TXOne Networks

2023

/Q2

Securing Digital Manufacturing: The Essence of ISA/IEC 62443 Implementation

txOne networks

Contents

Introduction

Industrial Control Systems (ICS) are control systems used for automating industrial production processes. These systems are prevalent in industries such as power, water, oil, natural gas, and others, with common control systems including SCADA, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC). ICS uses networks to connect control loops, Human Machine Interfaces (HMI), and remote diagnostic and maintenance tools. Control loops adjust the process to be controlled through sensors, actuators, and controllers such as PLCs.

Sensors convert the physical state they measure into digital data from analog signals and send it to controllers as control variables. Controllers parse control variables to calculate corresponding operation variables and send them to actuators (such as control valves, circuit breakers, switches, and motors). Upon receiving commands from the controller, the actuators adjust the process. HMIs can display the current state of the process and procedural information. Maintenance personnel and engineers can monitor and plan equipment set points, control logic, and parameters within the controller via the HMI. Remote diagnostic and maintenance tools primarily aim to identify and prevent anomalies or faults. If the anomalies or faults aren't prevented, these tools are also used to restore the operation process.

However, today's industrial networks and critical infrastructures have become a hotbed for cybercriminals. We have observed that since the outbreak of the COVID-19 crisis, the world's reliance on networks and information systems has soared to unprecedented levels, with industries and services becoming increasingly interconnected. The COVID-19 crisis illustrates the necessity to adequately prepare for the digital transformation of major global industries, especially in enhancing the cyber resilience of critical infrastructure services such as energy, transportation, chemical, and critical manufacturing. The increasing range and types of cyberattacks in recent years underscore the world's need for a higher level of cyber resilience to protect critical industries and the day-to-day lives underpinned by these industries.

The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have established the ISA/IEC 62443 series of standards. It is a framework for gradually implementing best practices in industrial network security and promoting continuous improvement. ISA/IEC 62443, formerly known as ISA 99, is a global standard for Industrial Control System (ICS) network security. The standard was founded by the International Society of Automation (ISA) and was taken over by the International Electrotechnical Commission (IEC), which is now responsible for its development. Thus, the main goal of IEC technical committees is the preparation of International Standards; every three years, technical specifications can be reviewed to assess whether they can become new International Standards. All that being said, the IEC does not hold any responsibility for misinterpretation on the part of the end user, necessitating a nuanced understanding of the latest IEC standards, which this paper shall attempt to impart.

Overview of ISA/IEC 62443

Understanding ISA/IEC 62443

The ISA/IEC 62443 in particular is concerned with security for industrial automation and control systems (IACS), i.e., control systems that use automated or remotely controlled/monitored assets. These IACS can be found in manufacturing and process plants/facilities, utilities that are geographically spread out, pipelines and petroleum production and distribution facilities and other industries like transportation networks. “Security” refers to the preventions of illegal or unwanted penetration, interference (intentional or otherwise), or unauthorized access to confidential information. To home in further, the ISA/IEC 62443 series includes several standards and technical reports, each discussing a specific aspect of the cybersecurity of Industrial Automation and Control Systems (IACS). The overall objective is to reduce the risk of cyber threats and safety failures in IACS. The standard consists of 14 documents divided into four groups: general, policies and procedures, system, and component.

1. General: This group explains the common elements across the series.
    a. ISA/IEC 62443-1-1, first released in 2007, introduces the concepts and modules of the ISA/IEC 62443 series.
    b. ISA/IEC 62443-1-2 is a technical report that explains the proprietary terms and acronyms used in the ISA/IEC 62443 series.
    c. ISA/IEC 62443-1-3 describes the standards of basic and system-related quantification methods for the ISA/IEC 62443 series.
    d. ISA/IEC 62443-1-4 uses examples to illustrate the lifecycle safety technical report of the IACS component layer.
2. Policies and Procedures: This group explains the policies and procedures related to IACS security.
    a. ISA/IEC 62443-2-1, first released in 2009, outlines the requirements and definitions for the IACS network security management system, including the responsibilities of users and device owners.
    b. ISA/IEC 62443-2-2 provides guidelines for the operation requirements of the IACS network security management system.
    c. ISA/IEC 62443-2-3 was jointly published by ISA and IEC in 2015 as an update management guidance report for IACS.
    d. ISA/IEC 62443-2-4 is a standard for requirements guidelines for other control system suppliers.

3. System Requirements: This group emphasizes security requirements at the system level.
   a. ISA/IEC 62443-3-1 describes the security technical report used in the IACS environment.
   b. ISA/IEC 62443-3-2 emphasizes the standard for IACS system security design and risk assessment.
   c. ISA/IEC 62443-3-3, released in 2013, is a standard for system security and security level requirements.
4. Component Requirements: This group emphasizes the security requirements for IACS-related product development.
   a. ISA/IEC 62443-4-1 is a standard for product development requirements.
   b. ISA/IEC 62443-4-2 is a standard for system specification requirements for subsystems, system components, and other control system suppliers.

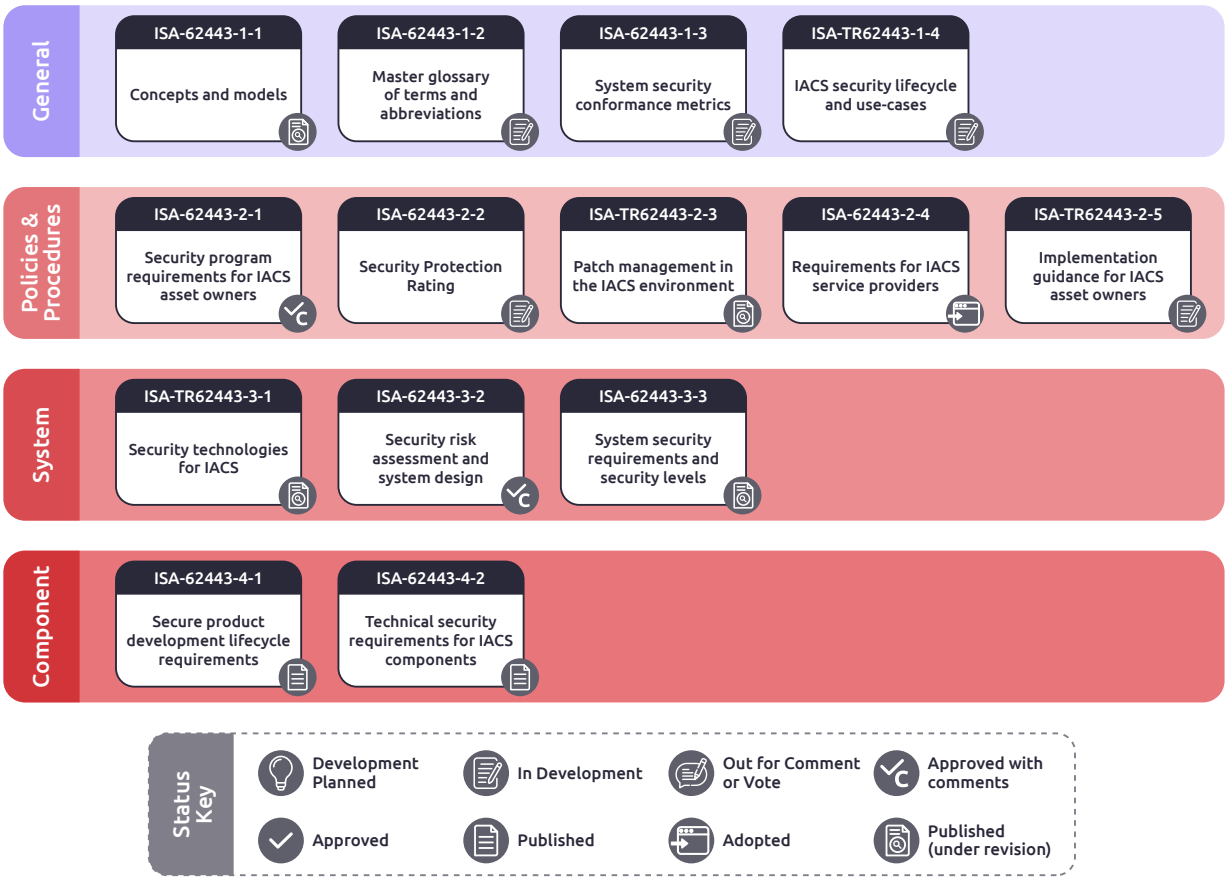

Figure 1. ISA/IEC 62443 Family
Source: International Society of Automation

Principal Roles in ISA/IEC 62443

ISA/IEC 62443 is a set of standards for Industrial Automation and Control Systems (IACS), providing guidance on how to safeguard these systems against cyber threats. This set is extensive and relevant to various stakeholders, including asset owners, service providers, and product manufacturers. Specifically, ISA/IEC 62443 assists all these parties in assessing whether their products or services offer functional cybersecurity capabilities to meet the cybersecurity objectives (SL-T) of asset owners. Here we have narrowed down three types of stakeholders and what the ISA/IEC 62443 means to them:

1. **Asset Owners:**

   These are entities that own and operate Industrial Control Systems (ICS). Generally, asset owners are aided by ISA/IEC 62443-2-1 security plan requirements to create a Cyber Security Management System (CSMS) that oversees the security of IACS throughout its lifecycle. When introducing ICS, they can utilize ISA/IEC 62443-2-3, which outlines the patch management requirements in the IACS environment. If an internal department is executing the integration of the IACS system, ISA/IEC 62443-3-3 helps them understand the cybersecurity technical requirements of automation solutions.

2. **Service Providers:**

   These can be consultants or companies offering services like system integration, maintenance, and other ICS-related services. Asset owners might require service providers to have a security plan based on ISA/IEC 62443-2-4, which is useful when creating procurement specifications. Additionally, service providers can carry out assessments and design based on the existing ICS environment by using the risk evaluation method delineated in ISA/IEC 62443-3-2 and define security function requirements as per ISA/IEC 62443-3-3. Therefore, ISA/IEC 62443-2-4 and ISA/IEC 62443-3-3 are of significant importance to service providers.

3. **Product Manufacturers:**

   These are companies that produce IACS hardware and software components. ISA/IEC 62443 provides them with a set of best practices for designing and developing secure products. This includes the secure development lifecycle process (ISA/IEC 62443-4-1) and integrating security measures into product design (ISA/IEC 62443-4-2). When product manufacturers have a service team providing support services for the product, ISA/IEC 62443-3-3 helps the manufacturer understand the cybersecurity technical requirements of automation solutions.

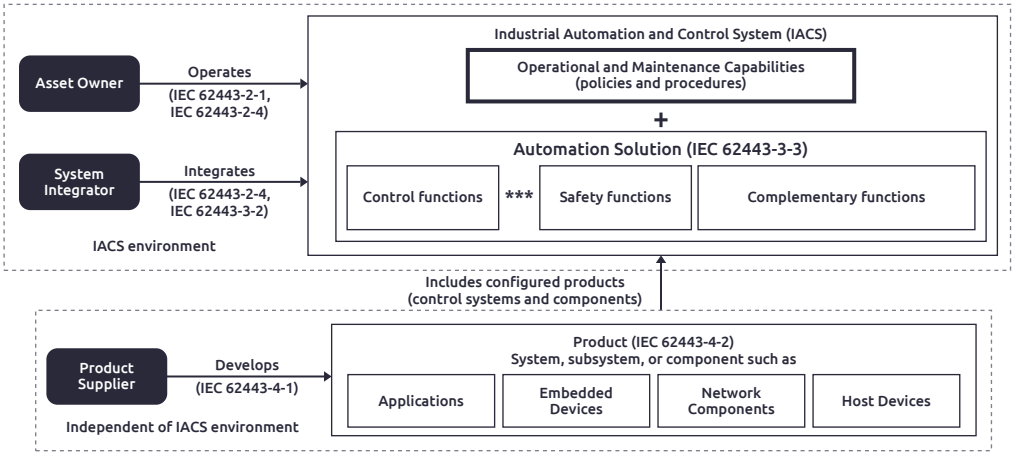

Figure 2. The roles of ISA/IEC 62443 family
Source: ISAGCA

Compliance and Certification

Adherence to this standard shows that an organization has implemented a systematic, risk-based approach to securing its IACS, thus supporting certification efforts and providing assurance to stakeholders and clients. The current verifiable standards can be roughly divided into two types:

- Security Standards: ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 are security standards. Essentially, they define the security level of the product, where the product refers to systems, subsystems, and related components in IACS. Further, 4-2 subdivides components into software, embedded devices, networking equipment, and control equipment.
- Process Standards: These processes and procedures apply to organizations. Basic processes under ISA/IEC 62443-2-4 are divided into service procedures such as maintenance, update, installation, deployment, configuration, etc., as well as the product development process procedures under ISA/IEC 62443-4-1.

1. ISASecure Certification Scheme

ISCI is a non-profit organization comprised of asset owners, equipment suppliers, testing laboratories, and experts in the industrial control sector, aiming to enhance the industry's security. ISASecure is a conformity certification program managed by ISCI. Passing ISASecure certification indicates that Industrial Automation Control (IAC) products and systems possess strong resistance to cyberattacks and are confirmed to have no known vulnerabilities.

- ISASecure Component Security Assurance (CSA) Certification

  This certification checks whether a component (product) is developed following the IEC 62443-4-1 process requirements and meets the security requirements of IEC 62443-4-2. The component (product) to be certified can have its compliance measured against any one of the four security assurance levels. (Different security assurance levels have different security requirements).

- ISASecure System Security Assurance (SSA) Certification

  This certification verifies whether a system is developed according to the IEC 62443-4-1 process requirements and meets the security requirements of IEC 62443-3-3. The system to be certified can also have its compliance measured against any one of the four security assurance levels. (Different security assurance levels have different security requirements).

- ISASecure Security Development Lifecycle Assurance (SDLA) Certification

  This certification verifies whether an organization develops products following the IEC 62443-4-1 secure development lifecycle. SDLA certification does not take into consideration the maturity of the process.

2. IECEE Certification System CB Scheme

The IECEE Certification Body Scheme is operated by the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE). It's an international system for mutual acceptance of test reports and certificates concerning the safety of electrical and electronic components, equipment, and products. It is a multilateral agreement between participating countries and certification organizations, aimed at facilitating trade through alignment of national standards with international standards and cooperation among globally recognized National Certification Bodies (NCBs).

- Scenario 1: Capability evaluation (Technical: IEC 62443-3-3 / IEC 62443-4-2 Process: IEC 62443-2-4 / IEC 62443-4-1)
- Scenario 2: Application of capabilities evaluation for specific products/solutions.

Table 1. IECEE Certification System CB Scheme

Standards	IEC 62443-2-4	IEC 62443-3-3	IEC 62443-4-1	IEC 62443-4-2
Process	Scenario 1	N/A	Scenario 1	N/A
Product	Scenario 1	Scenario 1	Scenario 2	Scenario 1
Solution	Scenario 2	Scenario 2	N/A	N/A

Source: www.iecee.org

Broad Industry Applicability

This standard is applicable across various industries, demonstrating its versatility. Whether a business operates in the energy sector, water treatment, manufacturing, or any other field that uses IACS, ISA/IEC 6244-3-3 remains relevant.

- Oil and gas
- Renewables
- Energy and power
- Utilities
- Manufacturing
- Electrical and electronic equipment

The System Security Framework for IACS: ISA/IEC 62443-3-3

The ISA/IEC 62443-3-3 standard provides a critical framework for cybersecurity in Industrial Automation and Control Systems (IACS). This part of the ISA/IEC 62443 series offers specific technical security requirements and defines distinct Security Levels (SLs), addressing various degrees of threats and potential impacts. Key features of this framework include:

Defense in Depth

Organizations typically cannot achieve security objectives (availability, integrity, confidentiality) through the application of a single protective measure or technology. A superior approach is the employment of the concept of Defense in Depth. This principle emphasizes building a defense mechanism through layered or step-by-step methods and the utilization of multiple protective measures. The primary advantage of this approach is that if one defense mechanism fails, other mechanisms should be capable of thwarting threats, thereby maintaining business continuity. This means deploying a variety of different controls and protective methods, such as firewalls, intrusion detection systems, access control, physical security measures (like locks and biometric systems), user education, and security policies, instead of solely relying on a single layer of defense. The ISA/IEC-62443 standard further recommends segregating systems into different “zones”, which can communicate with each other through communication channels known as “conduits”.

Zones and Conduits

The ISA/IEC-62443 proposes an industrial control system architecture that capitalizes on the Purdue reference model used in ISA95, dividing these functional levels into zones and conduits.[2,3]

1. **Zones:**

   Security zones, henceforth to be referred to as simply zones, are a way to address the different levels of security that are acceptable in a given system. A zone is defined in the IEC 62443-1-1 as “a logical grouping of physical, informational, and application assets sharing common security requirements”. The key points here are the common security requirements. When it comes to large or complex systems, it is not necessary to apply the same level of security to every single component—this is impractical and not an economical use of resources. Therefore, zones are created so that all the areas that need to be protected at the same level can have that security level applied at once. Zones can be trusted or untrusted, and the security protocol around them should be adjusted according to their status.

   This also contributes to defense in depth, since different properties can be assigned to zones and these zones can be further divided into subzones, creating layered security. Each zone has a border, delineating where the zone begins and ends, providing a boundary between included and excluded assets. They

can be roughly categorized as physical zones or virtual zones. Physical zones are literally defined by the assets' proximity to each other in their physical location and are considered in a physical sense. Virtual zones group assets, or parts of physical assets, based on their functionality or other common characteristics and are not defined by the assets' physical location and are considered in a logical manner.

An organization should assess the security requirements or security goals of a zone and, based on that, decide on which assets should be considered in or out of the zone. Since a zone has a boundary, there is an implied need for access to the assets in a zone both from within and without. Therefore, the security requirements based on access can be broken into the following types:

- Communications' access: Assets within a zone provide no value if they cannot be linked to assets outside of that zone. Access to entities outside the zone can be in the form of physical movement (of assets or people) or electronic communication. Communications can be divided into either a) remote communication, wherein the transfer of information occurs between entities that are not close to each other, or b) local access, which is when communication occurs between assets in the same zone.
- Physical access and proximity: When access to a particular area needs to be limited, physical security zones prove to be very useful. Within this zone, all the systems need to have the same level of clearance, or trust, between the human operators, maintainers, and developers of that area. Protecting against unauthorized access can be accomplished with something as simple as locks on doors. A typical manufacturing plant would be considered a physical security zone since only authorized people are granted access by an authorizing agent, usually a security guard or their ID card, and unauthorized people are prevented from entering by that authorizing agent. All assets within this physical zone need to be protected at the same minimum level of security requirements and those that fall outside of it are not protected and therefore cannot be trusted at the same security level.

2. Conduits:

Now that we've covered access between zones, we can move onto how information moves, either flowing into, out of, or within a security zone. In a system that isn't networked, there will be occasions where communication is necessary such as when programming devices are connected to create/upkeep systems. In order to provide a construct that encompasses the security aspects and requirements of communications, the ISA/IEC 62443 has identified a special type of security zone: a communications' conduit. A conduit bundles together communications that can logically be categorized together. They can connect entities within a zone, or they may connect a zone to another zone entirely. Conduits, like zones, can also be thought of as trusted or untrusted. Those that do not cross zone boundaries would largely be trusted by the zone's communicating processes, while conduits crossing zone boundaries need to have an end-to-end secure process to remain trusted. Conduits that are at a different level of security as the endpoint of the zone are untrusted.

Within conduits there are specific communication links that are called channels. Trusted channels allow secure communication with other security zones, and can be used to extend a virtual zone to include entities that aren't in the physical security zone. Untrusted channels are not at the same level of security

and communications to and from the zone; communications from untrusted channels need to be validated before accepting the information.

This division is based on the results of the security risk assessment specified in ISA/IEC-62443-3-2. Once a detailed risk assessment is conducted, optimal segmentation of zones and conduits can be achieved. This model aids in assessing common threats, vulnerabilities, and the corresponding threat levels required to achieve security objectives (SL-T) required for grouped assets. By grouping assets, a security policy can be defined for all assets and deployed to the assets in that zone, then the appropriate protection required can be determined based on the current security level (SL-A) based on the activities carried out within the zone.

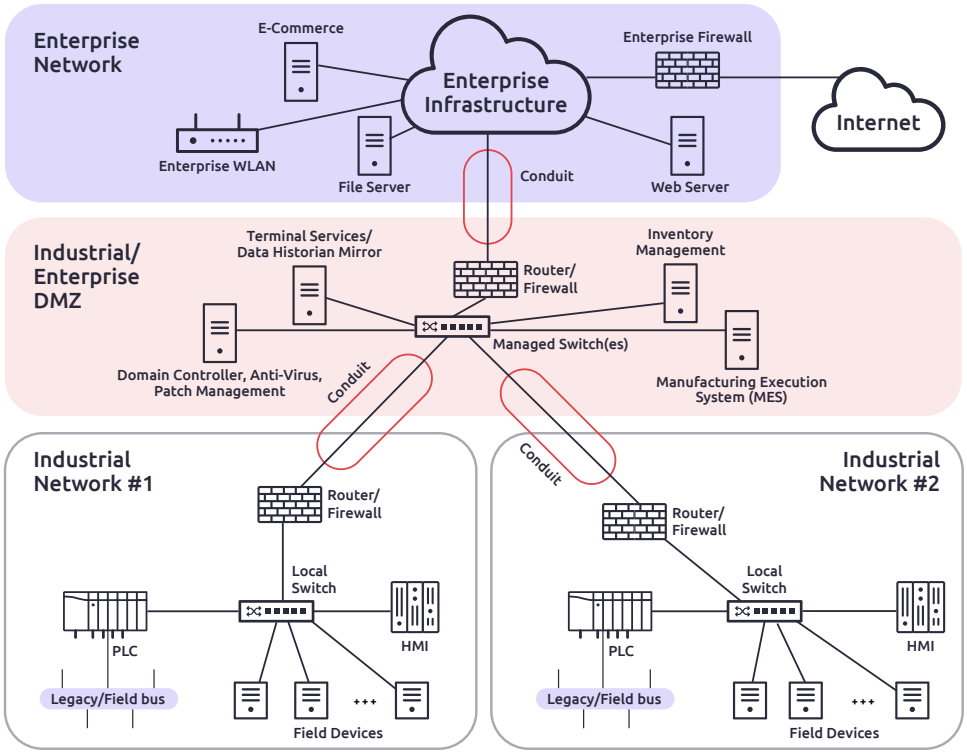

Figure 3. Example of industrial network zones and conduits
Source: IEC 62443-3-3

Application of Risk Analysis

The concept of risk analysis based on Criticality, Likelihood, and Impact is not new. It has been used to address risks related to production infrastructure, production capability (production downtime), impacts on people (injuries, death), and the environment (pollution). However, this technique needs to be extended to cybersecurity to address inherent risks of automated industrial control systems. ISA/IEC-62443-3-2 describes a method for cybersecurity risk assessment of Industrial Automation and Control Systems (IACS). Adhering to this method also facilitates the division of zones and conduits.

Principle of Least Privilege

This principle only grants users (humans, software, and devices) the permissions required to perform their tasks, in order to prevent unnecessary access to data or programs and to block or slow down attacks when users are under threat.

Security Levels

This technical specification has put forth the concept of security levels in order to make it easier for organizations to make decisions on how to implement countermeasures and devices that are inherently different in their security capabilities. It was also created to construct security solutions based on zones rather than on a systemic or individual basis. It also provides a qualitative method for comparing and managing the security of zones within an organization. Each organization using this method should, first of all, establish in no uncertain terms what each level represents and how the security level should be measured for that zone. It can be used to construct a layered defense-in-depth strategy for a zone that encompasses hardware and software-based technical countermeasures, as well as administrative-type countermeasures. Based on this, the security level method can be used to categorize risk for a zone or conduit and define the required effectiveness of countermeasures to repel unauthorized electronic interference within the zone or conduits.

General Blueprint of 3 Types of Security Levels:[3]

1. SL (Target) – the aspirational level of security, the standard that a zone or conduit should aim for
    - During the risk assessment stage, SL (target) for a zone and conduit should be determined. Whether risk assessment is conducted qualitatively, quantitatively, or semi-quantitatively, this should be a measurement of both the odds of a zone's security being compromised and the consequences thereof, were it to happen. Crucially, this security level delineates how effective countermeasures, devices and systems need to be in order to protect a zone or conduit's security from falling short. Countermeasures can be technical (firewalls, anti-virus software, etc.), administrative (policies and procedures), or physical (locked doors, etc.).
    - While calculating the SL (target) for a zone and conduit, some factors to consider would be network architecture, the SL (target) of other zones with which the current zone in question will communicate, the SL (target) of the conduit used for communication by the zone in question, and physical accessibility to the devices and systems of the zone.
2. SL (Achieved) – the current level of security for the zone or conduit.

    This level refers to the status of the zone or conduit, and will naturally decrease over time due to developing threats or attack methods, the decay of countermeasures, new vulnerabilities, security breaches, etc. Ideally, all of the security properties of the zone and conduit would be reviewed, updated, or upgraded on a regular basis in order to keep the SL (achieved) of a zone or conduit greater than or at least equal to the SL (target).

3. SL (Capability) – the security level capability of countermeasures or the inherent security level capability of devices or systems within a zone or conduit. This level is a measure of the countermeasure, device, or system's effectiveness. A given countermeasure, device, or system can address security properties such as:
    - Proof of peer entity authenticity
    - Preservation of message integrity and authenticity
    - Preservation of confidentiality
    - Confirmation of accountability

- Enforcement of access control policies
- Prevention of denial-of-service attacks
- Maintenance of platform trustworthiness
- Tampering detection
- Security status monitoring

The ISA/IEC 62443 standard divides Industrial Control Systems (ICS) into security zones based on risk assessment. This standard provides guidance on how to select zones and assign Security Levels (SLs). Meeting each level requires certain controls. Organizations must assess the gap between their existing security controls and the assigned levels defined by the standard. These zones are then assigned an SL ranging from 1 to 4, as illustrated in Table 2. Security Levels 1 and 2 correspond to threats from internal personnel or intruders with low skills and motivation. On the other hand, Security Levels 3 and 4 relate to threats from "professional" cybercriminals, industrial spies, or state-supported malicious actors, who exhibit high skill and moderate to high motivation.

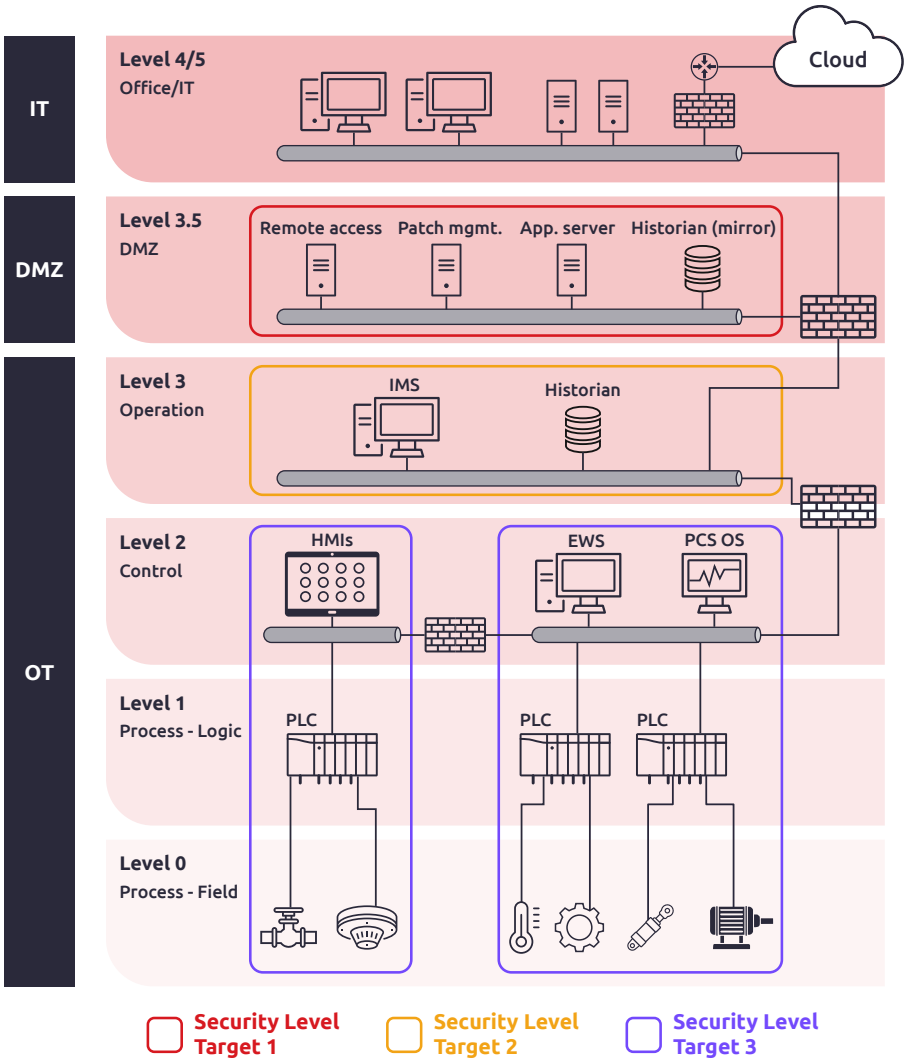

Figure 4. Example of Security Level Target

Even if an organization divides its ICS environment into multiple zones, there will never be zero risk between all zones, as a weakened zone can affect surrounding zones in two ways. Firstly, disruptions in service or operations within a weakened zone can spread to other zones depending on these services. Secondly, the compromise of a zone poses threats closer to other zones. To overcome these challenges, the standard recommends various Requirement Enhancements (REs), with the general rule being that the more REs are met, the higher the Security Level attained.

Table 2. ISA/IEC 62443 security assurance levels

Security level (SL)	Description from ISO/IEC 62443-3-3
SL0	No specific requirements or security protection requirements
SL1	Requires protection against casual or coincidental violations
SL2	Requires protection against intentional violation using simple means with low resources, generic skills and low motivation
SL3	Requires protection against intentional violation using sophisticated means with moderate resources, specific skills and moderate motivation
SL4	Requires protection against intentional violation using sophisticated means with extended resources, specific skills and high motivation

Source: IEC62443-3-3

Foundational Requirements (FRs) and Security Requirements (SRs)

When it comes to information security, the focus falls on achieving three principal objectives: confidentiality, integrity, and availability. For information technology (IT) security strategy, confidentiality may take priority, with integrity and availability falling into second and third priority. But the prioritization of these objectives is often different within the environment of industrial automation and control systems. Availability, instead of confidentiality, takes priority and therefore the security strategy for these systems is geared towards keeping the systems' components available. Due to the risks that are part and parcel to any industrial machinery that is controlled by industrial automation and control systems, integrity is of great importance. Since the data in this IACS environment is typically raw and needs to be both analyzed and contextualized before it can offer any meaningful information, confidentiality is actually of lowest importance. However, the priority of these three objectives are subject to change based on what the operational requirements are. To help users determine the SL requirements within each security zone, the standard categorizes seven Foundational Requirements (FRs) and expands them into a series of System Requirements (SRs) and Requirement Enhancements (REs) to boost security robustness. The ISA/IEC 62443 standard provides practical guidelines on how to implement protective measures against cybersecurity incidents based on defined security levels, broken down into seven basic requirements:[3]

- FR1: Identification and Authentication Control (IAC): Identifies and verifies all users (humans, software, and devices) through protective mechanisms, preventing unauthenticated entities from accessing the system.

- FR2: Use Control (UC): Enforces the specified permissions of authenticated users (humans, software, and devices) to operate the IACS upon request, and monitors these permissions.
- FR3: System Integrity (SI): Ensures the integrity of the industrial automation and control system to prevent unauthorized actions.
- FR4: Data Confidentiality (DC): Ensures data encryption of communication channels and databases to prevent unauthorized disclosure.
- FR5: Restricted Data Flow (RDF): Divides control systems by regions and channels to limit unnecessary data flow.
- FR6: Timely Response to Events (TRE): Notifies the appropriate enforcement agencies when a cybersecurity violation is detected, reports the evidence needed for the violation, and takes corrective measures in a timely manner.
- FR7: Resource Availability (RA): Ensures the availability of the control system, mitigating degradation of performance or denial of access to critical services.

To assist in defining each SL, the standard provides a threat definition for each level and offers a chart to map the SRs and REs to the 1-4 levels of FR security. The threat landscape for ICS varies across each sector, industry type, and organization. Therefore, while these are solid definitions and a good starting point, pay particular attention to your organization's unique defensive posture when considering them. Potentially, SLs may also produce unique differences for each security zone – threats, operational changes, and Industrial Internet of Things (IIoT) technologies can alter the attack surface of an ICS. SLs help to set targets, but these targets must always remain flexible and be actively adjusted to keep pace with changes in global threats.

Table 3. Example of ISA/IEC 62443 Security Levels

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	V	V	V	V
SR 1.1 RE 1 – Unique identification and authentication		V	V	V
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			V	V
SR 1.1 RE 3 – Multifactor authentication for all networks				V

Source: IEC62443-3-3

Simplify Implementation of ISA/IEC 62443-3-3 with TXOne Solutions

ISA/IEC 62443-3-3 provides detailed descriptions of the Security Technical Requirements (SR) for the seven foundational requirements (FR) described in IEC 62443-1-1. These include identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability. For example, for foundational requirement (FR1), SR 1.1 is specified, requiring the control system to provide the ability to identify and authenticate all human users, and some even put forward advanced requirements (RE).

However, when designing and implementing IACS control measures, the limiting factors are quite different from a typical IT environment. In the IT environment, most organizations prioritize confidentiality over integrity and availability. The design of control measures in the OT environment must take care not to impact availability and integrity while maintaining the availability of basic control functions. For instance, in an IT environment, to prevent passwords from being cracked by brute force, it is common to lock accounts after a certain number of unsuccessful attempts. But in an OT environment, to avoid system interruptions, this can't be done. In short, any security logs or control measures planned in an OT environment cannot adversely affect basic functions. We provide cybersecurity technical support to organizations that integrate ICS systems and components, assisting them to meet these product requirements for deployment in ICS/OT networks, in accordance with IEC 62443-3-3 requirements.[3]

FR1: Identification and Authentication Control (IAC)

Asset owners need to create a list of all users (personnel, software processes, and devices) and determine the required IAC (Identification and Authentication Control) protection level for each control system component. The goal of IAC is to protect the control system by validating the identity of any user requesting access to the control system before initiating communication. It is suggested to include mechanisms that operate in a hybrid mode; for instance, some control system components may require robust IAC, while others might not.

Table 4. System Requirements for Identification, Authentication Control, and Access Control

SR	Description	How TXOne Networks Supports Compliance
1.1	Human User Identification and Authentication	Edge Network defense solution has the ability to identify and authenticate users' identities before they gain access to the system.
1.2	Software Process and Device Identification and Authentication	Edge Network defense solution is capable of detecting and regularly monitoring the connectivity status of assets, to ensure that the device is verified and legitimate before any data exchange takes place.
		Stellar has the ability to detect behavioral anomalies and swiftly determine the trustworthiness of operations using an expanded ICS application and certificate library, achieving an optimal balance between performance and detection rates. Furthermore, Stellar employs Trust List technology for the validation of software applications, preventing malicious programs from sending and receiving commands.
		Utilize the Portable Inspector to scan assets; this enables stakeholders to verify the digital hygiene of the assets. This includes basic information about the assets as well as their security status.
1.3	Account Management	Edge Network defense solution has the capacity to empower authorized users to manage all accounts, including the abilities to add, activate, modify, disable, and delete accounts.
1.4	Identifier Management	Stellar has the ability to uniquely identify each device and support the establishment of asset identification tokens for OT system endpoints, centrally managed through StellarOne.
		Edge Network defense solution has the capacity to facilitate the management of identifiers based on user, group, role, or control system interface.
1.5	Authenticator Management	Edge Network defense solution has the capacity to assist with authenticator management, including the initialization of authenticator content, changing all default authenticators upon the system installation, refreshing all authenticators, as well as ensuring protection of all authenticators from unauthorized disclosure and modification during storage and transmission.

SR	Description	How TXOne Networks Supports Compliance
1.7	Strength of Password-Based Authentication	Edge Network defense solution supports the enforcement of configurable password strength, based on minimum length and diversity of character types.
1.8	Public Key Infrastructure Certificates	When PKI is employed, Edge Network defense solution possesses the ability to operate a PKI in line with widely recognized best practices or to acquire public key certificates from an existing PKI.
1.9	Strength of Public Key-Based Authentication	Edge Network defense solution delivers robust capabilities for bolstering the strength of public key-based authentication, including stringent validation of certificates, by scrutinizing signature validity, among other features.
1.10	Authenticator Feedback	Edge Network defense solution possesses the ability to obscure the feedback of authentication information during the authentication process.
1.11	Unsuccessful Login Attempts	Edge Network defense solution supports setting up cybersecurity policies and procedures for network access. When consecutive invalid access attempts occur, the system will record and generate abnormality alerts.
1.12	System Use Notification	Edge Network defense solution possesses the capability to display system usage notification messages prior to authentication, providing an added layer of security. Moreover, these system usage notifications are conveniently configurable by authorized personnel, so you can tailor security to your specific needs.
1.13	Access via Untrusted Networks	Edge Network defense solution is able to restrict access achieved through dial-up connections or connections from others' site networks, and prevent unauthorized connections (such as VPN). Network access can only be established when necessary and after authentication, thereby enabling businesses to reduce attacks on their OT networks.

FR2: Use Control (UC)

Once users are identified and authenticated, the control system must limit permitted actions to those that are authorized for use in the system. Asset owners and system integrators must assign privileges that define IACS (Industrial Automation and Control Systems) authorized usage for each user (personnel, software process, or device), group, role, etc. (SR 1.4 - Identity Management). The goal of Use Control is to prevent unauthorized operations on control system resources, such as reading or writing data, downloading programs, and setting configurations, by verifying that the necessary privileges have been granted before allowing a user to perform any actions.

Some control system resources require robust use control (restrictive privileges) for protection, while others do not. Additionally, user privileges might vary based on time/date, location, and access methods.

Table 5. System Requirements for Use Control

SR	Description	How TXOne Networks Supports Compliance
2.1	Authorization Enforcement	EdgeIPS series supports the principle of least privilege, allowing businesses to minimize the OT attack surface, restrict OT network attacks, enhance operational performance, and mitigate the impact of human error. By implementing fine-grained access control at different levels, businesses can strike a balance between availability and security while safeguarding critical data and systems.
		Stellar supports OT/ICS endpoints in enforcing custom-defined cybersecurity policies and procedures to ascertain whether the operations requested by users are actually permissible. It also supports segregation of duties and the principle of least privilege, all while minimizing the negative impact on operational processes.
2.3	Use Control for Portable and Mobile Devices	Stellar possesses lockdown capabilities, supporting operational lockdowns, USB device lockdowns, data lockdowns, and configuration lockdowns to ensure endpoint operational integrity. Simultaneously, it effectively reduces opportunities for downtime and costs.
		Portable Inspector employs cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas.
2.4	Mobile Code	Stellar's Trust List technology provides control systems to prevent unauthorized operations, such as restricting unauthorized programs from entering the control system and preventing the execution of VB Scrip and Powershell. In addition, the Permission Control feature can prevent unauthorized modifications. Meanwhile, StellarOne can monitor security events on endpoints.
2.5	Session Lock	EdgeIPS series comes equipped with a feature tailored to fit session lock requirements, ensuring seamless compatibility across SL1 to SL4. Our advanced access control list management aligns perfectly with the unique needs of both OT and ICS.

SR	Description	How TXOne Networks Supports Compliance
2.6	Remote Session Termination	Edge Network defense solution supports secure site-to-site VPN with remote access capabilities to secure OT networks from unauthorized access or interception. If access across different regional boundaries violates network security policies, the connection will be terminated.
2.7	Concurrent Session Control	Edge Network defense solution supports an editable network security policy feature, and restricts access to only legitimate devices, thereby preventing malicious connection behavior. With its dashboard, Edge Network defense solution enables easy monitoring of cases, receipt of notifications, and analysis of activities within the OT environment.
2.8	Auditable Events	EdgeOne can centrally manage the network defense provided by the Edge series nodes, and gives you comprehensive logs of activities including cybersecurity, policy enforcement, protocol filtering, system logs, audits, and asset detection at each EdgeIPS Family and EdgeFire Family node.
		Stellar can run on modern and legacy assets, and allows management from a single platform through StellarOne, strengthening both management of modern assets and defense of legacy equipment.
		ElementOne creates an inventory of OT asset information during routine scans, allowing verification of vulnerability status, OS (Operating System) updates, installed applications, and asset specifications.
2.9	Audit Storage Capacity	All products from TXOne Networks maintain sufficient storage capacity for audit log records, which can be exported in a standard format. Notably, the storage strategy and capacity are configurable.
2.10	Response to Audit Processing Failures	Stellar has the ability to uniquely identify each device and detect variations in their normal operation. Through deviation and behavioral analysis, it monitors unexpected changes and abnormal behavior in real-time. If anyone attempts to alter the default log configuration, Stellar will detect and respond to such actions.
		The EdgeIPS series is designed to send accurate alerts to personnel, thereby preventing any disruption of essential services or functionality during audit processing failures. Additionally, our EdgeIPS suite equips your team with the ability to adopt industry-leading actions in response to audits and handle failures in accordance with widely accepted practices and recommendations.
2.11	Timestamps	All products from TXOne Networks support system clock generated timestamps for audit records, and safeguards the time synchronization source from tampering.

FR3: System Integrity (SI)

IACS (Industrial Automation and Control Systems) often go through multiple testing cycles (unit tests, Factory Acceptance Tests (FAT), Site Acceptance Tests (SAT), certifications, debugging, etc.) to ensure that the system will perform as expected before initiating production. Once in operation, the asset owner has a responsibility to maintain the integrity of the IACS. Asset owners can use their risk assessment methods to allocate different levels of integrity protection for different systems, communication channels, and information within IACS.

The integrity of physical assets should be maintained in both operational and non-operational states, such as during production, storage periods, or maintenance downtime. The integrity of logical assets should be preserved during both transmission and at rest, such as when transmitted over the network or residing in data repositories.

Table 6. System Requirements for System Integrity

SR	Description	How TXOne Networks Supports Compliance
3.1	Communication Integrity	Edge Network defense solution supports multiple ICS protocols to secure OT network communication. Meanwhile, administrators are equipped with the ability to edit OT protocol allowlists to enable interactive interoperability between key production machine assets, as well as to deeply analyze L2-L7 networks by node group.
		Portable Inspector supports encrypted transmission, allowing ICS owners and operators to carry sensitive data in air-gapped environments, while maintaining the integrity of business operations. Even Windows XP or Windows 7 can be secured. Multiple platforms are securely protected with a single scanning tool.
3.2	Malicious Code Protection	Stellar offers OT native protection with its next-gen antivirus, application lockdown, and anomaly detection via a lightweight agent. It also includes an industrial application repository for operational baselines, anomaly detection, and real-time malware scanning to ensure operational integrity.
		Edge Network defense solution can protect an organization's network from the latest variants of malicious software, spyware, and other content-level threats, thereby reducing the risk of data leaks or damage resulting from malware infections. Meanwhile, use Edge series appliances to create special rules for traffic that allow assets to communicate on a strictly need-to-know basis in order to do their work, while highlighting all suspicious or potentially harmful activity.
		Portable Inspector provides a completely installation-free solution by loading scanning software onto a USB drive, enabling malware detection and removal without needing to reboot the target system.

SR	Description	How TXOne Networks Supports Compliance
3.3	Security Functionality Verification	All products of TXOne Networks support customers in conducting security functionality verification, such as antivirus software alerts, effectiveness of intrusion detection system rules, appropriate security monitoring and event handling, and log recording in accordance with security policies among other security tests.
3.4	Software and Information Integrity	Stellar can lock down sensitive assets, limit access, and preserve system resources with its simple and reliable Trust List technology. Once deployed, this solution allows only the execution of approved applications necessary to daily operations, preventing the spread and execution of malware without reliance on pattern files or other resources.
		Edge Network defense solution supports multiple ICS protocols to protect OT network communications. At the same time, administrators can edit OT protocol trust lists to achieve interactive interoperability between key production machine assets, and perform in-depth analysis of L2-L7 networks by node group. Meanwhile, administrators can use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity.
		Portable Inspector is equipped with an AES-256 hardware encryption engine. Data stored in encrypted form cannot be accessed without authorization.
3.5	Input Validation	Edge Network defense solution supports multiple ICS protocols to protect OT network communications. It also facilitates in-depth analysis of L2-L7 network packets by node group to prevent invalid inputs from causing system security issues, or unauthorized instructions, ensuring that network transmissions adhere to network security policy guidelines.
		Stellar ensures operational integrity through application lock-down to minimize downtime. It can check whether the input syntax of the control system complies with rules to verify that the information has not been tampered with and is in accordance with specifications. At the same time, Stellar also supports real-time malware scanning in maintenance mode to quickly identify threats.
		When Portable Inspector conducts a file transfer to secure storage, it automatically performs a security scan, and only validated files are permitted to be stored.
3.6	Deterministic Output	When a failover occurs on EdgeIPS, the port pairs can bypass the packets without impacting connectivity. Additionally, when a failover occurs on EdgeIPS Pro, the standby EdgeIPS Pro device will take over and become the active one.
3.7	Error Handling	The Edge Network defense solution offers robust capabilities to identify and address erroneous situations through effective remediation, all while ensuring security. Our solution is designed to satisfy requirements in a manner that doesn't expose information that could potentially be exploited by adversaries to attack IACS.

SR	Description	How TXOne Networks Supports Compliance
3.8	Session Integrity	The Edge Network defense solution is capable of safeguarding session integrity. It has the power to reject any usage of invalid session IDs, reinforcing the security of your digital interactions.
3.9	Protection of Audit Information	All products from TXOne Networks provide strict access control to safeguard audit information, preventing modification and deletion mechanisms.

FR4: Data Confidentiality (DC)

Certain information generated by some control systems holds a level of confidentiality or sensitivity, whether it's in storage or in transit. This means that certain communication channels and data storage require protection against eavesdropping and unauthorized access.

Table 7. System Requirements for Data Confidentiality

SR	Description	How TXOne Networks Supports Compliance
4.1	Information Confidentiality	Edge Network defense solution supports various technical means such as network segmentation or encryption to ensure information confidentiality, while making certain that it does not impact the performance of the OT/ICS systems.
		Define roles using trust list-based lockdown software Stellar to protect mission-critical systems data from disruption.
		Portable Inspector includes secure storage equipped with AES-256 encryption to completely safeguard all file transfers in your work site.
4.2	Information Persistence	Edge defense solution has the capability to thoroughly erase all explicitly read authorized information from components set for deactivation or decommissioning.
4.3	Use of Cryptography	When encryption is required, the Edge defense solution can employ encryption algorithms, key sizes, key creation and management mechanisms as needed, in line with widely accepted security industry practices and recommendations.
		Portable Inspector is a multipurpose secure transporter malware monitoring / inspection scanning and clean-up tool, for air-gapped systems and standalone PC's with 64GB of AES-256 encrypted storage for secure file transfer. It also provides greater OT visibility and insights into asset information.

FR5: Restricted Data Flow (RDF)

Segmenting the control system by zones and conduits helps to limit unnecessary data flow. Using their risk assessment method, asset owners need to determine their necessary information flow restrictions. Therefore, through the aforementioned risk assessment process, the settings for the zones and conduits providing this information are determined. The resulting normative recommendations and guidelines should include mechanisms to manage information flow restrictions, ranging from disconnecting the control system network from the business or public networks, to using unidirectional network gateways, stateful firewalls, and DMZs (Demilitarized Zones).

Table 8. System Requirements for Restricted Data Flow

SR	Description	How TXOne Networks Supports Compliance
5.1	Network Segmentation	Deploy EdgeIPS & EdgeFire to segment the network based on deep understanding of regulations, data sensitivity requirements, and work group productivity – this prevents attackers from moving within your network or accessing any sensitive devices.
5.2	Zone Boundary Protection	Edge Network defense solution can handily manage the group policies of networking and endpoint security assets, ensuring operational integrity across distant sites. It allows administrators to modify OT protocol allowlists for asset interoperability and to conduct deep L2-L7 network analysis.
5.3	General-Purpose Person to-Person Communication Restrictions	EdgeIPS & EdgeFire employs a variety of user-defined conditions to customize your own security rules, integrating common IT and ICS protocols with security rules to optimize protection for your OT network, whether that would be Modbus, SECS/GEMS, FTP, RDP, SMB, or others.
5.4	Application Partitioning	EdgeIPS & EdgeFire allows administrators to modify OT protocol allowlists for asset interoperability and to conduct deep L2-L7 network analysis to identify identical IP/MAC addresses, protocols, or port numbers. The organization's OT/ICS network is protected through customizable real-time threat detection.
		Stellar supports the principle of least privilege and Role-Based Access Control (RBAC), allowing different segmented endpoints to be used for different applications and services, such as operator workstations and engineer workstations.

FR6: Timely Response to Events (TRE)

The purpose of Timely Response to Events is to notify the cybersecurity forensic unit, collect and report all necessary evidence of violations, and take corrective measures in a timely manner to address security breaches. Asset owners should use risk assessment methods to develop security policies and procedures, as well as appropriate reporting and control processes required to respond to security violations. Derived explanatory recommendations and guidelines should include mechanisms for collecting, reporting, preserving, and automatically correlating forensic evidence to ensure prompt corrective actions. It is important to note that when organizations use monitoring tools and technologies, they should not negatively impact the operational efficiency and availability of control systems.

Table 9. System Requirements for Timely Response to Events

SR	Description	How TXOne Networks Supports Compliance
6.1	Audit Log Accessibility	Detailed scan logs and reports from TXOne solutions allow you to understand the target, nature, and potential impact of a threat. You can also determine the appropriate amount of time needed to retain logs.
6.2	Continuous Monitoring	StellarOne allows management from a single pane of glass with support for Syslog forwarding, indicators of compromise (IoC) integration, and centralized monitoring.
		EdgeOne manages the policies of networking and endpoint security assets, ensuring operational integrity across distant sites. It allows administrators to modify OT protocol allowlists for asset interoperability and to conduct deep network analysis. It organizes alerts, assets, and incident events, permitting direct monitoring of the enterprise's industrial control system security, in addition to providing insight into the shadow OT environment.
		ElementOne's collected asset information can be converted to the CSV format through the centralized management program as an asset inventory or sent to a SIEM or Rsyslog server for further asset management such as maintaining OT asset inventory or identifying impact levels, known vulnerabilities, and cyber risks.

FR7: Resource Availability (RA)

The purpose of resource availability is to ensure that these resources are readily available when they are needed to perform their intended functions. For instance, safeguarding the control systems against various types of DoS (Denial of Service) incidents. Resource availability also implies: 1) Ensuring the operational continuity of industrial processes by preventing downtime caused by cyberattacks. 2) Guaranteeing that system assets, networks, and services are resilient against cyberattacks. 3) Implementing backups, emergency power sourcing, and rapid recovery and rebuilding procedures to maintain continuous operation, even during a cyberattack or system failure. Particularly, security incidents within control systems should not impact the safety instrumented system (SIS) or other safety-related functions.

Table 10. System Requirements for Resource Availability

SR	Description	How TXOne Networks Supports Compliance
7.1	DoS Protection	EdgeIPS ensures uninterrupted service by defining thresholds for flood/scan attacks and blocking subsequent anomalous data packets once an attack is detected.
7.2	Resource Management	EdgeIPS & EdgeFire can support network segmentation technology and use pre-defined suspicious objects to identify malicious network behavior. Asset owners or service providers can maintain normal operation of production lines and avoid interference by tailoring their own OT/ICS security rules using a variety of user-defined conditions. Furthermore, control systems that cannot receive security updates can be protected and kept operational through the use of virtual patching.
		Stellar endpoint solution uses a system lockout feature to block unauthorized access and malware. It also provides endpoint monitoring and blocking features, such as blocking script execution and malware execution, to ensure system integrity without affecting the system's regular operation.
		Portable Inspector supports low-disruption malware scanning to avoid causing significant interference to normally operating assets.
7.3	Control System Backup	All TXOne Networks products inherently support configuration information backup without impacting normal factory operations. This ensures backups of important data and system status to handle unforeseen circumstances or needs for disaster recovery, all without causing interference of normal factory operations.
7.4	Control System Recovery and Reconstitution	All TXOne Networks products support the capability to restore control systems, such as the system's security status and measures for vulnerability remediation, to a pre-determined safe state, ensuring that the system continues to operate safely and reliably.
7.5	Emergency Power	EdgeIPS & EdgeFire are built with durable, industrial-grade components for harsh environments and temperatures. Meanwhile, their redundant power design is suitable for OT environments.

SR	Description	How TXOne Networks Supports Compliance
7.6	Network and Security Configuration Settings	EdgeIPS utilizes baseline auto-rule learning technology to automatically learn and seamlessly transform the organization's daily network traffic into powerful access policies, facilitating effortless network strategy deployment. This technology helps maintain strong control over the organization's OT/ICS network and enhances its network defense capabilities.
7.7	Least Privilege Functionality	EdgeIPS series supports the principle of least privilege, allowing businesses to minimize the OT attack surface, constrain OT network attacks, enhance operational performance, and mitigate the impact of human error. By implementing fine-grained access control at different levels, businesses can strike a balance between availability and security to safeguard critical data and systems.
		Stellar can operate without an internet connection, using policies designed around "least privilege" to thwart both known and unknown malware as well as fileless attacks.
7.8	Control System Component Inventory	Portable Inspector scans sensitive air-gapped or standalone assets that sometimes cannot accept installations or even light modifications, creating an inventory of them and ensuring they are threat-free while still adhering to their needs.
		EdgeIPS & EdgeFire support OT network visibility and look into assets from specific vendors and all network elements, assets, software, and devices as well as application traffic.

Conclusion

The ISA/IEC 62443 series of standards provides a framework for gradually implementing best practices for industrial cybersecurity and promoting continual improvement. This encompasses control systems used in manufacturing, processing plants, public utilities (i.e., electricity, natural gas, and water), as well as pipeline and oil production and distribution facilities. Additionally, the ISA/IEC 62443 series has gained recognition beyond its original scope, such as in building automation, medical systems, and other industries and applications. A key part of this is ISA/IEC 62443-3-3, which describes the security functions OT/ICS should implement. TXOne's OT zero trust solutions for simplifying compliance with the ISA/IEC 62443-3-3 effectively protect the endpoints and network systems of critical and essential entities' OT/ICS, ensuring operational availability, integrity, and confidentiality, while safeguarding entities from supply chain attacks.

a) Security Inspection: Portable Inspector uses a removable approach to provide effective malware scanning with independent computer and physical isolation. It can detect and remove malicious software by being inserted into the USB port of any Windows and Linux device without the need for software installation or rebooting the target system. In addition, Portable Inspector can collect asset information to generate an inventory list to increase IT/OT visibility and eliminate shadow IT/OT. With its use of an AES 256 hardware encryption engine and scanning of all files before storing data, it ensures that data is free from malware before being securely placed in storage.

b) Endpoint Protection: Stellar offers organizations an all-in-one OT solution for long-term endpoint security coverage, securing modernized assets with a library of ICS applications and certificates. For fixed-use and legacy systems, Stellar locks them down so that they can only conduct tasks related to their role, and StellarOne empowers smooth management throughout the asset lifecycle from a single pane of glass.

c) Network Defense: Edge series employs auto-rule learning technology to assist organizations in automatically generating a network trust list, and allows organizations to create and edit L2-L3 network policies strictly based on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. The Edge series also supports a wide range of industrial protocols and deeply analyzes network packets, enabling organizations to effectively block malicious behavior and errors without affecting production line operations. To protect legacy devices and production systems that are vulnerable to attack due to unpatched vulnerabilities, Edge series uses industry-leading signature-based virtual patching technology. In addition, Edge series minimizes the time required to configure and manage devices and can be easily deployed in an organization's existing OT environment.

The security framework and requirements provided by ISA/IEC 62443-3-3 may seem daunting. However, business leaders can establish a clear roadmap, creating an OT security improvement plan for relevant organizational team members. This begins with conducting a risk analysis to understand the difference between the organization's current status and the ISA/IEC 62443-3-3 standard, identifying weaknesses or non-compliant areas. This could involve revising processes, implementing new technologies, or conducting employee training. Ultimately, a phased approach allows for the execution of the compliance plan based on available resources, rather than attempting to achieve everything at once.

TXOne Networks possesses skilled OT/ICS cybersecurity professionals and technology, dedicated to maintaining the availability, stability, and security of critical infrastructure and manufacturing industries. This enables us to overcome network security challenges and ensure continuous operation. Our automation solutions can assist enterprises in effectively responding to the requirements of the ISA/IEC 62443-3-3 standard, and align with the organization's cybersecurity upgrade roadmap.

References

[1] IEC 62443," Industrial communication networks - Network and system security – Part 1-1: Terminology, concepts and models", International Electrotechnical Commission, July 2009.

[2] Maximillian Kon, "How to Define Zones and Conduits. How to Define Zones and Conduits", WisePlant, May, 2023.

[3] IEC 62443," Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels", International Electrotechnical Commission, August 2013.

Copyright © 2023 TXOne Networks. All rights reserved.

txone.com