Fachbereich AKTUELL

FBHM-102

DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

Sachgebiet Maschinen, Robotik und Fertigungsautomation

Safety and Security in Networked Production

Stand: 01.10.2018

Translation of the German version.

The safety of production systems is a central prerequisite for the success of the fourth industrial revolution "Industry 4.0". In contrast to English, the term "safety" is used in German for two different technical fields of work. On the one hand, this is the area of occupational safety or technical safety, but on the other hand it is also the area of IT or cyber safety. The German vocabulary does not provide for a clear distinction between the two terms "safety" and "security".

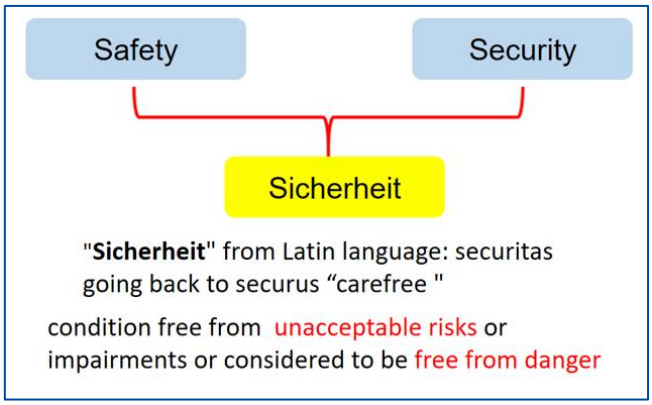

Figure 1: The term "Sicherheit"

So far, these two areas have been dealt with separately, and there has been no joint, interdisciplinary or coordinated approach. This information paper compares the two terms Safety and Security, explains them and describes possible effects of IT security threats for machines and plants, as well as the resulting hazards with a high risk of injury to employees. Basic procedures and measures are formulated to demonstrate awareness of the timely consideration of possible negative effects on production facilities and occupational safety.

A comprehensive description of protection mechanisms against unwanted or unauthorized access to technical equipment is specific to each plant or machine and is therefore not the aim of this information document.

> Definitions or explanations of terms, formulations and abbreviations are given in a glossary on page 8 of this publication.

Table of contents

1 Introduction

In the last twenty years, the degree of automation of machines and plants has increased faster and more comprehensively. In particular, the application of programmable electronic controls and computer systems with constantly increasing processing speed, complexity and extended interfaces to sensors and actuators enables permanently new applications. From the point of view of technical safety, this was not very problematic in the past, since although the degree of automation of machines and plants increased,

the machines were operated predominantly in "stand-alone operation" or only with networking within a production plant. As a rule, there was no overriding link with plants and machines in other production lines or plants. Thus the consideration of safety-related aspects has so far concentrated only on the trouble-free and application-safe operation of machines and plants. It considers hazards caused by failures that occur without external influence. These include in particular hardware or software errors as well as operating errors. The requirements were specified in the European Machinery Directive **2006/42/EC** and in various harmonized standards under the heading "functional safety" and are generally assigned to the term "safety".

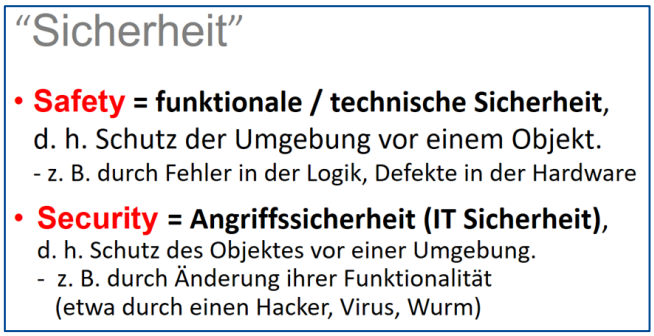

Figure 2: Definition "Safety and Security"

Taking into account further technical developments, the connections between individual machines and complete production lines will no longer be based only on networking within a single production facility, but also on regional and global links to production facilities at far-flung production locations. However, this also means that one can no longer speak of so-called encapsulated production systems. Rather, it must be taken into account that the data exchange of machine information takes place via data paths that also allow unwanted access to safety parameters and other production and safety-relevant data. Protection of data exchanged via data networks is therefore indispensable. Protection against possible deliberate attacks by unauthorized persons will be provided as information security, taking into account technical developments, the connections between individual machines and complete production lines will no longer be limited to networking within a single production facility, but will also extend regionally and globally to production facilities at far-flung production locations. However, this also means that one can no longer speak of so-called encapsulated production systems. Rather, it must be taken into account that the data exchange of machine information takes place via data paths that also allow unwanted access to safety parameters and other production and safety-relevant data. Protection of data exchanged via data networks is therefore indispensable. Protection against possible deliberate attacks by unauthorized persons is referred to as information security. Information security has the protection objective of ensuring the confidentiality, availability and integrity of information and is generally referred to as security, IT security or cyber security. Security aspects are currently neither included in the European Machinery Directive 2006/42/EC nor in harmonized standards for the safety of machines and plants.

In the past, there was little need to consider security aspects in the area of safety. The attack scenarios from the IT security area in recent years have shown that this topic should also be considered for the safety area (within the framework of occupational safety). From the point of view of the necessary development of machine and system controls, a simultaneous consideration of safety and security is already urgently required in automation systems of machines and systems.

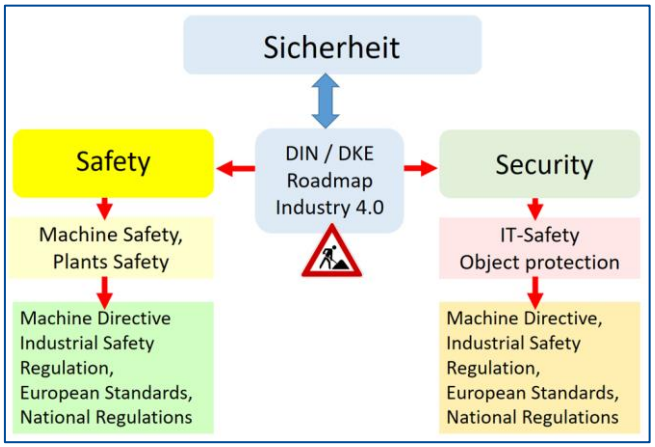

Figure 3: Application field of safety and security

2 Possible hazard factors and their consequences

IT manipulations in which people were endangered were, for example, attacks on control systems of railways, power supply systems, traffic lights or even complex blast furnace controls in a steel mills. In this context, it is a matter of time before further incidents with bodily injuries of employees become known to the public.

This shows that the manipulation of industrial controls is a focus of hackers who have long since

ceased to limit themselves to the theft of credit card or account information. The aim of the attackers in such cases is to maintain control over complex industrial plants. Possible attacks and manipulations can lead on the one hand to a complete loss of production or to the theft of production and process data as well as know-how; on the other hand they can also have massive effects on machine safety and thus on occupational safety. Changes in machine parameters can, for example, affect safety devices for personal protection. Safety functions could be manipulated in such a way that they are passivated, that speeds are changed or that an unwanted machine start occurs. This can result in major hazards with serious or even fatal injuries to employees. This must be prevented permanently by the actors in occupational health and safety.

However, the protection of networked industrial plants cannot be controlled with the tools with which, for example, office computer networks are protected, because industrial controllers do not currently have antivirus programs, firewalls and other measures known from IT applications. In addition, the operating systems of programmable controllers are also heterogeneous and there is a lack of any software update strategies for existing systems that are to be networked in the future.

Possible effects of hacker attacks
Loss of production
Destruction of machines
Theft of production data
Loss of know-how
Defeating of network communication
Changes in production data -> quality defects
Change of safety relevant information
Passivation of safety devices
Loss of availability due to external activation of safety procedures

Figure 4: Possible effects of hacker attacks

In particular, it should be noted that dangers with regard to manipulation and data theft in networked industrial plants do not only exist through attacks by third parties via the Internet. Direct activities on the machine itself by external maintenance or servicing personnel also entail dangers. Even the use of USB sticks or notebooks, for example, which are directly connected to the control system of a machine, can transmit viruses, Trojans or intentionally copy or modify data (e. g. process parameters).

3 Analysis of existing machines or plants

The lack of common considerations of safety and security requirements in the industrial environment is no longer acceptable against the background of the progressive networking of machines and systems. Measures, strategies and precautions that have become standard in office communication must also be transported into the world of industrial plants. The decisive question is therefore: "How can production systems be protected against unintentional attacks from outside and inside?"

3.1 Basic measure

The most important measure is that within a company the awareness of the danger of manipulation and industrial espionage in production facilities grows and a common "security safety management" for office and automation applications is implemented. The first step here is an analysis that shows which machines and plants can be affected at all. The recording and rough evaluation of the existing machines and plants can be carried out in the sense of a "cadastre". In principle, the following distinctions and initial rough evaluations can be made:

3.2 Machines with contact controls

Machines in which the controls were implemented using contact components are not critical with regard to attacks from outside and also from inside, since they do not have programmable components. External access is not possible.

> There is no need for security measures.

3.3 Machines with electronic controls

Machines in which the controls were implemented via electronic, but not via programmable components, are not critical with regard to external and internal attacks. The control sequence can only be deliberately changed by changing the electronics. External access is not possible.

> There is no need for security measures.

3.4 Machines with programmable controls

Machines in which the controls were implemented using programmable components (usually PLCs

or microprocessor systems) must be further differentiated in terms of execution.

3.4.1 Machine controls without network connections

Programmable controllers without a data connection to another controller or to a higher-level computer system have at least one interface via which a program can be loaded or read. The subsequent connection of a programming system (e. g. notebook, USB stick) makes it possible at any time to change a program intentionally or unintentionally. These program changes can also be triggered by the "infiltration of defective software. Another critical aspect is the PLC or microprocessor system itself. A so-called "sleeper" can already be present in this system since delivery, which can be activated time- or event-related and can influence the machine control. An analysis is therefore also necessary for older machines; possible precautionary measures must be taken.

3.4.2 Machine controls with network connections, but without connections to higher-level systems

Programmable controllers with data connections to other machine controllers, but no connection to a higher-level computer system, have interfaces that can be used to load or read programs. In addition, the connection to other control systems is made via further interfaces (e.g. connection of several PLC systems, decentralized I/O) for a desired data exchange. By connecting a programming system (e. g. notebook, USB stick), it is possible at any time to change a program and/or parameter in the entire networked system, either intentionally or unintentionally. These changes can be triggered by "infiltrating" defective software, which can manipulate not only a single controller, but the entire network, including the higher-level system. Another critical aspect is the PLC or microprocessor systems themselves. A so-called "sleeper" can already be present in them since delivery, which can be activated time- or event-related and can influence the machine controls. With these control architectures, it is particularly important to note that the connected systems do not have to come from a single manufacturer, but can also be from different manufacturers. Even with older machines and plants, an analysis is therefore necessary and possible precautions must be taken.

3.4.3 Machine controls with network connections and connections to higher-level systems

Programmable controllers with data connections to other machine controllers and a connection to a higher-level computer system have interfaces via which programs and data can be loaded or read. In addition, the connection to other control systems is made via further interfaces (e. g. connection of several PLC systems, decentralized I/O) as well as to the higher-level computer systems, which can have a direct connection to the Internet. By connecting a programming system (e. g. notebook, USB stick), it is possible at any time to carry out a program and/or parameter change in the entire networked system, either intentionally or unintentionally. This can be done either via the connection to an interface of the control system or via a higher-level computer. Communication via the Internet is also possible.

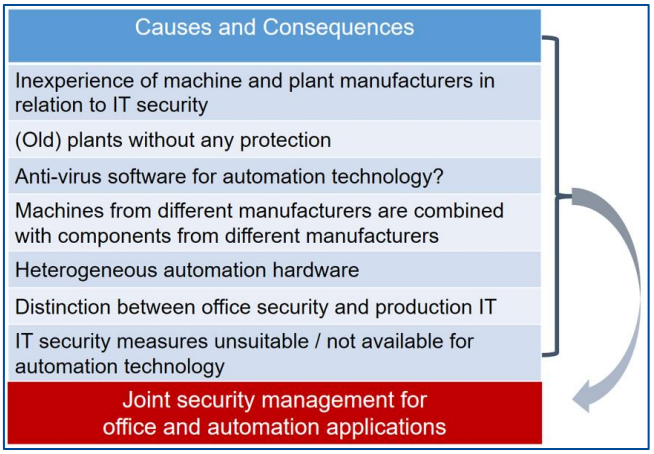

Figure 5: Aspects which favour defeating machines

Program or parameter changes can be triggered by "infiltrating" malicious software that can manipulate not just a single controller but the entire network, including the higher-level system.

In addition to the PLC or microprocessor systems, hazards can also exist in the higher-level computer system itself. Machine controls and/or computer systems can therefore be manipulated both via the "PLC-typical programs" and via the programs used in the office world. With these architectures, it is particularly important to note that the connected systems do not have to originate from a single manufacturer, but can also be from different manufacturers and that the operating systems used can therefore also be diverse. In these cases, the analysis must not only refer to the "control world", but must also include the entire "office environment". This is extremely difficult and complex due to the different views and

languages of the safety world and the security world.

4 Starting points for possible protective measures

The massive gaps in a missing "security view" of networked industrial plants are not manageable with the tools with which, for example, office computer networks are protected. In the private sector, firewalls and virus scanners are generally known and implemented for the security of computers and networks. From the point of view of corporate security, it is not sufficient to implement measures from the private sector in order to achieve comprehensive protection of data and machines. Rather, the project must be worked on systematically in order to achieve the highest possible level of protection. For this reason, the "Industry 4.0 Standardization Roadmap" [1] was developed within the framework of international and national standardization. This standardization roadmap describes already existing standards that may be relevant for implementation within the framework of industry 4.0 and also points out the gaps that need to be closed for successful implementation of future automation requirements.

In particular, the development of technical applications and new work processes, office communication, visualization and the integration of future-oriented products and methods will require new concepts and technologies. In order to achieve the highest possible protection against IT attacks in industrial plants, a systematic approach is required. The following points show an exemplary approach.

4.1 Risk analysis

First of all, a risk analysis should be carried out to identify vulnerable information and components. For the listing the importance must be evaluated.

This indicates whether, for example, data must be guaranteed to be available, traceability must be possible at all times, or it must not be changed (e. g. machine parameters). It should be evaluated what can happen if data, machine parameters or programs fail or get lost due to the access of an external threat.

4.2 Zone classification

As a result of the risk analysis, a zone division can be carried out in the second step. Machines, components and information with similar protection requirements should be combined. This division has many advantages if technical measures are used to derive network segmentation, for example by firewalls. If a zone fails, for example due to a hacker attack, a virus or internal manipulation, other zones are not affected and continue to operate uninfluenced. This network segmentation must be regularly checked for up-to-dateness and effectiveness.

4.3 Authentification and authorisation

In principle, there are individual user accounts in well-structured and secure networks. Each access is authenticated and authorized. Individual user identifications (authentication) and passwords (authorization) for all participants in the network can be used to assign rights in the network. These must be defined in advance and can also be grouped together. For example, machines could only have read access to a network storage if they have to load a machine program from there. Programmers of NC controls, on the other hand, also have write access to defined network components, e. g. machines and plants. In general, it must be specified that passwords are person-related, must be changed regularly and are only accessible to authorized persons. In order to achieve high productivity, it is now also necessary to enable remote access to machines, e. g. from manufacturers. For this application, too, changing passwords have to be assigned in a network and all accesses have to be monitored. In terms of security, there must be no anonymous access to the company network and all access must be secured by secure authentication. This also applies to external interfaces such as USB ports (external installation), Internet (production data acquisition and worldwide retrieval in the sense of Industry 4.0), VPN (remote machine access). Only through this individualization is it possible to assign clear rights in networks and restrict access to the most necessary.

Example 1:

In the event of a malfunction by an external fitter, a machine is contaminated with a Trojan horse smuggled into a USB stick. If the "machine" has unrestricted access to the company network, the Trojan will be able to spread unrestrictedly. If USB sticks are scanned in advance on a stand-alone computer using virus software and machines have clearly defined read and write rights as network components, the undisturbed spread of viruses and Trojans is halted and the damage limited.

Example 2:

Specially prepared USB devices are capable of attacking a system without users being aware of it or virus scanners being able to detect anything. An attacker ensures that prepared hardware (donated USB sticks at trade fairs, keyboards at factory tours left next to PLCs and wait...) is unconsciously connected by technical personnel.

4.4 Wireless communication

In the industrial environment, wireless communication, for example via tablets, laptops and the like, is becoming increasingly popular. It usually takes place via WLAN (wireless local area network) or Bluetooth. The standard passwords of the device manufacturers are often already publicly known after a short time. A change of the standard passwords with sufficient length is indispensable and also the limitation of the range must be limited.

4.5 Remote maintenance

During the remote maintenance of machines and plants, data is transmitted between the operator and the manufacturer via the Internet. If no precautions are taken, this results in several weak points with regard to security. Authentication and authorization mechanisms must be in place. This could be achieved, for example, by manually enabling the required port for remote maintenance or by a separate cable connection to the machine. The transmission of data via the Internet is to be considered. If no further measures are required, data could be intercepted by third parties and read in plain text. For this purpose, it makes sense to establish a VPN connection (virtual private network) and configure it correctly from a security point of view. The advantage is that this end-to-end encryption means that only authorized senders and receivers can read the data. Any "interception" of the data anywhere on the Internet is worthless because the information is encrypted. For secure remote maintenance, it must also be ensured that the maintenance personnel's computer has not been contaminated (e. g. by malware, loss of the key) and that secure encryption using the latest technology is used.

4.6 Monitoring

Once the technical, organisational and personal measures described above have been implemented, it is also essential to implement monitoring. It should archive security-relevant information in read-only form (log file). This includes successful and failed logins with user names and time stamps. Some internal and external attacks can be traced in these log files with technical aids. This can be used to initiate any necessary countermeasures. The use of the latest virus scanners, which are constantly updated, also enables the early detection of known viruses in the company network.

4.7 Backup

If, despite all preventive efforts, a weak point has still been exploited, precautions must also have been taken for this case. Regular backups are an important measure for this. Depending on the importance of the data and the required availability of the stored information, the backup should be organized. Backups must be checked for recoverability and ideally be redundant, e. g. by data carriers that are technically separated after the backup. If individual segments are affected, backups can quickly recover the data, information and process data.

4.8 Organization

Each company must have one person responsible for planning a secure network, implementing the measures and checking that they are up to date. They should also constantly check the system for weak points and organise patch management (repair or improvement management). Also superfluous software and services should be uninstalled and unused hardware components (e. g. USB ports) deactivated.

A good overview of the security measures is required. This documentation includes, among other things, all interfaces, the results of the risk analysis, the distribution of rights, the machine inventory with associated users and passwords (encrypted).

5 Summary and limits of application

The success of Industry 4.0 will essentially depend on whether it will be possible to apply the safety aspects in the same way for Safety and Security. The technical requirements and the behaviour of the machine and plant operators play an equally decisive role here. Even now, the term "safety" must no longer refer solely to the aspect of "safety", but must also always include **"IT security". This shows** that the methods for assessing "safety" have already changed and must continue to be adapted to the development of new products.

This "Fachbereich Aktuell" is based on expert knowledge gathered by the expert committee woodworking and metalworking, subcommittee machinery, robotics and automation of DGUV.

It is intended, in particular, to consider security aspects in the assessment of machines and plants and to implement necessary safety measures.

The provisions according to individual laws and regulations remain unaffected by this "Fachbereich AKTUELL". The requirements of the legal regulations apply in full.

In order to get complete information, it is necessary to read the relevant regulation texts and the current standards.

The expert committee woodworking and metalworking is composed of representatives of the German Social Accident Insurance Institutions, federal authorities, social partners, manufacturers and users.

This "Fachbereich Aktuell" FBHM-102 replaces the version of the same title issued as DGUV Information, published as draft 07/2018. This is the English translation of the German issue "FBHM-102" of 01.10.2018. The translation has been kindly supported by ISSA Section Machine and System Safety, Mannheim.

Further "Fachbereich Aktuell" or information sheets of the expert committee woodworking and metalworking (Fachbereich Holz und Metall) are available for download on the internet [5].

German bibliography:

[1] Deutsche Normungs-Roadmap Industrie 4.0, DIN e.V. und DKE, März 2018

[2] Top 10 Bedrohungen für Industrieanlagen, 24.08.2016, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[3] Leitfaden Industrie 4.0 Security. Handlungsempfehlungen für den Mittelstand, VDMA-Arbeitskreis Industrial Security, Mai 2018

[4] Die Lage der IT-Sicherheit in Deutschland, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[5] Internet: www.dguv.de/fb-holzundmetall Publikationen oder www.bghm.de Webcode: <626>

Picture credits:

The pictures mentioned in this "Fachbereich AKTUELL" have been kindly provided by:

Figure 1, 2, 3, 4, 5: FB HM, SG MRF, Heinke

Glossary

Term	Description
antivirus software	It tries to detect the patterns of known viruses in files and running processes in order to eliminate them..
backdoor	It allows third parties to control a PC remotely and also to use it for criminal purposes.
computer viruses	Are unwanted programs that infiltrate computer programs and can spread after they have been executed by the user.
computer-worm	Malware that, unlike the virus, spreads independently. A computer worm very often uses security holes to penetrate a system.
data securityt	The secure processing, storage and communication of information should be guaranteed by confidentiality, availability and integrity.
firewall	Software between two networks that uses a set of rules to decide which data packets may be transmitted on which path.
hacker	Hackers penetrate computer systems like crackers, but claim that they only want to point out abuses and security gaps.
integrity of data	Data security term: Data contains the correct content, is completely available and has not been altered without authorization.
key-logger	Programs or devices that log keyboard entries. This allows hackers to obtain passwords.
makro, makro-viruses	Macro programming languages allow automation in some document formats. Macro viruses are written in these languages and are embedded in a document (e. g. as a VBA script in a table in Excel format). They become active when the malicious macro is executed.
malware	Generic term for unwanted, malicious software. Malware can cause damage to computers and stored data.
phishing	These are attempts to access the personal data of an Internet user via fake websites, e-mails or short messages and thus commit identity abuse. The aim of fraud is to use the data received, for example, to commit account looting or industrial espionage and harm the relevant persons/companies.
pretexting, identity theft	Obtain data of a third person (under specification of a foreign identity). Pretexting is another term for identity abuse.
spam / junk e-Mails	Unwanted advertising mails. Processing and sorting these e-mails costs time and money. Spam filters try to detect and sort out spam.
spyware	This malware researches the usage behavior and sends the data to the malware manufacturer.
trojaner	This malware is hidden in an apparently useful program and can, for example, read passwords or access data in the network and transmit it to the client of the malware.
confiden-tiality	Data security term: Information should be kept confidential and protected from misuse. Only authorized persons may have access to confidential information.
VPN	Virtual Private Network, an encrypted connection that connects two networks, e. g. via the Internet.
WLAN	Wireless Local Network, wireless network
LAN	Wireless Local Network, wireless network
access to data	Only authorized users should be able to access data. • User authentication by entering user name and password • Password protection of files • Encryption of data makes unauthorized access more difficult
SCADA	Supervisory Control And Data Acquisition (superior control and data acquisition)

Anex 1: Checklist for operators of company networks

This checklist should help the operator to assess company networks and to make them more secure. It makes no claim to completeness.

Question	Yes	No	Not teasing	Where/How
1. basic principles				
(a) Are removable media scanned for viruses before each (even the first) use?				
(b) Are the operating personnel regularly trained in security aspects?				
(c) Are the system maintenance and programming, only systems that have been checked for viruses are used?				
(d) Are regular backups made?				
(e) Is a backup created before every software change?				
(f) Are protection measures updated regularly?				
2. risk analysis				
(a) Are the sensitive information and components identified and listed?				
(b) Has a risk assessment been carried out with regard to the importance and derivation of protection goals (e. g. guaranteed availability of data; digital traceability at all times of production data)?				
(c) Are possible threats and their consequences documented?				
3. zone division				
(a) Machines, components and information of similar protection requirements have been classified in zones divided up?				
(b) Are individual zones separated from each other by technical measures? (network segmentation), e. g. by firewalls?				
(c) In case of failure of a zone (e. g. due to hacker attack, virus, Trojan horse, ...) are as few other zones as possible are affected?				
(d) Is it organized that the network segmentation is periodically checked for effectiveness and timeliness (updates, filter rules, ...)?				
4. holistic organization of Authentication and Authorization				
(a) Are there individual user accounts for all users (User + Password)?				
(b) Is it defined and implemented which rights do users have in the network (read access, write access)?				

Question	Yes	No	Not teasing	Where/How
(c) Are standard passwords of machines and plants changed regularly and are only accessible to authorized persons?				
(d) Are remote accesses monitored and also protected with changing passwords?				
(e) Is every access from machines to the network or from persons to the network/machines authenticated?				
(f) Are accesses to external interfaces (USB, Internet, VPN...) also secured via secure authentication?				
5. protection of radio technologies				
(a) Do the ranges extend only to what is absolutely necessary (signal strength or shielding)?				
(b) Are there secure passwords?				
(c) Have preset passwords been replaced by individual passwords?				
(d) Safety relevant parameters can only be changed via secure communication?				
(e) Are there rules for setting up and terminating a communication?				
6. remote maintenance				
(a) Are there rules for setting up and stopping remote maintenance?				
(b) Are remote maintenance generally carried out via encrypted connections established (e. g. VPN, SSH)?				
(c) Are USB ports secured during on-site installation and equipped with organizational measures? (e. g. USB stick check on gate via virus scanner; maintenance releases USB ports afterwards)?				
(d) Changes that can cause hazards (e. g. machine startup) are only allowed possible, if a confirmation has been made on site at the machine before?				
7. Monitoring and hacker attack detection				
(a) Are at least all external accesses to secured networks logged?				
(b) Are suspicious events such as incorrect password entry, sending data to unknown recipients reported?				
(c) Are countermeasures then be taken?				
(d) Are virus scanners implemented in the network that are always up to date?				

Question	Yes	No	Not teasing	Where/How
8. Backups				
(a) Are regular backups performed?				
(b) Is each zone considered independently of other zones?				
(c) Are the backup media backed up?				
(d) Is the backup protected against unauthorized access and loss?				
(e) Are regular recoverability checks performed?				
(f) Are the backup systems redundant, so that another backup is available in case of non-recoverability?				
9. Organisational measures				
(a) Has an appropriate person responsible for security been designated?				
(b) Is the system regularly checked for vulnerabilities?				
(c) Is update management organized?				
(d) When the system is initialised, is it organised that all individual settings are restored (e. g. access data when a machine computer is replaced)?				
10. Documentation of the security measures				
(a) All interfaces (ports) are documented?				
(b) The results of the risk analysis are documented?				
(c) Has the rights distribution been documented?				
(d) The machine inventory with associated users and passwords (encrypted) is documented?				
(e) Security incidents and their countermeasures or strategies and protective measures derived from them are documented?				

Anex 2: Example Assessment of existing systems

Description of the machine, plant, etc.	Control Devices					Remarks
	Contact-based control devices	Electro-nical	Pro-gramm-able without network connection	Programmable with network connection, without connection to subordinate systems	Programmable with network connection, with connection to subordinate systems	
Bench drill		**X** No measure required				
Press 12			**X** Measures, see DOK…			Communication with machine 1 and 3
CNC milling				**X** Measures, see DOK…		
Automatic storage crane					**X** Coordination with storage computer Measures, see DOK…	Exchange of storage orders with storage computer Y

Publisher

Deutsche Gesetzliche
Unfallversicherung e.V. (DGUV)

Glinkastraße 40
10117 Berlin
Telefon: +49 30 13001-0 (Zentrale)
Fax: +49 30 13001-6132
E-Mail: info@dguv.de
Internet: www.dguv.de

Sachgebiet „Maschinen, Robotik und Fertigungsautomation“
im Fachbereich „Holz und Metall“
der DGUV > www.dguv.de Webcode: d544722

An der Erarbeitung dieser „Fachbereich AKTUELL“ FBHM-102 haben mitgewirkt:

- Normenausschuss Maschinenbau (NAM) im DIN Deutsches Institut für Normung e. V
- Referat 5.2 Maschinen und Anlagen des Instituts für Arbeitsschutz der DGUV (IFA)
- Fachbereich ETEM der Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse (BG ETEM)