Fraunhofer AUSTRIA

TÜV AUSTRIA

WhitePaper

Safety & Security Human-Robot-Collaboration

Influence of IT security

TU WIEN Pilotfabrik Industrie 4.0

TU WIEN

ABB

Photos
© Fotolia, Shutterstock, ABB AG

Imprint:

Human-Robot-Collaboration

Influence of IT security

Third Edition

21 March 2018, Vienna

Human-Robot-Collaboration

Influence of IT security

Third Edition

21 March 2018, Vienna

TÜV AUSTRIA
HOLDING AG
TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge

Ing. Sabrina Steger, MSc
DI Alexandra Markis
DI Harald Montenegro, MSc
Ing. Michael Neuhold
Ing. Andreas Oberweger
DI Christoph Schwald

FRAUNHOFER AUSTRIA
RESEARCH GMBH
Theresianumgasse 27
A-1040 Vienna

Prof. Dr.-Ing. Wilfried Sihn
Fabian Ranz, MSc
DI Thomas Edtmayr
Dipl.-Wirtsch.-Ing. Philipp Hold
DI Gerhard Reisinger


01011001100

Human-Robot-Collaboration

Table of Contents

Abstract 9

1. The Status Quo of IT Security 10

2. From Information Technology to Operational Technology 11

3. Points of Attack and Risks of Industrial Machines and Plants 12

4. Norms and Standards for Industrial IT Security 14

5. Practical Examples of Collaborative Robotics Used Interconnectedly 16
   - 5.1 Industry 4.0 and human-robot collaboration at ABB s.r.o. Elektro-Praga 16
   - 5.2 Human-robot collaboration at TU Wien Pilot Factory Industry 4.0 18

6. An Examination of Collaborating Robots from the Point of View of IT Security 20
   - 6.1 A general security testing procedure 20
   - 6.2 Results of an investigation related to the production network 21
   - 6.3 Results of the investigation of safety/security related to collaborating robots 21
   - 6.4 The correlation between threats to IT security and functional safety 23
   - 6.5 Countermeasures (related to the use case at TU Wien Pilot Factory Industry 4.0) 24

7. An Integrated Safety & Security Concept 25
   - 7.1 Determination of machine limits and interconnection 26
   - 7.2 Identifying risks 26
   - 7.3 Risk assessment and evaluation 26
   - 7.4 Defining risk mitigation measures 27

8. Conclusion and Outlook 28

Sources 30


01011001100

Abstract

Today, it is not uncommon for systems to be controlled and serviced remotely while tablets and smart glasses are supplying important information to staff in real time, and processes are becoming more transparent and controllable owing to mass data collection along with associated data analyses. In line with the concept and paradigm of Industry 4.0, more and more factory devices, tools, equipment and machines are able to receive information via well-known and widely used IP-based protocols, process it and return it to any places desired – the Internet of Things and smart factories are coming into being.

For these smart factories to operate efficiently, it is essential that machinery and systems be accessible at all times and supplied with the right information at the right time that they need for smooth operation. Not only efficiency, but also the safety and security of factories can be endangered by incorrect, faulty or missing information, with machines behaving in an unexpected manner and going into conditions that cause damage or even destruction - usually caused by malicious software or attackers from outside. As a result, there are particularly high risks for humans when they work closely with these machines – as in human-robot collaboration.

A key finding from the practical work carried out by TÜV AUSTRIA is that the functional safety of machines and systems can be compromised by threats to information security – and in this respect, the same importance as that of functional safety and security must be attached to risk assessment and certification of interconnected systems.

This third joint white paper on the topic "Safety and Security in Human-Robot Collaboration" by TÜV AUSTRIA and FRAUNHOFER AUSTRIA RESEARCH considers the growing role of information security in modern factories and highlights its importance using the example of human-robot collaboration.
To this end, the authors provide an overview of the status quo of industrial IT security in 2018 and illustrate the implications for human-robot collaboration applications on the basis of two practice-oriented use cases.

At the heart of these methods is the integrated assessment of functional and informational threats in risk assessments developed by TÜV AUSTRIA and FRAUNHOFER AUSTRIA RESEARCH.
The intention is especially to raise awareness about the dependency of both worlds in a highly interconnected and digitalized scenario, namley Industry 4.0.

1. Status-quo of IT-Security

Figures, Data & Facts

Almost every day, targeted cyberattacks are carried out on companies. Cybercrime is one of the most significant threats to the global economy today. At the same time, the dependence on information systems is constantly increasing, because more and more business processes only function now with IT support.
The threat of cyberattacks is also increasing in the context of production: In 2014 social engineering enabled attackers to gain access to a corporate network within a steel mill in Germany, gained access of the systems' control level and put a melting furnace in a state that resulted in it being damaged, while at the same time preventing the furnace from being shut down by the local personnel.
In a remote access attack on an American sewage treatment plant in 2011, a pump was destroyed by repeatedly switching it on and off.
In Austria, too, CERT, the Austrian national Computer Emergency Response Team, has been registering IT security incidents since 2013 with real security risks at a rate of well over 10,000 every year.
In view of this immense number of cases, the EU Commission recently passed the Cyber Security Act, which obliges providers and operators of networks and services to report attacks on their systems to the authorities.

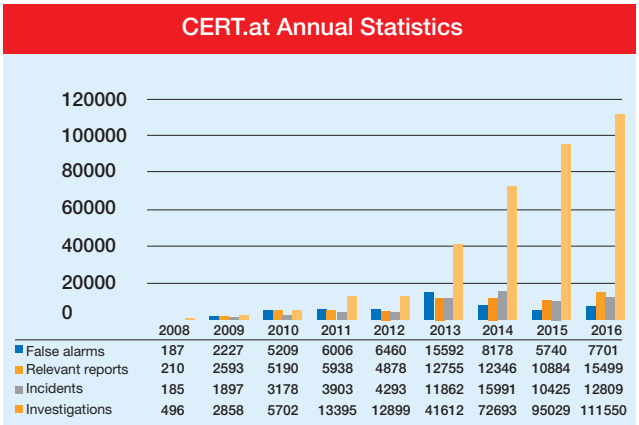

Figure 1: IT security incidents in Austria [2]

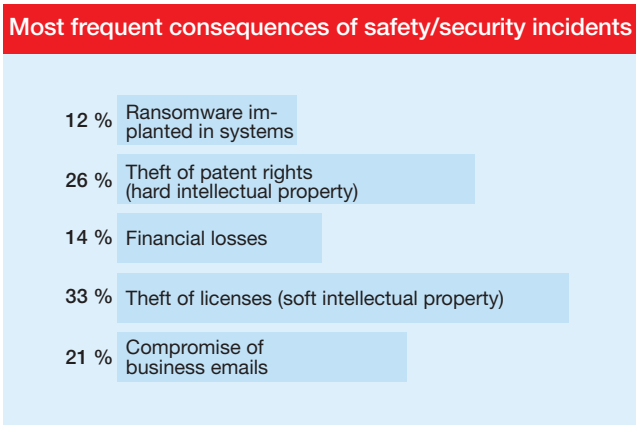

Figure 2: Consequences of Cyber attacks [1]

The buzzword "Industry 4.0" refers to the arrival of the Internet of Things in factories. Machines, plants and all kinds of equipment are now being designed as cyber-physical systems (CPS). A CPS is a combination of mechanical and electronic parts as well as informational and software-based components. The combination of technical and information technology components creates machines that are critical both in terms of functional safety and informational-technological security.
Although around 40% of the companies already work with external partners to improve the security of their IT systems.

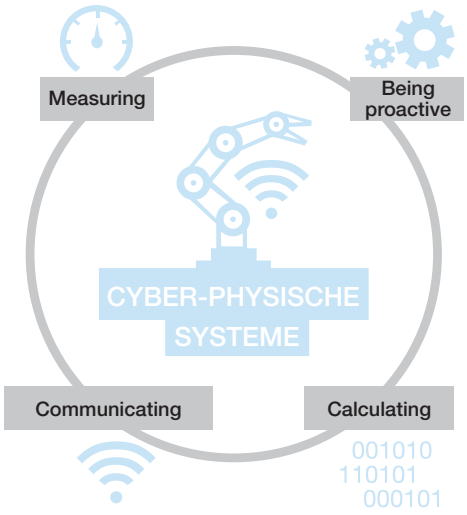

Figure 3: A cyber-physical system [4]

2. From Information Technology to Operational Technology

In conventional business organization, information technology (IT) is conceptually seperated from operational technology (OT), i.e. production and operating technology - according to this, an IT department is responsible for all technology required for data processing and its security.
However, it does not usually deal with industrial systems such as robots, machine tools or materials handling technology - and historically speaking that has been unproblematic, because industrial systems were not usually interconnected with each other, and certainly not connected to the Internet. By 2025 however, there are to be between 25 and 50 billion individual devices interconnected [3] - to a considerable extent within factories.

However, if such industrial, cyber-physical systems use the same means and paths of communication as, for example, conventional desktop computers in administration, and if they obtain information, for example, from the same company systems or return data to such places, then interfaces and coordination requirements arise between IT and OT.

	Office-IT=IT	Operational IT=OT
Service life	3-5 years	5-20 years
Patch management	Frequently to daily	Rarely, requires approval or assistance from the machine manufacturer
Time dependency	Delays accepted	Critical
Availability	Short outages tolerated	Subject to constant availability

Figure 4: Differences between IT and OT [5]

This means that OT systems must be viewed and protected in terms of security in the same way as conventional IT systems and equivalently integrated into company-wide considerations and measures for IT security - or even more intensively so. That is because expectations for fail-safety, reliability, functional efficiency and functional safety for industrial plants are higher than in office environments and can be of immense importance due to their supplying functions, for example for the population at large.

For this reason, an integral view of functional safety and IT security is indispensable for future infrastructures in Industry 4.0 environment - in order to be able to leverage the full potential of these technologies.

3. Points of Attack and Risks of Industrial Machines and Plants

There are many ways for attackers to penetrate the IT infrastructures of industrial plants. This is also reflected when looking at the most important threats that industrial and manufacturing plants see themselves exposed to (cf. Fig. 5). These are essentially primary attacks: These methods are often used by attackers to penetrate industrial plants, enabling sabotage and subsequent manipulation.

Nr.	Top 10 (2016)	Top 10 (2014)
1	Social Engineering and Pishing	Infection with malware via Internet and Intranet
2	Introduction of malware via hardware (e.g. USB sticks)	Introduction of malware via hardware (e.g. USB sticks)
3	Infection with malware via Internet and Intranet	Social Engineering
4	Incursion via remote maintenance access	Human error/sabotage
5	Human error/sabotage	Incursion via remote maintenance access
6	Internet-connected control components	Internet-connected control components
7	Technical malfunction, force majeure	Technical malfunction, force majeure
8	Compromise of extranet or cloud components	Compromise of extranet or cloud components
9	(D) DoS attacks	Kompromittierung von Extranet und Cloud-Komponeten
10	Compromise of smartphones in production operations	(D) DoS attacks

Figure 5: The most frequent causes of primary attacks [6]

These access risks have a potential impact on the essential protection objectives of information security, which apply to industrial machines and plants just as they do to conventional IT systems. According to this, information must not be taken from systems in an unauthorized manner (confidentiality), data within systems must not be manipulated in an unauthorized and unnoticed manner (integrity), and the (usual, intended) availability and usability of a system must not be restricted (availability). In technical terms, these protection objectives are summarized in the so-called CIA triad.
If these protection objectives are violated, this can result in immense consequential damage - from financial losses due to plant downtime or damage, to competitive disadvantages due to loss of information, up to injuries to employees due to out-of-control machines. Integrity therefore plays a particularly important role in machines and systems that can pose a risk to people in terms of functional safety in the event of manipulation.

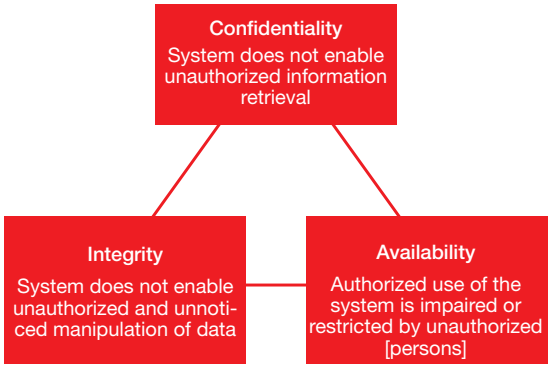

Figure 6: Protection objectives according to the CIA triad

4. Norms and Standards for Industrial IT Security

Similar to functional safety, operators of industrial plants are also guided and supported with regard to IT security by special standards and guidelines for ensuring the protection objectives of confidentiality, availability and integrity. In practice, however, there are hundreds of national and international IT security standards, more than a dozen of which still apply to industrial automation and control systems.

Similar to ISO 27001, which places requirements on general IT systems, the IEC 62443 family of standards deals specifically with industrial automation and control systems, providing a specific recommendation for action for the three main target groups concerned with building and operation: plant operators, plant constructors and component manufacturers.

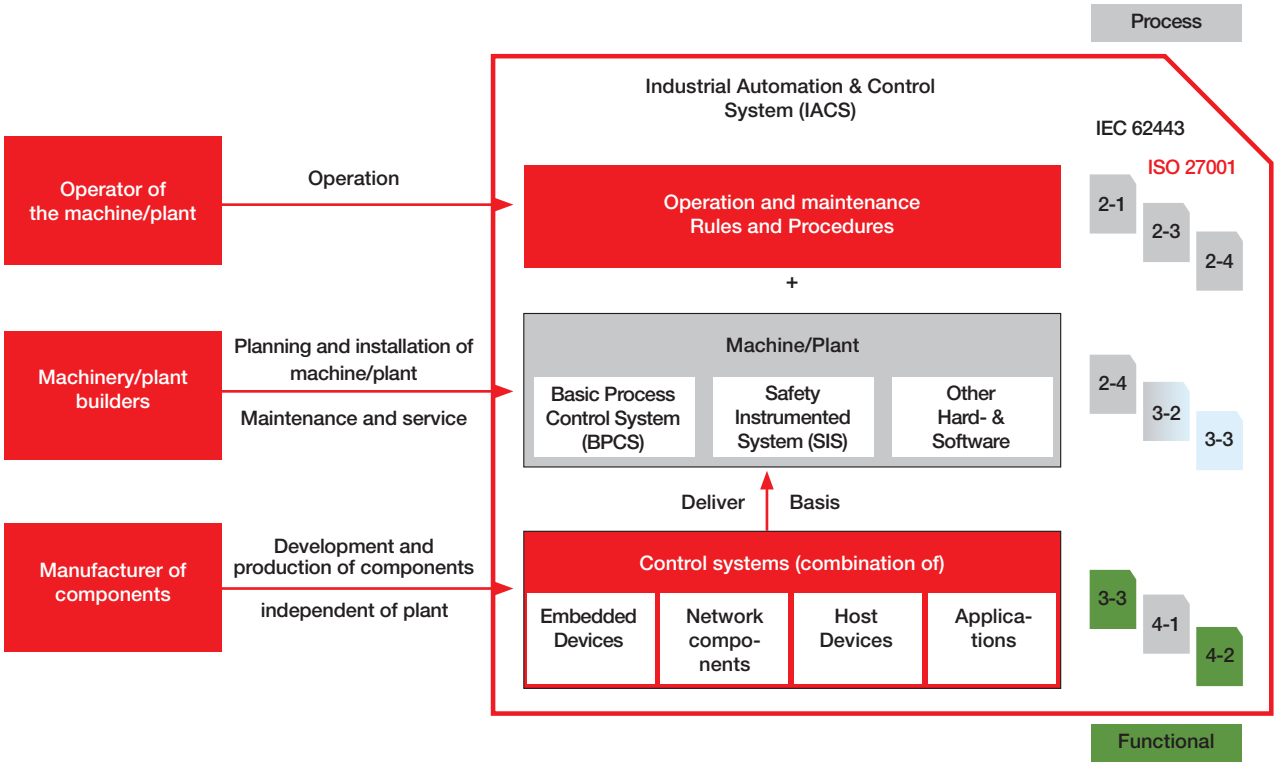

Figure 7: Target groups and structure of the IEC 62443 family of standards [7]

The Open Web Application Security Project, OWASP, can also provide orientation in designing machines, plants and other devices for the Industrial Internet of Things. OWASP is a project freely accessible to anyone that is committed to raising IT security standards also for the Internet of Thing-enabled terminal devices and has formed ten vulnerabilities to be avoided and respective countermeasures.

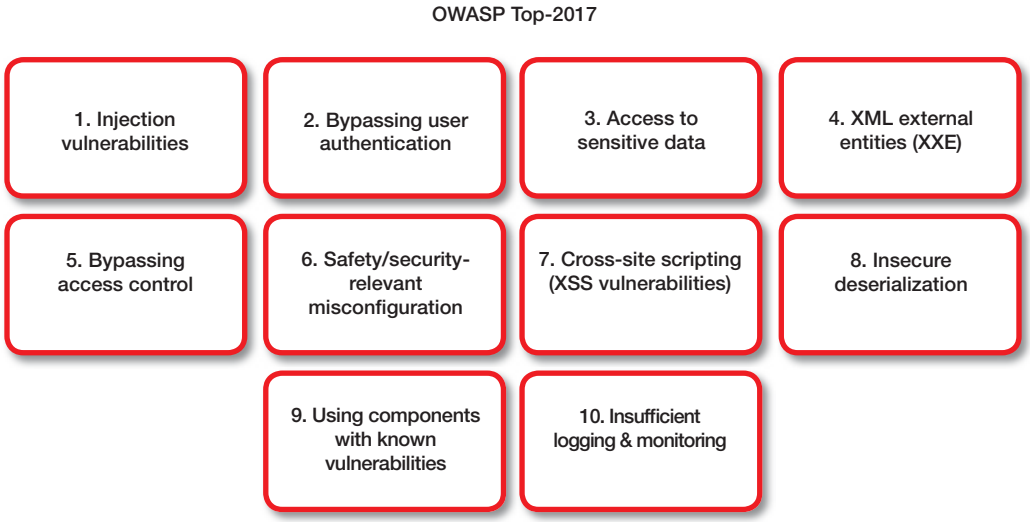

Figure 8: Typical vulnerabilities of IoT devices [8]

A third framework with reference to IT security, which can also be used for industrial machines and plants in particular, is the Framework for Improving Critical Infrastructure Cybersecurity of the National Institute for Standards and Technology (NIST). It does not provide specific requirements for the design and configuration of machines and plants that can also be operated safely and securely when interconnected, but rather sets out a methodical procedure for plant operators for identifying, assessing and combating risks and provides recommendations for its organizational anchoring.
Bearing in mind these available reference works and the recommendations they contain, it would be obvious to expect that manufacturers of modern industrial plants have already taken them into account and that modern machines have no or only very few points of attack for manipulation and sabotage via information paths, meaning that they can be operated without hesitation even in in highly interconnected Industry 4.0 scenarios.
In "conventional" factories, installations are usually programmed locally and only in some cases do they have interfaces, for example to load programs or save data. If individual machines are interconnected with each other on the basis of wired automation technology, such as with the aid of programmable logic controllers, these networks are frequently isolated, having no contact with the outside world. However, the increase in flexibility pursued in Industry 4.0 is mainly due to vertical and horizontal interconnection of subsystems, for example to supply machines more quickly with constantly changing job information or to enable remote maintenance, as the following examples also show:

5. Practical Examples of Collaborative Robotics Used Interconnectedly

Industrial robots celebrated a record year in 2017 with global sales of just under 350,000 units, which is an increase of 18% over 2016.
The global market volume was estimated at 50 billion dollars for 2017. Two million robots are in use worldwide, and the International Federation of Robotics (IFR) predicts that this figure will rise to three million by 2020.
The IFR expects further growth in the global robot population, most of all through an increasing range of collaborating lightweight robots and improved possibilities for interconnection within the framework of the Internet of Things and Industry 4.0. The following two practical examples are intended to provide an insight into this development.

5.1 Industry 4.0 and human-robot collaboration at ABB s.r.o. Elektro-Praga

Figure 9: MRK-Applikation with ABB YuMi

An industrial example of humans working with interconnected robots can be found at Elektro-Praga, an ABB subsidiary in the Czech Republic. At collaborative workplaces, humans and robots assemble standard commercial electrical outlets together. The tasks of the assembly process are divided according to the individual abilities of humans and machines.

Core Information	*Robot:* IRB 14000-0.5/0.5 - YuMi®	*Maturity level:* Industrial use
	Type of joint work: Collaboration	*Process area:* Assembly

Application

The workstation consists of a human operator, an ABB YuMi lightweight robot, various sensors, conveyor belts, vibration conveyors and a spring untangling system. During the process, YuMi mounts the springs, the child safety devices and their covers on the electrical outlets. The assembly process is triggered by the operator, who first places two caps and two covers for the child safety devices in front of the robot. YuMi then uses its vacuum cups to grasp the child safety devices from the vibration conveyor and insert them into the prepared caps of the electrical outlets. Then YuMi takes the appropriate springs from the supply unit (two parts per base) and places them in the space of the electrical outlets. The robot inserts the cover for the child safety device into the now prepared assembly group. YuMi ends the assembly process by clipping the cover into the cap. Finally, the operator inserts a screw into the electrical outlet and places it in the appropriate packaging. In addition to parts handling, the operator is also responsible for monitoring the entire process and can intervene if necessary.

Objectives	▸ Relieving the employee by transferring the non-ergonomic work to the robot ▸ 20% higher output through division of labor between human and machine

Product data	*Product:*	*Dimensions:*	*Weight:*
	Electrical outlets	approx. 80x80x14 mm	approx. 10 g

Safety/security concept

Surroundings:	▸ Safety glasses for employees, avoidance of sharp edges and corners, marking by signs
Tool:	▸ One gripper uses only vacuum cups; a second gripper has been adapted for collaborative work; sharp edges or corners on the gripper.
Program:	▸ Robot movements in the working area reduced to the bare essentials (no “excessive movements” of the arms), avoidance of movements that could lead to shearing
Certification:	▸ Self-certification

ABB provides digital services for YuMi for condition monitoring, maintenance and system optimization. The connection is wireless or via LAN. The MyRobot website with an alarm dashboard is the interface to Connected Services. The alarm dashboard provides information to both customers and the ABB service team. The application shows malfunctions and error messages that can lead to failures, analyzes trends and warnings, gives notifications and provides support in case of problems. The ABB Ability™ Connected Services consist of five components: Condition Monitoring & Diagnostics, Backup Management, Remote Access, Fleet Assessment and Asset Optimization.

The illustrated application thus strongly corresponds to the idea of Industry 4.0 - close cooperation between human and machine, a high degree of interconnection and value-adding use of the resulting data.

However, this also raises questions about the IT security of such interconnected robot applications. In chapter 7 the IT-related security of standard, articulated, collaborative robots is investigated in the research environment of the TU Wien Pilot Factory Industry 4.0.

5.2 Human-robot collaboration at TU Wien Pilot Factory Industry 4.0

In the initial situation, TU Wien Pilot Factory Industry 4.0 depicts a typical industrial assembly system, whose infrastructure is characterized by a high degree of interconnection. Pilot Factory Industry 4.0 produces customized 3D printers. During the assembly of the extruder carriage for these 3D printers, a lightweight robot is used in direct human-robot collaboration, which supports the employee during static holding work.

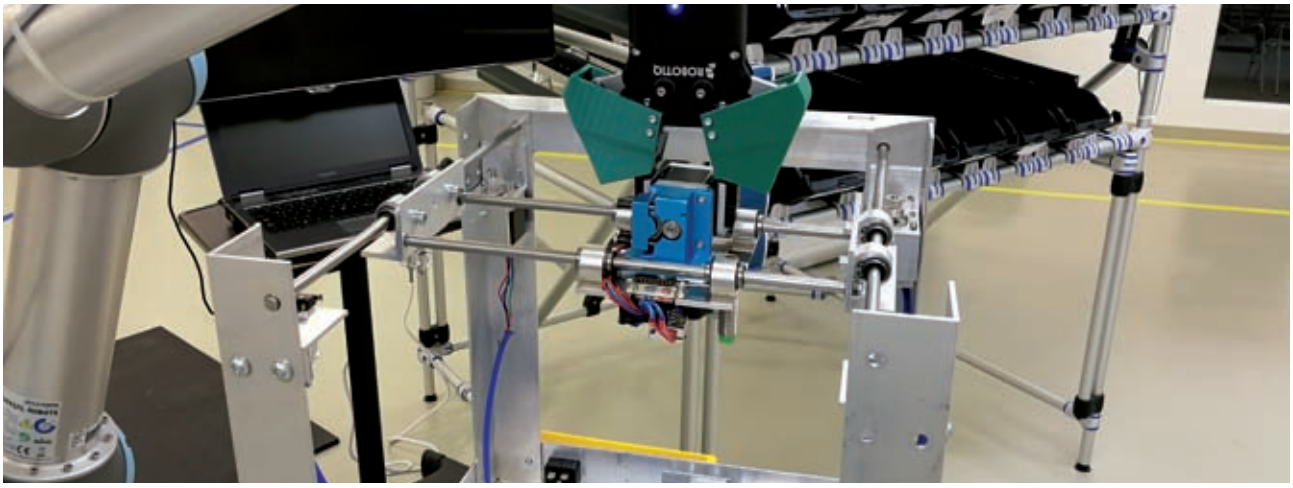

Figure 10: MRK-Applikation with Universal Robot UR5

Core Information

Robot: Universal Robot UR5

Maturity level: Demonstration mode

Type of joint work: Collaboration

Process area: Assembly

Application

The workpiece of the 3D printer is transported along the assembly line on automated guided vehicle systems. Being the central component, the extruder carriage has to be equipped with the kinematics module, which must be fixed to the printer housing. To do this, the robot first lifts the extruder carriage into a comfortable position for the operator to manually assemble the kinematics module. Afterwards, the robot lifts the extruder above the workpiece of the 3D printer so that the kinematics module can be bolted to the frame by the operator. Without the use of the lightweight robot, a second employee would berequired for this step, who would hold the extruder carriage in position. Since the automated guided vehicle system (AGV) does not stop at the assembly station with repeatable accuracy, its exact position is determined by a 2D camera, which informs the robot of the exact coordinates for positioning the extruder carriage above the workpiece.

Objectives

- Precise and stable positioning of the extruder carriage in the assembling position
- Relief for the employee from static holding work

Product data

Product:	*Dimensions:*	*Weight:*
3D-printer	approx. 40x40x40 cm	approx. 3 kg

Safety/security concept

Robot:

- Reduction of strength and power
- Adjustment of speed

Surroundings:

- Marking by signs and column traffic lights

Tool:
- Caps for gripper kinematics module and surface enlargement at gripper tips
- Securing the tool interface at the flange by a protective ring

Program:
- Avoidance of shearing points through vertical path design
- Monitoring of the gripping force to detect incorrect objects (not safety-related)

Certification:
- Not certified because this is a setup for research and testing

An ERP system, which is provided in the cloud, steers production orders into the factory. These are processed by the assembly controller and distributed to the individual assembly stations. Employees receive assembly instructions via tablet computers. Equipment such as an electronic kanban system or intelligent screwdriving systems are also connected via Ethernet and communicate bi-directionally with the assembly controller. This robot also communicates with the higher-level control systems, receiving, among other things, start signals for accepting the extruder carriage, the coordinates for its positioning above the workpiece and reporting back its successful execution of the task.
The network within the factory is connected to the Internet via a central router, and the WLAN for employees and visitors is provided via access points.

A simple network diagram, as IEC 62443 recommends creating, provides an overview of the individual components and the overall structure.

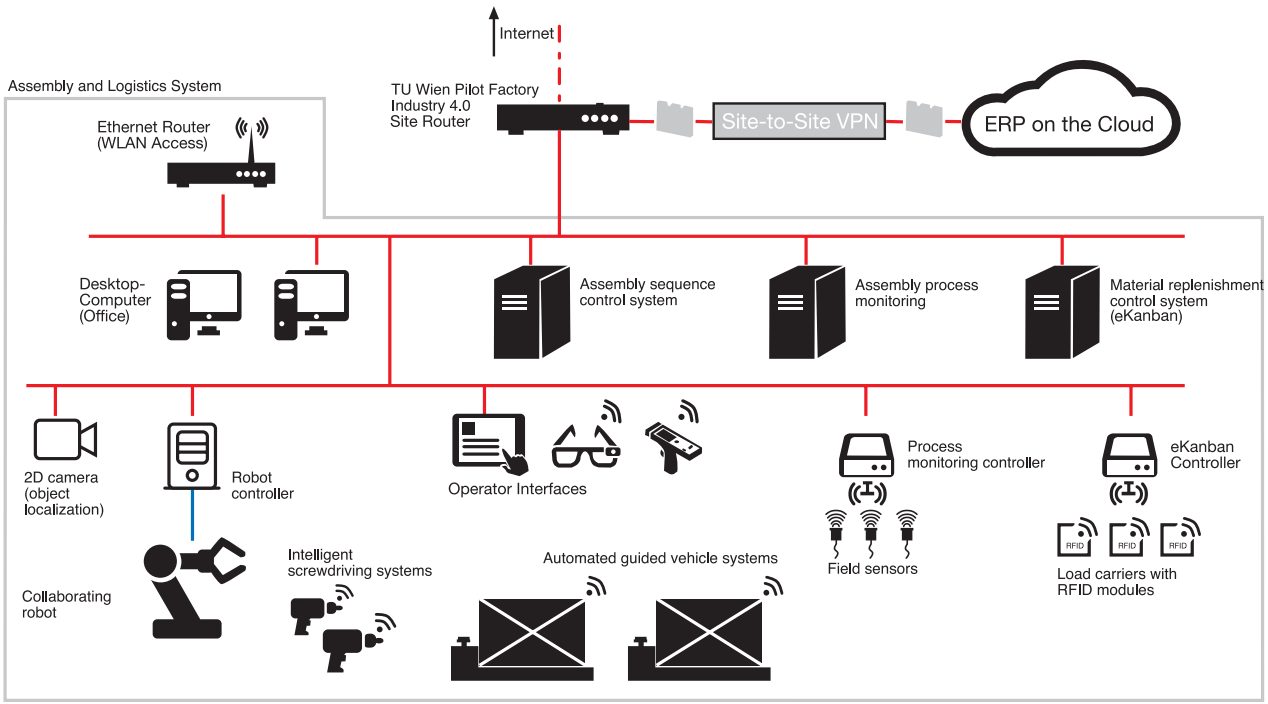

Figure 11: Initial situation of network architecture at TU Vienna's Pilot Factory Industry 4.0 (before optimization)

On the basis of this example scenario, the necessity of an integral view of systems for taking IT security into account in interconnected production, on the one hand, and the importance of integrative consideration of functional safety and IT security on the basis of individual machines and plants on the other hand, is identified in the following, using the example of a lightweight robot in human-robot collaboration.

6. An Examination of Collaborating Robots from the Point of View of IT Security

6.1 A general security testing procedure

The general procedure for a security test (penetration test) is described below.

During preparation, the objectives, the technical and time scopes as well as the type of investigation of safety/security are worked out and defined. In industrial environments, it makes sense to provide detailed information about devices and systems in order to tailor the testing to the specific requirements.

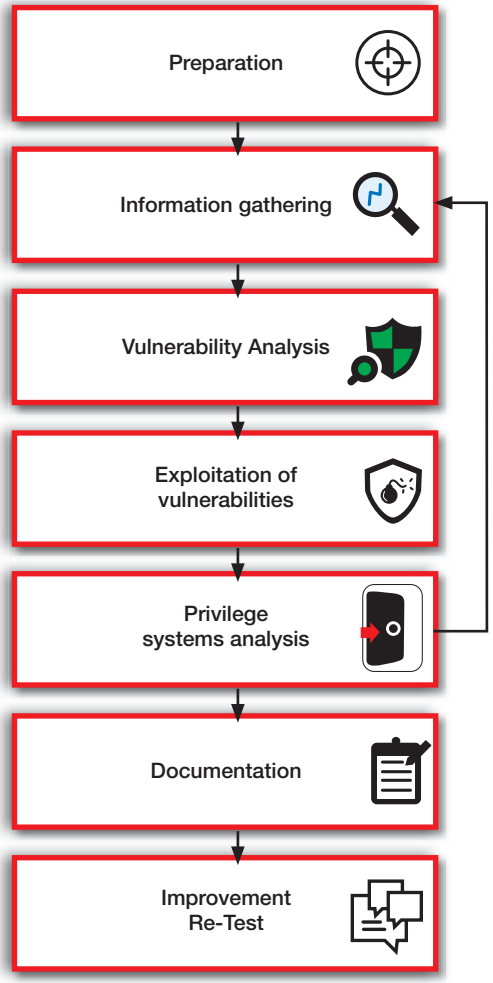

Figure 12: Test procedure IT-Security

In the information retrieval phase, the point of attack is identified, which is used as a basis for designing attack scenarios.

In the third phase of a penetration test, vulnerabilities are identified and validated. Queries are made which do not occur in normal use in order to identify security deficits of all kinds.

In the subsequent phases, the previously identified vulnerabilities are exploited. This can be the utilization of an an already known vulnerability or creating attack scripts oneself. In technical jargon, the term exploitation is used.

Once access to the system has been achieved, the next step is to extend its rights to administration rights (root) and continue the system analysis by testing access to other devices.

During these phases, one continues to attempt to jeopardize confidentiality and integrity. If availability in any form is at risk, this is indicated in a report, but not actively exploited.

Finally, the vulnerabilities found are comprehensibly documented in the form of findings and subjected to a risk assessment. It is essential to explain how the vulnerability has been exploited and to make recommendations and possible compensatory or hardening measures.

Once the report has been prepared, it is discussed in detail with all parties involved, and measures for implementation are defined. After implementation, it is necessary to carry out a re-test to check the effectiveness.

6.2 Results of an investigation related to the production network

The described procedure for carrying out penetration tests from Chapter 6.1 was applied by TÜV AUSTRIA's IT security experts to the outlined production network at TU Wien Pilot Factory Industry 4.0 in general and to various collaborative lightweight robots in particular. In the initial state, no security measures were explicitly considered or implemented when designing and setting up the production network.

The wireless LAN provided by the access points served as an entry point into the network to crack the password via a brute force attack.
Since the IT infrastructure was not divided into individual zones or areas, but rather the entire production system was operated in just one large network, using a network scanner made it possible to localize all the devices and machines in this network, including conventional IT components such as computers, network printers and servers as well as the components for the OT infrastructure, which include collaborating robots, screwdriving systems and transport systems, among others.
Access to and configuration and programming of individual devices and machines was in part possible via web interfaces. In some cases, the devices and machines used at TU Wien Pilot Factory 4.0 did not have any password protection, factory-set or very weak passwords, allowing them to be quickly controlled and manipulated.
If the data traffic was not encrypted, which was not the case with the devices and machines used and tested, it could also be read in plain text.
This applied not only to access data and passwords, but also to regular communication between the devices. In such a case, an attacker could have traced the logic of the information exchange and sent incorrect or manipulated information (e.g. job orders or configuration parameters), which could lead to malfunctions or outages of machines and plants.

6.3 Results of the investigation of safety/security related to collaborating robots

The possibilities for an attacker to disrupt operation, in particular with regard to the protection objectives of availability, confidentiality and integrity at the level of individual machines and systems, are illustrated using the example of collaborating robots. A selection of the results (findings) is presented in the following segment.

It was assumed that an attacker was in the same network (cf. Fig. 11) as the robot. In regular operation, the robot receives commands and requests exclusively from the assembly controller (load programs, start programs, send feedback messages).

Knowing the IP address, an attacker could then also send commands to the robot or query status information from it. Furthermore, the TÜV AUSTRIA experts were able to stop the program run or even completely switch off the robot. Switching off the robot endangers the protection objective of availability and the production system comes to a standstill. Especially in industrial plants, the availability of machines is critical, making for a high cost factor in the event of a standstill.
Beyond that, in some cases it was possible to acknowledge messages and malfunctions remotely. This also includes safety stops after a collision with a human or object. This can endanger functional safety because the robot continues to run without the operator on site being prepared for it, making it possible for a new collision to occur. This means that the personal security of people is directly endangered due to inadequately executed IT security.
In addition, when access is attempted, individual robots do not require any authentication, for example by user name and password, nor do they perform any authorization. Instead, the robots executes unconditionally execute every command sent to them from any source, which also applies to the critical commands mentioned above, such as for switching off a robot completely or releasing/acknowledging a safety stop.
In the course of further tests, the auditors were able to obtain administration rights to open, view and change robot programs and then save the changes. This means that the protection objectives of integrity and confidentiality are no longer given. On the one hand, this results in unforeseen changes in the motion or program sequences of robots for the operator and on the other hand, the security of company information can also be endangered by copied and stolen programs that contain specific know-how about products and processes. It was also possible to overwrite passwords set for safety and security so that it was no longer possible for the robot operators to change the settings themselves. Subsequently the availability of the plant is endangered.

Finally, it was also possible for new installation files (which also contain the safety and configuration, including permissible forces, speeds and safety limits) to be loaded. This once again violates the protection objective of integrity, allowing an attacker to modify robot data for its own purposes and compromise functional safety if, for instance, the robot enters a work area at a speed higher than that intended.

Another problematic fact is that, non-reputability, a further protection objective, is not given. It was identified that instances

of access and commands from outside in the robot's log files, which are usually also kept by every other machine, were not at all documented or scarcely so. As a consequence, the origin of unexpected (or even malicious) behavior is completely unclear and no conclusions can be drawn about the perpetrator (attacker).

The results show that, with their factory settings, not all collaborating robots, which are also suitable for cooperation with humans due to their low weight and built-in sensors, meet the essential requirements for the IT security of interconnected devices from IEC 62443 or other frameworks.
At the same time, depending on the individual case, it is difficult or even impossible for the machine operator to eliminate these machine-related vulnerabilities. For this reason, staggered defense is of great importance: taking protective measures "before" any machines at the levels of the network hardware and software that prevent an attacker from accessing the machine.
Subsequently, the correlation between the identified deficits is discussed with regard to the IT security and the functional safety.

6.4 The correlation between threats to IT security and functional safety

The functional safety of machines requires that residual physical risks for employees, in particular injury risks arising from a machine or plant, such as an HRC application, do not exceed a certain level.
With regard to the described application case of human-robot collaboration, technical measures can be taken, such as reducing the robot's traversing speeds, so as to exert only small collision forces in the event of contact between humans and robots.
A second example would be to design travel paths in such a way that the distances between the manipulator and the physical structures of the workstation are large enough at all times that no pinch points can arise.
Locally, the programming of these technical measures to increase the functional safety level can be protected against deliberate or undeliberate changes and manipulation, e.g., by defining different user authorizations for machine operators and programmers or passwords in the control panel of the robot.

However, as the trials and safety/security tests have shown, attackers can sometimes compromise the very technical safety/security measures via the network connection of the robot, depending on the specific robot model. Changing the safety/security configuration and sequential programs or even acknowledging safety stops and rebooting and starting up programs can be done remotely using simple commands sent to the robot via Ethernet, in some cases very easily.
The user or operator on site, who interacts with the robot, does not notice any of this. The fact that a machine which has also been assessed for risk no longer complies with its original specifications could behave unexpectedly and pose greater risks than assumed remains hidden to the operator.

This shows that an isolated review of functional safety for the operation of interconnected machines and systems is not expedient because these machines potentially - and this must be checked in individual cases - show deficits in the area of IT security, through which technical security measures can be compromised. Safety and security concepts are therefore indispensable.

Figure 13: The correlation between safety and security

6.5 Countermeasures (related to the use case at TU Wien Pilot Factory Industry 4.0)

In order to be able to operate these machines in a network anyhow, the production network offers starting points for safeguarding: In the first and decisive step, the predominant endangerments must be identified and evaluated, as visualized in the previous sections and described in detail in chapter 7 below. Appropriate risk reduction measures are then derived on this basis. IEC 62443 provides assistance in doing so. Compliance with these stipulations can massively increase the overall security of a production system against attacks, sabotage and manipulation, enabling interconnected operation of machines and systems, which in themselves may have significant security holes, in a highly protected network.

To implement these derived measures, Phoenix Contact, a specialized component manufacturer and service provider in the field of electrical engineering, electronics and automation, "zoned" the network at TU Wien Pilot Factory Industry 4.0. Individual zones are separated by barriers that control communication between two zones based on their respective configuration. Such barriers can be routers, switches or physical firewalls. Within a zone, devices and systems are grouped together according to common risk levels or the same need for protection.

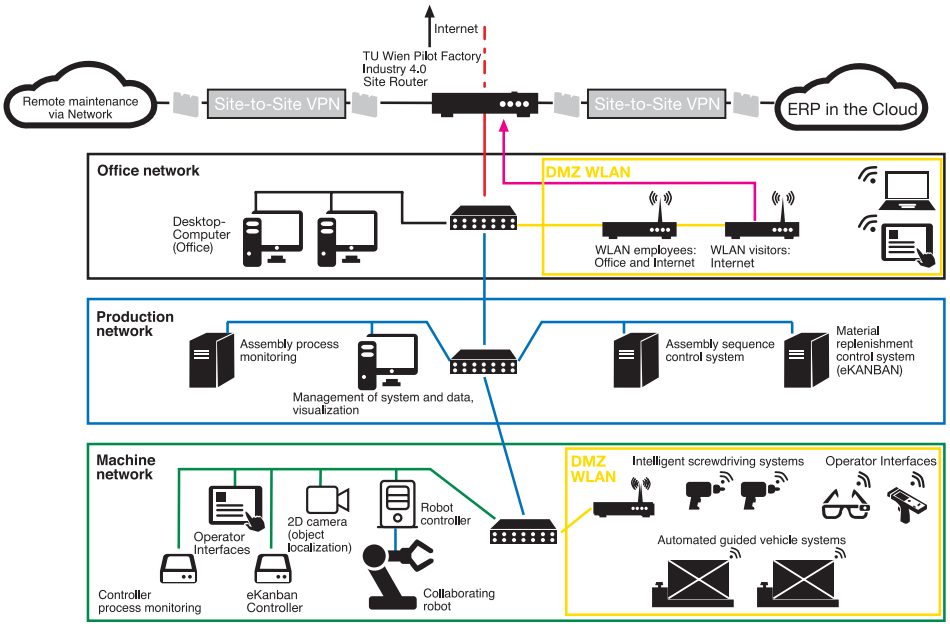

Figure 14: Network architecture at TU Wien Pilot Factory Industry 4.0 (after optimization)

In particular, the communication of the systems in the machine network is strongly channeled: Only individual control systems from the production network regularly have the option of addressing the production machines with commands or requesting information from them. This is guaranteed by an appropriately configured firewall. Those devices that operate with authentication use specific, complex user names and passwords. The devices within the machine network do not have access to the Internet. Devices in the office network, on the other hand, have no access to the machine network.

In such a structuring, even devices, machines and systems can be operated that have vulnerabilities regarding IT-security.

IEC 62443 recommends staggering countermeasures according to machine risk levels, with authentication via a two-factor system (such as a user name and password), antivirus prevention, system hardening, and network segmentation being indicated in the vast majority of cases of industrial automation and control systems.

7. An Integrated Safety & Security Concept

In terms of the identified vulnerabilities of collaborating robots with regard to IT security, when assessing the risk of applications, TÜV AUSTRIA and FRAUNHOFER AUSTRIA RESEARCH recommend an integrative procedure that is able to simultaneously detect and assess threats to functional safety and IT security according to the same scheme. The design of work cells and production lines must therefore follow the principle of "security for safety".

The project partners have developed the Integrated Safety & Security Concept for this purpose. It is based on the proven procedure for assessing functional safety risks in accordance with ISO 12100 and the application of best practices for checking and ensuring IT security in accordance with IEC 62443. The aim of the Integrated Safety & Security concept is to declare the CE conformity of the machine with regard to functional safety on the one hand and to ensure that the protection objectives of availability, integrity and confidentiality are achieved on the other.

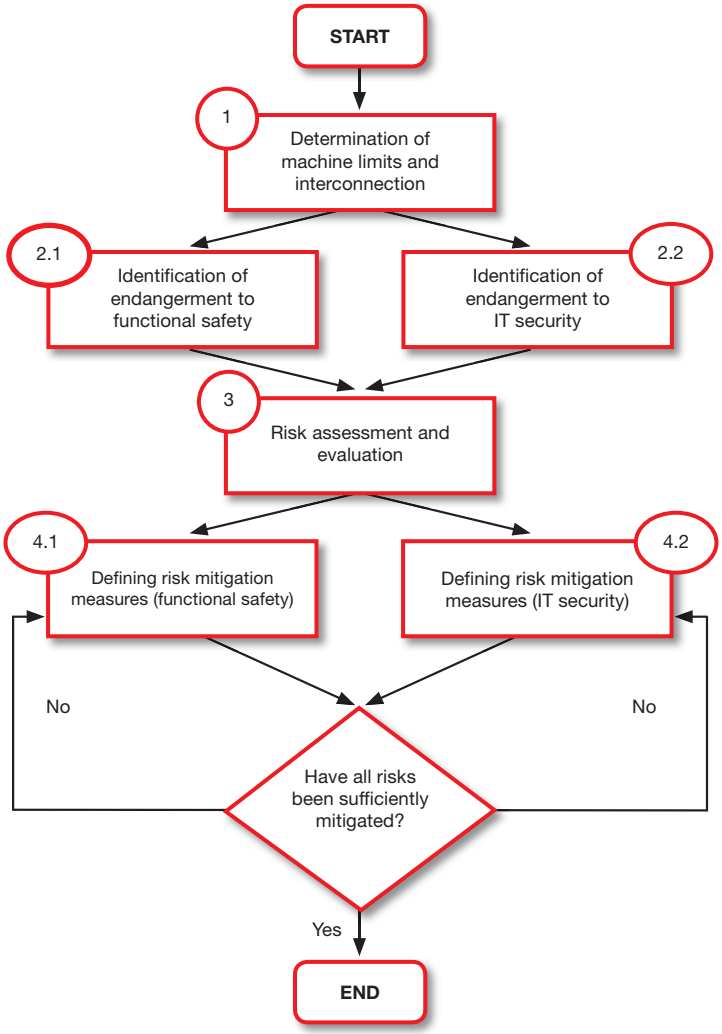

Figure 15: The structured process of integrated assessment of safety and security risks

7.1 Determination of machine limits and interconnection

In an initial step, the scope of the investigation necessary for an integrated assessment of machine and information safety/ security is determined, which includes in particular the degree of the machine's interconnection with regard to IT security.

7.2 Identifying risks

The identification of threats to functional safety is carried out in interdisciplinary cooperation by evaluating concept descriptions, process representations, existing prototypes or test setups of the machine or system. As already described in detail in the second edition of this white paper series, the various operational situations and life cycle phases of the machine are taken into account, as well as the dangers that can arise for the immediate operator of the machine, but also for all other groups of people who may come into contact with the machine, even if only seldomly.
The seven-step process of the test procedure for IT security described in Section 6.1 is used to identify IT security threats. The focus is both on the network and the interconnected machine itself. The evaluating security expert takes on the role of an attacker and tries to identify vulnerabilities in the network and the machine, to gain access and to increase his possibilities of sabotage and manipulation – without actually damaging the network or the machine.
Especially in the context of human-robot collaboration, several system elements from different manufacturers may be combined to form a complete system or application. Such individual elements are included in the analysis of vulnerabilities because manipulating them can keep the protection objectives from being achieved just as much as doing so to the robot itself.

7.3 Risk assessment and evaluation

A decision-making basis for prioritized implementation of measures to reduce the risks arising from identified threats is achieved by quantifying them individually.
Evaluating risks for IT security is something new. In order to do this, TÜV AUSTRIA's experts developed an assessment based on the evaluation of risks for functional safety, taking into account the factors extent of damage (D) and probability of occurrence (P). Multiplying the two factors yields a risk priority number (RPN).

$$D \times P = RPN$$

The extent of damage has a range of 0 to 4. A valuation of 0 corresponds to an insignificant extent of damage, which restricts a company's task accomplishment by a scarcely noticeable extent. An extent of damage identified as having a rating of 4 however, has significant effects, either in the sense of impairing the physical integrity of the employees or for the company's further development. While the assessment of risks to the functional safety of machines or systems primarily involves health risks, economic and business risks are also taken into account and at least roughly estimated or categorized when quantifying risks to IT security.
In addition to the severity of the consequences of a risk occurrence, its probability of occurrence, which ranges between 1 and 5 must also be determined. The value 1 correlates to an extremely low probability of occurrence, while 5 indicates a permanent possibility of occurrence with a high probability. This is based on the assumption that 100 percent exclusion of any possibility of occurrence, i.e., a value corresponding to 0, cannot be achieved.

Determining and heeding the risk priority number (RPN) resulting from the extent of damage and the probability of occurrence ensures that higher risks are also given priority and lowered by appropriate countermeasures. However, the RPN is only really meaningful if an acceptable residual risk is determined by the team responsible for risk assessment – while the need for action is determined by the difference between the residual risk sought and the currently existing risk.

7.4 Defining risk mitigation measures

Risk reduction measures are implemented iteratively upon the endangerment until the desired risk level (expressed by the RPN related to the endangerment) has been reached.
The following exemplification shows an example of the correlation between functional safety and IT security in human-robot, collaboration and the possible compromising mutual impact: The identified risk of injury from crushing between the robot, and the working environment is reduced to an acceptable level by limiting the robot's traversing speed, power and forces in the robot's safety programming – the RPN drops from 30 to 10. If, conversely, an endangerment to IT security exists that enables an attacker to alter the safety/security configuration unnoticed – whether remotely or locally – the original, unacceptable risk of injury is regained. Only by taking the additional countermeasures against the unauthorized compromising of the safety/security configuration, the original endangerment to the functional safety can be effectively reduced (Security for Safety).

	Machine										Creation date					Accepted residual risk						
	Mechanical endangerments	Risk before														Risk after						
Consec. no.	**Endangerment** Description of the endangerment/ danger point on the machine	S(0, 1-4)	F(1-5)	W(1-5)	P(1, 3,5)	risk class	Risk Priority numbe RPZ	PLr	SIL		**Measure(s)** Description of measures taken and to be taken, including justification of measures	Constructional	Technical	Organizational	IT	S(0, 1-4)	F(1-5)	W(1-5)	P(1, 3,5)	risk class	Close to risk priority RPZ I	
	Mechanical endangerments																					
102	Approach of a moving part to a fixed part, thus resulting in crushing of an upper part of the body, especially hands and arms (quasi-static contact with robot casing)	3	5	2	3	10	30	c	1		**Measure:** technical, limitation of the force (F) exerted by the robot; if necessary also robot power (W) and traversing speed (v), to a degree which reduces the risk of injury resulting from crushing to an acceptable level		x			1	5	2	3	10	10	
	Mechanical endangerments																					
Consec. no.	**Endangerment** Description of the endangerment/ danger point on the machine	S(0, 1-4)	W(1-5)	Risk Priority numbe RPZ							**Measure(s)** Description of measures taken and to be taken, including justification of measures	Constructional	Technical	Organizational	IT	S(0, 1-4)	W(1-5)	Close to risk priority RPZ				
	Endangerment to IT security																					
1211	Sabotage: Changing the installation file, in particular the safety/security configuration (limits for force, power & speed as well as spatial limits)	3	3	9							For physical import of a new installation file via USB interface: rights management, password protection, if necessary: sealing of the physical interfaces.				x	3	1	3			
		3	3	9							For changes via Ethernet socket: authentication, authorization, network zoning				x	3	1	3			

Figure 16: Correlation between safety & security using the risk priority number

8. Conclusion and Outlook

Thanks to available interconnected machines and systems, smart factories are not a future vision anymore, but can rather be realized today. However, the investigations carried out using the example of collaborative lightweight robots showed that even if the machines have a high level of functional safety, the IT security of the same machine can have vulnerabilities that not only restrict functional safety but also disrupt smooth production operations and reduce the security of company data.

A good knowledge of relevant standards and guidelines with regard to industrial IT security along with simultaneous consideration of functional safety and IT security in the context of risk assessment, as propagated by TÜV AUSTRIA's Integrated Safety&Security Concept, enables structured identification, evaluation and processing of vulnerabilities in the two essential dimensions of risk, thus enabling manufacturing companies to implement the vision of Industry 4.0 in a sustainable and secure manner while taking availability, confidentiality and integrity into account.

In this context, the increasing flexibility of digital factories is still an open challenge for safety and security. Changing products and changeable factory configurations require safety/security concepts which ensure that new threats and risks are covered functionally and informationally - even with frequent adaptations of work environments, machines and processes - without having to constantly and laboriously reassess this. The future work of our partners will be oriented toward this requirement, developing methods for risk assessment of industrial systems in order to enable flexible use with changing tasks while maintaining functional safety and informational security.

About TÜV AUSTRIA:

TÜV AUSTRIA is an independent Austrian company with branches in more than 40 countries around the world. TÜV AUSTRIA employs over 1,500 people.

The range of services offered by TÜV AUSTRIA Group extends from certifications of personal, systems and products to testing and inspections of elevators and pressure equipment, plant safety, basic and further training, medical technology, electrical engineering, expert assessments in sound-insulation matters, carbon footprint evaluations, IT security, Internet of Things, e-mobility, AppChecks, calibrations, product testings, robotics, technical due diligence and legal compliance checks through to testing and inspections of stage systems, photovoltaic systems and wind power stations.

Contact person for the topic of human-robot-collaboration:

Dipl.-Ing. Alexandra Markis - alexandra.markis@tuv.at

About FRAUNHOFER AUSTRIA RESEARCH GMBH:

Fraunhofer is the largest research organization for application-oriented research in Europe. Our research fields are based on human needs: health, safety, communication, mobility, energy and the environment. That is why our researchers' and developers' work has a big impact on the future life of mankind. We are creative. We design technologies. We develop products. We improve processes and we open up new paths. We invent the future.

Fraunhofer Austria Research was founded at the end of 2008 as the first European subsidiary of the Fraunhofer Society. At our locations in Vienna, Graz and Wattens, more than 50 scientists in the fields of production and logistics management, visual computing and industrial data science are currently researching application-oriented solutions for the benefit of industry and to the advantage of society.

Contact person for the topic of human-robot-collaboration:

Fabian Ranz, M.Sc. - fabian.ranz@fraunhofer.at

Sources:

[1] Global State of Information Security® Survey 2017, PWC.

[2] Bericht Internet-Sicherheit Österreich 2016, Computer Emergency Response Team Austria

[3] The Internet of Things – Mapping the Value beyond the Hype, Juni 2015, McKinsey & Company.

[4] VierNull Blog (https://viernull.blog/), ISAP AG.

[5] Orientierungsleitfaden für Hersteller zur IEC 62443, April 2017, Zentralverband Elektrotechnik und Elektronikindustrie e.V. (ZVEI).

[6] Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2016, Version 1.20, August 2016, Bundesamt für Sicherheit in der Informationstechnik.

[7] Leitfaden Security für den Maschinen- und Anlagenbau - Der Weg durch die IEC 62443, 2016, HiSolutions AG.

[8] OWASP Top 10 -2017 The Ten Most Critical Web Application Security Risks (https://owasp.org), The OWASP Foundation

WhitePaper

TÜV AUSTRIA Group

DI Alexandra Markis
TÜV-Austria Platz 1
2345 Brunn am Gebirge
Mail: *i4.0@tuv.at*

www.tuv.at/i40

Fraunhofer Austria Research GmbH
Fabian Ranz M.Sc.
Theresianumgasse 27
1040 Wien
Mail: *fabian.ranz@fraunhofer.at*

www.fraunhofer.at