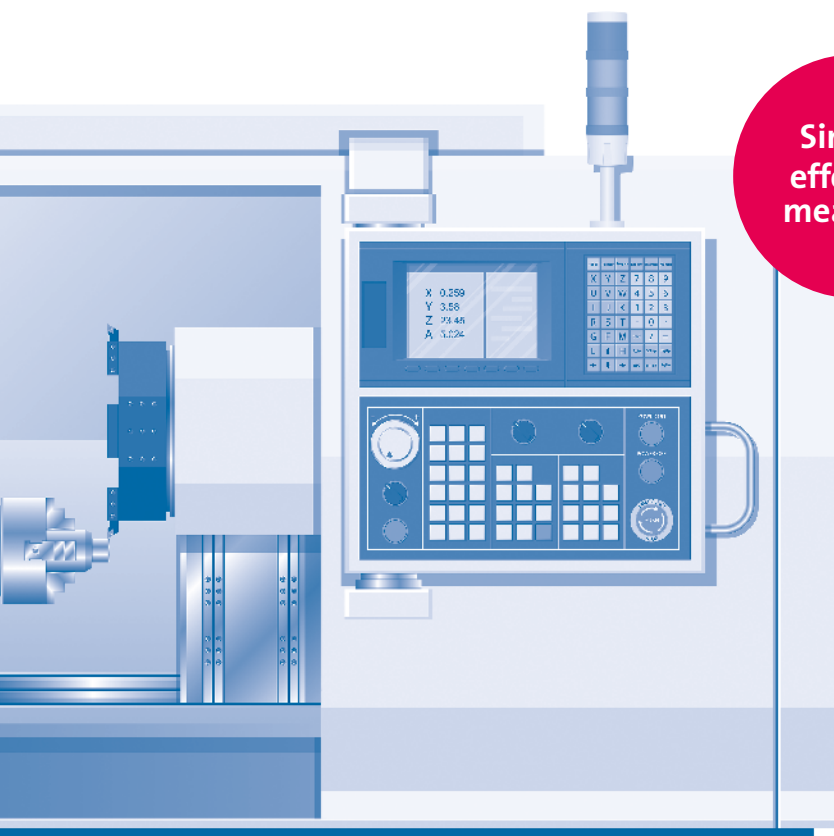


IT Security in Machine Tools

**Simple,
effective
measures**



IT Security in Machine Tools

Manufacturing and process automation systems – **Industrial Control Systems (ICS)** for short – are deployed in almost all infrastructures that handle physical processes. These range from energy generation and distribution through to gas and water supply, factory automation, traffic control technology and modern building management. These ICSs are increasingly exposed to the same **cyber attacks** as conventional IT systems ^[1] ^{[14]*}.

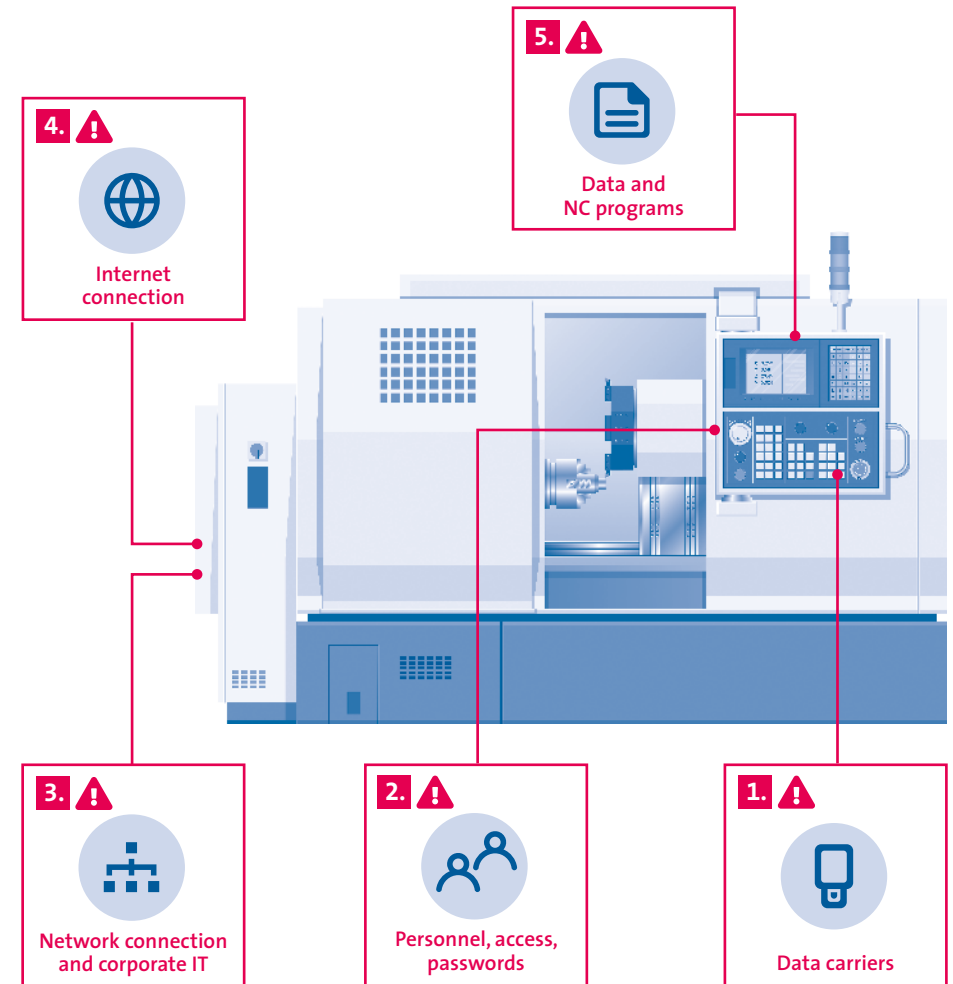
Operators of such systems urgently need to address this issue in view of the **increasing frequency of incidents** and newly identified vulnerabilities. This applies both to infrastructures that are directly connected to the Internet and to those that can be harmed indirectly by cyber attacks. **Equally affected are machines which are used in production, especially machine tools** ^[4]. To exclude oneself or one's company from this threat scenario is not only negligent, but downright dangerous! The question should not be whether but **when an attack will take place and how serious it will be** ^[14].

The question should not be whether but when an attack will take place and how serious it will be.

The **potential for optimisation which arises from the increasing use of IT technologies in the production process** and the possibilities for the enhancement of daily processes are too great for profit-based organisations to ignore. The goal must be to achieve full productivity while ensuring the highest possible level of IT security.

The diagram on the right shows an overview of the points at which special attention is recommended for machine tools with regard to IT security.

The primary aim of this document is to **sensitise** machine tool operators **to the threats** and to **highlight simple organisational and technical measures** which can be used to make **pragmatic** improvements to IT security – especially in existing machines.



A company-specific risk analysis of the cyber threat generally serves as the **starting point for a location assessment**. An initial appraisal can be made using the VDMA's IT security questionnaire ^[3], for example.

Aiming for **maximum comprehensibility and practicability**, this document deliberately avoids in-depth technical discussions of IT security with regard to the company-wide application of newer standards such as **IEC 62443** ^[15]. Anyone interested in these should refer to the relevant literature for further information.

* Further literature and sources of information: See page 13 and 14.

1. Data carriers



Current situation Removable media, **especially USB flash drives**, are in widespread use. They are used for many different purposes, such as **transferring machining programs** and other production or job data **to the machine**, but also as an advertising medium, for general data exchange, supplier catalogues and various other functions. Company employees **often use them privately**, e.g. to transfer documents when working at home. **External personnel**, such as maintenance staff or other service providers, **often use their own removable media**, which then inevitably come into contact with a large number of systems. Mobile phones which are connected to the machine via the USB port also count as removable media. Companies and users are often **not sufficiently aware of** the resulting threat ^{[1] [5]}.

Threats

- ! **Data security:** It is a simple matter to copy and transport data, even across corporate boundaries.
- ! **Risk of infection:** Malware can easily be transferred and introduced via removable media which come into contact with many different systems.

Actions



Organisational

Technical

- ● ● **Regular awareness-raising among users** in companies, especially in production
- ● ● **Obligation of staff to take care when handling removable media**
- ● ● **Provision of company-owned USB flash drives for exclusive use in the company**, ban on the use of private removable and other USB-connected data media, such as portable SSD hard drives or smartphones, in the company
 - Company policy for **access to lockable USB ports**
- ● ● **Exclusive use of company's own data carriers**, which can be personalised and regularly (!) checked for malware
 - ○ Transfer of programs to machines only by means of **dedicated USB flash drives** in computers with regularly updated (!) virus protection
 - **Installation of security gateways**, e.g. with (constantly updated [!]) virus scanners for removable media
 - Restriction of physical access to USB interfaces

2. Personnel, access, passwords



Current situation In many cases, there are **no individual access authorisations and passwords for means of production**. Either there is no active authentication process at all and the “standard user” has the rights of an administrator, or a universally known password is all that is used for protection (e.g. user: “admin”, password: “admin”). This negligence (= **security lapse!**) is often justified by claiming that the equipment requires fast, uncomplicated access to ensure high system availability. The **system password/control password is sometimes permanently activated** on machine tools, too, in order to grant the operator increased user rights. This bypasses the protection provided by the authorisation selection switch. This makes it easy to change key machining parameters, which can in turn lead to production defects and damage to the machine. Physical access to the machine itself is not usually restricted, nor is this possible.

Threats

- ! Access to the devices is often not restricted. **Anyone can then operate and (re)program the machines**. This can include loading, adapting, saving and deleting NC programs, changing parameters such as machine data (e.g. axis accelerations), etc.
- ! In addition, access to one device can often provide **access to other devices, systems or the company's entire IT infrastructure**.

Actions



Organisational

Technical

- ● ● **Confidential handling of passwords!** Only authorised employees should be able to use passwords, even if they are generally known
- ● ● If possible, **personalise** all passwords
- ● ● **Awareness-raising** among employees
- ● Development and implementation of an **access and authorisation system** (Identity and Access Management), e.g. use of **different user rights, also for the control system**, if this is supported by the system
 - **Appropriate use of the authorisation switch** on the machine tool. Most machine tools already have such a (key) switch, but in practice it is not always used
- ● ● **Activation and consistent use of authentication/authorisation as access restrictions**, if available
 - ○ Activation of an **automatic logout procedure** for non-active users, prohibition of permanently active passwords

3. Network connection and corporate IT



Current situation More and more production machines are being integrated into corporate networks (LAN) in order to tap the full potential of networked manufacturing. For example, a machine can communicate with a Manufacturing Execution System (MES), a Production Planning System (PPS) or an Enterprise Resource Planning (ERP) system, e.g. to query stock levels or to report productivity data back to higher levels. In the case of MES systems, connection to the company network is obligatory, but it is then necessary to deploy a separation layer, e.g. Virtual LAN (VLAN). **Separation**^{[1] [7] [9]} of the different network areas and access rights within the company is **highly recommended** and has long been state-of-the-art but has by no means been implemented everywhere.

Threats

- ! Malicious software that enters the network via the office IT environment can **infect or impair production machines**.
- ! Personnel and (possibly also) malware can **compromise devices and data in the office IT system from a production machine**.

Actions



Organisational

- ○ ● Company-wide **definition of necessary and prudent access rights** ("Is it really necessary for the management's printer to be accessible from the production machine?", "Does the security guard need access to the NC programs?", etc.)^[2]

Technical

- ● ● **Restriction of individual users' and devices' access rights** to what is prudent and necessary
 - Logical **separation of the network segments**, e.g. **production separated from the rest of the company**, by means of VLAN, or similar
 - Use of **firewalls, monitoring solutions**, etc.
 - **Restricted logical or physical access** to LAN ports

4. Internet connection



Current situation The connection of company networks and the production machines to the Internet **permits the use of numerous services** which otherwise would not be possible at all, would be much more expensive or would be severely limited (e.g. remote service^[6], business applications [e.g. for payment flows], connection to customer IT systems for order information, etc.). The Internet connection is usually protected by a firewall^[4].

Threats

- ! **External access to system components** if universally known standard passwords (e.g. user: "admin", password: "admin") are used.
- ! **Exploitation of known vulnerabilities** or execution of "zero-day exploits", i.e. attacks via newly discovered loopholes which cannot yet be detected by anti-virus products or similar.
- ! Ease with which **a company's vulnerable control components can be found** using appropriate search engines^[7].

Actions



Organisational

- ● ● Company-wide **determination of necessary and prudent access rights** ("Who's allowed to do what?")
- ● Personalisation of access

Technical

- ● ● Use of a constantly updated (!) and regularly maintained (!) **firewall**
- ● ● Use of **strong passwords, 2-factor authentication where possible, and certificates for external access**
- (Temporary) **deactivation of unused services** and features
- Logical **partitioning of the network segments**, e.g. **production separated from the rest of the company** by means of a VLAN

5. Data and NC programs



Current situation Nowadays **increasing amounts of business-critical information** (not only for production) are available in electronic form, in some cases exclusively. Careless use of removable media combined with inadequate access and authorisation systems allows **easy access to data** ^[4]. For example, technical drawings, quotations, orders, or process parameters and NC programs can be easily copied from a drive or machine to a USB flash drive and removed from the company in somebody's pocket ^{[7] [8]}. Without an access and authorisation system, it is impossible to trace such data theft.

Threats

- ! Data loss as a result of **incorrect operation** (accidental deletion or moving of data).
- ! Data loss due to **malware** (e.g. blackmail trojans, phishing, etc.).
- ! Data theft and **loss of know-how**.

Actions



- | | | |
|----------------|-------|--|
| Organisational | ● ○ ● | Classification of the value of corporate data and information , regulated handling, protection, backups and destruction |
| | ○ ● ● | Creation of a strategy for regular data backups , including production data such as NC programs, including data from machines on the shop floor |
| | ● ○ ● | Introduction of standardised procedures for handling the data that is accessible to new employees and to those leaving the company |
| Technical | ● ○ ● | Establishment of access restrictions for all information in the company (permissions) |
| | ○ ● ● | Inventory , personalisation or listing (whitelisting) of authorised data carriers in the ICS network |
| | ○ ○ ● | Data encryption for transfer of data on data carriers and in devices (e.g. PCs) |
| | ● ● ● | Monitoring and reporting of unusual data access, connections or connection attempts |
| | ● | Further technical security measures such as segmentation of networks, deactivation of Internet access, setting up VPNs, firewalls, etc. |

IT Security Glossary

Safety and security

Safety is generally used to describe **functional or personal safety**. **Security**, on the other hand, refers to the **protection of IT systems (data security)**.

Safety is always important and is a legal requirement. The increasing degree of digitalisation in production means that data security is becoming more and more crucial for trouble-free operation; see also the further explanations in this publication.

Credentials

Login data.

Usually a combination of username and password.

Phishing and social engineering

Fake information (concerning the sender or documents) is used in attempts to obtain **confidential information and access rights**.

Classic examples are emails from ostensibly known senders with requests to open a certain document (*"We enclose confirmation of your order. Please check for accuracy", "Please update your payment information", etc.*). The name of the sender of such mails is usually false. The documents or links they contain establish connections to background websites which, unnoticed, load the malware onto the computer and thus compromise the system: the attacker can/may do anything that the user can/may do (access/delete files on the network, etc.).

IAM (Identity and Access Management)

Management of the identification and access rights of a system's users.

Discrete access rights allow user-based access to data and information. Examples include a Windows login or ERP access authorisation. The software component which manages the various user identities and their access rights is called IAM.

Whitelisting / Blacklisting

Exclusive admission (whitelisting) or targeted exclusion (blacklisting) of specified devices, data media, etc.

Whitelisting can be used to restrict access to the company network to certain, desired devices. Blacklisting is used e.g. to block known and undesirable individual senders of spam.

(Zero day) exploits

Exploitation of (recently discovered) security vulnerabilities.

Exploits are used to take advantage of security vulnerabilities in software components in order to get access to the system. Particularly critical are security vulnerabilities when no patch (measure) is yet available from the manufacturer or when they are exploited for the first time so that protection software cannot detect them yet ("zero day").

Botnet

In a process usually unnoticed by the infected user, an external computer (master) remotely controls a large number of decentralised computers (slaves) by means of malware installed on them.

Botnets can cause damage in two ways: directly, by utilising the computing power which slows down the affected systems and can make a machine control difficult to operate; and indirectly through actions that are initiated by the master (= control computer) but carried out in the name of the slave (= the infected computer), e.g. sending spam using the company's address, or worse (copyright infringement, criminal content, etc.).

DDoS attack

DDoS stands for "Distributed Denial of Service"; a DDoS attack usually leads to mass requests from many different (distributed) devices, which then overload the attacked service/server and thus shut it down as a result.

In order to carry out DDoS attacks, the attacker needs control over a large number of devices which can be obtained via a → **botnet**, for example. Web servers are often the target of the attack (result: "*page not accessible*"), but other services can also be targeted, e.g. databases.

Network segmentation

Partitioning of a network into a number of segments that are logically separated from each other.

Network segmentation is the logical (as opposed to physical) separation of a large network into several sub-networks. This way, segregated areas can be set up for production and accounting, for example, without the need for new network cables to be laid. However, components such as switches may have to be replaced.

VPN (Virtual Private Network)

A virtual network segment that provides a protected area within a large network such as the Internet (e.g. for access to the company network via the Internet).

A VPN can be used to set up a "secure island" in an insecure environment. A VPN logically integrates the user fully (!) into the network, thereby permitting all activities normally performed in the local network to be carried out without the need for further measures.

IPsec, L2TP, OpenVPN, IKEv2, PPTP ...

Protocols for VPN provision, depending on the producer (e.g. IPsec from Cisco).

The protocols used depend on the producer of the VPN solution.

TLS (Transport Layer Security)

Modern encryption method used e.g. for websites (https://), successor to SSL (Secure Sockets Layer).

If data is transmitted in unencrypted form over the Internet (e.g. using "http://" instead of "https://"), it can be read by third parties. For this reason, modern web browsers often issue a warning if an attempt is made to access unencrypted pages.

OT (Operational Technology)

Is the means of production, as distinct from IT (Information Technology).

Term generally used by IT experts for production technology in the broader sense.

IT security affects the entire company


“Information security, once achieved, is not a steady state, but a process that needs to be continuously adapted.”

This is taken from the document **“Guide to Basic Protection based on IT-Grundschutz”** published by the German Federal Office for Information Security (BSI) ^{[12] [18]}, which is highly recommended for implementation. In practical terms it means that **all employees and company departments** – from management, production and the various other departments through to external service providers ^[10] – are responsible for ensuring IT security ^[11]. **Organisational and technical regulations must mesh together** and be constantly adapted to meet new requirements as they arise.

Production machines in particular place special demands on the company-wide IT environment. These are usually **preconfigured systems** consisting of many different and closely coordinated components that cannot or should not be changed or regularly updated. Key technical considerations include **exacting reliability requirements** and **coordination of the software components with the respective hardware**. The machine’s user interface (HMI) is also often adapted to customer needs. Changes to this system, such as a virus scanner, always require the approval of the machine manufacturer.

Accordingly, such production machinery and equipment must be protected by a robust and resilient IT environment. The **VDMA guidelines for SMEs** ^[1] and the aforementioned **BSI basic protection** ^[12] (especially its additional “IND” ^[13] module for industrial environments) provide a broad overview and useful introduction to the topic. The BSI also offers platforms for exchanging views and experience on IT security with other companies ^{[16] [17]}.

Further reading and sources of information

Associations		Source*			
[1]	Guideline Industrie 4.0 , ISBN 978-3-8163-0687-0 (2016) Content: Recommendations for SMEs, introduction to the topic for the whole company, focus on office IT (available on request)	VDMA	●	●	●
[2]	Guide Cyber Security Check (2020) Content: Introduction to internal IT security analyses, focus on office IT	ZVEI, VDMA, IDSA	○		●
[3]	Fragebogen zur Selbsteinschätzung der IT-Sicherheit (2014) ** Content: Guide for conducting internal self-assessments	VDMA	●	●	●

Federal agencies		Source*			
[4]	Sicherheit für die Industrie 4.0, Studie (2016) ** Content: Comprehensive study on IT security in industry	BMWi	●	○	●
[5]	Empfehlungen für Betreiber von ICS – Erfahrungen aus der industriellen Sicherheitsberatung v2.0 (2018) ** Content: Short information leaflet on the organisational framework	BSI	●	●	●
[6]	Remote maintenance in industrial environments v1.0 (2015) Content: Recommendations on remote service	BSI		○	●
[7]	Industrial Control System Security: Top 10 Threats and Countermeasures v1.3 (2019) Content: Summary of IT security, especially for automation technology and industrial production	BSI	●	●	●
[8]	Industrial Control System Security: Inside threat [English] v2.0 (2018) Content: Catalogue of measures and recommendations	BSI	○		●
[9]	Empfehlungen für Betreiber von ICS – Monitoring und Anomalieerkennung in Produktionsnetzwerken (2019) ** Content: Information booklet	BSI			●
[10]	Empfehlung zur Cyber-Sicherheit – Sicherheit von Geräten im Internet der Dinge (IoT) (2017) ** Content: Recommended action	BSI	○	○	●
[11]	Recommendations for further education and qualification measures in the ICS environment v2.0 (2018) Content: Recommended action	BSI	●		
[12]	Guide to Basic Protection based on IT-Grundschutz (2017) Content: Recommendations for handling IT security in the company as a whole	BSI	●		●
[13]	Plugin “IND”, excerpt of “IT-Grundschutz Compendium” (2019) Content: Special IT system requirements in production (ICS, OT)	BSI		●	●

Science and research

Source*



- [14] **Cyberangriffe gegen Unternehmen in Deutschland, Forschungsbericht (2020)****
Content: Comprehensive study on cybercrime, abridged version/ management summary also available

Criminological
Research
Institute
of Lower
Saxony



Standardisation

Source*



- [15] **IEC 62443 series (2020)**
Content: Multi-part series of international IT security standards

IEC



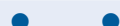
Online resources

Source*

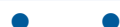


- [16] **www.allianz-fuer-cybersicherheit.de****
Content: IT security exchange forum for SMEs
- [17] **www.it-sicherheit-in-der-wirtschaft.de****
Content: Information portal on IT security, aimed primarily at SMEs
- [18] **Online course: "IT-Grundschutz"*****
Content: Online course linked to corresponding publication

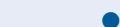
BSI



BSI



BSI



© Copyright 2021

Publisher

German Machine Tool Builders' Association
Machine Tool and Manufacturing Systems Association
within the VDMA
Lyoner Strasse 14
60528 Frankfurt am Main
Phone +49 69 756081-0
Fax +49 69 756081-11
E-Mail vdw@vdw.de
Internet www.vdw.de
Twitter www.twitter.com/VDWonline
YouTube www.youtube.com/metaltradefair

Chairman

Dr. Heinz-Jürgen Prokop,
Trumpf Werkzeugmaschinen GmbH + Co. KG, Ditzingen

Executive Director

Dr. Wilfried Schäfer

Authors

"Control Technology and Systems Engineering"
working group of the VDW Research Institute, with
expert advice from Prof. Dr. Felix Hackelöer, Institute
for Automation and Industrial IT (AIT), TH Köln

Design and layout

Klaus Bietz \ visuelle Kommunikation, Frankfurt am Main

Printing

Druck- und Verlagshaus Zarbock GmbH & Co. KG

Date

03/2021

Acknowledgements for photographs

Adobe Stock

* The sources can be found via a simple Internet search.

** Only available in German.

