issa

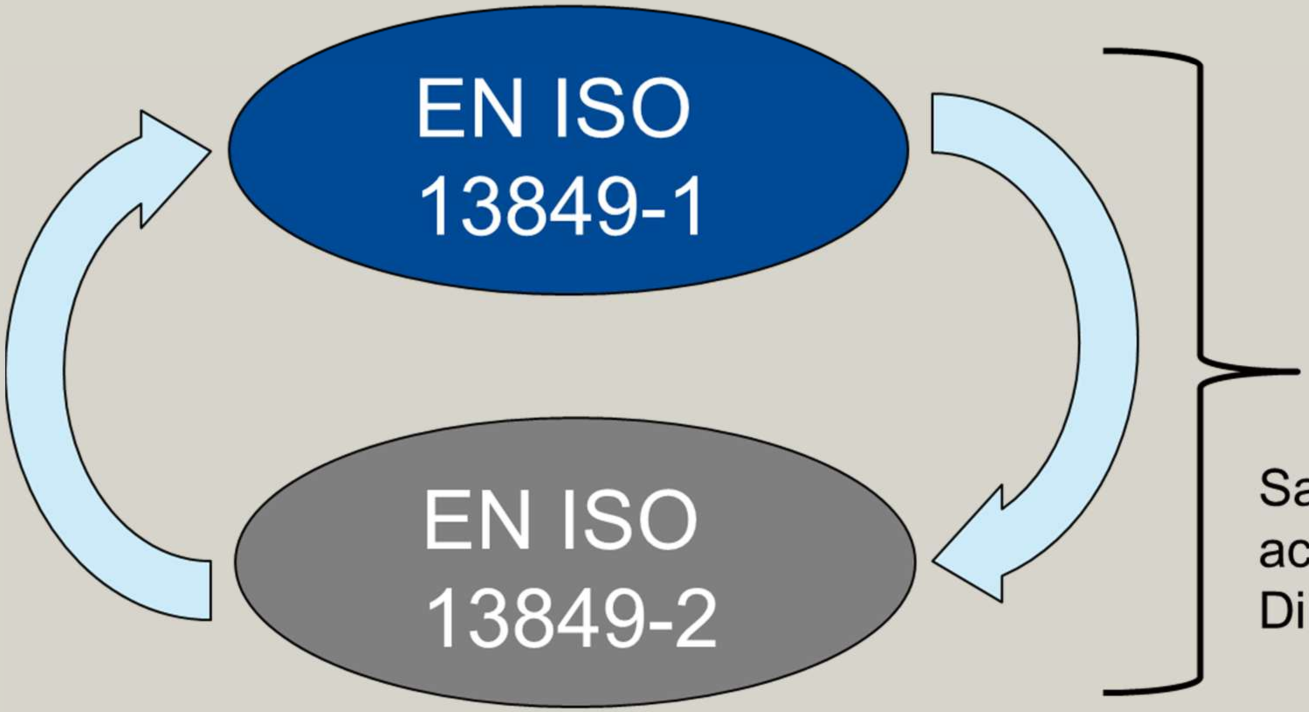
Promoting and Developing
Social Security Worldwide.

Safety-related parts of control systems
ISO 13849-2
Validation
Bangalore, India
Pune, India

www.issa.int

Functional safety, Dipl.-Ing. Klaus-Dieter Becker

The application of EN ISO 13849-1 only is not sufficient



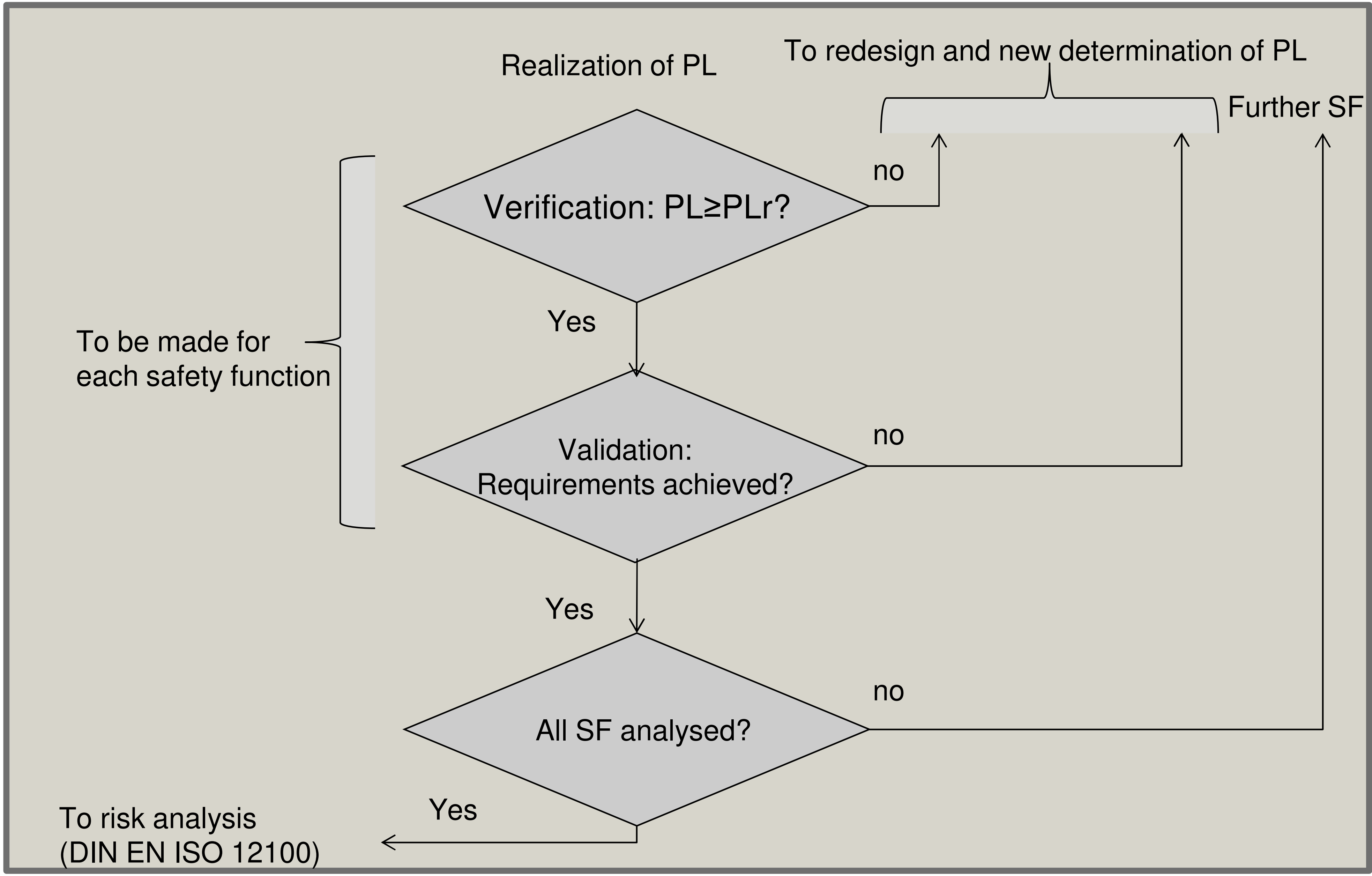
Target !

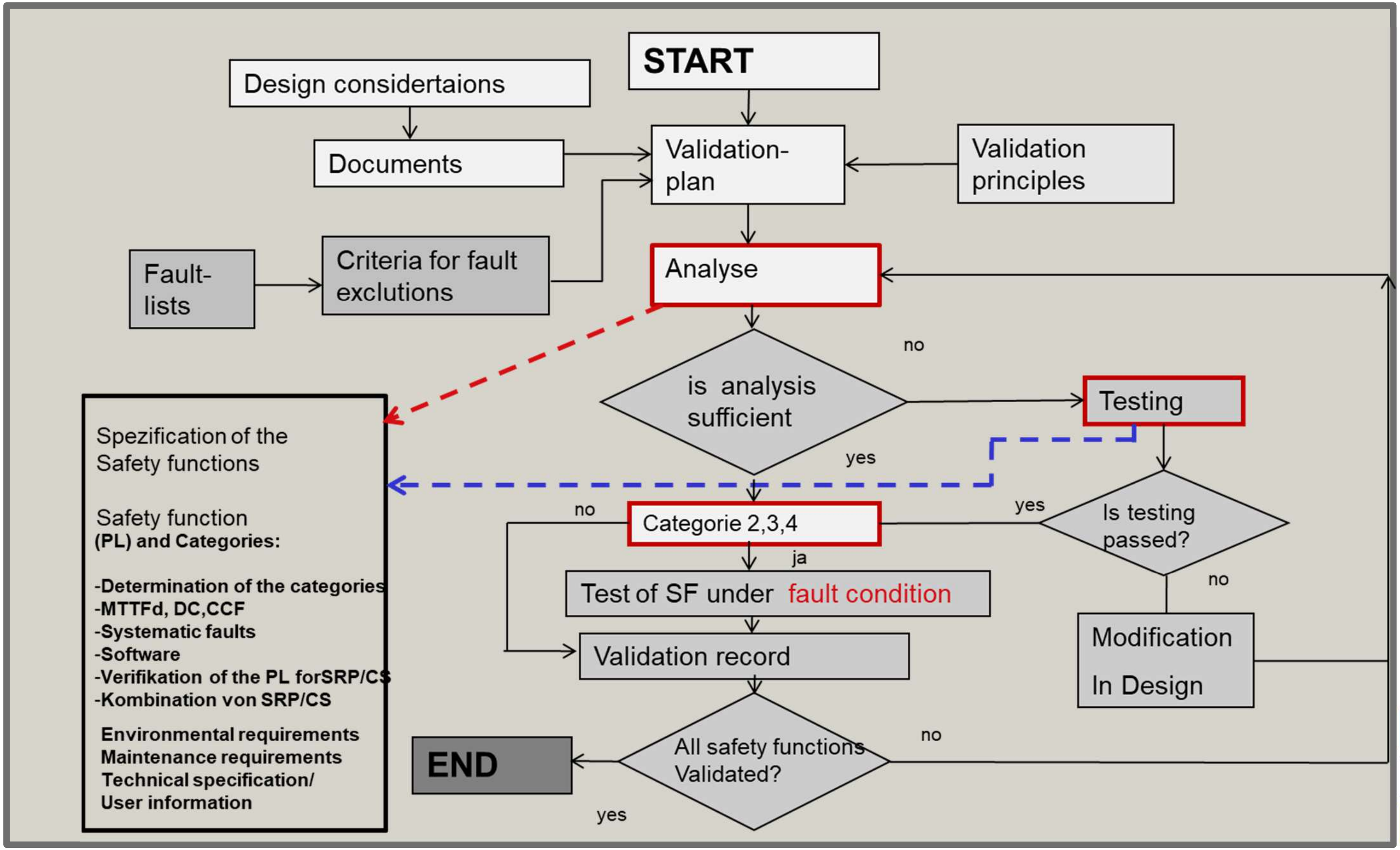
Safe control systems according Machinery Directive

Validation

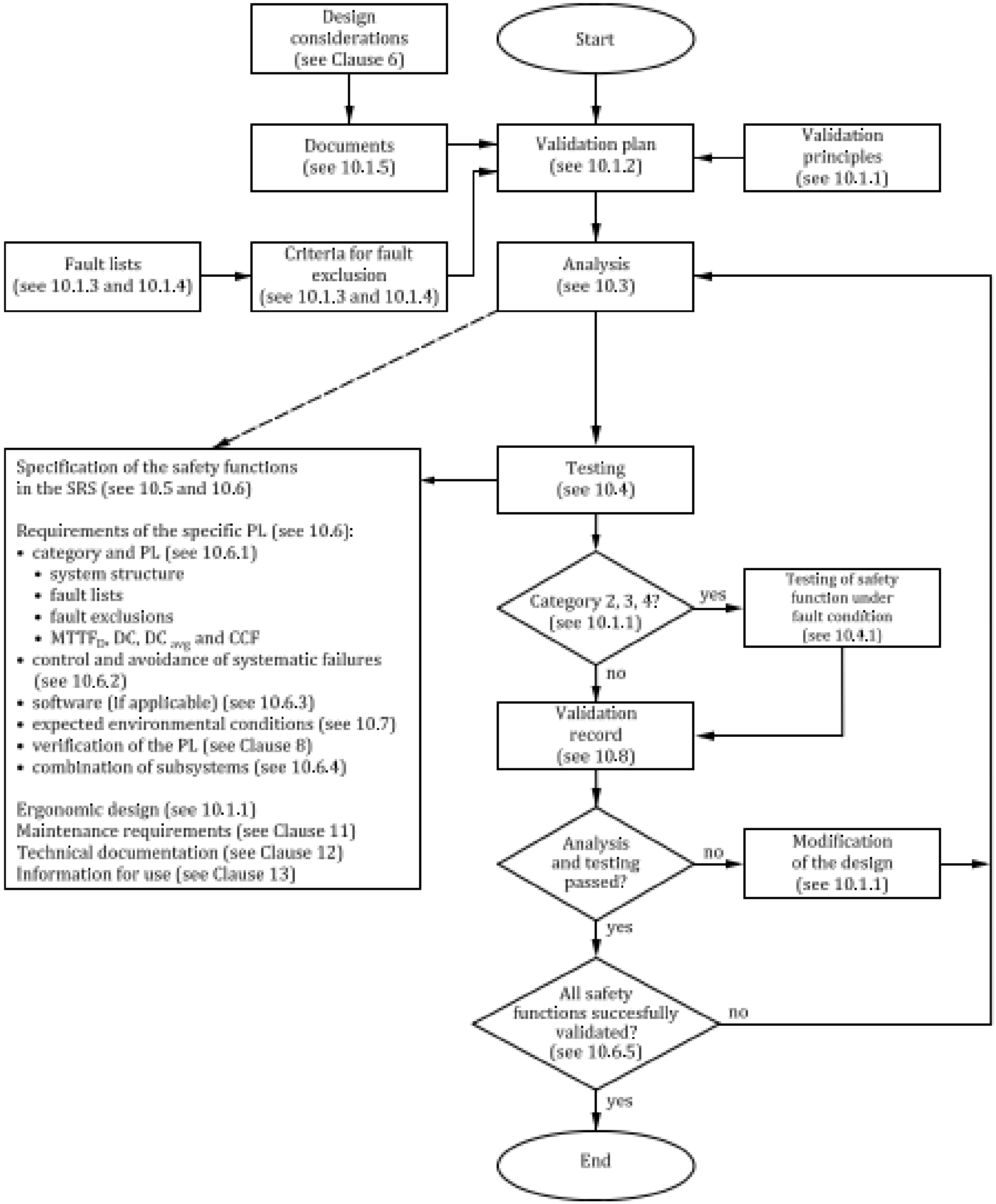
Verification and validation are intended to assure conformity of the design of the SRP/CS with the Machinery Directive.

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.


Realization of PL
To redesign and new determination of PL
Further SF
Verification: PL≥PLr?
no
Yes
To be made for
each safety function
Validation:
Requirements achieved?
no
Yes
All SF analysed?
no
Yes
To risk analysis
(DIN EN ISO 12100)


START
Design considertaions
Documents
Validation-
plan
Validation
principles
Fault-
lists
Criteria for fault
exclutions
Analyse
no
is analysis
sufficient
Testing
yes
Spezification of the
Safety functions
Safety function
(PL) and Categories:
-Determination of the categories
-MTTFd, DC,CCF
-Systematic faults
-Software
-Verifikation of the PL forSRP/CS
-Kombination von SRP/CS
Environmental requirements
Maintenance requirements
Technical specification/
User information
no
Categorie 2,3,4
yes
Is testing
passed?
ja
Test of SF under fault condition
no
Modification
In Design
Validation record
no
END
All safety functions
Validated?
yes

DIN EN 60204-1: 2007-06
Electrical equipment of machines



EN ISO 13849-2: Validation

- by analysis
- by testing
- of safety functions
- of category
- of environmental conditions
- of maintainance requirements

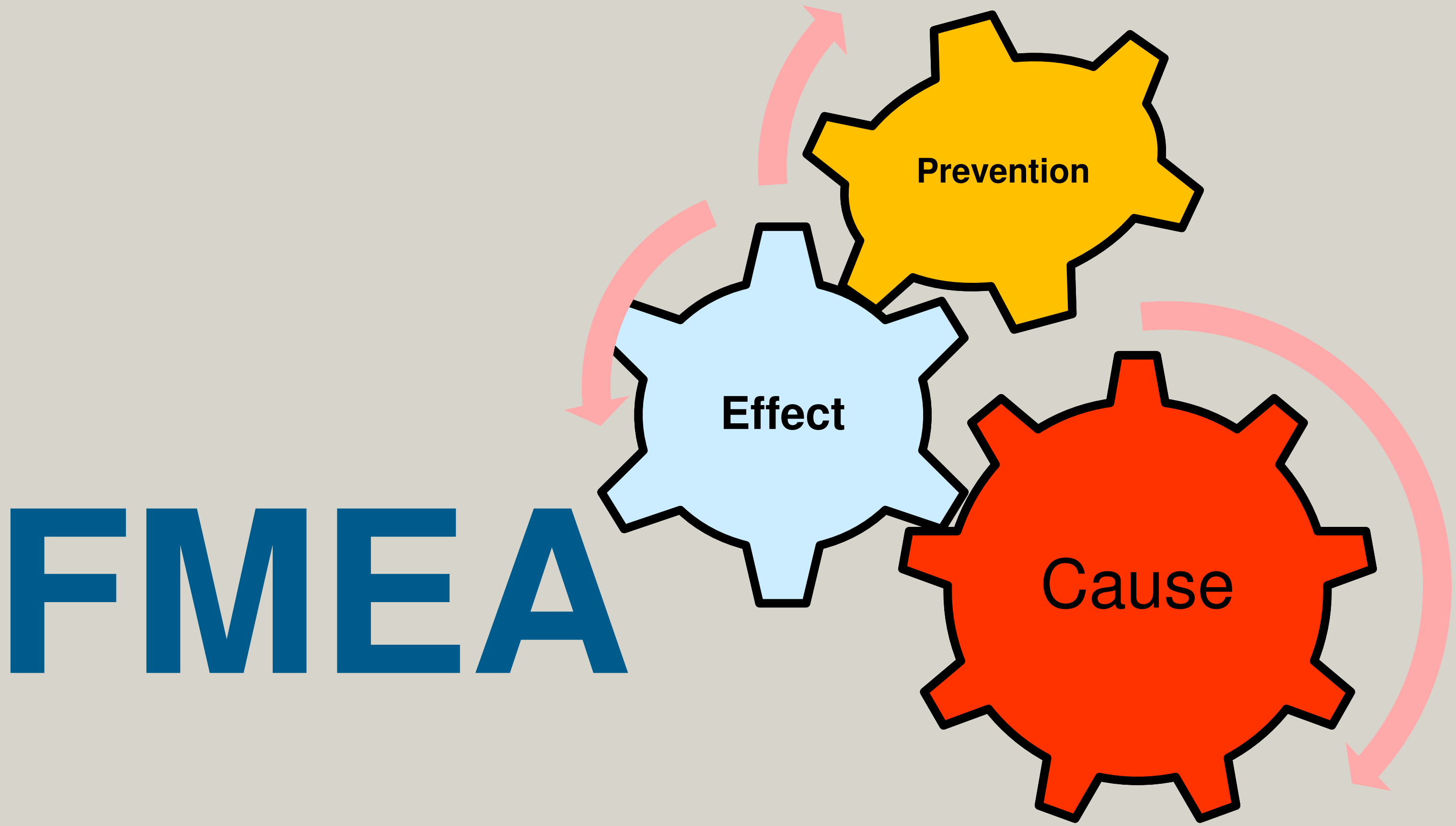
paragraph 4 to 9

- Mechanical systems
- Pneumatic systems
- Hydraulic systems
- Electric systems

Annex A to D

Basic safety principles
Well tried components
Well tried principles
Fault lists

Analysis and Validation Tool



FMEA: Fehler Mode Effect Analysis

Procedure for detecting mode and way how components and systems can fail and not provide the desired function anymore.

- Kinds of failure
- Effects of failure
- Causes of failure

Target: Prevention and reduction of failures

FMEA : Application

When: In the development, the production and during operation

Why: Selection of draft alternatives
Consideration of all kinds of failure and their effects

Target: Basis for planing the verification and maintenance
Basis for reliability analysis

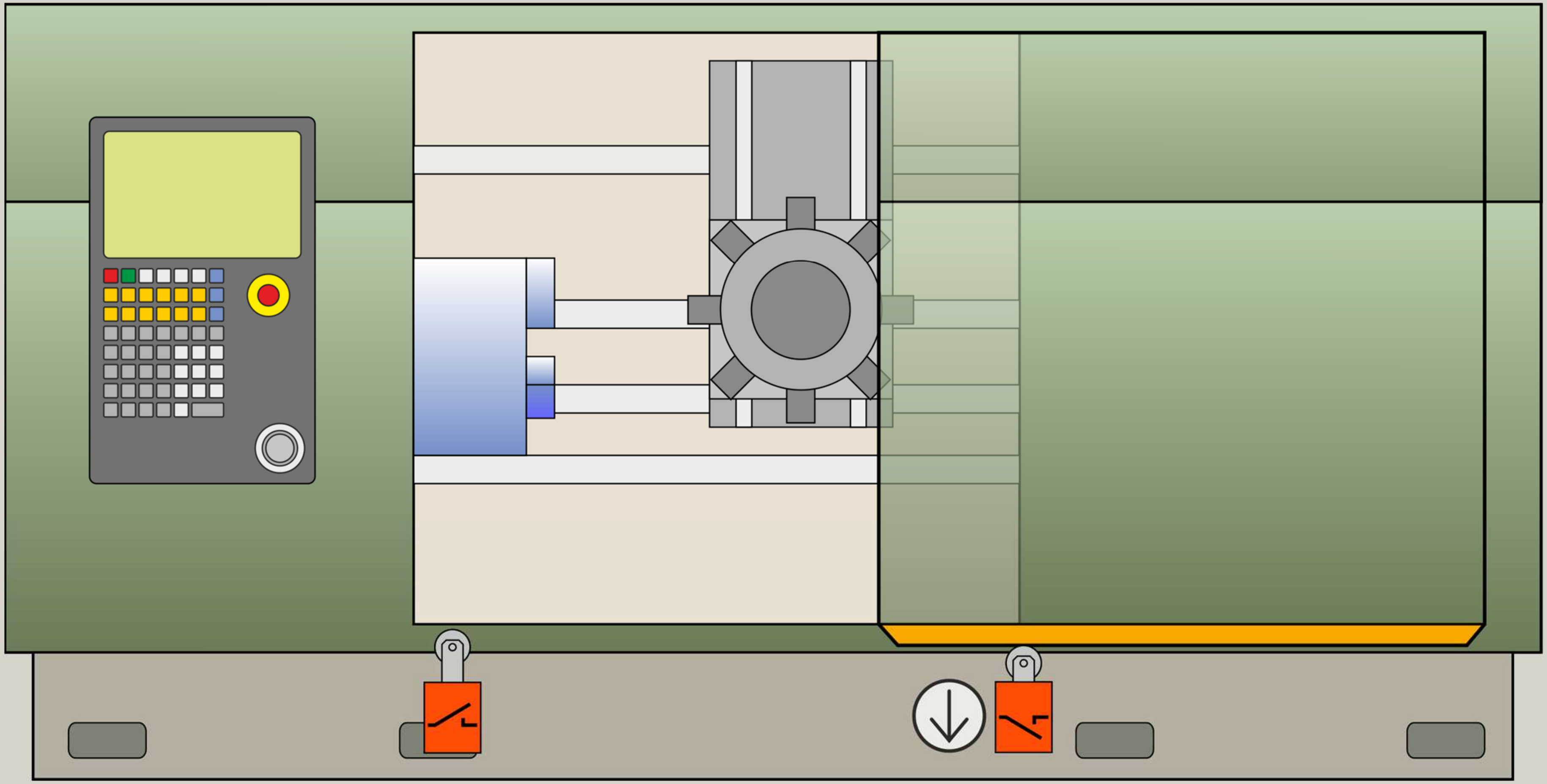
FMEA: Fehler Mode Effect Analysis

- Understand the system
- Divide the system in components
- Analysis of each component
  - How can the component fail?
  - Why can the component fail?
  - What are the consequences of the failure?
  - Follows the failure a safe or an unsafe direction?
  - Is the failure detected?
  - Whereby can the failure be prevented?

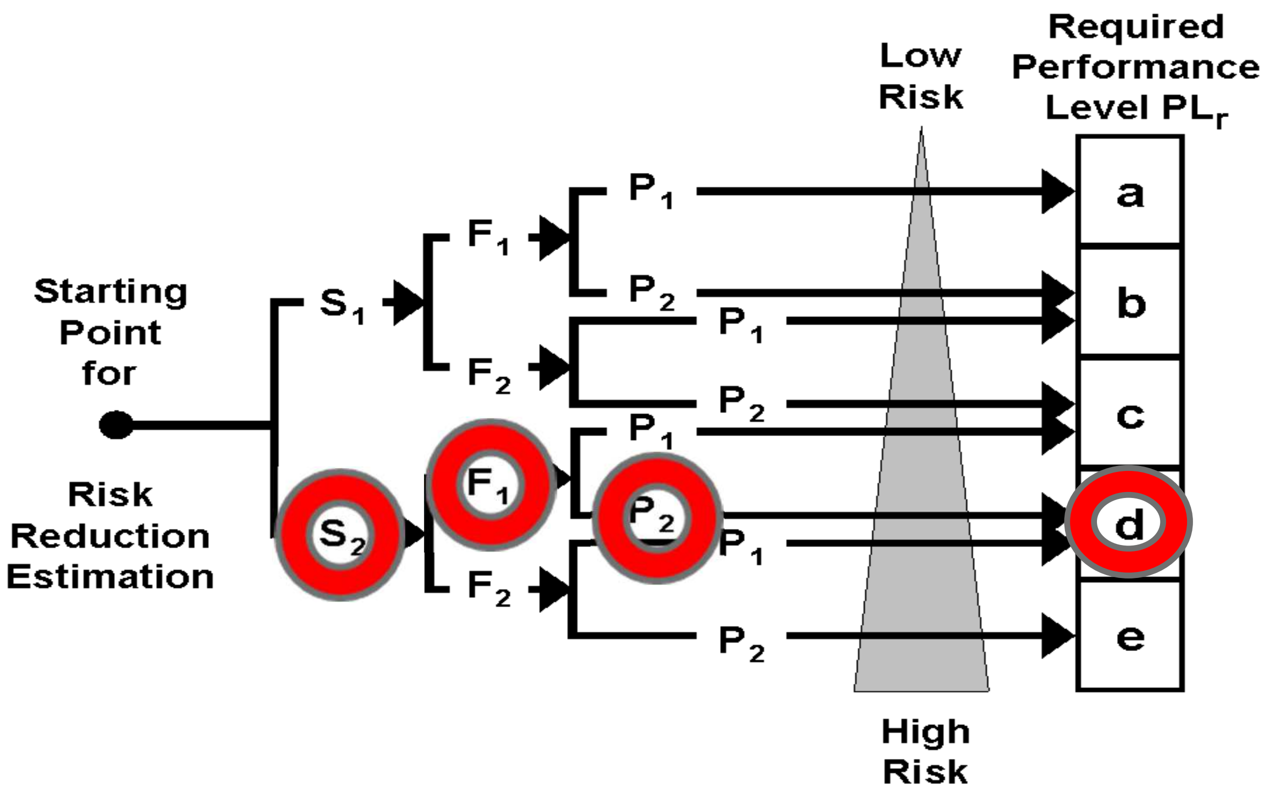
Validation of the safety-related parts of the hardware and software functions

1. Description of the safety mechanisms
2. Fixing the fault reactions
3. Hardware FMEA
   - Theoretical
   - Practical
4. Software FMEA
   - Theoretical
   - Practical

example:



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

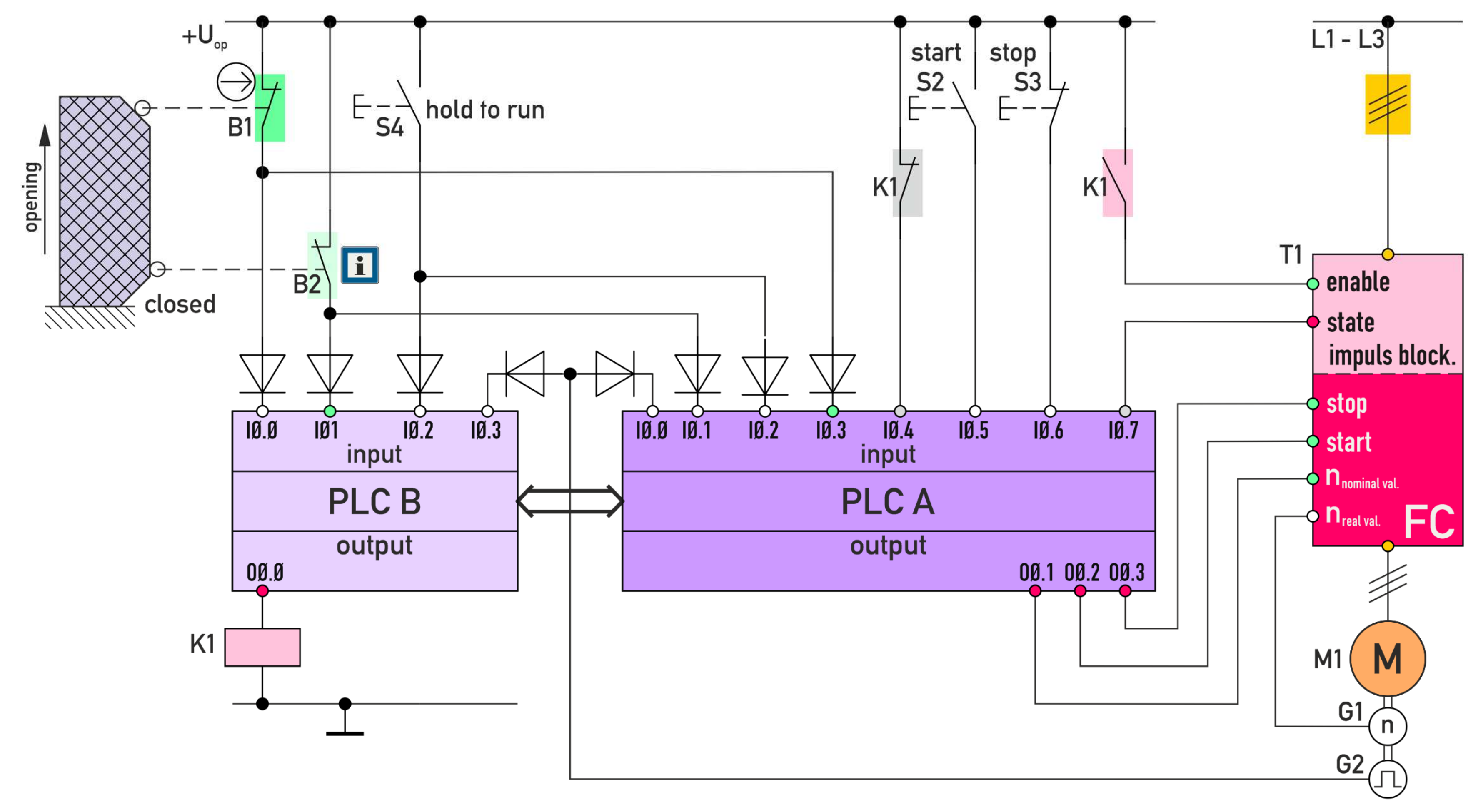
P = Possibility of avoiding or limiting the hazard

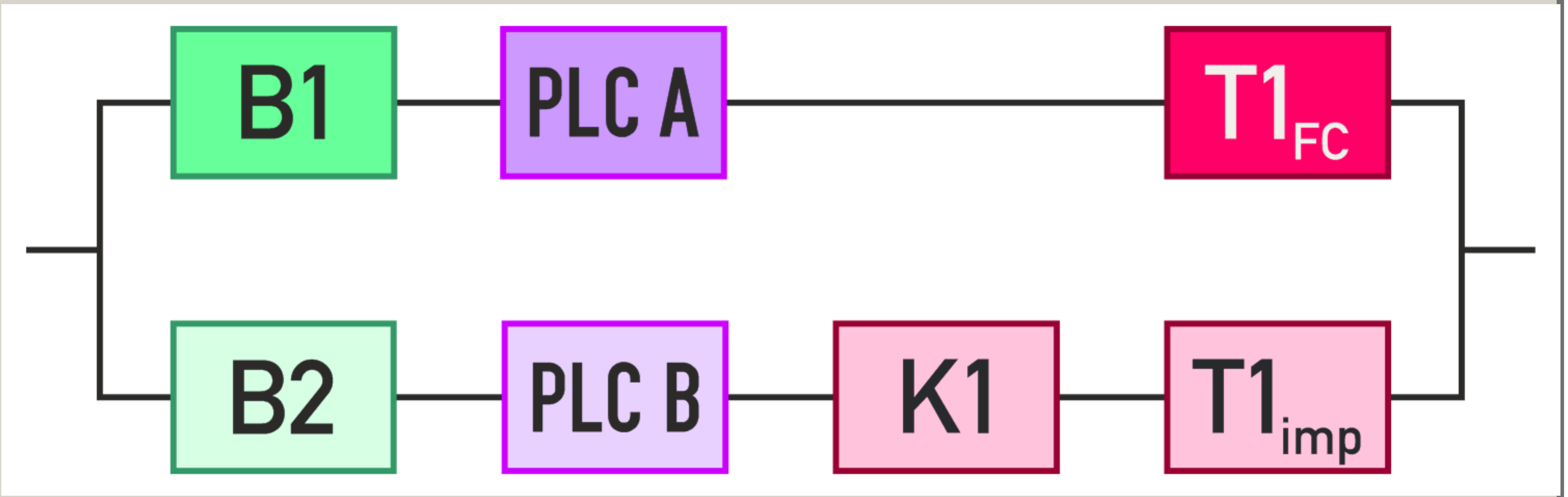
P1 = possible under certain circumstances

P2 = scarcely possible

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

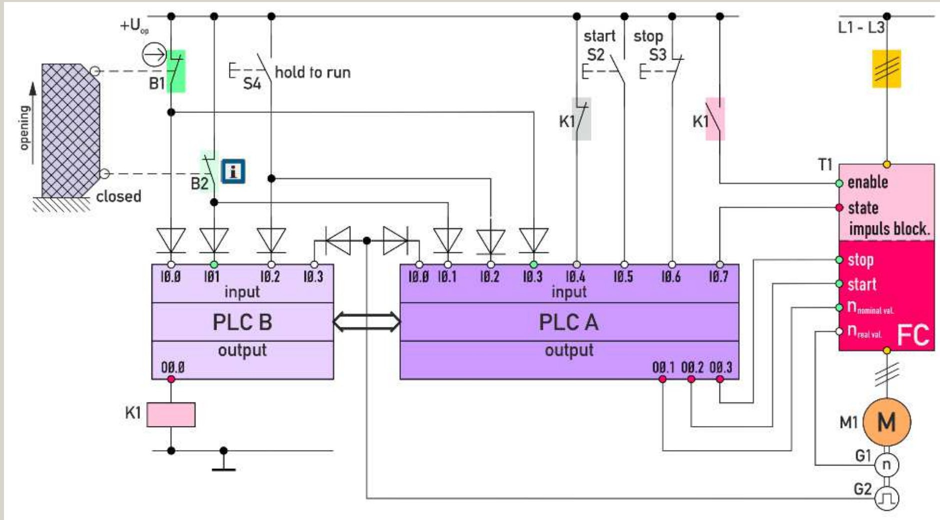
Automatic mounting machine, electrical diagram

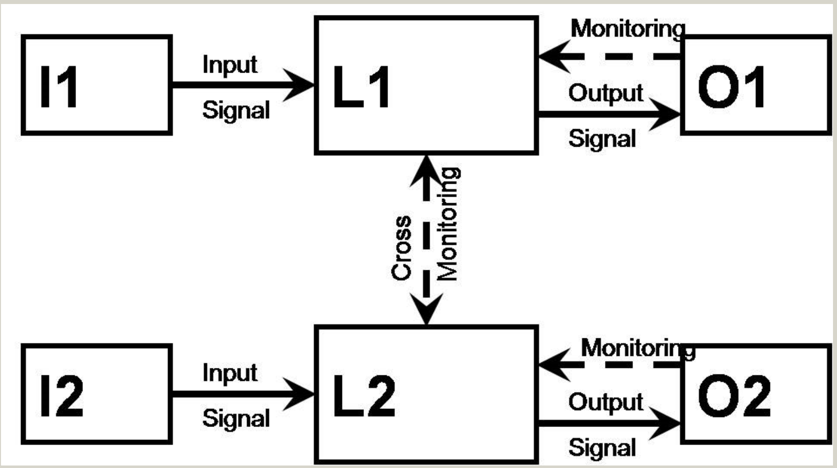



B1
PLC A
T1FC
B2
PLC B
K1
T1imp

Determination of PL: Category

- Requirements to category B met
- A fault does not lead to failure of SF?
- Fault detection exists





-> Category 3 is reached

Redundant control system with fault detection

Channel 1: B_1

PLC_A

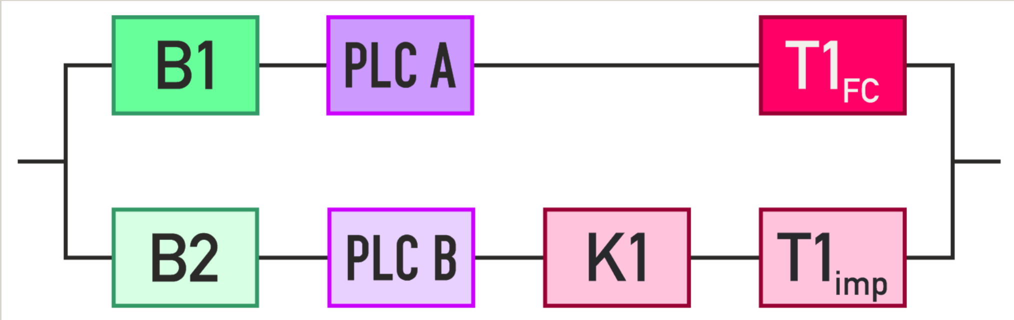
Inverter T_{1Fc}

Channel 2: B_2

PLC_B

auxiliary relay K_1

Inverter $T1_{imp}$



d_{op}: 240
h_{op}: 24
t_{cycle}: 3600
n_{op}: 5760 cycles/a

Fault detection: By reading the real value sensor G1 and G2 as well as K_1

Calculation of $MTTF_D$ for 34722 wear components

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

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

B_{10D} = 20000000

0,1 correspond to 10%

$MTTF_{DB1}$ = 34722 years

$MTTF_{DB2}$ = 34722 years

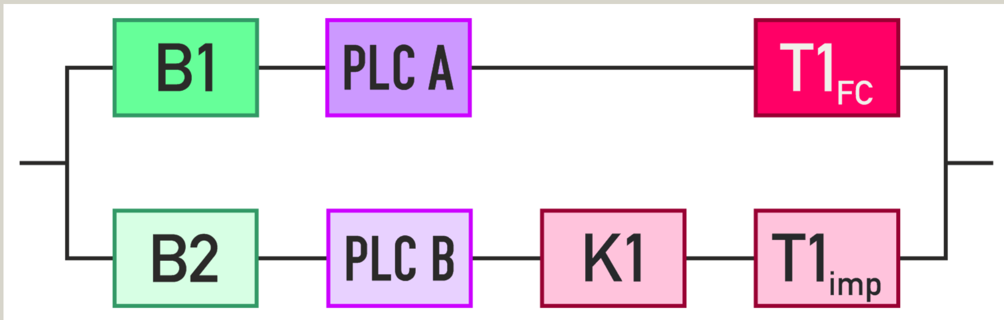
$MTTF_{DK1}$ = 34722 years

$MTTF_{DT1imp}$ = 34722 years

d_{op}: 240
h_{op}: 24
t_{cycle}: 3600
n_{op}: 5760 cycles/a

Calculation of $MTTF_D$ of channel 1

- B_1: Safety switch: $MTTF_D$ = 43722 years
- PLC_A: $MTTF_D$ = 45 years (Data from the manufacturer)
- Inverter $T1_{DFC}$ = 56 years (Data from the manufacturer



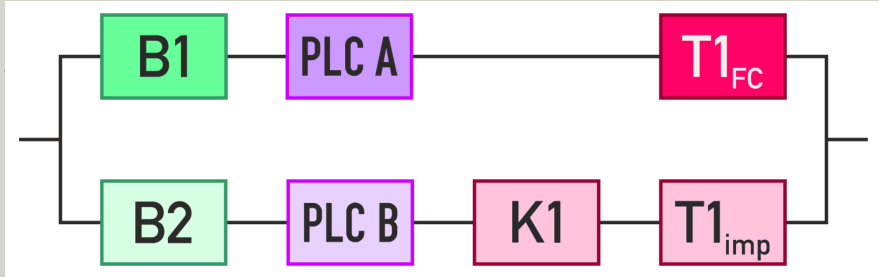
$$\frac{1}{MTTF_{DA}} = \frac{1}{MTTF_{DB1}} + \frac{1}{MTTF_{DPLCA}} + \frac{1}{MTTF_{DT1FC}}$$

channel 1: $MTTF_D$ = 24,90 y

Calculation of $MTTF_D$ of channel 2

- B_2: Safety switch switch: $MTTF_D$ = 43722 years
- PLC_B: $MTTF_D$ = 56 years (Data from the manufacturer)
- K_1: switch B_{10D}: $MTTF_D$ = 43722 years
- Inverter $T1_{imp}$ = B_{10D}: 20000000 ye
(Data from the manufacturer)

$MTTF_{DT1imp}$ = 43722 years



$$\frac{1}{MTTF_{DB}} = \frac{1}{MTTF_{DB2}} + \frac{1}{MTTF_{DPLCB}} + \frac{1}{MTTF_{DK1}} + \frac{1}{MTTF_{DT1imp}}$$

channel 2: $MTTF_D$ = 55,70 y

Determination of the complete $MTTF_D$ according to Annex D :

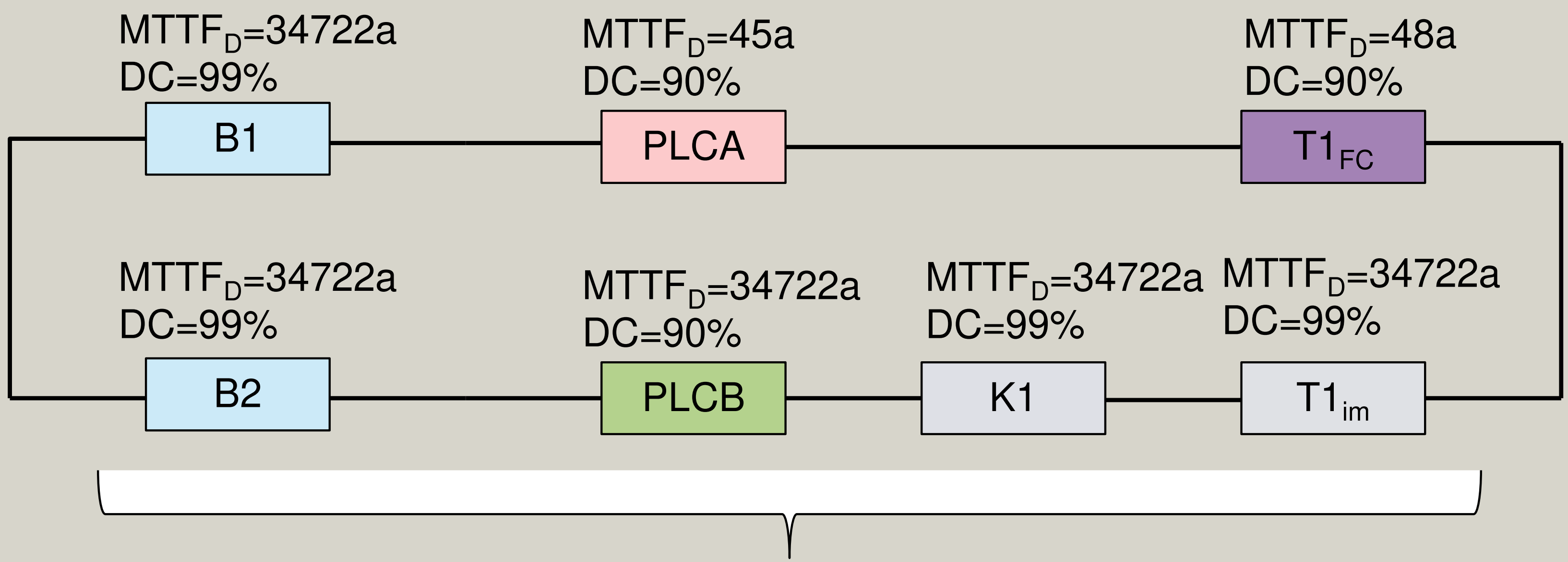
$$MTTF_D = \frac{2}{3}\left[MTTF_{Dcanal\,1} + MTTF_{Dcanal\,2} - \frac{1}{\frac{1}{MTTF_{Dcanal\,1}} + \frac{1}{MTTF_{Dcanal\,2}}}\right]$$

$$MTTF_D = \frac{2}{3}\left[24{,}9 + 55{,}7 - \frac{1}{\frac{1}{24{,}9} + \frac{1}{55{,}7}}\right]$$

$MTTF_D$=42,3years

Compo-nents	DC (%)	Estimation
B1	99	Is detected by dynamic signal change if required by the safety function (opening the locked protective device). Plausibility check is realized in both computer systems
B2	99	Is detected by dynamic signal change if required by the safety function (opening the locked protective device). Plausibility check is realized in both computer systems
K1	99	Fault is detected by reading K1 if required by the safety function in PLCA
PLCA	90	Reading G2 in PLCB. Some faults (for ex. faults of the output card etc.) can be detected by reading G1 in PLCA during the normal stop.

Compo-nents	DC (%)	Estimation
PLCB	90	Fault is detected by reading K1 in PLCA
Inverter T1a	99	Fault is detected if required by the safety function by reading G2 in PLC B. Fault is also detected in PLC A by reading G1 in case of operational stop of the drive
Inverter T1b	99	Fault is detected by reading K1 in PLCA if required by the safety function

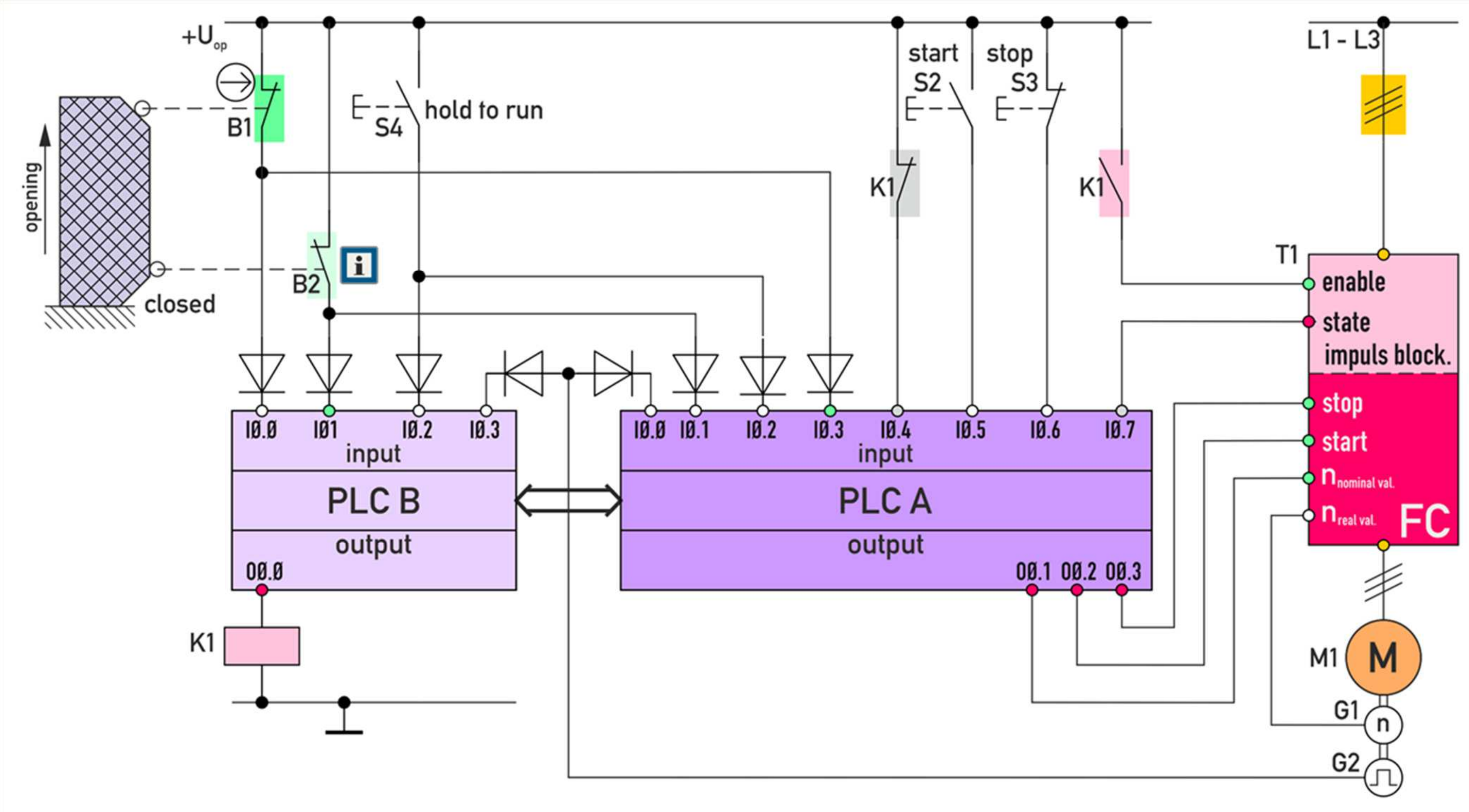


SRP/CS $_{\text{input/logic/Output}}$

$MTTF_{Dcomplet}$=42,3a
$DC_{complet}$=92,8%
PFH=1,3 10^{-7} (Calculation using SISTEM)

$$DC_{avg} = \frac{\frac{DC_{B1}}{MTTF_{dB1}} + \frac{DC_{B2}}{MTTF_{DB2}} + \frac{DC_{PLCA}}{MTTF_{DPLCA}} + \frac{DC_{PLCB}}{MTTF_{DPLCB}} + \frac{DC_{K1}}{MTTF_{DK1}} + \frac{DC_{T1FC}}{MTTF_{DT1FC}} + \frac{DC_{T1imp}}{MTTF_{DT1imp}}}{\frac{1}{MTTF_{dB1}} + \frac{1}{MTTF_{DB2}} + \frac{1}{MTTF_{DPLCA}} + \frac{1}{MTTF_{DPLCB}} + \frac{1}{MTTF_{DK1}} + \frac{1}{MTTF_{DT1FC}} + \frac{1}{MTTF_{DT1imp}}}$$

$MTTF_D$ [a]	Kat.3 DC_{avg} = mittel	
27	$3{,}70\ 10^{-7}$	c
30	$2{,}65\ 10^{-7}$	d
33	$2{,}30\ 10^{-7}$	d
36	$2{,}01\ 10^{-7}$	d
43	$1{,}54\ 10^{-7}$	d
47	$1{,}34\ 10^{-7}$	d
51	$1{,}19\ 10^{-7}$	d
56	$1{,}03\ 10^{-7}$	d
62	$8{,}84\ 10^{-8}$	e
68	$7{,}68\ 10^{-8}$	e
75	$6{,}62\ 10^{-8}$	e


+U op
B1
S4
hold to run
opening
closed
B2
start
S2
stop
S3
K1
K1
L1 - L3
T1
enable
state
impuls block.
stop
start
n nominal val.
n real val.
FC
I0.0
I0.1
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

Stop if required by the safety function (opening of the protection door)

Systems/ characters	Potentiel faults	Fault detection	Fault reaction	Testing measure
Failure of the personal safety switch B1	Cross circuit, mechanical failure, electrical failure, ground fault	Is detected by dynamic signal change if required by the safety function (opening of the locked protective device). Plausibility check is realized in both computer systems	Stop if detected and restart is prevented	Apply a static signal at the input of both PLCs
Failure of the personal safety switch B2	Contact does not open if the locked protection door is opened (electrical fault or mechanical fault)	Is detected by dynamoc signal change if required by the safety function (opening of the locked protective device). Plausibility check is realized in both computer systems	Stop if detected and restart is prevented	Apply a static signal at the input of both PLCs
Failure of the personal safety switch B2	Spontaneous contact if the locked protection door is in the opened position (for ex. failure of the spring)	Fault is detected in both computers as no signal change has been realized in B1	Restart is prevented	Apply a static signal at the input of both PLCs

As result of the fault detection measures a DC of 99% for B1 and B2 can be given !!!!

Systems / characters	Potentiel faults	Fault detection	Fault reaction	Testing measure
Failure of PLCA	Stuck-at-fault in the input/output card or wrong code or complex fault in CPU , preventing that a stop command is sent to the inverter T1a before or during the opening of the protective device	Reading G2 in PLCB . Some faults (for ex. fault in the output card, etc.) can be detected by reading G1 in PLCA during the normal stop. Fault detection is also realized by watchdog function. Other faults by watchdog function	The engine M1 is indirectly stoped with a time delay by PLCB, K1 und T1b. PLC A has the possibility to inform PLB in case of fault detection during the normal stop	Apply a static signal at the stop exit of PLCA
Failure of PLCA	Stuck-at-fault in the input/output card or wrong code or complex fault in CPU , preventing that a stop command is sent to the inverter T1a during the electrical locked protective device is open	Fault cannot be detected by reading G2 as M1 is hold in resting position by T1b in case of an opened locked protective device. Fault detection by the operator when closing the protective device. Some fault can be detected by watchdog function.	Unexpected restart in case of closing the locked protective device. PLCA can inform PLCB about the communication steps.	Send a start command to T1a in the case of an open locked protective device

Systems/ characters	Potentiel faults	Fault detection	Fault reaction	Testing measures
Failure of the inverter T1A	Stuck-at-fault and other internal complex faults in control and power electronics of the inverter, which prevent T1a from stopping the motor before or when the protective device is opened.	Fault is detected if required by the safety function by reading G2 in PLC B. Fault is also detected in PLC A by reading G1 in case of operational stop of the drive.	The engine M1 is indirectly stoped with a time delay by PLCB, K1 und T1b. PLC A has the possibility to inform PLB in case of fault detection during the normal stop	Stop input of the inverter before and during the safety requirement to high potential
Failure of the inverter T1A	Stuck-at-fault and other complex internal faults in control and power electronics of the inverter, which provide a starting command in case of opened locked protective device.	Fault cannot be detected by reading the signal G2 in PLC B as due to the pulse lock a start of the drive cannot be realized Fault detection by the user of the machine when closing the locked protective device by independent start of M1	Drive is held in resting position by PLB and also by K1. If the locked protective device is closed a start is independently made. PLC A can inform PLCB about the fault.	To force a start command in the inverter in case of opened locked protective device

As a result of the fault detection measures a DC of 99% for T1a can be given !!!!

Systems/ characters	Potentiel faults	Fault detection	Fault reaction	Testing measures
Failure of PLCB	Stuck-at-fault in the input/output card or wrong code or complex fault in CPU which prevent that the relay K1 can be switched off by PLCB before or during the protective device is opened	Fault is detected by reading K1 in PLCA	The engine M1 is kept in resting position by T1a and a new start is prevented.	K1 is not switched off
Failure of PLCB	Stuck-at-fault in the input/output card or wrong code or complex fault in CPU which prevent that the relay K1 can be switched off by PLCB in case of opened protective device	Fault is detected by reading K1, if required by the safety function in PLCA Some faults can be detected by the watchdog funtion.	Unexpected start when closing the locked protective device. PLCA can inform PLCB via the communication interface.	Switch K1 when the protective device is opened.

As result of the fault detection measures a DC of 90% for PLCB can be given !!!!

Systems/ characters	Potentiel faults	Fault detection	Fault reaction	Testing measures
Failure of PLCB	Stuck-at-fault in the input/output card or wrong code or complex fault in CPU which prevent that the relay K1 can be switched off by PLCB before or during the protective device is opened	Fault is detected by reading K1 in PLCA	The engine M1 is kept in resting position by T1a and a new start is prevented.	K1 is not switched off
Failure of PLCB	Stuck-at-fault in the input/output card or wrong code or complex fault in CPU which prevent that the relay K1 can be switched off by PLCB in case of opened protective device	Fault is detected by reading K1, if required by the safety function in PLCA Some faults can be detected by the watchdog funtion.	Unexpected start when closing the locked protective device. PLCA can inform PLCB via the communication interface.	Switch K1 when the protective device is opened.

Thank you very much for your attention !

Wish you much success

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

"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.)