White paper

IEC 62443 – the success factor for holistic security concepts

Protection against cyberattacks and compliance with new legal requirements

Find out more about:

- → Implementing cybersecurity in automation
- → The new legal directives NIS 2, CRA, and the new Machinery Regulation
- → The 360° security concept

PHOENIX CONTACT

Introduction

Can components and systems certified in accordance with IEC 62443 provide comprehensive protection against cyberattacks and at the same time meet EU legal requirements, such as NIS 2, the Cyber Resilience Act (CRA), and the new Machinery Regulation?

The digitalization and networking of production, product, and customer data are the decisive factors for increasing the added value of companies and thus a basis for the economic development of global regions.

The EU Commission recognized this and published the EU Cybersecurity Strategy back in December 2020. This strategy defines the requirements for resilience and attack blocking for manufacturers of components and systems as well as for all major manufacturing companies.

The international IEC 62443 series of standards sets out basic requirements for avoiding security risks for component manufacturers, system integrators, and operators. It is the leading standard for implementing security-by-design in products and systems.

"IEC 62243 is a success factor for compliance with current cybersecurity directives".

Boris Waldeck, Master Specialist Security PLCnext Technology

Contents

1 Added value as a goal

Increasing digitalization and networking increase the attack area for cyberattacks. In addition, the attackers and the attack methods are becoming increasingly professional. The aim of cybersecurity is to safeguard a company's added value and individual security goals. This includes, among other things, protecting know-how – for example, development results or contract terms – and complying with legal regulations, such as those relating to data protection.

In manufacturing companies, production and delivery capabilities are obviously important. Beyond these specific attack damages, there are other damages that are often underestimated beforehand.

For example, cyberattacks often lead to damage of the company's image as well, as they can affect how confident customers, partners, investors, and the public are in the affected company. Legal requirements for the implementation of cybersecurity have long been established for critical infrastructures, and are now being extended by the EU to many other companies through the NIS 2.0 directive.

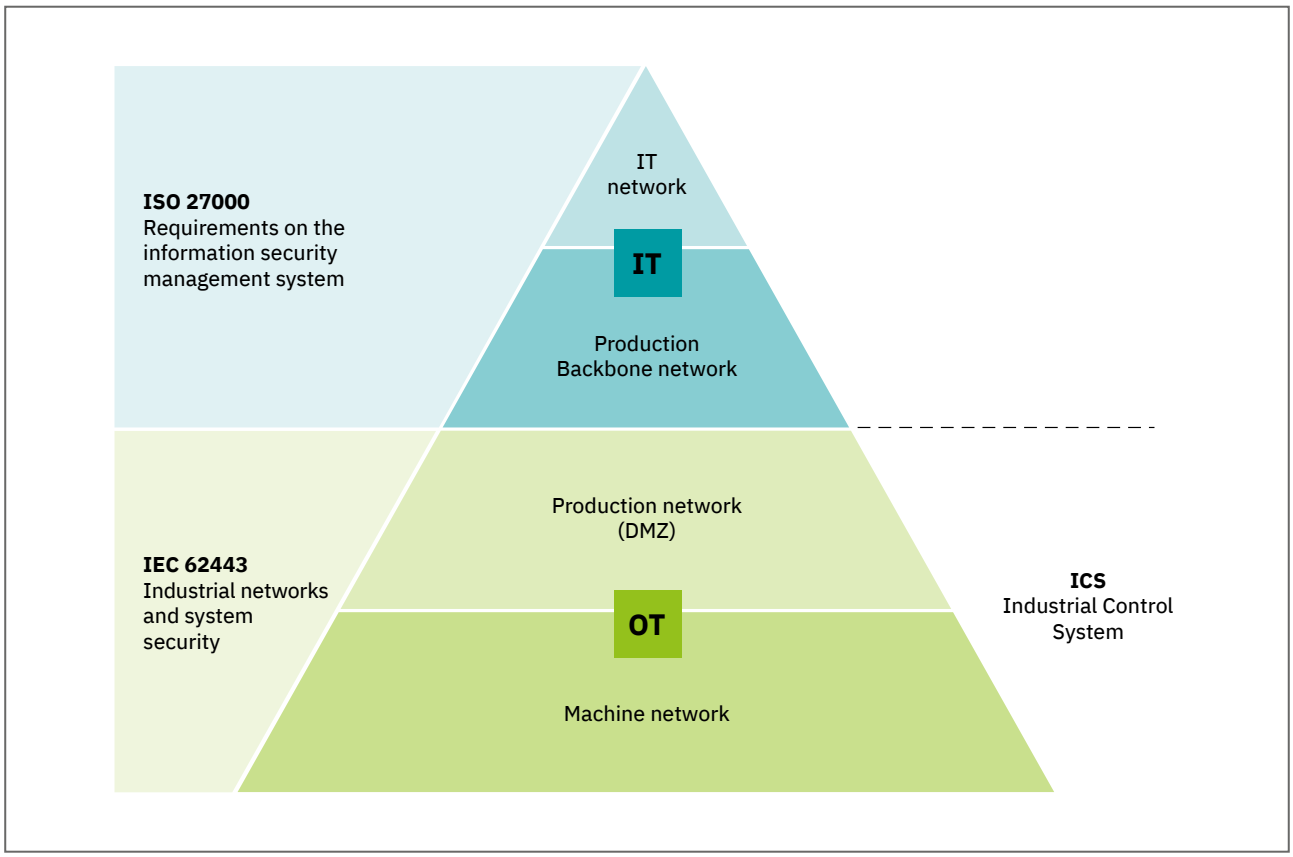
Securing added value is the primary goal of cybersecurity.

2 Implementation in automation

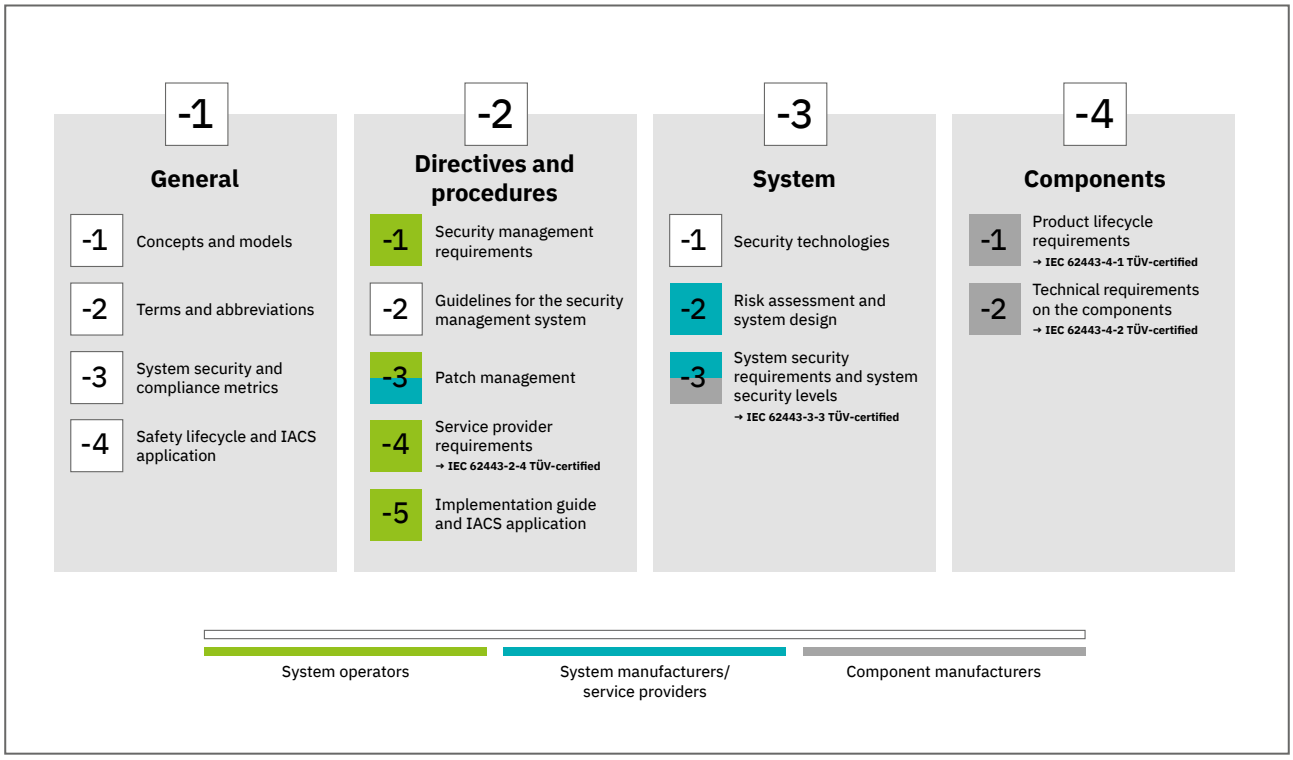
A company's security is rooted in two worlds: IT (information technology) and OT (operational technology). To protect both worlds, an information security management system (ISMS) in accordance with ISO 27001/2 is being introduced in IT, which is being expanded towards OT. The requirements of an ISMS include both technical and organizational requirements. Using IEC 62443-2-1, the technical requirements can be referenced to measures in OT, the industrial automation control system (IACS) environment. IEC 62443 therefore supplements the ISO 27001 standard. Together, the two standards provide a holistic approach to protecting against cyber threats.

Measures described in the IEC 62443 series of standards include:

- Configuration and segmentation of the networks
- Protection of data during storage and transmission
- Authentication of users
- Monitoring and logging the actions of users and systems
- Security hardening of the devices used
- Configuration, updates, backup, and restoring
- Organizational requirements for managing the system



Cybersecurity in IT and OT



Structure of IEC 62443

The specific measures of IEC 62443 are addressed for different perspectives:

Components

4-1 Secure process for the development and life cycle of components (products)
4-2 Security requirements for components

System

3-3 Security requirements for systems

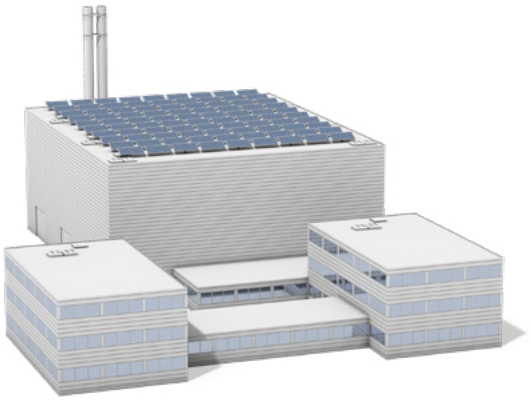
Operators

2-1 Security management system
2-3 Patch management
2-4 Security requirements on system integrators (service providers)

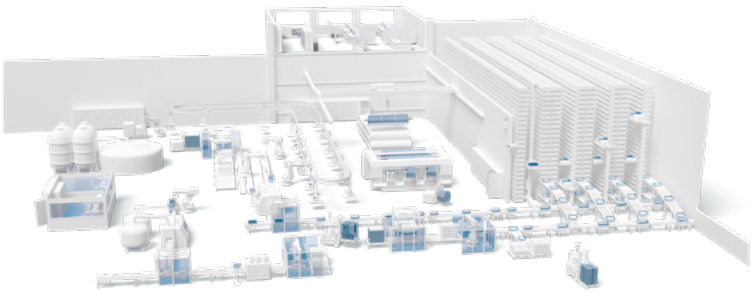
The special element of IEC 62443 is the comprehensive security-by-design approach, which ranges from requirements for the operating processes to requirements on the systems and products, right, and describes both procedural and technical measures and requirements.

One key security concept of the IEC 62443 is “defense-in-depth”, whereby the staggering multiple security mechanisms one after the other makes things more difficult for attackers. For instance, in order to launch an attack over the network, the attacker would first have to overcome one or more firewalls before reaching the target component. There, a user login must then be overcome, only to be stopped by internal security mechanisms.

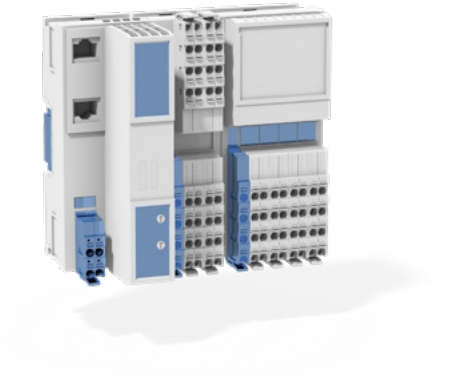
Defense-in-depth



Corporate level:
- Physical measures
- Authorization concept (entry, admission, access)
- Awareness training
- ISMS processes



Network level:
- Network segmenting (zones, conduits)
- VPN
- Encryption
- Firewalls
- Attack detection



Product level:
- Security features
- System hardening
- “Security-by-design” components

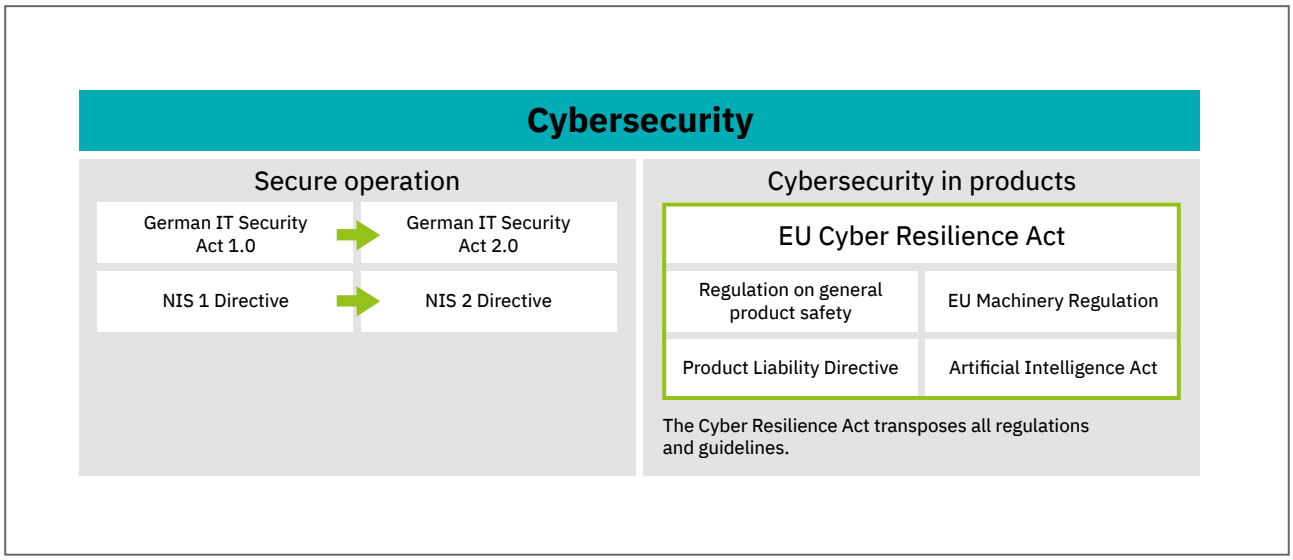
3 Legal directives

Cybersecurity measures were previously only required by law for critical infrastructures and were also implemented by large, mostly internationally active system operators. With the EU's new NIS 2 directive, this is now changing significantly.

NIS 2 directive

The European NIS 2 (Network and Information Security) directive requires operators of public or private entities to implement appropriate security tools to protect their systems from cyberattacks. Compared to the existing NIS 1, it extends the regulations to companies with more than 50 employees and more than 10 million euros in sales. It applies to essential and important facilities in the EU. The term "essential facilities" includes companies operating in critical infrastructure, such as electricity/gas generation, storage and transmission, transportation on water, road and rail, drinking water and wastewater facilities as well as digital infrastructure. The major facilities are selected from a list of seven sectors based on their criticality to their business sector and type of service. Examples include the production and distribution of food and chemicals, and the production of electrical equipment, machinery, and vehicles.

The NIS 2 directive came into force on January 16, 2023, and must be transposed into national law by EU states by October 18, 2024.
However, it is difficult to meet these requirements if the products installed have not been developed in accordance with security-by-design. The Cyber Resilience Act (CRA) was defined by the EU to address this challenge.



Overview of the new legal directives

Cyber Resilience Act (CRA)

The CRA requires manufacturers to develop security-by-design products. Products subject to the CRA will not receive a CE mark in the future if they do not with the legal regulations. Minimum security requirements are defined for the implementation of security measures. Depending on the product class, they must be verified by a product conformity test by notified bodies, such as TÜV, or by the manufacturers themselves using a harmonized standard.

The essential requirements of the CRA must be taken into account in the design, development, and manufacture – in other words, based on a secure development process. Requirements include access protection, protection of confidentiality, integrity, and availability, and a secure delivery state.
An additional component is vulnerability management and regulations governing the period during which manufacturers must provide security updates for their products. The draft text of the CRA was published in September 2022. The corresponding trilogue votes have been completed. As an EU ACT, it does not have to be transposed into national law, but is valid after publication in the Access the Official Journal. The implementation of NIS 2 is expected to be mandatory by 2027.

The IEC 62443 group of standards covers both the required secure development process and the technical requirements for individual products and systems. It follows that IEC 62443 or a derived sector standard is a promising candidate for a CRA harmonized standard.
To meet vulnerability management requirements, it is important that a standardized software bill of materials (SBOM), a list describing all software components of a product, is available for all products. In addition, the known vulnerabilities must be available in a standardized digital format such as the Common Security Advisory Framework (CSAF). This is the only way to ensure compliance with reporting deadlines and the elimination of vulnerabilities.

EU Machinery Regulation (MVO)

To protect people and the environment from negative consequences, such as injury or contamination, machines with functional safety technology must comply with Machinery Directive 2006/42/EC. This standard requires an update, as the risks of new technologies and new product safety regulations must be taken into account. In addition, it has become apparent that the directive (transposition into national law) requires different regulations in part. The subject of functional safety in combination with cybersecurity must also be taken into account in the future. These requirements gave rise to the Machinery Regulation 2023.

The MVO is a supplement to the CRA, which also sees machines as a product. For machines with functional safety, however, the MVO takes precedence.

4 Implementation of cybersecurity at Phoenix Contact

Phoenix Contact began implementing IEC 62443 in 2017. The "360° security concept" was established, which implements the guiding principle "Security is anchored in the entire life cycle of our products and solutions".

Secure development process

The secure development process in accordance with IEC 62443-4-1 is the prerequisite for development and the complete life cycle of the products. It defines the development in accordance with the established cybersecurity methods security-by-design and defense-in-depth, but also ensures the monitoring of vulnerabilities and regular security updates.

Secure products

Secure products are developed in accordance with the 4-1 development process and fulfill the functional security requirements of 4-2. These are, for example, protection against DDoS attacks (Distributed Denial of Service), user management, confidentiality of data during transmission, and storage. In 2021, PLCnext Control became the first controller on the market to be certified in accordance with the IEC 62443-4-1 ML3 / 4-2 SL2 Feature Set. Other secure products are currently under development or being certified.

Further information on the products →

Phoenix Contact has implemented IEC 62443-compliant cybersecurity

PLCnext Control: IEC 62443-certified safety and security

As part of the 360° security concept, PLCnext Control became the first controller on the market to be certified by TÜV SÜD in accordance with the IEC 62443-4-1 ML3 / 4-2 SL2 Feature Set. Further PLCnext Controls are continuously being added to this certification. For example, this certification was extended in 2022 to include the functionally safe devices from the PLCnext Control family.

The IEC 62443 certification of the PLCnext Control includes extensive security functions:

- Security profile as the configuration of the least functionality
- Firewall and network segmentation as well as monitoring and limiting the network load
- TLS security for access-secure communication
- Certificate management for asymmetric cryptography and key management
- User administration, role-based locally, and connection to central user management systems
- Event logging systems with local and central connection
- PSIRT automatically monitors known vulnerabilities in the software components used and publishes security advisories
- Device and update management app as central management of the devices for security updates (firmware and application) as well as the management of backups and restores
- SBOM in a standardized format and digital security advisories in accordance with the Common Security Advisory Framework (CSAF) are in preparation

The certified range of functions is documented in the PLCnext Security Info Center.

→ **Find out more:**
phoenixcontact.com/security-infocenter

mGuard security router: powerful protection for industrial networks

With comprehensive security functions, the mGuard security routers protect industrial networks against unauthorized access or malware. The proven mGuard security technology enables communication within the machine or production network to be controlled and secured. The products are a part of our comprehensive 360° security concept.

The industrial routers were developed in line with the certified development process in accordance with IEC 62443-4-1 ML3 and have extensive security functions:

- Intelligent firewall with various functions depending on the application:
  - Conditional firewall
  - DNS name-based firewall
  - User firewall
  - Firewall redundancy
  - Router with NAT and 1:1 NAT
- IPsec VPN functionality:
  - Certificate-based
  - Switchable via I/Os
- Local and centralized (RADIUS) user management configuration
- Local and centralized security logging
- NTP: network-wide time synchronization
- Device and update management with the mGuard Device Manager
- System usage notification

The cybersecurity of PLCnext Control can be systemically supplemented by the well-known mGuard technology. Depending on the application and risk analysis of the system, additional devices can be used for segmentation, as an additional firewall, or to secure access via VPN (e.g., remote maintenance or cloud access). The interaction of both solutions makes sense for the holistic protection of system or machine networks.

Further information on the mGuard security routers

→ **Find out more:**
phoenixcontact.com/mguard

Secure services

In order to discuss, advise, install, and maintain security solutions together with system integrators and operators, the teams must possess and demonstrate the appropriate cybersecurity skills. The corresponding teams, also in selected Phoenix Contact subsidiaries, are certified in accordance with IEC 62443-2-4.

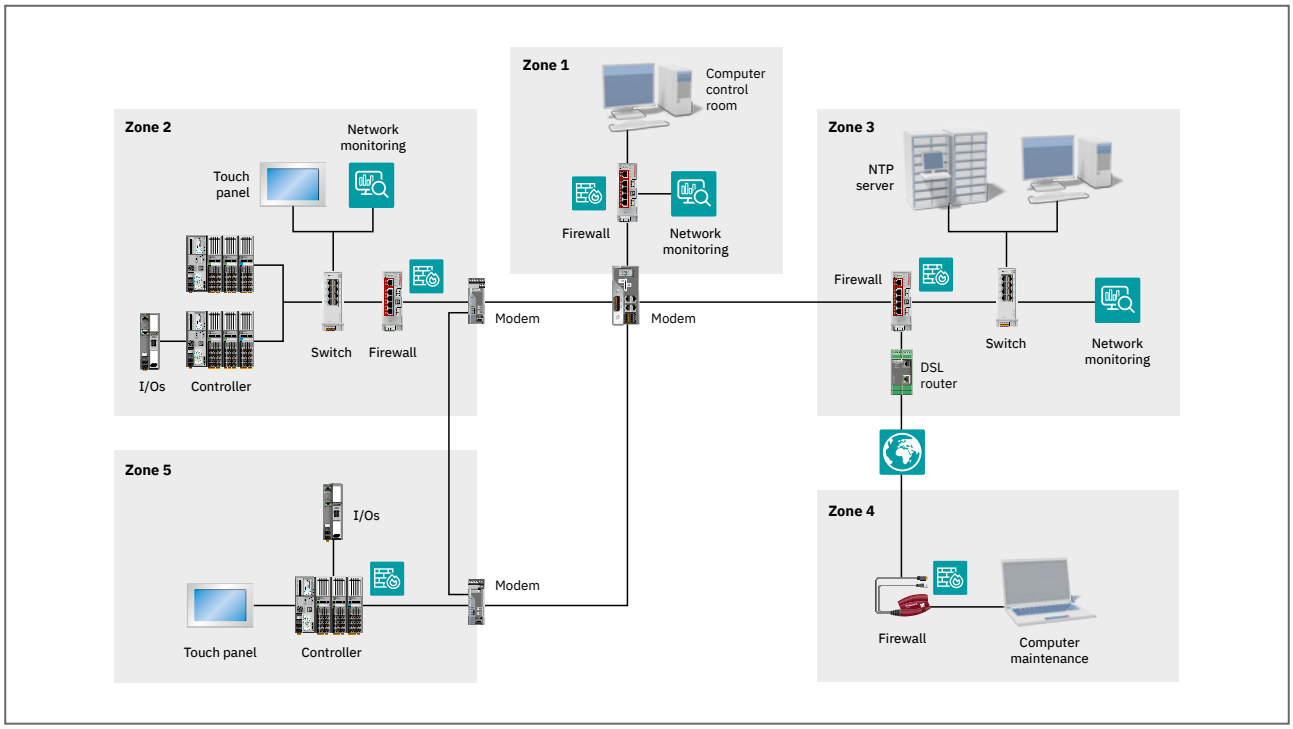
Secure solutions

Templates (blueprints) have been developed for different solutions and markets and, where appropriate, certified in accordance with IEC 62443-3-3. On the one hand, they facilitate discussion and concept work and, on the other, they demonstrate Phoenix Contact's expertise in certifying solutions with customers.

PSIRT

The Product Security Incidence Response Team (PSIRT) is the central team tasked with responding to potential security vulnerabilities, incidents, and other security issues related to Phoenix Contact products, solutions, and services. The PSIRT manages the disclosure, investigation, and internal coordination and publishes security advisories on confirmed vulnerabilities.

The above certifications are all monitored by TÜV SÜD through annual audits.

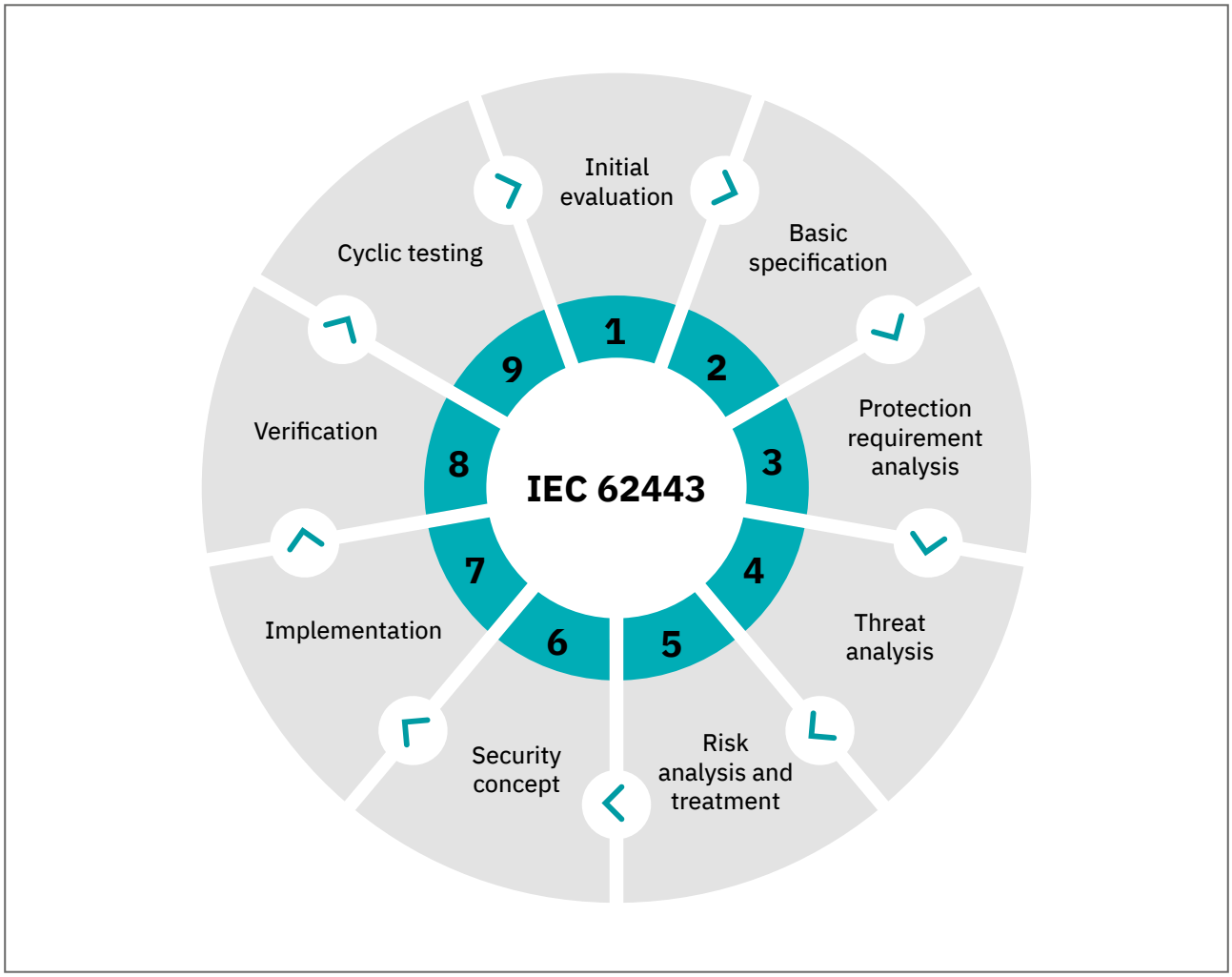


Our "Remote Monitoring and Control" blueprint certified by TÜV SÜD in accordance with IEC 62443-3-3

5 Summary: Phoenix Contact as your partner for cybersecurity

The NIS 2, the CRA, and the MVO are currently in the EU legislative process or being transposed into national law. If the typical transitional periods are applied, they are all expected to be fully applicable law in 2027. Considering the complexity of cybersecurity standards and laws, it quickly becomes clear that there is an urgent need for action on the part of product manufacturers, system integrators, and operators alike.

Phoenix Contact is well positioned with its many years of experience with the 360° security concept and, in addition to its products and systems, also offers operators and system integrators services in accordance with IEC 62443 for the design and operation of systems.
The 360° security concept begins with the "Nine steps to a secure system" approach, which enables system integrators and operators to fulfill security-by-design for their specific solution.



360° industrial security: Nine steps to a secure system

Security-by-design automation solutions in accordance with IEC 62443 must follow a strict process model. These are defined below in the “Nine steps to a secure system”:

1 Initial evaluation:
Recording of system information to identify the operating environment

2 Basic security specification:
Planning of basic measures for basic protection of the system

3 Protection requirement analysis:
Determination of the need for protection to safeguard assets worthy of protection

4 Threat analysis:
Identification of relevant threats to the automation solution

5 Risk analysis/management:
Preparation of a risk assessment including derivation of a catalog of measures

6 Security concept:
Finalization of an individual and comprehensive security concept

7 Implementation:
Implementation of the security concept – from theory to practice

8 Verification:
Checking the implementation in accordance with the defined security concept specifications from step 6

9 Cyclic testing:
Staying up-to-date – from the security concept through to expertise

Contact

Are you prepared for the new legal directives?

We will help you to implement the new requirements of the legal directive for your company and protect yourself against cyberattacks.
Together we will implement a 360° security concept for you!

For more information, visit:
phoenixcontact.com/cybersecurity

Boris Waldeck
Master Specialist Security PLCnext Technology
bwaldeck@phoenixcontact.com

Andreas Fuß
Product Marketing Network Security
afuss@phoenixcontact.com

3011401267