QUANTIFICATION [ISO 13849]
EXAMPLE OF APPLICATION

SICK
Sensor Intelligence.

Otto Görnemann

Research & Development

Rev. 1V1.e

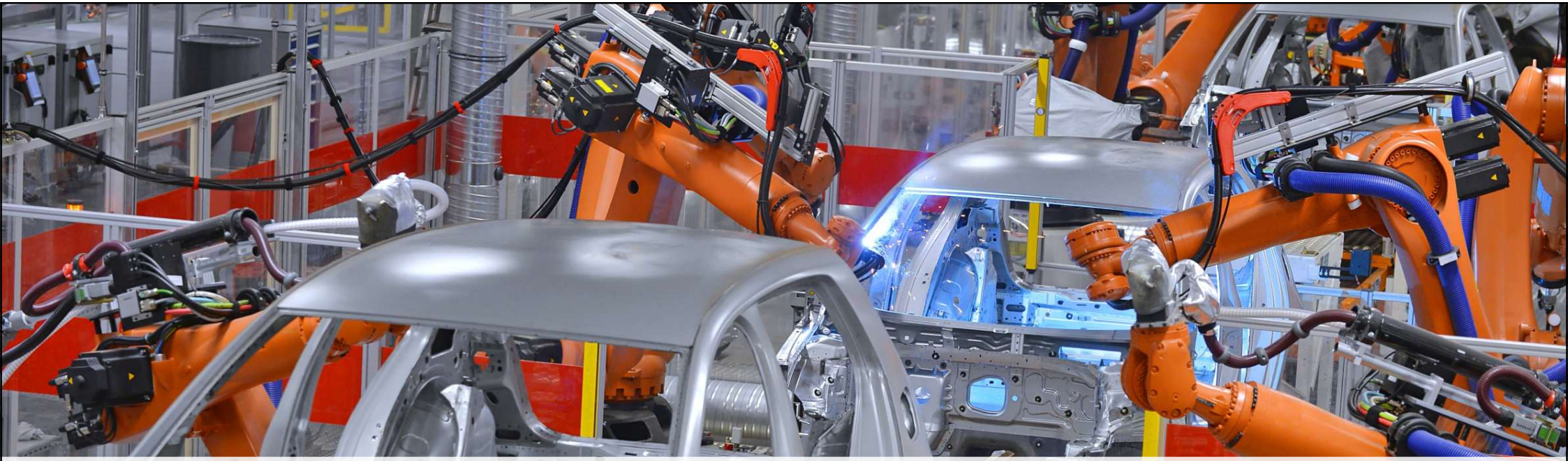
WE ARE ONE OF THE WORLD'S LEADING COMPANIES

SICK
Sensor Intelligence.

WE DEVELOP SENSOR SOLUTIONS FOR CUSTOMERS AROUND THE GLOBE

- Over 50 subsidiaries worldwide
- Around EUR 2 billion sales in 2021
- More than 12,000 employees

- Your speaker : Otto Görnemann
- Since 1995 employee of SICK AG
- Functional Safety Expert
  (TÜV Rheinland, #263/16, Machinery)
- Functional Safety Trainer
  CFSA E-T Trainer (SGS - TÜV Saar #13)
- **Chairperson of ISO/TC199 – Safety of Machinery**
- **Chairperson of CEN/TC114 – Safety of Machinery**
- Nominated Expert at ISO/TC299-WG3 (Industrial Robots)
- Nominatec Expert at ISO/TC110-SC10 (Safety of Industrial Trucks)
- Nominatec Expert at ISO/TC039-SC2 (Safety of Tooling Machines)



INDUSTRIAL ROBOT CELL – ISO 10218-2

SICK
Sensor Intelligence.

01

Origin

moving elements

Potential consequences

- crushing
- impact
- shearing

NEW ALTERNATIVE IN THE ONGOING REVISION

ISO 10218-2:2011

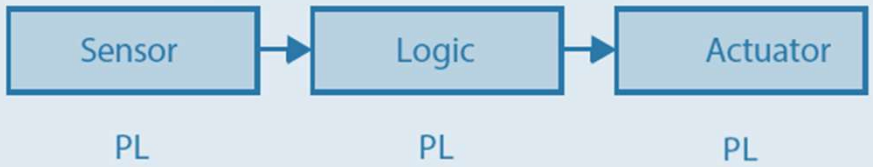
5.2.2. Performance requirement

Safety-related parts of control systems shall be designed so that they comply with **PL=d with structure category 3** as described in ISO 13849-1:2006, or so that they comply with **SIL 2 with hardware fault tolerance of 1** with a proof test interval of not less than 20 years as described in IEC 62061:2005.

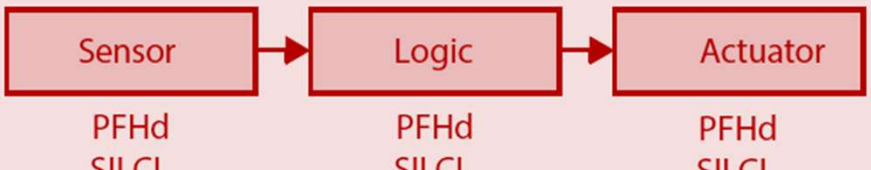
DETERMINING THE SAFETY LEVEL
VERIFICATION OF FUNCTIONAL SAFETY

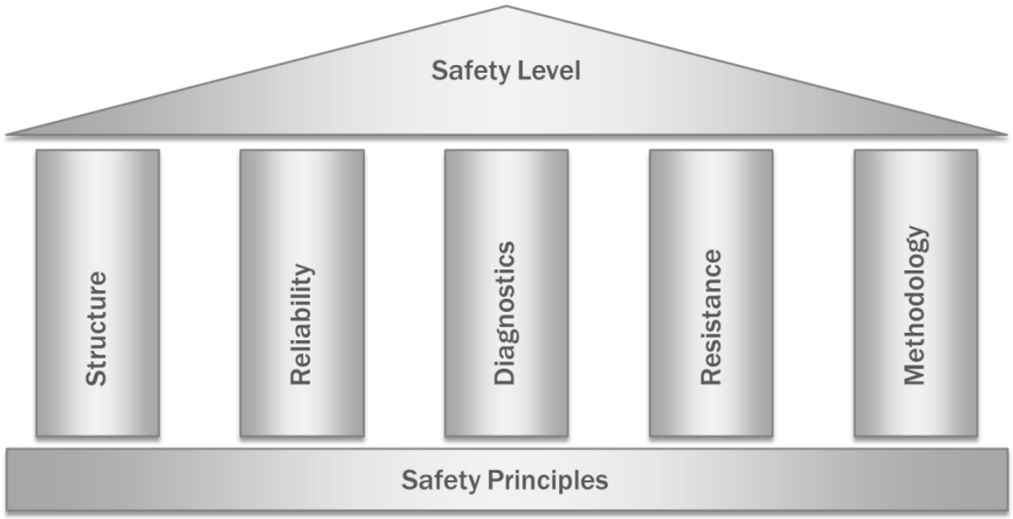
SICK
Sensor Intelligence.

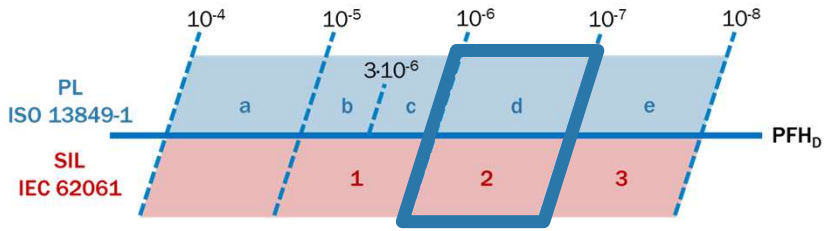
ISO 13849-1



IEC 62061

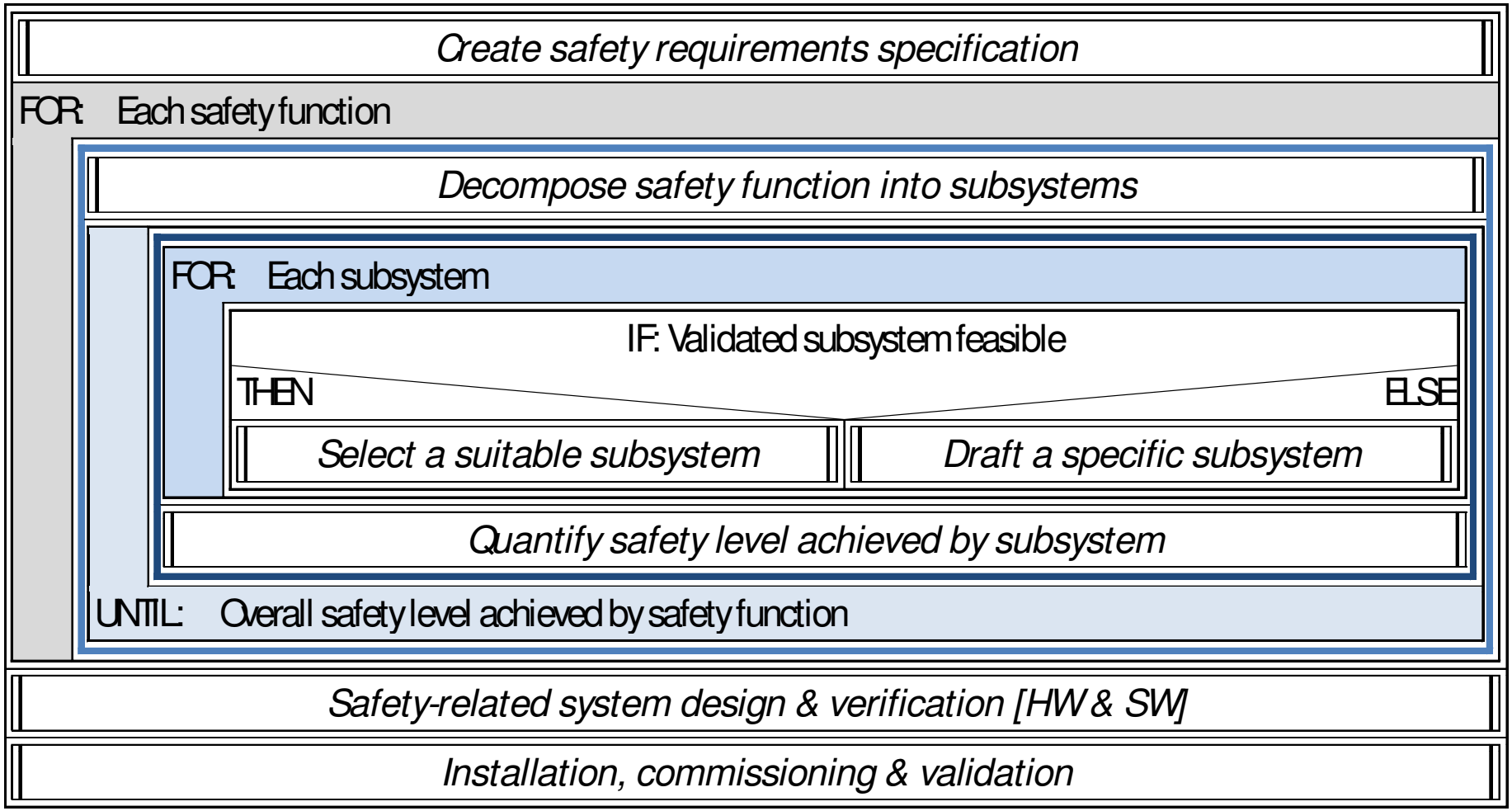






SAFETY-RELATED CONTROL SYSTEMS

THINKING IN SAFETY FUNCTIONS



SAFETY CONCEPT

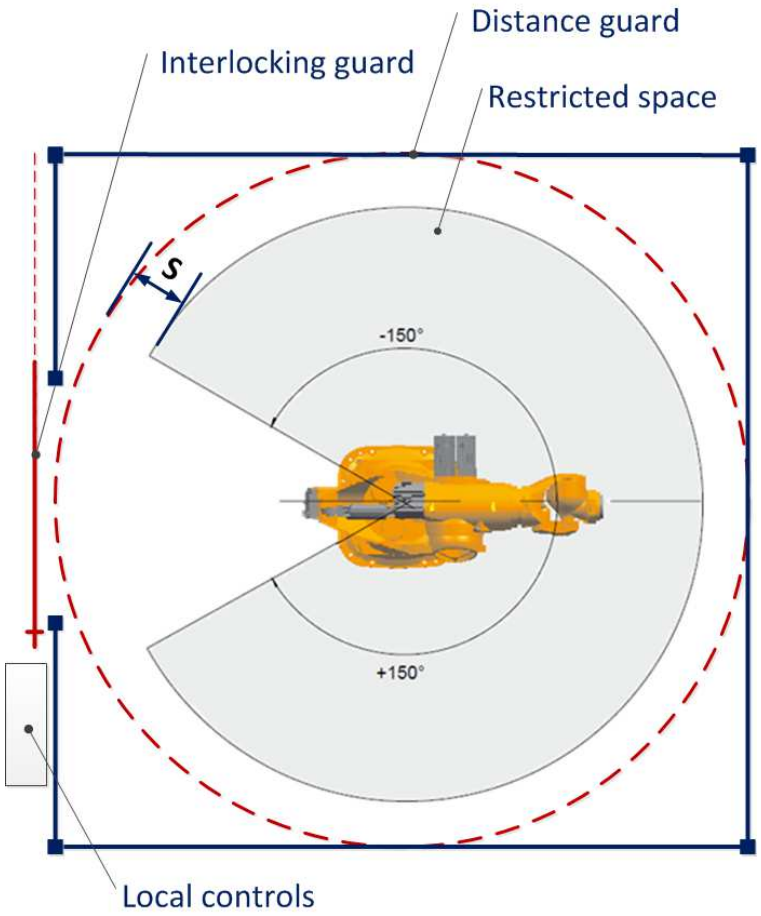
SICK
Sensor Intelligence.

02

SAFETY REQUIREMENTS SPECIFICATION
ACCESS FOR INTERVENTIONS (ACC. TO ISO 13849-1)

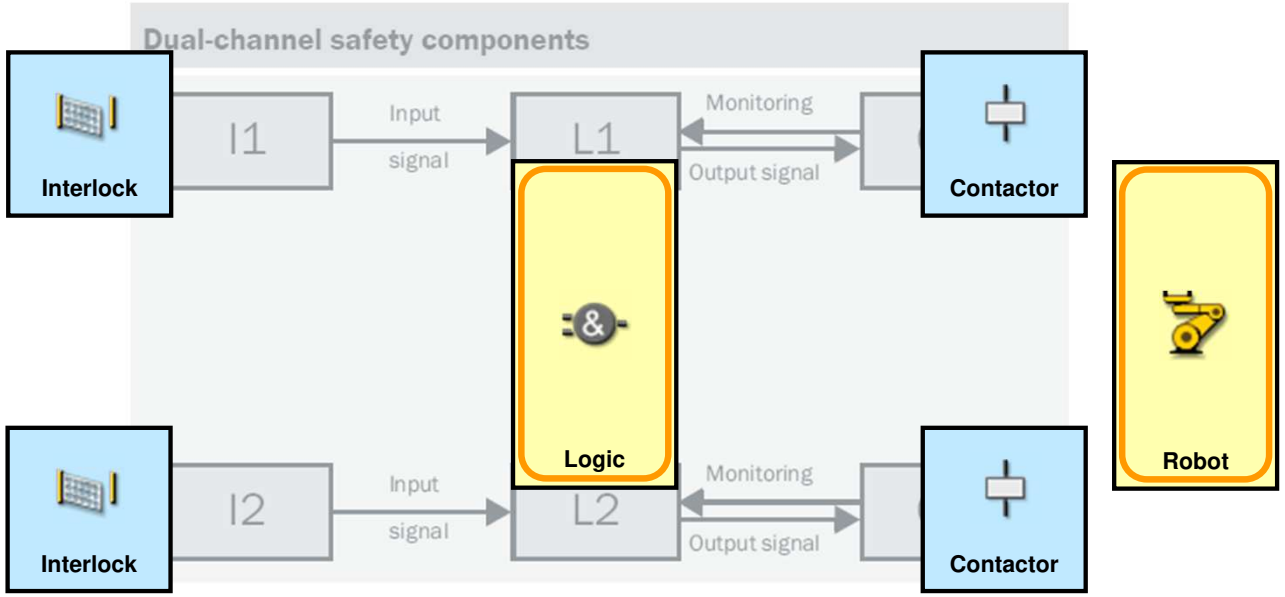
Dual channel system

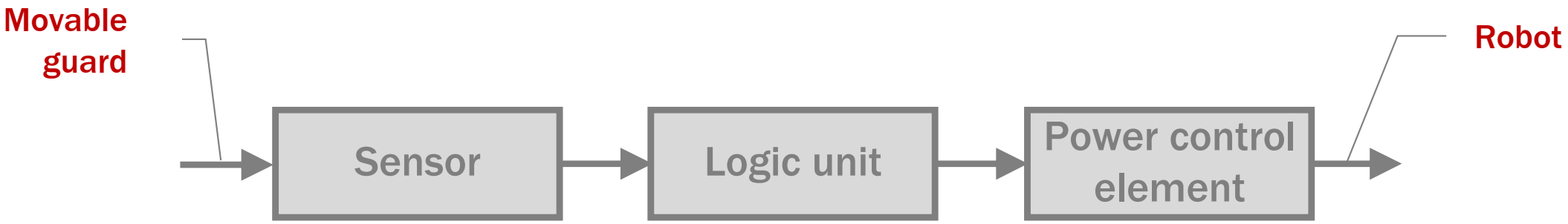
SF01:	Initiating a stop	PL_r d, cat. 3 SIL 2, HFT 1
SF02:	Avoiding unexpected start-up	PL_r d, cat. 3 SIL 2, HFT 1
SF03:	Temporarily preventing access	PL_r d, cat. 3 SIL 2, HFT 1



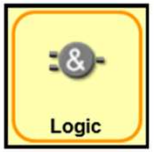
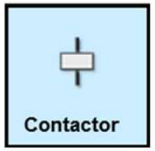
SAFETY FUNCTION SF01

DECOMPOSE SAFETY FUNCTION INTO SUBSYSTEMS





SAFETY CONCEPT
SAFETY FUNCTION SF01

SF01	Initiating a stop						PL$_r$ d
Subsystems .1							
Subsystems .2							
Identifier			*T01*	*L01*	*R01a*	*R01b*	
Requirements			Type 1 Type 2		EDM	SS1	

Trigger	Opening of the interlocking movable guard	1 / h	[frequency of demand]
Condition	At any time		
Reaction	Stopping the machine		
Safe state	Standstill	1 s	[overall stopping performance]

T01: type acc. to EN ISO 14119:2013

HARDWARE CONCEPT

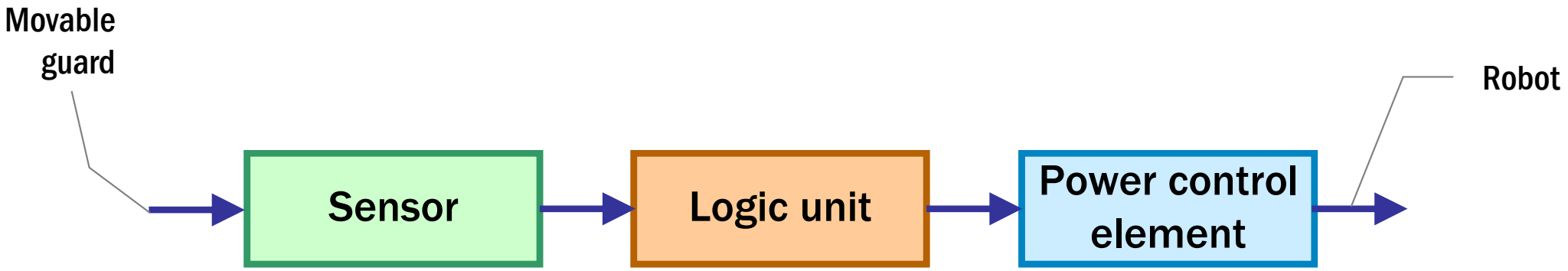
SICK
Sensor Intelligence.

03

SAFETY FUNCTION SF01
SELECTION OF PROTECTIVE DEVICES

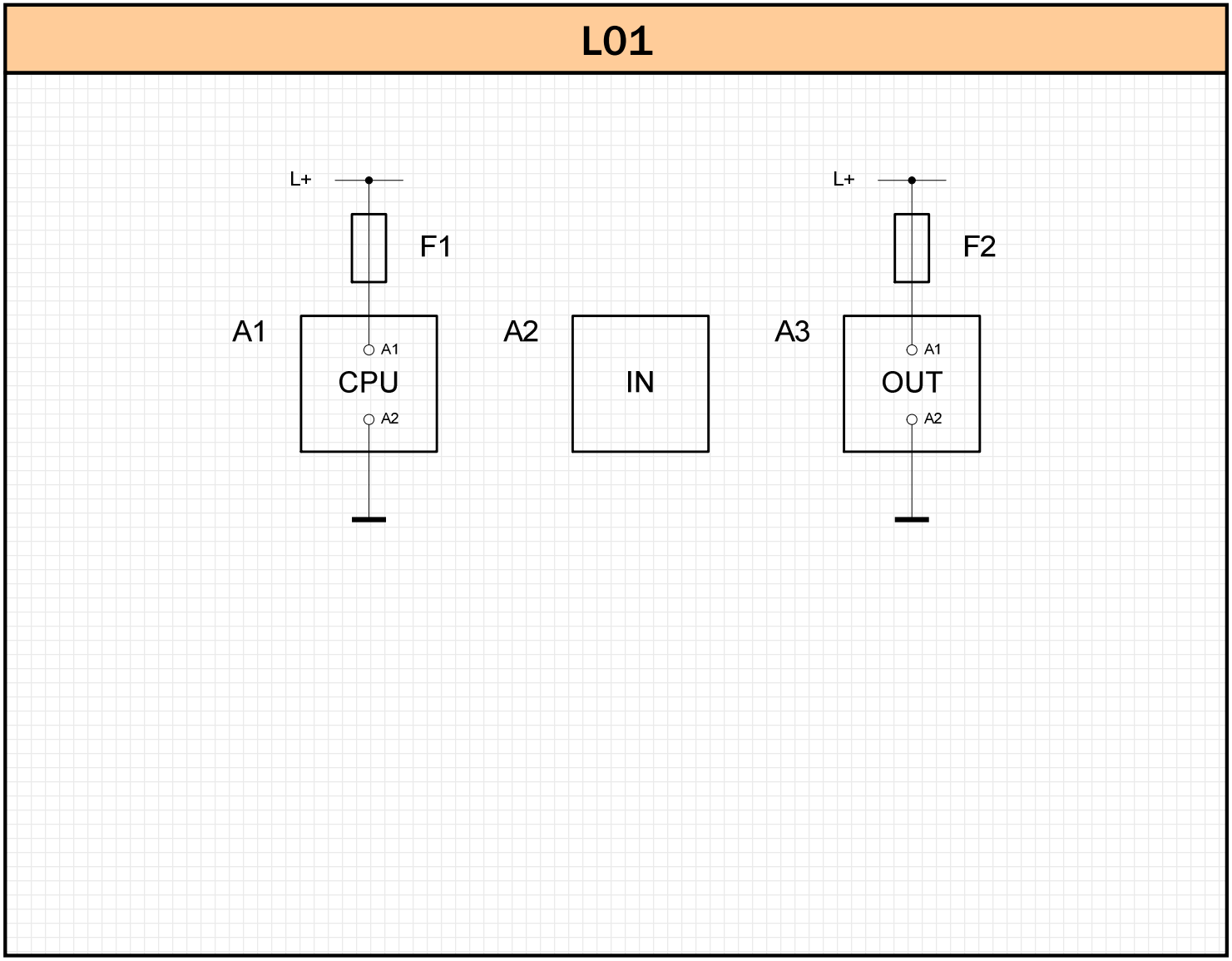




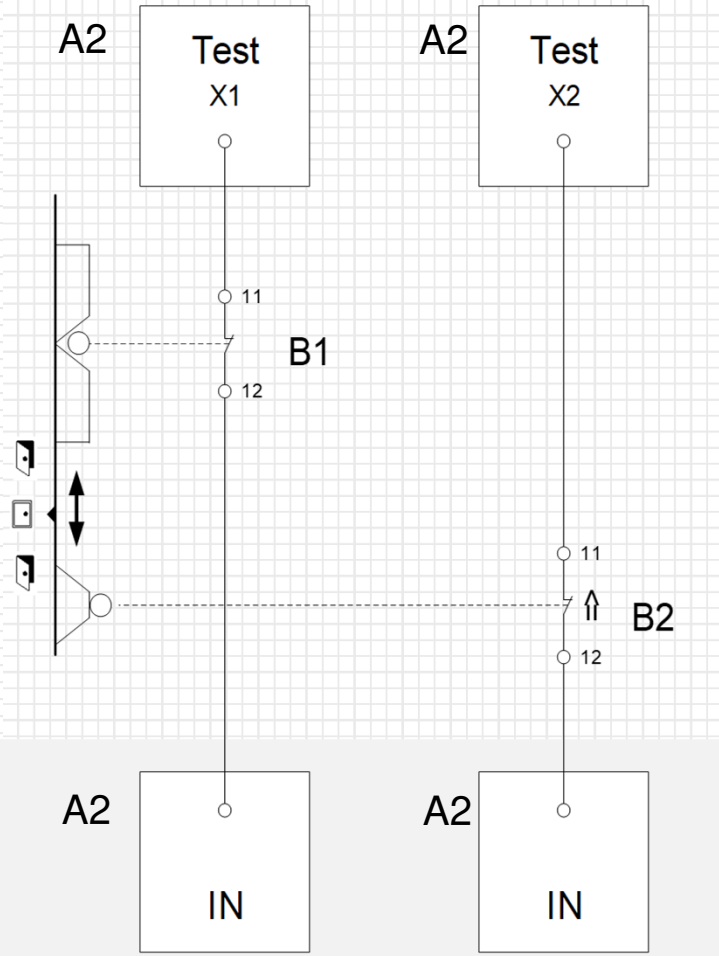
HW SKETCH “LOGIC UNIT”

LOGIC PROCESSING SUBSYSTEMS



HW SKETCH “SENSOR”
SAFETY TRIGGERING SUBSYSTEMS

T01

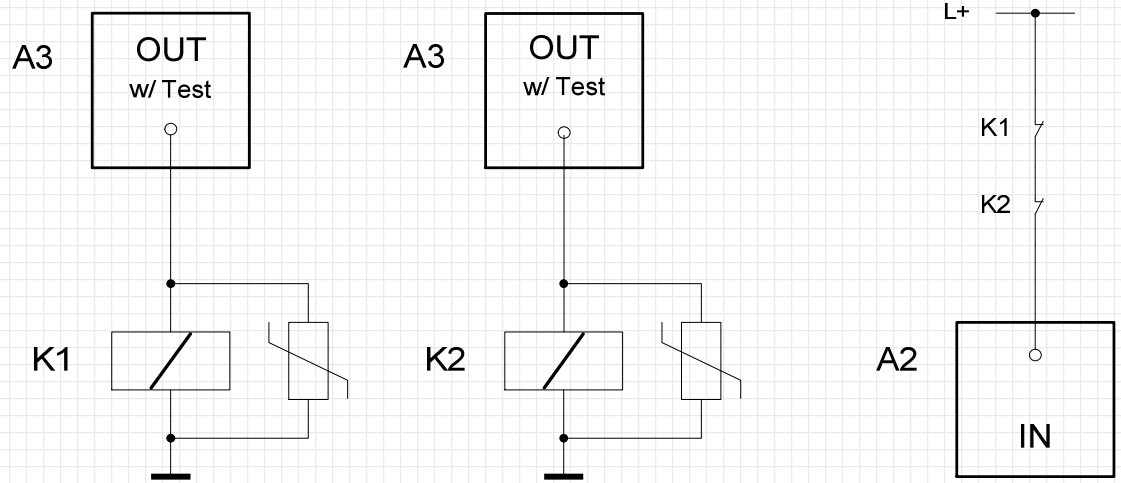


Dual channel equivalent
Discrepancy time 3s.

HW SKETCH “POWER CONTROL ELEMENT”

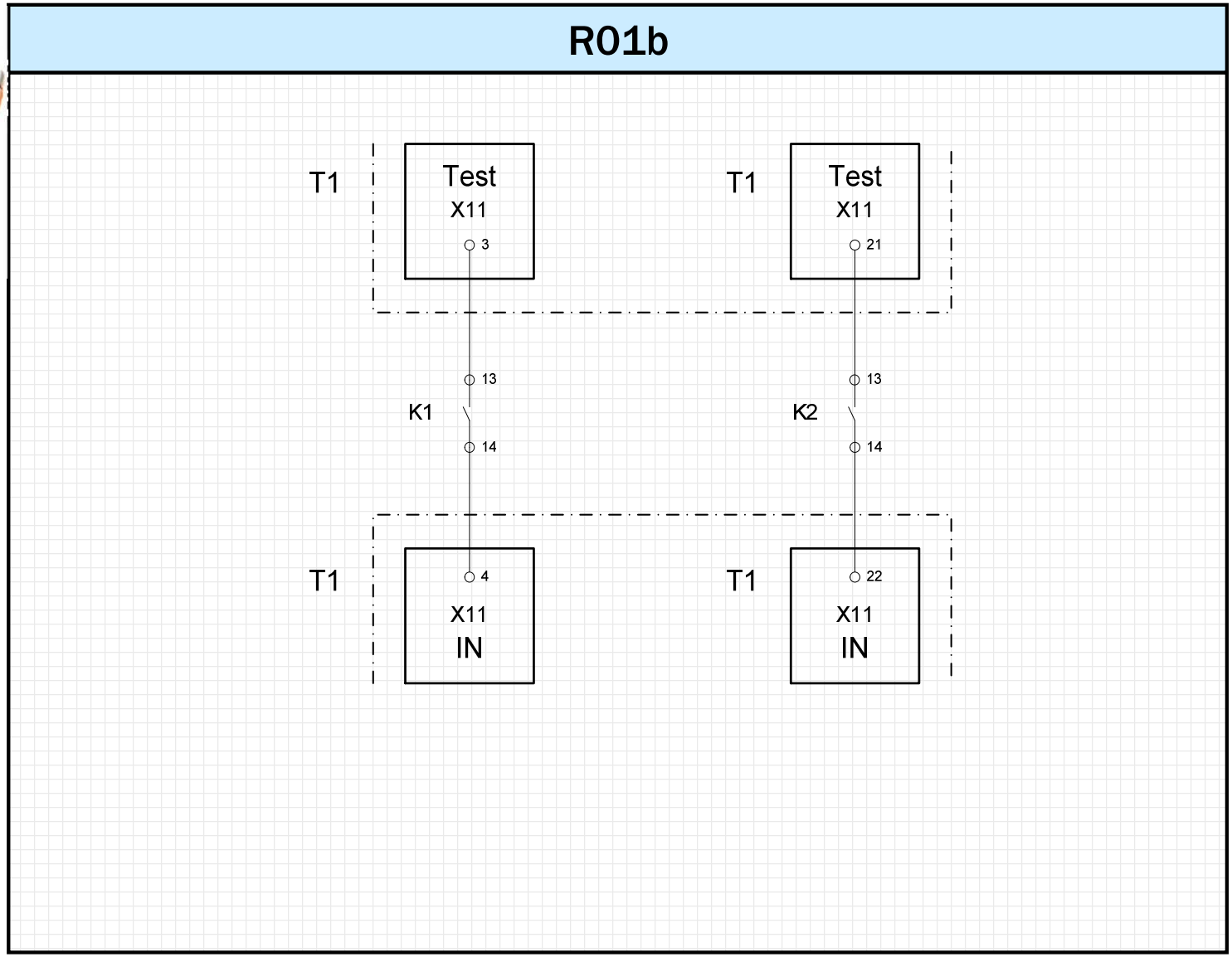
REACTION ACTUATING SUBSYSTEMS

R01a



HW SKETCH “POWER CONTROL ELEMENT”

REACTION ACTUATING SUBSYSTEMS



DETERMINE PL FOR SRP/CS

SICK
Sensor Intelligence.

04

DATA SHEET SICK AG FX3-CPU0

SUBSYSTEM L01a

	FX3-CPU0	FX3-CPU1/2/3
Safety Integrity Level[26)]	SIL3 (IEC 61508)	
SIL claim limit[26)]	SILCL3 (EN 62061)	
Category	Category 4 (EN ISO 13849-1)	
Performance Level[26)]	PL e (EN ISO 13849-1)	
PFHd	1.07×10^{-9}	
PFHd for Flexi Line station[27)]	–	
T_M (mission time)	20 years (EN ISO 13849)	

DATA SHEET SICK AG FX3-XTDI

SUBSYSTEM L01b

Safety Integrity Level[38)]	SIL3 (IEC 61508)
SIL claim limit[38)]	SILCL3 (EN 62061)
Category	Category 4 (EN ISO 13849-1)
Performance Level[38)]	PL e (EN ISO 13849-1)
PFHd	0.4×10^{-9}
T_M (mission time)	20 years (EN ISO 13849)

Safety Integrity Level[28)]	SIL3 (IEC 61508)
SIL claim limit[28)]	SILCL3 (EN 62061)
Category[29)] For dual channel outputs with or without test pulses disabled for this or any other safe output (Q1...Q4)	Category 4 (EN ISO 13849-1)
Performance Level[28)]	PL e (EN ISO 13849-1)
PFHd[29)] For dual channel outputs	0.9×10^{-9}
T_M (mission time)	20 years (EN ISO 13849)[30)]

DATA SHEET SICK AG i10 LOCK /i10-R

SUBSYSTEM T01

Safety-related parameters	
B_{10d} parameter	3 x 10^6 switching cycles (with small load)
Type	Type 2 (EN ISO 14119)

Mechanical service life	10 x 10^6 switching operations
$B10_d$	2x 10^6 switching operations with low load as per EN ISO 13849-1

SIEMENS STANDARD SN 31920:2012

SUBSYSTEM R01a

Contact load, utilization category		Normal B10 value (duty cycles)	Ratio of dangerous failures
Switching Devices – Contactors and Contactor Relays (only devices with positively driven contacts or mirror contacts allowed)			
SIRIUS-Contactor Relays and auxiliary switch block:			50 %
- Contactor Relays, Coupling Relays, 4-pole	3)	30,000,000	
- Contactor Relays with auxiliary switch block	3)	10,000,000	
- electronic compatible auxiliary switches, latched	3)	5,000,000	
Contactor Relays	AC-15/-14; 230 V DC-13; 24 V (< 0.3 x Ie)	1,000,000	73 %
	AC-15/-14; 230 V	200,000[11)]	73 %
	DC-13; 24 V	300,000[11)]	73 %

3) maximum value of B10 if the current is lower than 1% of the nominal value

DATA SHEET KUKA KR C4

SUBSYSTEM R01b

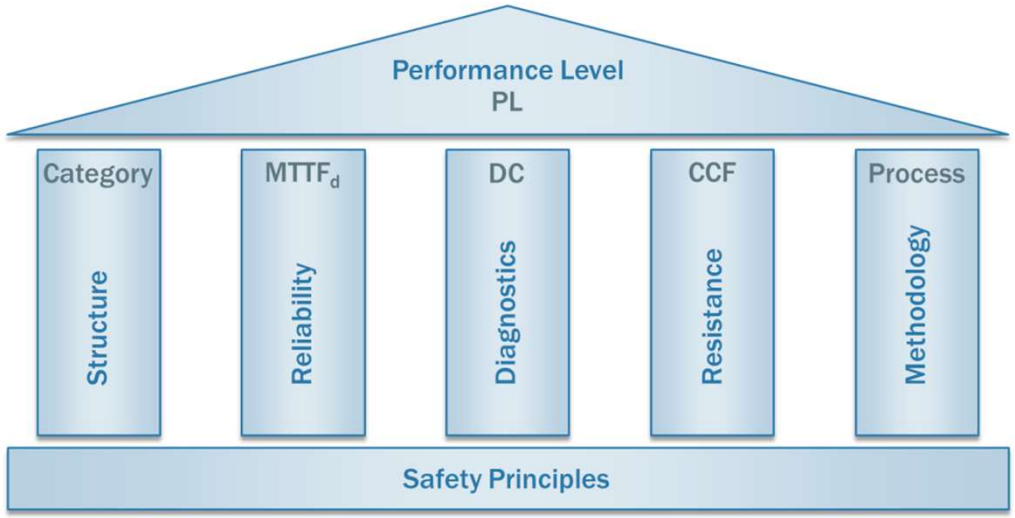
SICK
Sensor Intelligence.

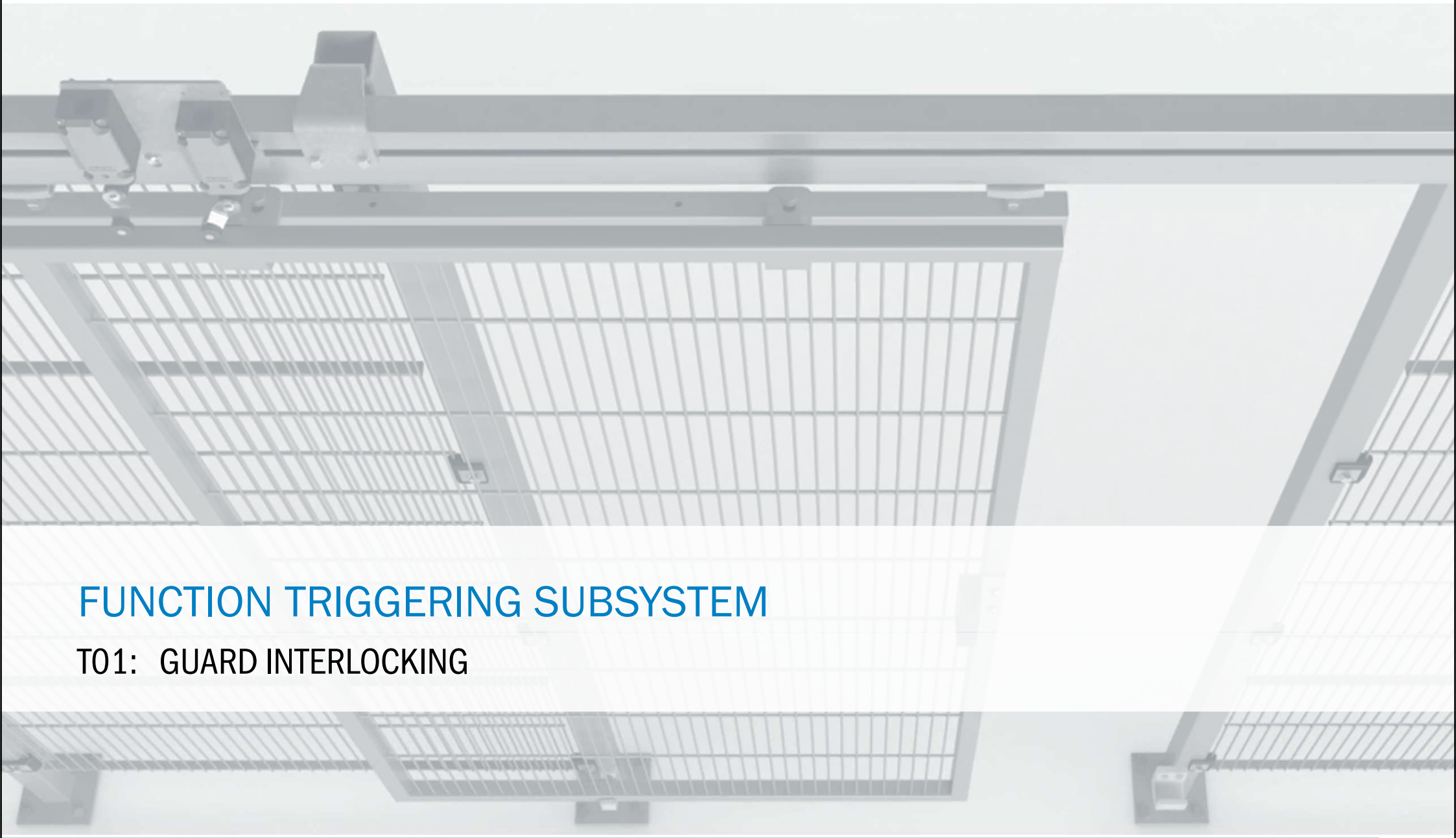
Robot controller variant	PFH value
KR C4; KR C4 CK	$< 1 \times 10^{-7}$

The safety functions of the robot controller conform to category 3 and Performance Level d according to EN ISO 13849-1.

Determining the level of safety for a **subsystem**:

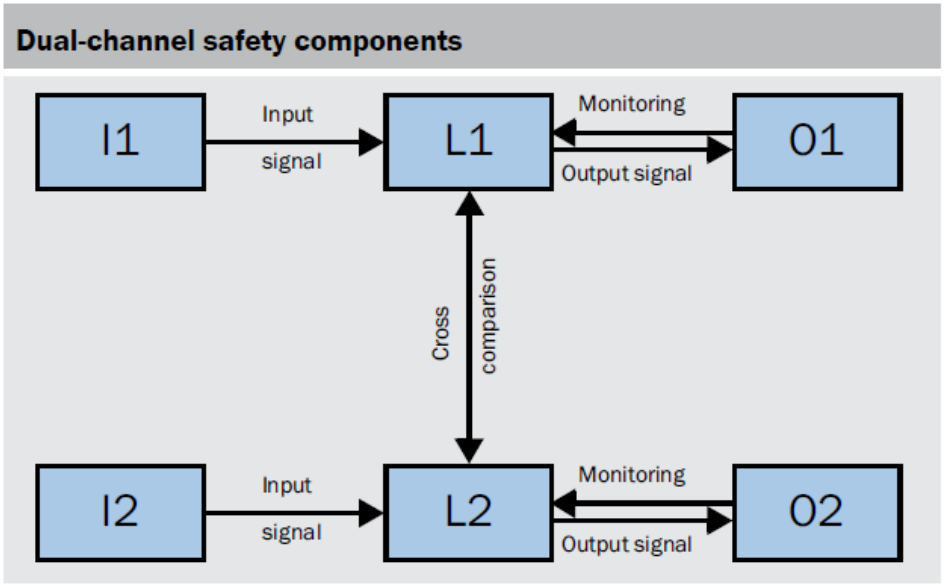
1. Delimitation of the subsystem
2. Determination of the category
3. Determination of the MTTFd per channel
4. Determination of DC
5. Evaluation of the measures to prevent common cause failures
6. Evaluation of process measures
7. Result: PL for the subsystem





FUNCTION TRIGGERING SUBSYSTEM

T01: GUARD INTERLOCKING



The structure of the subsystem is suitable for category 3/4 (dependent on DC and $MTTF_d$)

$MTTF_D$ PER CHANNEL
SUBSYSTEM T01.1

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

$$= \frac{3 \cdot 10^6}{0{,}1 \times 365\,d/y \times 24\,h/d \times 1/h}$$

$$= \frac{3 \cdot 10^6}{8.76/y}$$

$$\boxed{MTTF_D = 3.424y \geq 2.500\ y}$$

$$T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{MTTF_D}{10}$$

$$\boxed{T_{10D} = 342\ y}$$

$MTTF_D$ PER CHANNEL
SUBSYSTEM T01.2

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

$$= \frac{2 \cdot 10^6}{0{,}1 \times 365\,d/a \times 24\,h/d \times 1/h}$$

$$= \frac{2 \cdot 10^7}{8.760/a}$$

$$\boxed{MTTF_D = 2.283a}$$

$$T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{MTTF_D}{10}$$

$$\boxed{T_{10D} = 228a}$$

SYMMETRIZATION
SUBSYSTEM T01

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

$$= \frac{2}{3}\left[2.500a + 2.283a - \frac{1}{\frac{1}{2.500a} + \frac{1}{2.283a}} \right]$$

$$MTTF_D = 2.393\,a$$

Designation	Range
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

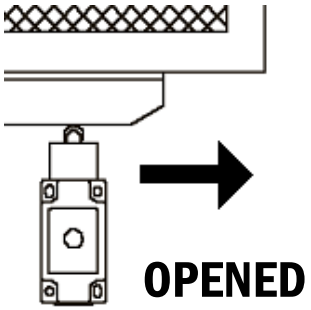
ESTIMATES FOR DIAGNOSTIC COVERAGE
SUBSYSTEM T01

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % 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 det	plication; nt for the
Monitorin analogue	

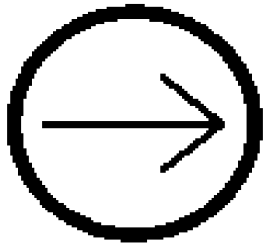
Designation	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

SICK
Sensor Intelligence.

- **Direct mechanical action (positive mechanical action)**
  - movement of a mechanical component which arises inevitably from the movement of another mechanical component either by direct contact or via rigid elements



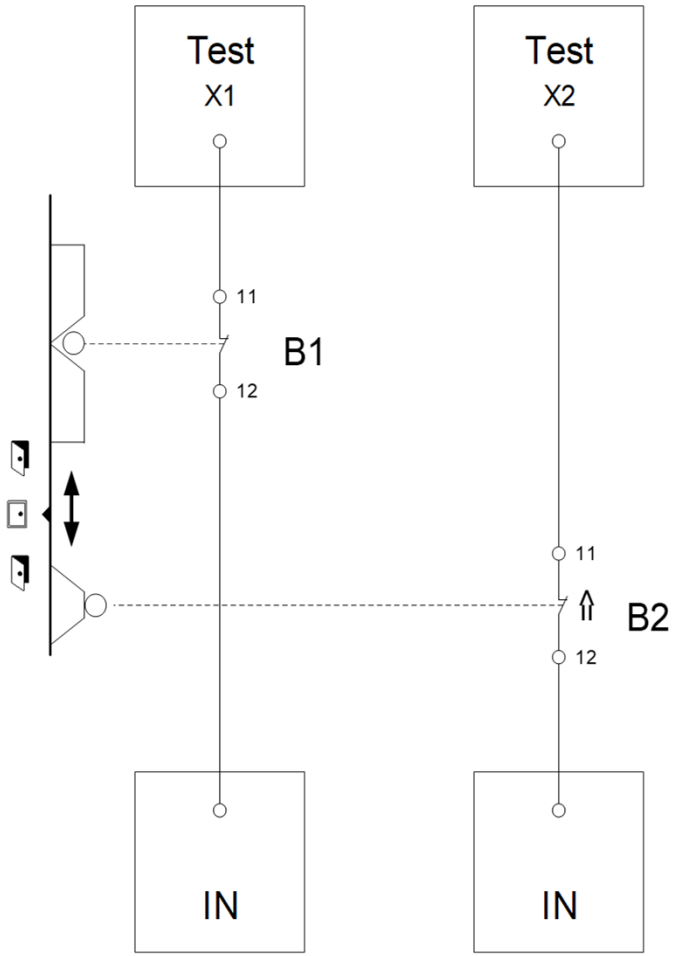
- **Direct opening action (of a contact element)**
  - achievement of contact separation as a direct result of a specified movement of the switch actuator through non-resilient elements (e.g. not dependent upon springs)

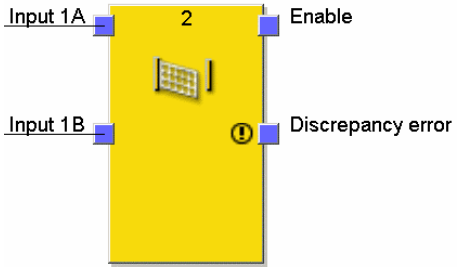


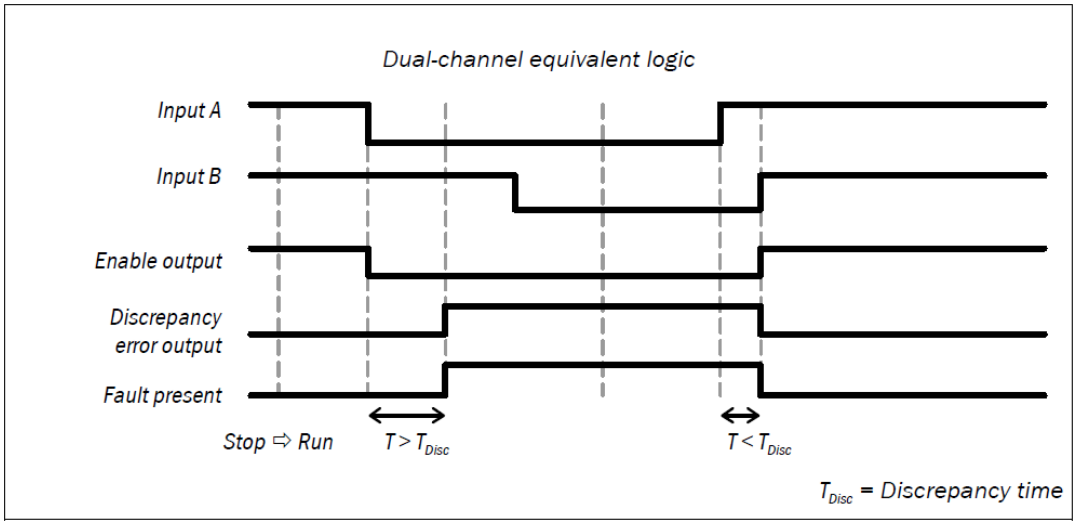
(IEC 60947 5.1 Annex K)

DIAGNOSTIC COVERAGE – DUAL CHANNEL EVALUATION

FAULT DETECTION (DISCREPANCY MONITORING / CROSS MONITORING)

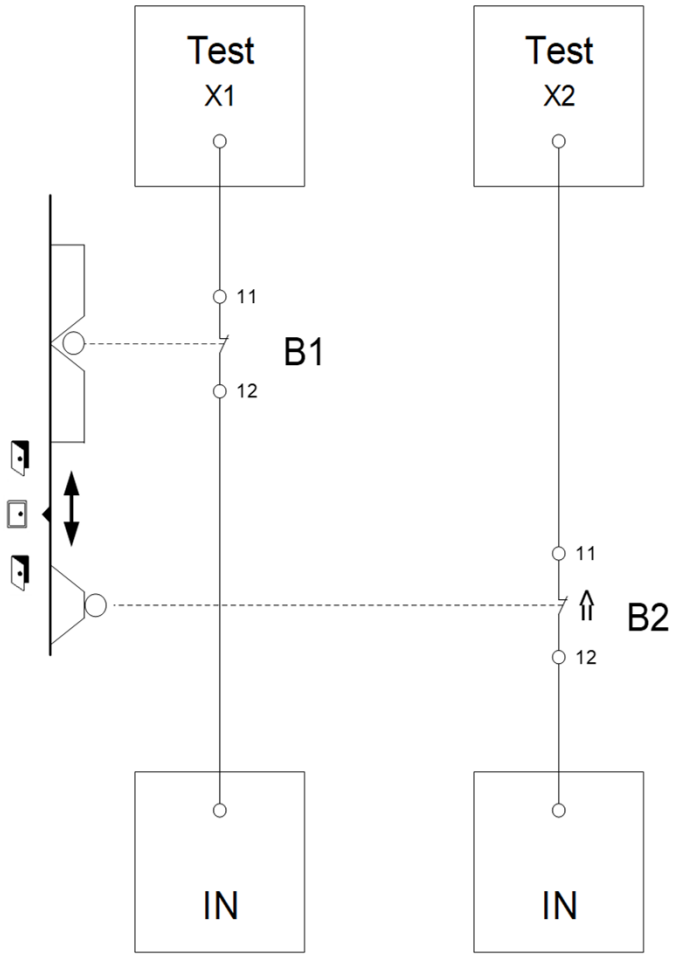


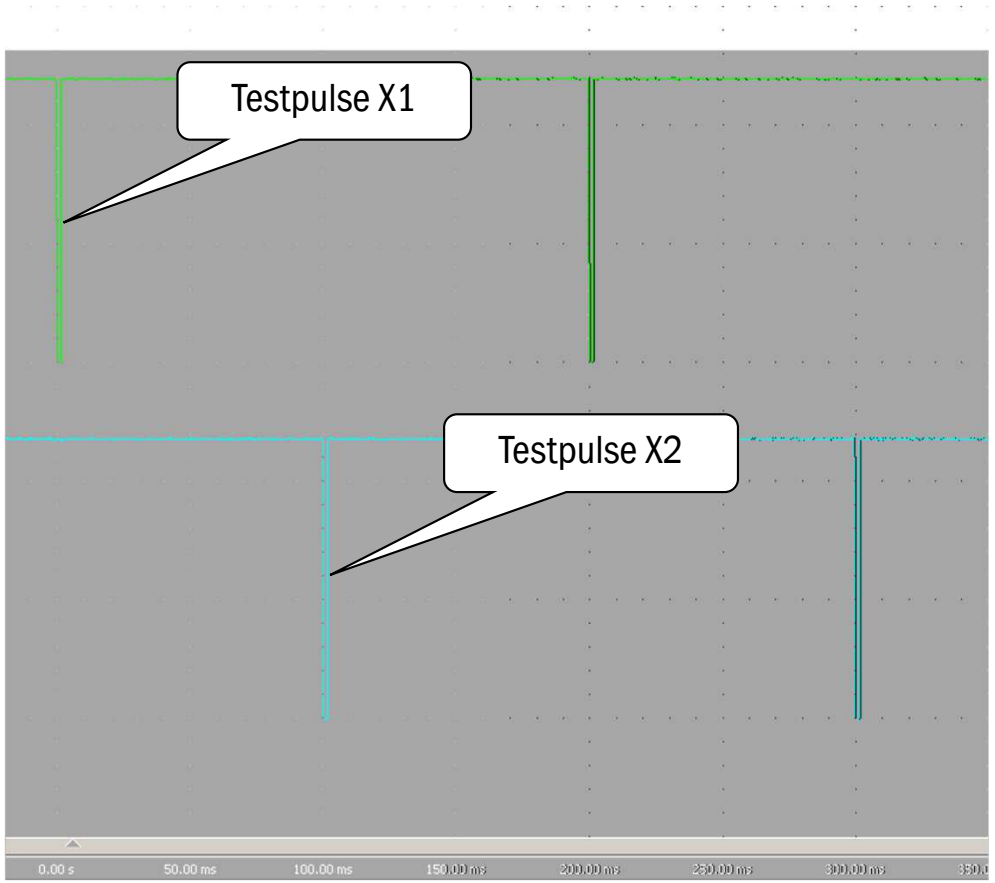




DIAGNOSTIC COVERAGE – TEST PULSES

DETECTION OF SHORT AND CROSS CIRCUITS





MEASURES AGAINST COMMON CAUSE FAILURES

SUBSYSTEM T01

SICK
Sensor Intelligence.

Requirement		Maximum value
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**
Diversity	Different technologies, components, principles of operation, designs	**20**
Layout, application, experience	Protection against overload, overvoltage, overpressure, etc. (depending on technology)	**15**
	Use of components and methods proven over many years	**5**
Analysis, evaluation	Use of a fault analysis to avoid common cause faults	**5**
Competence, training	Training for designers so that they understand and can avoid the causes and consequences of CCF	**5**
Effect of the environment	Test the system for susceptibility to EMC	**25** *
	Test the system for susceptibility to temperature, shock, vibration, etc.	**10**

* = there is no EMI effect on mechanical position switches

EVALUATION OF DESIGN PROCESS MEASURES
SUBSYSTEM T01

Following systematic aspects for fault avoidance and fault management shall be evaluated **and** implemented:

- Organisation and competency
- Design rules (e.g. specification masters, coding guidelines)
- Test concept and test criteria
- Documentation- and configuration-management

DETERMINATION OF THE PL
SUBSYSTEM T01

SICK
Sensor Intelligence.

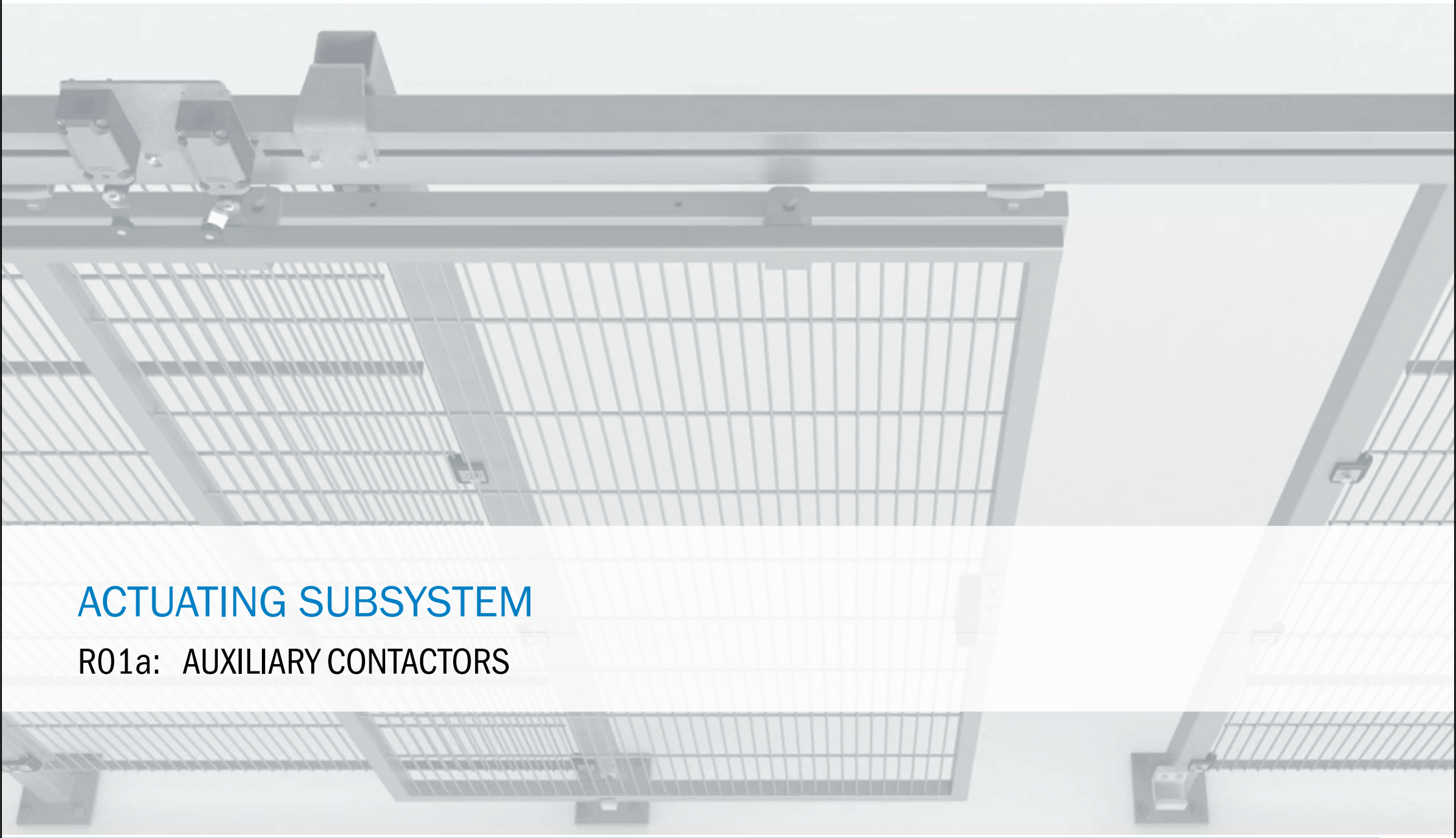
Table K.1 *(continued)*

$MTTF_D$ for each channel years	Average probability of a dangerous failure per hour, PFH_D (1/h) and corresponding performance level (PL)							
	Cat. B PL DC_{avg} = none	Cat. 1 PL DC_{avg} = none	Cat. 2 PL DC_{avg} = low	Cat. 2 PL DC_{avg} = medium	Cat. 3 PL DC_{avg} = low	Cat. 3 PL DC_{avg} = medium	Cat. 4 DC_{avg} = high	PL
1 600							$1{,}42 \times 10^{-9}$	e
1 800							$1{,}26 \times 10^{-9}$	e
2 000							$1{,}13 \times 10^{-9}$	e
2 200							$1{,}03 \times 10^{-9}$	e
2 300							$9{,}85 \times 10^{-10}$	e
2 400							$9{,}44 \times 10^{-10}$	e
2 500							$9{,}06 \times 10^{-10}$	e

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the testrate (see 4.5.4), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1,1 can be used as a worst case estimate.

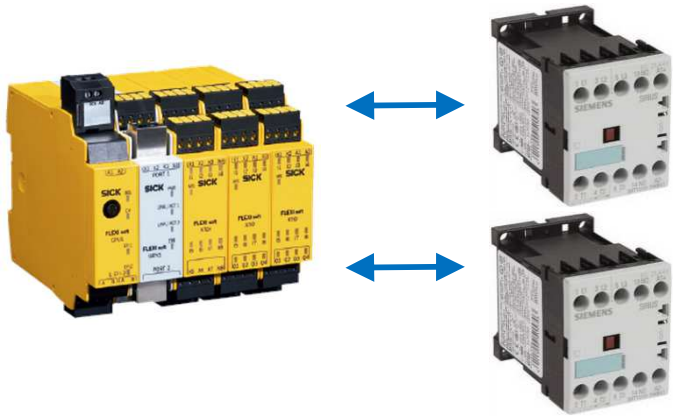
NOTE 2 The calculating of the PFH_D-values was based on following DC_{avg}:

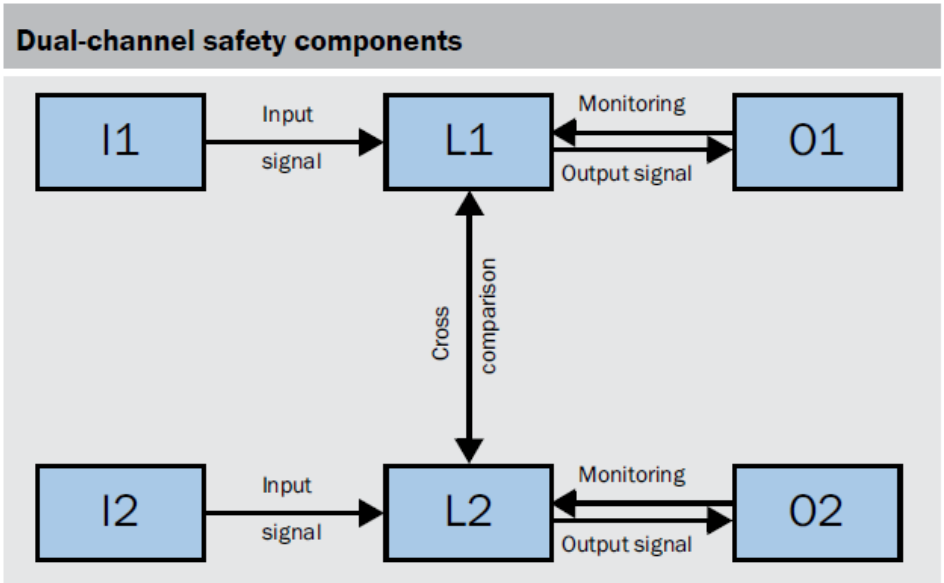
- DC_{avg} = low, calculated with 60 %;
- DC_{avg} = medium, calculated with 90 %;
- DC_{avg} = high, calculated with 99 %.



ACTUATING SUBSYSTEM

R01a: AUXILIARY CONTACTORS





The structure of the subsystem is suitable for category 3/4 (dependent on DC and $MTTF_d$)

$MTTF_D$ PER CHANNEL
SUBSYSTEM R01a

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

$$= \frac{1/0{,}73 \times 1 \cdot 10^6}{0{,}1 \times 365\,d/a \times 24\,h/d \times 1/h}$$

$$= \frac{13{,}7 \cdot 10^6}{8.760/a}$$

$$MTTF_D = 1.564\,a$$

$$T_{10D} = 156\,a$$

Designation	Range
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

ESTIMATES FOR DIAGNOSTIC COVERAGE

SUBSYSTEM R01a

Measure	Diagnostic coverage (DC)
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross mo within the monitor c and short	
Redunda	
Redunda actuators	
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 % depending on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %

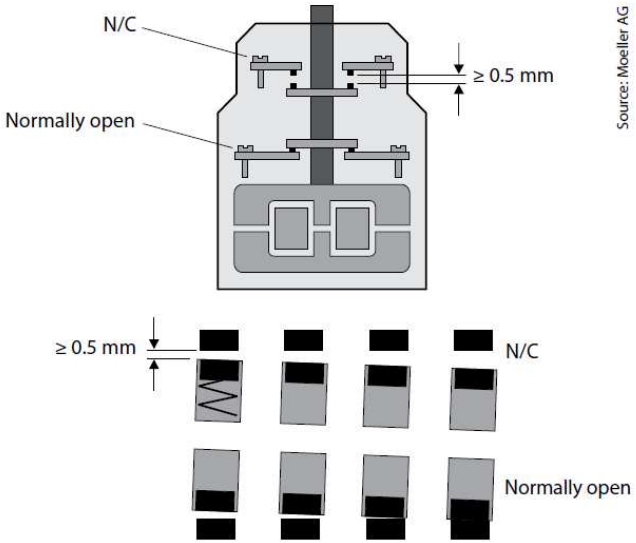
Designation	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

NOTE 1 For additional estimations for DC, see, e.g., IEC 61508-2:2000, Tables A.2 to A.15.

NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.

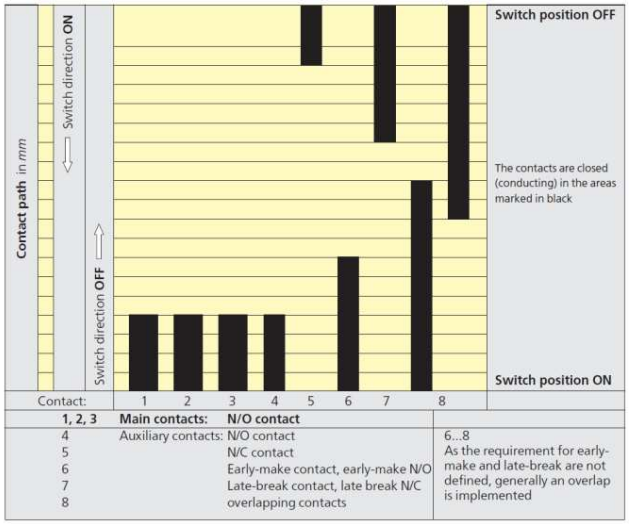
DIAGNOSTIC COVERAGE – EDM

SYSTEMATIC CAPABILITIES OF AUXILIARY CONTACTS

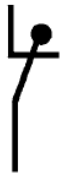


Source: Moeller AG

- Positively driven contact elements
  acc. to Annex L, IEC 60947-5-1:2003



- Mirror contacts
  acc. to Annex F, IEC 60947-4-1:2009



MEASURES AGAINST COMMON CAUSE FAILURES

SUBSYSTEM R01a

SICK
Sensor Intelligence.

Requirement		Maximum value
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**
Diversity	Different technologies, components, principles of operation, designs	**20**
Layout, application, experience	Protection against overload, overvoltage, overpressure, etc. (depending on technology)	**15**
	Use of components and methods proven over many years	**5**
Analysis, evaluation	Use of a fault analysis to avoid common cause faults	**5**
Competence, training	Training for designers so that they understand and can avoid the causes and consequences of CCF	**5**
Effect of the environment	Test the system for susceptibility to EMC	**25**
	Test the system for susceptibility to temperature, shock, vibration, etc.	**10**

EVALUATION OF PROCESS MEASURES

SUBSYSTEM R01a

Following systematic aspects for fault avoidance and fault management shall be evaluated **and** implemented:

- Organization and competency
- Design rules (e.g. specification masters, coding guidelines)
- Test concept and test criteria
- Documentation- and configuration-management

DETERMINATION OF THE ACHIEVED PL

SUBSYSTEM R01a

SICK
Sensor Intelligence.

$MTTF_D$ for each channel years	Average probability of a dangerous failure per hour, PFH_D (1/h) and corresponding performance level (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = none		DC_{avg} = none		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high	
200													$1{,}19 \times 10^{-8}$	e
220													$1{,}08 \times 10^{-8}$	e
240													$9{,}81 \times 10^{-9}$	e
270													$8{,}67 \times 10^{-9}$	e
300													$7{,}76 \times 10^{-9}$	e
330													$7{,}04 \times 10^{-9}$	e
360													$6{,}44 \times 10^{-9}$	e
390													$5{,}94 \times 10^{-9}$	e
430													$5{,}38 \times 10^{-9}$	e
470													$4{,}91 \times 10^{-9}$	e
510													$4{,}52 \times 10^{-9}$	e
560													$4{,}11 \times 10^{-9}$	e
620													$3{,}70 \times 10^{-9}$	e
680													$3{,}37 \times 10^{-9}$	e
750													$3{,}05 \times 10^{-9}$	e
820													$2{,}79 \times 10^{-9}$	e
910													$2{,}51 \times 10^{-9}$	e
1 000													$2{,}28 \times 10^{-9}$	e
1 100													$2{,}07 \times 10^{-9}$	e
1 200													$1{,}90 \times 10^{-9}$	e
1 300													$1{,}75 \times 10^{-9}$	e
1 500													$1{,}51 \times 10^{-9}$	e

OVERALL PL ACHIEVED BY A SAFETY FUNCTION

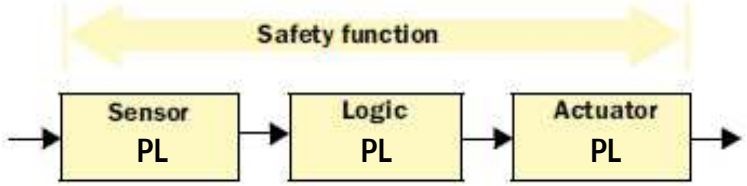
SF01: INITIATING A STOP

SAFETY FUNCTION SF01
ESTIMATION OF THE PL ACHIEVED

PL e | **PL e | PL e | PL e** | **PL e** | **PL d**

OVERALL PL ACHIEVED BY A SAFETY FUNCTION

SIMPLIFIED METHOD



PL (low) (lowest PL of a sub-system)	n (low) (number of subsys-tems with this PL)	PL (maximum achiev-able PL)
a	> 3	–
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

SAFETY FUNCTION SF01

CALCULATION OF THE PFHd ACHIEVED

$1{,}1 \times 10^{-9}$

$0{,}4 \times 10^{-9}$

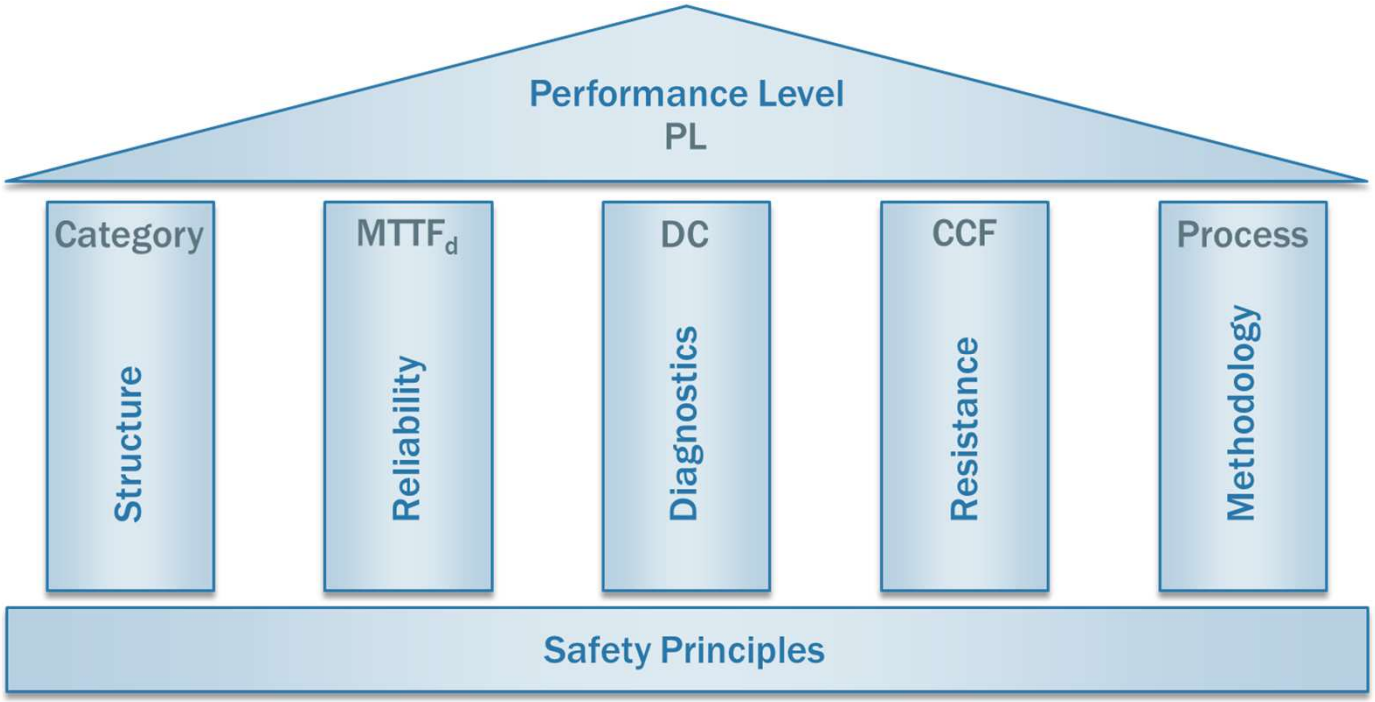
$0{,}9 \times 10^{-9}$

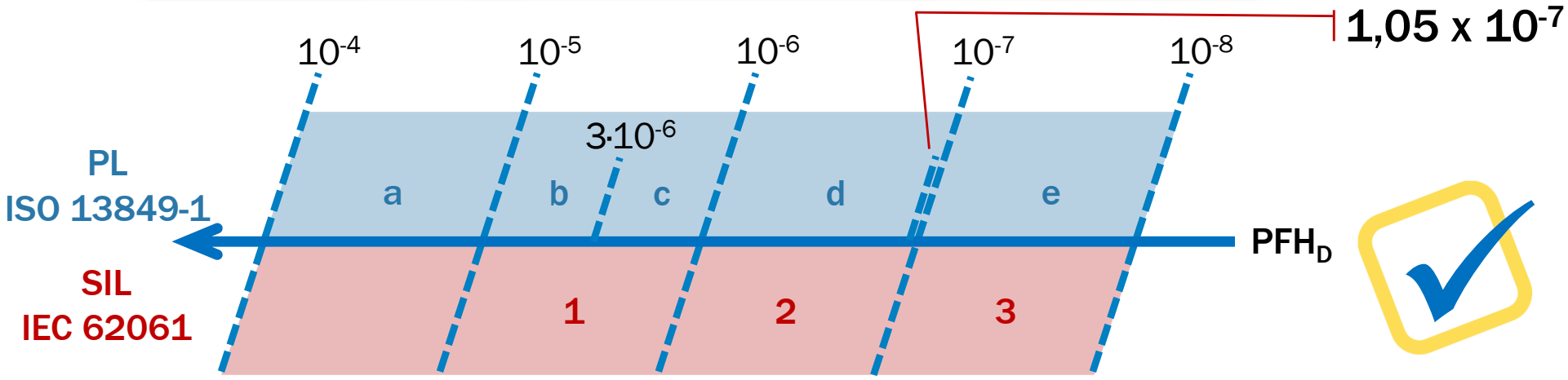
$1{,}0 \times 10^{-9} + 2{,}4 \times 10^{-9} + 1{,}5 \times 10^{-9} + 100 \times 10^{-9}$

$1{,}05 \times 10^{-7} \sim 1 \times 10^{-7}$

(dangerous failures/h)

DETERMINING THE SAFETY LEVEL
VERIFICATION OF FUNCTIONAL SAFETY





DO NOT HESITATE TO ASK QUESTIONS!

SICK
Sensor Intelligence.

Otto Görnemann
SICK AG, R&D
Erwin-Sick-Straße 1
D-79183 Waldkirch
Otto.Goernemann@sick.de