

## 2 The replacement of EN 954-1

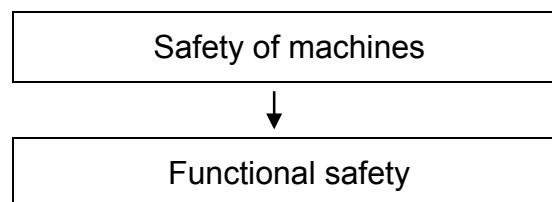
Previously, the machine constructing engineer had, according to the EN 954-1 (safety-related parts of control systems, part 1: General design principles) to proof the compliance of the general safety requirements according to the European machinery directive.

This standard demanded a risk analysis with the resulting safety categories (B, 1, 2, 3, 4). B stands for low and almost no safety respectively, 4 stands for high safety. The safety devices for a system were chosen with the safety category.

The EN 954-1 was replaced because programmable electronic systems were considered insufficiently and the time response (e.g. testing intervals, life cycles) and the failure probability of components were not considered. The following standards **EN 13849-1** (safety of machines – safety-related parts of control systems, part 1: General design principles) and **EN 62061** (safety of machines – functional safety of electrical, electronic and programmable electronic control systems) create remedy and consider the above approaches.

## 3 Definition of the safety requirements

It is divided into two parts: Safety of machines and the functional safety.

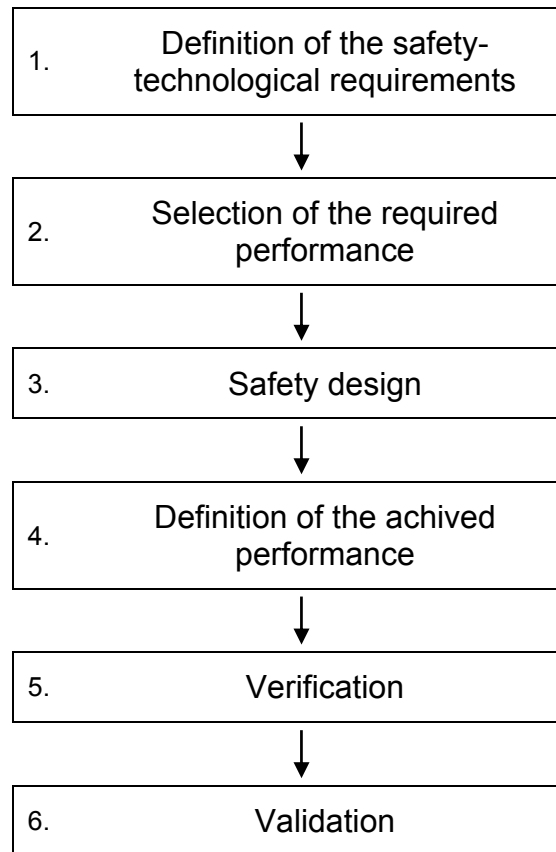


### 3.1 Safety of machines

After finished risk evaluation according to EN ISO 14121-1, measures for reducing of the detected risks will be defined. Afterwards, the risks will be reduced up to an acceptable residual risk.

### 3.2 Functional safety

The functional safety follows from the results of the machinery safety. The functional safety is divided into 6 steps:



### 3.2.1 Functional safety – the single steps:

#### 1. Definition of the safety-technological requirements

The required safety function characteristics are defined e.g. ESPD-function with automatic start, no simultaneity, etc. and a detailed description with the necessary interfaces to the other parts of control systems will be prepared.

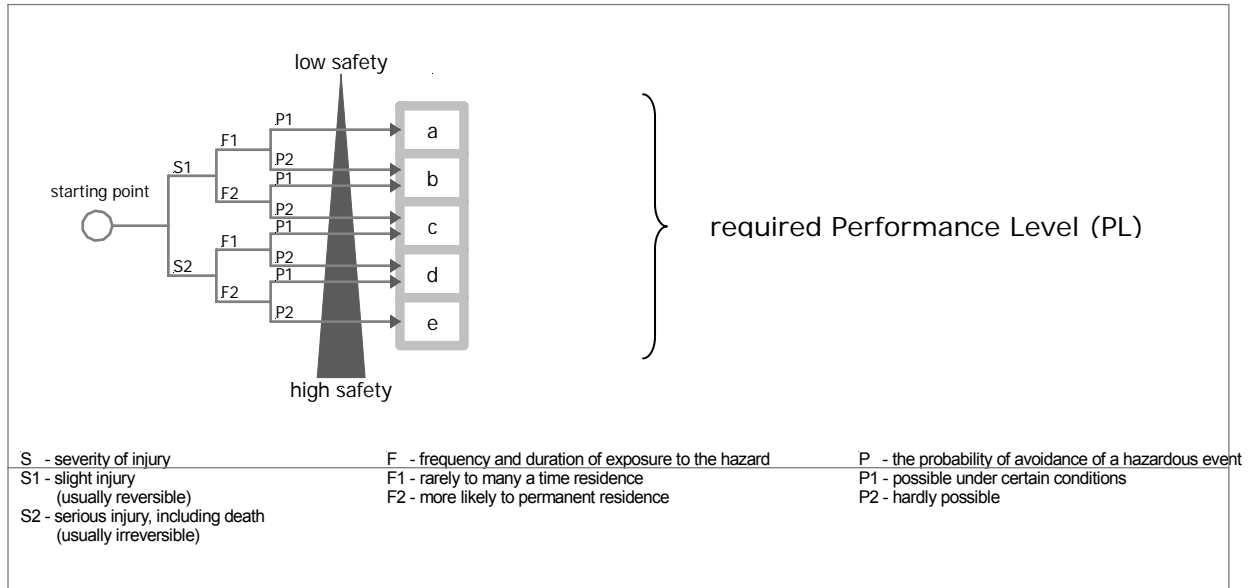
#### 2. Selection of the required performance

The definition is done with a risk graph. For new systems it can be generally done with two standards:

##### **EN 13849-1 (Safety of machines – safety-related parts of control systems, part 1: General design principles)**

With the risk graph it is possible to investigate all safety-related functions and areas of a machine respectively. The results are the so-called Performance Level / PL (**a-e**). The PL is needed for the selection of the safety setup and the corresponding components including wiring.

The **a** stands for low safety and the **e** for high safety.



### EN 62061 (Safety of machines - functional safety of safety-related electrical, electronic and programmable electronic control systems)

With the risk graph it is possible to investigate all safety-relevant functions and areas of a machine respectively. The results are the so-called Safety Integrity Level / SIL (1 - 3). The SIL is required for the selection of the safety setup and the corresponding components including wiring. The 1 stands for low safety and the 3 for high safety.

Effect and severity	S	Frequency and duration	F	Probability	P	Avoidance	A	Class K (=F+P+A)				
								3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	≤ 1 h	5	very high	5			SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, losing a finger	3	> 1 h - ≤ 1day	5	likely	4				OM	SIL1	SIL2	SIL3
Reversible, requiring attention from a medical practioner	2	> 1 day - ≤ 2 weeks	4	possible	3	impossible	5			OM	SIL1	SIL2
Requiring first help	1	> 2 weeks - ≤ 1 year	3	rarely	2	possible	3				OM	SIL1
		> 1 year	2	negligible	1	likely	1					

OM = other measures advised

### 3. Safety design

The safety function described in step 1 is designed. The single components are defined, e.g. safety relays SAFE CL for the ESPD-function.

### 4. Definition of the achieved performance

The actual performance of the safety function is detected. The safety function is divided in sensors, logic and actuators. The parameters required to calculation are provided by the component manufactures.

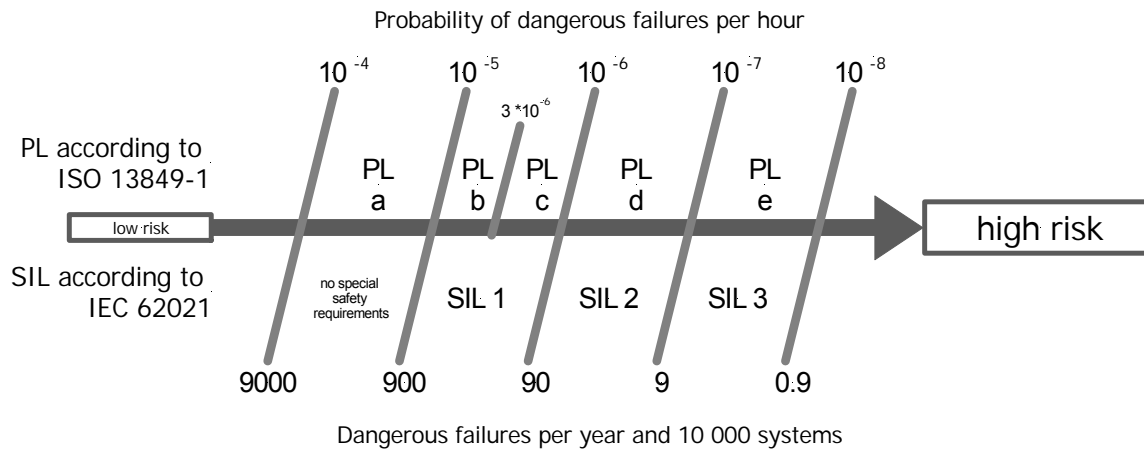
### 5. Verification

For each single safety function, the in step 4 achieved performance has to be bigger or equal as the in step 2 defined required performance. If this is not the case the safety function has to be improved.

### 6. Validation

For the safety function, the validation ensures that all safety-relevant parts achieve the requirements.

### 3.2.2 Relationship between PL and SIL:



### 3.2.3 Relationship between the categories, DC, MTTF<sub>d</sub> and PL:

