Whitepaper

Global trends in safety of machinery
New requirements for PL and SIL

Written By:
Carsten Gregorius
Product Marketing Safety
cgregorius@phoenixcontact.com

AI 04-20.001.L6

Table of contents

Introduction

Those who want to respond quickly and flexibly to customer requirements are dependent on complex and decentralized industrial production facilities. In this context, the topic of functional safety is of increasing importance. The trend of decentralization brings new challenges regarding the protection of people and the environment and the safety of machinery. Besides classical safety equipment, such as safety door interlocking systems, emergency stop equipment, or safety switches, more and more programmable or configurable safety systems for the safeguarding of machines and systems are being used as the degree of complexity increases. The availability of production equipment should not be restricted any more than is absolutely necessary.

The safety of machines and systems necessary to protect users mainly depends on the correct application of standards and directives. In Europe, the basis for this is the Machinery Directive, which provides standard specifications to support companies when designing safety-related machines. However, even outside the European Economic Area, many European standards are gaining in importance due to their international status. In this context, the standards on functional safety also play an important role. The requirements for machine control systems are specified both in EN ISO 13849 and IEC 62061.

In 2015, an attempt was made to merge the EN ISO 13849 and IEC 62061 standards into one document. Currently, both standards are being revised seperately. Publication of the modified versions is expected for 2021. For EN ISO 13849, publication is scheduled for April 2021. Until the adoption of the changed contents, likely in fall 2020, international votings will be held. Safety expert Carsten Gregorius, representing Phoenix Contact as a member in the standardization committees, explains which changes to expect with regard to PL and SIL: “In some respects, such as ‘safety-relevant software’ and the topic of cybersecurity, both standards have already become very similar. Many other detailed changes have been incorporated and, all in all, a greater consistency between the two standards results. Whether this is going to have consequences for existing safety assessments must be determined on a case-by-case basis.”

Read on for detailed information about the changes being made to the standards.

What will be the changes regarding PL and SIL?

Besides the fundamental wish to improve the readability of the standards, the work on EN ISO 13849 was focused on a clear and unambiguous specification of the **safety requirements (SRS)**. Moreover, the method for determining the **risk level** PLr, for which detailed specifications regarding the determination of the parameter P exist, will be expanded. The requirements for **safety-relevant software** in particular will be defined in more detail. Additional changes of the EN ISO 13849 relate to clarifications of the diagnostic coverage (DC) and the definition of "well-tried components". The aspect of "common cause failure" (CCF) has been detailed in EN ISO 13849 with respect to the influence of EMC.

For reasons of consistency with IEC 61508 and other sector standards, one important change was made to IEC 62061 regarding the safety characteristic data: in the future, the concept of "SIL" will be used instead of "SILCL" (SIL claim). Other than that, the method for determining the failure rates of components, as well as the validation process, have been detailed.

The parameter λ_D from the definition of failure rates of components in accordance with IEC 62061 is now related to the $MTTF_D$[1] and $B10_D$[2] definitions from EN ISO 13849.

The validation of the safety functions must prove that the requirements for the safety-relevant parts of the control system are implemented in accordance with their defined characteristics. A new element of IEC 62061 is the well-known validation process flow chart from EN ISO 13849, part 2.

Finally, both standards address the influence of **cybersecurity** on "functional safety".

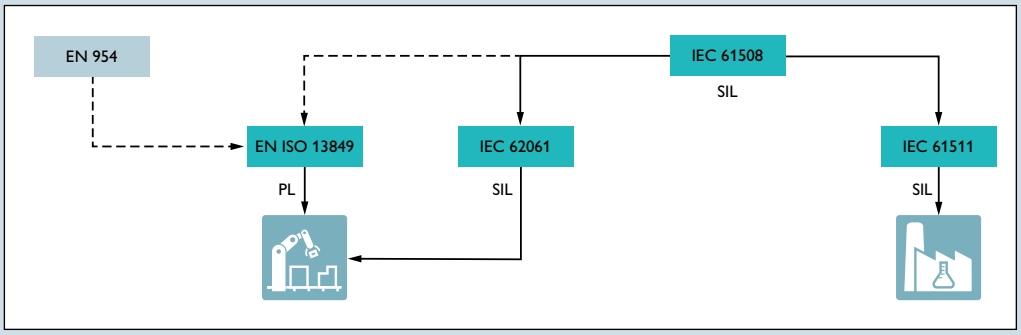
Overview of the most important changes to EN ISO 13849 and IEC 62061

EN ISO 13849	IEC 62061
Additional specifications for determining the parameter P[3] (risk level PLr)	Change of "SILCL" to "SIL"*
Unambiguous specification of safety requirements (SRS)	Consideration of low-demand applications
Precise definition of "well-tried components"	Adjustment of validation process on the basis of EN ISO 13849*
PFHD substitute values for inputs and outputs	
Precise requirements for safety-relevant software	
Influence of cybersecurity on "functional safety"	
Precise definition of "diagnostic coverage" (DC)*	Examples of failure rates ($MTTF_D$), diagnostic coverage (DC) on the basis of EN ISO 13849*
Detailed information on the "common cause failure" (CCF) with regard to the influence of EMC*	Examples of the evaluation of common cause failures on the basis of EN ISO 13849*

**These changes are not dealt with further in this white paper*

[1] $MTTF_D$ = Mean time to dangerous failure
[2] $B10_D$ = Mean number of switching cycles until 10 % of the components fail dangerously
[3] P = Possibility of avoidance of a hazardous situation

The importance of EN ISO 13849 and IEC 62061

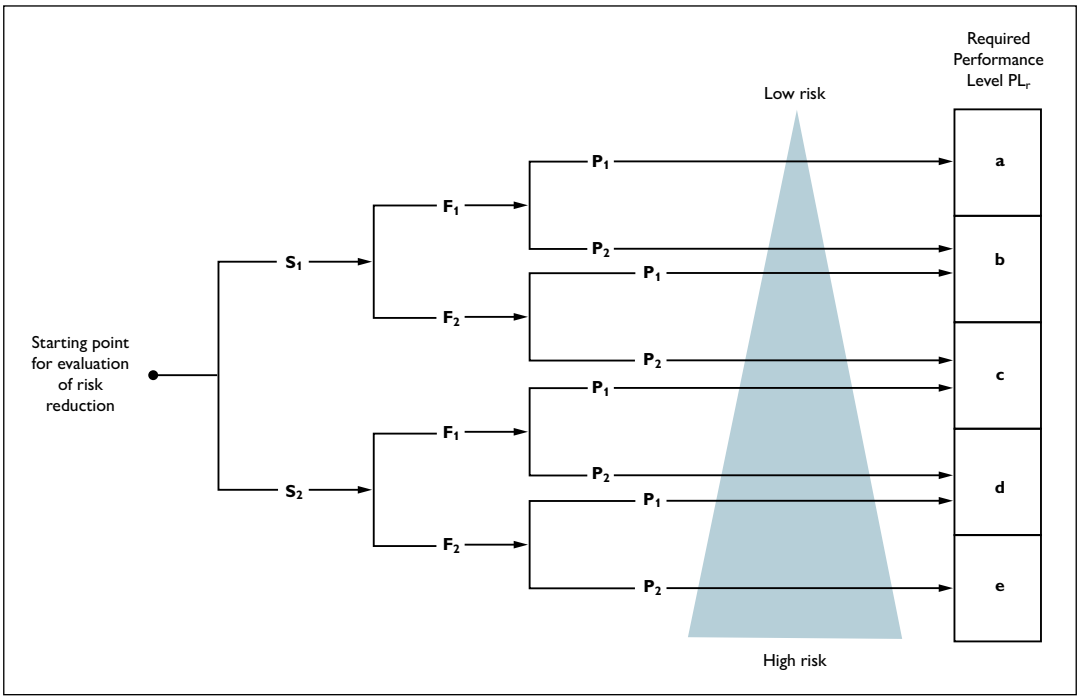


The requirements for machine control systems are specified both in EN ISO 13849 and IEC 62061. Many type-C standards refer to at least one of these standards when addressing the safe design of machinery. Both standards consider aspects from the IEC 61508 basic standard. EN ISO 13849 was developed about 20 years ago from the former EN 954, whereas IEC 62061 was developed as a sector standard for "machinery". In addition to that, IEC 61511 exists as a sector standard for the process industry, but will not be dealt with further in this document.

1. Specification of the required PLr in accordance with EN ISO 13849

The “required performance level (PLr)” is of essential importance in the process of risk reduction. Depending on the degree of risk, one of the five levels “a” to “e” is selected, taking into account the following parameters: S (seriousness of injury), F (frequency and/or duration of the exposure to the hazard), or P (possibility of preventing the hazard or limiting the harm).

In the past, the quesion often arose for parameter P when to select P1 (possible under certain conditions) or P2 (impossible).



Determination of the PLr

For determining the parameters P1 or P2, a selection guide will be provided which evaluates the aspects of qualification, velocity of hazard propagation, and complexity.

Description	A	B	C
Training	Trained personnel	Untrained personnel	–
Velocity of the hazardous movement	Low: <250 mm/s, time left until hazard is reached > 3 s	Medium: 251 mm/s -1000 mm/s, time left until hazard is reached < 3 s	High: <1000 mm/s, time left until hazard is reached < 1 s
Possibility of escaping the hazard in a specific place	> = 50 % of cases	<50 % of cases	Not possible
Possibility to recognize the hazard	> = 50 % of cases	<50 % of cases	Not possible
Complexity (number/ duration of operator interventions)	Low degree of complexity (e.g., adjustment of collets, inserting workpieces)	High or medium degree of complexity (trouble-shooting, set-up in inching mode)	–

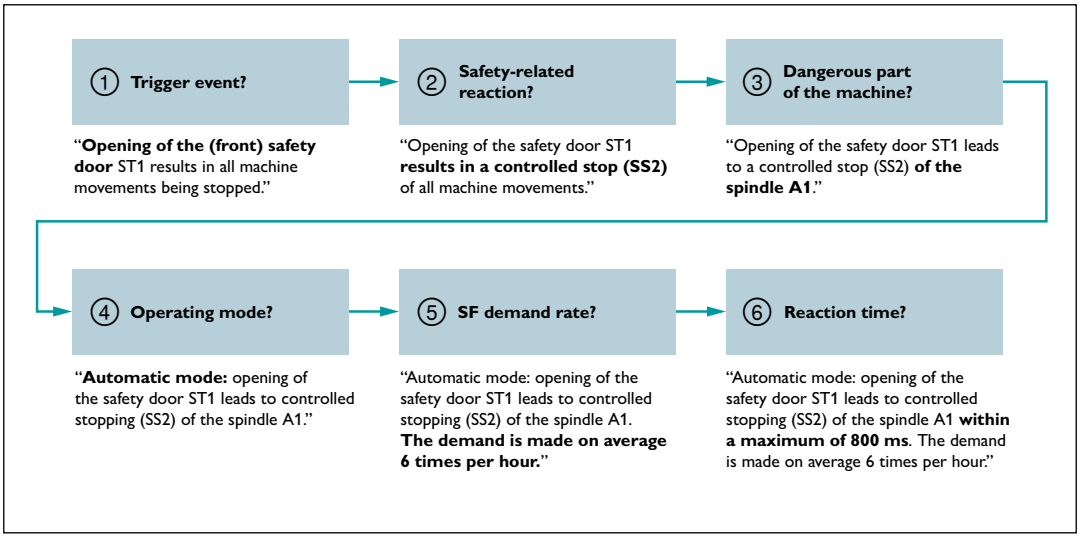
Depending on the number of resulting classifications A, B, or C, the parameters P1 or P2 can then be specified. When the evaluation process results in at least one C or three B classifications, this leads directly to a P2 classification.

2. Specification of the safety function in accordance with EN ISO 13849

Critical events related to safety-relevant control systems frequently occur due to an insufficient specification. This can mean that even if all other verfication steps are correctly taken, there may be only an insufficient risk reduction in the end. That is why the standard setters of EN ISO 13849 have placed a focus on the detailled description of what is known as SRS (Safety Requirements Specification).

The following questions should provide guidance during the validation process:

1. What is the trigger event?
2. What ist the safety-related reaction?
3. Which are the dangerous parts of the machine?
4. In which operating mode is the safety function effective?
5. How frequently is the safety function demanded?
6. Within what reaction time is the safe state reached?



Example of the procedure of safety function specification

The example includes every single step needed to achieve a detailed "specification of safety functions". This procedure enables common tools to be used that also support this approach (e.g. SISTEMA[4]).

3. Well-tried components in accordance with EN ISO 13849

The term "well-tried component" is particularly relevant for the interpretation in accordance with category 1 specified in EN ISO 13849. A component is considered to be "well-tried" when it has already been used successfully in similar applications in the past and documented accordingly.

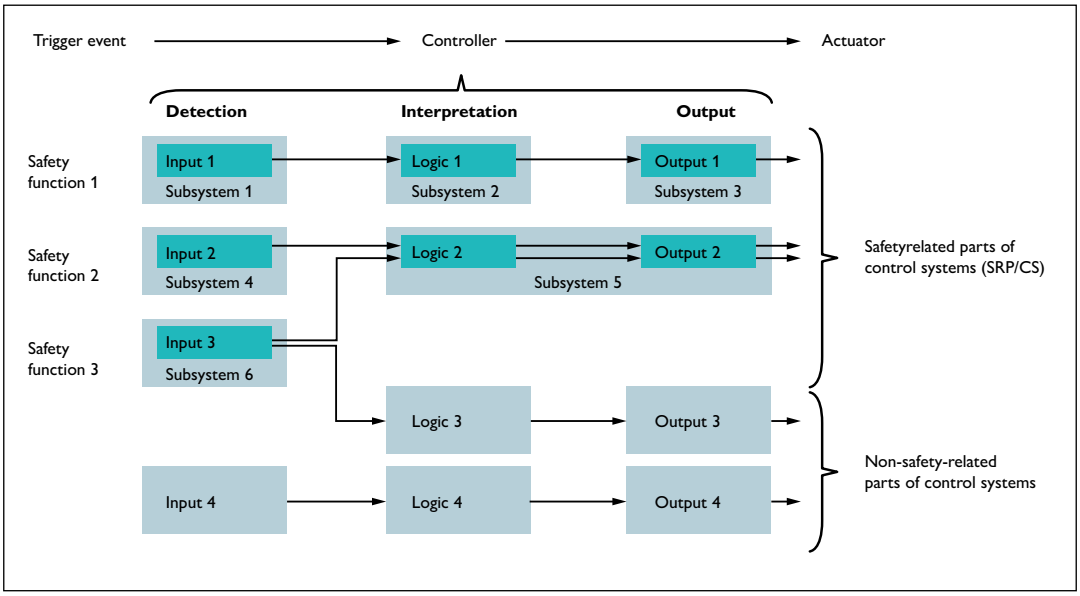
Alternatively, a "well-tried component" is a component that has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Whether a certain component is accepted as being "well-tried" depends on the application and environmental influences, for example. Complex electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to "well-tried".

[4] SISTEMA (= Safety Integrity Software Tool for the Evaluation of Machine Applications from the Institute for Occupational Safety and Health (IFA) of the German Social Accident Insurance (DGUV))

4. What to do when the characteristics are missing? Substitute values in accordance with EN ISO 13849

After defining the safety function (SRS) and determining the PLr in accordance with EN ISO 13849, the next step is to identify the safety-relevant parts of the control system before breaking down the safety function into "subsystems". In doing so, subsystems can be related to different safety functions.



Safety functions and their relation to subsystems

The next step is to determine the safety characteristics (PFH_D, service life, etc.) for each subsystem. The easiest way for the user is to take the values provided by the manufacturer of the component (e.g., safety SPS). However, some applications use standard components that don't have those characteristics. Until now, 10 years could be assumed for $MTTF_D$, but for many cases that was too "conservative". In the future, for subsystems with discrete components, it will be possible to use the PFH_D substitute values from the table below when no manufacturer's information is available.

	PFH_D [1H]	Category B	Category 1	Category 2	Category 3	Category 4
PL b	$5*10^{-6}$	X	O	O	O	O
PL c	$1,7*10^{-6}$	–	X*	X*	O	O
PL d	$2,9*10^{-7}$	–			X*	O
PL e	$4,7*10^{-8}$	–	–	–	–	X*

PFH_D-substitute values for inputs and outputs

X used category is recommended

O used category is optional

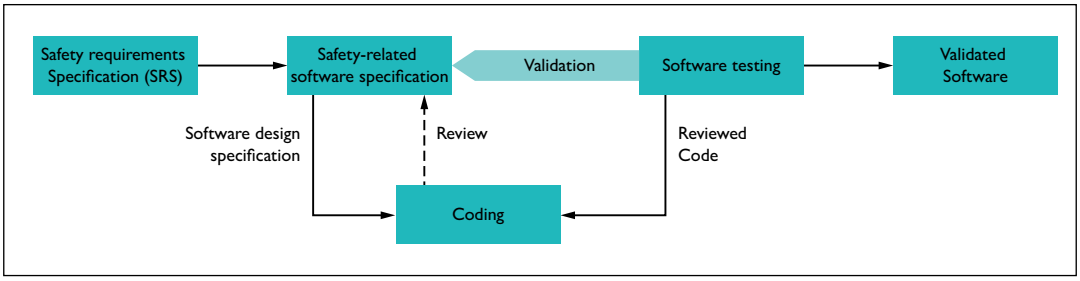
* *well-tried components and well-tried safety principles must be used*

– *category is not permitted*

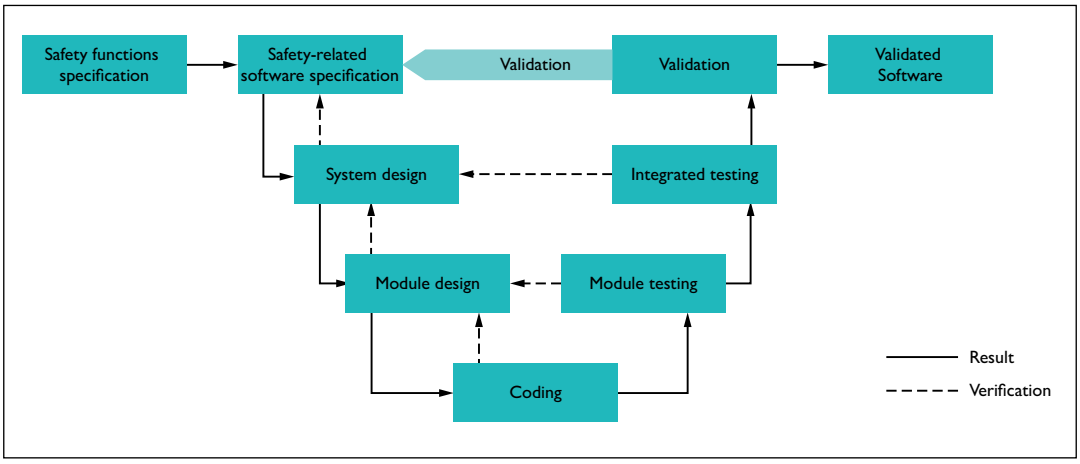
5. Requirements of safety-relevant functions in accordance with EN ISO 13849 / IEC 62061

For machine control systems, configurable or programmable systems that have already been certified in accordance with IEC 61508 are being increasingly used.

For those systems in particular as well as for systems using LVL[5] languages , significant simplifications regarding the verification and validation of safety functions can be anticipated. The existing v model, for example, has been simplified in EN ISO 13849 for this application, with "coding" and "software testing" the only steps remaining besides the software SPS.



Simplified V model



V model for FVL[6] languages

[5] LVL: Limited Variability Languages = programming languages with limited variability
[6] FVL: Full Variability Languages = programming languages with full variability

When FVL[6] languages , such as Ada, C, Assembler, etc., are used however, the former V model remains mandatory for the application.

The standard describes three levels: the first level includes the pre-designed systems described in LVL languages, for which a simplified validation method will be possible (similarly to EN ISO 13849). When the so-called FVL languages are used, the verification and validation process is more comprehensive.

Software Level	**Platform** (Combination of hardware and software)	**Example**
1	"pre-designed" in acc. with IEC 61508 Application software using LVL	Safety PLC with LVL or programmable safety relay module
2	"pre-designed" in acc. with IEC 61508 Application software not using LVL	Safety PLC with FVL in acc. with IEC 61508
3	"pre-designed" in acc. with IEC 61508 Application software not using LVL	Safety PLC with FVL in acc. with IEC 62061

The table below shows the minimum levels of independence resulting from this for **software level 1**. Additionally, the user may use the simplified v model (see EN ISO 13849).

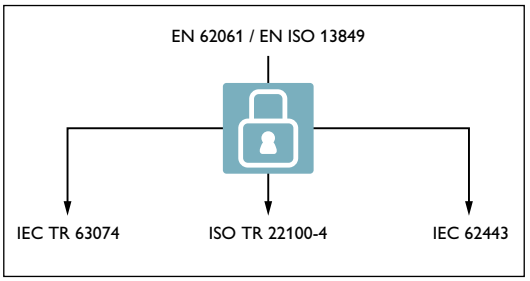
Minimum level of independence	**SIL required for the safety function**		
	1	**2**	**3**
Same person	Insufficient	Insufficient	Insufficient
Different person	Only if pre-certified software modules are used	Only if pre-certified software modules are used	Insufficient
Independent person	Sufficient	Sufficient	Sufficient
Independent department	Not required	Not required	Not required
Independent organization	Not required	Not required	Not required

All in all, it can be said that when using pre-certified systems and software blocks, a significant simplification of the verification and validation process can be expected.

6. Influence of cybersecurity on functional safety in accordance with EN ISO 13849 / IEC 62061

In contrast to functional safety, cyber security protects goods from detrimental impairment as a result of intentional or inadvertent attacks on the availability, integrity and confidentiality of the data.

This involves the use of preventative, technical, and organizational measures.



Situation regarding the standardization: Cybersecurity and functional safety

As networking of automation systems with the IT world is becoming more and more commonplace, scenarios are likely to arise where a different approach is required, especially for safety applications. The network interfaces between office IT systems and production networks represent a significant gateway for hackers. These potential risks are also being addressed by the two standardization projects and have to be considered in the future, for example by performing an IT risk assessment on the basis of the IEC 62443 standard.

7. Low-demand systems for machines in accordance with IEC 62061

The scope of the Machinery Directive is, on the one hand, a very broad one in practical use. Besides classical machines, the directive covers systems such as gas and steam turbines, compressors, generators, or pumps. On the other hand, the two harmonized standards on functional safety, EN ISO 13849 and IEC 62061, have not yet been addressing "low-demand applications"[7]. Due to the missing presumption of conformity, this has led to legal uncertainty for the manufacturers of such systems. Now, IEC 62061 at least takes this approach by defining PFD[8] target failure measures on the basis of IEC 61508.

When IEC 62061 is applied correctly, low-demand applications can now also be evaluated within the scope of the Machinery Directive, claiming "presumption of conformity".

SIL	PFDavg target failure measures for low demand
1	$<10^{-1}$
2	$<10^{-2}$
3	$<10^{-3}$

[7] Operating mode in which the frequency of safety function demands is no more than once per year and no more than twice the frequency of the proof test.
[8] Probability of dangerous failure on demand

Side note:
Working in a standardization committee

Carsten Gregorius

Experts from Phoenix Contact are members in every important standardization committee. Our customers can access this know-how either via our online sales channels or our local representatives.

Safety expert Carsten Gregorius represents Phoenix Contact as a member in the national standardization committees on EN ISO 13849 and IEC 62061.

What does the work in a standardization committee look like?

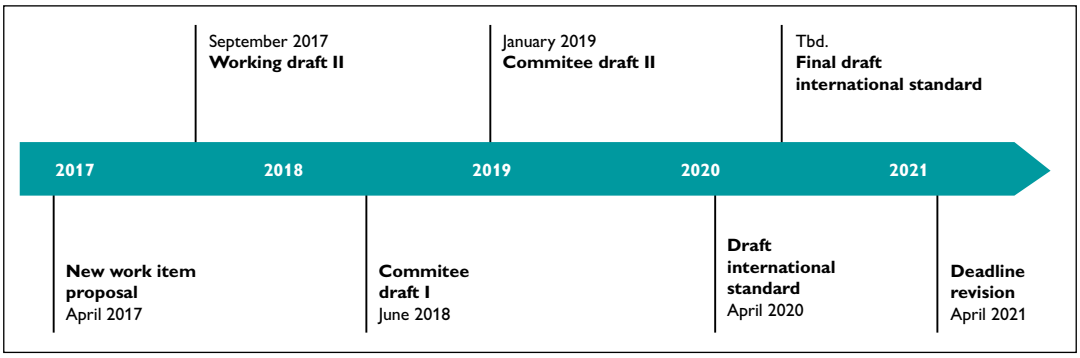
Before a new standardization project can start on an international level, a proposal (NWIP = New work Item Proposal), virtually a profile, has to be prepared. When this process has been competed successfully, the project starts with the nomination of an international group of experts. This international committee now works on the actual contents. The international working group then prepares draft standards called "committee drafts" or "FDIS". Those are circulated to all national standardization committes, also known as "mirror committees", for commenting. In Germany, the DIN (German Institute for Standardization) often directs the work of the mirror committees.

What happens next?

In principle, everyone can submit their comments or corrections for a draft standard via the national standardization committees. This is why it frequently occurs that, depending on the standardization project and member country, hundreds of single comments need to be considered. But because small and medium-sized companies in particular often don't have the time to contribute to all the different standardization committees, associations such as VDMA or ZVEI take on some of these tasks.

And how exactly is a new standard drawn up then?

When all comments from the national mirror committees have been returned to the international standardization group, they are incorporated into another draft. Finally, this FDIS[9] is circulated, for a final vote, to all countries eligible to vote. An FDIS is then either approved by a majority or rejected. A positive result means the new version of EN ISO 13849, as an example, can be published.



Schedule for the revision of EN ISO 13849

[9] FDIS: Final draft International Standard

What projects will follow?

When the revision of EN ISO 13849 (part 1) has been completed, another revision step is planned where calculation models for the determination of the PFHD are to be added to Technical Report ISO/TR 23849. Another project will be about revising part 2 of EN ISO 13849 (validation), before parts 1 and 2 will then be merged.

Glossary

Common cause failure

Refers to the operational failure of different elements resulting from common single events where these failures are not consequences of each other.

Diagnostic coverage

Measurement for the effectiveness of the diagnostics represented as the ratio between the failure rate of the identified failure rates and the rate of total failures. Diagnostic coverage can either relate to the entire system or certain components, such as sensors, logical systems or final elements.

Performance Level

The performance level (PL) is a qualitative classification of the individual SRP/CS (safety-related parts of control systems) with regard to the performance capability of the individual safety functions in the event of unforeseeable situations.

Dangerous failure per hour

PFH_D stands for probability of dangerous failure per hour.

Harmonized standard

Harmonized standards are European standards for products, listed in the Official Journal under a European Directive. They are part of the European Commission's "New Approach" where essential requirements for products are defined by standards organizations CEN and CENELEC. The harmonized standards are published in the Official Journal of the EU. Only goods and services that satisfy the essential requirements from the directives may be placed on the market. They can be identified by certificates or CE markings.

Related reading and links

Safety meets security – A common strategy is required

Visit us at phoe.co/safety-meets-security

Funktionale Sicherheit von Maschinen –

Praktische Anwendung der DIN EN ISO 13849-1
(Beuth-Verlag: ISBN 978-3-410-25249-8)

You can fi nd your local partner at

phoenixcontact.com

PHOENIX CONTACT