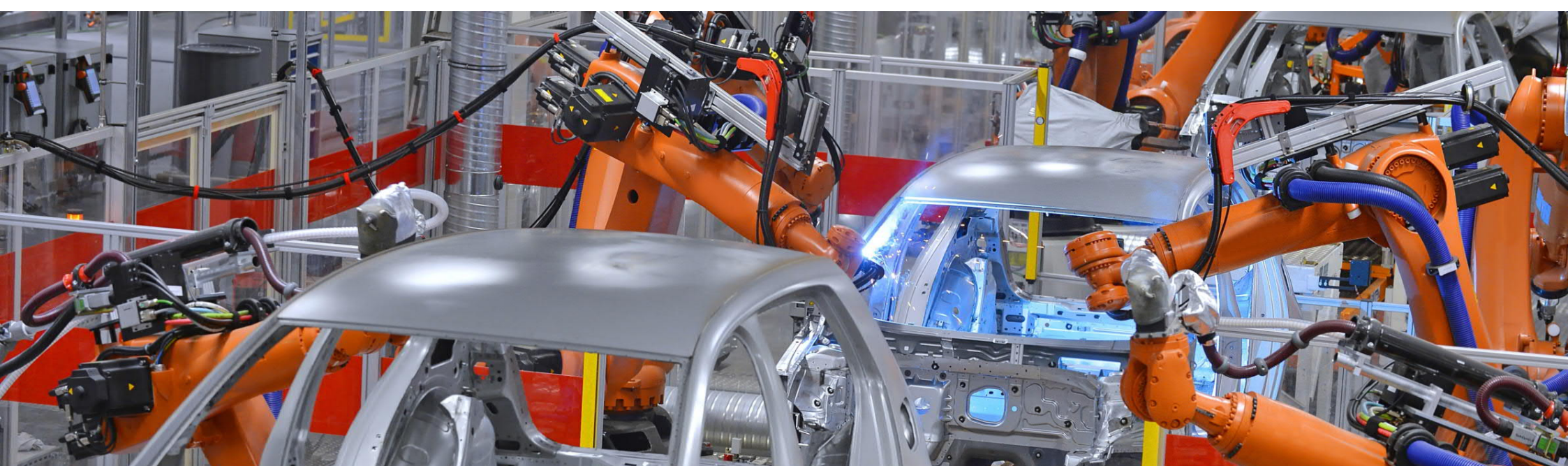




QUANTIFICATION [ISO 13849] EXAMPLE OF APPLICATION



Otto Görnemann
Research & Development
Rev. 1V0.d



INDUSTRIAL ROBOT CELL – ISO 10218-2

SICK
Sensor Intelligence.

01



Origin

moving elements

Potential consequences

- crushing
- impact
- shearing

NEW ALTERNATIVE IN THE ONGOING REVISION

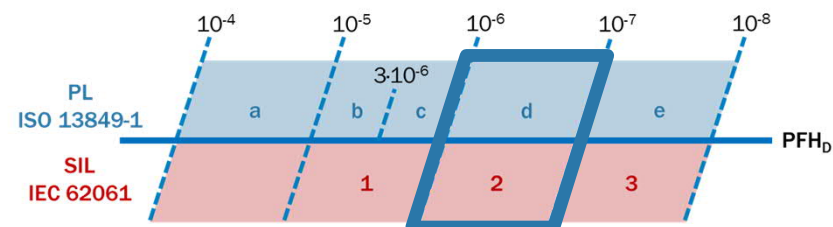
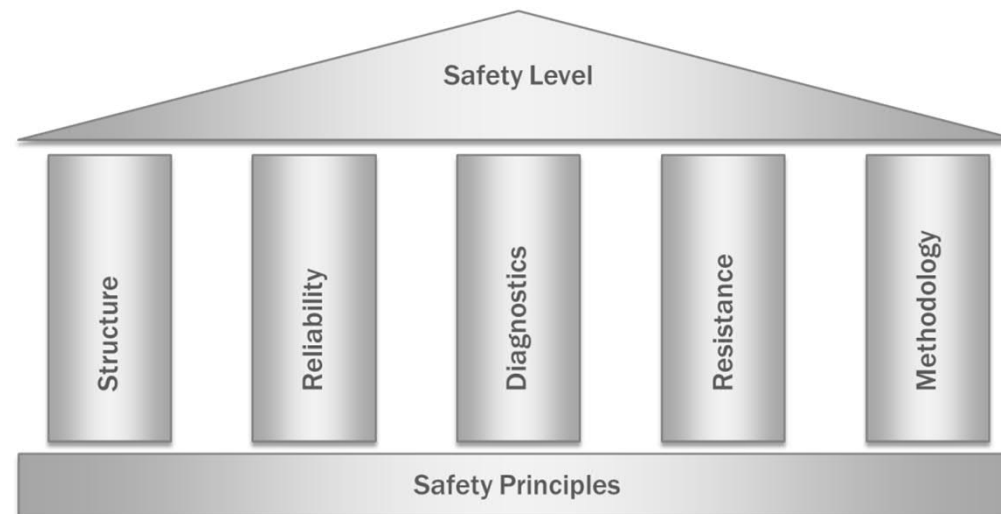
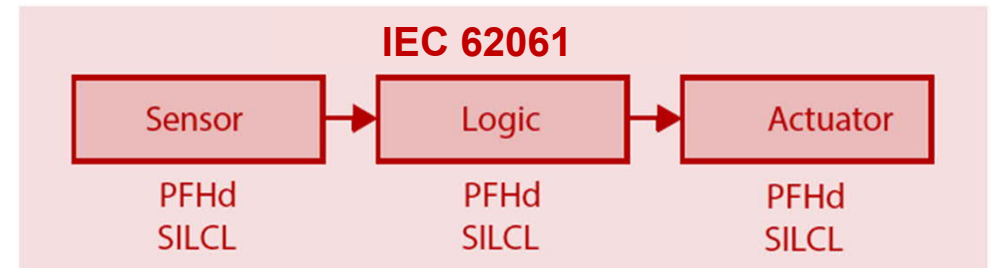
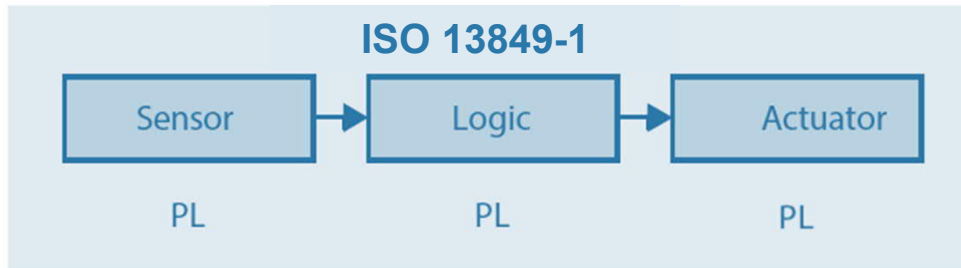
ISO 10218-2:2011

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.

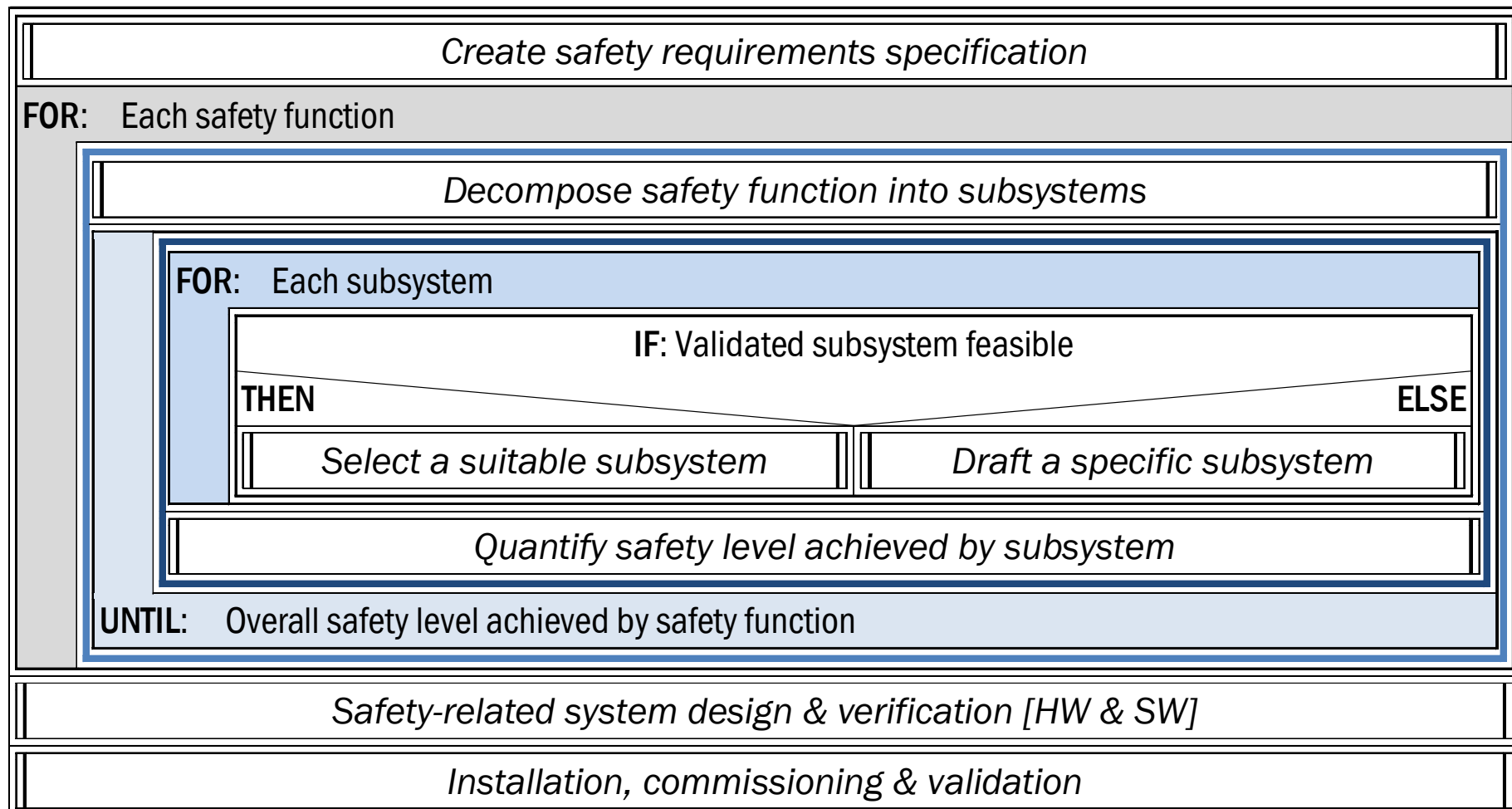
DETERMINING THE SAFETY LEVEL

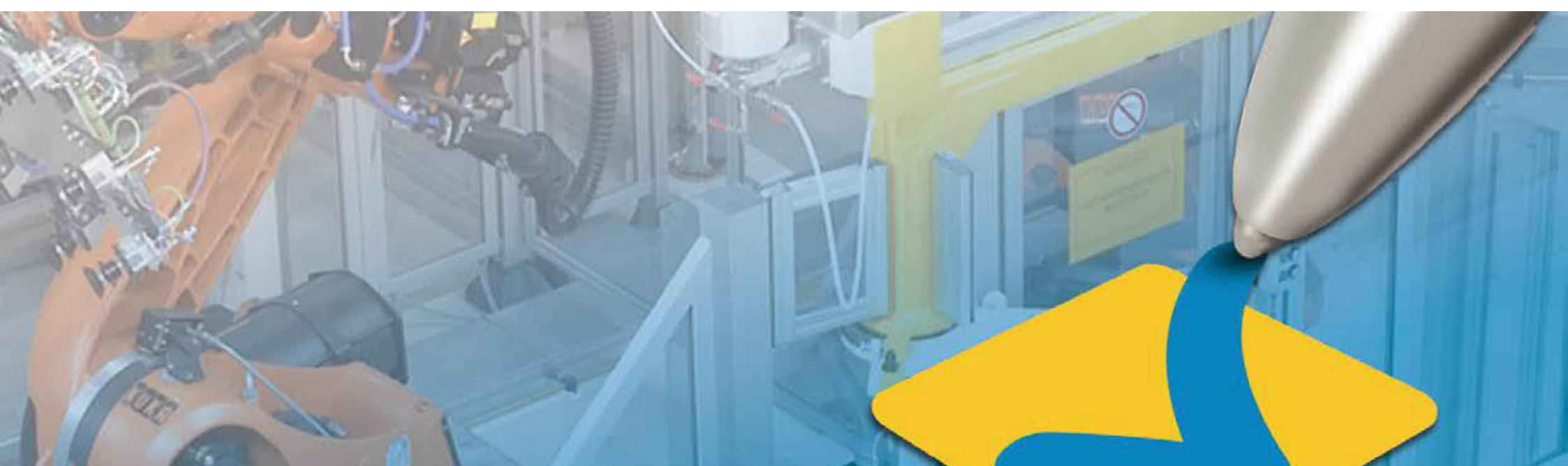
VERIFICATION OF FUNCTIONAL SAFETY



SAFETY-RELATED CONTROL SYSTEMS

THINKING IN SAFETY FUNCTIONS





SAFETY CONCEPT

SICK
Sensor Intelligence.

02

SAFETY REQUIREMENTS SPECIFICATION

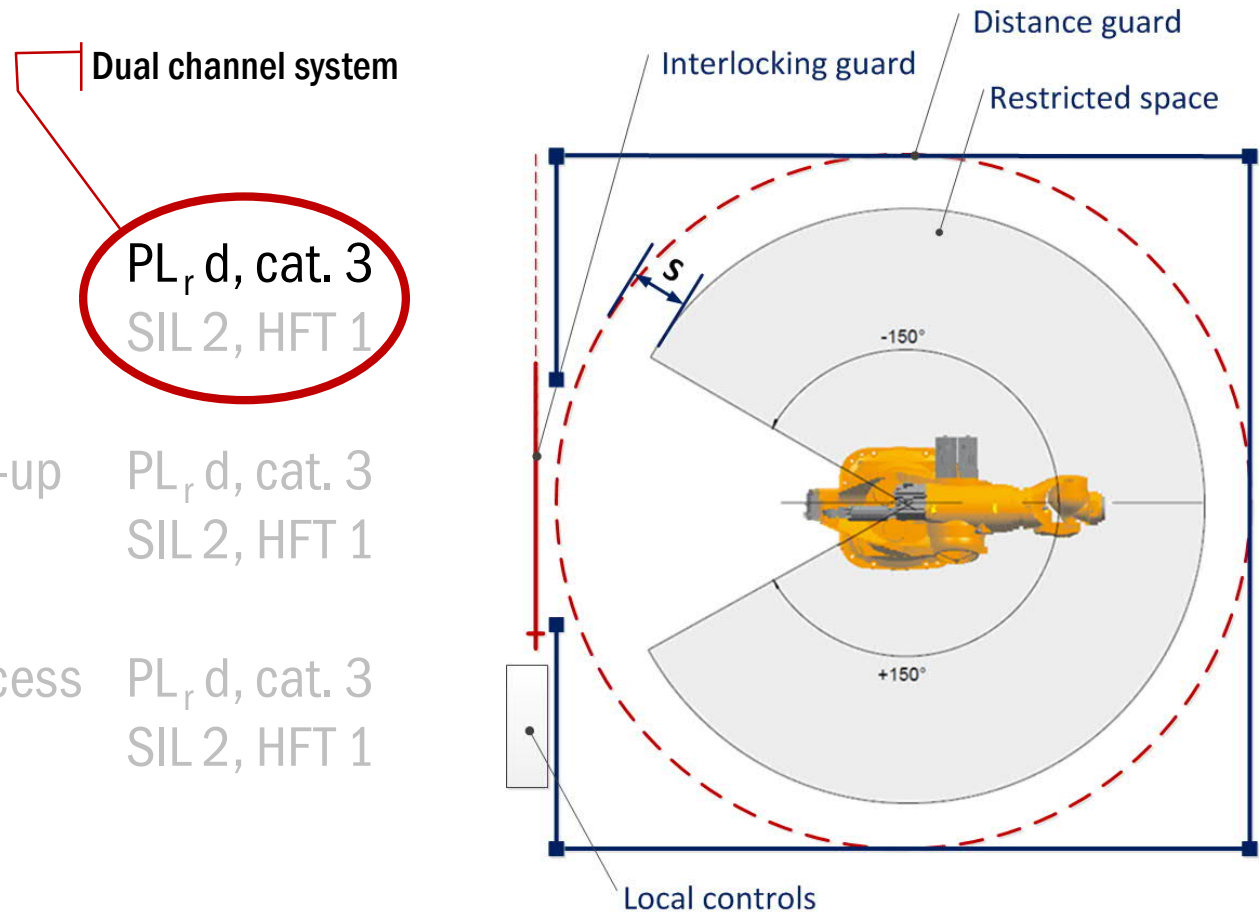
ACCESS FOR INTERVENTIONS (ACC. TO ISO 13849-1)

SF01: Initiating a stop

PL_r d, cat. 3
SIL 2, HFT 1

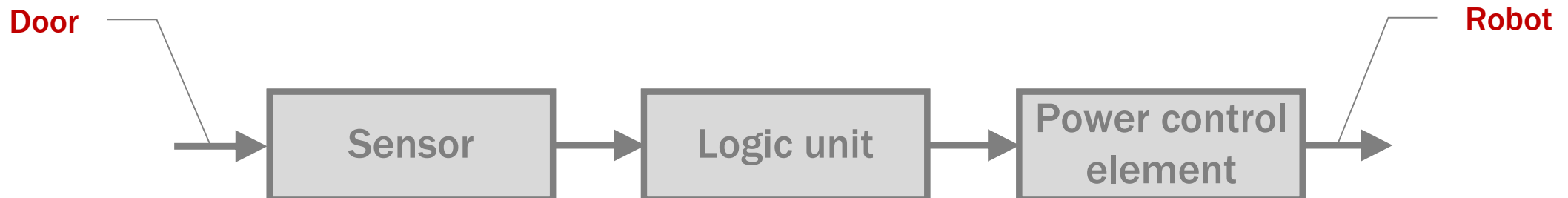
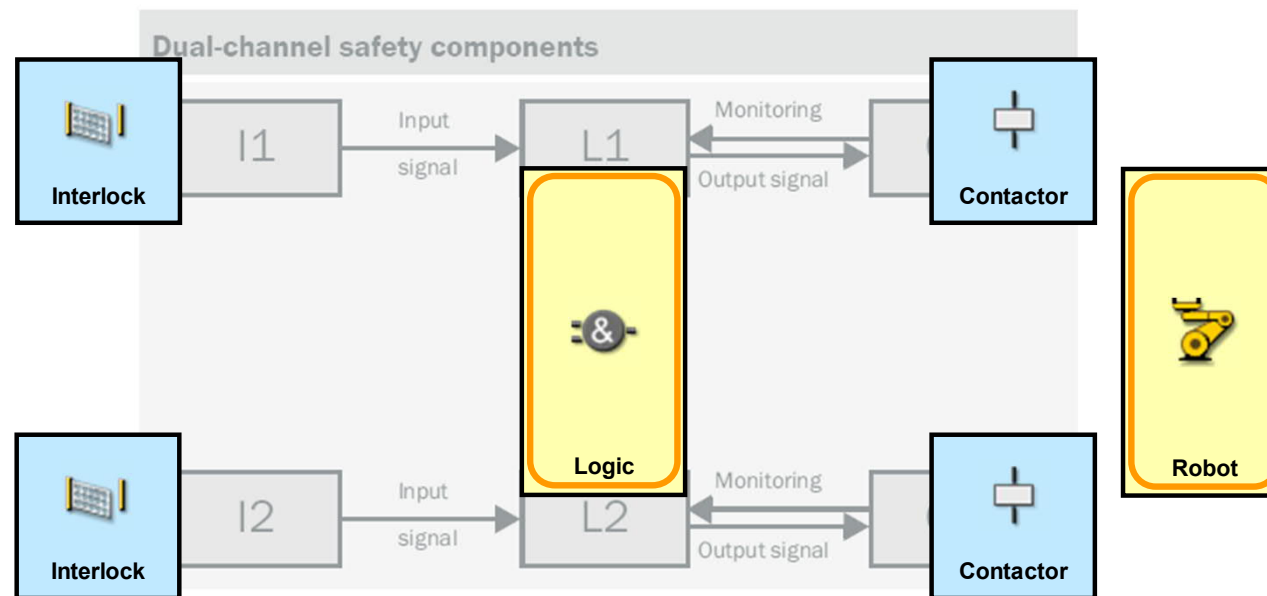
SF02: Avoiding unexpected start-up PL_r d, cat. 3
SIL 2, HFT 1

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		 Interlock		 Contactor		
	.2		 Interlock	 Logic	 Contactor	 Robot	
Identifier			T01	L01	R01a	R01b	
Requirements			Type 1 Type 2		EDM	SS1	
Trigger	Open door			1 / h [frequency of demands]			
Condition	At any time						
Reaction	Shutdown machine						
Safe state	Standstill			1 s [overall stopping performance]			

T01: type acc. to EN ISO 14119:2013



SICK
Sensor Intelligence.

HARDWARE CONCEPT

03

SAFETY FUNCTION SF01

SELECTION OF PROTECTIVE DEVICES



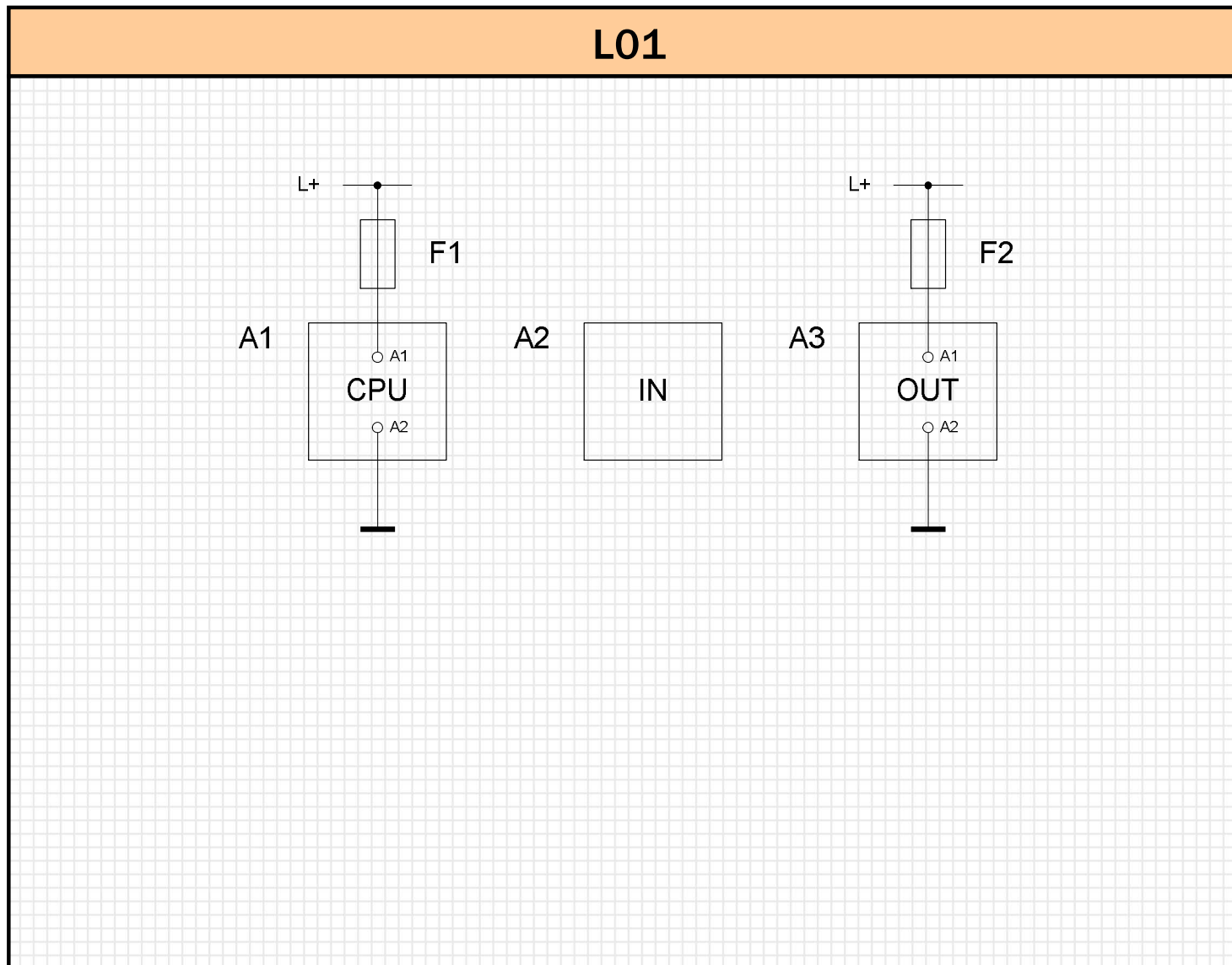
Door

Robot

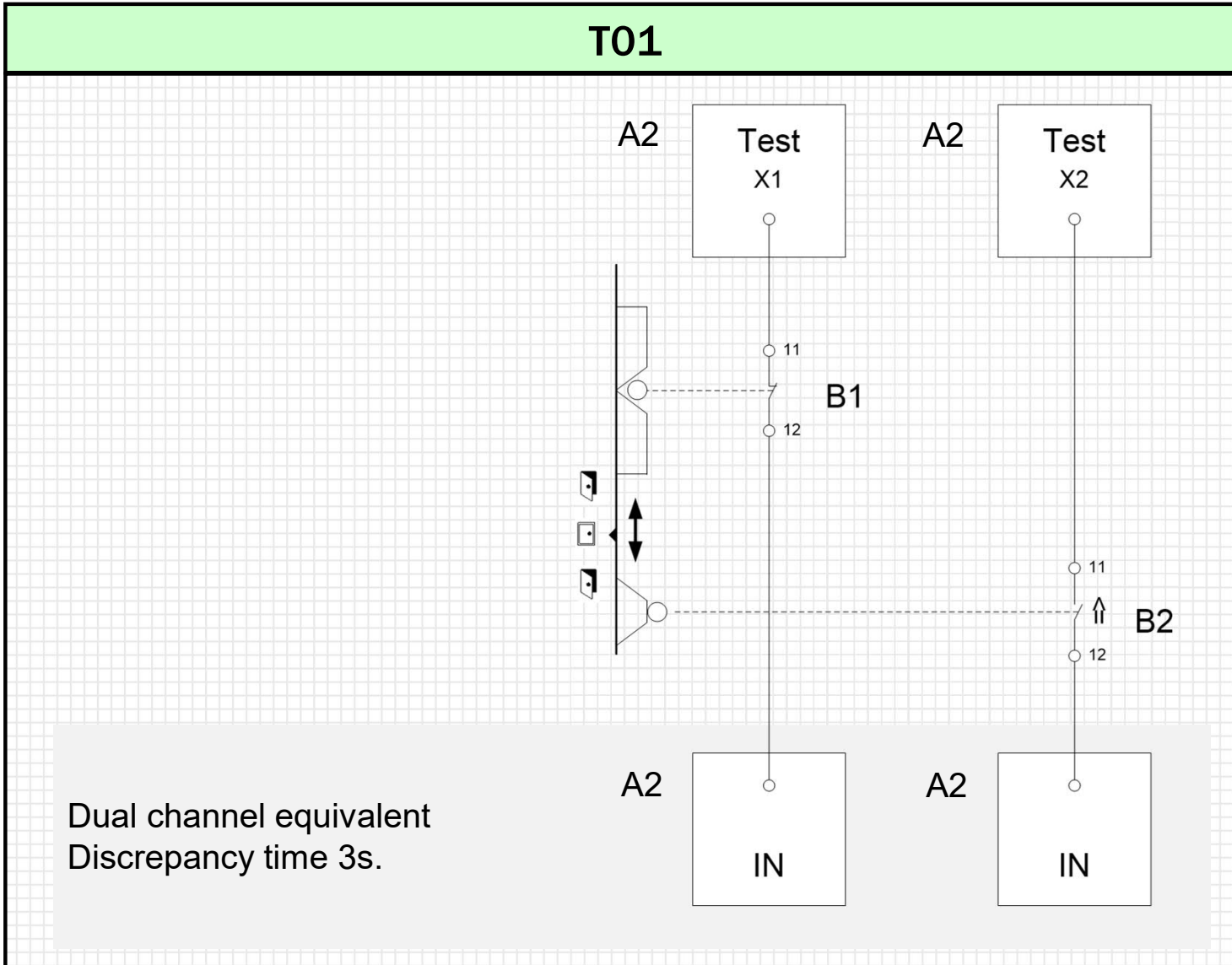


HW SKETCH “LOGIC UNIT”

LOGIC PROCESSING SUBSYSTEMS

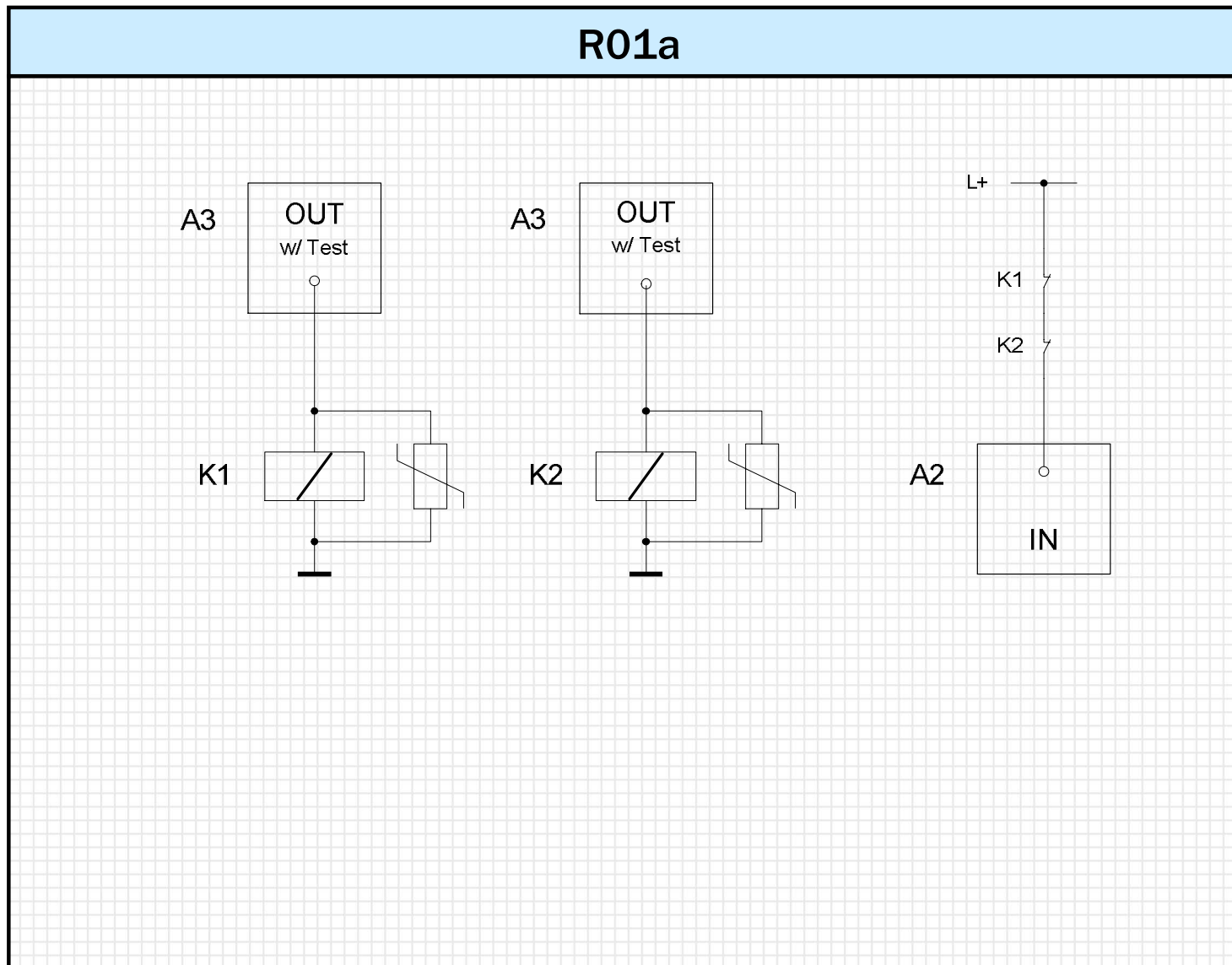


SAFETY TRIGGERING SUBSYSTEMS



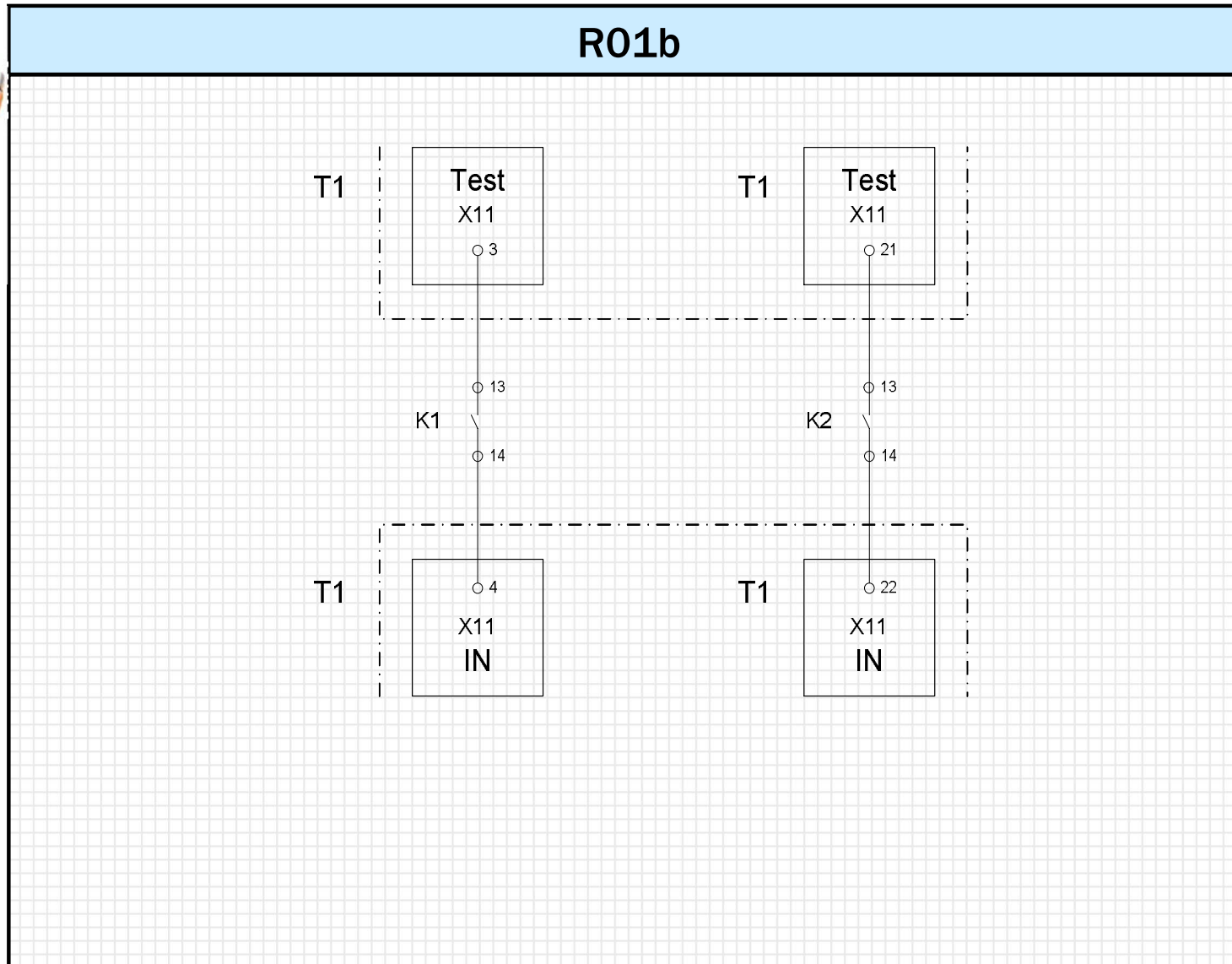
HW SKETCH “POWER CONTROL ELEMENT”

REACTION ACTUATING SUBSYSTEMS



HW SKETCH “POWER CONTROL ELEMENT”

REACTION ACTUATING SUBSYSTEMS





DETERMINE PL FOR SRP/CS



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)

DATA SHEET SICK AG FX3-XTIO

SUBSYSTEM L01c



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 i110 LOCK /i10-R

SUBSYSTEM T01



Mechanical switching operations max.	10^6
B10 _d	5×10^6 switching operations with low load as per EN ISO 13849-1
Mechanical switching operations with i110 ... S06	For retaining force 45 N: 10^5

Mechanical service life	10×10^6 switching operations
B10 _d	2×10^6 switching operations with low load as per EN ISO 13849-1



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: - Contactor Relays, Coupling Relays, 4-pole - Contactor Relays with auxiliary switch block - electronic compatible auxiliary switches, latched Contactor Relays	3)	30,000,000	50 %
	3)	10,000,000	
	3)	5,000,000	
	AC-15/-14; 230 V DC-13; 24 V ($< 0.3 \times I_e$)	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

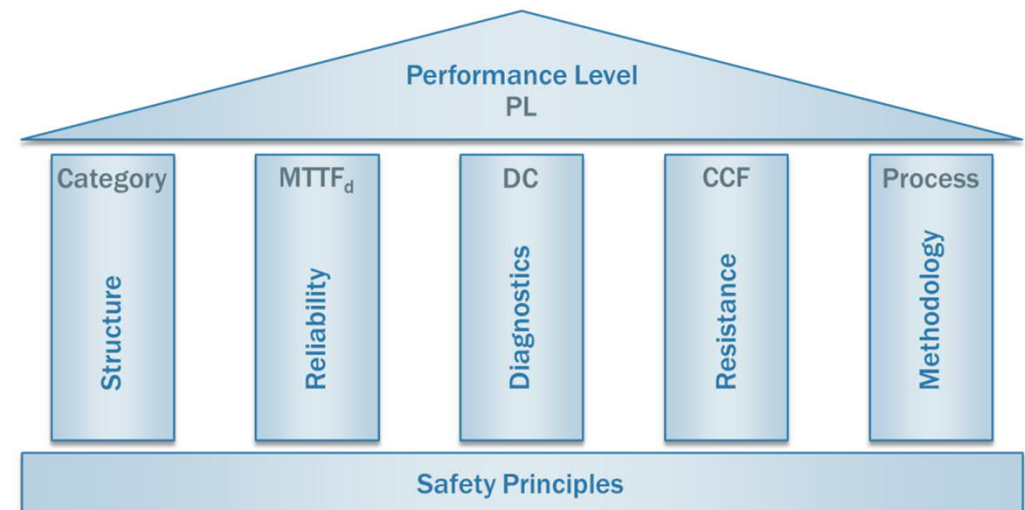


Robot controller variant	PFH value
KR C4; KR C4 CK	$< 1 \times 10^{-7}$

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

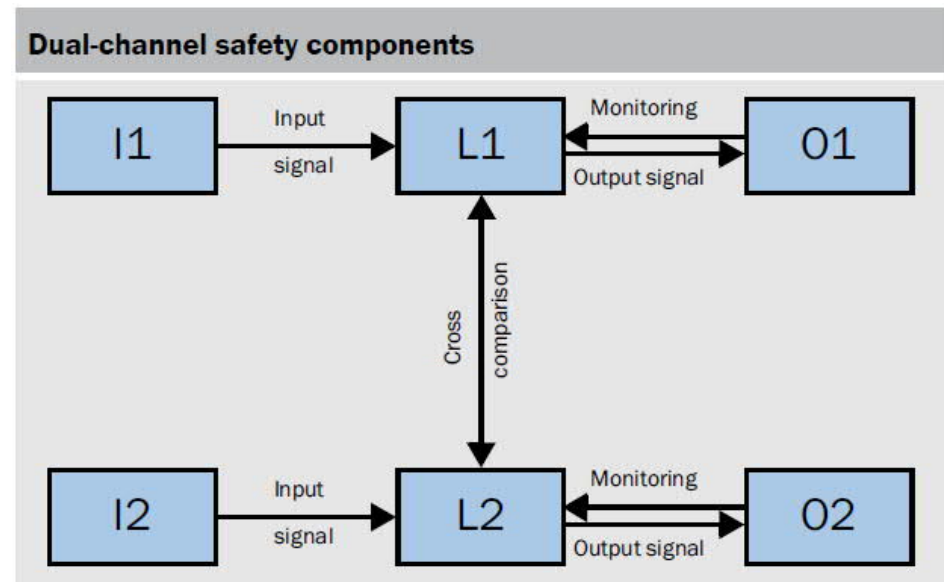
Determining the level of safety for a **subsystem**:

1. Delimitation of the subsystem
2. Determination of the category
3. Determination of the MTTF_d 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



SAFETY TRIGGERING SUBSYSTEM

T01: INTERLOCKING GUARDS



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

MTTF_D PER CHANNEL

SUBSYSTEM T01.1



$$\begin{aligned} \text{MTTF}_D &= \frac{B_{10D}}{0,1 \times n_{\text{op}}} \\ &= \frac{5 \cdot 10^6}{0,1 \times 365 \text{ d/a} \times 24 \text{ h/d} \times 1/\text{h}} \\ &= \frac{5 \cdot 10^7}{8.760/\text{a}} \end{aligned}$$

$$\text{MTTF}_D = 5.707 \text{ a} \geq 2.500 \text{ a}$$

$$\begin{aligned} T_{10D} &= \frac{B_{10D}}{n_{\text{op}}} \\ &= \frac{\text{MTTF}_D}{10} \end{aligned}$$

$$T_{10D} = 570 \text{ a}$$



$$\begin{aligned} \text{MTTF}_D &= \frac{B_{10D}}{0,1 \times n_{\text{op}}} \\ &= \frac{2 \cdot 10^6}{0,1 \times 365 \text{ d/a} \times 24 \text{ h/d} \times 1/\text{h}} \\ &= \frac{2 \cdot 10^7}{8.760/\text{a}} \end{aligned}$$

$$\text{MTTF}_D = 2.283 \text{ a}$$

$$\begin{aligned} T_{10D} &= \frac{B_{10D}}{n_{\text{op}}} \\ &= \frac{\text{MTTF}_D}{10} \end{aligned}$$

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

SYMMETRIZATION

SUBSYSTEM T01



$$\begin{aligned} \text{MTTF}_D &= \frac{2}{3} \left[\text{MTTF}_{DC1} + \text{MTTF}_{DC2} - \frac{1}{\frac{1}{\text{MTTF}_{DC1}} + \frac{1}{\text{MTTF}_{DC2}}} \right] \\ &= \frac{2}{3} \left[2.500a + 2.283a - \frac{1}{\frac{1}{2.500a} + \frac{1}{2.283a}} \right] \end{aligned}$$

$$\text{MTTF}_D = 2.393a$$

Designation	Range
Low	3 years $\leq$ MTTFd < 10 years
Medium	10 years $\leq$ MTTFd < 30 years
High	30 years $\leq$ 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 %
Designation	Range
None	DC < 60%
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

COMMON CAUSE FAILURES – RESISTANCE

SUBSYSTEM T01

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



Following systematic aspects for fault avoidance and fault management shall be considered **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

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	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL
	DC _{avg} = none		DC _{avg} = none		DC _{avg} = low		DC _{avg} = medium		DC _{avg} = low	
									DC _{avg} = medium	
										Cat. 4
										DC _{avg} = high
1 600										1,42 × 10 ⁻⁹
1 800										1,26 × 10 ⁻⁹
2 000										1,13 × 10 ⁻⁹
2 200										1,03 × 10 ⁻⁹
2 300										9,85 × 10 ⁻¹⁰
2 400										9,44 × 10 ⁻¹⁰
2 500										9,06 × 10 ⁻¹⁰

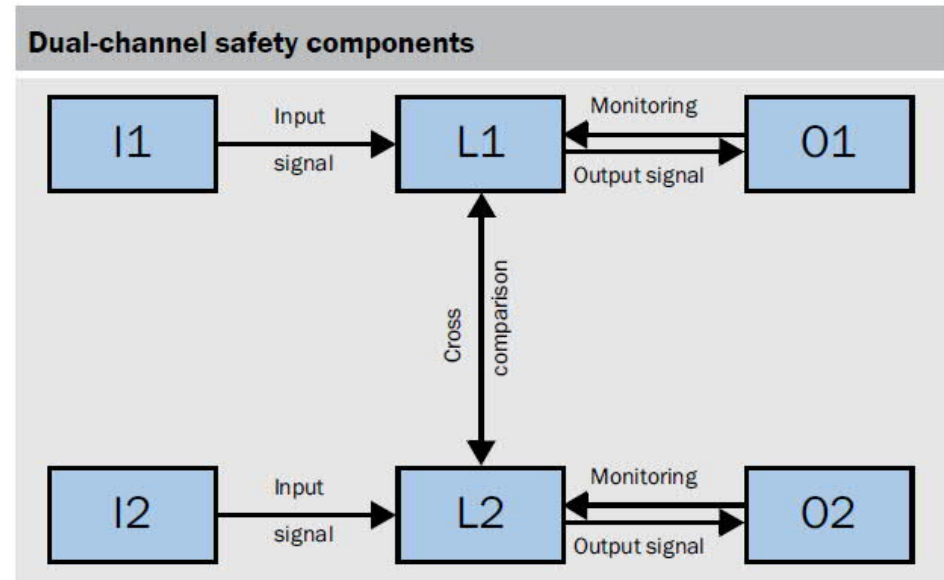
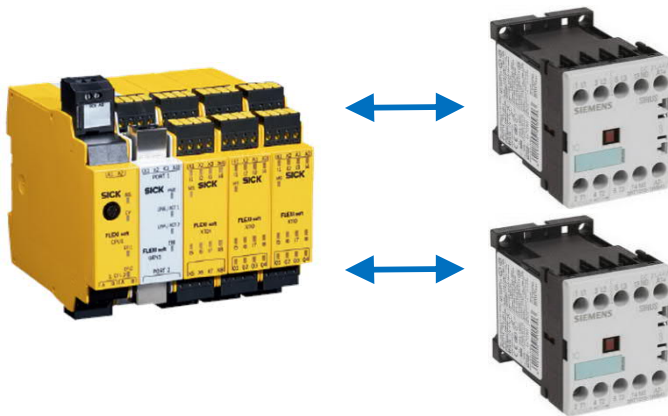
NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the testrate (see 4.5.4), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1 can be used as a worst case estimate.

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 %.

REACTION ACTUATING SUBSYSTEM

R01a: AUXILIARY CONTACTORS



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



$$\begin{aligned} \text{MTTF}_D &= \frac{B_{10D}}{0,1 \times n_{\text{op}}} \\ &= \frac{1/0,73 \times 1 \cdot 10^6}{0,1 \times 365 \text{ d/a} \times 24 \text{ h/d} \times 1/\text{h}} \\ &= \frac{13,7 \cdot 10^6}{8.760/\text{a}} \end{aligned}$$

$$\text{MTTF}_D = 1.564 \text{ a}$$

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

Designation	Range
Low	3 years $\leq$ MTTFd < 10 years
Medium	10 years $\leq$ MTTFd < 30 years
High	30 years $\leq$ 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 monitoring within the monitor channel and short circuits	Designation	Range
	None	DC < 60%
	Low	$60\% \leq DC < 90\%$
	Medium	$90\% \leq DC < 99\%$
	High	$99\% \leq DC$
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 %	
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.		

COMMON CAUSE FAILURES – RESISTANCE

SUBSYSTEM R01a

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



Following systematic aspects for fault avoidance and fault management shall be considered **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 PL

SUBSYSTEM R01a

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 × 10 ⁻⁸	e
220													1,08 × 10 ⁻⁸	e
240													9,81 × 10 ⁻⁹	e
270													8,67 × 10 ⁻⁹	e
300													7,76 × 10 ⁻⁹	e
330													7,04 × 10 ⁻⁹	e
360													6,44 × 10 ⁻⁹	e
390													5,94 × 10 ⁻⁹	e
430													5,38 × 10 ⁻⁹	e
470													4,91 × 10 ⁻⁹	e
510													4,52 × 10 ⁻⁹	e
560													4,11 × 10 ⁻⁹	e
620													3,70 × 10 ⁻⁹	e
680													3,37 × 10 ⁻⁹	e
750													3,05 × 10 ⁻⁹	e
820													2,79 × 10 ⁻⁹	e
910													2,51 × 10 ⁻⁹	e
1 000													2,28 × 10 ⁻⁹	e
1 100													2,07 × 10 ⁻⁹	e
1 200													1,90 × 10 ⁻⁹	e
1 300													1,75 × 10 ⁻⁹	e
1 500													1,51 × 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



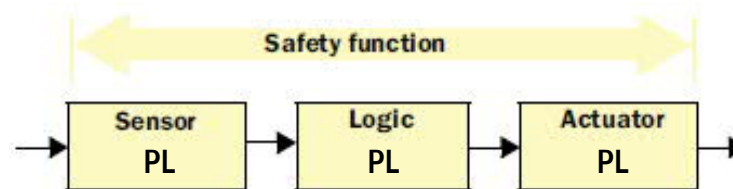
PL e



PL d

OVERALL PL ACHIEVED BY A SAFETY FUNCTION

SIMPLIFIED METHOD

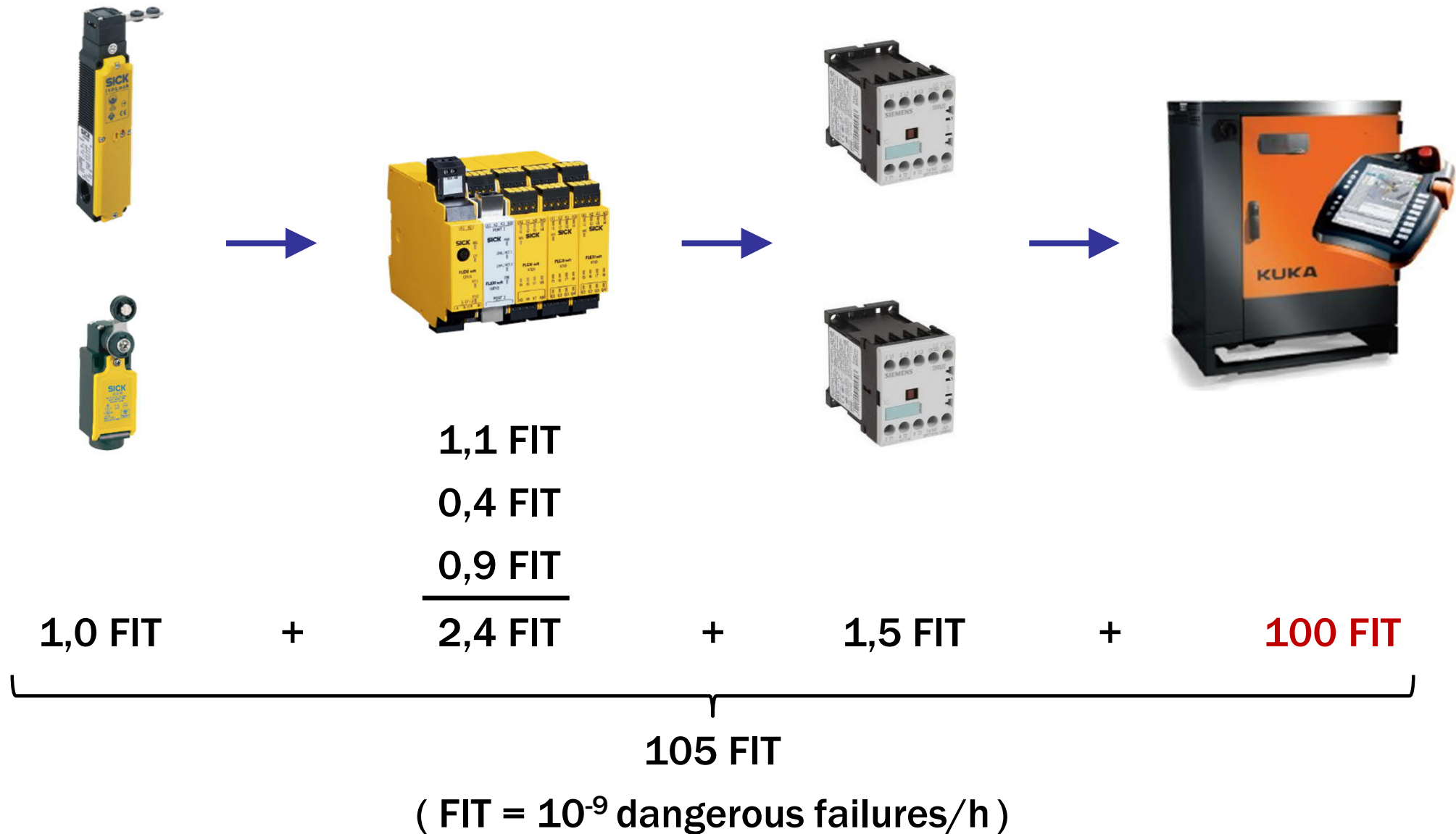


PL (low) (lowest PL of a sub-system)	n (low) (number of sub-systems with this PL)		PL (maximum achievable PL)
a	> 3	→	–
	≤ 3	→	a
b	> 2	→	a
	≤ 2	→	b
c	> 2	→	b
	≤ 2	→	c
d	> 3	→	c
	≤ 3	→	d
e	> 3	→	d
	≤ 3	→	e



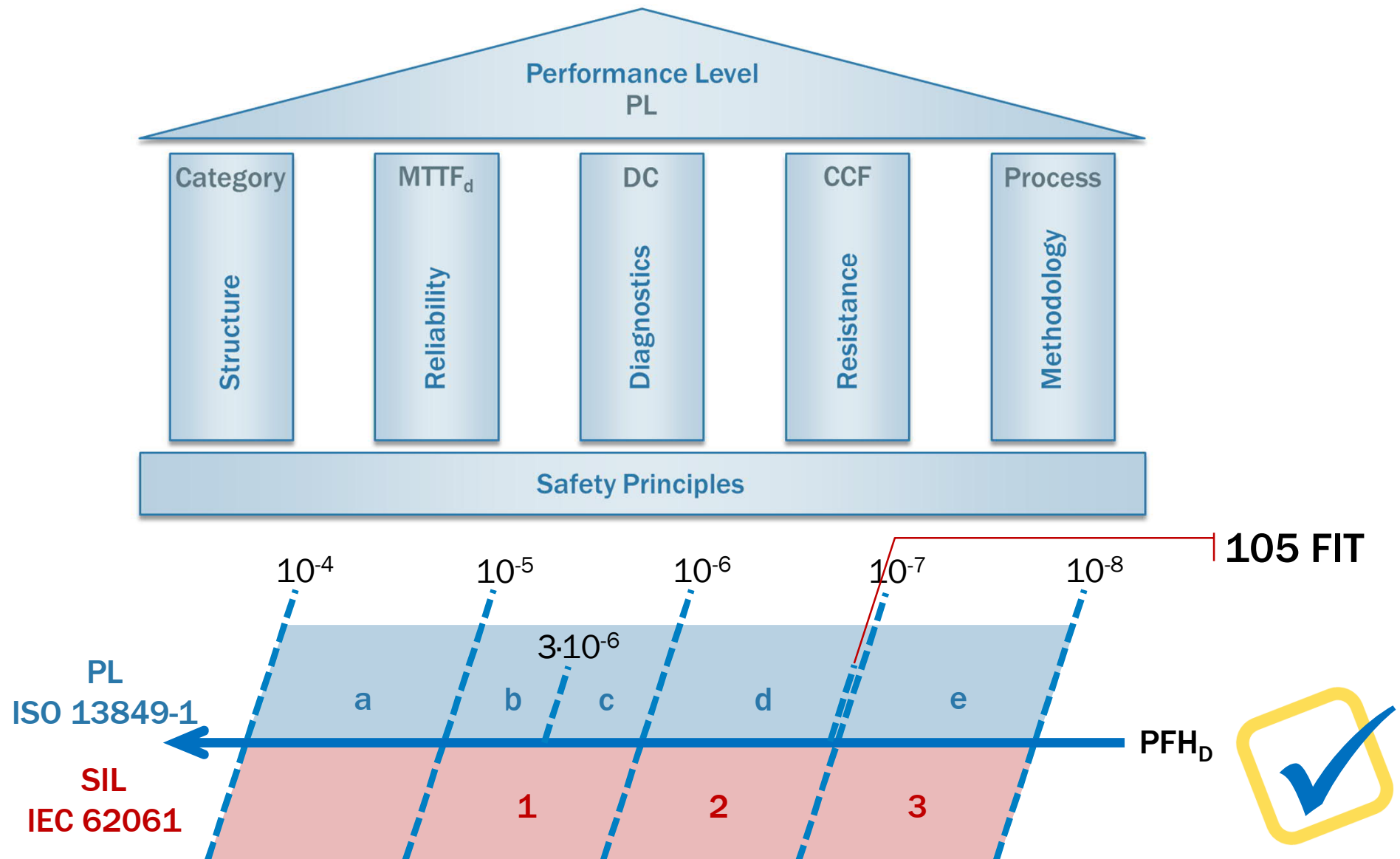
SAFETY FUNCTION SF01

CALCULATION OF THE PFHd ACHIEVED



DETERMINING THE SAFETY LEVEL

VERIFICATION OF FUNCTIONAL SAFETY



DO NOT HESITATE TO ASK QUESTIONS!



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

