mrl.news

Issue 2023.02

tec nicum

New challenges
From collaborative robots to cyber security

Exceptions not only confirm the rule, but may also be reasonable. When the British government decides to retain an EU regulation even after Brexit, this is good news which will open this issue of MRL News. The United Kingdom now plans to retain the European CE mark after Brexit – which will without question simplify the flow of goods. Not all of the EU's new rules are entirely positive: The current version of the Machinery Regulation is expected to be a barrier for users who want or need to upgrade their machines. Learn more on page 19.

The article on pages 4 to 7 explores the rules and standards to be observed when setting up a collaborative robotic workplace. The fenceless cooperation between humans and robots involves a high risk potential, which is why special requirements apply here.

In intralogistics, the risk potential is equally high. In this issue, we show you some new automation and safety solutions which increase both the safety and productivity of processes.

Challenges of a completely different kind arise in the remote maintenance of machines. Here, safety and security are to be kept in mind. External access to a company's IT infrastructure might be misused as a gateway for cyber attacks. Even direct attacks on control systems (PLCs) pose a real threat today. Prominent example: The 2010 attack on Iran's nuclear plants with the help of the Stuxnet computer worm.

And finally, one more piece of good news: tec.nicum increasingly offers its customers turnkey solutions – end-to-end solutions for machine safety. On page 8, you can read about the included services.

Enjoy the reading! Sincerely

Your Editorial Team

UK to retain European CE mark even post-Brexit

At the beginning of this August, the United Kingdom declared that it will retain the European CE marking for products indefinitely even after the country's withdrawal from the European Union.

Originally, the CE symbol was to be replaced by a new British safety mark called UKCA (UK Conformity Assessed) for products sold in the UK from the end of 2024. However, companies had complained about enormous additional costs and urged the government to abandon its plans, which initially would have meant merely mirroring the EU regulations.

According to press reports, Stephen Phipson, head of the British manufacturing association Make UK, called the move "pragmatic and reasonable". Companies can now choose whether or not to use the UKCA symbol – which is not recognized in the EU – to sell their products in the UK from the end of 2024.

The British Chambers of Commerce also welcomed the indefinite retention of the CE mark. A 2021 survey found that only 8% of companies wanted to abandon the EU labeling system, while 59% of those affected by the decision wanted to keep it.

Already in 2022, Schmersal had received the first UKCA certificate for its AZ300, AZM300 and AZM300-AS solenoid interlocks from TÜV Rheinland. By the beginning of 2023, Schmersal's most popular and most demanded products were to be equipped with the UKCA certificate so the customers can market their machines in the UK in compliance with the directive.

The UK government's change of direction facilitates the export of products to the UK, because companies can now choose between CE and UKCA markings. However, it's yet difficult to say whether between the UK and the EU the final say has been spoken on the issue of trade in goods. In any case, MRL News will keep you updated! ■

The safe cooperation between humans and robots in collaborative work systems is first of all possible and secondly offers distinct advantages – not least in packaging processes. However, some prerequisites must be met and various machine safety standards must be taken into account.

Design and construction of a collaborative robotized cell

Here's to good cooperation!

From robot to cobot: this step lends itself to many application areas in industrial automation – e.g. in food packaging when smaller quantities or special packaging are involved.

Collaboration, i.e. cooperation, between man and robot without separating protective devices can significantly increase flexibility here, and this precisely is required when small series are increasingly being produced or when different products are to be manufactured on the same line.

What should be considered when designing robotic cells with human-robot collaboration? The basic concept is that humans and robots work simultaneously in one work system and are additionally shielded from the outside by separating protective devices. This means: The cell needs a protective fence with safety gates plus means for feeding in and out of the hazardous area – e.g., conveyors or transfer stations for the products to be processed. But what the cell does not need (anymore) is a physical separation between the work areas of humans and robots. Regarding robotics and automation technology, this is a real game changer: For decades, robots and operators were never allowed to come into contact, and the robot had to do its job – all by itself – "under lock and key".

Now, the simultaneous activity of humans and robots in a work system is part of the Smart Factory. There are many manufacturers of collaborative robots (cobots) and at least as many system integrators whose plants are highly productive in producing smaller quantities of products and also packaging, also thanks to cobots. For each individual application, the strengths of the human operator (dexterity, force dosage, independent problem solving) are combined with those of the robot (precision, fatigue-free, repeatability).

Distinct principles for collaboration

Of course, at first the standard foundations had to be laid for this new type of collaboration – with the goal of equipping the robot with safety devices to →

protect humans and turning it into a collaborative robot. This has been done and will be briefly presented here.

As generally is the case with machine safety (i.e. in the scope of the Machinery Directive), the "standards pyramid" of harmonized Type A, Type B and Type C standards also applies in collaborative robotics.

A Type A standard is the basic safety standard EN ISO 12100 (risk assessment). Type B1 standards, which deal with special safety aspects, are a bit more specific. Examples are the well-known EN ISO 13849 (Safety-related parts of control systems) and EN ISO 11161 (Integrated manufacturing systems). Type B2 standards make statements on individual types of safety devices, e.g. emergency stop devices (EN ISO 13850).

For robotics, there are several specialized standards or Type C standards.
These include:

- EN ISO 10218 "Industrial robots – Safety requirements," divided into
  - Part 1 ("Robots") and
  - Part 2 ("Robot systems and integration"). Here, the safety requirements for robots and robot cells are defined.
- ISO/TS 15066 "Robots and robotic devices – Collaborative robots"

However, the "Technical Specification" ISO/TS 15066 is not harmonized, i.e. not listed under the MD. In addition, the EN ISO 10218 series of standards is about to be published in a revised version. Part two of the standards series from then on will include the requirements of ISO/TS 15066, so the requirements for collaborative robot systems will soon be completely contained in EN ISO 10218-2 and will thus also for the first time be harmonized under the MD.

Apart from the standards, there are other helpful documents on the subject of "Machine safety with collaborative robots," e.g. The DGUV Information 209-074 "Collaborative Robot Systems" including a checklist as well as a VDMA position paper "Safety in Human-Robot Collaboration" and several useful white papers from TÜV Austria.

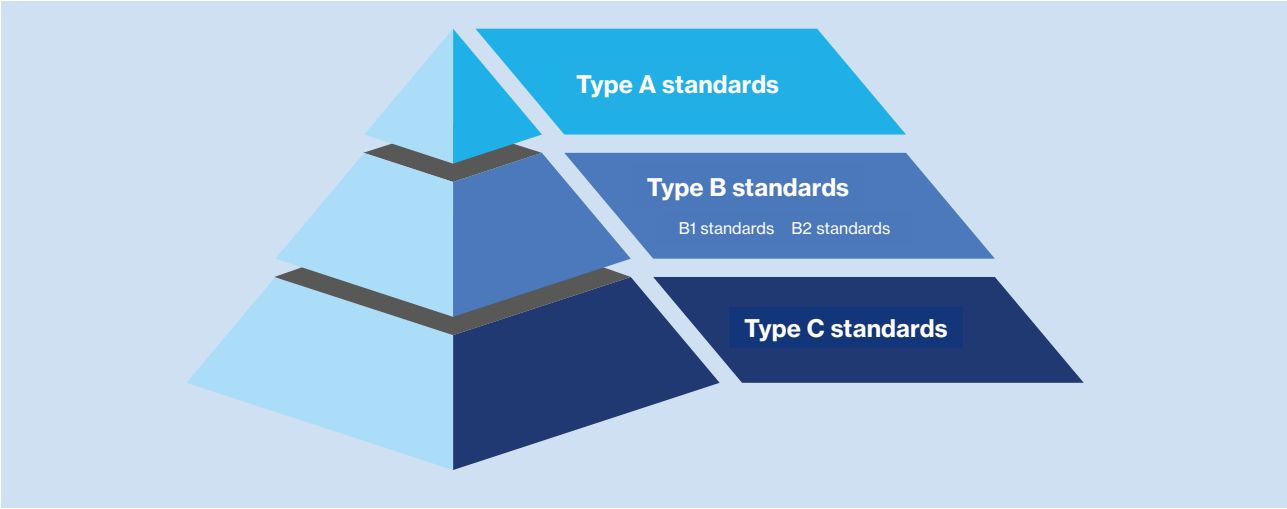
The path to a collaborative work system according to ISO/TS 15066

A collaborative robotic system can be achieved in three steps:

1. Use of a compliant robot according to EN ISO 10218-1
2. Integration of the robot into a robot cell in accordance with the requirements of EN ISO 10218-2 and applying EN ISO 11161 if necessary.
3. Design of the collaboration space according to ISO/TS 15066.

EN ISO 10218 defines the spaces to be considered when designing the safety measures of robot cells (maximum space, restricted space, operating space, protected space). What is more, with collaborative robots there is a collaboration space, which is described in both EN ISO 10218-1 and ISO/TS 15066. In this space, humans and robots can simultaneously be present to perform tasks. The corresponding mode is called "collaborative operation."

So, what are the specific requirements for the design and planning of a robotic cell as a "collaborative work system" according to ISO/TS 15066? After the layout of the cell is defined, the designer should identify the hazards and perform a risk assessment. This will provide the necessary measures to mitigate the risk. The measures that are permitted for a collaborative work system are described in ISO/TS 15066 and defined together with the corresponding requirements. →



Core Process: Design of the layout of the robot cell

Layout design is a core process in risk mitigation with collaborative robot cells. The layout will define the spaces mentioned above, including the collaboration space, and will also define the access points to the hazardous areas. In this important step, both the ergonomics at the man-machine interface should be considered as well as the additional space that may be required for the robot's runout movements (e.g., after the emergency stop device has been activated).

One of the tasks of the designer or safety engineer is to take into account the particular potential hazards posed by robots and to address them as part of the risk assessment. After all, it was not without reason that for decades the work areas of humans and robots had to be strictly separated. Helpful in this context are the hazard lists in Annex A of EN ISO 10218-1 and EN ISO 10218-2, which specifically address the hazards of robots and within robot cells.

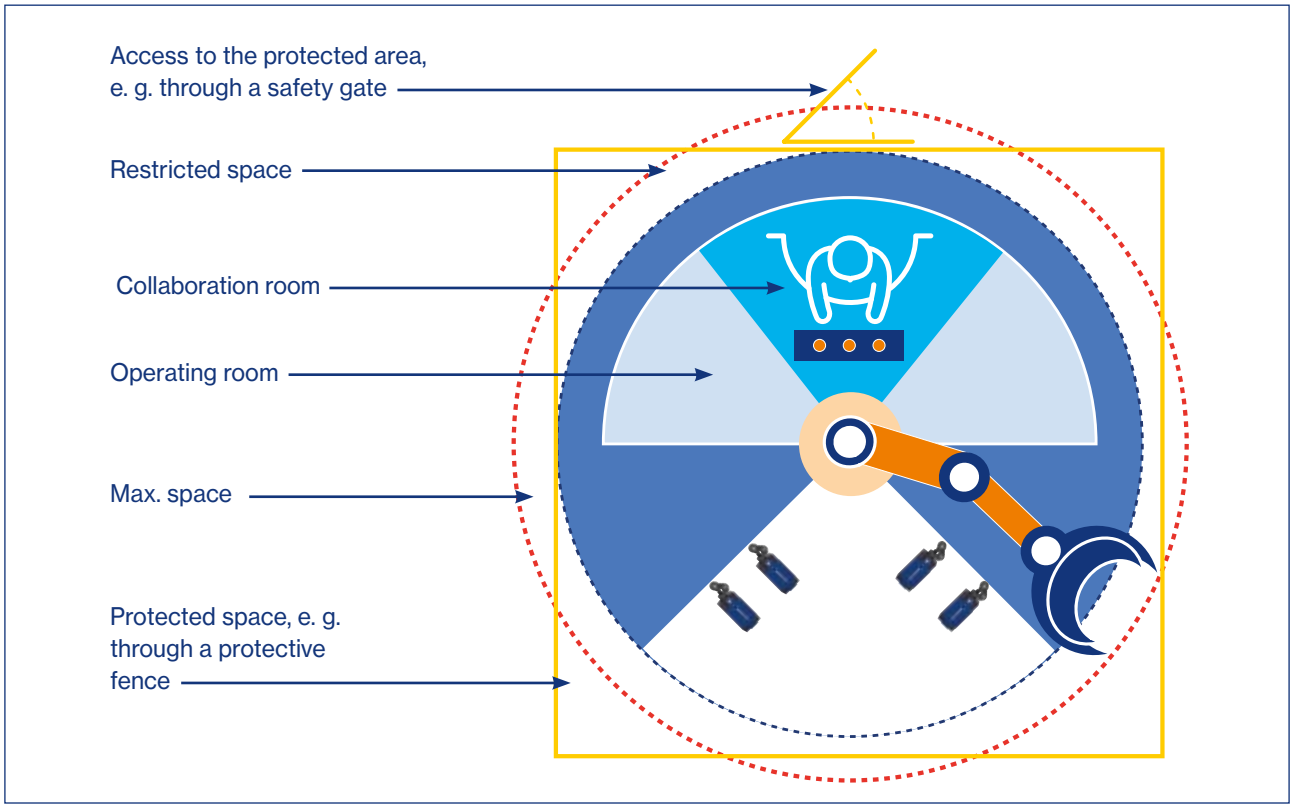
Specifically, the hazard potential results from the fact that robots perform movements with high energy and reach and that their travel path is difficult to predict. In some circumstances, it also has to be considered that several robots will be working in a common operating space. Therefore, the collaboration space must be clearly defined and in addition each operator in this space, i.e. in the working area of the robot, must carry their own control element. Equally mandatory is the use of safe axis and space limiting software, usually provided by the robot manufacturer.

Options for the design of a collaborative operation

ISO/TS 15066 focuses on four ways in which collaboration between the operator and the robot can be implemented. These include the manual operation of the robot (movement of the robot arm by human force), speed and distance monitoring (reduction of speed by distance), safety-assessed monitored stop (stop category 2, restart when leaving the collaboration space) and the limitation of power and force humans and robots can simultaneously be present to perform tasks (risk mitigation through reduced forces). As almost all of these methods require a control-based implementation, additional safety functions have to be created and evaluated.

Example: power and force limitation

The main hazard in the collaboration of humans and robots is the unintentional contact of both. Therefore, a power and force limitation is supposed to minimize the consequences of such contact. If such a contact is possible in the collaboration space, there are exposure limits related to the individual body parts that must be observed. This can be done by using →



With collaborative robots, there is a collaboration space described in both EN ISO 10218-1 and ISO/TS 15066. In this space, humans and robots can simultaneously be present to perform tasks.

passive protection measures, such as foam pads, increasing the contact area or limiting the moving masses. Alternatively, the designer of the collaborative robot cell can actively prevent this by using control technology – for example, by limiting the applied force or torque or by integrating sensor systems which detect the operator.

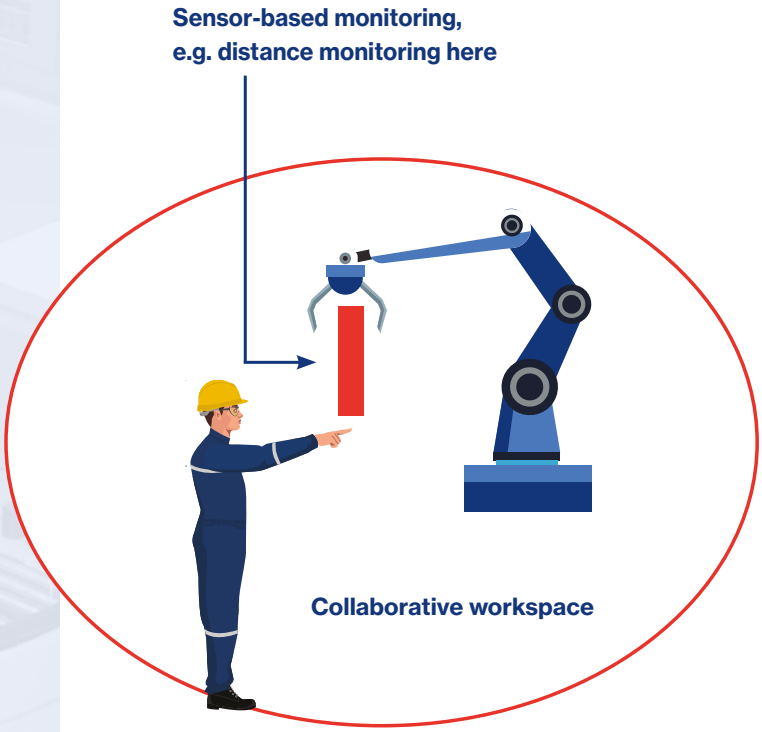
Thus, for the collaborative operation of robot cells, various safety functions have to be implemented. Depending on the selected implementation of the collaborative operation, aspects such as torque, force, speed or position of the robot axis are to be monitored in a safety-related manner. Likewise, an operating mode selector and enabling switch are usually part of the safety-related equipment. The corresponding products or system solutions are available – for example in the Schmersal product range – and have proved themselves in those applications.

After the design: Verification and validation

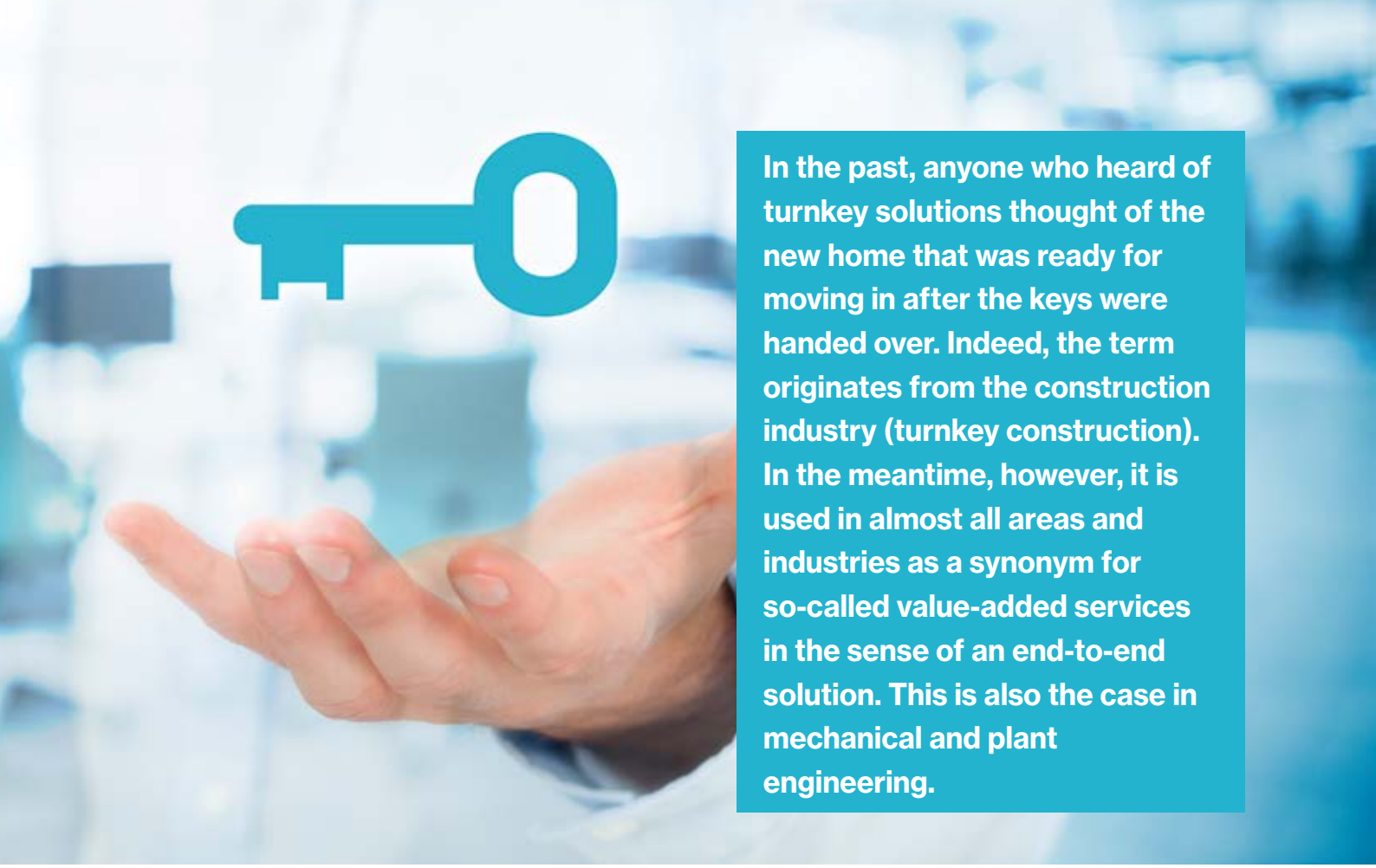
According to ISO/TS 15066, the result of the design of a collaborative robot cell must be conclusively verified and validated. Due to the high hazard potential in robotic systems, this step is elementary in order to positively confirm safety and achieve conformity in accordance with the Machinery Directive. For this – but also for the other necessary steps such as conformity assessment, risk assessment, force and pressure measurement – the user can call on the qualified services of Schmersal's tec.nicum. The safety consultants at tec.nicum contribute the necessary expertise and also have a high level of industry knowledge in packaging technology. ■

Benjamin Bottler
Safety Consultant,
Schmersal Group

Safety light grids monitor the collaboration space for a safe entry of a person.



For a collaborative operation of robot cells, various safety functions must be implemented, e.g. torque, force, speed or position of the robot axis must be monitored in a safety-related manner.



In the past, anyone who heard of turnkey solutions thought of the new home that was ready for moving in after the keys were handed over. Indeed, the term originates from the construction industry (turnkey construction). In the meantime, however, it is used in almost all areas and industries as a synonym for so-called value-added services in the sense of an end-to-end solution. This is also the case in mechanical and plant engineering.

Turnkey solutions – the key to success

Highly efficient safety-related modernization of machines and plants from a one-stop shop

Today, machine and plant safety is subject to constant evolution and a resulting continuous adaptation to technical progress. The growing requirements are placing increasing demands on operating companies, making it constantly harder for them to concentrate on their core task, that is, maintaining production processes with complex, high-quality precision machinery and equipment.

A machine's safety concept is an integral and absolutely necessary aspect of the operation of such production machines and plants. Initially, it does not matter whether the plant is new or already in operation. A machine must be safe at all times!

Therefore, turnkey solutions are equally becoming increasingly important in the area of machine and plant safety. Turnkey safety solution providers take care of the entire area of machine safety for the customers and provide them with a complete manufacturing chain up to the handover of a safe end-to-end solution. This ranges from security analysis and evaluation, through the development and engineering of security concepts, to turnkey handover after installation of the security solutions.

The Schmersal Group's tec.nicum has also adapted to this development and offers its customers precisely such holistic services.

Already at the time of the foundation of tec.nicum in January 2016, Schmersal has included safety services in its portfolio. Initially, it was only in the form of separate services such as risk assessments, calculations of safety functions or validations of safety functions.

However, true to the motto "standing still means going backwards", tec.nicum is facing the challenges of the future and is constantly evolving in order to be able to offer its customers the best possible and tailor-made service.

From component manufacturer to system and solution provider

Following exactly this concept, turnkey projects →

are now part of the standard offering of tec.nicum services. We offer our customers and partners complete solutions that meet all legal and customer requirements and thus ensure safe operation of the plant. In order to achieve the most cost-efficient and process-optimizing effect possible, our project coordinators and engineers are constantly in close contact with the client's responsible staff. This is the only way to achieve future-proof solutions in the interests of our customers. Our project partners get exactly what they need and not just what we have!

Should it become apparent in the course of a project that certain activities cannot be carried out by the tec.nicum experts themselves or must not be carried out by them, we will of course nevertheless take care of an appropriate implementation. A broad network of specialized partners enables us to react quickly to any task that is entrusted to us.

In the case of open turnkey projects, it is up to our customer to decide which trades they would like to carry out themselves and which they would like to outsource to us. In the end, however, we in any case hand over the project to our customer on a turnkey basis at the agreed time.

For our customers, the great advantage of our turnkey solutions lies in the fact that the machines and plants can be used immediately after turnkey handover without any further adjustments.

This is also the decisive advantage over generic, standard solutions, which usually have to be adapted by the operating company to their own needs and requirements with relatively high effort. Not with us! tec.nicum always delivers individually customized solutions that are 100% tailored to the customer's processes and requirements!

In order to avoid unnecessary production downtimes during the course of the project, all necessary modifications on the machine are coordinated with the customer's maintenance and servicing cycles and stored accordingly in the project plan. This ensures the smoothest possible project flow.

After-sales service with permanent professional support

Also after a modification, the safety technology has to be maintained. The scope of these maintenance services always depends on the requirements and needs of the customer as well as any external regulations and can include various services in connection with the safety-related equipment of the machine or plant. For example, recurring inspections of optoelectronic protective devices (light barriers or light curtains) are required at regular intervals, or individual components must be replaced because they have reached the end of their service life. With a reliable partner who knows the safety concept of your plant down to the last detail and always keeps an eye on it, this is no problem. ■

Conclusion:

Turnkey solutions represent a high added value for the owners of machines and plants which require a safety-related modernization. All relevant work – from the initial analysis to the complete technical implementation – is taken care of and executed by a single contractor.

The owner can rely on professional and high-quality project execution according to the latest state of the art. And since he does not have to deploy his own employees for this, he can consequently deploy them for other tasks and projects. All project-related practical and organizational tasks are implemented professionally and reliably by our employees.

The key to your success is our turnkey solution!

The experts at tec.nicum will be happy to support you with their many years of wide-ranging experience from countless projects in mechanical and plant engineering.

Just contact us. We are confident that we can provide you with the support you need!

Tobias Keller
Business Development Coordinator
Solutions & Services at tec.nicum of
the Schmersal Group

Does the remote maintenance of machines require a risk assessment? What challenges do Industry 4.0 and new regulations pose for security? What steps are necessary to ensure IT security? Which standards are relevant for remote maintenance? This article aims to encourage the readers to take a closer look at the topic of cyber security.

Challenges and opportunities when accessing machines remotely

Safety and security in remote maintenance

The German Federal Office for Information Security (BSI) describes remote maintenance “when an external IT system is used to access IT systems and the applications running on them. This access can facilitate configuration, maintenance, or repair work, for example.” [1]

The advantages of remote maintenance are manifold. Above all, it saves time and costs; for example, it eliminates the expenses and travel time for journeys. A technician can connect to the faulty system in seconds and locate the fault and either rectify it or instruct a technician from the owner. This allows service staff to be centralized at the machine builder, and this centralization often makes it easier and faster to access other specialists within the company.

The Covid-19 pandemic and the associated travel restrictions have exacerbated the need for remote solutions. This not only applies to remote maintenance for troubleshooting or as a planned revision, but among others also to the commissioning of a machine.

Technically speaking, in times of broadband connections, access via the Internet is not a problem. There are countless software tools that allow access to PCs. Also, many controllers are easily accessible via their IP addresses. However, two important aspects must be considered in the context of remote access: safety and security. Safety in this context refers to the protection of people from the machine as defined by the Machinery Directive; this is also referred to as functional safety. In contrast, security describes the protection of the machine from the human being.

In addition, there are legal questions, e.g. regarding liability, when the operator’s personnel work on site with a service technician who is connected online. These questions will not be considered here; we will only refer to the offer of the VDMA as an example. The Association of Machinery and Plant Manufacturers offers draft contracts to assist in the mutual (liability) legal safeguarding of operator and machine builder. [2]

For remote access, a distinction should be made between read-only and read/write access. During remote diagnostics, merely a read-only access is used. Likewise, the term condition monitoring, frequently used in the context of Industry 4.0, generally only requires →

reading access to machine or process data. From the perspective of machine safety, this is generally not critical, since there is no external intervention in the process, i.e. the machine does not leave its operating state and all safety functions are active as normal. With regard to security, read-only accesses can often be secured relatively easily via so-called data diodes. In the end, however, it is necessary to assess what data is being read and whether this data can fall into the wrong hands. In this case, appropriate measures have to be taken.

Safety

Both commissioning and troubleshooting, but also planned maintenance, often require the machine to be moved with deactivated protective devices, for example, in order to be able to carry out adjustment or cleaning work as efficiently as possible. Even under these conditions, the protection of the operators must be ensured, regardless of whether remote access to the machine is currently taking place.

To ensure this protection, suitable measures must be taken, in particular to prevent unexpected start-up. [3] Here, a special operating mode might be useful that must be actively initiated by the machine personnel. Furthermore, it should be ensured that emergency stop devices in particular always have priority and cannot be overridden by remote commands. Equally, it should not be possible to reset security functions remotely. Ideally, it should also be clearly indicated on the machine that a remote access is currently active. Last but not least, technical and organizational measures should also be taken to prevent third parties from intervening in the remote maintenance process without authorization and thus initiating dangerous machine states.

In the end, remote access is another operating mode of the machine that must be evaluated as part of the risk assessment and for which suitable safety functions must be defined and implemented to ensure operator protection. EN ISO 13849 [4] and EN ISO 12100 [5] provide important information here, although not explicitly with regard to remote maintenance.

For all changes to the safety application or changes to safety-relevant parameters, such as permissible speeds, pressures, temperatures, etc., the question also arises as to whether or not a significant change has occurred. A guideline in this respect is provided by the interpretation paper of the BMAS [6], but also by the Blue Guide [7] of the European Union. In case of doubt, the person who makes the change will become the new manufacturer of the machine, with all the associated obligations, such as performing a new conformity assessment in accordance with the current Machinery Directive. In Annex IV Machinery, such modifications must also be agreed with the notified body if a type examination has been used as the conformity procedure. Otherwise, the test certificate may become invalid. But even if it is not a significant change, the operating company must evaluate the change and take measures in accordance with the Ordinance on Industrial Safety and Health if necessary [8]. In any case, a comprehensive validation of the safety functions with each change should always follow.

Security

External access to the company's IT infrastructure has always been a major challenge for the responsible administrators. Whereas initially the main focus was on the protection of intellectual property (IP), today we are often faced with the hazards of ransomware. In a 2022 study by security vendor Sophos [9], 67% of the German companies surveyed said they had been victims of ransomware attacks. On average, this resulted in damage of €1.6 million, not only due to the payment of the ransom, but also due to production downtimes, disrupted supply chains, recourse claims, etc.

Even direct attack on control systems (PLCs) is a real threat today. The 2010 attack on Iran's nuclear facilities by means of the Stuxnet computer worm is just one pro minent example for this [10]. For example, in 2022 the →

prominent example for this [10]. For example, in 2022 the Industroyer2 malware was used to attack the Ukrainian energy supply. This malware can also be run on industrial control systems (ICS) [11]. In the course of Industry 4.0, the boundaries between the field level and ERP (enterprise resource planning) are increasingly disappearing due to the advancing vertical networking of these areas. This also means that the so-called air gap, i.e. the physical separation of OT (operational technology) and IT (information technology), is disappearing. For example, the use of IP-based fieldbuses offers new gateways for attackers. In addition, new regulations such as the Machinery Regulation [12], the EU Cyber Resilience Act [13] or the new version of the NIS Directive [14] create further pressure to act. Especially the NIS-2 Directive, which will come into force no later than October 2024, requires special attention because the criteria for when the directive applies to a company have been revised and expanded.

What should be done?

The first step should be an assessment of one's own situation, that is a risk analysis similar to that for functional safety. The IEC 62443 series of standards provides assistance here. In particular, parts 2-1 [15], 2-4 [16] and 3-3 [17] are relevant for operators and integrators. It defines so-called maturity levels for the process. The technical requirements for systems are evaluated by four security levels (SL). The different levels indicate the resilience to different attacker classes, i.e. how many resources would have to be expended. Even if at first glance there seem to be many analogies to functional safety, this standard – unlike EN ISO 13849 for example – does not provide any 'simple' instructions for achieving a certain safety level. There is no one solution that is optimal for all applications and network topologies – both in terms of the protection to be achieved and with regard to costs and administrative effort.

Basic safety principles

One of the basic requirements for a secure IT/OT topology is the segmentation of networks with intermediate so-called demilitarized zones (DMZ). These DMZs protect the transitions between the different network areas, e.g. by means of firewalls. At minimum, the different levels according to the Purdue reference model [18] should be protected accordingly. Depending on the network topology or the identified risk, it may also make sense to encapsulate individual production sections or even individual machines in a separate segment. →

Remote maintenance should always be under control of the operating company. This on the one hand means that remote maintenance can only be imitated or at least authorized by the operator. On the other hand, the hardware used should also be under the control of the operator. This is the only way they can ensure that access to their network is always up to date, i.e. that all known security vulnerabilities are closed promptly.

It is also advisable to set a time limit to prevent accesses to the network that have been opened for remote maintenance, e.g. VPN access, from remaining open after the remote maintenance has been completed. Remote sessions should also always be logged in order to be able to track access and any changes made.

Unlike functional safety, where the limits of the machine are defined at the beginning and a runtime of 20 years is considered, security is an ongoing process. In order to keep up with the constant development, continuous updating (patching) of the corresponding components and the software used is indispensable in order to be able to immediately close detected vulnerabilities. Presently, remote maintenance is described in only a few standards. One of them is the EN ISO 10218-2 standard [19]. For robot systems, it specifies that remote control should only be possible when the machine control is in manual operating mode. In addition, safety-relevant parameters, axis and space limitations, path changes, etc. can only be changed if the changes are accepted and confirmed by the operator on site. ■

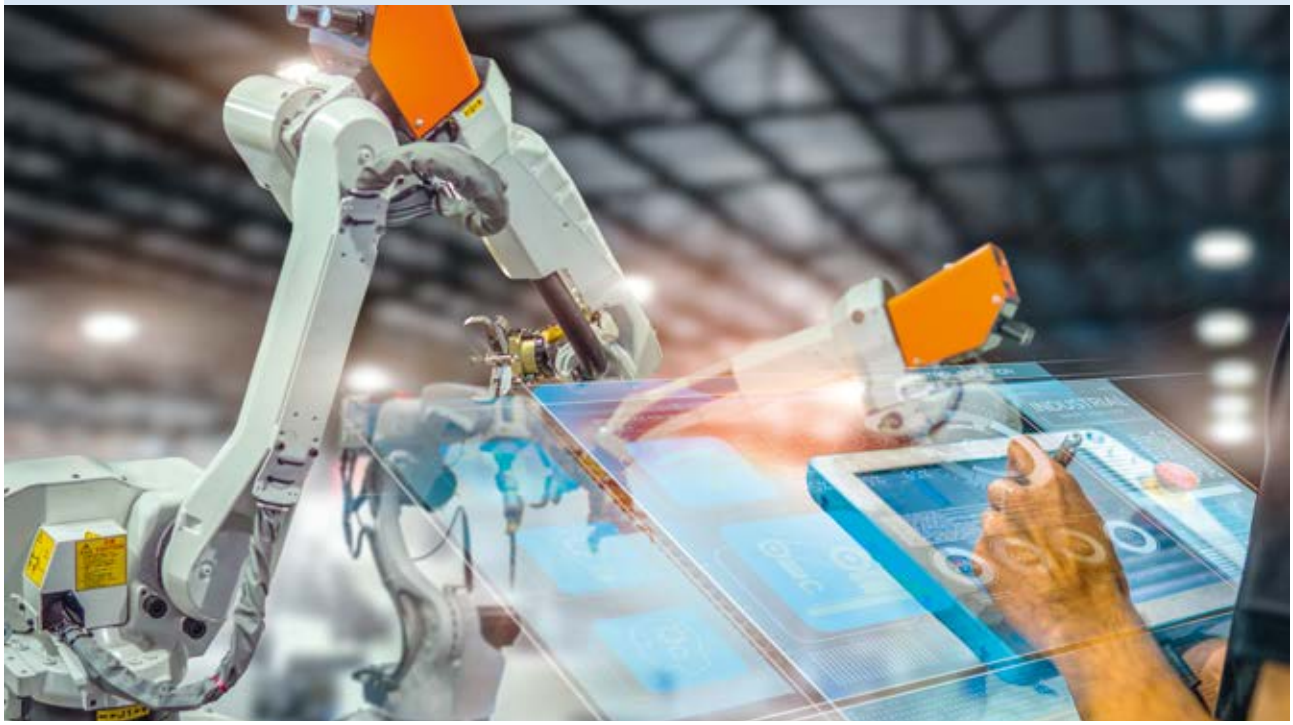
Conclusion

Remote access to machines is a modern tool for efficiently performing commissioning or maintenance work. However, it is important to be aware of the risks, both in terms of IT security and in terms of safety for the operator; in the form of functional safety. This text cannot and does not intend to provide a comprehensive account; rather, it is intended as an inventive to deal with the topic of cyber security in particular. It is here that the new EU directives are creating new challenges for both machine builders and operating companies. Challenges are becoming increasingly urgent due to the changes in the interaction between IT and OT in the framework of Industry 4.0.

Christian Lumpe
Product Manager Control Systems,
Schmersal Group

References

1. Federal Office for Information Security (BSI). OPS.1.2.5: Remote Maintenance
2. VDMA Verlag. Remote commissioning. EAN 4250697525225
3. EN ISO 14118: Safety of Machinery. Prevention of unexpected start-up
4. EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
5. EN ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction
6. Federal Ministry of Labor and Social Affairs. Interpretation Paper “Substantial Modification of Machinery”
7. Commission Notice: Guide for the implementation of the EU product rules 2016 (“Blue Guide”) (2016/C 272/01)
8. Ordinance on Safety and Health Protection in the Use of Work Equipment (Betriebssicherheitsverordnung – BetrSichV)
9. Sophos Ltd. “State of Ransomware 2022”
10. Product Notice, Posting ID: 43876783, posting date: 01.04.2011. “SIMATICWinCC/SIMATIC PCS 7: Information about Malware / Virus / Trojan Horses” 1 1.
11. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
12. Regulation (EU) 2023/1230 of the European Parliament and of the Council
13. Proposal for a regulation of the European Parliament and of the Council on horizontal cyber security requirements for products with digital elements
14. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cyber security across the Union
15. IIT security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners
16. IT security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers
17. Industrial communication networks – Network and system security – Part 3-3: System requirements for IT security and security level
18. Theodore J. Williams: The Purdue Enterprise Reference Architecture: A Technical Guide for CIM Planning and Implementation
19. EN ISO 10218-2 “Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration”



Schmersal's new magnetic track sensor box SSB-R.

New automation and safety solutions for intralogistics

In-house material flow: safe – productive – networked

Intralogistics is becoming increasingly important in many industries. Due to supply bottlenecks and material shortages, new concepts for warehousing and material flow are required. And also Industry 4.0 cannot be made a reality without efficient and networked logistics. Now there are new technical solutions and systems for a safe and productive intralogistics infrastructure.

In intralogistics, the demands on the systems' productivity and reliability are extremely high. Customers expect ever faster and more reliable order processing, which is why processes are increasingly being automated. In addition, the potential for hazards during in-house storage and transport is high. But accidents not only endanger the health of employees, they also disrupt operations and lead to high costs. When developing new automation and safety solutions for intralogistics, Schmersal therefore always keeps both in mind: safety and productivity.

Cost-efficient and maintenance-free: the new SSB-R magnetic track sensor box for electrified monorail systems

Electric monorail systems are used in a wide variety of industries to transport workpieces and materials of all kinds. The overhead conveyance is much more efficient and faster than stationary conveyor technology, and it frees up floor space in assembly and storage areas. In each overhead system, many trolleys travel on a common overhead track. They travel fast in some areas, slower in others, and stop at defined points. Therefore, monitoring the speed and position of each trolley is essential. In the past, this was done with magnetic sensors. Schmersal's new SSB-R magnetic track sensor box now performs these functions with significantly greater precision.

The sensor box enables polling four parallel and independent magnetic tracks. It detects the magnetic field of the actuators and changes their signal state as they pass. This level change, which is also generated during fast pass-by, remains until the next control signal. A connected control system uses the signals to determine the position and route section of the sensor box and controls e.g. speed (rapid/creep speed) or stop positions of the drive motor.

The sensor box is available in four versions. The version with the designation SSB-RH is equipped with additional sensor technology on two tracks and uses a high-level signal (100 ms). With these properties it delivers higher positioning accuracy and can bring a trolley to a stop at the desired stop position with an accuracy of +/– 1.5 mm. This is an advantage at robot workstations, for example, where components have to be positioned very →

precisely. By means of the second positioning track, a stop zone can be precisely defined, e.g. with start and end positions in case of overtravel.

Another bonus for productivity: The magnetic signal storage also works in the event of a power failure and enables a rapid restart of operation.

But not only when planning new installations the sensor box can provide simplified installation and more precise positioning of the trolley. Also on existing overhead systems, the box can easily replace four individual magnetic switches, e.g. of the Schmersal BN325 and BN310 series, with minimized installation effort and higher positioning accuracy, since the magnetic switches and tracks are installed at the standard distance of 30 mm.

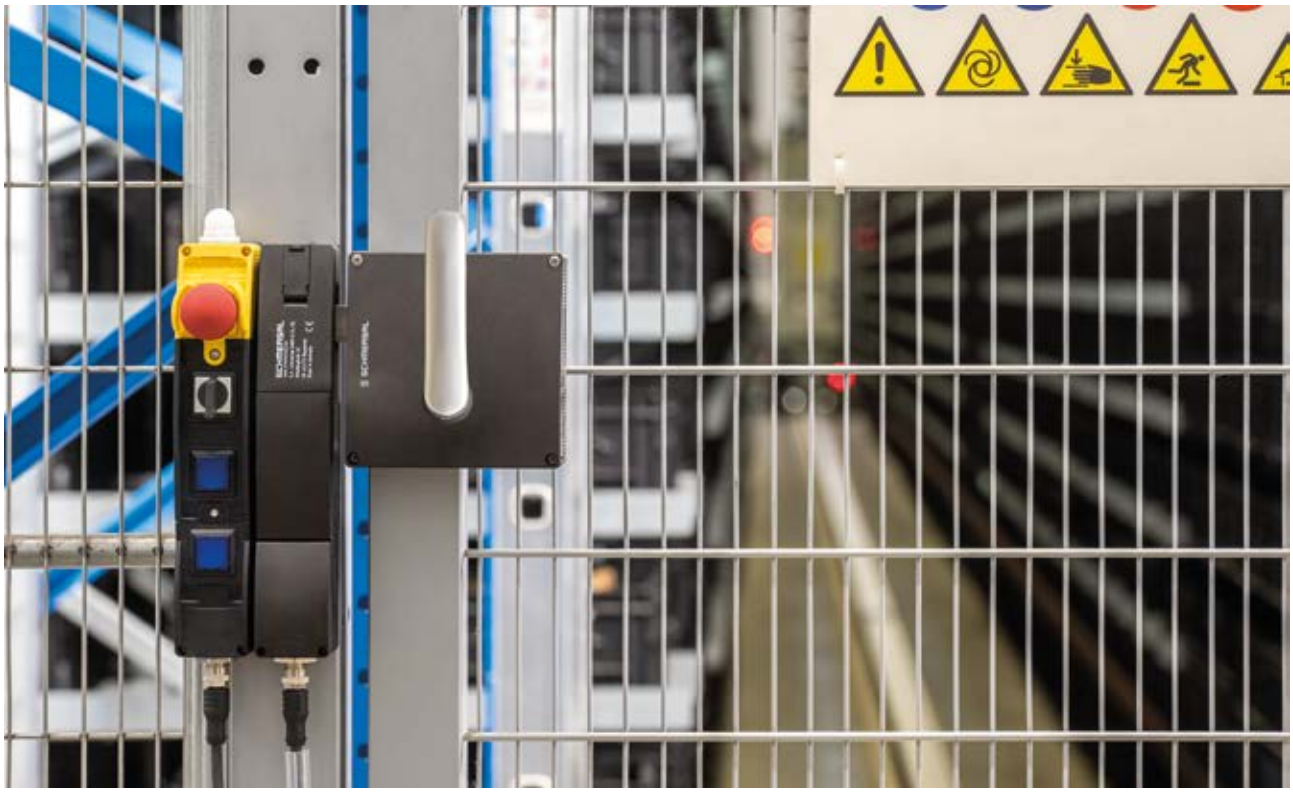
Flexible application options also result from the fact that there are various other materials handling systems that are supplied with power and signals via conductor rails – for example, storage/retrieval units, floor-based skids and shuttles on the individual levels of shuttle ASPWs (Automated Small Parts Warehouses). For these and other installations, the use of the magnetic track sensor box offers the same advantages as for electric monorail systems.

Networked security solutions

In large logistics sites, e.g. in the regional warehouses of discount grocery stores or goods distribution centers of contract logistics companies, the material handling is largely automated. Special requirements apply here for machine safety because the automated plants are spacious and there are many “interfaces” to the personnel – for example handover points. For these reasons, the networking of the safety switching devices lends itself here. This means: The traditional, individual wiring of each switching device is replaced by more efficient, network-like wiring concepts. There are several options to choose from.

Palletizers handle heavy loads at high speed. To protect employees, e.g. from the rapid movements of gantry robots, the work areas of humans and robots are separated by safety fences with at least one safety gate, the status of which must be monitored in a safety-related manner. The designer should preferably choose a solenoid interlock, e.g. Schmersal’s AZM201 interlock. It keeps the safety gate locked until the dangerous (overtravel) movement has stopped. This ensures uninterrupted operation because the palletizing process cannot be stopped by opening the safety door. This is even more important because palletizers are usually integrated into interlinked production and packaging processes.

Safety interlocks – as well as many other safety components from Schmersal – can be equipped with an integrated interface for the “AS-i Safety at Work” (AS-i SaW) safety bus and thus easily be integrated into a safety circuit. But the AS-i Safety standard not →



Solenoid interlocks such as the Schmersal AZM201 are used to monitor the status of safety gates, e.g. at robot workstations.

only enables fast installation with minimal wiring effort. It also offers a high degree of flexibility, e.g. in the event of plant modifications or new (safety) requirements.

Another advantage present the comprehensive diagnostic functions. In the event of irregularities or malfunctions, they allow a quick location of the error source. This is also an advantage, especially in the case of spacious, complex plants, as in such cases the downtimes can be significantly reduced. Therefore, many intralogistics systems that are equipped by Schmersal with safety systems are interconnected via AS-i SaW.

Connection via the safe field box

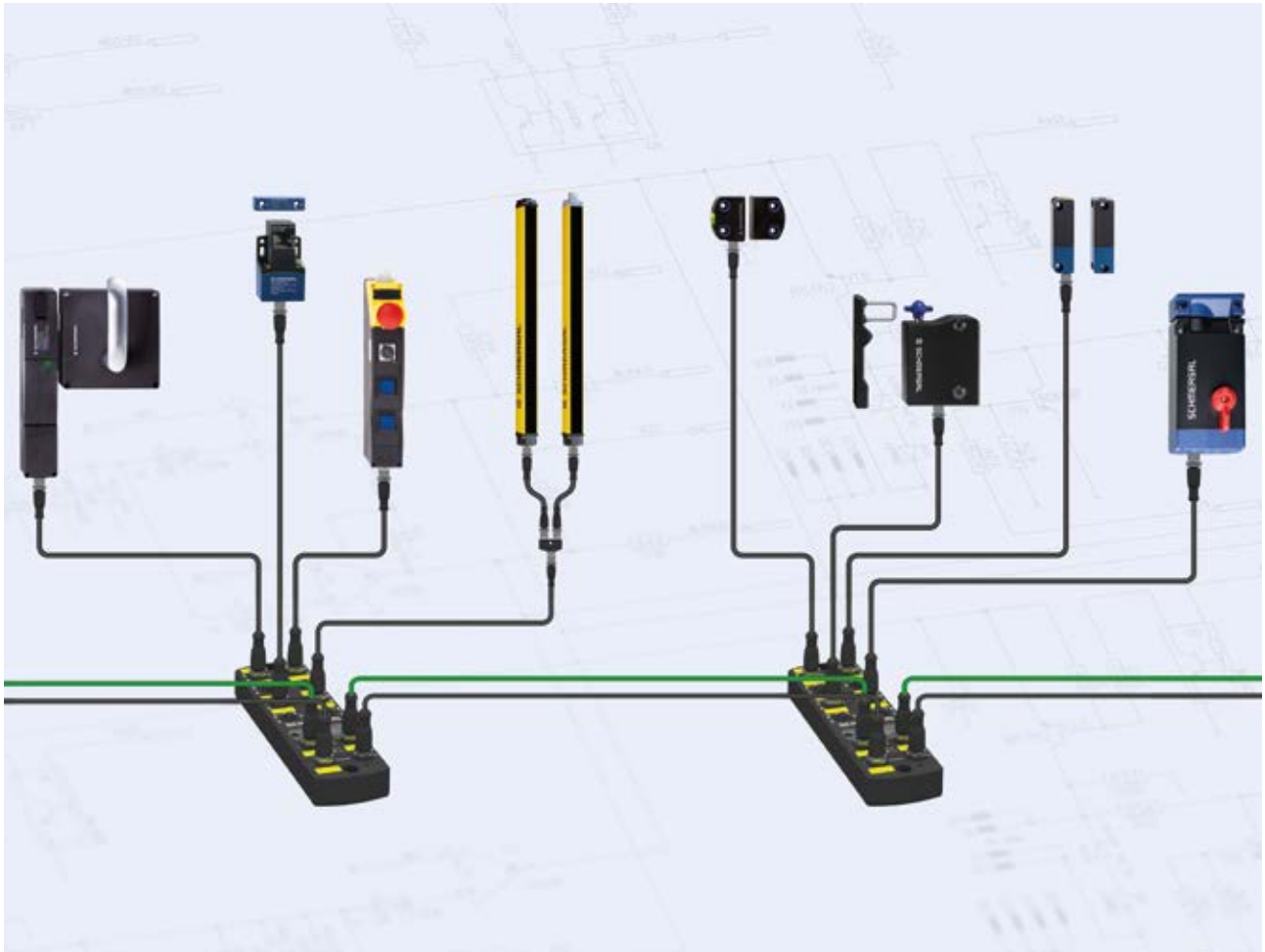
Alternatively, the "Safety Fieldbox" system (SFB) can be used instead of AS-Interface Safety at Work. A safety fieldbox enables the connection of up to eight safety switchgear of different types in the field. In this scenario, electromechanical and electronic devices each occupy only one device port. Both the safety-related and the operational signals are collected and transmitted via the PROFINET/PROFIsafe protocol – i.e. via the most commonly used bus system in Europe – connected to higher-level control modules.

New SD 4.0 bus system

If the user wants to collect and evaluate only operational, i.e. non-safety-related signals, SD 4.0 offers a third option. This is the latest version of a bus system developed by Schmersal which is used by electronic safety sensors and solenoid interlocks to transmit comprehensive status and diagnostic data to a higher-level machine control system.

A key difference between SD 4.0 and the previous SD bus is that it is much easier to communicate with higher levels. The prerequisite for this is provided by the connection to OPC UA as the standardized protocol for M2M communication. Among others, this has the advantage that the diagnostic information "collected" in the field can be better visualized and accessed via mobile devices such as tablets or smartphones. This facilitates the implementation of predictive maintenance concepts. ■

Marcel Bogusch
Industry Manager Logistics,
Schmersal Group



The Safety Fieldbox enables networked safety solutions.

Manufacturers and operators should deal with the new Machinery Regulation (MR) at an early stage, because the requirements must be implemented from 20.1.2027

Definition of the term “substantial modification” in the MR

What influence does the introduction of the Machinery Regulation have on existing plants or retrofitting?

The definition of “substantial modification” in the MR now also affects operating companies which convert or modify machinery.

The regulation to be applied from 20 January 2027 is set out as follows in the new MR.

Article 3 Definitions

16. “Substantial modification” means a physical or digital change “not foreseen or planned by the manufacturer”, to a machine or related product after it has been placed on the market or put into service, which affects the safety of that machinery or related product by creating a new hazard or by increasing an existing risk, which requires:

a. the addition of guards or protective devices to that machinery or related product the processing of which necessitates the modification of the existing safety control system; or
b. the adoption of additional protective measures to ensure the stability or mechanical strength of that machinery or related product.

The statement, “physical or digital change not foreseen or planned” initially means a “substantial modification” for 99.9% of the cases, because hardly any manufacturer plans a physical or digital change after placing the product on the market. What is more, according to the current version of the MR, the “substantial modification” **results in a new machine**. The simplification regarding the “assembly of machinery” will not cause much cheering.

Article 18, “Other cases in which obligations of manufacturers apply”, explains:

“A natural or legal person that carries out a substantial modification of machinery or a related product shall be considered to be a manufacturer for the purposes of this Regulation and shall be subject to the obligations of the manufacturer set out in Article 10 for that machinery or related product or, if the substantial modification has an impact on the safety of only machinery or a related product that is **part of an assembly of machinery**, for that affected machinery or related product, as demonstrated in the risk assessment.

The person who carries out the substantial modification shall in particular, but without prejudice to other obligations set out in Article 10, ensure and declare on its sole responsibility that the machinery or related product concerned is in conformity with the applicable requirements of this Regulation and shall apply the relevant conformity assessment procedure as provided in Article 25 (2), (3) and (4) of this Regulation.

A non-professional user who carries out a substantial modification to his or her machinery or related product, for his or her own use, shall not be considered to be a manufacturer for the purposes of this Regulation and →

shall not be subject to the obligations on the manufacturer set out in Article 10.

The “proportionality” mentioned in consideration (26) is not really clear to us in the articles, at least not for commercial operators of machinery and equipment.

However, since in practice many operators modernize their machines or convert them to meet operational requirements, the current version of the MR will certainly represent a major hurdle. Operators must think carefully about how “future-proof” their next acquisitions are and whether modifications remain justifiable from an economic point of view with regard to the MR.

tec.nicum supports manufacturers and operators in implementing the challenges of the new MR – from consulting and training to “turnkey” machines or systems. For example, turnkey projects with modifications are either accompanied or completely carried out as part of a general contractor agreement. ■

Jürgen Heimann
Lecturer, omnicon engineering GmbH,
member of tec.nicum

Staff reinforcement for tec.nicum

The services provided by tec.nicum are increasingly in demand. For this reason, personnel capacities are being expanded. Two new experienced experts are strengthening the tec.nicum team since the beginning of this year.

Thilo Potthast has been a new employee for project processing in Wuppertal since 01.04.2023. As a state-certified technician specializing in electrical engineering/automation technology, Thilo Potthast has vast expertise in the creation of control applications and visualization systems in the automation sector. His professional experience also includes robot applications and their programming as well as the implementation of industrial processes.

In his role as project manager in mechanical and plant engineering, he will contribute his expertise in the Solutions & Services division and deepen and apply his extensive knowledge in the new area of machine safety.

Since 01.07.2023, **Matthias Wellandt** strengthens the team of tec.nicum. He brings many years of experience in design and development as well as in the project business. As a graduate engineer specializing in electrical and automation engineering, Matthias Wellandt has been able to gain experience in the field of functional safety in nuclear technology as a project engineer since 2011. In the design and development department of a medium-sized mechanical engineering company, he has been responsible for electrotechnical products and developments since 2017 and acquired the Functional Safety Engineer qualification in 2019. At tec.nicum, he will use his expertise primarily in consulting and will also support the Solutions and Services division and the tec.nicum academy.

tec.nicum academy
Seminar program 2024

The tec.nicum academy provides you with a comprehensive range of training courses and seminars dealing with the safety of machines and plants.

Visit us at **www.tecnicum.com**, where you can find up-to-date detailed information and booking options for all seminars and special events.

We would be happy to prepare an in-house seminar tailored to the individual domain interests of the participants on your desired date.

Contact us:

Jasmin Ruda
Phone +49 202 6474-804, jruda@tecnicum.com

Agnes de Castro
Phone +49 202 6474 864, adecastro@tecnicum.com

Seminar topics	Wuppertal	Ulm	Wettenberg	Hamburg	Online	Inhouse
Law						
Machinery Directive 006/42/EC – CE conformity evaluation procedure	07.11.2024	on request	18.03.2024	on request	11.01.2024	on request
Legal aspects of machine safety for purchasers, designers, project coordinators **(half-day seminar)**	24.10.2024	on request	23.04.2024	on request	08.02.2024	on request
Basics of occupational health and safety for managers	04.06.2024	on request	22.03.2024	on request	02.09.2024	on request

Law	Wuppertal	Ulm	Wettenberg	Lübeck	Online	Inhouse
Legal aspects of machine safety for managers **(half-day seminar)**	27.02.2024	on request	on request	on request	20.09.2024	on request

(Continued on page 22)

Seminar program 2024 (continued from page 21)

Seminar topics	Wuppertal	Ulm	Wettenberg	Lübeck	Online	Inhouse
Standards – Regulations						
Risk assessment for infection prevention	Dates on request					
Risk assessment and operating instructions	21.02.2024	on request	19.03.2024	02.12.2024	07.10.2024	on request
Validation according to EN ISO 13849-2 **(half-day seminar)**	22.02.2024	on request	25.04.2024	03.12.2024	–	on request
Basics of the Ordinance on Industrial Safety and Health (BetrSichV)	13.06.2024	on request	20.03.2024	on request	25.11.2024	on request
Risk assessment for machinery and equipment	05.06.2024	on request	19.04.2024	on request	28.08.2024	on request
Technical documentation of machines and equipment	on request	on request	21.03.2024	on request	03.09.2024	on request
New construction, conversion, retrofitting – from manufacturer to owner/operator? **(half-day seminar)**	14.03.2024	on request	24.04.2024	on request	29.11.2024	on request

Standards – Regulations	Wuppertal	Ulm	Wettenberg	Hamburg	Lübeck	Inhouse
Application of EN ISO 13849-1 getting started with SISTEMA	19.06.2024	on request	11.09.2024	20.11.2024	12.03.2024	on request
Practical workshop Working with SISTEMA **(half-day seminar)**	20.06.2024	on request	12.09.2024	21.11.2024	13.03.2024	on request

Standards – Regulations	Wuppertal	Ulm	Wettenberg	Hamburg	Online	Inhouse
NEW Application of EN ISO 13849-1 getting started with SOFTEMA	29.02.2024	12.06.2024	04.12.2024	18.09.2024	–	on request

Standards – Regulations	Wuppertal	Kirkel	Wettenberg	Lübeck	Inhouse
Qualification as TÜV certified “Machinery CE Certified xpert® - mce.expert”	29.01.2024 bis 01.02.2024	08.04.2024 to 11.04.2024	02.12.2024 to 05.12.2024	on request	on request

Seminar program 2024 (continued from page 22)

Seminar topics	Wuppertal	Ulm	Wettenberg	Lübeck	Online	Inhouse
Application						
Basics of safety engineering – separating and non-parating protective devices	16.05.2024	on request	25.09.2024	on request	22.11.2024	on request
Electromagnetic compatibility EMC / EMEC in practice	Dates on request					
Safe fluid power – safe implementation of EN ISO 13849-1	Dates on request					
Fire protection in mechanical engineering	Dates on request					
Automated guided vehicles and their integration into the production environment	10.09.2024	on request	20.02.2024	on request	on request	on request
Safety in integrated robotic manufacturing plants	11.09.2024	on request	21.02.2024	on request	on request	on request
Human-robot collaborations	12.09.2024	on request	22.02.2024	on request	on request	on request
Application	**Wuppertal**	**Ulm**	**Wettenberg**	**Bremen**	**Online**	**Inhouse**
Explosion protection compact seminar	Dates on request					
Application	**Wuppertal**	**Ulm**	**Wettenberg**	**Lübeck**	**Online**	**Inhouse**
Safety-oriented design of battery production plants	09.09.2024	on request	19.02.2024	on request	on request	on request
Products	**Wuppertal**	**Ulm**	**Wettenberg**	**Bremen**	**Online**	**Inhouse**
Safety controller PSC1 **basic workshop**	on request	on request	11.06.2024	on request	on request	on request
Safety controller PSC1 **expert workshop**	on request	on request	12.06.2024	on request	on request	on request
Products	**Wuppertal**		**Mühldorf**		**Inhouse**	
Basics and inspection of opto-electronic protective devices according to BetrSichV **(seminar objective: Competent Person)**	24.04.2024		26.09.2024		on request	

Photos: K.A. Schmersal GmbH & Co. KG (shutterstock.com)

This brochure is printed on FSC® certified paper. The label on this product assures responsible stewardship of the earth's forests.

The greenhouse gas emissions generated in the production of this brochure were offset by investments in the project "LAYA energy efficient firewood stoves" in India.

Publisher:

tec.nicum

K.A. Schmersal GmbH & Co. KG

Möddinghofe 30
42279 Wuppertal

Phone: +49 202 6474-932
info@tecnicum.com
www.tecnicum.com