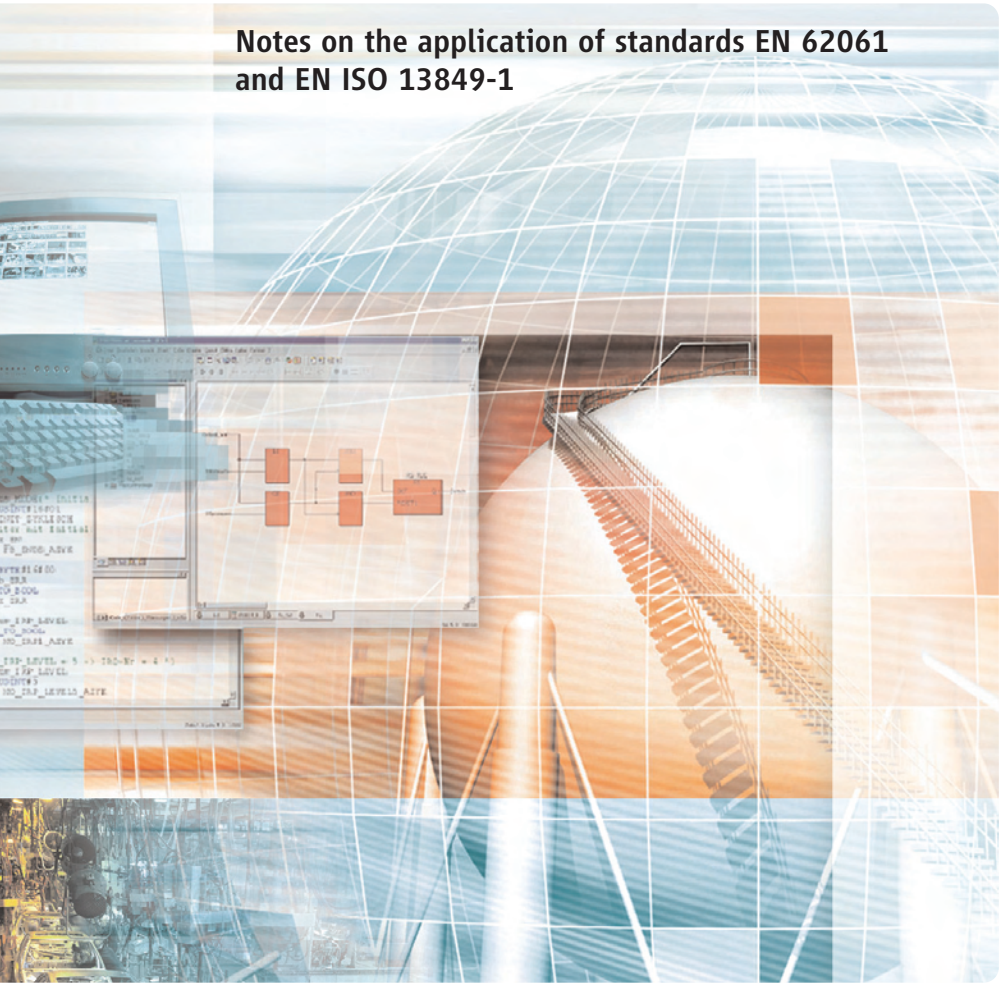
ZVEI:

Automation

Safety of machinery

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



IMPRINT

Safety of machinery

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

German Electrical and Electronic Manufacturer's Association
Stresemannallee 19
60596 Frankfurt am Main
Germany
Professional Association Automation
Specialist Area of Switchgears, Switchgears, Industrial Controls
Technical Committee Safety System in Automation

Autor: Gunther Bernd
Phone: +49 69 6302-323
Fax: +49 69 6302-386
Mail: bernd@zvei.org
www.zvei.org/automaton

June 2007

Safety of machinery

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

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

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

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 EU Machinery Directive stipulates that machinery should not present a risk (risk assessment in accordance with EN 1050 or EN ISO 14121-1). 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 errors is sufficiently low. If this isn't possible, any errors that occur shall not lead to the loss of the safety function. To meet this requirement it makes sense to use harmonised 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 demonstrating conformity in the event of a claim.

The two standards EN 62061 and EN ISO 13849-1 are compared below.

2. *Why is today's EN 954-1 not sufficient for the future?*

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

This was based on the calculated risk (formed into categories). The aim was to set an appropriate system behaviour ("control class") against a 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 standard to EN 954-1.

3. Scopes 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-electrical (e.g. hydraulic, pneumatic, electromechanical) safety-related control elements for machinery.

4. Brief overview of 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 the components 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. A **performance level (PL)** is used for this, building upon the categories.

Components/devices require the following safety parameters:

- 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-related parts of control systems, based on designated architectures, for the designated mission time T_M.

EN ISO 13849-1 refers any deviations to IEC 61508. Where several safety-related parts are combined into one overall system, the standard describes how to calculate the PL that can be achieved.

For additional guidelines on validation EN ISO 13849-1 refers to Part 2, which was published at the end of 2003. This part provides information on fault considerations, maintenance, technical documentation and usage guidelines. The transition period from EN 954-1 to EN ISO 13849-1 is likely to end in October 2009. Until then, either standard may be applied.

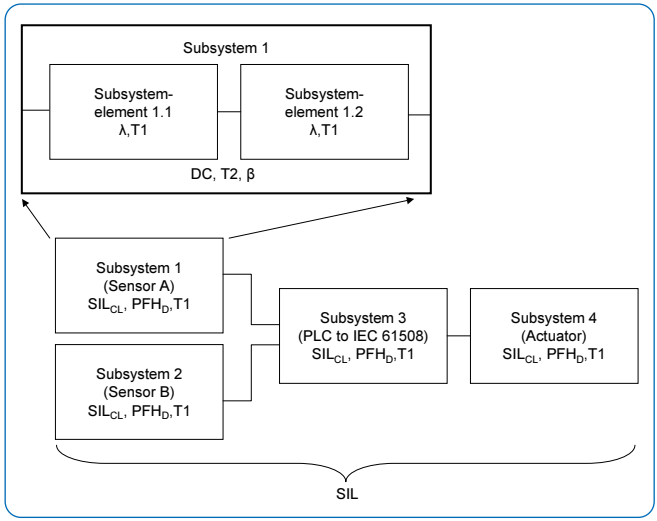
5. *Brief overview of EN 62061*

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

The performance level is described through 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 through parameters (SIL claim limit and PFH_D).



Safety-related parameters for subsystems:

- SILCL: SIL claim limit
- PFH_D: Probability of dangerous failure per hour
- T_1: Lifetime

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

Safety-related parameters for subsystem elements (devices):

- λ: Failure rate;
  for wearing elements: describe via the B_{10} value
- SFF: Safe failure fraction

On electromechanical devices the failure rate is indicated by the manufacturer as a B_{10} value, based on the number of cycles. The time-based failure rate and lifetime must be determined through 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
- PFH_D: The PFH_D value of the safety-related control system is calculated by adding the subsystems' individual PFH_D values.

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

- Use devices and subsystems that already comply with EN 954-1 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-related electrical, electronic and programmable electronic control systems. EN 62061 has been a harmonised standard since December 2005.

EN 954-1, or alternatively EN ISO 13849-1, should be applied for non-electrical systems.

6. *Achieving safety, step-by-step – Basic procedure*

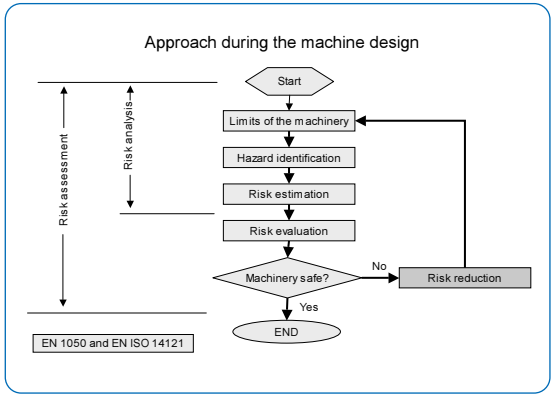
Step 1 – Risk assessment in accordance with EN 1050 / EN ISO 14121

It can be assumed that a hazard on a machine will result in harm sooner or later if safety measures are not put in place.

Safety measures are a combination of these measures taken by the designer and those implemented by the user. Measures taken at the design

phase are 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.

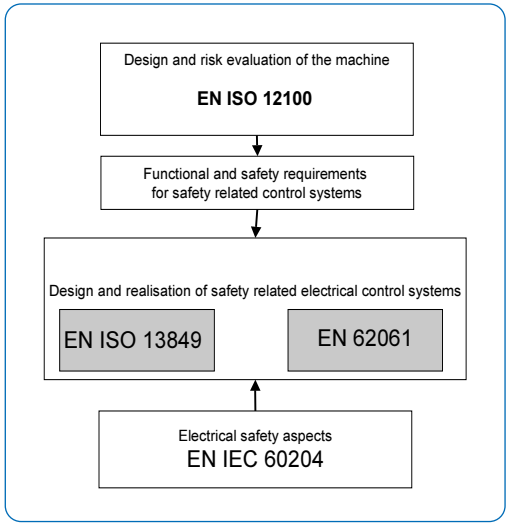
When carrying out the process, the following priority ranking shall apply:

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

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

- Hazard elimination or risk reduction through design
- Risk reduction through technical protection devices and potential additional protective measures
- Risk reduction through the availability of user information about residual risk



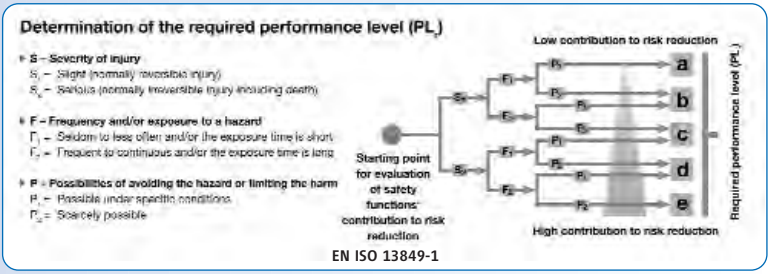
Step 3 – Risk reduction through control measures

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

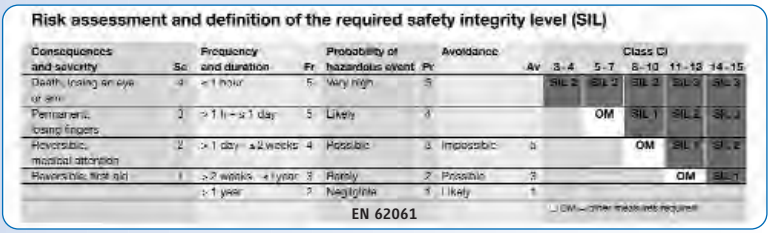
Step 4 – Implementation of control measures using EN ISO 13849-1 or EN 62061

1) Determination of the required performance level

EN ISO 13849-1



EN 62061



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. 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 on 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 modes (e.g. automatic & setup mode) and that the safety 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-related control parts and several safety functions may be divided over one or more safety-related control parts (e.g. logic module, energy transmission element(s)).

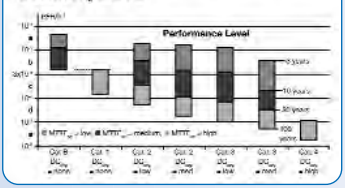
4) Determination of the achieved performance level

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 MTTFd value for single components • The DC • The CCF • The structure (category) • The behaviour of the safety function under fault condition(s) • Safety-related software • Systematic failures • The ability to perform a safety function under expected environmental conditions	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 failures. EN 62061 also describes requirements for implementing application programs. Safety-related parameters for subsystems: • SILCL: SIL claim limit • PFH_D: Probability of dangerous failure per hour • T_1: Lifetime

EN ISO 13849-1

Performance level	Probability (average) of a failure to danger [1/h]
a	$10^{-5} \leq PFH < 10^{-4}$
b	$3 \cdot 10^{-6} \leq PFH < 10^{-5}$
c	$10^{-6} \leq PFH < 3 \cdot 10^{-6}$
d	$10^{-7} \leq PFH < 10^{-6}$
e	$10^{-8} \leq PFH < 10^{-7}$

Relationship between the categories DC, MTTF$_d$ and PL



Note:

The PFH$_D$ comparisons are an essential requirement for determining the performance level. To complete the determination of the PL, CCF, category and DC shall also be considered.

EN IEC 62061

Probability (average) of a failure to danger [1/h]	SIL Level
$10^{-5} \leq PFH < 10^{-5}$	SIL 1
$10^{-7} \leq PFH < 10^{-6}$	SIL 2
$10^{-8} < PFH < 10^{-7}$	SIL 3

Safety-related parameters for subsystem elements (devices):

- λ: Failure rate
- B_{10} value: For wearing elements
- T_1: Lifetime
- T_2: Diagnostic test interval
- β: Susceptibility to common cause failure
- DC: Diagnostic coverage
- SFF: Safe failure fraction
- HTF: Hardware fault tolerance

SFF	HFT 0	HFT 1	HFT 2
< 60%	Not allowed	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

EN ISO 13849-1	EN IEC 62061

Performance level	SIL Level
a	--
b	SIL 1
c	SIL 1
d	SIL 2
e	SIL 3

Note:

The illustration describes the relationship between the standards' two concepts (PL and SIL), based on probability of failure.

5) Verification

For each individual safety function, the PL of the corresponding SRP/CS must match the "Required Performance Level". Where various SRP/CS from 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 dangerous failure of each safety-related 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 validation must show that the combination for each safety function of the safety-related parts meets the relevant requirements.

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	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 foreseeable conditions, to achieve the expected risk reduction
PL_r	Required performance level
SIL	Safety integrity level

Abbreviation	Explanation
SILCL	SIL claim limit (suitability)
SRP/CS	Safety-related parts of a control system
SRECS	Safety-related electrical control systems
T_1	Lifetime or proof test interval, assumed lifetime of safety system
T_2	Diagnostic test interval
TM	Mission time
β	Susceptibility to common cause failure
C	Duty cycle (per hour) of an electromechanical 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 machinery 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

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

No. Single components cannot have a SIL or PL rating.

What is the difference between SIL and SILCL?

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

Is there an analogy between PL and SIL?

A relationship between PL and SIL can be established through the PFH value. (See step 4: "Determination of the achieved performance level").

Performance level (EN13849-1)	Probability of a dangerous failure per hour [1/h]	SIL Level after EN IEC 62061
b	$3 \cdot 10^{-6} \leq PFH < 10^{-5}$	SIL 1
c	$10^{-6} \leq PFH < 3 \cdot 10^{-6}$	SIL 1
d	$10^{-7} \leq PFH < 10^{-6}$	SIL 2
e	$10^{-8} \leq PFH < 10^{-7}$	SIL 3

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

In accordance with both standards, a DC of 99% can be assumed due to the positive-guided contacts on contactors and relays.

A diagnostic function with an appropriate error reaction is a prerequisite.

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

No, just one error would cause the circuit to fail.

Is there a probability of failure or PFH_D value for wearing components?

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

What is the difference between MTBF and MTTF?

The MTBF describes the time between two failures, whereas

MTTF describes the time to the first failure.

What does the letter "d" mean on MTTFd?

"d" stands for "dangerous" –> the MTTFd describes the mean time to the first dangerous failure.

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

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.

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

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.

Can I apply EN ISO 13849-1 to calculate the MTTF on process valves/armatures that are only switched once or twice a year (low demand)?

No, EN ISO 13849-1 only describes high demand mode, so an MTTF assessment can only be made using additional measures such as “forced dynamisation”.

Can I apply EN 62061 to calculate the failure rate on process valves/armatures that are only switched once or twice a year (low demand)?

See question above.

Does application software have to be certified? If “Yes”, to which standard?

No. There is no mandatory certification for either standard. However, there may be mandatory certification for Annex IV machines under the Machinery Directive (e.g. presses). Requirements for software production can be found in both EN 62061 and EN ISO 13849-1.

German Electrical and Electronic
Manufacturers' Association
Stresemannallee 19
60596 Frankfurt am Main
Germany

Professional Association Automation

Specialist Area of Switchgears, Switchgears,
Industrial Controls

Technical Committee Safety System
in Automation