



EC MACHINERY DIRECTIVE

News on the subject:

“Safety of Machinery and Machine Control Systems”

– Issue 36/01/13 –

Dear Customer,

This issue of MRL News may be seen as a special edition, because it is the last to be edited by the undersigned who retired on 31.12.2012.

In future the MRL News as well as the Schmersal tec.nicum will be managed by my successor and colleague Uwe Wiemer. Mr. Wiemer (47) is a machinery construction graduate (from the RWTH Aachen) and has close ties with the subject of “machinery safety”; this includes the many years he has worked for Schmersal, as well as his additional qualification as TÜV Rheinland-certified Functional Safety Engineer. Therefore you can be quite certain that the new assignments are still in good hands – both in terms of technical competence and motivation.

He was already responsible for creating the 2013 tec.nicum programme, which we will be happy to send you if you do not have it yet. Once again we have put together a “mix” of seminars for 2013, some of which deal with cross-cutting issues while others investigate particular problems in depth. There are also items specifically for newcomers who want to learn about the requirements of functional machine safety.



Please use the [on form on page 34](#) or visit our website at www.tecnicum.schmersal.com if you would like further information about the 2013 tec.nicum programme.



This issue of MRL News also offers a mix of subjects related to functional safety (see the [Table of Contents on Page 3](#)). Among other things we focus on the limitations of EN ISO 13849, the implementation of RESET signal processing and a ruling from the Regional Court of Stuttgart concerning “Liability for faulty machinery”.

As always we wish you interesting reading!

The undersigned is leaving “with a tear in his button hole” [1] and wishes you all the very best and GOOD LUCK at all times!

Wettenberg, 31st December 2012/ January 2013

With best regards,

A handwritten signature in blue ink, appearing to read 'F. Adams', with a stylized arrow-like shape to the left.

Friedrich Adams

[1] According to the BROCKHAUS dictionary, this is a colloquial figure of speech that inverts “with a flower in his buttonhole and a tear in his eye” and expresses the fact that somebody is much moved. In short it was a wonderful time!

Disclaimer

The information and recommendations in “MRL News” are provided to the best of our knowledge and in good faith. Nevertheless they do not absolve you from your responsibility to check and weigh up different aspects. With the exception of any opposing and compelling statutory provisions, we shall assume no liability for any errors and misunderstandings arising from the presentation.

Table of Contents

<u>Limitations to the application of EN ISO 13 849</u>	<u>4</u>
<u>No “paper tiger”: product liability in the case of faulty machinery!</u>	<u>10</u>
<u>RESET with edge detection: “yes”, but which one?</u>	<u>15</u>
<u>Risk assessment: the essential points of machinery safety</u>	<u>21</u>
<u>Guide to MD 2006/42/EC</u>	<u>23</u>
<u>Hazardous products 2012 – information on product safety</u>	<u>24</u>
<u>News from the Schmersal Group</u>	<u>26</u>

Published by:

K.A Schmersal GmbH & Co. KG

Mödinghofe 30
42279 Wuppertal
Germany

Telephone: +49 (0)202 6474-0

Fax: +49 (0)202 6474-100

Email: info@schmersal.com

Internet: www.schmersal.com

Editor and responsible person under German Press Law (ViSdP):

Friedrich Adams, c/o K.A. SCHMERSAL Holding GmbH & Co. KG,

Mödinghofe 30, 42279 Wuppertal, Germany; Email: tec.nicum@schmersal.com

Gesamtherstellung: flick-werk – Werbe-Grafik Heinz Flick, 35075 Gladenbach,
Germany / Druckhaus Waitkewitsch, 36304 Alsfeld, Germany



Limitations to the application of EN ISO 13849

You have already been able to read frequently in MRL News and elsewhere that the standard EN ISO 13849 (Safety Related Parts of Control Systems) concerns a specific industry standard for machinery construction (teaser: Safety of Machinery). The same applies to EN IEC 62061 (Functional safety of safety-related electronic and programmable electronic control systems). The indirect force behind EN ISO 13849 and direct force behind EN IEC 62061 was EN IEC 61508: Functional safety of electrical, electronic and programmable electronic systems (E/E/PES).

But what are the specific features of EN ISO 13849 and EN IEC 62061 in terms of machinery construction?

Without claiming to be exhaustive, a few aspects are examined below that might be of interest to some readers because they also highlight the limitations to the application of both standards. The examination is geared principally to EN ISO 13849, however. The statements can be transferred analogously to EN IEC 62061.

Minimum test rate per year

In addition to the architecture (control category/CC), hardware reliability ($MTTF_d$) and adequate measures to prevent so-called common cause failures (CCF), the efficacy of fault detection measures (diagnostic coverage/DC) has a very important role to play in the case of “higher” performance levels (which refers here in particular to PL “d” and “e”).

Depending on the design of a safety-related part of a control system (SRP/CS), fault detection measures may take place regularly and automatically – typically using electronic and programmable systems – or when parts are requested (actuated) – as is the case in particular with traditional technologies such as electromechanics, hydraulics and pneumatics. How else can one find out with reasonable effort whether a function is working or not but by actuating it (in other words testing it). (By the way there is no cause for alarm: in the case of an error we generally have redundant architectures).

With respect to the question of the impact of the test rate on the PL, an “official” statement has now been made (see figure) with a so-called **Recommendation for Use (RFU)** from the EU committee “EUROPEAN CO-ORDINATION OF NOTIFIED BODIES”.

The EUROPEAN CO-ORDINATION OF NOTIFIED BODIES is a notified test body committee that permits an exchange of experience so as to achieve a harmonised European interpretation of specific safety-related issues. This committee is of particular significance in machinery construction for products that fall within Annex IV of MD 2006/42/EC. If you are interested in finding out more about this, google [1] “RFU – Recommendations for Use” which will take you to the European Commission/Enterprise and Industry website with access to these RFUs. They are divided into “horizontal” and “vertical” RFUs, whereby the latter in particular (categorised according to the different products in Annex IV) may well be of interest to those of you who are affected by Annex IV.

CO-ORDINATION OF NOTIFIED BODIES Machinery Directive 2006/42/EC + Amendment		Page 171 of CNB/M13.028/RVE Rev 03	
RECOMMENDATION FOR USE		CNB/M13.028 Revision 03 Language: E	
Date of first stage: 09/05/2008	To be approved by:	Approved on:	
Origin: VGI13 Full quality assurance	<input checked="" type="checkbox"/> Vertical Group	17/09/2007	
	<input checked="" type="checkbox"/> Horizontal Committee	10/06/2008	
	To be endorsed by:	Endorsed on:	
	<input checked="" type="checkbox"/> Machinery Working Group...	08/01/2009	
Question related to: Directive 2006/42/EC Article:	EN/EN:	Other:	
Annex: X clause 2.1 - 3 rd indent, clause 2.3 - 3 rd paragraph	ESR (1):	Other clause:	
	Clause:		
	CEN TC concerned:		
Key words: technical file, sample, manufacturing facilities, inspections, audit plan			
Question: What is the role of the Notified Body in the review of the technical file?			
Solution: The role of the Notified Body (NB) is to check whether the technical file fulfils the EHSR of the MD and to verify that the quality system can produce the product in conformance with the technical file. It is not the responsibility of the NB to test the product. When studying the technical file(s) submitted by the manufacturer, the NB prepares the audit and possible inspections at the places of design, manufacture, inspection, testing and storage. This will allow him to send an audit plan to the manufacturer before his assessment. There are two steps in the review of the technical file. 1. The NB will make a specific analysis of one technical file duly selected for each category of machinery and provided by the manufacturer in the context of section 2.1 - 3 rd indent. 2. During the audit, the NB will also review the existing technical files according to section 2.3 - 3 rd paragraph. The main purpose here is to check that the existing files are established with the same approach as the sample selected for deeper analysis. Note: For an annex X conformity assessment there will be no sample of the type of machinery to be examined at the site of the NB. All checks of samples to confirm compliance with the technical file have to be witnessed at the manufacturing facilities. A precondition to do these checks is the knowledge of the technical file of the representative model.			
(1) Essential safety requirement Note: According to point 6.6 of the Guide of the implementation of directives based on the New Approach and the Global Approach, the notified bodies apply as general guidance this recommendation for use.			
Page 230 / 239			

The pertinent question that was addressed above was: *What are the minimum requirements concerning the frequency of tests for failure detection in a safety-related system with 2 channels with electromechanical outputs (relays or contactors)? ... And the answer to this: A functional test (automatic or manual) to detect failures shall be performed within the following intervals:*

- a) at least every month for PL e with Category 3 or Category 4 (according to EN ISO 13 849-1) or SIL 3 with HFT (hardware fault tolerance) = 1 (according to EN 62 061);
- b) at least every 12 months for PL d with Category 3 (according to EN ISO 13 849-1) or SIL 2 with HFT (hardware fault tolerance) = 1 (according to EN 62 061).

The requirement for a minimum test rate of 1 × per month for PL “e” will not be critical in the vast majority of cases, as there is generally only a required PL ($PL_{r(\text{required})}$) of “e” with frequent demand of the safety function. For example reference may be made here to the risk graphs in accordance with Annex A of EN ISO 13 849-1 (Parameter F2, i.e. with

[1] Since its inclusion in DUDEN, the verb “to google” has been understood as using an internet search engine to find something out, to research etc. This can be in Google itself, or may involve an alternative search engine.

frequent to continuous presence in the danger zone and/or lengthy duration of exposure to danger; this is translated/interpreted as at least $1 \times$ per hour).

By contrast, application of EN ISO 13 849 would be limited when the test rate of an SRP/CS is less than $1 \times$ per year and a PL_r of “d” is required.

Admittedly this is rather improbable because the typical safety functions in machinery construction are integrated in process sequences and will therefore be tested (demanded) more frequently (through actuation) than $1 \times$ per year.

Theoretically a lower test rate could occur in the case of emergency stop functions because ideally these would not be actuated at all (as this is an additional precautionary measure, in other words a *belt and braces approach*). But it is not difficult to get round this figure by simply conducting a functional test of devices $1 \times$ per year (so that this would be a subject to address in the operating manual).

But what if ...?

Problems of this nature can indeed arise, for example in the case of power machines (turbines etc.) which also cannot be tested at will by means of actuation (a problem that may generally exist with traditional technology and high availability systems, loc. cit.). Consider here the emergency stop function or valve monitoring etc.

If the question of test rate is actually critical, one should check whether the safety standard EN IEC 61 511 [2] (or EN IEC 61 508 directly) might be a (more) suitable alternative. This recognises the so-called Low Demand Mode for applications of this kind (i.e. with tests $< 1 \times$ per year compared to High Demand Mode with tests $> 1 \times$ per year) and in such cases “works” with so-called $PFD_{(d)}$ values (Probability of ^{dangerous} Failure on Demand) in place of $PFH_{(d)}$ values (Probability of ^{dangerous} Failure per Hour). On the basis of EN ISO 13 849, irrespective of a 2-channel function, the result would in fact only be PL “c” (because of a DC of 0 in this case). In other words: we would have to deal with a limitation of EN ISO 13 849 in this case.

The question posed frequently in this connection of whether the two values ($PFH_{(d)}$ and $PFD_{(d)}$) can be mutually interchangeable must in principle be answered in the negative, because the calculation methods and approaches are different. At best a formula can be used to convert a $PFH_{(d)}$ value to a $PFD_{(d)}$ value (but not vice versa – see above). We can, however, assist Schmersal customers who work with $PFD_{(d)}$ values for their applications with the necessary inputs for this (in the form of a TÜV Rheinland report on research

[2] Functional safety: safety-related systems for the process industry (www.beuth.de)

into the failure rates of Schmersal electromechanical switchgear in the “low demand” operating mode. Please contact Frank Schmidt (Email: fschmidt@schmersal.com; phone number +49 (0)202 6474-867) if you need specific information on this subject.

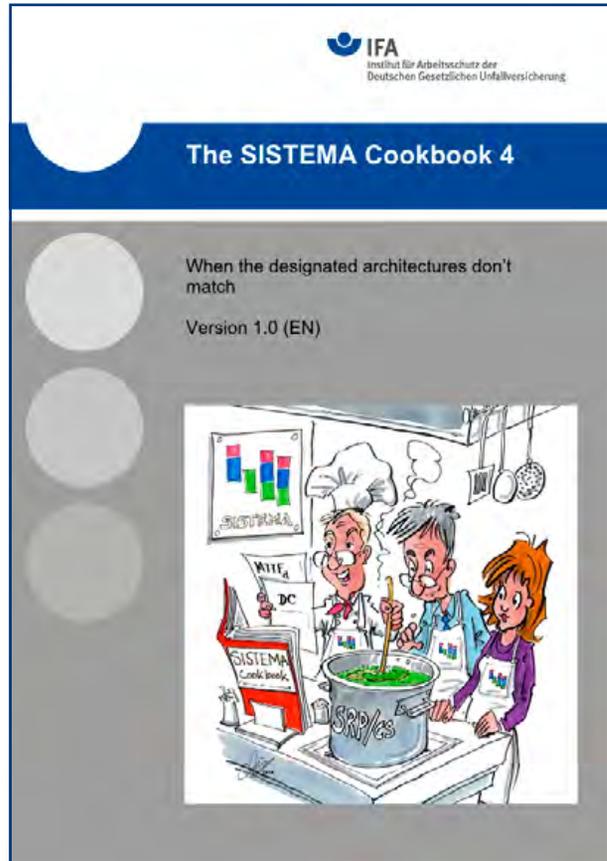
EN ISO 13849: link to the so-called designated architectures

A limitation to the application of EN ISO 13849 may also arise, however, if the so-called designated architectures are not (cannot be) realised. This refers to substantial derogations from the framework conditions for control categories B, 1, 2, 3 and 4 (see figure below). Whilst it is possible to deviate from this, different concepts based on a different safety standard may need to be assessed (typically in accordance with EN IEC 61 508). For example, think of 3-channel architectures with limited fault detection, of single channel architectures with highly dynamic testing or of architectures which do not use so-called tried and tested components, which could apply as equivalent for a simple PL “c” etc.

<p>Features and properties of CC B and 1:</p> <ul style="list-style-type: none"> • 1 channel system • Failure can lead to loss of the safety function • CC B: use of <u>state of the art devices</u> and application of <u>basic safety principles</u> • CC 1: use of <u>tried and tested components</u> and application of <u>basic and tried and tested safety principles</u> • Suitable for PLs “a” to “c” 	<p>Features and properties of CC 2:</p> <ul style="list-style-type: none"> • 1-channel system • Failure can lead to loss of the safety function, however the probability is very low due to the subsequent test demands • Test demand: $\geq 100 \times$ more frequent than $1 \times$ SF demand + 2nd shutdown path of “reduced” quality • Use of <u>state of the art devices</u> and application of <u>basic and tried and tested safety principles</u>, alternatively \rightarrow <u>safety components</u> • Suitable for PLs up to “d” 	<p>Features and properties of CC 3 and 4:</p> <ul style="list-style-type: none"> • 2-channel system • A failure does not lead to loss of the safety function • <u>Fault exclusions possible</u> • Use of <u>state of the art devices</u> and application of <u>basic and tried and tested safety principles</u>, alternatively \rightarrow safety components • CC3: fault detection: “yes” but not all faults must be detected and no consideration of fault accumulation • CC4: all faults must be detected, fault accumulation consideration can be substituted • Suitable for PLs up to “e”
<p>PS: See EN ISO 13849-2:2003 for basic and tried and tested safety principles and tried and tested components</p>		

A new SISTEMA Cookbook (the fourth) with the title “When the designated architectures don’t match” deals specifically with this subject. It says in the introduction:

... the probability of a dangerous failure per hour in accordance with the simplified method described in EN ISO 13849-1 is that the control system that is implemented must correspond to one of the designated architectures for the Categories. If this is not the case, the simplified method cannot be used and a more involved method, such as Markov modelling, is generally required. On occasions however, a minor – conceptual – change is sufficient to enable the architecture to be modelled to a designated architecture. Examples of such cases are described below. ...



In other words, irrespective of whether or not you use SISTEMA software when implementing EN ISO 13849-1, you can see what (and which derogations) is possible under the umbrella of EN ISO 13849. We think it is especially helpful that two possibilities are shown for achieving PL “d” for control category 2, even if it not possible to achieve a ratio of demand rate to test rate of $\geq 1 : 100$. 2 cases are illustrated:

- Case 1: The ratio of the test rate to the demand rate upon the safety function is lower than 100 but at least 25. Calculation is then possible with use of PFH allowance.
- Case 2: Fault detection and fault response are triggered by the demand upon the safety function and are faster than the occurrence of the hazardous situation.

If you are interested in this publication from the Institute for Occupational Health and Safety (IFA) from the German Statutory Accident Insurance, google “SISTEMA-Kochbuch 4” or go to the website www.dguv.de/ifa/en/prasoftwa/sistema/kochbuch/sistema_cookbook4_en.pdf www.dguv.de/ifa/13849.

System behaviour

Connected to the application range or any limitations to use, it is similarly important to point out that EN ISO 13 849 (and EN IEC 62061) only concern so-called shutdown systems, i.e. in the case of a fault, e.g. a hazardous movement, a safe state is achieved by a shutdown. These systems are typical for machinery construction but are not universally suitable, particularly not for high availability applications, e.g. in chemical and process engineering. This is illustrated by the exaggerated (and admittedly not very funny) fact that this is the reason why there are no emergency stop control devices in aircraft.

Rather there are so-called fault tolerant (fail-operational) systems for these specific applications. Examples are voting systems, i.e. where the system continues to work in the event of a fault. The system does not assume any fault status, but remains operational. In order to achieve this, the system must consist of at least 3 systems which must likewise have fault diagnostics and fault elimination. By comparing the systems to each other it is possible to ascertain that a fault is present and also which system has the fault. This system design can also be described as fault tolerant (author's remark: the above explanation has been copied from somewhere, but the source is no longer known).



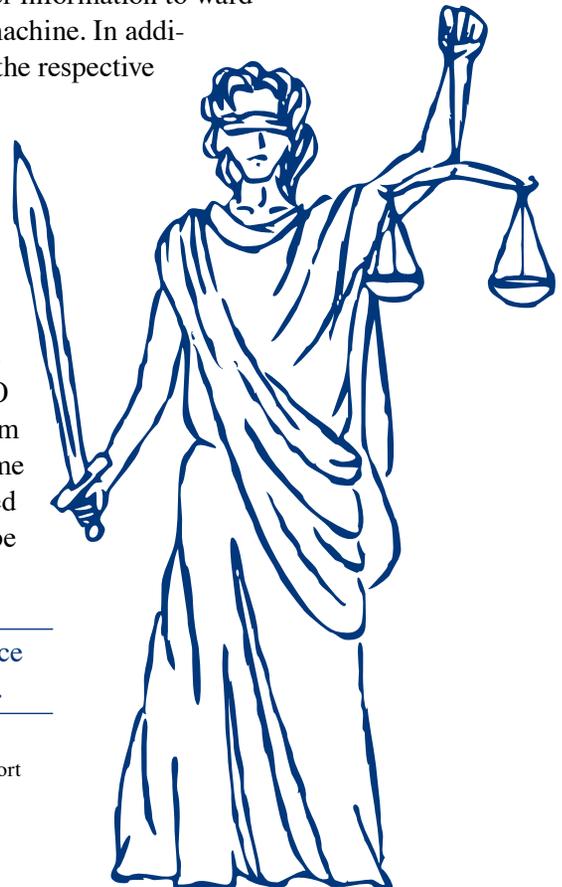
No “paper tiger”: Product liability in the case of faulty machinery!

The Regional Court of Stuttgart has upheld the action of an employer’s liability insurance association against a machinery manufacturer for 2/3 of the damages sustained through an industrial accident on a machine that blatantly failed to comply with the requirements of the Machinery Directive. It would appear in this case that there had neither been a risk assessment nor did the design correspond to state of the art safety technology. Ironically enough, a “perfect” declaration of conformity was submitted. The Regional Court of Stuttgart calculated the contributory negligence of the injured employee, who probably reached out without thinking to retrieve a cloth lost during cleaning work and whose hand was then pulled into the machine, at 1/3.

If you are interested in the details of this case, the ruling of the Regional Court of Stuttgart dated 10.04.2012 was covered under Reference No. 26 O 466/10 in NJW-RR 2012 [1], Number 40. (Free access is not possible, but you can read up on it:) Manufacturers of machinery with great danger potential are obliged to take all reasonable and necessary measures through design and user information to ward off dangers that can arise when using the machine. In addition to the expectations of the consumer, the respective level of knowledge of science and technology is decisive for product safety. ... Faults in a machine from EC law (Machinery Directive 98/37/EC, new version 2006/42/EC) incorporated in the Product Safety Law (ProdSG)...

You can also obtain information on the ruling if you google “LG Stuttgart, 26 O 466/10”. You will then see information from the law firm Schator (ProdR-Report, Volume 2012, 4th quarter) with an extremely detailed presentation of the case (which can also be downloaded as PDF).

Sorry, but information taken into reference
are available in German language only.



[1] Neue Juristische Wochenschrift – Rechtsprechungsreport
(New Legal Weekly– case law report)

Below – once again– two interesting items from the KAN-Brief (this time from Issue 2/12). Our selection does not imply that the other subjects covered in this information service are not interesting, merely that they deal with different subjects to those that we concentrate on in MRL News.

The KAN-Brief is a publication from the German Commission for Occupational Health and Safety and Standardization (KAN) which comprises 17 members and unites all relevant institutions in Germany for occupational health and safety (more information → www.kan.de). Funding of KAN is shared by the VFA and the BMAS (VFA: Verein zur Förderung der Arbeitssicherheit in Europa e.V – Association for the Promotion of Occupational Health and Safety in Europe), whose members are commercial employer's liability insurance associations and public accident insurance companies); BMAS: Federal Ministry of Labour and Social Affairs).

Test fingers: tested and found to be too short

A test finger can be used to check whether the enclosure of machines and plant are designed such that persons cannot come into contact with dangerous parts. However an assessment commissioned by KAN [1] has shown that test fingers in accordance with DIN EN 60 529 do not always guarantee this protection.

Enclosures must ensure that persons are unable to touch any dangerous electrical or mechanical parts. A jointed test finger which is intended to simulate a human finger is used to check this. The design of the test finger is set in the standard DIN EN 60 529:2000 “Degrees of protection provided by enclosures (IP Code)” at a length of 80 mm and a diameter of 12 mm.

In the course of the KAN study on anthropometric data in standards [2] it was established that the length of the test finger, which was defined over 30 years ago, no longer corresponds to the anthropometric circumstances in the population. For this reason in June 2011 the ASER Institute [3] was commissioned to check whether the underlying data are still up-to-date. In addition to the length and breadth of the finger, further factors such as a realistic series of joint angles and the influence of fingernails were to be examined. The first step was to compare current distributions of index finger length and breadth with the dimensions of the test finger. In addition to German data, data from

[1] www.kan.de/fileadmin/user_upload/docs/sonstige/prueffinger.pdf

[2] KAN-Bericht 44 „Anthropometrische Daten in Normen“ (anthropometric data in standards); 2009; www.kan.de → Webcode d3045

[3] Institute for Occupational Medicine, Safety Technology and Ergonomics, Wuppertal

other countries based on ISO/TR 7250-2 [4] were incorporated in the evaluation.

Test fingers must be longer

The result of the assessment is that the **diameter** of test fingers provides a high degree of protection: the finger width of almost all adults both in Germany and in other ISO countries reveals measurements between 14 and 18 mm, considerably larger than the 12 mm diameter of the test finger. This guarantees that enclosure openings which the test finger is unable to penetrate are also inaccessible to the human finger.

The situation is different in the case of the test finger **length**, however: the current length of 80 mm means that full protection is not assured for a considerable percentage of the population in Germany. If the distributions of index finger length recorded in other countries are taken into account, this reveals an even greater deviation from the length of the test finger. From an anthropometric perspective, therefore, the test finger must be extended.

The assessment concludes that a test finger length of over 90 mm is needed to allow for the actual index finger length of the population in the countries looked at. To make allowances for the length distribution of all countries where possible and for the potential penetration depth of index fingers, which is longer than the measurement in the standard due to the skin fold at the base of the finger, extension by 15 mm is proposed. In order for fingernails of different lengths to be included in the design of the test finger, a further 5 mm must then be added to the length.

EN ISO 13 857, which governs the safety distances on machines [5], stipulates a safety distance of at least 120 mm for square openings which can be penetrated by a finger (12 to 20 mm). In order for the test finger also to cover this standard, it must have a total length of 120 mm.

It must also be said that the lengths of the individual test finger joints in accordance with DIN EN 60 529 do not reflect those of actual index fingers. Whereas on the test finger the lowest phalanx (closest to the body) was the shortest, in most people the top phalanx is generally the shortest. A worst-case analysis (long, thin fingers) is however considered sufficient. It is not necessary for different types of test finger to be specified in the standard.

[4] ISO/TR 7250-2 “Basic human body measurements for technological design – Part 2: Statistical summaries of body measurements from national populations of ISO member states

[5] EN ISO 13 857:2008 “Safety of Machinery – safety distances to prevent hazard zones from being reached by upper and lower limbs”

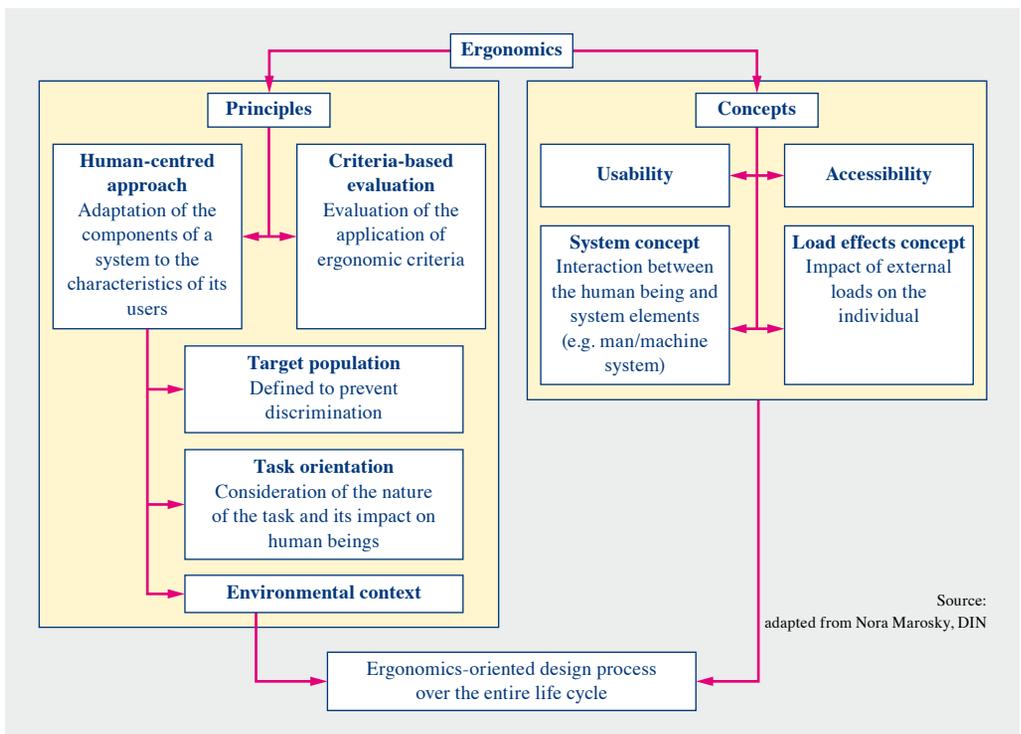
For implementation of the assessment results, the ASER institute proposes the use of a plug-on sleeve to test larger enclosure openings. KAN will discuss with experts in an ergonomics workshop whether this solution is suitable for use in practice and how the results of the assessment can best be implemented.

Dr. Beate Schlutter

Email: schlutter@kan.de

The new DIN EN ISO 26800 basic ergonomics standard

Ticket machines, household appliances, computer keyboards: any device intended for use by human beings should be not only safe, but also easy to reach and use. Irrespective of the environment in which it is used (work, home, leisure), the underlying ergonomic principles are always the same. These principles have now been summarised for the first time for all applications in a single standard: EN ISO 26800, published in November 2011.



DIN EN ISO 26800 “Ergonomics – General approach, principles and concepts” serves as a generic ergonomics standard and was developed in order for the essential principles and concepts of ergonomics addressed by other standards to be placed within a common framework. The standard presents generic principles which are of fundamental importance for the design of products. It also explains four concepts which can be referred to for a better understanding of these principles and for their application (see diagram).

The purpose of the standard is to assure the ergonomic design of systems and products by applying the principles and concepts over the entire life cycle. This means that designers must consider the needs and characteristics of future users from the first product design onwards and give consideration to ergonomics not only during normal use, but also during maintenance and disposal.

In addition, the standard is intended to serve as a basis for the development of more specific individual standards. Reference is made by way of example to certain existing ISO standards governing particular ergonomic aspects.

Load effects model now universally applicable

It is important for ergonomics and for those responsible in companies for the organisation of work that ergonomics standardisation does not develop concepts for the world of work which are divergent or, worse, conflicting. The load effects model was therefore identified in 2009 as the core ergonomic principle of ergonomics standardisation overall. This model is the guiding concept behind DIN EN ISO 6385 “Ergonomic principles in the design of work systems”, the main part of which was developed in 1975, and which has now also been adopted in EN ISO 26800.

Prof. Dr. Sascha Stowasser [6]

Institute for Applied Occupational Ergonomics and Industrial Engineering (ifaa)

Email: s.stowasser@ifaa-mail.de

End of the extract from the 2/12 KAN-Brief

[6] Chairman of the Working Committee “Principles of Ergonomics” in the DIN ergonomics standard committee

RESET with edge detection: “yes”, but which one?

In professional circles there have been arguments for some time about whether signal processing of the trailing edge is exclusively intended (permitted) to ensure compliance with the requirement of Section 5.2.2 of EN ISO 13849-1 – which is that a machine may only be made ready for restarting by releasing the drive element (the RESET button) in its actuated (on) position. This concerns the question of whether other solutions, namely signal processing of the rising edge, would also be acceptable from a safety point of view, and, depending on perspective, which type of signal processing would be better at “managing” any faults. The uncertainty even extends to fears that different solutions might lead to doubts about the conformity assumption. There are also already RESET solutions on the market that offer signal processing of both the rising and the trailing edge within a defined timeframe. However solutions of this kind are bound to cause trouble.

Extract from EN ISO 13849-1 Ch. 5.2.2 ...

...

Following the initiation of a stop command **by a protective device**, the stopped state must be maintained until a manual reset device is actuated and it is safe to restart the machinery. The restoration of the safety function by resetting the protective device interrupts the stop command. If indicated by a risk assessment, this cancellation of the stop command must be confirmed by a **manual, separate and intentional action** (manual reset).

The manual reset function

- must be provided by a separate, manually operated device in the SRP/CS;
- may only be achieved if all safety functions and protective devices are functional;
- may itself not initiate any movement or hazardous situation;
- must be an intentional action;
- must permit the control system to accept a separate start command;
- **may only take place by releasing the drive element in its actuated (on) position.**

The Performance Level of the safety-related parts for the manual reset function must be selected in such a way that the incorporation of the manual reset function does not diminish the requisite safety of the corresponding safety function.

...

Ad-hoc working group

Against this background, a German ad-hoc working group met recently at the initiative of BG Holz und Metall (the employer's liability insurance association for wood and metal) and the DGUV wood and metal department (BGHM FB HM/SB MAF [1]) to introduce clarity to this discourse. In addition to the BGHM, participants at the meeting included representatives of TÜV Rheinland, of the Department of Printing and Paper Machines at BG ETEM (Employer's Liability Insurance Association for Energy, Textiles, Electrical and Media products), of the IFA and some well-known manufacturers of safety components (including Schmersal).

The aim is that this will result in a new technical information sheet from the DGUV wood and metal department (of BGHM), according to which and assuming that there are no substantial further changes, both solutions, i.e. processing the trailing as well as the rising edge of RESET signals, are permissible. This is based on an FMEA (Failure Mode Effective Analysis) of both options which, according to this, are considered to be equal (the main thing is they are "dynamic"), provided that, for reasons of fault detection, the RESET signal is processed in a safety relay module, a safety PLC or an equivalent solution. What is more (and important for us): no changes need to be made to our previous reports to you on this subject.

We will provide detailed information about this as soon as the information sheet is published.

What does this mean in practice?

Firstly: those readers who are responsible for machinery and who do not have any danger areas that people can walk into or which are accessible from behind can lean back and relax; they are not affected by this discussion.

By contrast, if your machinery does have accessible danger areas, you are indeed affected by the subject, because in this case the manual reset function (the RESET) must be regarded as a safety-related part of a control system (with assessment of the performance level etc.).

However please note that it might not be enough to consider the question of the type of edge detection and safe signal processing!

[1] Employer's liability insurance association for wood and metal/DGUV Wood and Metal Department, field of machinery, plant, production automation and design

The RESET button must firstly be installed in a position that makes it possible to oversee the danger area involved in the restart standby (so as to ensure that nobody is still standing inside the machine and could be endangered by the machine suddenly restarting). It is self-explanatory that it must not be installed where it can be reached from inside the machine (keyword: improper actuation).

If the danger areas involved are not transparent, then additional measures are required. These include, for example, the procedure of double acknowledgement (1 × inside the machine and 1 × from outside within a set time frame), the so-called lock-out procedure (i.e. safeguarding with padlocks on the interlock when one is working inside the machine), the use of key transfer systems etc.

Quote from MRL News 30/04/10

Here is an extract from a previous article about this aspect that appeared in the MRL News issue dated 30/04/10, which went under the heading “Risk: unexpected start-up”:

Risk: Unexpected start-up

Yesterday at a recycling plant in Einbeck:

Fatal industrial accident

(Ms). A 43 year old worker old plant operator started up the machine in the usual way, unaware that maintenance work was being carried out. The fitter was then caught up in a worm thread sustaining fatal injuries.

...

Measure: permanently present stop command

The permanently present stop command plays an important role, especially if somebody has to work for a prolonged period in a hazardous area that is difficult for others to see.



“Permanently” is interpreted here in an exemplary manner, i.e. that the starting-up of the machine cannot be set in motion or initiated by any third party. The difficulty in seeing a hazardous area for a third party can occur quickly if one considers linked individual machines, integrated production systems and machine installations.

A simple and therefore more effective means of achieving this aim is offered by moving protective devices (guards, protective grilles etc.) – so-called lock-out tags in the terminology used by the Schmersal group (see Fig 4). These accessories make it possible to secure interlocking devices (safety switches with and without latching) in an open state using padlocks so that renewed actuation of the devices is prevented, i.e. the renewed closing of the moving protective device and renewed starting-up of a machine by a third party is effectively prevented both by mechanical and control-related means.

An embodiment of model AZM 200 electronic solenoid interlocks with lock-out tag SZ 200 is shown in Fig 5.

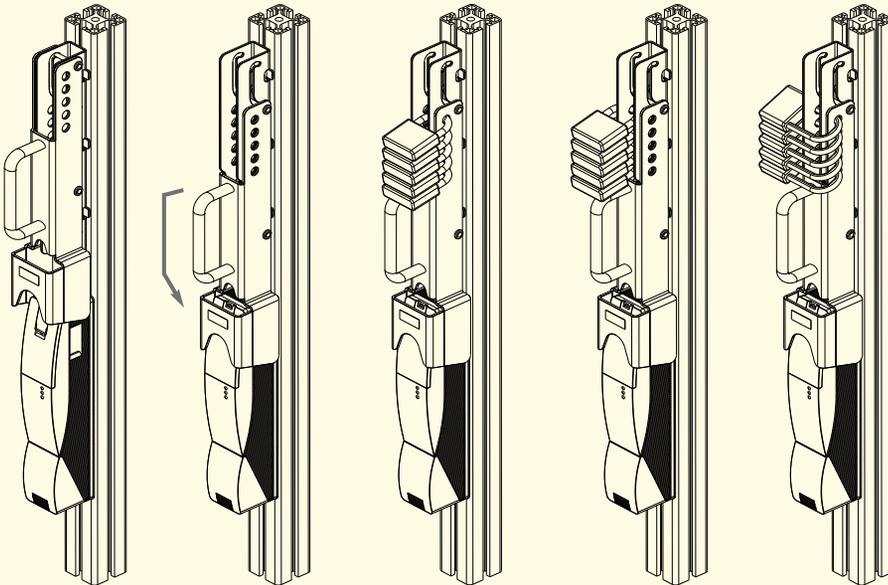


Fig. 5: A lock-out tag (the example depicted here is an SZ 200 as solenoid interlock and safety sensors from the AZ/AZM 200 series) prevents actuation of an interlocking device by enabling the operating staff to protect themselves by latching individually coded commercially available padlocks.

Key transfer systems

Key transfer systems offer intelligent possibilities to protect against unexpected (unintentional) starting-up where special operating modes also need to be performed by operators in the inside of a hazardous area that is difficult to see.

Actuation of a key-operated selector switch firstly ensures that the automatic operating mode is safely interrupted, i.e. the switch is moved from the I to the O position and a contact with positive break opens. Using the key that can only be removed in this position, the operator is then able to actuate a second key-operated selector switch in the inside of the machine (O position → I position) that enables the special mode, whereby in this position the key cannot now be removed. Due to an individually coded closing nobody, apart from the operator himself, can reverse the setting on the outer control panel. The stop command for the automatic operating mode is permanently and safely present.

Diverse embodiments for using the philosophy behind a key transfer system are conceivable. It would, for example, be possible to place an interlock in the intermediate cycle, likewise equipped with a key transfer station, i.e. the key from the external key-operated selector switch would firstly be used to unblock the protective device, whereupon a second key could be removed which could then be used to enable the special operating mode in the inside of the machine (refer to Fig. 6 to get a clearer understanding of this). The restarting of the machine takes place in reverse order.

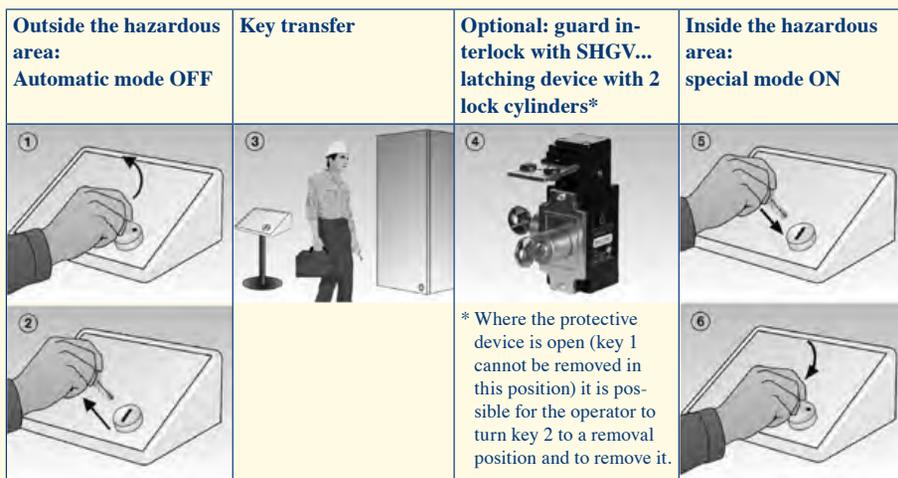


Fig. 6



Other possibilities for using the key transfer system idea to protect against unexpected start-up are provided by the key distribution stations (SVM series) and interlocking devices (SVE series).

Reset using double acknowledgement

These types of additional measures will not be necessary in all cases and – if we consider opto-electronics for example – the protected devices do not always involve moving guards that must be safeguarded using interlocking devices.

For other applications in hazardous areas that are difficult to see, the use of the double acknowledgment procedure comes into question, such as the one illustrated using the PROTECT SRB 100DR safety relay module (see Fig 7).

The function of the module ensures that it is only possible to restart the machine control system

- once the reset or restart button 1 has first been actuated by the operator;
- and – after he has left the hazardous area and if necessary has closed and locked a guard again –
- once a reset or restart switch 2 that is situated outside the plant has been actuated. For executing this “double“ acknowledgement an adjustable timeframe of between 3 and 30 seconds is provided (set via a DIP switch) within which actuation must take place (exclusively in the order button 1 → button 2). The timeframe can be oriented towards operational processes.

If the operator fails to actuate button 1 or to actuate button 2 within the set timeframe, no enabling takes place and the double acknowledgement procedure must be repeated. Further signal processing of the reset signal then takes place via the commercially available safety relay modules such as those from the PROTECT-SRB range, i.e. in the case of the SRB 100DR module this is an upstream device that is implemented with performance level “e”.



Fig. 7

Risk assessment: the essential points of machinery safety

Just how important the implementation (and documentation) of a complete and consistent risk assessment is during and for the design of safe machinery according to the specifications of MD 2006/42/EC is demonstrated not only by the ruling of the Regional Court of Stuttgart (see Page 10), but also more generally by the domination of this subject which might equally be termed “the essential points of machinery safety”.

The requirement to conduct a risk assessment has top priority in Annex I of the EC Machinery Directive and, by being transposed in the product Safety Law (ProdSG), is a mandatory legal provision. But in addition this requirement is substantiated and interpreted in the harmonised standard EN ISO 12 100 (risk assessment - previously EN ISO 14 121-1) and – to aid understanding – in a Technical Report on the subject (TR ISO 14 121-2). Last but not least, there are continuous cross-references to the requirement for a risk assessment in other standards, as well as a great deal of literature on the subject.

A risk assessment is indeed a very complex construct with clear requirements on the one hand, but with configuration scope that the legislator has consciously created via the so-called New Approach guidelines, on the other hand. The boundaries between over-engineering and too little engineering are quite fluid here at times.

In preparation: DIN ISO/TR 14 121-2

The TR on risk assessment referred to above is a very necessary help in this connection when it comes to approaching and understanding this question. However one hears that – at least in Germany there are limits to the interest in it (perhaps because TR ISO 14 121-2 is currently only available in English and is rather expensive at approx. € 135). You can pre-order the German version which is currently in preparation at a more favourable price, however (www.beuth.de → DIN ISO/TR 14 121-2 [1]).

New BAuA-Report on the subject

Interesting information on the subject, both with regard to configuration requirements and configuration scope, can also be found in the new report from the Federal Institute for Occupational Safety and Health (BAuA) which goes by the title “Risk Assessment in Mechanical Engineering”.

Following information is just of interest for our German-speaking readers.
English-speaking readers please refer to
“Guide to application of the Machine Directive 2006/42/EC”.

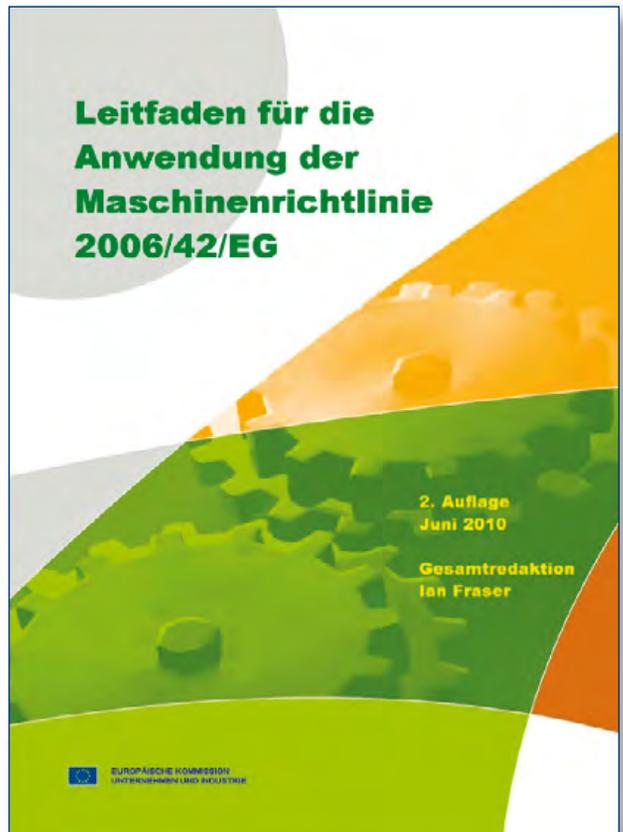
It was about time!

At the end of July 2012 the Federal Ministry of Labour and Social Affairs (BMAS) released the complete German translation of the Guide to Application of the Machinery Directive 2006/42/EC – 2nd edition June 2010”. Before this there had only been partial publications (“recitals” and “articles”) as well as unofficial translations of the English version. However for the important annexes I et seq. to MD 2006/42/EC in particular there is now the BMAS translation of these sections. The “overall works” has also been coordinated with Austria and Switzerland.

The guide is designed to aid the harmonised European design and application of the Machinery Directive 2006/42/EC. It is directed at all groups concerned with application of the Directive, such as manufacturers, dealers, importers of machines, market surveillance authorities, supervisory services of the employer’s liability insurance associations and test centres.

The German document is available as free download; google “BMAS, Leitfaden MRL 2006/42/EG”.

In view of the fact that this guide has over 400 pages, if you are looking for something specific it is worth using the search function in the PDF document. Alternatively you can look at and study the comments on the various articles in the operative part as well as the annexes and the sections of these annexes.



Hazardous products 2012 – information on product safety

In the past we have often been asked whether information is available on accidents in mechanical engineering that goes beyond mere overall statistics and development trends, and is also more than just general analyses of causes. Admittedly we have always found it difficult to come up with answers to these questions. I refer for example to the pleasing declining number of fatal industrial accidents, whereby it must be clearly stated that every accident is one accident too many. We have also been pleased to make reference to the British HSE study “Out of control: Why control systems go wrong and how to prevent failure” (which can be downloaded free of charge by googling the above title).

The “Gefährliche Produkte 2012 – Informationen zur Produktsicherheit” report (hazardous products 2012 – information on product safety) from the Federal Institute for Occupational Safety and Health (the BAuA) in Dortmund may now be able to cast more light on (“our”) darkness. The report summarises figures and findings from 2011. Each chapter provides “references” in the form of yellow boxes which summarise the essence of the matter.

On the subject of “Machinery” or “Technical products”, a total of 142 fatal industrial accidents are documented for 2011 (at the time of going to press on 31.01.2012) and the report states the following right at the beginning:

There were serious fatal industrial accidents in conjunction with products subject to the Machinery Directive (...). Caution: a slap in the face! Against this background it is astounding that complaints according to RAPEX were only registered in connection with four product groups by the competent market surveillance authorities. It can be read elsewhere that greater interaction between market surveillance and occupational health and safety would be desirable with respect to some aspects.



When classified according to product groups, it can be seen that the group of accidents with (earth) construction machinery (diggers, cranes, construction vehicles) dominates with a share of 56%; this is followed by work platforms and floor-borne vehicles (forklifts) and also – albeit a long way behind – by classic finishing and processing machines (see the table on the right).

The following figures can be found under “Evaluation of accident causes”, although there are questions about their validity (keyword: grey areas, playing down own responsibility etc.) (see table below):

You can find the detailed presentation in Chapter 1.3 of the above BAuA report (please google “BAuA, gefährliche Produkte 2012” [sorry, but this document is available in German language only] if you are interested).

	Frequency	Percent
Construction vehicles	20	25.6 %
Cranes	17	21.8 %
Work platforms	11	14.1 %
Diggers	7	9.0 %
Forklifts	7	9.0 %
Metal cutting machines	4	5.1 %
Saws	3	3.8 %
Miscellaneous	3	3.8 %
Ground conveyors	2	2.6 %
Doors and gates	1	1.3 %
Special machinery	1	1.3 %
Assembly bench	1	1.3 %
HGV vehicles	1	1.3 %
Total	142	100.0 %

Evaluation of product groups according to the Machinery Directive: individual products in acc. with the Equipment and Product Safety Act (GPSGV)

	Frequency	Percent
Human error (gross negligence, acting without reason)	78	55.3 %
Unknown cause	30	21.3 %
Can be prevented by better technology	15	10.8 %
Technical failure of materials and components	8	5.7 %
Predictable use due to communication errors	7	5.0 %
Predictable use resulting from overtiredness, stress, distractions etc.	3	2.1 %
Total	141	100.0 %

Evaluation according to accident cause: possible accident causes

Allow us to point out here that the focus of this section of the report (Chapter 1.3) is on fatal industrial accidents. However human suffering and destiny also lies behind non-fatal accidents, especially when the physical damage is irreversible or can only be put somewhat right by a great deal of medical intervention.

News from the Schmersal Group

With individual encoding and adjustable latching force – solenoid interlock with novel mode of action

The Schmersal Group introduced an innovative solenoid interlock with unusual switch and actuator design at the SPS IPC Drives 2012.

The solenoid interlock with designation AZM 300 distinguishes itself clearly from the other switchgear on the market at first glance. A novel latching system in the form of a rotating Maltese cross makes it possible to approach the interlock from three sides. This ensures universal usability. One and the same model can be used on revolving doors opening to the left or right and on sliding doors.

A further significant advantage is that the user needs no additional attachments here, for example a door stop or latching element, because these functions have been integrated in the interlock.





This wish has often been expressed in practice by design engineers in machinery and plant engineering.

Another practical function of the AZM 300 is the fact that the latching force can be adjusted, i.e. the non-safety-related latching function with unlocked guard. This property also contributes to ensuring that the interlock system can be well adapted to suit individual requirements.

Not only the mechanical design of the AZM 300 is innovative, but also the electronics. An integrated RFID sensor assumes the identification and encoding of the actuator. This means that the user can choose between three types of encoding.

In the basic version the sensor accepts every suitable target. A second, encoded version only reacts to an individually assigned target. The programming procedure can be repeated as often as wished. Finally a third version is available which only accepts the target that has been programmed when switched on for the first time.

The user can thus select the encoding version that is most suitable. The significance of this function in practice cannot be emphasised enough: practical tests show again and again that several protective devices are manipulated. Whilst the use of an individually encoded solenoid interlock cannot completely prevent manipulation, it can at least make it more difficult.

The new solenoid interlock satisfies the requirements of Performance Level “e” or Safety Integrity Level 3. The basis for its development included specific requests from customers in the packaging industry who wanted a universally usable, compact, encodable solenoid interlock with adjustable latching force. Since there is a large overlap between the packaging and food industry among Schmersal customers, the developers observed the basic principles of hygienic design wherever possible. Dead spots or zones in which material might become deposited were avoided, and even the actuator itself is made from rounded elements. What is more, the AZM 300 is resistant to a number of detergents. Thanks to protection class IP 69K it is also very suitable for use in sensitive hygienic areas.

Please use the [reply form on Page 34](#) or visit our website at www.schmersal.com, if you would like further information about the new solenoid interlock from the AZM 300 series.



News from the Schmersal Group

Safety in the system – new master/monitor combinations and safety gateways

With the Schmersal system, which was similarly presented for the first time at the SPS IPC Drives 2012, the Schmersal Group is taking an important step along the way to becoming a system provider in the field of machinery safety.

A complete range of components makes the connection from the field level – i.e. from the safety switchgear – to the higher control level. In doing so the user can choose between “safety integrated” and “safety separated” control concepts.

The new Schmersal system is based on the comprehensive range of safety switchgear with integrated AS-Interface Safety at Work (AS-i Safety) interface. These can now be directly connected to higher level control systems via various master-monitor combinations and safety gateways. This linking of the field and control levels produces a safety system – the Schmersal system.

Machine builders can choose between two system architectures. If a safety control system is used that is separate from the standard control system (“safety separated”), master-monitor combinations with various field bus interfaces, e.g. for PROFIBUS, PROFINET, Ethernet/IP and ModbusTCP, are available. The entire safety logic is programmed in the safety monitors by means of the user-friendly ASIMON software. Signals that are not safety-related are similarly transmitted through the master-monitor combinations and passed on to the standard control system. This means that comprehensive diagnostic-related information is available, for example in the event of a failure or during the evaluation of the operating statuses of a machine.



On the other hand, when the machine is equipped with a safety control system that processes both operational and safe signals (“safety integrated”), the Schmersal system represents a system solution that uses safety gateways. These have been designed for two AS-i circuits and transmit up to 60 safe inputs/outputs to the safety control system via a safe field bus. The operational diagnostic-related signals are likewise transmitted to the higher level control system, where they can be suitably evaluated. The safe signals can also be pre-processed in the safety gateway using the ASIMON software.

Both versions of the Schmersal system provide the machinery builder with clear advantages. Amongst other things, connecting the safety switchgear to the control level enables faster mounting and installation of the components in the safety circuit. Furthermore the occurrence of errors during the installation can almost be ruled out completely. The configuration of the desired or required parameters is also simplified because this takes place with the AS-i safety monitor using the ASIMON software.

From the point of view of the user, the advantage of the Schmersal system is that an installed system can be changed or extended at any time. This applies both to adding more safety switchgear and to configuration of the switchgear (e.g. safety links, STOP category, filter times etc.). It gives machinery builders and users greater flexibility and allows them to adapt safety functions to suit any changed requirements.

Schmersal offers the new system as a complete solution. In addition to different master-monitor combinations and safety gateways, which differ both in the connection options to the various field bus systems and in the number of safety circuits and of inputs and outputs, the range also includes modules that enable safe speed monitoring and power supply units as well as the required accessories such as bus distributors, bus cables and M12 connecting cables.

Please use the [form on Page 34](#) or visit our website www.schmersal.com, if you would like further information about the new ASi-SaW master/monitor combination with gateway.



News from the Schmersal Group

New versatile two-pedal safety foot switch

Robust, ergonomic, safe and versatile. The range of safety foot switches has been expanded to include the T2FH 232 series with a new two-pedal model.

As with the tried-and-tested one-pedal TFH 232 version, the new two-pedal series features an ergonomic design which is the ideal prerequisite for effortless and safe actuation. This stable switchgear can be operated well even when the operator is wearing safety shoes, partly due to the generously dimensioned protective guard that prevents inadvertent actuation of the switch. There is a fold on the inside of this guard which enables the operator to make concerted movements of the switch with his feet. The powder-coated die-cast enclosure can withstand even high mechanical loads.

The user can configure and customise the foot switch as desired. In the standard versions, at least one of the two pedals is designed as safety foot switch. This type of safety switchgear is used as enabling switch on machinery and plant where manual actuation is either impossible or not practical.



When the foot pedal is actuated up to the pressure point, the NO contact is closed. If, in case of danger, the pedal is actuated beyond the pressure point, then the positive break NC contact is opened and mechanically latched. The locking can only be reset again manually using an unlock button.

In the pertinent models the second pedal can be used to actuate a process function. The user can choose between different switching and contact options, whereby a maximum of four contacts are possible for each pedal.

Safety foot switches are typically used on presses and other forming machinery, on woodworking machinery and for packaging machinery and systems.

Please use the [reply form on Page 34](#) or visit our website at www.schmersal.com if you would like further information about the new 2-pedal safety foot switch.



News from the Schmersal Group

Consolidation of Schmersal and Elan

As from 20.09.2012, the former Elan Schaltelemente GmbH & Co. KG in Wettenberg and K.A. Schmersal GmbH in Wuppertal have been amalgamated to form a joint company, K.A. Schmersal GmbH & Co. KG, with locations in Wuppertal and Wettenberg,.

In doing so, the Schmersal Group executed at a strictly legal level what had already been successful in practice for some time: the product ranges of both companies have been merged since Schmersal took over the then specialist for low voltage switchgear in 1997. Since then Elan has increasingly focused on the development and production of operating and monitoring switchgear, of safety relay modules and safety-related control technology. The Wettenberg site is furthermore the competence centre for the Schmersal Group for safety-related radio technology and explosion protection.

These areas of specialisation, together with development and production capacities, will remain at the Wettenberg location. Graduate industrial engineer Philip Schmersal, CEO of the Schmersal Group: “With the consolidation of the enterprise we are underlining our systems approach. Ever more of our customers purchase complete machinery safety solutions with safety switchgear ‘made in Wuppertal’ and the corresponding monitoring electronics from the Elan portfolio. Both come from one company and are perfectly coordinated with each other. The unification of the company and the brand name makes this clear at first glance.”

From the point of view of customers, the only change is that they have central sales contact partners for the entire Schmersal product range and that all Schmersal products are now listed with all relevant technical data in the joint online catalogue at www.schmersal.net.

The logistics of both sites will also be amalgamated in coming weeks. The central European logistics centre for the Schmersal Group in Wuppertal will then commence operations.

We would be happy to send you further information.

Please photocopy this page and send to

K.A. Schmersal GmbH & Co. KG, attn. Ms. Höhn

– by fax: +49 (0)202 6474-871

– by post:

K.A. Schmersal GmbH & Co. KG, Möddinghofe 30, 42279

Wuppertal

Please send us information on ...



2013 tec.nicum range brochure

(referred to on Page 1)



AZM 300 solenoid interlock

(referred to on Page 26)



ASI-Saw master/monitor combination

(referred to on Page 29)



T2FH 232 foot switch

(referred to on Page 31)

Request fo

Company

Name

Phone No.

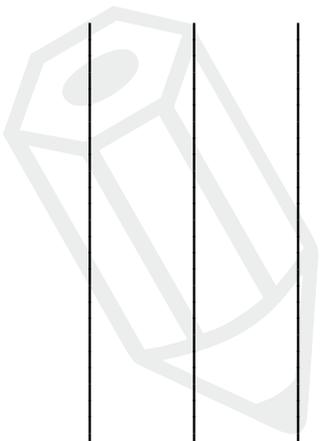
Fax No.

Email

Dept.

Street

Town/city
postcode





K.A. Schmersal GmbH & Co. KG

**Möddinghofe 30
42279 Wuppertal
Germany**

Telephone: +49 (0)202 6474-0

Fax: +49 (0)202 6474-100

Email: info@schmersal.com

Internet: www.schmersal.com