Basic Knowledge

Safe Machines

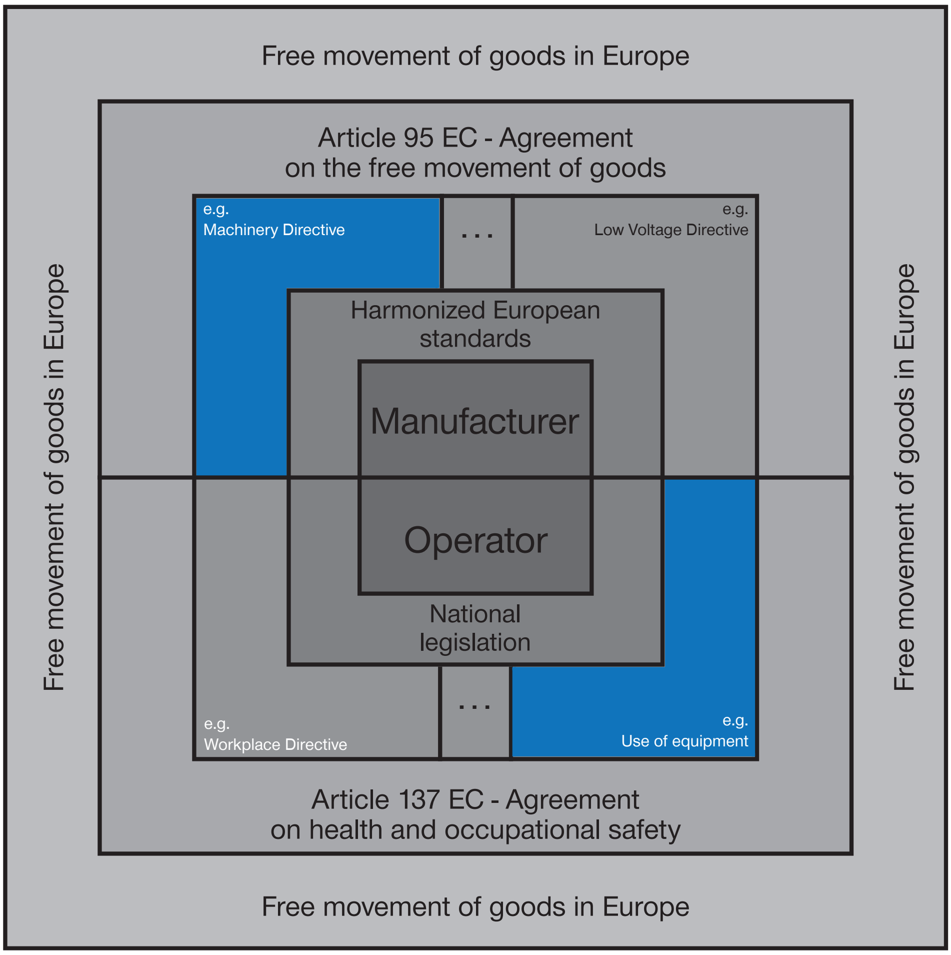
DDOC00626

THE KNOW-HOW FACTORY

Content

1. Basic legal principles

Mechanical engineering is an important technical subsector and one of the core industrial areas of the EC economy. The social costs of numerous accidents resulting directly from machine operation can be reduced if the aspect of safety is incorporated into the engineering and construction of machines and these machines are installed and maintained properly.


Free movement of goods in Europe
Article 95 EC - Agreement
on the free movement of goods
e.g.
Machinery Directive
. . .
e.g.
Low Voltage Directive
Harmonized European
standards
Manufacturer
Operator
National
legislation
e.g.
Workplace Directive
. . .
e.g.
Use of equipment
Article 137 EC - Agreement
on health and occupational safety
Free movement of goods in Europe
Free movement of goods in Europe
Free movement of goods in Europe

1.1 European rules and regulations

Products must be assembled such that humans, animals and the environment are protected. This is the principle on which applicable European rules and regulations are based.

1.2 CE marking

When a manufacturer, distributor or EU authority affixes the CE marking to a product, it is declaring that this product meets the requirements of EU Regulation defined in the legislation of the European Community.

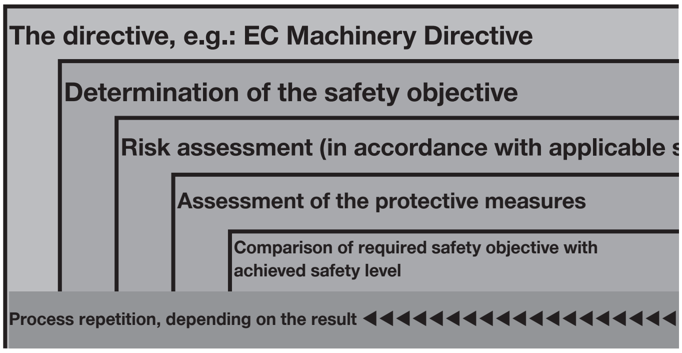
The CE marking is a symbol of the free movement of goods within the EU.
Legally, the CE marking is not a seal of approval (quality label), and is only intended to document compliance with the minimum legal requirements.

2. The path to a safe machine

⇨ Identify hazards

⇨ Assess risks

⇨ Reduce risks



The directive, e.g.: EC Machinery Directive

Determination of the safety objective

Risk assessment (in accordance with applicable s

Assessment of the protective measures

Comparison of required safety objective with achieved safety level

Process repetition, depending on the result ◀◀◀◀◀◀◀◀◀◀◀◀◀◀◀◀◀◀◀

Companies such as Zimmer Group that manufacture products subject to the scope of validity of the 2006/42/EC Machinery Directive and that can verify a quality management system certified in accordance with ISO 9001 carry out a procedure for Declaration of Conformity in accordance with Appendix VIII of the Machinery Directive.

A risk assessment is an integral part of this process carried out during development.

This risk assessment analyzes danger zones, assesses the associated risks, determines actions for reducing risk and repeats the evaluation until it can be proven that sufficient risk reduction is in place.

Risk = severity of the potential damage + probability of occurrence

2.1 Safe machine – relevant standards

EN ISO 12100	Safety of machinery – General principles for design – Risk assessment and risk reduction
EN 60204-1	Safety of machinery – Electrical equipment of machines
EN 62061	Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems
DIN EN ISO 13849-1/-2	Safety of machinery – Safety-related parts of control systems (Part 1 and Part 2)

Engineering and risk evaluation of the machine	Electrical safety aspects
EN ISO 12100 Safety of machinery – General principles for design – Risk assessment and risk reduction	EN 60204-1 Safety of machinery – Electrical equipment of machines
⇩	⇩
Preliminary design and implementation of safety-related control systems	
EN 62061 Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems	
Any architecture (safety integration level (SIL))	
DIN EN ISO 13849-1 Safety of machinery – Safety-related parts of control systems (Part 1)	
Intended architectures (control categories/Performance Level (PL))	

3. Performance level, failure, diagnostics, etc.

The performance level (PL) is a function of:

- The control category used (Cat. B through 4)
- The diagnostic coverage (DC)
- The mean operating time until a failure occurs ($MTTF_d$)
- The common cause failures (CCF)

This means that the PL of an individual product can only ever be calculated together with the control architecture being used and the application-related data.

3.1 B10d value

The $B10_d$ value is the point at which statistics indicate that 10% of test objects fail. With respect to machine safety, only the dangerous failures are relevant.
ISO 13849-1 permits the assumption that every second failure is dangerous.
Based on this, it is safe to assume the following:

$$B10_d = 2 \text{ x } B_{10}$$

The $B10_d$ value of our products is therefore specified in the catalogs and in the installation and operating instructions. Zimmer Group determines this value in in-house test laboratories in conjunction with designated authorities.

3.2 $MTTF_d$ value

Mean operating time until a failure occurs (mean time to failure)
The value of the $MTTF_d$ of each channel is specified in three levels (see Table “5”) and must be taken into account individually for each channel (e.g. single channel or each channel of a redundant system).

For all products that are installed in safety-related parts, machines or systems of control systems and that have a direct effect on the safety function, this value has to be calculated according to the following formula:

$$MTTF_d = \frac{B10_d}{0{,}1 \text{ x } n_{op}}$$

Here, the variable n_{op} indicates that this value is directly related to the operating conditions for the user.
n_{op} = average number of annual actuations
d_{op} = operating days/year
h_{op} = operating hours/day
t_{cycle} = cycle time in [s]

$MTTF_d$ value for various channels, symmetrization of the $MTTF_d$ for each channel:

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} + MTTF_{dCn} \dots - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}} + \frac{1}{MTTF_{dCn}} \dots}\right]$$

$$n_{op} = \frac{d_{op} \text{ x } h_{op} \text{ x } 3600s/h}{t_{cycle}}$$

The following is an excerpt from Table “5” “Mean time of each channel to dangerous failure“ (MTTF) from EN ISO 13849-1.

$\mathrm{MTTF_d}$	
Designation for each channel	**Range for each channel**
low	3 years ≤ $\mathrm{MTTF_d}$ < 10 years
medium	10 years ≤ $\mathrm{MTTF_d}$ < 30 years
high	30 years ≤ $\mathrm{MTTF_d}$ < 100 years

3.3 DC value

Degree of diagnostic coverage = measurement of the effectiveness of the process diagnosis.
Calculating this value provides a ratio of the dangerous failures that are identified to the total number of dangerous failures:

$$DC = \frac{\sum \text{(identified dangerous errors)}}{\sum \text{(identified dangerous errors)}}$$

The total diagnostic coverage can be calculated as the sum of the values of individual elements (1 – n) of a control architecture.

$$DC = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dn}}}$$

Diagnostic coverage is particularly important in selecting the necessary control category.
This value is not relevant for categories B and 1.

Failure mode and effects analyses (FMEA) can be used in accordance with ISO 60812 to estimate the DC.

Appendix E of EN ISO 13849-1 offers a simplified approach for estimating the DC.

The DC is specified in one of four levels: none, low, medium, high

If the DC increases thanks to improved diagnostic measures, a higher PL can be achieved for the same control architecture.

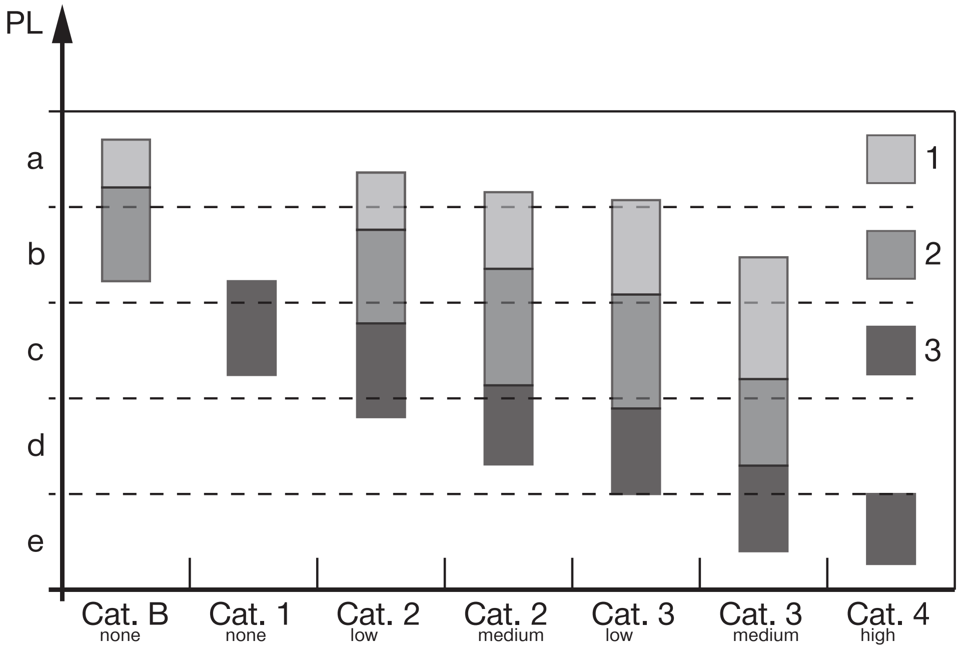
3.4 Degree of diagnostic coverage / safety architecture

The degree of diagnostic coverage (DC) indicates the probability with which the errors are transmitted by means of a test. The safety systems (test channels) can be single-channel, dual-channel or multi-channel.
While single-channel safety systems usually only react to errors with a failure, dual-channel or multi-channel safety systems check each other and identify potential errors.

The degree of diagnostic coverage is rated as being in one of the following categories: “small”, “low”, “medium” and “high”.
Individual degrees of diagnostic coverage can be read from Table E1 of EN ISO 13849.
The following is an excerpt from Table 6 of the degree of diagnostic coverage from EN ISO 13849.

Degree of diagnostic coverage (DC)	
Designation	**Area**
small	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Relationship between categories DC, $MTTF_d$ of each channel and the PL:



PL	Performance level
1	$MTTF_d$ of each channel = low
2	$MTTF_d$ of each channel = medium
3	$MTTF_d$ of each channel = high

The figure above depicts the various possible combinations for estimating the category with DC (horizontal axis) and $MTTF_d$ of each channel (bars). The bars in the diagram depict the three $MTTF_d$ ranges of each channel (low, medium, high) that can be selected to achieve the required PL.

4. Examples of control categories

The control examples shown here are not 100% transferable to the customer-specific requirement. They are merely an example depiction of how to achieve the required PL in accordance with EN ISO 13849-1. To implement the safety function, the use of “proven components,” as described in Chapter 6.2.4 of the EN ISO 13849-1, is sufficient.

⇨ If an activation valve for a product is monitored by a pressure switch in a single-channel control architecture, this can increase machine safety substantially.

⇨ This can be seen in the table in Chapter 4.5.4 of EN ISO 13849-1. Here, this is indicated by the increased PL d in Category 2.

⇨ Without the described monitoring measure (no DC), only PL b/c would be reachable in control category 1.

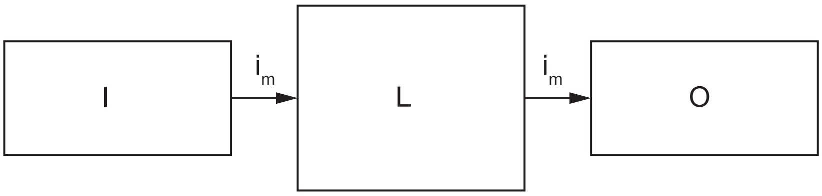
4.1 Control category B

In the safety systems of control category “B”, there is no DC (DC_{avg} = none) and the $MTTF_d$ of each channel can be “low” to “medium”. In such safety systems (usually single-channel systems), the consideration of failures due to common causes (CCF) is not relevant.
The maximum PL that can be achieved with Category “B” is “PL = b”.

⇨ THE OCCURRENCE OF AN ERROR CAN LEAD TO LOSS OF THE SAFETY FUNCTION.
⇨ Chapter 6.2.3 of EN ISO 13849-1

Special requirements for electromagnetic compatibility can be found in the corresponding product standards, for example IEC 61800-3 on power drive systems. The requirements for interference immunity are of particular importance for the functional safety of the SRP/CS.
If there is no product standard that is available, at the very least, the requirements of IEC 61000-6-2 regarding the interference immunity should be followed.

Intended architecture for Category B:



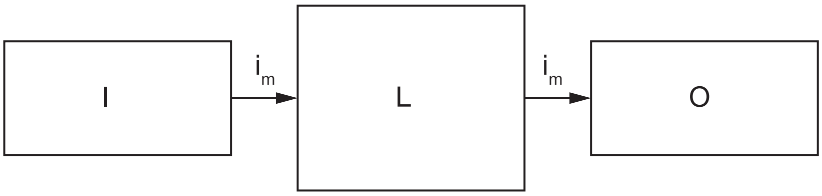
i_m	Connectors
I	Input unit, e.g. sensor
L	Logic
O	Output unit, e.g. main contactor

WARNING:

The occurrence of an error can lead to the loss of the safety function.

4.2 Control category 1

Intended architecture for Category B:



i_m	Connectors
I	Input unit, e.g. sensor
L	Logic
O	Output unit, e.g. main contactor

In safety systems of control category “1” there is no DC (DC_{avg} = none).

WARNING:

The occurrence of an error can lead to the loss of the safety function. However, the $MTTF_d$ in each channel of control category “1” is greater than in control category “B”.

As a result, the loss of the safety function is less likely.

4.3 Control category 2

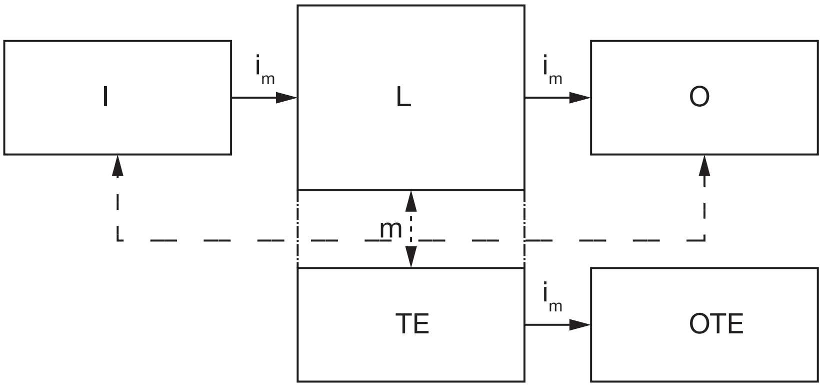
For control category “2”, the identical requirements must be fulfilled as the requirements for control category “B”. The following safety principles also apply to control category “2”:

- The SRP/CS of control category “2” must be designed in such a way that their function is tested at reasonable intervals by the machine or system controller.

⇨ The test must be carried out during machine or system startup and before a hazardous situation is initiated.

⇨ This test can be initiated automatically.

Intended architecture for Category 2:



i_m	Connectors
I	Input unit, e.g. sensor
L	Logic
O	Output unit, e.g. main contactor
m	Monitoring
TE	Testing device
OTE	TE output

4.4 Control category 3

For control category “3”, the identical requirements must be fulfilled as the requirements for control category “B”.
The following safety principles also apply to control category “3”:

- The SRP/CS of control category “3” must be designed in such a way that a single error does not result in loss of the safety function. Whenever this is reasonably feasible, a single error shall be detected upon or before the next safety function request.
- The degree of diagnostic coverage (DC_{avg}) of the entire SRP/CS, including the error detection, must be low. The $MTTF_d$ of each redundant channel must be low to high, depending on the PL_r. Measures against CCF must be taken (see EN ISO 13849-1, Appendix F).

INFORMATION:

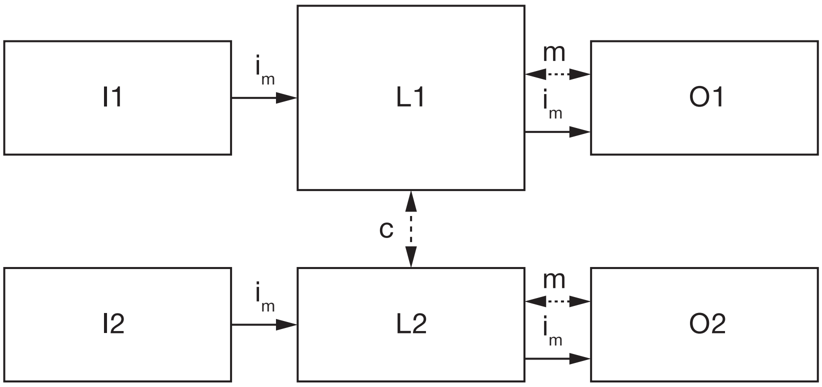
The requirement to detect individual errors does not mean that all errors are able to be detected. As a result, the accumulation of undiscovered errors can lead to an unintended output signal and a dangerous situation at the machine.

The system behavior of control category “3” permits the following:

- In the event of the occurrence of a single fault, the safety function is always carried out
- Some, but not all errors are detected
- The accumulation of unidentified errors can lead to the loss of the safety function

The technology that is utilized influences the possibilities for the implementation of error detection.

Intended architecture for Category 3:



i_m	Connectors
c	Cross comparison
I1, I2	Input unit, e.g. sensor
L1, L2	Logic
O1, O2	Output unit, e.g. main contactor
m	Monitoring

The dashed lines (m) indicate the reasonably feasible error detection!

4.5 Control category 4

For control category “4”, the identical requirements must be fulfilled as the requirements for control category “B”.
The following safety principles also apply to control category “4”:

- SRP/CS of control category “4” must be designed so that:
  - A single error in any of these safety-related parts does not lead to loss of the safety function.
  - The individual error is detected upon or before the next safety function request, e.g. immediately upon switch-on or at the end of the machine cycle.

WARNING:

If it is not possible to detect errors, then the accumulation of unidentified errors must not lead to the loss of the safety function.

- The degree of diagnostic coverage (DC_{avg}) of the entire SRP/CS, including the error detection, must be low. The $MTTF_d$ of each redundant channel must be low to high, depending on the PL_r. Measures against CCF must be taken (see EN ISO 13849-1, Appendix F).

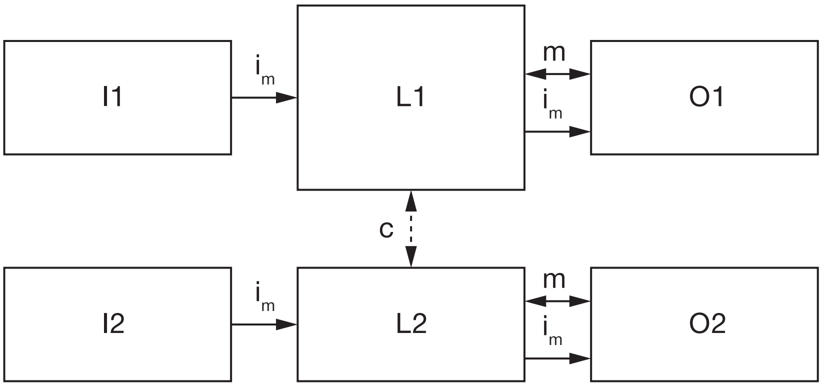
INFORMATION:

The system behavior of control category “4” permits the following:

- In the event of the occurrence of a single fault, the safety function is always carried out
- Detection of the errors in a timely manner to prevent the loss of the safety function
- The accumulation of unidentified errors can be considered

The difference between control categories “3” and “4” is the higher DC_{avg} in control category “4” and the required $MTTF_d$ of “high” only.

Intended architecture for Category 4:



i_m	Connectors
c	Cross comparison
I1, I2	Input unit, e.g. sensor
L1, L2	Logic
O1, O2	Output unit, e.g. main contactor
m	Monitoring

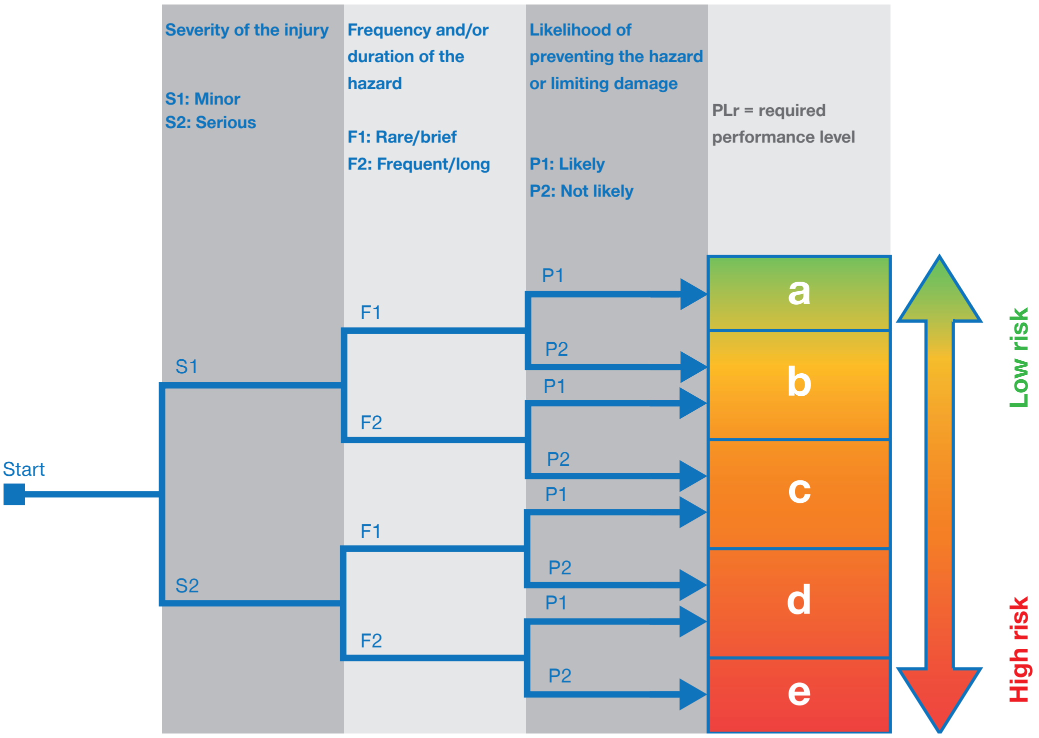
The solid lines (m) for monitoring represent a higher degree of diagnostic coverage than with the intended architecture of Category 3.

4.6 Summary of the requirements for categories

A summary of the individual requirements for the categories can be found in Table 10 of EN ISO 13849-1.

5. Required PLr - Achieved PL

5.1 Step 1

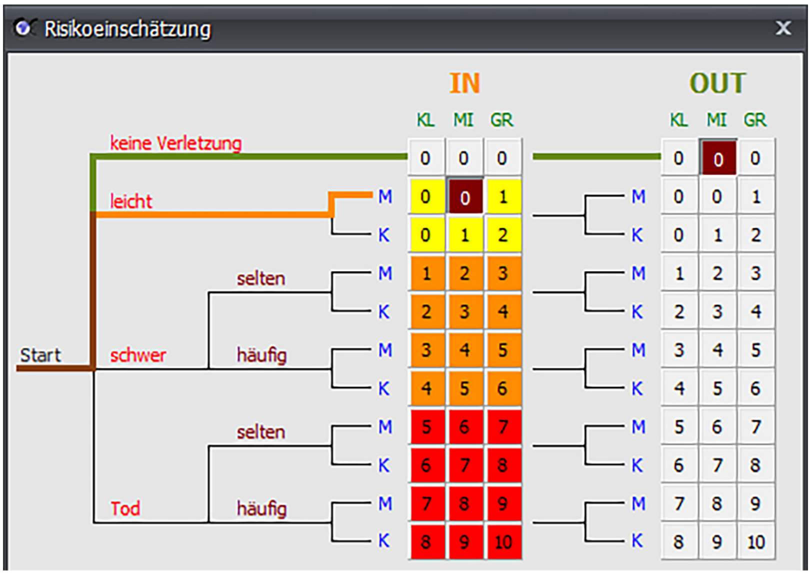


The EN ISO 13849-1 also uses a risk graph to determine the required safety level **PLr**. Parameters S, F and P are used to determine the severity of the risk.
This result of this process is the **required performance level (PLr)**.
In practice, the PLr is often defined in the customer's requirements specifications.

NOTICE:

When assessing the effectiveness of the actions taken to assess risk, we once again encounter the structure of risk graphs used to determine the PLr. A classification of the achieved risk reduction has replaced the column for the PLr. It is in the form of a number, which serves as an abstract symbol for the risk severity.

For this purpose, see the following figure “Risk estimation”.



			IN			OUT		
			KL	MI	GR	KL	MI	GR
Start	keine Verletzung		0	0	0	0	0	0
	leicht	M	0	0	1	0	0	1
		K	0	1	2	0	1	2
	schwer selten	M	1	2	3	1	2	3
		K	2	3	4	2	3	4
	schwer häufig	M	3	4	5	3	4	5
		K	4	5	6	4	5	6
	Tod selten	M	5	6	7	5	6	7
		K	6	7	8	6	7	8
	Tod häufig	M	7	8	9	7	8	9
		K	8	9	10	8	9	10

5.2 Step 2

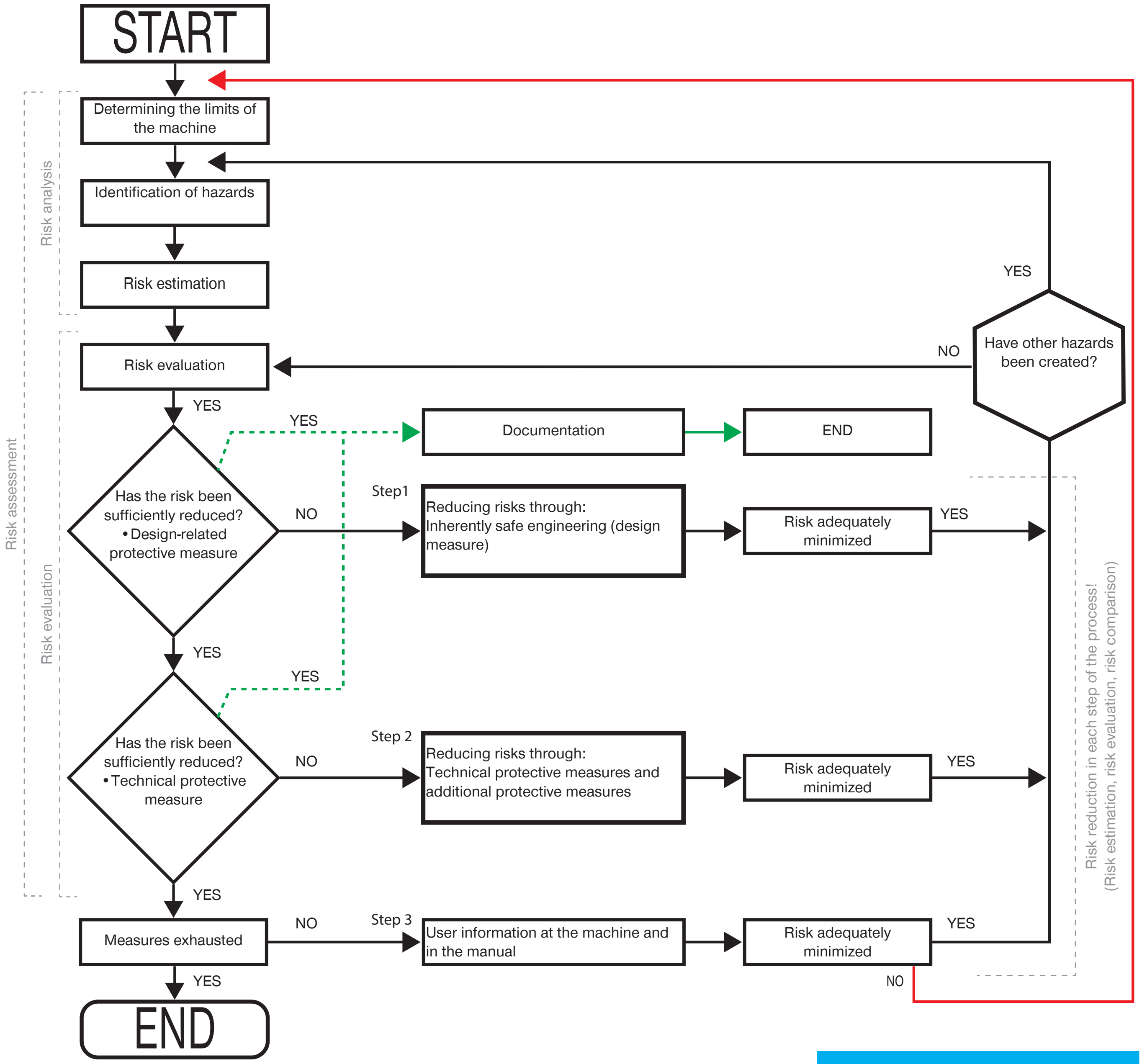
As part of the risk assessment, the achieved performance level must be determined for all risk-reducing actions that also contain **control engineering components**.

The SISTEMA program of the DGUV (German Social Accident Insurance) is available for this purpose.

INFORMATION:

In each case, the result of this determination must read as follows:

PL ≥ PLr (achieved Performance Level ≥ required Performance Level)


START
Determining the limits of the machine
Identification of hazards
Risk estimation
Risk evaluation
Risk analysis
Risk assessment
Risk evaluation
YES
YES
Documentation
END
Has the risk been sufficiently reduced?
• Design-related protective measure
NO
Step1
Reducing risks through: Inherently safe engineering (design measure)
Risk adequately minimized
YES
YES
YES
Has the risk been sufficiently reduced?
• Technical protective measure
NO
Step 2
Reducing risks through: Technical protective measures and additional protective measures
Risk adequately minimized
YES
YES
Measures exhausted
NO
Step 3
User information at the machine and in the manual
Risk adequately minimized
YES
NO
YES
END
Have other hazards been created?
YES
NO
Risk reduction in each step of the process!
(Risk estimation, risk evaluation, risk comparison)

SOURCE: EN ISO 12100

6. Risk assessment

It is the responsibility of each manufacturer to carry out a risk assessment for their product.
Risk assessment includes the process of risk evaluation in which appropriate measures for risk reduction must be implemented. Here, the focus is on technical protective measures that contribute to minimizing risks.

Limits of the machine:	Usage limits, space limits, time limits, etc.
Hazards:	Determining/defining
Risk estimation:	Intervention by personnel, operating states, unintentional behavior, foreseeable misuse

blank page