issa

Promoting and Developing
Social Security Worldwide.

Safety-related parts of control systems ISO 13849-1

Bangalore, India
Pune, India

Klaus-Dieter Becker
BGETEM

www.issa.int

Overview

EN ISO 13849 part 1:

- Scope
- Motivation for the revision of ENISO 13849-1
- overview over the new concept
- *Performance Level*
- *introduction of the designated architectures“*
- *requirements for the safety related software*
- Use of the standard
- *Combination SRP/C*
- ***New requirements (revision)***

Changing

ISO 13849-1:23

content:

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

Requirements of control systems
(new regulation machinery, Annex III)

1.2.1 Safety and reliability of control system

Control systems shall be designed and constructed in such a way that:

- **they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation;**
- **a fault in the hardware or the logic of the control system shall not lead to hazardous situations;**
- **errors in the control system logic shall not lead to hazardous situations;**

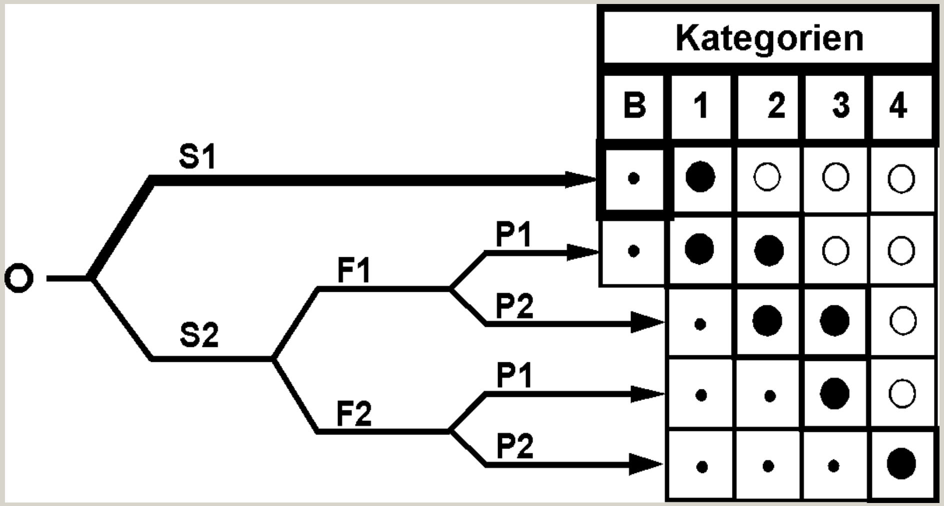
Requirements of EN 60204-1 clause 9.4.1

Where failures or disturbances in the electrical equipment can cause a hazardous condition or damage to the machine or to the work in progress, appropriate measures shall be taken to minimize the probability of the occurrence of such failures or disturbances

The required measures and the extent to which they are implemented, either individually or in combination, depend on the level of risk associated with the respective application (see 4.1).

criticism to the previously valid EN 954-1

- EN 954-1 has no requirements for complex electronics and programmable electronic systems
- no causal relationship between categories and risk reduction
- no requirements for the reliability for the components



Risk reduction =
Category ???

Situation of the standards

Machinery directive →

construction and risk assessment

EN ISO 14121
EN ISO 12100

Functional safety for machinery control systems

Design and realisation of safety control systems of machinery

EN 62061/IEC 62061

EN ISO 13849-1/2

Elektric
Hydraulic
Pneumatic
Mechanic

IEC 61508

EN 60204/IEC 204

Balance between deterministic and probabilistic

EN ISO 13849-1:2023

DIN EN 954-1:1997	**DIN EN IEC 61508:2010**
deterministic	**Probabilistic**
Well proven methods	**New approach**

- Safety functions
- Risk graph
- Categories

- Quantification: reliability and diagnostic
- Commen cause failture
- Software requirements

Scope

:

- Safety related parts of control systems of all kind of machines independent of the technology and the energy
    - elektric,
    - hydraulic,
    - pneumatic,
    - mechanic.

supply safety requirements and an guideline for the design of

- Safety related parts of control systems and
- Software

Risk reduction from the safety function carry out by SRP/CS:

- The strategy for the risk reduction at the machine is given in ISO 12100, clause 6
- For **each selected safety function** to be carry out by a SRP/CS, a **required performance level (PLr)** shall be determined and documented.
- The **contribution does not cover** the overall risk of machinery under control
- By the ENISO 13849-1 can the amount of risk reduction by design and safeguarding techniques which are realized by **control systems**, be **assessed**

goal:

In order that the safety function can be performed by the control system, the following has to be considered

- Determination of required characteristics of the safety related part of control systems (SRP/CS) and
- Perform an „Assessment plan " (Performance Level = PL) for the control systems
- As the result of the assessment plane (Performance Level = PL) it is possible to compare the quality of the control systems, including the software

- PL illustrates the performance of the control systems.

- Category: Graduation of the safety of control systems in terms of resistance against faults
- CCF: Common Cause Failure
- PES: Programable electronic systems
- PLr: performance level (PL) in order to achieve the required risk reduction for each safety function
- PL: Discrete level used to specify the ability of safety related parts of control systems to perform a safety function under foreseeable conditions
- $MTTF_D$: mean time to dangerous failure
- DC: measure of the effectiveness of diagnostic
- B_{10D}: number of cycles until 10% of the componets fail dangeroursly (for pneumatic and electromechanical components)
- SRP/CS: safety part of control systems

The key to success: Performance Level PL

PL: discrete level to specify the ability of safety–related parts of control systems to perform a safety function under foreseeable conditions

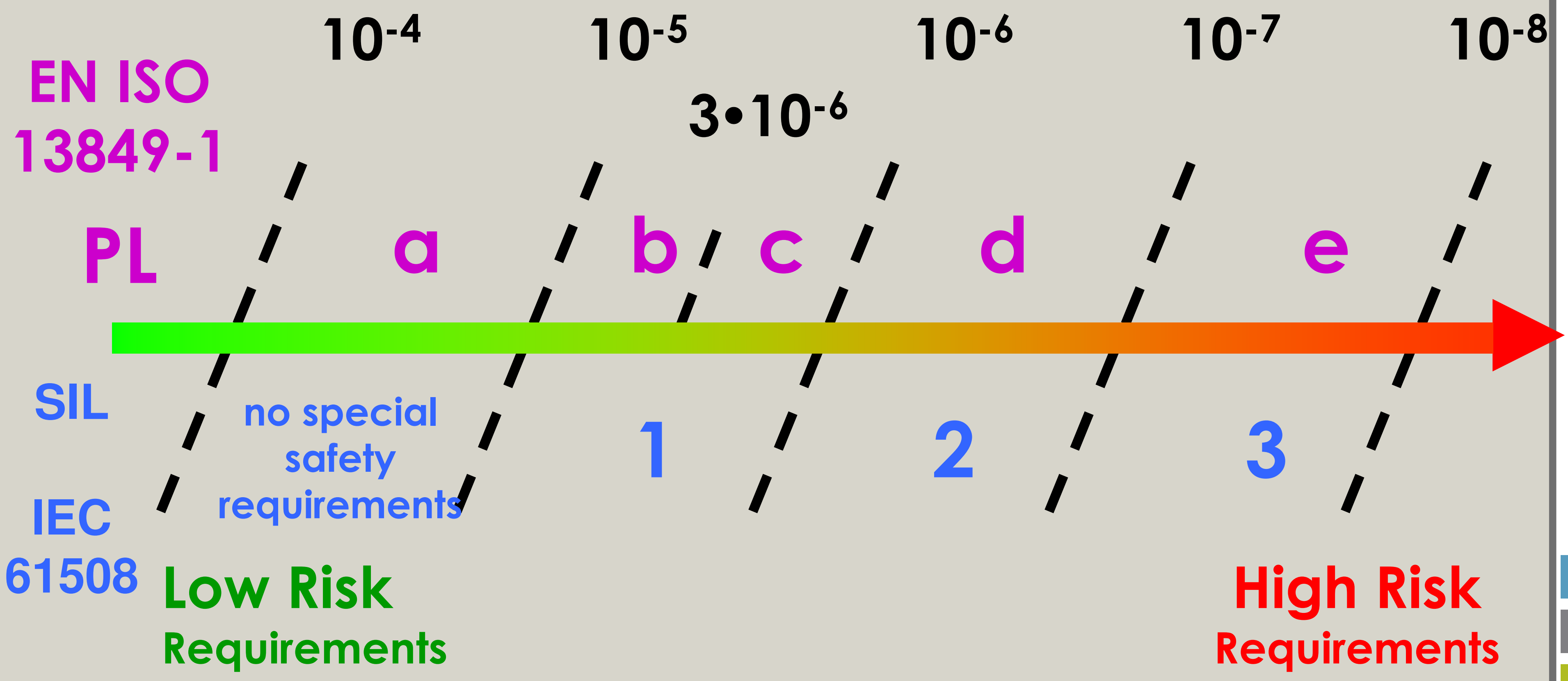
PL is determined:

- Category (Architecture)
- $MTTF_D$ - Mean Time to Dangerous Failure
- DC – Diagnostic coverage (Tests)
- CCF – common cause failure
- Measures against systematic failure
- Software

failures of different items, resulting from a single event, where these failures are not consequences of each other

Definition of PL and Relation to SIL

Probability of a Dangerous Failure per Hour



Performance Level (PL)	Max. toleranced failure degree:
a	1 dangerours failure per 10.000 h
b	1 dangerours failure per 30.000 h
c	1 dangerours failure per 100.000 h
d	1 dangerours failure per 1.000.000 h
e	1 dangerours failure per 10.000.000 h

Priority levels of safety objectives

1

Avoiding risks

Direct safety technology

2

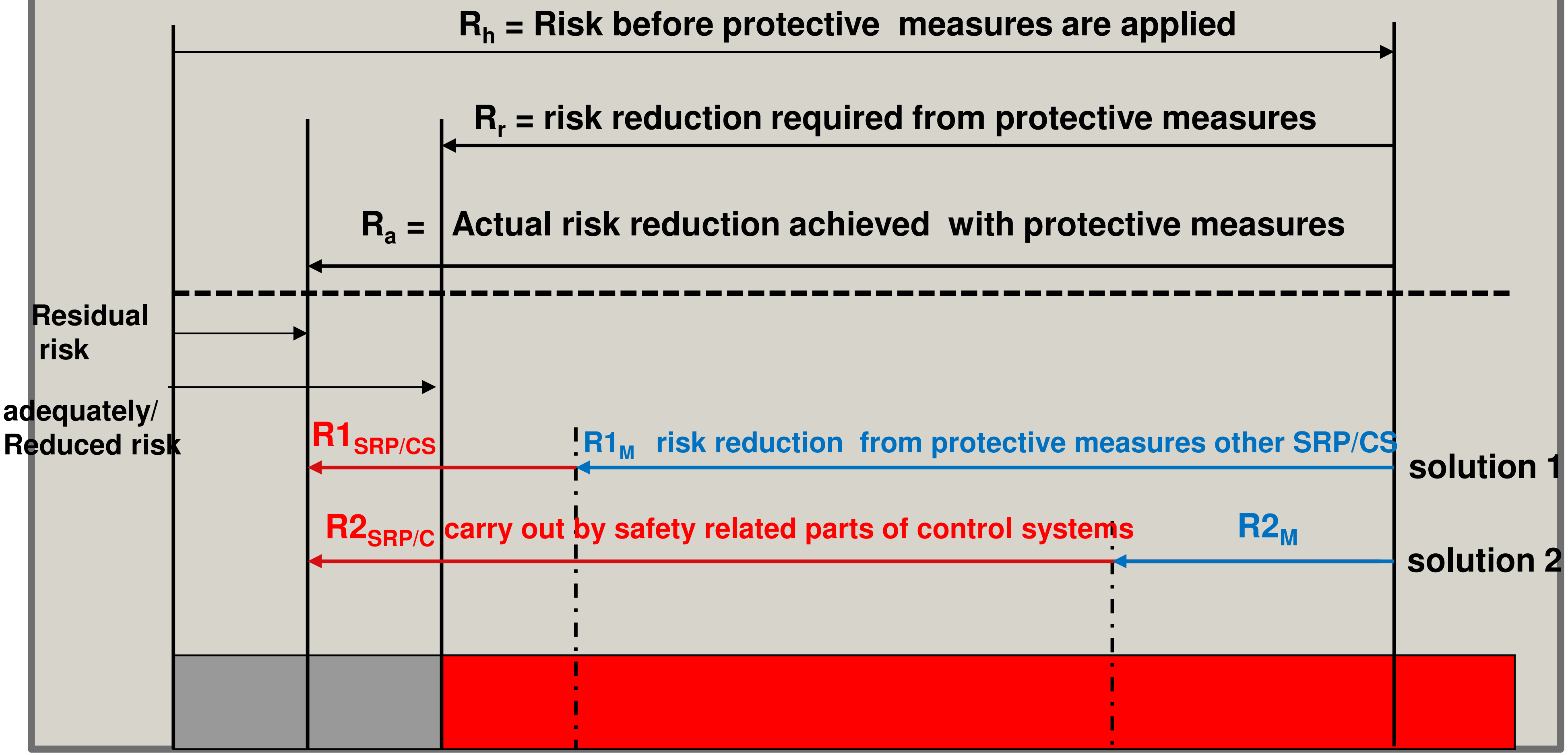
Safeguarding risks

Indirect safety technology

3

Warning of danger points

Risk assessment ⇒ Risk reduction



Requirements according to EN 12100, EN 1050, EN ISO13849

Identifikation of all hazards

↓

i.e.
assignment to safety function

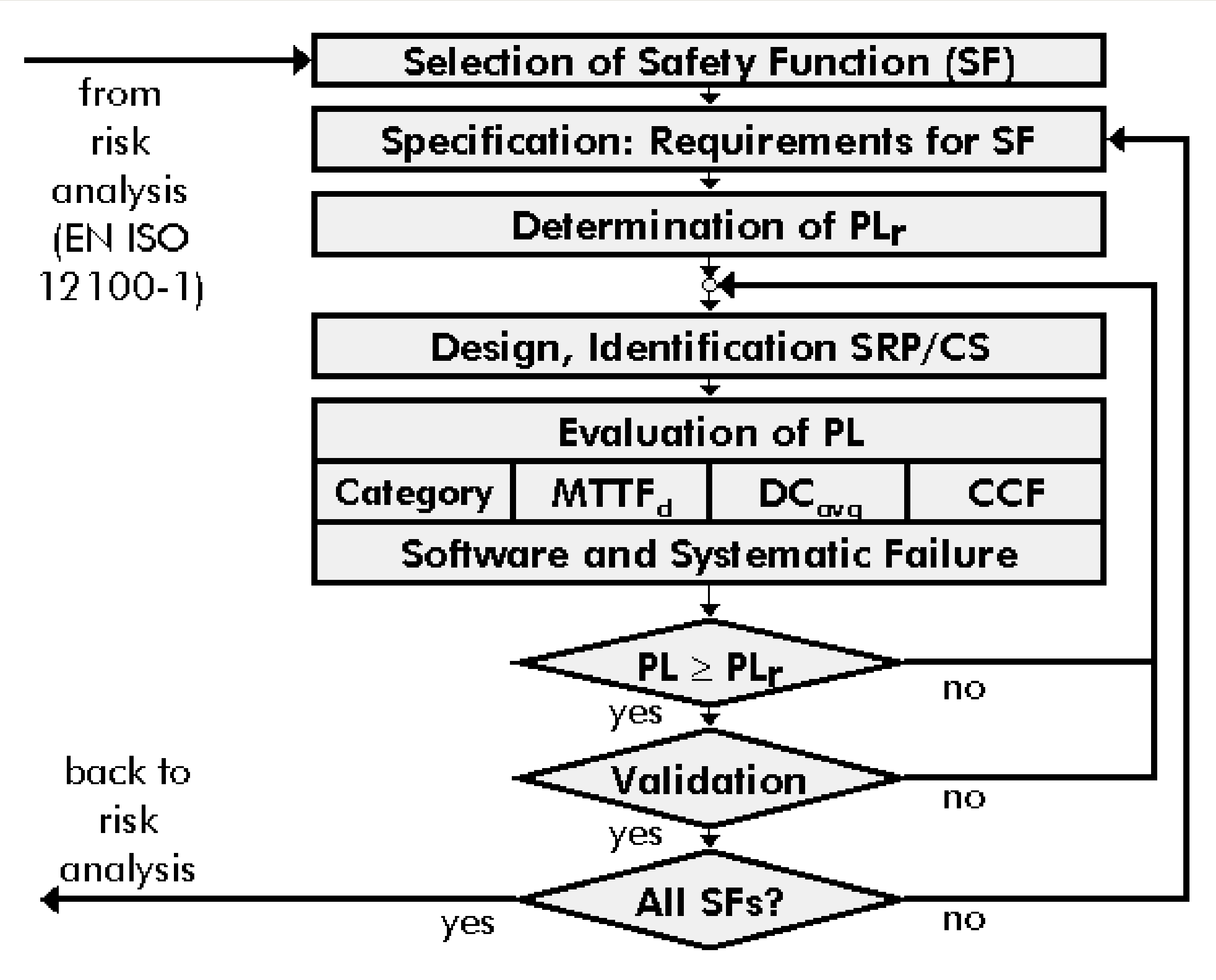
↓

For each safety function :
Determination of the required
Performance level

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

Functional Safety needs Safety Functions



1. Safety requirements specification

term	name of the safety function
Triggering event	the initiation event that triggers the safety function
Safety reaction	What is the safety related reaction
Operation mode	the mode(s) of operation during which the safety function is to be active
PLr	the required performance level PL_r for each safety function
frequency	How often is the safety related function requested
Stopping time	the response time for the machine to achieve a safe state after the demand is made upon the safety function e.g., the overall system stopping performance (reaction time plus stopping time) according to ISO 13855
Behaviour by loss of the power	the behaviour of the machine on the loss of power

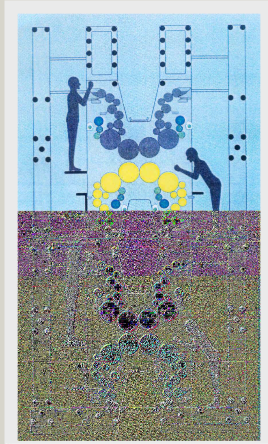
1. Safety requirements specification

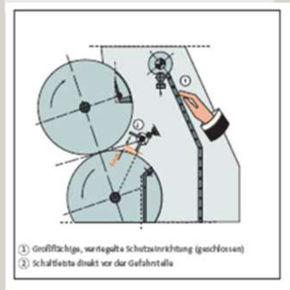
term	Name of the safety function
priority	Is the safety function prior or subordinate to other safety functions?
Addional safety function	Does the use of the safety function require further active safety functions?
Addional parameters	What kind of parameters have to be taken to account?
fault-detecting measures	Which diagnostic measures must be taken into account?
reaction reaction activities	What measures are required for fault detection?

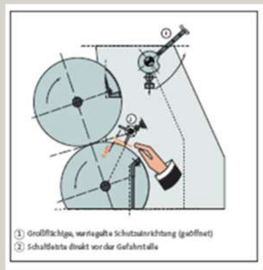
1. Specification of each safety function

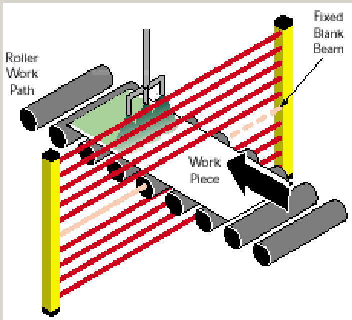
Determination of the safety function

- emergency stop circuits
- electric interlocking circuits
- prevention of unexpected start up
- muting
- limitation of speed and travel under hold-to-run control
- throttle valve control on continuous flow driers
- safe stops









Review of the safety requirement specification

The safety requirements specification shall be verified before starting the design, since every other activity is based on these requirements. The check shall assure that all safety functions are specified to achieve the intended risk reduction at the machine.

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

2. Determination of the („r“ = required) Performance Level PL_r for each safety function:

- taking to account exsisting **european standards** (e.g. EN ISO 12643)

  or
- using **risk graf**

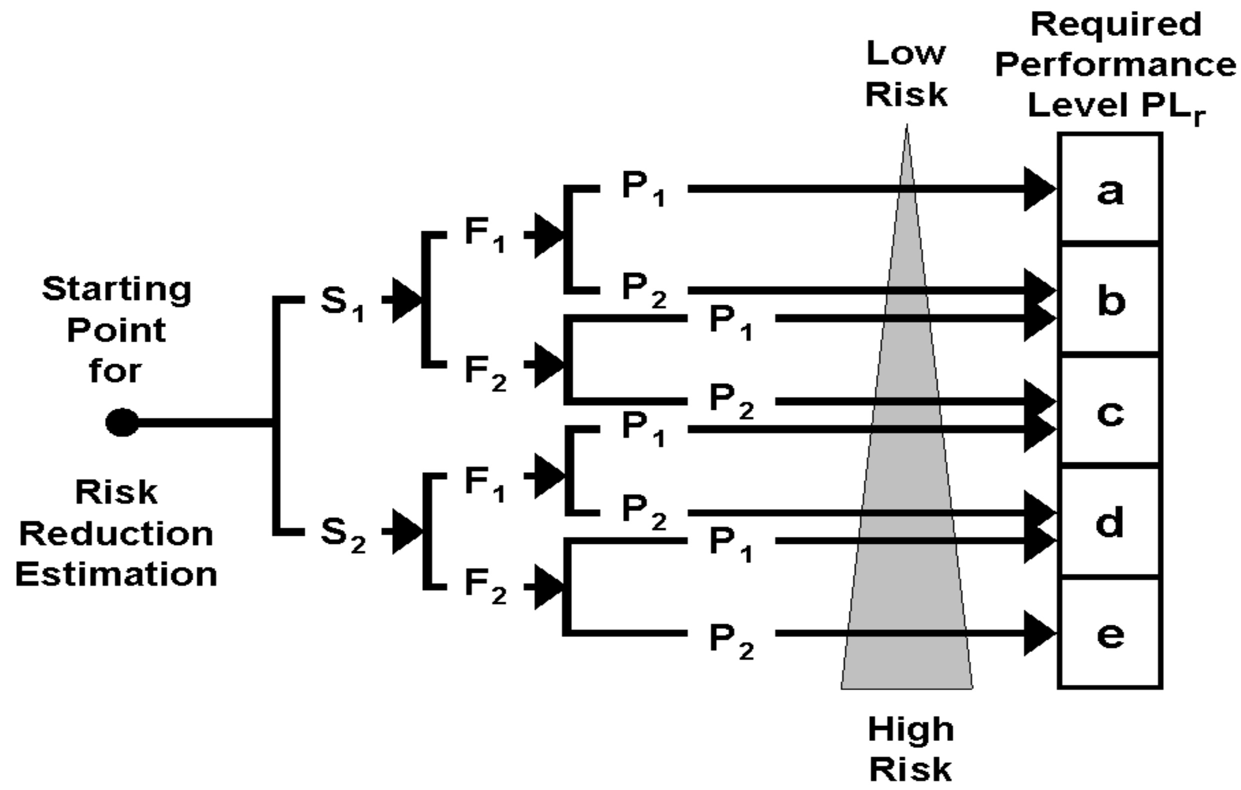
the PL_r correlated to „desired-value“.

It will be incooperated:

- severity of injury S
- Frequency and the duration of exposure
- Possibility of avoiding the hazard P

2. Determination of the PLr

The Easy Method: Risk Analysis by Risk Graph



RISK PARAMETERS

S = Severity of Injury

S1 = slight (normally reversible) injury

S2 = serious (normally irreversible) injury or death

F = Frequency and/or exposure time to hazard

F1 = seldom to less ofen and/or short exposure time

F2 = frequent to continuous and/or long exposure time

P = Possibility of avoiding or limiting the hazard

P1 = possible under certain circumstances

P2 = scarcely possible

Note: In case of no other justification F2 should be chosen, if the frequency is higher than once per 15 minutes.

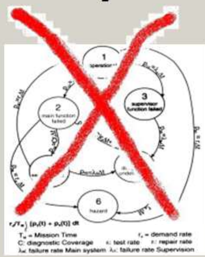
probability of failure: mathematically methods

Reliability block diagrams

Markov models

Petri networks

Fault Tree ?
Reliability Block ?

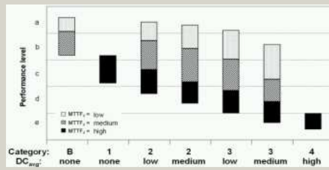


Markov-Models ?

problem:

- partially complicated, for machine designer not reasonable methods
- difficult determination of the input data
- $MTTF_D$, DC and ß
- so: simplified precedure

Precalculated Models

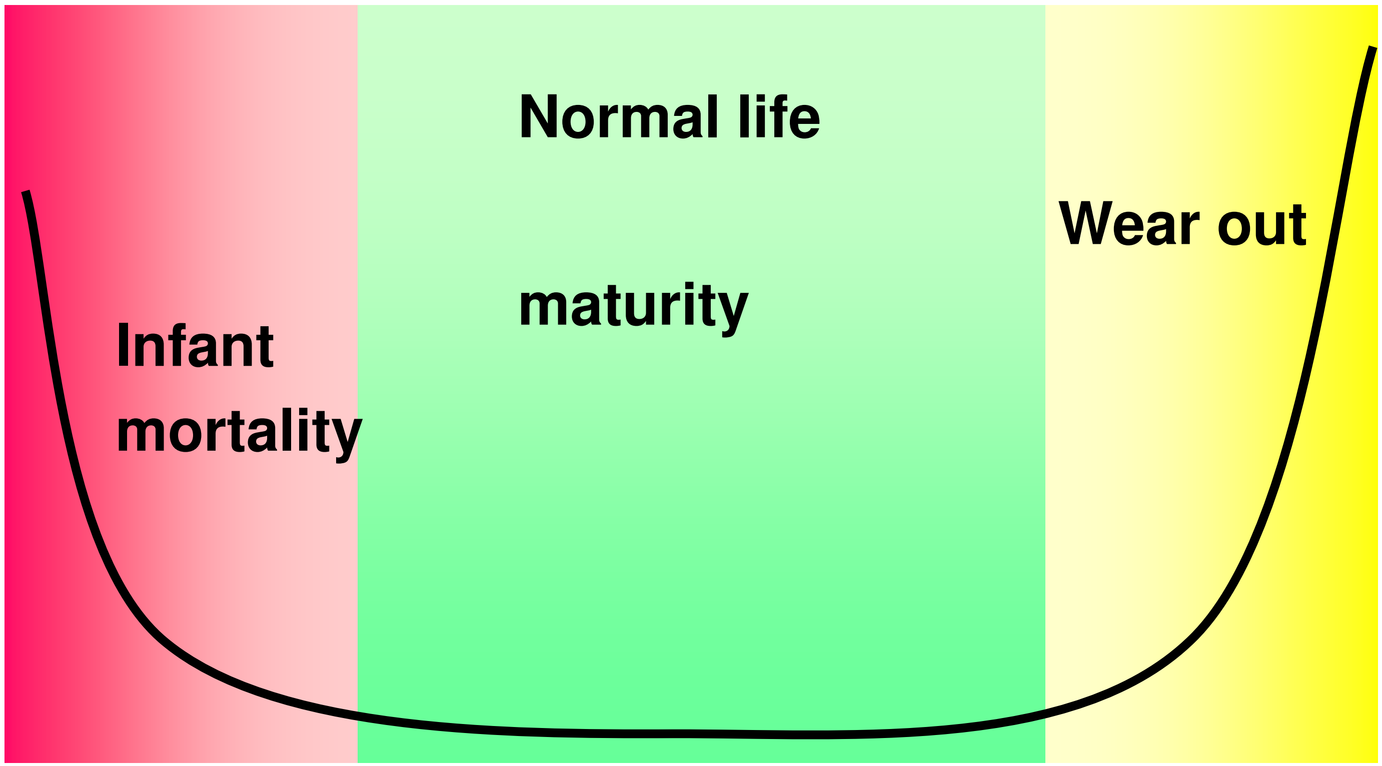


precalculated architecture: designated architectures

„designated architectures“, typ. Designed Architectures

- Already precalculated typical structures with inputs, logic and outputs (I/L/O)
- Conditions by the quantification:
  - Mission time 20 years
  - Constant failure rates within the mission time

„Typical diagramme for failure rate over time - called a "bathtub curve“



- assembly fault
- manufacturing defect
- materials fault
- design fault

- fatique fracture
- ageing
- wear
- dimples

- operation fault
- soil particle
- service faults

Thus a component's lifetime can be divided into three periods:

- Infant mortality, precocious failures.
- Useful life, failure rates significantly constant.
- Wear out, wear failures.

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

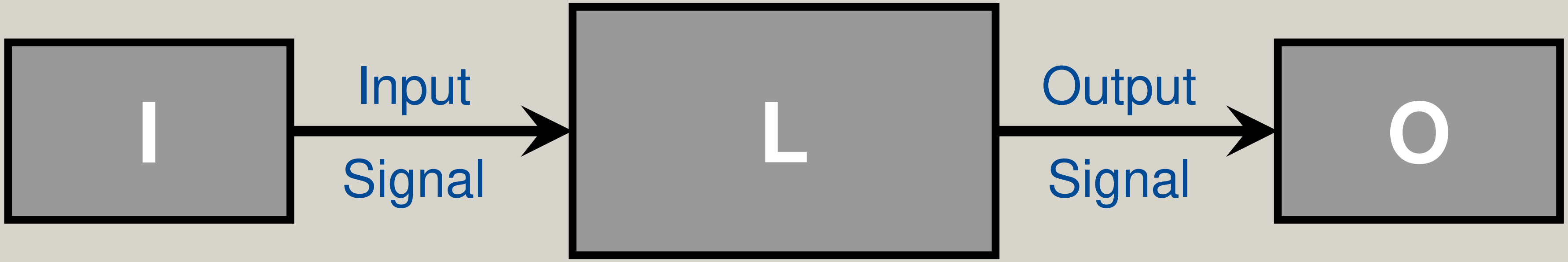
3./4. Design of the safety related block diagram and determination of the Categories

Categorie	Short description	System behaviour	Principle applied to achieve safety
B	Control system according to state of the art	A fault can lead to the loss safety	By selection of com-ponents and safety principles
1	Use of well-tried safety principles	As described for category B, but with higher reliablity	
2	Checking of safety function by the machine control system	Possible loss of safety function between checks	By structure and de-sign of the control system
3	Redundancy with partial fault detec-tion, as far as practicable according to the state of the art	A fault does not lead to the loss of safety	
4	Self-monitoring, faults are detected in time	multiple faults do not lead to the loss of safety	

Die EN ISO 13849-1 provides **5 designated architectures**:

category				
B	1	2	3	4
maximum reachable: PL = b	maximum reachable: PL = c	maximum reachable: PL = d	maximum reachable: PL = e	maximum reachable: PL = e

Category B

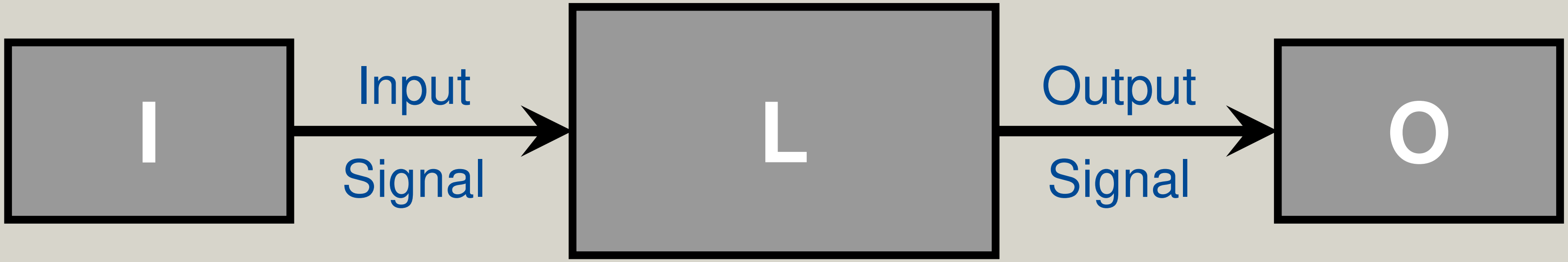


- their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence
- Zero fault tolerance
- Mainly characterised by selection of components
- $MTTF_D$ = low to medium

Example for category B

- Selection of degree of protection
- Correct selection of the cross section
- Selection of cable insulation
- Selection of the colours of indication instrument
- Selection of measures against environments influence
- Selection of protection measures
- Correct dimensioning of motors

category 1

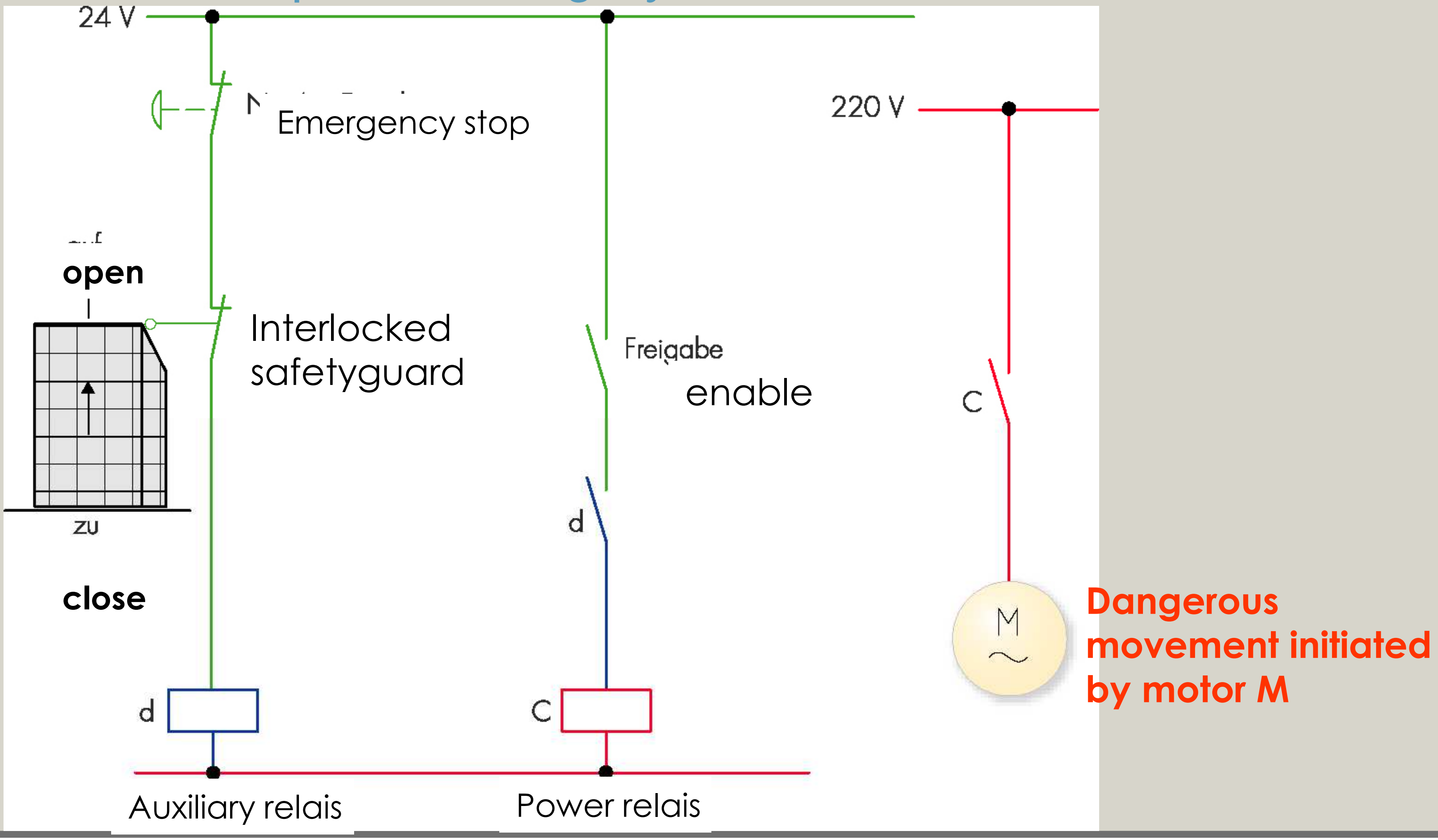


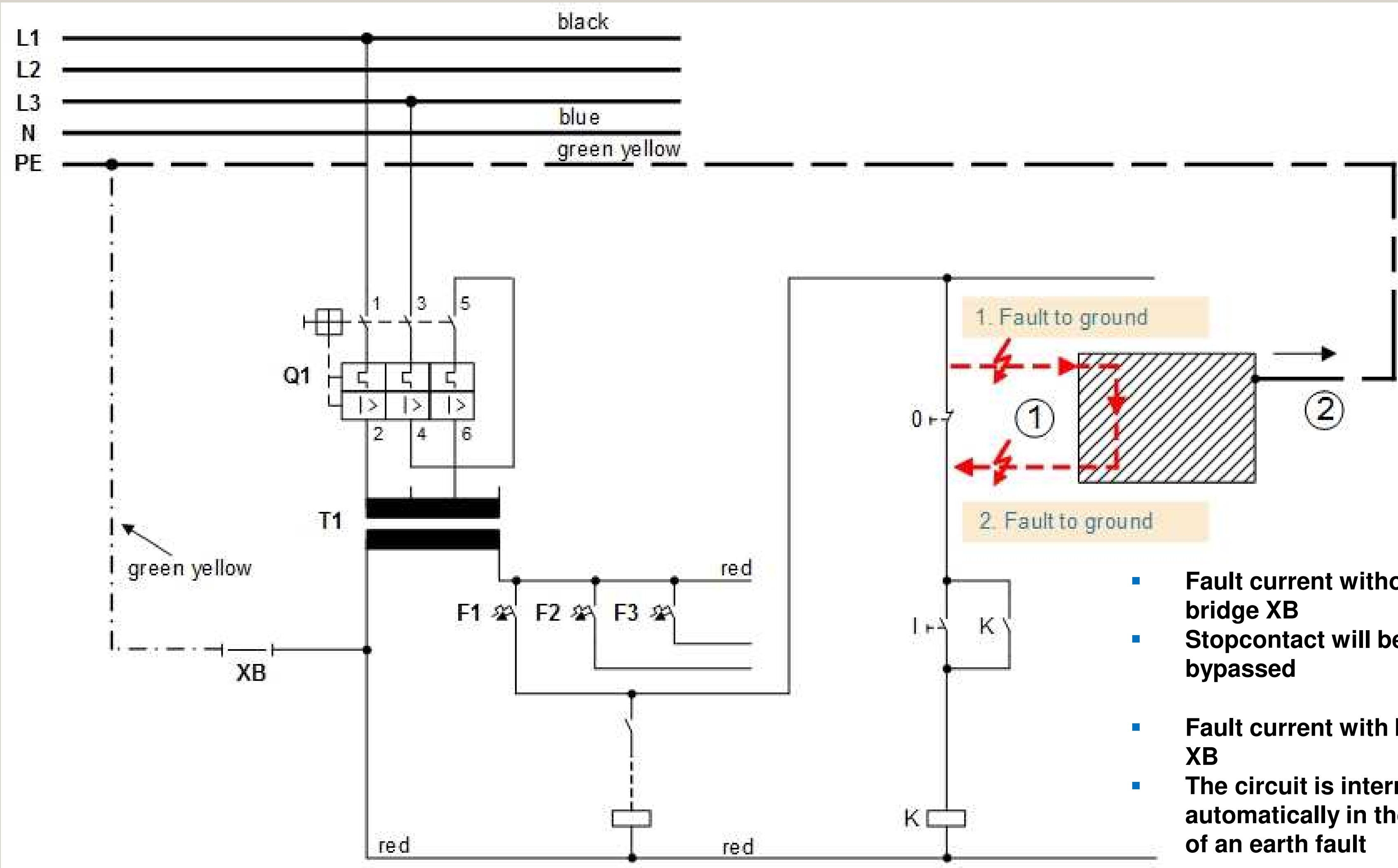
- Requirements of B shall apply
- Well-tried components and well-tried safety principles shall be used
- Zero fault tolerance but better than category B
- Mainly characterised by selection of components
- $MTTF_D$ = high
- Dc_{cav} = non

Example for category 1

- Separation distance
- Over–dimensioning
- Bonding of the controlsystem
- Emergency stop device (EN 418)
- Circuit breaker (EN 60947-2)
- fuse (EN 60269-1)
- Transformer (EN 60741)
- Fault avoidance in cables
- Positive mode actuation
- Positive mechanically linked contacts
- Limitation of electrical parameters

Example for category 1



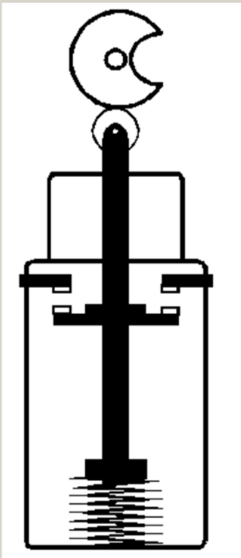


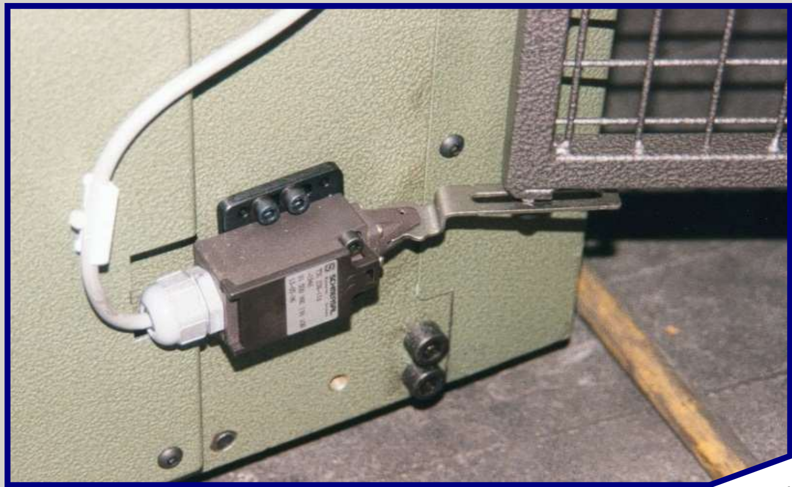
- Fault current without bridge XB
- Stopcontact will be bypassed

- Fault current with bridge XB
- The circuit is interrupted automatically in the event of an earth fault

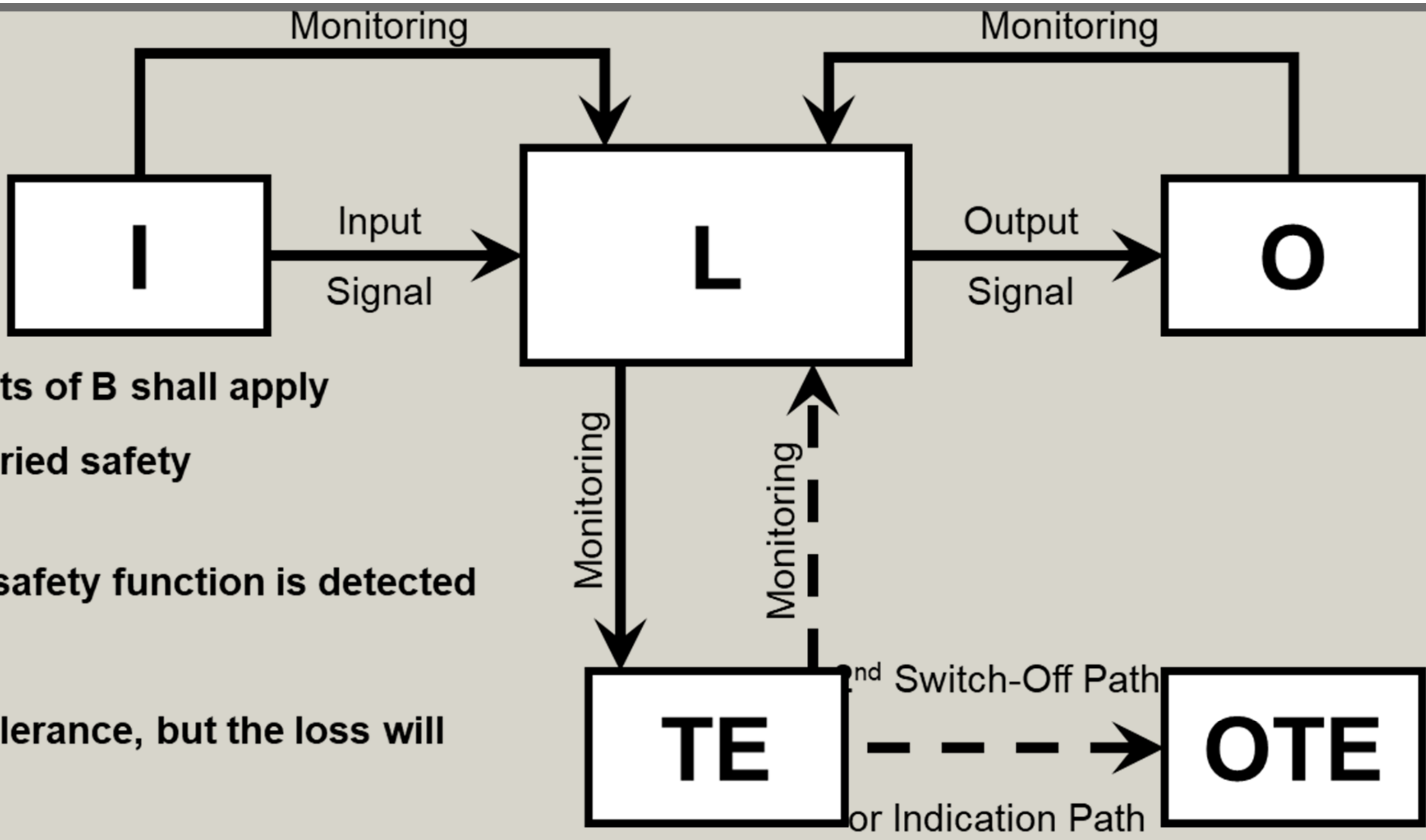
Safety switch according category 1

Safety switch
positive
mechanically
linked contacts



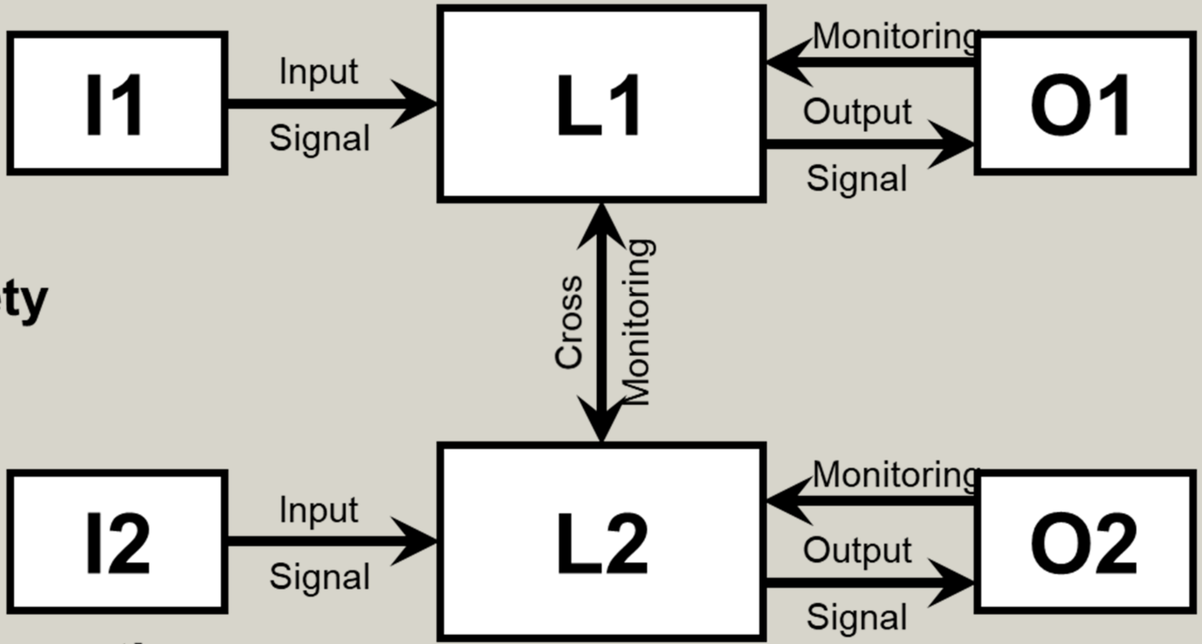


Schaltglied und Betätigungsorgan
bilden konstruktiv und funktionell
eine Einheit



- Requirements of B shall apply
- use of well-tried safety principles
- The loss of safety function is detected by the check
- Zero fault tolerance, but the loss will be detected
- $MTTF_D$ = low to high
- Dc_{cav} = low to medium
- CCF 65 points required

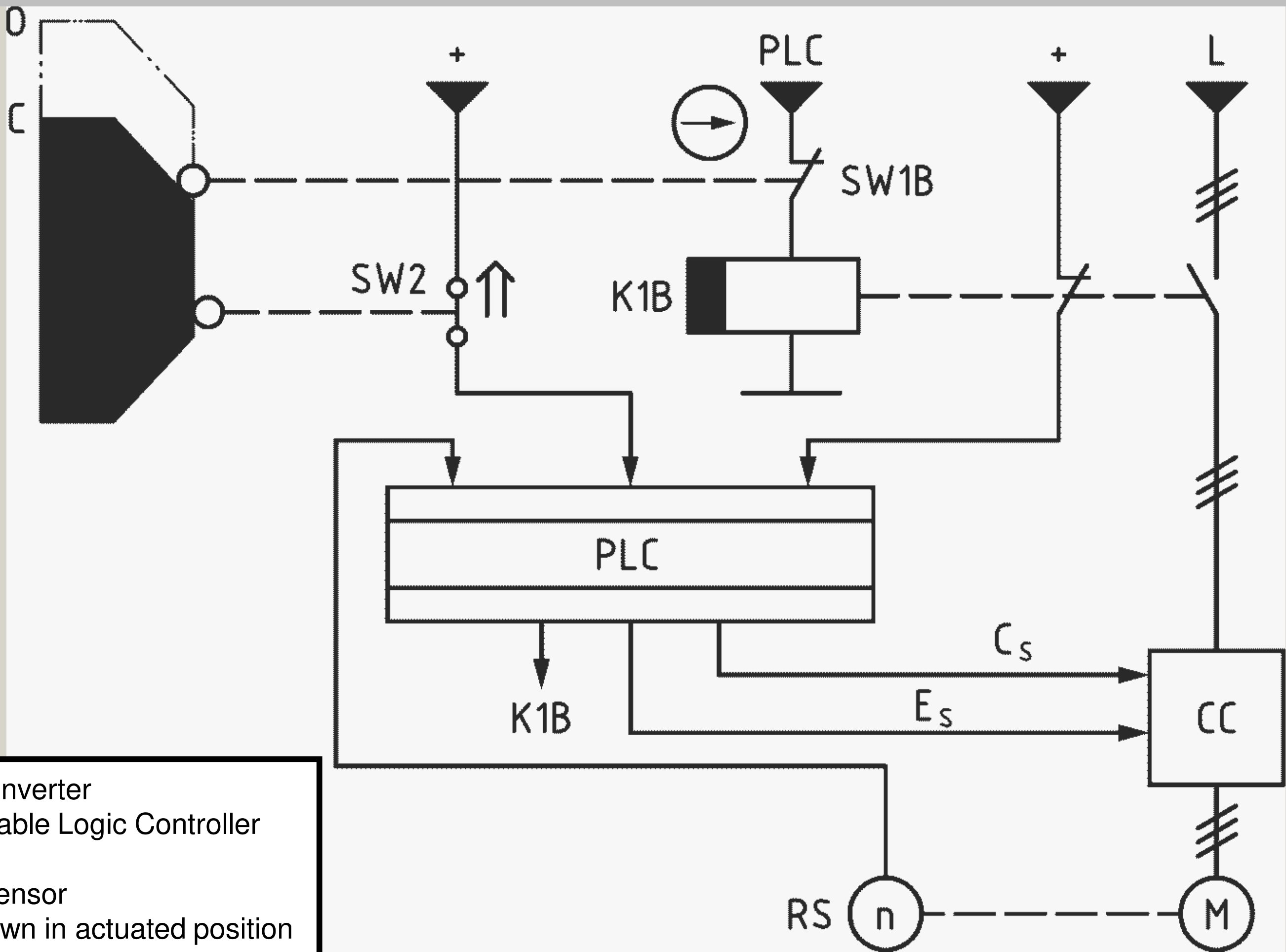
Categorie 3



- **Requirements of B shall apply**
- **use of well-tried safety principles**
- **one fault tolerance**
- **Different level of diagnostic coverage**
- **$MTTF_D$ = low to high**
- **Dc_{cav} = low to high**
- **CCF 65 points required**

Example for category 3

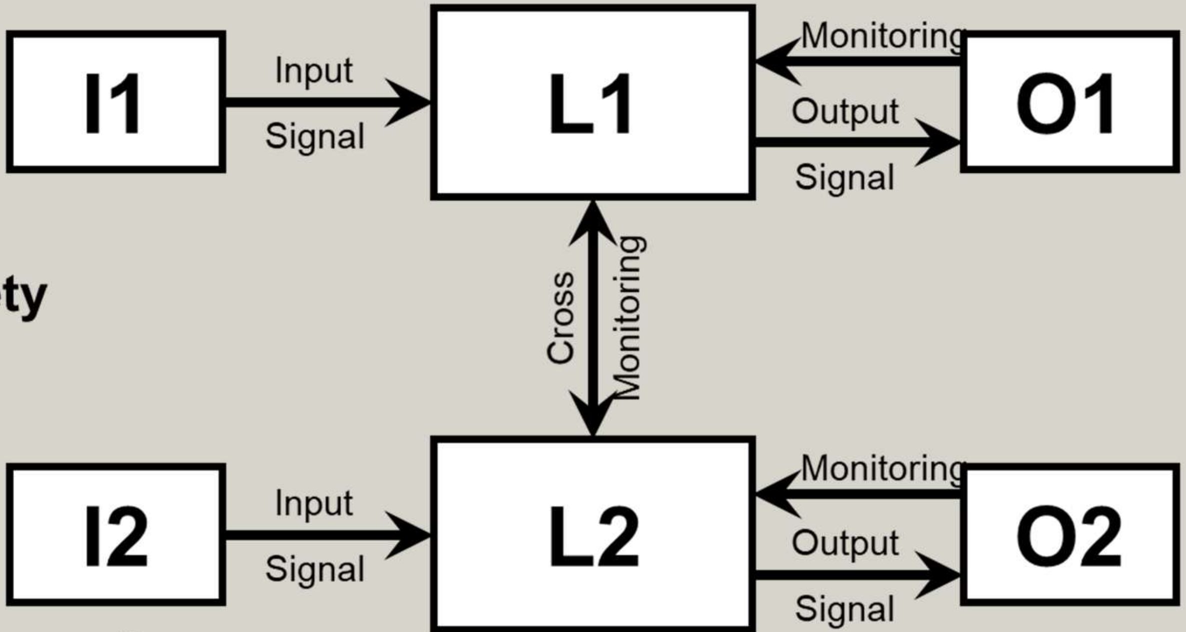
Interlocked safetyguard



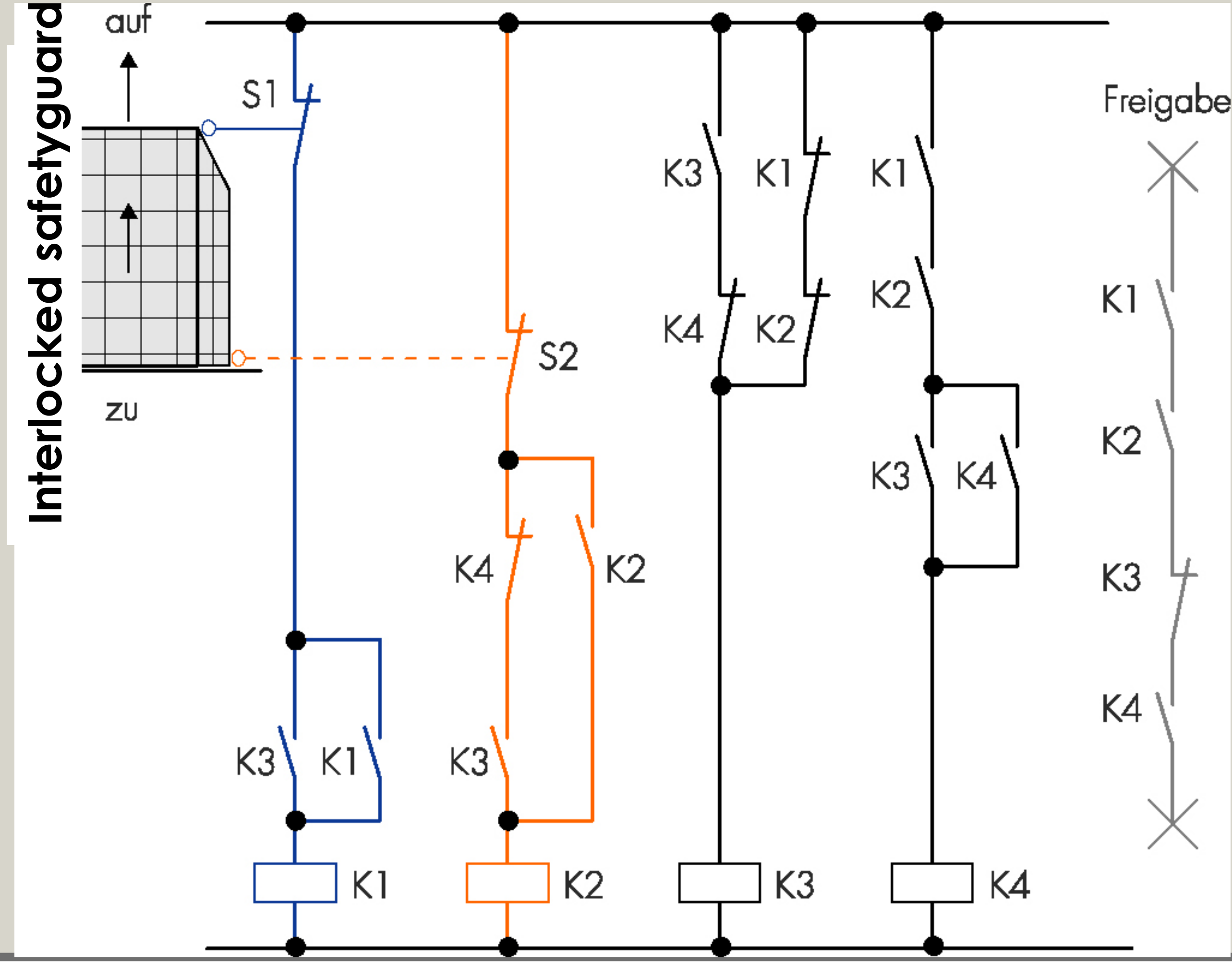
CC:	Current Converter
PLC:	Programmable Logic Controller
M:	Motor
RS:	Rotation Sensor
⇑	Switch shown in actuated position

Categorie 4

- Requirements of B shall apply
- use of well-tried safety principles
- one fault tolerance
- Different level of diagnostic coverage
- $MTTF_D$ = high
- Dc_{cav} = high
- CCF 65 points required



Example for category 4



Identification of SRP/CS

SRP/CS: Parts of control system what generate
Input signals to safety related output signals

Typical safety function

SRP_a → i_{ab} → SRP_b → i_{bc} → SRP_c

Input	Logic	Output

Actuation by hand
Other signal

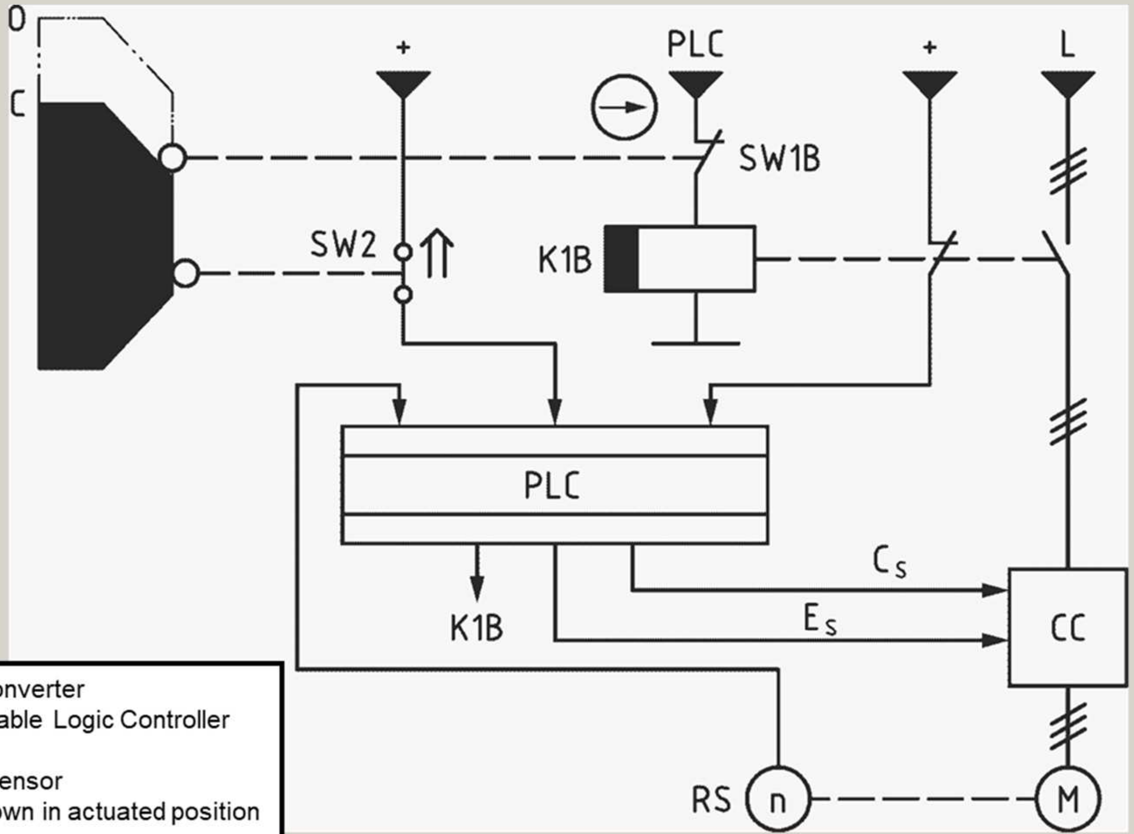
Actors
Breaks

Steps to performance level

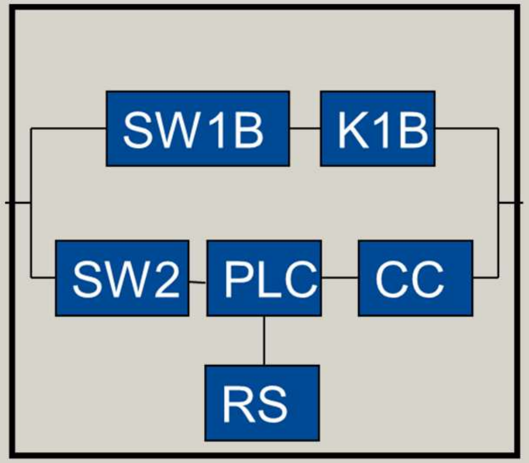
1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

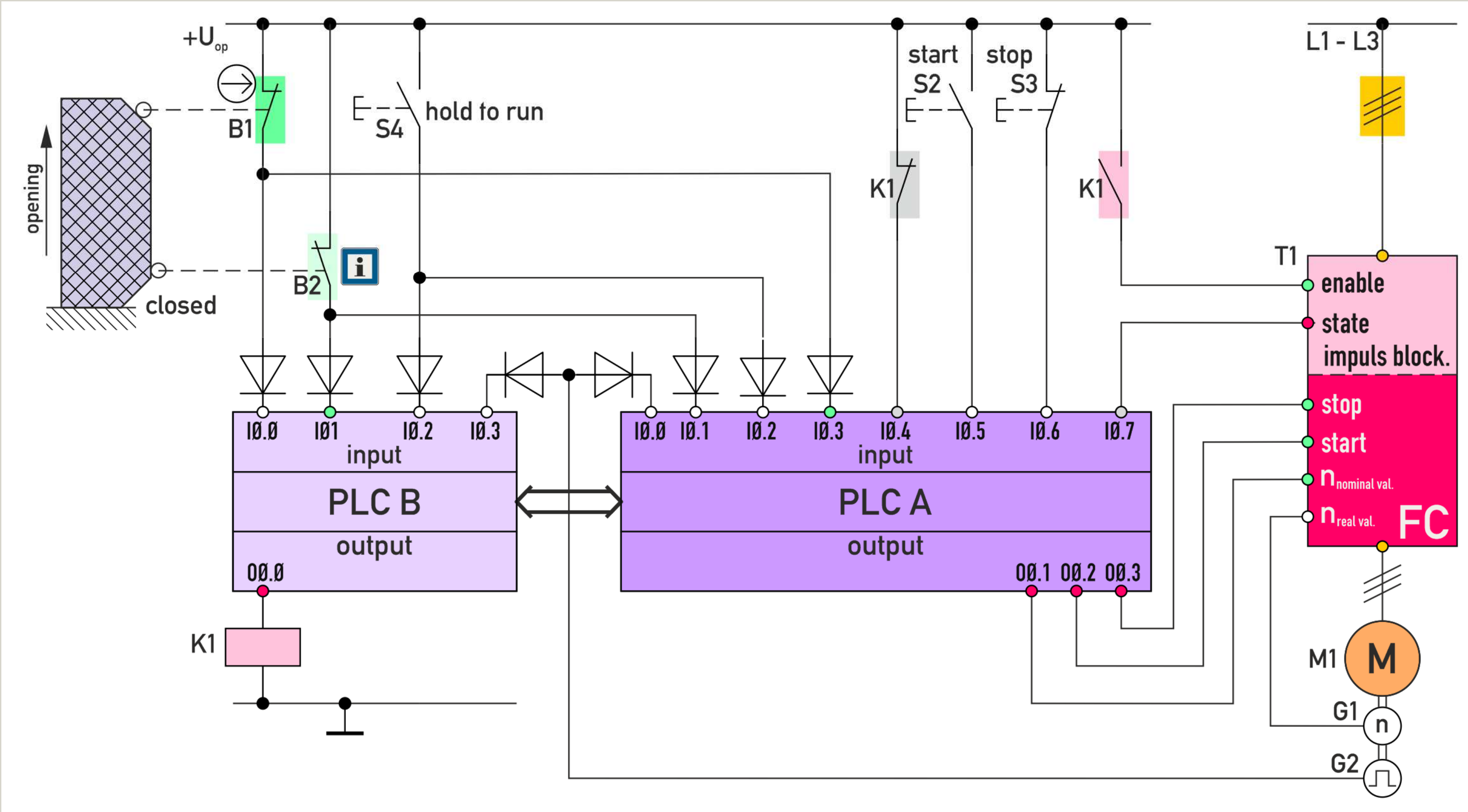
Determination of the logical Block diagram of SRP/CS

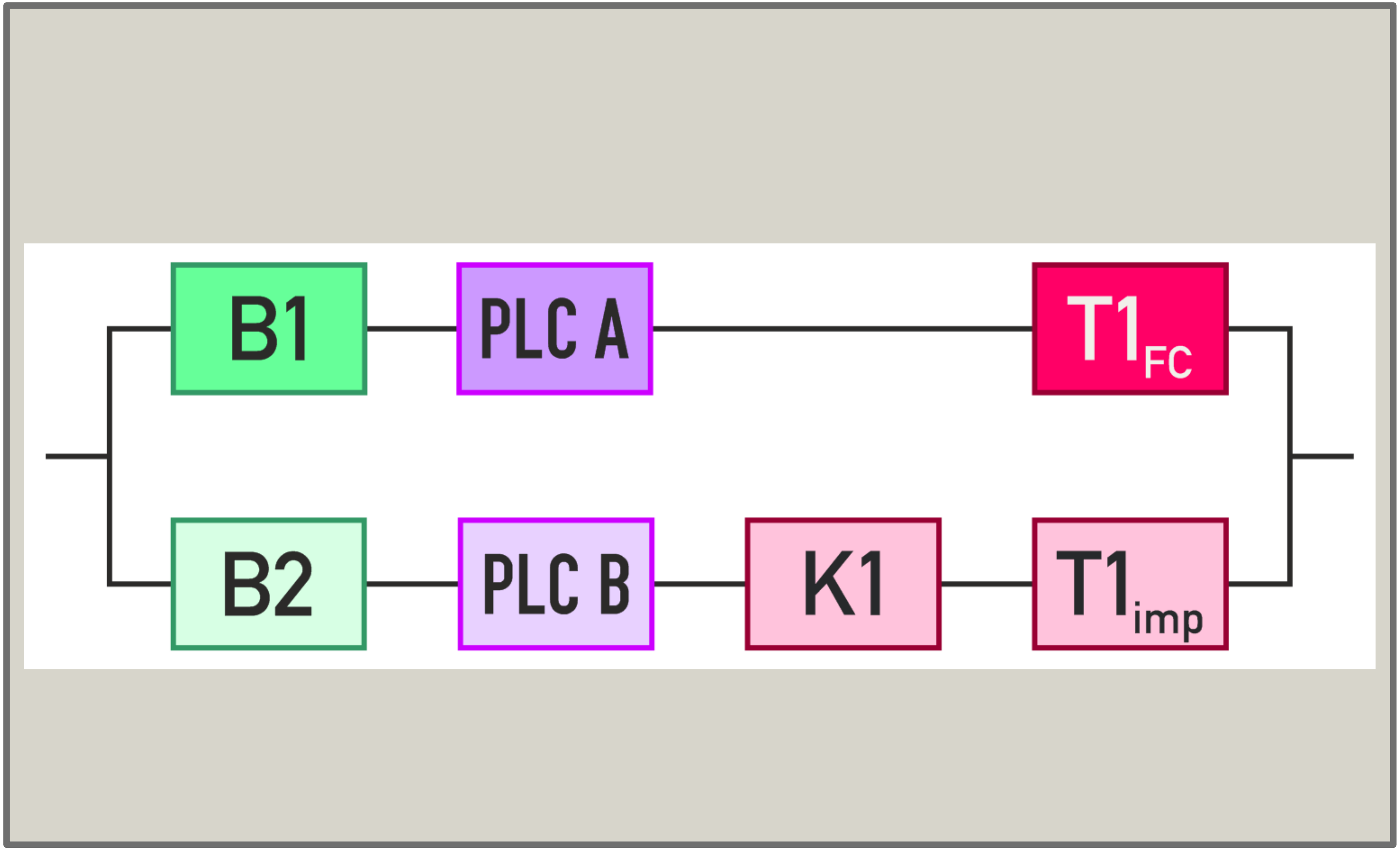
Interlocked safetyguard



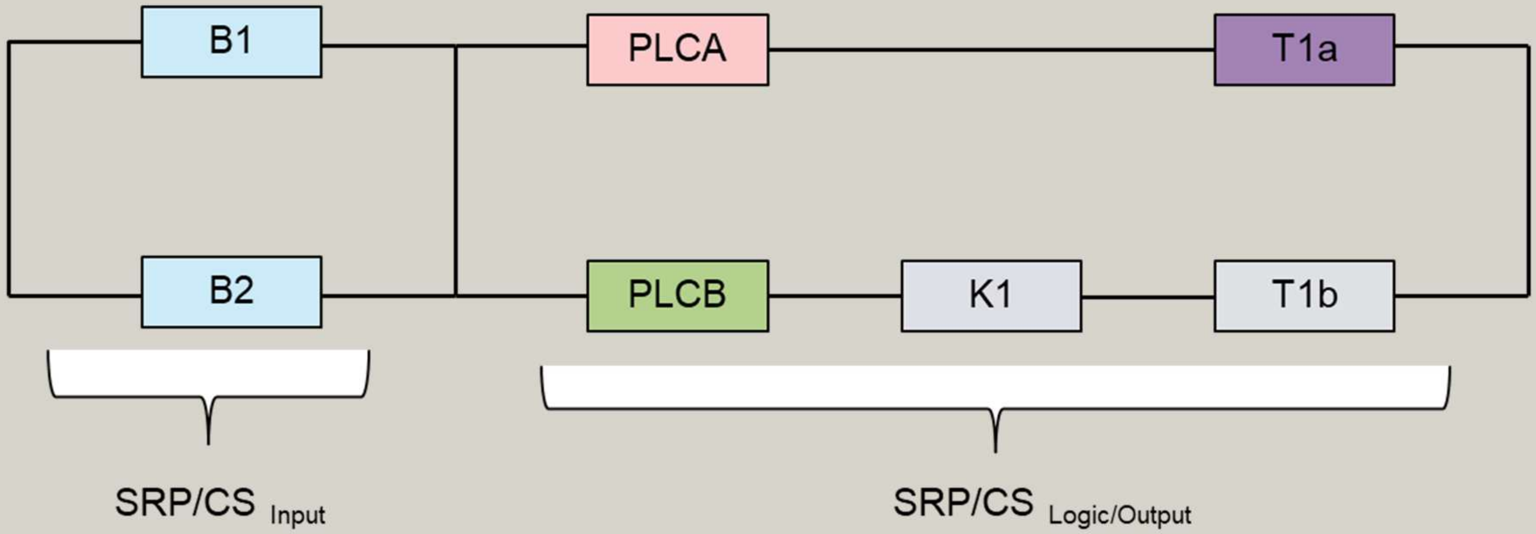
CC: Current Converter
PLC: Programmable Logic Controller
M: Motor
RS: Rotation Sensor
⇑ Switch shown in actuated position




+U op
B1
opening
closed
B2
S4
hold to run
start
S2
stop
S3
K1
K1
L1 - L3
T1
enable
state
impuls block.
stop
start
n nominal val.
n real val.
FC
I0.0
I01
I0.2
I0.3
input
PLC B
output
O0.0
K1
I0.0
I0.1
I0.2
I0.3
I0.4
I0.5
I0.6
I0.7
input
PLC A
output
O0.1
O0.2
O0.3
M1
M
G1
n
G2


B1
PLC A
$T1_{FC}$
B2
PLC B
K1
$T1_{imp}$

Logical bloc diagram of stop function



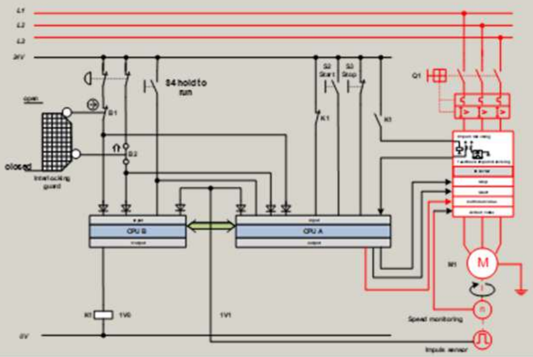
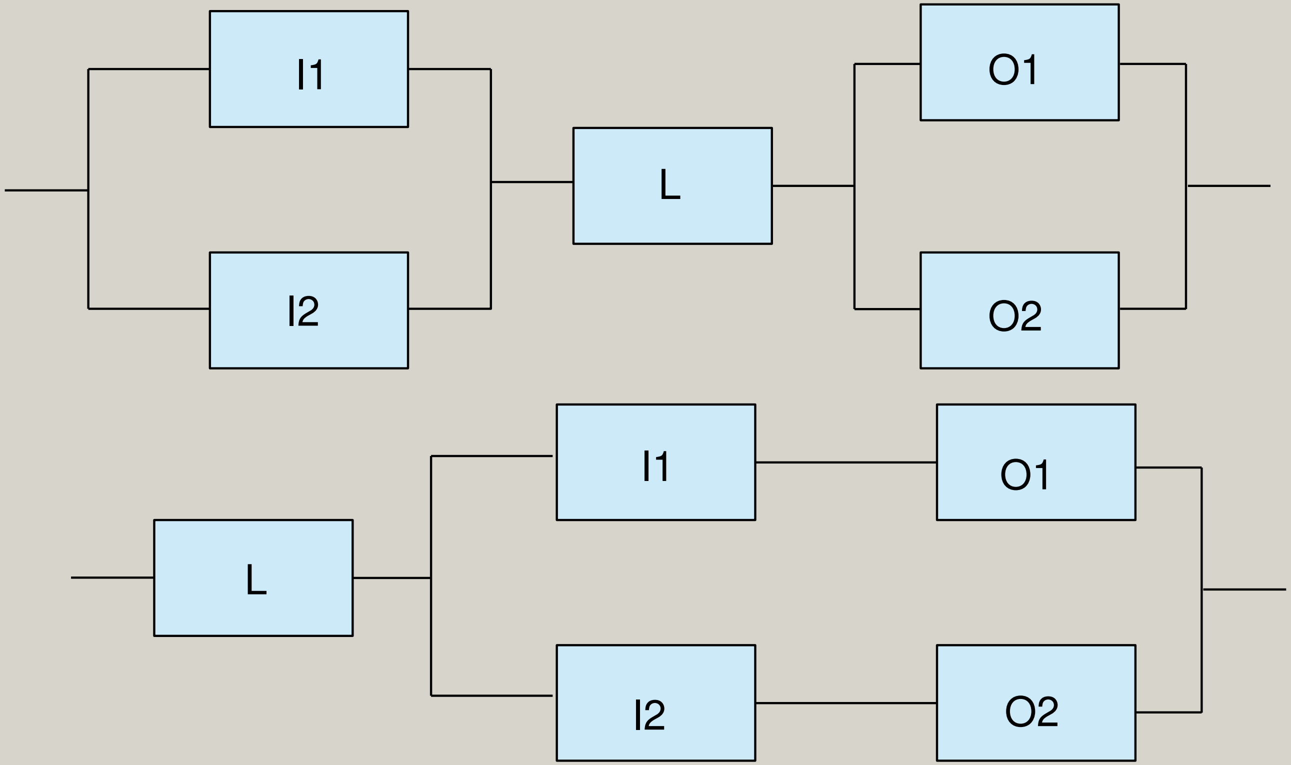


Illustration of logical block diagram of different systems



data from the producer
e.g.: PFH values

Calculation considering:
$ß10_D$, DC_D, structur

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

5. Calculation of $MTTF_D$

Some Definitions: $MTTF_D$

$MTTF_d$: mean value of operation time where a <u>single</u> channel of the system is expected to have no <u>dangerous</u> failure

denotation	range of $MTTF_D$
low	3 years $\leq MTTF_D <$ 10 years
medium	10 years $\leq MTTF_d <$ 30 years
high	30 years $\leq MTTF_d \leq$ 100 years

Determination of $MTTF_D$ for each channel

For each channel separately

identification of all safety relevant components in each channel

↓

Determine for each component the $MTTF_D$-Values

↓

calculate the $MTTF_D$ value for each channel

$MTTF_D$ pneumatic & (elekctronic-) mechanical Components

determination of the components $MTTF_D$-values

- use manufacturer’s data;
- use methods in Annexes C and D;
- choose ten years.

$MTTF_D$ pneumatic & (elektro-)mechanical Components

Good engineering practices method: Worst Case Werte

For <u>pneumatic, mechanical , electromechanical components, position switches etc.</u>

- The components are manufactured according to basic and well-tried safety principles in accordance with ISO 13849-2:2012, or the relevant standard (see Table C.1) for the design of the component (confirmation in the data sheet of the component).
- The manufacturer of the component specifies the appropriate application and operating conditions for the user.
- The design of the SRP/CS fulfils the basic and well-tried safety principles according to ISO 13849-2:2015, for the implementation and operation of the component.

assumptions: $B10_D$ = 2*B10 (50% dangerous faults)

$MTTF_d$ pneumatischer & (electro-)mechanical components

Mechanical components		$MTTF_D$ = 150 years
Hydraulic components		$MTTF_D$ = 150 years
Pneumatic components		B_{10D} = 20.000.000
Relays and Contactor, Näherungsschalter	Small load Maximum load	B_{10D} = 20.000.000 B_{10D} = 400.000
Main contactor	Small load Rated load	B_{10D} = 20.000.000 B_{10D} = 2.000.000
Position switch (with separated actuator, Interlocking)		B_{10D} = 20.000.000 (B_{10D} = 2.000.000)
Enabeling switch*		B_{10D} = 100.000
Emergency stop devices* (maximum load)		B_{10D} = 100.000 (B_{10D} = 6.050)

$MTTF_D$ pneumatic & (electro-)mechanical components

e.g. pneumatic valves, relays, contactors, position switches, cam of position switches)

- Determination of the mean cycle of machine
- the manufacturers of these kinds of components only give the mean number of cycles until ten percent of the components fail dangerously (B_{10d}).
- method to calculate a $MTTF_d$ for components by using B_{10d}:

$$MTTF_D = \frac{B_{10D}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\frac{s}{h}}{t_{cycle}}$$

n_{op}:mean number of annual operations

d_{op} mean operation days per year

h_{op} mean operation hour per day

correspond to 10% (0,1)

Determination of B_{10D} and $MTTF_D$ of relais

$$n_{op} = \frac{240 \cdot 16 \cdot 3600}{20} = 691.200 \frac{cycles}{year}$$

d_{op}: 240
h_{op}: 16
t_{cycle}: 20

$B10_D$=20000000 for relais

$$MTTF_D = \frac{20.000.000}{0,1 \cdot 691.200} = 289\ years$$

According to the standard maximum application time:

$T_{10D} = B_{10D}/n_{op}$ = 28,9 years

MTTFd - Mean Time To (dangerous) Failure

$MTTF_d$: mean value of operation time where a single channel of the system is expected to have no dangerous failure

Components

Typical Values	Basic and well-tried safety principles ISO 13849-2:2003	Typical $MTTF_d$ (y) or B_{10d} (cycle) values
Mechanical components	Tables A.1 and A.2	$MTTF_d$ = 150 y
Hydraulic components	Tables C.1 and C.2	$MTTF_d$ = 150 y
Pneumatic components	Tables B.1 and B.2	B_{10d} = 20 000 000
Relays and contactor relays with small load (mechanical load)	Tables D.1 and D.2	B_{10d} = 20 000 000 $MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}}$

Channel

$$\frac{1}{MTTFD} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{D,j}}$$

Symmetrisation

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

System

Classes	
low	3 years ≤ $MTTF_d$ < 10 years
medium	10 years ≤ $MTTF_d$ < 30 years
high	30 years ≤ $MTTF_d$ ≤ 100 years

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

Diagnostic Coverage DC

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

probability of detected dangerous failures

probability of total dangerous failures

Denotation	Values of DC
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Example:
Dynamic testing of inputs using cyclic testing procedure

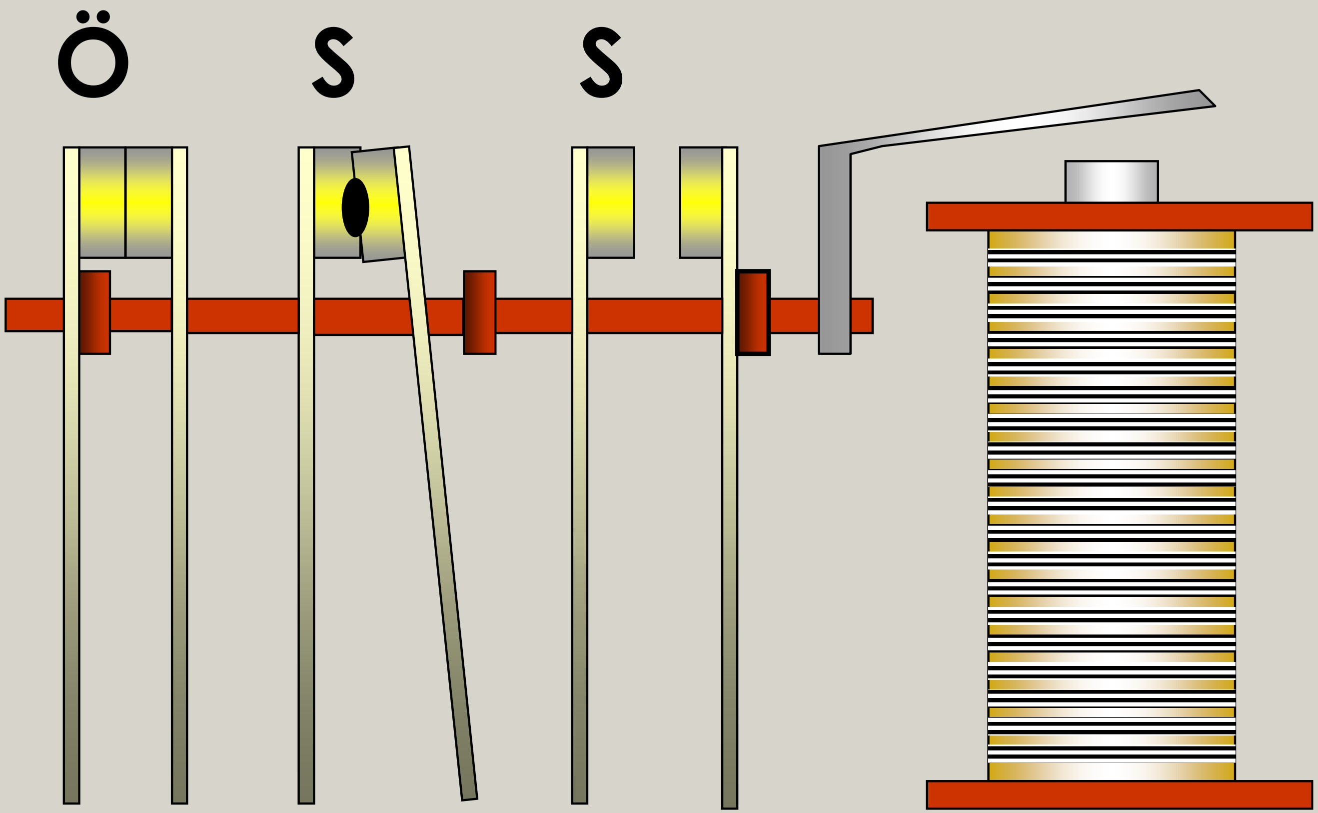
⇨ **medium**

Other sources for DC-Values

DIN EN ISO 13489-1 list in chart E.1 the efficiency of diagnostic measures ,

Measure	Maximum of Diagnostic coverage	Comment
Sensors (process discover failures)	low to middle (depends on the rate of demands)	depends on the DC for failures
switch with positive mechanically linked contacts (plausibility-check)	high	
Actors (redundand switch-off circuit with supervising)	middle	
Logic Dynamic Principles	high	All parts of the logic asume the change on-off-on in the case of demand of safety (function)

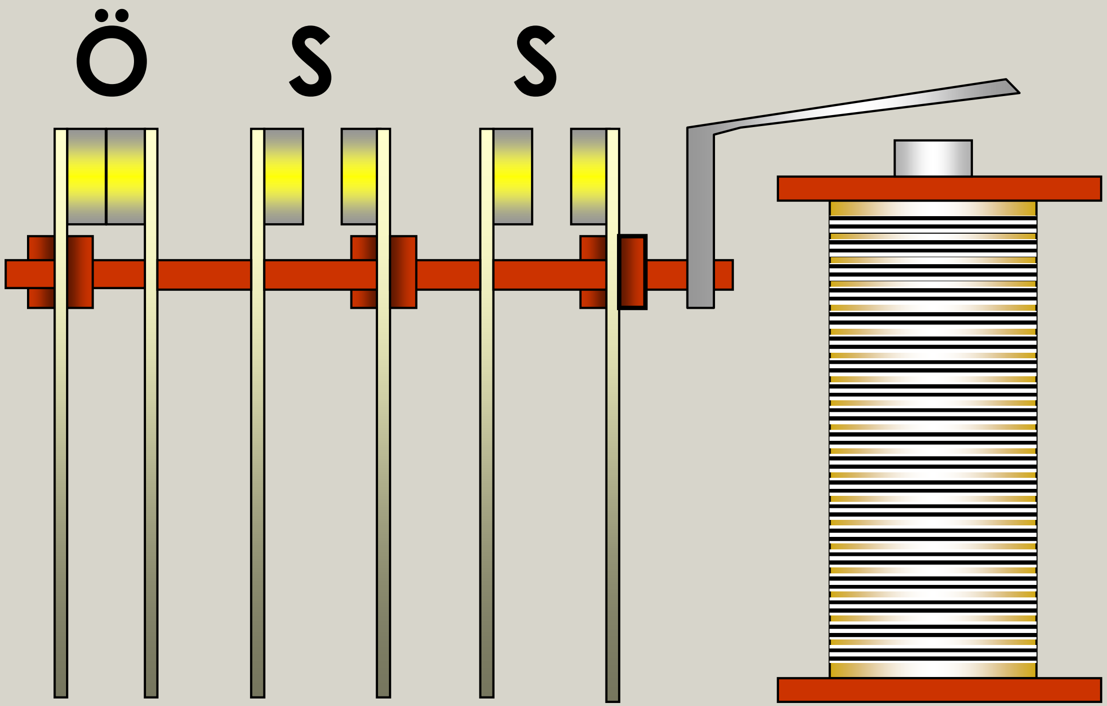
Monotoring of relais



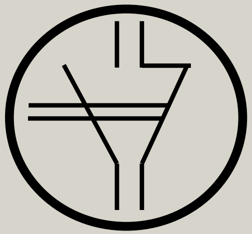
Relais without positive mechanically linked contacts

Monotoring of relais

Use of well- tried principle and components



Relais with positive mechanically linked contacts

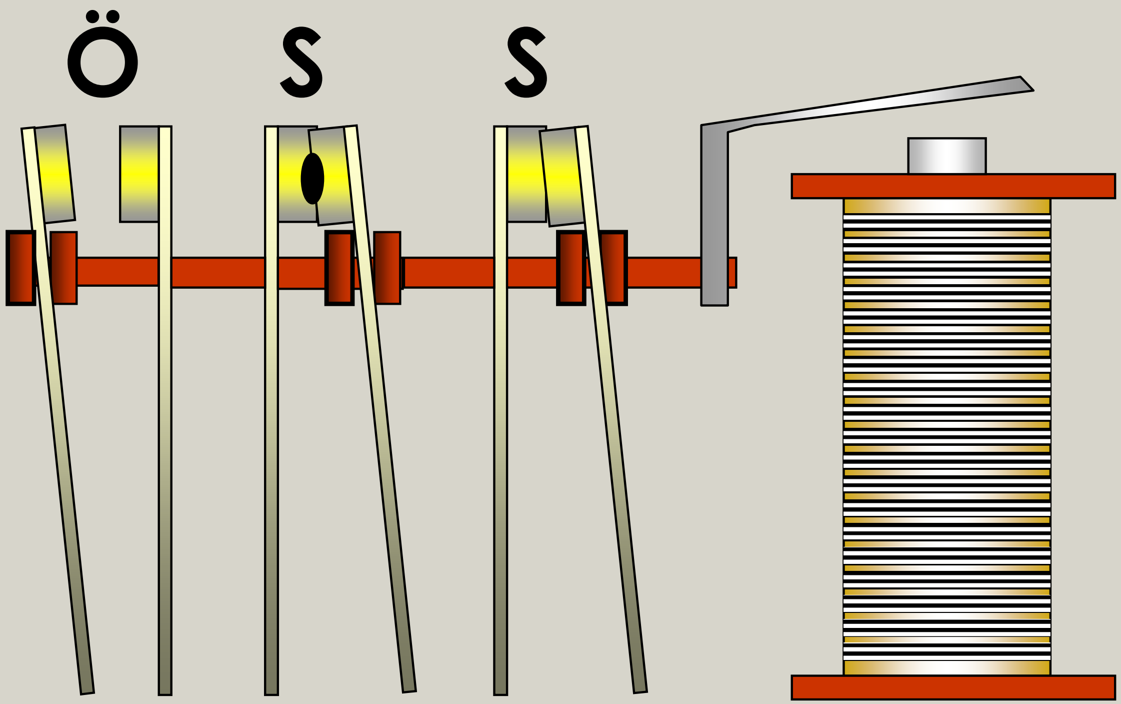


EN 50205 04/97 Abs. 4.6.2

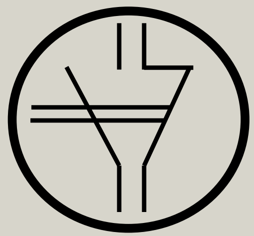
Symbol for mechanically linked contacts

Monotoring of relais

Opener and closer have always a different mode



Relais without positive mechanically linked contacts



EN 50205 04/97 Abs. 4.6.2

Symbol for mechanically linked contacts

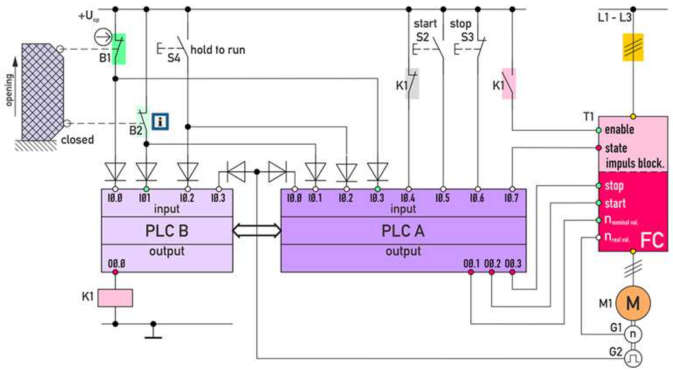
Measures for Input devices	DC
Cyclic test stimulus by dynamic change of the input signals	90%
Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts	99%
Cross monitoring of inputs without dynamic test	90% to 99% depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90%
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99%
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99% depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
Fault detection by the process	0 % to 99% depending on the application.This measure alone is no sufficient if the required performance level is "e"
Monitoring some characteristics of the sensor (response time, range of analogue signals) e.g. electrical resistance, capacitance	60%

The ratio of the test rate (r_t) to the request rate of the safety function (r_d) limits the effectively achievable DC:

$r_t/r_d = 1$	The maximum DC achievable by the process is limited to 60%.
$r_t/r_d = 10$	The maximum DC achievable by the process is limited to 90%.
$r_t/r_d = 100$	The maximum DC achievable by the process is limited to 99%.

For Category 3 and 4

r_t<1/year	DC is 0%
r_t >=1/year	DC is limited to 90%
r_t >=1/month	DC is limited to 99%



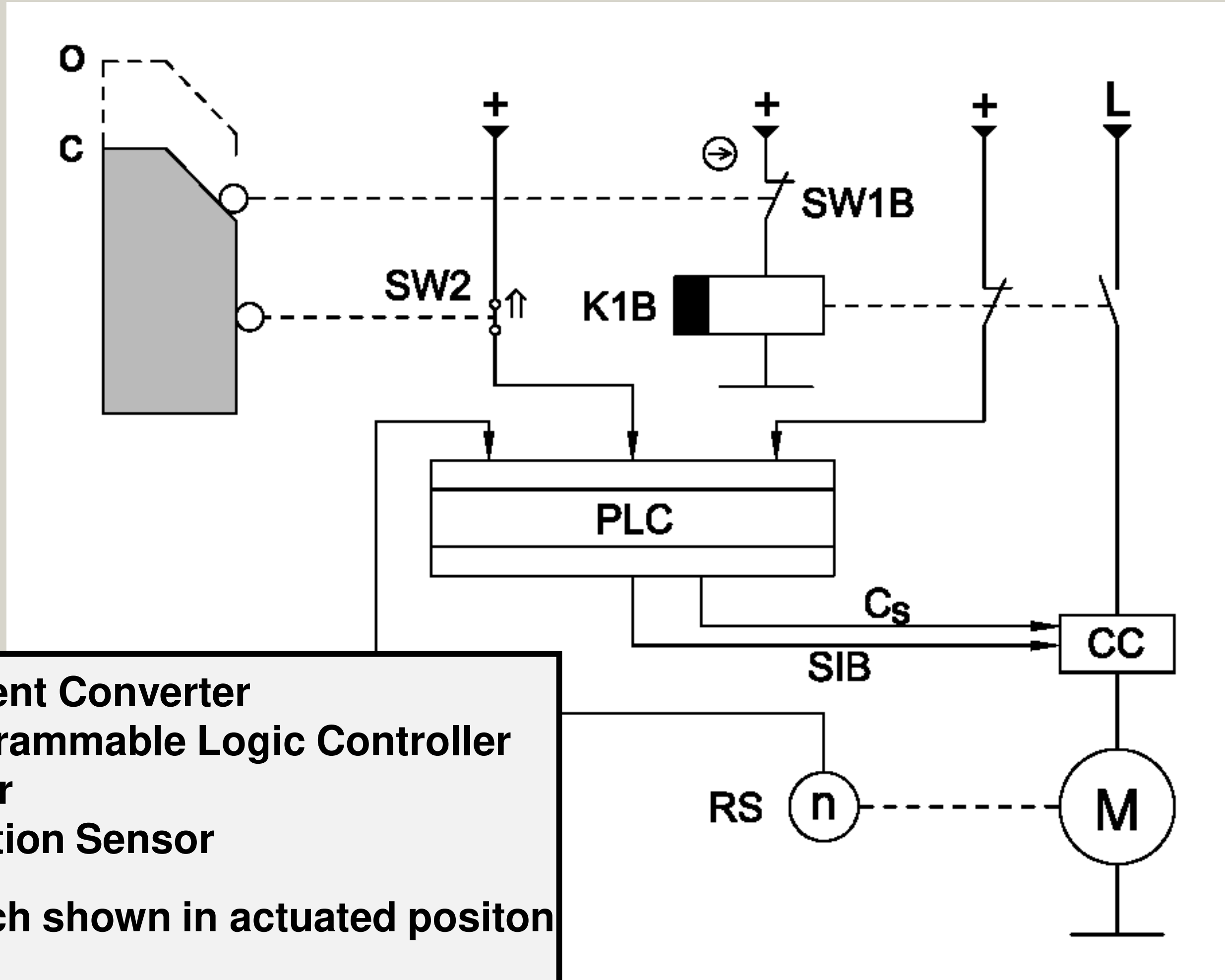
How to determine DC using Chart

Identify all Selftests and all Possibilites for Diagnostic

Withdraw the particular DC-values from the charts

Apply the averaging-formula to determine the general DC

Determination of the diagnostic value DC



DC_{SW2}=90%

DC_{K1B}=99%

DC_{PLC}=60%

DC_{CC}=90%

DC_{SW1}=99%

CC:	Current Converter
PLC:	Programmable Logic Controller
M:	Motor
RS:	Rotation Sensor
⇑	Switch shown in actuated positon

DCavg

In PL is only the average value of DC_{avg} taken in account, weightes and evaluated over all the tests.
Factor for weighting is $MTTF_d$ of the tested part:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}}$$

For non-tested parts is DC = 0.
To summerise, all parts without failures-exclusion must be taken in to account. (failures-exclusion => $MTTF_D = \infty$).

Determination of DC_{avg}

- DC_{SW2}=90%
- DC_{K1B}=99%
- DC_{PLC}=60%
- DC_{CC}=90%
- DC_{SW1}=99%

$$DC_{Davg} = \frac{\frac{0,90}{MTTF_{DSW2}} + \frac{0,99}{MTTF_{DK1B}} + \frac{0,30}{MTTF_{DPLC}} + \frac{0,90}{MTTF_{DCC}} + \frac{0,99}{MTTF_{DK1B}}}{\frac{1}{MTTF_{DSW2}} + \frac{1}{MTTF_{DK1B}} + \frac{1}{MTTF_{DPLC}} + \frac{1}{MTTF_{DCC}} + \frac{1}{MTTF_{DK1B}}}$$

DC_{avg} of 87,6% in the case all componets have the same $MTTF_D$ value

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

7. Considering of CCF

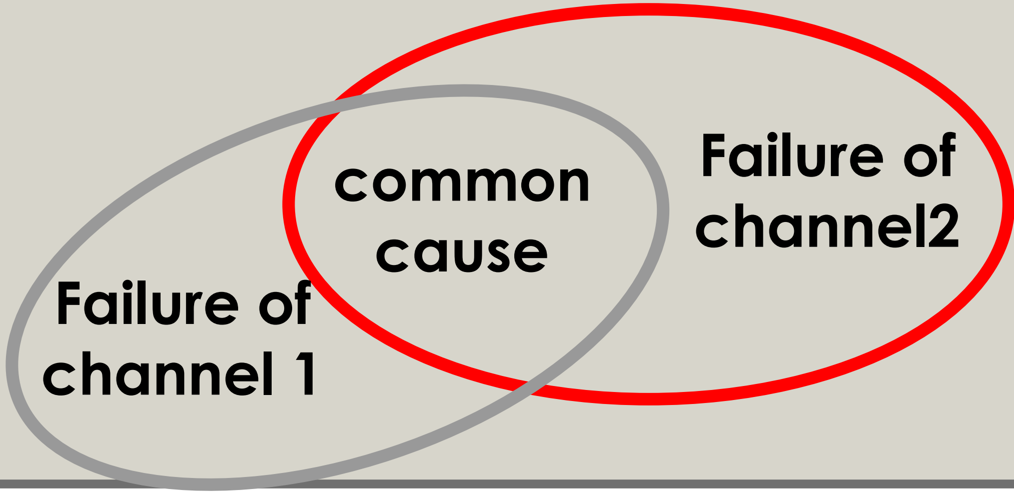
Measures against Common Cause Failure

Minimum requirement for CCF

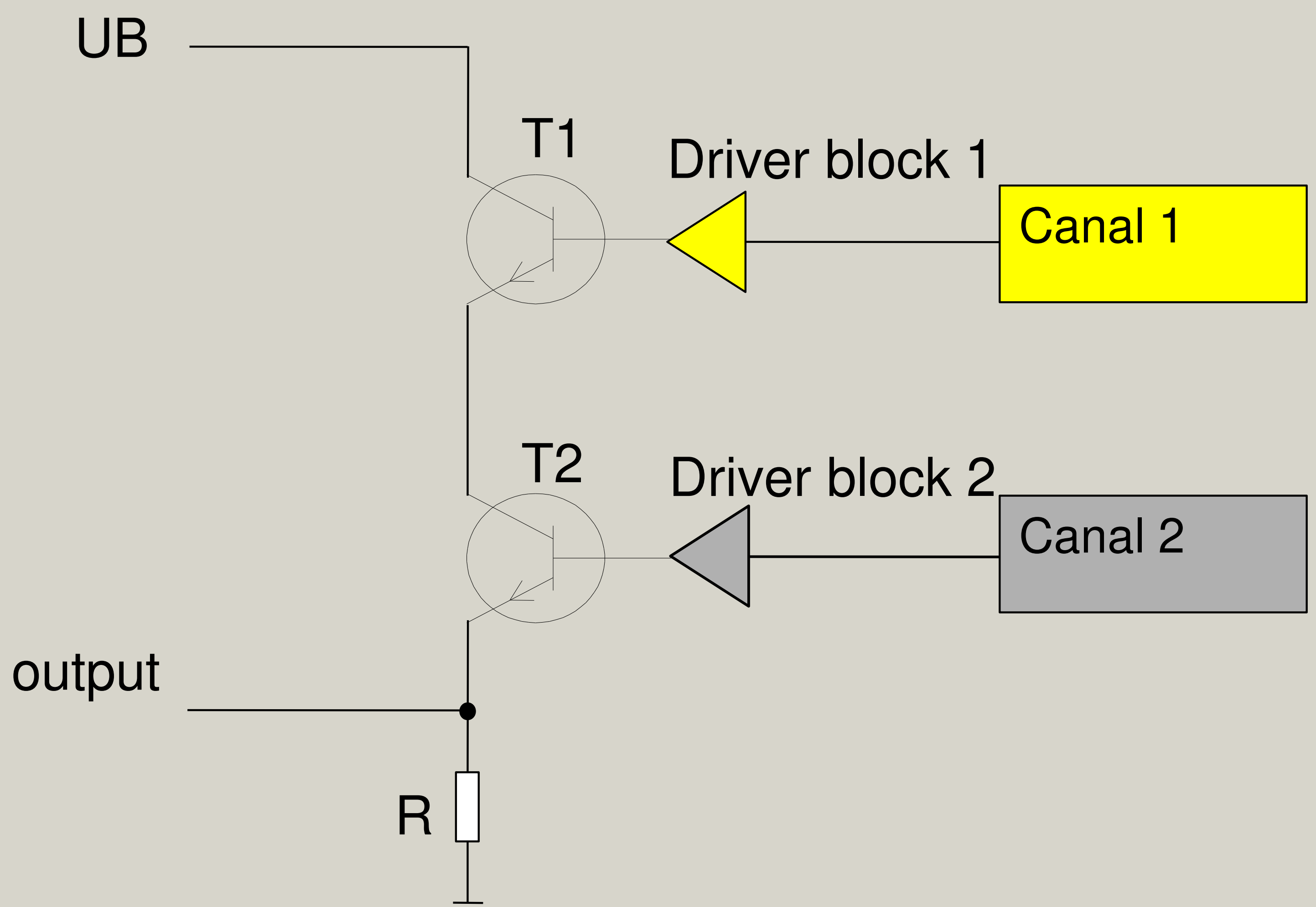
↓

Choose a measure in the chart

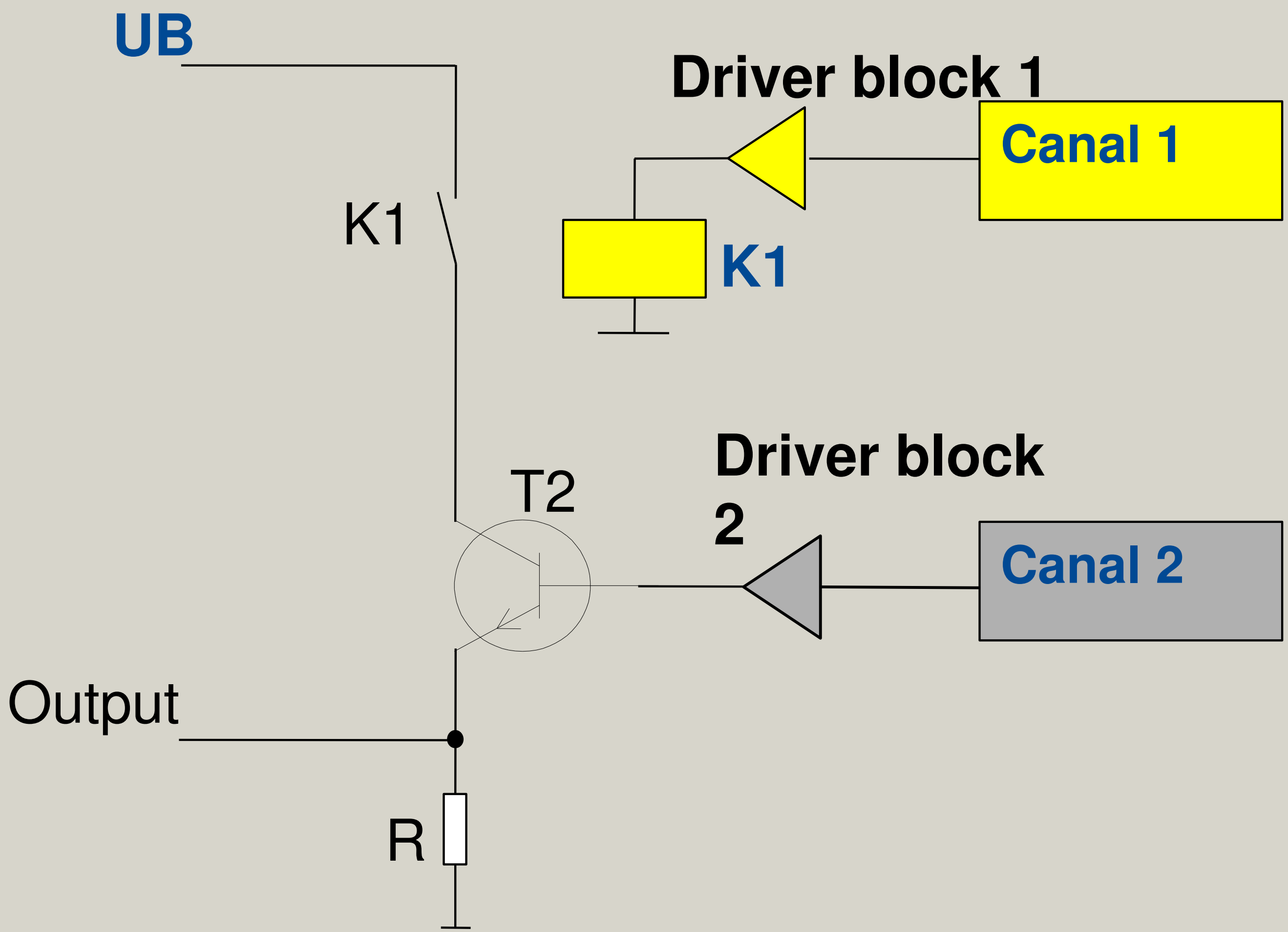
Technology
Architecture
Application
Environment



Measures against common cause failure



Measures against common cause failure



Measures against Common Cause Failure (CCF)

CCF: failures of different part through a common cause

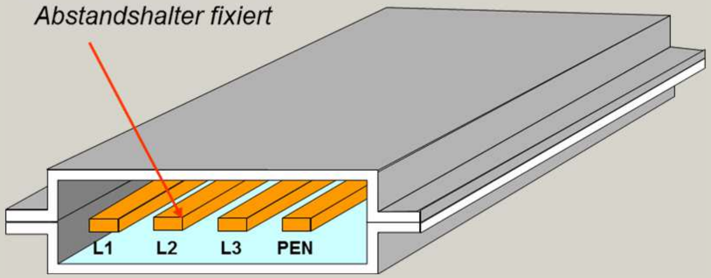
For redundant channel (Cat. 2, 3 and 4) are measures against CCF required in according to IEC 61508-6,

65 scores or better meets the requirements:

▪ Separation of signal path	15 Pt
▪ Diversity	20 Pt
▪ Design (e.g. protection against over-voltage, over-pressure etc)	15 Pt
▪ Components used are well-tried	5 Pt
▪ FMEA	5 Pt
▪ Competence/Training of the designer	5 Pt
▪ environmental - EMC	25 Pt
▪ Others (e.g. shock, temperature	5 Pt

Separation & segregation

- Proper design of cable trays, piping ways, wiring ducts
- Apply ISO 3313 for hydraulik equipment
- Apply IEC 60204-1 for electrical equipment
- Seperate power cables from signaling cables
- Apply mechanical shielding to piping
- Avoid kinking of hoses
- Use accessories offered by installation material providers

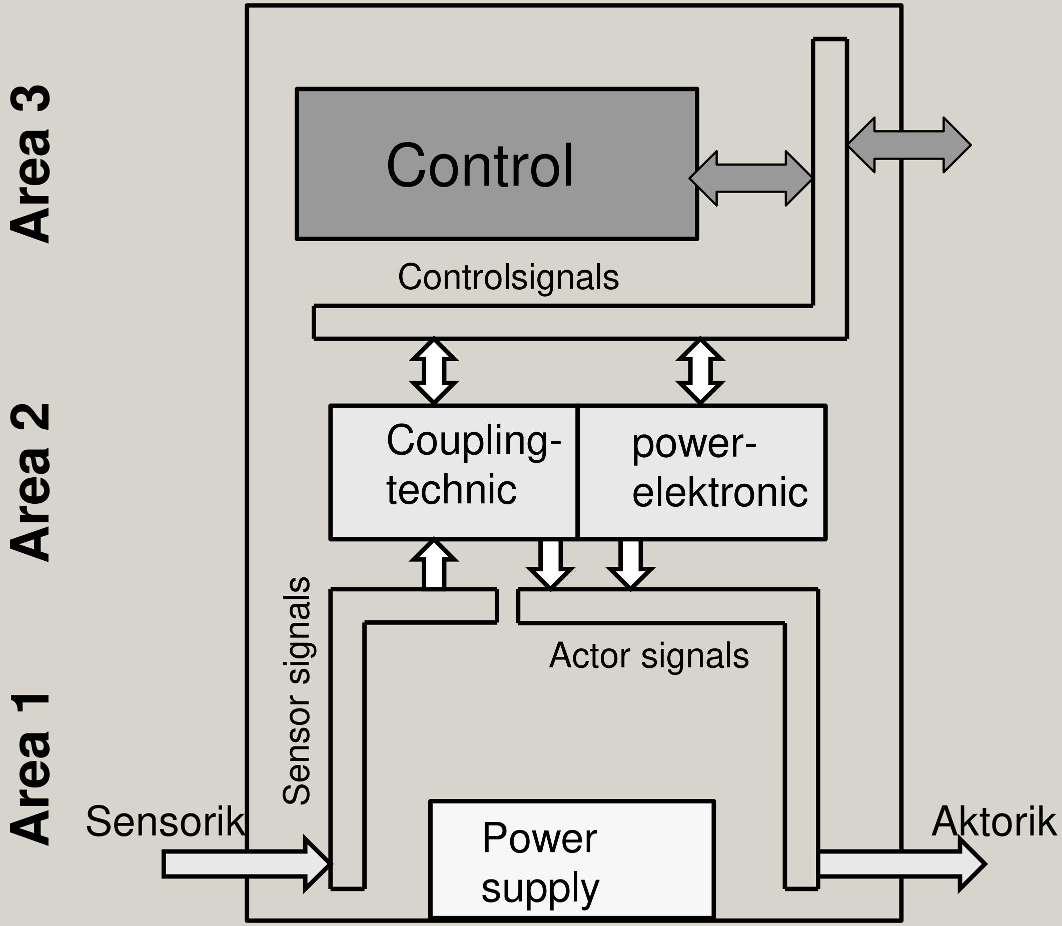


Diversity

- Use of different sensor technollogies
- Use of different modes of actuation
- Use componests of different maufactures but check of different!!
- Use different techniques for insulating energy

design with specified limits

Planung EMC areas within the cabinet



EMC Levels and limits

Risk assessment of safely related in accordance of EN ISO 13849-1:2023:

The following properties are determined:

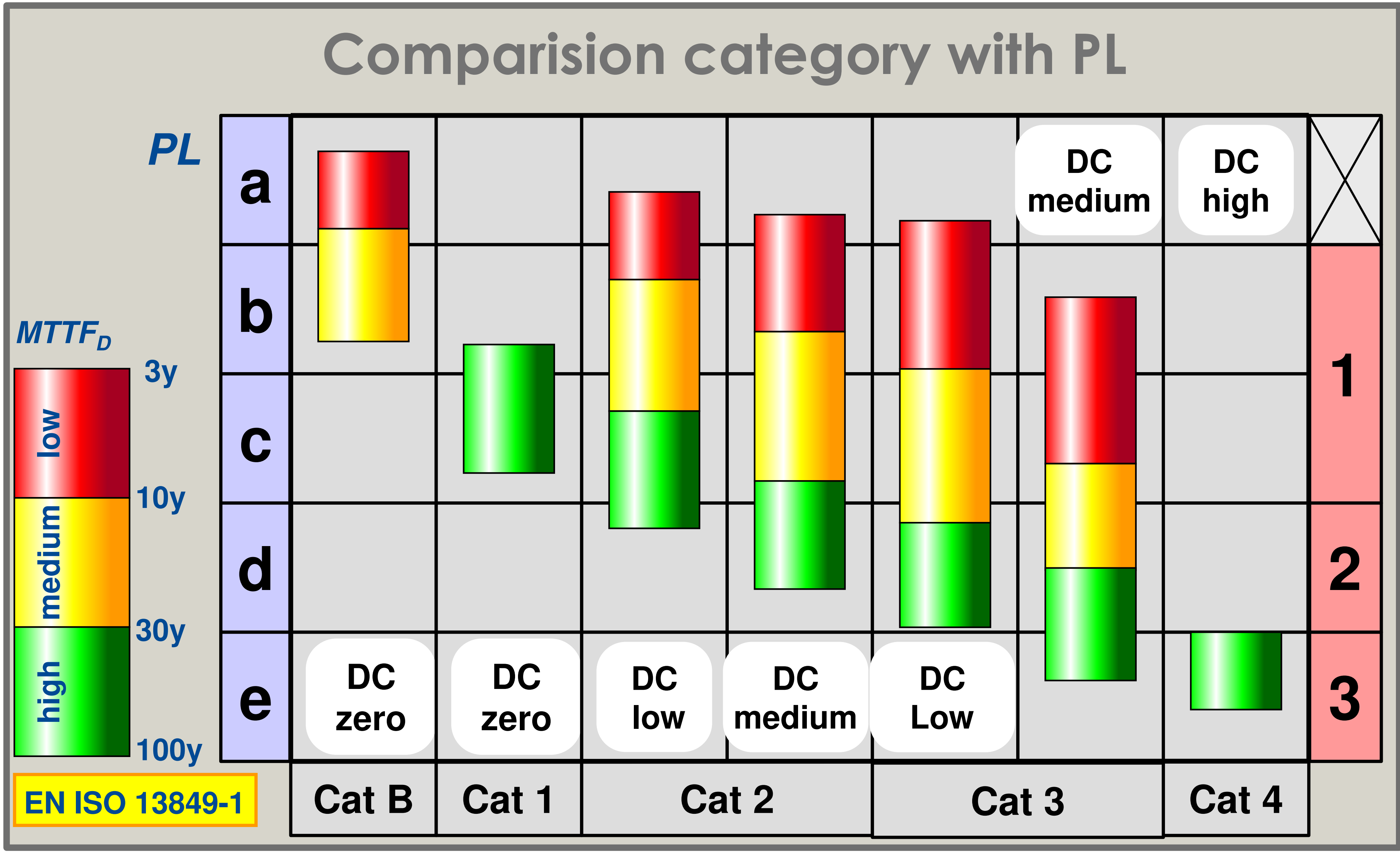
- Design of an logical diagram (**Designated Architecture**)
- Mean time to dangerous failure **$MTTF_D$**,
- Diagnostic Coverage **(DC)**,

failures of different items, resulting from a single event, where these failures are not consequences of each other (**CCF**): **As a last** Step the Performance Level PL („actual-Value“) for each Safety function has to be determinded.

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

8. Determination of PL



Average frequency of dangerous failure per hour)PFH) (1/h) and corresponding performence Level (PL)

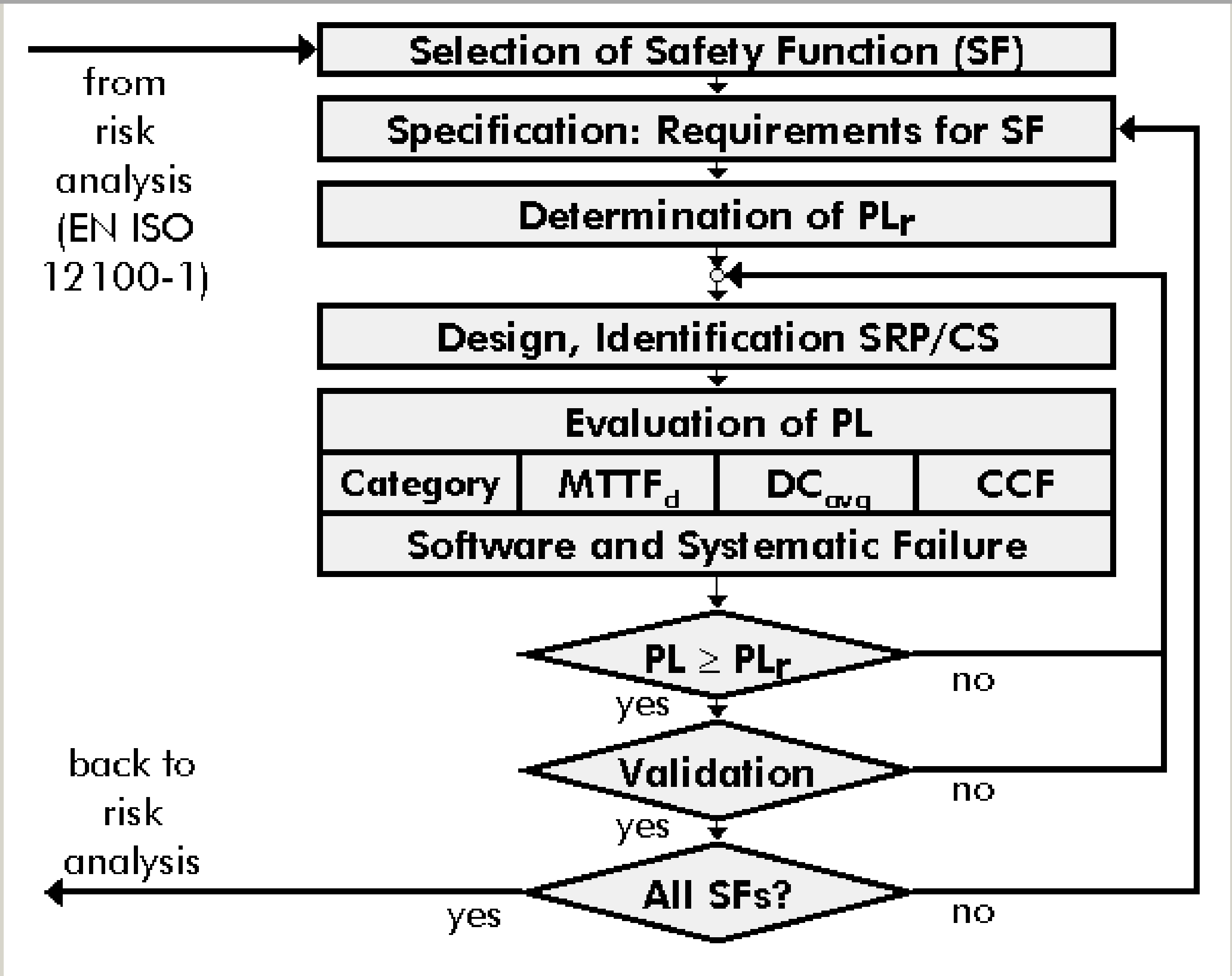
$MTTF_D$	$MTTF_D$ [a]	Cat.B DC_{avg} = no	Cat.1 DC_{avg} = no	Cat.2 DC_{avg} = low	Cat.2 DC_{avg} = low	Cat.3 DC_{avg} = low	Cat.3 DC_{avg} = low
medium	12	9,51 10^{-6} b		5,84 10^{-6} b	4,04 10^{-6} b	2,49 10^{-7} c	1,04 10^{-6} c
	13	8,78 10^{-6} b		5,33 10^{-6} b	3,64 10^{-6} b	2,23 10^{-7} c	9,21 10^{-7} d
	15	7,61 10^{-6} b		4,53 10^{-7} b	3,01 10^{-6} b	1,82 10^{-7} c	7,44 10^{-7} d
	16	7,13 10^{-6} b		4,21 10^{-7} b	2,77 10^{-6} b	1,67 10^{-7} c	6,76 10^{-7} d
	18	6,34 10^{-6} b		3,68 10^{-6} b	2,37 10^{-6} c	1,41 10^{-7} c	5,67 10^{-7} d
	20	5,71 10^{-6} b		3,26 10^{-6} c	2,06 10^{-6} c	1,22 10^{-7} c	4,85 10^{-7} d
	22	5,19 10^{-6} b		2,93 10^{-6} c	1,82 10^{-6} c	1, 07 10^{-7} c	4,21 10^{-7} d
	24	4,76 10^{-6} b		2,65 10^{-6} c	1,62 10^{-6} c	9,47 10^{-7} d	3,70 10^{-7} d
	27	4,23 10^{-6} b		2,32 10^{-6} c	1,39 10^{-6} c	8,04 10^{-7} d	3,10 10^{-7} d
high	30		3,80 10^{-6} b	2,06 10^{-6} c	1,21 10^{-6} c	6,94 10^{-7} d	2,65 10^{-7} d
	33		3,46 10^{-6} b	1,85 10^{-6} c	1,06 10^{-6} c	5,94 10^{-7} d	2,30 10^{-7} d
	36		3,17 10^{-6} b	1,67 10^{-6} c	9,39 10^{-7} d	5,16 10^{-7} d	2,01 10^{-7} d
	39		2,93 10^{-6} c	1,53 10^{-6} c	8,40 10^{-7} d	4,53 10^{-7} d	1,78 10^{-7} d
	43		2,65 10^{-6} c	1,37 10^{-6} c	7,34 10^{-7} d	3,87 10^{-7} d	1,54 10^{-7} d
	47		2,43 10^{-6} c	1,24 10^{-6} c	6,49 10^{-7} d	3,35 10^{-7} d	1,34 10^{-7} d
	51		2,24 10^{-6} c	1,13 10^{-6} c	5,80 10^{-7} d	2,93 10^{-7} d	1,19 10^{-7} d
	56		2,04 10^{-6} c	1,02 10^{-6} c	5,10 10^{-7} d	2,52 10^{-7} d	1,03 10^{-7} d
	62		1,84 10^{-6} c	9,06 10^{-7} d	4 ,43 10^{-7} d	2,13 10^{-7} d	8,84 10^{-8} e
	68		1,68 10^{-6} c	8,7 10^{-7} d	3,90 10^{-7} d	1,84 10^{-7} d	7,68 10^{-8} e
	75		1,52 10^{-6} c	7,31 10^{-7} d	3,40 10^{-7} d	1,57 10^{-7} d	6,62 10^{-8} e
	82		1,39 10^{-6} c	6,61 10^{-7} d	3,01 10^{-7} d	1,35 10^{-7} d	5,79 10^{-8} e
	91		1,25 10^{-6} c	6,88 10^{-7} d	2,61 10^{-7} d	1,14 10^{-7} d	4,94 10^{-8} e
	100		1,14 10^{-6} c	5,28 10^{-7} d	2,29 10^{-6} d	1,01 10^{-7} d	4,29 10^{-6} e

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

9. Verification of PL

Functional Safety needs Safety Functions

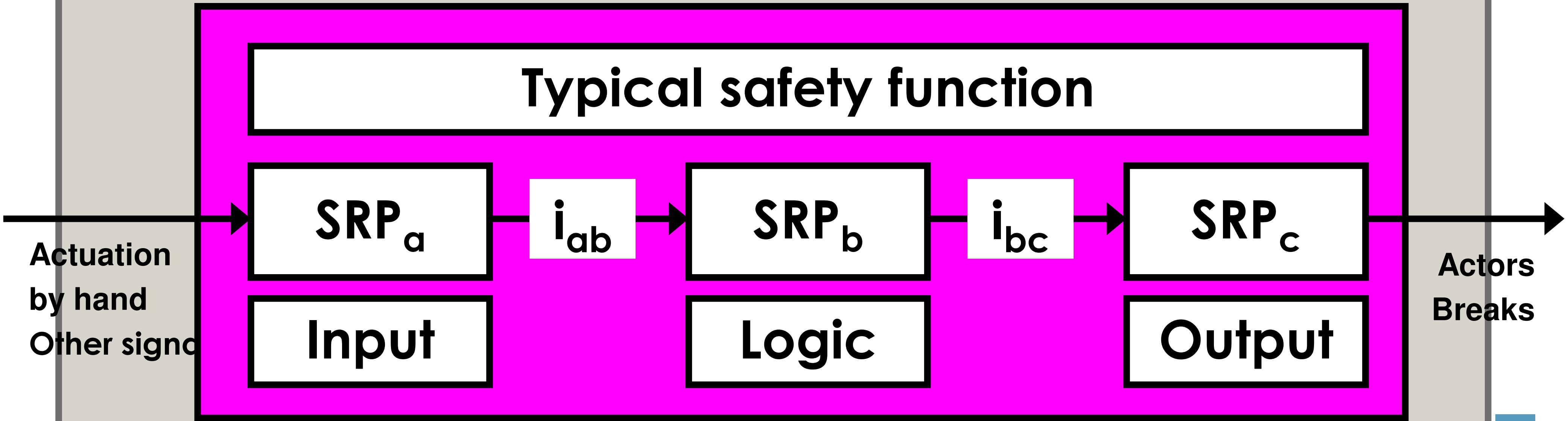


Observation of Failure, Exclussion of Failure

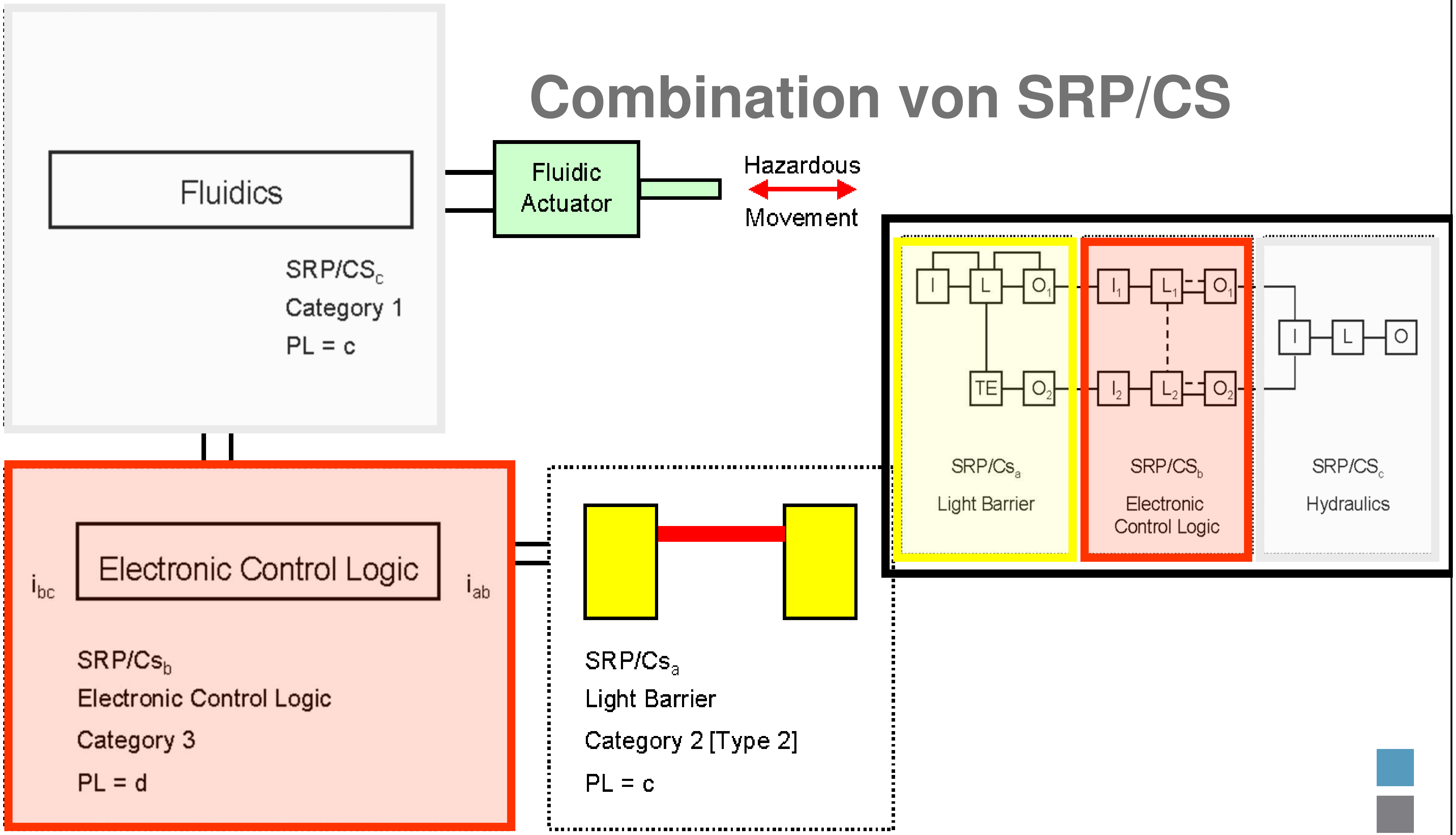
- as an exception only
- justification in detail is necessary
- listed failures in EN ISO 13849-2
- for new Components the application of FMEA is necessary as an evidence for exclusion of certains failure
- consecutive failure consider as single failure
- common cause failure consider as single failure

Identification of SRP/CS

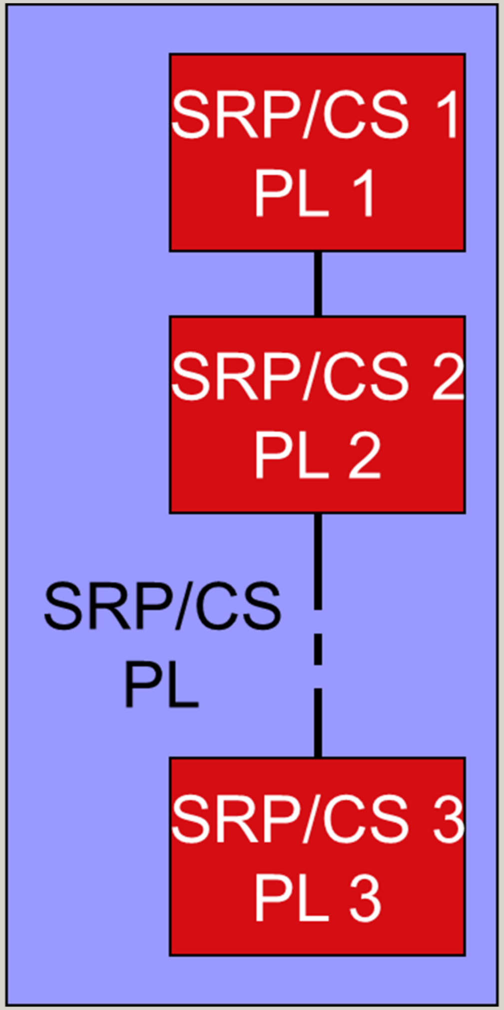
**SRP/CS: Parts of control system what generate
Input signals to safety related output signals**



Combination von SRP/CS



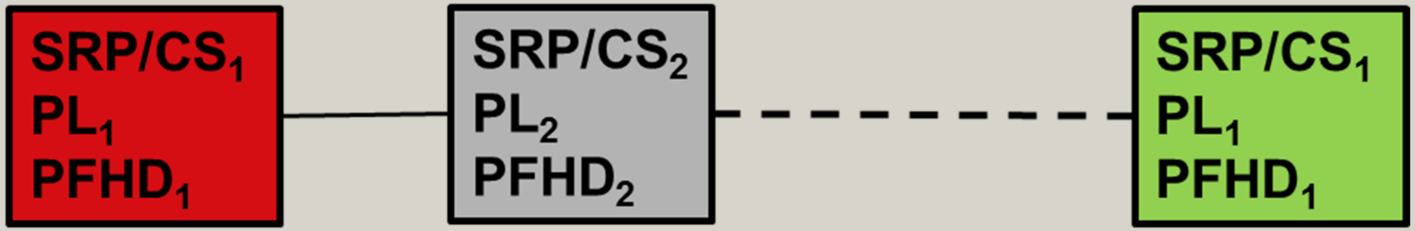
Serial combination of SRP/CS



PL low	N low		PL
a	> 3	= >	none
	≤ 3	= >	a
b	> 2	= >	a
	≤ 2	= >	b
c	> 2	= >	b
	≤ 2	= >	c
d	> 3	= >	c
	≤ 3	= >	d
e	> 3	= >	d
	≤ 3	= >	e

Functional safety ISO 13849-1, Dipl.-Ing. Klaus-Dieter Becker

Serial Combination of SRP/CS

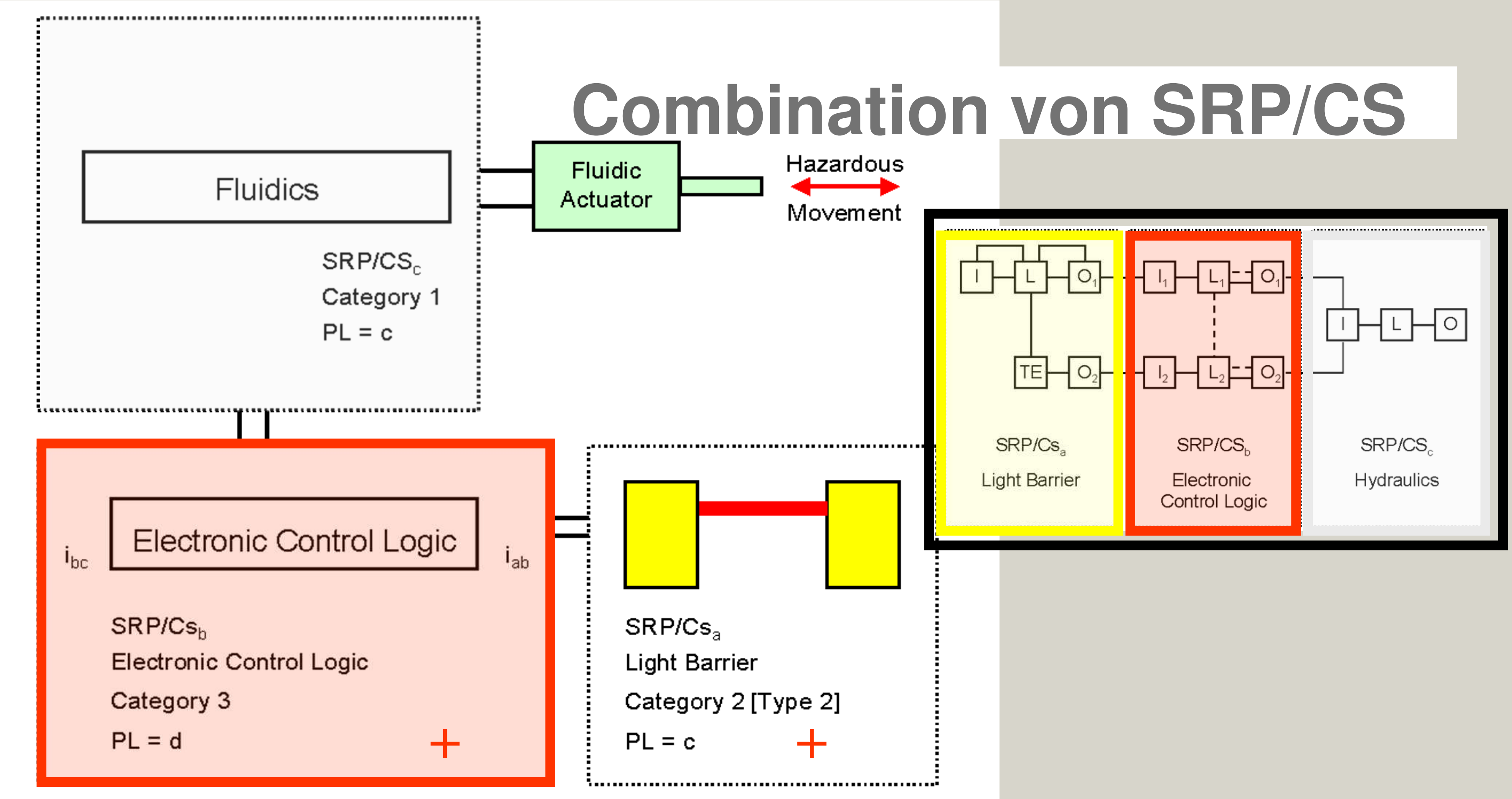


$$\sum_{i=1}^{i=n} PFH_{Di} = PFH_{D1} + \; .... \; + PFH_{Dn}$$

N = number of all involved safety functions of the sub systems

PFH_i = average probability of an dangerous fault per hour of the each Subsystem

Combination von SRP/CS



$1{,}21\times10^{-6}$ $2{,}65\times10^{-7}$ $1{,}14\times10^{-6} = 2{,}62\times10^{-6}$

issa

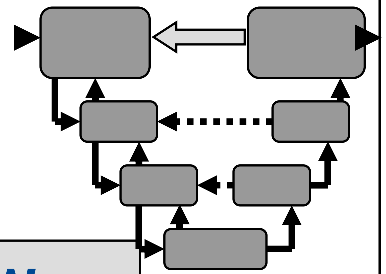
Promoting and Developing
Social Security Worldwide.

Average frequency of dangerous failure per hour)PFH) (1/h) and corresponding performence Level (PL)

$MTTF_D$	$MTTF_D$ [a]	Cat.B DC_{avg} = no	Cat.1 DC_{avg} = no	Cat.2 DC_{avg} = low	Cat.2 DC_{avg} = low	Cat.3 DC_{avg} = low	Cat.3 DC_{avg} = low
medium	12	9,51 10^{-6} b		5,84 10^{-6} b	4,04 10^{-6} b	2,49 10^{-7} c	1,04 10^{-6} c
	13	8,78 10^{-6} b		5,33 10^{-6} b	3,64 10^{-6} b	2,23 10^{-7} c	9,21 10^{-7} d
	15	7,61 10^{-6} b		4,53 10^{-7} b	3,01 10^{-6} b	1,82 10^{-7} c	7,44 10^{-7} d
	16	7,13 10^{-6} b		4,21 10^{-7} b	2,77 10^{-6} b	1,67 10^{-7} c	6,76 10^{-7} d
	18	6,34 10^{-6} b		3,68 10^{-6} b	2,37 10^{-6} c	1,41 10^{-7} c	5,67 10^{-7} d
	20	5,71 10^{-6} b		3,26 10^{-6} c	2,06 10^{-6} c	1,22 10^{-7} c	4,85 10^{-7} d
	22	5,19 10^{-6} b		2,93 10^{-6} c	1,82 10^{-6} c	1, 07 10^{-7} c	4,21 10^{-7} d
	24	4,76 10^{-6} b		2,65 10^{-6} c	1,62 10^{-6} c	9,47 10^{-7} d	3,70 10^{-7} d
	27	4,23 10^{-6} b		2,32 10^{-6} c	1,39 10^{-6} c	8,04 10^{-7} d	3,10 10^{-7} d
high	30		3,80 10^{-6} b	2,06 10^{-6} c	1,21 10^{-6} c	6,94 10^{-7} d	2,65 10^{-7} d
	33		3,46 10^{-6} b	1,85 10^{-6} c	1,06 10^{-6} c	5,94 10^{-7} d	2,30 10^{-7} d
	36		3,17 10^{-6} b	1,67 10^{-6} c	9,39 10^{-7} d	5,16 10^{-7} d	2,01 10^{-7} d
	39		2,93 10^{-6} c	1,53 10^{-6} c	8,40 10^{-7} d	4,53 10^{-7} d	1,78 10^{-7} d
	43		2,65 10^{-6} c	1,37 10^{-6} c	7,34 10^{-7} d	3,87 10^{-7} d	1,54 10^{-7} d
	47		2,43 10^{-6} c	1,24 10^{-6} c	6,49 10^{-7} d	3,35 10^{-7} d	1,34 10^{-7} d
	51		2,24 10^{-6} c	1,13 10^{-6} c	5,80 10^{-7} d	2,93 10^{-7} d	1,19 10^{-7} d
	56		2,04 10^{-6} c	1,02 10^{-6} c	5,10 10^{-7} d	2,52 10^{-7} d	1,03 10^{-7} d
	62		1,84 10^{-6} c	9,06 10^{-7} d	4 ,43 10^{-7} d	2,13 10^{-7} d	8,84 10^{-8} e
	68		1,68 10^{-6} c	8,7 10^{-7} d	3,90 10^{-7} d	1,84 10^{-7} d	7,68 10^{-8} e
	75		1,52 10^{-6} c	7,31 10^{-7} d	3,40 10^{-7} d	1,57 10^{-7} d	6,62 10^{-8} e
	82		1,39 10^{-6} c	6,61 10^{-7} d	3,01 10^{-7} d	1,35 10^{-7} d	5,79 10^{-8} e
	91		1,25 10^{-6} c	6,88 10^{-7} d	2,61 10^{-7} d	1,14 10^{-7} d	4,94 10^{-8} e
	100		1,14 10^{-6} c	5,28 10^{-7} d	2,29 10^{-6} d	1,01 10^{-7} d	4,29 10^{-6} e

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation



10. Software

readable, understandable, testable & maintainable SW:
simplified V-model for lifecycle

Safety Related Embedded Software (SRESW)

PL a, b: basic → + → PL c, d: additional → + → PL e: diversity or 61508-3 (SIL 3)

Safety Related Application Software (SRASW)

PL a, b: basic → + → PL c, d and e: additional, increasing effectiveness

software based parameterisation

Schritt 10: Softwareanforderungen

application software (SRA-SW) z.B.
- Programming methods for PLC:
- Parameterization devices

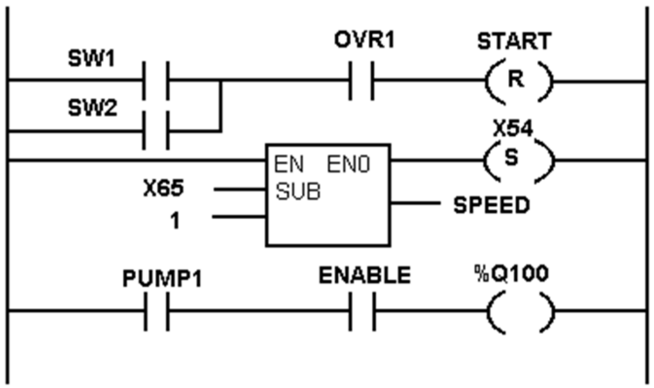
Embedded Software (SRE-SW) z.B.
- system software
- Operating system of a PLC
- Firmware

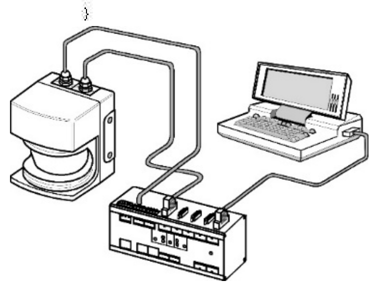
Programming methods for PLC:
- ladder diagram)
- functional block diagram
- Sequential function chart

```
public static void main(String[] args) {
    DataRecord inst = new DataRecord();
    inst.setVisible(true);
}

private DataRecord() {
    super();
    // Create a timer.
    timer = new Timer(ONE_SECOND, new ActionListener() {
        public void actionPerformed(ActionEvent evt) {
            jProgressBar1.setValue(value);
            if (value == 180) {
                //Toolkit.getDefaultToolkit().beep();
                timer.stop();
                jButton1.setEnabled(true);
                setCursor(null); //turn off the waitcursor
                jProgressBar1.setValue(jProgressBar1.getMinimum());
            }
        }
    });
    initGUI();
}

private void initGUI() {
    try {
        this.setLocation(new java.awt.Point(250, 200));
        this.setSize(428, 305);
        this.addWindowListener(new WindowAdapter() {
            public void windowClosing(WindowEvent evt) {
                shutdown();
            }
```





Parameterization Laserscanner

EN ISO 13849-1:2023

Prinziples of SW-requirements

- For PL a to PL e and Embedded SW as well as Application SW
- Based of generell akzepted SW-design methods
- … as prevention of faults and defensive coding
- Taken to account, that faults will be done during the specification and the design
- The Prinziples of SW-Standard 61508-3 take as a basis…
- … but not too much sophisticated
- As far as possible without refernces to 61508-3
- understandable, applicable und usable

Steps to performance level

1. Specification of the safety functions
2. Determination of the required PL (PL_r)
3. Category selection for each Subsystem
4. Modeling the safety-related block diagram
5. Determination of reliability at component & structure level
6. Determination of the diagnostic coverage DC
7. Consideration of the CCF
8. Determination of PL (table in Appendix K
9. Verification whether the achieved PL ≥ PLr
10. Implementation of software requirements according to EN ISO 13849-1 paragraph 7
11. Measures to avoid systematic faults
12. Validation

12. Valdation of PL

The proof that each safety-related part of the control system and each of its executed safety functions comply with the requirements of EN ISO 13849-1 shall begin as early as possible during the development, in order to detect and eliminate faults in time.

Operating instruction

The manufacturer has the duty to inform the user about:

- Limits of SRP/CS and excluded failure
- precisely description of interfaces to SRP/CS
- Restriction of operability (incl. ambient conditions)
- Reaction time, optical and acoustic signalling devices
- Muting and cancellation (override) of safety function by hand
- Type of control system
- maintenance, check-lists
- ...

Technical File

The Designer (Developer) has to document:

- Safety function (SF) and their characteristic
- precise beginning and end of the SF
- permissible field conditions
- Performance Level PL, decidede category
- reliability-parameter ($MTTF_D$, DC, CCF, operation time)
- Measures against systematic failure
- Observation of failure,
  justification for all excluded failure

scope

Safety related parts of control systems (machines))

Independent of the technology

- **electro mechanic**
- **electronic**
- **Programmable electronic**
- **Hydraulic**
- **Pneumatic**
- **Mechanic**

Conclusion: EN ISO 13849 ...

1. Determination of the required Performance Levels
2. design of the safety related block diagram
3. Determination of Category for each subsystems
4. Calculating or evaluating $MTTF_D$ values for single components
5. Determination of the diagnostic coverage
6. Considering of CCF
7. determSpecification of each safety function
8. ination of PL (Table in Annex K)
9. Verification if $PL>=PL_r$
10. Software requirements according to EN ISO 13849-1 para 4.6
11. considering of the prevention of systematic failures
12. Validation

"Everything which is merely possible, is possibly wrong."
René Descartes (1596 – 1650

"The first rule a mathematician has to follow is to be exact. The second rule is to be clear and precise and as far as possible simple." *Lazare Nicolas Marguerite Carnot (1753 – 1823)*

"There are things which seem to be unbelievable to those who have not studied mathematics."
Archimedes (ca. 285 – 212 v. Chr.)

Thank you very much for your attention !

Wish you much success

in integration of safety in design and marketing of machines
in European Union