

mrlnews

Issue 2019.01

Page 2

Editorial – Changes in standards

Page 3

Machine safety and product liability

Page 5

Fixed-position safety –
two-handed switches in accordance with
DIN EN ISO 13851:2019-11

Page 6

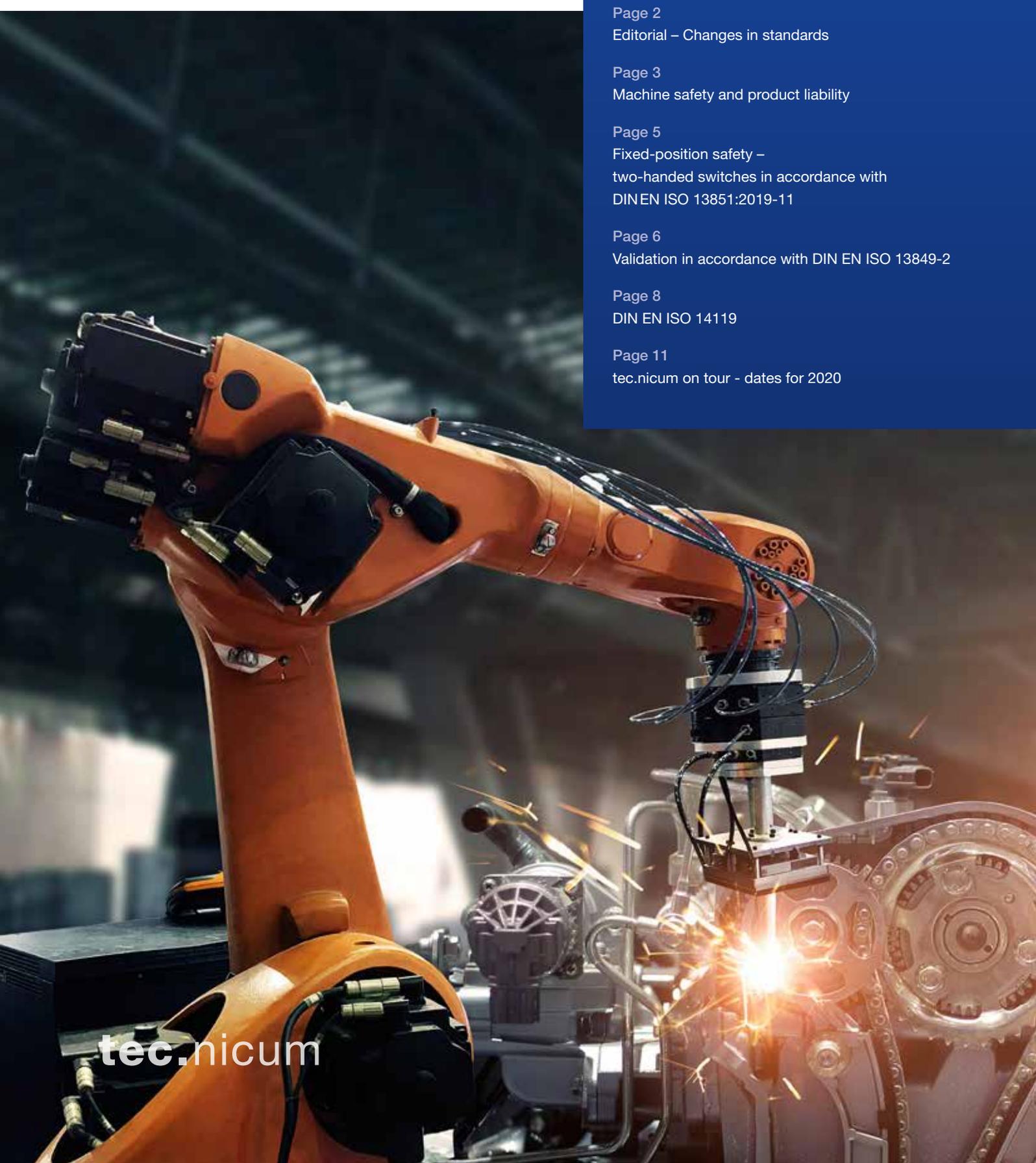
Validation in accordance with DIN EN ISO 13849-2

Page 8

DIN EN ISO 14119

Page 11

tec.nicum on tour - dates for 2020



tec.nicum

Editorial

Changes in standards

“Change favours the prepared mind,” according to a quote from Louis Pasteur, the 19th century chemist and physicist. And these words of wisdom undoubtedly still apply in the 21st century. Even when, in times of digital transformation and the breakneck pace of technological change, it is becoming increasingly difficult even to keep pace with the changes.

The world of standards is constantly changing. This is exactly what our article on “Legal & Standards News” is all about, providing information on the current status of the ongoing reform of the Machinery Directive, in which the “state of the art” plays an important role.

There are also changes to the standard defining the design principles for two-handed switches in the new ISO 13851:2019. By contrast, the DIN EN ISO 14119 has been available for many years, but still needs explaining since, as elsewhere, the devil is very much in the detail.

Last but not least, another article in this edition of our MRL News is dedicated to an important but little regarded, DIN EN ISO 13849-2. This standard allows optimum analysis

and, where necessary, systematic improvement of the safety level of machines and equipment.

There is also further information about our “tec.nicum on tour” series of events. This brochure contains the programme for 2020.

Enjoy the read!

With all the best from the editorial team



Machine safety and product liability

News and details on the law and standards

The European Machinery Directive (EMD) is the foundation for legally-compliant circulation of mechanical engineering products within the European Union market. It obliges manufacturers to guarantee a minimum level of safety for machines and equipment.

In accordance with the Directive, machines must comply with the basic health and safety requirements set out in its Appendix I. Initially, machine constructors are themselves liable for designing their machines in accordance with the Directive and for the associated documentation, as the declaration of conformity is what is known as a “self-declaration” with no mandatory involvement by an external body. If, against expectations, a machine on the market is the cause of an accident, initial checks are carried out as to whether this can be attributed to a design fault by the initial vendor. If this is the case, there could be legal consequences under some circumstances. Not least, damages could also be claimed against the initial vendor in accordance with section 823 BGB (German civil code).

Results of MRL evaluation

The Machinery Directive which is currently valid, 2006/42/EU, dates back to 2006. In the EU, it is standard practice that EU regulations and directives are reviewed at regular intervals in order to check their applicability and, where necessary, adapt them to new legal framework conditions. The EMD has been subject to an evaluation process of this kind since 2015. On 7 May 2018, the EU Commission presented a working paper with the results of the evaluation. It comes to the conclusion that the EMD can fundamentally comply with the assessment criteria of relevance, effectiveness, efficiency and coherence (interaction with other directives). This means that, in principle, the EMD is flexible enough to react to the latest developments in terms of the digitalisation of mechanical engineering, which has become increasingly important in the industry.

Notwithstanding, it becomes clear that the EMD in its current version could easily reach its limits when it comes to future technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT). For example, autonomous AI robots represent an increased risk, a potential hazard which is not necessarily completely reflected in the safety targets of the current version of the EMD. The systems

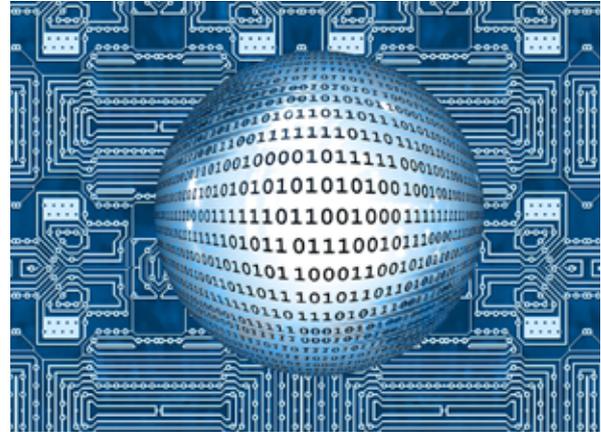


Image: Pixabay

are also more prone to tampering and hacking due to increasing digitalisation and networking. An attack on central or decentralised IT structures can quickly turn from a security risk to a safety risk.

Security by design

Leading experts from the fields of safety, security and compliance are in agreement in their joint assessment of future structures that the resulting new risks in this context cannot be caught based on the current product safety philosophy. Currently, manufacturers can only meet the requirements for this new development by analysing and assessing acute potential risks and those which are predictable in the medium term in the risk assessment element of the design process in accordance with the current state of technology. In this context, these are known as “security by design” solutions.

State of the art

The “state of the art” is an important term in the legislation and in standardisation. Section 1, paragraph 2 no. 5 of the Product Liability Act states: “The manufacturer does not have to pay compensation if the fault could not have been detected based on the state of knowledge and technology at the point at which the manufacturer initially sold the product.” At this point, it becomes very clear that this ‘technology clause’ plays an important role not only in a technical context, but also in a legal one, as in both cases (technical/legal) it is used to define the starting point for the further proceedings.

The “state of the art” describes the developed stage of



Image: Pixabay

technical feasibilities at a given point in time, based on the secured findings of science, technology, and experience (cf. DIN EN ISO 45020). In selecting an appropriate technical solution based on the “state of the art”, economical aspects initially play a relatively subsidiary role, but they are not entirely excluded from the decision-making process. So financial aspects can be taken into consideration if they are not contrary to the safety objectives set out in the relevant directive. In the case of the Machinery Directive, this would mean that financial aspects only are allowed to have an impact inasmuch as they do not jeopardise the health and safety of the subsequent operator or user.

Proposal for new Machinery Ordinance

In accordance with the results of the EMD evaluation, the EU has begun work on a follow-up assessment, which could lead to a proposal for a new Machinery Ordinance by as early as the middle of next year. It would be conceivable that this could be passed in 2022, which would possibly make applying it mandatory as of 2023, based on the current plans.

The important points covered by a new version of the EMD include:

- Clarification of the area of application, especially delineation to the Low Voltage Directive, Pressure

Equipment Directive and other directives,

- Specification of definitions of terms, e.g. “unfinished machine,”
- Adaptation to the NLF (New Legislative Framework), e.g. definition of economic stakeholders and their obligations.

However, there is also one clearly positive aspect to the evaluation: The EMD makes buying and selling machines within the EU considerably easier. In mechanical engineering, this kind of free, consistent transport of goods would not be possible without the Machinery Directive and its associated contracts and agreements. So, the added value remains undisputed for the Member States of the EU.

Fixed-position safety – two-handed switches in accordance with DIN EN ISO 13851:2019-11

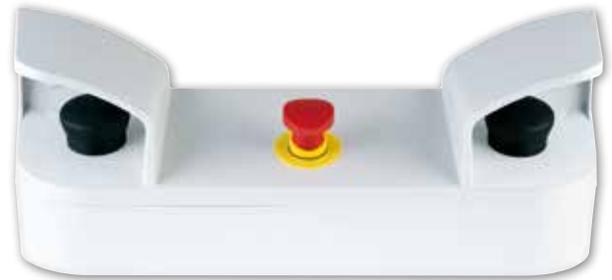
DIN EN 574 for two-handed switches will be replaced by DIN EN ISO 13851:2019-11

Two-handed control panels are a safe and practical solution for securing machines requiring manual insertion and removal. They ensure that both hands of the person triggering a control command for a hazardous movement are in a fixed position. Two-handed control panels and the correct distance to the hazardous movement prevent the operator being able to get enmeshed in hazardous movements after starting the machine.

The requirements and design principles for two-handed switches are defined in the harmonised European type B2 standard DIN EN 574. In the near future, this standard will be replaced by the new ISO 13851:2019. Apart from the fact that there is now a standard for two-handed control panels not only at a European level but also an international one, the standard has only changed in one important point to its predecessor references to the area around the safety-related parts of the control system have been reworked. If, in future, a safety controller is used to evaluate the signals from a two-handed control panel, standards ISO 13849-1 (General Design Principles) and ISO 13849-2 (Validation) are applicable.

Emergency stop button in accordance with EN ISO 13850

Various technical solutions are conceivable for a fixed position for this “non-separating safety device”. The requirements depend on the specific machine application and the role of the operator. If the machine-specific type-C standards do not state specific requirements for the safety level of a two-handed switch, an individual risk assessment must be carried out for the selection and design of the model.



The Schmersal Group offers various designs of two-handed control panels, e.g. with housings made of die cast lightweight metal or plastic. Up to eight additional command and signalling devices can be fitted to the centre section of the folding housing. Two-handed control panels are normally fitted as standard with an emergency stop button in accordance with EN ISO 13850. The two-handed control panels are also designed, as required by ISO 13851, to prevent bypassing or manipulation of the safety function (control elements) by simple means, such as hands, elbows, stomachs, hips, upper thighs or knees. Various stands are available as accessories.

tec.nicum offers professional support on carrying out risk assessments, safety analyses of your existing systems or carrying out safety analyses on existing machines.

Validation in accordance with DIN EN ISO 13849-2

An important standard which gets too little attention

In mechanical engineering, it is often necessary to secure machines by incorporating safety-related control functions. DIN EN ISO 13849 part 1 is a central standard for the construction and design of “safety-related parts of controllers”. By contrast, part 2 of this standard, which defines the approach for targeted validation of safety functions, still gets too little attention. In fact, validation is the first evidence of suitability relative to the actual application purpose. Therefore, validation in accordance with DIN EN ISO 13849 is very important to the overall CE conformity assessment process.

DIN EN ISO 13849 part 2 defines the validation process for the safety functions incorporated into the machine. The term SRP/CS (safety-related parts of a control system) is also used in this context. The validation process must conclusively demonstrate that the design of the SRP/CS complies with the safety requirements of DIN EN ISO 13849-1.

The validation process consists of various steps and makes a fundamental distinction between verification and validation. Verification consists of analysis and tests on SRP/CS and parts thereof in order to ascertain whether the results of a design process meet the specifications for this phase, i.e. whether the switching layout corresponds to the design, for example. The key question is whether the Performance Level (PL) achieved at least meets (or exceeds) the Performance Level required (PL_r). If this is not the case, the design can be adjusted. Evidence of suitability for the actual application purpose is known as validation. One of the elements at this phase is an error simulation, which aims to demonstrate that the system moves to a safe condition in accordance with the specifications and that there are no new hazards as a result.



Independent testers

Verification and validation can be carried out based on analysis or based on a combination of analysis and testing. As a general rule, the whole validation process should be carried out by independent persons, i.e. people that were not directly involved in the design and construction of the SRP/CS. However, testing by a third party is not strictly necessary. The IFA Institute¹⁾ provides recommendations on the principle that the degree of independence should be commensurate with the risk, i.e. the PL_r.

The validation process set out in DIN EN ISO 13849-2 also stipulates that a validation plan should be drawn up. This plan describes the requirements and objectives of all activities to be carried out and the means for validating the defined safety functions, categories and Performance Level, including, for example, specifications for safety functions, a document list, references to applicable

testing standards, etc. In order to prepare for the validation process, extensive documentation also needs to be collated, including circuit diagrams, error lists, user information, etc.

The categories classify the SRP/CS with respect to their resistance to faults and their behaviour in the event of a fault. They are also the starting point for determining failure probabilities and PL.

Another step in the process is the validation of measures to avoid systematic failures, for example, by means of fault analysis, known as Failure Mode and Effects Analysis (FMEA). In addition, the performance and interference immunity of the SRP/CS to environmental influences such as mechanical strain or temperature fluctuations must be validated.

For the validation of safety-related software, on the one hand, it checks whether the requirements for the safety-related software specification for functional behaviour and the performance criteria (e.g. time-related specifications) have been correctly implemented. On the other hand, tests are carried out in order to check how errors are detected and controlled by the software. At the end of the analysis, the correct estimation of the PL is checked, and a validation carried out on the question as to whether a combination of safety-related parts achieves the Performance Level defined in the design process. A validation report is then drawn up.

Benefits of validation in the design process

If the risk reduction is based on using a safety-oriented controller, then achieving a Performance Level is necessary but not sufficient. Only documented validation is sufficient evidence that the defined objective has been achieved to an acceptable extent.

Early consideration of validation in the design process can improve economic viability, as potential errors are discovered at an early stage and there is no further necessity for a subsequent redesign of the SRP/CS.

The validation does not have to be carried out by third parties, but it can be helpful to involve external experts who have an objective view of the situation. tec.nicum, the service division of the Schmersal Group, offers both one-off services required in line with the validation process and support throughout the whole process.

1) IFA – Institute for Occupational Safety and Health of the German Social Accident Insurance



DIN EN ISO 14119

Interlocking devices with guard locks and their safety functions

The standard DIN EN 1088 “Safety of Machinery – Interlocking devices associated with guards” was previously applicable for all machines with safety doors. Its successor, DIN EN ISO 14119, was published in early 2014, this describes guidelines for the design and selection of interlocking devices. This article aims to shed light on the aspect of the safety functions of a guard lock, as there is ongoing discussion about the actual safety functions that machine constructors need to evaluate based on their risk assessment.

Compared to DIN EN 1088ⁱ, there were a few changes introduced in DIN EN ISO 14119ⁱⁱ, such as a clear allocation and designation of the construction types of interlocking devices, description of the technologies used including advantages and disadvantages and, in particular, requirements relating to reducing opportunities to tamper with safety equipment.

The norm also provides in-depth coverage of the subject of interlocking devices with guard locks and their safety functions, and of safety considerations.

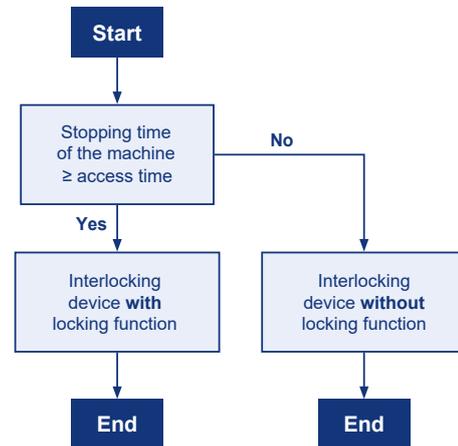
Safety functions of an interlocking device with guard lock

First, machine design engineers need to consider whether a guard lock is required on a safety door. DIN EN ISO 14119 provides plenty of information:

“If the run-on time of the whole system is greater than or equal to the time taken for a person to access the danger zone, then an interlocking device with a guard lock must be used. The access time must be calculated based on the distance between the danger zone and the safety equipment, together with the approach speed. The approach speed of the person and the response time of the controller must be taken into consideration.”

For machines and equipment where it is not possible to shut down a hazardous movement immediately, e.g. machines with run-on movement, “Interlocking devices with a guard locking function”, as they are called in DIN EN ISO 14119, must be used.

This is shown clearly in the diagram “Determining whether guard locks are required”:



In everyday use, the term “interlock” is often confused with “guard lock”. This refers to the locking in the electrical part of the machine control system. The “guard lock” element holds the door in the closed position by means of a lock or electromagnetic forces. Guard locks are often used for process safety. In this case, the guard lock is only used to protect against interruptions in the working process and the control of the guard lock plays a subordinate role. So, in this application, only the locking part of the guard lock is considered from a safety perspective and included in the safety circuit.

Two safety functions

An interlocking device with guard lock therefore consists of two parts, which need to be considered separately and incorporated into the safety circuits for the controller in accordance with the risk assessment. DIN EN ISO 13849:2015 again contains references to “Controllers in accordance with DIN EN ISO 13849-1ⁱⁱⁱ or IEC 62061^{iv}”.

a) Interlocking devices

Even when part of a guard lock system, electromechanical safety switchgear devices cannot achieve higher than PL d on an individual basis, including fault exclusions (see DIN EN ISO 13849-2^v; Table D.8). In order to achieve the PL e, there must be a second switch fitted to the safety door (redundancy).

Interlocking devices working on a contactless basis (see DIN EN 60947-5-3^{vi}, PDDb) can be used up to PL e. Please note the manufacturer’s instructions.

b) Requirements for guard locks

This point is only covered in a very rudimentary fashion in DIN EN 1088. A whole chapter has now been dedicated to it in DIN EN ISO 14119.

Additional requirements for guard locks

Chapter 5.7 of DIN EN ISO 14119 describes the use, execution, monitoring, additional unlocking function and further requirements for guard locks. The performance of the guard locks with respect to “unlocking guard locks” is especially important. This is also a safety function, which is taken into consideration as part of the risk assessment and which the safety-related controller (SRP/CS) must fulfill for the required PL_r or SIL. This PL_r or SIL depends on the application-specific risk assessment and can be lower than for the interlocking device.

“All parts of the device for locking/unlocking the guard lock (control signal) are considered safety-related parts of the guard lock, including the mechanical parts.” This poses the question as to whether two guard locks should be used for PL_e or SIL 3.

See also DIN EN ISO 14119, Chapter 8.4: Note 2:

“The probability of the guard locking function failing and a person entering at the same time is very low. Fault exclusions for the mechanical parts are also possible for the guard locking function in the case of PL_r= e (see DIN EN ISO 13849-2, Appendix A); DIN EN ISO 13849-2 Table D.8 does not apply to guard locks as D.8 applies only to interlocking devices.

In order to justify this fault exclusion, the guard lock must be built and tested to criteria set out in the standard, and it must withstand these tests. The manufacturers of interlocking devices with guard locks specify the guard locking forces on the datasheet and on the nameplate. It is up to the manufacturer of the machine to determine what guard lock and what guard locking forces the safety door actually requires.

Another point which should be highlighted is the control (unlocking) and position monitoring of the guard lock magnets (locking device). It goes without saying that a machine fitted with an interlocking device with guard lock can only be started once the safety door is closed and locked. This means a position query for both the interlocking device and the lock on the guard lock is required. Conventional guard locks are designed to be safe against erroneous closure.

(Safe against erroneous closure is given when the connection between the locking system and the contact allows monitoring of the position of both the lock and the guard lock with a single device. The lock and the interlocking device are only effective when the actuator is introduced into a guard lock. The machine can be authorised to start.)

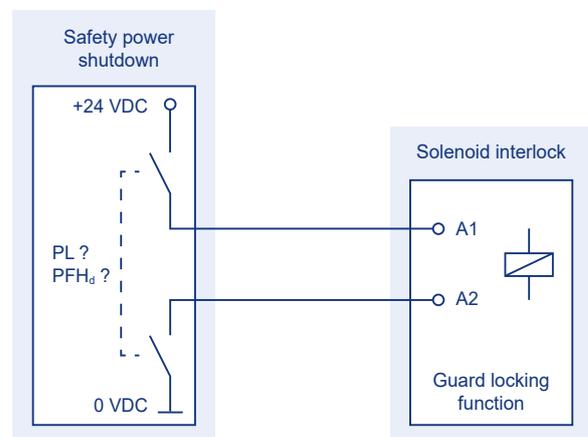
The way that the guard lock unlocks must be assessed in line with the risk assessment. The aim is to prevent a guard lock unlocking erroneously, thus enabling access to the hazardous movement. As the unlocking for conventional guard locks is generally introduced from the machine controller component, this part represents a safety function if required by the risk assessment. The safety chain must be designed accordingly.

This includes:

- Detection of the standstill in the technical controller component (motion monitoring, time delay, position monitoring, etc.)
- Processing of logical signals and
- Controlling the guard lock (one channel or two)

So, the performance of a guard lock does not depend on the guard locking forces alone. Both the controller component and the cable routing also play a role. In case of a two-channel control a fault exclusion can be assumed for the locking device on the guard lock because of the safe energy isolation from outside. In this case, the locking device on the guard lock does not contribute to the failure probability of the unlocking function.

The safety level of the unlocking function is thus determined exclusively by the external safe energy shut-down on the controller section.



If guard locks are controlled on a single-channel basis, then the maximum which can be achieved for this safety function is PL d / SIL 2.

IN SHORT: In principle, the functionality and use of an interlocking device with guard lock is very easy to understand. But the devil is in the detail. Essentially, the recommendation is to study the relevant standards and their requirements if using an interlocking device or devices with guard lock. But it is always possible to take external advice: The experts at tec.nicum can provide manufacturer-neutral consultancy on this subject.

ⁱ DIN EN 1088: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection

ⁱⁱ DIN EN ISO 14119: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection (ISO 14119:2013); German version EN ISO 14119:2013

ⁱⁱⁱ DIN EN ISO 13849-1: Safety of machinery – Safety-related controller components – Part 1: General design principles (ISO 13849-1:2015); German version EN ISO 13849-1:2015

^{iv} DIN EN 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (IEC 62061:2005 + A1:2012 + A2:2015); German version EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015

^v DIN EN ISO 13849-2: Safety of machinery – Safety-related controller components – Part 2: Validation (ISO 13849-2:2012); German version EN ISO 13849-2:2012

^{vi} DIN EN 60947-5-3: Low-voltage switchgear and controlgear – Part 5-3: Switchgear and controlgear – requirements for proximity switches with defined behaviour under fault conditions (PDDb) (IEC 60947-5-3:2013); German version EN 60947-5-3:2013

tec.nicum on tou – dates for 2020



The “tec.nicum on tour” bus is off around the country again! For 2020, there are 13 dates for the half-day Lunch & Learn seminars, including one in Austria.

tec.nicum on tour 2020 has three topics on the agenda:

- Machine safety and product liability: Current information and details on the law and standards
- Brief introduction to new products from the Schmersal Group
- Human-robot collaboration: Safety-related challenges in everyday design

We recommend signing up early, as there are limited spaces available at each location.

You can find the agenda, the timetable and the registration form here:

www.tecnicum.com/academy/tecnicum-on-tour/

We look forward to your participation!

25/02/2020 Schwerin
 26/02/2020 Achim
 24/03/2020 Bregenz (Austria)
 25/03/2020 Asperg
 29/04/2020 Bad Kreuznach
 07/05/2020 Leipzig
 16/06/2020 Wuppertal
 08/07/2020 Neu-Ulm
 10/09/2020 Münster
 29/09/2020 Nuremberg
 13/10/2020 Kranzberg
 10/11/2020 Wettenberg
 07/12/2020 Dresden

The label on this product guarantees responsible treatment of the world's forests.

The greenhouse gas emissions released during the production of this catalogue have been offset through investment in the „LAYA energy-efficient wood stoves“ project in India.



Publisher:

tec.nicum

K.A. Schmersal GmbH & Co. KG

Möddinghofe 30

42279 Wuppertal

Phone: +49 202 6474-932

info-de@tecnicum.com

www.tecnicum.com