mrl.news

The latest on the Machinery Regulation

Edition 2026.01

tec.nicum

Safety in a time of change – shaping opportunities, securing the future

Dear readers,

Industrial automation is undergoing a period of profound change. New regulatory requirements, innovative communication technologies and increasing digitalisation are transforming not only machinery and plant, but also the demands placed on manufacturers, integrators and operators.

With the new Machinery Regulation, which will become legally binding from January 2027, and the Cyber Resilience Act, issues such as functional safety and cybersecurity are becoming even more closely intertwined. Companies face the challenge of adapting their products and processes to future requirements at an early stage. At the same time, this creates opportunities to rethink safety in a holistic way and to gain a competitive edge.

In our article 'Safe Automation in Practice', we explore how modern machine designs can be made safe and flexible in the future. Technologies such as the Safety Fieldbox, IO-Link Safety and Single Pair Ethernet lay the foundations for high-performance, end-to-end and future-proof automation.

Our case study on the TREIF machines from JBT Marel demonstrates that innovative safety concepts are already being successfully implemented in practice today. The example of modern cutting systems clearly illustrates how intelligent safety solutions can combine productivity with user-friendliness.

Another key focus of this issue is the digitalisation of safety processes. With Digital LOTO, the digital management of lockout-tagout processes is becoming increasingly important. Particularly against the backdrop of increasing demands for documentation, transparency and efficiency, digitalisation offers considerable potential for greater safety in day-to-day operations.

The rapid developments in the field of robotics are also raising new questions. Humanoid robots and AI-powered systems are raising high expectations in terms of flexibility and performance. At the same time, security strategies must keep pace in order to build the necessary confidence in the safe use of these technologies. The combination of functional safety and artificial intelligence will therefore play a key role in the future.

We will also take a look at the requirements for the North American market. For many companies, UL certification remains a decisive factor in entering international markets and, at the same time, sets the course for global competitiveness.

Last but not least, we are delighted to inform you that our Academy seminars are now available with an even wider range of courses. Knowledge transfer and skills development remain key elements in successfully tackling the challenges of an increasingly complex technological world.

We hope you find this an engaging read, that it provides fresh inspiration for your day-to-day work, and that it offers plenty of ideas for shaping a safe industrial future.

Your mrl.news editorial team

What machine manufacturers and operators need to know

The new EU Machinery Regulation (EU) 2023/1230

QUICK BOX

On 20 January 2027, Regulation (EU) 2023/1230 will come into force, introducing a fundamentally new set of rules for machinery manufacturers, importers and operators. It replaces the Machinery Directive 2006/42/EC, which has been in force since 2009 – and there are no ifs or buts about it: there is no phased transition, but a strict cut-off date. Anyone who is not prepared risks no longer being able to place machinery on the market in compliance with the law. It's high time for an overview.

Author: Tobias Keller

Head of Administration,
tec.nicum

1. From draft to regulation – the process

The Machinery Directive 2006/42/EC has long been the cornerstone of machinery safety in Europe. But the world has changed: in 2006, digitalisation, connectivity, artificial intelligence (AI) and cyber security were barely on the radar, if at all. Furthermore, differences in the way the Directive has been transposed into national law across the Member States have led to differences in interpretation and distortions of competition.

The European Commission responded with a new approach: rather than revising the directive, it opted for a regulation. This means that the new set of rules applies directly and uniformly across all 27 EU member states without the need for national transposition. The European Parliament adopted the regulation by a large majority on 18 April 2023, and the European Council gave its approval on 22 May 2023. It was published in the Official Journal of the EU on 29 June 2023 and formally entered into force on 19 July 2023.

The regulation will become binding on manufacturers from 20 January 2027, exactly 42 months after it came into force. In Germany, the so-called Machinery Regulation Implementation Act (Maschinen-DG) will also replace the previous national implementing regulation (9. ProdSV).

2. What is changing fundamentally

A regulation rather than a directive: no more national leeway

The most fundamental change is of a formal nature, but has significant practical implications. An EU regulation is directly applicable, whereas a directive must first be transposed into national law. Until now, member states have been able to interpret and implement the Machinery Directive in different ways. That's all over now. The Machinery Regulation (EU) 2023/1230 is applied uniformly across the EU and is therefore a real boon for legal certainty and for the single market. →

The new EU Machinery Regulation establishes a modern legal framework for the placing of machinery on the market in Europe.

For the first time: Cyber security and artificial intelligence

Perhaps the most significant technical innovation is that, for the first time, the new regulation explicitly addresses cyber security risks relating to safety control systems and safety-critical software. Manufacturers must protect machinery and its software against unauthorised access and tampering. In addition, requirements for AI-based safety functions are being introduced, in line with the EU AI Act, which is being introduced at around the same time. Anyone using AI in safety-critical machine functions will need to take both sets of regulations into account in future. Autonomous and remote-controlled machines will also have their own regulations.

Risk assessment includes software

The basic principle of risk assessment remains the same, but its scope is expanding. A new requirement is the explicit obligation to assess risks arising from machine software as well, including planned future software updates following the placing on the market. Manufacturers must decide at the design stage which updates they plan to release and analyse the associated risks in advance. This marks a paradigm shift: responsibility for machine safety no longer ends when the machine is delivered.

Clarity on 'material changes'

A point of contention that has frequently arisen in the past is now being codified: the Regulation specifies precisely when a modification to an existing machine is deemed to be a 'substantial change' and therefore requires a new conformity assessment procedure. This has direct implications for operators carrying out modifications or retrofits. Where there is any doubt, they are quicker to assume their responsibilities as manufacturers – including CE marking and technical documentation.

Extended third-party inspection requirement for high-risk machinery

For six product categories with a particularly high risk potential (Annex I to the MVO), the involvement of a notified body for conformity assessment is mandatory. In addition, the obligations on importers and retailers are being tightened, and the requirement for authorities to report safety defects is being extended. The definition of a safety component has also been broadened. It now explicitly covers software and digital components that perform safety functions.

Digital operating instructions permitted

The Machinery Regulation introduces a practical and resource-efficient approach by allowing operating instructions, assembly instructions, and EU declarations of conformity to be provided entirely in digital form. However, operators should retain local copies of these documents. Relying solely on online access is not sufficient, as links to a manufacturer's documentation may not be available at a later date.

3. Key deadlines at a glance

Date	Event
2023-06-29	Publication of Regulation (EU) 2023/1230 in the Official Journal of the European Union
2023-07-19	Formal entry into force of the Regulation (voluntary application permitted)
2025-01-20	The European Commission has tasked CEN/CENELEC with finalising the standards
End of 2026	Planned publication of harmonised standards (hENs) in the Official Journal of the EU; Implementing Decision containing the full list of standards
2027-01-20	**Cut-off date:** Machinery Directive 2006/42/EC ceases to apply. Only MVO (EU) 2023/1230 now applies. Parallel operation is not possible.

4. The state of standardisation – the clock is ticking

Harmonised standards provide manufacturers with a practical toolkit. Anyone who applies such a standard may generally assume that the legal requirements are met ('presumption of conformity'). However, this is precisely where one of the biggest challenges of the new Machinery Regulation currently lies.

All standards harmonised to date under the Machinery Directive (there are several hundred) must be reviewed in the light of the new requirements of the MVO and amended where necessary. On 20 January 2025, the European Commission issued the final standardisation mandate to CEN and CENELEC. The timetable is, however, ambitious: CEN/CENELEC should submit a draft of the joint work programme by July 2025 at the latest; the harmonised standards should be adopted by early 2026 and published in the Official Journal of the EU by the end of 2026 – shortly before the deadline of 20 January 2027. The technical committees have been working on the standards since February 2025. According to → CEN/CENELEC, the results for around two-thirds of

all harmonised standards had been submitted to the European Commission by mid-2025. It is currently unclear whether all standards will be published on time. However, the Regulation provides for 'Common Specifications' as an alternative should harmonised standards not be available by the deadline of 20 January 2027.

New standards due to be published before the 2027 deadline must comply with the requirements of both the old Machinery Directive and the new Regulation. As things stand at present, they will therefore include two normative annexes in future: the existing Annex ZA (for the MRL) and a new Annex ZB (for the MVO). In addition, the European Commission is drawing up a set of guidelines on CSR. The editorial group's first meeting took place in January 2025, and the first drafts were ready by early 2026. A side issue with practical relevance: the ECJ's 'Malamud' judgement (March 2024) requires harmonised standards to be made available free of charge as part of EU law. The first so-called 'readability platforms' have already been set up.

5. Conclusion: Act now, don't wait

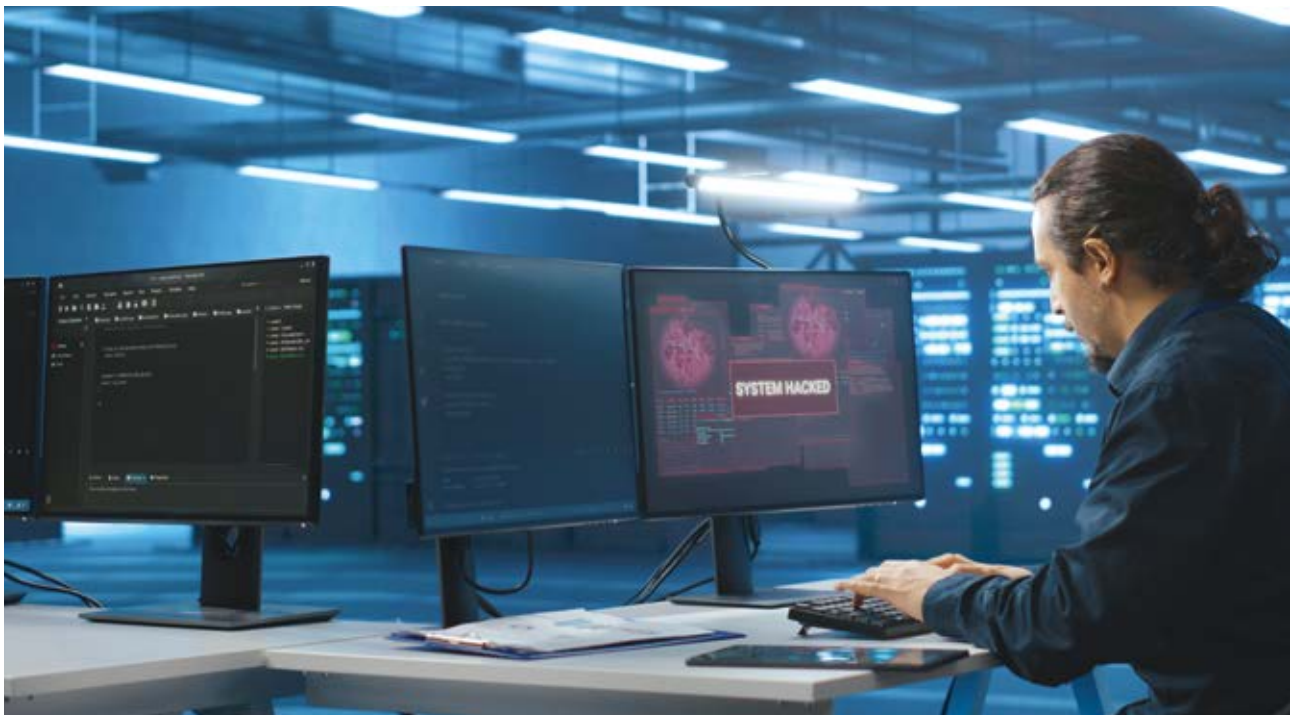
20 January 2027 is closer than it seems. Anyone still working in accordance with the Machinery Directive should start adapting their processes to the new Machinery Regulation at the same time. Risk assessments must cover software and cyber security; technical documentation must be updated; and the question of whether third-party certification may be required should be examined at an early stage.

Manufacturers with complex projects in the pipeline that will not be delivered until after the deadline should start applying the new regulation now. This saves a lot of time-consuming rework later on. Voluntary early compliance with the requirements of the Machinery Regulation is already possible and permitted – for example, through the early implementation of the new cyber security requirements.

The new Machinery Regulation is not merely an administrative document. It is a response to a world transformed by technology, with connected, intelligent and increasingly autonomous machines. Those who understand and implement the requirements at an early stage will not only ensure legal certainty, but also gain a genuine competitive advantage. ■

Note on standardisation:
The publication of the list of harmonised standards under the MVO in the Official Journal of the EU is scheduled for the end of 2026. Until then, the harmonised standards under the Machinery Directive 2006/42/EC may continue to be applied, provided that their content meets the requirements of the MVO. Organisations should keep a close eye on publications from CEN/CENELEC and the European Commission.

Companies that act early on ensure planning certainty, avoid unnecessary pressure to adapt and bring their products into line with the new requirements in good time.



Impact on mechanical engineering and automation technology

The Cyber Resilience Act (CRA) and OT security

Author: Tobias Keller
Head of Administration, tec.nicum

1. What is the Cyber Resilience Act?

The Cyber Resilience Act (CRA) refers to EU Regulation (EU) 2024/2847, which came into force on 10 December 2024. The aim is to ensure that products with digital elements (PDE) remain cyber-secure throughout their entire life cycle, from development through to distribution and decommissioning.

The CRA applies to all manufacturers, importers and distributors who make hardware or software with network capabilities or digital connectivity available on the EU market. In the context of mechanical engineering, this means that as soon as a machine, control system, sensor or drive is connected or can be connected, the CRA comes into play.

Timetable

Oct. 2024:	CRA published in the Official Journal of the EU
Dec. 2024:	Entry into force
Sep. 2026:	Reporting requirements for actively exploited vulnerabilities
Dec. 2027:	Full applicability of all CRA requirements

2. Relevance to mechanical engineering and automation technology

Traditional machine components such as PLCs, SCADA systems, industrial robots, HMI panels, networked drives and IIoT gateways fall within the scope of the CRA, provided they are network-enabled. This means that virtually all modern Industry 4.0 products are affected.

Key obligations for machinery manufacturers

- Secure by Design: Cybersecurity must be built in from the development phase onwards, rather than added as an afterthought
- Vulnerability management: Security updates must be provided throughout the entire product lifecycle (at least 5 years)
- Conformity assessment: Different verification procedures depending on the risk class (Standard, Class I, Class II), up to and including mandatory third-party testing
- SBOM (Software Bill of Materials): Comprehensive documentation of all software components and dependencies
- Reporting obligation: Vulnerabilities that are actively being exploited must be reported to ENISA within 24 hours

→

3. OT security vs. IT security: A crucial difference

For the first time, the CRA also explicitly addresses Operational Technology (OT), i.e. industrial control systems and field devices. There are fundamental differences here compared with traditional IT security:

Criterion	IT security	OT security
Conservation objective	Confidentiality, Integrity, Availability (CIA)	Availability, Integrity, Confidentiality (AIC) – priorities in reverse!
Downtime	Updates may be issued at short notice	Downtime = loss of production; updates only during maintenance windows
Life cycles	3–5 years	15–30 years (machines are often older than operating systems)
Connectivity	Fully connected	Often air-gapped or connected indirectly
Protocols	TCP/IP standard	Profibus, PROFINET, Modbus, OPC-UA, EtherCAT
Patches	Immediate distribution possible	Validation, testing and manufacturer approval required

4. The regulatory triangle: CRA – NIS-2 – Machinery Regulation

Three sets of EU regulations are interlinked in the mechanical engineering sector and together form a comprehensive cyber security framework:

Cyber Resilience Act (EU) 2024/2847	**NIS 2 Directive** (EU) 2022/2555 / NIS2UmsuCG	**Machinery Regulation** (EU) 2023/1230
Focus: Product ■ Obligations for manufacturers of connected products ■ CE marking for PDE ■ Valid from December 2027	**Focus: Operators** ■ Obligations for businesses in critical sectors (including manufacturing) ■ ISMS, reporting obligations, risk management ■ In Germany: NIS2UmsuCG / new BSIG from December 2025	**Focus: Machine** ■ Replaces the old Machinery Directive (2006/42/EC) ■ Cyber security as a new ESHA criterion ■ Valid from July 2027

Context: The CRA and the Machinery Regulation apply at product level (manufacturers), while NIS-2 applies at organisational level (operators). Organisations that manufacture and operate machinery may be subject to all three sets of regulations at the same time. CRA-compliant products make it easier for operators to comply with NIS 2. →

5. What this means for the German mechanical engineering sector

With around 6,500 mechanical engineering companies and exports accounting for over 70 per cent of their output, Germany has been particularly hard hit. The VDMA estimates that the majority of the sector falls under the CRA. Action is needed on several levels:

Immediate measures up to 2026

- Gap analysis: Which products should be classified as PDE? Which risk class applies?
- Establish processes for reporting vulnerabilities within 24 hours (effective from September 2026)
- Establish SBOM processes – provide an overview of all open-source and third-party components used

In the short term, up to 2027

- Integrating the Secure Development Lifecycle (SDL) into the engineering process
- Develop OT-specific security architectures: network segmentation, defence-in-depth, using IEC 62443 as a reference framework
- Alignment of the CRA and the Machinery Regulation: Integrating CE conformity assessment for cyber security
- Check the supply chain: Suppliers must themselves comply with the CRA (liability throughout the supply chain)

Conclusion

The Cyber Resilience Act marks a paradigm shift: cyber security is becoming a product characteristic – comparable to the CE marking for mechanical safety. For the German mechanical engineering sector, this represents a considerable challenge, but also an opportunity: those who invest at an early stage will secure market access and competitive advantages.

The key factor is the combination of the CRA (product safety), NIS-2 (operators' obligations) and the Machinery Regulation (machine safety). OT security is not simply an IT issue – it requires its own methods, standards (IEC 62443, ISA/IEC 62443) and expertise, which must be developed within the mechanical engineering sector. ■

Safe automation in practice:

Safety Fieldbox (SFB), IO-Link/IO-Link Safety and Single-Pair Ethernet at Schmersal

QUICK BOX

Safe Automation 4.0:
At Schmersal, SFB, IO-Link/IO-Link Safety and, in future, Single Pair Ethernet form an integrated platform for modular machine construction. They reduce the amount of wiring required, improve diagnostic capabilities and enable secure, IP-based communication straight from the sensor. This results in flexible and future-proof machine designs.

Author: Volker Heinzer

Strategic Product Manager – Industrial Communication Systems and Industry 4.0

"With the SFB, IO-Link Safety and Single Pair Ethernet, we are systematically steering safety technology into the digital future. These technologies open up new possibilities for machine designs and simplify design, commissioning and operation in equal measure."

The mechanical engineering sector is undergoing a period of far-reaching technological change. Growing demands for flexibility, modular machine designs and the increasing digitalisation of manufacturing processes call for new communication solutions – particularly in the field of functional safety. As a manufacturer of safety-related components and systems, Schmersal develops technologies that both simplify design and enable new concepts in safe automation. **The focus is on three key technologies: the Safety Fieldbox (SFB), IO-Link/IO-Link Safety and, in future, Single Pair Ethernet (SPE).**

The Safety Fieldbox (SFB) – decentralised safety for modular machines

Modular machines and flexible production lines require an architecture that can be easily adapted and rapidly expanded. This is where Schmersal's Safety Fieldbox (SFB) offers a decisive advantage. As a decentralised safety peripheral, it enables safety functions to be implemented directly on the machine module – without the need for central control cabinets, without time-consuming parallel wiring and without complex cabling structures.

The SFB communicates via PROFINET / PROFIsafe, EtherNet/IP / CIP Safety or EtherCAT / FSoE, integrates safe inputs and outputs, control panels with safe emergency stop functionality, and enables the integration of standardised I/O signals via optional expansion modules (port extenders).

For design engineers, this means a significant simplification:

- Safety functionality is becoming modular, scalable and fully digital
- Wiring effort is reduced, sources of error are minimised, and commissioning is significantly sped up
- Machine modules can be supplied pre-configured and combined flexibly in the field

Particularly in applications involving frequently changing machine configurations – such as packaging machines or assembly cells – the SFB provides a safety solution that is truly plug-and-play.

IO-Link and IO-Link Safety – transparency right through to the sensor

While IO-Link has long been demonstrating its strengths as an established communication standard at field level, Schmersal is taking the next logical step with IO-Link Safety. This means that continuous, bidirectional communication is now possible for safety-related devices for the first time.

The benefits for design and operation are considerable:

Simplified device integration
IO-Link reduces the number of component variants and enables automatic parameterisation during product changes and configuration when components are replaced during servicing. Devices no longer need to →

be adjusted manually – the control system or machine module does this automatically.

Transparency and Diagnosis

With IO-Link, in addition to the status 'Door closed and interlock activated', not only is an electronic nameplate available, but also comprehensive status and diagnostic data, including temperature readings, RFID signal strength, fault conditions and status warnings. In addition, operational data such as cycle, fault and operating hours counters provide valuable information for predictive maintenance. Secure configuration and parameterisation, combined with custom system commands, enable the integration of entirely new functions.

Flexible safety concepts

With IO-Link Safety, safety technology is also software-defined. Device parameters, safety levels or configurations can be transmitted digitally and documented centrally. This simplifies both validation in accordance with ISO 13849 and the subsequent expansion of machinery. Schmersal is set to launch its first devices and components supporting IO-Link and IO-Link Safety as early as the second half of the year – an important step towards seamless communication right down to the sensor/actuator level.

Single Pair Ethernet (SPE) – the path to a unified infrastructure

The growing volume of data from sensors, actuators and safety components calls for high-performance communication channels. Single Pair Ethernet (SPE) is already regarded as the 'next-generation Industrial Ethernet' – and Schmersal is actively adapting its safety technology to embrace this future technology.

SPE offers significant advantages:

Ethernet right down to the sensor

With just a single twisted-pair cable, end-to-end IP-based communication can be achieved – from the sensor to the cloud. This means: no more fieldbus islands, no more media breaks.

Long ranges and high bandwidths

With a range of up to 1,000 metres in the field, combined with a high data rate, SPE is ideal for large-scale facilities, intralogistics systems or the process industry.

Reduced variety of cables and plugs

SPE lays the foundations for compact connectors and innovative sensor concepts in safety technology.

Forward-looking safety concepts

When combined with secure communication protocols, this creates a unified and high-performance platform for the transmission of both safe and non-safe signals. For machine designers, this means long-term planning certainty and the opportunity to design systems today to be compatible with future Ethernet architectures.

Synergies arising from the interaction of technologies

The greatest benefits arise from the interaction of all three technologies:

- The Safety Fieldbox becomes a modular safety node
- IO-Link Safety enhances them with flexible, safe device communication
- Single Pair Ethernet provides the IP-based backbone for high-performance, real-time data streams

This results in an architecture that is perfectly suited to modern, scalable machine concepts – in other words, one that is modular, flexible, efficient, digital and safe throughout. Design engineers benefit from reduced complexity, technicians from simplified commissioning, and developers from new freedom in the design of safety-related functions.

Practical benefits in design

Fewer variants, less effort

IO-Link and modular SFB nodes reduce the variety of devices and simplify documentation and wiring.

Faster commissioning

Digital parameterisation, automatic detection and improved diagnostics significantly reduce installation and service times.

New machine designs

SPE and decentralised safety concepts open up new approaches for mobile, flexible and networked production units.

Future-proofing

Planners can already equip machines today for future Ethernet-based safety architectures. Schmersal no longer views safety technology merely as individual components, but as an integrated system – ranging from connection technology and decentralised peripherals to digital integration. ■

Slicing and dicing – quickly, precisely and safely

OEM safety controller in industrial cutting machines

QUICK BOX

A brief profile of JBT Marel and TREIF machines

For more than 75 years, the name TREIF has been synonymous with food-cutting machines. The company in Oberlahr/Westerwald, which has been part of JBT Marel since early 2025, develops and manufactures, amongst other things, slicers (which cut thin slices), dicers (for cutting into cubes) and portion cutters across a wide range of capacities. The focus is on machinery for the food industry. However, as there is also a wide range of slicing machines for the retail sector – particularly for bakeries – TREIF machines are also familiar to consumers.

JBT Marel develops and manufactures a very wide range of machinery and equipment/systems for food processing (meat, poultry, fish, convenience foods, etc.). The plant in Oberlahr operates with a high degree of vertical integration – including the manufacture of knives – and employs around 370 staff. Thanks to its innovative strength and high market penetration, the company is regarded as one of the 'hidden champions' of the mechanical and plant engineering sector and has a global presence through its sales subsidiaries and partners.

Author: Dirk Plastwich

Systems and Solutions Sales Representatives
Functional Safety Engineer (TÜV Rheinland Certified)

Under its world-renowned TREIF product range, JBT Marel in Oberlahr/Westerwald manufactures industrial cutting systems, utilising a customised compact safety control system across all its product ranges – including the new TREIF PUMA range, which is due to be launched shortly. This solution offers clear advantages – not only for machine manufacturers, but also for operating staff.

Steaks, meatloaf, cutlets: JBT Marel's 'TREIF PUMA' slices food at high speed, with great precision and a high degree of flexibility. That is why this series is used worldwide, particularly in many meat-processing plants. Preparations are currently under way at the Oberlahr/Westerwald plant for the mass production of the new generation of PUMA. **(Figure 1)**

Image 1: Shortly before market launch: The new generation of the Puma series will set new standards for the fast and precise cutting of meat.

Compact and customisable: the (small) safety controller

Even at the maximum output of 260 cuts per minute and with frequent manual product changes, operators need not worry about safety during the cutting process. Safety is a top priority for the machine designers, as demonstrated by the well-thought-out operating concept discussed later in this article. In addition, the new TREIF PUMA, like its predecessor and most other machines in the TREIF product line manufactured by JBT Marel, is equipped with a compact PROTECT SELECT OEM safety controller. (Figure 2)
The controller is programmed and validated by Schmersal according to the customer's specifications and requirements, in this case those of JBT Marel. It is supplied as a fully programmed and validated safety controller with a selection of application programs. The appropriate I/O configurations, safety switchgear combinations and signals for the various machine types are selected through the PROTECT SELECT OEM application programs in accordance with the safety concept developed for TREIF machines.

First six, now seven application programmes on a single controller

For several years now, the engineers have been using this OEM-specific safety controller for at TREIF machines. Mike Vogelsberg, Head of Software & Electrical Engineering Development: "We previously had different control models for the individual model ranges." →

Figure 2: The control unit of the new PUMA bread slicers. On the right of the picture: the PROTECT SELECT OEM compact safety controller.

Since we switched to PROTECT SELECT, stock management has become much simpler, and the safety features are perfectly tailored to our needs – across all product ranges. All we need to do after installation is register the controller and specify the relevant applications."

Originally, there were six such application programmes, written by software specialists at Schmersal. The functions of these programmes include, for example, the safety-related coordination of the monitoring and operation of the protective cover, the feed mechanism (gripper), the discharge conveyor and the blade, as well as defined maintenance positions. The optional non-electric spring-loaded lid opening mechanism – which allows for faster loading of new cutting material – is also taken into account from a safety perspective.

For the new generation of PUMA controllers, the Schmersal programmers have now 'programmed' a seventh application into the controller. And, if necessary, further functions or programmes can easily be added to meet new requirements. This means that this type of safety controller is future-proof and can also be used across different product ranges.

The comprehensive connectivity of the PROTECT SELECT OEM (18 safe digital and two safe analogue inputs, six safe outputs) paves the way for a wide range of application scenarios. A unidirectional interface enables signal processing and enhances usability while minimising the amount of wiring required.

Standard feature on all machines: Safe Torque Off

One application used on all machines fitted with the PROTECT SELECT OEM is the 'Safe Torque Off' emergency stop function. The application programmes can be easily selected as required or during installation, as a single version of the PROTECT SELECT OEM compact safety controller covers a wide range of machines. Mike Vogelsberg: "We use the PROTECT SELECT OEM not only for portion cutters such as the TREIF PUMA, but also, amongst other things, for dicers – these are machines that, for example, cut bacon and ham into cubes – and for the self-service bread-slicing machines in supermarkets, which are fitted with solenoid interlocks. Only our most complex machines, which feature particularly sophisticated safety functions – often requiring safe drive functions such as Safe Limited Speed – are fitted with a suitable safety PLC."

Close cooperation during the programming phase

When defining the required applications and assigning inputs and outputs, Schmersal's safety experts worked closely with the TREIF development team; on several occasions, Schmersal's programmers also visited the site in Oberlahr. The result: the programme logic is perfectly adapted to the machine functions, the programme codes from several previously used control systems have been mapped, and a minor hardware modification has also been implemented. A type examination of the software was part of the scope of services provided by Schmersal.

Hygienic, precise cuts: the new PUMA

Greater standardisation at the drive and machine levels was a key objective pursued by the design engineers in Mike Vogelsberg's team during the development of the new PUMA generation – an approach that has already proven its worth in terms of machine safety. "The drives are speed-controlled. The operator enters the thickness of the discs and the cycle rate per minute, and the machine adjusts these automatically." The controller coordinates the drives, while the operating mode of the compact safety controller is in turn coordinated with the operational signals.

Operation: as intuitive as possible – and with the new H series

When it comes to operating the PUMA and other machines, the designers adhere to the principle that "less is more". Mike Vogelsberg: "The machines are often used in smaller businesses. They are not usually operated by qualified electricians, but by staff at meat-cessing plants or bakery branches. That is why the aim is to make operation as simple and intuitive as possible." This is achieved by means of a touch screen **(Figure 3)** combined with just a few physical operating elements. TREIF relies on Schmersal's H series of operating elements for this purpose. **(Figures 4 and 5)** This series was launched only recently, and it also meets very high hygiene standards. This is precisely what is required of TREIF machines, as Mike Vogelsberg explains: "We test everything. We fit it very thoroughly to ensure it can withstand →

Figure 3: Everything in view: The PUMA's tochscreen.

frequent and intensive cleaning – and we literally test a lot of it until it breaks. However, we have always been satisfied with the switches from Schmersal's previous N series and will therefore now be gradually switching to the successor series." According to Vogelsberg, slicers in particular are subject to very high hygiene standards: "These machines often cut raw products that are eaten as they are, i.e. without being cooked. The halls are colder here, and hygiene standards are higher."

In focus: Tamper-proof design

When developing both the safety guards and the HMI (Human-Machine Interface) for TREIF machines, tamper-resistance is a key consideration – after all, there is a high risk of injury if the safety guards are bypassed. This is why, for example, the magnets in safety sensors are concealed, and a test cycle is specified once the machines have been switched on: the safety guard must be opened and closed once to check that the safety-related shut-down function operates correctly when the guard is open. This cycle is also monitored by the OEM compact safety controller.

The benefits of a bespoke security solution

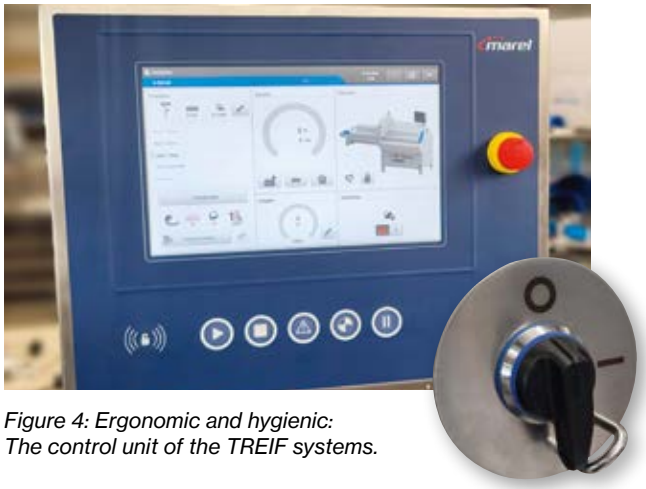


Figure 4: Ergonomic and hygienic: The control unit of the TREIF systems.

Figure 5: The control units from Schmersal's H series – shown here is a main switch – meet the highest hygiene standard.

In summary, the advantages of the customised compact safety controller are clear to those responsible for the TREIF product range: standardisation based on the 'one controller for everything' principle saves costs, reduces complexity and simplifies stock management, while the OEM version includes all the functions required for safe machine operation. The necessary variations for the different machine types and series have been integrated into the controller; the relevant application programme is activated during installation via selection buttons and the touchscreen.

Those in charge at TREIF are also satisfied with the 'soft facts': according to Mike Vogelsberg, the ongoing collaboration is working well. This is another reason why new generations of machinery will increasingly feature hygiene-compliant switchgear from Schmersal's H series in future, not to mention the TREIF-specific OEM version of the compact safety controller. ■

Figure 6: Mike Vogelsberg, Head of Software & Electrical Engineering Development, in the technical center for the TREIF product line, standing in front of the "LevelUp" slicer – which, like the PUMA, is on the verge of market launch.

Since 2023, the Safety Fieldbox has been part of Schmersal's range of around 13,000 UL-certified products.

Compliant with standards, reliable and future-proof.

UL certification of safety switchgears

QUICK BOX

UL certification at a glance

- A prerequisite for many applications in North America
- Additional requirements beyond those set out in IEC standards
- Focus on product safety, materials and installation
- Product and manufacturing assessment
- Regular audits of the production site

Author: Jörg Eisold, Dipl.-Ing. (FH)

Head of Standards, Committees and Association Work

Safety switchgears are a key component of modern machinery. Whether they are position switches, optoelectronic sensors or RFID-based safety ystems: they must function reliably – and, above all, be approved for use worldwide.

While the CE marking is established in Europe on the basis of the IEC 60947-5-x series of standards, the North American market imposes additional requirements. The rule here is that, without certification from a recognised testing body such as UL (Underwriters Laboratories), market access is, in many cases, virtually impossible.

Although UL has increasingly aligned its standards with the IEC series, even as the standards converge, the safety philosophies remain different.

The standards in the IEC 60947-5-x series specify how a device must function – including electrical parameters, mechanical properties and environmental conditions. This technical basis is incorporated into the UL standards framework – for example, as UL 60947-5-1 or UL 60947-5-2 – but is supplemented by national requirements. Furthermore, products must be installed in accordance with the National Electrical Code (NEC), which imposes additional constraints.

Additional national requirements relate, for example, to the appliance's fire safety performance, the materials used, and safety in the event of incorrect installation. As a result, even technically mature products that comply with IEC standards are not automatically UL-compliant. With conventional safety switches in accordance with IEC 60947-5-1, the focus is on characteristics such as positive opening, mechanical robustness and service life.

UL certification involves a number of additional aspects, such as the assessment of clearances and creepage distances, the verification of material properties (e.g. flammability) and testing under UL-specific load and fault conditions.

A key point here is that approved materials (e.g. plastics with a 'UL Yellow Card') are used. This makes the choice of materials a critical factor in the development process. With non-contact sensors in accordance with IEC 60947-5-2, the focus shifts even more towards the application. Whilst the IEC standard describes the sensor's function – such as switching distances or EMC characteristics – UL considers the system as a whole, including the power supply, the connection cable, the fuse protection in the control cabinet and the operating environment. A sensor is therefore not only assessed on its own, but there are also UL tests for the system as a whole.

With modern safety sensors, such as RFID-based systems, the issue takes on a new level of complexity. The IEC 60947-5-3 standard requires a defined response to faults (deterministic behaviour), the monitoring of internal states, and the integration of functional safety principles. This presents a particular challenge for UL certification, as electronic and software-based functions must be assessed. In addition, safe behaviour under fault conditions must be demonstrated. Functional safety and traditional product safety therefore both play a crucial role here. The additional requirements must be taken into account at an early stage in the development process. This includes, for example, the selection of approved materials and components.

Another important aspect is that UL assesses not only the product itself, but also the manufacturing process. The production site is also specified in the UL file for the certified product. To this end, regular audits are carried out at the respective production sites.

Once all the requirements have been met, the necessary tests have been completed and the formal evidence has been provided, there is nothing to stand in the way of gaining access to the North American market. ■

Safety in humanoid robots

New challenges for safety concepts and functional safety

QUICK BOX

Safety in relation to humanoid robots:
Like many non-stationary or interactive robots, humanoid robots work directly alongside humans and are increasingly using AI to recognise their surroundings and act autonomously. This gives rise to new safety requirements which traditional machine designs can only partially meet.

Key risks include:

- Risk of falling in the event of a loss of power
- Collisions caused by high-speed movement
- AI behaviour that is difficult to predict
- Cyberattacks on networked systems

That is why functional safety, sensor fusion, safe motion functions and cyber security are becoming increasingly important. Existing standards are currently being expanded to better cover AI-enabled robotic systems.

Author: Katrin Wirz

Product Manager
K.A. Schmersal GmbH & Co. KG

What is a humanoid robot?

Humanoid robots are on the cusp of moving from the research laboratory to industrial application. They promise a new form of automation: flexible, adaptive and ready for immediate use in human working environments. **At the same time, however, safety-related issues arise which can only be partially addressed by the traditional concepts of the Machinery Directive.**

Humanoid robots are characterised by their human-like design and their ability to interact with their environment. They usually have a torso, two arms, various sensors and a means of locomotion, which is achieved either via legs or alternative systems.

However, it is not just their external form that is crucial, but their functional purpose: they are designed to take over human tasks and integrate into existing working environments. This characteristic does not fundamentally distinguish mobile robots from traditional industrial robots, which usually operate within enclosed cells and are optimised for specific tasks.

The growing scope for integrating artificial intelligence (AI) is significantly reinforcing this trend. Modern systems are capable of perceiving their surroundings, interpreting situations and making decisions based on them. In doing so, they move away from strictly deterministic systems and towards decision-making processes based on probability calculations. On the one hand, this new quality opens up far-reaching possibilities; on the other hand, however, it also brings with it new uncertainties, particularly with regard to the predictability of behaviour.

Areas of application and market players

The future roles of intelligent robots will become particularly apparent in areas where flexibility and adaptability are required. In industrial production, they can take on tasks that were previously the preserve of humans, without the need for major modifications to existing plant. This is seen as offering considerable benefits, particularly at a time of skills shortages, as collaborative robots can take on physically demanding, monotonous or dangerous tasks. In addition, there are opportunities for application in logistics, the healthcare sector and the service sector. Applications range from providing support in care settings and carrying out service tasks to operations in hazardous environments, such as rescue operations. →

The market for humanoid robotics in particular is currently dominated by a number of international players. Companies such as Boston Dynamics and the Toyota Research Institute are driving forward the development of highly dynamic movement sequences and AI-based behavioural models in particular. With the Optimus project, Tesla is pursuing a strategy of industrial scaling, while companies such as SoftBank Robotics and Hanson Robotics are focusing on social interaction. At the same time, companies such as Unitree Robotics and UBTECH are developing compact and comparatively low-cost systems. What all these approaches have in common is the combination of advanced actuators, high-performance sensors and increasingly complex software architecture.

Safety challenges and new dimensions of risk

The combination of physical interaction and intelligent control presents new safety challenges. Unlike with traditional industrial robots, it is often not feasible to maintain a physical separation between 'human and machine'. Instead, humanoid robots are also being used specifically to interact directly with people, shifting the focus from isolation to safe collaboration.

A key risk lies in the mechanical design of these systems. Humanoid robots, for example, are usually dynamically unstable and must continuously and actively control their balance. An abrupt shutdown or loss of power – such as that caused by 'Safe Torque Off (STO)' – therefore does not result in a safe state, but may trigger a fall. At that moment, the robot becomes an uncontrolled object with considerable kinetic energy, which poses a high risk of injury, particularly in the case of larger systems.

In addition, there are significant risks of collision. Owing to their momentum and mass, even smaller robots can generate forces that exceed standardised pain thresholds. In the case of humanoid robots, this risk is further exacerbated by the high degree of mobility of the entire body, including the legs, torso and arms. In addition to the physical risks, there are also software-related challenges. At the same time, new demands are being placed on situation and context recognition: a robot must not only recognise that an object is moving, but also understand whether it is, for example, a tool or a potential hazard.

Aspects of cyber and data security are also becoming significantly more important. Robots often process large amounts of sensitive data and are increasingly connected, which means they can potentially become targets of attacks. Safety strategies must therefore take into account not only physical integrity but also digital integrity.

Safety concepts, standards and industrial classification

Against this backdrop, new safety architectures are emerging that go beyond traditional concepts. Modern approaches combine several levels of protection. At the lowest level are safe drive and motion functions which, for example, limit speeds and forces or provide active damping mechanisms. This is supplemented by comprehensive environmental monitoring based on sensor fusion, which captures the workspace as a three-dimensional safety field and evaluates it dynamically. Furthermore, higher-level monitoring systems are becoming increasingly important; these analyse the behaviour of the AI itself and can intervene in critical situations.

From a regulatory perspective, this area of technology is still under development. Existing standards such as ISO 12100, ISO 10218 and ISO 13482 provide an important foundation, but their applicability to humanoid systems is limited. In particular, aspects such as dynamic stability, AI-based decision-making processes and safe operation in the event of a power loss are not fully addressed in the existing regulatory frameworks. At the same time, overarching regulatory frameworks – such as the new Machinery Regulation (EU) 2023/1230 – are becoming increasingly important, as they set out, for the first time, explicit requirements for software-based and AI-supported systems.

Functional safety and systematic safety assessment

A key aspect that goes beyond traditional safety considerations is the consistent application of functional safety to interacting robotic systems. While existing standards such as ISO 12100 provide a framework for risk assessment, IEC 61508 and ISO 13849, in particular, provide the methodological basis for the development of safety-related systems.

Functional safety encompasses the analysis, specification and validation of safety-related functions, including the demonstration of their reliability. This includes both hardware and software components and covers the entire system architecture. This approach is becoming increasingly important for all robots, as safety-critical functions no longer relate solely to traditional control elements, but are increasingly implemented using complex software and AI algorithms.

A key component is the systematic assessment of default risks. This takes into account both random hardware faults and systematic errors – for example, in software or AI models. The aim is to demonstrate that the overall system achieves defined safety levels →

(e.g. SIL or Performance Level) and that critical malfunctions occur with a sufficiently low probability.

Furthermore, a holistic view of the life cycle is required. Safety assessments must not only cover the design phase, but must also take into account operation, maintenance, updates and the system's learning behaviour. With AI-based systems in particular, behaviour can change over time, which necessitates ongoing evaluation and validation processes.

The semiconductor components used play a particularly important role. Processors, sensor chips and AI accelerators form the technical foundation for perception, decision-making and actuation. Faults in these components can lead directly to safety-critical situations. It is therefore necessary to carry out a specific assessment of these components, including their architecture, their failure mechanisms and their integration into the overall system.

In addition, AI-specific security assessments are becoming increasingly important. Normative approaches such as ISO/PAS 8800 address the systematic analysis of AI models, including their robustness, generalisability and potential errors. The aim is to integrate non-deterministic decision-making processes into a robust safety framework.

In addition to analysis, the focus is on the validation of risk-mitigation measures. These include, amongst others:

- Sensors and sensor fusion for reliable environmental perception
- Limiting speed, forces and working areas
- Safe motion functions and controlled stopping strategies
- Visualisation and simulation of hazard zones

These measures must not only be implemented, but also systematically reviewed and proven to be effective.

After all, functional safety is closely linked to cyber security considerations. Networked humanoid systems must be protected against tampering and unauthorised access, for example in accordance with the IEC 62443 standard. Only by combining functional safety and IT security can a comprehensive protection strategy be implemented.

Tapping into new markets

This presents both challenges and opportunities for companies in the safety technology sector. The Schmersal Group, as an established supplier of safety components and systems, possesses extensive expertise in the functional safety of machinery. These capabilities can be applied to humanoid applications in many areas, such as safe signal processing, the control of safety-related functions and the safeguarding of work areas. At the same time, it will be necessary to further develop existing technologies in order to meet new requirements such as three-dimensional environmental monitoring or AI-based safety assessment.

In summary, it can be said that mobile robots – including humanoid robots – offer considerable potential for innovation, but at the same time require a paradigm shift in machine safety. Traditional approaches, such as safe shutdown or the physical separation of humans and machines, are reaching their limits. Instead, the focus is shifting towards adaptive, multi-layered safety approaches that integrate mechanical, sensor-based and IT-related aspects. The success of this technology will depend largely on the extent to which it is possible to establish a robust level of safety whilst at the same time realising its economic potential. ■

Sources:

- Fraunhofer IPA, Guidelines on the Safety of Humanoid Robots, September 2025
- White Paper, Out of the Cage: Advanced Functional Safety for Humanoids – Positron Safety AI Architecture, Synapticon GmbH, Dr.-Ing. Florian Weißhardt, Dr.-Ing. Tim Fröhlich, Dieter Volpert, 23 January 2026
- Safety considerations for humanoid robots, 2026, Industriezeitschrift.de
- SGS-Société Générale de Surveillance SA (2026), leaflet 'Safety Assessment for Humanoid Robots'
- [1)] Standards:

  ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction
  ISO 10218: Robotics – Safety requirements, Part 1: Industrial robots, Part 2: Industrial robot applications and robot cells
  ISO 13482: Robots and robotic devices – Safety requirements for personal care robots
  IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
  ISO 13849: Safety of machinery – Safety-related parts of control systems
  ISO/PAS 8800:2024: Road vehicles – Safety and artificial intelligence
  IEC 62443: Industrial communication networks – IT security for networks and systems

Humanoid robots are opening up new possibilities in industry. Their use requires clear safety standards and regulations. The key factor is safe integration into existing processes.

Digital lockout/tagout

Reliable maintenance without mountains of paperwork

QUICK BOX

Key points for operators

- LOTO remains a core process in safe maintenance – particularly when working on energy sources, residual energy and hazardous areas.
- tec.dloto does not replace physical locking, but makes preparation, authorisation, verification and release significantly more robust.
- Starting with a QR code, step-by-step guidance, reference images, photographic evidence and approvals help to minimise the typical shortcomings of paper-based processes.
- Centralised logs, dashboards and audit-traceable records provide safety managers with greater transparency during day-to-day operations.
- As part of the tec.nicum service offering, the solution can be integrated into existing plant processes in a practical manner, supported by consultancy, training, engineering and integration.

Author: Tobias Keller

Head of Administration,
tec.nicum

With tec.dloto, tec.nicum – the services division of the Schmersal Group – offers a digital solution that transforms traditional LOTO procedures into guided, traceable and audit-ready processes.

Maintenance is the moment when machine safety becomes particularly tangible. Safety guards are activated, drives are shut down, power sources are disconnected and residual energy is dissipated. While safety in production operations is ensured by fixed procedures and technical safety devices, safety during maintenance, cleaning, fault rectification or modifications often depends on thorough preparation and consistent implementation. This is precisely where lockout/tagout comes into play – and this is precisely where it becomes clear why a digital solution such as tec.dloto is more than just a convenient piece of software for operators of industrial plants.

Lockout/Tagout, or LOTO for short, refers to a systematic procedure for controlling hazardous energy sources. 'Lockout' refers to the physical locking of an energy-isolating device, such as a main switch, valve or shut-off device. 'Tagout' supplements this lockout procedure with clear labelling: who carried out the lockout, why it was carried out, and that the equipment must not be put back into operation. The concept of this procedure originates from Anglo-American occupational health and safety. Of particular significance was the US OSHA standard 29 CFR 1910.147, 'The control of hazardous energy', which, since the late 1980s, has set out requirements for programmes, procedures, training and regular inspections relating to maintenance and repair work.

The underlying safety concept is also firmly established in the European and German contexts, even if the term 'LOTO' is not always used. ISO 14118 deals with the prevention of unexpected start-up of machinery and covers various forms of energy: electrical, hydraulic and pneumatic energy, as well as stored kinetic energy, for example resulting from position, pressure or springs. The Industrial Safety Regulation also stipulates that work equipment must be able to be safely shut down and disconnected from energy sources. The practical principle is the same everywhere: a machine must not start up unexpectedly during hazardous operations, and stored energy must not be released in an uncontrolled manner.

A standard LOTO procedure therefore follows a clear line of reasoning. First, the work is prepared and all relevant energy sources are identified. The machine is →

then shut down in an orderly manner, disconnected from its power sources and secured to prevent it from being switched on again. Any residual energy is then dissipated or reliably controlled. Work may only commence once it has been verified that the system is de-energised or in a safe state. Before recommissioning, the work area and the machine must be checked, the relevant personnel informed, and the safety devices properly deactivated. That sounds simple, but in day-to-day operations it is prone to errors – particularly in the case of complex systems, shift changes, contractors, time pressure or frequently changing maintenance tasks.

Basic principle of LOTO:
Prepare the work, identify energy sources, shut down and disconnect the machine, lock and tag it, discharge or secure any residual energy, verify that it is in a safe condition, and, once completed, release it again after a check.

Traditional, manual solutions usually involve printed instructions, forms, tags, personal locks and handwritten logs. Physical locks remain essential for on-site protection. However, the organisational side of things is often less reliable: paper documents can get lost, become illegible or no longer reflect the current situation. Photos are stored on private or decentralised devices; authorisations are granted by telephone or email; and during an audit, it is a laborious process to piece together who carried out which step and when. Even more critical is the lack of visibility while work is in progress. With purely manual procedures, managers and safety officers often only realise after the event whether a process has been documented fully and correctly.

tec.dloto addresses precisely these vulnerabilities. The tec.nicum solution is a web-based and mobile platform for LOTO management. It digitises the energy isolation process and guides users through the necessary steps. The process begins in a practical way: the employee scans a QR code on the machine, initiates the LOTO request and receives step-by-step digital instructions. Reference images help to clearly identify the correct cut-off point or fuse position. Photo uploads and inspections document the actual condition on site. Critical steps can be safeguarded via approval workflows before maintenance begins.

This turns a checklist into a guided process. Every action is recorded with a time stamp, user actions are assigned, and the LOTO history is available in a consolidated form. This creates a level of transparency for safety officers, line managers and plant managers that paper-based systems can only achieve at considerable cost. Dashboards, live tracking, notifications and a centralised overview of facilities show which LOTO measures are active, which authorisations are pending and where work is in progress. This not only reduces audit-related stress, but also improves day-to-day operational management.

The advantage over traditional manual solutions therefore lies not solely in the fact that no paper is used. The key point is that tec.dloto introduces a sense of commitment into the process. It is not so easy to skip steps, outdated instructions are replaced centrally, and responsibilities can be traced within the system. Whereas previously scattered documents, local folders and verbal agreements had to be collated, audit-ready records are now created, complete with photos, time-stamps and clearly defined roles. It is also easier for new staff or external service providers to get started, as they are not simply given instructions but are guided through the process. →

LOTO improves safety during maintenance work. Digital solutions make processes efficient and traceable.

This represents significant added value for tec.nicum's customers. tec.nicum does not view tec.dloto as a standalone IT tool, but rather as part of a comprehensive service offering covering all aspects of machinery and occupational safety. tec.nicum – Solutions & Services GmbH is part of the Schmersal Group and brings together services from the academy, consulting, engineering, integration, digitalisation and outsourcing divisions. This is important because an effective LOTO system does not end with the purchase of software. Processes must be tailored to the plant; roles must be clearly defined; staff must be trained; and procedures must be maintained in line with operational needs. This is precisely where tec.nicum can support its customers.

In practice, this means that companies not only receive a digital platform, but also support in setting up a robust, scalable and verifiable LOTO process. tec.dloto supports mobile access, can be deployed either in the cloud or on-premises, and makes getting started easier through bulk uploads and customisable workflows. The solution therefore grows in line with the organisation's needs. In the future, further safety modules, such as permit-to-work functions, may be added. For operators with multiple lines, sites or rotating teams, this scalability is a key advantage.

Particularly when it comes to safety-critical tasks, digitalisation only makes sense if it makes work on site easier and safer. tec.dloto meets this requirement because it does not replace the tried-and-tested basic principles of lockout/tagout, but rather ensures their consistent implementation. Physical separation and locking remain the key elements. The digital solution ensures that preparation, approval, verification and return are managed and documented properly. This creates a practical link between health and safety, maintenance and compliance. ■

The conclusion is clear: LOTO is not a mere formality, but a key element of safe maintenance. Manual methods can work, but they require a great deal of discipline. With tec.dloto, tec.nicum offers its customers a service that goes beyond the tool itself, making this process more professional, transparent and efficient. For customers, this means less paperwork, less uncertainty, faster verification and a significantly better basis for reliably managing safety-critical work.

tec.nicum

tec.nicum academy
The 2026/2027 seminar programme

Over the coming months, the tec.nicum academy will once again be offering a wide-ranging programme of training courses on current topics relating to machine safety.

September 2026:

2026/09/15: New Machinery Regulation (MVO), Wuppertal

2026/09/16: Cyber Resilience Act (CRA), Wuppertal

In addition, further seminars and events are being planned nationwide at various locations.

As well as specialist seminars, the range of courses on offer also includes certified qualification programmes such as **MCEexpert (Machine CE Expert)** and **FSM tec.nicum (Functional Safety Manager).**

If you are interested, all seminars can also be delivered as in-house training directly at our company and tailored to your specific requirements.

You can find the latest seminar and event dates, as well as all the information you need about registration, at www.tecnicum.com.

academy

Education center
- Training courses
- Customer-specific trainings
- In-house seminars
- Certified courses (MCEexpert and FSE)

consulting

Analysis and documentation
- Technical support
- Risk assessment
- CE conformity assessment
- Evaluation of machines and production lines
- Reports

engineering

Planning and design
- Technical project planning
- Conceptual project development
- Electrical and mechanical design
- Executive project management
- LiDAR scan

integration

Practical application
- Turnkey approach
- Installation
- Retrofit

digitalisation

Software integration
- tec**.ps** (Product Service System)
- tec**.ssm** (Schmersal Smart Machine)
- tec**.cvs** (Computer Vision Solutions)
- tec**.dloto** (Digital Lockout Tagout)
- tec**.ems** (Energy Monitoring System)

outsourcing

Serial solutions
- Plug & Play products
- Engineer to Order projects
- Systems and cabinets

tec.nicum's range of services comprises six modules.

Images: K.A. Schmersal GmbH & Co. KG, shutterstock.com,
JBT Marel for the TREIF machines case study

Publisher:

tec.nicum

K.A. Schmersal GmbH & Co. KG

Möddinghofe 30
42279 Wuppertal

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