GLOBAL CYBERSECURITY ALLIANCE

Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments

THE TIME IS NOW

July 2021

www.isa.org/ISAGCA

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

This document offers guidance for organizations familiar with ISO/IEC 27001 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.

62443 does not require the use of an underlying Information Security Management System (ISMS), However it requires that, if the organization has an established ISMS, the security program in the OT environment should be coordinated with it. In this document we are considering the use case of an existing ISMS based on ISO/IEC 27001/2.

Other information security standards similar in scope to 27001 might be used effectively together with 62443 under an approach similar to that described here. Evaluation of such approaches is outside the scope of this paper. However, users of such standards are encouraged to explore that possibility.

Background

Scope of ISO/IEC 27001/2

The standard ISO/IEC 27001 provides requirements for establishing, implementing, maintaining, and continually improving an ISMS as well as a list of commonly accepted controls to be used as a reference for establishing security requirements (ISO/IEC 27000, the glossary and introduction to the 27000 series, defines the term control as “measure that is modifying risk”). In addition, ISO/IEC 27002 provides further detailed guidance for organizations implementing these information security controls. It is designed for organizations to use as a reference for selecting controls within the process of implementing an ISO/IEC 27001 conformant ISMS.

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 [Gartner-ITG]. "Operational technology" or "OT" is hardware and software that detects or causes a physical change, through the direct monitoring and/or control of industrial equipment, assets, processes and events [Gartner-ITG]. Increasingly, IT products and systems are used in OT infrastructures, and recently, the advent of IoT (Internet of Things) and Industrial Internet of Things has further blurred the IT/OT distinction. However, the main difference is that OT environments in general must comply with strict integrity, availability, 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 infrastructures. 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 the ISA/IEC 62443 series. Part 62443-2-1 [62443-2-1] is targeted at organizations that are responsible for IACS facilities, which includes owners and operators (termed "asset owners" in the series) and provides requirements for asset owner IACS security programs.

Table of Contents

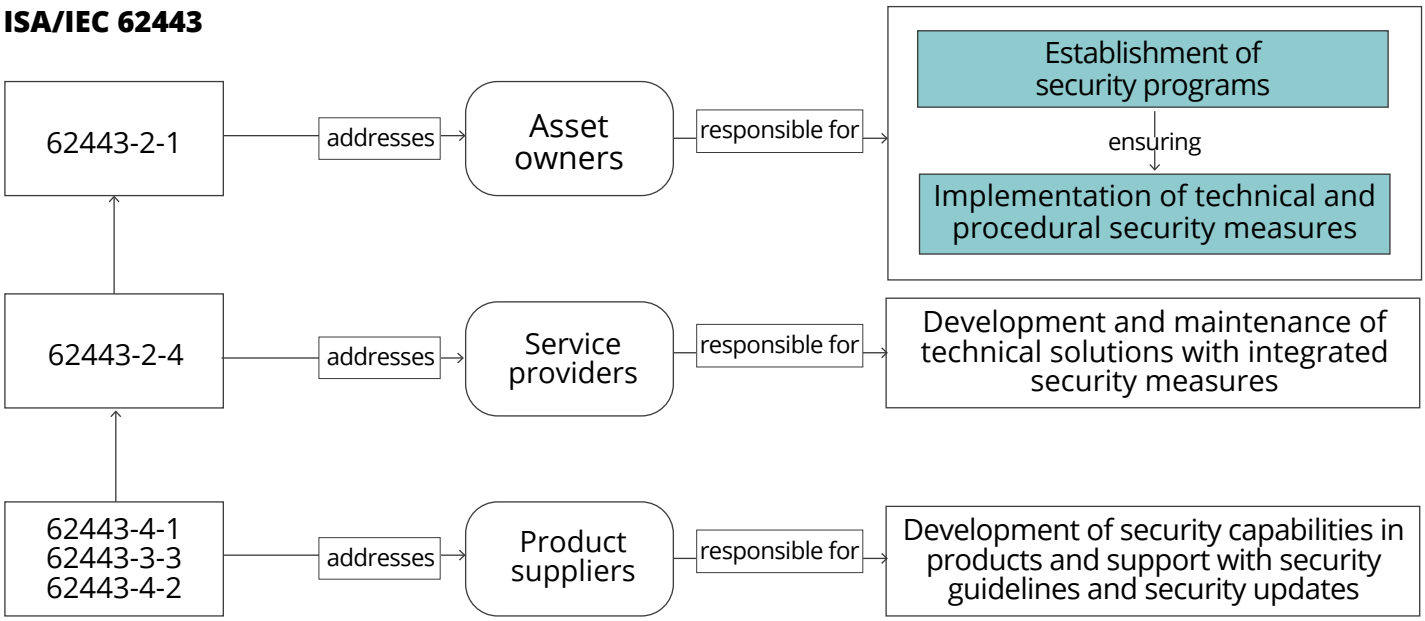

Figure 1. ISA/IEC 62443 addresses all entities involved in the protection of operating facilities

Note: The present document refers to the most recent version of part 62443-2-1, which is not finally approved as an International Standard and may be subject to changes. It is not expected that these changes will impact the recommendations of this paper.

In addition, the ISA/IEC 62443 series provides conformance requirements for all entities supporting asset owners in the implementation of technical and procedural security measures for the protection of operating facilities from cyber threats. Part 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. Parts 62443-3-3 [62443-3-3] and 62443-4-2 [62443-4-2] define requirements for security capabilities of systems and components, respectively. Part 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, the ISA/IEC 62443 series includes guidance documents for specific issues like patch management and risk-based system partitioning in zones and conduits.

ISO/IEC 27001/2 and the ISA/IEC 62443 series 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

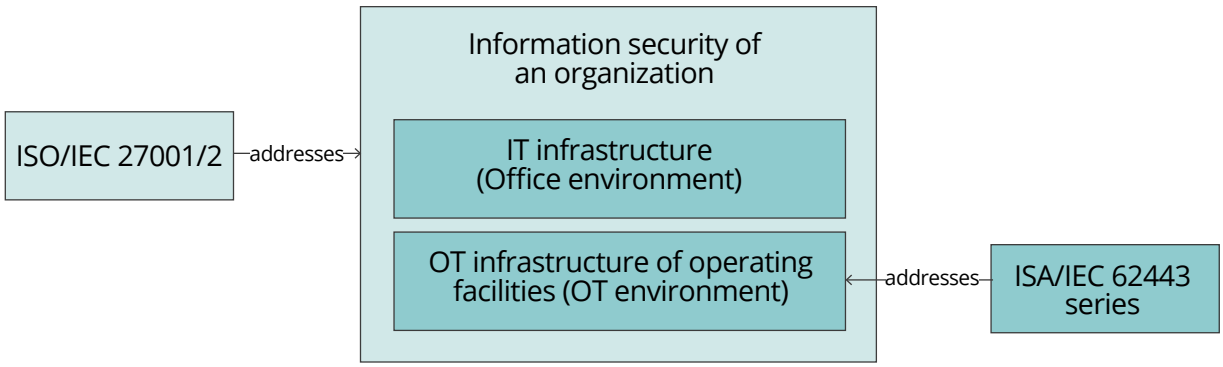

Figure 2. Scope of ISO/IEC 27001/2 and ISA/IEC 62443

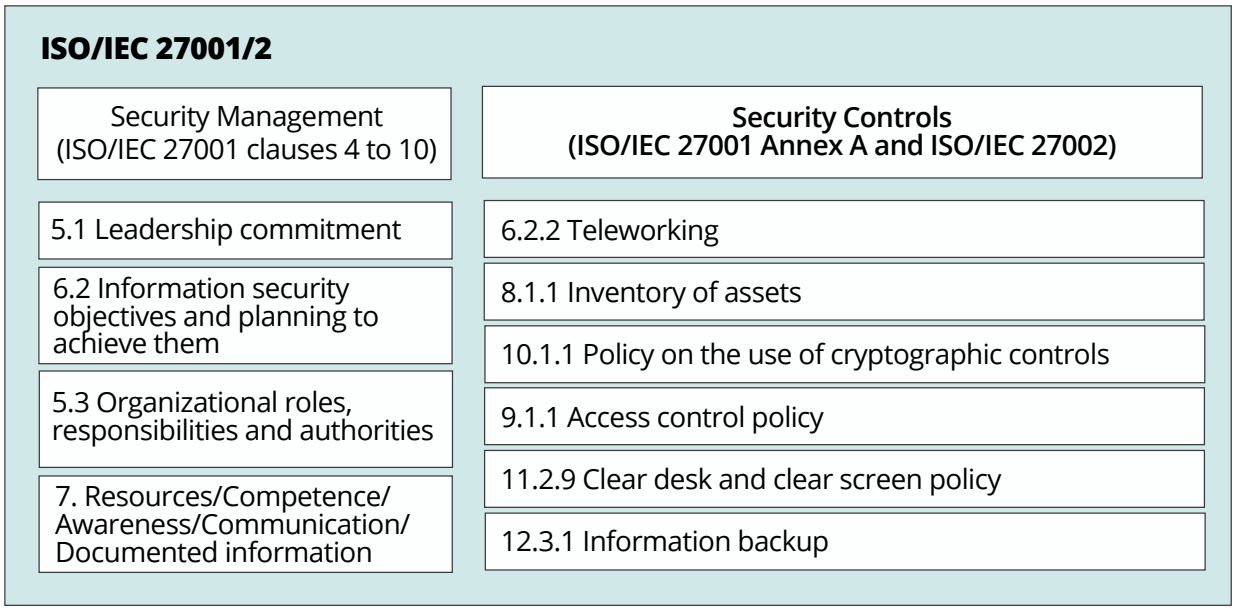

Figure 3. Examples of ISMS requirements and security controls

the information security of organizations. The processes and overall management structure of organizations responsible for OT environments may be integrated with an ISMS based on these standards as will be described here. The ISA/IEC 62443 series addresses specific needs of OT infrastructures and complements the ISMS. The OT infrastructure of operating facilities may be embedded in the IT infrastructure of the responsible organization or autonomously organized. In both situations ISO/IEC 27001/2 and the ISA/IEC 62443 series can be used for addressing complementary parts of an overall cybersecurity approach for OT environments.

ISO/IEC 27001/2 addresses 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, ISO/IEC 27001/2 includes a set of controls addressing security topics which it requires to be given consideration in a comprehensive security strategy. In a risk-based approach, an organization can ultimately select controls from the list provided by ISO/IEC 27001/2 or from other control sets, or new controls can be designed to meet specific needs as appropriate. The distinction between ISMS requirements and information security controls found in ISO/IEC 27001/2 is illustrated by a few examples shown in Figure 3.

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

The OT infrastructures of 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 requirements in ISA/IEC 62443 are designed not to prevent or disrupt safe operation. Further, dedicated safety functions require unique protections and therefore are subject to unique security requirements in the standard. As examples, the challenges mentioned above, often faced when extending existing IT security

Security Control ISO/IEC 27001/2	OT consideration	ISA/IEC 62443 reference
11.2.9 Clear desk and clear screen	OT Operator screen locking can create unsafe conditions	*ISA/IEC 62443-2-1 USER 1.18* may require to exclude OT operator screen lock
12.2.1 Controls against malware	Antivirus products are often incompatible with OT assets	I*SA/IEC 62443-2-1 COMP 2.3* requires testing malware protection software for compatibility with IACS
12.3.1 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
12.6.1 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

control implementations to OT, are addressed by 62443 as shown in Figure 4.

The ISA/IEC 62443 series includes requirements addressing various security topics to be handled in a comprehensive security program, in the same way that ISO/IEC 27001/2 includes a list of controls addressing these security aspects. The ISA/IEC 62443 requirements address specific needs in the OT environment and complement the list of controls of ISO/IEC 27001/2 by adding critical details relevant to that environment.

ISO/IEC 27001/2 and ISA/IEC 62443 should be combined to protect of the OT infrastructure 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 to secure OT. In particular, ISO/IEC 27001/2 provides ISMS requirements and controls/guidance that are fully common to IT and OT and are not found in 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 infrastructures; consequently, this part of ISA/IEC 62443 should be linked to ISO/IEC 27001/2. The other documents of the ISA/IEC 62443 series have the purpose to provide support to asset owners and have their roots in the requirements of 62443-2-1.

Extend and adapt ISMS for the OT infrastructure

Although the ISA/IEC 62443 series 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 organizations establish an ISMS based on ISO/IEC 27001/2, or use an already defined security management system that complies with clauses 4 to 10 of ISO/IEC 27001 for the OT infrastructure. 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 ISMS. 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 all security controls of ISA/IEC 27001/2 when applying 62443-2-1 requirements for OT infrastructure

One practical way to organize the combined set of ISO/IEC 27001/2 security controls and 62443-2-1 requirements for managing coordination of control selection and compliance, is to leverage the structure already present in 62443-2-1. The requirements are structured 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. In addition, some SPEs are subdivided where different security aspects included in the same SPE must be addressed by specific measures. The proposed approach recommends adding to each SPE / sub-SPE the related security controls of ISO/IEC 27001/2, as shown in Figure 5.

Although most of the ISO/IEC 27001/2 controls are related to one or several topics addressed by the SPEs, some are of general nature such as contact with authorities, terms and conditions of employment, and reporting security weaknesses. 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 ISO/IEC 27001/2 controls and 62443-2-1 requirements does not mean that all of them must be applied. The relevant requirements should be selected as the result of a risk analysis by the asset owner according to its specific needs and application conditions.

The benefits of adding in each SPE and sub-SPE the related security controls of ISO/IEC 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). When specifying the security program, the asset owner may then consider in a risk-based approach to all relevant aspects, based on the combination of requirements on this topic from both standards.

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

- ensure that only authorized remote applications are allowed,
- 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
- ensure that the remote access is terminated after a period of inactivity.

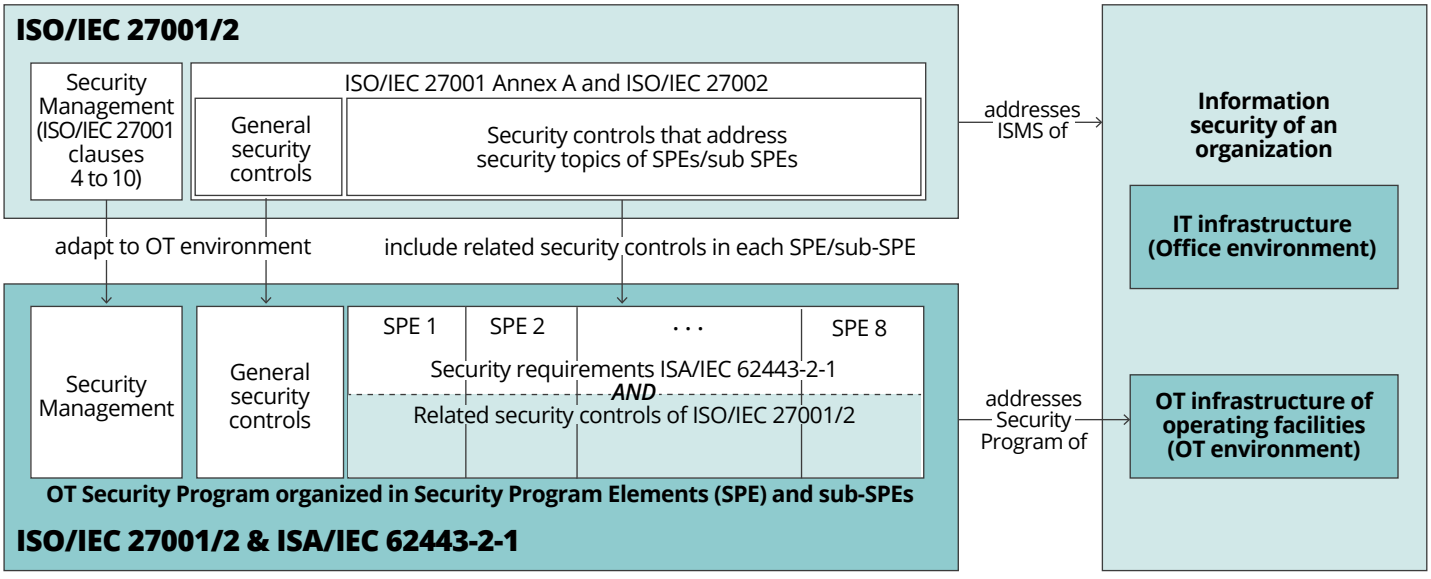

Figure 5. Combining ISO/IEC 27001/2 controls and 62443-2-1 requirements for OT Security Programs

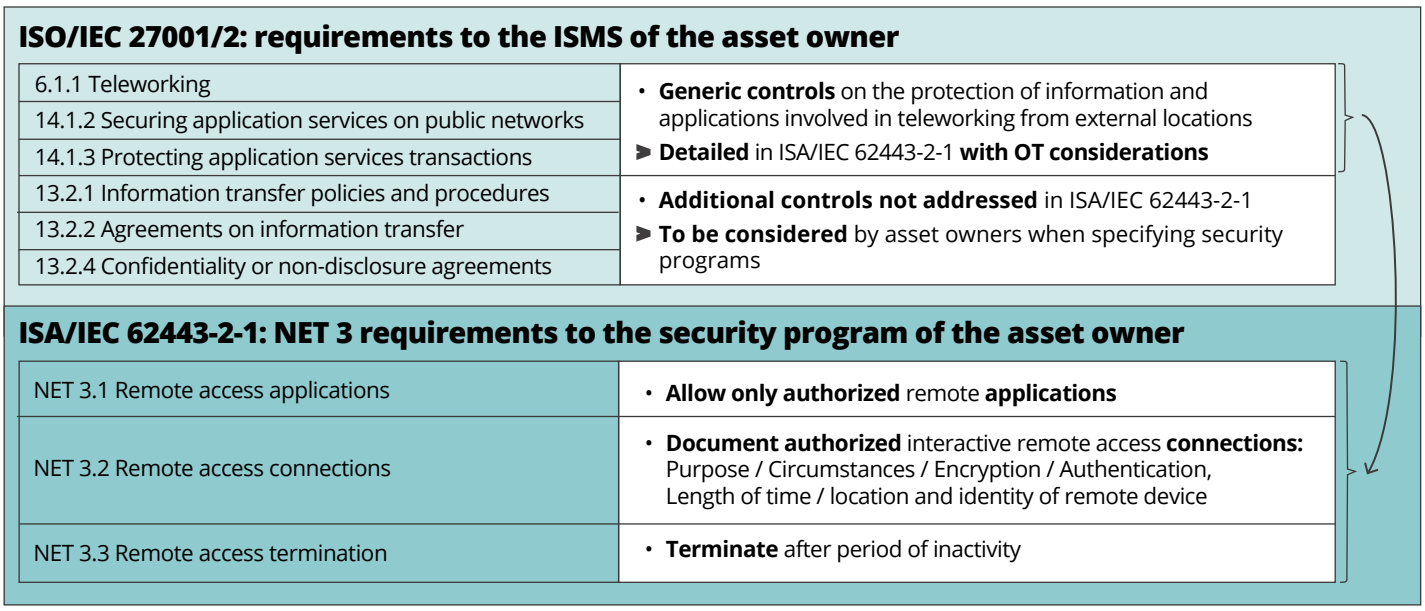

Figure 6. *NET 3 – Secure remote access:* Combining ISO/IEC 27001/2 controls and 62443-2-1 requirements

The above requirements are OT specific, detailing the recommended administrative controls of ISO/IEC 27001/2 addressing teleworking from external locations. As an example, Figure 6 shows a non-exhaustive list of controls relevant for this topic. ISO/IEC 27001/2 requires protection of information accessed, processed, or stored at teleworking sites, securing application services on public networks and protection of application services transactions. 62443-2-1 NET 3.1, NET 3.2, and NET 3.3 add specific requirements that apply to these controls to incorporate OT considerations. On the other hand, ISO/IEC 27001/2 addresses aspects which are not addressed by 62443-2-1 but are possibly relevant to be considered for security programs in OT environments, as shown in Figure 6:

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

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

The ISA/IEC 62443 series brings added 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

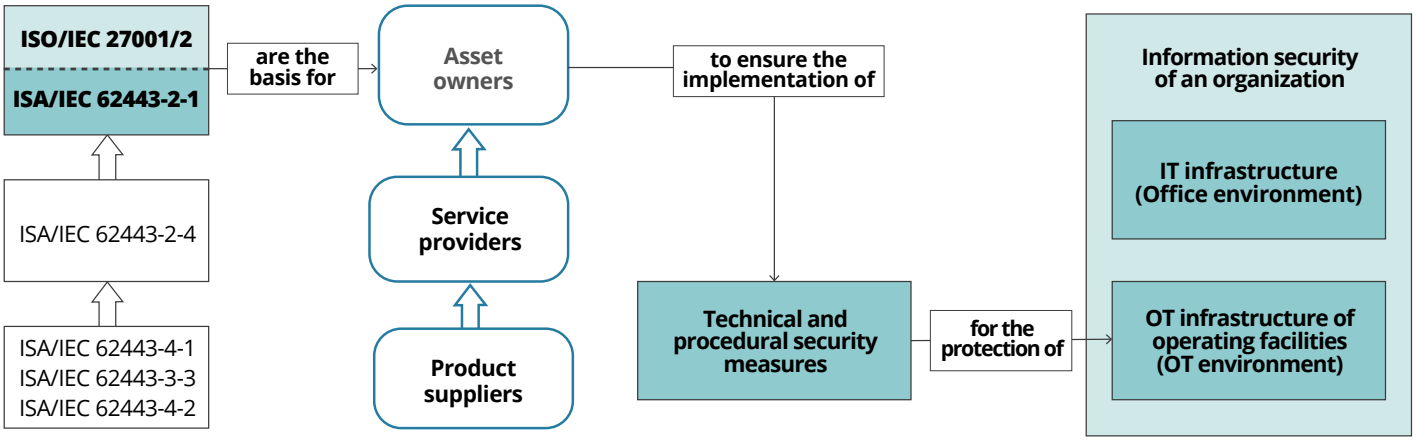

Figure 7. Together with ISO/IEC 27001/2, the ISA/IEC 62443 series provides the basis for a comprehensive protection of operating facilities

products used in these solutions. As shown in Figure 1, the ISA/IEC 62443 series provides a significant added value by addressing all other entities that support asset owners in applying a defense-in-depth approach for the protection of operating facilities against cyber threats. Figure 7 illustrates the relationships between ISO/IEC 27001/2 and the ISA/IEC 62443 series, 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 five controls (class A.15) specifically about suppliers, and a number of mentions of suppliers in guidance for other controls. The ISA/IEC 62443 series 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 the 62443 standard for their OT suppliers 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, the ISA/IEC 62443 series includes requirements for the technical security capabilities of products used in OT infrastructures and defines Security levels (SLs) to differentiate the level of protection which can be potentially reached commensurate to the tolerable cybersecurity risks of asset owners.
ISO/IEC 27001/2 and the ISA/IEC 62443 series complement one another for 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 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 IEC/ISA 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 IEC/ISA 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 IEC/ISA 62443-3-3 and 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

To implement the described approach, a mapping of the set of related ISO/IEC 27001/2 controls under each SPE or sub-SPE of 62443-2-1 is required. An organization may use this approach that relies on 62443-2-1 SPE's, or any other approach they find convenient for merging ISO/IEC 27001/2 controls with 62443-2-1 requirements. A reference mapping could be developed for this purpose as a commonly used resource; ISA's Global Cybersecurity Alliance (ISAGCA) is considering developing such a reference. Organizations could use such a reference mapping as a starting point for the development of their OT security programs and adjust it to their specific needs as necessary.
successful exploitation of a vulnerability.

References

[27001] ISO/IEC 27001 Second Edition 2013-10-01 - Information technology - Security techniques - Information security management systems - Requirements

[27002] ISO/IEC 27002 Second Edition 2013-10-01 - Information technology - Security techniques - Code of practice for information security controls

[Gartner-ITG] Gartner: IT Glossary, retrieved 2021-03-22 http://www.gartner.com/it-glossary

[62443-2-1] IEC CDV 62443-2-1 ED2: 2019-08-23 - Security for industrial automation and control systems - Part 2-1: security program requirements for IACS

[62443-2-4] ISA/IEC 62443-2-4: 2017 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

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

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

[62443-4-2] ISA/IEC-62443-4-2:2019 - Security for industrial automation and control systems - Part 4-1: Technical security requirements for IACS components