Industrial Security

PILZ
THE SPIRIT OF SAFETY

A guideline for manufacturers and operators of machinery
on dealing with current EU legislation

White paper
Version: April 2025

Disclaimer

Our white paper has been compiled with great care. It contains information about the current Pilz interpretation of the new EU Machinery Regulation, the NIS 2 Directive and the Cyber Resilience Act. All details are provided in accordance with the current state of knowledge and interpretation and to the best of our knowledge and belief. While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular, it should be noted that statements do not have the legal quality of assurances or assured properties. We are grateful for any feedback on the contents.

Copyright

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany

2nd revised edition

At a glance

The term Industrial Security has many facets. In this guideline, the most important aspects for machine manufacturers and operators are described. It is important to facilitate the introduction of both manufacturers and operators to the subject so that they are able to understand and manage the new requirements.

The guideline describes the legal situation in Europe, gives an overview of the technical foundations, describes the most important points for machine manufacturers and for machine operators and refers to follow-up options for our customers.

In Europe in recent months, numerous extensive legal texts have been published which have a direct impact on mechanical engineering:

- The **Machinery Regulation** (EU) 2023/1230 sets new requirements for machinery such as protection against corruption.
- The **EU Directive on measures for a high common level of cybersecurity** across the Union (NIS 2) 2022/2555 stipulates an Information Security Management System for many companies.
- The **Cyber Resilience Act** (EU) 2024/2847 defines requirements for products with digital elements, which also includes machinery.

When implementing the legislation, certain standards and terms are of key significance:

- The family of standards **IEC 62443** has been established on the topic of Information Security in the industrial environment.
- The **Security Level** from 0 to 4 describes the abilities of the attacker.
- Industrial Security is an ongoing task, which is why organisational measures are essential in addition to the technical measures. An **Information Security Management System** (ISMS) helps here and is mandatory for many companies.

Machine manufacturers are subject to a number of legal requirements and must navigate between the specifications of operators and the products offered by component manufacturers. The machine manufacturer will be required to take on a mediating role here to continue to be able to offer compliant and high-quality products.

The operators of machinery will also have to think about how to best secure their machinery in future. To gain an overview, a recommended course of action is to perform a systematic risk analysis and efficiently shore up any vulnerabilities.

Pilz GmbH & Co. KG offers advanced training and services on this topic.

The author

Matthias Kuczera completed his studies in Mechanical Engineering, after which he gained an extensive understanding of Machinery Safety in different industrial sectors.

As a development engineer for sensors, he has far-reaching knowledge about the options for implementing functional safety requirements.

During his work as a technical expert in the area of materials handling, he was responsible for the performance of type examinations of safety components at a notified body.

In his current role of technical expert for “Functional Safety – Standards” at Pilz, he is active in standards committees and supervises standards management.

His tasks include:

- Cooperation in standards committees for Machinery Safety
- Assessment of new legal requirements
- Performance of internal training courses

Pilz – the Spirit of Safety in Digital Automation

With everything we do, we make the world a safer place. As a global supplier of products, systems and services for automation technology, Pilz can look back on a success story that spans more than 75 years: Founded in 1948, today the Pilz Group employs around 2 500 staff in 42 subsidiaries and branches. The Machinery Safety expert, with its headquarters in Ostfildern, creates safety worldwide for human, machine and environment with its complete automation solutions. The portfolio of the technology leader includes sensor, control and drive technology, as well as systems for industrial communication, diagnostics and visualisation. An international range of services with consulting, engineering and training completes the portfolio. The Safety and Security solutions are used in many industries beyond mechanical engineering, such as intralogistics, railway technology or the robotics sector, for example.

Contents

1. The legal situation in Europe

New technologies come with opportunities and risks. The most important innovations in our industry at the moment are the extreme networking of machinery via the Internet of Things, Artificial Intelligence and robotics.

With the networking of companies and machinery, the risk increases that vulnerabilities in information systems are exploited and that economic losses and physical harm occur. For example, cases of successful cyber attacks against companies have risen in recent years, resulting in damages in the billions. Statista.com estimates that around 8.15 trillion dollars in damages were caused globally by cyber attacks in 2023. In Germany alone it was almost 206 billion euros in 2023, or about 5 percent of the gross domestic product.

To reduce the risks, European lawmakers have introduced new sets of rules. For machine construction, these are primarily the Machinery Regulation, the NIS 2 Directive (NIS 2) and the Cyber Resilience Act (CRA). Through these, Industrial Security is mandatory. How to handle existing plant and machinery is described in the Directive 2009/104/EC for safety and health requirements for the use of work equipment.

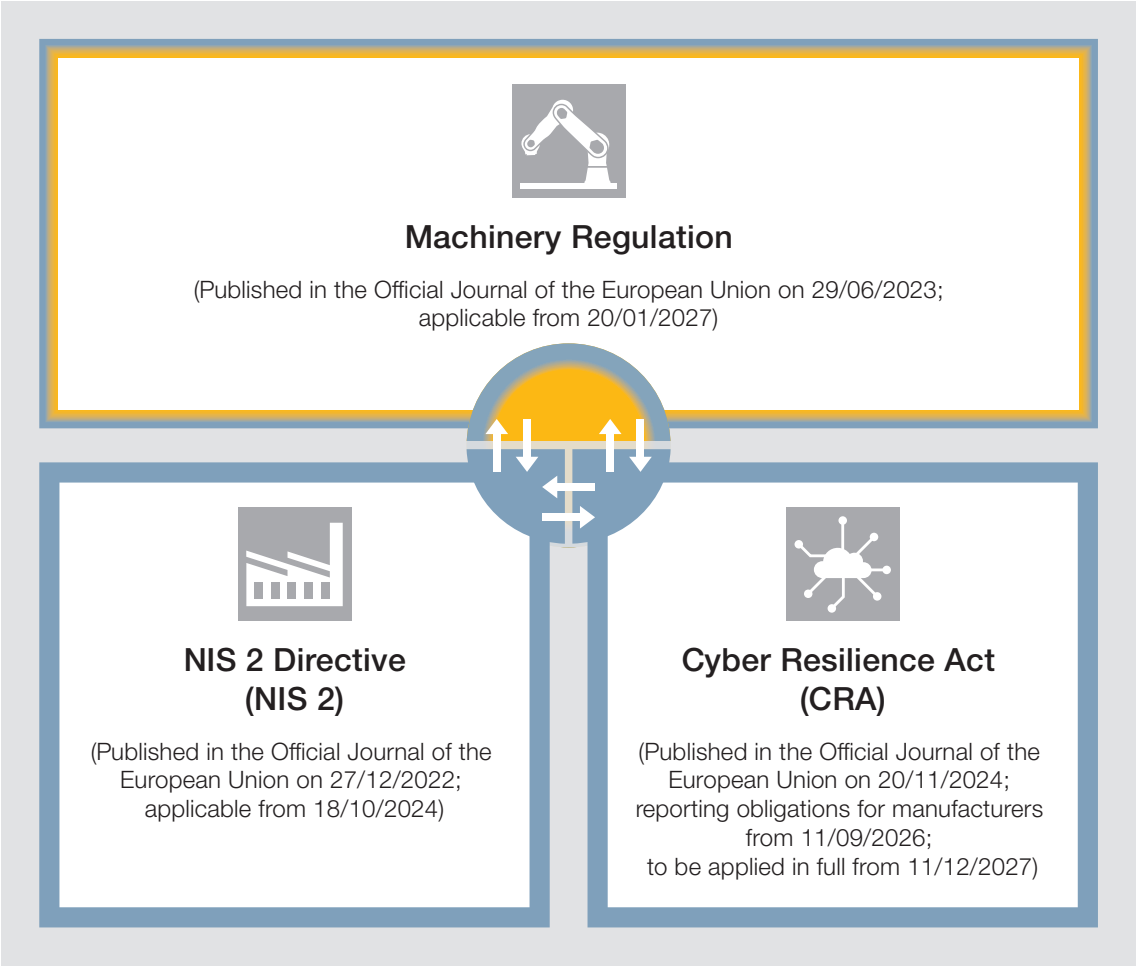

Figure 1: Depiction of an excerpt of new basic legislation that describes the requirements for Industrial Security

	Machinery Regulation (EU) 2023/1230	NIS 2 Directive (EU) 2022/2555	Cyber Resilience Act (EU) 2024/2847
Directed toward	Machinery	Companies	Components
Adopted on	29/06/2023	27/12/2022	20/11/2024
Binding from	20/01/2027	18/10/2024	11/12/2027
Obligations	▸ Protection against corruption (with focus on functional safety functions) ▸ Attention to malicious attempts by third parties	▸ Measures for managing cyber security risks ▸ Compliance with technical and organisational measures ▸ Notification of significant security incidents	▸ Manufacturer reporting obligations from 11/09/2026 ▸ Secure Development Lifecycle Process ▸ EU type examination for critical products ▸ Notification of vulnerabilities ▸ Provision of security updates

Table 1: Comparative overview of Machinery Regulation, NIS 2 Directive and Cyber Resilience Act

1.1. Machinery Regulation (EU) 2023/1230

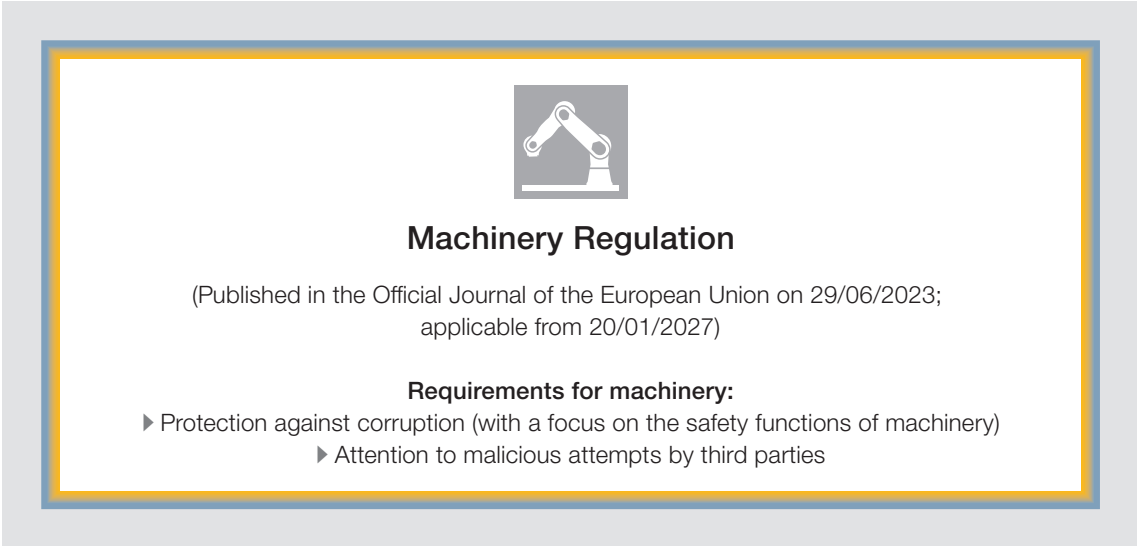

Figure 2: Overview of the Machinery Regulation

The Machinery Regulation (EU) 2023/1230 was adopted in June 2023 and will be binding in all EU states following a transition period of 42 months. It will replace the Machinery Directive 2006/42/EC as of 20 January 2027.

The Machinery Regulation affects manufacturers, importers, dealers and authorised representatives of machinery or associated products. In future, they must confirm that the machinery complies with the Machinery Regulation, including security requirements. This also includes the protection of safety-related control functions against corruption. Manufacturers of machinery must take precautions against risks that could result from the malicious actions of third parties and affect the Machinery Safety. Compliance with the Machinery Regulation is formally confirmed in the Declaration of Conformity and indicated with the CE mark on the machine. Machinery that does not satisfy the requirements of the new Machinery Regulation can no longer be placed on the market in the EU.

Practical tip:
Compared to the Machinery Directive, the topic of security is not the only change in the Machinery Regulation. Other requirements such as dealing with Artificial Intelligence have also been added. Pilz offers a guide to the Machinery Regulation, available to download at: **www.pilz.com/mr**

1.2. The NIS 2 Directive (EU) 2022/2555

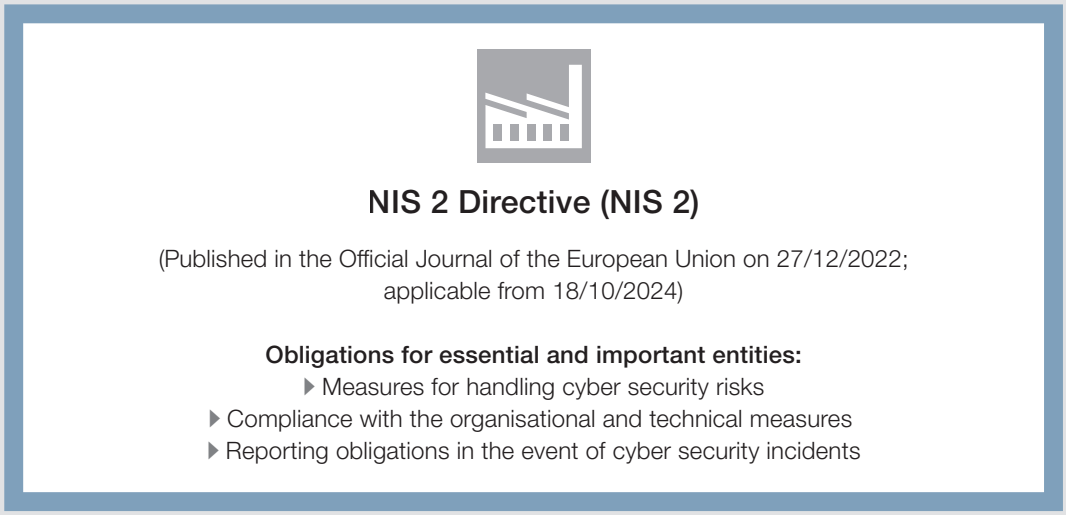

Figure 3: An overview of the NIS 2 Directive

The NIS 2 Directive can be found in the Official Journal of the EU under the name “Directive (EU) 2022/2555 … on measures for a high common level of cybersecurity across the Union … (NIS 2 Directive)”. The abbreviation “NIS” has a historical basis and in general parlance stands for “Network and Information Security”. The NIS 1 Directive primarily applied to critical infrastructures and providers of relevant digital services. The NIS 2 Directive expands the sectors to include the producing trade, among others: Engineering, manufacturers of data processing devices, electronic and optical products, electrical equipment, motor vehicles and motor vehicle parts as well as any other vehicle construction. **Within these industries, companies with more than 50 employees or an annual turnover or an annual balance sheet of over 10 million euros are affected.**

These companies will in future be obligated to implement risk management measures for cyber security. This includes:

- **Risk analyses and security concepts** for information systems, protection of the supply chain and the safety of personnel
- Concepts for **access control** and the management of plants
- **Mandatory training** for management
- In the event of serious security incidents, an **early warning** within 24 hours and within 72 hours **notification of the responsible authority**

The NIS 2 was adopted at the end of 2022 by the European Parliament and the Council of the EU. The EU member states had until 18 October 2024 to adopt the Directive into domestic law.

Practical tip:
The European Union Agency for Cybersecurity (ENISA) offers a lot of helpful information on the topic of cyber security, including a tool for self assessment with which companies can check their cyber security strategy: **www.enisa.europa.eu**

Practical tip:
Software tools such as OpenVAS can help companies to identify vulnerabilities and check countermeasures.

1.3. Cyber Resilience Act (EU) 2024/2847

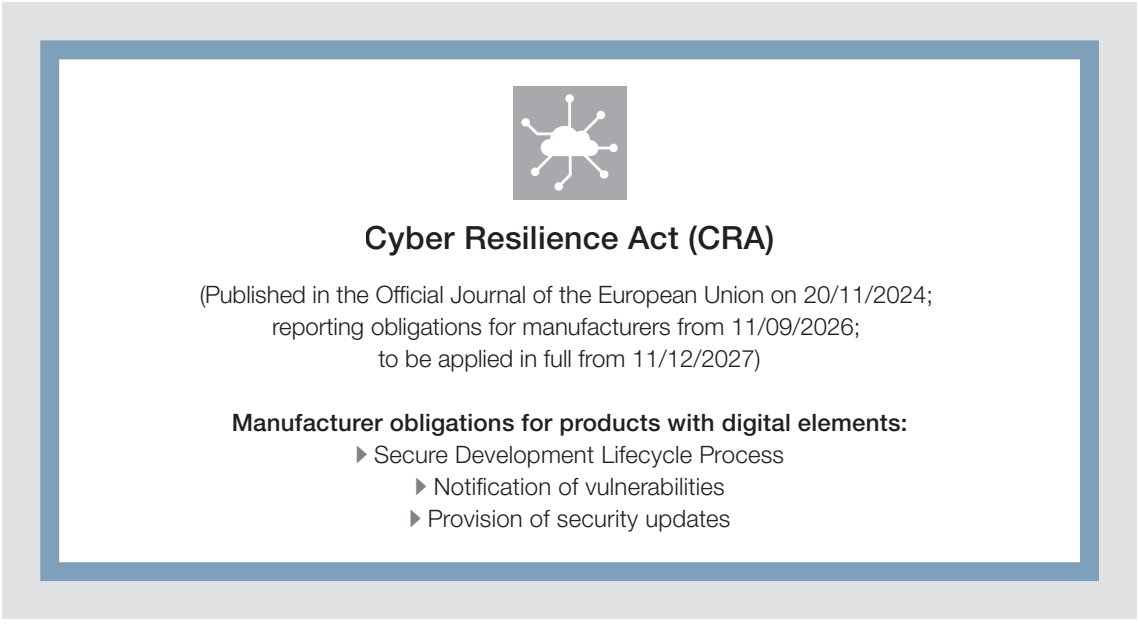

Figure 4: An overview of the Cyber Resilience Act

The European Commission considers cyber attacks to be a matter of public interest, as these can have critical consequences not only for the economy of the Union, but also for democracy, the safety of consumers and their health.

For this reason, the European Commission submitted a draft for a Regulation in 2022 intended to increase the cyber security of products.

This Cyber Resilience Act (CRA) is directed toward **manufacturers of products with digital elements (hardware and software)** that are capable of communicating with other products.

In other words, products from the B2C segment such as smartphones or robotic vacuum cleaners are affected by this, as are those from the B2B segment such as **controllers and sensors,** as well as pure software products such as operating systems.

In accordance with the CRA, in future only products that guarantee an appropriate level of cyber security may be placed on the market – and that's over the whole lifecycle of a product. The regulation was published on 20/11/2024 in the Official Journal of the European Union. The reporting obligations for exploited vulnerabilities for manufacturers apply from 11/09/2026. Products with digital elements must satisfy the requirements of the CRA from 11/12/2027 in order to be able to be made available on the market in the EU. The CRA is an EU Regulation and will thus be immediately valid in the EU member states.

The CRA is to be applied in parallel with the Machinery Regulation. This means that a machine is also viewed as a product with digital elements. This in turn means that in addition to the requirements from the Machinery Regulation, there are also requirements from the CRA.

This is necessary as the Machinery Regulation aims to protect the persons in the immediate vicinity of the machine, while the CRA additionally protects natural and legal persons against economic losses.

In practice there may potentially be synergy effects in that a cyber security measure also meets requirements from the CRA and from the Machinery Regulation for example. These synergy effects must be verified by the manufacturer, e.g. through the application of harmonised standards.

Practical tip:
Subscribe to the newsletter and RSS feeds at **https://eur-lex.europa.eu** to ensure that you are always informed of legislative changes on the EU level.

1.4. Directive for safety and health requirements for the use of work equipment 2009/104/EC

The question of which obligations they must now comply with is one that companies that operate plant and machinery must also ask themselves. The Directive on the minimum safety and health requirements for the use of work equipment by workers at work makes specifications in this regard. The Directive was published on 3 October 2009 in the Official Journal of the European Union and was subsequently implemented by all member states in domestic law. It defines “work equipment” as any machine, apparatus, tool or installation used at work.

According to this Directive, one of the employer’s obligations is to provide the employees with suitable work equipment so that the safety and health of the employee is guaranteed to be protected while the equipment is in use.

During the entire period of use, the work equipment must be kept in a condition, e.g. by means of corresponding maintenance, that guarantees that it corresponds to the provisions of all applicable relevant EU Community Directives.

Even though the Machinery Regulation is officially a Regulation – and not a Directive – it must be assumed that it is recognised as a relevant Community Directive from a legal perspective. The new requirements from the Machinery Regulation thus also apply for existing machines from the point in time at which the Machinery Regulation applies.

Figure 5: Legal requirements for Machinery Safety must be observed and complied with

2. Security for machine manufacturers

The security requirements for machinery are increasing for two reasons: On the one hand, demanding customers are already asking questions about the security properties of machinery, and on the other, beginning in 2027 legislators will be requiring basic properties so that machinery can be put on the market or provided in Europe.

And don't forget that most machine manufacturers are considered important entities by legislators and are therefore subject to the NIS 2 Directive. This means that it is advisable for them to think about introducing an **Information Security Management System (ISMS)**.

In short:
Machinery that does not satisfy the security requirements of the Machinery Regulation can no longer be placed on the market in the EU from 20/01/2027. Whether measures must be taken and what those measures are can be determined using a structured risk analysis.

The Cyber Resilience Act (CRA) will also call for comprehensive information and documentation obligations.
The reporting obligations for manufacturers apply from 11/09/2026; the CRA is to be applied in full from 11/12/2027.

2.1. Security in the Machinery Regulation

The Machinery Regulation requires protection against corruption in the essential health and safety requirements in Section 1.1.9. This is described as follows:

> "[…] The machinery or related product shall be designed and constructed **so that the connection to it of another device**, **via any feature of the connected device itself** or via any remote device that communicates with the machinery or related product **does not lead to a hazardous situation.**
>
> **A hardware component transmitting signal or data,** relevant for connection or access to software that is critical for the compliance of the machinery or related product with the relevant essential health and safety requirements **shall be designed so that it is adequately protected against accidental or intentional corruption. The machinery** or related product **shall collect evidence of a legitimate or illegitimate intervention in that hardware component,** when relevant for connection or access to software that is **critical** for the compliance of the machinery or related product.
>
> **Software and data** that are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements **shall be identified as such and shall be adequately protected against accidental or intentional corruption.**
>
> The machinery or related product shall identify the software installed on it that is necessary for it to operate safely, and shall be able to provide that information at all times in an easily accessible form.
>
> The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery or related product or its configuration. […]"

Section 1.2.1 Safety and reliability of control systems also includes the requirement:

> "[...] Control systems shall be designed and constructed in such a way that:
>
> a) they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, **including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation;** […]"

A more specific definition of the protection objective "protection against corruption" and its technical implementation are to be specified in a new European standard EN 50742. This is currently being developed. Because it cannot yet be predicted whether this standard will be published and harmonised before the end of the transition period for the Machinery Regulation, it is advisable to read up on the state of the art now. A helpful resource here is IEC TS 63074, for example. This specification describes the security aspects in connection with the functional safety of safety-related control systems. IEC 62443-3-3 also explains the security requirements for industrial automation systems. The appendix of this guideline presents basic information on the family of standards.

Some requirements from the Machinery Regulation can be satisfied through the selection of appropriate components, while others require additional documentation. To find a pragmatic approach, it is advisable to start planning a systematic risk analysis already in the design phase of the machine development. This can also be performed later, but experience shows that the further the development is, the greater the effort.

Figure 6: The EU Machinery Regulation makes Industrial Security mandatory in the conformity assessment process

2.2. Between component manufacturers and customers

Safe and legally compliant operation of the machine is the mission of machine operators. During implementation, machine manufacturers and integrators must navigate between the requirements of customers and the products offered by component manufacturers.

Type C standards provide support. They describe the state of the art for certain application areas and specify the minimum level of safety that a machine must possess. Because there are currently no harmonised C standards that take into consideration the security aspect, the only available course of action is to perform a risk analysis applying established international standards to the best of one's ability and to derive measures for risk reduction from this.

To be able to perform the risk analysis correctly, it is important to be familiar with the ambient conditions and security requirements at the machine. Two things are important here: on the one hand the potential extent of the damage, meaning how high the motivation of the attacker is to cause damage, and on the other the probability of an attack. One can assume that a freely accessible machine is more likely to be attacked than a machine to which only one limited group of people has access.

Everybody knows about security updates on everyday products like smartphones and computers. Machine controllers and other machine components also require updates should a security loophole be detected. As it currently stands, most components do not perform automatic updates and the component manufacturers are generally not in direct contact with the operators. This leads to the question of how the operators can make sure that their machines receive the necessary updates in good time.

The integrator, meaning the machine manufacturer or system integrator, plays a key role here and can use its position to communicate between the operator and the component manufacturer. They can approach the component manufacturer with the security requirements of the operator and select the correct components. They can also share information about the components, such as new security updates, with the operator.

Practical tip:
To support a uniform approach, the German engineering association VDMA e. V. created the "Supply Chain Security" document series in the Industrial Security working group that is intended to facilitate communication between operators, integrators and component manufacturers:
www.vdma.org

The following illustration shows the interfaces between operators, integrators and component manufacturers.

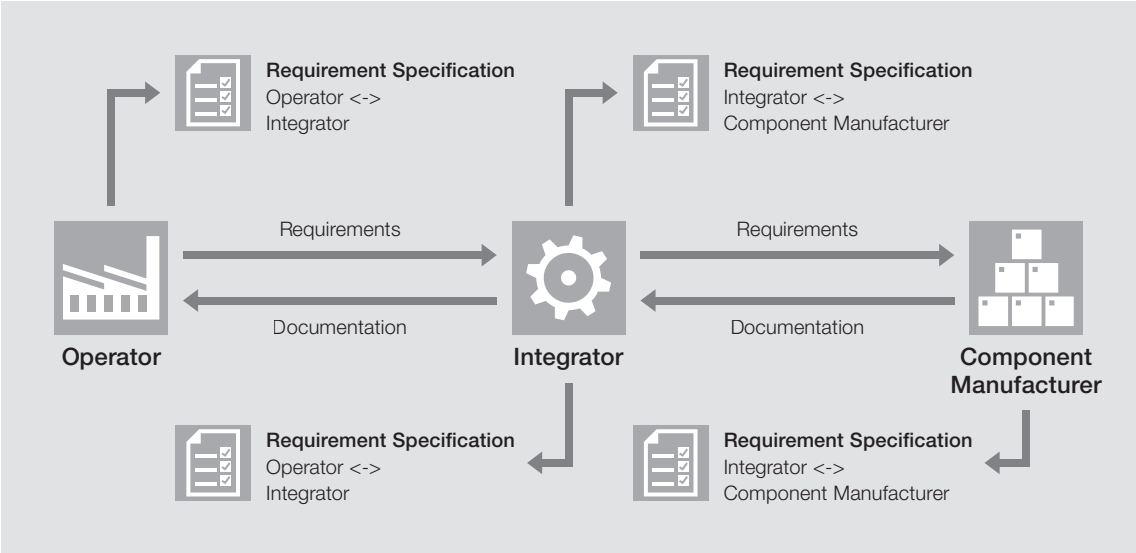

Figure 7: Recommendations for supply chain from VDMA (source: https://www.vdma.org/cybersecurity)

2.3. Cyber Resilience Act for machine manufacturers

The Cyber Resilience Act (CRA) is a regulation that was published on 20/11/2024 in the Official Journal of the European Union. It refers to products with digital elements. All products with digital elements must meet the requirements of the CRA from 11/12/2027. Manufacturers of products with digital elements must comply with the reporting obligations before this, from 11/09/2026. It can be assumed that if a machine falls under the CRA, the manufacturer must also certify compliance with the CRA. This means that a number of requirements must be met.

The following requirements are worth mentioning here, though others also apply:

- **Reporting obligation** for manufacturers for exploited vulnerabilities to the authorities within 24 hours
- Products with digital elements are designed, developed and manufactured so that they **ensure an appropriate degree of cyber security** that corresponds to the determined risk
- Based on the risk analysis, the products can only be made available on the market **without detected exploitable vulnerabilities**
- Guarantee that vulnerabilities can be rectified by means of **security updates**
- **Protection of the availability of critical and basic functions,** even after an incident, including by means of fail safety and remedial measures against denial-of-service attacks
- Identification and documentation of **vulnerabilities and components by manufacturers of products with digital elements,** including by creating a Software Bill Of Materials in a machine-readable format that at least covers the most important dependencies of the products
- Additional **documentation about handling security loopholes,** such as the time period in which the manufacturer provides security updates for the product
- Creation of an EU Declaration of Conformity

This (incomplete) list of requirements from the CRA clearly shows that considerable effort will be required for all economic operators involved. How these specifications affect the product diversity and whether the estimated transition period of three years is sufficient remain to be seen.

Pilz recommends that all machine manufacturers delve into this topic soon and work together with component manufacturers and operators to develop concepts to satisfy the requirements of the CRA.

Practical tip:
The Common Security Advisory Framework (CSAF) is a standardised, open source framework for communication and automated distribution of machine-processable vulnerability and mitigation information, so-called Security Advisories:
https://oasis-open.github.io/csaf-documentation

Practical tip:
Thanks to the introduction of a Software Bill Of Materials (SBOM), it is possible to maintain an overview of all software versions used.

3. Security for machine operators

Operators of machines are also affected by the new legal acts: be it in the procurement of new machines, changes to existing machines or the recurring check of whether the state of the art is still being maintained.

Because machines are typically used in the production industry, machine operators must also satisfy the NIS 2 Directive.

In short:
Operators of existing installations are also affected by the new Machinery Regulation. Through network segmentation and the restriction of access opportunities, the required protection can generally also be achieved retrospectively. With a structured risk analysis that is performed in advance, required actions are determined.

The NIS 2 Directive requires comprehensive security concepts from a large group of manufacturing companies. Networked machinery must be included in these considerations.

3.1. Handling existing installations

Operators of machines that are typically used as work equipment must make sure that the employees enjoy sufficient occupational safety and that nobody is injured. This is described in the **EU Directive for safety and health requirements for the use of work equipment** from 2009 described above which was implemented by all member states in domestic law.

This Directive requires that the operator uses recurring checks to make sure that the work equipment is kept at a level that corresponds to the provisions of all applicable relevant EU Community Directives during the entire period of use by means of corresponding maintenance.

Conversely, this means: From the day on which the Machinery Regulation comes into effect, meaning 20 January 2027, all active machines must have been checked as to whether they correspond to the level of the Machinery Regulation. There will be cases in which the employer cannot meet the requirements in full. In such cases, there is still an obligation to take suitable measures to reduce the risks to the greatest possible extent.

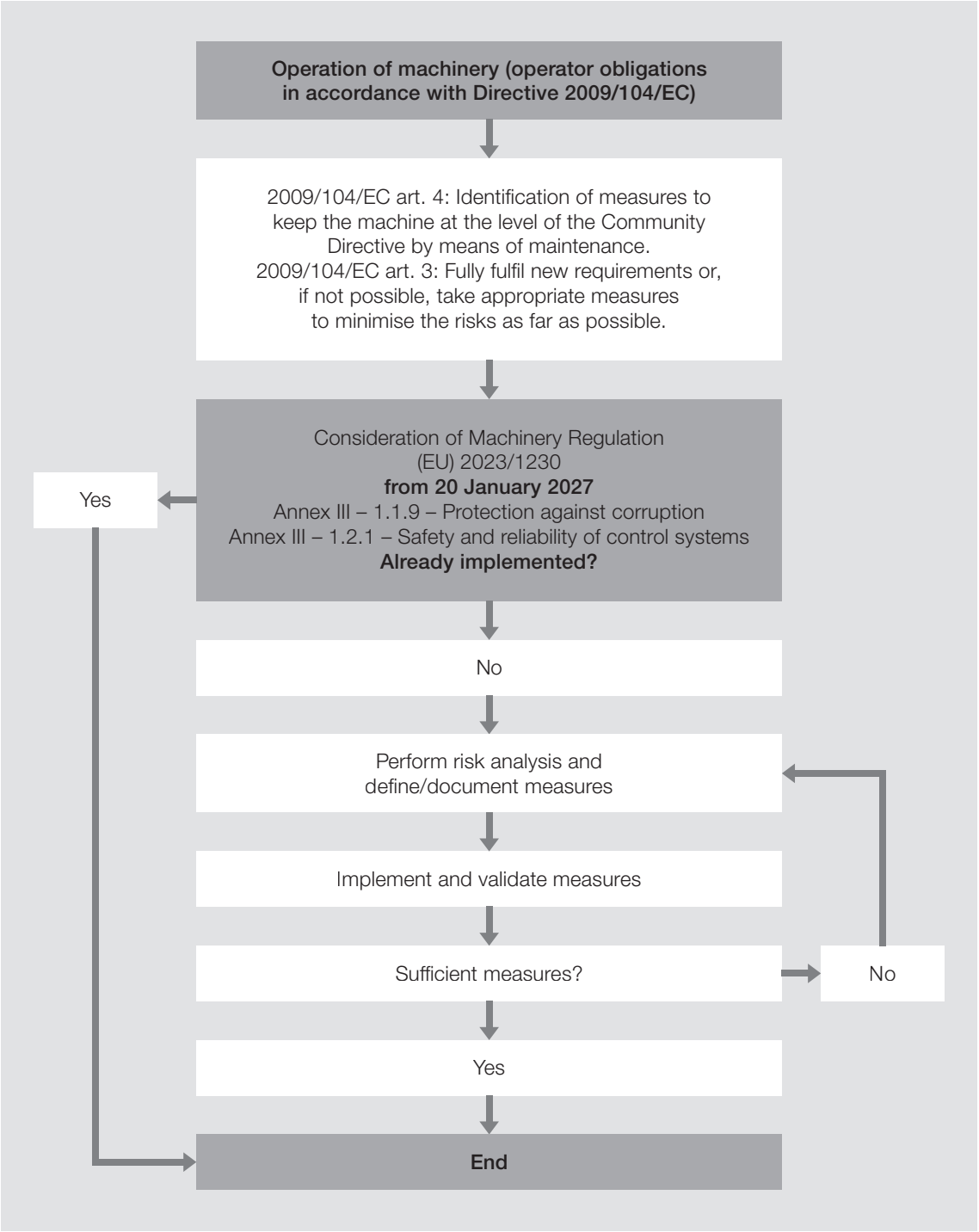

Figure 8: Process workflow – handling existing installations

Operators who have not yet grappled with the topic must take measures to satisfy the new requirements with regard to cyber security.

The first step is a risk analysis. The measures to be implemented result from this risk analysis. In most cases, this includes segmentation of the network and the restriction of access opportunities.

3.2. From IT Security to company-wide Security

Generally, the IT department (Information Technology) is responsible for information and communication technology at a company, including IT Security.

In companies, the topic of security is assigned in the form of a staff function, for example. These security experts or officers, e.g. in the role of Chief Information Security Officer (CISO), should be familiar with the requirements of the NIS 2 Directive and have a concept of how these can be implemented in the entire company.

Experience shows that the production area in the company relies on the IT department in the event of questions regarding IT Security and only deals with the topic peripherally.

A new way of thinking is absolutely essential here as machinery in the production area is part of the company's security concept. To be able to correctly implement the overall concept, the company must be divided into safety zones and the interfaces and requirements for the individual zones must be defined and implemented down to the machine level in the company.

Figure 9: Industrial Security also affects the correlation between IT Security and OT Security

Practical tip:
Using the search engine **https://www.shodan.io/**, networked devices can be found and frequently also devices that should no longer be found due to network segmentation. Are your devices listed there too?

Practical tip:
One of the most frequent types of attack is via employees at a company, such as via phishing emails. Regular training of staff reduces this risk.

4. The route to safe machinery – Safe and Secure

In short:
With a structured risk analysis, the costs for countermeasures and also for the analysis itself can be drastically reduced. Consideration of the number of possible paths of attack is reduced here to those that actually threaten the defined protection objectives. Assessment of the possible level of damage and of the likelihood of occurrence provides additional indications for sensible work to minimise risks.

Security risks on machinery can develop in a number of ways, both via data networks as well as physically through direct access to the machine. In order to offer a machine the most cost-efficient protection possible, a structured approach as described below is advisable.

- **Identify assets**
  In the first step, the assets to be protected are defined and distinguished from one another. The result provides a complete and consistent image of the plants and plant sections to be protected. This measure makes sure that no parts are forgotten, but also that threat vectors are not unnecessarily considered several times.
- **Analyse threats**
  In the next step, the amount of possible damage in the event of a compromise is to be determined. The question is easier to answer if the three protection objectives of Information Security are considered separately. These are: Confidentiality, Integrity and Availability – frequently abbreviated as CIA.
  - **Confidentiality**
    Does the machine contain information that if disclosed could damage the company? This could be notes on production processes, recipes or other trade secrets that give the company a competitive edge. How serious is the potential damage?
  - **Integrity**
    What effects can an unwanted change to data have? Can the change to data lead to economic losses, such as through damage to the machine, or endanger people, e.g. by affecting safety functions? How serious is the potential damage?
  - **Availability**
    What economic losses are caused by failure of a machine, e.g. through production interruptions?
- **Determine protection objectives**
  The protection objectives can be formulated following this preliminary work. A more concrete definition of these objectives allows for more specific determination of the threat vectors. This avoids unnecessary measures that may increase the security of machines but do not help to achieve the defined protection objectives.
- **Assess risks**
  Once the protection objectives have been determined, the likelihood of the determined risks actually occurring is estimated. The result provides an indication of the sensible scope of the further measures.
- **Analyse threat vectors**
  In this step, the paths through which an attack can actually take place and what protective measures already exist, e.g. through intrinsic protective measures in the machine components used, are systematically determined. This results in a list of the remaining threat causes.

- **Create and implement security concept**
  The security concept provides a concrete description of all measures that are necessary to achieve the defined protection objectives for the machine under consideration. These can be design measures on the machine as well as organisational adjustments of the processes.
- **Check implementation**
  The actual effectiveness of the performed measures can only be checked with very complicated penetration tests in which hacker attacks are simulated by specialised providers. Alternatively, the correct implementation of the security concept should be checked.
- **Perform regular reassessments**
  Compared to safety, protective measures for security are not a one-time thing. Because new vulnerabilities crop up constantly in complex systems, the analysis should be repeated at regular intervals or in the event that threats emerge. New vulnerabilities can occur at all levels of the procurement pyramid, e.g. with hardware components, open source code in devices or specific device firmware. As soon as a vulnerability has been detected, the responsible manufacturers publish corresponding Security Advisories with information about the threat and notes on suitable countermeasures. It is advisable to regularly check for new Security Advisories from suppliers.

Figure 10: Components, plant and machinery are only truly reliably secure and protected against corruption through a security inspection

Practical tip:
Pilz Security Advisories can be found at **www.pilz.com/advisories**

5. One-stop Safety and Security

The new legal specifications on the subject of security bring new challenges for machine manufacturers and operators. The processes for risk reduction for attacks on machinery (Security) are quite similar to the procedures for the reduction of risks that can stem from machinery (Safety). Pilz is an expert in Machinery Safety and helps step by step to achieve tailor-made solutions and safe machines – Safe and Secure.

Figure 11: Safety and Security are part of a holistic concept in Machinery Safety

- Specialist knowledge and expertise through participation in standards committees
- Research and tracking of the current standards and legal practice
- Basic and expert training for machine-oriented Industrial Security
- Services as part of machine-oriented Industrial Security
  - Protection requirements analyses
  - Risk analyses
  - Holistic security concepts
  - Validation/verification
  - Process optimisation
- Products and solutions for physical access control and cyber security on the machine

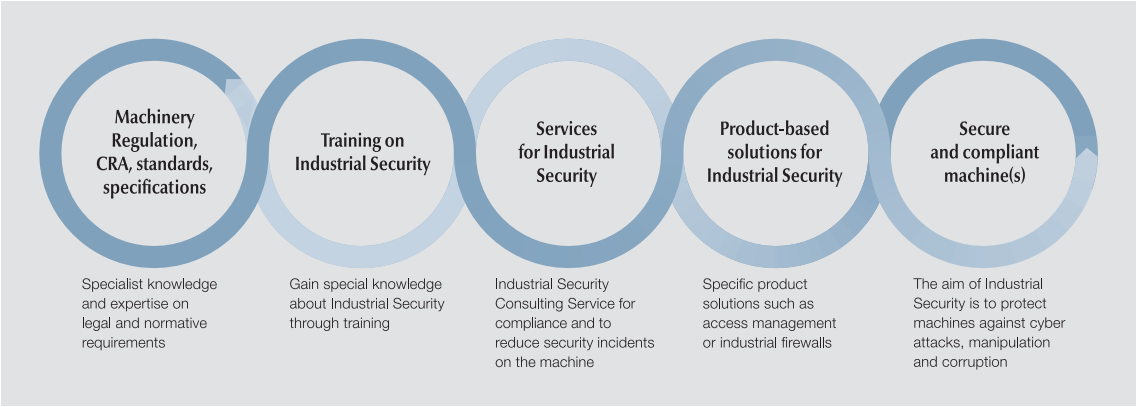

Figure 12: Secure machinery with Industrial Security solutions, step-by-step

Practical tip:
Learn more about Industrial Security solutions at Pilz at **www.pilz.com/security**

6. Summary and outlook

The increase of threats through cyber attacks and corruption is having a direct impact on the legal situation in Europe and resulting in a clear course on the part of legislators with regard to Industrial Security: In future, legislators will put in place new requirements for Industrial Security, in particular through the Machinery Regulation, NIS 2 Directive and CRA. For machine manufacturers and operators, this means active involvement through the development and implementation of organisational and technical measures to meet the new requirements for companies, machinery and components. The above guideline has explored these tasks and how to handle them.

The NIS 2 Directive is already binding for the majority of machine manufacturers and operators, while the new Machinery Regulation and the CRA will follow in 2027. Acting proactively will make it possible to plan and implement the necessary projects in good time.

Standards committees provide machine manufacturers with orientation regarding how to implement the new requirements. A structured approach is important, as described in the series of standards IEC 62443.

Experienced and qualified service providers help to analyse the necessary measures step by step in order to meet the new target specifications, generally with reasonable effort.

Machinery Safety will mean Safety and Security in future – to protect people and to protect machines. With a holistic, coordinated concept, complex problems in Machinery Safety can be efficiently and cleanly segmented. A risk analysis is also the first step for Industrial Security and offers a structured orientation and methodology for breaking down requirements for your own company.

This approach gives companies the tools they need to meet the growing challenges in the field of Industrial Security.


Further information
from Pilz on Industrial Security –
discover more now
PILZ
Find out more at:
www.pilz.com/security

7. Appendix

7.1. Terms from the field of Industrial Security

Cyber security as set out by the EU Commission refers to all tasks that are necessary to protect network and information systems, the users of these systems and other people affected by cyber threats.

Cyber threat refers to a possible circumstance, a possible event or a possible action that could damage, disrupt or otherwise adversely affect network and information systems, the users of these systems and other people.

Industrial Security has the objective of guaranteeing the availability of plant and machinery, as well as the integrity and confidentiality of machine data and processes.

IT Security (Information Technology) is the safeguarding of data not connected to physical processes.

OT Security (Operational Technology) is the safeguarding of plant and machinery that take part in physical processes.

IACS is an abbreviation from IEC 62443 and stands for Industrial Automation and Control System(s).

Security Level from the series of standards IEC 62443 is the level that corresponds to the required measures and the intrinsic security features of devices and systems for a zone or a conduit based on the assessment of the risk for the zone or the conduit.

Zone is the collection of units that reflect a division of an inspected system based on their functional, logical or physical relationships (including the location).

Conduit is the logical grouping of communication channels that combines two or more zones for which common IT Security requirements apply.

7.2. IEC 62443 – basic standard for Industrial Security

IEC 62443 is a series of international standards for “Industrial communication networks – Network and system security”.

7.2.1. Overview

The family of standards IEC 62443 is made up of different parts; of these, the following standards have already been published at the present time.

Part 1 concerns the general principles:
- IEC TS 62443-1-1: Part 1: Terminology, concepts and models
- IEC TS 62443-1-5: Part 1–5: Scheme for IEC 62443 security profiles

Part 2 refers to security requirements for operators and service providers:
- IEC 62443-2-1: Security program requirements for IACS asset owners
- IEC 62443-2-2: IACS Security Program Ratings
- IEC TR 62443-2-3: Patch management in the IACS environment
- IEC 62443-2-4: Security program requirements for IACS service providers

Part 3 refers to security requirements for automation systems:
- IEC TR 62443-3-1: Security technologies for Industrial Automation and Control Systems
- IEC TR 62443-3-2: Security risk assessment for system design
- IEC 62443-3-3: System security requirements and security levels

Part 4 describes the security requirements for automation components:
- IEC 62443-4-1: Secure product development lifecycle requirements
- IEC 62443-4-2: Technical security requirements for IACS components

Part 5 defines the profiles of the IEC 62443:
- IEC TS 62443-1-5: Scheme for IEC 62443 security profiles

Part 6 describes the evaluation methodology:
- IEC 62443-6-1: Security evaluation methodology for IEC 62443-2-4

7.2.2. Security Level (SL)

The requirements for systems and components are described with Security Levels.
These are defined as follows:

- Security Level 0: No special requirement or protection required
- Security Level 1: Protection against unintentional or accidental misuse
- Security Level 2: Protection against intentional misuse by simple means with few resources, general skills and low motivation
- Security Level 3: Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific skills and moderate motivation
- Security Level 4: Protection against intentional misuse by sophisticated means with extended resources, IACS-specific skills and high motivation

This means that as the required Security Level increases, so does the required effectiveness of the implemented measures.

There are seven Foundational Requirements (abbreviated as FR):

- FR 1 – Identification and authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

Behind each of the Foundational Requirements are measures of varying quality that can be applied to achieve the required level. Typical measures are multi-factor authentication or encryption mechanisms.

The Security Level that must be reached depends on the cyber risk. European legislators differentiate between important and essential assets. The cyber risk that must be assumed therefore depends on the type of company, the size of the company and the potential effects. Various standards organisations are currently addressing this topic and are in the process of defining universal requirements for industries and machine types.

7.2.3. Information Security Management System (ISMS)

In addition to the technical requirements for components and systems, there are also organisational measures that must be implemented in order to reduce the risk of a successful attack. Every company must decide for itself how it would like to set up the Information Security Management System (ISMS). The series of standards ISO/IEC 27000 is established and widely known. IEC 62443-2-1 can be considered a guideline for the implementation of ISO/IEC 27001 to industrial automation systems. There is also, among other things, the certification program TISAX from the automotive industry which has also proven to be suitable.

In the ISMS, the risks are named, classified, assessed and there is a description of how to handle them. Typically the application area and the interfaces to additional areas must first be defined. The following are also essential:
- Acceptance of responsibility for security by management
- Clarification of the responsibilities
- Definition of the advanced training activities
- Creation of security guidelines at the company

The ISMS helps to systematically consider the risks and derive corresponding measures.

Company risks may include:
- Economic losses due to production downtimes
- Injury to employees
- Data protection breaches
- Environmental damage
- Loss of customer confidence

Typical measures include, among other things:
- Development of emergency plans to be applied
- The definition of authorised users
- Physical and virtual access control
- Network segmentation

The implementation of measures is also described by the ISMS. These include:
- System development
- System maintenance
- Data backup
- Planning and handling of incidents

7.3. Other helpful documents for machine manufacturers and operators

In addition to the family of standards IEC 62443, there are already other security standards that affect machine construction and define requirements.

IEC TS 63074 describes the security aspects in connection with the functional safety of safety-related control systems. In this technical specification, the relevant aspects of the family of standards IEC 62443 are defined that must be taken into consideration to ensure safe and secure operation of a machine.

For the “protection against corruption” requirement from the Machinery Regulation, a new European standard EN 50742 is currently being developed. Pilz is an active member of the standards committee.

The Radio Equipment Directive 2014/53/EU and its delegated Regulation (EU) 2022/30 also result in security requirements. The series of standards EN 18031 was developed for these requirements.

7.4. Network segmentation using the Purdue model

To provide a visualisation of the subject of network segmentation, the Purdue model can be used. It was published by Theodore Joseph Williams (Professor of Engineering at Purdue University in the USA) back in 1990. In the following figure, the Purdue model was expanded to include examples of measures for our purposes.

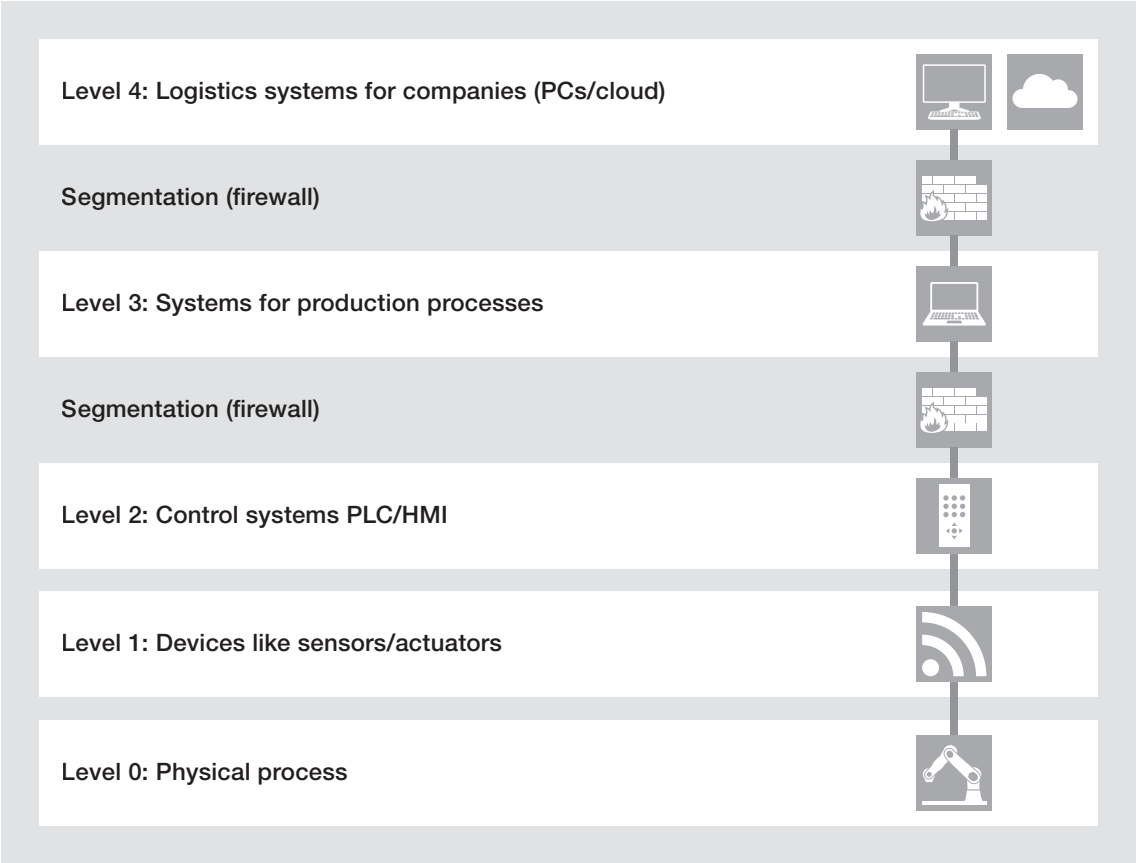

Figure 13: Network segmentation using the Purdue model

Level 0 is the actual physical process that is typically performed in the producing trade. This is generally monitored and actuated by sensor and actuator technology. These devices are contained in Level 1. The process is typically controlled by a programmable logic controller (PLC), which is contained in Level 2. Programming of the PLC is performed via the systems for production processes in Level 3. The actual jobs come from the logistics system in Level 4.

Level 0 to 3 fall under the designation of Operational Technology (OT), Level 4 and everything above it are covered by the designation of Information Technology (IT).

The figure already shows one type of segmentation that functions in this case via firewalls that limit the data transfer between Levels 4 and 3 or 3 and 2 in order to minimise the potential target area for an attack.

The objective is to implement a successful segmentation, meaning that there are both an effective reduction of the opportunities for attack as well as a system whose performance is not limited. It is necessary here to clearly define the interfaces; as a result all necessary ports and protocol types are taken into account when configuring the firewall, for example.

The correct selection of the right components is essential for safe and secure operation. After all, the best firewall achieves nothing if additional vulnerabilities exist in the lower levels due to components. Depending on the required Security Level, it may be necessary for the components in the system to authenticate one another, thereby monitoring changes to the system. This must also be taken into account when selecting the components and their configuration.

In this example, all components from Level 3 are permanently wired to one another and the flow of information is secured by two firewalls. In the industrial environment it is quite common that systems also have wireless interfaces (e.g. with automated guided vehicle systems). Here, checks must be performed to determine how security measures can be implemented effectively.

Practical tip:
Practical examples for the configuration of your devices is available at **www.pilz.com**.
Simply use the search function with the keyword “application notes”.

8. Literature

- 1. Reference model for Computer Integrated Manufacturing (CIM): a description from the viewpoint of industrial automation. Edited by Theodore J. Williams, 1989
- 2. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels IEC 62443-3-3:2013
- 3. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components IEC 62443-4-2:2019
- 4. EU Machinery Regulation 2023/1230 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1230)
- 5. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555)
- 6. Cyber Resilience Act P9_TA(2024)0130 (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.pdf)
- 7. Directive 2009/104/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0104)
- 8. European Union Agency for Cybersecurity (https://www.enisa.europa.eu/)
- 9. Pilz GmbH & Co. KG (https://www.pilz.com/en-INT/products/industrial-security/security-incident-management)
- 10. VDMA e. V. (https://www.vdma.org/cybersecurity)
- 11. Information Security, cyber security and privacy protection – Information Security Management Systems – Requirements ISO/IEC 27001
- 12. White paper Industrial Security (Pilz 2018) (www.pilz.com/security)
- 13. Guide to the Machinery Regulation white paper (Pilz 2023) (www.pilz.com/mr)
- 14. https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/#overview (viewed 20/01/2025)
- 15. Cybersecurity Act EU 2019/881, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1728407971719

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 400-088-3566
Japan
+81 45 471-2281
South Korea
+82 31 778 3390

Australia and Oceania
Australia
+61 3 95600621
New Zealand
+64 9 6345350

Europe
Austria
+43 1 7986263-444
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Türkiye
+90 216 5775552
United Kingdom
+44 1536 460866

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

BLUEcoMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards
BRAND OF THE CENTURY 2022

Quality Management ISO 9001:2015 REG. NO. 2462
Environmental Management ISO 14001 REG. NO. 2462
Energy Management ISO 50001 REG. NO. 2462

Presented by:

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany
Tel.: +49 711 3409-0
E-Mail: info@pilz.com, Internet: www.pilz.com

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, E-Mail: info@pilz.com, Internet: www.pilz.com

Printed on 100 % recycled paper for the good of the environment.

PILZ
THE SPIRIT OF SAFETY

8-4-en-3-023, 2025-04 Printed in Germany