Technical article, published in:
elektro AUTOMATION 09 / 2016

Changes of relevance to practice or simply cosmetic revisions?

Experts in safety technology on the updated standard DIN EN ISO 13849-1:2016 – Safety of machinery

After several years of standardisation work, DIN EN ISO 13849-1:2016 was published at the end of May. Since July it is therefore only this standard that is allowed to be used as the basis for the presumption of conformity. As there are a lot of changes in the standard, there may be new requirements for issuing EC declarations of conformity as a result. The effect these changes have on the practical work of machinery and plant manufacturers is explained by the seven experts in the trend interview. They also explain which special requirements need to be addressed on the usage of collaborative robots.

elektro AUTOMATION: With DIN EN ISO 13849-1 one the harmonised standards for machine safety has been revised. What are the key changes in the new version?

Bauder (Leuze): During the revision the focus was on the readability and the applicability of the standard. In addition, the normative references in DIN EN ISO 13849-1 were updated. For example for the basic standard DIN EN ISO 12100. There are various changes from the new DIN EN ISO 13849-1: with the increase in the MTTFD value (Mean Time To a Dangerous Failure) for subsystems to 2500 years, the Performance Level PL e can be achieved for the entire SRP/CS (Safety-Related Parts of a Control System) even with a significantly higher number of subsystems with Performance Level PLe. Due to the expanded graph for determining the Performance Level required, the required Performance Level PL r for hazardous events with low probability of occurrence can also drop one level. In addition, experience with the operation of a part in a special configuration and safety application can be taken into account in the proven-in-use characteristic. The requirements on the usage of standard components in a safety function equipped with embedded software have also changed.

Gast (Phoenix Contact): One of the most important changes relates to the non-normative Annex A in which the risk graph has been changed. On the one hand an additional parameter for the probability of occurrence of the hazardous event has been introduced.

If the probability is categorised as low, the resulting PL r can be reduced by one level. On the other hand there is a new interpretation for the parameter F (frequency and exposure).

Furthermore, the requirements on the frequency of testing for category 2 have been changed. Fault detection on demand is possible provided the hazardous point cannot be reached within the shutdown time. Other changes relate to the frequency of testing.

The ratio in relation to the demand rate can be reduced. However, in this case a supplement to the PFH value is to be expected. The requirements in relation to the usage of safety-related embedded software on the usage of standard components are also described. Here essentially the usage of diverse technologies is relied upon.

The safety experts discuss in a trend interview the effect the changes in the DIN EN ISO 13849-1:2016 have on the practical work of machinery and plant manufacturers. The requirements on the usage of standard components in a safety function equipped with embedded software have also changed

Kramer-Wolf (Wieland): Along with a series of changes in the names and units for safety parameters such as MTTFD, B10D and PFHD [1/h] to harmonise them, the introduction of a new evaluation parameter in the risk graph as well as comments on the evaluation of exposure frequencies in the risk graph can be identified as important changes. The changes to the category 2 definition as well as the modified Annex C table values for relays and hydraulic valves will have the greatest effects in practice. Although other changes are more obvious, they will have fewer effects in daily practice. The new section 4.5.5 on the simplified evaluation of actuators without reliability data is superfluous in practice, as the necessary characteristic data were already available in Table C.1. The expansion of Table K.1 in category 4 for MTTFD up to 2500 years is also of only minor practical importance.

Rothenburg (Euchner): The new issue of the standard does not contain any new requirements for the machinery and component manufacturers. Its purpose was to achieve better readability as well as simpler applicability. The goal has definitely not been achieved in full, but many points are now better explained. IFA has published a very good summary of the changes to the standard: 'Amendment of EN ISO 13849-1, A survey of the essential improvements in 2015'.

Wimmer (Pilz): The new version has a few topics that are really of relevance for practice. First there is the expansion of the probabilities of failure in the form of Annex K. For category 4 subsystems it is now possible to achieve lower probabilities of failure than before. In practice this means that even very comprehensive safety functions can be evaluated more easily. This new feature has particular importance during the consideration of overlapping hazards where complex safety functions are the order of the day. The new feature is the further expansion of category 2. As such it is now possible again to realise safety functions in this category also using mechatronic components. The description in sub-section 4.5.5 on how components without an MTTFD (Mean Time To Dangerous Failure) available can be evaluated in safety functions with a Performance Level is new. This exception applies expressly only to mechanical, hydraulic and pneumatic components. And finally, the new version also addresses the topic of overlapping hazards, that is whether a person is placed at risk by several hazards at the same time in the same place. However, the standard does not provide any detailed information, instead it only requires that this issue must be taken into account in a risk assessment.

Wolf (Schmersal): Along with editorial changes to improve the readability and comprehensibility of the text in the standard, a series of details have been changed and added that will become apparent in practice. Among others, these include a new simplified method for estimating the quantifiable aspects of the Performance Level for the output stage of a SRP/CS – that is the elements that transfer energy – in the safety-related control section. Also on the determination of the required Performance Level (PL r), the probability of occurrence of a hazardous event can be taken into account.

In addition, for the first time the boundary conditions are defined in which standard components with embedded software can be used in safety functions without the need to

"During the revision the focus was on the readability and the applicability of the standard"
Frank Bauder from Leuze electronic

"The possible effects of the new issue should be evaluated by the manufacturer in all circumstances"
Torsten Gast from Phoenix Contact Electronics

fulfil completely the specific requirements on safety-related embedded software (SRESW).

elektro AUTOMATION: Both the risk assessment and the calculation of safety functions have caused problems time and again in the past. What are the advantages and disadvantages of the changes for the user? Does the new standard simplify practical work?

Bauder (Leuze): In our opinion there has not been a significant change in the risk assessment method. In the detail, for example, a specific value for frequency and duration of exposure now aids the differentiation between F1 and F2 in the risk graph. This simplifies the assessment in practice. On the other hand, users can now reduce the PL r if there is a low probability of the occurrence of a hazardous event, which increases the complexity of the assessment. However, this step is optional. The calculations that are used to determine the Performance Level achieved have also not changed fundamentally in our opinion. Sound expertise on the part of the user is still required. Alternatively, professional support during the calculation from a service provider like Leuze electronic helps to keep the effort within limits for the user.

Gregorius (Phoenix Contact): Due to the introduction of the new parameters for the probability of occurrence, a closer link to EN ISO 12100 is possible. In the context of the services it offers, Phoenix Contact has therefore developed a matching process to synchronise the two approaches from EN ISO 13849-1 and EN ISO 12100. In the past during the evaluation of actuator elements (energy transmission elements), there was often the problem that insufficient information was available from the manufacturers. Due to the introduction of a reference table, substitute values for the determination of PFHD as a function of the category are established that permit a conservative calculation even without characteristic data from the manufacturer. Also, in the past in particular the connection of safety chains with a large number of subsystems in some cases resulted in a lower Performance Level due to 'excessively poor' results as a result of capping the MTTFD figures at 100 years. This shortcoming has been rectified by raising the MTTFD to 2500 years for category 4.

Kramer-Wolf (Wieland): In relation to the risk assessment, practically nothing has changed in the method. New is the possibility of evaluating the 'probability of occurrence of a hazardous event' with the option of reducing the PL r by one level. This new parameter provides a new way of lowering the PL r. How this is to be determined is not defined by the text in the standard. The second change goes in a similar direction: in the past there was a recommendation in the text in the standard to consider exposure frequencies that exceed once per hour as frequent. This has been reduced to every 15 minutes. At the same time a total exposure duration of less than 5 % was described as seldom, which corresponds to 72 minutes per 24-hour working day. Overall, although the work is not simplified by these aspects, the necessary PL r safety levels are lower.

Rothenburg (Euchner): For the risk assessment a note has been added in Annex A about the W parameter, which characterises the probability of occurrence. Although this parameter has not flowed into the graphs for determining a PL r, it has always been included in the basic standard, EN ISO 12100.

„Due to the introduction of an additional parameter for the probability of occurrence a closer link to EN ISO 12100 is possible"
Carsten Gregorius from Phoenix Contact Electronics

„Overall, although the work is not simplified by these aspects, the necessary safety levels are lower"
Thomas Kramer-Wolf from Wieland Electric

In principle, the calculation of the PL has not changed. There is a significant simplification on the usage of components for which a safety figure such as MTTFD or B10D is not stated.

On the usage of such components in the output stage of a safety circuit, it is not necessary to calculate the MTTFD, it is sufficient to determine the category. Overall, useful changes that make the usage of the standard easier.

Wimmer (Pilz): The risk assessment for a machine is orientated on EN 12100 and not on EN 13849. In the past this procedure has indeed been portrayed a little incorrectly. The current EN 13849 provide clear instructions that within this standard the assignment of a Performance Level leads to the necessary risk reduction, but not the assessment of a risk and the risk reduction itself. A thorough revision of the section on software would be desirable, however for organisational and time-related reasons this revision is only to be expected in a subsequent issue.

Wolf (Schmersal): With the current issue of DIN EN ISO 13849-1:2016, a successor to DIN EN 954-1, for the first time the consideration of the probability of occurrence of a hazardous event is included in this standard. This probabilistic approach, that is an approach that takes into account the probability, can now also be used to determine the required Performance Level (PL r) for a safety function. In Annex C the standard also provides expanded MTTFD and B10D values for contactors and hydraulic components for which no characteristic data are available from the manufacturer. The limit on the MTTFD for subsystems in category 4 has also been raised from 100 years to 2500 years.

Expanded PFHD values can therefore be found in Annex K of the standard. As a consequence, if necessary PL e subsystems can be combined and better PFHD values achieved, without reducing the overall SRP/CS in total to PL d. My conclusion is that this revision of the standard includes many advantages for the user and predominantly involves simplifications.

However, in all the euphoria for calculations and for ‘great’ PFHD calculation values, it should not be forgotten that good, safety-related design is more important than any calculation of probability.

elektro AUTOMATION: Initial comments on the changes suggest that they could result in a simplification during the evaluation of the safety functions and also a worse result. Do machinery manufacturers now have to check their existing installations again?

Bauder (Leuze): It is the nature of standardisation that changes to the content will also produce changes to the results. In principle, after the appearance of DIN EN ISO 13849-1 in the Official Journal of the EU the presumption of conformity only applies for the new issue of the standard. However, the basic, legally binding requirements of the Machinery Directive, that is the national law on product safety related to health and safety must still be met.

All users who have used DIN EN ISO 13849-1 in the past to assess safety functions should be advised to investigate the specific effects of the changes. Only then can it be estimated whether any changes are necessary to machines that are placed on the market after the publication in the Official Journal. In our opinion there is, however, no general obligation to check existing machines.

„In principle the calculation of the Performance Level has not changed“
Jens Rothenburg at Euchner

„The new version has a few topics that are really of relevance for practice“
Matthias Wimmer from Pilz

Gast (Phoenix Contact): The possible effects of the new issue should be evaluated by the manufacturer in all circumstances. Machines that were placed on the market as per the Machinery Directive and according to the previous EN ISO 13849-1:2006 do not need to be checked again without reason. In most cases lawmakers have introduced practical concessions that are intended to give users further flexibility. However, due to the topic of 'overlapping hazards' a new aspect has been added: here it is assumed that with multiple hazards concentrated at one hazardous point, all energy transmission elements must be considered on determining the PFHD value in a safety function. This relates in particular to applications with multiple axis systems, for example robots, however also machine tools.

Kramer-Wolf (Wieland): Due to three changes, machinery manufacturers can no longer generally assume that their previous assessments will produce (as a minimum) the same result on the application of the new edition: The most frequent situation is probably the usage of the B10D value for contactors from Table C.1. This has been reduced by 35 % compared to the previous edition. The second point is the clarification that category 2 structures in PL d now require a mandatory second shutdown path.

Simple signalling is no longer enough. The third point is in Annex E. In the past it was possible to evaluate a redundant shutdown path on which only one channel has direct diagnostics with DC = 90 %. This option has been dropped with no substitute.
If one of these points is used in the machine, it is strongly advised to check the existing assessment for the series-production machine.

Rothenburg (Euchner): It is not necessary to undertake any new calculations. In fact they would produce the same results anyway. A worse situation would only occur if you use the new simplified approaches that we have already discussed. As here only the category has been taken into account, not probabilities of failure, only the lower limits for these categories can be used as the basis for further calculations. Here the principle applies that the worst case must always be assumed for safety technology. If probabilities of failure are stated, the value is then always better.

Wimmer (Pilz): These new possible variations in the calculation of the safety functions are primarily to be attributed to the new freedom on the selection of the risk parameter P. EN 13849 is one of the European standards that should be taken into account during the design and construction of machinery. The issue therefore relates to machines that are currently being planned or built. The current standards are always to be taken into account during this phase. For machines that are already in operation, in Germany there is the Betriebssicherheitsverordnung (ordinance on health and safety), which implements some European directives.

On the one hand, operating organisations must take into account the state-of-the-art also during operation (and therefore also current standards).

On the other hand, the Betriebssicherheits-verordnung only places requirements on the operation of machinery – the design requirements come however from the directives for placing on the market which the manufacturer has already taken into account.

„In the area of collaborative robots there is some movement"
Siegfried Wolf from Schmersal

Wolf (Schmersal): I assume that due to the changes in EN ISO 13849-1:2015, it will not be generally necessary to re-assess safety-related parts of control systems (SRP/CS). However, from now on it forms the framework for all machinery manufacturers during the design and evaluation of their SRP/CS. The revised version is already listed in the Official Journal of the EU in relation to the Machinery Directive 2006/42/EC and only with EN ISO 13849-1:2015 is the so-called presumption of compliance as per the Machinery Directive valid.
For machinery manufacturers who have already met the requirements described in the standard, I do not see any direct need for action – however the changes in the content of the standard should of course be evaluated during the construction of series-production machines and also taken into account. Type examination certificates that were obtained by applying the old standard also retain their validity. I advise all others to use the possibilities of this now really comprehensible and easy to read standard and to apply it.

elektro AUTOMATION: Collaborative robots and their areas of application form part of the trends currently subject to intensive discussion in automation – but which requirements must be met in relation to the safety technology? Are the existing standards adequate for the evaluation of safety functions of collaborative robots? What are the current developments in this area?

Bauder (Leuze): With collaborative robots the classic, proven risk-reducing measures such as distance to the hazardous movement and the usage of guards can of course not be applied. However, the standardisation forums are already active here and in the ISO 10218 series have described and also classified the possibilities for the collaboration between man and robots. On this topic the draft standard ISO/TS 15066 has been produced; this standard is intended to cover safety-related aspects. For instance these are limiting the force and travel, the monitored stop and especially of course manual operation. All these safe functions are the basis for the acceptance of collaborative robots by the user or machine operator. In the industrial environment, the burden on people can be further reduced by the new systems. In the non-industrial environment, on the other hand, there have been very interesting developments with support for older or sick people with mobile robots.

Gregorius (Phoenix Contact): If the working area is common, in a flexible cell this area must be dynamically adjusted to the robot's co-ordinates. Alternatively, the robot itself detects an intrusion into its working area. At the moment this feature is realised by force/torque limiting. The sensors must react to the robot's co-ordinates or detect them on their own. In EN ISO 10218-2, collaboration is only permitted for tasks defined in advance; the collaboration space must be clearly defined, for instance by a mark on the floor. If there are several persons in the collaboration space, they are to be protected via individual control elements. A new type of usage also requires the dynamic adaptation of the tasks to design a flexible workplace with robot support.

The protected workspace can be variable for a common activity, also due to several persons. A fixed mark on the floor is therefore no longer possible. The standard describes here the current state of sensor technology, which does not permit individual differentiation between persons. Currently in various research projects new sensors are being tested that can dynamically acquire the workspace. In this way even heavy-duty robots can be approved more easily for collaborative operation.

Kramer-Wolf (Wieland): The greatest uncertainty is still the evaluation of the risks of collaborative machines and robots. A key question as to the permissible forces that a machine is allowed to apply to a person is currently under investigation in standardisation circles. Here ethical, legal, technical and medical aspects come together. Various studies are currently evaluating the technical and medical aspects. The legal aspects here are very clear: a machine or a robot must not injure a person or cause a person pain. It is therefore necessary to define a fine boundary at which the effect of force will cause an injury or pain. As this issue has a highly subjective aspect, we can be curious as to how and whether a practicable path will be described by our standards makers.

Rothenburg (Euchner): In general all risks, including those from collaborative robots, can be assessed using the existing general standards (A and B standards). In future a dedicated C standard for collaborative robots is to be produced that will ease the assessment and usage. Whether this will then be based on the standard for machine safety used today or more on EN 61508, I do not know.

Wimmer (Pilz): Lawmakers oblige the manufacturer of a robot application to undertake a conformity assessment process. The application of the CE mark then confirms that the robot application meets all the necessary health and

safety requirements. The challenge of the underlying risk assessment is that the boundaries for the working areas for man and robot disappear and that collisions can be a real scenario. However, they must not result in any injuries. A central role is played here by the Technical Specification ISO/TS 15066 'Robots and Robotic Devices – Collaborative industrial robots' published this spring. Using this specification, safe man-robot collaborations can be implemented after corresponding validation.
In its Annex A the technical specification is also the first standard that provides detailed information on pain thresholds for various regions of the body. These values form the basis to be able to implement the application with a power and force limit.

Wolf (Schmersal): For man-robot collaboration, the 'safety requirements for industrial robots' were published almost a decade ago with EN ISO 10218-1 – however more detailed rules of play are also to be expected in the near future. For example also from the point of view of the DGUV (German Social Accident Insurance) the safety requirements for industrial robots are not yet comprehensibly described and DGUV information 209-074 'Industrieroboter' (Industrial robots) dated January 2015, provides additional assistance. At the start of 2016 the International Organisation for Standardization (ISO) published ISO/TS 15066, the first technical specification that only addresses man-robot collaboration. This specification provides support during the risk assessment obligatory as per the Machinery Directive.

Of the various collaboration concepts, power and force limiting is the most promising on this bases. Here the potential hazard is limited to a non-hazardous level by the restriction of the contact forces between man and robot. In this area there are certainly aspects to improve, and as such the draft DGUV information 'Kollaborierende Robotersysteme' (Collaborative robot systems) will also make a further important contribution. However, robot workplaces are also taken into consideration in the changes to EN ISO 13849-1: the new section 'Overlapping hazards' addresses situations in which a person can be injured by different hazardous movements in one place, for instance within the hazardous area of an industrial robot. There is therefore some movement in the area of safety measures for robots…

The experts
- Frank Bauder, Head of Competence Center Services, Application Support & Service Management at Leuze electronic GmbH + Co. KG in Owen
- Torsten Gast, Competence Center Safety at Phoenix Contact Electronics GmbH in Bad Pyrmont
- Carsten Gregorius, Product Marketing Safety at Phoenix Contact Electronics GmbH in Bad Pyrmont
- Thomas Kramer-Wolf, specialist for safety/machinery manufacture at Wieland Electric GmbH in Bamberg
- Jens Rothenburg, standards and safety expert at Euchner GmbH + Co. KG in Leinfelden-Echterdingen
- Matthias Wimmer, member of the standardisation group ISO/TC 199/WG8 and standards specialist (functional safety of machinery) at Pilz GmbH & Co. KG in Ostfildern
- Siegfried Wolf, Head of tec.nicum academy at K.A. Schmersal GmbH & Co. KG in Wuppertal

www.euchner.de
www.leuze.de
www.pilz.com
www.phoenixcontact.de
www.wieland-electric.com
www.schmersal.com

Images:
Schmersal
Leuze electronic
Phoenix Contact
Phoenix Contact
Wieland Electric
Euchner

K. A. Schmersal GmbH & Co. KG
Möddinghofe 30
42279 Wuppertal
Telefon: +49 202 6474-0
info@schmersal.com
www.schmersal.com