



Industrial Security

Why comprehensive security goes beyond office networks

Find out more about:

- ➔ The importance of cybersecurity for an enterprise
- ➔ The implementation of comprehensive security in automation
- ➔ Central areas of action and suggested initial solutions

Introduction

The importance of cybersecurity in all areas of a company has increased greatly in recent years. This shift represents the merger of two different trends. First, the opportunities for criminals to stage attacks are growing as digitalization and networking increase. Second, attackers and their methods are becoming more professional. Accordingly, measures must be taken to protect a company against cyber attacks.

This paper begins by describing the protection of value creation as a security objective in Section 2, along with the special considerations impacting the ICS environment in Section 3. Key action areas are listed along with initial recommended solutions in Section 4.

Content

→ Value creation as a security objective	3
Special features of IT and ICS	4
Joint approach/adapted measures	5
→ Implementation in automation	6
Defense in Depth	7
Consideration within the system	9
→ Areas of action	10
Data loss	11
Malfunctions from external systems	11
Malware	
(USB flash drives/laptops, network)	12
Remote access	13
User management	13
Hardening through secure parameterization	14
Vulnerability and patch management	14
Detection and reaction	15
Security of the runtime environment	15
Awareness and training	15
→ Summary	16
→ References	18
→ Contact	19

1 Value creation as a security objective



Value creation is at the heart of every company. The purpose of cybersecurity is to protect the company's value creation. Individual security objectives are derived from this purpose, such as protecting know-how – including development results or contractual conditions – and complying with statutory regulations, such as data protection. In manufacturing companies, production and delivery capabilities are obviously important. Statutory regulations have been established for critical infrastructure.

Special features of IT and ICS

When comparing the areas of IT and Industrial Control Systems (ICS), arguments often center around the different requirements of the two areas (see figure 1). In automation, the physical process is the focus: something needs to be drilled, punched, or measured. Systems are operated as long as they facilitate economical manufacturing.



ICS security 	IT security 
Priorities	
Availability Integrity Confidentiality	Confidentiality Integrity Availability
Properties	
Availability	
100 %	99% sufficient
Restart	
Difficult	Possible
Patch management	
Great challenge	Automated possible
Service life of hardware	
7 - 20 years	3 - 5 years

Figure 1: Comparison of security in IT and ICS environments

This means they have a much longer service life than in an IT environment. The other challenges associated with automation are sufficiently clear: each malfunction reduces productivity. In addition, the options for eliminating vulnerabilities are restricted, since restarts can only be carried out in some cases, and since any change to an automation system is associated with the risk of further malfunctions.

The security measures selected and implemented in IT and ICS environments differ. However, all elements are needed for value creation. Whether production is shut down due to a cybersecurity incident in the manufacturing process, or due to the failure of a central service – such as the ERP system – is not relevant when it comes to the economic result.

Joint approach/ adapted measures

Therefore, cybersecurity is not an issue that can be addressed with isolated individual concepts. An effective and efficient approach can only be developed through a coordinated joint procedure.

This is particularly important because security expertise is available in the IT environment, although it is frequently lacking in production. On the other hand, the specific features of production must also be taken into consideration.

This must be based on an information security management system, for instance in accordance with ISO 27001 (1) or IT basic protection (2) from the German Federal Office for Information Security, which is generally extended starting from the IT to the ICS environment.

2 Implementation in automation



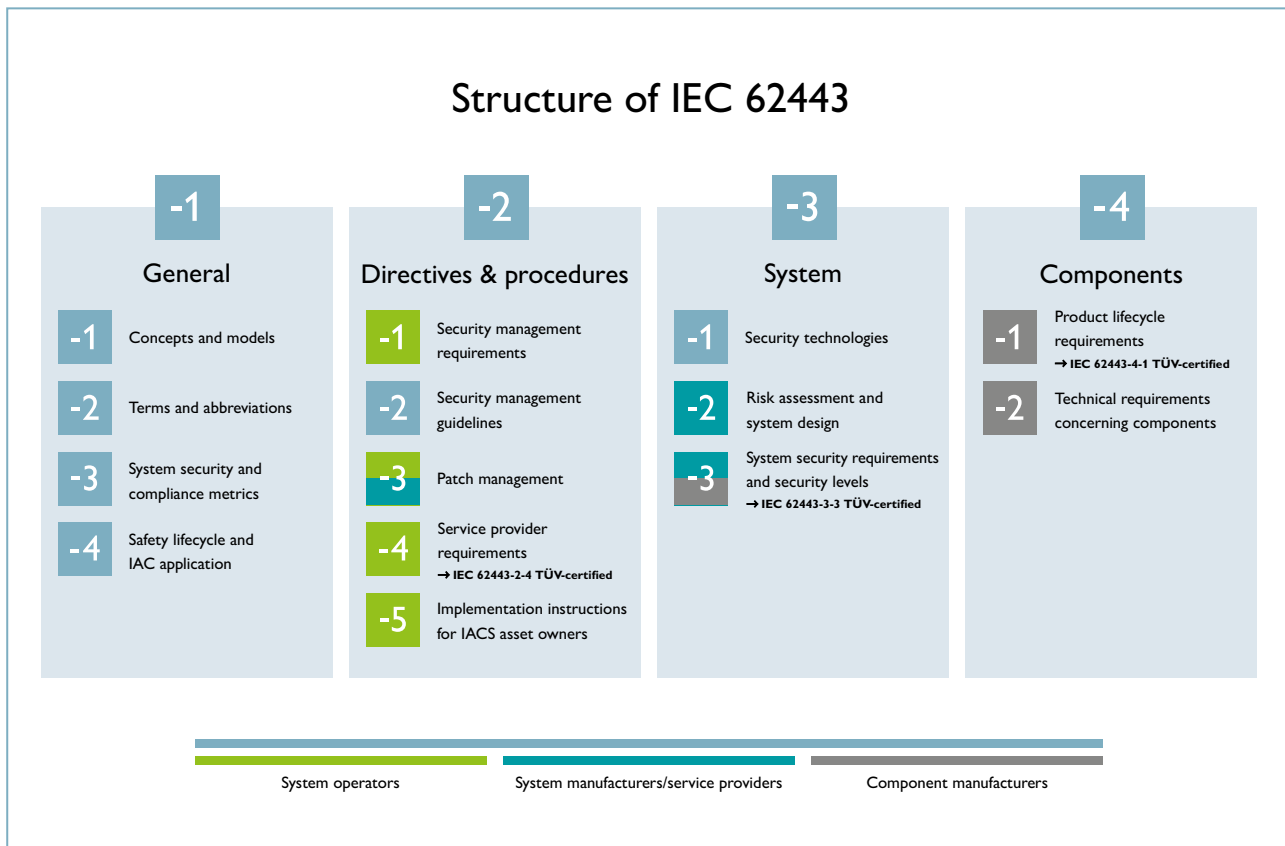


Figure 2: Overview of IEC 62443

The security standard IEC 62443 (3) was developed to address these special features of the ICS environment. It describes and provides further detail on the automation-specific process. The areas of action listed in Section 4 are based on the issues addressed in IEC 62443. One special element of IEC 62443 is the comprehensive approach, which ranges from requirements for operating processes to requirements for systems and products, and describes both procedural and technical measures and requirements. The following section explains the two key principles that underly IEC 62443.

Defense in Depth

One key security concept that is also used in IEC 62443 is “Defense in Depth”, see figure 3. 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 have to first overcome one or more firewalls before reaching the target component. There, the attacker would have to overcome a user login, only to be stopped by internal security mechanisms, see figure 4. Even if one of the security mechanisms fails, therefore, the entire security model does not fall like a stack of cards.

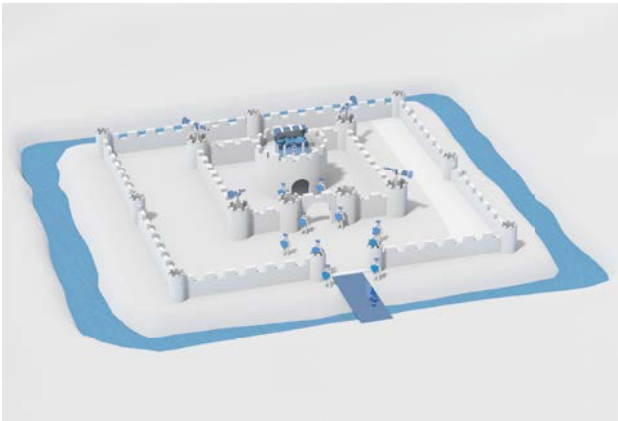
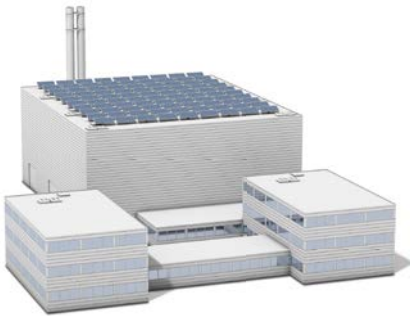


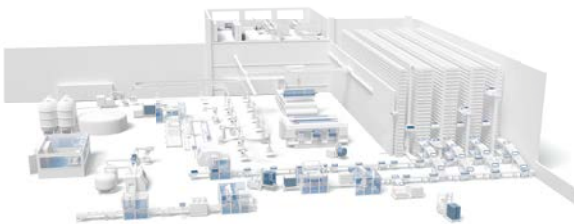
Figure 3: The Defense in Depth concept

The “Defense in Depth” concept is, therefore, realized through the interaction between the different security mechanisms. Therefore, it is also important to consider all of the security mechanisms as a system.



Company level

- Physical measures
- Rights concept (access, entry, authorization)
- Awareness training
- ISMS processes



Network level

- Network segmentation (zones, conduits)
- VPN
- Encryption
- Firewalls
- Attack detection



Product level

- Security features
- System hardening
- “Security by Design” components

Figure 4: Defense in Depth implemented

Consideration within the system

The interaction of different individual aspects within a system is one area of conflict within threat and risk analysis. Designing a secure system requires secure components. However, the level of security that can be achieved depends only very indirectly on the security characteristics of the components. Unsecure components, for instance, can be operated in a secure system if they are isolated via upstream measures – such as a firewall – or if they are only secured by technical and organizational measures.

Conversely, it is possible to implement and configure components with a high level of security inappropriately, ultimately creating an unsecure system.

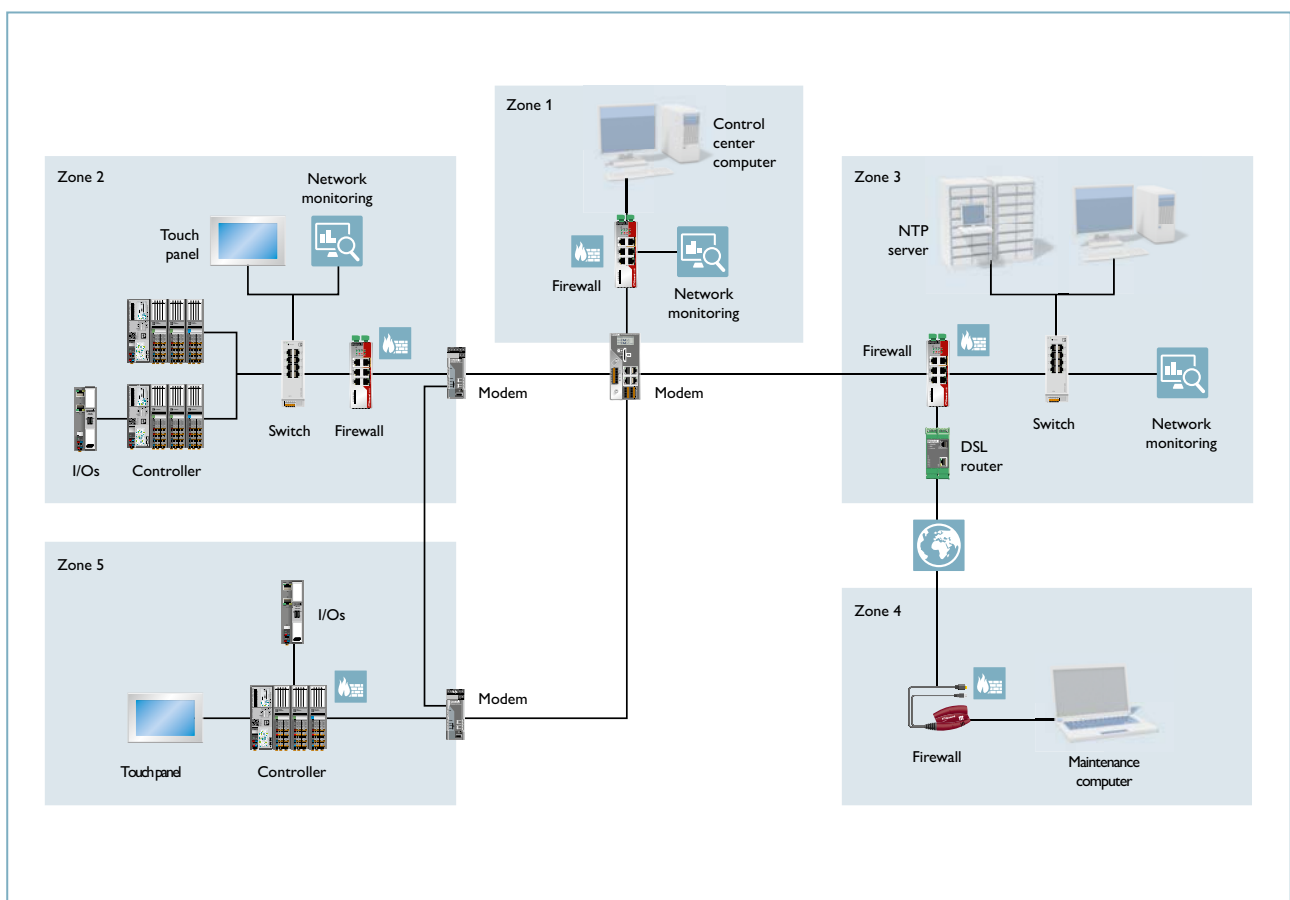


Figure 5: Security in the system framework

3 Areas of action



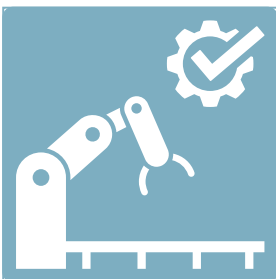
Although there will always be individual requirements and measures in each use case when protecting automation systems, there are central areas of action that are comparable for the majority of applications. These are described in the following section.



Data loss

Data loss can be caused by a variety of different events. In addition to natural catastrophes that cause property damage, systems or data storage media may also be defective. Data can also be deleted accidentally or intentionally, or encrypted in the case of ransomware.

Different counter-measures can be implemented depending on the threat, and should, ideally, be combined. Simple hardware failures can be addressed through redundancy (storing data in multiple locations). Appropriate access control, which narrowly limits who requires write access, restricts damages caused by deletion or encryption. Backup data storage systems should not be permanently connected to active systems; a data storage system in a cabinet is immune to ransomware. Regularly moving backups out of the facility, for instance to a bank vault, can help prevent major damages within a company's own systems. And never forget to check the backups to ensure they can be uploaded once again.



Malfunctions from external systems

Malfunctions in the production network can also be caused by access from other areas. These could be other units of the company or other production areas. The causes include, for instance, incorrect network settings or access that was accidental or not agreed.

In general, it is a good idea to segment networks by application area, and to only permit the connections that are actually necessary. Most office areas, for instance, do not need access to production. Manufacturing areas or machines likewise only communicate directly with one another in very rare cases; instead, they communicate with control systems and central IT services, such as ERP systems or user management. For segmentation purposes, IP networks should be created that are connected through firewalls, routers, and layer 3 switches.



Malware

One important element is protection against malware, such as viruses and Trojan horses. Many Windows systems are used in automation technology on which virus scanners can disrupt the automation function, or in which updates of virus patterns are impossible or possible only with difficulty. In this respect, different protective concepts must be used which are also based around the potential infection pathway.

USB flash drives/laptops

Many infections occur through mobile data storage media; USB flash drives, in particular, represent a high risk since they do not offer any hardware write-protection. A USB flash drive can become infected without the user's knowledge.

Unless absolutely necessary, the use of USB flash drives should be avoided and USB ports should be blocked. If USB flash drives are used, then dedicated flash drives should be used for each application that are not used for any other purpose. Private use of these flash drives should be prohibited. In addition, USB flash drives can be scanned with the latest virus software. External USB flash drives, for instance those brought in by service personnel, should always be scanned and only inserted by service personnel if they have explicit permission to do so.

External laptops should be treated in a similar fashion, and should only be connected to a system or to the company network after a virus scan and with explicit approval.

Network

If systems in a network are infected with malware, there is a risk that it may spread further, for instance through transfer to network drives or by being spread actively from one system to the next. Malware can be brought in unintentionally and without being detected when accessing the Internet.

Network segmentation is also effective in this case, as production systems normally do not communicate directly with one another. A firewall can be used to restrict the exchange of data only across necessary connections. Services that are not required should be deactivated. Only very few automation systems require access to the Internet. Wherever such access is needed, only the necessary connection should be possible. If access is necessary for employees in production, they can access the Internet through a normal work station computer assigned to the office segment.



Remote access

Remote maintenance is an important concept for increasing productivity. However, remote access also poses risks, such as infection with malware. In addition, it could be technically possible to receive access to other resources through the system via remote access. Finally, it must be remembered that the operator is not on site, and therefore not necessarily aware of the surrounding environment. They could, for instance, cause an accident through remote access, because they have no visual contact with employees on site.

Therefore, remote access should be possible only “on demand”. Frequently, a key switch is used to switch to a “maintenance mode”, in which a system only operates under special considerations, for instance for the purpose of operational safety. A suitable firewall should activate specialized rules in this case to block access to the production network. Here, as well, access should be restricted only to the required interfaces. For instance, if access is restricted only to the transfer of the desktop, then the risk of infection with malware is greatly reduced. Creating (encrypted) VPN connections directly to the individual carrying out the remote maintenance is particularly dangerous, since there is no way to control the actions.



User management

Using group accounts with known passwords exposes systems to attack. There is no way to track actions.

Using individual user accounts with assigned rights reduces the risk. Operators, for instance, may not need the right to write files, so this can be left to the administrators. It may then be possible to eliminate password protection for purely operational purposes. In general, accounts for individual users should be set to central user administration, through which updating passwords and blocking unused user accounts can be regulated efficiently.



Hardening through secure parameterization

Often, automation systems are not delivered with secure default settings, but instead with multiple services and settings activated to make commissioning as simple as possible.

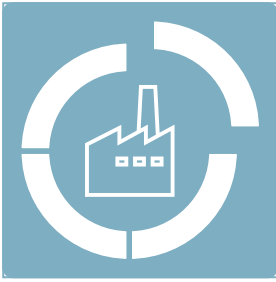
Therefore, a hardening process should be carried out, during which all unnecessary user accounts are deleted or blocked. Software that is not in use should be uninstalled or turned off, and unused functions should be deactivated so that only required services are running. A port scan can be conducted to check for open communication ports and unnecessary services.



Vulnerability and patch management

The risk assessment for a component or system can change very quickly when a vulnerability is found. Often, the cause is an implementation error; however, errors have been found in publicly recommended algorithms and protocols.

Here, as well, a vulnerability in one component does not necessarily result in the same assessment on the system level. A critical error in one component function may have no effect on the system level, if the function itself is not relevant or accessible. In this case, users can consider implementing a patch. In general, vulnerabilities should be tracked through the supply chain to evaluate any risks and initiate counter-measures. In the field of automation, the risk of a malfunction following a patch should also be considered.



Detection and reaction

Since it cannot be assumed that preventative measures will defend completely against all threats, provisions for detecting attacks must be implemented.

These include collecting records (log files) and installing systems for detecting anomalies that aggregate further information beyond log data. Analysis of the information can be supported by tools, but ultimately additional time must be planned for personnel to work on this issue as well.

Defense and restoration procedures should be planned and documented for key scenarios, then practiced if necessary. Can systems be quickly disconnected and isolated from the network? Who are the main contact persons? Are there plans and backups for restoration?



Security of the runtime environment

If software is installed for automation applications, then this is reliant on the security of the environment in which it is executed. If engineering software is used on a PC, for instance, then it could be attacked through the operating system or through other applications. In this case, the automation system could be attacked through the engineering software on the compromised PC. The hardening recommendations from the software and operating system manufacturers should be observed in order to reduce this risk.



Awareness and training

Technical measures alone are not sufficient to ensure ongoing secure operations. Employees must develop an awareness for security. Many attacks can only be executed with the (involuntary) support of employees who open mail attachments containing malware or use infected data storage media.

Detecting threats and implementing security measures requires an appropriate level of technical expertise in the area.

4 Summary





Figure 5: 360°security approach

Cybersecurity requires a holistic approach. It starts in the minds of management and employees – people. In addition to technical measures, such as using security products (technology), organizational measures are also an essential part of the picture.

In order to ensure long-term cybersecurity, security management (processes) must be established where IT and ICS collaborate to secure value creation, without ignoring the special considerations in both areas.

References

1. Information technology – Security Techniques – Information Security Management System
ISO/IEC 27000:2017
2. IT basic protection catalog: German Federal Office for Information Security
3. Security for industrial automation and control systems
IEC 62443

Contact

How secure is your company?

Let us help you protect your industrial networks against unauthorized access and malware.
Book your consultation now!

<https://phoe.co/Cyber-Security>

Stay on the ball

- 360° security: Our comprehensive range without compromises
- IEC 62443: Protect your systems against cybersecurity risks with the IEC 62443 standard series
- Check list: Where do you stand when it comes to industrial security? Our checklist is intended to help you gain an initial overview of the state of cybersecurity in your system.