4. What is behind the categories?
The categories describe what the safety function does in the event of a fault and the possibilities for error detection. Differentiations are made between categories B, 1, 2, 3 and 4.

Category B:
Components are constructed according to the applicable standards (basic safety principles) and withstand the expected operating stress.
Occurrence of fault: Loss of safety function is possible.
Fault detection: None (DC = 0)

Category 1:
Requirements of category B must be met.
Well-tried components and well-tried safety principles must be used.
Occurrence of fault: Loss of safety function is possible, but less likely than is the case with category B.
Fault detection: None (DC = 0)

Category 2:
Requirements of category B must be met.
Start-up check and periodical safety-function check
Well-tried safety principles must be used.
Occurrence of fault: Loss of safety function is possible between checks.
Fault detection: At every check (DC = low or medium)

Category 3:
Requirements of category B must be met.
Well-tried safety principles must be used.
An individual occurrence of fault does not lead to the loss of the safety function, whenever reasonably practicable.
Occurrence of fault: No loss of safety function.
Fault detection: Good, but not complete (DC = low or medium)

Category 4:
Requirements of category B must be met.
Well-tried safety principles must be used.
A single fault does not lead to the loss of the safety function, an accumulation of undetected faults shall not lead to the loss of the safety function.
Occurrence of fault: No loss of safety function
Fault detection: Very good (DC = high)

5. Do not forget validation!
EN ISO 13849-2 lays down procedures and conditions with which a safety function as well as the performance level and category attained can be validated. For categories 2, 3 and 4 the validation of the safety function shall also include testing by appropriate fault injection.

Our support for you
Our seminar on EN ISO 13849-1 offers extensive training in theory and practice. Please apply to:

www.suva.ch/kurse
>> Kataloge >> Arbeitssicherheit und Gesundheitsschutz
>> Deutsch >> Maschinenbau und Instandhaltung
>> EN ISO 13849-1 Sicherheitsfunktionen für Maschinen - NOST

Mechanical engineering product safety – we can help

We can answer your questions on the following topics:
- CE conformity
- European directives and standards
- Safety of machines and control systems

We can provide you with:
- Type examinations
- Assessments of machinery protective measures
- Seminars on product safety

Benefit from our years of experience, our up-to-date knowledge and visit our website: www.suva.ch/certification

Suva
Section Technology
Accredited Certification Body SCESp 0008
European notified body, identification number 1246
P.O. Box 4358, CH-6002 Lucerne
Tel. +41 41 419 61 31
Fax. +41 41 419 58 70
technik@suva.ch
www.suva.ch/certification

Orders
www.suva.ch/CE13-1.e
Tel. +41 41 419 58 51

Orders for standards
Schweizerische Normen-Vereinigung
www.snv.ch
Tel. +41 52 224 54 54

Electrosuisse
SEV Association for Electrical Engineering, Power and Information Technologies
www.electrosuisse.ch
Tel. +41 44 956 11 11

Order no.
CE13-1.e - 10.2021

Safety functions for machines – the most important points in brief

Overview of EN ISO 13849-1

suva
CERTIFICATION

Directive 2006/42/EC (Machinery Directive) prohibits in clause 1.2.1 hardware or software faults in the control system of a machine from becoming hazards. This requirement is set forth in standard EN ISO 13849-1 “Safety of machinery – safety-related parts of control systems”. This document provides an overview of the main aspects contained in EN ISO 13849-1. It is not a substitute for reading and applying the standard.

1. Combining established practice and innovations

A performance level shall be determined for each subsystem and/or each combination of subsystems that provide a safety function. The PL of the subsystem shall be determined by the estimation of the following aspects:

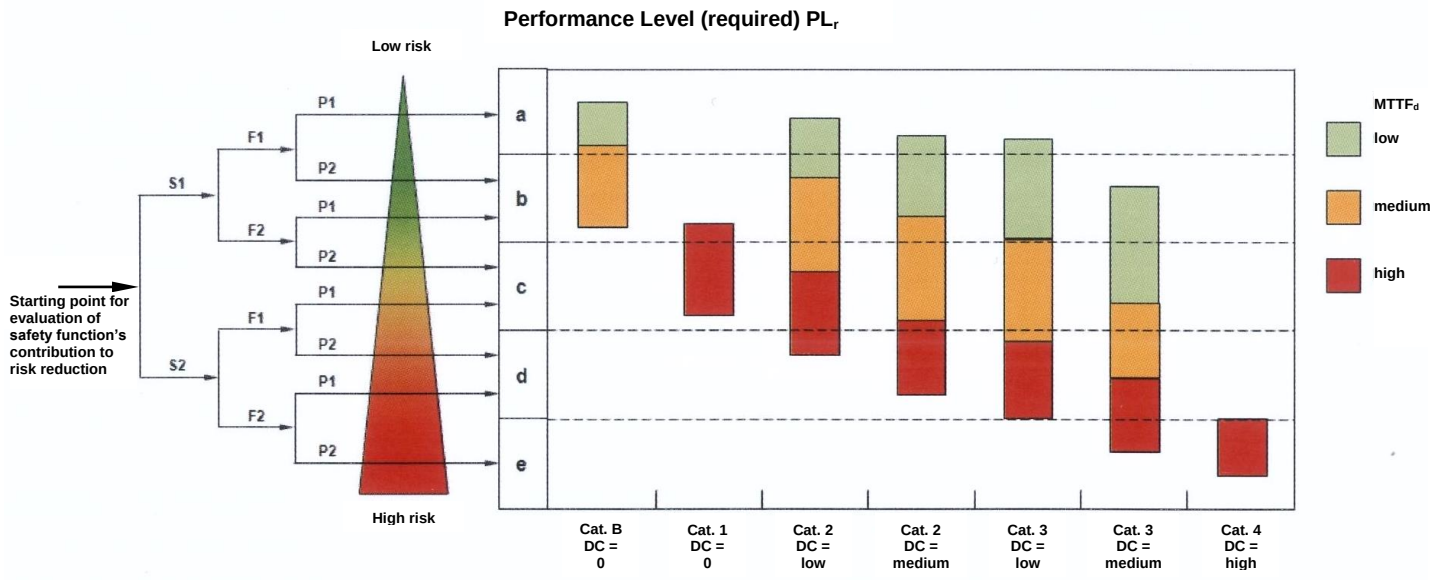
- Architecture of the safety function (category)
- Component reliability ($MTTF_D$)
- Quality of tests, diagnosis coverage (DC)
- Common-cause failures (CCF)
- Behavior under error condition (s)
- Safety-related Software
- Measures against systematic failures
- Ability to perform safety functions under foreseeable environmental conditions
- etc.

The standard allows a simplified procedure based on the definition of the five designated architectures that meet special design features and behaviour in the event of a fault.
The simplified procedure allows the PL to be determined based on the first three parameters listed above with the aid of EN ISO 13849-1, Figure 5.
The advantage: users can either accept the designated architecture or design their own architecture. However, if they design their own architecture then they must perform complex mathematical calculations, which are not supported by this standard.

2. Terms used

PL	Performance level Discrete level specifying the capability of the safety-related parts of a control system to carry out a safety function under foreseeable conditions.
$MTTF_D$	Mean time to dangerous failure (annexes C, D)
DC	Diagnostic coverage (annex E)
CCF	Common cause failure (annex F)

3. From risk to performance level



Source: Fig. A.1 and Fig. 5 from EN ISO 13849-1

The following steps go from the risk to the performance level of each individual safety function:

1. The first step is to determine which performance level is required for the corresponding safety function (PL_r, required performance level). The PL_r is ascertained according to the risk assessment and using of a type-C standard or - if not available - with the help of the diagram shown above (q.v. the key to the diagram above for the parameters S, F and P).
2. The next step consists of the design of a safety-related part of the control system (SRP/CS) that implements the safety function.
3. The parameters of the components ($MTTF_d$), their diagnostic coverage (DC) and the category are required from the design of the safety-related part of the control system. The PL attained can then be estimated with the help of this information and the chart shown above. It is assumed that all other relevant demands have been met (measures against CCF, demands on software, etc.).
4. The performance level PL achieved with the draft must be at least as reliable as the required performance level PL_r. ($PL \geq PL_r$).

Key:

Severity of injury

S1	Slight (normally reversible injury)
S2	Serious (normally irreversible injury or death)

F	**Frequency and/or exposure to the hazard**
F1	Seldom-to-less-often and/or exposure time is short
F2	Frequent-to-continuous and/or exposure time is long

P	**Possibility of avoiding the hazard or limiting harm**
P1	Possible under specific conditions
P2	Scarcely possible

$MTTF_D$	**Mean time to dangerous failure**
low	3 years ≤ MTTFD < 10 years
medium	10 years ≤ MTTFD < 30 years
high	30 years ≤ MTTFD ≤ 100 years

DC	**Diagnostic coverage**
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC