MEETING RELEVANT ISA/IEC 62443

Security Controls addressed by the XONA Critical Systems Gateway (CSG)

+1 866-849-6629 | info@xonasystems.com

The ISA/IEC 62443 set of security requirements is an expansive yet flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The standards are applicable to all critical infrastructure industry sectors and cover a wide range of topics from terminology, concepts, and models to security technologies for IACS, and much more.

XONA™ provides security capabilities to meet the requirements of the 62443 standards pertaining to access control, identification and authentication control, use control, data confidentiality, and least privilege. XONA utilizes protocol and system isolation, encrypted display, multi-factor authentication, session logging, and recording of user access to support this compliance, thus securing against cybersecurity risks.

ANSI/ISA-62443-2-1 (99.02.01) – 2009

The XONA platform provides foundational requirements and additional security levels for Access Control to cyber assets through the following:

4.3.3.5 Element: Access Control: Account Administration – XONA ensures, on an ongoing basis, that only appropriate entities have accounts that allow access and that these accounts provide appropriate access privileges.		
✓	4.3.3.5.3 Authorize account access	XONA grants, changes, or terminates access on the authority of an appropriate manager.
✓	4.3.3.5.4 Record access accounts	XONA maintains a record of all access accounts, including details of the individual(s) and devices authorized to use the account, their permissions, and the authorizing manager.
✓	4.3.3.5.5 Suspend or remove unneeded accounts	XONA suspends or removes access accounts as soon as they are no longer needed (for example, job change).

4.3.3.6 Element: Access Control: Authentication – XONA positively identifies network users, hosts, applications, services, and resources for computerized transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.		
✓	4.3.3.6.2 Authenticate all users before system use	XONA authenticates all users before using the requested application, unless there are compensating combinations of entrance control technologies and administrative practices.
✓	4.3.3.6.3 Require strong authentication methods for system administration and application configuration	XONA uses strong authentication practices (such as requiring strong passwords) on all system administrator and application configuration access accounts.
✓	4.3.3.6.4 Log and review all access attempts to critical systems	XONA log files record on all access attempts to critical systems and reviews them for successful and failed access attempts.
✓	4.3.3.6.5 Authenticate all remote users at the appropriate level	XONA employs an authentication scheme with an appropriate level of strength to positively identify a remote interactive user.
✓	4.3.3.6.6 Develop a policy for remote login and connections	XONA has a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity.
✓	4.3.3.6.7 Disable access account after failed remote login attempts	After some number of failed login attempts by a remote user, XONA disables the access account for a certain amount of time.
✓	4.3.3.6.8 Require re-authentication after remote system inactivity	After a defined period of inactivity, XONA requires a remote user to re- authenticate before he or she can re-access the system.
✓	4.3.3.6.9 Employ authentication for task-to-task communication	XONA employs appropriate authentication schemes for task-to-task communication between applications and devices.

4.3.3.7 Element: Access Control: Authorization – XONA grants access privileges to resources upon successful authentication of the user and identification of his or her associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.		
✓	4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices	XONA's permission to access IACS devices is logical (rules that grant or deny access to known users based on their roles), physical (locks, cameras, and other controls that restrict access to an active computer console), or both.
✓	4.3.3.7.3 Control access to information or systems via role-based access accounts	XONA's access accounts are role based to manage access to appropriate information or systems for that user's role. Safety implications are considered when defining roles.
✓	4.3.3.7.4 Employ multiple authorization methods for critical IACS	In critical control environments, XONA employs multiple authorization methods to limit access to the IACS.

4.3.4.3 Element: System Development and Maintenance – XONA ensures that the organization's desired risk tolerance level is maintained as its IACS assets evolve through the maintenance of existing systems and development and procurement of new systems.		
✓	4.3.4.3.7 Establish and document a patch management procedure	XONA ensures that the organization's desired risk tolerance level is maintained as its IACS assets evolve through the maintenance of existing systems and development and procurement of new systems.
Note: XONA does not support 4.3.4.3.1 - 6, 8 & 9.		

ANSI/ISA-62443-3-3 (99.03.03) – 2013

The XONA platform supports requirements for Identification and Authentication Control, Use Control, Data Confidentiality, Network Segmentation, and Timely Response to Events through the following:

5 FR 1 – Identification and authentication control (IAC) – XONA provides the capability to identify and authenticate all human users. This capability enforces 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

✓	5.3.1 SR 1.1 – Human user identification and authentication	XONA provides the capability to identify and authenticate all human users.
✓	5.3.3 RE (1) Unique identification and authentication	XONA provides the capability to uniquely identify and authenticate all human users.
✓	5.3.3 RE (2) Multifactor authentication for untrusted networks	XONA provides the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).
✓	5.3.3 RE (3) Multifactor authentication for all networks	XONA provides the capability to employ multifactor authentication for all human user access to the control system.

5.4 SR 1.2 – Software process and device identification and authentication – XONA provides the capability to identify and authenticate all software processes and devices. This capability enforces 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.

✓	5.4.3 RE (1) Unique identification and authentication	

5.5 SR 1.3 – Account management – XONA provides the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling, and removing accounts.

✓	5.5.3 RE (1) Unified account management	XONA provides the capability to support unified account management.

5.6 SR 1.4 – Identifier management – XONA provides the capability to support the management of identifiers by user, group, role or control system interface. Identifiers: user identification may be role-based, group-based or device-based.

5.7 SR 1.5 – Authenticator management – XONA provides 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.
Control system authenticators include, but are not limited to, tokens, symmetric keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys, and key cards.

✓	5.7.3 RE (1) Hardware security for software process identity credentials	For software process and device users, XONA provides the capability to protect the relevant authenticators via hardware mechanisms.

5.8 SR 1.6 – Wireless access management – XONA provides the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

✓	5.8.3 RE (1) Unique identification and authentication	XONA provides the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.10 SR 1.8 – Public key infrastructure certificates – XONA provides the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

5.11 SR 1.9 – Strength of public key authentication – Utilizing public key authentication, XONA provides the capability to:
a) validate certificates by checking the validity of the signature of a given certificate;
b) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued;
c) validate certificates by checking a given certificate's revocation status;
d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).

✓	5.11.3 RE (1) Hardware security for public key authentication	XONA provides the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations.

5.12 SR 1.10 – Authenticator feedback – XONA provides the capability to obscure feedback of authentication information during the authentication process.

5.14 SR 1.12 – System use notification – XONA provides the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

5.15 SR 1.13 – Access via untrusted networks – XONA provides the capability to monitor and control all methods of access to the control system via untrusted networks.

✓	5.13.3 RE (1) Explicit access request approval	XONA provides the capability to deny access requests via untrusted networks unless approved by an assigned role.

6 FR 2 – Use control (UC)

6.3 SR 2.1 – Authorization enforcement – On all interfaces, XONA provides 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.

✓	6.3.3 RE (1) Authorization enforcement for all users	On all interfaces, XONA provides the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.
✓	6.3.3 RE (2) Permission mapping to roles	XONA provides the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.
✓	6.3.3 RE (3) Supervisor override	XONA supports supervisor manual override of the current human user authorizations for a configurable time or event sequence.
✓	6.3.3 RE (4) Dual approval	XONA supports dual approval where an action can result in serious impact on the industrial process.

6.5 SR 2.3 – Use control for portable and mobile devices – XONA provides the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and
c) restricting code and data transfer to/from portable and mobile devices.

✓	6.5.3 RE (1) Enforcement of security status of portable and mobile devices	XONA provides the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.

6.7 SR 2.5 – Session lock – XONA provides 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.

6.8 SR 2.6 – Remote session termination – XONA provides 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.

6.9 SR 2.7 – Concurrent session control – XONA provides the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.

6.10 SR 2.8 – Auditable events – XONA provides 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 include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

✓	6.10.3 RE (1) Centrally managed, system-wide audit trail	XONA provides 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. XONA provides 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).

6.14 SR 2.12 – Non-repudiation – XONA provides the capability to determine whether a given human user took a particular action.		
✓	6.14.3 RE (1) Non-repudiation for all users	XONA provides the capability to determine whether a given user (human, software process or device) took a particular action.
8.0 FR 4 – Data confidentiality (DC)		
✓	8.3 SR 4.1 – Information confidentiality	XONA provides the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.
✓	8.3.3 RE (1) Protection of confidentiality at rest or in transit via untrusted networks	XONA provides the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.
9.3 SR 5.1 – Network segmentation – XONA provides 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.		
✓	9.3.3 RE (1) Physical network segmentation	XONA provides the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.
✓	9.3.3 RE (2) Independence from non-control system networks	XONA has the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.
✓	9.3.3 RE (3) Logical and physical isolation of critical networks	XONA provides the capability to logically and physically isolate critical control system networks from non-critical control system networks.
10 FR 6 – Timely response to events (TRE)		

10.3 SR 6.1 – Audit log accessibility – XONA provides the capability for authorized humans and/or tools to access audit logs on a read-only basis.		
✓	10.3.3 RE (1) Programmatic access to audit logs	XONA provides programmatic access to audit records using an application programming interface (API).

ANSI/ISA-62443-4-2-2018

The XONA platform supports technical security requirements for IACS components in the following ways:

4.4 CCSC 3 Least privilege – When required and appropriate, XONA provides the capability for the system to enforce the concept of least privilege. XONA provides the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability is available when required.		

5.3 CR 1.1 – Human user identification and authentication – XONA provides the capability to identify and authenticate all human users according to ISA-62443-3-3 [11] SR 1.1 on all interfaces capable of human user access. This capability enforces such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability can be provided locally or by integration into a system level identification and authentication system.		
✓	5.3.3 Requirement enhancements	XONA provides the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.
✓	5.3.3 RE (1) Unique identification and authentication:	XONA provides the capability to uniquely identify and authenticate all human users.
✓	5.3.3 RE (2) Multifactor authentication for all interfaces	XONA provides the capability to employ multifactor authentication for all human user access to the component.

5.4 CR 1.2 – Software process and device identification and authentication – XONA provides the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA-62443-3-3 [11] SR1.2. All entities are identified and authenticated for all access to the control system. Authentication of the identity of such entities is accomplished by using methods such as passwords, tokens, or location (physical or logical). This requirement is applied to both local and remote access to the control system

✓	5.4.3 Requirement enhancements	
✓	5.4.30 RE (1) Unique identification and authentication	XONA provides the capability to uniquely identify and authenticate itself to any other component.

5.7 CR 1.5 – Authenticator management – XONA provides the capability to:
a) support the use of initial authenticator content;
b) support the recognition of changes to default authenticators made at installation time;
c) function properly with periodic authenticator change/refresh operation; and
d) protect authenticators from unauthorized disclosure and modification when stored, used, and transmitted.

✓	5.7.3 RE (1) Hardware security for authenticators	XONA protects the authenticators via hardware mechanisms.

5.10 CR 1.8 – Public key infrastructure certificates – When public key infrastructure (PKI) is utilized, XONA provides or integrates into a system that provides the capability to interact and operate in accordance with ISA-62443-3-3 [11] SR1.8.

5.11 CR 1.9 – Strength of public key-based authentication – For components that utilize public-key-based authentication, XONA provides directly or integrates into a system that provides the capability within the same IACS environment to:
a) validate certificates by checking the validity of the signature of a given certificate;
b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;
c) validate certificates by checking a given certificate's revocation status;
d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device); and f) ensure that the algorithms and keys used for the public key authentication comply with 8.5 CR 4.3 – Use of cryptography.

✓	5.11.3 RE (1) Hardware security for public key-based authentication	XONA provides the capability to protect critical, long-lived private keys via hardware mechanisms.

5.12 CR 1.10 – Authenticator feedback – XONA's authentication capability provides the capability to obscure feedback of authenticator information during the authentication process.

5.13 CR 1.11 – Unsuccessful login attempts – XONA's authentication capability provides the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and

5.14 CR 1.12 – System use notification – For local human user access/HMI, XONA provides the capability to display a system use notification message before authenticating. The system use notification message is configurable by authorized personnel.

5.15 CR 1.13 – Access via untrusted networks – The access via untrusted networks requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

6 FR 2 – Use control

6.1 Purpose and SL-C(UC) descriptions – XONA enforces the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

6.3 CR 2.1 – Authorization enforcement – XONA provides an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

✓	6.3.3 Requirement enhancements	
✓	6.3.3 RE (1) Authorization enforcement for all users	XONA provides an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.
✓	6.3.3 RE (2) Permission mapping to roles	XONA provides for an authorized role to define and modify the mapping of permissions to roles for all human users.

✓	6.3.3 RE (3) Supervisor override	XONA supports a supervisor manual override for a configurable time or sequence of events.
✓	6.3.3 RE (4) Dual approval	XONA supports dual approval when action can result in serious impact on the industrial process.

6.5 CR 2.3 – Use control for portable and mobile devices – There is no component level requirement associated with ISA-62443-3-3 SR 2.3.

6.7 CR 2.5 – Session lock

✓	6.7.1 Requirement	With XONA's human user interface, whether accessed locally or via a network, XONA provides the capability: a) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and b) for the session lock to 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.

6.8 CR 2.6 – Remote session termination

✓	6.8.1 Requirement	With regard to remote sessions, XONA provides the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.

6.10 CR 2.8 – Auditable events – XONA provides the capability to generate audit records relevant to security for the following categories:

a) access control;
b) request errors;
c) control system events;
d) backup and restore event;
e) configuration changes; and
f) audit log events. Individual audit records include:
a) timestamp;
b) source (originate device, software process or human user acct);
c) category;
d) type;
e) event ID; and
f) event result.

6.13 CR 2.11 – Timestamps		
✓	6.13.1 Requirement	XONA provides the capability to create timestamps (including date and time) for use in audit records.
✓	6.13.3 Requirement enhancements	
✓	6.13.3 RE (1) Time synchronization	XONA provides the capability to create timestamps that are synchronized with a system wide time source.
✓	6.13.3 RE (2) Protection of time source integrity	XONA's time synchronization mechanism provides the capability to detect unauthorized alteration and cause an audit event upon alteration.

6.14 CR 2.12 – Non-repudiation		
✓	6.14.1 Requirement	XONA provides the capability to determine whether a given human user took a particular action.
✓	6.14.3 Requirement enhancements	
✓	6.14.3 RE (1) Non-repudiation for all users	XONA provides the capability to determine whether a given user (human, software process or device) took a particular action.

8.5 CR 4.3 – Use of cryptography		
✓	8.5.1 Requirement	If cryptography is required, XONA will use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

10.3 CR 6.1 – Audit log accessibility		
✓	10.3.1 Requirement	XONA provides the capability for authorized humans and/or tools to access audit logs on a read-only basis.
✓	10.3.3 Requirement enhancements	
✓	10.3.3 RE (1) Programmatic access to audit logs	XONA provides programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system

12.3 SAR 3.2 – Protection from malicious code		
✓	12.3.1 Requirement	XONA qualifies and documents which protection from malicious code mechanisms are compatible with XONA and note any special configuration requirements.

15.2 NDR 1.6 – Wireless access management		
✓	15.2.1 Requirement	A network device supporting wireless access management provides the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.
✓	15.2.3 Requirement enhancements	
✓	15.2.3 RE (1) Unique identification and authentication	XONA's network device provides the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

15.3 NDR 1.13 – Access via untrusted networks		
✓	15.3.1 Requirement	XONA provides the capability to monitor and control all methods of access to the network device via untrusted networks.
✓	15.3.3 Requirement enhancements	
✓	15.3.3 RE (1) Explicit access request approval	XONA provides the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.

15.7 NDR 3.10 – Support for updates		
✓	15.7.1 Requirement	XONA supports the ability to be updated and upgraded.
✓	15.7.3 Requirement enhancements	
✓	15.7.3 RE (1) Update authenticity and integrity	XONA validates the authenticity and integrity of any software update or upgrade prior to installation.

15.8 NDR 3.11 – Physical tamper resistance and detection		
✓	15.8.1 Requirement	XONA provides tamper resistance and detection mechanisms to protect against unauthorized physical access into the device

15.11 NDR 3.14 – Integrity of the boot process		
✓	15.11.1 Requirement	XONA verifies the integrity of the firmware, software, and configuration data needed for the device's boot process prior to it being used in the boot process.
✓	15.11.3 Requirement enhancements	
✓	15.11.3 RE (1) Authenticity of the boot process	XONA uses its own roots of trust to verity the authenticity of the firmware, software, and configuration data needed for the device's boot process prior to it being used in the boot process.

5.1 Purpose and SL-C(IAC) descriptions
Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets.
SL 1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities.
SL 2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
SL 3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
SL 4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

+1 866-849-6629 | info@xonasystems.com