IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Amendment of EN ISO 13849-1

A survey of the essential improvements in 2015

Survey

Almost ten years after it was first published in revised form as EN ISO 13849-1, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, the first amendment of this standard is expected to appear by the end of 2015 in a consolidated version. Since the amendment was intended primarily to improve clarity and ease of application, it contains only a few significant changes. A number of detail improvements and additions have however been made that are apparent in the standard's practical application. These include consideration of the probability of occurrence of a hazardous event during determining of the required performance level (PL_r), a new simplified method for determining the PL of the output part of the safety-related part of the control system (SRP/CS[1]) and a proposed method for dealing with the requirements concerning SRESW (safety-related embedded software) when standard components are used. This paper describes the essential changes. Where the text of the amendment needs interpretation, it provides recommendations.

1 Introduction

Table 1, "Recommended application of IEC 62061 and ISO 13849-1", has been replaced by a reference to the technical report ISO/TR 23849 [1], which has since appeared. The latter addresses in detail the differences between the two standards and their common aspects.

2 Scope

It is now clarified that the standard applies to safety-related parts of control systems (SRP/CS) with high demand or continuous mode of operation. According to definition 3.1.38 the frequency of demands on a SRP/CS in this mode of operation is greater than one per year.

3 Terms and definitions

The abbreviation “PFH_D“[2] has been introduced for the "average probability of dangerous failure per hour". The dimension of this variable is 1/time and its typical unit is 1/h.

The notation for the "mean time to dangerous failure" now has a capital D, i.e. "$MTTF_D$"[3] (formerly "$MTTF_d$"). The same applies for B_{10D}, T_{10D} etc.

4 Chapter 4 design considerations and Annex K

Besides updating of the references to ISO 12100:2010 (instead of to the preceding standard, ISO 12100-1:2003), the amendment explains that the sub-systems of an SRP/CS can also be designed

[1] SRP/CS = Safety related parts of a control system
[2] PFH_D = Probability of a dangerous failure per hour
[3] $MTTF_D$ = Mean time to dangerous failure

against other standards governing functional safety (e.g. IEC 62061, IEC 61508, IEC 61496). They can then – where applicable following "translation" of an SIL[4] to a PL in accordance with Table 4 of the standard – be integrated as sub-systems. In this case, the rules for "combination of SRP/CS" (Section 6.3 of the standard) are to be applied. This is also explained in ISO/TR 23849 [1].

The limitation of the $MTTF_D$ for each channel to 100 years has been increased to 2,500 years for Category 4 sub-systems. The corresponding pairs of $MTTF_D$ and PFH_D values have been added to Annex K of the standard. The limitation to 100 years was originally introduced in order to enable high Performance Levels to be attained on a basis other than a high statistical reliability of the individual components. However, since redundancy and fault detection (DC, Diagnostic coverage) are already at a very high level in Category 4, the $MTTF_D$ constraint can be loosened in this case. The superior PFH values that can be attained as a result then also enable a greater number of PL e sub-systems to be combined without the entire SRP/CS "slipping down" to PL d. Further information can be found in [2].

Two changes have been made concerning the assumptions for the designated architectures, which form the basis for the simplified method for estimation of a PL:

- **Frequency of tests in Category 2**
  For Category 2, so far the demand rate had to be ≤ 1/100 of the test rate.
  Now the testing may occur immediately upon demand of the safety function, if the overall time to detect the fault and to bring the machine to a non-hazardous condition (usually the machine is stopped) is shorter than the time to reach the hazard. Here ISO 13855 for the calculation of safety distances is referenced.
  Chapter 4 of the SISTEMA Cookbook 4 [3] gives further explanation.

- **$MTTF_D$ of the test channel in Category 2**
  So far the $MTTF_{D, TE}$ of the test equipment was compared to the $MTTF_{D, L}$ of the logic.
  Now the $MTTF_D$ of the test channel has to be greater than half the $MTTF_D$ of the functional channel. Previously this new rule was only given in a note under the condition that the blocks of each channel cannot be separated.

Annex K contains a new note on the aspect of the test rate in relation to the demand rate:

- If for category 2 the condition mentioned above (function tested 100 times more frequently than demanded) cannot be fulfilled, but the demand rate is less than or equal to 1/25 of the test rate, then the PFH_D values stated in the table K.1 for category 2 multiplied by a factor of 1.1 can be used as a worst case estimate.

A further comment explains that the PFH_D values in Annex K were calculated for all categories with the discrete values for DC_{avg}, 60%, 90% and 99%.

5 New simplified procedure for the output part of the SRP/CS (power transmission elements) to estimate PL and PFH_D without $MTTF_D$

In response to calls voiced by industry, an additional and further simplified method for determining the PFH_D and the quantifiable aspects of the PL of a subsystem has been added in the form of a new Section 4.5.5. The method is based primarily upon the implemented Category inclusive of DC_{avg} and CCF (common cause failures). This method does not require calculation of the $MTTF_D$;

[4] SIL = Safety integrity level

however, well tried (in Categories 1, 2, 3 and 4) or proven-in-use (in Categories 2, 3 and 4) components must be used throughout.

Proven-in-use is a new feature in the framework of the standard, not to be confused with well-tried components. Proven-in-use demonstration is based upon an analysis of experience in the field for a specific configuration of a component in a particular application. The analysis must show that the probability of dangerous systematic faults is sufficiently low for each safety function using the component to reach its required Performance Level (PL_r). Such a demonstration has not been common in machine construction before now. It is also unclear why the requirement refers only to systematic faults, and the random component faults are not considered.

The new method to estimate PL and PFH_D is applicable only in special cases, which are:

- for the output part of the SRP/CS and
- when for mechanical, hydraulic or pneumatic components (or components employing mixed technology, e.g. mechanical brake with pneumatic control) no application-specific reliability data ($MTTF_D$, failure rate, B_{10D} or similar) are available.

Table 1 shows the estimated PFH_D value and the resulting attainable PL according to the implemented Category and under the additional conditions placed upon the method.

Table 1: PL and PFH_D as worst case estimation based on Category, DC_{avg}, and use of well-tried-components (on the basis of the table in Section 4.5.5 of the standard).

	PFH_D (1/h)		Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL b	$5.0 \cdot 10^{-6}$	⇦	●	○	○	○	○
PL c	$1.7 \cdot 10^{-6}$	⇦	-	●	●	○	○
PL d	$2.9 \cdot 10^{-7}$	⇦	-	-	-	●	○
PL e	$4.7 \cdot 10^{-8}$	⇦	-	-	-	-	●
●	Applied Category is recommended						
○	Applied Category is optional						
-	Category is not allowed						

The method is subject to the following additional conditions:

- In Category 1: use of well-tried components and well-tried safety principles (as previously, and established in the Category 1 definition).
- In Category 2: the $MTTF_D$ of the test channel is at least 10 years.
- In Categories 2, 3 and 4: use of well-tried or proven-in-use components and use of well-tried safety principles. In Category 2 according to the standard this applies also for the test channel.

- In Categories 2 and 3: adequate measures against CCF, and for each component DC at least "low".

- In Category 4: adequate measures against CCF, and for each component DC "high".

The following additional information is provided:

- Category 1: For safety-related components the machine manufacturer shall determine the T_{10D} values based on data for the components to be proven in use. This applies where failure of the components is not evident in the process.

- Categories 2, 3 and 4: since recourse cannot be made to formula E.1 of the standard for calculation of the DC_{avg} owing to the unavailability of $MTTF_D$ values, the DC_{avg} is formed in this case simply as the arithmetic mean of the single DC values of all components in the functional channels of the output part.

6 Handling of requirements concerning SRESW (safety-related embedded software) where standard components are used

The use of bought-in industrial standard components not developed specifically for use in safety functions and containing embedded software was not previously addressed in its own right in the standard. Numerous examples of SRP/CS exist in practice however that make use of standard components such as programmable logic controllers (PLC), frequency converters or sensors and that achieve safety for example by diverse redundancy with fault detection at system level. An example employing a standard PLC and a standard frequency converter is shown in Annex I of the standard. Since observance of the SRESW requirements is not generally confirmed by the manufacturer for such standard components and cannot be performed subsequently by the integrator, satisfaction of the SRESW requirements could often strictly speaking not be demonstrated in the past.

Amendment 1 now dispenses with the need for satisfaction of the SRESW requirements be demonstrated, provided the following conditions are met:

- The SRP/CS is limited to PL a or PL b and uses Categories B, 2 or 3.

- The SRP/CS is limited to PL c or PL d and may use multiple components for two channels in Categories 2 or 3. The components of these two channels use diverse technologies. The required diverse technologies in the two channels lead to a significantly lower probability of a dangerous failure of the SRP/CS due to a fault in the SRESW.

Besides the SRESW requirements, the standard sets out further more hardware related requirements, concerning for example the avoidance and control of systematic faults and suitability for the expected environmental conditions such as climate, vibration and electromagnetic compatibility. These additional requirements continue to apply irrespective of SRESW. They also include the requirement for basic safety principles to be applied from Category B upwards and well-tried safety principles from Category 1 upwards. In addition, for all Categories, the basic requirement of Category B must be met that the SRP/CS must be designed, constructed, selected, assembled and combined at least in compliance with the relevant standards, for example with EN 61131-2 for PLCs or EN 61800-1/-2 for standard frequency converters.

Development with quality assurance in accordance with ISO 900x is not made an explicit requirement by the standard; however, it constitutes an intelligent requirement that is reflected in the seven basic measures for PL a and b in Section 4.6.2 of the standard that apply to SRP/CS with embedded software (SRESW) developed in-house.

7 Chapter 5, Safety functions

A provision has been added at this point stating that depending upon the application, it may be advantageous to define a separate safety function without power available. An example are vertical axes which must be prevented from lowering under gravity even in the event of loss of power. Where power is available, the axis is held for example by an electric drive, whereas in the event of power loss a mechanical brake is applied (see [4] section 4.3 and 6.4.2. as well as example 14).

8 Chapter 6, Categories

It was previously permissible in Category 2 "only" to provide a warning of the hazard when the initiation of a safe state following detection of a fault is not possible (e.g. welding of the contact in the final switching device).

It is now specified explicitly – depending on the PLr – in which case a warning alone is permissible:

- For PL_r a up to and including PL_r c, **whenever practicable** the output (OTE) shall initiate a safe state that is maintained until the fault is cleared. When this is not practicable (e.g. welding of the contact in the final switching device), it may be sufficient for the output of the test equipment (OTE) to provide a warning.

- For PL_r = d, the output (OTE) **shall** initiate a safe state that is maintained until the fault is cleared. In this case a warning is not sufficient.

9 Chapter 6, Combination of SRP/CS

Manufacturers of almost all bought-in SRP/CS (encapsulated subsystems) now also state the PFH_D value in addition to the PL (or SIL). On SRP/CS developed in-house, these values are in any case available. The following procedure can therefore be followed for combination (in series) of SRP/CS that together execute a safety function:

- Limitation by non-quantifiable aspects: the total PL is at most as great as the lowest PL of all combined SRP/CS.

- Limitation by quantifiable aspects: the total PL is also at most as great as the PL corresponding to the summated PFH_D in accordance with Table 3 of the standard. The summated PFH_D is formed as the sum of all PFH_D values of all combined SRP/CS.

The combination method according to Table 11 of the standard is now intended only as an exception for cases in which only PL values and no PFH_D values are available for the combined SRP/CS.

10 Annex A, Determining of the PL_r

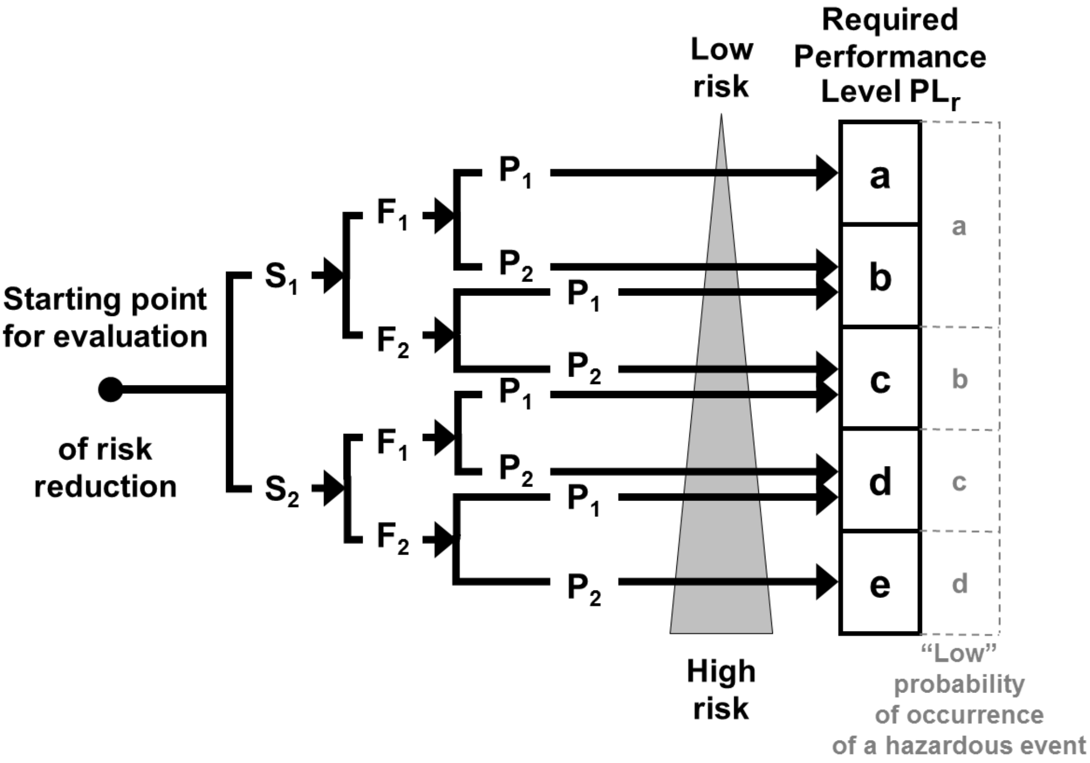
Several changes have been made to Annex A. Firstly, substantially more emphasis is now placed upon the informative character of the method described here for determining the PL_r. This method is not binding and constitutes only an estimate of the risk reduction. Owing to the normative compromise reached in the group of experts in consideration of reasons that may also lie outside the parameters of the risk graph, it is acceptable for Type C standards to contain provisions concerning the PL_r that deviate from the PL_r that would be produced from the risk graph.

The comment for distinguishing between F1 and F2 is now formulated as follows:

- In case of no other justification, F2 should be chosen if the frequency is higher than once per 15 minutes.
- F1 may be chosen if the accumulated exposure time does not exceed 1/20 of the overall operating time and the frequency is not higher than once per 15 minutes.

The probability of occurrence of a hazardous event has now been added. If this quantity can be justified as low, the PL_r may be reduced by one level. A further reduction of PL_r a is not intended, see Figure 1.

Figure 1: Determination of the PL_r from the risk parameters S, F und P with additional possibility of reduction taking into account the probability of occurrence of a hazardous event (on the basis of the graph in Annex A of the standard)


Low risk
Required Performance Level PL_r
Starting point for evaluation
of risk reduction
S_1
S_2
F_1
F_2
F_1
F_2
P_1
P_2
P_1
P_2
P_1
P_2
P_1
P_2
a
b
c
d
e
a
b
c
d
High risk
"Low" probability of occurrence of a hazardous event

The probability of occurrence of a hazardous event is known from ISO 12100 (there “occurrence of a hazardous event”) and called O parameter in ISO/TR 14121-2 (Pr parameter in EN 62061). It is mentioned in the standard in conjunction with the P parameter, but both are determined independently. The determination is dependent upon human behaviour or technical failure and is generally very difficult to assess with the required statistical reliability. Reliability data and history of accidents on comparable machines (with the same risk, same process, same operator action and same technology causing the hazard) may justify the assessment. Where the history of accidents is concerned, it must be considered that it is generally based upon technical protective measures that have already been installed, and not upon the situation prior to specification of the intended safety function (starting point of the risk graph). A low number of accidents could therefore confirm the existing PL_r assessment upon which the history of accidents is based. It does however not justify assessing the PL_r to be specified as being lower than is currently the case.

In a new Section A.3, the standard now addresses the subject of overlapping hazards and clarifies that each hazard can be assessed separately during the risk assessment. The safety functions for separate hazards may be separated, as a result of which only the power control elements for **one** hazard arise as the output of the associated SRP/CS (and are input into the PFH_D). In a manufacturing cell involving multiple robots, the safety-related stop functions, for example in response to opening of a safety door, can therefore be defined individually as separate safety functions for each robot. The same consideration applies for example when a rotary table features multiple clamping devices. However, when multiple hazards in a part of a machine are directly connected to each other, it is advisable for them to be considered together in a combined safety function. An example is a welding robot in continual use on which an operator is exposed at one and the same time to the hazards of crushing by movement and burning by the welding process, both hazards being presented by the tool centre point. More detailed explanations on the analysis of overlapping hazards can be found in [5, 6]

11 Annexes C and D, $MTTF_D$ values

Changes shown by industrial practice to be necessary have been made at several points in Table C.1, "Good engineering practices method":

- For hydraulic components (essentially, valves), higher typical $MTTF_D$ values can now be applied as a function of the mean number of annual operations n_{op}. The previous $MTTF_D$ value of 150 years can be doubled to 300 years when n_{op} < 1,000,000 cycles per year. Even less frequent actuation (fewer than 500,000 or 250,000 cycles per year) leads to further doubling (to 600 and 1,200 years respectively). The estimation has thus been brought more closely into line with that for pneumatic components.

- The typical B_{10D} value for contactors under nominal load has been reduced from 2,000,000 to 1,300,000 cycles per year. The reason is that the product standard for contactors (EN 60947-4-1) states 74% as the proportion of dangerous failures.

- The two lines for emergency-stop devices have been merged. Emergency-stop devices and enabling devices can be assessed as Category 1 or Category 3/4 sub-systems, depending upon the number of electrical output contacts and fault detection in the downstream SRP/CS. Each contact element (including the mechanical actuation) can be regarded as a channel with a relevant B_{10D} value of 100,000 cycles. For enabling switches, this encompasses both break functions, i.e. fully depressing and releasing. ISO 13849-2, Table D.8, according to which fault exclusion is permitted under certain conditions, can also be applied independently of the above. The revised BGIA Report 2/2008e will contain detailed explanations for the modelling of emergency stop devices, enabling switches, position switches, guard-locking and push buttons.

The "$MTTF_D$ for components, worst case" column has been deleted from Tables C.2 to C.7 for semiconductors and passive components. The figures stated there with a safety factor of 10 compared to the typical case are of no practical relevance, since more suitable failure data are available in any case directly from the manufacturer for the majority of components of this type, and the "typical" case is otherwise adequate for the purpose of estimation.

Typical values are now also applied for the electrical components in place of the worst case for the "parts count method" in Table D.1.

12 Annex E, Diagnostic coverage

Two measures have been deleted from Table E.1 owing to their lack of practical relevance:

- Redundant shut-off path with no monitoring of the actuator (DC = 0%).
- Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment (the DC is to be estimated individually for each shut-off path; analysis in combination is not appropriate).

The DC measure of "fault detection by the process" is now described in more detail:

- For estimation of the DC in the range stated from 0 to 99%, all relevant dangerous failures can first be identified, and of these the failures can subsequently be determined that are detected in the process. From the detected proportion, one of the values can then be estimated from none (0%), low (60%), medium (90%) or high (99%).
  This provision applies by analogy to other measures for which a DC range is stated, for example "indirect monitoring".
- This measure may of course be used for a component only when dangerous failures of the component concerned are actually apparent in the (production) process. When components in the safety path are only actuated on demand of the safety function, fault detection by the process cannot be assumed for these components.

13 Annex F, CCF

Clarity has been improved or information added at certain points in Table F.1.

14 Annex I, Illustrating examples

Certain information has been updated in Annex I (examples) in order for the content to be brought more closely into line with the rest of the standard, particularly Annexes C to F. For example, the $\mathrm{MTTF_D}$ values of both switches and of the contactor are now determined from $\mathrm{B_{10D}}$ values via n_{op}.

15 Conclusion

The Amendment 1 of ISO 13849-1 has made great contributions for improved applicability by integrating many proposals arising from practical needs throughout the last years. The changes fit neatly into the concept of the standard, so that in general for existing SRP/CS no re-assessment is necessary. Although some experts recommended a fundamental revision of the requirements for the design of safety-related software, this was not possible within the framework of this amendment.

The IFA will support the improvements of the amended standard by successively updating their well-established tools, available at www.dguv.de/ifa/13849e. The Performance Level Calculator disc [7] has already been updated. The software tool SISTEMA will include all changes in its version 2.0 and also the reports 2/2008e and 7/2013 including the circuit examples will be adapted to the new content of the standard.

16 References

[1] ISO/TR 23849: Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (05.10). Beuth, Berlin 2010

[3] Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) No 6, pp. 34-37
http://www.dguv.de/webcode/m199422

[3] Hauke, M.; Apfeld, R.: The SISTEMA Cookbook 4: When the designated architectures don't match. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2012
http://www.dguv.de/webcode/e109249

[4] Apfeld, R.; Zilligen, H.; Köhler, B.: Safe drive controls with frequency converters (IFA Report 7/2013e). Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2014
http://www.dguv.de/webcode/e635980

[5] Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachausschuss-Informationsblatt Nr. 047, Ausgabe 5.2010. Hrsg: Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau, Mainz
http://www.bghm.de/fileadmin/user_upload/Arbeitsschuetzer/Praxishilfen/Fachbereichs-Informationsblaetter/047_MFS_A2010-05_ueberlagerteGefaehrdung.pdf

[6] Apfeld, R.; Schaefer, M.: Safety functions to EN ISO 13849-1 where multiple overlapping hazards are present, IFA, Sankt Augustin 2011
http://www.dguv.de/webcode/m203682

[7] Performance Level Calculator Disc. 5th ed. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2015
http://www.dguv.de/webcode/e20892

Authors: Michael Hauke, Ralf Apfeld, Thomas Bömer, Michael Huelke, Paul Rempel,
Björn Ostermann
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA),
Sankt Augustin, Germany