ZVEI:
Die Elektroindustrie

Safety of Machinery

Notes on the application of standards EN 62061 and EN ISO 13849-1

Edition II

Fachverband Automation

IMPRINT

Safety of Machinery

Notes on the application of standards EN 62061 and EN ISO 13849-1

German Electrical and Electronic Manufacturer's Association
Lyoner Straße 9
60528 Frankfurt am Main
Germany

Automation Division
Switchgear, Controlgear,
Industrial Control Systems Section
Technical Committee Safety Systems in Automation

Author: Dr. Markus Winzenick

Phone: +49 69 6302-426
Fax: +49 69 6302-386
Mail: winzenick@zvei.org
www.zvei.org/automation

June 2012

Safety of Machinery

Are you a machine manufacturer or system integrator? Do you upgrade machinery?

This is what you need to consider in the future in terms of functional safety!

Notes on the application of standards EN 62061 and EN ISO 13849-1

1. Basic procedure for complying with the requirements of the machinery directive

What do I need to do to place a machine on the market in compliance with the directives?

The EC machinery directive stipulates that machinery should not pose a danger (risk assessment in accordance with EN ISO 12100). Given that there is no such thing as zero risk in technology, the aim is to achieve an acceptable residual risk. If safety is dependent on control systems, these must be designed so that the probability of functional faults is sufficiently low. If this is not possible, any faults that occur shall not lead to the loss of the safety function. To meet this requirement, it makes sense to use harmonized standards that have been created in accordance with a mandate from the European Commission and are published in the Official Journal of the European Communities (presumption of conformity). This is the only way to avoid spending extra time and effort when demonstrating conformity.

The two standards EN 62061 and EN ISO 13849-1 are compared below and a selection guide is provided for the user.

2. Why is EN 954-1 not sufficient for the future?

In the past, the safety-related parts of a machine control were designed in accordance with EN 954-1.

This was based on the calculated risk (formed into categories). The aim was to assign an appropriate system behavior to each category (deterministic approach). Once electronics, and programmable electronics in particular, had made their mark on safety technology, safety could no longer be measured purely in terms of the simple category system found in EN 954-1. Furthermore, it was unable to provide information on probability of failure (probabilistic approach).

Help is now available from EN 62061 and EN ISO 13849-1, the successor standards to EN 954-1.

3. Scope of the two standards

EN ISO 13849-1: *"Safety-related parts of control systems – Part 1: General principles for design"*

This standard may be applied to SRP/CS (safety-related parts of control systems) and all types of machinery, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.).

EN ISO 13849-1 also lists special requirements for SRP/CS with programmable electronic systems.

EN 62061: *"Functional safety of safety-related electrical, electronic and programmable electronic control systems"*

This standard defines requirements and gives recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery.

It does not define requirements for the performance of non-electronic (e.g., hydraulic, pneumatic or electro-mechanical) safety-related control elements for machinery.

4. Brief overview on EN ISO 13849-1

EN ISO 13849-1 is based on the familiar categories from EN 954-1:1996. It examines complete safety functions, including all of the devices involved in their design.

EN ISO 13849-1 goes beyond the qualitative approach of EN 954-1 to include a quantitative assessment of the safety functions. Performance Levels (PL) are used for this, building upon the categories.

Devices require the following safety-related characteristic parameters depending on device type:

- Category (structural requirement)
- PL: Performance Level
- $MTTF_d$: Mean time to dangerous failure
- B_{10d}: Number of cycles by which 10% of a random sample of wearing components have failed dangerously
- DC: Diagnostic coverage
- CCF: Common cause failure
- T_M: Mission time

The standard describes how to calculate the Performance Level (PL) for safety-relevant parts of control systems, based on designated architectures, for the designated mission time T_M.

In case of deviations EN ISO 13849-1 refers to IEC 61508 for electrical/electronic systems. Where several safety-relevant parts are combined into one overall system, the standard describes how to calculate the resulting PL that can be achieved.

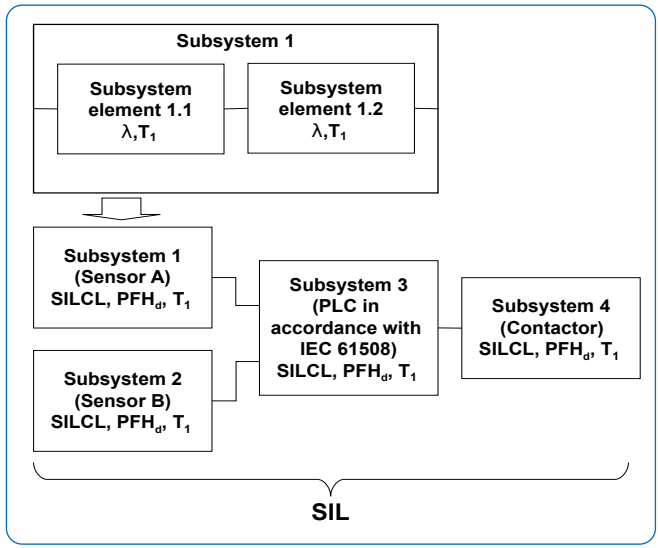
For the subsequent validation, EN ISO 13849-1 refers to Part 2, which was published at the end of 2003. This part provides information on, among other topics, fault considerations, maintenance, technical documentation and usage guidelines. The transition period from EN 954-1 to EN ISO 13849-1, during which either standard may be applied, ended in Europe on December 31, 2011.

5. *Brief overview of EN 62061*

EN 62061 represents a sector-specific standard under IEC 61508. It describes the implementation of safety-relevant electrical and electronic control systems on machinery and examines the total life cycle from the concept phase through to decommissioning. Quantitative and qualitative examinations of the safety-related control functions form the basis.

The performance of a safety function is described by the **Safety Integrity Level (SIL).**

The safety functions identified from the risk analysis are divided into safety subfunctions; these safety subfunctions are then assigned to actual devices, called subsystems and subsystem elements. Both hardware and software are handled this way. A safety-related control system is made up of several subsystems. The safety-related characteristics of these subsystems are described by characteristic parameters (SIL claim limit and PFH_d).



Safety-related characteristic parameters for subsystems:

- SILCL: Safety integrity claim limit
- PFH_d: Probability of dangerous failure per hour
- T_1: Smaller of either lifetime or proof test interval

These subsystems may in turn be made up of various interconnected subsystem elements (devices) with characteristic parameters to calculate the subsystem's corresponding PFH_d value.

Safety-related characteristic parameters for subsystem elements (devices):

- λ: Failure rate; for wearing elements (or without constant failure rate): B_{10} value
- SFF: Safe failure fraction

For electro-mechanical devices, the failure rate is indicated by the manufacturer as a B_{10} value, based on the number of switching cycles. The time-related failure rate and the life expectancy must be determined on the basis of the switching frequency for the respective application.

Internal parameters to be established during design / construction for a subsystem comprised of subsystem elements:

- T_2: Diagnostic test interval
- β: Susceptibility to common cause failure
- DC: Diagnostic coverage.

The PFH_d value of the safety-relevant control system is calculated by adding the subsystems' individual PFH_d values.

Users have the following options when designing a safety-relevant control system:

- Use devices and subsystems that already comply with EN ISO 13849-1 and IEC 61508 or EN 62061. The standard specifies how to incorporate qualified devices when implementing safety functions.
- Develop their own subsystems.
  - Programmable, electronic subsystems or complex subsystems: apply IEC 61508.
  - Simple devices and subsystems: apply EN 62061.

The standard represents a comprehensive system for the implementation of safety-relevant electrical, electronic and programmable electronic control systems. EN 62061 has been a harmonized standard since December 2005.

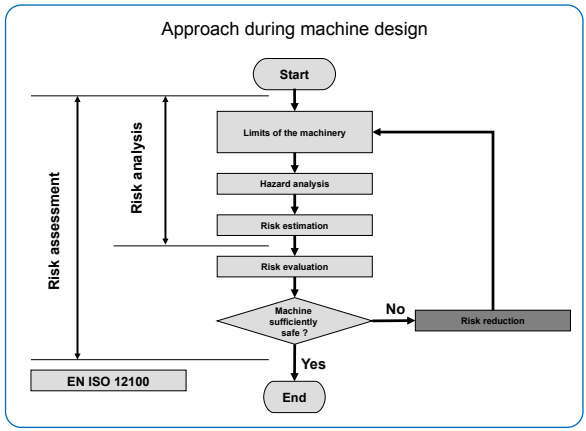
EN ISO 13849-1 should be applied for non-electrical systems.

6. Achieving safety, step-by-step – basic procedure

Step 1 – Risk assessment in accordance with EN ISO 12100

It can be assumed that a hazard on a machine will result in harm sooner or later if protective measures are not put in place. Protective measures are a combination of the measures taken by the designer and those implemented by the user. Measures taken during the design phase are always preferable to those implemented by the user, and generally they are also more effective.

The designer must follow the sequence described below, bearing in mind the experience gained by users of similar machinery and information gained from discussions with potential users (if this is possible):



- Establish the limits and the intended use of the machinery
- Identify the hazards and any associated hazardous situations
- Estimate the risk for each identified hazard and hazardous situation
- Evaluate the risk and decide on the need for risk reduction

Step 2 – Define the measures required to reduce the calculated risks

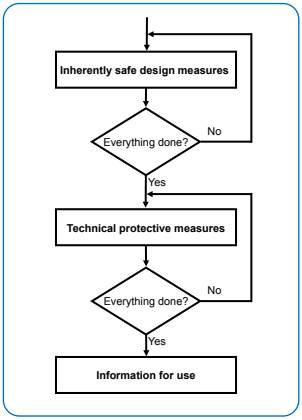
The objective is to reduce risk as much as possible, taking various factors into account. The process is iterative; making the best possible use of the available technologies, it may be necessary to repeat the process several times in order to reduce the risk.

When carrying out the process, the following priority ranking shall apply:

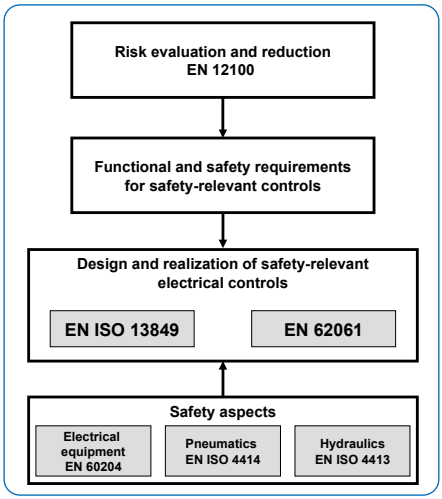
1. Safety of the machine in all phases of its lifetime;
2. The ability of the machine to perform its function;
3. User friendliness of the machine.

Only then the machine's manufacturing, operating and disassembly costs shall be taken into consideration.

The hazard analysis and risk reduction process requires hazards to be eliminated or reduced through a hierarchy of measures:



1. Hazard elimination or risk reduction through design
2. Risk reduction through technical protective devices and potential additional protective measures
3. Risk reduction through the availability of user information about the residual risk



Step 3 – Risk reduction through control measures

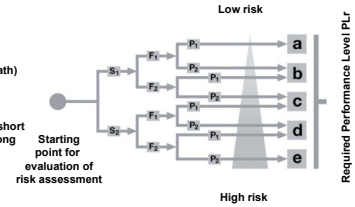
If safety-relevant control parts are used to implement a protective measure in order to achieve the necessary risk reduction, the design of these control parts is to be an integral part of the overall design procedure for the machine. The safety-relevant control system provides the safety function(s) with a SIL or PL that achieves the necessary risk reduction.

Step 4 – Implementation of control measures using EN 13849-1 or EN 62061

1) Determination of the required Performance

EN ISO 13849-1

Determination of the required Performance Level (PL_r)



EN 62061

Risk estimation and definition of the required Safety Integrity Level (SIL)

Consequences and severity	S	Frequency and duration	F	Probability of hazardous event	W	Avoidance	P	Class Cl 3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	≤ 1/hour	5	Very high	5			SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, losing fingers	3	> 1/hour - ≤1/day	5	Likely	4				AM	SIL1	SIL2	SIL3
Reversible, medical attention	2	> 1/day - ≤2/week	4	Likely	3	Impossible	5			AM	SIL1	SIL2
Reversible, first aid	1	2/week - ≤1/year	3	Rarely	2	Possible	3				AM	SIL1
		> 1/year	2	Negligible	1	Likely	1					

OM = other measures recommended

2) Specification

The specification of the functional requirements shall describe each safety function that is to be performed. Any interfaces with other control functions shall be defined and any necessary error reactions established. Furthermore, the required SIL or PL must be defined.

3) Design of the control architecture

Part of the risk reduction process involves the definition of the machine's safety functions. This includes the safety functions of the control system, e.g. to prevent unexpected start-up. When defining the safety functions, it is always important to consider that a machine has different operating states (e.g., automatic & setup mode) and that the protective measures in these different modes may be totally different (e.g., safely limited speed in setup mode <-> two-hand in automatic mode). A safety function may be implemented via one or more safety-relevant control parts and several safety functions may be divided over one or more safety-relevant control parts (e.g., logic module, energy transmission element(s)).

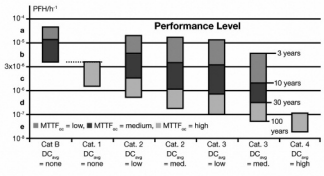
4) Determination of the achieved Performance

EN ISO 13849-1	EN 62061
The PL shall be estimated for each selected SRP/CS and/or combination of SRP/CS that performs a safety function. The PL of the SRP/CS shall be determined by the estimation of the following parameters: • The $MTTF_d$ or B_{10d} value for single components; • The DC • The CCF • The structure • The behavior in the case of failure • Safety-related software • Systematic failures • The ability to perform a safety function under expected environmental conditions • Application of demonstrated safety principles	The selection or design of the SRECS shall always meet the following minimum requirements: • Requirements for hardware safety integrity, comprising • Architectural constraints for hardware safety integrity • Requirements for the probability of dangerous random hardware failures plus requirements for systematic safety integrity, comprising • Requirements for avoidance of failures and • Requirements for the control of systematic faults. EN 62061 also describes requirements for implementing application programs. Safety-related characteristic parameters for subsystems: • SILCL: SIL claim limit • PFH_d: Probability of dangerous failure per hour • T_1: Lifetime

EN ISO 13849-1

Performance Level (PL)	Probability (average) of dangerous failure [1/h]		
a	≥ 10^{-5}	PFH_d	< 10^{-4}
b	≥ $3x10^{-6}$	PFH_d	< 10^{-5}
c	≥ 10^{-6}	PFH_d	< $3x10^{-6}$
d	≥ 10^{-7}	PFH_d	< 10^{-6}
e	≥ 10^{-8}	PFH_d	< 10^{-7}

Relationship between the categories DC, $MTTF_d$ and PL



Note:
The PFH values represent a necessary prerequisite for determining the Performance Level. Furthermore, measures for failure avoidance such as CCF, category and DC must be taken into account for a complete determination of the PL.

EN IEC 62061

SIL (IEC 61508)	Probability (average) of dangerous failure [1/h]		
1	≥ 10^{-6}	PFH_d	< 10^{-5}
2	≥ 10^{-7}	PFH_d	< 10^{-6}
3	≥ 10^{-8}	PFH_d	< 10^{-7}

Safety-related characteristic parameters for subsystem elements (devices):

- B_{10d} value: For wearing elements (without constant failure rate)
- T_1: Lifetime
- T_2: Diagnostic test interval
- β: Susceptibility to common cause failure
- DC: Diagnostic coverage
- SFF: Safe failure fraction

SFF	HFT 0	HFT 1	HFT 2
< 60%	Not allowed	SIL1	SIL2
≥ 60% to < 90%	SIL1	SIL2	SIL3
≥ 90% to < 99%	SIL2	SIL3	SIL3
≥ 99%	SIL3	SIL3	SIL3

EN ISO 13849-1	EN IEC 62061

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

Note:
The table describes the relationship between the two concepts of the standards (PL and SIL). The "PFH coupling" used in this table is, however, not sufficient on its own for the determination.

5) Verification

For each individual safety function, the PL of the corresponding SRP/CS must match the "Required Performance Level". Where various SRP/CS form part of a safety function, their PLs shall be equal to or greater than the Performance Level required for this function.

Where several SRP/CS are connected in series, the final PL can be determined using Table 11 from the standard.

The probability of a dangerous failure of each safety-relevant control function (SRCF) as a result of dangerous random hardware failures shall be equal to or less than the failure threshold value defined in the specification of the safety requirements.

The SIL that is achieved by the SRECS on the basis of architectural constraints shall be less than or equal to the lowest SILCL of any subsystem involved in performing the safety function.

6) Validation

The design of a safety-related control function shall be validated. The suitability of the safety-related control function is examined for the application. The validation can be performed by means of an analysis or test (e.g., by targeted simulation of individual or multiple faults).

7. Glossary

Abbreviation	Explanation
B_{10d}	Number of cycles until 10% of components fail causing danger
λ	Failure Rate
λ_s	Failure Rate (failure to safe side)
λ_d	Failure Rate (failure to danger)
CCF	Common cause failure
DC	Diagnostic coverage
DC_{avg}	Average diagnostic coverage
	Designated architecture of an SRP/CS
HFT	Hardware fault tolerance
MTBF	Mean time between failures (during normal operation)
MTTF	Mean time to failure
$MTTF_d$	Mean time to dangerous failure
MTTR	Mean time to repair (always significantly less than the MTTF)
PFH	Probability of failure per hour
PFH_d	Probability of dangerous failure per hour
PL	Performance level; ability of safety-related parts to perform a safety function under expected conditions, to achieve the expected risk reduction
PL_r	Required Performance Level
SIL	Safety integrity level
SILCL	SIL claim limit (suitability)
SRCF	Safety-related control function
SRP/CS	Safety-related parts of a control system
SRECS	Safety-related electrical control systems
T_1	Lifetime or repeat test of the safety system
T_2	Diagnostic test interval
T_M	Mission time

Abbreviation	Explanation
β	Susceptibility to common cause failure
C	Duty cycle (per hour) of an electro-mechanical component
SFF	Safe failure fraction
Security	Common term for protective guarding. A person or item is safeguarded through monitoring.
Safety	Collective term for functional safety and machine safety, among others
Machinery safety	State achieved when measures have been taken to reduce the risk to an accepted residual risk after the hazard analysis has been carried out
Functional safety	Part of the safety of the machine and the machine control system which depends on the correct functioning of the SRECS, other technology safety-related systems and external risk reduction facilities.

8. FAQ list

Q: Do solenoid valves / contactors have a SIL or PL rating?

A: No. Single components cannot have a SIL and PL.

Q: What is the difference between SIL and SILCL?

A: The SIL rating always refers to a complete safety function while the SILCL refers to the subsystem.

Q: Is there an analogy between PL and SIL?

A: A relationship between PL and SIL can be established through the PFH_d value. (See step 4: "Determination of the achieved Performance Level".) Please note – the table does not take into account the specific specifications of the two standards with respect to approved structure, diagnostic coverage or their systematic requirements.

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]			Performance level (PL) EN ISO 13849-1	SIL Level (IEC61508)
$\geq 10^{-5}$	PFH_d	$< 10^{-4}$	a	-
$\geq 3x10^{-6}$	PFH_d	$< 10^{-5}$	b	1
$\geq 10^{-6}$	PFH_d	$< 3x10^{-6}$	c	
$\geq 10^{-7}$	PFH_d	$< 10^{-6}$	d	2
$\geq 10^{-8}$	PFH_d	$< 10^{-7}$	e	3

Q: What diagnostic coverage can I claim for relays and contactors with positive-guided contacts?

A: In accordance with both standards, a DC of 99% can be assumed for positive-guided contacts with redundant (2-channel) contactors and relays.

A diagnostic function with an appropriate error reaction or at least a warning of the hazard is a prerequisite.

Q: Can I achieve a hardware fault tolerance of 1 with a single, mechanical door monitoring (safety gate) switch?

A: No, just one fault would generally result in failure. For magnetically actuated or RFID-based systems, it is possible for the manufacturer to confirm a hardware fault tolerance of 1.

Q: Is there a PFH_d value for wearing components?

A: No. Users can calculate a PFH_d value for wearing components for the specific application using the B_{10d} value in relation to the number of duty cycles.

Q: What is the difference between MTBF and MTTF?

A: The MTBF describes the time between two failures, whereas the MTTF describes the time to the first failure.

Q: What does the letter "d" mean in $MTTF_d$?

A: "d" stands for "dangerous" –> the $MTTF_d$ describes the time to the first dangerous failure

Q: May I apply EN ISO 13849-1 when integrating complex programmable electronics?

A: Yes. However, for operating system software and safety functions in accordance with PL "e", the requirements of IEC 61508-3 will need to be considered.

Q: What can I do if I do not receive any characteristic data from my component manufacturer?

A: The annexes of both EN ISO 13849-1 and EN 62061 contain substitute reference values for frequently used components. Where available, however, manufacturer's values should always be used.

Q: Can I apply EN ISO 13849-1 to calculate the MTTF on process valves/armatures that are switched less than once per year (low demand)?

A: No, EN ISO 13849-1 only describes high-demand mode. For this reason, an MTTF assessment can only be made using additional measures such as "forced dynamization".

Q: Can I apply EN 62061 to calculate the failure rate on process valves/armatures that are switched less than once per year (low demand)?

A: See question above.

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

A: No. There is no separate mandatory certification for the software on the basis of either standard; rather, it is oriented on the size and complexity of the overall project. Within the scope of verification and validation of safety functions, a software test may be necessary. Information on this topic can be found in EN ISO 13849-1 Chapter 4.6 and EN 62061 Chapters 6.9 and 6.10 as well as in EN 61508-3.

Q: Can any component with MTTF be used for safety technology?

A: No, in addition to the statistical characteristic data such as MTTF and B_{10d}, the component must also be functionally suited for the function and it must satisfy certain minimum requirements such as constructive and safety-related requirements (implementation and application of safety principles).

German Electrical and Electronic
Manufacturers' Association
Lyoner Straße 9
60528 Frankfurt am Main
Germany

Automation Division
Switchgear, Controlgear,
Industrial Control Systems Section

Technical Committee
Safety Systems in Automation