НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

CYBER SECURITY AND INFORMATION SECURITY

Mark Dietz
University of Library Studies and Information Technologies

Abstract: *In recent decades progressive digitalization and networking of industrial plants have led to considerable efficiency gains and innovations. At the same time, however, this development has also massively increased the surface of attacks for cyber threats. Industrial plants, which used to be largely isolated and protected by physical security measures, are now part of complex, globally networked systems. This makes them vulnerable to various cyberattacks from criminal organisations and state actors. To meet these challenges, numerous standards have been developed to strengthen cyber security in the industrial environment. Two of the most important and widely used standards are IEC 62443-x series and ISO/IEC 2700x series. The ISO/IEC 2700x series describes establishing and operating an IT security management system (ISMS). This series of standards deals with information security and does not differentiate between data in IT systems and intellectual property. The IEC 62443-x series focuses on protecting industrial automation systems and is therefore assigned to the area of Operational Technology.*

Keywords: *information security, cyber security, vocabulary, requirements, guidelines*

INTRODUCTION

IEC 62443-x is a series of standards developed specifically for the safety of industrial automation and control systems (IACS). It provides comprehensive guidelines for implementing safety measures throughout an industrial plant's life cycle, from planning and design to operation and decommissioning.

ISO/IEC 27001, on the other hand, is an internationally recognised standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive corporate information and aims to ensure its confidentiality, integrity, and availability. Although ISO/IEC 27001 is not specifically designed for industrial environments, it still provides valuable guidelines that can be applied in these contexts.

By combining both standards, companies can develop a holistic security strategy that considers the specific requirements of industrial systems and the general principles of information security management.

Scientific research and innovation in this area are essential to keeping pace with constantly evolving threats. New technologies and approaches need to be developed and tested to continuously improve the effectiveness of security measures. It is, therefore, vital that scientists, engineers, and security experts work closely together to develop innovative solutions that ensure the protection of industrial facilities against cyber threats.

To summarise, securing industrial facilities against cyber threats is one of the critical challenges of our time. IEC 62443-x and ISO/IEC 2700x provide valuable tools to meet this challenge, and continuous research and innovation in this area are crucial to ensure the security and resilience of industrial systems.

ISO/IEC 2700x series of standards

The ISO/IEC 2700x series of standards is a series of sixty sub-standards on information security management systems (ISMS). The most important of these are ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, and ISO/IEC 27019.

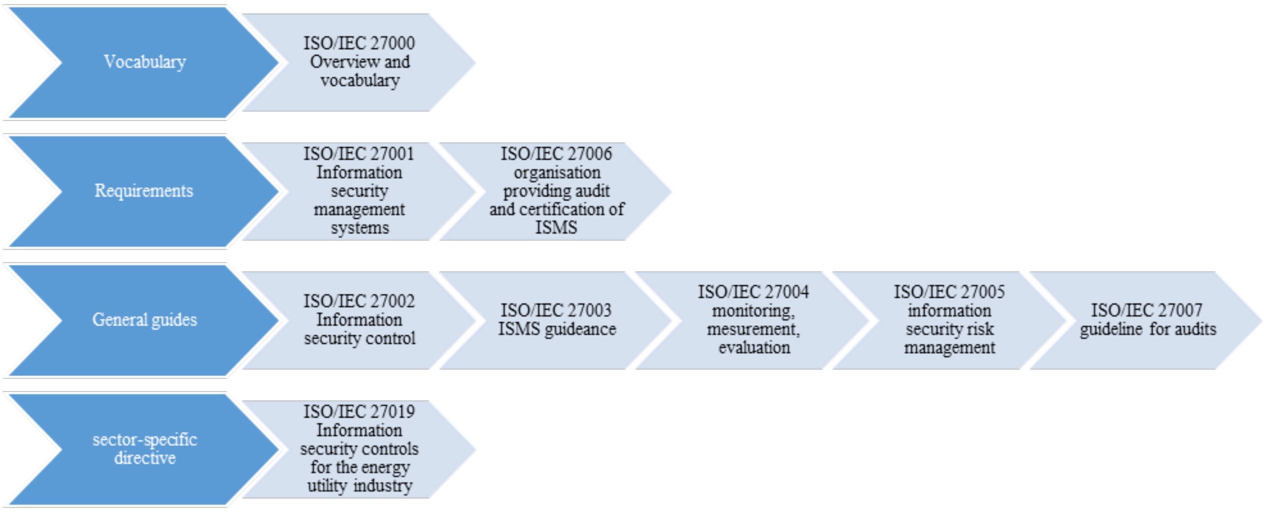
Vocabulary
ISO/IEC 27000 Overview and vocabulary
Requirements
ISO/IEC 27001 Information security management systems
ISO/IEC 27006 organisation providing audit and certification of ISMS
General guides
ISO/IEC 27002 Information security control
ISO/IEC 27003 ISMS guideance
ISO/IEC 27004 monitoring, mesurement, evaluation
ISO/IEC 27005 information security risk management
ISO/IEC 27007 guideline for audits
sector-specific directive
ISO/IEC 27019 Information security controls for the energy utility industry

Fig. 1. Extract from the structure of the ISO/IEC 2700x series of standards (Kroeselberg 2017)

ISO/IEC 27000 first explains the technical terms used and then provides an overview of the other standards in the series. The series of standards deals with the establishment of an information security management system (ISMS). The standard focuses on information security to ensure the availability, integrity, and confidentiality of information (ISO/IEC 27000 2018).

ISO/IEC 27001 defines requirements for ISMS. It specifies the requirements for introducing, implementing, operating, monitoring, reviewing, maintaining, and improving formalised information security management systems (ISMS) about an organisation's overarching business risks. The content includes, among other things, the organisation's context, management leadership and commitment, the company's security policy, the organisation's responsibilities and authorities, and measures for dealing with risks and opportunities, including the improvement processes (ISO/IEC 27001 2022).

ISO/IEC 27002 is a guide for implementing information security measures. It provides specific advice and best practice guidance on implementing measures specified in ISO/IEC 27001. These include, for example, the assignment of access rights, user management, access management, password management, data carrier disposal, physical security perimeter, protection against malware, and data backup (ISO/IEC 27002 2022).

ISO/IEC 27003 guides the requirements for an information security management system (ISMS) specified in ISO/IEC/IEC 27001 and gives recommendations and explanations for better understanding (ISO/IEC 27003 2017).

ISO/IEC 27004 guides to help organisations evaluate the ISMS's information security performance and effectiveness to meet the requirements of ISO/IEC 27001. It addresses the monitoring and measurement of information security performance, the monitoring, the measurement of the effectiveness of an information security management system, including the processes and measures, and the analysis and the evaluation of the results of the monitoring and measurements (ISO/IEC 27004 2016).

ISO/IEC 27005 contains guidelines for the risk management of information security. In addition to supporting the general ideas outlined in ISO/IEC 27001, its goal is to facilitate the application of risk-based information security. To fully comprehend, one must be familiar with the concepts, models, procedures, and jargon covered in ISO/IEC 27001 and ISO/IEC 27002. This document pertains to all categories of organizations (such as for-profit businesses, government agencies, and nonprofits) that plan to manage risks that could jeopardize their information security. (ISO/IEC 27005 2022).

The requirements outlined in ISO/IEC 27001 provide guidance to organizations that must manage an ISMS audit program or conduct internal or external audits of an ISMS. An audit can be conducted against several audit criteria, for example, the requirements defined in ISO/IEC 27001; policies and requirements specified by relevant interested parties; legal and regulatory requirements; ISMS processes and controls defined by the organisation or other parties; and plans for achieving information security objectives (ISO/IEC 27007 2020).

ISO/IEC 27019 is of interest in the context of automation technology. This provides guidance based on ISO/IEC 27002 and is applied to process control systems used by the energy supply industry to control and monitor the production or generation, transmission, storage and distribution of electrical energy, gas, oil, and heat, and to control the associated supporting processes. Nuclear facility process control is not covered by ISO/IEC 27019. ISO/IEC 27019 also includes adapting the risk assessment and handling processes described in ISO/IEC 27001 to the energy utility sector (ISO/IEC 27019 2017).

IEC 62443 series of standards

Based on the models and requirements of the ISO 2700x series of standards, the IEC 62443 series of standards considers the special requirements of IT security in the production sector. Figure 2 shows the structure of the standard series.

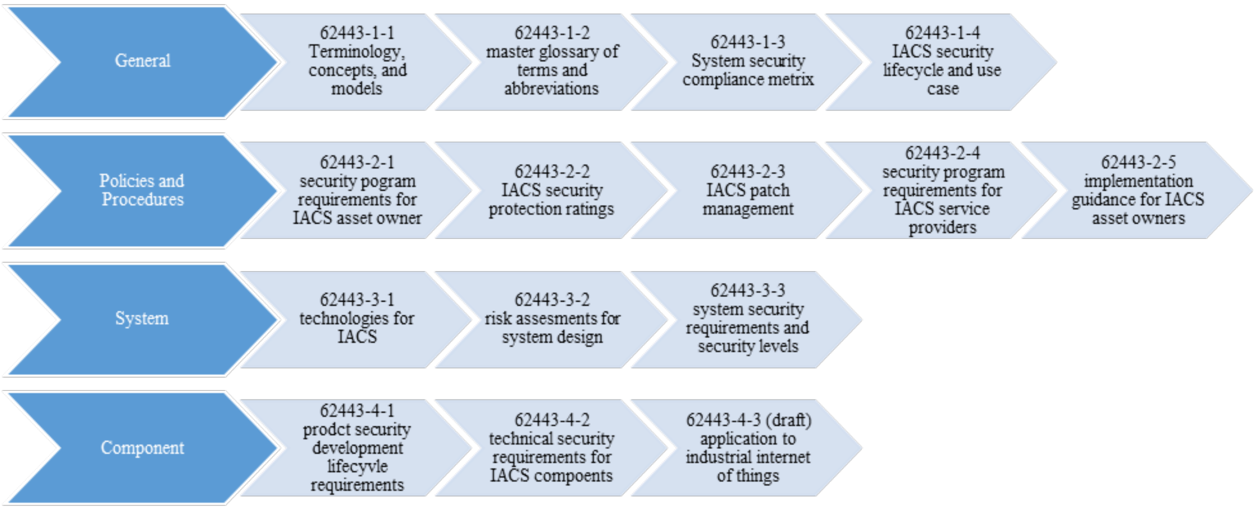
General
62443-1-1 Terminology, concepts, and models
62443-1-2 master glossary of terms and abbreviations
62443-1-3 System security compliance metrix
62443-1-4 IACS security lifecycle and use case
Policies and Procedures
62443-2-1 security pogram requirements for IACS asset owner
62443-2-2 IACS security protection ratings
62443-2-3 IACS patch management
62443-2-4 security program requirements for IACS service providers
62443-2-5 implementation guidance for IACS asset owners
System
62443-3-1 technologies for IACS
62443-3-2 risk assesments for system design
62443-3-3 system security requirements and security levels
Component
62443-4-1 prodct security development lifecyvle requirements
62443-4-2 technical security requirements for IACS compoents
62443-4-3 (draft) application to industrial internet of things

Fig. 2. Extract from the structure of the IEC 62443 series of standards (DKE, 2020)

IEC/TS 62443-1-1 is a technical specification that defines the terminology, concepts and models for *the* security of industrial automation and control systems (IACS). It forms the basis for the other standards in the IEC 62443 series, and its components include risk assessment, the maturity level of the security programme, policies, models, and reference architecture (IEC/TS 62443-1-1 2009).

IEC/TR 62443-1-2 defines all the terms used in the technical standards (IEC/TR 62443-1-2 2010). IEC/TS 62443-1-3 defines the metrics for evaluating IT security in technical specification (IEC/TS 62443-1-3 2014), and IEC 62443-1-4 describes the security lifecycle and use cases (IEC 62443-1-4 2018).

OPERATORS AND SERVICE PROVIDERS

IEC 62443-2-1 describes the requirements for an IT security management system, including the definitions of security procedures, risk management, training requirements, business continuity plans, access control, and the improvement process (IEC 62443-2-1 2024).

IEC 62443-2-2 guides how and in which areas these procedures will be implemented. It specifies a framework for evaluating the protection of an IACS. It contains a method for combining the evaluation of organisational and technical security measures in numerical values, the so-called "protection level" (IEC-62443-2-2 2020). The framework forms the structure for evaluating the defence-in-depth strategy of the IACS in operation based on the technical and organisational requirements specified in other documents of the IEC 62443 series of standards (DKE 2020).

IEC/TR 62443-2-3 is dedicated to updating the software of automation systems for technical standards. Patching is critical because improper procedures can lead to malfunctions (IEC/TR 62443-2-3 2015).

IEC 62443-2-4 deals with using service providers for commissioning and service from an IT security perspective. It specifies requirements for IT security guidelines, procedures and practices that apply to suppliers of industrial automation systems during the life cycle of their products and to maintenance service providers (IEC 62443-2-4 2023).

IEC 62443-2-5 contains implementation instructions for operators (IEC 62443-2-5 2024). The Processing status of IEC is in planning.

REQUIREMENTS FOR AUTOMATION SYSTEMS

IEC/TR 62443-3-1 first describes the underlying technologies, such as authentication, encryption, filtering and logging for techical standards (IEC/TR 62443-3-1 2009).

IEC 62443-3-2 describes the entire safety analysis process and, based on this, the structuring of a system into zones (isolated areas) and conduits (secured connections between the regions). This is intended to divide an automation system into sub-areas, which are sealed off from each other (IEC 62443-3-2 2020).

IEC 62443-3-3 describes specific requirements for automation systems in the form of foundational requirements. These Foundational Requirements (FR) define the IT security aspects of the system. This part provides concrete instructions for planners and operators of automation systems about specific technical measures and so-called security levels (SL) assigned (IEC 62443-3-3 2013).

Table 1. Security Level based of IEC 62443-3-3, 2013

SL	Description – security level defined
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple mean
3	Protection against intentional violation using sophisticates means
4	Protection against intentional violation using sophisticates means with extended resources

Specifies SL1 (low requirements) to SL4 (high requirements). Depending on the system's protection requirements, the requirements can be selected according to the desired security level (IEC 62443-3-3 2013).

REQUIREMENTS FOR AUTOMATION COMPONENTS

IEC 62443-4-1 defines the development process that must be observed when developing components for automation technology.

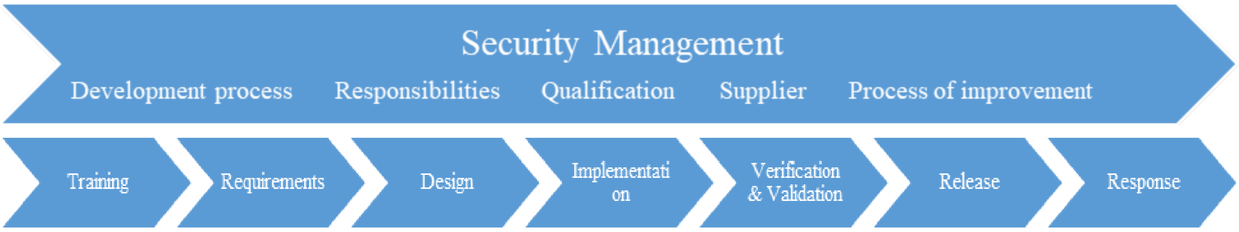

Fig. 3. Secure development life cycle (Waldeck 2020)

Figure 3 shows the secure development life cycle described in the standard. This extends across all phases of the development process. By implementing this standard, manufacturers of automation components can build up the product development life cycle in accordance with the security-by-design approach and thus lay the foundation for component certification. The abbreviations in the grey boxes correspond to the requirement classes from the respective parts of the standard. Maturity levels from 1 to 4 are assigned for an organisation structured in this way.

IEC 62443-4-2 describes the technical requirements for the components of automation systems, applications and functions. The structure of the requirements follows IEC 62443-3-3, but the requirements that the components must fulfil are described here. A distinction is made between component requirements (CR) and further requirements (RE = Requirement enhancements). These requirements are derived from the system requirements (SR). The components of an IACS defined in this document are the software applications, host devices, embedded devices and network components (IEC 62443-4-2 2019).

IEC/TR 62443-4-3 has been published as a technical standard draft and deals with the Industrial Internet of Things (IIoT). It deals with components and products (IEC/TR 62443-4-3 2024).

Assignment of the IEC 62443-x standard parts to the players in the safety process

The operator Service provider is responsible for operating and maintaining a production facility. The guidelines for operation and maintenance are relevant for these actors. The parts of the standard that regulate the structure and operation of the ISMS (IEC 62443-2-1) and the involvement of service providers (IEC 62443-2-4) are relevant here. IEC/TR 62443-2-3, which regulates updating the control system software (patch management), is also appropriate for operators.

The role of the system integrator is to design and install the automation system. IEC 62443-3-3 is relevant here, as it specifies the design and structure of the system. IEC 62443-3-2 can also be used for safety risk assessment and system design. If a service provider carries out the planning process, IEC 62443-2-4, which describes the requirements for service providers, must also be observed. If the system operator carries out the planning work themselves, the standards mentioned in this section also apply to the operator in their role as system planner. The third role is that of the product supplier. IEC 62443-4-1, which specifies the requirements for a secure development process (security by design), initially applies to these suppliers. The requirements for the products developed by the product supplier are described in IEC 62443-4-2 and IEC 62443-4-3, which has been published as a draft.

DELIMITATION OF IT SECURITY STANDARDS

Now that the two series of standards, IEC 62443-x and ISO 2700x, have been described in the previous chapters, a distinction must be made between them regarding their applicability in the production sector. Therefore, these requirements are described below, and the areas of IT (Information Technology and ISO 2700-x) and OT (Operational Technology ans ISO 2700x) are differentiated from each other.

Table 2. Delimitation of the IT and OT domains (Gartner 2024).

Domain	Definition	Application examples
IT	”IT“ is the common term for information processing technologies, including software, hardware, communication technologies and related services. In general, IT does not include embedded technologies as long as they do not generate data for corporate use.	• Client systems for personal • Notebooks • Web server • Mail server • SAP systems • File Server • Networks
OT	Operational technology (OT) is hardware and software that detects or causes a change by directly monitoring and/or controlling industrial devices, systems, processes, and events.	• Programmable logic controllers (SPS) • Display systems (touch panels) • Server for production control • Industrial robots • Remote IO systems • Real-time networks

Information security is defined by ISO/IEC 2700x as guaranteeing the confidentiality, availability, and integrity of data. The term IT security is a sub-aspect of information security. It refers to the protection of technical systems. The term “cyber security” or “ICS security” is often used for production systems (BSI, 2014). This focuses on the security of production systems (OT). The term data protection is only mentioned here for the sake of completeness but has no relevance here. The different areas of application of IT and OT also result in different requirements in terms of IT and OT security.

CONCLUSION

The ISO/IEC 2700x series describes the structure and operation of an IT security management system (ISMS). The series of standards addresses information security in general and does not differentiate between data in IT systems or intellectual property. The ISO/IEC 27001 standard is to be regarded as the basic standard by which essential requirements for IT security, such as planning, responsibilities, risk assessment, communication, resources, and internal audit) are defined. The focus is on the organisational and process-related aspects of IT security. ISO/IEC 27002 defines specific requirements for IT security, such as access control, network security, separation of networks, etc. One focus of the series of standards is monitoring and evaluating the ISMS ISO/IEC 27004 and certification per ISO/IEC 27007. The standard is generic and can be used for IT applications in the same way as for OT. However, the standard makes no specific reference to the requirements of OT. One exception is IEC 27019, which refers to energy supply systems.

The IEC 62443 series focuses on protecting industrial automation systems and is therefore assigned to the area of Operational Technology (OT). Specific features of OT are taken into account. For example, the requirements relating to service providers (IEC 62443-2-4) are considered, as is patch management in production facilities (IEC/TR 62443-2-3). The aspect of setting up and operating an ISMS is also included in the series of standards (IEC 62443-2-1), but the focus is on specific technical requirements for automation systems (IEC 62443-3-3) and the components of automation systems (IEC 62443-4-2), with the latter being aimed at the manufacturers of automation components.

Both series of standards have similarities. The basic concepts and technologies can be found in both series of standards. However, it should be noted that the IEC 62443 series of standards clearly focuses on automation technology, while the ISO/IEC 2700x series is more process-orientated and generic (Kohl 2018).

REFERENCES

BSI (2014). *ICS-Security-Kompendium. Testempfehlungen und Anforderungen für Hersteller von Komponenten*. Bundesamt für Sicherheit in der Informationstechnik [viewed 30 August 2024]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf?__blob=publicationFile.

DKE (2020). *Elektronik Informationstechnik DIN und VDE EC 62443*. Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. Deutsche Kommission Elektrotechnik [viewed 30 August 2024]. Available from: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

Gartner (2024). *Glossary Information Technology* [viewed 30 August 2024]. Available from: https://www.gartner.com/en/information-technology/glossary?glossaryletter=I.

IEC/TS 62443-1-1 (2009). *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. International Electrotechnical Commission.

IEC/TR 62443-1-2 (2010). *Security for industrial automation and control systems – Master Glossary*. International Electrotechnical Commission.

IEC/TS 62443-1-3 (2014). *Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics*. International Electrotechnical Commission.

IEC 62443-1-4 (2018). *Security for industrial automation and control systems Life Cycle and Use Cases.* International Electrotechnical Commission.

IEC 62443-2-1 (2024). *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.* International Electrotechnical Commission.

IEC-62443-2-2 (2020). *Security for industrial automation and control systems – Part 2-2: IACS security program rating.* International Electrotechnical Commission.

IEC/TR 62443-2-3 (2015). *Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment.* International Electrotechnical Commission.

IEC 62443-2-4 (2023). *Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for IACS solution suppliers.* International Electrotechnical Commission.

IEC 62443-2-5 (2024). *Implementation guidedance for IACS asset owners.* International Electrotechnical Commission, not released [viewed 30 August 2024]. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

IEC/TR 62443-3-1 (2009). *Industrial communication networks – Network and system security – Part 3-1: Security*

technologies for industrial automation and control systems. International Electrotechnical Commission.
IEC 62443-3-2 (2020). *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design.* International Electrotechnical Commission.
IEC 62443-3-3 (2013). *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.* International Electrotechnical Commission.
IEC 62443-4-1 (2018). *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.* International Electrotechnical Commission.
IEC 62443-4-2 (2019). *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.* International Electrotechnical Commission.
ISA/TR 62443-4-3 (2024). *Security for industrial automation and control systems – Part 4-3: Application to industrial internet of things.* International Electrotechnical Commission.
ISO/IEC 27000 (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary.* International Standardization Organization.
ISO/IEC 27001 (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* International Standardization Organization.
ISO/IEC 27002 (2022). *Information security, cybersecurity and privacy protection – Information security controls.* International Standardization Organization.
ISO/IEC 27003 (2017). *Information technology – Security techniques – Information security management systems – Guidance.* International Standardization. Organization. International Standardization Organization.
ISO/IEC 27004 (2016). *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation.* International Standardization Organization.
ISO/IEC 27005 (2022). *Information security, cybersecurity and privacy protection – Guidance on managing information security risks.* International Standardization Organization.
ISO/IEC 27006 (2024). *Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems.* International Standardization Organization.
ISO/IEC 27007 (2020). *Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing.* International Standardization Organization.
ISO/IEC 27019 (2017). *Information technology – Security techniques – Information security controls for the energy utility industry.* International Standardization Organization.
Kohl, A., C. **Bisale** (2018). *Effektive und effiziente Security auf Basis internationaler Standards.* In np, 9, S. 12–14.
Kroeselberg, D., F. **Buchi,** H. **Meulenbroek** (2017). *Cyber Security Tutorial Energy Automation and IEC 62443* [viewed 30 August 2024]. Available from: https://www.pcic-library.com/sites/default/files/final/EUR17_63.pdf.
Waldeck, B. (2020). *Zertifizierter Entwicklungsprozess nach 62443-4-1* – Security by design, Online Seminar, Lemgo.

КИБЕРСИГУРНОСТ И ИНФОРМАЦИОННА СИГУРНОСТ

Резюме: *През последните десетилетия прогресивната цифровизация на промишлените предприятия и свързването им в мрежа доведоха до значително повишаване на ефективността и до иновации. В същото време обаче това развитие увеличи значително и полето на атаките за киберзаплахи. Промишлените предприятия, които преди бяха до голяма степен изолирани и защитени с физически мерки за сигурност, сега са част от сложни, глобално свързани в мрежа системи. Това ги прави уязвими за различни кибератаки от страна на престъпни организации и държавни субекти. За да се отговори на тези предизвикателства, са разработени множество стандарти за укрепване на киберсигурността в индустриалната среда. Два от най-важните и широко използвани стандарти са сериите IEC 62443-x и ISO/IEC 2700x. Серията ISO/IEC 2700x описва създаването и функционирането на система за управление на информационната сигурност (СУИС). Тази серия стандарти се занимава със сигурността на информацията и не прави разлика между данните в ИТ системите и интелектуалната собственост. Серията IEC 62443-x се фокусира върху защитата на системите за индустриална автоматизация и поради това е отнесена към областта на оперативните технологии.*

Ключови думи: *информационна сигурност, киберсигурност, речник, изисквания, насоки*

Д-р Марк Дийтц
Университет по библиотекознание и информационни технологии
E-mail: mark-dietz@gmx.net