Security

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Disclaimer

Our white paper has been compiled with great care. It contains information about our company and our products. All statements are made in accordance with the current status of technology 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

1st edition

At a glance

Systems are increasingly being networked due the digitisation of the factory. As a result, the risk of important data being spied out or manipulated also increases. In the past, communication in automation was primarily performed via fieldbuses such as CAN and proprietary, or in other words manufacturer-specific, protocols. In order to do any damage, an attacker would have to enter the factory hall or access a machine via a telephone line with a modem. Because these protocols are now increasingly being replaced by Ethernet and IP protocols, however, attacks can now also be performed over the Internet.
The motives range from terrorist intentions, industrial espionage and sabotage of systems to extortion of payments. The actions of the attackers are facilitated by the increased usage in automation of open-source software and software components from the consumer sector which potentially have vulnerabilities that the attackers are aware of. Security, meaning data protection, is thus also of ever greater importance.
Experience shows, however, that this message has not yet been fully understood by everybody. For this reason, the central aspects of security and solutions that have proven themselves in practice are introduced in this white paper. As a result, the machine builders, plant designers, installation engineers and maintenance engineers can recognise what role their products or services play in the security strategies of their customers and what they must pay attention to, for example. In addition, the aspect of functional safety is also included. Because security and safety are two sides of the same coin, namely safe production processes.

Content

1. Security and safety

1.1. Definition

Security used to be almost exclusively a topic for classic information technology (IT). Today, the worlds of IT and automation are growing ever closer. The degree of networking of production plants and the use of standard protocols like Ethernet for the physical transmission of the data are thus increasing considerably. In addition, standardised protocols such as OPC UA allow for access to controllers via IT systems, whereby the data communication becomes even more open.
In automation, the term security primarily means the protection of a plant or machinery from unauthorised access from outside as well as the protection of sensitive data from corruption, loss and unauthorised access from within. The threats stem from the cyber world, which includes the Internet as well as the entirety of modern information and communication technology. It begins with the access control at the plant door and extends all the way to the defence against attacks by hackers. However, says German IT security expert Ralph Langner, it is not always the “bad guys” who do the damage. Many security violations occur unintentionally, for example due to operating errors by colleagues and staff.
The term safety denotes the functional safety of plants, meaning the protection of people and the environment against foreseeable threats that can stem from machinery. Residual risks that are more or less always present must not exceed acceptable levels here. One method to guarantee this is the use of components such as safety relays and safety switches that ensure that the machine is brought to a safe condition in the event of a problem that does not pose a hazard for man, machine and environment.
After the functional safety of a machine had been approved according to the specifications of the Machinery Directive, plant operators would no longer have to worry about safety as long as no substantial changes had been made to the machine following this. Those days are gone, however. Thanks to the threats from the cyber world, security is an essential element of safety.

1.2. Reciprocal effects

Because production processes can be interrupted by safety functions, there are frequent attempts to – illegally – bypass these, which in past was prevented primarily through mechanical means. An example of this is the sealed screws that prevent the simple removal of safety switches. It is currently possible to perform this type of manipulation over the network, however. If, for example, a machine is brought to a safe condition because of a light guard, its program can be changed so that the corresponding data are no longer evaluated. The protective function is hereby deactivated and the machine continues to run, even in hazardous situations.
On the other hand, safety mechanisms could also be used to cripple machines over the network in a targeted manner. A simple interruption of the data communication is sufficient here. Because the safety mechanisms perform cyclical checks of whether the network subscriber on the other side of the connection is still active. As soon as there is no answer, the machine stops. An option for achieving this are the DoS attacks already mentioned, which create an overload of the network.
Not only production processes can be compromised over the network, however. Instead other hazards may arise as well. Safety mechanisms that check whether a machine is switched on or off are also a target for attackers. If these mechanisms are changed so that the drive runs constantly, this may lead to a machine being destroyed in the worst case scenario.

High-cost capital goods such as wind turbines frequently have double and triple protection for this reason.

2. Meaning of security in automation

2.1. Objective

Through approaches like Industrie 4.0, which focusses mainly on networking, threats from the cyber world pose a serious problem for manufacturing companies. All IT-based processes can generally be protected, but it is complex and expensive. An investigation should therefore initially be performed to determine which risks actually exist. Then a security strategy must ultimately always balance the costs and the benefits for the productivity of a company.
Security aims to guarantee the availability of the network and the devices and the integrity and confidentiality of the data. To do so, distributed control systems must not only be protected against attacks such as DoS attacks, but also against software, device and operating errors. Another option for interrupting production processes is manipulating the transmission or storage of data, which is why data integrity plays an important role. And a violation of the data confidentiality can have serious consequences, such as when the application program of a machine is spied out and this is then copied.

2.2. More than IT security

In order to be able to react flexibly to various threat scenarios, security strategies are currently implemented that comprise several layers of protection: the core comprises the automation components. This is followed by the network via which these components can communicate with other networks or e.g. with an ERP (enterprise resource planning) system. The top layer is the factory, which is shielded from the outside by a firewall concept.
Such designs are not sufficient, however, for all round protection of plants. Because, as already mentioned, threats can also come from within. The physical protection against unauthorised access to network devices such as firewalls and switches are the basis for every security strategy. The only way to prevent these devices from being manipulated on site is if they are not freely accessible. Installing the network devices in lockable control cabinets or junction boxes can be a simple but effective measure. At the same time, the risk of operating errors caused by unauthorised personnel can also be considerably reduced by this.

2.3. Effects on the lifecycle of plants

Plants can have a lifecycle of 20 years or longer. Until now, they have generally been operated according to the principle “Never change a running system”. This means that when a safety mechanism had to be updated, the controller was normally replaced with a new model of the same type. Because the functional safety is guaranteed as long as no substantial changes are made to the machine. It is based on the statistical fault models that define how probable it is that a damage event occurs. And virtually nothing about this changes over time.

Security, on the other hand, is a “moving target”. Unlike with safety, the object here is not that a fault can occur with a probability of 1:100.000, for example, but instead the ratio can be 1:1 if an attacker infiltrates the network first. In addition, increasingly sophisticated methods of defeating defensive measures are constantly being developed and algorithms that used to be secure are suddenly not secure any more. A few years ago, the Data Encryption Standard (DES) was a common process. The BSI (German Federal Office for Information Security) currently no longer recommends using it. The same is true for the hashing algorithm MD5. And with quantum computers, it will soon be possible to calculate cryptographic keys in just minutes or even seconds; something that would take ages with current computers.
Because security is not a physical parameter but rather a “moving target”, the measures against cyber threats must be updated constantly. The responsibility for this primarily lies with the plant operators, for whom data protection also means protection of their investment. Because using an effective security strategy, it is possible to use your plants just as long as before. On the other hand, machine builders and component manufacturers are obliged to inform the operators immediately in the event of new safety problems and to provide updates for the software on their devices with which vulnerabilities can be rectified. This requires that both sides work in close collaboration throughout the entire product lifecycle, however.

3. Forms of threats

3.1. External attacks

Ethernet-based automation networks are exposed to various threat scenarios that can be categorised based on the point of origin. After all, there are only external and internal attacks and unintentional security violations, for which the motives vary.
If networks are attached from the outside, this generally occurs with malicious intent. This includes sabotaging plants, for example. The possible consequences are shown by an example that was publicised, but without naming names: After a successful attack on a blast furnace in Germany, this had to be torn down because the melt had become hard.
A different threat scenario that can have negative effects is industrial espionage. If, for example, information on products or manufacturing knowledge is spied out, the competitiveness of the company is potentially at risk. This is also the case if confidential financial data or information about customers, tenders and orders are stolen.
In order to access passwords and login data, attackers sometimes use perfectly imitated websites and e-mails, so-called phishing. If the recipients are not alert, the attackers have an easy time of it. This is why it is so important that companies raise their employees’ awareness on the topic of security and put guidelines in place that are binding for everyone.
Finally, there have been an increasing number of attacks lately that are simply performed with criminal intent. The method of choice is so-called ransomware that can be hidden in Word, PowerPoint or Excel files, for example, which are sent by e-mail. When the recipient opens it, all the files on his computer are encrypted. The malware can also spread to other devices in the network. The only way to access the data again is by paying a ransom.

3.2. Internal attacks

Although attacks from the outside continue to make headlines, attacks from the inside are just as dangerous. Here it is possible to literally bypass security strategies. The intentions of the attackers are essentially the same as those for attacks from the outside; only the approach differs.
One option involves the attackers entering the company and looking for a free Ethernet connection in order to introduce malware to the network. A small USB stick is sufficient for this and is not noticeable during a check at the plant door.
More frequently, attackers take advantage of the fact that humans are also the weakest link when it comes to security. An effective method for manipulating personnel is so-called social engineering, for example.
The goal here is to gain the employees' trust and then use them as willing tools. The most important thing here is thorough research in advance, like on company websites where the names and job titles of the employees can be found. Sometimes all that it takes for an attacker to be accepted as a member of the company is for him to mention to an employee that he spoke with Mr X, who said he should contact this employee.

3.3. Unintentional security violations

By far the most cyber incidents do not result from either external or internal attacks, however, but instead are unintentional. The consequences can be just as serious as with the other two threat scenarios, such as leading to a failure of networks or the dissemination of sensitive information. The reasons are primarily incorrectly configured devices and operating errors.
The employees from production, who usually are not IT experts, must therefore be trained accordingly. Furthermore, networks can also be implemented such that the effects possibly resulting from incorrectly configured or incorrectly operated devices are limited by means of segmentation, meaning a division into subnetworks, and the use of different security measures.

4. Assessment of security

4.1. Normative bases

Security has played a central role in classic IT for many years, which is why there is a series of standards such as the series ISO/IEC 27000 "Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016); German version EN ISO/IEC 27000:2017". The requirements cannot simply be applied to automation, however. After all, the availability of data is of the utmost importance here and this is a critical precondition for smooth production processes, while in IT the confidentiality of data is top priority.
To enable effective security solutions for the automation, different organisations have begun to develop corresponding standards. But these only describe partial aspects such as the differentiation of security and safety. In addition, they are not available as a draft or as an official standard, but are instead more like technical references.

With IEC 62443 “Industrial communication networks - Network and system security”, there is an international series of standards, parts of which have already been adopted, and that comprehensively handles IT security in automation. The range of topics spans from risk

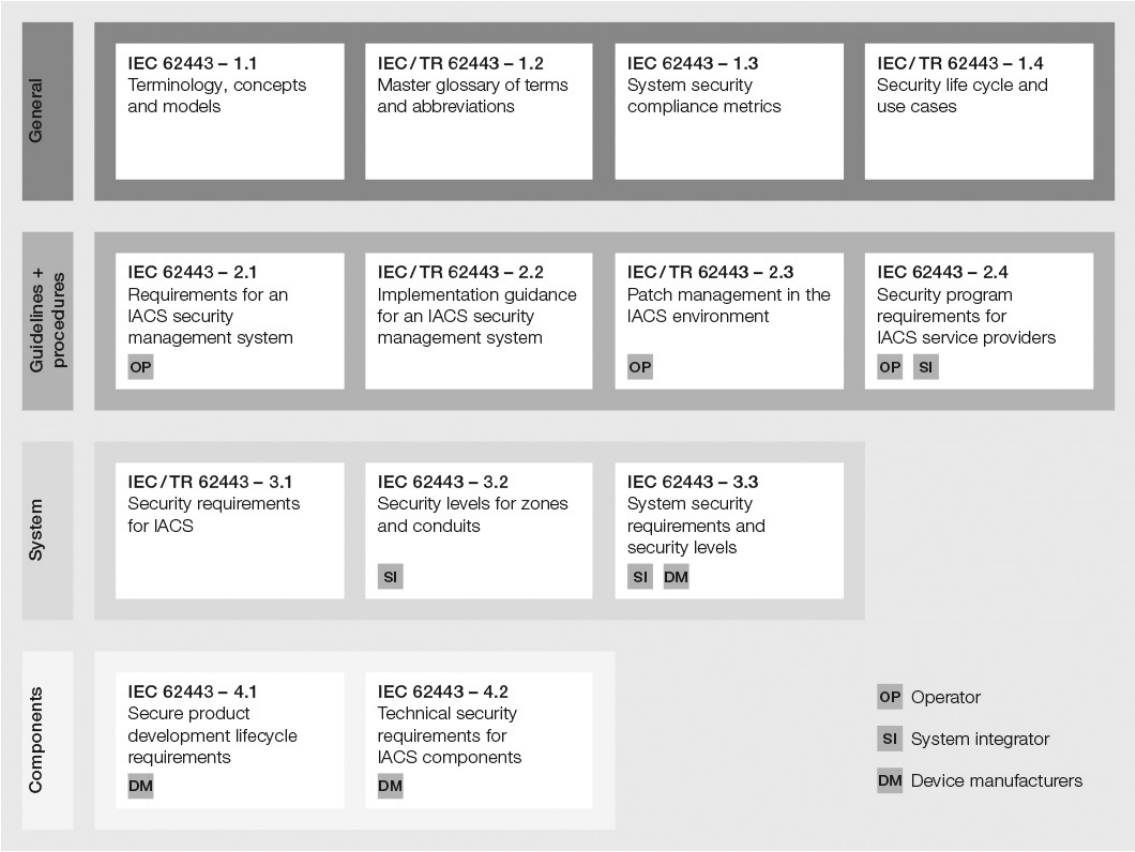


Figure 1: Standard IEC 62443

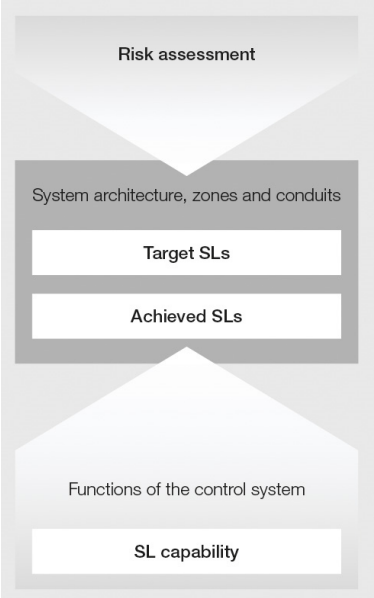
analysis, through best practices and all the way to the secure development of products (security by design). As a result, IEC 62443 currently offers the best orientation aid for plant operators and device manufacturers for effectively implementing security.
The “ICS Security Compendium” from the German Federal Office for Information Security (BSI) is directed in particular at the operators of industrial control systems. Not only general principles are explained here, but also particular requirements and relevant standards. In addition, suitable measures are introduced and paths for executing them are illustrated.
While IEC 62443 and the “ICS Security Compendium” are more something for experts, the VDI directive VDI/VDE 2182 provides a comparably straightforward introduction to the topic. In addition, various companies from the automation industry have also published writings, which in some cases have the length of a book. Due to the complexity of industrial security, it is definitely advisable to involve external specialists – at the latest when beginning the implementation.

4.2. Risk analysis

Just like every other strategy, a security strategy begins with a stocktaking, or in other words: the plant operators must first get an idea of what threats they are exposed to and what company

Figure 2: Project steps of risk analysis

values they wish to concentrate on protecting. In the second step, five security levels can be defined as per IEC 62443 that range from 0 (no risk) to 5 (extreme risk) and are valid for the requirements that vary respectively. However there is no explanation of how exactly these can be satisfied.



Security Level	Protection
SL 0	No protection
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means
SL 3	Protection against intentional violation using sophisticated means
SL 4	Protection against intentional violation using sophisticated means with extended resources

Figure 3: Risk assessment

As a general rule of thumb, all devices that have an Ethernet connection can be considered at risk as they can essentially be used as a gateway for attacks from the outside and the inside or can be the starting point for unintentional security violations. If common operating systems are additionally installed on these devices, the risk increases. In particular if no more safety updates are offered for them. A simple search engine is sufficient for finding out which systems can be attacked successfully and what malware exists for this.
A risk analysis is always only a snapshot, however. New threats that have to be included can develop at any time. If processors were previously considered not critical, for example, security loopholes were recently discovered on them that have been compiled under the names “Meltdown” and “Spectre” and render many PCs vulnerable. Attackers are now also setting their sights on soft PLCs (software -based programmable logic controllers). In brief: Security is a permanent process that requires persistence.

4.3. Countermeasures

After the company values to be protected have been identified and prioritised – a successful attack on a controller normally has more serious consequences than one on a visualisation tool – the approach for facing the threat must be decided upon.
The ideal solution is preventing attacks and unintentional security violations before they occur. Due to the complexity and dynamics of the matter, however, this cannot always be accomplished. Because even if specialists are commissioned to constantly search for new vulnerabilities in the network, there is ultimately no all-round insurance against every eventuality.
What it comes down to here is thus immediately recognising security problems and acting without delay. For this purpose, all events in the network can be logged and then evaluated, among other things. It is thus possible, for example, to recognise when a certain device was accessed. If maintenance work was performed at a time that is highly unusual, for example, this should set off alarm bells.

If an attack was successful or the data protection was already unintentionally violated, the problem must be rectified as quickly as possible and the cause thoroughly analysed so that it cannot happen again in the future.

5. Implementation of security strategies

5.1. Firewalls

A measure for implementing security strategies is the protection of the network through special devices. Even though routers and switches can support safety mechanisms, firewalls still play an important role. Either software solutions or appliances (combination of hardware and software) are concerned here that monitor the entire data traffic based on individually defined rules and with functions such as deep packet inspection or intrusion detection.
Because firewalls normally require complicated configuration, extensive IT knowledge is required and this is usually not present in the production sector. With the SecurityBridge, Pilz has therefore developed an industry-standard firewall that is easy to put into operation through application-specific presettings in line with the plug and play principle. With this, it is possible to not only protect Pilz control systems against attack and unauthorised access, process data can also be transmitted with low latency.
The most effective security devices do not help much, however, if they were not developed safely from the ground up and this aspect is also taken into account over the entire lifecycle – key word secure by design. Because processors can suddenly no longer be secure, as shown by the example of Meltdown and Spectre. In addition, it is possible that malware is introduced into a production process and then installed in the products, to then be used later as a back door for attacks. In order to prevent this type of scenarios, the manufacturers must constantly monitor the cyber world for new threats and – if necessary – integrate additional safety mechanisms into their devices and provide patches (safety updates) as quickly as possible.

5.2. Segmentation of the network

Firewalls are typically positioned at the transition between a secure and a non-secure network, like between intranet and Internet. This so-called perimeter protection quickly hits its limits, however, when the objective is preventing malware from spreading through the entire network like an epidemic and crippling this together with the connected plants.

The standard IEC 62443 therefore stipulates sectioning networks according to the “Zones and conduits” model.

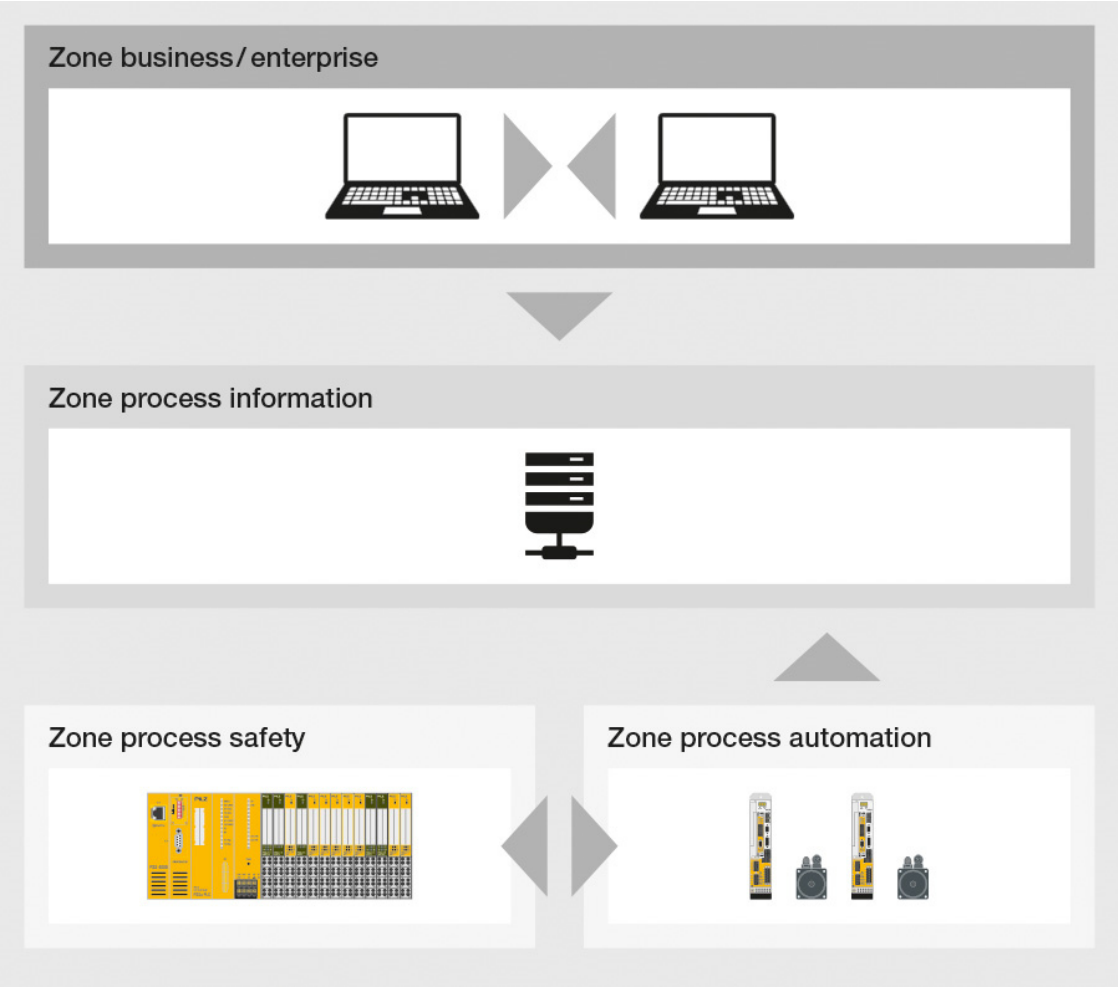


Figure 4: “Zones and conduits” model

The administrative and production networks can be separated in this manner, for example. If necessary, this network can also be segmented, down to the individual manufacturing cells. First zones are identified in which devices have similar security requirements, and then these are sealed off from one another using firewalls or secure routers. It is thus possible to ensure that only devices that are authorised to do so can send and receive information over the lines (conduits) between the zones.
What this means in practice can be seen on the following example: unintentional security violations are frequently caused by incorrectly configured devices. The consequences are, for example, a transmission of data or so-called broadcast storms that can impair other devices in turn. But if networks are segmented into protected subnetworks, only the devices within the zone in which the problem occurred are affected. This is also the case for the effects of unintentional or malicious internal access.

5.3. Defence in depth

To make the work of attackers as difficult as possible, the “Zones and conduits” model can also be used as a central element for defence in depth for the network. This principle, which is used in the construction of fortifications, is based on always placing new and different obstacles in the path of intruders. In the Middle Ages, castles were thus protected by a moat, pit traps, drawbridges, towers and several walls.
The zones and conduits of a network correspond to the gates of a castle. The walls and the other obstacles are formed by firewalls and secure routers that support different security mechanisms. These include for example access control as per IEEE 802.1x and access control lists that block unknown devices and protocols. In addition, there are mechanisms that trigger alarms in the event of suspicious network activity or detect if IP packets with false sender addresses are sent (IP spoofing).
This ensures that one method of attack does not lead to “success” on its own. In order to

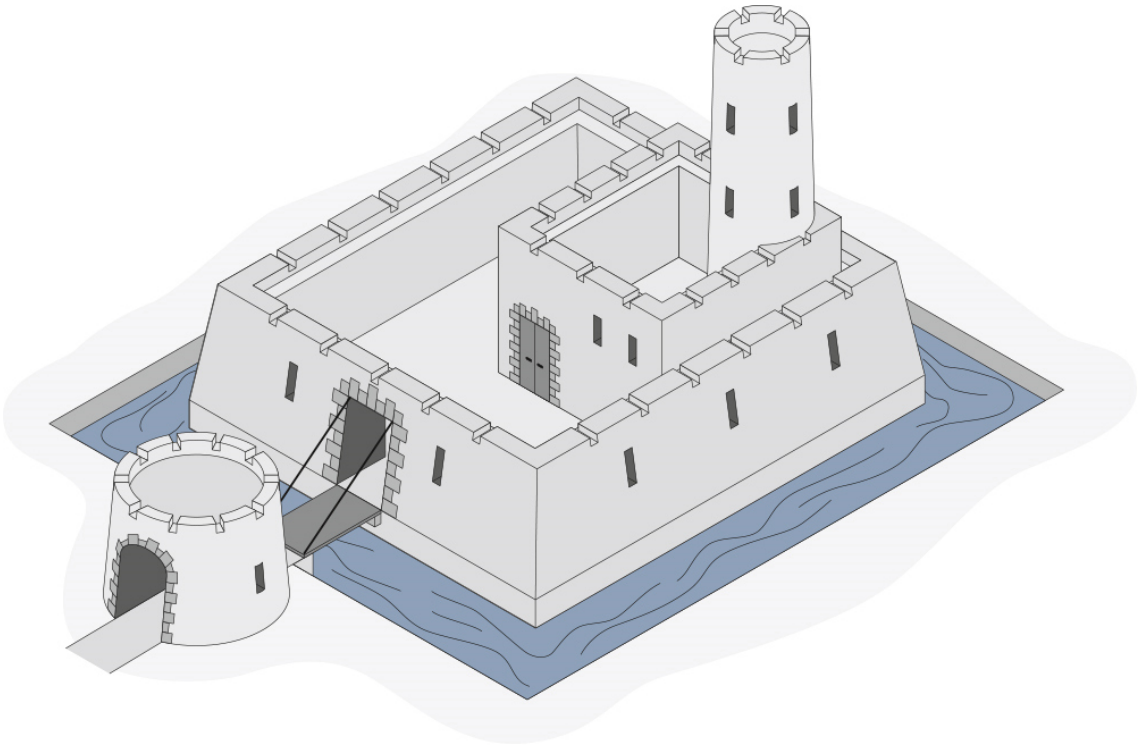


Figure 5: Defence levels using a castle by way of example

advance further into a network, an attacker must therefore continually overcome new, overlapping protective layers. And even if they should manage to infiltrate into the subnetwork of a manufacturing cell, they would find it virtually impossible to attack targets in the adjacent subnetworks from there.

5.4. Organisational measures

Whether manufacturing companies protect themselves against threats from the cyber world is always a comparison of cost and benefit, as already discussed. In Germany, for example, the IT Security Act only obligates those operators of infrastructures that have overall social relevance, such as the energy, traffic and health sectors, to this. Other countries also have comparable legal specifications, like in the USA for the protection of power grids.
Based on the numerous threats, there are many factors to support protecting plants against intentional and unintentional security violations. Sophisticated firewall concepts are not sufficient on their own, however. Instead, the entire company must internalise security, as it were. In addition, guidelines should be established that are not only valid for all employees, but also for partners such as device manufacturers and service providers.
Furthermore it is important that IT and automation specialists work in close collaboration, which means they must become familiar with one another's different requirements and modes of operation. Finally, an organisation should be established whose members are responsible for the data protection in production and its constant improvement. A security representative is ideally at the forefront and is a member of the upper management level or at least reports directly to this.

5.5. Training courses

"If you stop improving, you stop being good" is a recipe for success that companies should also take to heart when it comes to security. Regular training courses offer a possibility for this; they can be used to sharpen the awareness of the employees, for example. Other contents could include information on current threats or instructions on how certain security loopholes can be closed. Because it is only possible to prevent employees from making the wrong decisions due to insufficient qualification if the security competence is expanded in a targeted manner.
There are many providers who perform security training. The seminars from Pilz, which are organised both at headquarters in Ostfildern near Stuttgart as well as at the customer's or – in a more concise form – as a webinar, are particularly aimed at machine designers and plant designers. They give a thorough overview and explain how hazards can be recognised and minimised. The range of topics includes network architecture, the authentication of network subscribers and the encryption of data, as well as secure remote maintenance.

6. Summary and outlook

To achieve the highest possible security, the most important factor is precise knowledge of the architecture of the network as well as the communication protocols and the type of data traffic. This is the only way that both external and internal threats can be averted, whether intentional or unintentional.
Security used to only be a topic in classic information technology (IT). Since series products from the consumer sector and complex operating systems are now increasingly being used in production plants as part of Industrie 4.0, however, automation must now deal with this as well. Because the standards from IT cannot be adopted one-to-one, new standards were developed; of these, IEC 62443 is the most important. This defines how a comprehensive security strategy can be developed and implemented, step by step, for the industrial sector.
At the same time, these strategies must also incorporate safety as their functions can only be guaranteed if the corresponding data are reliably transmitted. Security threats can change constantly and with them the countermeasures. This means that even though both aspects of automation continue to remain independent, they must be closely harmonised with one another. The good news: Anyone already well versed in safety will have an easier time with security because the approaches are similar.

Glossary

Access control list	An access control list (ACL) defines the extent to which individual persons, computers or networks are allowed to use certain services to access the router or switch. Access can be defined for individual computers or networks and for the respective access method.
Broadcast storm	A broadcast storm is a large accumulation of broadcast traffic in a computer network as a result of which it is no longer possible to establish any more network connections and existing connections may be interrupted. A broadcast storm can result from an attack, incorrect configuration or even poor network design.
Deep packet inspection	Deep packet inspection is a procedure in network technology for monitoring and filtering data packets. Through this, spam can be combated and deep packet inspection can also be used for overload check and the reduction of data traffic.
DES (Data Encryption Standard)	Data Encryption Standard, or DES for short, is a standardised symmetrical encryption method.
Hashing algorithm MD5	MD5 (Message Digest Algorithm 5) is included in the group of mathematical one-way functions. This means that there is no easy way to use the result to identify the input parameter. With MD5, any amount of input data is included in a value with a length of 128 bits. With a hashing algorithm, it is assumed that it would be extremely difficult to find two input documents that supply the same result value (collision). In the case of MD5, weaknesses have long been identified that allow an attacker to create collisions.
Intrusion detection system	Using intrusion detection, attacks targeting a computer system or computer network can be recognised in good time so that countermeasures can be initiated quickly.
IP spoofing	IP spoofing refers to falsifying sender IP addresses for IP packets in computer networks in order to use a false identity to try to trick the attacked IT system. Each IP packet contains its sender address in its header data. An attacker can falsify this sender address in the header data so that it looks like the packet was sent from a different computer. Many protocols from the TCP/IP family can only be authenticated via an IP address. If this was falsified, security measures such as authentication based on the IP address in the network can be tricked. IP spoofing is just one type of spoofing here. Currently, “spoofing” is understood to mean all methods with which the authentication and identification process can be bypassed that use trustworthy addresses or host names in network protocols.

Meltdown and Spectre	Meltdown and Spectre are security loopholes that were discovered in microprocessors and through which it is possible to gain unauthorised access to the memory of outside processes.
Network standard IEEE 802.1x	IEEE 802.1X is a network standard for the authentication of users in IEEE-802 networks. This standard functions as a supervisory body that checks the user before it accesses the LAN or WLAN network.
Security objective: Integrity	Integrity in the context of data ensures that data and the mode of operation of a system are always correct. If integrity is guaranteed, unauthorised or undetected changes can be detected and ruled out immediately.
Segmentation of networks	Segmentation means dividing a network into smaller units. These units are then connected using firewalls or other devices with which the communication can be limited. It is therefore possible to limit both the effects of broadcast storms and of other “unintentional” events as well as the effects of attacks.

List of diagrams

We are represented internationally. For further information, please visit our website www.pilz.com or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Fax: +49 711 3409-133, E-Mail: info@pilz.de, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY