRA)	Claroty solutions offer the configuration of user and/or group capabilities via strict RBAC parameters. These can be broken down into three high-level permission tiers: view-only, restricted management, and full management. These controls help to increase the integrity of the data in Claroty solutions and streamline the user experience based on their specific role in the organization.
SR 1.5 – Authenticator management The control system shall provide the capability to: A. initialize authenticator content; B. change all default authenticators upon control system installation; C. change/refresh all authenticators; and D. protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	Solution Support (xDome, CTD, and SRA)	Claroty requires that all default user accounts must be changed after their initial setup and does not store credentials in clear-text format. Platform components are authenticated via tokens in order to provision access and share data with the user.

Description	Claroty Solution Coverage	Claroty Support Description
SR 1.6 – Wireless access management The control system shall provide the capability to identify and authenticate all users engaged in wireless communication.	Environment Support (CTD and xDome)	Using multiple discovery methods, Claroty CTD and xDome provide a comprehensive asset inventory that enables the identification of any wireless devices that are discovered and operating within the network. This visibility provides a foundation for further cybersecurity controls on wireless devices.
SR 1.7 – Strength of password-based Authentication For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	Solution Support (xDome, CTD, and SRA)	When using password-based user authentication, Claroty solutions offer the capability to configure user passwords based on length, character type, and alphanumeric controls. Once set, password rules surrounding change frequency, reuse, global reset, expiry, and more can be configured by system administrators. These granular password rules help to ensure the integrity of Claroty solutions.
SR 1.7 RE 1 – Password Generation and Lifetime Restrictions for Human Users The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users.	Solution Support (xDome, CTD, and SRA)	
SR 1.7 RE 2 – Password Lifetime Restrictions for all Users The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users.	Solution Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
SR 1.8 – Public Key Infrastructure 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.	Environment Support (CTD and xDome)	Claroty uses PKI as well as allows the use of external certificate authorities, allowing users to make use of their own trusted certificate authority when accessing their 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	Solution Support (xDome, CTD, and SRA)	
SR 1.10 – Authenticator feedback The control system shall provide the capability to obscure feedback of authentication information during the authentication process.	Solution Support (xDome, CTD, and SRA)	All authentication events within Claroty solutions are secured and encrypted, offering 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.	Environment Support (xDome, CTD, and SRA)	Claroty solutions offer the capability 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 Claroty solutions, multiple failed login attempts will generate alerts within the solution that can be addressed by users.

Description	Claroty Solution Coverage	Claroty Support Description
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions provide 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 – 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.	Environment Support (xDome, CTD, and SRA)	Claroty solutions monitor and alert on all network access by users or devices from untrusted networks Claroty offers SRA to monitor and control access to the system via untrusted networks.
SR 1.13 RE 1 – Explicit access request approval The control system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.	Environment Support (SRA only)	

FR2 - Use Control

Ensuring that each user, whether a human, software process, or device, is granted only the appropriate level of privileges is a central part of IACS security and is critical in preventing unauthorized actions on control system resources. Once a user is identified and authenticated, the system should verify that they have the necessary privileges to perform actions such as reading or writing data, downloading programs, and adjusting configurations. Asset owners and system integrators must therefore carefully manage user privileges, taking into account various factors like time, location, and access method. Per the System Requirements of FR2 - Use Control, the implementation of such control mechanisms, particularly in environments where different components have varying security requirements, helps maintain the operational integrity and security of the IACS, protecting both the system and its data.

Description	Claroty Solution Coverage	Claroty Support Description
SR 2.1 – Authorization enforcement On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.	Solution Support (CTD and xDome) Environment Support (SRA)	Claroty solutions enable the segregation of duties via granular RBAC assignments that are configurable by a system administrator. These can be broken down into three high-level permission tiers: view-only, restricted management, and full management. An additional level of granularity can be added to access specific assets, zones, or sites using the same RBAC profile. Access permissions can also be mapped via an integration with Active Directory services. In the case of Dual Approval, Claroty SRA supports this when performing critical change operations such as configuration downloads and changes on OT assets.
SR 2.1 RE 1 – Authorization Enforcement for all Users On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all users for controlling use of the control system to support segregation of duties and least privilege.	Solution Support (CTD and xDome) Environment Support (SRA)	
SR 2.1 RE 2 – Permission Mapping to Roles The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.	Solution Support (CTD and xDome) Environment Support (SRA)	
SR 2.1 RE 3 – Supervisor Override The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence.	Environment Support (SRA)	
SR 2.1 RE 4 – Dual Approval The control system shall support dual approval where an action can result in serious impact on the industrial process.	Environment Support (SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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 according to commonly accepted security industry practices.	Environment Support (CTD and xDome)	Claroty CTD and xDome provide a comprehensive asset inventory that enables the identification of any wireless devices that are discovered and operating within the network. These solutions provide the capability to group, create communication policies, and monitor these devices within the network. Wireless devices which violate their assigned policies will generate alerts within the solutions that can either be addressed internally or sent to an integrated SOC solution for investigation and remediation.
SR 2.2 RE 1 - Identify and Report Unauthorized Wireless Devices The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.	Environment Support (CTD and xDome)	
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.	Solution Support (xDome, CTD, and SRA) Environment Support (SRA)	Claroty solutions offer 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.	Environment Support (SRA)	Claroty SRA supports the ability for a system administrator/supervisor to terminate a current 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.	Solution Support (xDome, CTD, and SRA)	Claroty Industrial Solutions support concurrent session controls for solution access via the GUI.

Description	Claroty Solution Coverage	Claroty Support Description
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.	Environmental Support (xDome, CTD, and SRA)	Claroty solutions offer audit records that provide detailed information for both the solution itself and the networked devices it monitors. System health records from Claroty solutions provide detailed information on system health, alerts, asset changes, system backups and events, updates, and more, all in a centralized location. Claroty solutions support syslog integrations that enable them to export this information and more to external syslog servers, SIEM, SOAR, and others for centralized collection.
SR 2.8 RE 1 – Centrally managed, system-wide audit trail The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system- wide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).	Environmental Support (xDome, CTD, and SRA)	
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.	Environmental Support (xDome, CTD, and SRA)	Claroty solutions provide the capability to store audit logs internally as well as take snapshots in time for backup. System health checks include information related to internal disk space usage.
SR 2.9 RE 1 - Warn when Audit Record Storage Capacity Threshold Reached The control system shall provide the capability to issue a warning when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.	Environmental Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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 and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Solution Support (xDome, CTD, and SRA)	If a solution's available storage space fills up to a specified limit it will begin making room in order to continue to deliver critical functionality like generating alerts.
SR 2.11 – Timestamps The control system shall provide timestamps for use in audit record generation.	Solution Support (xDome, CTD, and SRA)	Claroty solutions identify events in real-time and provide timespots for all recorded events, additionally providing the option to connect to an external NTP server. The configuration of time sources within the system is restricted to users with administrative access only.
SR 2.11 RE 1 - Internal Time Synchronisation The control system shall provide the capability to synchronize internal system clocks at a configurable frequency.	Solution Support (xDome, CTD, and SRA)	
SR 2.11 RE 2 - Protection of Time Source Integrity The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration.	Solution Support (xDome, CTD, and SRA)	
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions provide a detailed log of all user activities that take place within the solution, including alert resolution/configuration, report scheduling, system changes, threat detection settings, zone rules, and more. All user actions/changes are captured in an exportable log.

FR3 - System Integrity

The rigorous testing and maintenance of IACS are critical to ensuring their reliable and secure operation. These systems undergo various testing stages, including unit testing, factory acceptance testing (FAT), site acceptance testing (SAT), certification, and commissioning, to confirm that they function as intended before production begins. This thorough testing process is vital in identifying and rectifying potential issues, thereby preventing costly and potentially dangerous failures during operation. Once operational, it falls to asset owners to uphold the integrity of the IACS. This involves using risk assessment methodologies to assign appropriate levels of integrity protection to different systems, communication channels, and information within the IACS. A comprehensive approach to securing system integrity, as outlined in FR3 - System Integrity, is crucial for the safe and secure functioning of an IACS.

Description	Claroty Solution Coverage	Claroty Support Description
SR 3.1 – Communication integrity The control system shall provide the capability to protect the integrity of transmitted information.	Solution Support (xDome, CTD, and SRA)	Claroty solutions secure communications between all connected components (Sensors, CTD servers, CTD Enterprise Management Console, xDome collectors) and check for errors in the data being transmitted between them. Additionally, Claroty solutions 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 3.1 RE 1 – Cryptographic integrity protection The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.	Solution Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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.	Environment Support (CTD and xDome)	Claroty solutions can identify if an asset has an antivirus or 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 Claroty solutions, 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.	Environment Support (CTD and xDome)	
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.	Environment Support (CTD and xDome)	

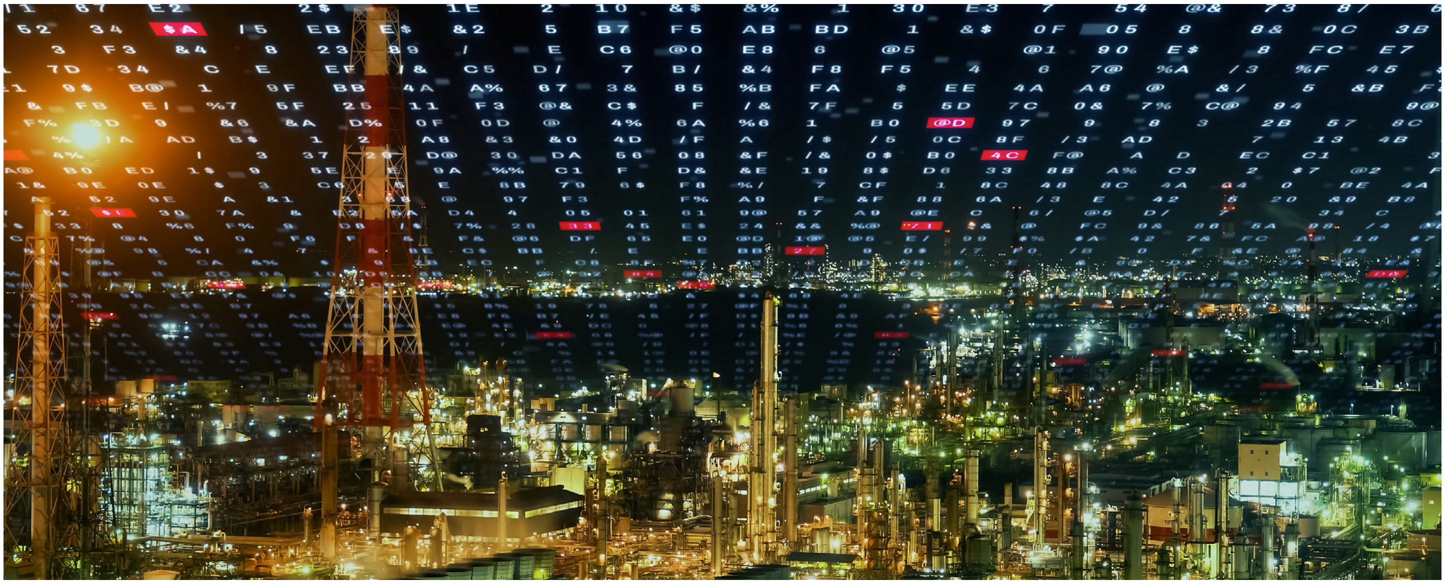
Description	Claroty Solution Coverage	Claroty Support Description
SR 3.3 – Security functionality verification The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	Solution Support (xDome, CTD, and SRA)	Claroty deploys rigorous testing of our platforms for security functionality verification during PoVs, FAT, and SAT, as well as scheduled maintenance. Claroty also provides mechanisms to test EICAR test files, host and port scans from known assets in order to generate alerts and automatically resolve them as a way to test known threat alert response. These alerts can be manually tuned in order to adjust the system's tolerance for potential false positives.
SR 3.3 RE 1 – Automated Mechanisms for Security functionality verification The control system shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance.	Solution Support (xDome, CTD, and SRA)	
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.	Solution Support (xDome, CTD, and SRA)	
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.	Environmental Support (CTD and xDome)	Claroty solutions identify and alert when changes to software or information at rest occur within monitored assets in the CPS environment. These alerts help to protect against unauthorized changes to asset configurations, programs, or functionality. These alerts include: • Configuration Download • DCS Configuration Change • Firmware download • Mode Change • Memory Reset • Online Edit • Suspicious File Transfer • And more... Please refer to Claroty user documentation for a comprehensive list of device change alerts.
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.	Environment Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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.	Solution Support (CTD and xDome) Environment Support (SRA)	Claroty solutions generate unique tokens for every new session and protect session integrity by invalidating tokens after session termination, either from logging out or closing the session window. This mechanism extends when using Claroty SRA to remotely access IACS assets, helping to ensure increased session security.
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).	Solution Support (CTD and xDome) Environment Support (SRA)	
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.	Solution Support (CTD and xDome) Environment Support (SRA)	
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.	Solution Support (CTD and xDome) Environment Support (SRA)	
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions help ensure the protection of all audit and network information with the use of granular RBAC settings.

FR4 - Data Confidentiality

Given the sensitive nature of the information that is generated by IACS, certain communication channels and data repositories necessitate robust protection measures to guard against eavesdropping and unauthorized access. Implementing security measures is a critical aspect of preventing potential breaches that could lead to data leaks, operational disruptions, or even more severe consequences. This protection is not just a matter of safeguarding data privacy, but it is also fundamental to ensuring the overall reliability and trustworthiness of the control systems that play a vital role in various industrial and infrastructure operations.

Description	Claroty Solution Coverage	Claroty Support Description
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions protect the information collected from IACS environments at rest and in-transit with the use of SSH and SSL protocols. Information collected from assets across zone boundaries makes use of encryption as well to help ensure confidentiality of information as it traverses the network.
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.	Solution Support (xDome, CTD, and SRA)	
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.	Solution Support (xDome, CTD, and SRA)	
SR 4.2 – Information Persistence The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.	Solution Support (CTD and xDome)	Claroty solutions provide a mechanism to remove asset information and alerts either by user action or by automated retention rules. These rules can be configured by solution administrators to determine the length of time which asset information is stored.
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.	Solution Support (xDome, CTD, and SRA)	Claroty employs the use of Advanced Encryption Standard (AES) for tokens when accessing our solutions.



FR5 - Restricted Data Flow

The application of risk assessment methodologies by asset owners is a useful exercise for determining the appropriate restrictions for information flow within IACS and implementing tailored measures helps to mitigate risks associated with information flow. These measures can vary widely, from completely isolating control system networks from business or public networks to employing advanced techniques like directional gateways, firewalls, and demilitarized zones (DMZs). Strategies like those laid out in FR5 - Restricted Data Flow are not just about preventing unauthorized access; they are about maintaining the delicate balance between operational efficiency and a strong security foundation.

Description	Claroty Solution Coverage	Claroty Support Description
SR 5.1 – Network segmentation The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	Environment Support (CTD and xDome)	Claroty solutions leverage superior visibility and profiling to automatically virtually segment CPS into zones–logical groups of assets that communicate with one another under normal operations. These zones can be tailored to fit the unique communication paths in your environment and provide a visualized look at "normal" network behavior. As a method of network segmentation, Claroty solutions network protection capabilities help lay the foundation for Zero Trust practices that are core to improving an organization's industrial cybersecurity posture.
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.	Environment Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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.	Environment Support (CTD and xDome)	Claroty solutions can monitor the above-mentioned zones for communication anomalies and policy deviations. If observed, these anomalies will generate alerts for system administrators and/or security personnel to investigate. Monitored zone communications can be configured into policy rules and exported to existing network infrastructure for enforcement.
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).	Environment Support (Integrations - CTD and xDome)	

FR6 - Timely Response to Events

In order to create effective lines of communication and controls to respond effectively to security violations, asset owners must establish policies and procedures for communication and reporting as outlined in FR6 - Timely Response to Events. This includes the formulation of guidelines and recommendations for collecting, reporting, preserving, and correlating forensic evidence. Additionally, while the implementation of monitoring tools and techniques is vital for maintaining system security, it is equally important to ensure that these measures do not negatively impact the operational performance of the control system. Balancing security vigilance with operational efficiency is key to maintaining the reliability and effectiveness of the IACS environment.

Description	Claroty Solution Coverage	Claroty Support Description
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions' audit logs are comprehensive across all users' actions and are available on a read-only basis
SR 6.2 – Continuous monitoring The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	Environment Support (CTD and xDome)	Claroty solutions continuously monitor network assets via the passive monitoring of network traffic. This continuous monitoring allows the network to categorize "normal" network behavior and track anomalous activity, known indicators of compromise, and threat signatures, among other types of threats to the environment. Any event which meets a configurable threshold of relevance automatically generates a context-rich alert for users to investigate and address as needed.

FR7 - Resource Availability

The primary aim of this section is to ensure that the control system is resilient against various types of Denial of service (DoS) events. A core aspect of this is to ensure that security incidents within the control system do not compromise Safety Instrumented Systems (SIS) or other safety-related functions. Ensuring resilience is vital to maintain not only the operational integrity of IACS, but also to safeguard against potential safety hazards that could arise from system failures or disruptions.

Description	Claroty Solution Coverage	Claroty Support Description
SR 7.1 – Denial of service protection The control system shall provide the capability to operate in a degraded mode during a DoS event.	Solution Support (xDome, CTD, and SRA)	Claroty solutions provide alerts for denial of service attacks against CPS. The effects of these attacks can be limited via context-rich alerts that provide a summary of all assets involved in the attack and recommendations for how to mitigate its effects. Claroty solutions are able to continue operating during DoS events as part of our solutions built-in security controls.
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.	Solution Support (xDome, CTD, and SRA)	

Description	Claroty Solution Coverage	Claroty Support Description
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions provide internal resource management options for disk / CPU usage within the system health information interface in order to help prevent resource exhaustion that can hamer security functions.
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions support creating one-time or scheduled backups of data with the platform. By default the system configuration, data (including assets, insights, and alerts), events, and PCAP files (if desired) are included in the backup data. These backups can be scheduled based on user-defined times and frequency. Backup files can be saved locally or by SMB share and can be created by the centralized interface.
SR 7.3 RE 1 – Backup verification The control system shall provide the capability to verify the reliability of backup mechanisms.	Solution Support (xDome, CTD, and SRA)	
SR 7.3 RE 2 – Backup automation The control system shall provide the capability to automate the backup function based on a configurable frequency.	Solution Support (xDome, CTD, and SRA)	
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions maintain flexible deployment options and can be configured according to the specific environments in which they are being deployed. Based on assessments of the user's environment Claroty recommends configurations that will help meet the security policies and goals of the environment.

Description	Claroty Solution Coverage	Claroty Support Description
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.	Solution Support (xDome, CTD, and SRA)	Claroty solutions provide 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.
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.	Environment Support (CTD and xDome)	Claroty solutions leverage a broad CPS protocol library and multiple discovery methods (passive, safe queries, Claroty Edge, project file analysis, and ecosystem integrations) to create an in-depth, comprehensive inventory of networked assets. This multi-spectral method of asset discovery helps to uncover areas of the network that are traditionally hard to reach for standard or IT-centric discovery techniques.

Conclusion

The ISA/IEC-62443-3-3 framework Foundational and System Requirements highlight the critical role of cybersecurity measures in safeguarding IACS against an increasing cyber threat landscape. The framework underscores the complexities of industrial environments and operational technology networks, which necessitate these tailored cybersecurity approaches. Claroty's industrial cybersecurity solutions, including Claroty xDome, Continuous Threat Detection (CTD), and Secure Remote Access (SRA), are specifically designed to meet the unique challenges of OT networks, aligning with the ISA/IEC-62443-3-3 framework across a variety of the Foundational Requirements listed within it. The sections above detail how Claroty's industrial solutions support the framework's Foundational Requirements, offering both solution-level and environmental support to ensure the protection and continued operation of industrial systems.

To learn more about Claroty's comprehensive suite of industrial cybersecurity solutions, visit https://claroty.com/industrial-cybersecurity.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.

CLAROTY