ISA GLOBAL CYBERSECURITY ALLIANCE

Applying ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 Series for Operational Technology Environments

June 2025

www.isagca.org

Table of Contents

Applying ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 Series for Operational Technology Environments

Introduction

Many organizations (especially very large ones) have established policies and procedures governing the IT security in their office environment; many of these are based on ISO/IEC 27001:2022 [27001] and ISO/IEC 27002:2022 [27002].[1] Some have attempted to address their operational technology (OT) infrastructure under the same management system, and have leveraged many IT/OT commonalities. Although it would be ideal to always select common controls and implementations for both IT and OT, organizations have been confronted with challenges in doing so, such as OT operator screen locking creating unsafe conditions, antivirus products incompatible with OT equipment, patching practices disrupting production schedules, or network traffic from routine backups blocking safety control messages.

The ISA/IEC 62443 standard series [62443][2] explicitly addresses issues such as these; this helps an organization to maintain conformance with ISO/IEC 27001:2022 and ISO/IEC 27002:2022 [27001/2][3] through common approaches wherever feasible, while highlighting differences in IT vs. OT approaches where needed.

The ISO/IEC 27001 and ISO/IEC 27002 series of standards were revised in 2022. In this context this document offers guidance for organizations familiar with 27001/2 and interested in protecting the OT infrastructure of their operating facilities based on the ISA/IEC 62443 series.

It describes the relationship between the ISA/IEC 62443 series and ISO/IEC 27001/2 and how both standards may be effectively used within one organization to protect both IT and OT.

1 When ISO/IEC 27001 is addressed, we may use the reference [27001]. When ISA/IEC 27002 is adddressed, we may use the reference [27002].

2 When all documents of the ISA/IEC 62443 series of standards are addressed, we may use the reference [62443].

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

ISA/IEC 62443 does not include any specific requirement to an Information Security Management System (ISMS), but it requires the establishment of a security management as part of the security program of the asset owner. If the organization has an established ISMS, the security program in the OT environment shall be coordinated with it. In this document we are considering that the organization has an established ISMS based on ISO/IEC 27001 and policies and procedures addressing the IT security based on ISO/IEC 27002.

Background

Scope of ISO/IEC 27001:2022 and ISO/IEC 27002:2022

ISO/IEC 27001 provides requirements for establishing, implementing, maintaining and continually improving an ISMS as well as a list of commonly accepted risk treatment controls. In addition, [27002] provides further guidance for organizations implementing these risk treatment controls (the term "control" is defined in ISO/IEC 27000—the glossary and introduction to the 27000 series—as "measure that is modifying risk". The risk treatment controls are designed to be used by organizations as a reference for selecting the relevant controls for their specific scope of application. A certified implementation requires conformance to all controls to the ISMS and to the risk treatment controls that have been selected within the scope of applicability.

IT and OT

"IT" is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use. Operational technology or "OT" is defined as "technology for detecting, managing, or causing change through the monitoring or control of a physical entity. Note 1 to entry: Including the personnel and processes to manage the systems. Note 2 to entry: Operated by skilled or unskilled people or fully automated. Note 3 to entry: includes digital and any other technologies" [IEC]. Increasingly, IT products and systems are used in OT infrastructures, and recently, the advent of IoT (Internet of Things) and Industrial IoT has further blurred the IT/OT distinction. However, the main difference is that OT environments in general must comply with strict integrity, availability

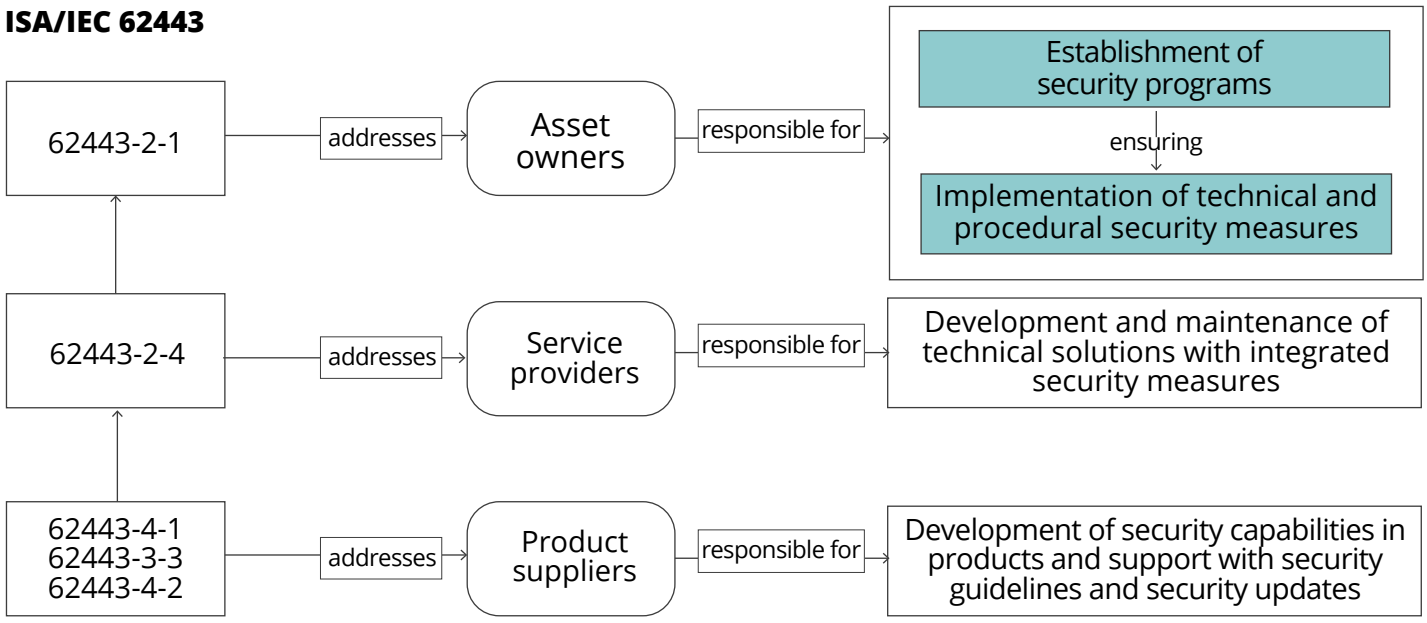

Figure 1. The ISA/IEC 62443 standard series addresses all entities involved in the protection of operating facilities

and performance constraints due to the fact that operation outside of the constraints may impact health, safety or the environment.

Scope of the ISA/IEC 62443 series

The scope of the ISA/IEC 62443 series of standards is the security of "Industrial Automation and Control Systems (IACS)" used in OT operating facilities. This includes control systems used in manufacturing and processing plants and facilities, geographically dispersed operations such as utilities (*i.e.*, electricity, gas and water), pipelines and petroleum production and distribution facilities. The ISA/IEC 62443 series has also gained acceptance outside of its original scope, for example in building automation, medical systems, and in other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.

Figure 1 gives an overview of the scope of some core documents of [62443]. ISA/IEC 62443-2-1 [62443-2-1] is targeted at organizations that are responsible for IACS, which includes owners and operators (termed "asset owners" in the series) and provides requirements for the security program of asset owners.

In addition, the ISA/IEC 62443 series provides conformance requirements for all other entities supporting asset owners in the implementation of technical and procedural security measures for the protection of operating facilities from cyber threats. ISA/IEC 62443-2-4 [62443-2-4] provides security requirements for integration and maintenance service providers supporting asset owners in the development and operation of OT specific technical solutions. ISA/IEC 62443-3-3 [62443-3-3] and ISA/IEC 62443-4-2 [62443-4-2] define requirements for security capabilities of systems and components, respectively. ISA/IEC 62443-4-1 [62443-4-1] includes lifecycle requirements for product suppliers for the development and support of products with adequate security capabilities. In addition, ISA/IEC 62443 includes guidance documents for specific issues like patch management and risk-based system partitioning in zones and conduits. Note that product suppliers and service providers may own production facilities, thus be in the role of an asset owner for these facilities.

ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 series of standards address two complementary parts of an overall OT cybersecurity approach

ISO/IEC 27001/2 standards have been broadly used for many years as a base for organizing the information security of organizations. The processes and overall management structure of organizations responsible for OT

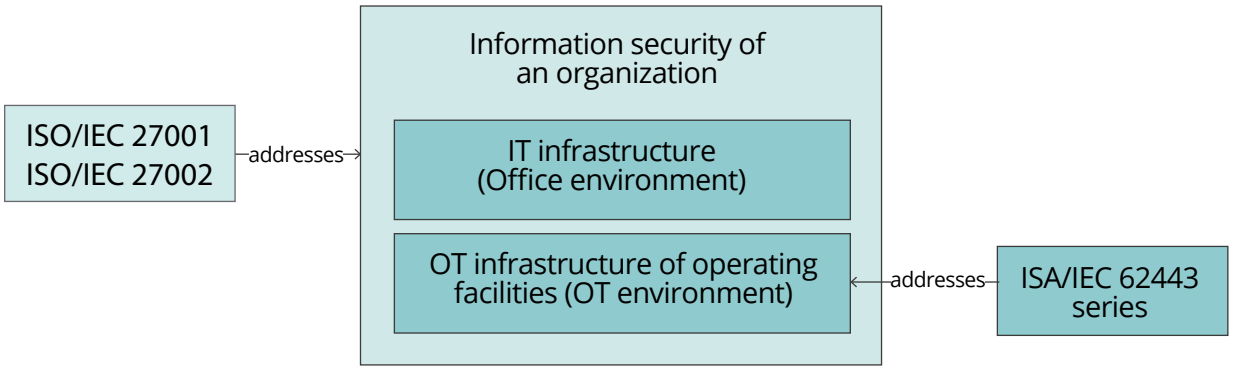

Figure 2. Scope of ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 series of standards

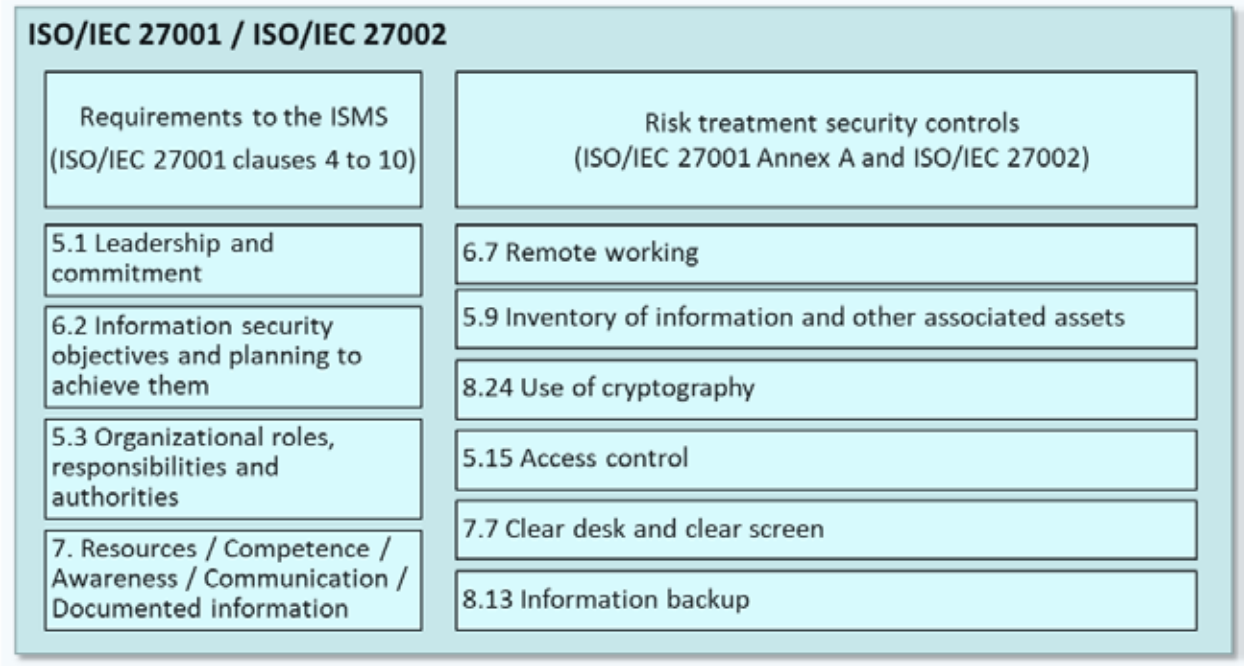

Figure 3. Examples of requirements to the ISMS and risk treatment security controls

environments may be integrated with an ISMS based on these standards as will be described here. ISA/IEC 62443 addresses specific needs of OT infrastructures and complements established ISMS.

The OT infrastructure of operating facilities may be embedded in the IT infrastructure of the organization or autonomously organized. In both situations ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 series can be used for addressing complementary parts of an overall cybersecurity approach for OT environments.

ISO/IEC 27001 / ISO/IEC 27002 address the establishment of an information security management system for the IT infrastructure of an organization

ISO/IEC 27001/2 specifies generic requirements which are intended to be applicable to all organizations, regardless of type, size or nature. The requirements for establishing, implementing, maintaining and continually improving an ISMS are described in clauses 4 to 10 of ISO/IEC 27001. Excluding any of the requirements specified in these clauses is not acceptable when an organization claims conformity to this standard. In addition, it includes risk treatment controls addressing security topics that require consideration in a comprehensive security strategy. According to the standard, an organization can select controls from the list provided by [27001/2] and design additional controls to meet the specific needs of the organization. The distinction between ISMS requirements and risk treatment security controls specified in [27001/2] is illustrated by a few examples shown in Figure 3.

The ISA/IEC 62443 series of standards addresses specific needs required for cybersecurity in OT environments

IACS in operating facilities must fulfill specific requirements of integrity, performance and availability to ensure operational continuity. Loss of operational continuity may for example manifest as an explosion, a blackout, or the use of an incorrect formula or dose of a life-saving medicine. Many operating facilities implement dedicated safety systems to prevent operational conditions that would have health, safety and environmental consequences.

Security Control ISO/IEC 27001/2	OT consideration	ISA/IEC 62443 reference
7.7 Clear desk and clear screen	OT Operator screen locking can create creating unsafe conditions	*ISA/IEC 62443-2-1 USER 1.18* may require to exclude OT operator screen lock
8.7 Controls against malware	Antivirus products are often incompatible with OT assets	*ISA/IEC 62443-2-1 COMP 2.3* requires testing malware protection software for compatibility with IACS
8.13 Information backup	Network traffic from routine backups blocking safety control messages	*ISA/IEC 62443-3-3 SR 5.1 RE(1)* requires physically segmenting critical control system networks from non-critical control system networks
8.8 Management of technical vulnerabilities	Patching practices can disrupt production schedule	*ISA/IEC 62443-2-3 section 5, part f* requires testing and planning patch application to ensure operational continuity

Figure 4. OT considerations regarding some IT security control implementations

Security requirements in ISA/IEC 62443 are designed to avoid preventing or disrupting safe operation. Furthermore, dedicated safety functions require unique protection and therefore are subject to unique security requirements in the standard.

These typical challenges, often faced when extending existing IT security control implementations to OT, are addressed by ISA/IEC 62443 as shown in Figure 4. The ISA/IEC 62443 series includes requirements addressing all security topics to be handled in a comprehensive security program, in the same way that ISO/IEC 27001/2 includes a list of risk treatment controls addressing similar security aspects. ISA/IEC 62443 requirements address specific needs in the OT environment and complement the list of risk treatment controls of ISO/IEC 27001/2 by adding critical details relevant to that environment.

ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 series of standards should be combined for the protection of operating facilities

The above discussion shows how ISA/IEC 62443 augments ISO/IEC 27001/2 by incorporating specifics unique to the OT environment. However, ISA/IEC 62443 does not include all elements needed for the security in OT. In particular ISA/IEC 62443 does not include requirements to the security management, but delegates it to an established ISMS of the asset owner. ISO/IEC 27001/2 also includes some controls that are relevant for OT but are out of the scope of ISA/IEC 62443. Therefore, a method for applying both standards to OT infrastructure is recommended, and one such method is described here.

The concept recognizes that [62443-2-1] is addressing the security program of asset owners for their OT operating facilities; consequently, this part of the ISA/IEC 62443 series of standards should be the link to ISO/IEC 27001/2. The other documents of ISA/IEC 62443 have the purpose to provide support to asset owners and have their roots in the requirements of [62443-2-1].

Extend and adapt ISMS based on ISO/IEC 27001 for the OT infrastructure

Although ISA/IEC 62443 doesn't define requirements for establishing, implementing, maintaining and continually improving an

ISMS, the first requirement of [62443-2-1] requires that IACS security programs must be coordinated with any established ISMS. It is recommended that for the OT infrastructure organizations establish an ISMS based on clauses 4 to 10 of ISO/IEC 27001. It should be ensured that the structure and implementation is conducive and flexible to inclusion of the OT environment in its scope without causing negative impacts on the established ISMS in IT. For example, this will require clarity about allocation of IT/OT management responsibilities, responsibilities for IT/OT system interfaces, adequate resource planning for overlapping and unique technical skills across IT/OT and effective use of concepts and terminology from both standards.

Consider the risk treatment security controls of ISO/IEC 27002 when applying ISA/IEC 62443-2-1 requirements for OT infrastructure

One practical way to organize the combined set of [27002] security controls and [62443-2-1] requirements is to leverage the structure of [62443-2-1] in Security Program Elements (SPE) which are logical groupings of requirements covering a specific topic. All security topics should be addressed in a comprehensive security program. Examples of SPEs are configuration management, network and communication security, component security, user access control and protection of data. Some SPEs are subdivided to cover different security aspects included in the same SPE. The proposed approach recommends adding to the requirements in each SPE respectively sub-SPE, the related risk treatment security controls of [27002], as shown in Figure 5.

Although most of the [27002] controls are related to one or several topics addressed by the SPEs, some are of general nature such as "5.5 Contact with authorities", "6.2 Terms and conditions of employment", and "5.32 Intellectual property rights". These are the "General security controls" in Figure 5. They must be considered in the risk-based approach of the asset owner and adapted to the OT environment in the same way as the ISMS is adapted. It should be noted that considering the combination of the [27002] controls and [62443-2-1] requirements does not mean that all of them must be applied. The applicable requirements should be selected as the result of a risk analysis by the asset owner according to its specific needs and operating conditions.

When implementing the security program, the asset owner may then consider in a risk-based approach all relevant aspects, based on the combination of requirements on this topic from both standards.

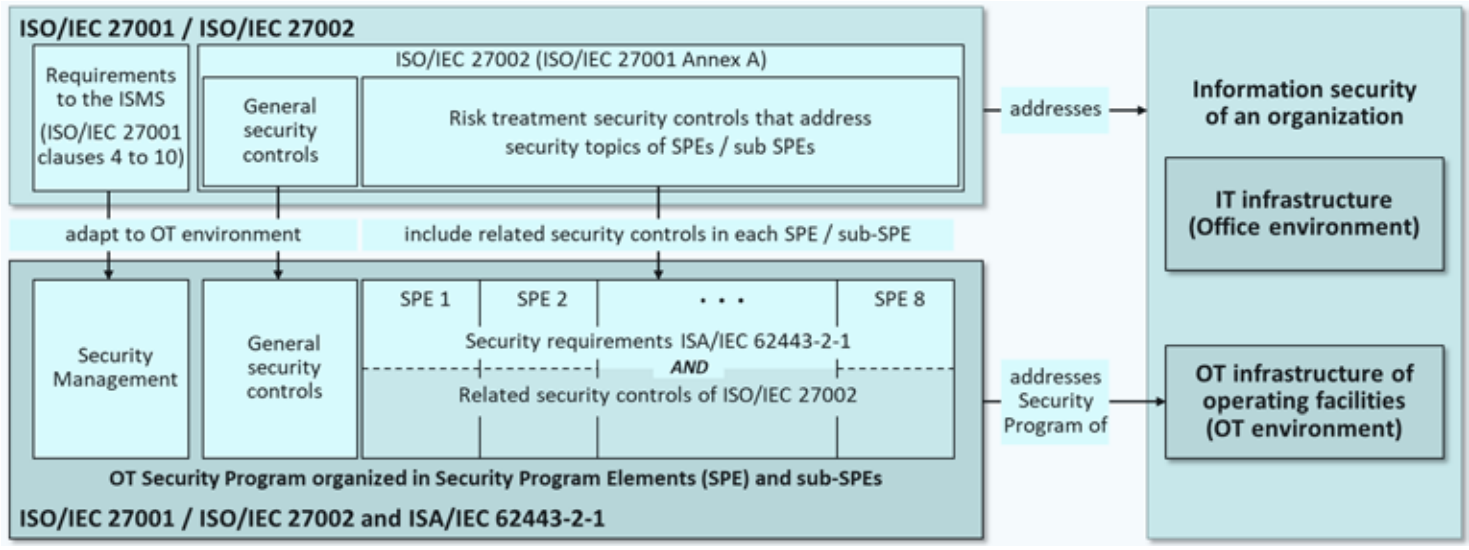

Figure 5. Combining controls of ISO/IEC 27001 / ISO/IEC 27002 controls and requirements of ISA/IEC 62443-2-1 OT security programs

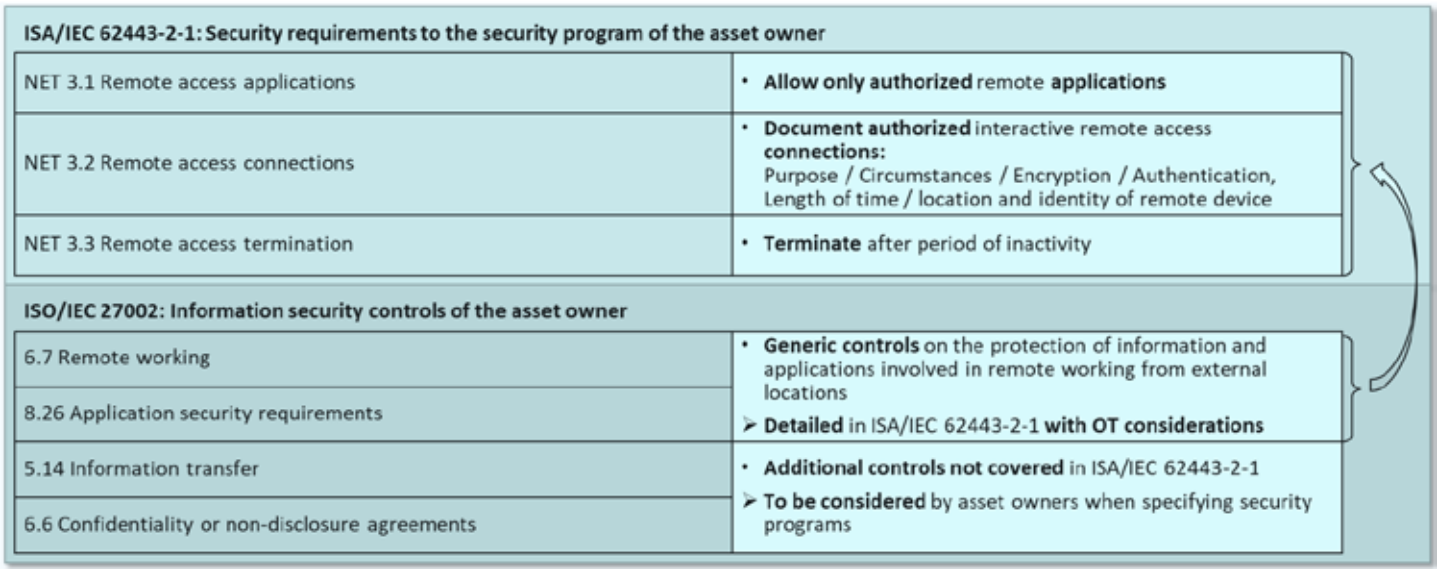

Figure 6. ***NET 3 – Secure remote access:*** **Combining [62443-2-1] requirements and [27002] controls**

The benefits of adding in each SPE and sub-SPE the related security controls of [27001/2] can be illustrated with the example of the sub-SPE "NET 3 - Secure remote access," which is part of "SPE 3 – Network and communication security" (Figure 6).

OT assets in operating facilities are often maintained by external service providers from locations outside of the operating facility. Allowing remote access to the OT infrastructure must be strictly controlled to avoid creating unnecessary attack surfaces. Consequently, [62443-2-1] NET 3 requires asset owners:

- to ensure that only authorized remote applications are allowed,
- to ensure that authorized interactive remote connections are documented including the purpose, circumstances, encryption and authentication technologies, length of time, and location and identity of remote client device, and
- to ensure that the remote access is terminated after a period of inactivity.

The above requirements are OT specific, detailing the recommended [27002] controls addressing remote working from external locations. Figure 6 shows an example list of controls relevant to this topic. [27002] requires protection of information accessed, processed or stored at remote working sites, securing application services on public networks and protection of application services transactions. [62443-2-1] adds OT considerations based on use cases involving remote access by defining the OT specific requirements NET 3.1 to NET 3.3 as shown in Figure 6. On the other hand, [27002] addresses aspects which are not covered by [62443-2-1] but may be considered for security programs in OT environments, for example:

- information transfer policies and procedures,
- agreements on information transfer, and
- confidentiality or non-disclosure agreements.

A comprehensive protection scheme for securing remote access to the OT infrastructure of operating facilities should consider all aspects addressed by both standards.

The ISA/IEC 62443 series of standards brings unique value by supporting a holistic approach

Asset owners rely on the design of adequate technical solutions with integrated security measures and on security capabilities of products used in these solutions. As shown in Figure 1, ISA/IEC 62443 provides significant added value by addressing all other entities that support

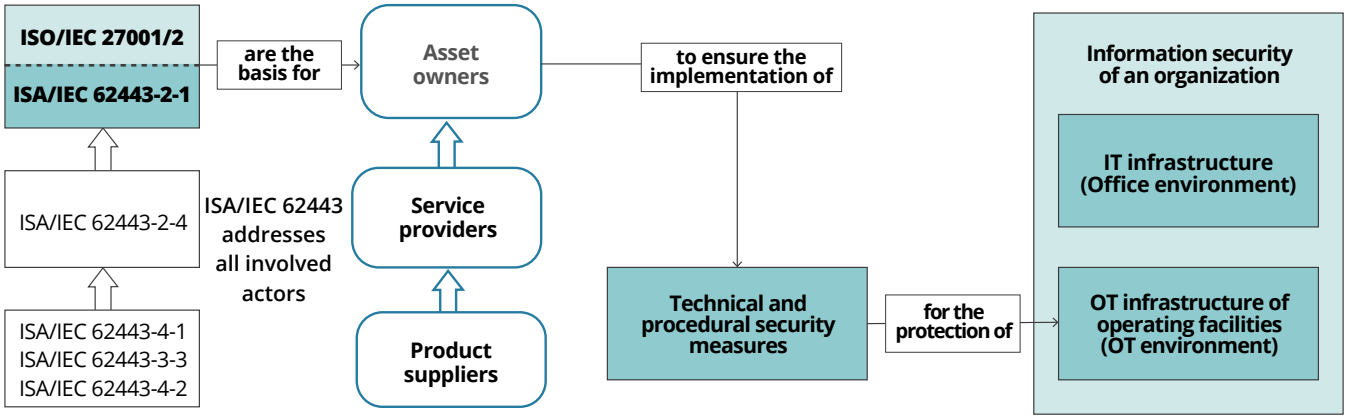

Figure 7. Together with ISO/IEC 27001 / ISO/IEC 27002, the ISA/IEC 62443 series of standards provides the basis for the protection of operating facilities

asset owners when applying a defense-in-depth approach for the protection of their operating facilities against cyber threats. Figure 7 illustrates the relationship between ISO/IEC 27001/2 and ISA/IEC 62443, as well as associated organizational entities, to produce a comprehensive cybersecurity program for the protection of operating facilities against cyberthreats.

ISO/IEC 27001/2 includes four controls (5.19 to 5.22) specifically about suppliers, and a number of mentions of suppliers in guidance for other controls. ISA/IEC 62443 supports implementation of these controls by providing specific parts of the standard with which OT suppliers in specific roles should comply. This gives the asset owner a basis for placing cybersecurity requirements on OT suppliers and potentially requiring third party certification to relevant parts of ISA/IEC 62443 for their OT service providers or for product purchases. For example, [62443-4-1] includes requirements on product suppliers for reducing and managing vulnerabilities such as threat modelling, applying secure design principles, eliminating coding vulnerabilities by following coding guidelines, finding and eliminating vulnerabilities via testing such as fuzz testing, penetration testing and binary analysis, providing security guidelines for users, and addressing vulnerabilities discovered in the field with a process for security updates.

In addition, ISA/IEC 62443 includes requirements to the technical security capabilities of products used in OT infrastructures and defines security levels (SLs) to differentiate the strength of the security requirements commensurate to the tolerable cybersecurity risks of asset owners.

ISO/IEC 27001/2 and ISA/IEC 62443 complement one another when implementing a comprehensive, risk-based, defense-in-depth strategy for the protection of operating facilities including the contribution of all entities:

- The combined requirements and controls of ISO/IEC 27001/2 and ISA/IEC 62443-2-1 are the basis for asset owners to establish security programs and ensure the design and implementation of technical and procedural security measures.
- The requirements of ISA/IEC 62443-2-4 are the basis for service providers to support asset owners by designing and maintaining technical solutions providing the required security capabilities.
- The requirements of ISA/IEC 62443-4-1 are the basis for product suppliers to support asset owners and service providers by employing secure development processes and providing guidelines and support for integrating and maintaining the security of products used in OT infrastructures.
- The requirements of ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 are the basis for providing product security capabilities necessary for the implementation of protection schemes by asset owners and service providers.

Next steps

A mapping of the relevant [27002] controls to each SPE or sub-SPE of [62443-2-1] should be the base to implement the described approach. A reference mapping could be developed for this purpose as a commonly used resource. Organizations could use such a reference mapping for the development of their OT security programs and adjust it to their specific needs as necessary.

References

[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

[IEC] International Electrotechnical Commission
https://www.iec.ch/

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

[62443-3-3] 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


ISA
ISA GLOBAL
CYBERSECURITY
ALLIANCE