mrl.news

Issue 2024.02

tec.nicum

How to arm yourself against potential hazards

‘But where danger is there the saving powers will grow as well’ is a famous line from a poem by Friedrich Hölderlin, and could also serve as the motto of this edition of MRL News, running like a thread through the magazine.

For example, in our article on the EU‘s Cyber Resilience Act. It is quite clear that the risks to organisations from cyber attacks have increased considerably. The Cyber Resilience Act, which is expected to be adopted by the European Council in the autumn of 2024, seeks to boost the EU’s resilience to such attacks. Our article on page 16 outlines the new requirements and the obligations that organisations will have to meet.

The hazards posed by climate change are also undeniable, another area in which the EU intends to take action through the Green Deal. See the opposing page for information on Schmersal’s endeavours to reduce the carbon footprint along the value chain.

When it comes to greenhouse gas emissions, electric cars are a plus for climate protection. But the safety of machine is also essential in the production of lithium batteries for electromobility. On page 6, we report on how an international team of functional safety engineers from tec.nicum is helping a global battery manufacturer to meet the requirements of the EU Machinery Directive.

The considerable danger posed by fires is often underestimated. The key lies in prevention – a comprehensive fire protection concept is essential to any organisation. The guidelines and standards that need to be taken into consideration are detailed from page 9 onwards.

Averting potential hazards – this is also the topic of our article on page 14. Or, more specifically, how Artificial intelligence can be used for accident prevention.

The saving powers grow! So, in this sense, remain optimistic!

Happy reading!

The editorial team

En route to more sustainable safety switchgear

Schmersal researches ways to reduce carbon footprint

The EU Commission has presented a proposal for a new Ecodesign for Sustainable Products Regulation (ESPR), which is to become a central element of the European Green Deal. Schmersal is also already en route to sustainability.

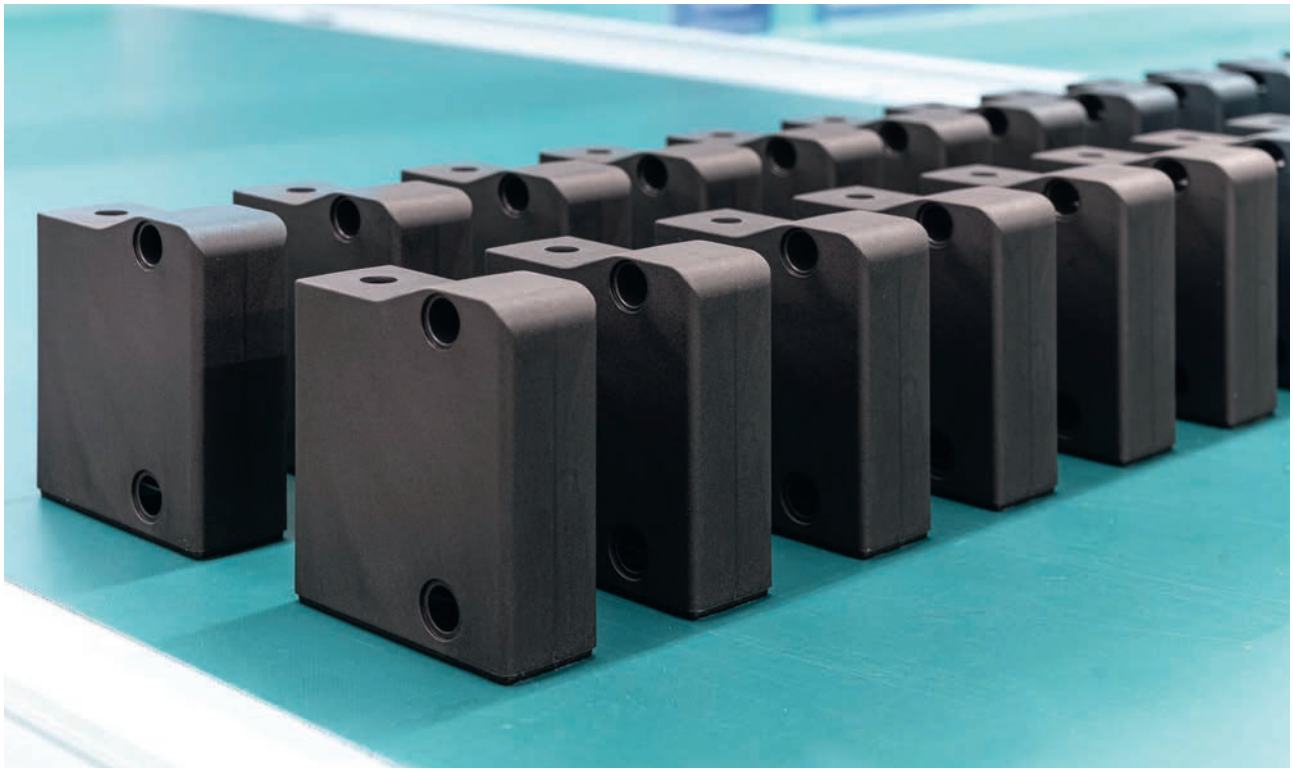
And has set itself the goal of not only supporting customers in the introduction of future technologies as part of the digital transformation, but of reducing the carbon footprint along the value chain as well. For this, the company is starting at the beginning – with the material that most safety switchgear is made of: plastic.

The biggest challenge with machinery safety products is ensuring that new, environmentally-responsible solutions in product design or material usage do not impair the quality and, in particular, the safety functionality of the safety switchgear. Optimised devices must also comply with the standards, plus their suitability needs to be checked and confirmed by certification.

Schmersal has long worked with universities and research institutions in order to chalk up progress in this field, including with Kunststoff-Institut Luedenscheid (Lüdenscheid Plastics Institute), with whom Schmersal is currently working on an extremely promising project. The project is considering the use of recycled material in the production of safety switchgear featuring a plastic enclosure. ‘Our goal is to use twenty per cent regranulate in the switches manufactured using the injection moulding process,’ explains Matthias Banaszek, Manager Value Engineering & Expert in Plastics at Schmersal. ‘So over the past two years, we have collected around 30 tonnes of material from production waste, including sprues and start-up residues, i.e. unsuitable initial components that are produced when a new production batch is started.’

According to the UL organisation, which awards globally recognised safety marks, a regranulate content of 25 per cent can be attained in safety switches. ‘This is permitted if you prepare it yourself. With this in mind, Abdel El Makrini, head of production for plastic components, and Matthias Banaszek are currently examining the possibility of acquiring their own centralised mill and establishing space and infrastructure for its operation. The plans are due to be finalised soon so that implementation can commence.

The TÜV can also certify safety switches containing recycled content, provided that there is a way to prove that the recycled material used has no impact on the →



Schmersal has set itself the goal of using 20 per cent recycled granulate in its injection-moulded switches.

Many Schmersal switches are manufactured using the injection moulding process.

quality of the safety functions. To this end, the Plastics Institute is undertaking a comparative test with switches from Schmersal involving an analysis of switches made purely from virgin material against switches consisting of 80 per cent virgin material and 20 per cent regranulate.

The analysis takes in a number of parameters using standardised test methods, such as the Charpy impact strength test in accordance with EN ISO 179-1, which is used to characterise a plastic at high elongation rates or density measurement in accordance with EN ISO 1183-1 and the IEC 60093 test method for contact resistance to describe electrical insulation behaviour. The aim of the tests is to evidence that the switches made of mixed material can withstand adverse environmental impacts as well as those made of solely virgin material.

'Really, we can calculate this in advance with quite high precision, but of course we need to carry out testing to furnish the evidence,' explains Banaszek.

If the results of the comparative tests from the Plastics Institute are available and meet expectations, that is there are no quality impairments due to the use of mixed material, the next step will be to have the TÜV certify them. This would clear the way for series production of switches containing regranulate content. This would make Schmersal the first manufacturer to use recycled material in the production of safety switches.

Poly4Nature – plastics from alternative raw materials

Another environmental project is also underway through the Lüdenscheid Plastics Institute, if indirectly: Schmersal has joined the German innovation network Poly4Nature as an active partner. A network funded by the Federal Ministry for Economic Affairs and Climate Protection and managed by the Lüdenscheid Plastics Institute, the goal of Poly4Nature is to produce plastics from alternative raw materials and using alternative processes, such as with natural fibres or primary products from natural materials or waste streams. These materials will replace previously used fossil materials in order to reduce or even neutralise CO_2 emissions as, after all, the components used in the production of plastics are carbon compounds from crude oil and natural gas. The extraction and transport of fossil fuels, such as crude oil and natural gas, and the production of plastics release considerable volumes of harmful CO_2.

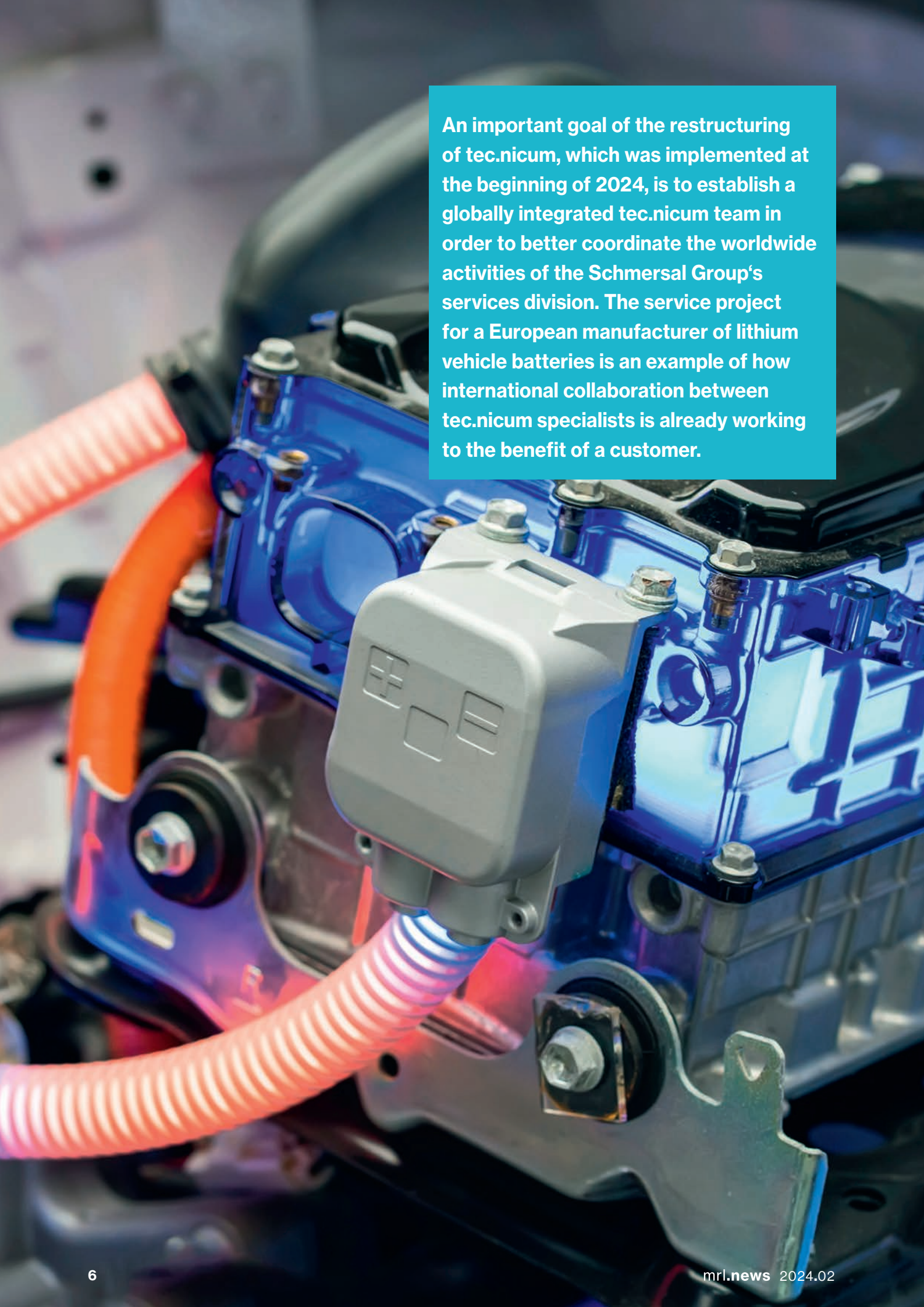
As a network partner, Schmersal has agreed a specific project with Poly4Nature to develop biodegradable protective plugs based on alternative raw materials. These plugs will be used to cover screws and screw holes and are currently used in their hundreds of thousands at Schmersal, solely for the transport of Schmersal switches. When the user takes the switch from the transport packaging, the plugs are thrown away. →

‘These protective plugs are not safety-related components so alternative materials are much easier to use in this case,’ explains Matthias Banaszek. ‘I can also imagine natural polymers being used for all sorts of other packaging materials and components, such as for accessories like slotted covers, screw plugs or the transport locks that we use for our AZM40 solenoid interlocks.’

The alternative plastics for these packaging materials could, for example, be of marine origin, such as algae. Poly4Nature also foresees ‘the use of renewable carbon from pyrolysis processes, lignin-based material systems, natural fibres or primary products made from natural material or waste streams (side streams)’ as future possibilities. ‘These materials should not only replace previously used fossil materials, but also give products new functionality, depending on characteristics profiles, or at offer carbon reduction or neutrality at a minimum.’ Also important however, is that ‘in contrast to previously known materials, new value chains of natural origin are discussed that do not compete with agricultural land and the food-processing industry.’

Whether or not protective plugs will actually be made of algae in the future remains to be seen. The project is set to continue until early 2026, but thus far at least, there has been a start. ■

Protective plugs are used to cover screws and are to be made from alternative plastics in future.



An important goal of the restructuring of tec.nicum, which was implemented at the beginning of 2024, is to establish a globally integrated tec.nicum team in order to better coordinate the worldwide activities of the Schmersal Group's services division. The service project for a European manufacturer of lithium vehicle batteries is an example of how international collaboration between tec.nicum specialists is already working to the benefit of a customer.

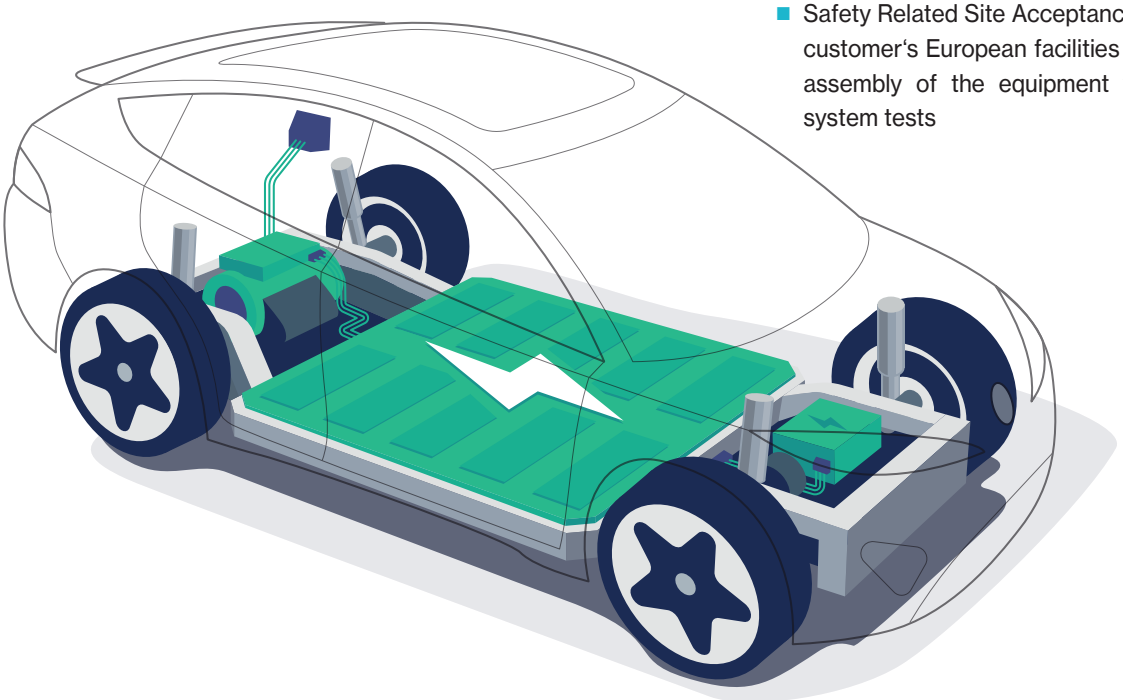
Cooperation across four continents

In a major international project, a customer benefits from tec.nicum‘s global network

The global market for lithium-ion batteries is booming: according to a study, sales are set to grow by around eleven per cent annually until 2027. The main drivers are the automotive industry with its electric cars on the one hand and the electronics industry on the other. Global battery production is dominated by a few countries, above all China. However, the production of lithium batteries is now increasingly shifting to Europe. So it is no wonder that contact with a new tec.nicum customer – a European manufacturer of lithium-ion batteries for electromobility – was established via a project in China: In 2023, tec.nicum carried out risk assessments for a machine supplier based in China.

tec.nicum has signed an umbrella agreement with the new customer, effective from January 2024, to provide consultancy services to its suppliers who manufacture battery production machines in China, Japan and South Korea and export them to Europe. Companies from these Asian continue to be among the leading manufacturers of battery production machines. However, they will have to prove that their machines meet the requirements of the European Machinery Directive (MD) and are CE compliant.

Since 2024, tec.nicum is the exclusive provider of consulting services for CE conformity for all non-European machine suppliers of the battery manufacturer. This means that tec.nicum is responsible for ensuring that all suppliers working for and supplying machines to the European customer comply with the EU Machinery Directive.



This enables the European battery manufacturer to efficiently implement the safety requirements of the MRL and CE labelling with a central coordination for all local sites of its non-European machine suppliers. And the battery manufacturer also benefits from tec.nicum‘s global network: tec.nicum teams from Germany, Sweden, Brazil, China, South Korea – where Schmersal will soon open a subsidiary – and India and India are involved in the project. A tec.nicum team from Schmersal North America is also involved, as a new battery factory is currently being built in Canada, which will be supplied by machine builders from Europe, China and South Korea.

The tec.nicum services for the tec.nicum customer‘s partner companies in Asia and Canada are provided in five phases:

- Training of the partner companies with regard to the requirements of the European Machinery Directive, the standards and the requirements of the customer's GTS (General Technical Specifications)
- Review of existing documentation, preparation of a gap report (comparison of the current status with the target status)
- Provision of engineering services to support the correction of identified gaps and the drafting of other required documents
- Safety Related Factory Acceptance Test (SR-FAT), validating the manufacture of the equipment by testing the safety systems and physical verification of their CE conformity at the manufacturers‘ production plants in China, South Korea and Japan
- Safety Related Site Acceptance Test (SR-SAT) at the customer‘s European facilities to validate the correct assembly of the equipment with additional safety system tests →

The service packages offered by tec.nicum to the Asian machine suppliers also include compliance testing for various EU directives.

These include:

- Base Package (Machinery Directive (MD) 2006/42/EC and General safety and health requirements (EHSR))
- ATEX (Directive 1999/92/EC and Directive 2014/34/EU)
- Hazardous Chemicals (ROHS and REACH)
- Pressure Equipment Directive (PED)
- Safety of machinery – Laser processing machines (EN ISO 11553)
- Electromagnetic Compatibility (EMC)
- specific standards related to the use and safety of hydraulic systems in machinery
- Integrated Machine Systems (IMS) EN ISO 11161

The tec.nicum teams can carry out some of the consulting services digitally. However, the tests and documentation are mainly carried out on site at the supplier‘s premises. This requires good communication with the supplier in the local language (mainly Chinese, but also Korean) and in English. This is easily guaranteed by native-speaking members of the tec.nicum teams at the various Asian tec.nicum locations.

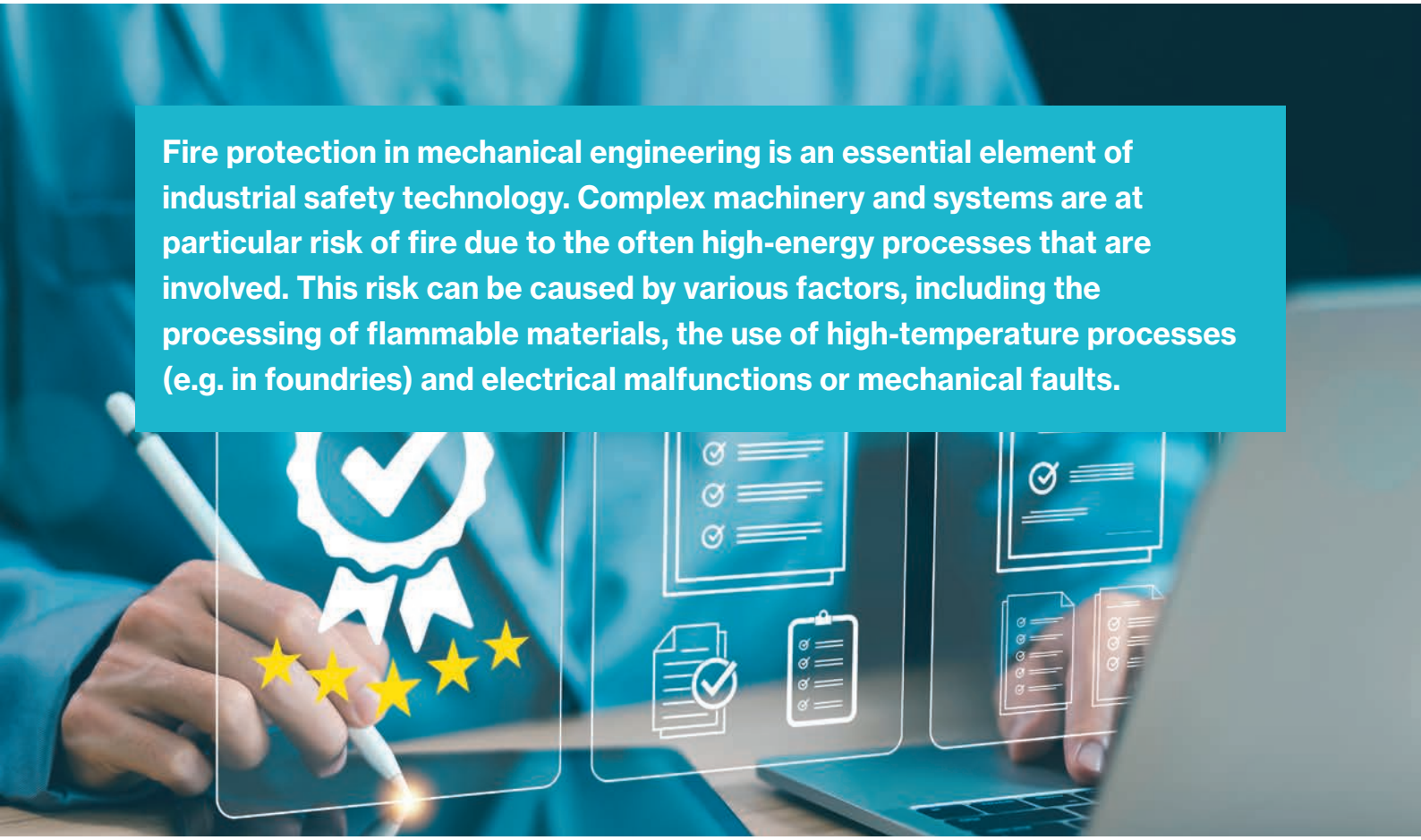
Another requirement of the tec.nicum customer – that the tec.nicum team should have a high level of technical expertise in order to understand the functions of the existing machines and their documentation – can also be easily met. The experts at tec.nicum have many years of experience in implementing technical projects in a wide range of industries. They are also experts certified by TÜV Rheinland, e.g. as Functional Safety Engineers – Machinery or IECEx-certified specialists.

Overall, the project is a mammoth task due to the large number of machines and locations as well as the services to be provided. For the tasks in phase 1 alone, 100 working hours are estimated for a medium complex machine.

And that is why there is another essential requirement for everyone involved: ‘We all need a great deal of patience.’

Leading members of the international tec.nicum team for the battery production project:

- Bruno Diniz
  (tec.nicum Global Director)
- Leo Schytt
  (Managing Director – Schmersal Nordiska)
- Michele Seassaro
  (Managing Director – Schmersal China)
- Gary Ferguson
  (Managing Director – Schmersal North America)
- Sagar Bhosale
  (Managing Director – Schmersal India)
- Tetsuya Horimoto
  (Managing Director – Schmersal Japan)
- Uwe Seeger
  (Director Middle East, Asia & Pacific – Schmersal South Korea)
- Enildo dos Santos
  (Business Development Manager – tec.nicum Europe)
- Carsten Doll
  (Site Manager – tec.nicum Germany)
- Girish Alawe
  (General Manager - tec.nicum Asia)
- Devin Murray
  (Manager – tec.nicum North America) ■



Fire protection in mechanical engineering is an essential element of industrial safety technology. Complex machinery and systems are at particular risk of fire due to the often high-energy processes that are involved. This risk can be caused by various factors, including the processing of flammable materials, the use of high-temperature processes (e.g. in foundries) and electrical malfunctions or mechanical faults.

Preventing fire damage and production losses

Fire protection in mechanical engineering – normative requirements and practical examples

In addition to preventing employee injury, fire protection also puts operational continuity and protecting manufactured products front and centre. Production losses due to fire damage can cause considerable economic loss and hamper business continuity.

According to the DGUV, around 3500 occupational accidents with fires and explosions as their cause have been reported to the accident insurance institutions in Germany in recent years. A tragic example illustrates the urgency of effective fire protection measures:

> On 6 February 2023, auto supplier Burgmaier in Allmendingen suffered damage totalling around 200 million euros when a major fire broke out and destroyed the entire factory building after a tank containing 50,000 litres of hydraulic oil caught fire. The result was devastating, with five injured, damage in the hundreds of millions of euros, around 250 people ultimately without a job and a company with no headquarters.

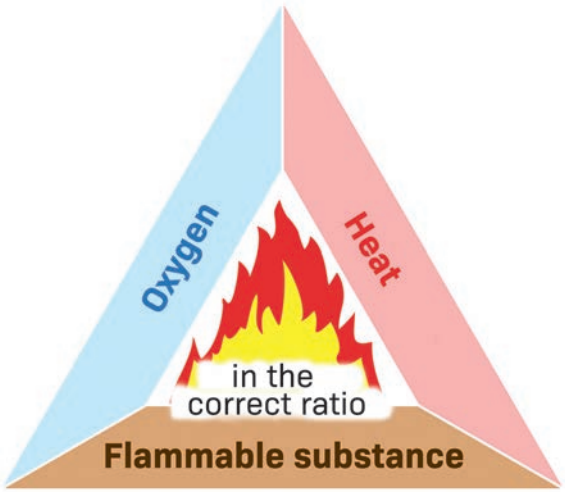
A comprehensive fire protection concept is thus essential to ensuring both the safety of employees and the integrity of production processes.

Development and persistence of a fire – the fire tetrahedron

The fire tetrahedron is an extended model of the traditional fire triangle and describes the four essential elements that are needed for a fire to develop and persist. Understanding the fire tetrahedron is key to developing effective fire prevention and extinguishing strategies, as it shows that eliminating or disrupting one of the four elements is enough for a fire to be extinguished.

These four elements are:

- Fuel: Any flammable substance consumed in a fire, whether solid, liquid or gas. Examples include wood, paper, petrol and methane.
- Oxygen: A fire requires oxygen for combustion. This usually comes from the air, which is made up of around 21 per cent oxygen.
- Heat: A sufficient quantity of heat is required to elevate the fuel to its ignition temperature and maintain combustion.
- Chemical reaction: The exothermic chemical reaction that occurs between fuel and oxygen and that emits heat and light. →



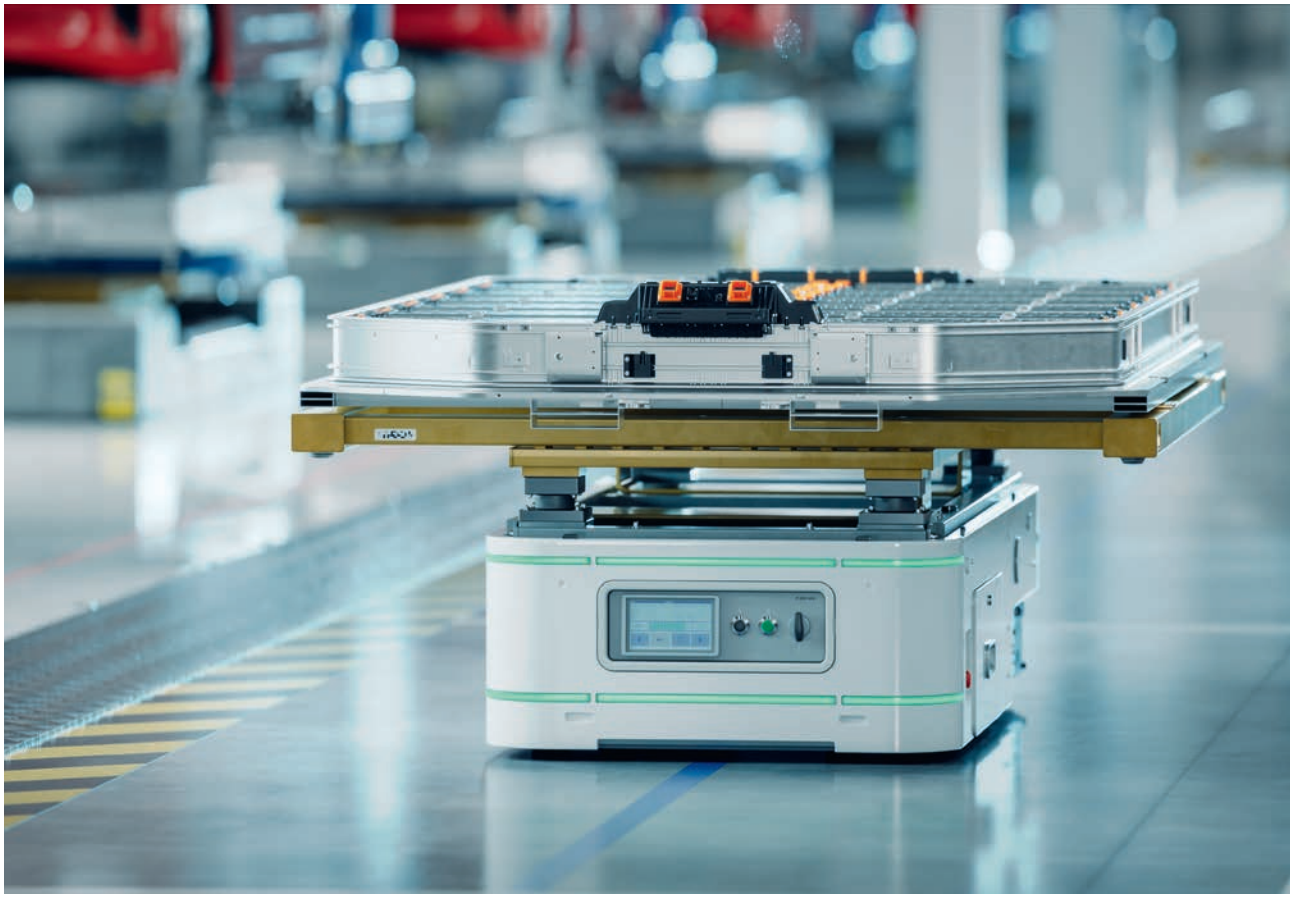
Directives and standards

The basic health and safety requirements are provided in the applicable Machinery Directive 2006/42/EC, whose stipulations include the consideration of fire and explosion hazards as early as the design phase of (stationary) machinery. The requirements are not overly specific and do not give the designer any specific measures for implementation:

'Machinery must be designed and constructed such as to avoid any risk of fire or overheating arising from the machinery itself or from gases, liquids, dusts, vapours or other substances released by or used by the machinery' These basic health and safety requirements are specified in more detail in harmonised standards. ISO 19353 'Safety of machinery – fire prevention and fire protection' is the core standard for fire protection requirements in mechanical engineering and deals comprehensively with the fire prevention and protection of machinery. The goal of the standard is to minimise the fire hazards posed by a piece of machinery to an acceptable level. To do this, the standard specifies methods that are used to identify fire hazards and to carry out risk assessments. It also defines basic concepts and methods for fire protection measures.

In addition, more in-depth research into standards for the machinery pending assessment is essential in each individual case. Where available, any machinery-specific C standard may contain requirements for machinery-related fire protection that are not taken into consideration in the less detailed 'basic safety standards' (type B standards).

In addition to the obligation of the manufacturer to consider fire protection in the design, the machinery operator is also subject to certain requirements. The German Industrial Safety and Health Regulation obligates employers to carry out risk assessments and to implement suitable protective measures to ensure the health and safety of employees. These include specific fire protection measures. →



ISO 19353 – core standard for fire protection requirements in mechanical engineering

ISO 19353 provides the machinery manufacturer with methods for identifying, determining and evaluating risk, and measures for minimising it. It is very important to pay attention to the standard's scope of application: it applies only to stationary machinery and not to mobile machinery, machinery for controlled combustion processes, machinery for use in potentially explosive areas and fire detection and extinguishing systems as part of fire protection systems for buildings.

The key aspects include:

1. Identification of fire hazards:

a. Analysis of potential sources of fire:
   This includes identifying internal and external factors that could cause fires, such as electrical components, mechanical friction and flammable materials.
b. Determination of the causes of fires:
   The standard requires a detailed investigation of the possible causes that could give rise to a fire, including short-circuits, overheating and sparking.
c. Evaluation of the risks of fire:
   The risk assessment is carried out by estimating the likelihood and potential extent of the damage caused by a fire. This requires a systematic and methodical approach to the qualitative and quantitative evaluation of the risks.
d. Documentation of the results:
   All identified risks and evaluations must undergo complete documentation in order to ensure transparent tracing and future review.

2. Risk reduction:

a. Inherently safe design measures:
   These include the use of materials of low flammability and minimising the use of combustible liquids and lubricants.
b. Technical protective measures:
   These include the encapsulation of hazardous components or extraction (e.g. of smoke, heat) as well as measures to guard against the escape of flames from production-related openings (e.g. door gaps, workpiece feed).

The risk minimisation process follows the iterative three-stage procedure outlined in ISO 12100. If inherently safe design measures and technical protective measures are insufficient to minimise the risk of fire, additional protective measures must be provided (e.g. an EMERGENCY STOP in accordance with ISO 13850, connections for the supply of extinguishing agents, etc.). Integral fire detection and extinguishing systems are preferred in any event. →

The ultimate solution concept or the selection of suitable fire protection equipment depends on the defined risk level and ranges from automatic warning and fire alarms to permanent, manually operated or automatic extinguishing equipment. In the latter case, suitable extinguishing agents must be defined in accordance with the four fire classes A, B, C and D in accordance with ISO 3941.

Practical example: Fire protection on stationary grinding machinery in accordance with ISO 16089

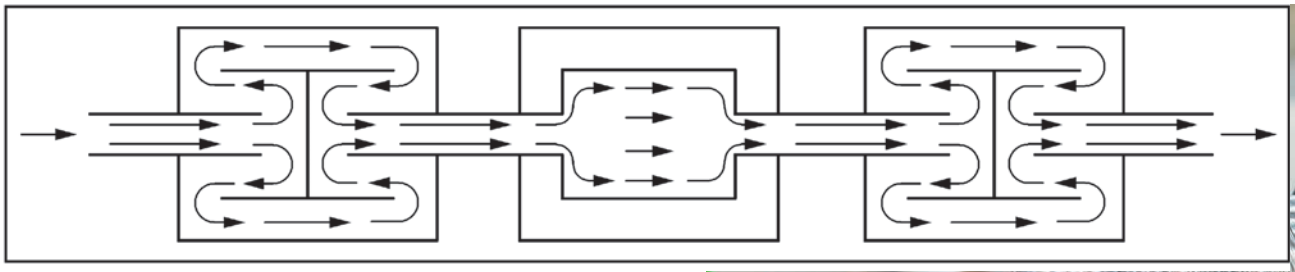
ISO 16089 specifies safety requirements for stationary grinding machinery. It also covers fire protection, which is supplemented by implementation of the requirements of ISO 19353. A stationary grinding machine is used to illustrate how these requirements and the fire protection measures are implemented.

The first stage is to perform a detailed risk assessment to identify the potential hazards of fire. In the case of grinding machinery, there is a high likelihood of sparking during the grinding process. Other sources of hazards include the development of heat due to friction, the accumulation of combustible grinding dust and the use of combustible cooling lubricants.

Specific technical protective measures can then be defined on the basis of previously identified hazards.

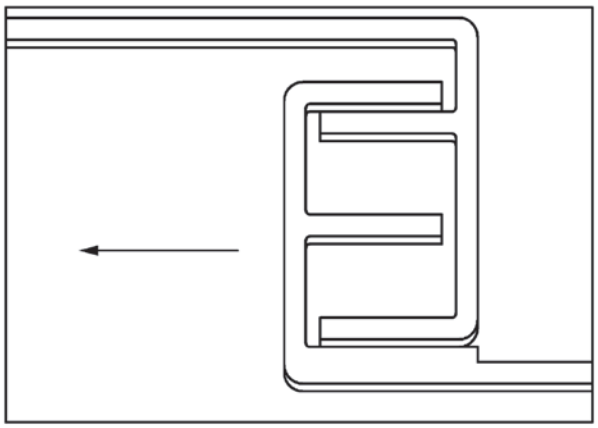
Automatic spark extinguishing systems (preventive fire protection) are a central element and are designed to detect and extinguish sparks the moment that they occur. Automatic spark detectors, which are integrated into the extraction systems on the grinding machine itself, detect sparks and activate water or gas extinguishing nozzles to suffocate the spark with a fine water mist or extinguishing gas.

Dust extraction is also determinative at the same time. Effective extraction devices eliminate combustible grinding dust from the work area. Flame arrestors should also be fitted to ensure that flames are unable to penetrate the extraction ducts and thus prevent flames from spreading through the ducts. In addition, 'slowdown' sections should also be integrated into the extraction ducts to cool hot particles and to extinguish sparks before they can pose a hazard. →



Flame arrester (from ISO 16089)

Also important are flameproof labyrinth seals, which prevent flames from escaping from the machine.



Labyrinth seal (from ISO 16089)

These seals can be fitted to the guards or maintenance flaps on the machine and feature a labyrinth design that reverses the direction of the flames multiple times in order to suffocate them.

ISO 16089 also outlines the hazards posed by flammable cooling lubricants. Cooling lubricants with an oil content that exceeds 15 per cent can pose a risk of fire or low-pressure explosion. Wherever possible, cooling lubricants with low evaporation losses and high flash points should have high viscosity, though the choice should always take the requirements of the machining process into consideration.

The systematic identification of fire hazards, the careful selection and implementation of suitable technical protective measures and regular maintenance and inspection of these systems can help to minimise fire hazards on stationary grinding machinery and ensure the safety of operators. ■

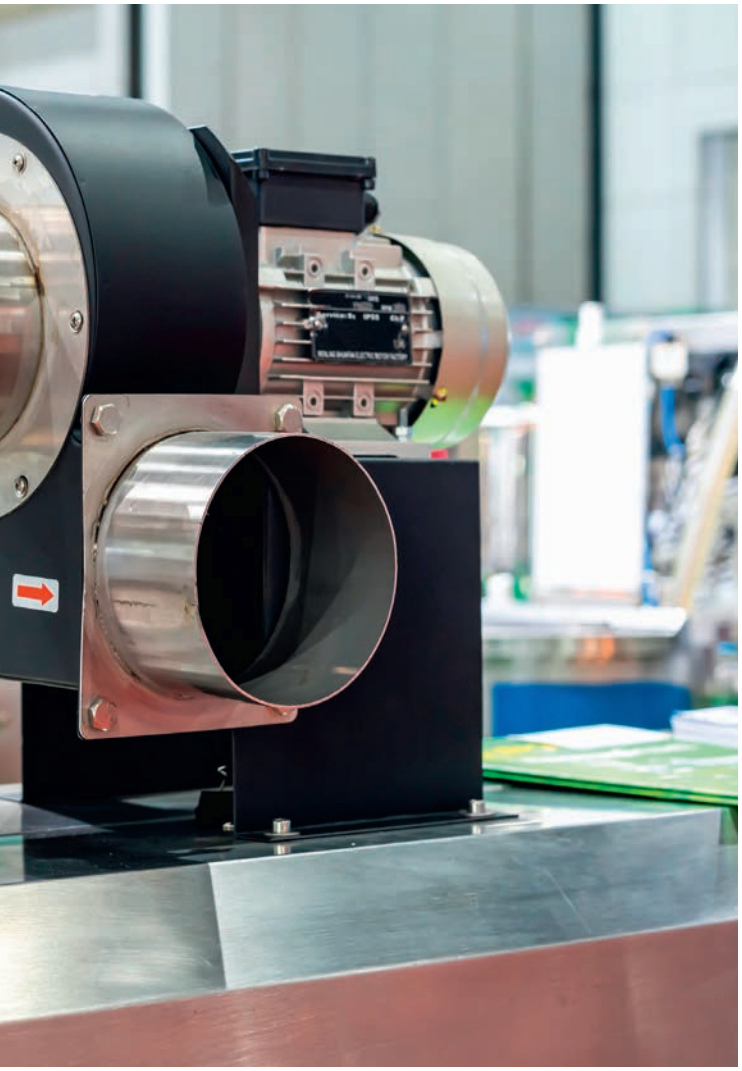
Tristan Willigsecker
Electrical Engineer, Safety Consultant/
tec.nicum

Conclusion:

Fire protection in mechanical engineering requires an integrated approach and implementation of specific measures based on a substantiated risk assessment.

The risk of fire can be significantly reduced by adhering to standardised requirements, most notably ISO 19353, and by combining technical and supplementary protective measures.

The example provided illustrates the importance of careful planning and consistent implementation of fire protection measures in not only meeting the legal requirements, but in increasing operational safety and efficiency as well.



Seminars from the tec.nicum academy

The tec.nicum academy offers the ‘Fire protection in mechanical engineering’ seminar and the compact ‘Explosion protection’ seminar. Dates will be communicated on request.

Dates will be communicated on request.

Contact person:
Melanie Peters-Schuster
Tel. +49 202 6474 864
info-de@tecnicum.com

Artificial Intelligence (AI) is seen as a pioneering technology that is helping to advance automation in industry by enabling analysis of large volumes of data. AI is also opening up new opportunities and possibilities for the safety of machinery and occupational health and safety: tec.nicum also offers AI-based visual safety monitoring systems as part of its new 'digitalisation' module.

Preventing potential hazards
Artificial Intelligence for accident prevention

As part of the expansion of its service offering, tec.nicum has now incorporated 'digitalisation' as an important new element in its range. The new digitalisation range consists of three areas:

- **IIoT solutions/Schmersal Cloud Solution**
  This is a collection of software modules that are used for the capture, storage, analysis, control and visualisation of safety and process data. The area includes solutions for safety and condition monitoring, predictive maintenance as well as software solutions for energy and KPI monitoring.
- **tec.dloto – digital Lockout–Tagout**
  The software offers supportive, digital monitoring of Lockout–Tagout, which prevents occupational accidents by temporarily disconnecting machinery fully from its sources of energy.
- **Computational vision solutions**
  A modular system of video analysis solutions that integrates information from various areas of industry into a single environment. It is capable of measuring images, performance indicators, availability, quality and, most importantly, the safety of people and systems. It includes the 'Artificial Intelligence to Reduce Accidents' (AI.RA) video analysis system.

Visual safety monitoring with intelligent data processing

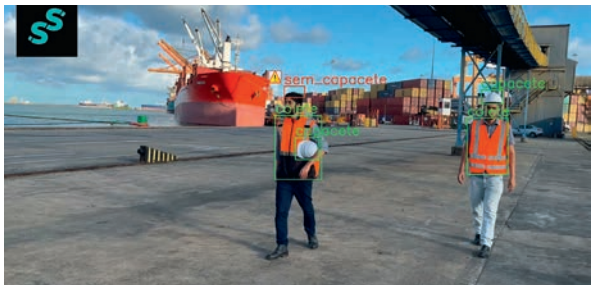
The **tec.iara Artificial Intelligence to Reduce Accidents** video analysis system is AI-based, visual safety monitoring that can recognise the risks of accident in real time by having the system observe the interaction between people, objects and the working environment. The integration of AI has significantly modified the way in which monitoring cameras work. With the support of machine learning and advanced algorithms, AI-supported systems can not only record static images and videos, but perform complex analyses as well. With their capability of processing data intelligently, they are not only able to store recordings, but to automatically recognise and respond to previously learned events.

As an example, they can identify whether or not an employee is about to enter a hazardous area and respond by triggering an alarm signal, if necessary. In addition, the system can also detect the proximity of an employee to a hazardous object and check and assess the proximity and inclination of suspended loads. It can also identify whether employees are wearing prescribed personal protective equipment, such as helmets, goggles, gloves or safety shoes.

With this form of operation, the system enables proactive safety monitoring and immediate notification of responsible parties in the event of risky activities, so that incidents like falls and accidents can be avoided. The system also allows verification of adherence to prescribed safe routes within spaces such as production halls and outdoors.

The capability of the AI-based visual monitoring system to promptly identify threats or unusual activities and to then analyse them in real time allows potential hazards to be proactively averted or, at the very least, allows for a prompt response. →

Hybrid architecture



The tec.iara video analysis system is based on a hybrid architecture that makes use of both cloud and on-premise servers.

With the latter, algorithms can be executed locally, which not only leads to high processing efficiency, but to a high level of data security as well. Cloud servers are only used to host dashboards and processed data, ensuring that all sensitive data (such as images) remain within the organisation.

No special network is required to operate the tec.iara system. Rather, a standard CCTV network is used to capture and transmit the image data, as with conventional video monitoring.

Other computational vision solutions – tec.saci and tec.cuca

Other computational vision solutions offered by tec.nicum include tec.saci, a system for analysing behaviour and interaction, and tec.cuca (Unified Characteristics Classifier). These video analysis solutions require an IP camera image capture system. Existing devices can also be used. Data can be processed on premise or in the cloud, with reports provided via a customised dashboard platform.

tec.saci – behaviour and interaction analysis system

Video analysis system to identify human actions in production areas and production halls with the ability to:

- Perform real-time chronoanalysis
- Identify all human activities within a defined area, separated according to job profile
- Evaluate compliance with routines, checklists and setup standards
- Identify usage patterns and device defects
- Analyse and standardise execution and performance
- Identify bottlenecks and areas of inefficiency

tec.cuca – Unified Characteristics Classifier

tec.cuca is a system that is able to recognise quality standards and collect information, including:

- Sizes and dimensions
- Quantities and losses
- Visual errors
- Conformity analyses (e.g. holes)
- The causes and effect of problems to enable immediate solutions
- Trend analysis

Labour and data protection aspects

There's no doubt that visual monitoring systems offer a significant boost to safety and occupational health and safety for employees. At the same time, it is important that systems are carefully planned, with employee involvement from an early stage, because systems will not only be monitoring occupational health and safety, but performance and behaviour as well. Consideration must also be given to data protection. Aspects of labour and data protection legislation should be discussed and clarified with responsible departments and employees well in advance of implementation. Doing this also helps to boost acceptance of AI systems amongst employees. ■

Volker Heinzer
Product Manager for Programmable Electronic Systems and Industry 4.0/IIoT,
Schmersal Group

The goal is as obvious as it is welcome – to boost the resilience of companies across the EU in the fight against cyber attacks on digital products and systems. With this in mind, the European Parliament passed the Cyber Resilience Act in March 2024. Its ascent means that manufacturers of components and machinery, as well as operating companies, will have to meet new requirements and obligations. This article looks at what these are and what questions remain unanswered.

Cyber resilience in mechanical engineering

The EU's Cyber Resilience Act introduces new obligations for machinery manufacturers and operating companies

No one at Schmersal is in any doubt about the importance of cyber security following the cyber attack on the Group in May 2020. The aim of cyber attacks is less about gaining access to data and information from the production process, but more about the integrity and availability of production processes.

The functional safety of machinery and systems is particularly vulnerable as safety systems need to transition machinery to a safe state even in the event of minor impairments, i.e. the machine needs to be shut down. No surprise then that the economic impact of such cyber attacks is so severe.

The Cyber Resilience Act (CRA), which is expected to be adopted by the European Council in the autumn of 2024, seeks to boost the EU's resilience to cyber attacks on digital processes, systems and products (hardware and software). The new regulation is likely to come into effect in the autumn of 2027 and will then have direct application in all Member States. It will apply to all products containing digital elements that are able to communicate with other products. This means that industry is particularly affected by networked production in the Industrial Internet of Things (IIOT): devices, machinery and components used for production capture and generate data using sensors and actuators and exchange those data.

Manufacturer obligations

The CRA obligates manufacturers to develop and manufacture products in accordance with the basic requirements of Annex I to the Regulation.

These requirements include (Annex 1/Part 1):

- The product may only be placed on the market without known vulnerabilities
- Secure default settings
- Provision of security updates
- Protection against unauthorised access
- A design incorporating 'security by design'

The requirements also mandate the creation of technical documentation for hardware and software and stipulate a duty of care in the integration of components obtained from third parties. This also applies to software modules that are integrated into components or machinery.

In addition, manufacturers are obligated to provide ongoing vulnerability management and to ensure that security breaches are closed throughout the product's lifecycle, or five years at a minimum. They must also provide updates for a minimum of ten years.

Vulnerability management includes (Annex 1/Part 2):

- Reporting, rectification and documentation of vulnerabilities
- Creation of an SBOM (software version history documentation)
- Regular cyber security checks
- Reporting obligations to EU agencies ENISA and CSIRT

Reporting obligations in the event of security breaches

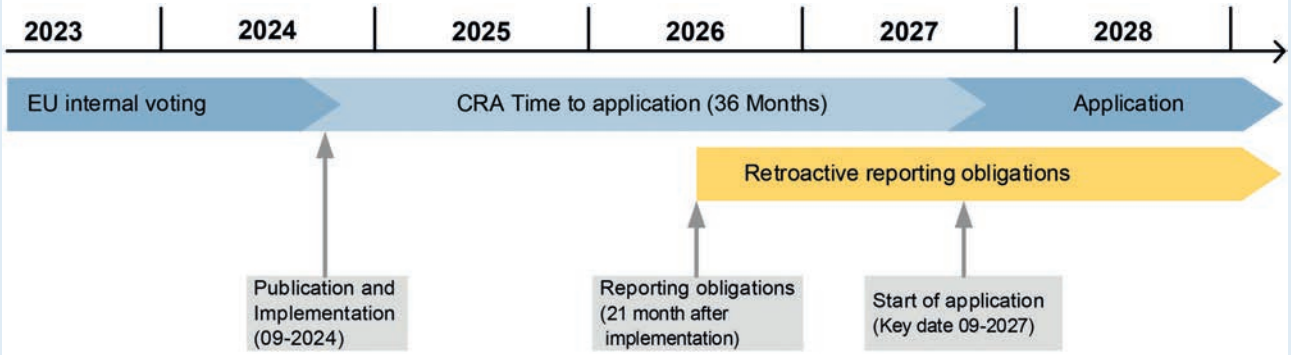
To allow users to close security breaches as promptly as possible, such as with software updates, users and the European Union Agency for Cybersecurity (ENISA) must be informed whenever an actively exploitable vulnerability becomes known.

The manufacturer's reporting obligations include (Article 14):

- Notification on becoming aware of any actively exploited security vulnerability or incident to ENISA and CSIRT
- Notification, including information and rectification measures within 72 hours
- Final report of exploited security vulnerabilities and incidents
- Description, level of severity and impacts of the attack
- Potential causes and actors, security updates
- Provision of rectification measures for affected users

The reporting obligation will enter into effect 21 months after publication of the CRA Regulation. →

Cyber Resilience Act (CRA): Roadmap



Security level defines resistance to different threat potentials

The normative requirements for cyber security are laid down in IEC 62443, which defines protection targets and security levels as well as procedures for realising cyber security requirements for industrial automation systems. The standard evaluates technical requirements for systems (IEC 62443-3-3) and products (IEC 62443-4-2) using 'security levels' (SL). The different levels indicate the level of resistance to potential attackers with different knowledge and resources.

IEC 62443 defines four security levels:

Security Level 1 (SL1)
Ensures prevention of unauthorised disclosure of information through eavesdropping or accidental detection

Security Level 2 (SL2)
Ensures prevention of unauthorised disclosure of information to a person or body actively seeking it with straightforward means involving little effort, general skills and motivation

Security Level 3 (SL3)
Ensures prevention of unauthorised disclosure of information to a person or body actively seeking it with sophisticated means and moderate effort, IACS-specific skills and average motivation

Security Level 4 (SL4)
Ensures prevention of unauthorised disclosure of information to a person or body actively seeking it with sophisticated means and considerable effort, IACS-specific skills and high motivation

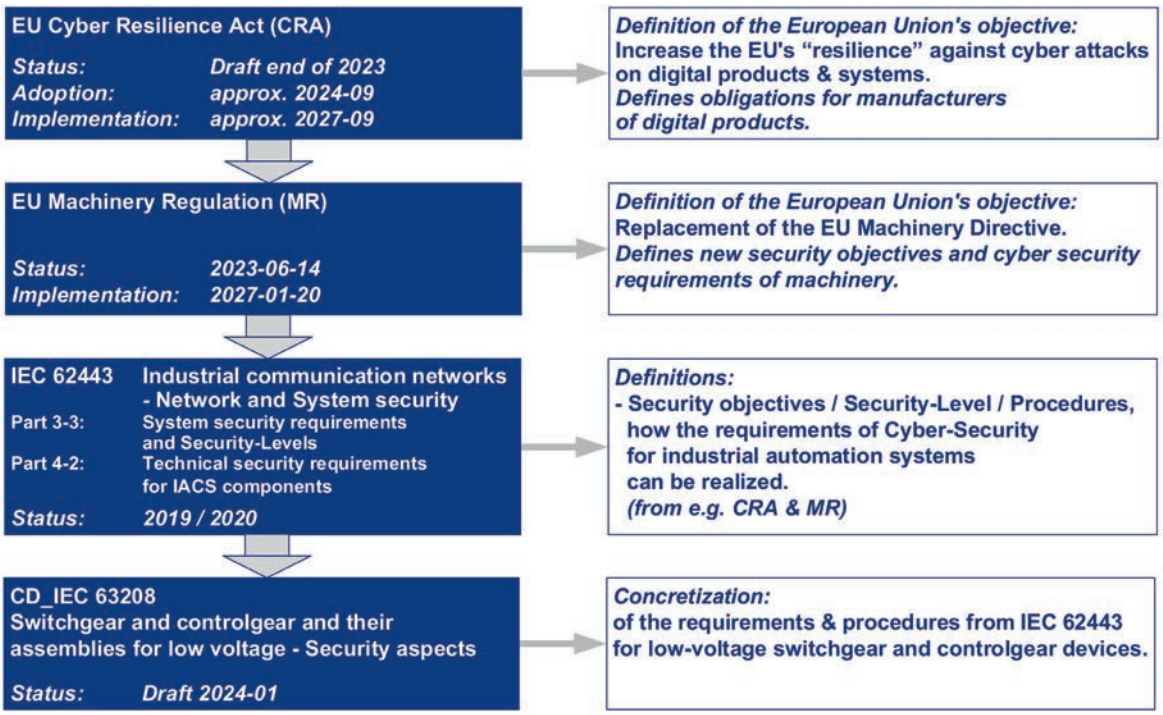
Manufacturers of components and machinery must assess which security level or security properties a component or machine requires in order to remain resilient to the identified potential attacks.

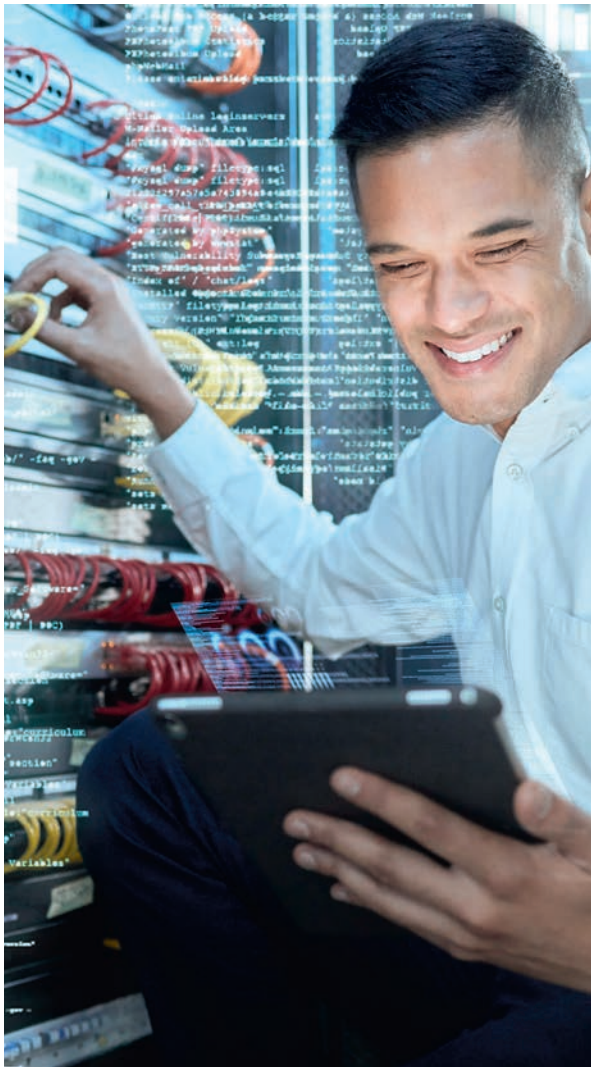
Using this risk assessment, suitable control mechanisms must then be implemented in order to guard against unauthorised access. Such measures can include authentication, identity or access management systems to protect the integrity of stored, transmitted or otherwise processed data, whether personal or otherwise, commands, programmes and configurations against manipulation.

This makes IEC 62443 a suitable guide for machinery manufacturers and operating companies when it comes to effectively implementing cyber security.

The Cyber Resilience Act does, however, pose a number of yet unresolved questions and issues. According to a statement by the German Chamber of Industry and Commerce (DIHK): 'The CRA can only fulfil its true potential if it imposes requirements that not only serve the intended purpose, but that are also appropriate and →

EU Cyber Resilience Act (CRA), EU-Machinery Regulation (MR) and Standards (IEC)





practicable. Organisations must review their internal measures for CRA compliance or establish new processes and implement a mechanism for handling vulnerabilities. This will require guidance by European standards, many of which are still to be developed. Organisations also report that they are unable to recruit the skilled labour that they need. This applies equally to establishing organisational structures and employees for market monitoring. It would, in this regard, be advisable to extend the transition period, additionally not to further exacerbate the already existing lack of skilled labour.' ■

Udo Weber
Product Manager for Safety Technology at the Schmersal Group and member of the DIN joint committee – safety principles – control systems

Lockout–Tagout–Tryout (LOTOTO)

Getting the implementation right!

Lockout–Tagout prevents occupational accidents by temporarily but fully disconnecting machinery from its sources of energy. Before maintenance work can be carried out on machinery or systems, devices must de-energised and secured against being reactivated by unauthorised persons (Lockout) so that they can no longer pose a hazard. In addition, machinery that has been switched off must be clearly labelled (Tagout).

In recent years, ever more companies have introduced Lockout–Tagout processes or provided appropriate tools. The concept of Lockout–Tagout does not, however, appear in Machinery Directive 2006/42/EC or in the new Machinery Regulation (EC) 2023/1230. It is not referenced in the German Industrial Safety and Health Regulation (BetrSichV) either.

So where does this trend come from?

The origin can be found in the USA, which is where the first standard was developed in 1973, and which can now be found in ANSI/ASSP Z244.1-2016 (R2020) 'The Control of Hazardous Energy Lockout, Tagout and Alternative Methods'. Product safety in America and product safety in Europe have developed differently. Europe seeks more of a constructive and technical solution, while in America, organisational protective measures have high importance. Global operators endeavour to implement uniform standards for their companies. As such, it makes sense that American companies (are eager to) transfer the standards that they are familiar with to their operations in Europe. In many cases, this means that the European requirements are not sufficiently taken into account. Product safety is strictly regulated in Europe and offers ample protection so long as the protective measures are implemented correctly by manufacturers and operators of machinery and systems.

Extract from the Machinery Directive 2006/42/EC (Annex I, 1.6.3.):

The machine must be equipped with devices that allow it to be disconnected from each individual source of energy. These devices must be clearly marked. It must be possible to lock them if their reactivation could cause a hazard to people. The disconnection device must also be lockable if operating personnel cannot monitor the permanent interruption of the energy supply from every access point. ...

In addition, harmonised standards supplement these basic health and safety requirements from directives and regulations. Residual hazards and their protective measures must be outlined in the operating instructions. This ensures that the machinery or system is completely safe from a legal perspective. It is not uncommon to find gaps in the implementation of essential protective measures in Europe, which can be attributed to very different causes. The most common cause is most likely ignorance of the statutory requirements and the 'state of the art.'

What does the practice look like?

Where gaps in the design and technical aspects are to be expected, it makes sense to close them with organisational or personal protective measures. Lockout–Tagout makes for a sensible and reliable addition, provided that the processes are carried out properly. To summarise, those who mind all product that all product safety or occupational health and safety procedures, whether European or American, are based on knowledge (expertise) of the respective protective measures will be in a position to achieve the goal (safety).

Which is the right way?

Manufacturers who wish to sell machinery and systems in Europe must apply European law and meet its requirements. The same applies to operating companies in Europe. As an addition to those requirements, Lockout–Tagout processes are helpful and ensure additional safety. Essential, however, is that the processes are implemented properly and checked to verify their effectiveness. In Lockout–Tagout processes, this is referred to as 'Tryout' (checking whether the Lockout was successful). Hence the abbreviation 'LOTOTO'. This means that when Lockout–Tagout processes are defined, the existing protective measures are evaluated by specialists (dual control principle) and supplemented by Lockout–Tagout measures if necessary. In our Lockout–Tagout seminar, we show you how to supplement the statutory requirements in Europe with Lockout–Tagout processes. You can learn more about how to implement the primary requirements in our 'Machinery Directive 2006/42/EC – CE conformity assessment procedure' seminar and Machinery Directive 2023/1230 (compact or intensive seminar), as well as in various other seminars. The tec.nicum team is also on hand to provide all-round support for machinery and system safety. ■

Jürgen Heimann
Lecturer in product safety and occupational health and safetytec.nicum Solutions & Services GmbH

tec.nicum academy

Seminar programme 2024/25

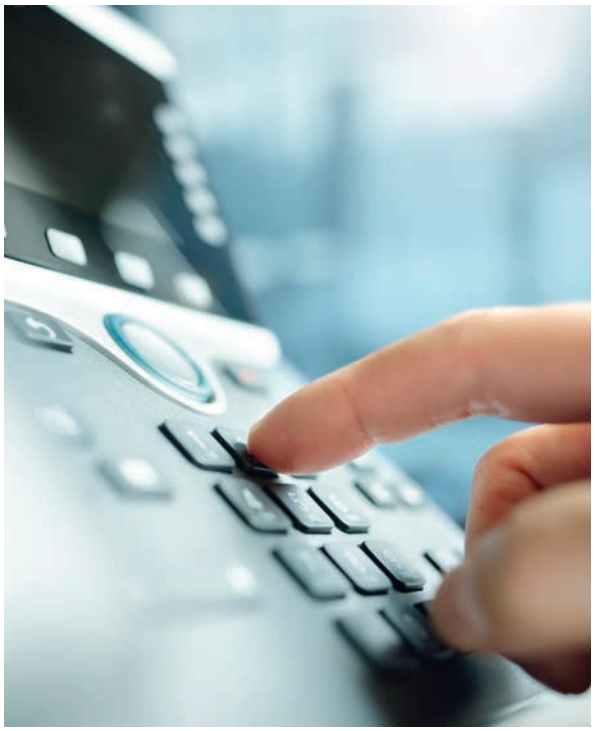
The tec.nicum academy provides a comprehensive training and seminar programme of topics focusing on the safety of machinery and systems.

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

We would be happy to organise a bespoke in-house seminar for you on the date of your choice that is matched to the individual professional interests of participants.

We would be happy to advise you personally.
Please get in touch:

Melanie Peters-Schuster
Tel. +49 202 6474 864
Available by telephone:
8.00-11.00 a.m. and 1.30-3.30 p.m.
info-de@tecnicum.com



Seminar topics	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
Law					
NEW Machinery Directive 2023/1230 **(compact seminar)**	29.01.2025	26.06.2025	12.03.2025	On request	On request
NEW Machinery Directive 2023/1230 **(intensive seminar – 2-day seminar)**	24.06.2025 until 25.06.2025	29.10.2025 until 30.10.2025	17.02.2025 until 08.02.2025	On request	On request
Machinery Directive 2006/42/EC – CE conformity assessment procedure	07.11.2024	–	–	On request	On request
The basics of occupational health and safety for managers	28.03.2025	On request	29.04.2024	On request	On request
The legal aspects of the safety of machinery for executive personnel **(1/2-day seminar)**	24.10.2024	–	–	On request	On request

tec.nicum

(Continued on page 22)

Seminar programme 2024/25 (continued from page 21)

Seminar topics	Wuppertal	Wettenberg	Lübeck	Kirkel	Online	Inhouse
Standards – regulations						
Risk assessments for infection prevention	–	–	02.12.2024	–	On request	On request
Risk assessment in accordance with EN ISO 12100	30.01.2025	02.07.2025	–	05.03.2025	On request	On request
Risk assessment for machines and systems in accordance with the Ordinance on Industrial Safety and Health	28.01.2025	01.07.2025	–	28.04.2025	On request	On request
Technical documentation of machinery and systems	03.04.2025	03.07.2025	–	06.03.2025	On request	On request
Application of EN ISO 13849-1 and introduction to SOFTEMA	On request	–	–	On request	On request	On request
Application of EN ISO 13849-1 and introduction to SISTEMA and validation	On request	–	–	On request	On request	On request
NEW Electrical equipment of machines according to EN 60204-1 (VDE 0113-1) **(2 days)**	01.04.2025 until 02.04.2025	–	–	–	On request	On request
New-build, conversion, retrofitting – from manufacturer to operator? **(1/2-day seminar)**	–	–	–	–	29.11.2024	–
Validation in accordance with EN ISO 13849-2 **(1/2-day seminar)**	–	–	03.12.2024	–	–	–

Seminar topics	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
Qualification courses with a special qualification					
Qualification as a TÜV-certified 'Machinery CE Certified Expert® – mce.expert'	11.02.2025 until 14.02.2025	02.12.2024 until 05.12.2024 13.05.2025 until 16.05.2025	01.09.2025 until 04.09.2025	–	On request
Basic course for safety officers **(2 days)**	13.02.2025 until 14.02.2025	–	05.02.2025 until 06.02.2025	–	On request
NEW Electrotechnically instructed person (EUP)	–	04.12.2024	–	–	–

Seminar programme 2024725 (continued from page 22)

Seminar topics	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
Application					
Practical workshop - working with SISTEMA (half-day seminar) Note: Can be combined with the SISTEMA introductory seminar on the following day	On request	On request	On request	–	On request
Fundamentals of safety engineering – guards and protective devices	On request	–	On request	22.11.2024	On request
Safety-orientated design of battery production systems	17.03.2025	15.09.2025	On request	On request	On request
Driverless transport systems and their integration into the production environment	18.03.2025	16.09.2025	On request	On request	On request
Safety in integrated robot production systems	19.03.2025	17.09.2025	On request	On request	On request
Human-robot collaboration	20.03.2025	18.09.2025	On request	On request	On request
NEU Electrically instructed person (EUP)	04.04.2025	–	27.11.2025	On request	On request
Lockout–Tagout (LOTO)	09.07.2025	–	18.11.2025	On request	On request
Crane operator qualification (ground-operated cranes)	28.10.2025	–	–	–	On request
Safe conversion of machinery and systems	08.07.2025	11.11.2025	25.11.2025	On request	On request

Seminar topics	Wuppertal	Mühldorf	Wettenberg	Kirkel	Online	Inhouse
Products						
Basic workshop PSC1 safety controller	On request	–	On request	On request	–	On request
Expert workshop on the PSC1 safety controller	On request	–	On request	On request	–	On request
The basics and inspection of opto-electronic protective equipment in accordance with the BetrSichV **(seminar objective: competent person)**	May 2025	September 2025	–	–	–	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
europe@tecnicum.com
www.tecnicum.com