Low voltage switchgear and controlgear – functional safety aspects

Guidance how to use low voltage switchgear and controlgear in functional safety applications

Picture Siemens AG

CAPIEL

european coordinating committee of manufacturers of electrical switchgear and controlgear

Philippe Sauer
CAPIEL President

Karlheinz Kaul
CAPIEL Vice-President

A message from the CAPIEL Presidents

In the recent years machinery has become more and more complex. Based on the European Machinery Directive the requirements for safety have also increased. Therefore the European Union is very influential with regard to functional safety in machine systems.

This has a major effect on CAPIEL products as well. Some CAPIEL products may not meet the definition for a "safety component", but nevertheless they can have features or functions which allows a machine builder to use them as a part of a system intended for safety applications.

It is one of our most important duties, as CAPIEL, to work with regulators in order to ensure that features or functions are consistent with our common safety objectives. It is our responsibility to make sure that these are clearly defined, understandable and correctly interpreted by designers, installers and other users of electrical products, systems and solutions.

This brochure provides information concerning the application of current standards and the European Machinery Directive relevant to the implementation of low voltage switchgear and controlgear in functional safety applications.

We hope that you will find it of interest.

Yours sincerely

Philippe Sauer & **Karlheinz Kaul**

CAPIEL is the European Coordinating Committee of Manufacturers of Electrical Switchgear and Controlgear

CAPIEL notably provides various **start, control & safety solutions for machines.**

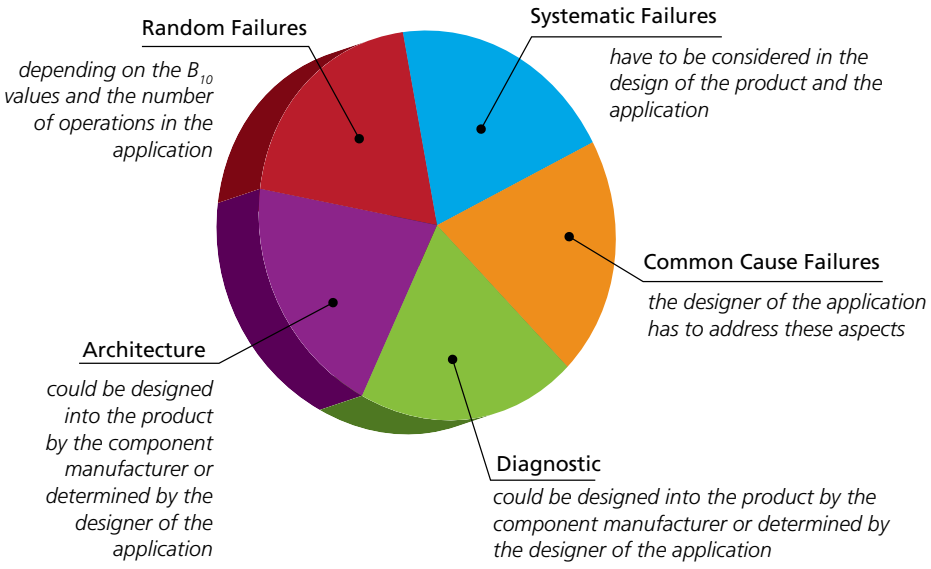
CAPIEL plays an active role in driving emerging technologies, especially regarding innovations in the areas of environmental preservation and sustainability, but also in health and safety.

Safety Factors

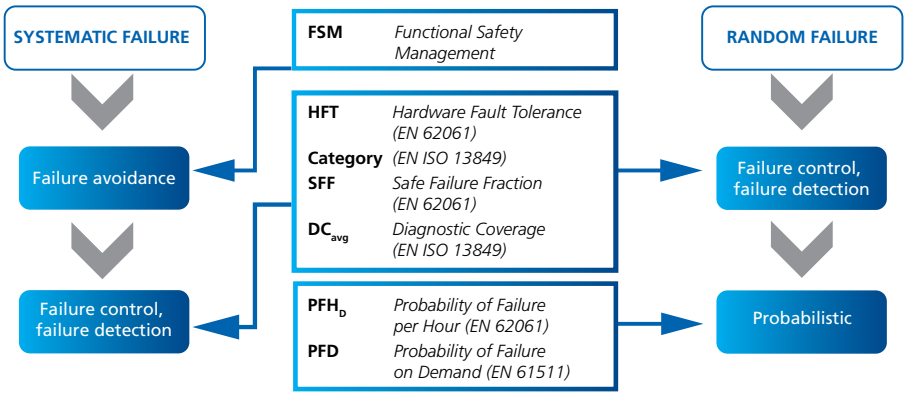
- The Machinery Directive 2006/42/EC has applied since 2009.
  Machine manufacturers have to consider how they can demonstrate compliance with the Machinery Directive (2006/42/EC), concerning safety in control systems, preferably using the following harmonized EN Standards:
  - EN ISO 13849
  - EN 62061 (identical to IEC 62061)
- To ensure these EN Standards can be applied effectively, CAPIEL manufacturers provide functional safety related data to machine manufacturers in order to help them design suitable safety related control systems. The type of data supplied depends on the type of product and its use. (See page 11)
- The format of the data provided in this document is relevant for use in the simplified calculation methods given in EN ISO 13849 and EN 62061.
- Functional safety is also important for process industry, explosive atmospheres, railway application and others. There is a range of applicable Directives and standards, e.g.:
  - ATEX Directive 94/9/EC (will be replaced by 2014/34/EU): EN 50495
  - Process industry: EN 61511
  - Railway application: EN 50155

Factors for Functional safety for electromechanical products

- To make a machine safe it is necessary to consider a number of factors:



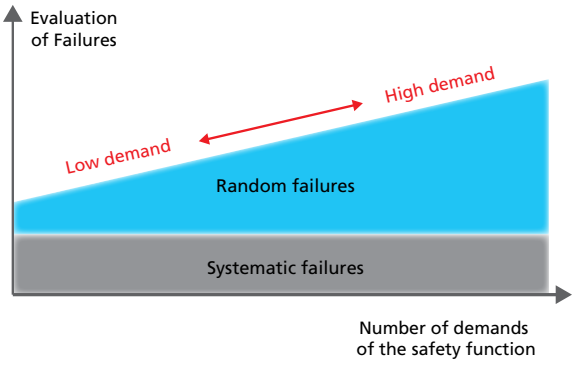
Why is it necessary to differentiate between types of failures?



- The difference between systematic failures and random failures is the way they are caused.
- Systematic failures are caused mainly by the design of a system. These failures are present in the products or systems from the beginning of their life (e.g.wrong requirements or specification, wrong dimensioning, software fault).
- Random failures are difficult to predict because there is virtually no way to identify the fault before the failure happens. This is why statistical methods are used.

What is the difference between “low demand” and “high demand”?

- The most important objective for low demand with wear based applications is to reduce the systematic failures. The types of measure employed to reduce the systematic failures are the same for both high demand and low demand applications, for example “failure avoidance”, “quality management”, use of “proven principles” or “prior use”.



Mode of operation

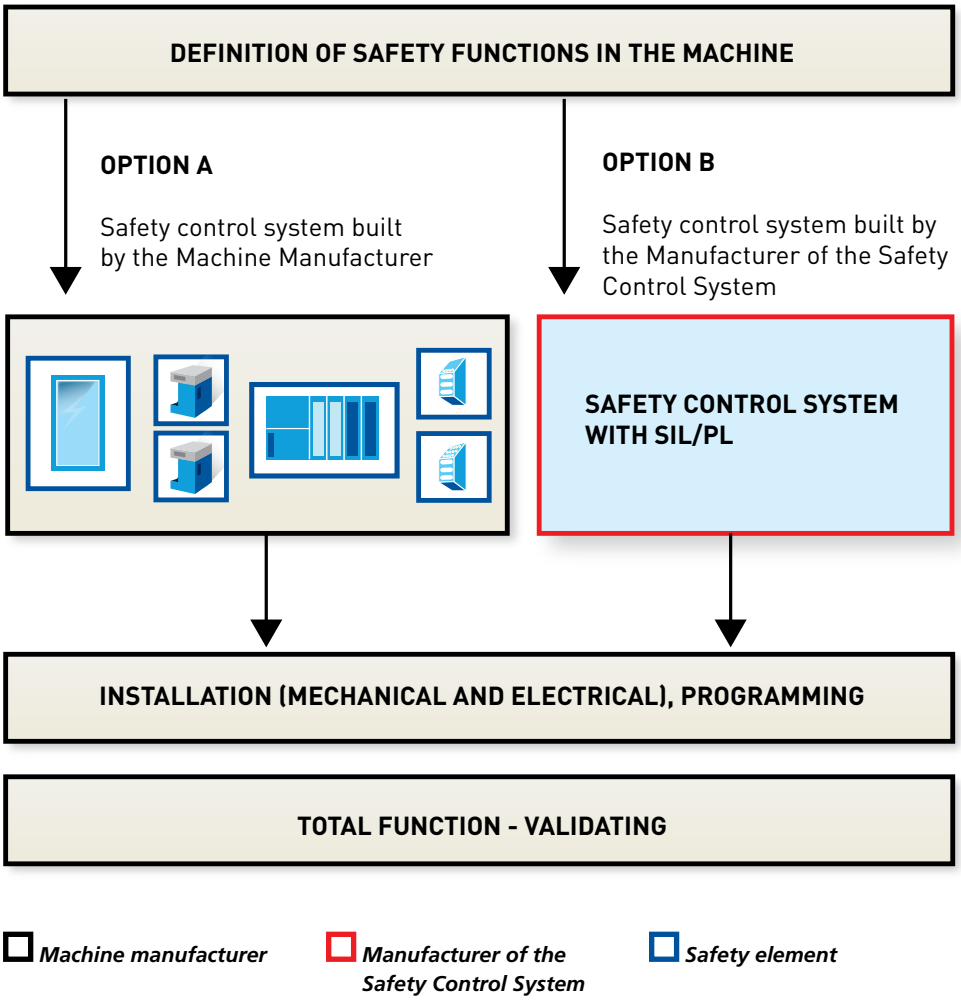
Demand:
- *safety function is performed in order to transfer the equipment into a specified safe state*

Low demand mode
- *frequency of demands ≤ 1 / year*
- *loss of safety function does not neccessarily lead to a hazardous situation at the same time*

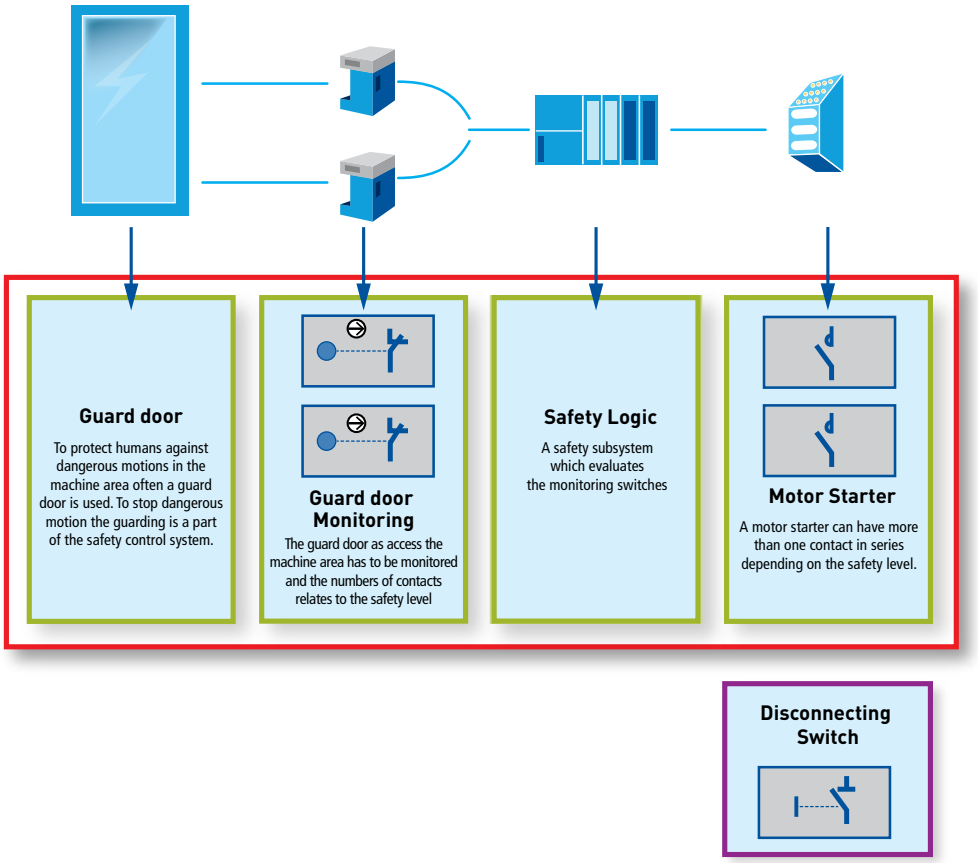
High demand mode
- *frequency of demands > 1 / year*
- *loss of safety function leads to a hazardous situation*

Responsibilities

- The machine manufacturer is responsible for the overall development and safety of the machine.
- This is fundamental irrespective of whether Option A or B is chosen in the chart below.
- During the selection of the products to be used, the machine manufacturer chooses either to use safety elements to design the safety sub-systems or to use pre-designed sub-systems.



Safety Product Implementation Levels



Safety Control System

Example: *Protection cover with monitoring and actuating function (no single CAPIEL product)*

Safety subsystem

Example: subfunction to stop dangerous motion of a conveyor realized by a motor starter with integrated safety features.

Other examples: Safety relay

Safety element

Example: *contactor (with B_{10d})*

Other examples: relay with positively driven contacts, emergency stop device, interlocking device.

Generic element

Example: *Disconnecting switch*

Other examples: contactor (without B_{10d}), relay, push button, terminal block, standard-PLC, proximity switches, disconnector, indicating towers. All examples without safety function.

What safety product related values are needed – overview

For each implementation level, different data is required in order for the machine manufacturer to verify of the required PL/SIL of the safety functions. The following table shows the data required.

Information to be provided by product manufacturer	Implementation levels							
	Safety control system		Safety subsystem		Safety Element		Generic element	
	TB	WB	TB	WB	TB	WB	TB	WB
SIL and/or PL	■	■						
SILCL and/or PL			■	■				
PFH_D and/or PFD	■	■	■	■				
Operation limit		■		■		■		■
$MTTF_d$ or MTTF and RDF					■			
B_{10d} or B_{10} and RDF						■		
MTBF							■	
B_{10}								■
T_M	■	■	■	■	■	■	■	■

■ ***Mandatory field, data required,***

■ ***Optional field, data optional (application-specific),***

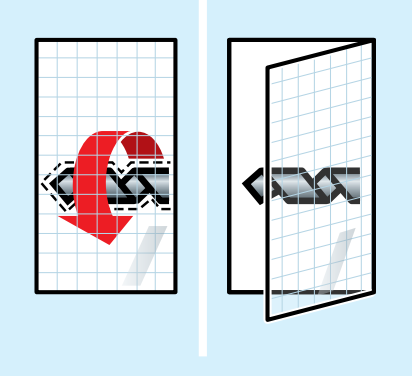
TB ***Time based, e.g. electronic products***

WB ***Wear based, e.g. electro-mechanical products***

PL *Performance Level (EN ISO 13849)*
SIL *Safety Integrity Level (EN 61508)*
SILCL *Safety Integrity Level Claim Limit (EN 62061)*
PFH_D *Probability Failure per Hour (EN 62061)*
T_M *Mission time (EN ISO 13849)*
MTBF *Mean Time Between Failure (EN ISO 13849)*

$MTTF_d$ *Mean Time To Dangerous Failure (EN ISO 13849)*
RDF *Ratio of Dangerous Failures*
B_{10} *10% of the devices failed (EN ISO 13849)*
B_{10d} *10% of the devices failed dangerous (EN ISO 13849)*
PFD *Probability of failure on Demand (EN 61511)*
Operation limit *maximum number of operations that is used in the calculation on the PFH_D*

Case Study: High Demand Application



Picture Eaton Industries GmbH

A movable protective guard is monitored by means of a door monitoring switch (may be two depending on required PL/SIL) with a separate actuator.

Conditions in this example:

- This guard is opened four times per hour, (C=4).
- Architecture is a two channel
- B_{10} = 1 000 000
- RDF = 20%
- CCF, β = 10% (Common Cause Factor EN 62061)
- T_1 = 20 year (Proof Test Interval EN 62061) ≈ 200 000 hours
- DC = 0

Calculation of the SIL Claim for the safety subsystem 1:

Ratio of Dangerous Failure (RDF) and the B_{10} are given by the product standard or the manufacturer, e.g. 20% and 1 000 000*. The B_{10d} value used in EN ISO 13849 can be determined as follows:

$$B_{10d} = \frac{B_{10}}{RDF} = \frac{1\,000\,000}{0.2} = 5\,000\,000$$

The total failure rate λ_D according EN/IEC 62061 of the position switch is as follows:

$$\lambda_D = \frac{0.1 \times C}{B_{10d}} = \frac{0.1 \times 4}{5\,000\,000} = 8 \times 10^{-8}$$

In this example the function of the sensors is not monitored, therefore λ_{DD}=0. Also λ_S =0, this is because "not closing faults" are not part of the safety function and are therefore not relevant for the SFF calculation. ➡ $SFF = (\lambda_{DD} + \lambda_S)/(\lambda_D + \lambda_S) = (0+0)/(8 \times 10^{-8} + 0) = 0$

For calculation of SFF only failures relevant for the safety function should be used.
The no effect failure is not used for SFF calculations**.

$PFH_D \approx 2 * \lambda_D^2 * T_1/2 + \beta * \lambda_D$

$PFH_D \approx 2 * (8 \times 10^{-8})^2 * 200\,000/2 + 0{,}1 * 8 \times 10^{-8} = 8 \times 10^{-9}$ [1/h]

*See also "CAPIEL WHITE PAPER, Low voltage controlgear products and functional safety", www.capiel.eu.
**See also EN 61508-4 2nd Ed subclause 3.6.14/15

With the 3 factors given from the application

two channel = HFT = 1

SFF = 0

PFH_D =8 x 10^{-9}

Maximum allowable safety integrity level for a safety function carried out by a safety-related element or subsystem:

Hardware Fault Tolerance (HFT)			Safe Failure Fraction of an element (SFF)
HFT 0	**HFT 1**	HFT 2	
Not allowed	SIL 1	SIL 2	**< 60%**
SIL 1	SIL 2	SIL 3	60% – < 90%
SIL 2	SIL 3	SIL 3	90% – < 99%
SIL 3	SIL 3	SIL 3	≥ 99%

(Reference: EN 62061)

Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation:

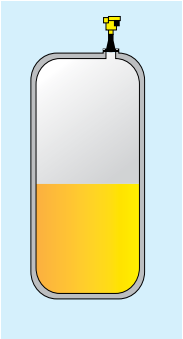
Average frequency of dangerous failure of the safety function (PFH_D)	Safety Integrity Level (SIL)
$10^{-6} \leq PFH_D < 10^{-5}$	SIL 1
$10^{-7} \leq PFH_D < 10^{-6}$	SIL 2
$10^{-8} \leq PFH_D < 10^{-7}$	SIL 3

(Reference: EN 62061)

The result for the safety subsystem 1 = SILCL 1

In this example the PFH value is good enough for SIL 3, but the SIL is limited by SFF and HFT to SIL 1.

Case Study: Low Demand Application



Picture Vega Grieshaber KG

Level switch in a process application signals when the tank is full.

Three possibilities of evaluation according to IEC 61511:

- calculation according to IEC 61508
- prior use (field experience)
- fault exclusion

Operating in low demand mode:

- Main failures are systematic, random failures are not determined by the wearing of the products but based on other causes
- B_{10} value not applicable for PFD calculation
- Failure rate is determined by field data

For low demand applications in the process industry the reliability data is taken from relevant databases or from the safety manual of the manufacturer.

Manufacturer value: $\lambda_D = 20\ FIT = 20 \times 10^{-9} = 2 \times 10^{-8}$ failure/h

User Value: T_1=1 year (8760 hours)

PFD $= \lambda_D * T_1/2$

With the 3 factors , given from the application

single channel = HFT = 0

SFF = 0

PFD = 8.76 x10^{-5}

Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem:

Hardware Fault Tolerance (HFT)			Safe Failure Fraction of an element (SFF)
HFT 0	HFT 1	HFT 2	
SIL 1	SIL 2	SIL 3	SFF < 60%
SIL 2	SIL 3	SIL 4	60% ≤ SFF ≤ 90%
SIL 3	SIL 4	SIL 4	90% ≤ SFF ≤ 99%
SIL 3	SIL 4	SIL 4	SFF ≥ 99%

(Reference: IEC 61508-2)

Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation:

Average probability of a dangerous failure on demand of the safety function (PFD_{avg})	Safety Integrity Level (SIL)
$10^{-2} \le PFD_{avg} < 10^{-1}$	SIL 1
$10^{-3} \le PFD_{avg} < 10^{-2}$	SIL 2
$10^{-4} \le PFD_{avg} < 10^{-3}$	SIL 3
$10^{-5} \le PFD_{avg} < 10^{-4}$	SIL 4

(Reference: IEC 61508-1)

The result for the safety subsystem 1 = SIL 1

In this example the PFD value is good enough for SIL 4, but the SIL is limited by SFF and HFT to SIL 1.

Conclusions

- The machine manufacturer is responsible for the overall development and safety of the machine.
- When designing a machine, the manufacturer can:
  - Select an appropriate safety control system for his application. The safety control system supplier will provide relevant functional safety data.
  - Select and combine suitable safety subsystems in order to create a safety control system that provides the required level for a safety function.
  - Design a subsystem using safety elements and combine it with other subsystems to create a safety control system that provides the required level for a safety function.
- If a generic element is used in a safety related application, the machine manufacturer has to justify its usage as a safety element. This includes deriving all functional safety values and ensuring its suitability for the intended function.

  The table on page 7 shows which safety related values will be provided by the component manufacturer.
- Probabilistic determination methods are not always suitable when evaluating reliability. Therefore a systematic analysis of all possible sources of failure of the system and its components shall always be carried out before designing the system.
- The calculation is just one of a range of verification measures that are required to show that a sufficient safety level has been achieved.
- Probabilistic values for random failures in low demand mode are provided by the manufacturer or taken from relevant databases or field data.
- Some examples of common databases:
  - Exida Electrical & Mechanical Component Reliability Handbook
  - MIL HDBK 217F
  - NAMUR NE 93
  - RAC FMD 91
  - SN29500
  - SN31920
  - VDE 2180
  - IEC/TR 62380
  - IEC 61709
  - White paper CAPIEL PG5

References

EN 61508	Functional safety of electrical/ electronic/programmable electronic safety-related systems
EN 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN 61511	Functional safety – Safety instrumented systems for the process industry sector
EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems Part 1: General principles for design
EN ISO 13849-2	Safety of machinery – Safety-related parts of control systems Part 2: Validation
EN 60947-series	Low-voltage switchgear and controlgear
EN 61649	Weibull analysis
VDMA 66413	VDMA-Specification
EN 50495	Safety devices required for the safe functioning of equipment with respect to explosion risks
EN 50155	Railway applications – Electronic equipment used on rolling stock

CAPIEL at a glance

CAPIEL represents **9 national associations** from 8 European countries comprising **more than 550 manufacturers**.

Members of national associations represented by CAPIEL include small, medium and large-sized companies **employing 120,000 people** directly in Europe and have a combined turnover of **€18.25 billion**.

CAPIEL membership includes **global players** such as Siemens, Schneider Electric, ABB, Eaton, Rockwell Automation, etc.

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

www.capiel.eu