DGUV
Deutsche Gesetzliche
Unfallversicherung
Spitzenverband

Fourth edition of EN ISO 13849-1 Most important new features in 2023 at a glance

Overview

The International Organisation for Standardisation (ISO) has published a new version of the basic safety standard for machine controls, ISO 13849-1 “Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design” [1]. A quarter of a century after the first publication of this standard, this is now a completely revised and modernised version. There is still quite some time before the EU Standard EN 13849-1 is harmonised, before the transitional three-year period has been completed and before the new version becomes binding. Yet it is nevertheless worth taking an early glimpse at its new features.

Whereas the changes in the third edition of 2015 were merely editorial, to improve readability and usability, the latest update contains a range of more substantial adjustments and additions. For instance, the core sections “Design considerations”, “Safety functions” and “Categories”, which had grown and been supplemented since 1997, were systematically reorganised in order to map – after an “Overview” – first the “Specification of safety functions” and then the design process. Also, the role of subsystems within a safety chain has now been defined in more detail – especially concerning the integration of subsystems that have been given safety integrity levels (SILs) under IEC standards (IEC: International Electrotechnical Commission) on functional safety. The final design stage of validation, which was previously included in part 2 of the standard, has now been placed in part 1 as section 10 – largely unchanged in terms of content – so as to clearly emphasise its importance in the context of safety-oriented design. Further important improvements are the more detailed presentation of requirements for safety-related software and the newly included strategies for the practical implementation of electromagnetic interference immunity.

The following article provides a detailed presentation of the main changes and, where necessary, recommendations for interpretation.

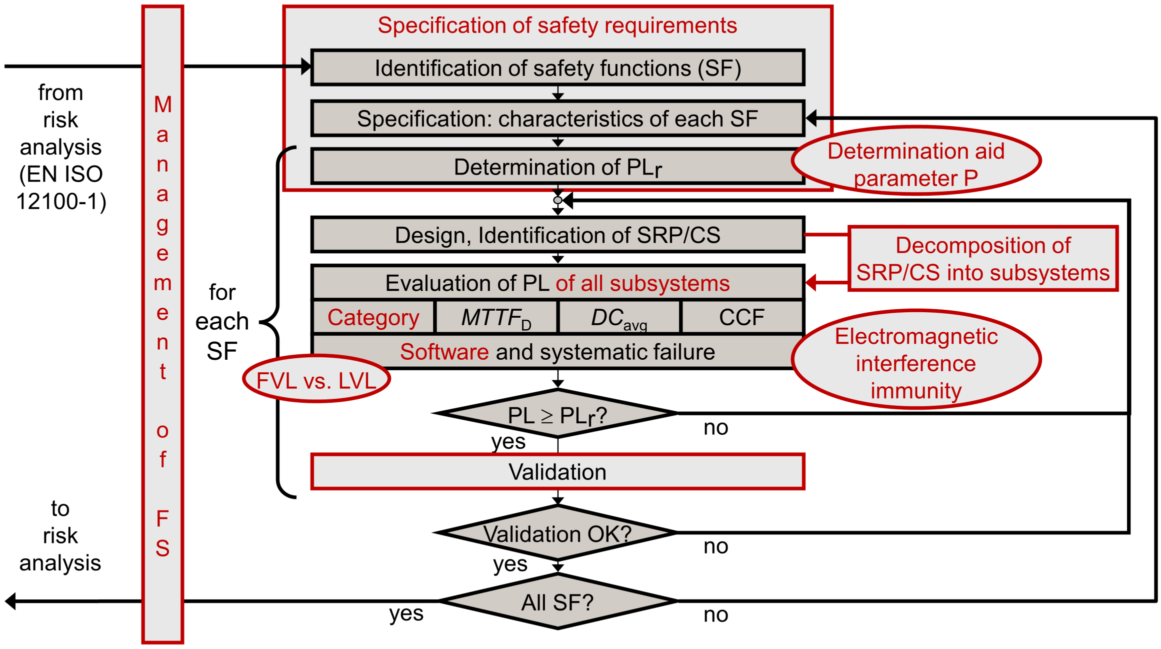
from risk analysis (EN ISO 12100-1)
Management of FS
Specification of safety requirements
Identification of safety functions (SF)
Specification: characteristics of each SF
Determination of PLr
Determination aid parameter P
Design, Identification of SRP/CS
Decomposition of SRP/CS into subsystems
Evaluation of PL of all subsystems
Category
MTTFD
DCavg
CCF
Software and systematic failure
Electromagnetic interference immunity
for each SF
FVL vs. LVL
PL ≥ PLr?
yes
no
Validation
Validation OK?
yes
no
All SF?
yes
no
to risk analysis

Illustration: Major changes to the design process for SRP/CS in the fourth edition of the standard

1 Introduction

Regarding the scope of the standard, a new note clarifies that its content is geared towards stationary machinery, although other types of machinery, such as mobile machinery, are also expressly covered.

The position of the standard in the iterative process of risk reduction under EN ISO 12100 is now presented in more detail. The informative Annex A of the standard can be used in this context to determine the required performance level (PL_r) unless it is specified in a product standard (type-C standard).

Unlike the preceding version, this edition of the standard specifies in more detail that it can also be used, for instance, for the integration of logic units and electro-sensitive protective equipment into safety-related parts of control systems (SRP/CS) as well as for the design of subsystems using safety components, such as two-hand control devices, interlocking devices, relays, valves, position sensors and enable switches.

The reference to Technical Report ISO/TR 23849 [2] on the application of ISO 13849-1 and IEC 62061 – withdrawn in 2020 – was deleted. That content is now included in the current editions of both standards. Both standards have been harmonised under the Machinery Directive and can be used for the design and integration of safety-related control systems of machinery (including software) (see also below, section 6).

Concerning the adoption of validation requirements from part 2 of the standard in section 10, the authors clarify that the more recent requirements from part 1 take priority during the transitional period until the revision of EN ISO 13849-2 has been completed. At the same time, it can be assumed that they will be met as soon as the validation requirements from part 2 have been implemented.

2 Section 1: Scope

As in the previous edition, the authors point out that the standard only applies to SRP/CS for a high demand or continuous mode of operation. According to definition 3.1.44, the demand for this mode is more frequent than once a year. For SRP/CS in low demand mode, i.e. where the frequency is less than once a year – for instance in the processing industry – the authors now refer expressly to the IEC 61508 series of standards.

IT security aspects are not covered by the standard, but the authors point out that the such aspects can also impact safety functions. For further details, reference is given to ISO/TR 22100-2 [3] and IEC/TR 63074 [4].

3 Section 3: Terms, definitions, symbols and abbreviated terms

The revised standard contains a large number of new definitions, whereas some of the previous definitions have been dropped. Nearly all existing definitions have been renumbered.

It should be emphasised, in particular, that the previous "probability of dangerous failure per hour" is now referred to as "average frequency of a dangerous failure per hour". Its abbreviation has been changed back to PFH (without the "D" index), to ensure that it has the same name as in the IEC standards on functional safety. This does not result in technical changes.

4 Section 4: Overview

To meet the stated aim of an improved structure, this section starts first with items from the previous section 4 "Design Aspects" on embedding in the iterative process of risk assessment and risk reduction as specified in EN ISO 12100. Figure 2 of the standard shows, as did Figure 1, that the application of EN ISO 13849-1 must be regarded as stage 2 of the risk reduction process, i.e. as risk reduction through technical protective measures. This is followed by a brief overview of the subsequent sections of the standard, based on the typical workflow of a design process for SRP/CS: The specification of safety functions (including their PL_r) is followed by the technical realisation and specification of PLs, including their validation and documentation.

This section finishes with an overview of the basic options for realising a safety function:

- integration of subsystems that have previously been validated under a functional safety standard for machine control systems,
- proprietary design of a new subsystem based on EN ISO 13849 itself or
- combination of subsystems of both of the above options.

All requirements on the design of subsystems, including hardware and software, have been moved to section 6 and subsequent sections, as safety functions need to be defined first in the development process.

5 Section 5: Specification of safety functions and Annex M

Safety functions now need to be defined in detail as part of a safety requirements specification (SRS) The definition of each safety function continues to be based on the risk assessment and reduction process as per EN ISO 12100. The required details for a precise and complete definition of each safety function include the following items:

- brief description or title (as a unique reference),
- triggering event that demands the safety function,
- required reaction that must be initiated by the safety function in order to achieve the intended safe state,
- required performance level PL_r,
- permitted response time, i.e. the time between demanding the safety function and achieving the safe state,
- operating modes in which the safety function must be active,
- interfaces of the safety function with the machine control system and with other safety functions,
- if necessary, a description of the failure response, i.e. how the machine can be returned to a safe state after a fault has been detected in a functional channel,
- behaviour of the machine in the event of energy loss, e.g. a requirement for non-return valves directly on a cylinder or additional mechanical brakes (separation into two safety functions is also possible – one with available energy or a second one without available energy),
- demand rate for the safety function,
- prioritisation of different safety functions that can be enabled at the same time and can trigger conflicting responses,
- additional safety requirements from product standards (type-C standards),
- conditions permitting a restart after the safety function has been requested.

Further guidance on this topic can also be found in SISTEMA Cookbook 6 [5].

What follows is the familiar additional requirements for special safety functions, such as a safety-related stop function, a manual reset function, etc. Regarding a manual reset, the authors clarify that a monitored signal change is required in order to avoid foreseeable misuse. In practice, this means that a falling or rising signal edge is suitable for triggering a manual reset. As the response time now needs to be specified in general terms, it is no longer required as a separate item. As a new element, the standard specifies additional requirements for the selection of the operating mode, with a view to preventing any negative impacts on other safety functions. If operating mode selection enables or disables safety functions, it is treated as a safety function in its own right. The authors have also added notes on safety functions for maintenance and servicing tasks.

The familiar tables with references to international standards for typical safety functions in machinery and some of their characteristics have now been moved from section 5 to a new informative Annex M.

A new subsection 5.2.3 requires designers to minimise any motivation to defeat safety functions. Practical feasibility during machine use must be considered at an early stage, when defining a safety function. Another new subsection, 5.2.4, specifies that, by default, remote access must be limited in such a way that no dangerous situations can arise through the unnoticed presence of persons within the hazard zone of the machinery.

The next steps, which complete the specification phase, are the determination of the PL_r and the review of the safety requirements specification (SRS). This review must be carried out before entering the SRP/CS desgn phase, so that any specification errors can be rectified at an early stage.

The final subsection, 5.5, is about the decomposition of SRP/CS into subsystems. At this point, we can see that the standard in its fourth edition makes a clear distinction between SRP/CS and subsystems. SRP/CS describes the safety-related part of a control system that carries out an entire safety function – from the triggering event to the reaction required to either achieve or maintain a safe state. Along the hardware chain from the input (sensors) through the logic (processing) to the output (power control elements), the SRP/CS can be decomposed into subsystems, each carrying out a (safety) sub-function. The number of participating subsystems, however, may vary. As explained in the previous section, any subsystems that have previously been validated can be integrated, and subsystems can be composed of subsystem elements under EN ISO 13849. The relevant design requirements for subsystems are dealt with in the next section of the standard.

6 Section 6: Design considerations and Annex K

The new section 6 now provides not only a description of categories and combinations of subsystems, but all the properties and parameters that were previously mentioned to some extent in subsections 4.4 and 4.5 and which help to define the achieved PL.

After a general introduction, the first focus is on the correlation between PL and SIL. Referring to subsystems developed under IEC 61508 and IEC 62061, the standard only deals with the integration of those intended for use under high demand or continuous mode of operation and dsigned according to Route 1_H (see IEC 61508-2:2011, 7.4.42).

6.1 Subsection 6.1.3: Categories

When describing categories, a number of important details have changed or have been given a clearer emphasis:

- **Category assignment at the subsystem level (6.1.3.1)**
  A neat distinction between SRP/CS and subsystems must involve the assignment of a category to each subsystem developed under EN ISO 13849. It follows that an SRP/CS may also include subsystems of different categories and subsystems with SIL classifications.

- **Proven Category 1 components (6.1.3.2.3)**
  Whilst the content of Category 1 requirements has not changed much, the description for well-tried components has now been moved to a separate subsection 6.1.11, where direct reference is made to the well-tried components listed in EN ISO 13849-2 for various technologies and where informative reference is made to the concept of “proven in use”, as defined in IEC 61508. It is now part of the standard (and no longer a comment) that complex components are unsuitable as well-tried components.

- **Testing in Category 2 (6.1.3.2.4)**
  In the future, the main feature of Category 2 will be fault detection in the functional channel instead of the checking of the safety function. This clarifies that what is required is not necessarily the checking of the entire sub-function of a Category 2 subsystem (which might be interpreted as 100% fault detection), but that effective fault detection is required in the functional channel – and indeed for each of its parts (input unit, logic and output unit), at least with “low” diagnostic coverage (DC), i.e. 60% fault detection.
  Two conditions were previously mentioned only in the context of the simplified procedure for estimating the quantifiable aspects of the PL. They now apply generally under Category 2:

The test rate must be at least 100 times higher than the demand rate, or testing occurs immediately upon demand of the safety function and prevents the hazard. This does not affect the exceptional case in Appendix K where a test rate is described that is only 25 times higher.
Also, the mean time to dangerous failure ($MTTF_D$) of the test channel (including OTE, output of test equipment) must be greater than half the $MTTF_D$ of the entire functional channel.

- **Fault accumulation in Category 4 (6.1.3.2.6)**
  A new note has been added to clear up a possible misunderstanding when implementing Category 4. In a failure mode and effects analysis (FMEA), it is sometimes impossible to classify 100% of theoretically possible dangerous failures as detectable. This is why “only” a high DC of 99% is required for PFH calculation in Category 4. On the other hand, according to the definition of Category 4, the accumulation of (up to two) undetected dangerous failures must not lead to the loss of the safety function. If there were indeed an undetected dangerous failure with practical relevance, the second dangerous failure could then lead to the failure of a Category 4 structure. This is where the new note becomes relevant: Undetected failures with a very low probability (theoretically conceivable, but practically irrelevant) do not need to be factored into the fault accumulation – provided that this fault consideration is documented and verified.

6.2 Subsection 6.1.4: $MTTF_D$

The list of possible data sources for estimating an $MTTF_D$ value has been updated to include a new option: Reliable field data for identical component applications from similar applications can be used if there are no manufacturer’s details and if the methods in Annex C (including good engineering practice method) are not applicable.

6.3 Subsection 6.1.6: CCF

The requirement to avoid common cause failures is now specified in a separate subsection 6.1.6, which refers to the familiar Annex F for guidance on practical implementation.

6.4 Subsection 6.1.7: Systematic failures

A separate subsection 6.1.7 has now been added, to provide for the requirement of avoiding and controlling systematic failures. What is new is the express requirement for a functional safety plan that defines functional safety management in order to protect against systematic failures in specification, implementation or modification. The relevant details have been added to Annex G (see section 15 of this article).

6.5 Subsection 6.1.8: Simplified procedure, bar chart and Annex K

The simplified procedure for estimating quantifiable aspects of a PL, including the bar chart (now Figure 12 in the standard) can now be found in subsection 6.1.9. There are only two major changes: The requirements on the test rate and the reliability of the test channel now apply generally to Category 2, as mentioned above. Secondly, the authors of the standard have removed the previous edition’s Table 6, which was the bar chart in the form of a simplified table.

6.6 Subsection 6.1.9: Alternative procedure to determine the PL and PFH without MTTF$_D$

The alternative procedure introduced for the output part of an SRP/CS in the previous edition of the standard has now been modified and extended to include the input and logic parts. At the same time, it has been limited in its application: It continues to apply to subsystems containing mechanical, (electro-)hydraulic and (electro-)pneumatic components for which no reliability data is available. Now, however, it only applies if it is impossible to use the good engineering practice method provided in Annex C.2 of the standard.

The familiar procedure for the output part (energy transfer elements) is now also applicable to the input part. However, an additional requirement in Categories 2, 3 and 4 is that, like in Category 1, only well-tried components are permitted. The alternative use of proven in use components has been omitted.

A new approach has been added for the logic part: Category B, 2 and 3 subsystems may use an estimated value of ten years for the MTTF$_D$ of each channel. In Category 1, this estimate has been increased to 30 years, as well-tried components are required. This method is not permitted for logic subsystems in Category 4. The achievable maximum is PL c.

6.7 Subsection 6.1.10: Fault consideration and fault exclusion

The previous section 7 of the standard on fault considerations and fault exclusions has now been moved to subsection 6.1.10 and has been given a more detailed introduction. In addition, a restriction is mentioned that was previously only known from ISO/TR 23849 [2]: A PL e for subsystems must not be based on fault exclusions alone.

6.8 Subsection 6.2: Combination of subsystems

As well as making a clear conceptual distinction between subsystems and SRP/CS (as a combination of subsystems), the preferred method of adding familiar PFH values has been separated more distinctly from the alternative, table-based method for subsystems without PFH.

6.9 Subsection 6.3: Software-based manual parameterisation

The requirements on software-based parameterisation of safety-related parameters are now intentionally distinct from the rest of the software part of the standard. Furthermore, the authors emphasise that this only involves manual, software-based parameterisation by authorised persons. This includes, for example, parameterisation using specially designated parameterisation tools, but not parameterisation based on DIP switches (DIP: dual in-line package) and not automated parameterisation or direct control of a machine by an operator, e.g. speed control of a forklift truck. Two things are new: firstly, additional information on possible influences that can lead to incorrect parameterisation, and secondly, more detailed requirements on the documentation of parameterisation processes.

7 Section 7: Software safety requirements and Annexes J and N

The requirements on the development of safety-related software are now summarised in a separate section 7. In the introduction, the authors state that the section does not contain any specific requirements on software using artificial intelligence.

The V model of the software safety lifecycle provides more precise details of the verification steps (reviews and tests) and the results of the phases. It also covers documentation that is written further down the line, i.e. documentation that gets increasingly more detailed. What is new is a simplified two-stage version of the V model for programming languages with limited variability languages (LVL) that use validated function blocks and run as application programs (SRASW) on verified hardware. Here, the programming typically implements only simple logical assignment of input and output blocks, so that the safety-related software specification can proceed directly to the coding phase.

Safety-related embedded software (SRESW) usually requires a full variability language (FVL), while SRASW can also be written in LVL. The software section has now been supplemented to include a new decision-making aid for classifying a programming language as either LVL or FVL. Programming languages are considered LVL if they comply with IEC 61131-3 [6] – ladder diagram, function block diagramm, sequential function chart and Boolean algebra. But a programming language can also be classified as LVL if a defined programming flow has been put in place through restrictions realised by programming guidelines, compilers or development tools.

Whereas the requirements on SRESW were previously only described rather briefly, the new edition of the standard now contains exemplary extended guidance for all measures, both basic and additional. Further detailed information can be found in IFA Report 1/2020 [7].

The boundary conditions for the option of using components with non-accessible embedded software have been updated: The diversity requirement for PL c and d can now be met not only through different types of technology, but also through different types of design. The authors have clarified that the associated hardware and existing SRASW must meet the requirements of the standard.

The software measures, graded according to PL_r and available diversity, cannot always be directly and unambiguously assigned in each instance. This is where part one of the new informative Annex N should be helpful: First, one of four use cases can be specified from within the application – use cases that are based on the PL (a/b, c, d or e) but which can be downgraded by one level, depending on where the software is used. Such downgrading is possible for software in the test channel of Category 2 or in diverse functional channels of Category 3 or 4. Based on the applicable case, it is then possible to identify the mandatory and recommended individual measures in two tables.

Part two of the new Annex N demonstrates software validation through analysis and testing, using the example of an SRASW based on validated function blocks.

The example of the SRESW implementation in the informative Appendix J has been adapted to the current V model of the software safety lifecycle.

The previous subsections on the verification of the achieved performance level and on ergonomic aspects of the design have become sections 8 and 9 without any major changes.

8 Section 10: Validation

The new section 10, Validation, has been taken over entirely from sections 4 to 12 of EN ISO 13849-2. Except for some restructuring, the content and the requirements have essentially remained unchanged. They follow familiar patterns in dealing with validation principles, including a validation plan, validation protocol and validation through analysis and testing. Validation primarily concerns the specification of safety requirements as well as safety functions, safety integrity (effectiveness of safety functions), including categories, hardware, software as well as requirements on the operating environment and user information. The overview of the validation process makes it clear that, irrespective of the category, at least a functional test of the safety functions is required in addition to the analysis.

By using the validation requirements from the less familiar part 2 of the standard, the aim is to emphasise validation as an important measure against faulty specifications, faulty design and faulty implementation, and to reinforce their practical implementation. In the long term, after a revision of part 2 of the standard – a revision that will be limited to the tables and the validation examples in the Annexes – there are plans to migrate the entire part 2 into part 1 of the standard. Until then, the validation requirements in the two parts of the standard will continue to be compatible, so that there will be no inconsistencies.

9 Section 11: Maintainability of SRP/CS

The previous section on maintenance has been extended to include the aspect of maintainability, so that accessibility, ease of use, visibility, simplification and automatically generated maintenance advice are now also included.

10 Sections 12 and 13: Technical documentation and information for use

Minor amendments have been made to the previous requirements on the (manufacturer's in-house) technical documentation, and the requirements on the information for use have been divided into two subsections: the first subsection is for SRP/CS integrators, providing a detailed list of technical parameters, and the second one is for machine users, providing details on operation, displays, cleaning, maintenance, etc.

11 Annex A: Determination of PL_r

The informative Annex A on the determination of the PL_r contains two significant changes.

The parameters "possibility of avoiding or limiting harm" (Parameter P) and "probability of occurrence of a hazard event" are no longer merged. The "probability of occurrence of a hazard event" is now merely mentioned in passing and, to be on the safe side, is generally estimated as being high (100%). In cases where a low estimate is possible, the PL_r that has been determined via the risk graph can be downgraded by one level. What is new is that this decision must be justified and documented. The fourth edition of the standard no longer specifies how to determine the "probability of occurrence of a hazard event", so that only edition 3 of the standard can be used for information purposes here, as EN ISO 12100 does not provide much information on this risk element, either.

On the other hand, more detailed assistance is offered for the determination of parameter P, based on five factors. Three of these factors are each alone sufficient to justify the choice of P2 (avoiding or limitating of harm scarcely possible) if they are unfavourable: the speed with which the hazardous situation arises, the possibility of avoiding the hazard in terms of physical space, and the perceptibility of the hazard. The other two factors only justify the choice of P2 in combination with other unfavourable factors: first, whether the machine is used by skilled persons and, second, the complexity of its operation.

12 Annexes C and D: $MTTF_D$ values

If the manufacturer of a component with mechanical wear, e.g. a pneumatic or electromechanical component, specifies only a B_{10} value instead of a B_{10D} value (number of cycles until 10% of the components have dangerously failed), then the rate of dangerous failures RDF – where known – can be used for the conversion according to the relationship $B_{10D} = B_{10}/RDF$. Up to now, there has only been the indication that 50% dangerous failures should be assumed as an estimate, i.e. $B_{10D} = 2 * B_{10}$. However, even in the new edition of the standard, the additional condition applies that the T_{10D} value is limited to a maximum of $2 * T_{10}$ where the RDF is below 50%. This increases the B_{10D} value (and the $MTTF_D$ value derived from it) for a small ratio of dangerous failures, but not the T_{10D} value, i.e. the time after which a component with mechanical wear must be replaced in order to maintain the identified PL.

13 Annex D: Diagnostic coverage

In Table E.1 with examples of fault detection measures, there are now additional notes for the estimated DC, where previously a range of achievable DC values was provided:

- An FMEA (failure mode and effects analysis) must generally be used as the basis for determining the DC in the actual application.

- When monitoring outputs and cross-monitoring input or output signals without dynamic testing, the test rate resulting from the relevant application can act as a limiting factor for the DC, e.g. by allowing only tests that occur at least once a month to achieve a DC of 99%, and by estimating tests at a DC of 0% if they occur less frequently than once a year.

- For fault detection by the process, the ratio between the process diagnostic rate (test rate) and the demand rate of the safety function can be used to limit the achievable effective DC value down to a value of 60%.

- Several DC measures acting on a component can be combined to achieve a higher DC. Furthermore, this combination of DC measures can overcome the limitation that fault detection by the process is insufficient as the only measure for PL_r e.

14 Annexes F and I: CCFs and examples showing the simplified procedure to estimate PL

Measures against common cause failures (CCFs) are now only listed in Table F.1, but are described in more detail than previously in the new subsection F.3. A new note has been added, emphasising that where SRP/CS are not sufficiently protected against over-voltage or other environmental influences at the component level, the required protection can also be achieved at the system level, e.g. through external protection components, filters or shielding. Anti-CCF measures are usually assessed at the subsystem level, as they can differ from one subsystem to another. The assessment must be based on expected use, including foreseeable faults and reasonably foreseeable misuse. An engineering assessment serves to eliminate typical causes of CCF wherever possible or to reduce the effects of the causes. This assessment, too, must be documented.

Accordingly, in the second example in Annex I, which serves to illustrate the simplified procedure for estimating the PLs of subsystems, the anti-CCF measures are now each specified in detail.

15 Annex G: Systematic failure and functional safety plan

The reference to Annex F of IEC 61508-2 on avoidance of systematic failures in the design of ASICs, FPGAs and PLDs has been removed, but continues to be implicitly applicable.

A new subsection G.5 specifies how functional safety management methods can be used to implement the standard requirements arising from section 6.1.7. The aim is to specify a systematic approach to designing and implementing SRP/CS and thus to prevent faulty specification, implementation and modification. The centrepiece is a functional safety plan that documents all activities in this regard. Its form and extent depend, for example, on the project size, complexity and novelty. Its purpose is to identify all the relevant activities throughout the design process, from specification to validation and modification, and to describe the relevant responsibilities, resources and procedures.

16 Annex L: Electromagnetic interference immunity

Since the third edition of the standard, there has been the introduction of a new generic standard – IEC 61000-6-7 [8] – on immunity requirements for safety-related functional safety systems. To facilitate their implementation, a new informative Annex L now provides guidance on the implementation of the required measures for electromagnetic interference immunity. Depending on the application, four alternative options are provided:

A. Electromagnetic immunity requirements from an applicable product standard have the highest priority (independent of the PL that is to be achieved) and override the general requirements of the generic standard.

B. For PL a and PL b, compliance with the lower immunity requirements of IEC 61000-6-2 [9] for industrial settings that are not designed for functional safety is considered sufficient.

C. Up to PL d (and even up to PL e if the requirements for category 4 are met), the necessary immunity can also be achieved through protective measures at the system level, such as shielding, filters, interference-resistant cables, separation, fault detection or risk analysis, instead of through interference immunity tests. This alternative verification strategy is also expressly mentioned in IEC 61000-6-7, 4.1, Note 1. Table L.1 of the standard lists 23 different measures for this purpose, with compliance resulting in 10 to 30 points. The immunity requirements are considered to be met if the total score for two-channel systems (Categories 2, 3 and 4) is at least 280, or if the total score for single-channel systems (Categories B and 1) is at least 230. Five measures are not applicable to single-channel subsystems. Eight of the listed measures are marked as strongly recommended: If they are applicable but have not been implemented, detailed justification must be provided as to how immunity is to be achieved in an equivalent manner.

D. Up to PL e, compliance with the increased immunity levels can be demonstrated by applying IEC 61000-6-7 or other general EMC standards on functional safety, such as IEC 61326-3-1.

17 Annex O: Device types

A new Annex O defines four device types and associated characteristic values, which must be specified, for example, in the manufacturer’s data sheet. While subsystems (device types 1 and 4) are usually specified in terms of PL (or SIL), PFH, category (or hardware fault tolerance) and mission time, subsystem elements are usually described in terms of $\mathrm{MTTF_D}$ or λ_D (device type 2) or B_{10D} (device type 3) in conjunction with their mission time. Further information can be found in the VDMA specification 66413 (universal database) [10].

18 Conclusion

The fourth edition of EN ISO 13849-1 is the result of a thorough overhaul of the standard. A clearer structure has been created on the basis of proven concepts, and further application aids have been added. Although the number of pages has increased substantially as a result, so has its ease of use.

The IFA’s known application aids for EN ISO 13849 are gradually being adapted to the changes in the standard and are being made available at www.dguv.de/ifa/13849e. The SISTEMA software wizard will contain all the changes in version 3.0, and the IFA Reports 2/2017 and 4/2018, including the circuit examples, will also gradually be updated to reflect the new version of the standard.

19 References

[1] ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (04.23).

[2] 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).

[3] ISO/TR 22100-2: Safety of machinery – Relationship with ISO 12100 - Part 2: How ISO 12100 relates to ISO 13849-1 (12.13).

[4] IEC/TS 63074: Safety of machinery – Security aspects related to functional safety of safety-related control systems (02.23).

[5] Apfeld, R., Hauke, M. and Otto, S.: The SISTEMA Cookbook – Part 6: Definition of safety functions: what is important? – Version 1.0 (EN). Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015
https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook6_en.pdf

[6] IEC 61131-3: Programmable controllers - Part 3: Programming languages (02.13).

[7] Bömer, T., Büllesbach, K.-H., Hauke, M., Otto, S. and Werner, C.: Practicable implementation of the requirements concerning safety-related embedded software to EN ISO 13849-1 (IFA Report 1/2020e). Published by: The German Social Accident Insurance (DGUV), Berlin 2021.
https://publikationen.dguv.de/DguvWebcode?query=p021987

[8] IEC 61000-6-7: Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations (10.14).

[9] IEC 61000-6-2: Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments (08.16).

[10] VDMA 66413: Functional Safety – Universal data format for safety-related values of components or parts of control systems (10.12). VDMA Specification, Verband Deutscher Maschinen- und Anlagenbau e.V., Frankfurt/Main 2012. Beuth, Berlin 2012

Authors: Michael Hauke, Thomas Bömer, Karl-Heinz Büllesbach
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Sankt Augustin

Publisher German Social Accident Insurance Association (DGUV)

Glinkastrasse 40
10117 Berlin
Germany
Phone: +49 30 13001-0 (Head Office)
Fax: +49 30 13001-9876
Email: info@dguv.de
Web address: www.dguv.de
Webcode: p022540