Baština Akademije nauka i umjetnosti Bosne i Hercegovine

Basic Technologies and Models for Implementation of Industry 4.0

Karabegović, Isak

2023-10-04

https://bastina.anubih.ba/handle/123456789/779

Preuzeto s Baštine Akademije nauka i umjetnosti Bosne i Hercegovine

https://bastina.anubih.ba/

DOI: 10.5644/PI2023.209.02

Occupational Safety when Accessing Machine Remotely

Viktorijo Malisa[*1]

Abstract: *Machines have been equipped with the technical capabilities to send and receive data over networks for a long time. Today, not only machines, but entire production systems are networked worldwide to take advantage of information technology. Remote access to the machine is increasingly used to commission the machine, diagnose faults, adapt it to production, update functions and operating systems, or even have a machine repaired remotely by a specialist. However, the type of remote access must be tailored to the specific machine and therefore described in detail in the machine documentation. The special feature of remote access is that it combines cybersecurity with machine safety and occupational health. This requires that both the machine operator and the remote maintenance service provider are integrated into the respective organizational structure. The aim of this article is to describe the technical requirements for the secure implementation of remote access to machine controls and to highlight the necessary normative, organizational and preventive security measures.*

Keywords: *Occupational safety, OT-safety, remote access, remote maintenance, IT-security*

1. Introduction

With the Industry 4.0 initiative and the associated increasing digitalization of all technologies, machines and production processes, remote services have also evolved. Remote access to machine controls, IT systems, servers and computers is primarily used for remote control, remote monitoring and maintenance work.[13] Efficient service, fast troubleshooting and expert system diagnostics from a distance enable the operator to minimize downtime and provide the machine manufacturer or system integrator with efficient remote support, especially during the warranty period. Remote maintenance has gained tremendous importance due to the globalization of markets, technological advances in digitalization such as the Internet of Things (IoT), cloud services, video conferencing technologies and remote access software, and most recently increased global crises and supply chain disruption. However, in the context of remote maintenance, there are not only advantages, but also threats and dangers, so that technical and organizational prerequisites must be created and special

[*1]AUVA Allgemeine Unfallversicherungsanstalt, Vienna
E-mail: viktorijo.malisa@auva.at

security measures must be observed.Due to frequent cyberattacks through remote connections on production systems [7], IT security measures must be adapted to the systems in use [8].
Remote maintenance is not explicitly defined in the Machinery Directive 2006/42/EC, which is still valid. However, more and more established standards are being supplemented by the topic of remote maintenance and safety of IT (information technology) and OT (operational technology). For example, the current C standard EN ISO 10218-2 ‘’Industrial robots - Safety requirements - Part 2: Robot systems and integration’’ deals in detail with the topic of remote access to the robot controller, as well as the Technical Report CEN ISO/TR 22100-4:2021, ‘’Safety of machinery - Relationship with ISO 12100 - Part 4: Guidelines for machinery manufacturers on the consideration of related IT security (cyber security) aspects’’, which establishes the relationship between EN ISO 12100 ‘’Safety of machinery - General principles for design - Risk assessment and risk reduction’’ and cyber security.

2. ‘’Remote Access’’ Operating Mode

Remote access to a machine is when a person connects to the machine control via an electronic device without being able to see the machine and its surroundings. For example, the production equipment is on the ground floor and the office area of the technical department is above the production hall. If the technician (see Fig. 1, item 3) connects to the machine (see Fig. 1, item 1) via the company’s internal network (intranet), this is also referred to as remote access, just as when the remote maintenance specialist (see Fig. 1, item 2.) is in another location, in another country, and can access the machine control via a connection. It often happens that the production manager (see Fig. 1, item 4.) wants to view the machine’s data from the home office via the Internet or directly from a meeting on the company premises via W-LAN, so this operating mode is set up.

Basically, the following services are performed remotely by specialists (modified according to [14]):
1. In the remote access operating mode
- Diagnosis of the software
- Error analysis
- Production monitoring
- Inspection, data analysis and data transmission
- Training of operating and maintenance personnel
- Regular drills for all departments involved, scheduled drills as well as extraordinary drills after installation of new hardware and software

2. In remote control mode:
   - Starting and stopping certain functions (heating up, cooling down, emptying, feeling up, etc.)
   - Starting and stopping the machine

3. In remote maintenance mode:
   - Remote parameterization (changing adjustable parameters)
   - Software patch and updates (installation of new programs)
   - Commissioning (transfer of all software)
   - Maintenance support, retrofitting, support
   - Malfunction management, machine diagnosis (intelligent error detection, error codes with stored measures)
   - Installation of new functions

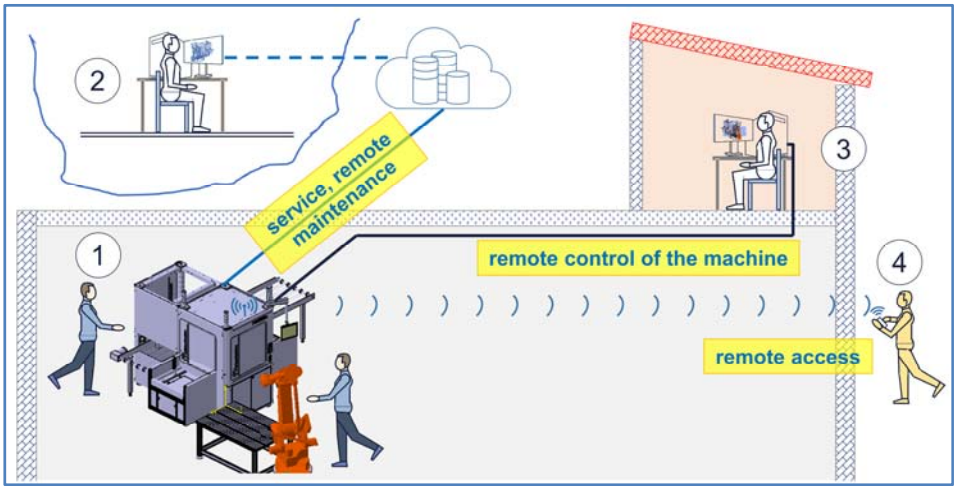


Figure 1. Remote access to the machine
1- machine, 2- remote maintenance specialist,
3- remote control of the machine, 4- remote access to the machine

Remote access, remote control and remote maintenance are operating modes that are integrated into the machine control system and are described in detail in the documentation of the respective machines. These operating modes are also taken into account in the risk assessment, whereby both occupational safety and cyber safety are taken into account (see Fig. 3). These operating modes can be integrated into the system control by the machine manufacturer or by a system integrator. Operating modes are secured, for example, with a key switch, a chip card and/or an access code. It is recommended to provide multiple authentications. In addition, the operating instructions must contain information

on ‘’which user groups are granted remote access to the machines at what time, for what period of time and with what rights. Remote access must be prevented at a time when the machine is performing critical functions’’ [1].
The documentation also specifies how remote maintenance is to be carried out. The machine manufacturer or system integrator trains the staff for remote services so that they are able to prepare the machine for remote access, organize the connection and track and document the communication. With the commissioning of the machine/production system, remote services are also tested and adopted by the operator.
The remote services can be carried out passively or actively by the remote maintainer. Passive remote maintenance is carried out in such a way that a remote connection is established to the trained specialist on site at the machine. The specialist at the machine has, for example, AR glasses (augmented reality glasses), a smartphone, a headset, a tablet, a PC with monitor or a display at the machine with which communication with the remote maintenance specialist can be established. The remote maintenance specialist gives instructions and the specialist on site carries them out.
Active remote maintenance means that the maintenance specialist can directly intervene in the control system and make changes.
The change of parameters on the safety elements or the change of the safety control system can be suggested by the remote specialist, but must be confirmed by the specialist on site at the machines.

3. Connectivity

In order for remote access specialists to access the machine control at an operator’s site, a secure and stable connection must be established, regardless of location, and usually across countries.A connection can technically be established in various ways, the most common being via the internet VPN (see Fig.2). As a rule, a VPN line will be established by the machine operator, IT/OT specialists, from the inside to the outside. The data traffic is encrypted, established security protocols are used and only required IP and ports are released. The remote access area is specifically restricted via the firewall rules.
In production systems that consist of several machines and have integrated higher-level controls, it is recommended to install a uniform remote access system for all controls. The components for this should be designed redundantly and with high availability and should only be used for remote access.
Remote maintenance components, equipment and software should be tested every six months. Unscheduled remote maintenance tests are particularly necessary when new employees are added to the remote maintenance team, e.g., when there is a change of personnel at the machine, in maintenance, in the

IT/OT department and when new hardware or software is used in the operator's company network and by service providers.

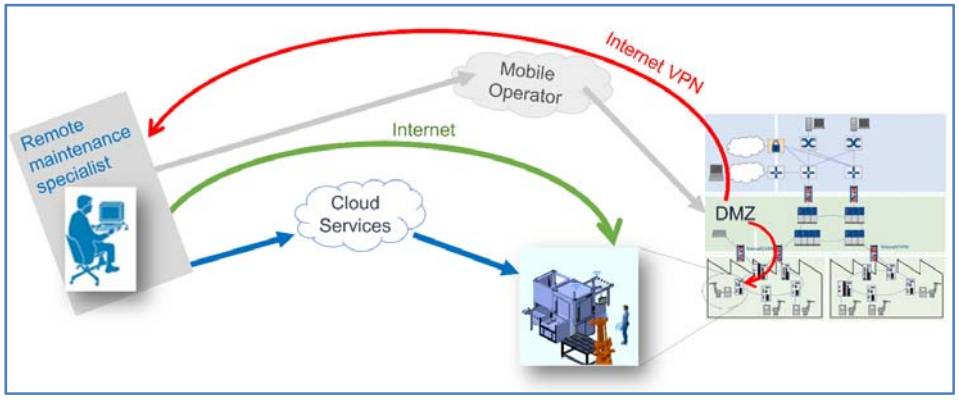


Figure 2. Connections from remote location and the machine

As part of the tests, the roles of all parties involved, communication among each other, possible process disruptions as well as exceptional situations such as interruption of the internet connection, timeout of remote access, connection with long delay time, failed installation of new user software and import of backup software to the machine are tested.
A connection can also be established via cloud services. Machines are deposited with access data on a platform and remote specialists are registered with their access data. The responsible employee of the operator is given admin rights and can create remote maintenance jobs. It is also possible to dial in via a telephone line and establish a direct ad-hoc connection via the internet using various software tools. For the connection to the machine control and for the remote maintenance operating mode, such connections are considered insecure and are therefore not recommended.

4. Risk Assessment

Cyber-attacks on companies are steadily increasing. Attacks on corporate networks via the internet pursue different goals, such as disrupting production processes, inflicting targeted damage or even stealing know-how. If a hacker succeeds in accessing the machine via the remote connection, he is virtually sitting in the middle of the machine operator's IT network, making it easy for him to attack the IT network from the inside and infect it with malware. One measure would be to implement network segmentation per machine to be maintained, so that only the respective machine can be accessed via the remote connection and further intrusion into the IT network is made more difficult.

Based on the risk assessment, cyber security measures must also be implemented (see Fig. 3). The operator is obliged to carry out a new risk assessment in case of hardware and software changes as well as updates and to implement risk-reducing measures if necessary.

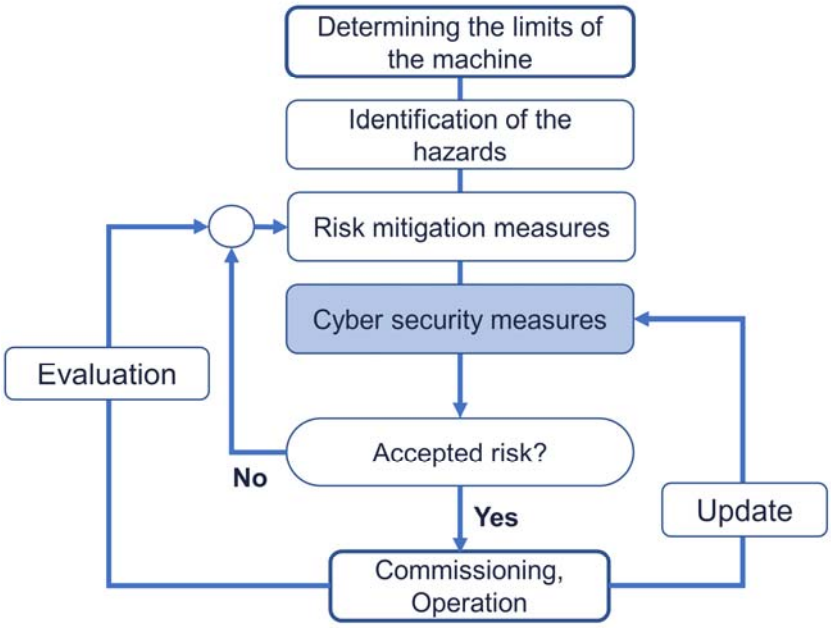


Figure 3. Risk assessment process with integrated cyber security

Remote access can cause some of the following dangers:

- incorrect configuration of the IT network leads the remote maintenance specialist to the wrong machine;
- incorrect configuration of the IT network allows the remote maintenance specialist to access the network outside the machine concerned;
- a premature maintenance leads to a partial or complete failure of machine functions;
- an update or modification of the machine control system leads to further unforeseeable malfunctions;
- malware is intentionally or unintentionally installed on the engineering PC and the machine control via the remote maintenance connection;
- misunderstandings in communication lead to unpredictable movements of the machine and damage to machine components or even injury to on-site maintenance personnel;

According to [1], [3] and [4], in order to establish a secure connection for accessing and performing remote maintenance, the following should generally be observed:

- Remote access should pass through a firewall and only allow access to the appropriate IP address and specific port. Any attempt to access other IP addresses must result in termination of the remote access.
- Remote access must be limited to the machine in question.
- Remote access must be activated by the operator's personnel.
- Secure authentication methods, such as current certificates, must be used for the software.
- The implementation of two-factor authentication is advisable, i.e., the proof of identity of a remote maintenance specialist should be done by a combination of two independent and different components (e.g., web access, personalized cards, fingerprint, smartphone, etc.).
- The devices and their data protection capabilities must be verified by routine validation tests on the network.
- A restriction of the connection to only one logged-in remote maintenance specialist at a time shall be implemented.
- Monitoring of accesses and continuous logging as well as their archiving by the operators of the industrial facility are essential.
- Only secure protocols such as IPSec, SSH or SSL/TLS should be used for communication, and always the latest version.
- Remote maintenance must be carried out in accordance with the operating instructions of the machine concerned.
- Encryption of data transmission should be implemented for remote maintenance; in addition, the following is recommended:
  - Remove malicious traffic before decryption (use of Threat Intelligence Gateway).
  - Use active SSL encryption
  - Use a stand-alone device
  - Protect plaintext data using intelligent data masking systems.

5. Use Cases

5.1 Special machine integrated in a production system

The machine is integrated into a production line and a fault analysis is to be carried out and serviced. The machine is brought into a safe state according to the instructions of the machine manufacturer and a backup of the machine control is created. Normally, machines in the production line exchange data with

each other within the production network. The data from production is usually processed, analyzed and stored in the edge server.

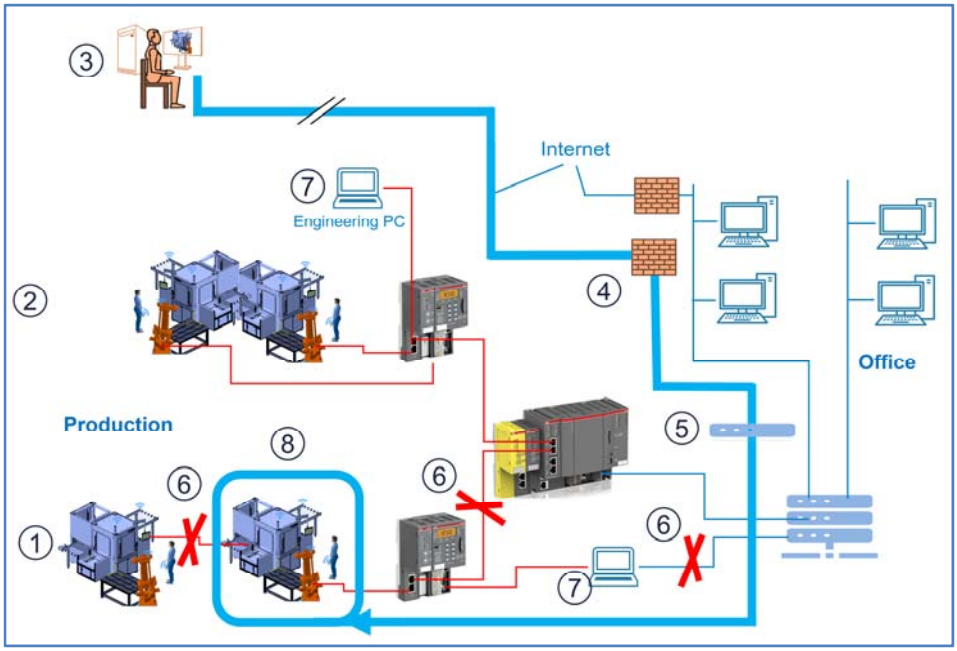


Figure 4. Remote maintenance on a machine in the production line 1,2- production lines, 3- remote maintenance specialist, 4- firewall, 5- hardware for remote maintenance, 6- disconnect connections before maintenance, 7- engineering PC, 8- machine to be serviced

Due to advanced digitalization, data from the production line is further forwarded to the administration and management in the office network. Before the remote maintenance specialist is connected to the machine, the machine to be maintained is disconnected from the other machines in the network and from the office network so that the remote maintenance specialist only has access to the specific machine. Access to the machine is granted for a certain time, after which the connection is automatically disconnected. Only the ports necessary for service remain open. The hardware components necessary for remote maintenance should not be used for other purposes. The connection to the remote maintenance specialist is always established by the operator IT department to the remote specialist. After authorization, the specialist's computer is scanned for malware and a connection to the engineering PC is established. The person responsible at the machine must first instruct the remote specialist, i.e., explain the problem area, show the machine status, introduce the persons on site and state their tasks. On the engineering PC, the communication

with the remote maintenance specialist is monitored, recorded and saved after completion of the maintenance and archived with the operator.

5.2 Implementation of remote services on the injection moulding machine

Injection moulding machines for plastic parts are series products supplied by machine manufacturers to customers worldwide. Support for the operators of such machines via remote services are successfully established.
Before remote access is set up, a backup must be made of the user program and archived so that the previous status can be restored if necessary. An operating manual for remote maintenance is prepared and all persons involved are instructed according to the role within the remote maintenance team. The machine is brought to a ‘’safe mode’’ and the upcoming remote access is discussed.
The remote access set up on an industrial machine is summarized in seven steps in an example in Fig. 5:

1. The operating instructions for the injection moulding machine describe the operating modes for remote maintenance. In particular, the preparation of the machine for remote access must be clearly explained.
2. The remote maintenance process is contractually agreed between the operator of the machine and the service provider/machine manufacturer. In particular, the duties and responsibilities of the respective contractual partners must be specified.
   Note: Remote maintenance is carried out in accordance with the legal regulations of the country in which the injection moulding machine is installed.
3. Before starting the remote maintenance, the operator puts the machine into the ‘’safe mode’’ and prepares the machine according to the operating instructions or the agreement.
   An example of the safe condition of an injection moulding machine could be defined as follows
   - Machine is cold
   - Screw conveyor is empty, without pellets
   - Mould in ‘’open’’ position
   - Safety doors are closed
   - Control is in manual mode

   All parts of the system that are not required for remote maintenance and are potentially dangerous are switched off, e.g., feed system, extraction system, cooling systems, etc. The control system is switched on in the operating mode for remote maintenance.

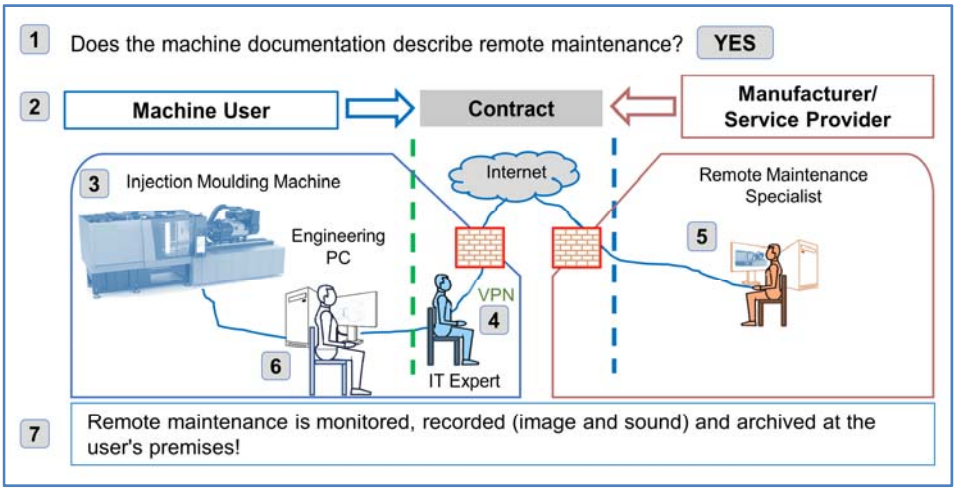


Figure 5.Implementing remote maintenance correctly in seven steps

4. The operating company's IT specialist prepares a VPN connection for remote maintenance and sends an access code to the remote maintenance specialist. The remote maintenance specialist's computer is scanned for viruses. After successful authentication, the VPN line is integrated into the IT network segment of the machine to be maintained, including the engineering PC, and communication is monitored.
5. After the connection to the control system has been established, the remote specialist is instructed by a safety specialist of the operator. Then the remote specialist first checks the safety status of the machine. After being prompted by the remote specialist, the operator performs the necessary steps.
6. During maintenance, an employee of the maintenance department observes and documents the work of the remote specialist via engineering PC.
7. After completion of the remote service, all records and documentation are archived at the operating company.

5. Conclusion

For remote maintenance, the machine manufacturer must provide the ''Remote Services'' mode in the machine control, therefore a risk assessment must be performed for all modes and described in the technical documentation. When the machine is commissioned, all operating modes are checked for their function and integrated into the company organization. Before starting remote maintenance, the machine must be set to ''safe mode'' and a backup of the software must be made. The connection from the machine to the remote maintenance specialist is established by the IT/OT department and the

communication is monitored. Work and cybersecurity measures must be followed. The agreed maintenance work is carried out by the remote maintenance specialist and the operating company documents the work. After the remote maintenance is completed, the documentation is archived.
Remote maintenance must be tested at regular intervals so that the hardware and software can be checked, the roles of the specialist personnel can be practiced and the process can be evaluated. Only when personnel are trained and practiced, all software is tuned, and networks are functioning, can remote maintenance be expected to be fast, efficient, and, most importantly, secure when needed.

6. References

[1] EN ISO 10218-2:2016, *Industrieroboter – Sicherheitsanforderungen – Teil 2: Robotersysteme und Integration*

[2] CEN ISO/TR 22100-4:2021, *Sicherheit von Maschinen - Zusammenhang mit ISO 12100 - Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits-(Cybersicherheits) Aspekte*

[3] VDMA 66481:2017: *Industrial Security – Grundlegende Anforderungen an die Security von Maschinen, Anlagen und deren Komponenten*

[4] BSI IT-Grundschutz, 2021. *OPS.1.2.5 Fernwartung, Bundesamt für Sicherheit in der Informationstechnik*, online: https://lmy.de/RRDQg, Zugriff am 15.12.2021

[5] ÖNORM EN ISO 20607: 2019 *Sicherheit von Maschinen – Betriebsanleitung – Allgemeine Gestaltungsgrundsätze*, 27. 1. 2020

[6] ISO/TR 22100-5:2021 *Safety of machinery — Relationship with ISO 12100 — Part 5: Implications of artificial intelligence machine learning*

[7] BSI, 2019. *Top 10 Bedrohungen, Bundesamt für Sicherheit in der Informationstechnik*, online: https://lmy.de/rBEj1, Zugriff 15.12. 2021

[8] BSI, 2020. *Sichere Fernwartung nach BSI – Alle Anforderungen in einer umfassenden Übersicht*, online: https://www.sichere-industrie.de/fernwartung-nach-bsi/, Zugriff am 15.12.2021

[9] BSI. *IT-Grundschutz-Kompendium, Bundesamt für Sicherheit in der Informationstechnik*, Bonn, Reguvis Fachmedien GmbH, online https://lmy.de/RRDQg. Zugriff am 15.12.2021

[10] Bokämper, W. *Leitfaden Industrie 4.0 Security, Handlungsempfehlungen für den Mittelstand*, VDMA und Partner, 2016. online: https://lmy.de/sZf12, Zugriff 15.12. 2020
[11] ISO/IEC 27005:2018 *Information technology — Security techniques — Information security risk management*
[12] IEC TR 63069: 2019. *Industrielle Prozess-Leittechnik, Steuerungs- und Automatisierungstechnik*. Technical Report, S. 20–21.
[13] Malisa, V. *Arbeit in der Industrie 4.0 sicher und gesund gestalten*, https://lmy.de/l9yQS, Stand 31.07.2020, S.5). 2018
[14] Becker, K.-D. *Arbeitsschutz und Digitalisierung (Fernzugriff)*. BG ETEM Fachtagung Digitale Arbeitswelt 7/8 September 2021
[15] EN ISO 12100:2013. *Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung*