BG ETEM
Energie Textil Elektro
Medienerzeugnisse

Fachausschuss Druck und Papierverarbeitung

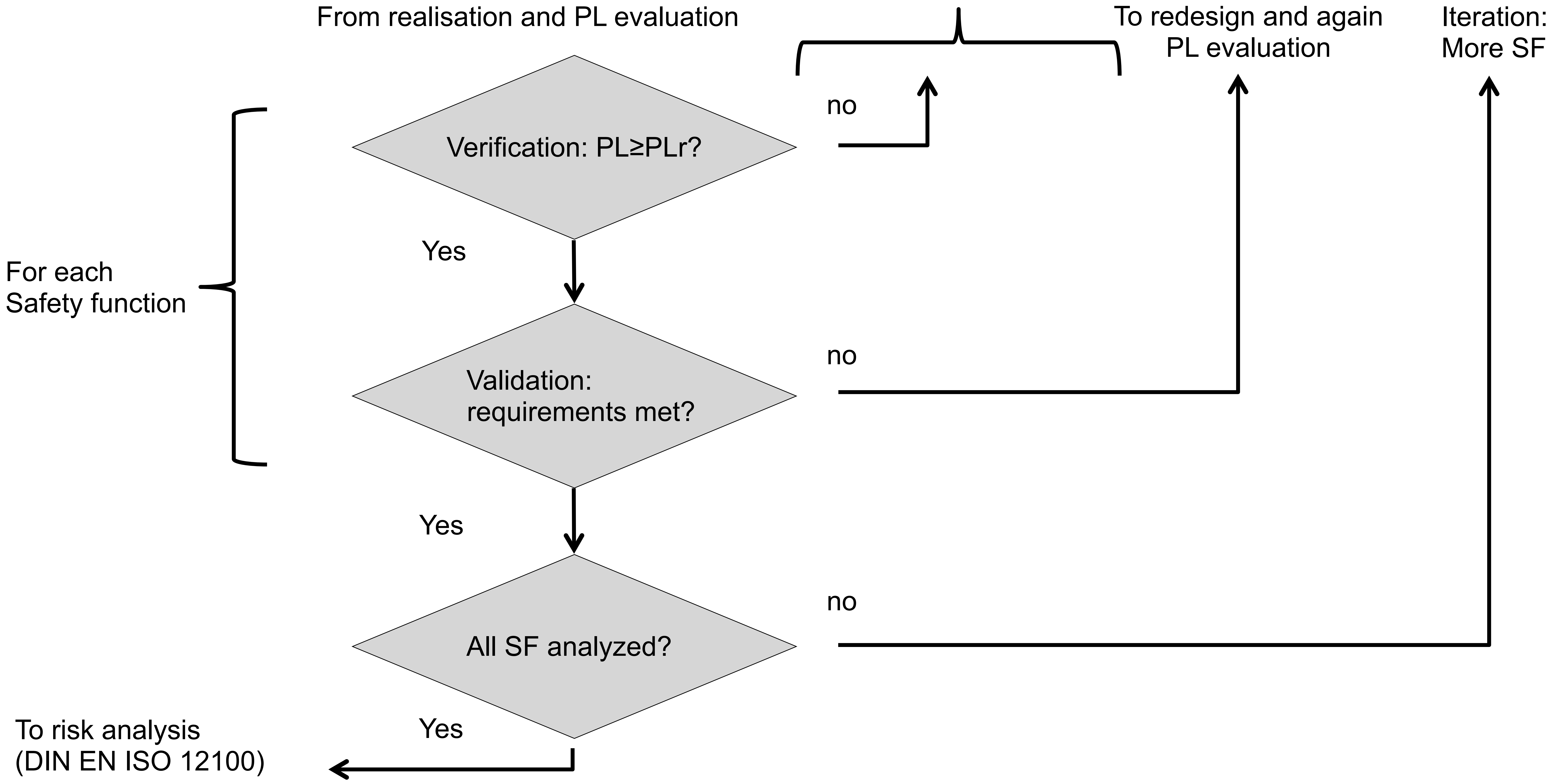
Validation of machines under consideration of the new EN ISO 13849-2

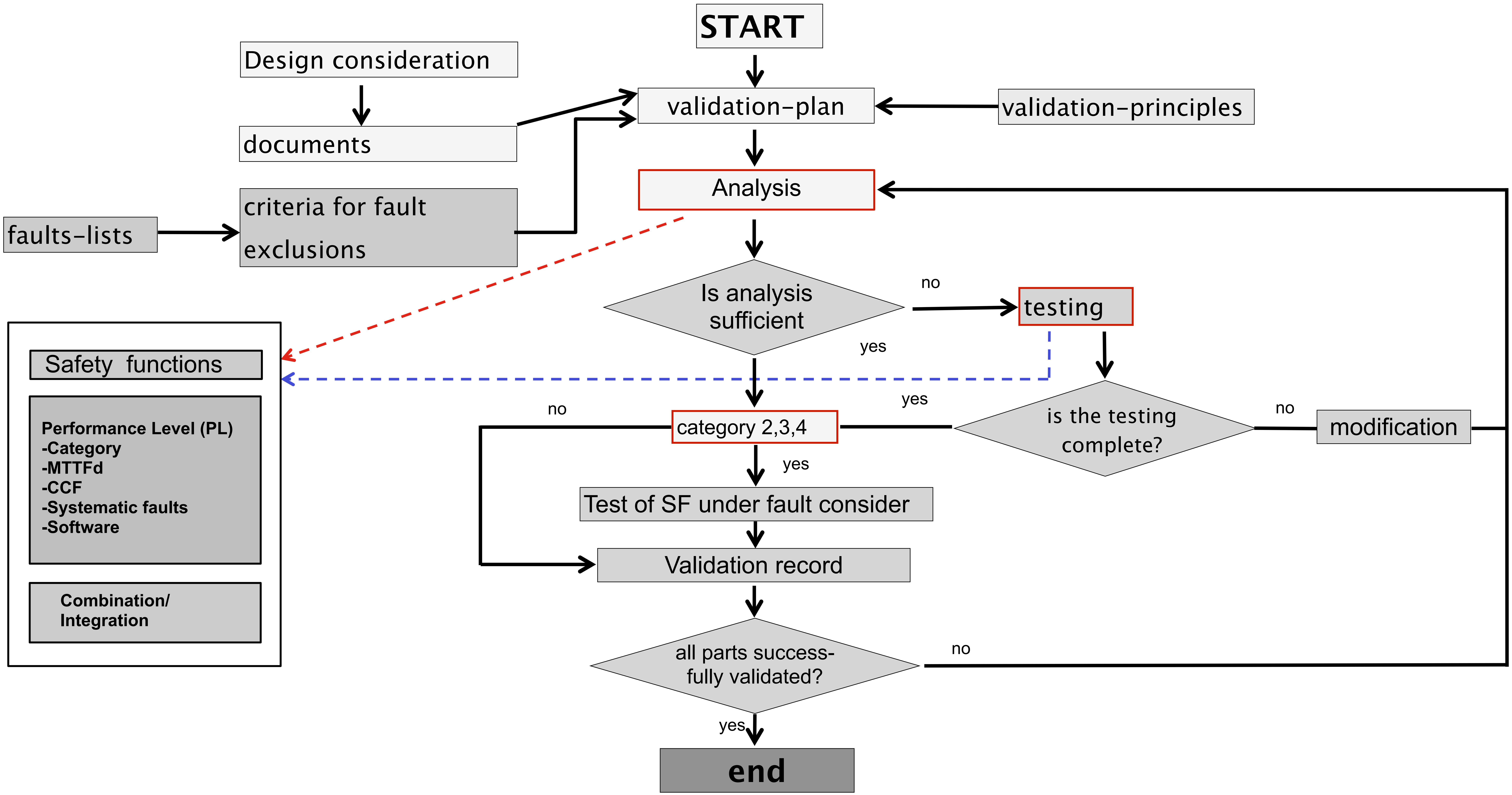
Dipl.-Ing. Becker

Verification and validation

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

These activities should begin as early as possible during the development, in order to detect and eliminate faults in time. If possible, the test should be performed by persons not involved in the process of designing the safety related parts, (i.e. who are independent of the design and development process).


From realisation and PL evaluation
To redesign and again PL evaluation
Iteration: More SF
no
Verification: PL≥PLr?
Yes
For each Safety function
no
Validation: requirements met?
Yes
no
All SF analyzed?
Yes
To risk analysis (DIN EN ISO 12100)


START
Design consideration
validation-plan
validation-principles
documents
Analysis
faults-lists
criteria for fault exclusions
Is analysis sufficient
no
testing
yes
Safety functions
Performance Level (PL)
-Category
-MTTFd
-CCF
-Systematic faults
-Software
Combination/ Integration
no
category 2,3,4
yes
is the testing complete?
no
modification
yes
Test of SF under fault consider
Validation record
all parts success-fully validated?
no
yes
end

Verification and Validation plan

- Identification of the SRP/CS products to be tested
- Identification of the safety function with their assignment to the SRP/CS involved
- Reference to documents with requirements/specifications (e.g. SRS/safety requirements specifications)
- Test principles (standards) and internal company requirements (e.g. company standards, design rules and programming guidelines) to be applied
- Analyses and tests (methods) to be performed, including identification of the dedicated tests specification documents
- Fault lists to be employed
- Personnel responsible for the analyses and tests (testers, department or body)
- Specified results documentation (test reports/records to be generated)

Validation of the safety functions

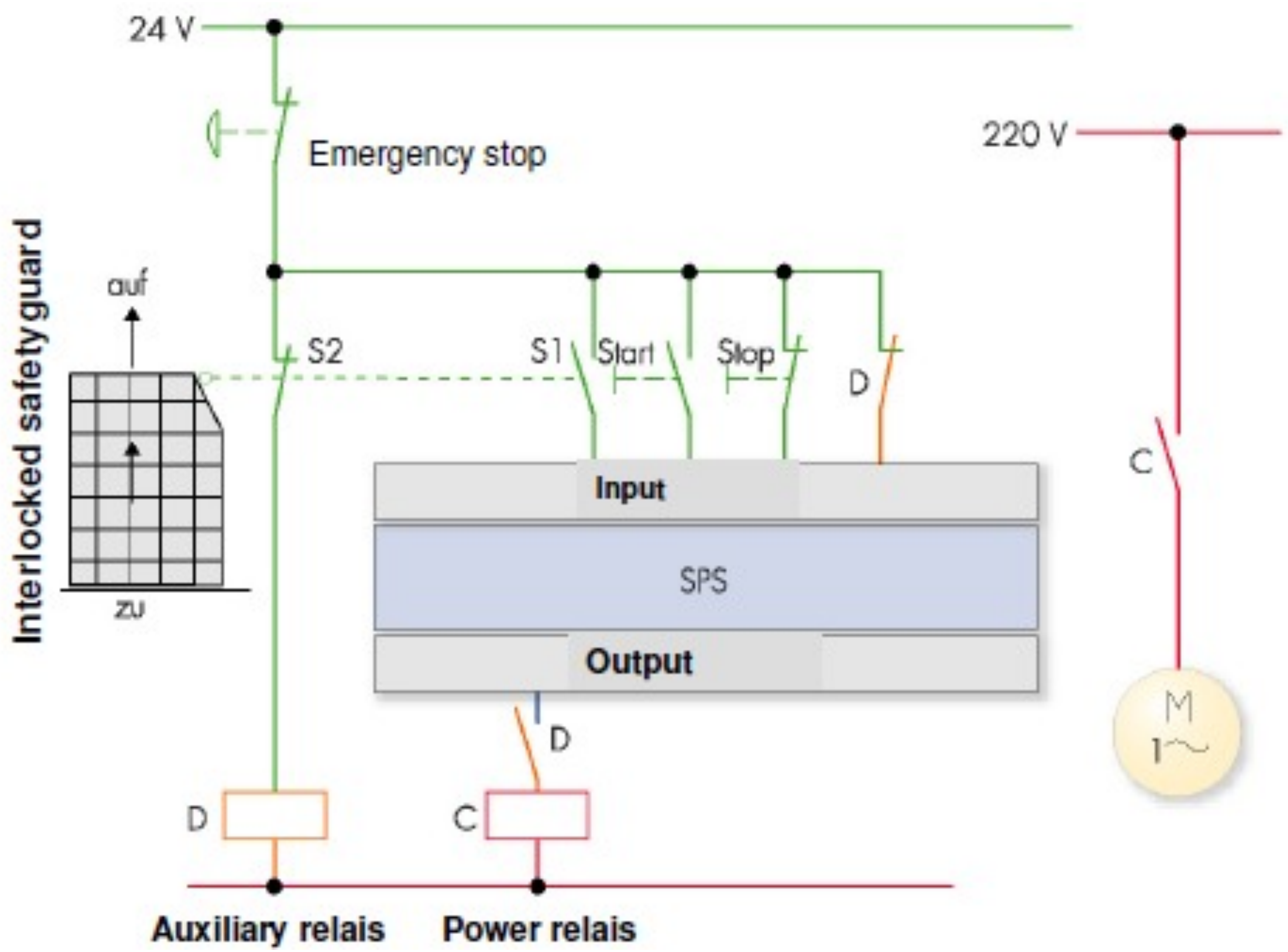
- Has the safety function been defined properly and completely?
- Has the correct safety function been implemented?
- Are the provisions for the safety function appropriate for the design?
- Have all necessary operating modes been considered?
- Have the operating characteristics of the machine been considered (including reasonably foreseeable misuse)?

Validation of the safety functions

- Have response actions to the emergencies been considered?
- Are all safety-related input signals processed properly and with the correct logic to safety-oriented output signals?
- Have the results of the risk assessment for each specific hazard or hazardous situations been incorporated into the definition of the safety function?

Validation of the category

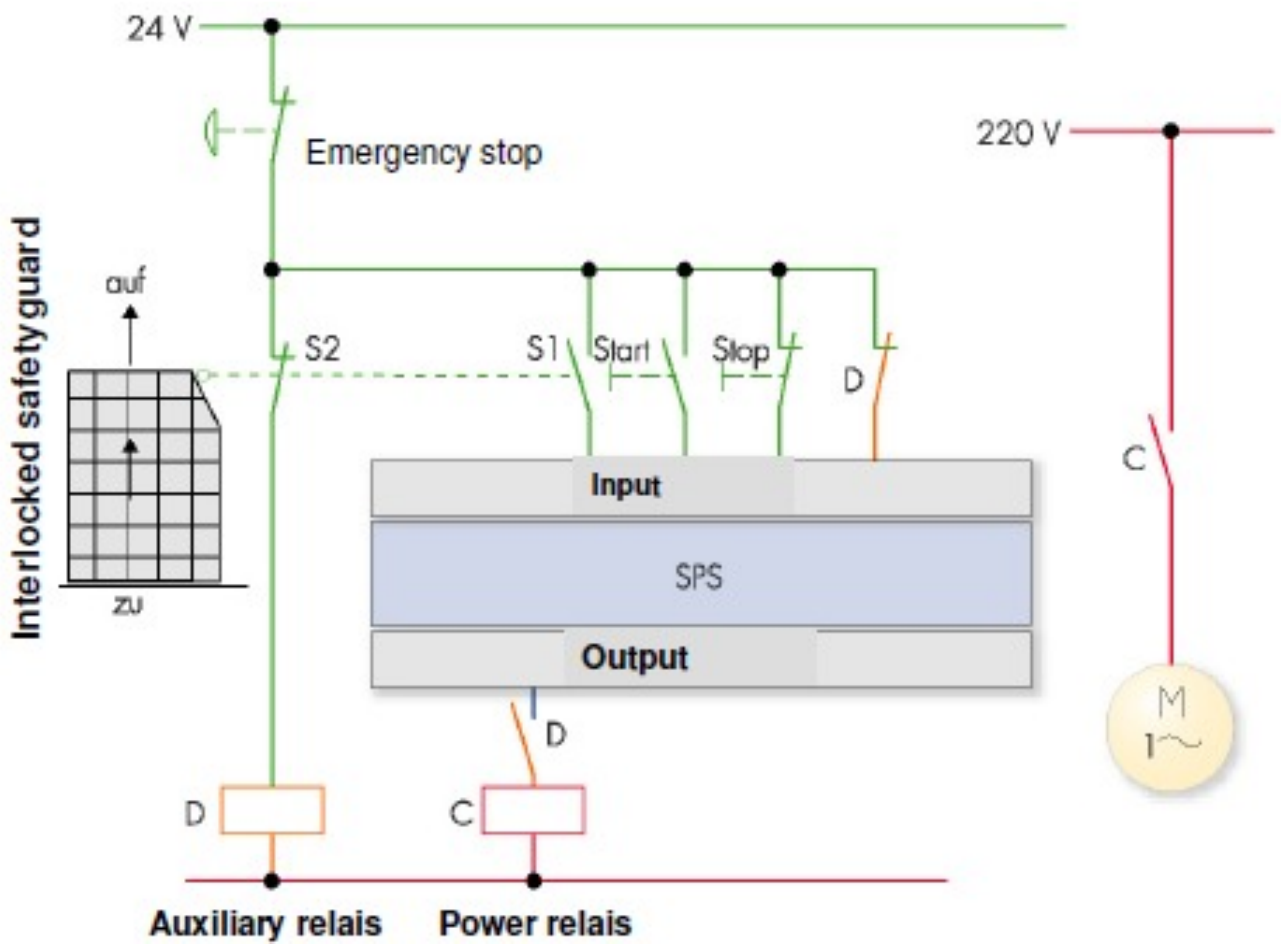
- Specifications of the SRP/CP
- Design descriptions
- Block diagrams/description of the structure
- Circuit diagrams
- Fault lists
- Tests of the fault-mode behavior of the SRP/CS, with failure mode and effects testing and testing by fault injection



Validation of the DC values

- Comprehensible reasoning must be provided for diagnostic coverage assigned to the blocks on the basis of test measures. The information on origin of the values is typically examined here, e.g. whether the values obtained are credible or questionable.

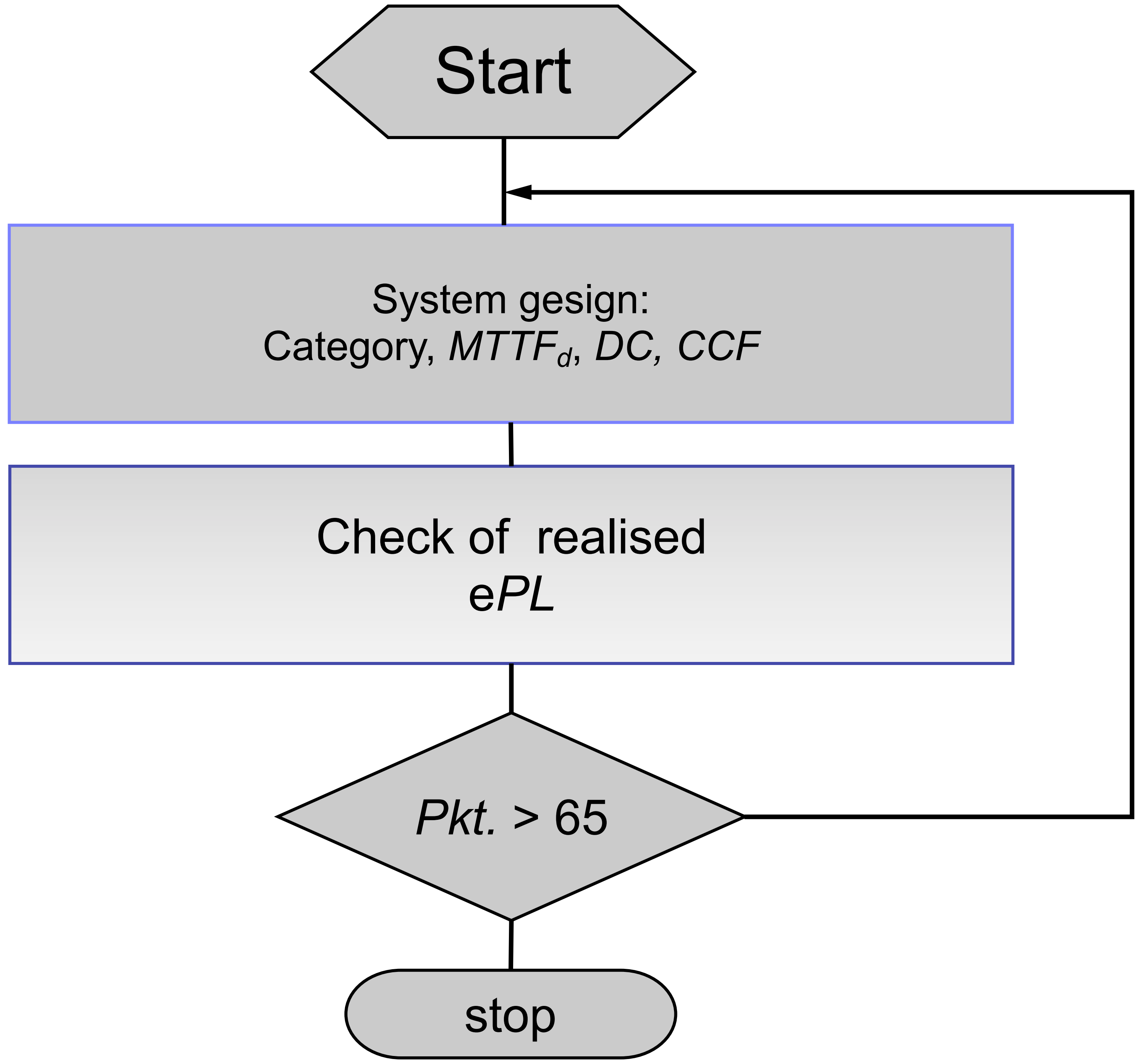
- Tests of fault mode behaviour of the SRP/CS (failure mode and effects testing/testing by fault injection) are to show that proper fault detection is assured by the diagnostic functions.



Validation of the measures against CCF

- Besides attainment of total number of points, the method examines whether the selected measures are adequately described in the associated documentation.

- Analyses and/or tests must demonstrate that the measures have actually been implemented.

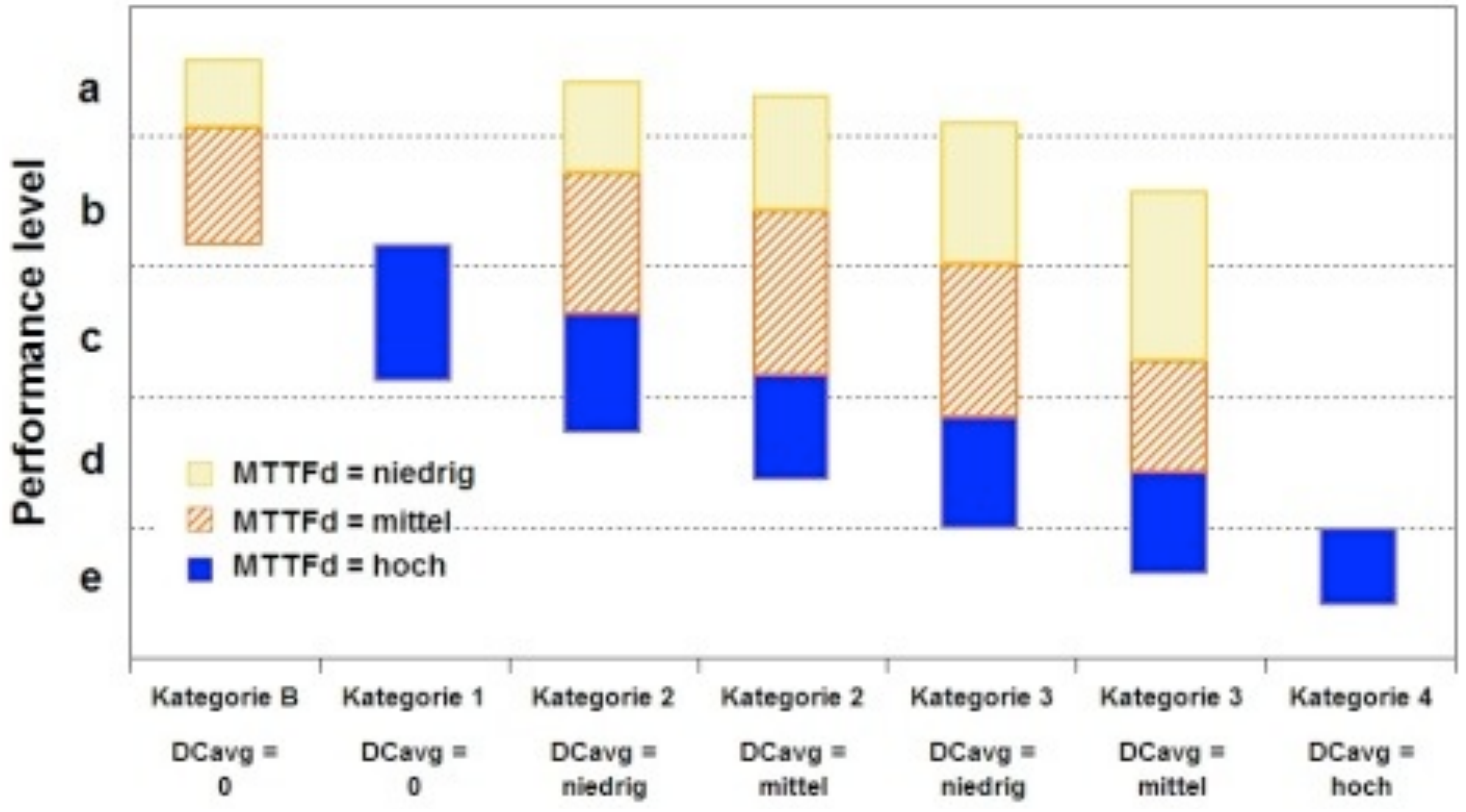


Validation of the PL and SRP/CS

- review of the determination of the obtained PL taken to account Category, DCavg and MTTFd in accordance with EN ISO 13849-1, 4.5.4 and Annex K

- evidence that the obtained PL meets the PLr

PL≥PLr



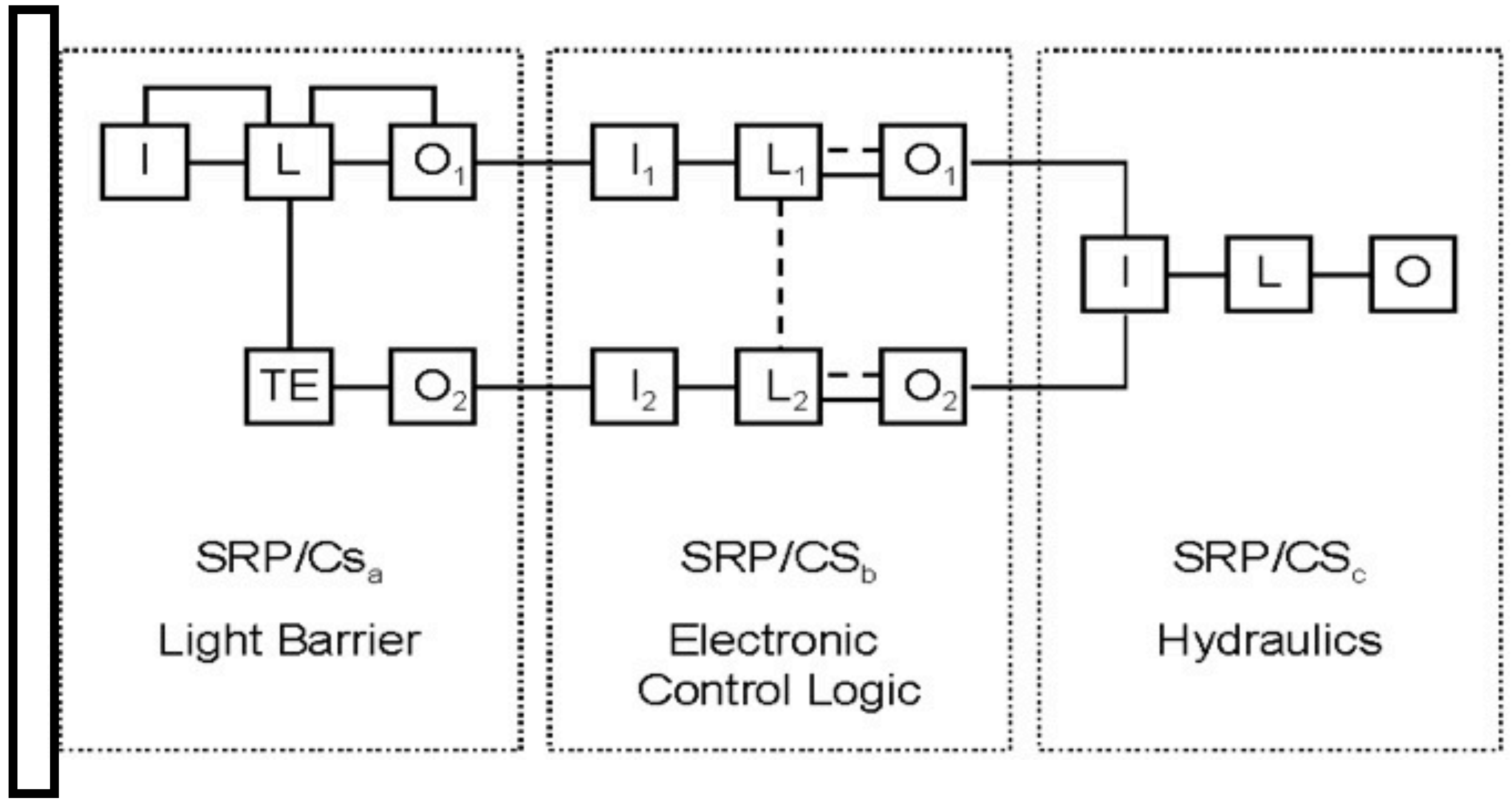
When not using simplified calculation method, the following parameters has to be considered:

- MTTFd- Value for each Part
- the DC
- the CCF
- the structure
- review of the documentation, use and calculation

Validation of the combination and intergration of SRP/CS

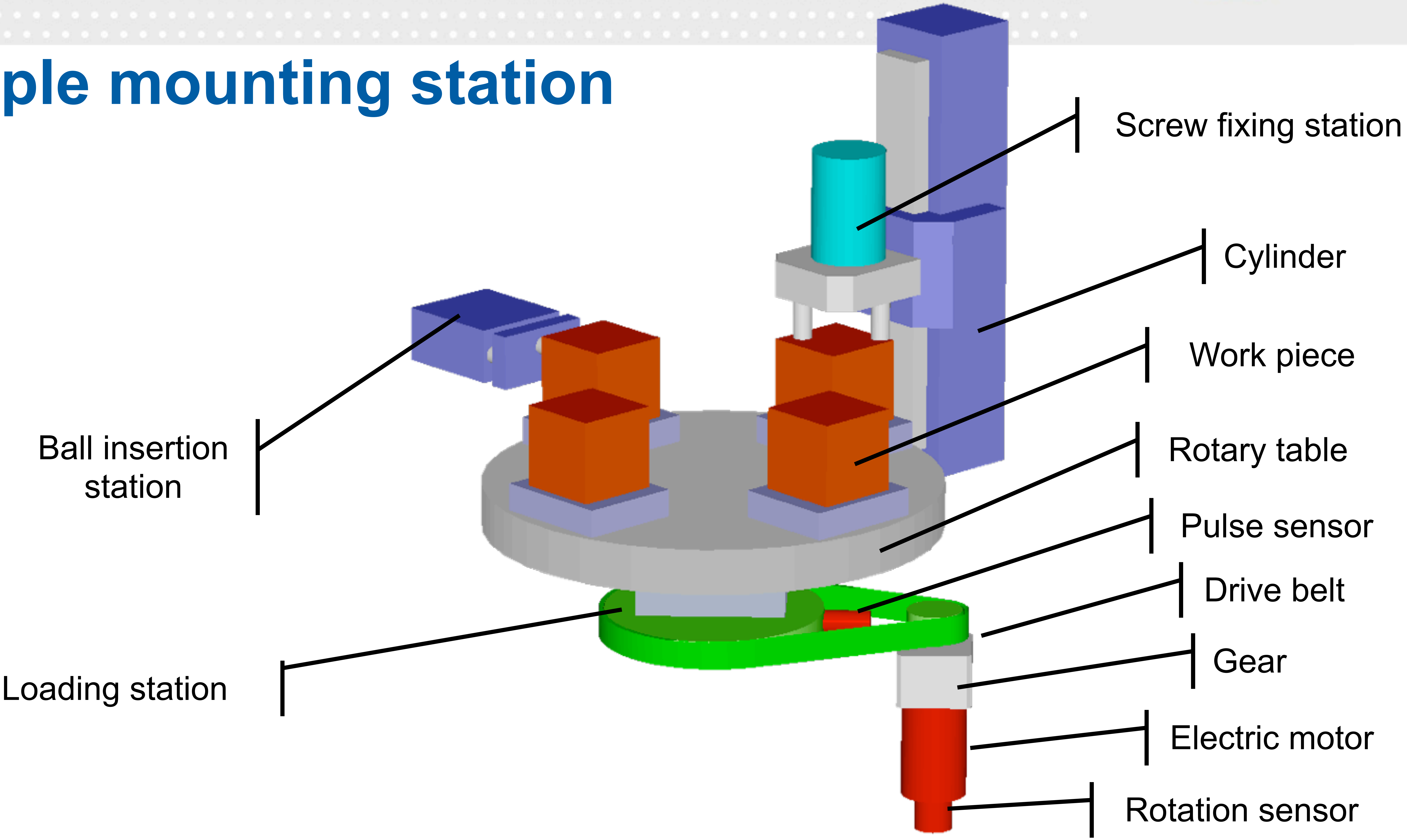
Required Validation steps:

- Inspection of the design documents which together describe the safety function
- Comparison of the characteristic data for the interfaces between the SRP/CS (e.g. Voltages, currents, pressures, information data)
- FMEA of combination/integration
- Function test/Black test
- Extended functional test
- Checking of the simplified determination of the overall PL from the PLs of the individual SRP/CS

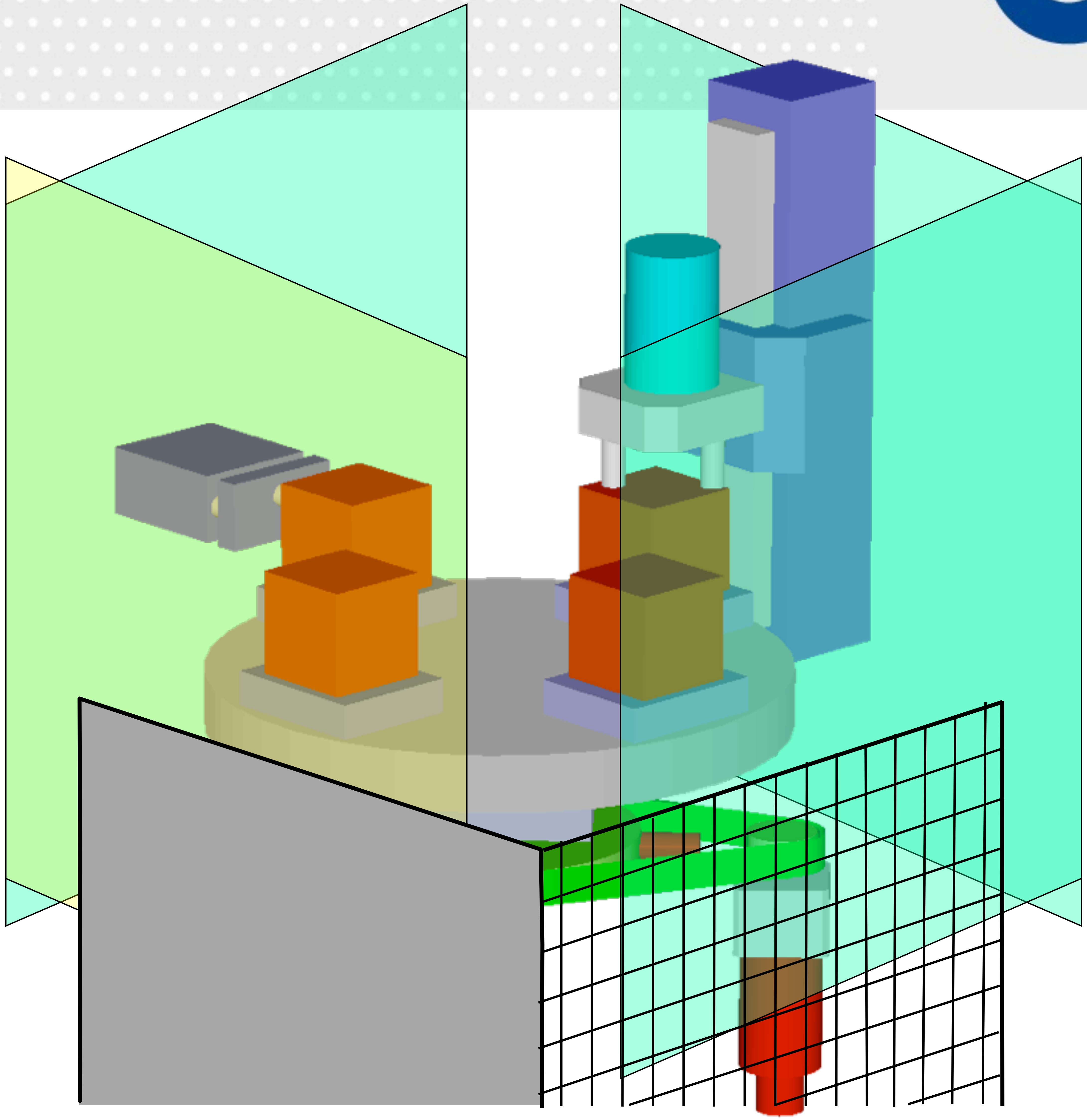


$$\sum_{i=1}^{i=n} PFH_i = PFH_1 + \ldots\ldots + PFH_n$$

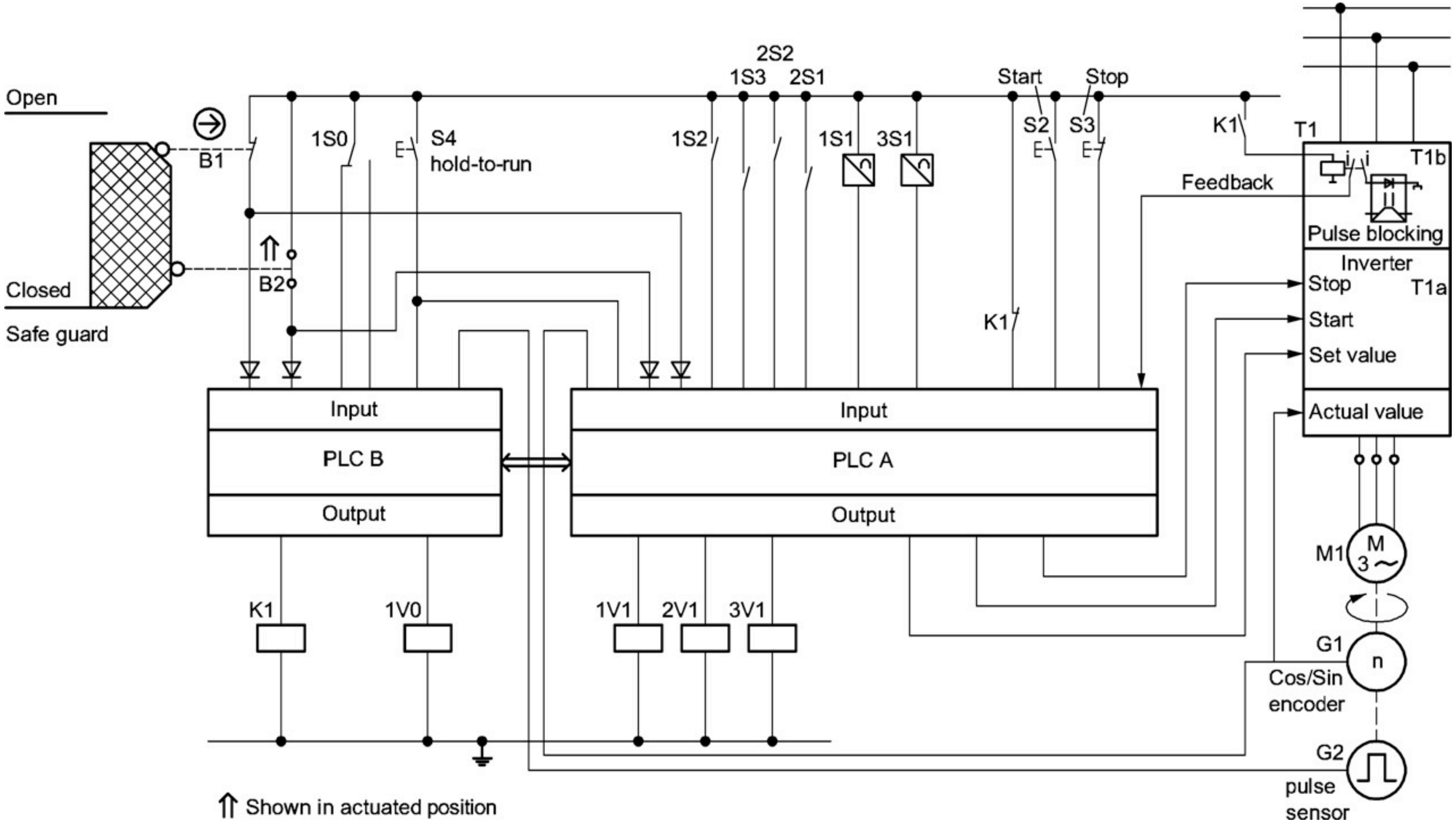
Example mounting station



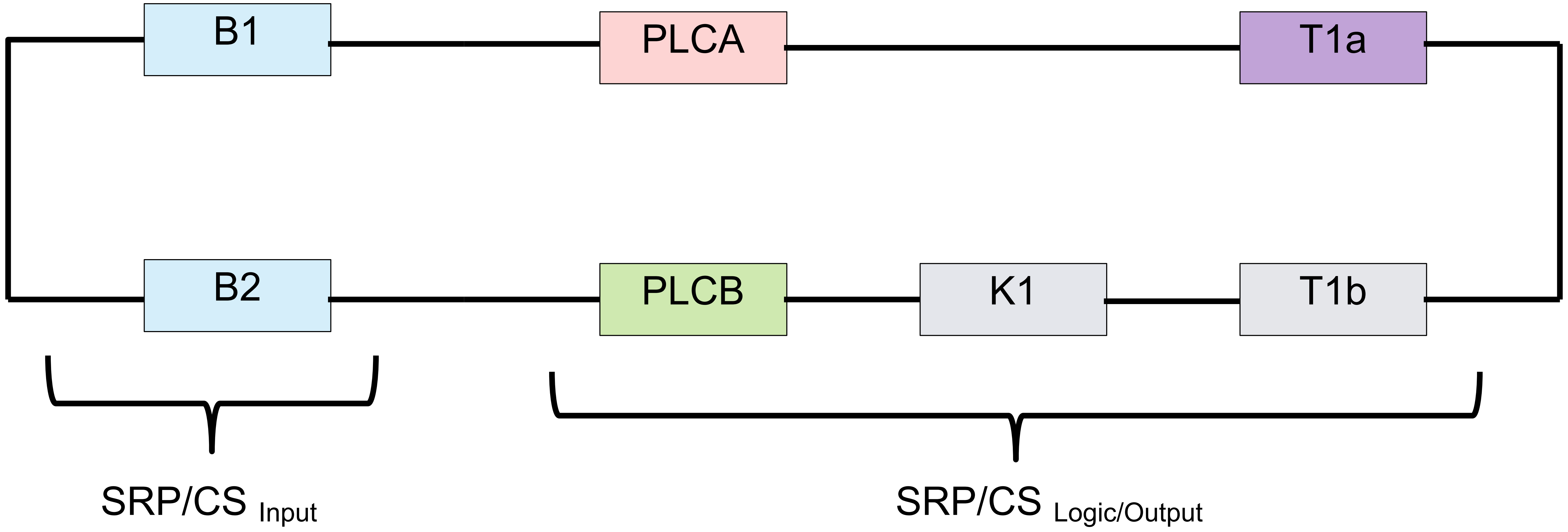
Safeguarding with interlocking guard

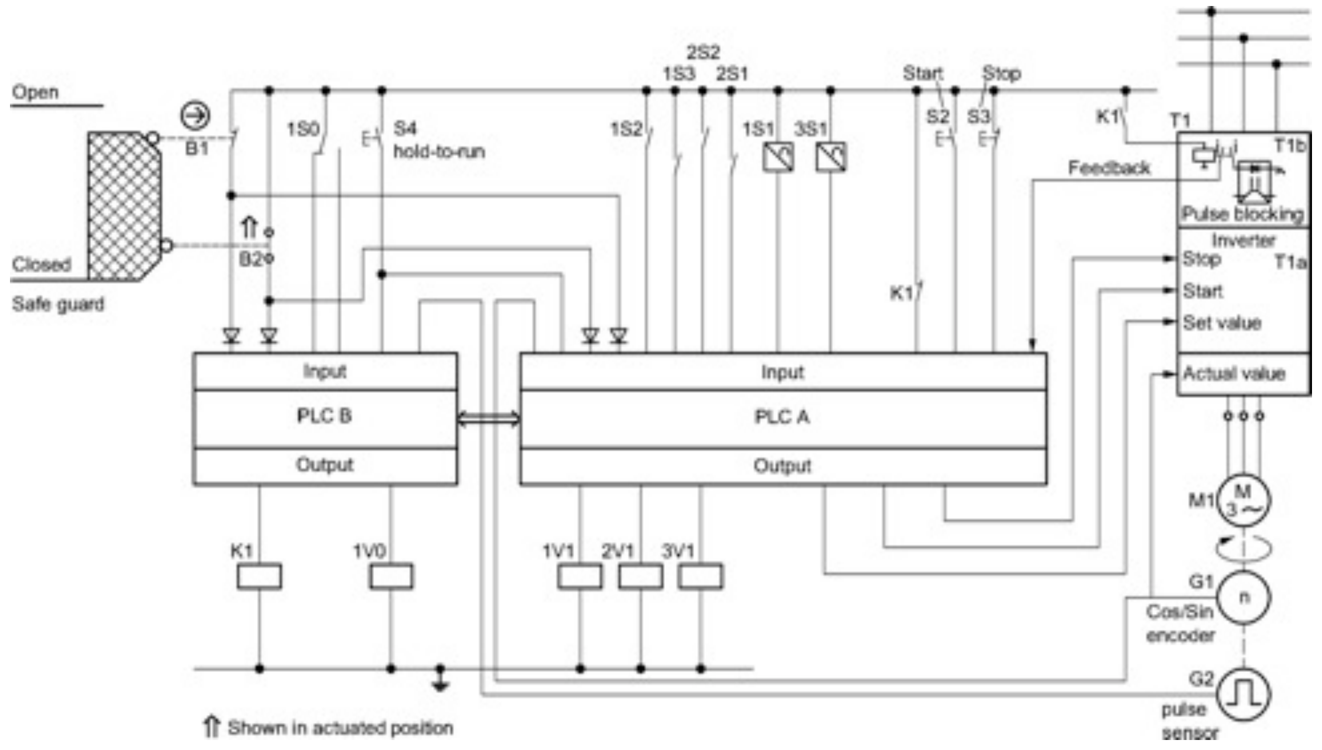


EN ISO 13849-1:2006



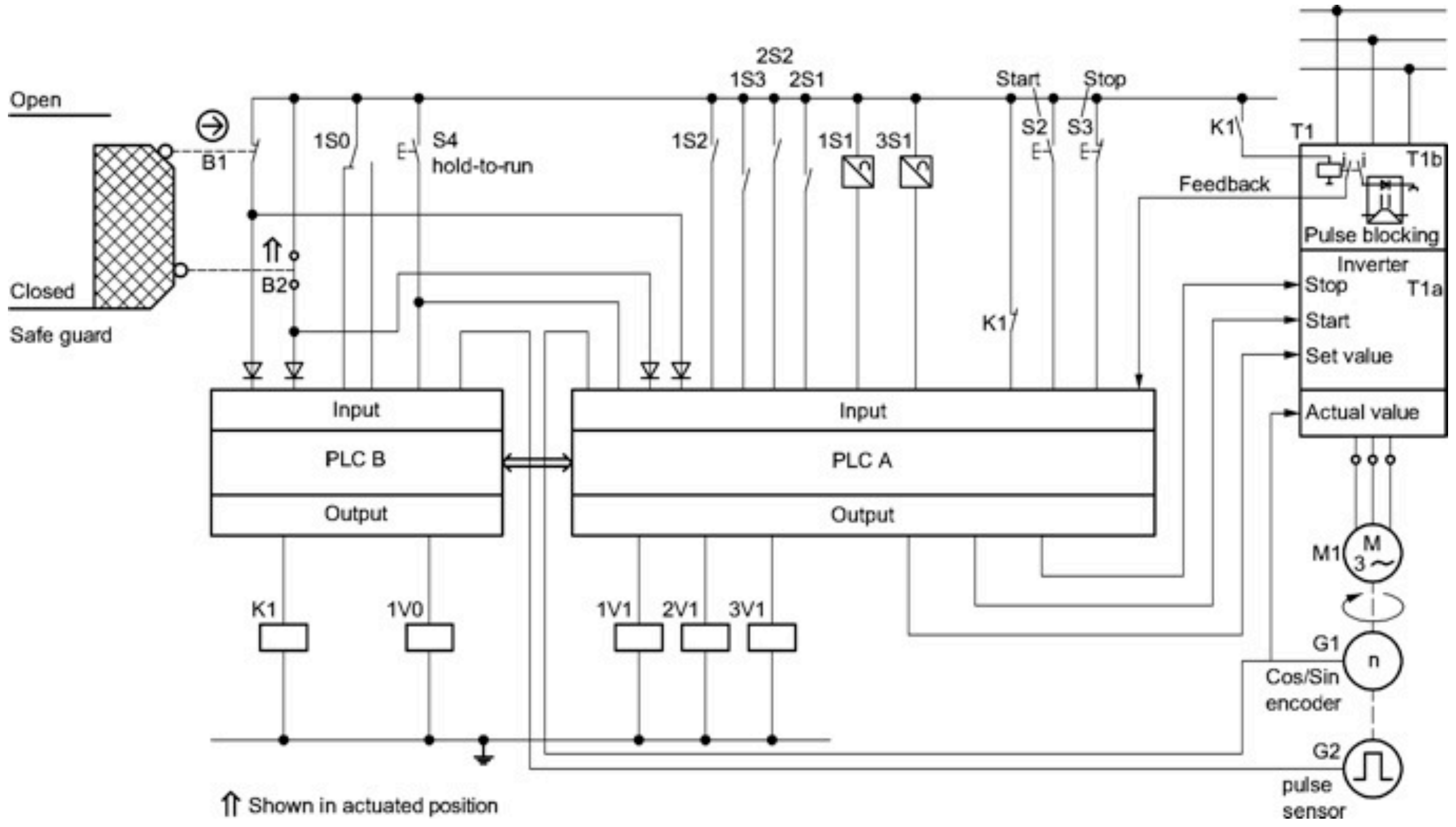
Logical Block diagram “Stop function”

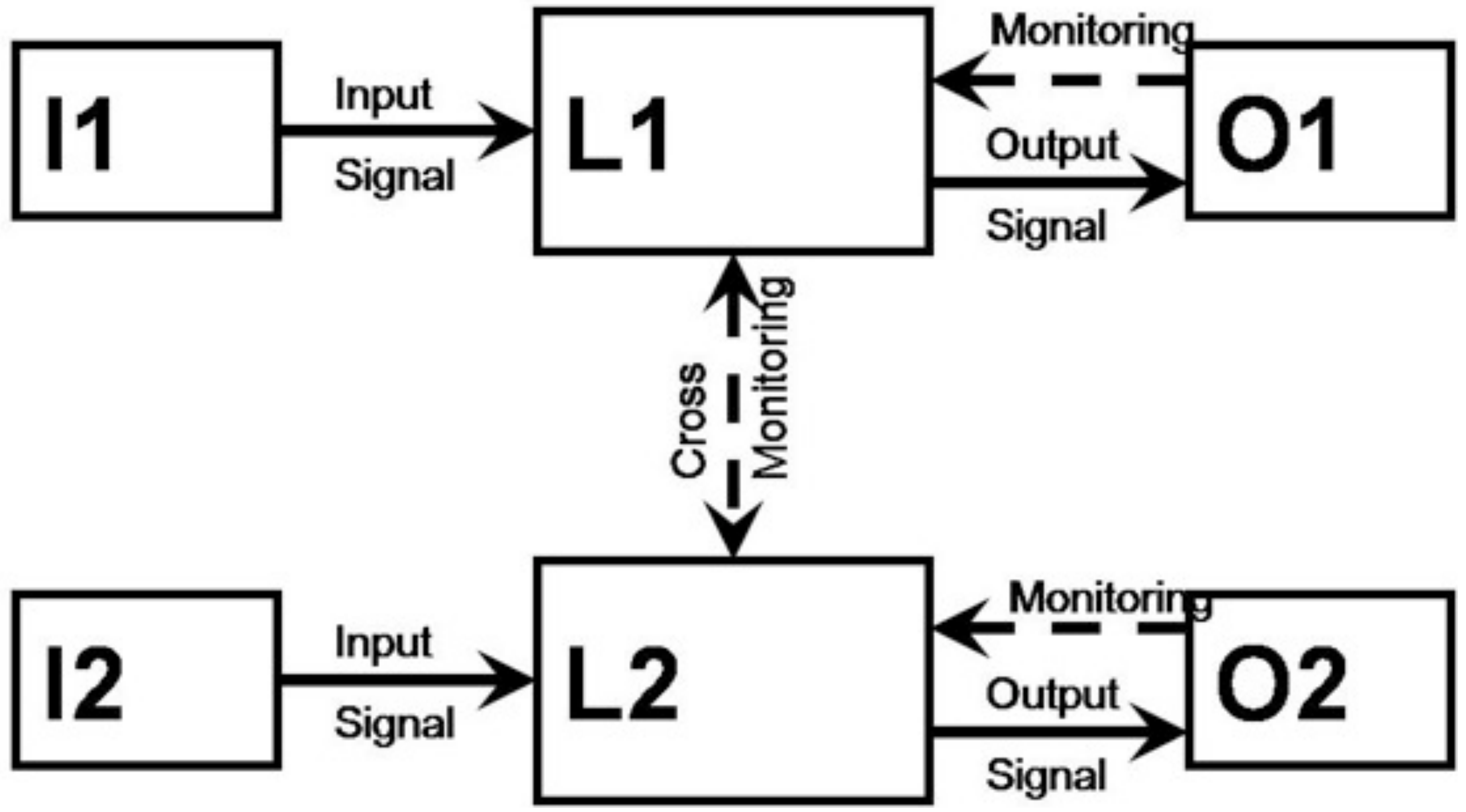




Determination of PL: Category

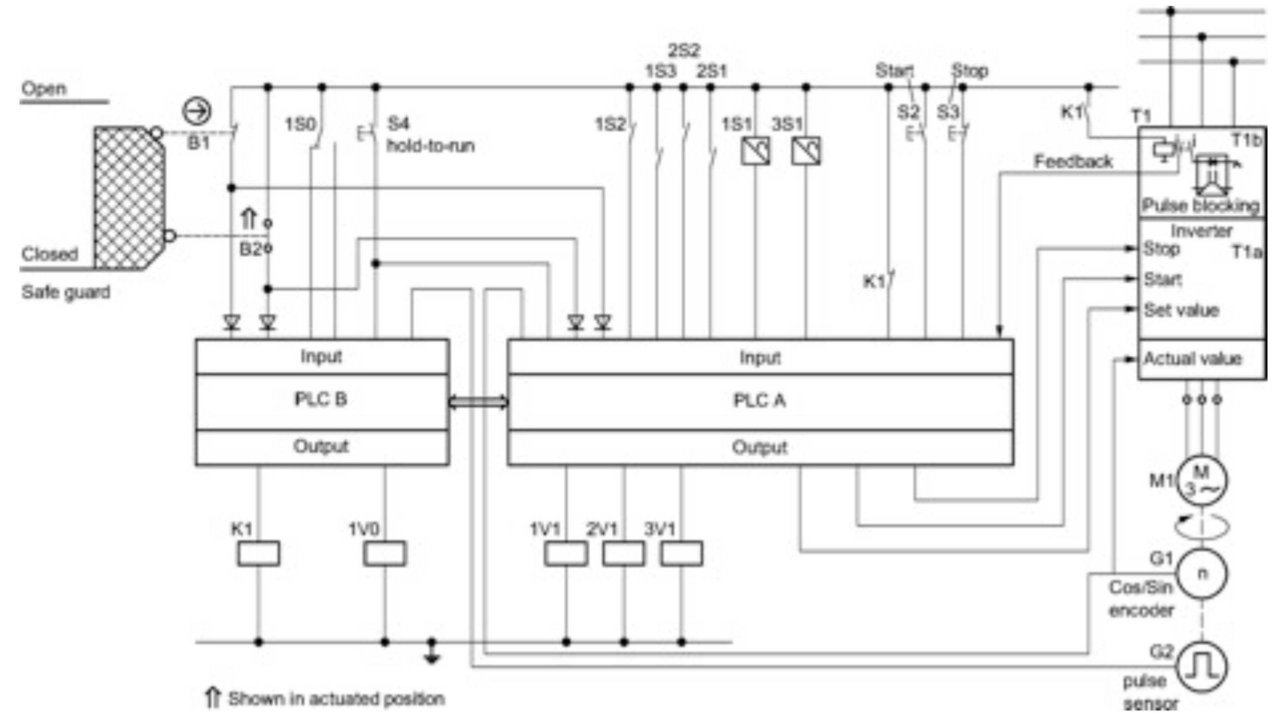
- Requirement of category B is met
- A fault does not lead to loss of SF
- Fault detection realised





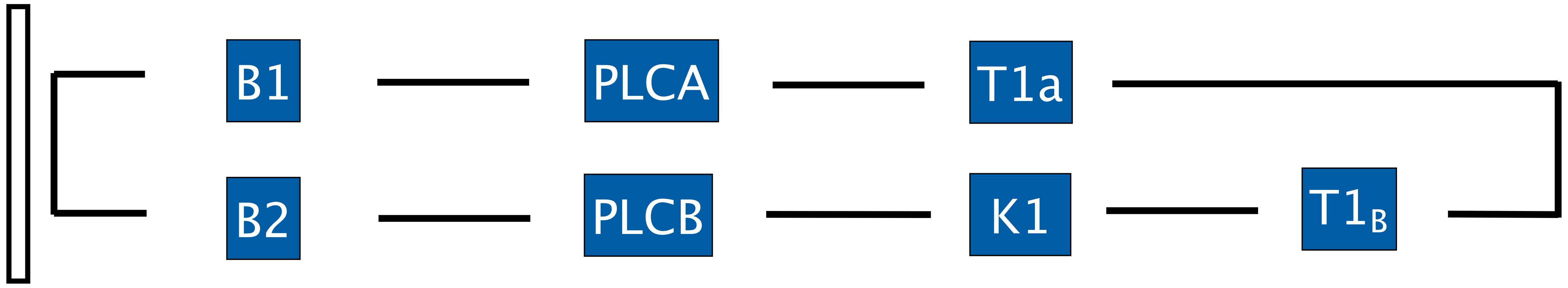
-> category 3 is met

Redundant control system with fault detection



Canal 1: B1
PLCA
Inverter T1a

Canal 2: B2
PLCB
relay K1
Inverter T1b



Fault detection through: e.g feedback G1, G2 and K1

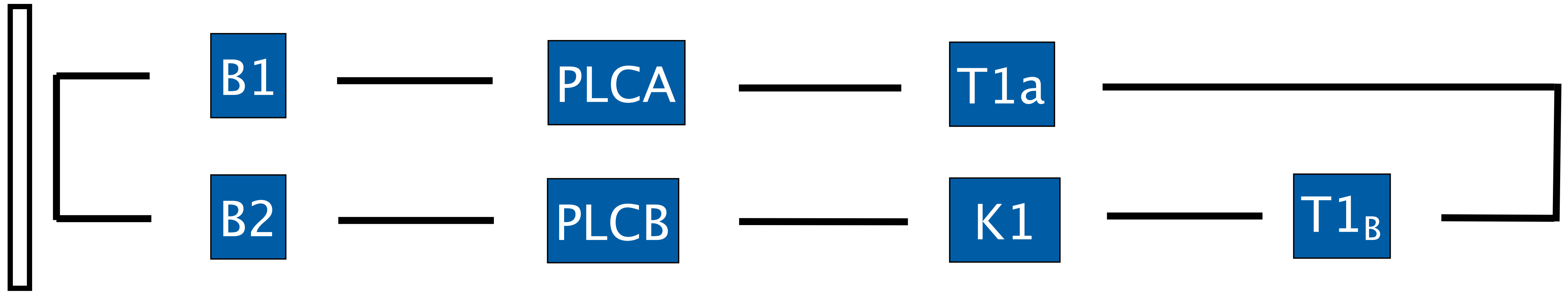
d_{op}: 240
h_{op}: 24
t_{cycle}: 3600

Calculation of $MTTF_d$ for canal 1

- **PLCA: $MTTF_d$ = 25 years (data from producer)**
- **Inverter T1a = 30 years (data from producer)**
- **B1 = 570 years**

$$\frac{1}{MTTF_{dB}} = \frac{1}{MTTF_{dB1}} + \frac{1}{MTTF_{dPLCA}} + \frac{1}{MTTF_{dT1A}} + \frac{1}{MTTF_{dB1}}$$

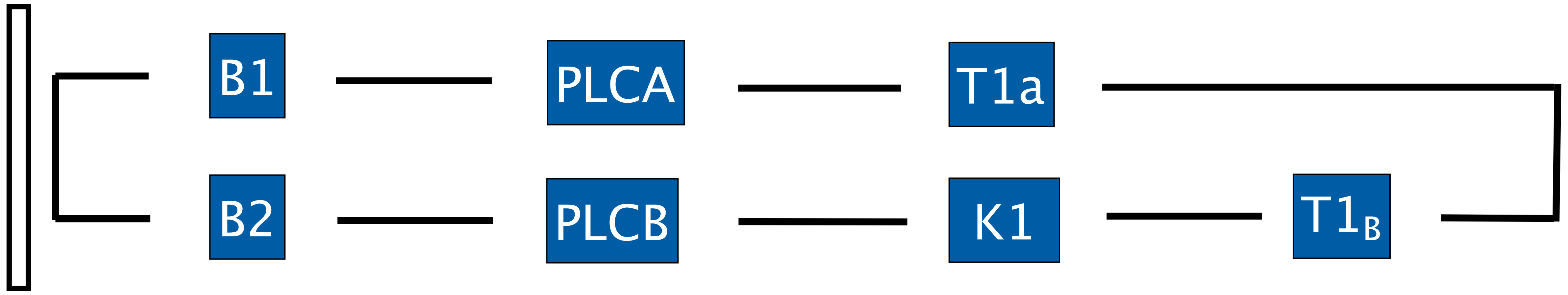
canal 1: $MTTF_d$ = 13,64 y



Calculation of $MTTF_d$ for canal 2

d_{op}: 240
h_{op}: 24
t_{cycle}: 3600

- **B2:**
- **PLCA: $MTTF_d$ = 25 years (data from producer)**
- **Relay K1: $MTTF_d$ = 570 years**
- **Inverter T1b :$MTTF_d$ = 570 years**



$$\frac{1}{MTTF_{dB}} = \frac{1}{MTTF_{dB2}} + \frac{1}{MTTF_{dPLCB}} + \frac{1}{MTTF_{dK1}} + \frac{1}{MTTF_{dT1b}}$$

	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 $MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}}$

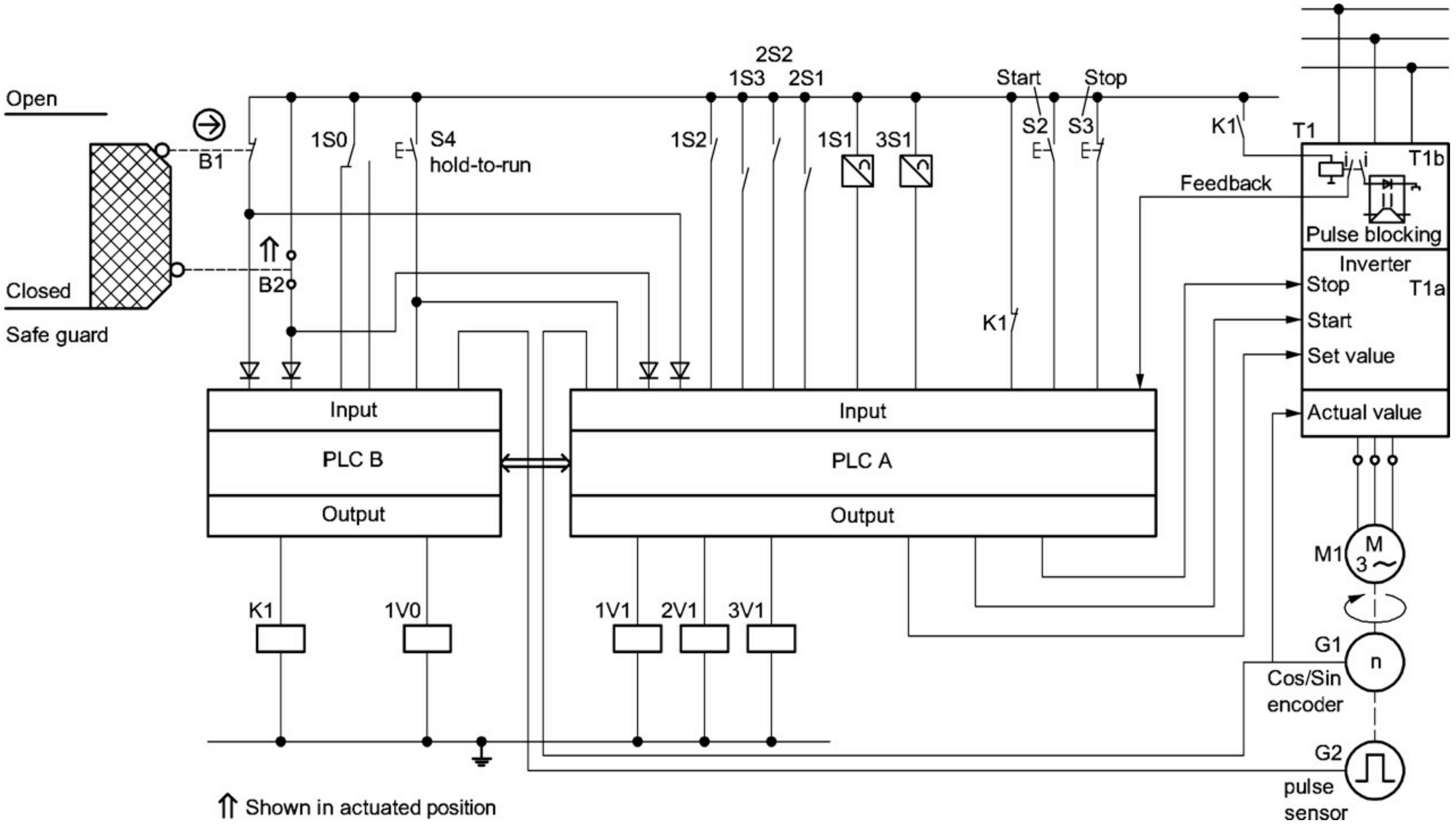
Kanal 2: $MTTF_d$ = 22,99 years

Determination of $MTTF_d$ for redundant according to annex D :

$$MTTF_d = \frac{2}{3}\left[MTTF_{Dcanal1} + MTTF_{Dcanal2} - \frac{1}{\frac{1}{MTTF_{Dcanal1}} + \frac{1}{MTTF_{Dcanal2}}}\right]$$

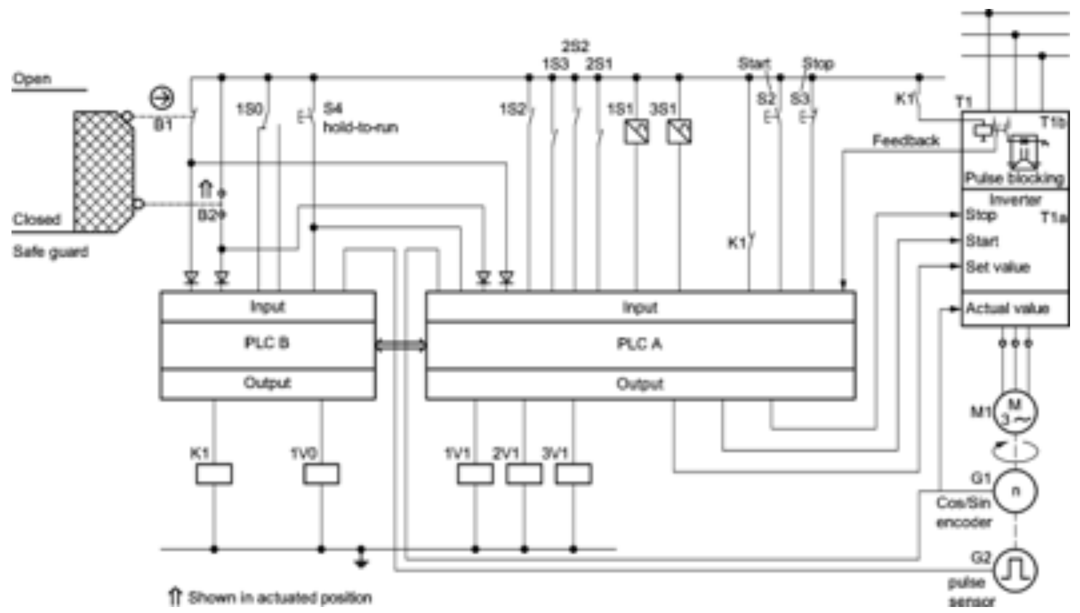
$$MTTF_d = \frac{2}{3}\left[13{,}64 + 22{,}99 - \frac{1}{\frac{1}{13{,}64} + \frac{1}{22{,}99}}\right]$$

→ $MTTF_d = 18{,}07a$

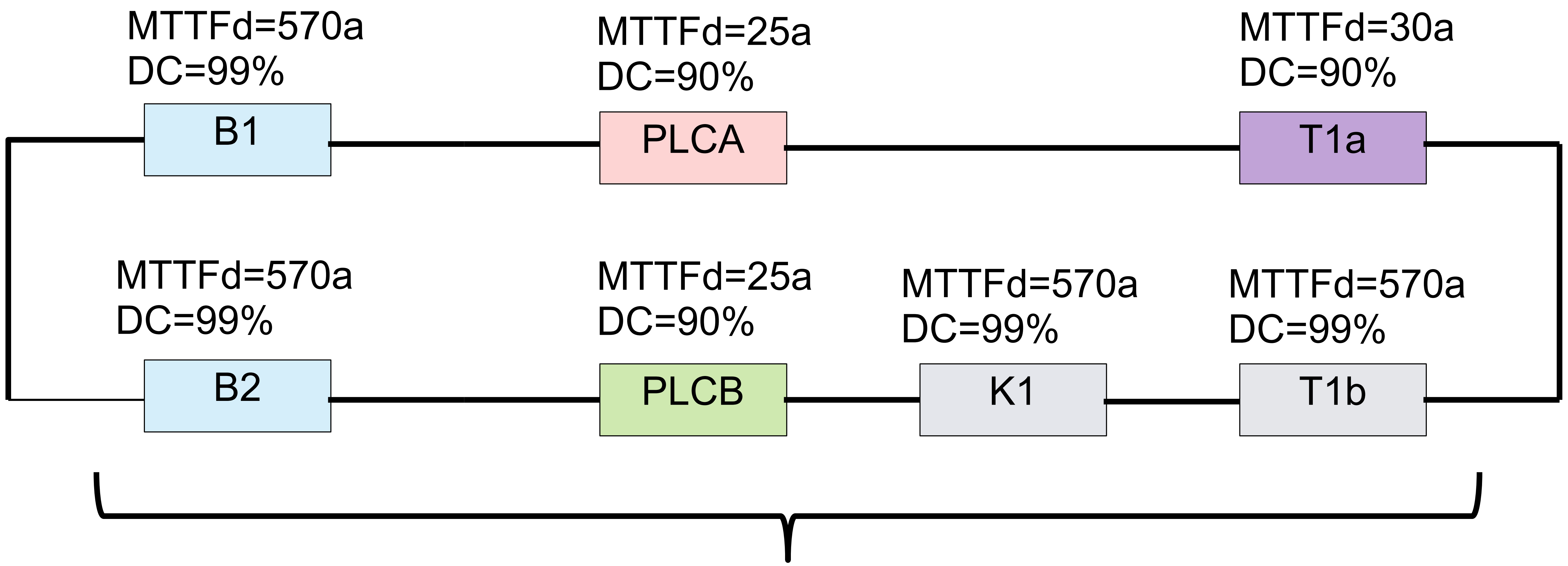


Open
Closed
Safe guard
B1
B2
1S0
S4
hold-to-run
2S2
1S3
2S1
1S2
1S1
3S1
Start
Stop
S2
S3
K1
T1
T1b
Feedback
Pulse blocking
Inverter
Stop
T1a
Start
Set value
Actual value
Input
PLC B
Output
Input
PLC A
Output
K1
1V0
1V1
2V1
3V1
M1
M
3 ~
G1
n
Cos/Sin
encoder
G2
pulse
sensor
Shown in actuated position

SRP/CS	DC (%)	Assessment
B1	99	Due to normally open and normally closed mechanical linked contacts
B2	99	Due to normally open and normally linked contacts
K1	99	Due to normally open and normally closed mechanical linked contacts
PLCA	90	Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demands it, through an input facility.
PLCB	90	Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demands it, through an input facility.
Inverter T1a	90	Fault is recognized by PLC B through reading of G2 when the safety function is demanded. Fault is recognized also by PLC A through reading of G1 at an operational stop of the electric motor M1 or when the safety function is demanded.
Inverter T1b	99	Indirect monitoring (monitoring of relay K1)



$MTTF_d$ [a]	Kat.3 DC_{avg} = mittel	
12	$1{,}04\ 10^{-6}$	c
13	$9{,}21\ 10^{-7}$	d
15	$7{,}44\ 10^{-7}$	d
16	$6{,}76\ 10^{-7}$	d
18	$5{,}67\ 10^{-7}$	d
20	$4{,}85\ 10^{-7}$	d
22	$4{,}21\ 10^{-7}$	d
24	$3{,}70\ 10^{-7}$	d
27	$3{,}10\ 10^{-7}$	d
30	$2{,}65\ 10^{-7}$	d
33	$2{,}30\ 10^{-7}$	d
36	$2{,}01\ 10^{-7}$	d
39	$1{,}78\ 10^{-7}$	d



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

$MTTFd_{gesamt}$ =18,07a
Dc_{gesamt}=90,52%
PFH=$5{,}42\ 10^{-7}$ (Berechnung mit Systema)

$$DCavg = \frac{\frac{DCdB1}{MTTFdB1}+\frac{DCdB2}{MTTFdB2}+\frac{DCdPLCA}{MTTFdPLCA}+\frac{DCdPLCB}{MTTFdPLCB}+\frac{DCdK1}{MTTFdK1}+\frac{DCdT1a}{MTTFdT1a}+\frac{DCdT1b}{MTTFdT1b}}{\frac{1}{MTTFdB1}+\frac{1}{MTTFdB2}+\frac{1}{MTTFdPLCA}+\frac{1}{MTTFdPLCB}+\frac{1}{MTTFdK1}+\frac{1}{MTTFdT1a}+\frac{1}{MTTFdT1b}}$$

CCF: Common Cause Fault

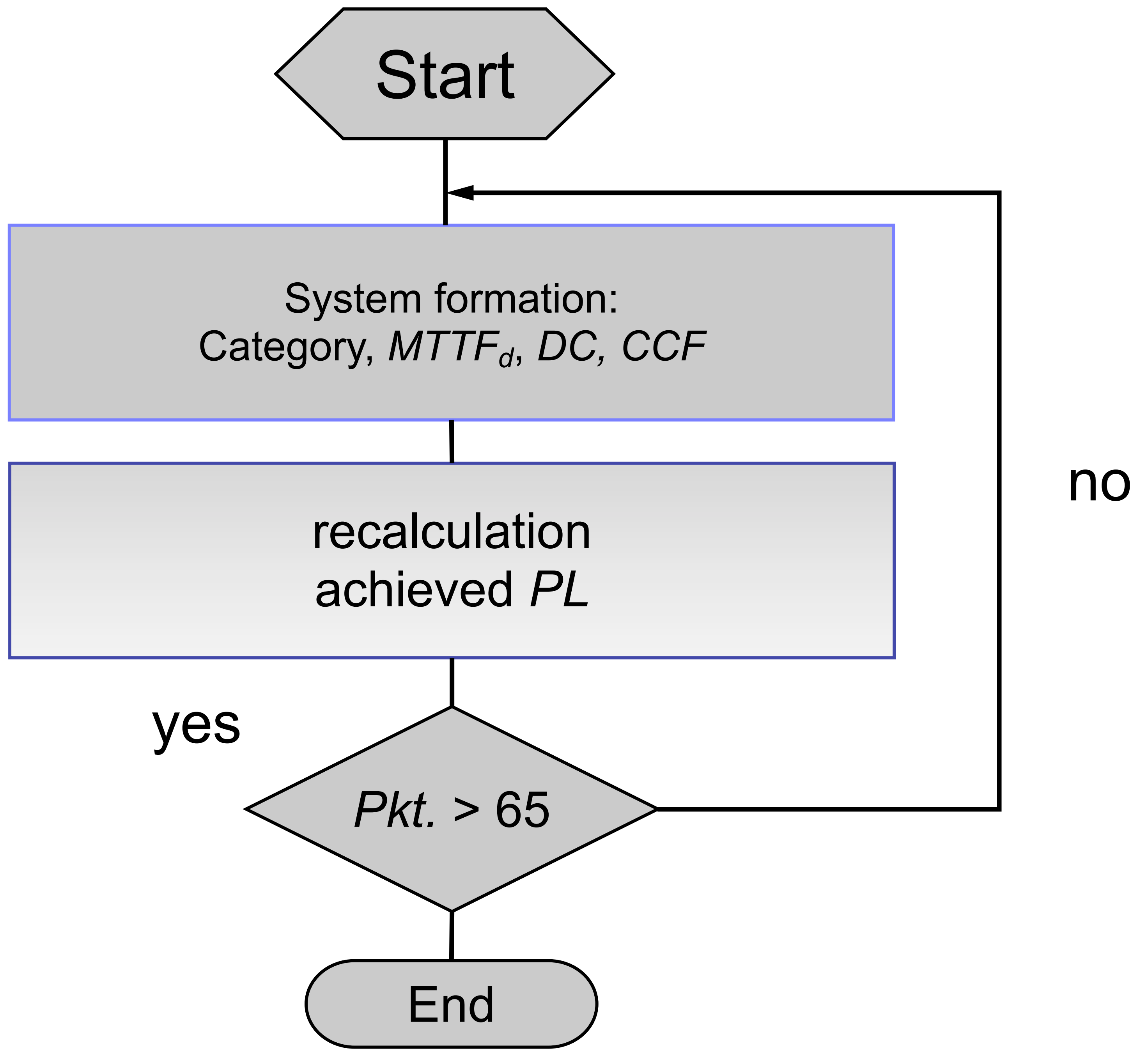
For redundant control systems (Cat. 2, 3 and 4) the probability of common cause failure of a SRP/CS shall be taken into account, (IEC 61508-6, Annex D of Beta-Factor from 2%)

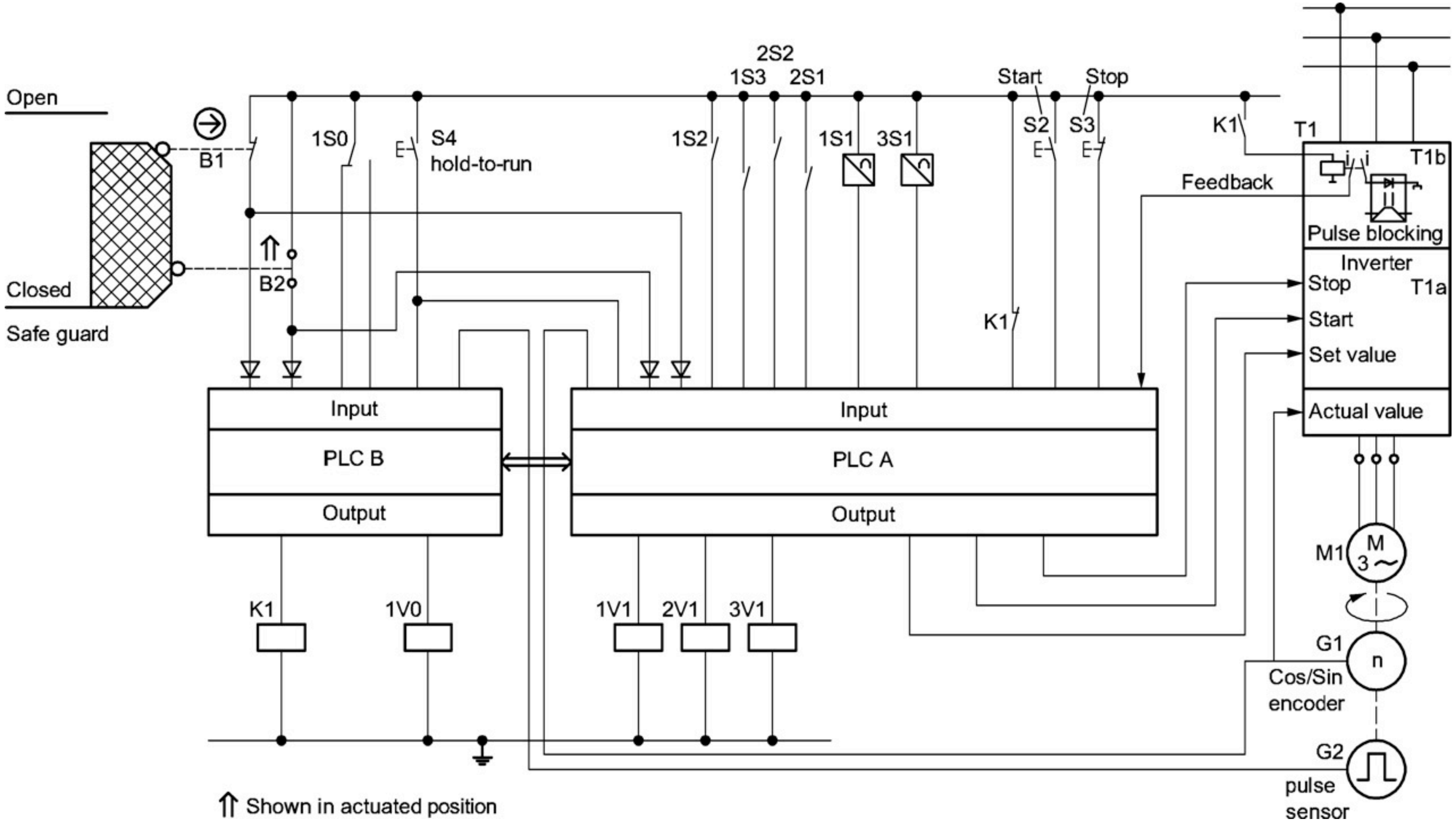
or be less:

point system minimum 65 points

■ Physical separation between channels	15 points
■ Diversity	20 points
■ Design (e.g. Protection against overload, over current)	15 points
■ Well tried components	5 points
■ FMEA	5 points
■ Competence/Training of designer	5 points
■ Environmental - EMC	25 points
■ Other influences, e.g. temperature, shock, etc.	10 points

goal: minimum 65 points





Open
Closed
Safe guard
B1
B2
1S0
S4
hold-to-run
1S2
2S2
1S3
2S1
1S1
3S1
Start
Stop
S2
S3
K1
T1
T1b
Feedback
Pulse blocking
Inverter
Stop
T1a
Start
Set value
Actual value
Input
PLC B
Output
Input
PLC A
Output
K1
1V0
1V1
2V1
3V1
M1
M
3 ~
G1
n
Cos/Sin
encoder
G2
pulse
sensor
Shown in actuated position

Stop function initiated by opening the interlocked guard

Component/unit	Potential fault	Fault detection	Effect/reaction	Test for conformation
Interlocking switch B1	Contact does not open when the guard is opened (mechanical faults).[a]	Fault is recognized independently by PLC A and PLC B through signal change in B2 when the safety function is demanded (opening of the safety guard, plausibility check).	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs before the guard is opened.
Interlocking switch B2	Contact does not open when the guard is opened (electrical or mechanical faults)	Fault is recognized independently by PLC A and PLC B through signal change in B1 when the safety function is demanded (opening of the safety guard, plausibility check).	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs before the guard is opened.
Interlocking switch B2	Spontaneous contact closure while the guard is open (mechanical faults).	Fault is recognized independently and immediately by PLC A and PLC B as a result of there being no corresponding signal change in B1.	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs while the guard is open.

A plausibility check of B1 and B2 by PLC A and PLC B gives a DC of 99 % for B1 (see ISO 13849-1:2006, Table E.1).

Component/unit	Potential fault	Fault detection	Effect/reaction	Test for conformation
PLCA	Stuck-at fault at the input/ output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC A from sending a stop command to T1a before or when the guard is opened.	Fault is recognized by PLC B through reading of G2 to compare its time-related signal with the expected change in the number of revolutions. Some faults (e.g. output cards) are recognized by PLC A through reading of G1 at an operational stop of the electric motor M1 or when the safety function is demanded. Other faults can be detected early by the internal watchdog (WDa) function of PLC A.	Electric motor M1 is stopped by PLC B via K1 and T1b after a time delay when the guard is opened, and re-start is prevented. In the case of faults detected by PLC A through reading of G1 during the operational stop, PLC A informs PLC B. As a result of reporting PLC B, the electric motor M1 is stopped and re-start is prevented by PLC B. In the case of faults detected by WD, PLC A tries to stop electric motor M1 and prevent the re-start via T1a before the safety function is demanded or before electrical motor M1 comes to an operational stop, and then to inform PLC B.	Apply a static high level at the stop output of PLC A before the guard is open.
Failure of the PLCA	Stuck-at fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which removes the PLC A stop command from T1a while the guard is open.	Faults cannot be recognized by PLC B through reading of G2 because the motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. Some faults (e.g. output cards) are recognized by PLC A through reading of G1 on closing the guard. The above and additional faults are detected by operator through process observation on closing the guard, or by PLC B when the safety function is next demanded (opening of the guard). Other faults can be detected early by WDa function of PLC A.	Electric motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. In the case of faults detected by PLC A through reading of G1 on closing the guard, PLC A informs PLC B. As a result of reporting PLC B, the unintended start-up of electric motor M1 is prevented by PLC B. In the case of faults detected by WD, PLC A tries to keep electric motor M1 stopped, to prevent the re-start via T1a, and to inform PLC B.	Electric motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. In the case of faults detected by PLC A through reading of G1 on closing the guard, PLC A informs PLC B. As a result of reporting PLC B, the unintended start-up of electric motor M1 is prevented by PLC B. In the case of faults detected by WD, PLC A tries to keep electric motor M1 stopped, to prevent the re-start via T1a, and to inform PLC B.

Component/unit	Potential fault	Fault detection	Effect/reaction	Test for conformation
T1A	Stuck-at fault and other complex internal faults in control and power electronics of the inverter, which prevent T1a from stopping the motor before or when the guard is opened.	Fault is recognized by PLC B through reading of G2 when the safety function is demanded. Fault is recognized also by PLC A through reading of G1 at an operational stop of the electric motor M1 or when the safety function is demanded.	Electric motor M1 is stopped by PLC B via K1 and T1b after a time delay when the guard is opened, and re-start is prevented. PLC A informs PLC B when a fault is recognized during the operational stop. As a result of reporting PLC B, the electric motor M1 is stopped and re-start is prevented by PLC B.	Set the stop-input of the inverter to high before or when the guard is opened.
T1A	Stuck-at fault and other complex internal faults in control and power electronics of the inverter, which provides gate signals to power semiconductors of T1a, while the guard is open.	Fault cannot be recognized by PLC B through reading of G2 because the motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. Fault will be detected by operator through process observation on closing of the guard. Fault is also recognized by PLC A through reading of G1 on closing the guard.	Electric motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. On closing the guard an un-intended start-up of the motor occurs (non-hazardous). PLC A informs PLC B when a fault is recognized. As a result of reporting PLC B, the unintended start-up of electric motor M1 is prevented and re-start is prevented by PLC B.	Transfer the start signal to the inverter while the guard is open.

Component/unit	Potential fault	Fault detection	Effect/reaction	Test for conformation
PLCB	Stuck-at fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC B from switching off K1 before or when the guard is opened.	Fault is recognized by PLC A monitoring of K1 mechanically-linked feedback contact when the safety function is demanded. Some faults can be detected early by the WDa function of PLC B.	Electric motor M1 is immediately stopped by PLC A via T1a when the guard is opened and re-start is prevented. In the case of faults detected by WD, PLC B tries to inform PLC A and then to stop the electric motor M1 and prevent the re-start via T1b before the safety function is demanded.	Keep K1 in the energized position when the guard is opened
PLCB	Stuck-at fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which removes the PLC B stop command from K1 while the guard is open.	Fault is immediately recognized by PLC A monitoring of K1 mechanically-linked feedback contact. Some faults can be detected early by the WDa function of PLC B.	Electric motor M1 is kept stopped by PLC A via T1a while the guard is open, and re-start is prevented. In the case of faults detected by WD, PLC B tries to keep stopped the electric motor M1 and prevent the re-start via T1b, and to inform PLC A.	Switch K1 to its energized position while the guard is open

Component/unit	Potential fault	Fault detection	Effect/reaction	Test for conformation
K1	The contact does not open when the guard is opened (electrical fault, e.g. welded contacts).	Fault is recognized by PLC A monitoring of K1 mechanically-linked feedback contact when the safety function is demanded.	Electric motor M1 is immediately stopped by PLC A via T1a when the guard is opened and re-start is prevented.	Keep K1 contact in the ON position when the guard is opened.
Inverter T1b	Non-opening of internal relay contact when the guard is opened.	Fault is recognized by PLC A monitoring of mechanically-linked feedback contact for T1b internal relay when the safety function is demanded.	Electric motor M1 is immediately stopped by PLC A via T1a when the guard is opened and re-start is prevented.	Keep the input of the coil of blocking relay in T1b to high level when the guard is opened.

Thank you very much for your attention !!!