ISA GLOBAL CYBERSECURITY ALLIANCE

June 2025

Securing Operational Technology: Understanding the ISA/IEC 62443 Series of Standards from an ISO/IEC 27001 and ISO/IEC 27002 Perspective

www.isagca.org

Sections

Table of Tables

Table of Figures

Foreword

This report was developed by the International Society of Automation Global Cybersecurity Alliance (ISAGCA). Further information about this organization can be found at www.isagca.org. This document is an interpretation of the ISA/IEC 62443 standards to facilitate understanding and application of the series of standards. It is not a product of the ISA99 committee that develops the standard, and as such may not represent the views of the committee.

1 Executive Summary

The purpose of this paper is to answer the questions – if you already have a security management system covering your IT operations based on ISO/IEC 27001 [27001] and ISO/IEC 27002 [27002], how can you use the ISA/IEC 62443 standard series [62443][1] to extend that security management system to also cover your OT (operational technology) operations? What aspects of this extension are likely to be unique for OT, and what aspects common with IT?

Requirement ORG 1.1 of ISA/IEC 62443-2-1 Edition 2 [62443-2-1] requires that if you already have an information security management system for IT (an ISMS), whether it is based on ISO/IEC 27001 / ISO/IEC 27002 [27001/2][2] or some other approach, you need to coordinate what you do for OT security management with that ISMS. This means in practice that controls that address common concerns of IT and OT, as well as those that meet unique OT requirements, together efficiently and effectively protect the overall enterprise. While not intended as a complete standards mapping, this paper includes partial mappings between [27001/2] and contents of [62443] toward answering these questions, and includes specific references to roughly half of the requirements in [62443-2-1].

The driving principle for [62443] is that protection of OT data and of the OT itself is addressed as a means to mitigate the physical risks associated with computer control of a physical process, rather than as an end in itself. Unique benefits from [62443] conformance for the security of OT environments are described in these areas: mitigating risks to health, safety and the environment, continuity of the physical process being controlled, disruption of control of a physical process as an "undesired effect" of security controls, zoning based on security requirements, rigorous system integrity controls and the linkage of risk to the selection of security controls.

The standards [27001/2] and [62443] also share a significant area of common concern, evidenced by requirements of [62443] that are seen to be either refinements of, or virtually identical to, [27001/2] security controls or recommendations. Therefore, [62443] not only offers unique benefits for OT environments, but also provides input to the prioritization process that guides the application of [27001/2] for these environments.

[1] When all documents of the ISA/IEC 62443 standard series are addressed, we will use the reference [62443]

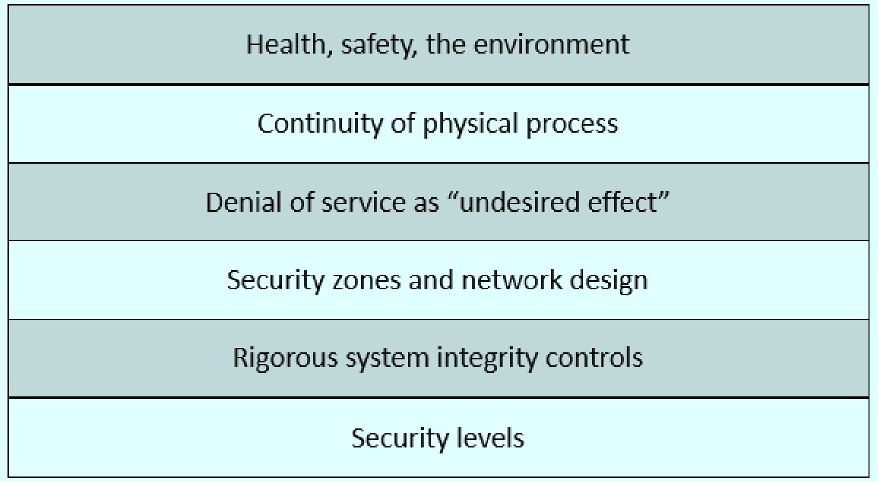
[2] When both documents [27001] and [27002] are addressed, we will use the reference [27001/2].

2 Critical contributions of the ISA/IEC 62443 standard series for OT security

Since OT manages a physical process, its operation may entail physical risks. Risk management for OT is focused on mitigating the physical risk associated with the physical process being managed, and related risks to life and the environment external to the OT system. The protection of OT data and of the OT itself are not ends in themselves, but rather a *means* to mitigate these physical risks. Risk management for OT is therefore not focused on adverse impacts to information technology. It is rather necessarily integrated with "non-cyber" enterprise risk management activities that manage physical risks. These risks are distinct from typical consequences of cyber attacks that affect IT systems such as loss of customer privacy or loss of business operations.

Because OT manages a physical process, the consequences if OT becomes unavailable or loses integrity extend beyond privacy, financial or business loss to include injury, loss of life and destruction of property and the environment. While confidentiality of data used by OT systems can be important, the consequences of loss of system availability or integrity are often far more severe. Further, the tolerable time period for unavailability before experiencing significant consequences may be several orders of magnitude shorter for OT systems than for IT systems.

These characteristics of the OT risk environment shape the requirements in [62443]. Figure 1 shows six critical areas for requirements that [62443] contributes to an operating facility that is already following [27001/2]. Requirements of [62443] in these areas either reference concepts that are unique to an OT environment (such as process operator or safety function) or describe an area for which the level of associated risk addressed by the requirements is significantly higher in an OT environment than for a typical enterprise IT environment. Text following Figure 1 briefly describes each of these areas.



Health, safety, the environment

Continuity of physical process

Denial of service as "undesired effect"

Security zones and network design

Rigorous system integrity controls

Security levels

Figure 1. Critical topics – contributions of the ISA/IEC 62443 standard series for OT security

1. **Health, safety, the environment.** [62443] identifies physical risks as risks to health, safety and the environment, and refers to these as "HSE." These risks may be realized if OT functionality is not designed with these risks in mind, is not operating as designed, or because it

is not operating at all. In other words, lack of design for security, loss of OT integrity or loss of OT availability creates HSE risks. Although integrity and availability of both data and systems are well recognized as standard aspects of cyber security, the potential severity of physical risks and unforgiving time frames for their realization drive more rigorous requirements on these topics in [62443] than may be necessary in a non-OT environment.

2. **Continuity of the physical process**. A physical process does not stop when its associated OT stops operating. Requirements of [62443] not only seek to minimize the amount of time for which the overall OT system is unavailable, but also require intentional design for what happens to the physical process being managed when normal OT functions become unavailable.

3. **Denial of service as "undesired effect."** Requirements of [62443] consider not only OT response to a denial-of-service condition caused by an adversary, but also how to avoid common circumstances that might unintentionally cause a denial of service due to the application of a security control, or in other words, caused by "friendly fire."

4. **Security zones and network design.** The risk assessment and system design process described in [62443-3-2] requires grouping of assets into security zones. Risks are considered per zone, and boundaries and connections of zones (called conduits) are protected. Network segmentation and related requirements offer a possible implementation of the security zone concept. [62443] also explicitly requires risk-based considerations for the design of network interconnections and dependencies.

5. **Rigorous system integrity controls.** [62443] requires capturing a detailed description of the system. To maintain "system integrity" means to maintain and comply with this description over time. Detailed system definition and strict compliance are feasible in OT environments due to the fact that OT systems are relatively stable over time. Such controls are required, because small changes in system behavior may entail significant risks in these environments. These same controls may not be feasible nor necessary in many IT environments, which interact with a broader set of users and can be more dynamic, as well as more forgiving of unexpected system behavior.

6. **Security levels.** All organizations with a security program face the decision, "How much security is enough?" The [62443-3-2] risk assessment process includes assigning a target security level to a security zone. All system and component technical requirements, including those addressing the other topics shown in Figure 1, are categorized by security level in [62443-3-3] and [62443-4-2], respectively. This provides a link between risk assessment outcome (target level) and procurement specification (capability level).

All of these topics ultimately trace back to the single characteristic that OT interacts with the physical world, and therefore its use entails physical risks. Sub sections 2.1 to 2.6 further describe how specific requirements of [62443] address each of these areas, and how these requirements are related to existing [27001/2] controls and guidance.

Many of these topics are expressed as individual requirements in [62443], for which there is not a direct analogue in the controls list in [27001/2]. In a few cases, ISA/IEC 62443 and [27001/2] both express the same general requirement, but a key OT-driven aspect of that requirement is found in [62443] that is not explicitly mentioned in ISO/IEC 27001 or in further guidance in ISO/IEC 27002.

In the remainder of Section 2, content formatted as in the example below provides an alphanumeric identifier, title and text for a requirement quoted from [62443]. Requirement text quoted from [62443] is shown in italic font, and a grey background is used.

> ISA/IEC 62443-2-1 **USER 1.3 User identity persistence**
>
> *The asset owner shall have policies and procedures to verify that IACS-specific user identifiers, authenticators, roles and their associated access rights that are used to support essential IACS operations, including operator accounts, are configured so they are not disabled automatically.*

2.1 Health, safety, the environment

2.1.1 Relationship to [27001/2]

A unique characteristic of operational technology is that it is responsible for a process in the physical world and creates the potential for cyber attacks that pose "physical" risks to health, safety and the environment. Health and safety consequences may affect employees and/or the public. Many organizations that employ [27001/2] do not have operational technology, nor these associated risks. For those organizations that do, such risks would be identified under the risk management requirements in clause 6.1.2 of ISO/IEC 27001, since they are "risks associated with the loss of confidentiality, integrity and availability for information," in particular for parameters that influence a physical process, and process status information. However, no [27001/2] controls explicitly call out physical risks from cyber attack.

2.1.2 Excerpts from the ISA/IEC 62443 standard series

Treatment of risks to health, safety and the environment in the context of cyber security is a major contribution of [62443]. In particular, [62443-2-1] includes unique requirements related to safety and safety functions.[3]

A related concept to safety function in ISA/IEC 62443 is essential function. A safety function is one type of essential function, per the following definition from [62443-4-2]:

> **Essential function**
> *Function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control.*

Three [62443-2-1] requirements quoted below, explicitly address either safety functions or essential functions. These requirements state, in summary, that operator access to safety or other essential functions cannot be removed automatically, that there is strict control over configuration of safety systems, and that non-safety systems do not interfere with safety systems. Below are these requirements (shown on grey background), preceded by a discussion of associated rationale and possible distinctions from non-OT environments.

The [62443-2-1] requirement USER 1.3 reflects the fact that in the OT environment, the risks of an operator not being able to interact with a safety system or other essential function, outweigh the efficiency and security benefits of automating revocation of access rights. In contrast, in many information technology environments, passwords might be automatically removed if not used for some time period, or upon job transfer, as an implementation of the [27001/2] control **5.18 Access rights**.

ISA/IEC 62443-2-1 **USER 1.3 User identity persistence**

The asset owner shall have policies and procedures to verify that IACS-specific user identifiers, authenticators, roles and their associated access rights that are used to support essential IACS operations, including operator accounts, are configured so they are not disabled automatically.

[3] Examples of safety functions are controllers that can open a relief valve when a sensor indicates high pressure; or a braking system designed to slow down a train if a speed threshold is exceeded.

DATA 1.3 provides for strict control of the configuration of safety systems, since this data is highly critical and rarely needs to change. In many information technology environments, system reconfiguration may be a common occurrence. General recommendations in ISO/IEC 27002 do call for planning and assessing the potential impact of changes, and including emergency considerations such as fallback procedures, under **8.32 Change management**.

ISA/IEC 62443-2-1 **DATA 1.3 Safety system configuration mode**

If safety systems are authorized for use in the IACS, the asset owner shall have policies and procedures related to:
a) updating the safety system configuration only when configuration mode is enabled, and
b) only enabling configuration mode when configuration changes are necessary.

The purpose of NET 1.3 is to prevent interference from other devices or networks with the operations of the safety system, ensuring that the safety system can perform its functions effectively and within the required timeframe. In many IT environments, traffic incoming from other networks often may delay internal traffic on a network, and brief interruptions may be considered acceptable. Guidance related to the general 27002 control **8.22 Segregation of networks** states that criticality of function may be a reason for segregating particular networks.

ISA/IEC 62443-2-1 **NET 1.3 Network segmentation from safety systems**

If the IACS contains a safety system network, the asset owner shall have policies and procedures related to protecting the safety system from interference by non-safety system networks and their devices.

2.2 Continuity of the physical process

2.2.1 Relationship to [27001/2]

The [27001/2] control **5.30 ICT readiness for business continuity** addresses ensuring the availability of all organization information and related assets under disruption, including cyber attack. For an organization with OT, a business impact analysis for a cyber-attack scenario would include not only the disruption of business processes, but also the disruption of physical processes controlled by OT.

The 27002 guidance for control **5.24 Information security incident management planning and preparation** recommends defining and implementing the *"organization's priorities for handling information security incidents including resolution timeframe based on potential consequences and severity."*

2.2.2 Excerpts from the ISA/IEC 62443 standard series

Related to these practices in [27001/2], ISA/IEC 62443 requires policies and procedures to address disruption of normal IACS control of the physical process and calls out the potential need for immediate response to some IACS cyber attacks.

In particular, requirement [62443-2-1] AVAIL 1.3 quoted below addresses designing and planning for consequences of unplanned disruption of physical processes due to cyber-attack. It requires that if normal operation cannot be maintained due to cyber-attack, then the OT equipment can be placed in a predetermined state. This allows the organization to plan for the state of the control system while under attack, and avoid equipment/facility damage if possible. Loss of production capability can be minimized. Any unavoidable impacts to health, safety or the environment that occur as a result of transition to the predetermined state can be identified in advance, and mitigations planned.

> ISA/IEC 62443-2-1 **AVAIL 1.3 Failure-state**
>
> *The asset owner shall have policies and procedures related to bringing the IACS to a predetermined state if normal operation cannot be maintained as a result of a detected security compromise.*

Because impact on the physical process due to unavailability of the Automation Solution may occur very quickly, [62443-2-1] explicitly calls out consideration of events that need immediate detection and response, as stated in the requirement EVENT 1.1.

> ISA/IEC 62443-2-1 **EVENT 1.1 Event detection**
>
> *The asset owner shall have policies and procedures related to the reporting, logging, analysis and response (immediate or delayed) of IACS security-related events that are detected to support security management activities.*

2.3 Denial of service as “undesired effect”

2.3.1 Relationship to [27001/2]

Sub clause 6.1.1 of ISO/IEC 27001 requires that planning for the information security management system includes addressing risks to “prevent, or reduce, undesired effects” of implementing that system. Thus, it is required that an organization identifies and manages the risk of undesirable side effects of the implementation of security controls.

2.3.2 Excerpts from the ISA/IEC 62443 standard series

In particular, a number of common cyber security controls may themselves adversely affect system availability. The preceding discussion of physical risks pointed out that in the OT environment, there may be severe consequences if the system is unavailable and therefore users are unable to take required actions to manage the physical process. Severe consequences of OT unavailability may occur very quickly, whereas in many IT environments, short periods of "downtime" may be undesirable, but have less severe consequences.

For this reason, the following [62443-2-1] requirements address specific situations in which security mechanisms are designed to avoid creating denial of service conditions.

In requirement [62443-2-1] USER 1.8 quoted below, [62443-2-1] does not require automatic screen locking if failure to access the screen can result in a greater risk to the IACS than access to an unattended screen would. 27002 guidance for control **7.7 Clear desk and clear screen**, part c recommends that all computers and systems should be configured with a timeout or automatic logout feature.

ISA/IEC 62443-2-1 **USER 1.18 Screen lock**

The asset owner shall have policies and procedures related to locking user screens … unless failure to access the screen can result in a greater risk to the IACS…

Under requirements [62443-2-1] NET 1.5 and NET 1.5, the IACS is designed to operate when disconnected from external networks, since disconnection is a common attack response (as described in [27002] guidance for control **8.20 Networks security**, part m).

ISA/IEC 62443-2-1 **NET 1.4 Network autonomy**

The asset owner shall have policies and procedures around the ability to operate the IACS as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).

ISA/IEC 62443-2-1 **NET 1.5 Network disconnection from external networks**

The asset owner shall have policies and procedures around the ability to disconnect the IACS from external networks to protect itself or the external networks from actual or suspected threats.

[62443-2-1] COMP 2.3 quoted next addresses the issue that malware protection has been found to introduce performance or availability issues for Automation Solution components, that interfere with process control or other system functions. Therefore, [62443-2-1] requires that an organization ensure that such software as well as malware definition files are tested for compatibility with Automation Solution devices and systems. For many IT systems covered by [27001/2], the *supplier* of malware protection software will typically run such tests on common platforms. Hence this would not typically fall as a testing requirement for the *owners* of such IT assets. However, providers of malware protection software would rarely have facilities to perform compatibility testing for Automation Solution products. [27002] guidance for control **8.7 Protection against malware** does note under "other information" that "It is not always possible to install software that protects against malware on some systems (*e.g.,* some industrial control systems)."

ISA/IEC 62443-2-1 **COMP 2.3 Malware protection software validation and installation**

The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of malware protection software and any related malware signature files in a timely manner after their release.

Backup processes themselves may also have unintended effects on IACS operations, as reflected in the following requirement.

ISA/IEC 62443-2-1 **AVAIL 2.2 Backup non-interference**

The asset owner shall have policies and procedures validating that backup processes do not adversely affect normal operations of the IACS.

The requirement [62443-2-1] **USER 1.3 User identity persistence** quoted previously in Section 2.1.2 is an additional example of a requirement on user authentication, to avoid a denial-of-service condition for access to essential functions due to automatic removal of user access rights.

2.4 Security zones and network design

2.4.1 Relationship to [27001/2]

The [27001/2] Control **8.22 Segregation of networks** reads "Groups of information services, users, and information systems should be segregated in the organization's networks." Further guidance includes "…[network] domains can be chosen based on levels of trust, criticality and sensitivity (*e.g.,* public access domain, desktop domain, server domain, low and high-risk systems), along organizational units…"

2.4.2 Excerpts from the ISA/IEC 62443 standard series

The more general principle of partitioning assets into security zones is central in [62443]. The concept of zones in [62443] does not necessarily entail use of a specific technique such as network segregation. The standard requires partitioning techniques that support protection between zones (partitions). Other possible techniques are the use of virtualized hardware or containerization of applications.

Specifically, [62443-2-1] requires zone partitioning as in the two requirements following.

ISA/IEC 62443-2-1 **NET 1.1 Segmentation from non-IACS zones**

The asset owner shall have policies and procedures segmenting IACS from non-IACS zones and limiting any interconnections to the minimum necessary for IACS operations and within tolerable risk.

ISA/IEC 62443-2-1 **NET 1.2 Documentation of zones and network zone interconnections**

The asset owner shall have policies and procedures for documenting and maintaining a baseline of all IACS zones and network zone interconnections and/or conduits, the security risks associated with each, and their designation as trusted or untrusted.

[62443-3-3] in requirement SR 5.2 requires protections for zone boundaries (regardless of how zones are implemented).

ISA/IEC 62443-3-3 **SR 5.2 Zone boundary protection**

The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

Further specifications regarding zoning is provided in [62443-3-2], which requires partitioning of IACS assets from other enterprise or business assets, and safety assets from other assets, in requirements ZCR 3.1 to ZCR 3.3 quoted below.

ISA/IEC 62443-3-2 **ZCR 3.1 Establish zones and conduits**

The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.

ISA/IEC 62443-3-2 **ZCR 3.2 Separate business and IACS assets**

IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets.

ISA/IEC 62443-3-2 **ZCR 3.3 Separate safety related assets**

Safety related IACS assets shall be grouped into zones that are logically or physically separated from zones with non-safety related IACS assets. However, if they cannot be separated, the entire zone shall be identified as a safety related zone.

In addition to these requirements for zoning, [62443-2-1] also includes specific requirements on the topic of network segmentation.

[62443-2-1] requirements on network segmentation say in summary, that safety networks are protected from interference (NET 1.3, previously quoted above in Section 2.1.2 under the topic of safety) and that the IACS can be disconnected from all external networks and must be able to operate as designed in this situation (NET 1.4, NET 1.5, previously quoted in Section 2.3 under the topic of denial of service). Further, risks of connection between internal IACS network segments are identified, documented, and managed (NET 1.6).

ISA/IEC 62443-2-1 **NET 1.3 Network segmentation from safety systems**

If the IACS contains a safety system network, the asset owner shall have policies and procedures related to protecting the safety system from interference by non-safety system networks and their devices.

ISA/IEC 62443-2-1 **NET 1.4 Network autonomy**

The asset owner shall have policies and procedures around the ability to operate the IACS as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).

ISA/IEC 62443-2-1 **NET 1.5 Network disconnection from external networks**

The asset owner shall have policies and procedures around the ability to disconnect the IACS from external networks to protect itself or the external networks from actual or suspected threats.

ISA/IEC 62443-2-1 **NET 1.6 Internal network access control**

The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing security risks associated with communications between internal IACS network segments, including determining a tolerable risk level and responding to risks outside that tolerable risk level.

2.5 Rigorous system integrity controls.

2.5.1 Relationship to [27001/2]

[27001/2] control **5.9 Inventory of information and other associated assets** requires maintaining an inventory of assets. [27002] guidance includes: “The granularity of the inventory of information and other associated assets should be at a level appropriate for the needs of the organization.” Further, requirement **8.9 Configuration management** states “Configurations, including security configurations, of hardware, software, services, and networks should be established, documented, implemented, monitored and reviewed."

2.5.2 Excerpts from the ISA/IEC 62443 standard series

[62443-2-1] includes detailed requirements regarding asset inventory and configuration management. Just as the loss of system *availability* can have severe consequences, loss of OT system *integrity* also may affect health, safety and the environment. The components of a Automation Solution in production cannot deviate from those tested and ultimately approved due to the potential for severe consequences. This concern drives [62443-2-1] requirements for maintaining documentation to identify and describe current system components, as well as their network connections.

The [62443-2-1] standard specifies in CM 1.1 that the asset inventory includes devices, hardware components, software components and all communications protocols/ports used.

ISA/IEC 62443-2-1 **CM 1.1 Asset inventory baseline**

The asset owner shall have policies and procedures to document, verify and maintain, throughout the full life cycle of the IACS, the inventory baseline of all devices, hardware components, software components, communications protocols and open communications ports used in the IACS including but not limited to:

a) organizational responsibilities,
b) manufacturer,
c) model,
d) version numbers,
e) serial numbers,
f) network interfaces,
g) communication addresses,
h) revision/patch levels, and
i) *history.*

[62443-2-1] also specifies in CM 1.1 and in the requirements quoted below, particular data fields required for asset inventory documentation, which defines a minimal level of granularity appropriate for the OT environment. Example data fields specified by [62443-2-1] requirements CM 1.1 and CM 1.2 are: manufacturer, model number, serial number, version number, revision/patch level, history, and physical and logical connectivity of all Automation Solution devices and software components. CM 1.3 requires documentation and verification of configuration settings.

ISA/IEC 62443-2-1 **CM 1.2 Infrastructure drawings/documentation**

The asset owner shall have policies and procedures to verify and maintain the current baseline of drawings/documentation showing the physical and logical connectivity of all IACS devices and software components.

ISA/IEC 62443-2-1 **CM 1.3 Configuration settings**

The asset owner shall have policies and procedures to document the configuration settings of all IACS devices and software applications and to verify their operational compliance with the documented configuration.

[62443-2-1] CM 1.4 further requires that changes to this asset inventory data be authorized, validated and approved.

ISA/IEC 62443-2-1 **CM 1.4 Change control**

The asset owner shall have policies and procedures to authorize, validate and approve changes to the current configuration baseline and infrastructure drawings/documentation, including revision and patch levels.

[62443-2-1] also requires tracking remote access connections in NET 3.2 quoted below. In the IACS environment it is a frequent occurrence for IACS equipment suppliers to require remote access for troubleshooting, repairs or upgrades to their equipment. These scenarios may not be pre-planned, may be short-term, and require specific limited privileges on the IACS, which may be different in each scenario. Careful management is critical to the security of the Automation Solution. General IT assets and their connections may be more dynamic than IACS, making asset and connection tracking at the level of granularity required in [62443-2-1] less feasible in an IT environment than for an OT environment, even with significant automation.

ISA/IEC 62443-2-1 **NET 3.2 Remote access connections**

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around authorizing, authenticating, encrypting, documenting, logging and monitoring all interactive remote access connections. Documentation for each connection shall include, but not be limited to:

a) its purpose,
b) the remote access application to be used,
c) encryption and authentication technologies used,
d) how the connection will be established (for example, via the Internet through a virtual private network (VPN) through a DMZ) with instructions, as necessary,
e) the circumstances requiring the connection,
f) the length of time the connection needs to be open, including expected inactivity periods,
g) the location and identity of the remote client device, application and user, and
h) any compliance requirements that need to be met prior to establishing the connection

Although asset tracking is not the main focus of the following [62443-2-1] requirement, the requirement implies careful tracking of assets:

The 27002 guidance for control **8.8 Management of technical vulnerabilities** identifies under "Taking appropriate measures to address technical vulnerabilities": " ...if no update is available or the update cannot be installed, considering other controls…" [62443-2-1] COMP 3.5 quoted below expands requirements for this scenario, stating that in any cases where a patch is not installed, it is required that the associated risk be addressed and the resolution for that risk be documented. This is essentially a requirement to track certain types of system changes *not made*, in addition to the requirement for tracking of changes made.

ISA/IEC 62443-2-1 **COMP 3.5 Security patch mitigation**

The asset owner shall have policies and procedures related to assessing the risk of not installing any applicable security patches, and if the risk is not tolerable, addressing the risk and documenting the resolution.

2.6 Security levels

2.6.1 Relationship to [27001/2]

Most explicitly in 6.1.2 and 6.1.3, 27001 requires that decisions about security controls are to be "risk-based." Likewise, [62443], and many other cyber security standards, use this approach. A challenge for any risk-based approach is, how is one to translate a level of risk to a selection of a specific implementation of a control? Many security controls may be implemented in differing "strengths." Perhaps the most common example is single-factor vs. multi-factor authentication. Risk is typically given a numerical or qualitative ranking assigned by an organization (such as a number between 1 and 5, or high, medium, low). So, what level of risk justifies multi-factor authentication?

2.6.2 Excerpts from the ISA/IEC 62443 standard series

[62443] helps with the translation of risk to control selection, using the concept of security level. There are four levels. These levels represent one factor used in determining risk, which is the type of adversary against whom a security zone is to be protected. The lowest security level requires protection against unintentional errors by benign individuals. The highest security level requires protection against a highly skilled and motivated attacker. The [62443-3-2] risk assessment process includes assigning a target security level to a security zone. Other parts of [62443] enumerate capabilities for components and systems and categorize these by security level. Each level includes the requirements for all lower levels.

As an example, [62443-3-3] SR 1.1 quoted below requires that for the highest security level of 4, multi-factor authentication is available for all human users. At security level 3, multi-factor authentication is available for all human users that access the system via untrusted networks. At security levels 1 or 2, multifactor authentication is not required. This categorization by security level is not an automated algorithm for selecting controls, but offers a starting point for making those decisions.

ISA/IEC 62443-3-3 **SR 1.1 – Human user identification and authentication**
Base requirement, Security Level 1

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

SR 1.1 Requirement enhancement 1
Unique identification and authentication, Security Level 2

The control system shall provide the capability to uniquely identify and authenticate all human users.

SR 1.1 Requirement enhancement 2
Multifactor authentication for untrusted networks, Security Level 3

The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network.

SR 1.1 Requirement enhancement 3
Multifactor authentication for all networks, Security Level 4

The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.

Likewise, all requirements for components and systems in [62443-4-2] and [62443-3-3] have an associated security capability level.

The Section 2 discussion has addressed the question – what are the key differences in OT cyber security requirements for asset owners found in ISA/IEC 62443, from those found in [27001/2]? The next two sections focus on common security areas addressed by these standards.

2.7 OT Purpose

The white paper "Applying ISO/IEC 27001 / ISO/IEC 27002 and the ISA/IEC 62443 standard series for Operational Technology Environments" [OTE] provides an overview of how [27001/2] and [62443] of standards may be used together as complementary standards by organizations responsible for securing operational technology (OT) environments. Each of these standards provides unique contributions to a security program for OT environments. The present paper describes in further detail the unique value provided by [62443] for an OT environment, for an audience that has already implemented or is familiar with [27001/2]. The purpose here is to answer the questions – if you already have an [27001/2] security management system covering your IT operations, how can you use the ISA/IEC 62443 series to extend that security management system to also cover your OT (operational technology) operations? What aspects of this extension are likely to be unique for OT, and what aspects common with IT?

The international standards organization IEC has recognized and structured the development of standards for IT and OT as two related but distinct efforts. Quoting from the IEC website: *"Cyber security is often associated with IT and often led by IT with a focus to protect data flow in the virtual world. However, critical infrastructure and the automated environment in factories, or refineries, have security requirements that are part of the real world. They rely on operational technologies (OT) to ensure the correct execution of automated actions such as shutting down a valve to avoid the overflow of chemicals or bringing a generator online to avoid a blackout…The ISO/IEC Joint Technical Committee (JTC 1) develops the ISO/IEC 27000 family of standards for information technology (IT) systems. IEC Technical Committee 65 (TC 65) publishes IEC 62443 for operational technology found in industrial and critical infrastructure, including but not restricted to power utilities, water management systems, healthcare and transport systems."*

The primary intent of this paper is to offer detailed technical insight into the relationship between these two standards for decision-makers considering the adoption of [62443] in addition to [27001/2] for their OT environment. For organizations that have made the decision to adopt both standards, the paper identifies major topics unique to [62443] for the OT environment, and related rationale. Further, the discussion of topics common to both standards identifies areas where an organization will benefit by considering desired IT/OT coordination, as well as any necessary differences between IT and OT implementations of security controls to meet the requirements.

2.8 Scope

2.8.1 Scope of discussion

[27001/2] applies to an organization of any kind, and to its own information technology used to conduct its own business. The focus of this analysis is those parts of [62443] that contain requirements to be met by entities responsible for an IACS (industrial automation and control system) in operation, a role analogous to that of the audience for [27001/2]. In [62443] these organizations are called asset owners.

Note: In [62443], an asset owner is distinguished from a *product supplier*, which is responsible for developing an IACS product to be used by another entity. That entity then becomes an asset owner, using the product supplier's IACS product. A different part of [62443], ISA/IEC 62443-4-1 [62443-4-1], applies to product suppliers and covers the topic of how to develop a secure control system product. Thus, an organization that develops control system products might apply [27001/2] to its own internal IT, and may apply [62443-2-1] to its own manufacturing facility. However, neither of these addresses the process for developing a secure control system product, which is a separate topic covered by [62443-4-1].

The parts of [62443] that apply to asset owners and references are

- ISA/IEC 62443-2-1 [62443-2-1],
- ISA/IEC 62443-3-2 [62443-3-2] and
- ISA/IEC 62443-3-3 [62443-3-3].

Section 3 below further describes the use of roles in the overall structure for [62443]. This paper includes partial mappings between [27001/2] and contents of [62443], toward answering the questions posed earlier, and includes specific references to roughly half of the requirements in [62443-2-1]. The paper points out specific differences between IT and OT environments to describe the benefits of these specific requirements of [62443].

The intent for the present paper is that the scope of content in the two standards selected for discussion conveys the nature and value of key unique contributions of [62443], as well as the extent of similarities between the two standards.

2.8.2 Related Topics

The following related topics are outside the scope of the present paper. However, they would also be of interest for organizations considering application of both [27001/2] and [62443]. Further benefits accrue from applying the other parts of [62443] in conjunction with [62443-2-1], [62443-3-2] and [62443-3-3]. The other parts of the standard apply to entities other than the asset owner, which fill critical roles supporting the asset owner in achieving OT security. These roles include hardware/software developers ([62443-4-1]), integrators and maintenance service providers ([62443-2-4]), as further described in Section 3.

There is unique value from applying [27001/2] where [62443] has already been applied, which is the reverse topic to that considered here. [62443] itself requires under the [62443-2-1] requirement labelled ORG 1.1 Information security management system (ISMS), that management processes required by an ISMS, be either coordinated with, or a part of, an IACS security program. This requirement could be met by using an ISMS conformant to [27001/2]. Accordingly, the paper [OTE] referenced above recommends using both standards for the OT environment and provides examples of unique contributions for each. Examples of topics addressed in [27001/2] that are not explicitly enumerated in [62443-2-1] but fall under the requirement ORG 1.1, are leadership and commitment, internal audit and cyber security terms in employment agreements.

A useful resource focused on framing and detailing the differences between IT and OT environments is section 2.3 of NIST 800-82 Rev.3 [NIST 800-82].

2.8.3 OT and IACS

"Operational Technology (OT)" is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events [Gartner-ITG].

The reader will note that [62443] does not use the term "OT," but uses the term "Automation Solution," which is defined in turn as the hardware and software elements of an IACS. IACS is the stated scope of application for [62443] of standards. Nevertheless ISA/IEC 62443 has been accepted and applied in non-industrial areas that involve managing physical processes such as medical devices and building automation. This paper acknowledges the broader application of [62443] and uses the more general term "OT," except when directly quoting [62443].

Continuing the quote from the IEC website presented in Section 2.7: "The IEC Technical Committee 65 (TC 65) publishes IEC 62443 for operational technology found in industrial and critical infrastructure, including but not restricted to power utilities, water management systems, healthcare, and transport systems. These horizontal standards, also known as base standards, are technology independent. They can be applied across many technical areas."

2.8.4 Overview of analysis

The analysis portion of this paper is found in Sections 2, 4 and 5 as shown in Figure 2. Section 3 provides background information on the structure of [62443], and followed by a summary of conclusions.

Section 2 *Critical contributions of the ISA/IEC 62443 standard series for OT* security describes critical security areas that uniquely benefit OT security programs, the requirements of [62443] for these areas, and the unique characteristics of OT environments that drive these requirements.

Section 4 *Refinements of common concerns* describes requirements of [62443] that could be viewed as refinements to recommendations found in [27002]. These recommendations are further guidance provided for the implementation of controls listed in the Annex to [27001]. This guidance is not mandatory for compliance under 27001, since it has the status of recommendations and not of requirements (per the definitions in Section 4 of this report). However, specific *instances* of these 27002 recommendations do have the status of requirements in [62443].

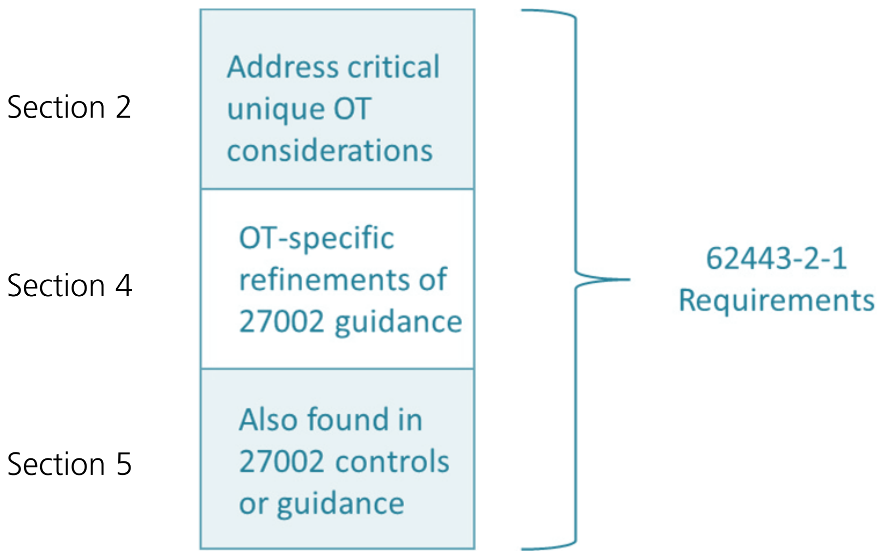

Section 2
Address critical unique OT considerations
Section 4
OT-specific refinements of 27002 guidance
Section 5
Also found in 27002 controls or guidance
62443-2-1 Requirements

Figure 2. Categories of ISA/IEC 62443-2-1 requirements described in this document

Section 5 *IT/OT* common practices identifies topic areas for which the two standards contain largely identical content. In some cases, the use of a control identified in [27001/2] is required by [62443]. In other cases, adherence to a recommendation found in ISO/IEC 27002 guidance, is required by [62443].

Therefore, for the topic areas discussed in Sections 4 and 5, [62443] provides insight on how to prioritize controls and recommendations in [27001/2] for an OT security program.

3 Structure of the ISA/IEC 62443 standard series

According to the definition in Section 7.1, an IACS includes a technical solution – the Automation Solution – as well as the people and policies involved in the operation of the technical solution.
A unique contribution of [62443], derives from its structure, which is designed from the perspective of users of the standard. The standard consists of a number of parts, each of which addresses a different actor and distinct phases of the lifecycle of an IACS. It is well understood that the most securely designed Automation Solution can become insecure in operation due to inadequate integration, operation, and maintenance practices. [62443] explicitly partitions the roles and responsibilities of the principal actors for cyber security:

- product suppliers, addressing development process, component security capabilities, and system security capabilities ([62443-4-1], [62443-4-2], [62443-3-3])
- service providers, including integrators and maintenance service providers, addressing system design and maintenance ([62443-2-4], [62443-3-2], [62443-3-3])
- asset owners, addressing secure operation ([62443-2-1]).

Due to this organization of the standard, actors that have a role to play in IACS security may easily identify the requirements for which they are responsible. The requirements in the various parts of the standard are mutually supportive and efficient across the full spectrum of actors and lifecycle phases that can impact IACS security. For example, an OT asset owner that employs procurement requirements based on [62443-3-3], is assured that the system they purchase will have sufficient technical system capabilities for them to carry out a secure operation in compliance with [62443-2-1]. Likewise, a system integrator designing a system in accordance with [62443-3-3] is assured that such compliance is feasible if they select components for that system that comply with [62443-4-2].

Figure 3 shows the duties of the principal actors for the IACS security and the most relevant parts of [62443] for them. See Section 8 for full reference listings for these parts of [62443].

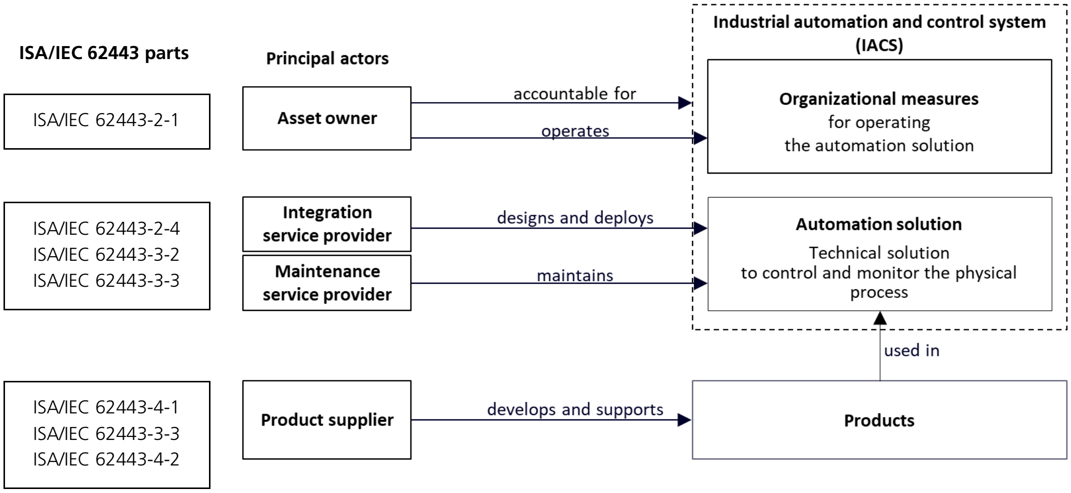


Figure 3. Duties of the principal actors in the ISA/IEC 62443 standard series

4 Refinements of common concerns

For some controls, [27002] guidance calls for an organization to "consider" implementation of the control for some situations. For some of these controls, [62443-2-1] includes a requirement that specifies conditions under which the control is to be applied for OT. Such requirements could be viewed as refinements of ISO/IEC 27002 guidance that consider the risk typically inherent under these conditions in the OT environment.

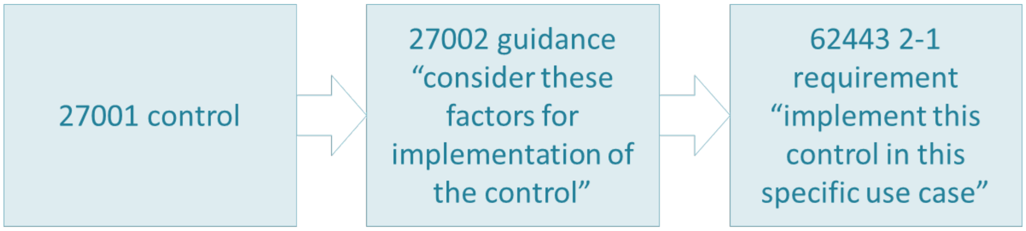

27001 control
27002 guidance "consider these factors for implementation of the control"
62443 2-1 requirement "implement this control in this specific use case"

Figure 4. Refined ISO/IEC 27002 recommendations that are requirements of the ISA/IEC 62443 standard series

Table 1 shows examples of [62443-2-1] requirements that specify particular cases for application of guidance found in [27002]. As an example from the table, in guidance related to control **5.14 Information transfer**, [27002] advises consideration of restrictions on electronic communication facilities. In [62443-2-1], requirement NET 1.8 states specifically that policies and procedures should address payloads allowed on user-to-user messages on IACS networks.

Table 1. Example ISA/IEC 62443-2-1 requirements that refine ISO/IEC 27002 guidance

ISO/IEC 27001 control ID	**ISO/IEC 27002 guidance reference**	**ISO/IEC 27002 guidance – summary**	**ISA/IEC 62443-2-1 requirement ID and name**	**ISA/IEC 62443-2-1 requirement – summary**
5.14 Information transfer	Electronic transfer Parts a), d), f)	Consider malware protection and restrictions on electronic communication facilities.	NET 1.8 User messaging	For user-to-user messages on IACS networks, policies and procedures address restrictions for messages containing potentially malicious payloads such as attachments, network links, and scripts.
6.1 Screening	Third to last paragraph	Procedures should define how, when and why to carry out ongoing screening of personnel after they initially join the organization.	ORG 1.2 Background checks	Policies and procedures address screening personnel before granting access to the IACS.
6.7 Remote working	Part k) (first list)	Consider vulnerability of single-factor authentication for remote access.	USER 1.9 Multifactor authentication (MFA)	Policies and procedures address multi-factor authentication for IACS devices supporting human login for remote access or where device is in public access area.
6.7 Remote working	Part d) (second list)	Among guidelines/arrangements for remote working, consider inactivity timers.	NET 3.3 Remote access termination	Policies and procedures address terminating interactive remote access connections after configured inactivity period.

ISO/IEC 27001 control ID	ISO/IEC 27002 guidance reference	ISO/IEC 27002 guidance – summary	ISA/IEC 62443-2-1 requirement ID and name	ISA/IEC 62443-2-1 requirement – summary
8.26 Application security requirements	Part k)	Consider if application has requirements for automated controls (e.g., approval limits or dual approvals).	USER 2.3 Multiple approvals	Policies and procedures address approval by two or more users for actions that can result in serious impact to the industrial process, unless failure to perform the action can result in a greater impact to the industrial process.

5 IT/OT common practices

A number of requirements in [62443-2-1] in effect require either implementation of [27001/2] controls, or adherence to recommendations found in ISO/IEC 27002 guidance regarding those controls. Application of such a [27001/2] control would therefore imply conformance to the related [62443-2-1] requirement. These requirements of [62443] comprise a significant area of common concern for both IT and OT environments. They cover topics such as classification of information by security protections needed, verifying authenticity and integrity of software to be installed, access control using least privilege principles, vulnerability management, security event management, incident management and secure disposal of equipment. Practices under these topics have a very similar expression in both standards.

Table 2 provides examples mapping these IT/OT common practices as they appear in [27001/2] and [62443-2-1].

Importantly, although the expression of a recommendation or requirement may be the same in the two standards, the actions taken to comply with that recommendation or requirement are often not the same in the IT and OT environments. The authors of the standards elected to leave the next level of refinement to the judgment of the organization implementing the standard. For example, [27001/2] and [62443] both discuss authentication of human users, but neither mandates use of multi-factor authentication. Even though the same type of equipment may be used in both an IT and OT context, the decision of whether or not to use multi-factor authentication for access to that equipment may be different, due to differences in the risk environment related to that equipment. As a second example, cybersecurity awareness training is a control in [27001/2] and a requirement in [62443-2-1] for all who interact with the OT system. However, there may be differences in awareness training for personnel that interact with the OT system, just as there may be differences in such training for those that interact with HR information systems and with accounting systems. In addition to general awareness training, [62443-2-1] has an additional requirement for training relevant to assigned OT cyber security responsibility.

For compliance with ISO/IEC 27001 as required by sub clause 6.1.3 of that standard, an organization is not required to implement all [27001/2] controls, but is required to consider the applicability of the [27001/2] controls to their organization. In that decision process, they would have typically consulted the related guidance in [27002] to understand considerations for implementing the control. The organization would also have documented their decisions on applicability of these controls in a statement of applicability, that comprises "*…the necessary controls; … justification for their inclusion; … whether the necessary controls are implemented or not; and … the justification for excluding any of the controls*."

The fact that the requirements shown in the following table appear in [62443-2-1], provides a strong justification for *inclusion* of the associated [27001/2] control in the statement of pplicability for an organization that has an OT infrastructure within the scope of their information security management system being managed under ISO/IEC 27001.

Table 2. Example controls and guidance in ISO/IEC 27002 that are ISA/IEC 62443-2-1 requirements

ISO/IEC 27001 Control ID and name	ISO/IEC 27002 Control or Guidance excerpt	ISA/IEC 62443-2-1 Requirement ID and name	ISA/IEC 62443-2-1 Requirement text - excerpt
6.3 Information security awareness, education and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training … (Control)	ORG 1.4 Security awareness training	The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cyber security awareness training that is updated on a regular basis.
8.9 Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed. (Control)	CM 1.3 Configuration settings	The asset owner shall have policies and procedures to document the configuration settings of all IACS devices and software applications and to verify their operational compliance with the documented configuration.
8.7 Protection against malware	…scanning any data received over networks or via any form of electronic storage media, for malware before use… (Guidance part f)1))	COMP 2.1 Malware free	The asset owner shall have policies and procedures to verify that all components and portable media (if portable media is authorized for use in the IACS) are free of known malware before being used in the IACS.

ISO/IEC 27001 Control ID and name	ISO/IEC 27002 Control or Guidance excerpt	ISA/IEC 62443-2-1 Requirement ID and name	ISA/IEC 62443-2-1 Requirement text - excerpt
5.15 Access control	entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use. (Guidance second list, re Implementing access control rules part c))	USER 1.5 Least privilege	The asset owner shall have policies and procedures to verify that IACS users are only granted the access rights that they require to perform their assigned tasks.
5.21 Managing information security in the ICT supply chain	Implementing processes to ensure that components from suppliers are genuine and unaltered from their specification… (Guidance part j))	COMP 3.1 Security patch authenticity/integrity	The asset owner shall have policies and procedures related to verifying the authenticity and integrity of all patches prior to installation.
5.25 Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents. (Control)	EVENT 1.7 Event analysis	The asset owner shall have policies and procedures around the analysis of IACS security-related events to identify and characterize attacks, security compromises and security incidents in a timely manner.
8.25 Secure development life cycle	Rules for the secure development of software and systems should be established and applied … Secure development is a requirement to build up a secure service, architecture, software and system. (Control and Guidance)	ORG 2.3 Secure development and support	The asset owner shall have policies and procedures addressing the use of a secure development lifecycle process for the development and support of systems and components used in the IACS.

ISO/IEC 27001 Control ID and name	ISO/IEC 27002 Control or Guidance excerpt	ISA/IEC 62443-2-1 Requirement ID and name	ISA/IEC 62443-2-1 Requirement text - excerpt
8.8 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization’s exposure to such vulnerabilities should be evaluated and appropriate measures should be taken. (Control)	EVENT 1.9 Vulnerability handling	The asset owner shall have policies and procedures related to identifying, addressing and resolving existing and newly identified IACS vulnerabilities in a timely manner.
8.8 Management of technical vulnerabilities	…an accurate inventory of assets …the inventory should include the software vendor, software name, version numbers, current state of deployment… (Guidance first paragraph)	COMP 3.3 Security patch status	The asset owner shall have policies and procedures related to the documentation and maintenance of the security patch status of all components.
8.8 Management of technical vulnerabilities	Testing and evaluating updates before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. (Guidance under Taking appropriate measures to address technical vulnerabilities, part d))	COMP 3.2 Security patch validation and installation	The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of security patches applicable to components in a timely manner after their release.
5.12 Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements. (Control)	DATA 1.1 Data classification	The asset owner shall have policies and procedures related to identifying and classifying all IACS data requiring safeguarding according to their protection requirements.

ISO/IEC 27001 Control ID and name	ISO/IEC 27002 Control or Guidance excerpt	ISA/IEC 62443-2-1 Requirement ID and name	ISA/IEC 62443-2-1 Requirement text - excerpt
5.16 Identity management	The full life cycle of identities should be managed. (Control) Identities are disabled or removed in a timely fashion if they are no longer required… (Guidance part d))	USER 1.2 User identity removal	The asset owner shall have policies and procedures for removing/disabling IACS-specific identifiers, authenticators, roles and access rights for human users, software processes and devices that do not or no longer need access.
5.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control. (Control) Modifying access rights of users who have changed roles or jobs … Removing or adjusting physical and logical access rights, which can be done by removal, revocation or replacement of keys, authentication information, identification cards or subscriptions (Guidance parts i) and j))	USER 1.2 User identity removal	The asset owner shall have policies and procedures for removing/disabling IACS-specific identifiers, authenticators, roles and access rights for human users, software processes and devices that do not or no longer need access.

ISO/IEC 27001 Control ID and name	ISO/IEC 27002 Control or Guidance excerpt	ISA/IEC 62443-2-1 Requirement ID and name	ISA/IEC 62443-2-1 Requirement text - excerpt
7.14 Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. (Control)	DATA 1.4 Data retention policy	The asset owner shall have policies and procedures related to data retention during the entire IACS lifecycle, including purging.
8.15 Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analyzed. (Control)	EVENT 1.4 Logging	The asset owner shall have policies and procedures related to writing IACS security-related events to one or more protected event/audit logs and retaining them for an adequate time period.
5.24 Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. (Control)	EVENT 1.8 Incident handling and response	The asset owner shall have policies and procedures for employing and keeping current a process for evaluating and responding to IACS security-related incidents.

ISO/IEC 27001 Control ID and name	ISO/IEC 27002 Control or Guidance excerpt	ISA/IEC 62443-2-1 Requirement ID and name	ISA/IEC 62443-2-1 Requirement text - excerpt
8.5 Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control. (Control)	USER 1.8 Human user authentication	The asset owner shall have policies and procedures related to identifying and authenticating all human users on all IACS interfaces that can be used by human users to access the IACS. This includes, but is not limited to: a) device interactive human user login interfaces, b) application interfaces such as web services, file transfers and OPC servers, and c) remote desktop interfaces that provide human users login access to IACS devices over the network. NOTE Some OSs manage the conveyance of the authenticated user identity transparently to the application and make the user identity available to the application.
8.5 Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control. (Control)	USER 1.6 Software service authentication	The asset owner shall have policies and procedures related to identifying and authenticating software services prior to their execution.

6 Conclusion

In several critical areas, [62443] addresses cyber security topics not commonly encountered in an IT environment. In these areas, an organization can expect controls and approaches for their OT environment to be distinct from those that are effective for their IT environment. Severe health, safety, and environmental consequences may be risks in the event of the loss of availability or integrity of the physical control function which relies upon the OT system. These risks drive requirements of [62443] to avoid system unavailability caused by "friendly fire," to permit recovery to a known state if control is lost, to prevent external interference with safety or control functions, and to rigorously track the configuration of the Automation Solution and all connections.

A second subset of requirements of [62443] such as the examples in Section 4 may be viewed as specific instances of more general recommendations found in [27002] guidance. [62443] therefore in effect requires conformance to 27002 recommendations under specific OT scenarios.

In addition, there is a broad area of common concern for IT and OT cyber security that is reflected in the commonality of expression for many recommendations and controls of [27001/2], with requirements of [62443]. Thus, [62443] has in effect "selected" some of the [27001/2] controls as of particular interest for OT. Therefore, an organization that is applying both standards for an OT environment, would place a priority on including these controls in developing their Statement of Applicability that is required to comply with [27001/2]. At the same time, the organization would thereby achieve compliance with these requirements of [62443]. However, the actions taken by an organization to comply with the same [27001/2] recommendation or requirement for their OT and IT environments may not be the same, due to differences in risk and operational characteristics for these environments.

7 Definitions and abbreviations

7.1 Definitions

asset owner
organizational role ultimately accountable for one or more IACS

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

Note 2 to entry: In the context of this document, asset owner also includes the operator of the IACS.
[SOURCE ISA/IEC 62443-2-1]

Automation Solution
control system and any complementary hardware and software components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this document.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution can be comprised of components from multiple suppliers, including the product supplier of the control system.
[SOURCE ISA/IEC 62443-2-1]

control
measure that is modifying risk

NOTE 1 Controls include any process, policy, device, practice or other actions which modify risk.

NOTE 2 It is possible that controls not always exert the intended or assumed modifying effect.
[SOURCE ISO/IEC 27000]

control system
hardware and software components of an IACS

NOTE 1 Control systems include systems that perform monitoring functions.

NOTE 2 Control here refers to the control of a physical process. This is distinct from the term "control" used in ISO/IEC 27001/2 as defined in the entry above.
[SOURCE ISA/IEC 62443-4-2, NOTE 2 added]

essential function
function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.
[SOURCE ISA/IEC 62443-4-2]

industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation
[SOURCE ISA/IEC 62443-3-3]

operational technology (OT)
hardware and software that detects or causes a physical change, through the direct monitoring and/or control of industrial equipment, assets, processes and events
[SOURCE: Gartner IT Glossary]

recommendation
expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable without necessarily mentioning or excluding others
[SOURCE ISO/IEC Directives Part 2 : 2021]

requirement
expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled and from which no deviation is permitted if conformance with the document is to be claimed
[SOURCE ISO/IEC Directives Part 2 : 2021]

security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner
[SOURCE ISA/IEC 62443-3-3]

security zone
grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization
[SOURCE ISA/IEC 62443-3-2]

7.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
DMZ	demilitarized zone
ED	edition
FDIS	Final Draft International Standard
HR	Human Resources
HSE	Health, Safety, Environment
IACS	industrial automation and control system(s)
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISAGCA	ISA Global Cybersecurity Alliance
ISO	International Organization for Standardization
IT	Information Technology
JTC	Joint Technical Committee
NIST	National Institute of Standards and Technology (US)
NIST SP	NIST Special Publication
OPC	Open Platform Communications
OT	Operational Technology
SR	system requirement
SUC	system under consideration
TC	Technical Committee
ZCR	zone and conduit requirement

8 References

8.1 ISA/IEC 62443 standards

Note: The IEC 62443 and ANSI/ISA 62443 standards share the same technical content. The references below address the IEC as well as the ANSI/ISA document.

[62443-2-1] IEC 62443-2-1: 2024 - Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

ANSI/ISA-62443-2-1-2024 - Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

[62443-2-4] IEC 62443-2-4: 2023 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

ANSI/ISA-62443-2-4-2023 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

[62443-3-2] IEC 62443-3-2: 2020 - Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

ANSI/ISA 62443-3-2: 2020 Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design

[62443-3-3] IEC 62443-3-3: 2013 - Industrial communication networks - Network and system security – Part 3-3: System security requirements and security levels

ANSI/ISA 62443 3 3 (99.03.03)-2013 - Industrial communication networks - Network and system security – Part 3-3: System security requirements and security levels

[62443-4-1] IEC 62443-4-1:2018 - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

ANSI/ISA-62443-4-1-2018 - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

[62443-4-2] IEC-62443-4-2:2018 - Security for industrial automation and control systems - Part 4-1: Technical security requirements for IACS components

ANSI/ISA-62443-4-2-2018 - Security for industrial automation and control systems - Part 4-1: Technical security requirements for IACS components

8.2 ISO/IEC 27001 and ISO/IEC 27002 standards

[27001] ISO/IEC 27001 Third Edition 2022-10 - Information security, cybersecurity and privacy protection - Information security management systems – Requirements

[27002] ISO/IEC 27002 Third Edition 2022-02 - Information security, cybersecurity and privacy protection - Information security controls

8.3 Other references

[OTE] Applying ISO/IEC 27001 / ISO/IEC 27002 and the ISA/IEC 62443 standard series for Operational Technology Environments, ISA Global Cybersecurity Alliance, www.isa.org/otstandards

[Gartner-ITG] Gartner: IT Glossary, retrieved 2025-02-08
http://www.gartner.com/it-glossary

[NIST 800-82] NIST SP 800-82 Revision 3 Guide to Operational Technology (OT) Security