ZVEI:
Die Elektroindustrie

Safety of machinery

Information on the application and delimitation of the standards EN 62061 and EN ISO 13849

Version 1.1

German Electro and Digital Industry Association

ZVEI:
Die Elektroindustrie

Safety of machinery
Information on the application and delimitation
of the standards EN 62061 and EN ISO 13849
Version 1.1

Publisher:
ZVEI e. V.
Trade Association Automation
Lyoner Straße 9
60528 Frankfurt

Dr. Markus Winzenick
Phone: +49 69 6302-426
E-Mail: markus.winzenick@zvei.org

www.zvei.org

Februar 2022

Content

1 Motivation

Responding quickly and flexibly to customer demands requires complex and decentralised industrial production. A key function here is the topic of
"functional safety". To support the trend towards digitalisation and decentralisation, the requirements for machine safety and productivity must complement each other. Increasingly, configurable or programmable safety systems are being used to safeguard machines and plants, with a growing level of complexity.

The safety of machines and systems for the protection of the user is essentially dependent on the correct application of standards and directives. The basis for this in Europe is the Machinery Directive, which supports uniform protection goals objectives in the design of machinery. However, many European standards also have great significance outside the European Economic Area due to their international status. The standards on functional safety also play an important role in this context. The requirements for the safety-related parts of machine controls are specified both in EN ISO 13849 and in EN 62061.

The following explanations describe the main features of both standards based on the editions IEC 62061:2021 and EN ISO 13849:2015 including the planned amendments prEN ISO 13849-1:2021. Therefore, this overview cannot claim to be complete.

Note: At the time of writing, the harmonisation process with the 2021 editions has not yet been completed.

2 Comparison of the most important differences

Both standards have continued to converge in the course of the maintenance projects. Both standards are harmonised under the Machinery Directive and can be used to evaluate the functional safety of machinery.

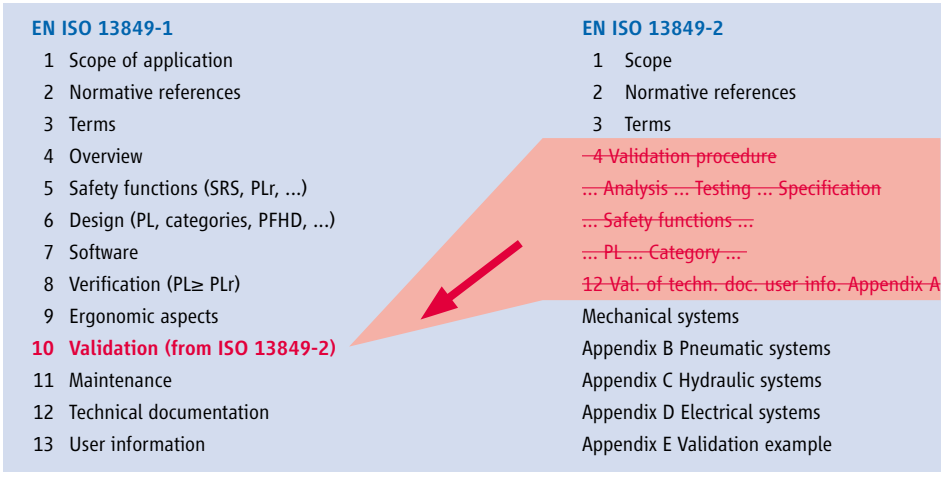
While EN 62061 adopts basic features and terminology of IEC 61508, the probabilistic approaches were considered in EN ISO 13849-1, taking into account the categories. In detail, there are differences in the validation of safety-related software and in the determination of the required risk reduction. EN 62061 defines the Safety Integrity Level (SIL) as the target value, whereas EN ISO 13849-1 speaks of the Performance Level (PL).

2.1 What is new?

2.1.1 EN ISO 13849

In EN ISO 13849-1, the following chapters in particular were newly created or revised:

- Overview (Chapter 4)
- Software (Chapter 7)
- Validation (Chapter 10 was taken over from EN ISO 13849-2)
- The combinations of subsystems (Appendix H)
- EMC requirements Annex L
- Typical safety requirements (Annex M)
- Software Requirements (Use-Cases Appendix N)
- Security
- Device types 1 to 4 (Annex O)



2.1.2 EN 62061

In EN 62061, the following chapters in particular were newly created or revised:

- Scope: technology-independent (no longer restricted to E/E/PES)
- New annexes on failure rates (Annex C), diagnostic coverage (Annex E) and reliability calculations (Annex K).
- Renaming from "SILCL" to "SIL
- New SW levels for application software (Chapter 8)
- Level of independency in SW verification and general validation
- EMC requirements (chapter 6.6)
- SW-based parameterisation more clearly defined (chapter 6.7)
- Addition of requirements to periodic test, e.g. proof test
- Security

3 What do I have to do to place a machine on the market in conformity with the directive ?

The social cost of the many accidents directly caused by the use of machinery can be reduced if safety is incorporated into the design and construction of machinery and if machinery is properly installed and maintained.

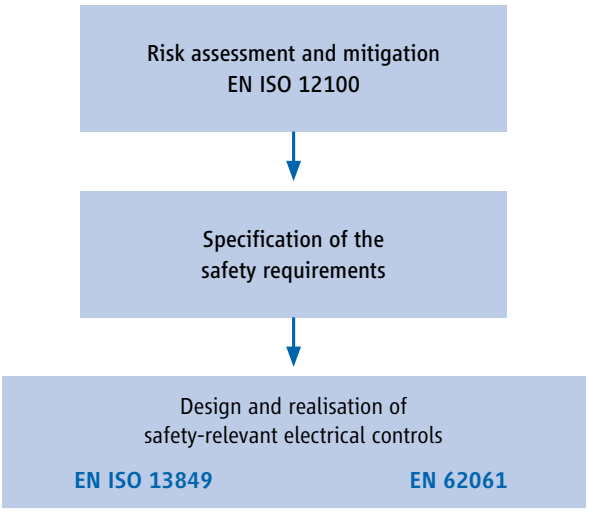
(2nd recital, Machinery Directive 2006/42/EC)

This makes it very clear that one of the central requirements of the Machinery Directive is that machinery must not present an unacceptably high risk. In order to achieve this, the Machinery Directive requires in Annex I that a risk assessment is carried out for every machine placed on the market within the EU and that the machine is built taking into account the results of the risk assessment. How such a risk assessment can be carried out can be found in the harmonised standard EN ISO 12100. As there is unfortunately no such thing as "zero risk" in technology, every effort must be made to achieve an acceptable residual risk.

The risk reduction measures are manifold and should follow the 3-step concept:
1. Inherently safe design
2. Technical protective measures
3. Organisational measures

The technical protective measures include guarding systems, design adjustments to the machine and various other measures. If safety depends on the correct functioning of control systems (e.g. hazardous movement must stop when a safety gate is opened), these must be designed in such a way that the probability of safety-related failures is sufficiently low. It must also be checked that any faults that occur do not lead to the loss of the safety function. To fulfil this protection goal, it makes sense to consider the two harmonised standards intended for this application - EN ISO 13849 and EN 62061 - which were drawn up in accordance with a mandate from the European Commission and published in the European Official Journal (presumption of conformity). This is the only way to avoid increased effort in proving conformity.

Fig. 1: Functional safety in the risk assessment process



In the following, the two central standards for functional safety on machines are compared and assistance for the user is given.

4 Areas of application of the two standards

4.1 EN ISO 13849

EN ISO 13849 specifies a methodology and provides related guidance for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. It specifies the characteristics required to determine the required level of performance of safety functions. EN ISO 13849 applies to SRP/CS for high-demand mode including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, mechanical), for many types of machines. The standard does not apply to the low-demand mode.

EN ISO 13849 does not specify the safety functions or required performance levels to be used in specific applications.

It does not contain specific requirements for the construction of elements that are part of SRP/CS.

4.2 EN 62061

The International Standard specifies requirements and gives recommendations for the design, integration and validation of safety-related control systems (SCS) for machinery. It applies to control systems used either individually or in combination to implement safety functions on machines that are not manually portable during work, including a group of machines working together in a coordinated manner. The design of complex programmable electronic subsystems or subsystem elements is not within the scope of this standard. This is within the scope of IEC 61508 or related standards. Complex (programmable) subsystems are, for example, safety controls based on microcontroller technology. Low-demand applications are currently not considered in EN 62061. However, an "amendment" on this topic is planned.

5 Brief description of the standards

5.1 EN ISO 13849

The performance of a safety function is described by the Performance Level (PL). Here, based on the safety functions resulting from the risk analysis, a division into subsystems is made. An essential feature of EN ISO 13849 are the assessment that define the architectural properties of an SRP/CS. EN ISO 13849 considers complete safety functions with all components involved in their execution. In addition to electrical systems, it also includes pneumatic, hydraulic and mechanical systems.

EN ISO 13849 goes beyond a qualitative approach (architecture of the control system) and also takes a quantitative view of the safety functions. Based on the categories, Performance Levels (PL) are used for this purpose.
Depending on the type, the following safety-related parameters are defined for SRP/CS:

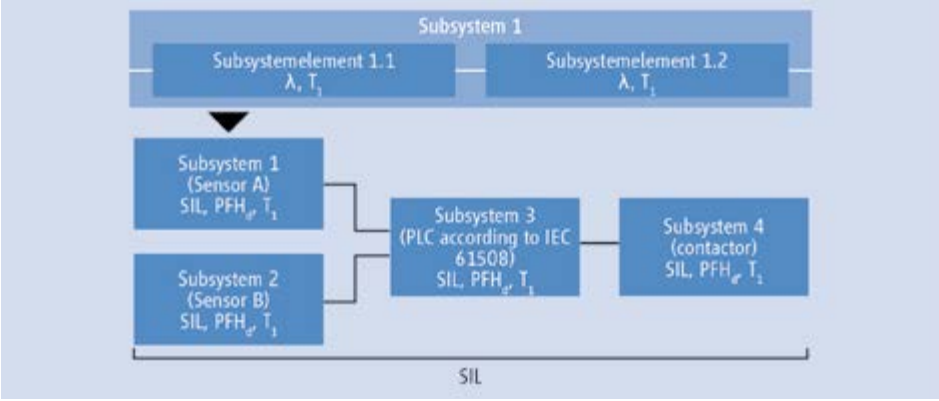
- Category (structural requirement)
- PL: Performance Level
- $MTTF_D$: Mean time to dangerous failure
- B_{10D}: Number of cycles in which 10% of a sample of the the components subject to wear under consideration have failed dangerously
- DC: Diagnostic coverage
- CCF: Common cause failure (CCF): Failure due to common cause.
- T_M: Mission Time

The standard describes the determination of the performance level (PL) for safety-related parts of control systems on the basis of designated architectures for the intended service life T_M.

In the case of deviations from the intended structures or a very high complexity of the systems, EN ISO 13849 refers to IEC 61508 for electrical/electronic systems. In the case of a combination of several safety-relevant parts to form an overall system, the standard provides information on determining the resulting PL.

5.2 EN 62061

The performance of a safety function is described by the Safety Integrity Level (SIL). Here, based on the safety functions resulting from the risk analysis, a division into partial safety functions and finally an allocation of these partial safety assessment to real devices - called subsystems and subsystem elements - is made. A safety-related control system (SCS) consists of various subsystems. The subsystems are described in terms of safety by the characteristic values (SIL and PFH_D as well as T1). EN 62061 considers complete safety functions with all components involved in their execution. In the new version - like EN ISO 13849 - it includes pneumatic, hydraulic and mechanical systems in addition to electrical systems. EN 62061 has been harmonised since December 2005.



- SIL: Safety Integrity Level
- PFH_D: Probability of dangerous failures per hour
- T1: Smallest value from life expectancy or test interval
- λ: failure rate; for elements subject to wear (or without constant failure rate): B10D
- SFF: Safe Failure Fraction
- T2: diagnostic test interval
- β: Susceptibility to common cause errors
- DC: Diagnostic coverage

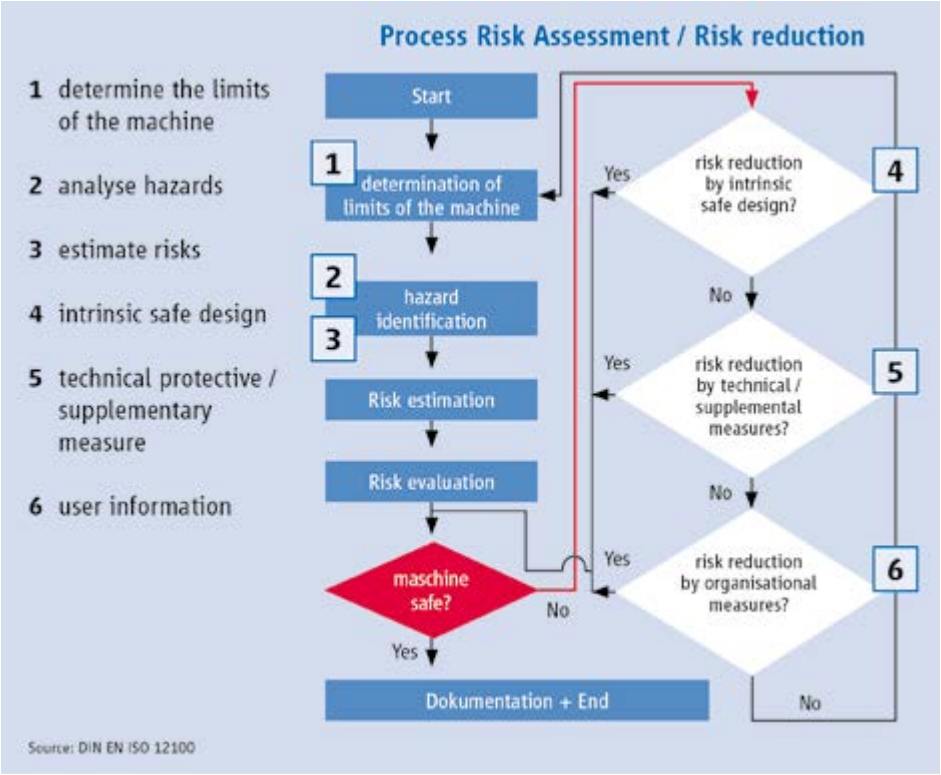
6 Basic Procedure

6.1 Risk assessment according to EN ISO 12100

It is assumed that a hazard present on a machine will sooner or later lead to damage if protective measure(s) are not implemented. Protective measures are a combination of the measures implemented by the designer and those implemented by the user. Measures that can be taken at the design stage are always preferable to, and generally more effective than, those carried out by the user.

Taking into account the experience of users of similar machines and the exchange of information with potential users (whenever possible), the designer must proceed in the order given below:

Fig. 2: Risk assessment process based on EN ISO 12100



6.2 Risk reduction through control measures

If the required risk reduction is achieved with technical protective measures by safety-related control parts, the design of these control parts is an integral part of the overall design procedure for the machine. The safety-related control system provides the safety function(s) with a SIL or PL that achieves the required risk reduction.

6.3 Specification of the safety requirements

Tab. 1

Specification	Note
Triggering event	What event triggers the safety function?
Safety-related response	What is the safety-directed response?
Operating mode	In which operating mode should the safety function be active?
PL_r	With which Performance Level PL_r should the safety function be executed?
Frequency of the request	How often is the request for the safety function to be expected?
Response time	In what time after the request of the safety function should the safe state be reached?
Behaviour in the event of a power failure	What safety-oriented reaction is required in the event of a power failure?
Priority	Is the safety function prior or subordinate to other safety functions?
Supplementary safety function	Does the use of the safety function require other active safety functions?
Additional parameters	What additional parameters need to be considered?
Fault detection measures	What diagnostic measures need to be considered?
Fault response measures	What measures are required when errors are detected?

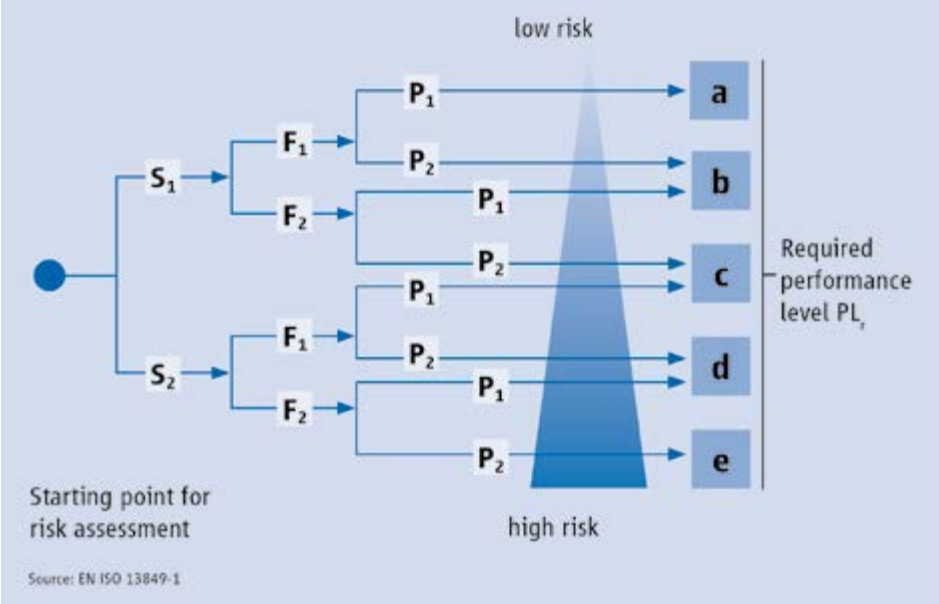
The safety requirement specification is the most important document (alpha document). It describes in detail the functional requirements of each individual safety function to be performed. The required interfaces as well as all items from Table 1 are important parts of this document. All further documentation as well as its validation has its origin in this document. Errors in the specification continue systematically.

6.4. Overlapping Hazards

If combinations of hazards always occur simultaneously, then they should be considered in combination when assessing the risk. For example, a continuously operating welding robot creates different hazardous situations at the same time. For example, crushing due to movement and burning due to the welding process can occur at the same time. In this case, the relevant subsystems would be considered combined in a safety function by adding the respective PFH_D values.

6.4.1 Determination of the required performance level according to EN ISO 13849-1

Fig. 3: Determination of the PL_r



The informative Annex A of EN ISO 13849-1 provides an estimate of the required risk reduction and is intended as a guide for the designer and standard setter in determining the PL_r.

Severity of injury S1 and S2
S1 = light reversible injuries
S2 = severe irreversible injuries and death

Frequency and/or exposure times to the hazard, F1 and F2
A generally valid time period cannot be specified for the parameter F1 or F2.
F1: if the cumulative exposure time is not more than 1/20 of the total operating time and the frequency is not higher than once per 15 min.
F2: should be chosen if a person is frequently or continuously exposed to the hazard.

Possibility to avoid the damage P1 and P2
P1: possible under certain conditions
P2: not possible

In the case of a dangerous event, P1 should only be selected if there is a realistic chance of avoiding the hazard. Otherwise P2 should be selected. The following two tables have been added to the 2021 version and are intended to help determine the P parameter.

Determination of the parameter P on the basis of five factors

Factor	C	B	A
1. use of the machine by		Unskilled person	Qualified person (specialist)
2. speed of the part of the machine that can trigger a dangerous event (depending on the specific machine)	High speed event No possibility to escape (e.g. over 1000 mm/s, time to hazard < 1 s)	Event at medium speed Limited possibility to escape (e.g. 251 mm/s to 1000 mm/s, time to hazard < 3 s)	Low or very low speed event Sufficient possibility to escape (e.g. max. 250 mm/s, time to hazard ≥ 3 s)
3. possibility to avoid the hazard	Not possible	Possible in less than 50 % of cases	Possible in more than or equal to 50% of cases
4. possibility of perception of the hazard	Not possible (e.g. Instrumentation necessary, the human sense is not able to perceive the danger, Environmental conditions obscure perception)	Possible in less than 50 % of cases	Possible in more than or equal to 50% of cases
5. complexity of operations (human interaction in terms of the number of operations and/or the time available for these operations)		High complexity (e.g. Troubleshooting) or Medium complexity (e.g. using the Hold-To-Run control to set up a part of the machine)	Low complexity (e.g. adjusting the workpiece clamps) or Very low complexity / or no interaction (e.g. insert a workpiece into the machine)

Source: ZVEI based on prEN ISO 13849-1:2021

Selection of parameter P1 or P2		
Total score		Parameter "P"
one or more "C"	■ □ □ □ □	P2
no "C", three or more "Bs"	■ ■ ■ □ □	P2
no "C", two "B", the rest "A"	■ ■ □ □ □	P1 or P2 depending on the specification of the machine
no "C", one or no "B", the rest "A".	■ □ □ □ □ □ □ □ □ □	P1

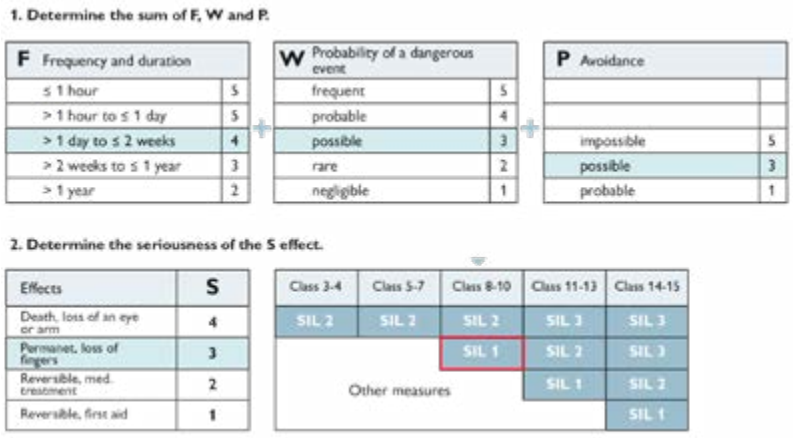
Source: ZVEI based on prEN ISO 13849-1:2021

Overlapping hazards

If combinations of hazards always occur simultaneously, then they should be considered in combination when assessing the risk. A continuously operating welding robot, for example, creates different hazardous situations at the same time. For example, crushing due to movement and burning due to the welding process can occur at the same time. In this case, the relevant subsystems would be considered combined in one safety function.

6.4.2 Determination of the required performance Safety Integrity Level according to EN 62061

Fig 4: Determination of the required SIL



Source: Phoenix Contact

Class K = Fr + Pr + Av

The informative Annex A of EN 62061 provides methods for a qualitative approach to risk assessment and SIL assignment that can be applied to SCS for machinery to determine the required SIL.
Experience in the successful handling of similar machines/hazards should be taken into account when estimating the required SIL.
Further SIL assignment methods are available in IEC 61508-5 and IEC 61511-3.

Risk assessment

Risk assessment should be carried out for each hazard by determining the risk parameters:

- Severity of the damage
- Probability of occurrence of this damage
- Frequency and duration of exposure of persons to the hazard
- the probability of the occurrence of a hazardous event
- Ways to avoid or limit the damage

Severity (Se) classification

Consequences	Severity (Se)
Irreversible: death, loss of an eye or arm	4
Irreversible: broken limb(s), loss of finger(s)	3
Reversible: requires treatment by a doctor	2
Reversible: First aid required	1

lassification of frequency and duration of exposure (Fr)

Frequency of exposure	Frequency, Fr	
	Duration of exposure ≥ 10 min	Duration of exposure < 10 min
≥ 1 per h	5	5
< 1 per h an ≥ 1 per day	5	4
< 1 per day on ≥ 1 per 2 weeks	4	3
< 1 per 2 weeks an ≥ 1 per year	3	2
< 1 per year	2	1

Probability (Pr) classification

Probability of avoiding or limiting damage (Av)	
Impossible	5
Rare	3
Probably	1

7 Design of the control architecture

7.1 EN ISO 13849

For each selected SRP/CS and/or combination of SRP/CS performing a safety function, an estimation of the achieved safety function shall be made.
PL to be carried out.
The PL of the SRP/CS must be determined by estimating the following parameters:

- of the $MTTF_D$ or B_{10D} value of individual components;
- the DC;
- the CCF;
- of the structure,
- the behaviour in the event of a fault;
- safety-related software
- Systematic failures
- the ability to perform a safety function under foreseeable environmental conditions.
- Application of well-tried safety priniciples

Performance level (PL)	Average probability of a dangerous failure [1/h]
a	$10^{-5} \leq PFH_D < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH_D < 10^{-5}$
c	$10^{-6} \leq PFH_D < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH_D < 10^{-6}$
e	$PFH_D < 10^{-7}$

7.2 EN 62061

The selection or design of the SRECS must in principle meet at least the following requirements:
Requirements for the safety integrity of the hardware consisting of:

- the structural constraints on the safety integrity of the hardware
- the requirements for the probability of dangerous random hardware failures
- as well as the requirements for systematic safety integrity consisting of
- the requirements to avoid failures and
- the requirements to control systematic errors.

EN 62061 also describes requirements for the implementation of application programmes.

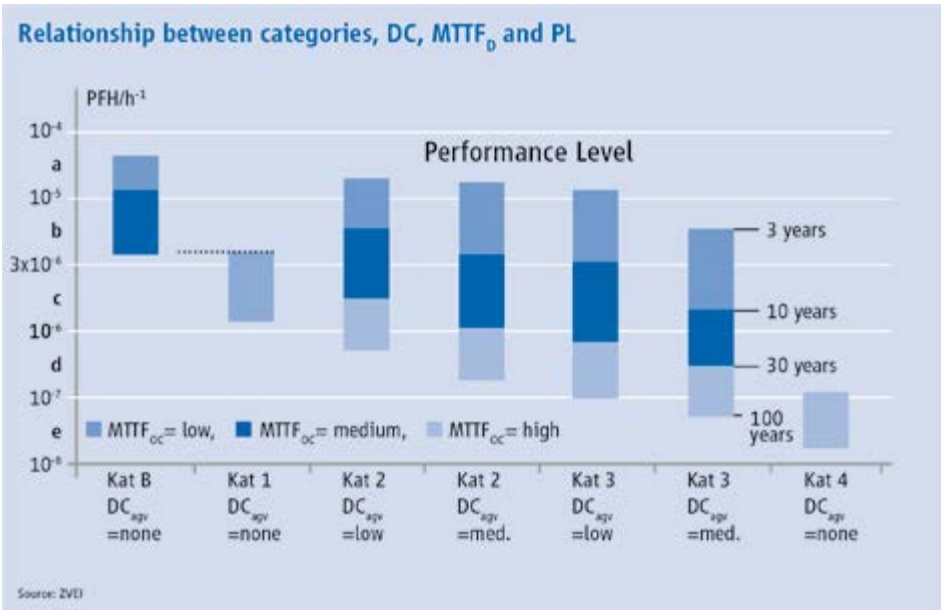
Safety-related parameters for subsystems:

- SIL: SIL suitability
- PFH_D: Probability of dangerous failures per hour
- T1: Proof Test Interval

SIL (IEC 61508)	Average probability of a dangerous failure [1/h]
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

7.3 EN ISO 13849-1

Fig 5: Relationship between categories, DC, $MTTF_D$ and PL



Remark:
The PFH_D values are a necessary prerequisite for determining the performance level. In addition, measures for error prevention such as CCF, category and DC must also be taken into account to fully determine the PL.
For category 4, the $MTTF_D$ = high can be increased up to 2,500 years.

7.4 EN 62061

Safety-related parameters for subsystem elements (devices):

- λ: Failure rate;
- $B10_D$ value: for components subject to wear (without constant failure rate)
- T1: Service life expectancy
- T2: Diagnostic test interval
- β: Sensitivity to failures of common
- Cause
- DC: Diagnostic coverage
- SFF: Safe failure fraction (en: Safe failure Fraction)
- HFT: Hardware Fault Tolerance

SFF	HFT 0	HFT 1	HFT 2
< 60%	Not permitted	SIL 1	SIL 2
≥ 60% to < 90%	SIL 1	SIL 2	SIL 3
≥ 90% to < 99%	SIL 2	SIL 3	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

Source: ZVEI following the EN 62061

Performance level (PL)	Safety Integrity Level (SIL)
a	-
b	-
c	1
d	2
e	3

Source: ZVEI following the EN 62061

Remark:
The table above describes the relationship between the two concepts of the standards (PL and SIL). Unless a specific category is required by C standards, a subsystem according to SIL 3 (EN 62061), for example, can be used within a safety function according to EN ISO 13849 up to PL e.

8 Software

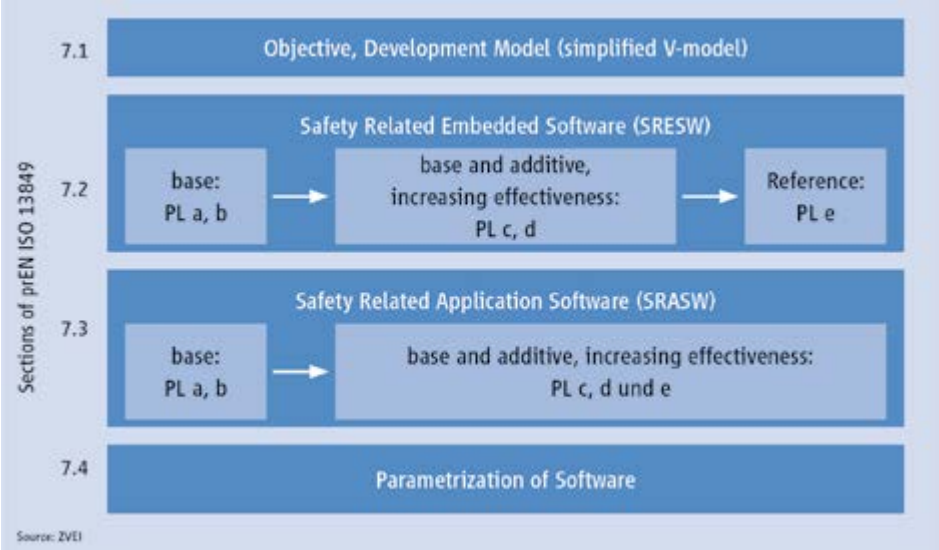
Like no other technology, software today assumes a higher level of responsibility than ever before, and this thus also applies to the programmers. EN ISO 13849 refers to the parts of IEC 61508 just as EN 62061 does. The safety-relevant software must be readable, understandable, testable and maintainable. For this reason, failures must already be detected in the development phase.

8.1 EN ISO 13849

In EN ISO 13849, the software requirements for programmable controllers were adapted to the current state of the art. The measures described in section 7 of the make it possible to develop safety-related application software for machine controls up to Performance Level PLr e.

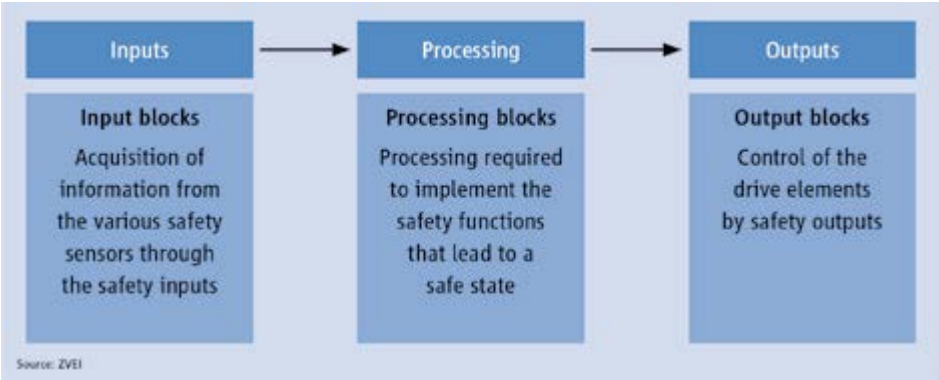
Failures in software do not result from random component failures, but have systematic causes. When developing safety-related software, everything possible must be done to avoid failures.

Fig. 6: SW requirements



EN ISO 13849 describes the risk and defines failure-avoiding measures depending on the types and language types of the software and the required performance level.

Fig. 7: Design of a SW example at function block level



The same requirements apply to the software in order to fulfil the performance level (e.g. structure, reliability, validability, etc.).

Fig. 8: V-model

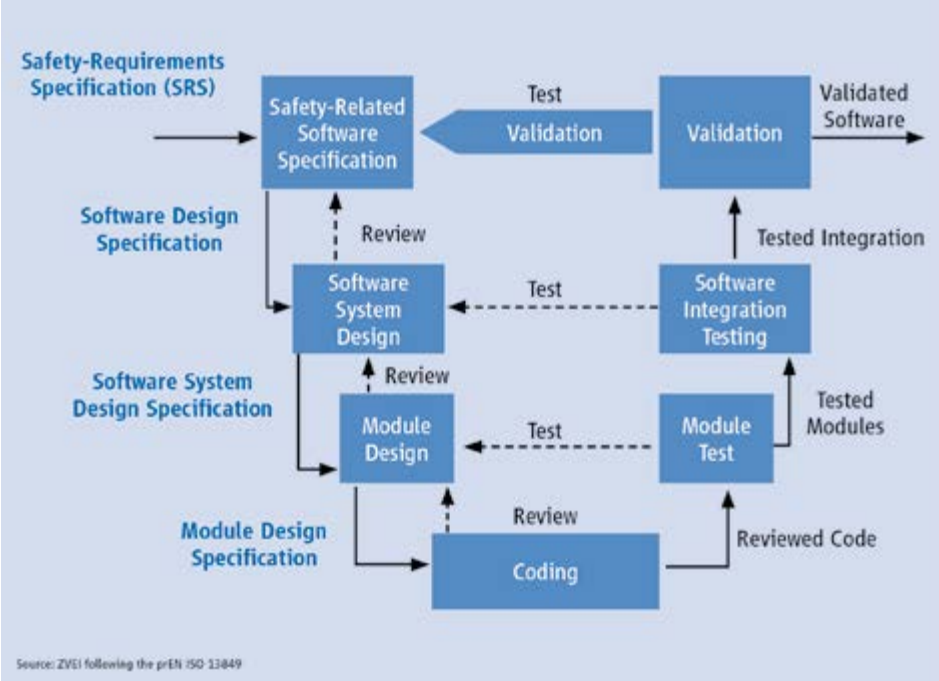
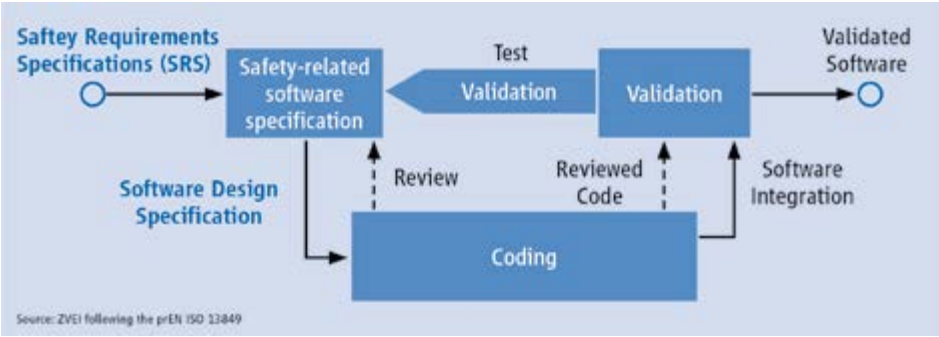


Fig. 9: Simplified V-model



V-Model for software when pre-assessed safety-related hardware and software modules are used in combination with LVL.

Full variability language (FVL)
This type of language is intended for programmers and offers the possibility to implement a variety of functions and applications.

FVL typical examples: Ada, C, Pascal, statement list, assembly languages, C++, Java, Math- lab, Simulink and SQL (without usage restrictions and full variety of statements).

Limited variability language (LVL)
Software programming language whose notation is textual or graphical or has features of both.
LVL should be designed in such a way that it is easy for the software developer to understand and implement. Note: Annex J of ISO EN 13849 describes a software example.

8.2 EN 62061

EN62061 introduces the term "new" SW level: Depending on the level of complexity, a PES is classified in one of the following SW levels 1-3:

Classification in Software Level (SW)

SW level	Essential principle	Basis	Example
1	Platform (combination of hardware and software) that complies with IEC 61508 or other functional safety standards linked to IEC 61508, e.g. IEC 61131-6, has already been designed and tested. Application software that uses a language with limited variability (LVL).	Application software that complies with this document.	Safety PLC with LVL or programmable safety relay
2	Platform (combination of hardware and software) that complies with IEC 61508 or other functional safety standards linked to IEC 61508, e.g. IEC 61131-6, has already been designed and tested. Application software that uses a language with limited variability (LVL).	Application software that complies with this document.	Safety PLC with FVL (FVL corresponding to this document.)
3		Application software that complies with IEC 61508-3.	Safety PLC with LVL or FVL (FVL according to IEC 61508)

Source: ZVEI following the EN 62061

Depending on the SW level (1-3) and the SIL to be achieved (1-3), there are different requirements for

a) Minimum levels of independence for V&V (verification and validation)
b) Scope of V&V activities (V model)

Levels of independence Verification and validation

For verification activities, the following levels of independence apply depending on the SIL to be achieved.

Minimum level of independence for verification activities	req. SIL for the safety function		
	SIL 1	SIL 2	SIL 3
Same person	insufficient	insufficient	insufficient
Other person	not sufficient *	not sufficient *	insufficient
Independent person**	Sufficient	Sufficient	Sufficient

Source: ZVEI following the EN 62061

** For software level 1, where only combinations of prefabricated software modules are used, one "other person" is sufficient. Software level 2 is not applicable for SIL 3.*

*** Depending on the company organisation and expertise within the company, the requirement for an "independent person" may need to be met through the use of an external organisation. Conversely, companies that have internal organisations skilled in risk assessment and the application of safety-related systems that are independent and separated (by management and other resources) from those responsible for the main development may be able to use their own resources to meet the requirements for an independent organisation.*

For validation activities, the following levels of independence apply depending on the SIL to be achieved

Minimum level of independence for validation activities	Erf. SIL for the safety function		
	SIL 1	SIL 2	SIL 3
Same person	insufficient	insufficient	insufficient
Other person	insufficient	insufficient	insufficient
Independent person**	Sufficient	Sufficient	Sufficient

Source: ZVEI following the EN 62061

For SW level 1, the simplified V-model can be applied.

Fig. 10: simplified V-model SW-Level 1

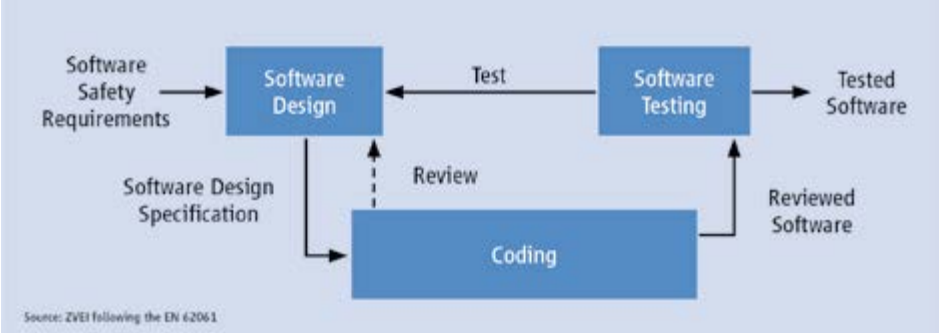
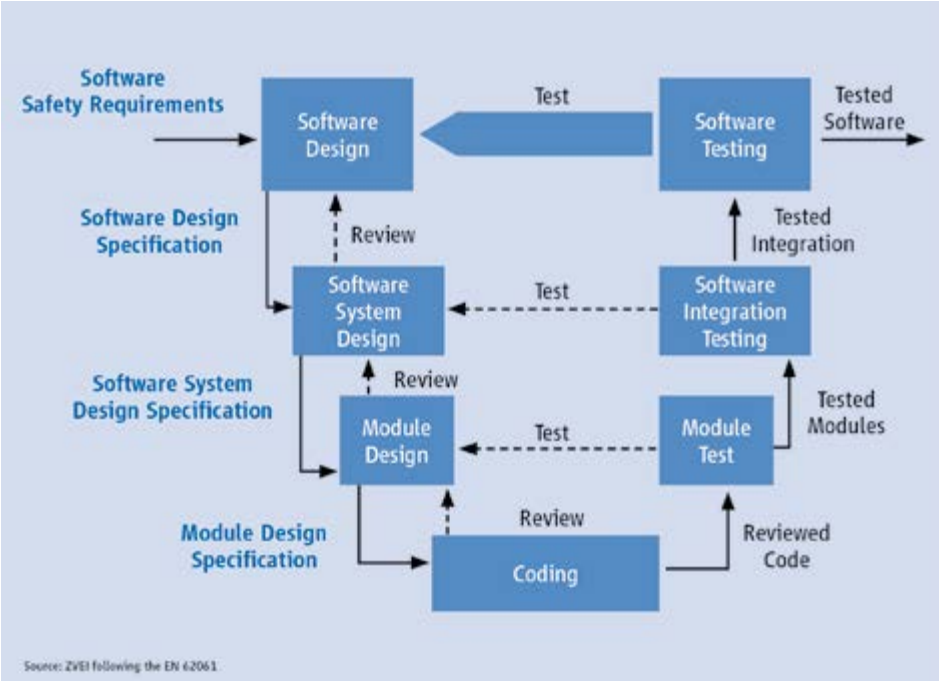


Fig. 11: V-model SW-Level 2



For SW level 3 see IEC 61508-3.

9 Security

If security has an influence on functional safety, measures must be taken. Security aspects with an influence on functional safety must be taken into account. However, no specific requirements are described. Instead, reference is made to IEC TR 63074, ISO TR 22100-4 and IEC 62443.

10 Verification

For each individual safety function, the PL of the associated SRP/CS(s) must correspond to the "Required Performance Level". The PLs of different SRP/CSs that are part of a safety function must be greater than or equal to the required performance level of that function.

In the case of interconnection of several SRP/CS, the final PL can be determined with the help of Table 9 from EN ISO 13849. The probability of a dangerous failure of each SRCF (Safety related control function) as a result of dangerous random hardware failures shall be equal to or less than the failure limit specified in the safety requirement specification.

The SIL achieved by the SRECS due to the structural constraints is lower than or equal to the lowest SIL of any subsystem involved in the execution of the safety function.

11 Validation

The design of a safety-related control function must be validated. The suitability of the safety-related control function for the application is checked. The validation can be done by analysis or testing (e.g. by specific simulation of single or multiple faults). EN ISO 13849 has adopted sections 4-9 from ISO EN 13849-2 in chapter 10 Validation.

12 What do the changes mean for the user?

Both standards have continued to converge following the expected amendments. In practice, this means that subsystems developed according to one of the two standards can be more easily transferred to the other. The adjustments in risk classification should be re-evaluated in retrospect of existing concepts. In some cases, there is greater flexibility with regard to the risk parameters to be assumed. In particular, the influence of cyber security with regard to functional safety must be taken into account again. Here, specific IEC and ISO regulations offer further assistance in implementing the relevant protection goals from the EN 62443 standard (IT security for industrial automation systems). With regard to programmable or configurable systems that have been developed and certified according to IEC 61508, significant simplifications can be expected with regard to the verification and validation of user software.

At present, however, it is still open whether and what transitional periods are envisaged for the publication of the standards in the Official Journal. There is, however, a justified hope that there will be a transition period of approx. 2-3 years.

13 Glossary

Abbreviation	English term
B_{10D}	
λ	Failure Rate
λ_s	Failure Rate, Safe
λ_D	Failure Rate, Dangerous
CCF	Common Cause Failure
DC	Diagnostic Coverage
DCavg	Average Diagnostic Coverage
	Designated Architecture
HFT	Hardware Fault Tolerance
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
$MTTF_D$	Mean Time To Dangerous Failure
MTTR	Mean Time To Repair
PFH	Probability Of Failure Per Hour
PFH_D	Probability Of Dangerous Failure Per Hour
PL	Performance Level
PL_r	Performance Level required
SIL	Safety Integrity Level
SRCF	Safety Related Control Function

Abbreviation	English term
SRP/CS	Safety Related Parts of a Control System
SRECS	Safety Related Electrical Control Systems
T_1	Proof test intervall
T_2	Diagnostic Test Interval
T_M	Mission Time
β	Common Cause Failure
C	Duty Cycle
SFF	Safe Failure Fraction
Security	
Safety	
Maschinen-sicherheit	
Funktionale Sicherheit	

14 FAQ

The following collection provides answers to frequently asked questions in the context of functional safety.

Q: Is there a SIL or PL specification for solenoid valves / contactors from the manufacturer?

A: If these components are "only" electromechanical components, there is usually only one $B10_D$ value. Based on the $B10_D$ value, the operating conditions (e.g. switching frequency, load case,...) and the diagnostic measures implemented in the safety function, a SIL or PL can be determined for the safety function.

Q: What level of diagnostic coverage can I use for relays and contactors with forcibly guided contacts?

A: The "pure" contactor / relay has no diagnostic coverage. A DC of 99% can be achieved by evaluating the positively driven contacts by a higher-level instance. The prerequisite for this is a corresponding fault reaction.

Q: Can I achieve the hardware fault tolerance of 1 with a single mechanical safety interlock switch?

A: No, as a rule already one error leads to failure. For magnetically actuated or RFID - based systems, a confirmation of a hardware error tolerance of 1 is possible by the manufacturers.

Q: What does the index "D" mean in $MTTF_D$?

A: The index "D" stands for "dangerous". The MTTFD describes the expected value of the time until the first dangerous fault.

Q: Can I use EN ISO 13849 when integrating complex programmable electronics?

A: Yes. The new edition of EN ISO 13849 describes requirements for complex systems including software up to PLe.

Q: What do I do if I don't get any characteristic values from the manufacturer of my components?

A: EN ISO 13849 and EN 62061 offer alternative reference values for frequently used components in the appendix. However, it is preferable to always use the manufacturer's original values.

Q: Can I use EN ISO 13849 to calculate the $MTTF_D$ for process valves/valves in safety functions that are requested/switched less frequently than once a year (low-demand mode)?

A: No, EN ISO 13849 only describes the high-demand mode. Therefore, an MTTF assessment can only be made with additional measures such as "forced dynamisation", which ensures that a demand takes place at least once a year.

Q: Can I use EN 62061 to calculate the failure rate for low-demand components that are switched less frequently than once a year?

A: It is planned that EN 62061 will offer the possibility to evaluate low-demand applications in the future. This is to be implemented as part of an "amendment" to EN 62061.

Q: Does application software have to be certified? If "yes", according to which standard?

A: No. A certification obligation based on the two standards does not exist separately for the software, but is based on the scope and complexity of the overall project. Software testing may be required as part of the verification and validation of safety functions. Information on this can be found in EN ISO 13849 and EN 62061 as well as in EN 61508-3 and, if a safety PLC or a comparable component is used, in the documentation of the safety PLC. However, it is planned that there will be adaptations within the framework of the revision of the Machinery Directive.

Q: Can standard components for which, for example, only an MTTF value is specified be used for safety technology?

A: Safety-relevant controls can in principle be realised by using standard components, but safety components offer the advantage that the machine designer is relieved of the safety-related assessment and analysis of the components used by the manufacturer of safety components. To achieve functional safety, the systematic suitability of components must be considered in addition to the use of a suitable architecture (category), the realisation of a required fault detection and the consideration of failure rates/probabilities. The use of complex elements or subsystems of similar design (homogeneous redundancy) must generally be excluded, as questions about systematic suitability and the required fault detection often cannot be answered adequately.

15 Authors

Carsten Gregorius – Phoenix Contact

Michael Niehaus - Lenze

Thomas Schulz-Basten – Berufsgenossenschaft Holz und Metall

Klaus Stark - Pilz

Related informations about the topic **"functional safety" can be found at www.zvei.org, Fachverband Automation "Schaltanlagen, Schaltgeräte & Industriesteuerungen"** and on the Internet of the participating member companies of the ZVEI.

ZVEI e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Phone: +49 69 6302-0
Fax: +49 69 6302-317
E-mail: zvei@zvei.org
www.zvei.org