

***Safety manual***

Functional safety  
EN ISO 12100 and EN ISO 13849-1&-2  
and their application



Authors: Christoph Kindervater, Thomas Kramer-Wolf, Matthias Lang, Matthias Taub, Peter Winter  
Issuer: Wieland Electric GmbH  
Brennerstr. 10-14  
96052 Bamberg

Internet: [www.wieland-electric.com](http://www.wieland-electric.com)  
Tel: 0951 / 9324-0  
Fax: 0951 / 9324-198  
Email: [info@wieland-electric.com](mailto:info@wieland-electric.com)

## The authors:

For the past 10 years, Mr Kindervater worked in the design and account management of laser machines. Since 2012, he is responsible as a Certified Safety Engineer for the branch management of safety switchgear and safety controllers.



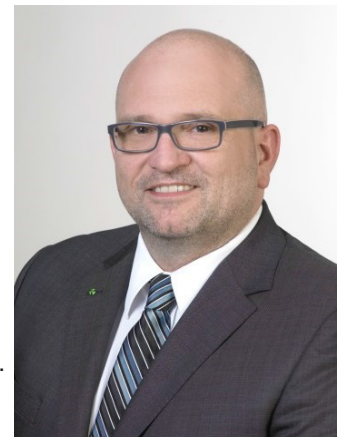
Mr Kramer-Wolf has been working in industry automation for over 30 years. He has been primarily occupied for many years with the functional safety of machines. In addition to his work as a consultant and lecturer in this area, he is active in a number of standardisation committees for functional safety.



Mr Matthias Lang works in product management as an application engineer. Due to his decade-long experience in the laboratory, in development and in product management, he makes a significant contribution to the success of Wieland's safety products. Our customers already profit from his expert knowledge in the concept phase.



Since 1992, Mr Matthias Taub has worked in the design of plant and machine construction as well as distribution. Since 2013, he has been jointly responsible as a Certified Safety Engineer for the branch management of Wieland Electric GmbH with the main focus on safety controller and safety switchgear.



Mr Peter Winter works as a Functional Safety Engineer on the Technical Hotline. For over 30 years, he worked in electrical maintenance, most recently as a leading master craftsman. Since changing to the Technical Hotline, he is a competent contact for our customers regarding all safety applications.



## Contents

1	Foreword.....	8
2	Introduction.....	9
2.1	The reason behind safety technology – Laws and guidelines.....	9
2.2	How does my machine become safe?.....	11
2.3	The safety function.....	12
3	Safety functions.....	13
3.1	Door switch, magnetic – SS2 in PL d.....	13
3.2	E-Stop – single-channel in PL c.....	24
3.3	E-Stop – two-channel in PL d.....	27
3.4	E-Stop – two-channel, cross-circuit detection in PL e.....	30
3.5	Door switch, mechanical – single-channel in PL c.....	34
3.6	Door switch, mechanical – two-channel, equivalent in PL c/d.....	37
3.7	Door switch, mechanical – two-channel, antivalent in PL c/d.....	41
3.8	Door switch, mech. & magn. – 2x single-channel in PL e.....	45
3.9	Door switch, magnetic – two-channel, equivalent in PL e.....	49
3.10	Door switch, magnetic – two-channel, antivalent in PL e.....	52
3.11	Door switch, magnetic and safety mat – 4-wire version in PL d.....	55
3.12	Bumper, single-channel – positively-driven in PL d.....	59
3.13	Two-hand control, type III A in PL c.....	64
3.14	Two-hand control, type III C in PL e.....	67
3.15	Light curtain/grid, type 2 in PL c.....	70
3.16	Light curtain/grid, type 4 in PL e.....	73
3.17	E-Stop in series – two-channel in PL d.....	76
3.18	E-Stop & door switch, mech. in series, single-channel in PL c.....	79
3.19	E-Stop & door switch, magnetic in series, two-channel in PL c.....	82
3.20	Door switch, magnetic in series – two-channel in PL d.....	85
3.21	Door switch, RFID in series – two-channel, equivalent in PL e.....	89
3.22	Door switch, RFID & E-Stop in series (1) – E-Stop –S1 in PL c.....	92
3.23	Door switch, RFID & E-Stop in series (1) – Door –B1 in PL e.....	96
3.24	Door switch, RFID & E-Stop in series (1) – Door –B2 in PL e.....	100
3.25	Door switch, RFID & E-Stop in series (2) – E-Stop in PL e.....	104
3.26	Door switch, RFID & E-Stop in series (2) – Doors in PL e.....	108
3.27	Mode selector in PL e.....	112
3.28	Enabling button in PL e.....	116
3.29	Door guard with interlocklocking in PL d.....	120
4	Terms.....	124
4.1	Doors and other protective equipment.....	124
4.2	Reset or restart.....	126
4.3	Fault exclusions.....	127
4.4	Fault masking.....	127

---

5	Tables & formulae .....	131
5.1	Symbols .....	131
5.2	Determination of PL .....	133
5.3	DC measures .....	140
5.4	Safety principles.....	144
5.5	Hazards (EN ISO 12100 Table B.1) .....	156
5.6	Protective devices.....	158
5.7	Actuators.....	161
6	Standards and references .....	165
7	Notes .....	167
7.1	Copyright.....	167
7.2	Liability .....	167

## Figures

Figure 1: Europe – Standards and laws .....	9
Figure 2: Overview of essential standards of safety technology .....	10
Figure 3: Risk assessment .....	11
Figure 4: Risk graph of EN ISO 13849-1 .....	12
Figure 5: Direct fault masking according to ISO/TR 24119 .....	130
Figure 6: Safety distances - Screenshot of an Excel table .....	159

## Overview of the safety functions

	PL	Cat	Series connection	Emergency STOP	Two-hand control	Enabling button	Mode selector	Door switch, mechanical	Door switch, magnetic	Door switch, RFID	Safety mat/bumper	Light curtain/grid	Door guard locking	Pneumatic valve, STO	Relay, STO	Frequency converter, STO	Frequency converter, SS2	Frequency converter, SLS	Time delay	Chapter
E-Stop – single-channel in PL c	c	1		X											X					3.2
E-Stop – two-channel in PL d	d	3		X												X				3.3
E-Stop – two-channel, cross-circuit detection in PL e	e	4		X											X					3.4
Door switch, mechanical – single-channel in PL c	c	1						X							X					3.5
Door switch, mechanical – two-channel, equivalent in PL c/d	c/d	4						X							X					3.6
Door switch, mechanical – two-channel, antivalent in PL c/d	c/d	4						X							X					3.7
Door switch, mech. & magn. – 2x single-channel in PL e	e	4						X	X						X					3.8
Door switch, magnetic – two-channel, equivalent in PL e	e	4							X						X					3.9
Door switch, magnetic – two-channel, antivalent in PL e	e	4							X						X					3.10
Door switch, magnetic – SS2 in PL d	d	3							X								X			3.1
Door switch, magnetic and safety mat – 4-wire version in PL d	d	4							X	X					X					3.11
Bumper, single-channel – positively-driven in PL d	d	3									X			X						3.12
Two-hand control, type III A in PL c	c	1			X											X				3.13
Two-hand control, type III C in PL e	e	4			X										X					3.14
Light curtain/grid, type 2 in PL c	c	2										X				X				3.15
Light curtain/grid, type 4 in PL e	e	4										X						X		3.16
E-Stop in series – two-channel in PL d	e	4	X	X											X					3.17

	PL	Cat	Series connection	Emergency STOP	Two-hand control	Enabling button	Mode selector	Door switch, mechanical	Door switch, magnetic	Door switch, RFID	Safety mat/bumper	Light curtain/grid	Door guard locking	Pneumatic valve, STO	Relay, STO	Frequency converter, STO	Frequency converter, SLS	Time delay	Chapter
E-Stop & door switch, mech. in series, single-channel in PL c	c	1	X	X				X							X				3.18
E-Stop & door switch, magnetic in series, two-channel in PL c	c	1	X	X					X						X				3.19
Door switch, magnetic in series – two-channel in PL d	d	3	X						X						X				3.20
Door switch, RFID in series – two-channel, equivalent in PL e	e	4	X							X						X			3.21
Door switch, RFID & E-Stop in series (1) – E-Stop –S1 in PL c	c	1	X	X						X					X				3.22
Door switch, RFID & E-Stop in series (1) – Door –B1 in PL e	e	4	X	X						X					X				3.23
Door switch, RFID & E-Stop in series (1) – Door –B2 in PL e	e	4	X	X						X					X				3.24
Door switch, RFID & E-Stop in series (2) – E-Stop in PL e	e	3	X	X						X					X				3.25
Door switch, RFID & E-Stop in series (2) – Doors in PL e	e	4	X	X						X					X				3.26
Mode selector in PL e	e	4					X									X			3.27
Enabling button in PL e	e	3				X			X							X			3.28
Door guard with interlocklocking in PL d	d	2											X					X	3.29

With this application manual, we would like to offer you practical support during the design of your safety solutions. Sample solutions for daily applications using your machine help you to profit from our experience. Wieland has been active in electrical connection technology since 1910 and is therefore a pioneer in this field. As a manufacturer of safety controllers and safety sensors, Wieland can look back on over 30 years of experience in these areas. Our experts in training, advice and technical support are always there for you. Make use of our knowledge and experience.



Ihr Dr. Eitrich  
(Geschäftsführer Wieland Electric GmbH)

## **Wieland Electric supports the entire life cycle of a machine including the following on-site services:**

Wieland Electric unterstützt über den gesamten Lebenszyklus einer Maschine auch mit Serviceleistungen direkt vor Ort:

- Risk assessment
- Verification and validation
- Commissioning check
- Caster measurement
- Recurring testing of light grids
- Inspection before and during operation
- Programming support
- CSE Certified Safety Engineer acc. to EN ISO 13849
- by SGS-TÜV Saar







appropriate standard thus has legal certainty. By using a harmonised standard, he can assume that he is acting in compliance with the law within the scope of the standard. Standards thus do not become technical laws, in particular because other solutions than those described in the standards must always be possible, but those who comply with the standards no longer need to worry about the legal text. Currently almost 800 standards relating to the Machinery directive alone are listed as harmonised, in particular standards for hazardous machines. The most important representatives of the general standards are EN ISO 12100 and EN ISO 13849-1 which are explained in more detail in the following section. As the research into standards proves difficult for many in the absence of access to standards databases, the supplied overview of the standards may prove helpful at least for type B standards which refer to hazards, aspects and technologies. You should always be conscious that standards are also subject to a continuous update process. Typical update intervals are 3 to 5 years which is why a regular check of the topicality of the applied standards is strongly recommended. One of the few research sources which are free of charge and always up-to-date are provided by the online shops of publishers such as Beuth (<http://www.beuth.de/de>), ISO (<http://www.iso.org/iso/home/store>) or IEC (<https://webstore.iec.ch>), even if they have not actually been designed for this purpose.

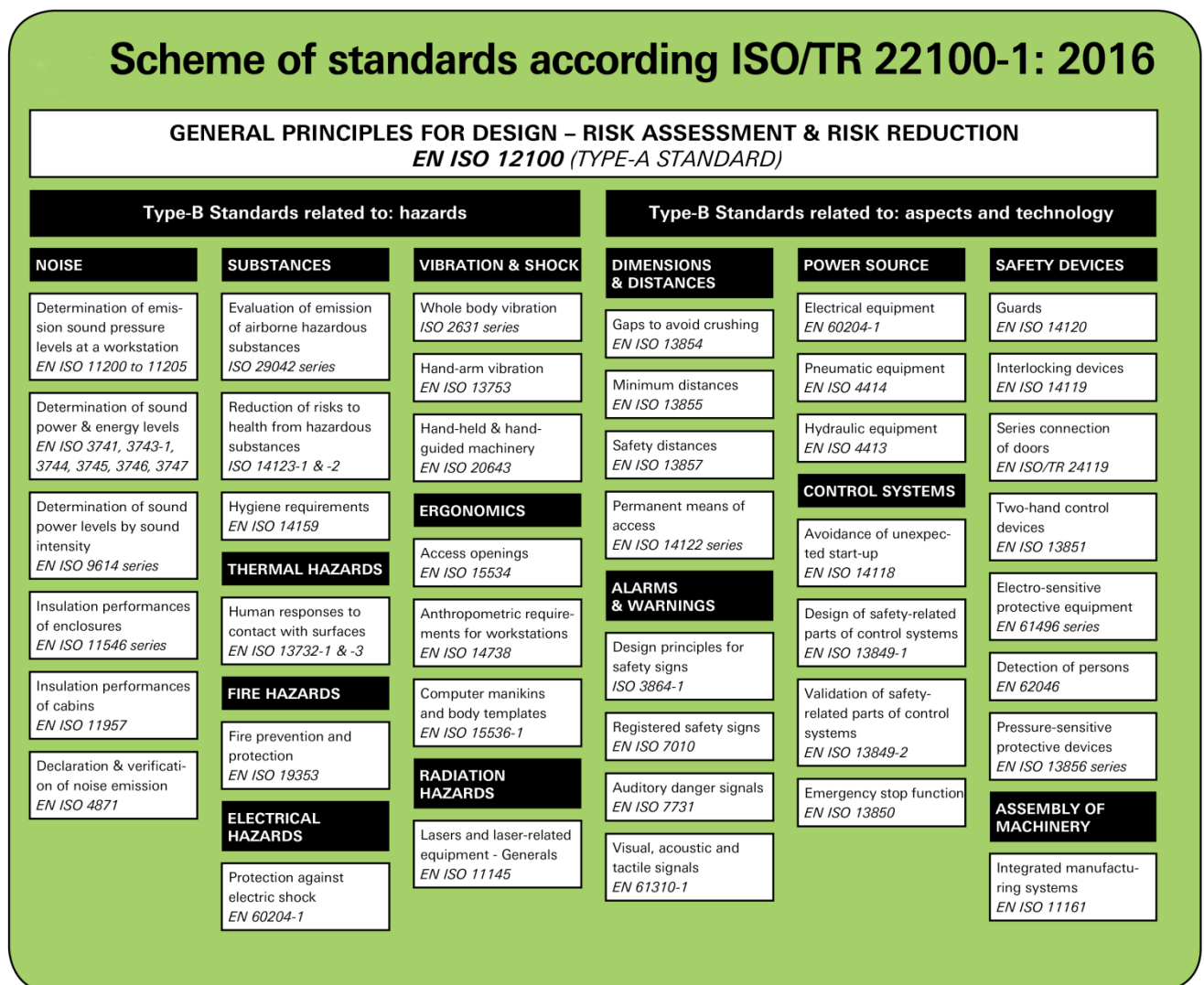


Figure 2: Overview of essential standards of safety technology

### 2.2 How does my machine become safe?

The basis for any type of safety technology is the risk assessment of the machine. Harmonised standards for the respective machine, so-called C type standards, help in this regard. If there is no C type standard or if it cannot be applied to all the aspects of the machine, EN ISO 12100 is used. This standard explains how the limits of the machine are defined, which hazards should be taken into account and how the risk assessment and risk analysis should be carried out (see Fehler! Verweisquelle konnte nicht gefunden werden.).

The risk assessment is typically carried out using a risk graph. The most well-known risk graph is certainly the risk graph in EN ISO 13849-1, (see Figure 4 on page 12) which only carries out a rough classification of the severity of the injury, frequency of exposure to the hazard and avoidability. Other risk graphs are equally usable.

The risk reduction only occurs in the second step. It is important to consider that the measures associated with risk reduction have a clear priority. According to EN ISO 12100, inherently safe design measures must always be used first. These types of solutions are also generally the most cost-effective. If the risk cannot be sufficiently reduced using inherently safe design measures, technical protection measures can be implemented. The effectiveness and suitability of these measures can be assessed according to EN ISO 13848. If it is also not possible to sufficiently reduce the risk using technical measures, is it permitted to use user information as a final option. This is however quite comprehensive as there is the need to document options for a safe operation extensively and to train the users accordingly.

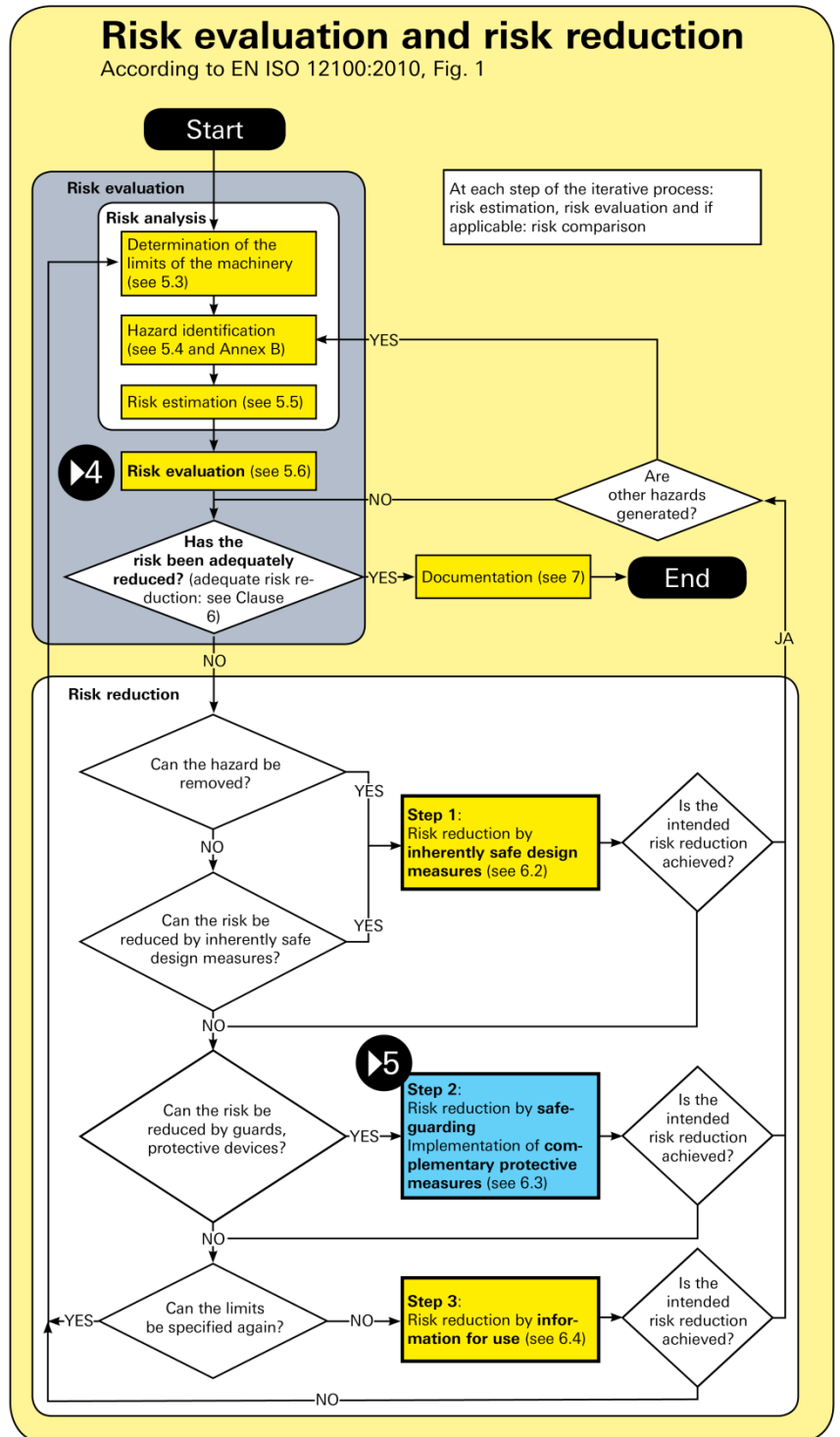


Figure 3: Risk assessment

### 2.3 The safety function

If the risks are known and evaluated and if they should be reduced using technical protective measures, the standard EN ISO 13849-1 is used. The first step in the implementation is always the formulation of the safety function which is frequently described using the abbreviation SRP/CS (safety-related part of a control system). The safety function must be selected so that the risk is reduced to an acceptable level. When formulating the safety function, it helps to clearly name the *trigger event*, the *reaction* and the *safe state*. Generally speaking, the safety function is realised using several elements. Typically, there is a three-step implementation. The evaluation of the situation occurs via a sensor which detects the hazardous state. This is described in EN ISO 13849-1 as *Input*. The logical processing is carried out in the *Logic* unit. The reaction is implemented by the *Output* or actuator and leads to the safe state. The individual elements are mainly used not in one but several safety functions. For example, the same relays can therefore be used for the safety shutdown of an emergency stop or the safety function which monitors access to a risk. The same safety logic is usually used in both cases. Only the *Input* is different in these two cases, namely an emergency stop button, a light grid or curtain.

The applications outlined in this manual show a complete safety function but the focus is on the *Input* or *Output* side depending on the example. Provided that the number of inputs and outputs is not the limiting element and there are no particular requirements for the diagnosis of sensors and actuators, most examples can be varied without any problem by simply combining the required input and output modules. Wherever possible, reference is made to concrete products. The safety-related characteristic data must therefore be seen as examples. Contrary to many standards or collections of examples, requirements that must be met by the machine builder are explicitly named. This relates primarily to fault exclusions and their conditions.

The safety-related calculations are typically carried out with calculation tools such as Sistema which is why they are not given any special consideration in this document and only the input parameters which are required for the calculation are named. All the examples are available separately as Sistema projects to download (<http://wie.li/safetytools>).

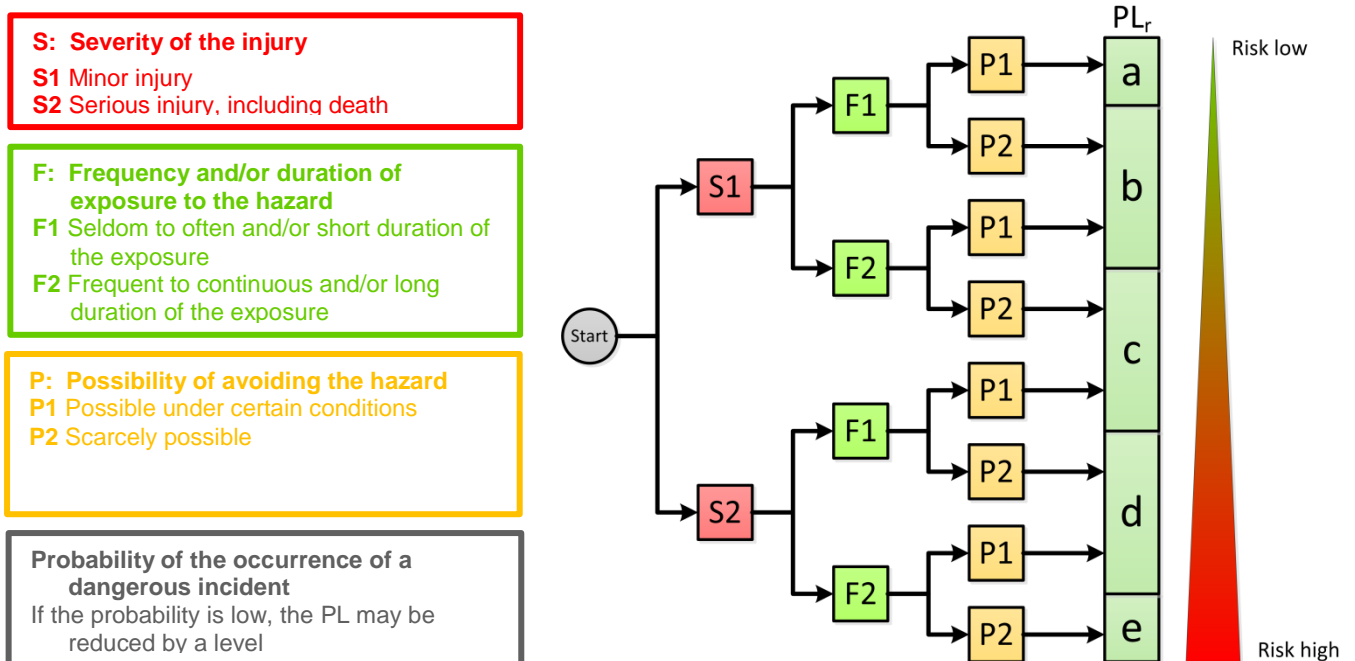


Figure 4: Risk graph of EN ISO 13849-1

Since the individual examples of the safety functions have deliberately been kept concise, a slightly more comprehensive example is shown beforehand in 3.1, together with all the associated steps. Unfortunately, it is impossible to show all the combinations of sensors, logic and actuators. Normally, the relevant aspects from several of the example safety functions named here can be put together with minimal effort by combining the individual subsystems for sensors, logic and actuators. The sensors of a safety function can therefore in most cases be combined with the actuators of another safety function without any problems. An overview of the individual functions as well as their main aspects can be found in Combinations of sensors and the resulting DC on page 128.

### 3 Safety functions

#### 3.1 Door switch, magnetic – SS2 in PL d

##### 3.1.1 Problem definition

In a work area, the drive can lead to a hazard for the workers. The work area is safeguarded with a protective fence and a safety door with door sensor –B1. As the calibration of the drive position is time-consuming, a safe stop under energy (SS2) should be used instead of an energy release. A frequency converter –T1 with integrated SS2 safety function is used for this purpose. To function correctly, the frequency converter requires the position information of the drive which is determined using a rotary transducer –B11. The safety controller –K1 is used as safety logic.

##### 3.1.2 Safety function

<b>Safety function</b>	By opening the door –B1, the drive –T1 is brought to a controlled stop. The safe state is achieved if the drive shaft remains in the current position.
<b>Trigger event</b>	Opening the safety door –B1.
<b>Reaction</b>	Activation of the safety function SS2 in the frequency converter –T1 and prevention of unintentional start-up.
<b>Safe state</b>	Safe standstill of the drive and holding in position.

##### 3.1.3 Description

<b>Function</b>	By opening the safety door –B1: <ul style="list-style-type: none"><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the frequency converter –T1 activates SS2</li><li>• the frequency converter –T1 monitors the standstill using the rotary transducer –B11</li><li>• the frequency converter –T1 triggers STO in the event of a fault</li></ul>
<b>Manual reset</b>	As it is not possible to step behind the safety door –B1, the manual reset of the safety function occurs by closing the door –B1.
<b>Restart</b>	The restart function occurs automatically with the closing of the doors or via a separate start command.

# Safety functions

## Door switch, magnetic – SS2 in PL d

### 3.1.4 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"><li>• Earth faults and cross-circuits in the input circuit are detected by –K1 through test pulses on the sensor cables.</li><li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li><li>• Monitoring of synchronous time between the input circuits -K1:I1 and –K1:I2.</li></ul>
<b>Actuators</b>	Special monitoring of the actuators is not required as it is a certified safety device.

### 3.1.5 Frequencies

The frequencies for operation and access to the hazardous area must be determined.

<b>Operating days per year</b>	$d_{op}$	<b>365</b>
<b>Operating hours / day</b>	$h_{op}$	<b>16</b>
<b>Interval in hours between two occurrences of access into the hazardous area</b>	$T_{cycle}$	<b>4</b>

### 3.1.6 Determination of the Performance Level $PL_r$

The  $PL_r$  is determined using the risk graph of EN ISO 13849-1 in accordance with Figure 4 (page 12). A detailed justification should be carried out for the parameters in which a low risk has been assumed. Note that the  $PL_r$  and the category that is to be applied are sometimes defined by product standards (C type standards). This should be documented in these cases.

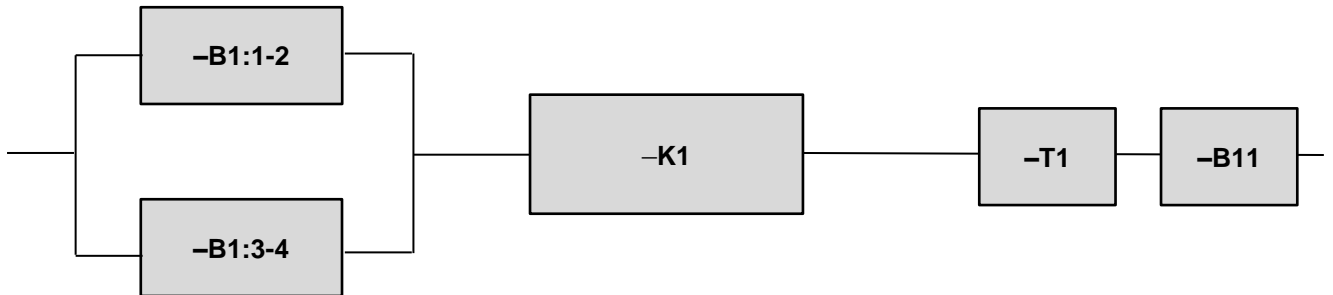
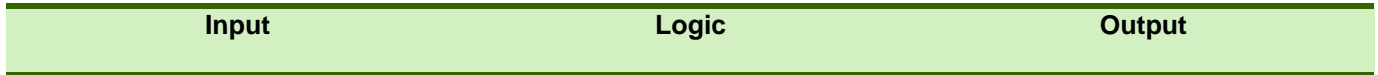
<b><math>PL_r</math></b>	PL d
<b>Reason for the selection of the parameters</b>	F1: A frequency of every 4 hours is regarded as rare. A fault rectification only lasts a few minutes (< 5 minutes).
<b>Are there category requirements from C type standards?</b>	No

# Safety functions

Door switch, magnetic – SS2 in PL d

## 3.1.7 Implementation

Selection of the components required for the safety function and modelling of the block circuit diagram:



**Required data from the device manufacturer**

$B_{10D}; T_M$

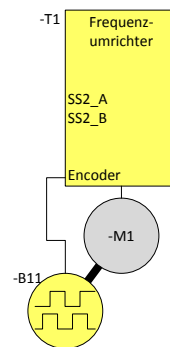
PL;  $PFH_D, T_M$

PL;  $PFH_D, T_M$  for -T1 and -B11

**To be determined/confirmed for the application**

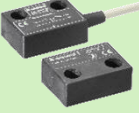

Cat. 4, DC, CCF,  $n_{op}$

**Components**



### 3.1.8 Products

Determination of the characteristic data for the utilised components with the aid of the manufacturer documentation.

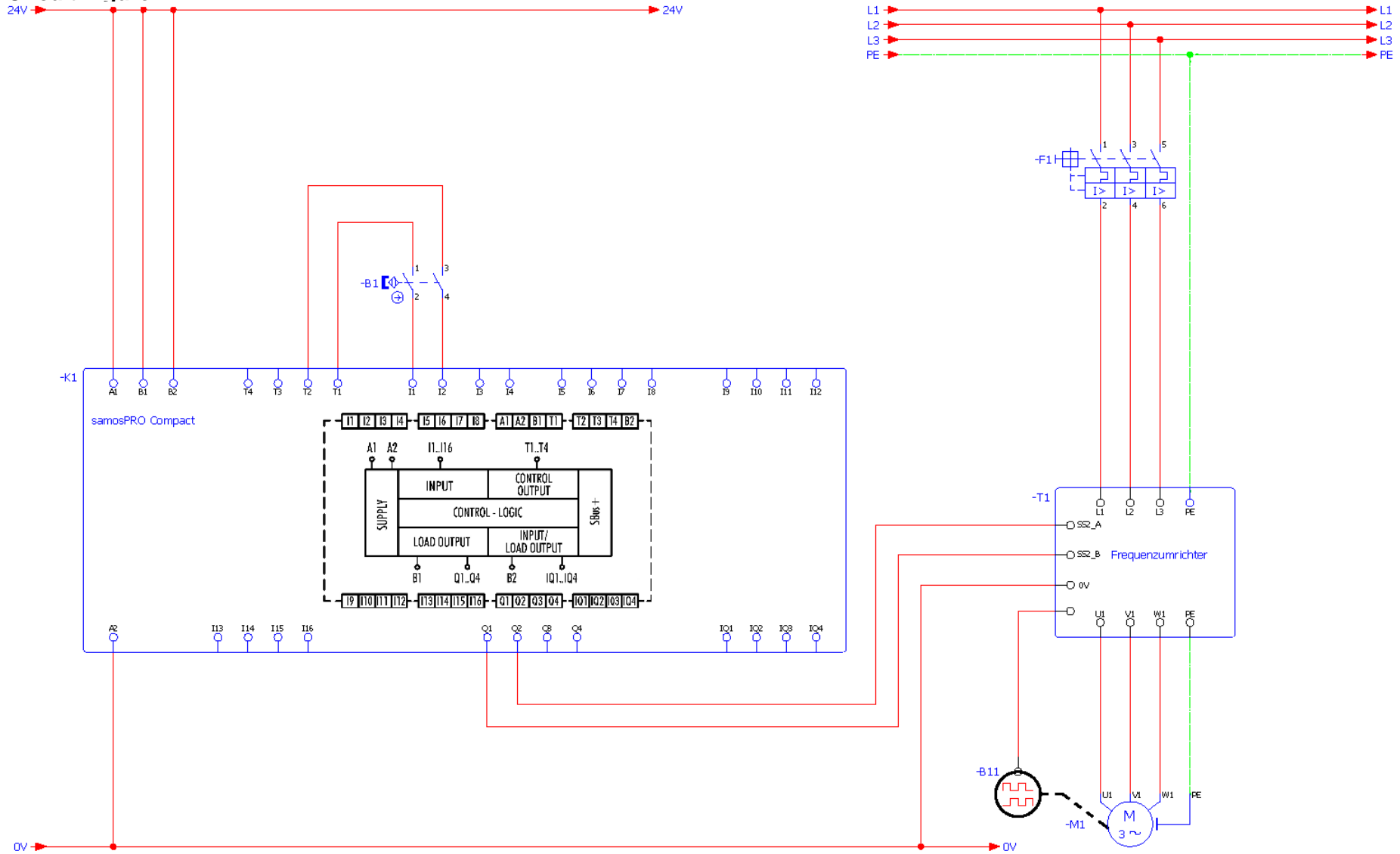
	Product
<b>-B1</b> 	<p>Interlocking device type 3 (door switch with magnetic operation) <b>sensor</b> PRO: SMA01xx Order number: R1.100.0113.0</p> <p>Characteristic data:</p> <ul style="list-style-type: none"><li>• <math>B_{10D} = 10,000,000</math></li><li>• <math>T_M = 20</math> years</li></ul>
<b>-K1</b> 	<p>Programmable safety controller <b>samos</b> PRO: SP-COP2 Order number: R1.190.1310.0</p> <p>Characteristic data:</p> <ul style="list-style-type: none"><li>• <math>PL = PL e</math></li><li>• <math>PFH_D = 1.3 \times 10^{-9}</math></li><li>• <math>T_M = 20</math> years</li></ul>
<b>-T1</b>	<p>Frequency converter with integrated diagnostics and evaluation as PL e. Integrated SS2 safety function.</p> <p>Characteristic data:</p> <ul style="list-style-type: none"><li>• <math>PL = PL e</math></li><li>• <math>PFH_D = 7.79 \times 10^{-10}</math></li><li>• <math>T_M = 20</math> years</li></ul>
<b>-B11</b>	<p>Rotary transducer (for connection to –T1)</p> <p>Characteristic data:</p> <ul style="list-style-type: none"><li>• <math>PL = PL d</math></li><li>• <math>PFH_D = 2.16 \times 10^{-8}</math></li><li>• <math>T_M = 20</math> years</li></ul>



# Safety functions

Door switch, magnetic – SS2 in PL d

## 3.1.9 Circuit Figure



# Safety functions

## Door switch, magnetic – SS2 in PL d

### 3.1.10 Determination of the $MTTF_D$ for Subsystem Input based on frequency of use

In the case of components where wear is dependent on the frequency of usage, the  $MTTF_D$  is determined via the  $B_{10D}$ .

Components	Door switch –B1		
Manufacturer data	$B_{10D}$	10,000,000	cycles
	$T_M$	20	years
Frequencies	$d_{op}$	365	days
	$h_{op}$	16	hours/day
	$t_{cycle}$	4	hours
		14,400	seconds
Determine $n_{op}$	$n_{op}$	$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{cvcle}} \cdot 3600 \frac{s}{h}$ <b>1,460</b>	
Determine $MTTF_D$	$MTTF_D$	$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}}$ <b>68,493</b>	

### 3.1.11 Determination of the DC for Subsystem Input

Determine the DC for the subsystem, ideally using EN ISO 13849-1 Annex E.

Subsystem	Input			
Values according to EN ISO 13849-1 Annex E or values determined via FMEA	Components	DC		Reason
	-B1	99	%	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)
Determine $DC_{avg}$  (no limitation of $MTTF_D$ to 100 or 2,500 years)	$DC_{avg}$	$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D,1}} + \frac{DC_2}{MTTF_{D,2}} + \dots + \frac{DC_n}{MTTF_{D,n}}}{\frac{1}{MTTF_{D,1}} + \frac{1}{MTTF_{D,2}} + \dots + \frac{1}{MTTF_{D,n}}}$		
DC designation (high / medium / low / none)	$DC_{avg}$	high		

### 3.1.12 Determination of the $MTTF_D$ for Subsystem Input

Determine the  $MTTF_D$  of the subsystem from the  $MTTF_D$  values of the individual components.

Subsystem	Input			
Manufacturer data or calculated values	Components	$MTTF_D$	$T_{10D}$	
	-B1	68,493	6,849	years
$MTTF_D$ of channel 1	$MTTF_{D,C1}$	$MTTF_{D,Ci} = \frac{1}{\sum_{i=1}^n \frac{1}{MTTF_{D,i}}}$		
		68,493		
$MTTF_D$ of channel 2	$MTTF_{D,C2}$	68,493		
If 2 channels  (limit channels to 100 or 2,500 years)	$MTTF_{D,total}$	$MTTF_{D,total} = \frac{2}{3} \left[ MTTF_{D,C1} + MTTF_{D,C2} - \frac{1}{\frac{1}{MTTF_{D,C1}} + \frac{1}{MTTF_{D,C2}}} \right]$		
		2,500		
$MTTF_{D,total}$	$MTTF_{D,total}$	2,500		

### 3.1.13 Determination of the CCF for Subsystem Input

If category 2 or higher has been used for the subsystem and not all the elements have been classified with PL values by the manufacturer, the determination of the CCF for the subsystem is required.

Measures against CCF	For electronics	Points	Fulfilled?
Separation between the signal paths	Creepage distances and clearances on printed circuit boards	15	15
Diversity	e.g. different processors	20	0
Protection against overvoltage, excess pressure ...	Protection against overvoltage (e.g. contactors, power supply unit)	15	15
Well-trying components		5	0
FMEA in development	FMEA in the system conception	5	5
Competence / training	Qualification measure	5	5
Protection against contamination and EMC	EMC test	25	25
Other influences (e.g. temperature, shock)	Compliance with the environmental conditions according to the product specification	10	10
<b>Total CCF</b>	<b>Total number of points (<math>65 \leq CCF \leq 100</math>):</b>		<b>75</b>

### 3.1.14 Determination of the PL and PFH<sub>D</sub> for Subsystem Input

With the established data, the PL and PFH<sub>D</sub> can be determined for the Subsystem Input using EN ISO 13849-1 Annex K (see Chapter 5.2.6).

Subsystem	Input	
Dependent on the subsystem	Determined values (EN ISO 13849-1 Annex K)	
MTTF <sub>D,total</sub>	2,500	years
DC <sub>avg</sub>	99	%
Category	4	
PL	e	
PFH <sub>D</sub>	9.06 x 10 <sup>-10</sup>	1/h
CCF fulfilled?	Yes	Fulfilled?
T <sub>M</sub>	20 years	years

# Safety functions

## Door switch, magnetic – SS2 in PL d

### 3.1.15 Determination of the PL and PFH<sub>D</sub> for Subsystem Logic

As the Subsystem Logic is a pre-certified component, no determination of the data is required.

<b>Subsystem</b>	<b>Logic – SPS –K1</b>	
<b>Dependent on the subsystem</b>	Manufacturer data	
<b>Category</b>	4	
<b>PL</b>	PL e	
<b>PFH<sub>D</sub></b>	1.1 x 10 <sup>-9</sup>	1/h
<b>T<sub>M</sub></b>	20 years	years

### 3.1.16 Determination of the PL and PFH<sub>D</sub> for Subsystem Output

The Subsystem Output consists of two pre-certified components. They can either be considered as separate subsystems or combined into one subsystem as shown here.

Subsystem	Output				
<b>Values according to manufacturer data</b>	Components	PL	PFH <sub>D</sub>	Cat.	T <sub>M</sub>
	-T1	e	7.79 x 10 <sup>-10</sup>	4	20
	-B11	d	2.16 x 10 <sup>-8</sup>	3	20
<b>Determine PFH<sub>D</sub></b>	PFH <sub>D</sub>	$PFH_D = 7.79 \times 10^{-10} + 2.16 \times 10^{-8}$ $= 2.24 \times 10^{-8}$		$PFH_D = \sum_i PFH_{D,i}$	
<b>Determine PL</b>	PL	$PL \leq \min_i PL_i$ and consider PL limits for PFH <sub>D</sub> <b>PL d</b>			
<b>Determine category</b>	Cat.	$Cat. \leq \min_i Cat_i$ <b>Cat. 3</b>			

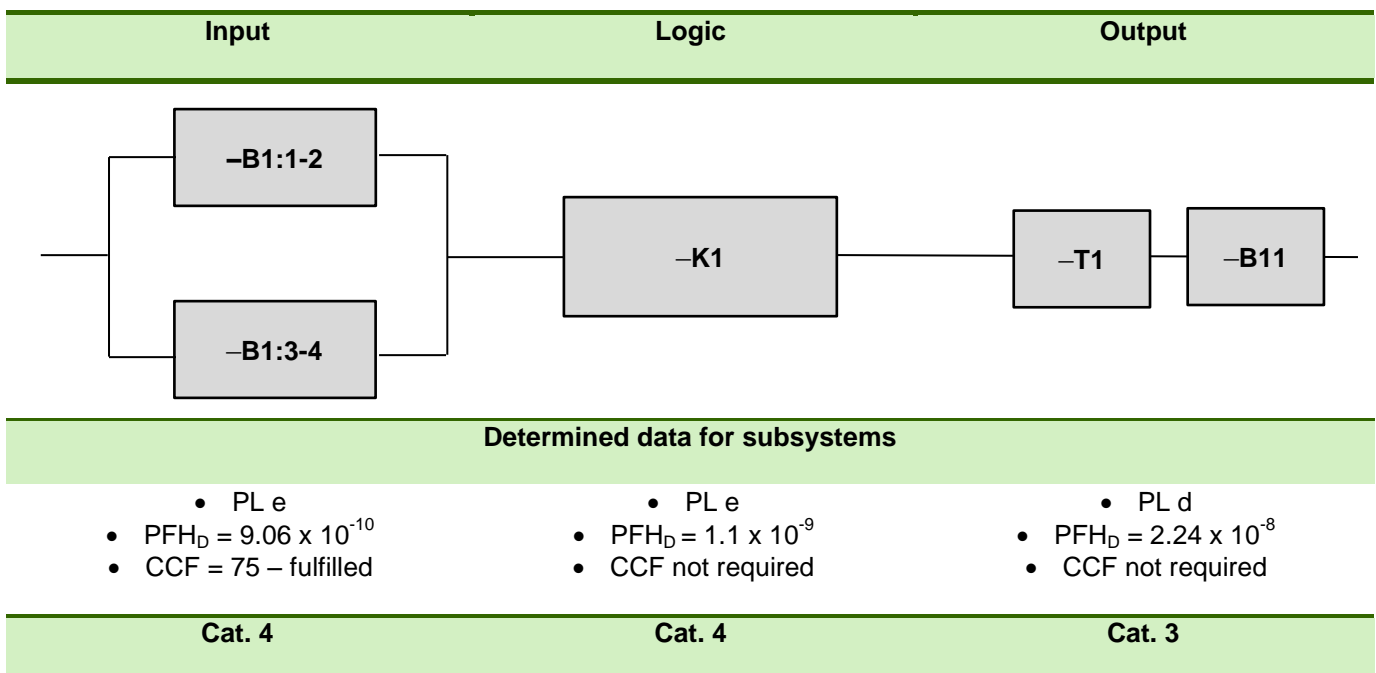
# Safety functions

Door switch, magnetic – SS2 in PL d

Subsystem	Output	
Dependent on the subsystem	Determined data	
Category	3	
PL	PL d	
PFH <sub>D</sub>	2.24 x 10 <sup>-8</sup>	1/h
T <sub>M</sub>	20	years

### 3.1.17 Determination of the overall PL

The overall PL is determined based on the previously established values of the subsystem. Finally an assessment is made whether the achieved PL is sufficient for the required PL.



# Safety functions

Door switch, magnetic – SS2 in PL d

Summary		
Required performance level	PL <sub>r</sub>	PL d
CCF fulfilled for all subsystems?	Fulfilled?	Yes
Category requirements from C type standards met for all subsystems?	Fulfilled?	No requirements
Determine PFH <sub>D,total</sub>	PFH <sub>D,total</sub>	$PFH_D = \sum_i PFH_{D,i}$ $2.45 \times 10^{-8}$
PFH <sub>D</sub> sufficient until (requirements from EN ISO 13849-1 Tab. 3 – see 5.2.3)	PL <sub>PFHD</sub>	PL e
Determine PL <sub>total</sub> based on PL of the subsystems and requirements from EN ISO 13849-1 Tab.3	PL <sub>total</sub>	$PL_{total} \leq \min_i PL_i$  PL d
PL <sub>r</sub> ≤ PL?	Fulfilled?	Yes

### 3.2 E-Stop – single-channel in PL c

#### 3.2.1 Safety function

<b>Safety function</b>	By pressing the emergency stop button –S1, all the drives of the system are brought to a controlled stop.
<b>Trigger event</b>	Activation of one of the emergency actuators by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.2.2 Description

<b>Function</b>	By pressing the emergency stop button –S1: <ul style="list-style-type: none"><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the contactor –Q1 drops out</li><li>• the motor –M1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function is carried out by turning the emergency stop button –S1 to release.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"><li>• the emergency stop button –S1 is not pressed</li></ul>
<b>Feedback circuit</b>	No feedback circuit is used

#### 3.2.3 Safety review



<b>Sensors</b>	<ul style="list-style-type: none"><li>• Earth faults in the input circuit are detected on the sensor cable by –K1.</li><li>• The emergency stop button has a safeguard against malfunctions. It detects when the actuator is disconnected from the switch contacts and interrupts the electric emergency stop circuits.</li></ul>
<b>Actuators</b>	<ul style="list-style-type: none"><li>• A well-tried component in the sense of EN ISO 13849-2.</li></ul>



# Safety functions

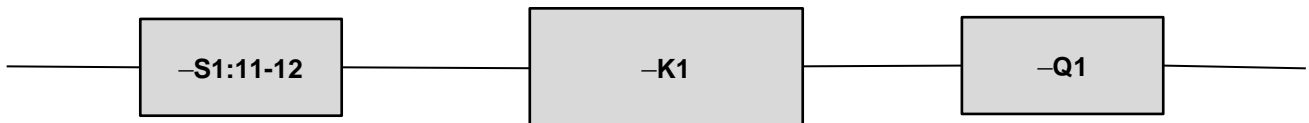
## E-Stop – single-channel in PL c

### 3.2.4 Products (options)

	Product
<b>-S1</b> 	Emergency stop device (1-channel) with contact block detachment monitoring <b>sensor</b> PRO: SNH-1102 Order number: R1.200.1102.0
<b>-K1</b> 	Safety relay <b>safe</b> RELAY: SNO 4003K Order number: R1.188.0500.1
<b>-Q3</b>	Power contactor with the following properties: <ul style="list-style-type: none"> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

### 3.2.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------



Required data from the device manufacturer		
--	--	--

$B_{10D}$ ;  $T_M$

PL; PFH<sub>D</sub>,  $T_M$

$B_{10D}$ ;  $T_M$

To be determined/confirmed for the application		
--	--	--

- CCF not required
  - Cat. 1
- DC not required
  - $n_{op}$

- CCF not required
  - Cat. 4
- DC not required
- $n_{op}$  not required

- CCF not required
  - Cat. 1
- DC not required
  - $n_{op}$

Maximum achievable PL		
-----------------------	--	--

PL c

PL e

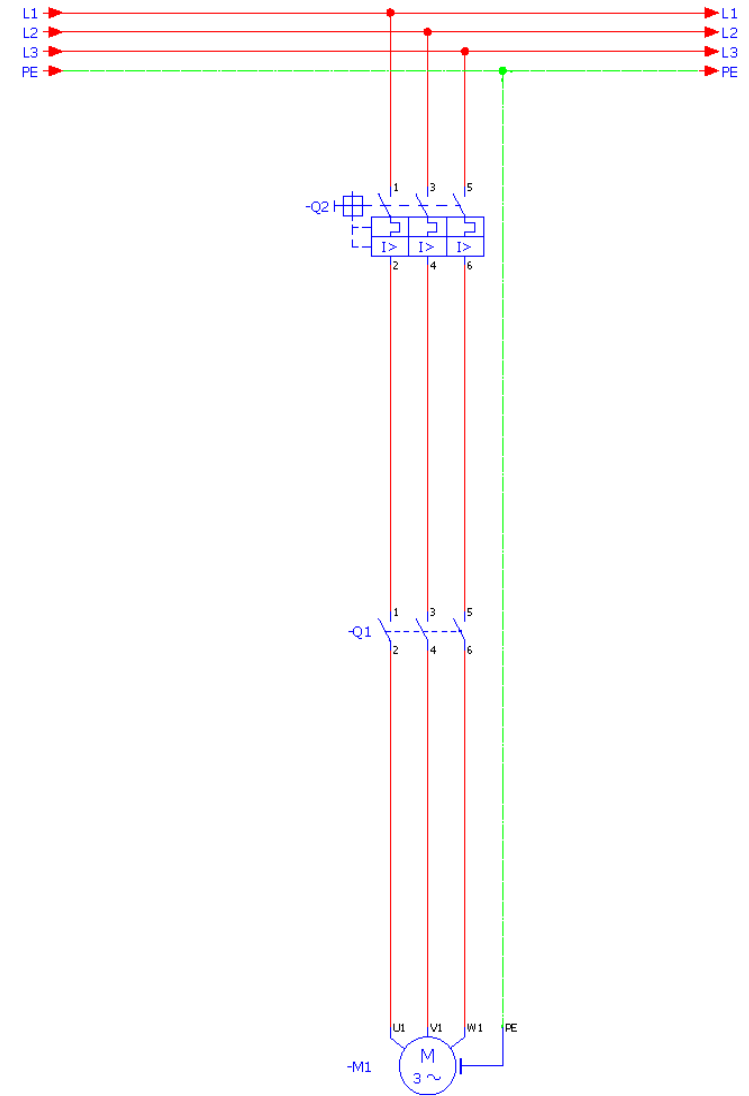
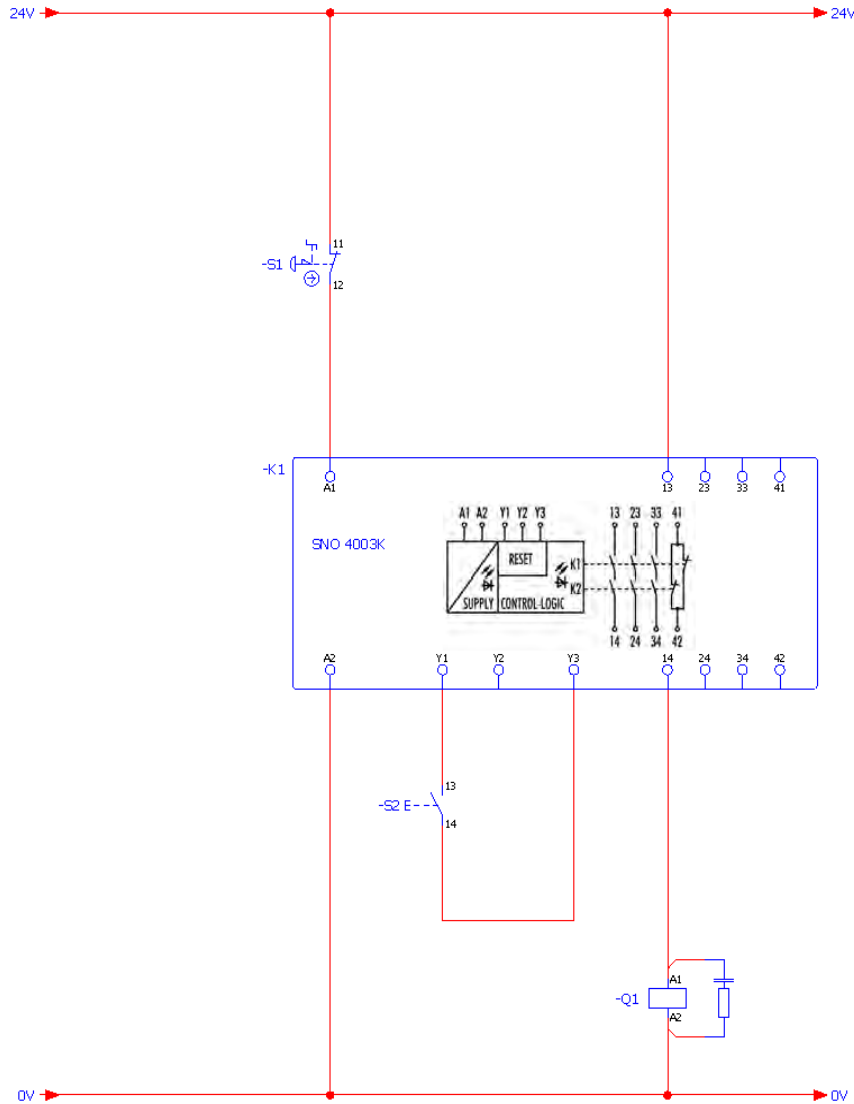
PL c

PL c		
------	--	--

# Safety functions

E-Stop – single-channel in PL c

## 3.2.6 Circuit diagram



### 3.3 E-Stop – two-channel in PL d

#### 3.3.1 Safety function

<b>Safety function</b>	By pressing the emergency stop button –S1, all the drives of the system are brought to a controlled stop.
<b>Trigger event</b>	Activation of one of the emergency stop actuating elements by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.3.2 Description

<b>Function</b>	By pressing the emergency stop button –S1: <ul style="list-style-type: none"><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the frequency converter –T1 with STO safety input is de-energised</li><li>• machine 1 is stopped.</li></ul>
<b>Manual reset</b>	The manual reset of the safety function is carried out by turning the emergency stop button –S1 to release.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"><li>• the emergency stop button –S1 is not pressed</li></ul>
<b>Feedback circuit</b>	Not required here as –T1 is a device with integrated diagnostics.



#### 3.3.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"><li>• Earth faults in the input circuit are detected on the sensor cables by –K1.</li><li>• Cross-circuits are not detected due to the Cat. 3 structure and thus “Cross comparison with dynamisation without high-performance fault detection” → DC = 90%.</li><li>• The emergency stop button has a safeguard against malfunctions. This detects when the actuating element is disconnected from the switch contacts and interrupts one of the electric emergency stop circuits.</li><li>• Monitoring of synchronous time between the input circuits –S12 and –S22.</li></ul>
<b>Actuators</b>	<ul style="list-style-type: none"><li>• Frequency converter with integrated diagnostics and evaluation as PL d.</li><li>• STO input is classified as PL d.</li><li>• Fault exclusion on wiring from –K1 to –T1 as in switch cabinet.</li></ul>

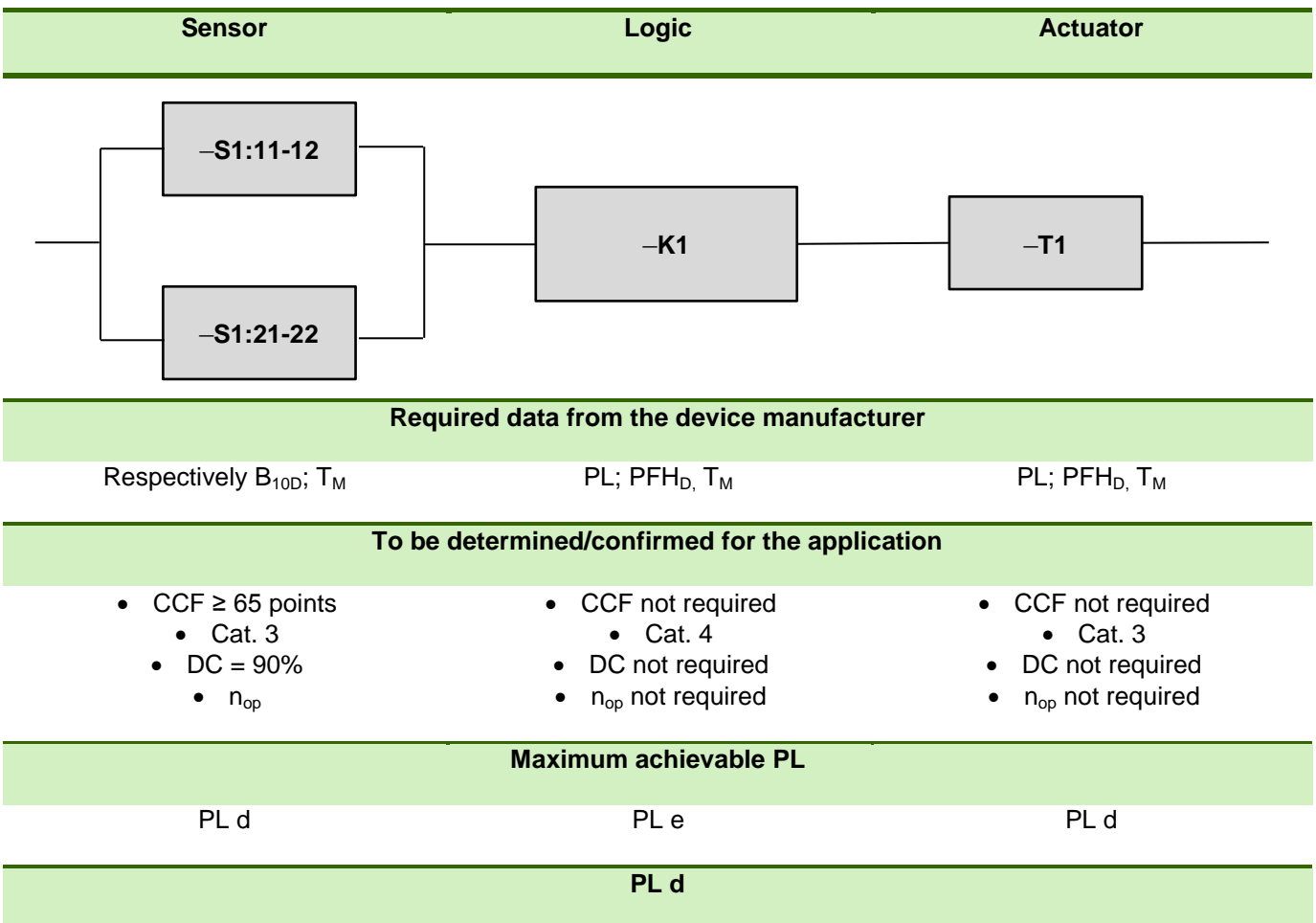
# Safety functions

## E-Stop – two-channel in PL d

### 3.3.4 Products (options)

	Product
 <p><b>-S1</b></p>	Emergency stop device (2-channel) with contact block detachment monitoring <b>sensor</b> PRO: SNH-1122 Order number: R1.200.1122.0
 <p><b>-K1</b></p>	Safety relay <b>safe</b> RELAY: SNO 4062KM Order number: R1.188.0720.2
<p><b>-T1</b></p>	Frequency converter with integrated diagnostics and evaluation as PL d. Integrated STO safety function.

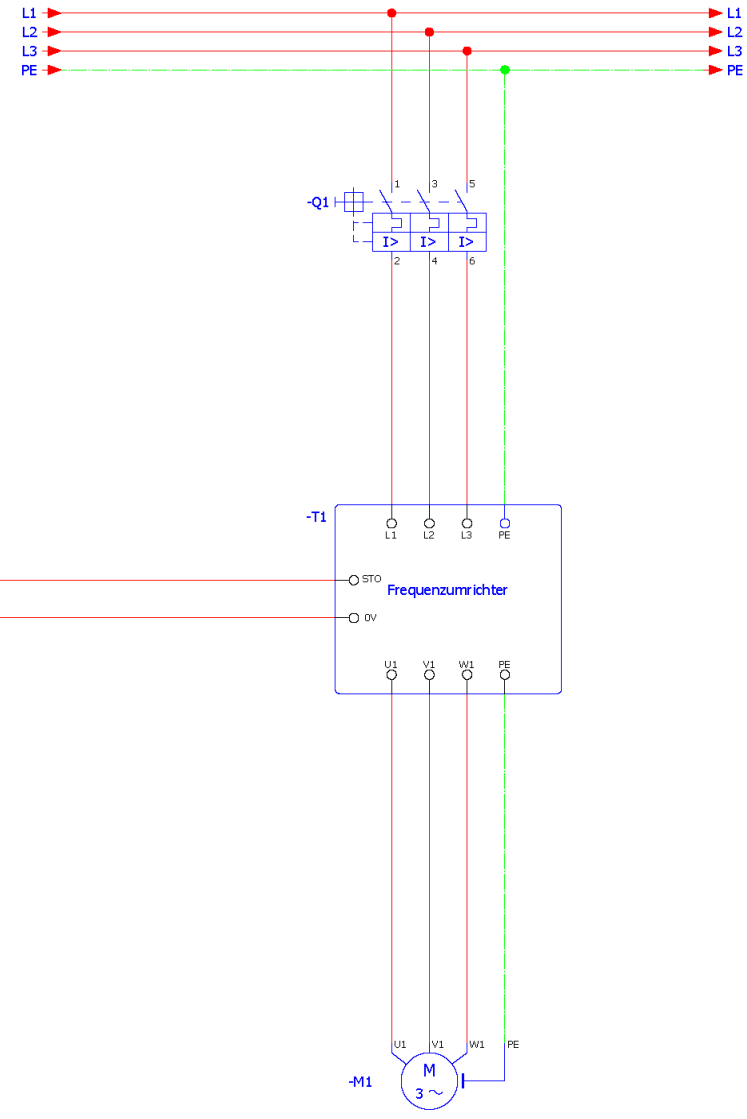
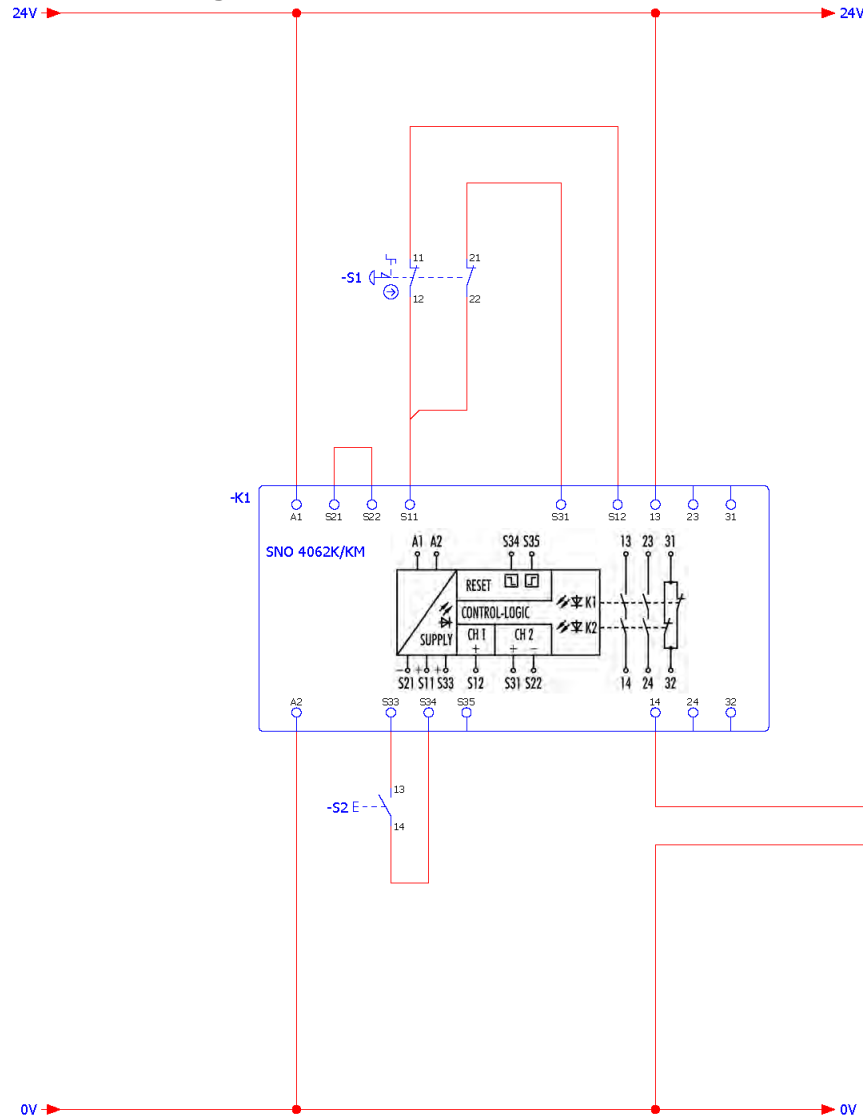
### 3.3.5 Modelling according to EN ISO 13849-1



# Safety functions

E-Stop – two-channel in PL d

## 3.3.6 Circuit diagram



### 3.4 E-Stop – two-channel, cross-circuit detection in PL e

#### 3.4.1 Safety function

<b>Safety function</b>	By pressing the emergency stop button –S1, all the drives of the system are brought to a controlled stop.
<b>Trigger event</b>	Activation of the emergency stop button –S1 by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.4.2 Description

<b>Function</b>	By pressing the emergency stop button –S1: <ul style="list-style-type: none"><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the contactors –Q1 and –Q2 drop out</li><li>• machine 1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function is carried out by turning the emergency stop button –S1 to release.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"><li>• the emergency stop button –S1 is not pressed</li><li>• the contactors –Q1 and –Q2 have dropped out</li></ul>
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of the safety switchgear –K1.



# Safety functions

## E-Stop – two-channel, cross-circuit detection in PL e

### 3.4.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults and cross-circuits in the input circuit are detected by –K1 through test pulses on the sensor cables.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li> <li>• The emergency stop button has a safeguard against malfunctions. This detects if the actuating element is disconnected from the switch contacts and interrupts one of the electric emergency stop circuits.</li> <li>• Monitoring of synchronous time between the input circuits –K1:S12 and K1:S22.</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</li> <li>• The contactors have positively-driven feedback contacts.</li> <li>• Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.</li> </ul>

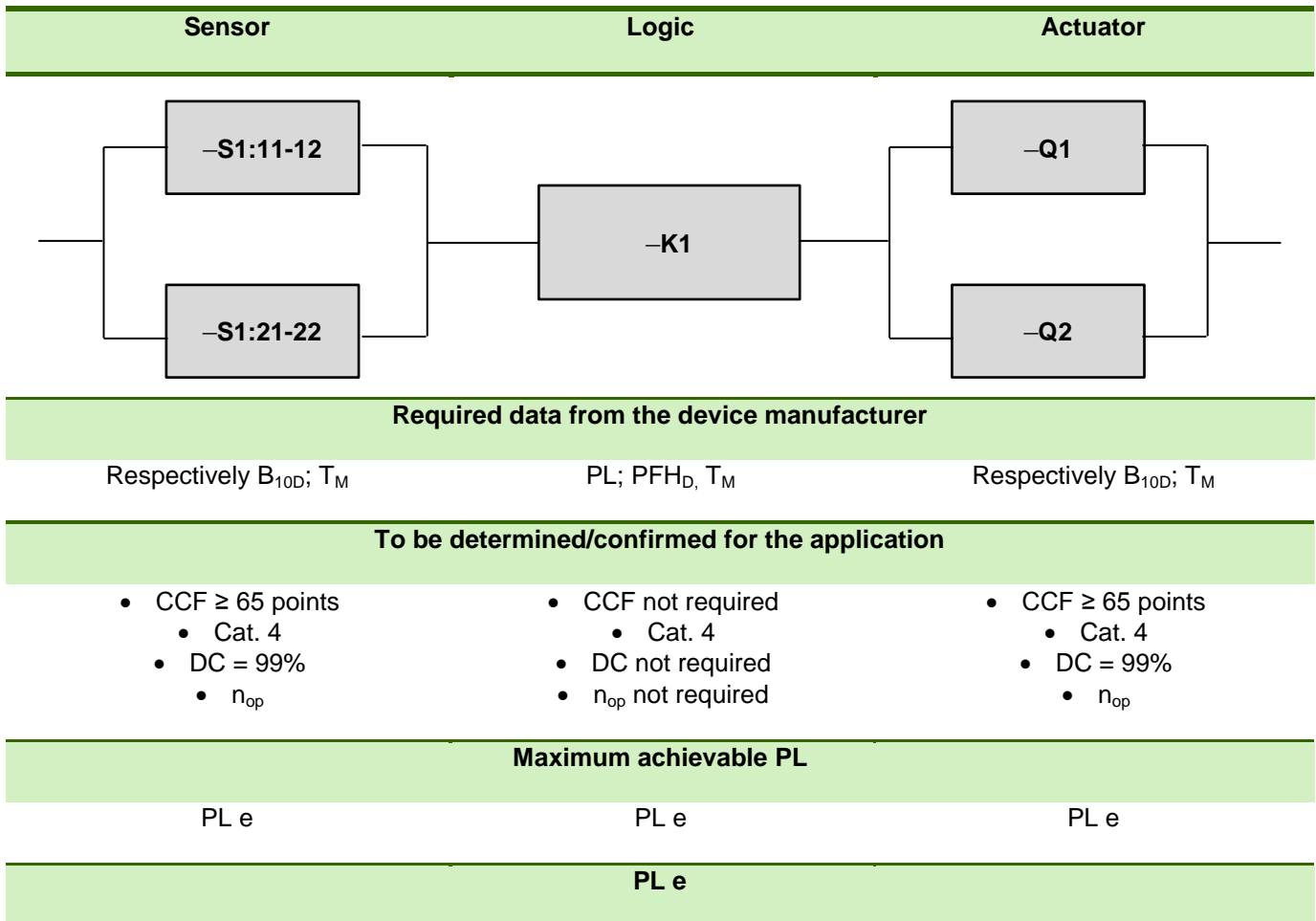
### 3.4.4 Products (options)

	Product
<b>–S1</b> 	Emergency stop device (2-channel) with contact block detachment monitoring <b>sensor</b> PRO: SNH-1122 Order number: R1.200.1122.0
<b>–K1</b> 	Safety relay <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>–Q1; –Q2</b>	Power contactor with the following properties: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts.</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

# Safety functions

## E-Stop – two-channel, cross-circuit detection in PL e

### 3.4.5 Modelling according to EN ISO 13849-1

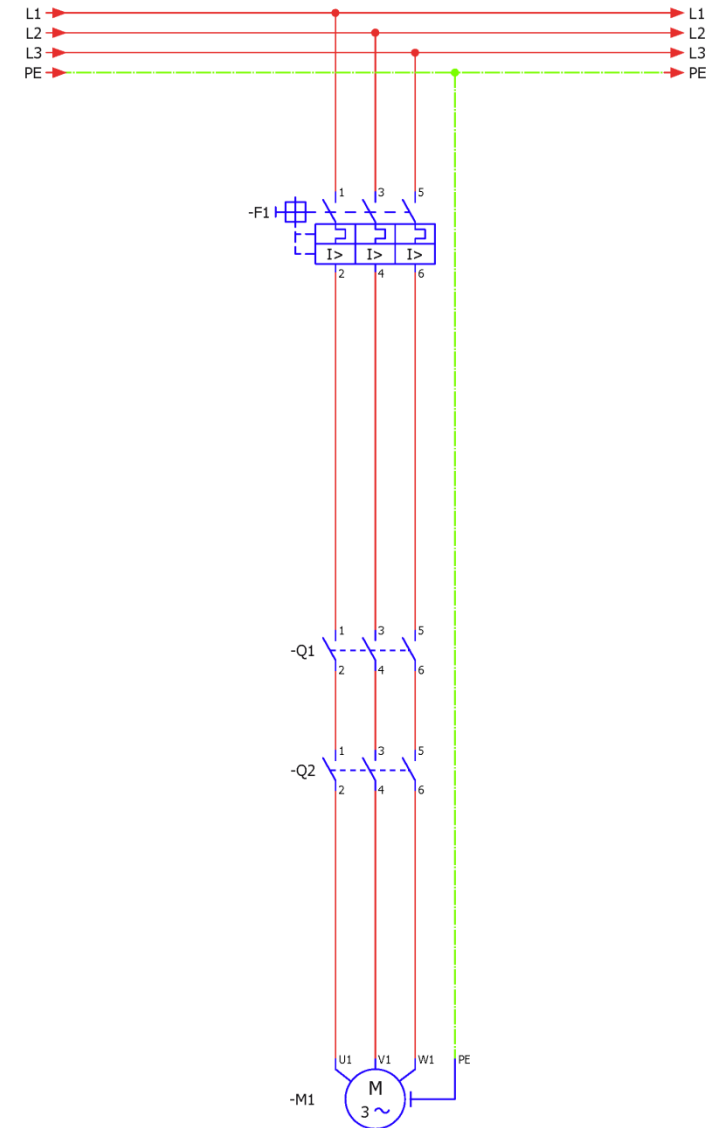
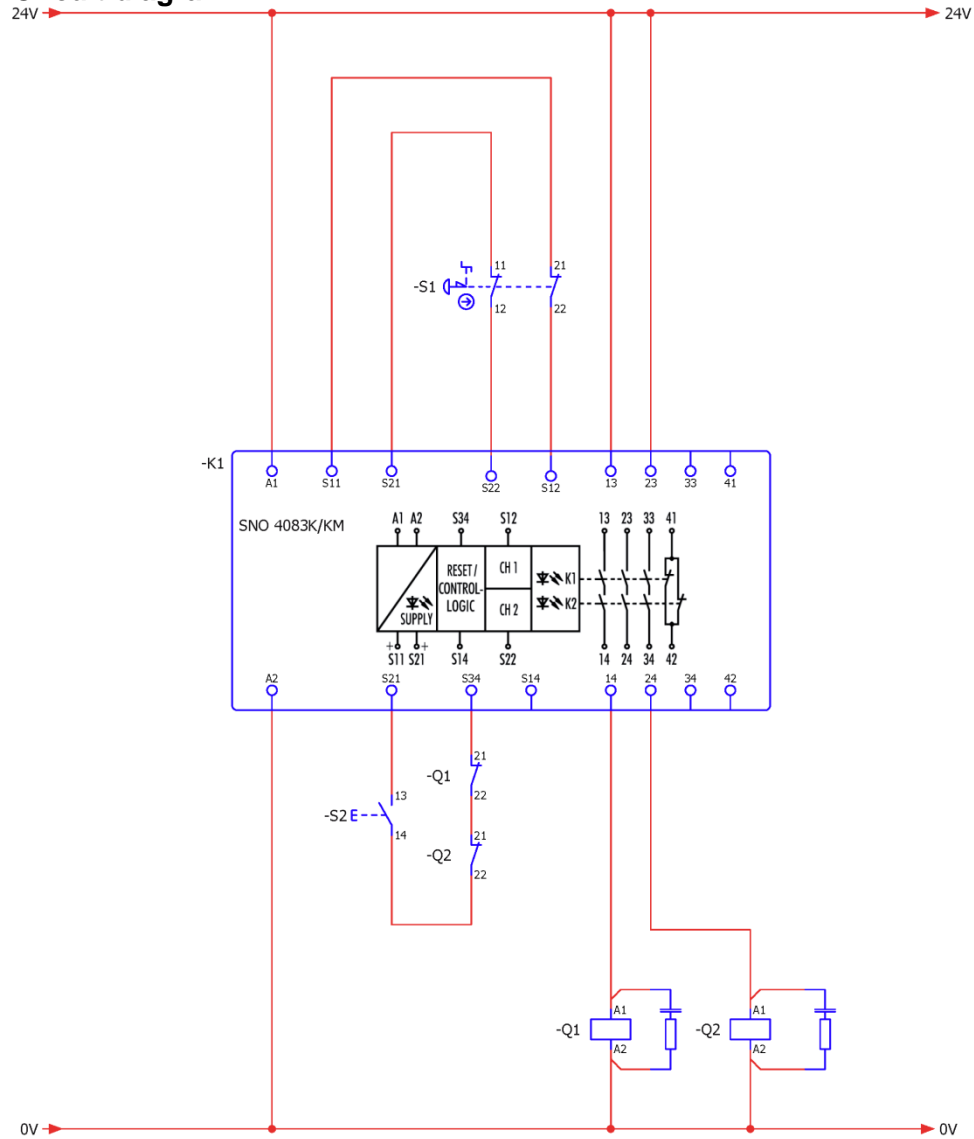




# Safety functions

E-Stop – two-channel, cross-circuit detection in PL e

## 3.4.6 Circuit diagram



### 3.5 Door switch, mechanical – single-channel in PL c

#### 3.5.1 Safety function

Safety function	By opening the door, all the drives in the system are stopped / de-energised.
Trigger event	Opening of a door by the operator.
Reaction	De-energising of the drives.
Safe state	Drives are de-energised.

#### 3.5.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch is operated</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the positively-driven contactor –Q1 drops out</li><li>• machine 1 is stopped.</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door. The door switch –B1 is closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart function occurs by closing the door(s). A restart is only possible if: <ul style="list-style-type: none"><li>• the doors are closed</li><li>• the positively-driven contactors –Q1 and –Q2 have dropped out</li></ul> It is not possible to step behind the doors due to the design.
<b>Feedback circuit</b>	The positively-driven normally closed contact of the contactor –Q1 is monitored in the feedback circuit of the safety switchgear –K1.



#### 3.5.3 Safety review

Sensors	<ul style="list-style-type: none"><li>• Earth faults in the input circuit are detected by –K1 on the sensor cable.</li><li>• A fault can lead to the loss of the safety function. DC = none</li><li>• Faults are only detected on the next test cycle (manual).</li></ul>
Actuators	The contactor has a positively-driven feedback contact. DC = 99%. The DC is however negligible in Cat. 1.

# Safety functions

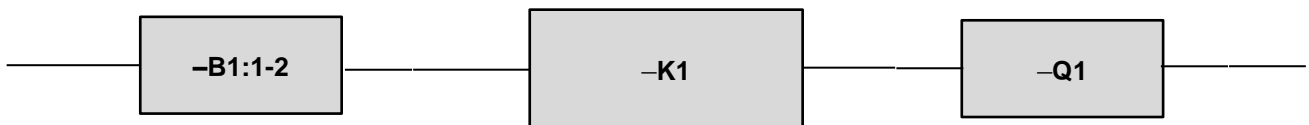
Door switch, mechanical – single-channel in PL c

## 3.5.4 Products (options)

Product	
-B1	 <p>Interlocking device type 2 (door switch with separate actuating element)  <b>sensor</b> PRO: SMS3x10                      Order number: R1.320.3010.0</p>
-K1	 <p>Safety relay  <b>safe</b> RELAY: SNO 4003K                      Order number: R1.188.0500.1</p>
-Q1	<p>Power contactor with the following properties:</p> <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

## 3.5.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------



Required data from the device manufacturer		
--	--	--

$B_{10D}$ ;  $T_M$

PL; PFH<sub>D</sub>,  $T_M$

$B_{10D}$ ;  $T_M$

To be determined/confirmed for the application		
--	--	--

- CCF not required
  - Cat. 1
- DC = none
  - $n_{op}$

- CCF not required
  - Cat. 4
- DC not required
- $n_{op}$  not required

- CCF not required
  - Cat. 1
- DC = none
  - $n_{op}$

Maximum achievable PL		
-----------------------	--	--

PL c

PL e

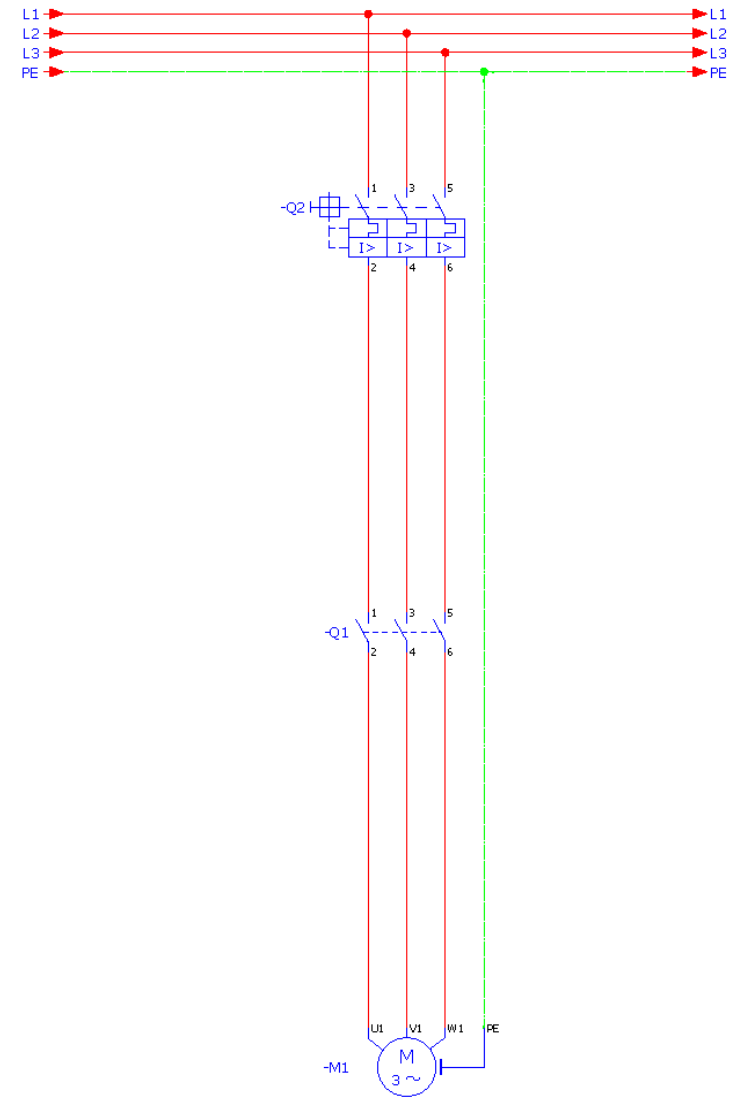
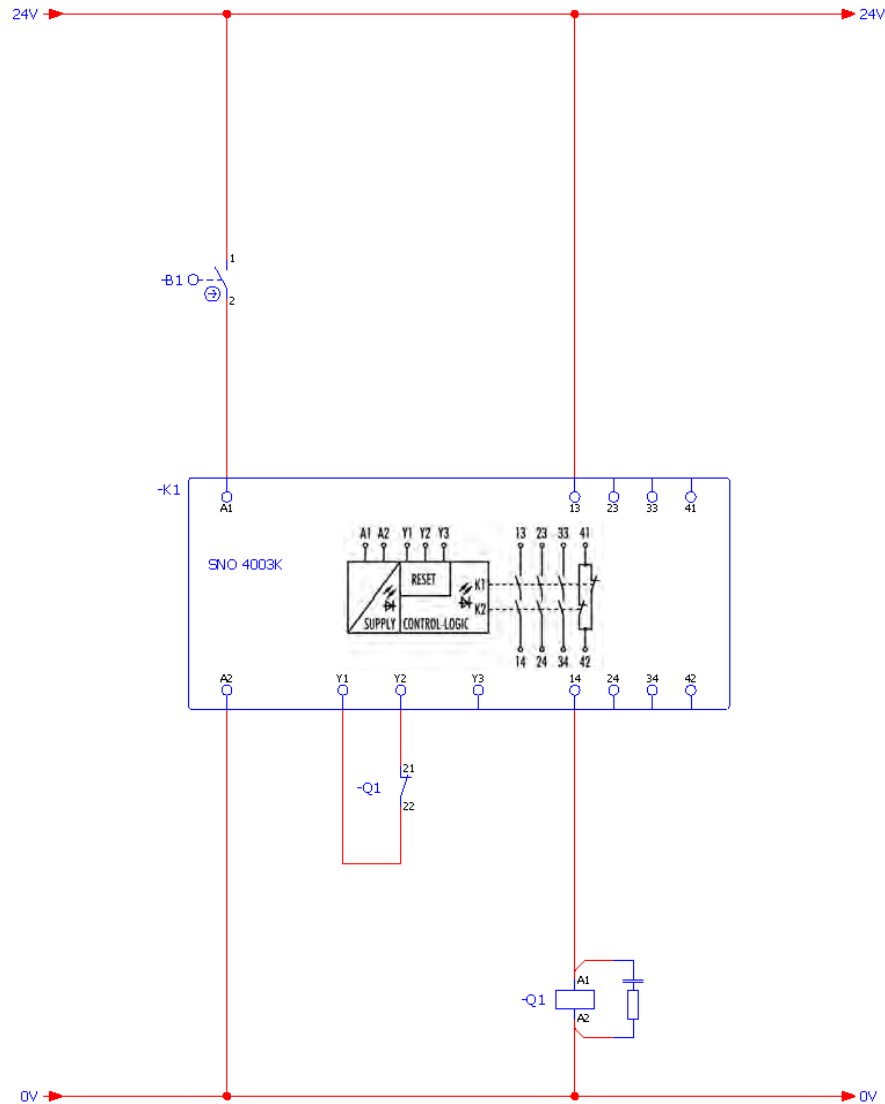
PL c

PL c		
------	--	--

# Safety functions

Door switch, mechanical – single-channel in PL c

## 3.5.6 Circuit diagram



### 3.6 Door switch, mechanical – two-channel, equivalent in PL c/d

#### 3.6.1 Safety function

<b>Safety function</b>	By opening the door, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of the door by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.6.2 Description

<b>Function</b>	<p>By opening the door(s):</p> <ul style="list-style-type: none"> <li>• the door switch is operated</li> <li>• the input circuit on safety switchgear –K1 is interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the positively-driven contactors –Q1 und –Q2 drop out</li> <li>• machine 1 is stopped.</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door. The door switch –B1 is closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	<p>The restart function occurs by closing the door. A restart may only be possible if:</p> <ul style="list-style-type: none"> <li>• the doors are closed</li> <li>• the positively-driven contactors –Q1 und –Q2 have dropped out</li> </ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.

#### 3.6.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults and cross-circuits in the input circuit are detected by –K1 through test pulses on the sensor cables.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1.</li> </ul> <p>Fault exclusions:</p> <ul style="list-style-type: none"> <li>• Fault exclusion on failure of the actuating element by the machine builder. The installation must generally be carried out according to the installation instructions of the switch manufacturer.</li> <li>• Fault exclusion on the mechanical failure of the switch. The installation must generally be carried out according to the installation instructions of the switch manufacturer.</li> <li>• If the fault exclusions are made, Cat. 4 can be achieved but the PL is limited to PL d.</li> <li>• If these fault exclusions are not possible, Cat. 1 can be achieved as a maximum.</li> </ul>
----------------	---



# Safety functions

## Door switch, mechanical – two-channel, equivalent in PL c/d

### Actuators

Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2. The contactors have positively-driven feedback contacts. DC = 99%.

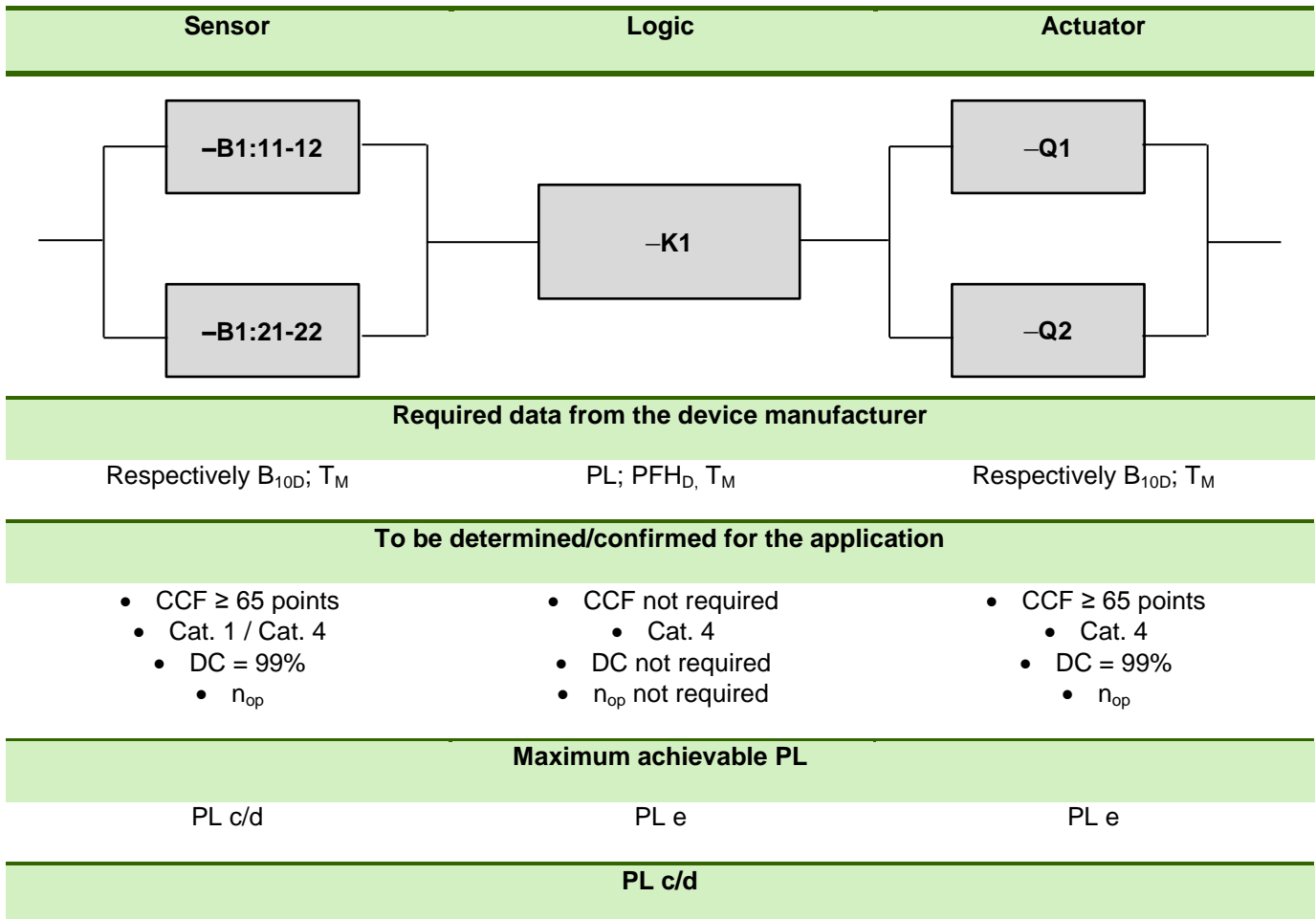
### 3.6.4 Products (options)

	Product
<b>–B1</b> 	Interlocking device type 2 (door switch with separate actuating element) <b>sensor</b> PRO: SMS2x20 Order number: R1.320.2020.0
<b>–K1</b> 	Safety relay <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>–Q1; –Q2</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"><li>• Contactor with positively-driven feedback contacts</li><li>• Suitable for the expected switching load and frequency</li><li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li></ul>

# Safety functions

Door switch, mechanical – two-channel, equivalent in PL c/d

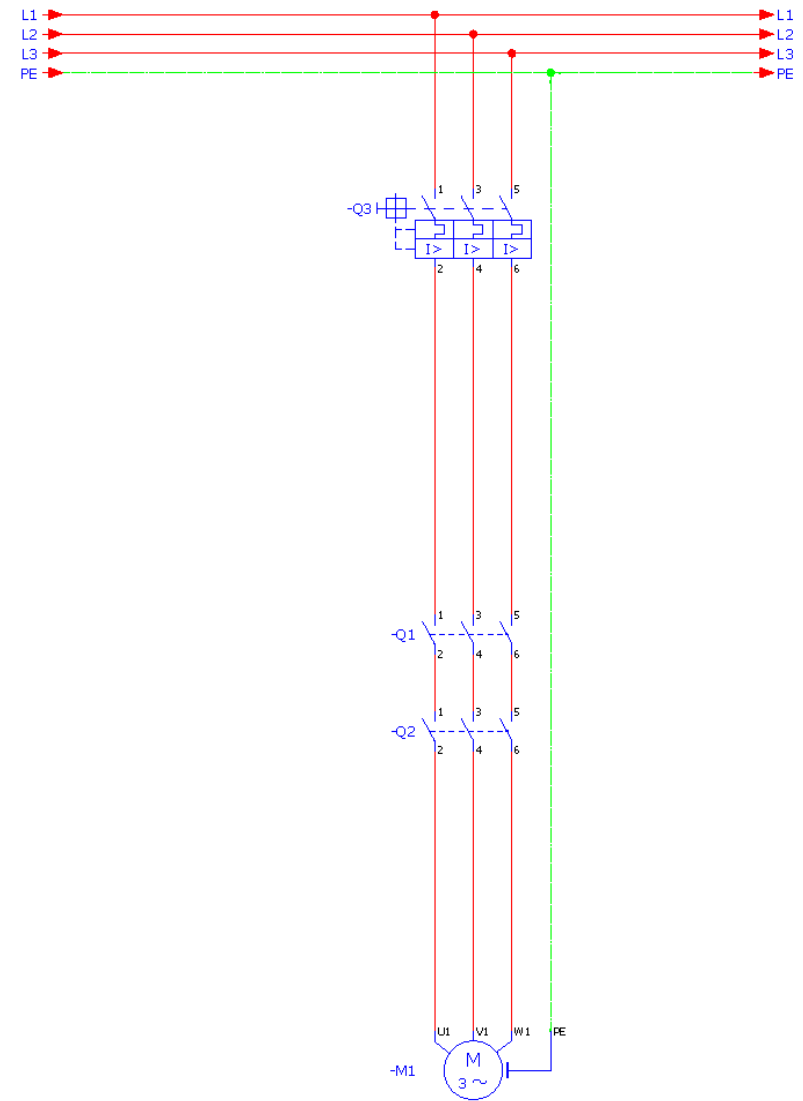
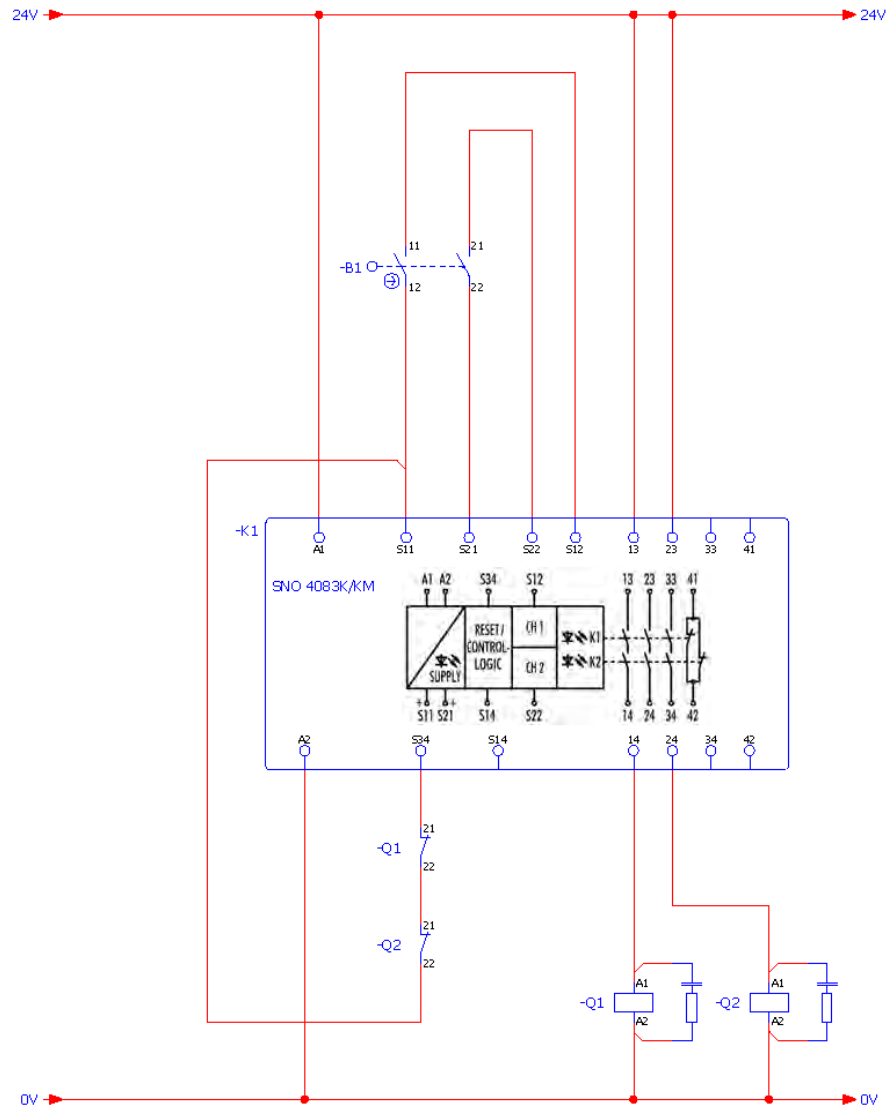
## 3.6.5 Modelling according to EN ISO 13849-1



# Safety functions

Door switch, mechanical – two-channel, equivalent in PL c/d

## 3.6.6 Circuit diagram





### 3.7 Door switch, mechanical – two-channel, antivalent in PL c/d

#### 3.7.1 Safety function

<b>Safety function</b>	By opening the door, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of the door by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.



#### 3.7.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch is operated</li><li>• the input circuit on safety switchgear –K1 is interrupted or closed</li><li>• the safety contacts of –K1 open</li><li>• the positively-driven contactors –Q1 and –Q2 drop out</li><li>• machine 1 is stopped.</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door. The door switch –B1 is closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart function occurs by closing the door. A restart may only be possible if: <ul style="list-style-type: none"><li>• the doors are closed</li><li>• the positively-driven contactors –Q1 and –Q2 have dropped out</li></ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.

### 3.7.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults, cross-circuits and short-circuits against 24VDC in the input circuit are detected by different potentials on the two sensor cables by –K1.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1.</li> </ul> <p>Fault exclusions:</p> <ul style="list-style-type: none"> <li>• Fault exclusion on failure of the actuating element by the machine builder. The installation must generally be carried out according to the installation instructions of the switch manufacturer.</li> <li>• Fault exclusion on the mechanical failure of the switch. The installation must generally be carried out according to the installation instructions of the switch manufacturer.</li> <li>• If the fault exclusions are made, Cat. 4 can be achieved but the PL is limited to PL d.</li> <li>• If these fault exclusions are not possible, Cat. 1 can be achieved as a maximum.</li> </ul>
<b>Actuators</b>	<p>Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</p> <p>The contactors have positively-driven feedback contacts. DC = 99%.</p>

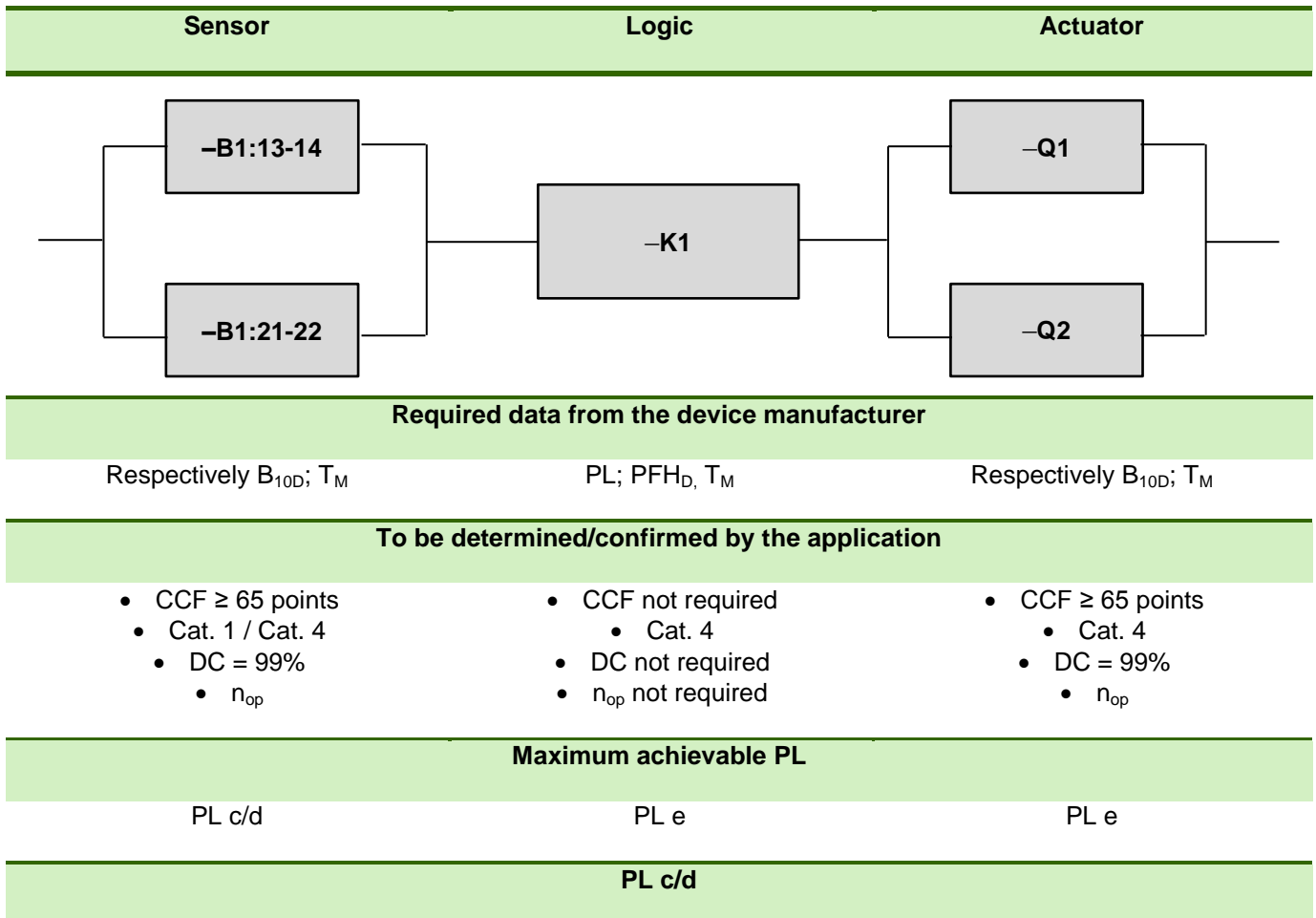
### 3.7.4 Products (options)

<b>Product</b>	
<b>–B1</b> 	Interlocking device type 2 (door switch with separate actuating element) <b>sensor</b> PRO: SMS2x40 Order number: R1.320.2040.0
<b>–K1</b> 	Safety relay <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>–Q1; –Q2</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

# Safety functions

Door switch, mechanical – two-channel, antivalent in PL c/d

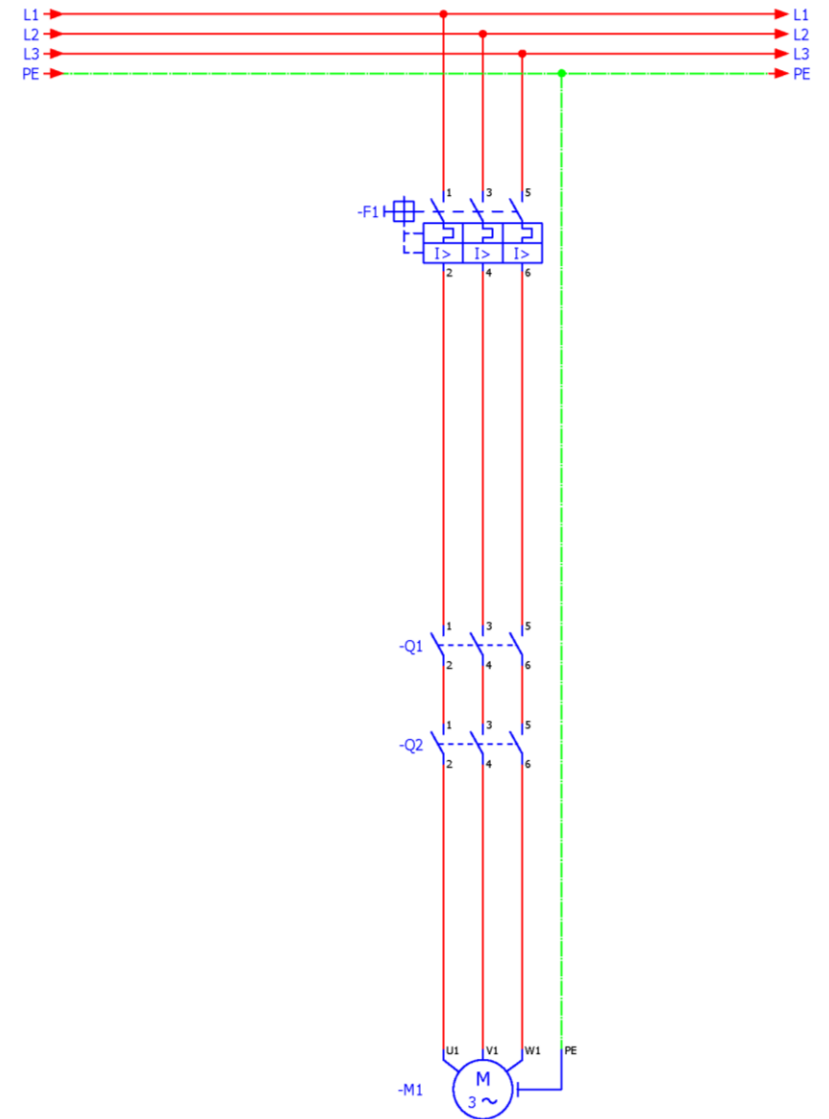
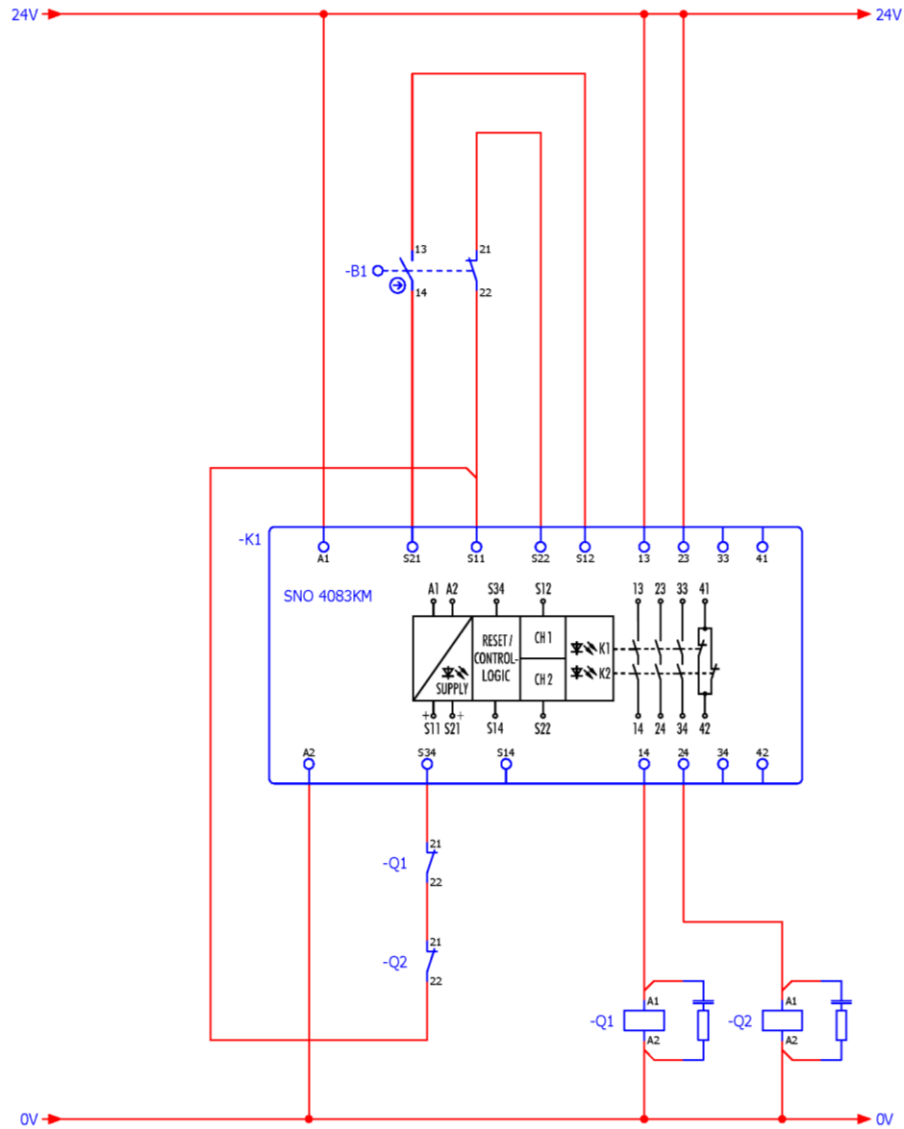
## 3.7.5 Modelling according to EN ISO 13849-1



# Safety functions

Door switch, mechanical – two-channel, antivalent in PL c/d

## 3.7.6 Circuit diagram



### 3.8 Door switch, mech. & magn. – 2x single-channel in PL e

#### 3.8.1 Safety function

<b>Safety function</b>	By opening the door, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of the door by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.




#### 3.8.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch –B1 is operated</li><li>• the door switch –B2 is operated</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the positively-driven contactors –Q1 and –Q2 drop out</li><li>• machine 1 is stopped.</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door. The door switches –B1 and –B2 are closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart function occurs by closing the door. A restart may only be possible if: <ul style="list-style-type: none"><li>• the door is closed</li><li>• the positively-driven contactors –Q1 und –Q2 have dropped out</li></ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.

### 3.8.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults, cross-circuits and short-circuits against 24V in the input circuit are detected through test pulses on the sensor cables by –K1.</li> <li>• A single fault does not lead to a loss of safety due to the diverse redundancy.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li> </ul>
<b>Actuators</b>	<p>Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</p> <p>The contactors have positively-driven feedback contacts. DC = 99%.</p>

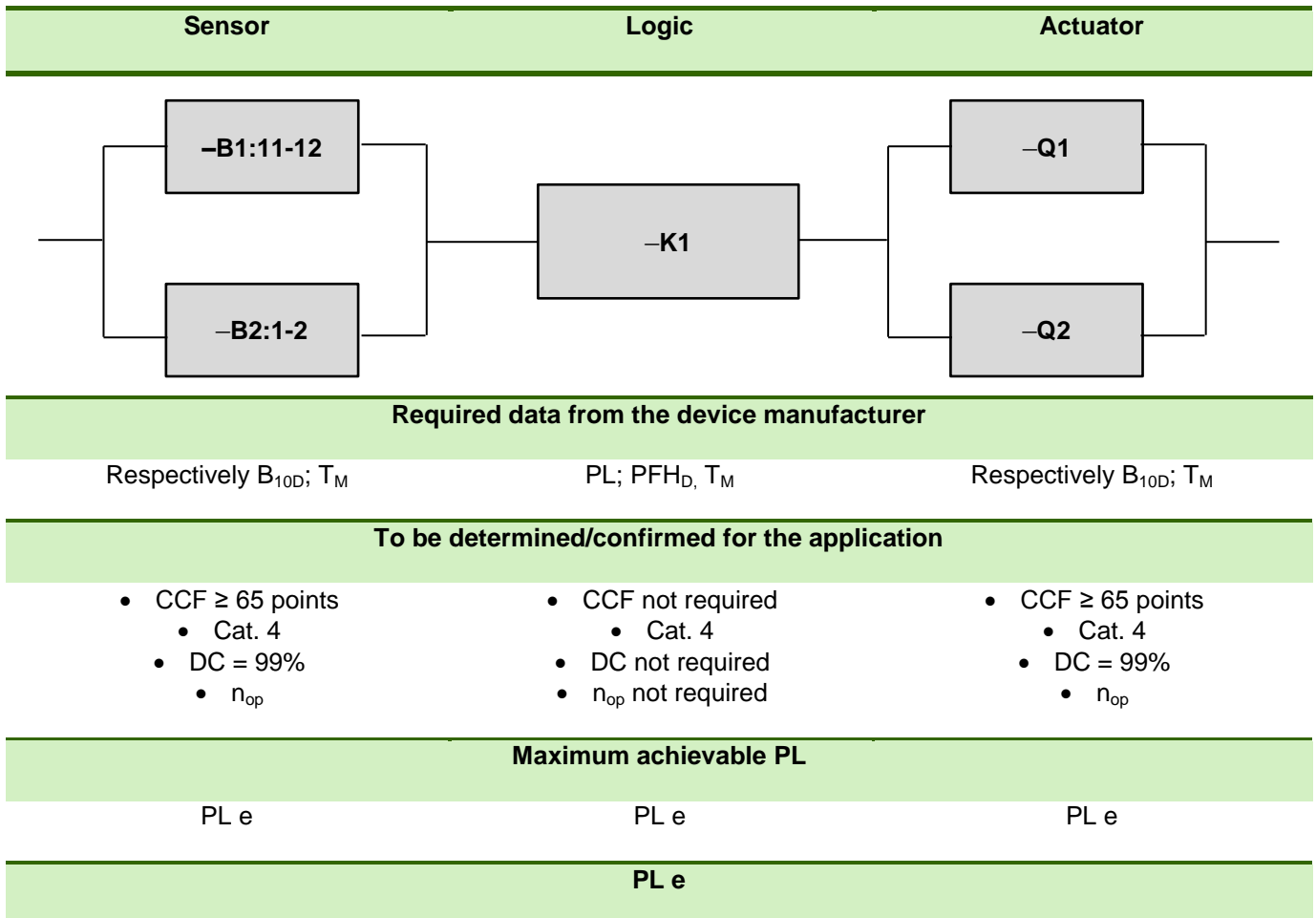
### 3.8.4 Products (options)

<b>Product</b>	
<b>–B1</b> 	<p>Interlocking device 2 (door switch with separate actuating element) and spring actuated guard locking  <b>sensor</b> PRO: SIN11xx                      Order number: R1.310.1150.0</p> <p><b>Note:</b> <i>As this requirement frequently occurs in combination with door guard lockings, a door switch with a spring actuated guard locking is used here. If no guard locking is required, a type without a guard locking can be used e.g. SMS3x10 Order number: R1.320.3010.0.</i></p>
<b>–B2</b> 	<p>Interlocking device type 3 (door switch with magnetic operation)  <b>sensor</b> PRO: SMA01xx                      Order number: R1.100.0113.0</p>
<b>–K1</b> 	<p>Safety relay  <b>safe</b> RELAY: SNO 4063K/KM                      Order number: R1.188.1280.0</p>
<b>–Q1; –Q2</b>	<p>Power contactor with the following characteristics:</p> <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

# Safety functions

Door switch, mech. & magn. – 2x single-channel in PL e

## 3.8.5 Modelling according to EN ISO 13849-1







## 3.9 Door switch, magnetic – two-channel, equivalent in PL e

### 3.9.1 Safety function

<b>Safety function</b>	By opening the door, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of the door by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

### 3.9.2 Description

<b>Function</b>	<p>By opening the door(s):</p> <ul style="list-style-type: none"> <li>• the door switch –B1 is operated</li> <li>• the input circuit on safety switchgear –K1 is interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the positively-driven contactors –Q1 and –Q2 drop out</li> <li>• machine 1 is stopped.</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door. The door switch –B1 is closed. The design ensures that the door cannot close accidentally.
<b>Restart</b>	<p>The restart function occurs by closing the door. A restart may only be possible if:</p> <ul style="list-style-type: none"> <li>• the door is closed</li> <li>• the positively-driven contactors –Q1 and –Q2 have dropped out</li> </ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.

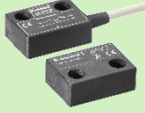

### 3.9.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth circuits, cross-circuits and short-circuits against 24V in the input circuit are detected through test pulses on the sensor cables by –K1.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li> </ul>
<b>Actuators</b>	<p>Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</p> <p>The contactors have positively-driven feedback contacts. DC = 99%.</p>

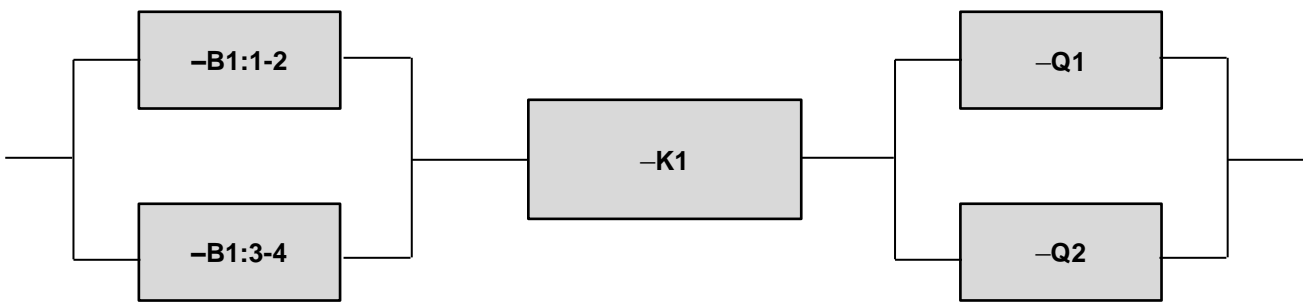
# Safety functions

Door switch, magnetic – two-channel, equivalent in PL e

## 3.9.4 Products (options)

Product	
<b>-B1</b> 	Interlocking device type 3 (door switch with magnetic operation) <b>sensor</b> PRO: SMA01xx Order number: R1.100.0113.0
<b>-K1</b> 	Safety relay <b>safe</b> RELAY: SNA 4043K/KM Order number: R1.188.3250.0
<b>-Q1; -Q2</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

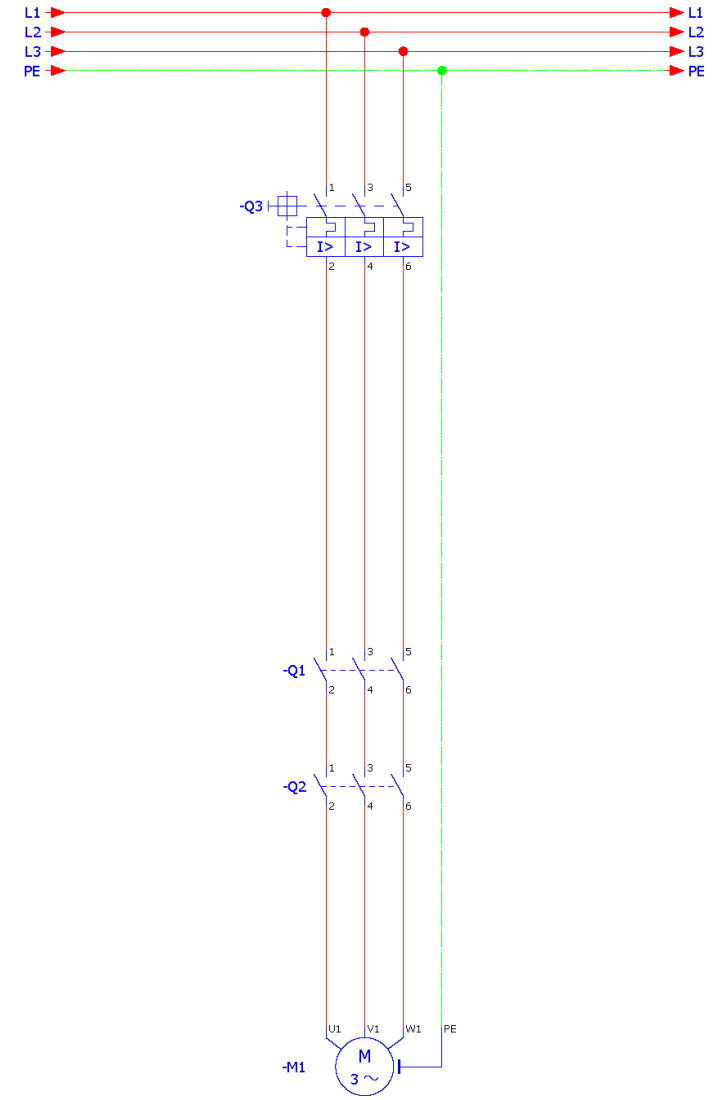
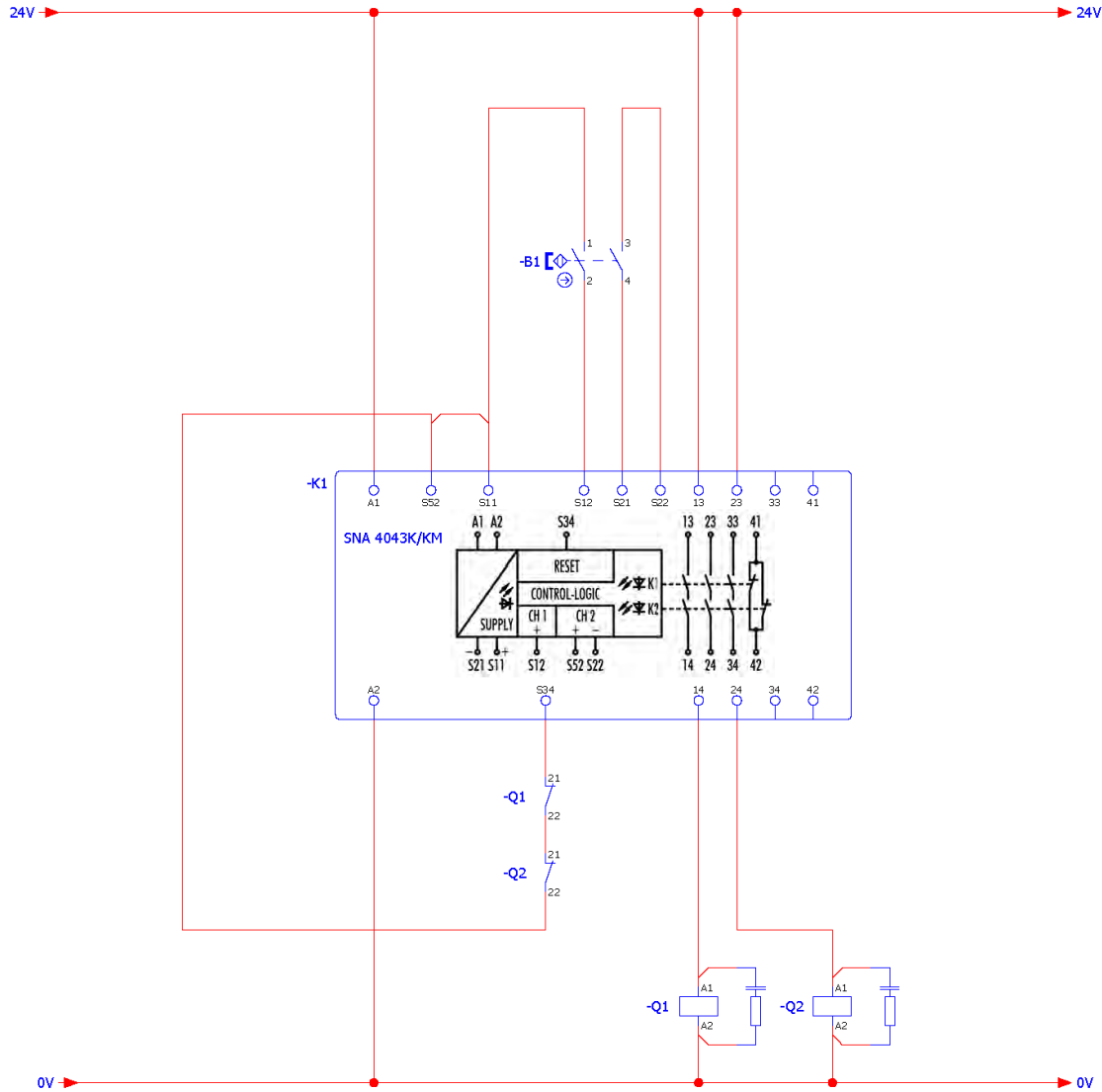
## 3.9.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
		
Required data from the device manufacturer		
Respectively $B_{10D}$ ; $T_M$	PL; $PFH_D$ ; $T_M$	Respectively $B_{10D}$ ; $T_M$
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>• CCF <math>\geq</math> 65 points                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC = 99%                             <ul style="list-style-type: none"> <li>• <math>n_{op}</math></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• <math>n_{op}</math> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF <math>\geq</math> 65 points                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC = 99%                             <ul style="list-style-type: none"> <li>• <math>n_{op}</math></li> </ul> </li> </ul>
Maximum achievable PL		
PL e	PL e	PL e
PL e		

# Safety functions

Door switch, magnetic – two-channel, equivalent in PL e

## 3.9.6 Circuit diagram



### 3.10 Door switch, magnetic – two-channel, antivalent in PL e

#### 3.10.1 Safety function

<b>Safety function</b>	By opening the door, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of the door by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.10.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch –B1 is operated</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the positively-driven contactors –Q1 and –Q2 drop out</li><li>• machine 1 is stopped.</li></ul>
<b>Manual reset</b>	The manual reset of the safety function is carried out by closing the door. The door switch –B1 is closed. The design ensures that the door cannot close accidentally.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"><li>• the door is closed</li><li>• the positively-driven contactors –Q1 and –Q2 have dropped out</li></ul> It is not possible to step behind the doors due to the design.
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.

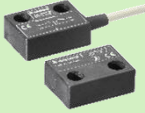

#### 3.10.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"><li>• Earth faults, cross-circuits and short-circuits against 24V in the input circuit are detected through antivalent signals on the sensor cables by –K1.</li><li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” through –K1. DC = 99%.</li></ul>
<b>Actuators</b>	Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.  The contactors has positively-driven feedback contacts. DC = 99%.

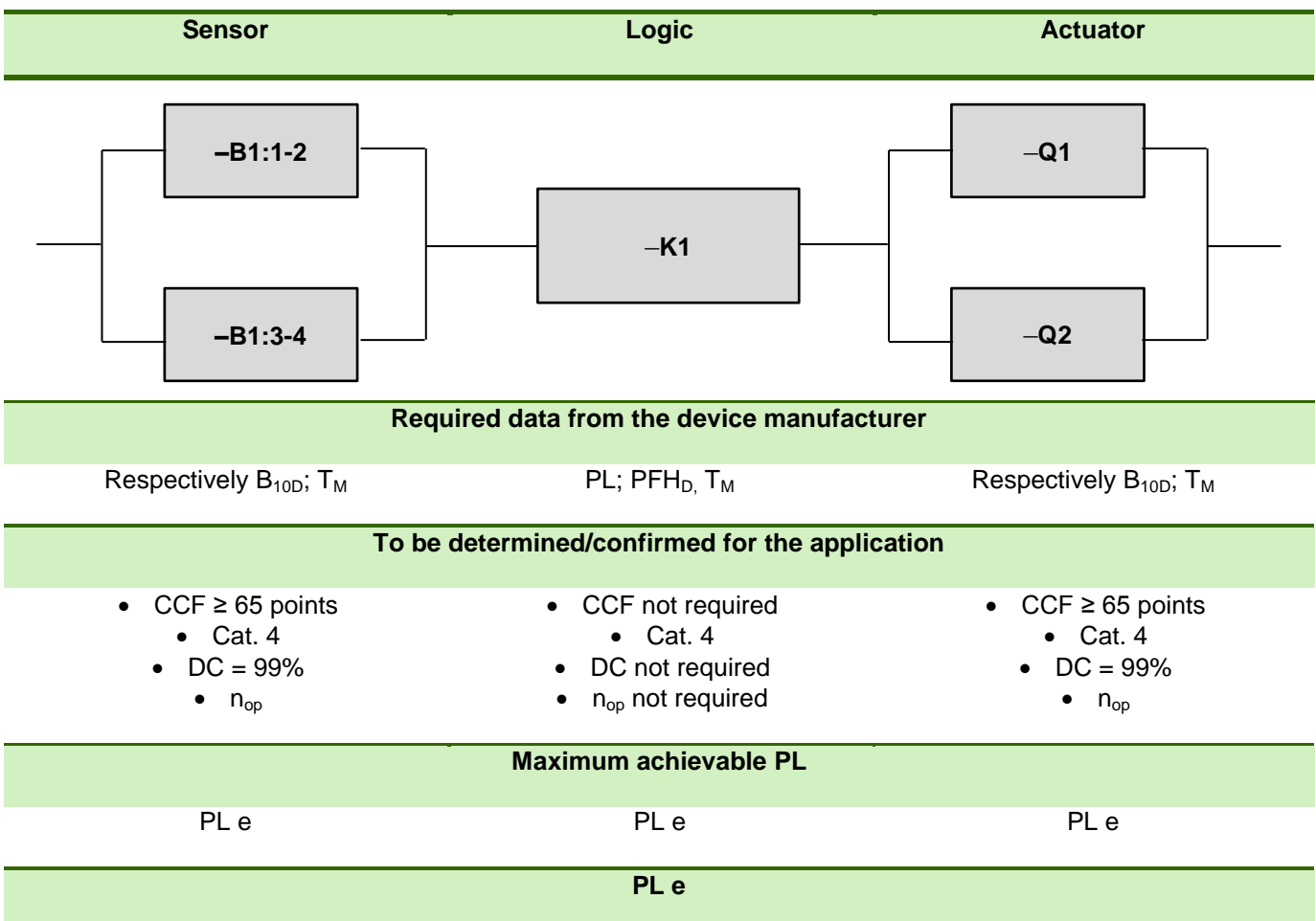
# Safety functions

Door switch, magnetic – two-channel, antivalent in PL e

## 3.10.4 Products (options)

Product	
<b>-B1</b> 	Interlocking device type 3 (door switch with magnetic operation) <b>sensor</b> PRO: SMA01xx Order number: R1.100.0113.0
<b>-K1</b> 	Safety relay <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>-Q1; -Q2</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

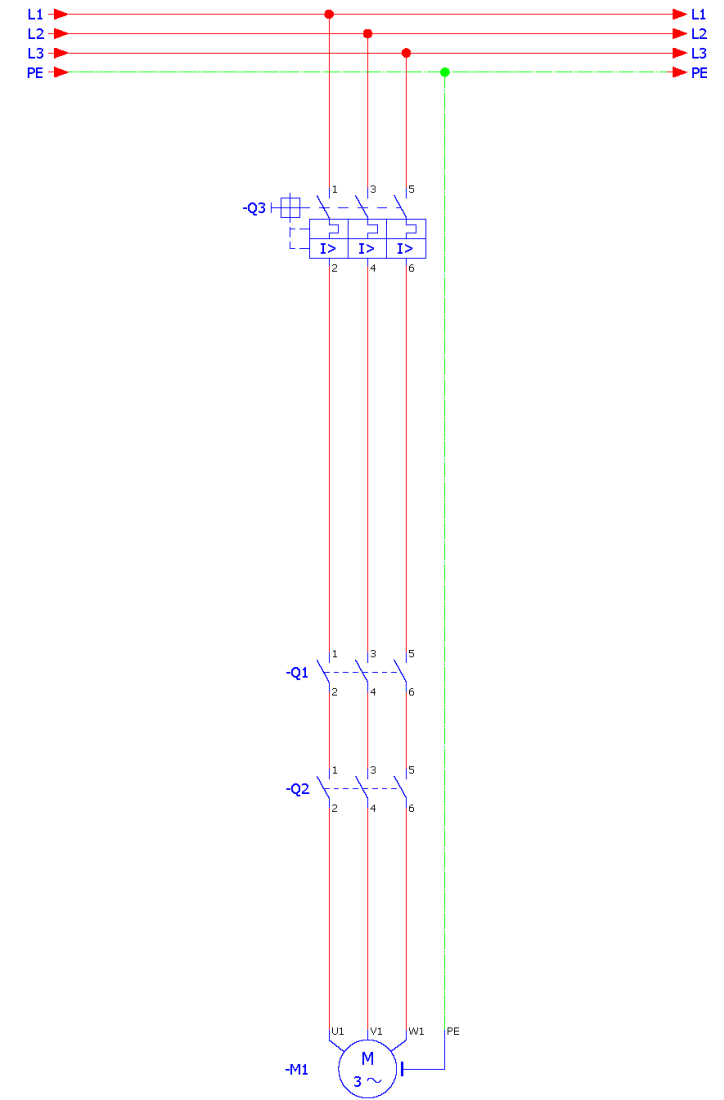
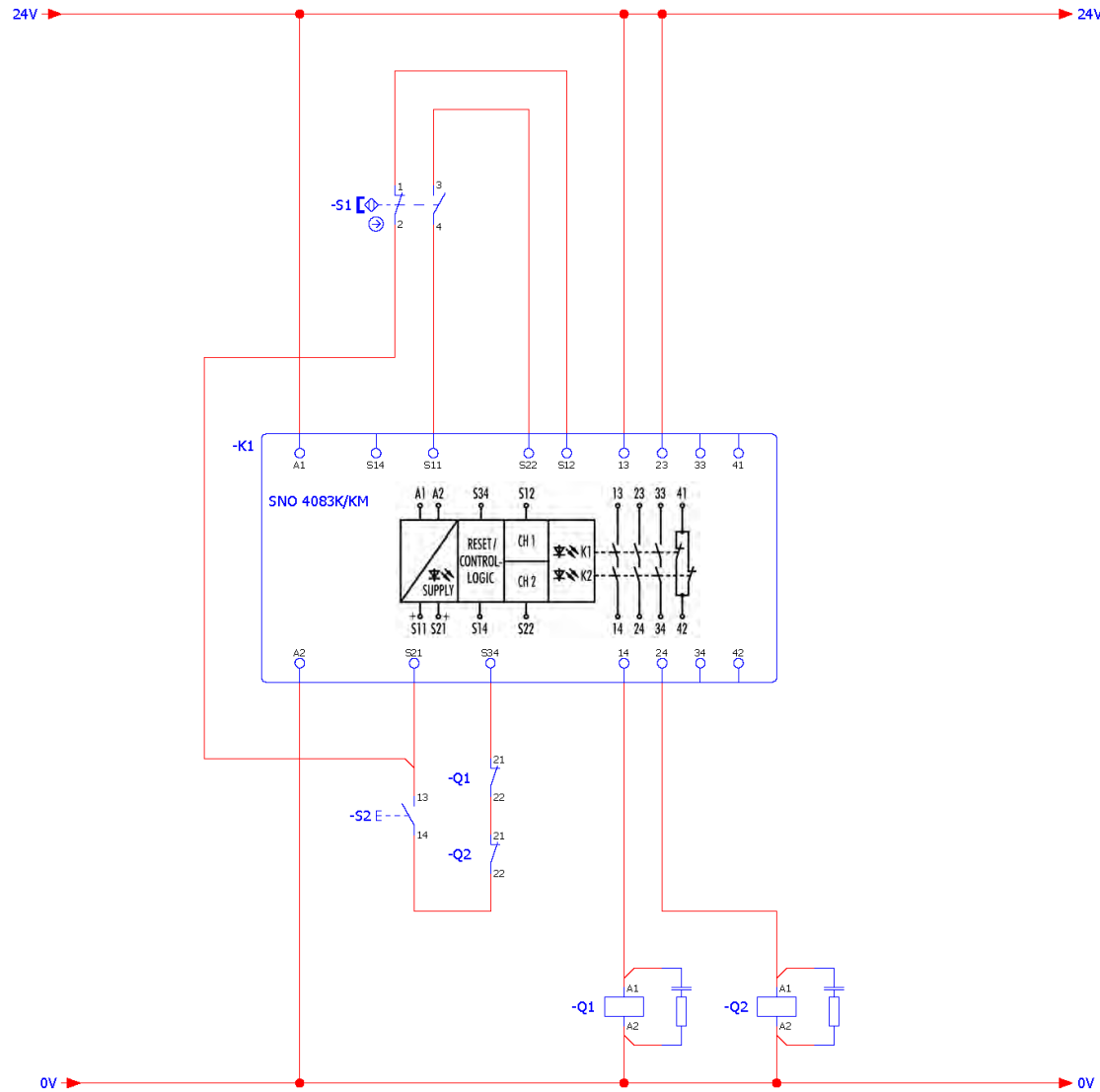
## 3.10.5 Modelling in accordance with EN ISO 13849-1



# Safety functions

Door switch, magnetic – two-channel, antivalent in PL e

## 3.10.6 Circuit diagram



### 3.11 Door switch, magnetic and safety mat – 4-wire version in PL d

#### 3.11.1 Safety function

<b>Safety function</b>	By opening the doors –B1 and stepping on the safety mat –S1, all the drives of the system are de-energised. A reset of the safety function may only be possible if the safety mat –S1 is not activated.
<b>Trigger event</b>	Operator opens the doors –B1 or steps on safety mat –S1.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.



#### 3.11.2 Description

<b>Function</b>	<p>By opening the doors –B1:</p> <ul style="list-style-type: none"> <li>• both channels of –B1 are opened</li> <li>• input circuit –K1:T3-I3 and –K1:T4-I4 is opened</li> <li>• the safety contact –K1:Q1 opens</li> <li>• the positively-driven contactors –Q1 and –Q2 drop out</li> <li>• machine 1 is stopped.</li> </ul> <p>By stepping on the safety mat –S1:</p> <ul style="list-style-type: none"> <li>• both circuits of –S1 are short-circuited</li> <li>• the short-circuit of the input circuit –K1:T1-I1 and –K1:T2-I2 is detected by –K1</li> <li>• the safety contact –K1:Q1 opens</li> <li>• the positively-driven contactors –Q1 and –Q2 drop out</li> <li>• machine 1 is stopped.</li> </ul>
<b>Manual reset</b>	<p>The manual reset of the safety function occurs by closing the doors –B1. Prerequisites are:</p> <ul style="list-style-type: none"> <li>• the hazardous area must be cleared</li> <li>• safety mat –S1 is not activated</li> <li>• the design ensures that the door –B1 cannot close accidentally</li> </ul>
<b>Restart</b>	<p>The restart function occurs by closing the door. A restart is only possible if:</p> <ul style="list-style-type: none"> <li>• the door –B1 is closed</li> <li>• the safety mat –S1 is not activated</li> <li>• the positively-driven contactors –Q1 and –Q2 have dropped out</li> </ul>
<b>Feedback circuit</b>	The positively-driven normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.

### 3.11.3 Safety review

<b>Sensors</b>	<p>Door switch –B1 and safety mat –S1</p> <ul style="list-style-type: none"> <li>• Earth faults, cross-circuits and short-circuits against 24V in the input circuits of –B1 and –S1 are detected through test pulses on the sensor cables by –K1.</li> <li>• –B1: Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li> <li>• –S1: Diagnostics using “Cross comparison with dynamisation without high-performance fault detection” by –K1. DC = 99%.</li> </ul>
<b>Actuators</b>	<p>Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</p> <p>The contactors have positively-driven feedback contacts. DC = 99%.</p>

### 3.11.4 Products (options)

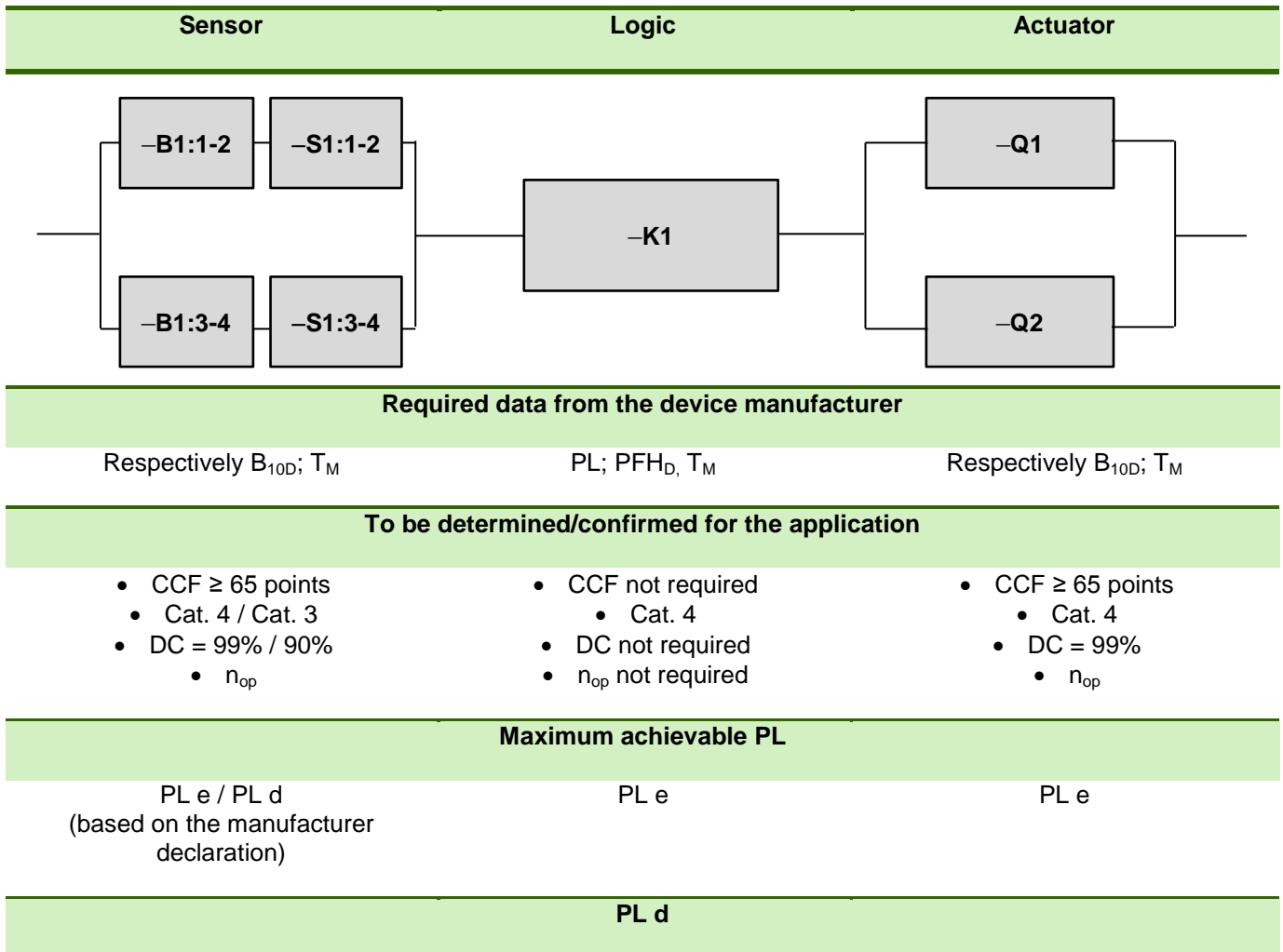
	<b>Product</b>
<b>–B1</b> 	<p>Interlocking device type 3 (door switch with magnetic operation)  <b>samos</b> PRO: SMA01xx                      Order number: R1.100.0113.0</p>
<b>–S1</b>	<p>Short-circuit forming safety mat with the following requirements:</p> <ul style="list-style-type: none"> <li>• must be sufficient for the expected loads</li> <li>• number of electric switching cycles must meet the expected frequency of use</li> <li>• manufacturer specification of <math>B_{10D}</math> und <math>T_M</math> as well as the achievable category</li> </ul> <p>Usually the use of these types of safety mats are limited to PL d, Cat. 3 by the manufacturer.</p>
<b>–K1</b> 	<p>Programmable safety controller  <b>samos</b> PRO: SP-COP2                      Order number: R1.190.1310.0</p>
<b>–Q1; –Q2</b>	<p>Power contactor with the following characteristics:</p> <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>



# Safety functions

Door switch, magnetic and safety mat – 4-wire version in PL d

## 3.11.5 Modelling according to EN ISO 13849-1





### 3.12 Bumper, single-channel – positively-driven in PL d

#### 3.12.1 Safety function

<b>Safety function</b>	By activating the bumper –B4 (switching strip), the pneumatic drive –M1 of the system is stopped.
<b>Trigger event</b>	Activation of the bumper –B4 by the operator.
<b>Reaction</b>	De-energising of the pneumatic drive –M1.
<b>Safe state</b>	The drive –M1 is depressurised and de-energised.  <b>Note:</b> <i>It is assumed that the depressurised state of the cylinder is the safe state. In the case of a vertical installation, the pressurised state of –M1 is frequently the safe state as only then an independent movement may be excluded. The pneumatic diagram must be adapted accordingly.</i>

#### 3.12.2 Description

<b>Function</b>	By activating the bumper –B4: <ul style="list-style-type: none"> <li>the input circuit on the safety switchgear –K1 is interrupted</li> <li>the safety contacts of –K1 open</li> <li>the magnets –Q2:14 and Q2:12 are de-energised</li> <li>the valve –Q2 goes into the central position and depressurises –M1</li> <li>the drive –M1 is stopped</li> <li>the valve –Q1 is de-energised in the event of a fault (detectable via –B2 and –B3). Valves –Q3 and –Q4 are likewise de-energised and –M1 is depressurised via –Q3 and –Q4</li> <li>the valves –Q1, –Q3 and –Q4 do not switch in the operating state or only rarely as an entire group of valves is switched via –Q1 in most cases</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by activating the bumper –B4.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"> <li>Bumper –B4 is not activated</li> </ul>
<b>Feedback circuit</b>	<ul style="list-style-type: none"> <li>The position switch –B1 on –Q1 is used for directly reading back the valve position.</li> <li>The position switches –B2 and –B3 are monitored in the process sequence of –K1. The specification of the process status occurs via additional inputs on –K1.</li> </ul>

### 3.12.3 Safety review

#### Sensors

- Earth faults and short-circuits against 24VDC in the input circuit are detected through test pulses on the sensor cables by –K1.
- The sensor is positively opened, classified and certified by the manufacturer as Cat. 3.
- The evaluation of the signal is carried out via an input on –K1 which has at least Cat. 3.
- The manufacturer's specifications regarding the bumper must be taken into account. In general the protected installation of the cable is required.
- DC = 90%

#### Actuators

Diagnosis of –Q1 via –B1

- Direct monitoring → DC = 99%

Diagnosis of –Q2 via –B2 and –B3

- Indirect monitoring at the end of the path from –M1 → DC = 90%

Diagnosis of –Q3 and –Q4 via –B2 and –B3

- only indirect and at the end of the path from –M1
- only possible at certain times
- e.g. switching on the machine or shift change


Possible test procedure:

- move –M1 to left limit position
- disable –Q3 and –Q4
- –Q2 in position: Right direction
- –M1 may not leave the limit position. Detection by –B2 or –B3
- Test other limit position accordingly
- If it is detected during the test that –M1 has left the limit position, then end the movement via –Q2
- If tested at least 1x per month: DC = 90%  
(compare with CNB/M/11.050/R/E rev.05 from 18.10.2011)

# Safety functions

## Bumper, single-channel – positively-driven in PL d

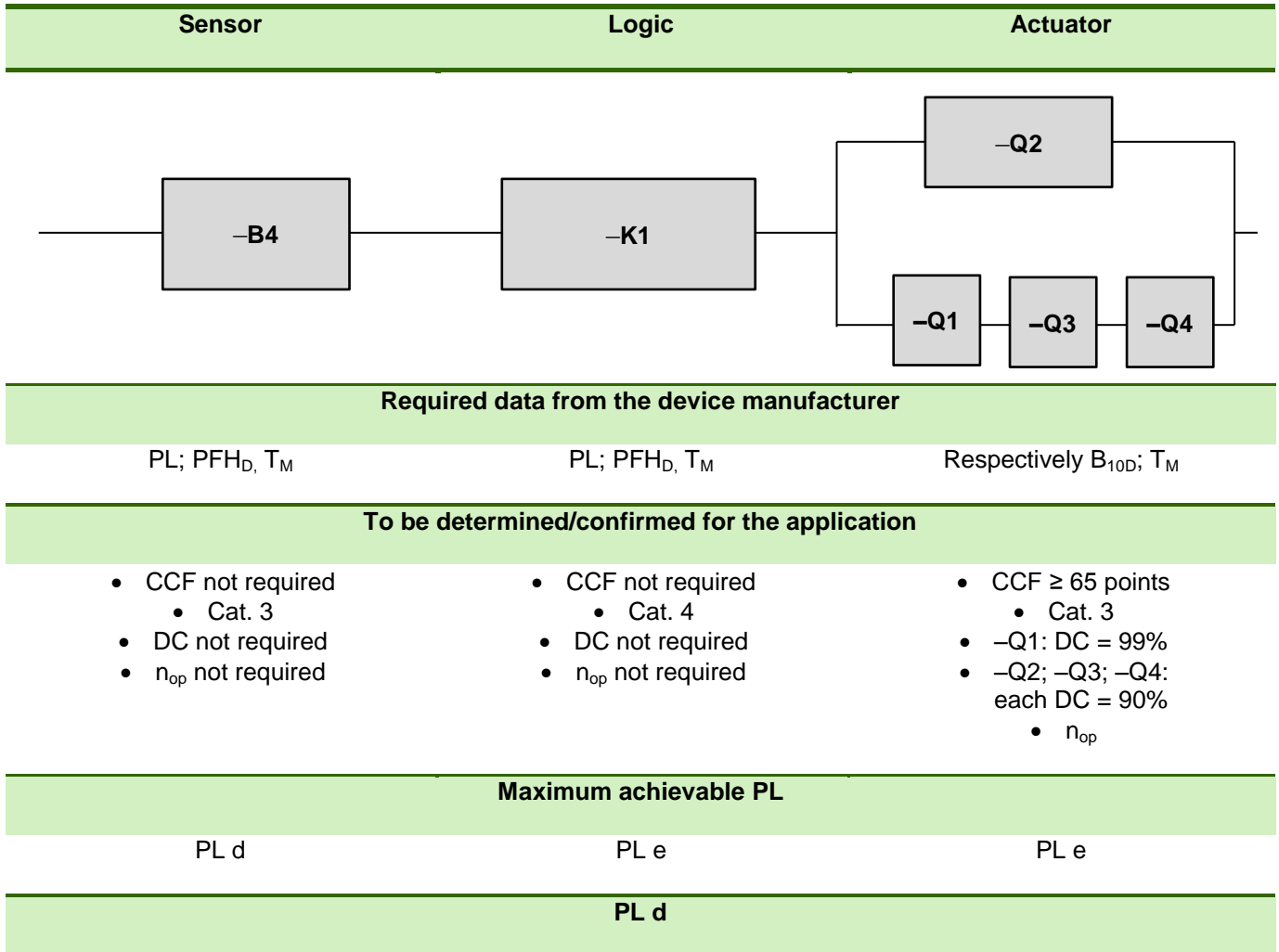
### 3.12.4 Products (options)

	Product
-B4	Bumper with positively-driven contact and Cat. 3 / PL d defined by the manufacturer
-K1 	Programmable safety controller <b>samos</b> PRO: SP-COP2 Order number: R1.190.1310.0
-Q1	2/3-way valve with the following characteristics: <ul style="list-style-type: none"><li>• Electrically pilot-controlled</li><li>• Neutral position for venting</li><li>• Reset mechanically using well-trying spring</li><li>• Suitable for the expected application</li><li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li></ul>
-Q2	5/3-way valve with the following characteristics: <ul style="list-style-type: none"><li>• Electrically pilot-controlled</li><li>• Neutral position for venting</li><li>• Reset mechanically using well-trying spring</li><li>• Suitable for the expected application</li><li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li></ul>
-Q3, -Q4	Pneumatic 2/3-way valve with the following characteristics: <ul style="list-style-type: none"><li>• Pneumatically controlled</li><li>• Neutral position for venting</li><li>• Reset mechanically using well-trying spring</li><li>• Suitable for the expected application</li><li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li></ul>
-B1 to -B3	Position switch with the following characteristics: <ul style="list-style-type: none"><li>• Switch contact in the open position in the inactive position of the valve/cylinder</li></ul>

# Safety functions

Bumper, single-channel – positively-driven in PL d

## 3.12.5 Modelling according to EN ISO 13849-1



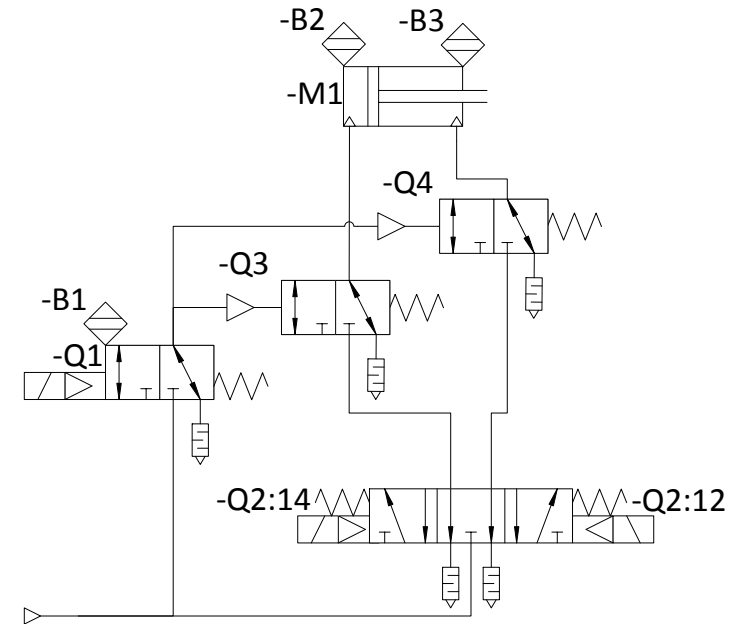
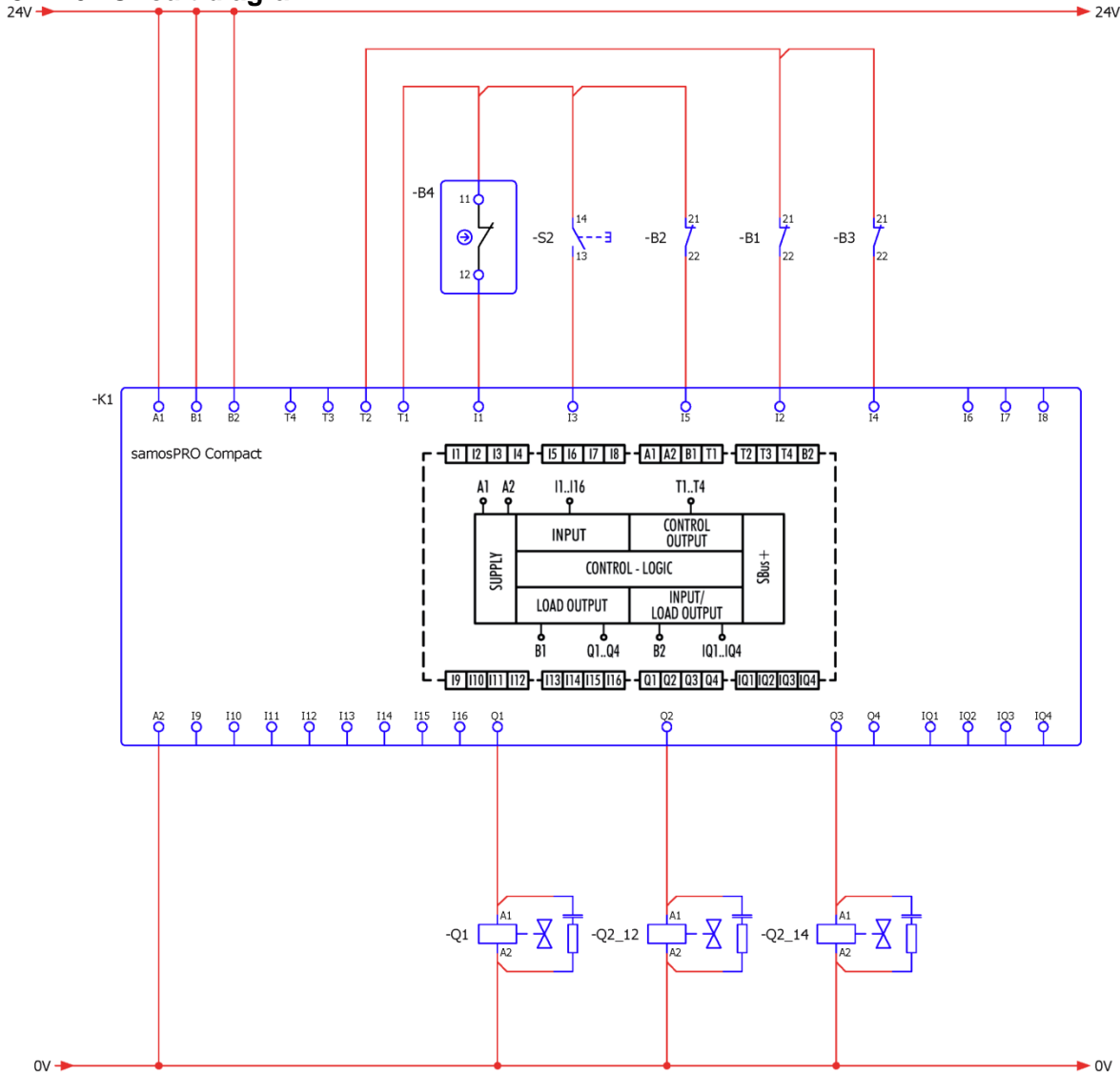
**Note 1:** n<sub>op</sub> will have a different value in many cases for each of the elements as the valves sometimes do not switch after each operation of the bumper and sometimes switch more often than the bumper.

**Note 2:** The reading back of –B1 to –B3 can alternatively also be carried out via a standard controller. The diagnosis is however part of the program of the standard controller and must be taken into account when determining the CCF. The standard controller is not included mathematically in the determination of the PL and PFH<sub>D</sub>. The diagnosis result must be communicated to –K1. Finally, the program of the standard controller must also be validated from a safety perspective. It should be noted that validation is required after any change which is made to the program of the standard controller.

# Safety functions

Bumper, single-channel – positively-driven in PL d

## 3.12.6 Circuit diagram



### 3.13 Two-hand control, type III A in PL c

#### 3.13.1 Safety function

<b>Safety function</b>	By removing your hands from one or both buttons –S1 / –S2 of the two-hand control device, the drive –T1 is stopped.
<b>Trigger event</b>	Removal of one or two hands from the two-hand control device –S1 / –S2 by the operator.
<b>Reaction</b>	De-energising of drive M1.
<b>Safe state</b>	Drive M1 is de-energised.

#### 3.13.2 Description

<b>Function</b>	By removing your hands from buttons –S1 and –S2: <ul style="list-style-type: none"><li>• the input circuit –K1:T11–T12 on the safety switchgear –K1 is closed</li><li>• the input circuit –K1:T11–T13 on the safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1:11-14 open</li><li>• the STO safety function is requested at the frequency converter –T1</li><li>• machine M1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by pressing buttons –S1 and –S2 after both have previously not been pressed and the switches have the associated switch positions.
<b>Restart</b>	The restart function occurs automatically with the manual reset function. <b>Note: The restart function can depend on other states.</b>
<b>Feedback circuit</b>	Not required here as T1 is a device with integrated diagnostics.

#### 3.13.3 Safety review

<b>Sensors</b>	A single fault can lead to the loss of safety.
<b>Actuators</b>	Frequency converter with integrated diagnostics and evaluation as PL d.


**Note:** *If switches with normally closed and normally open contacts are used for –S1 and –S2, only the normally open contact of one button and the normally closed contact of the other button should be used. If the contacts of one switch are interconnected in series or parallel with those of another switch, then fault masking is unavoidable. An initial fault would then not be revealed in any case.*



# Safety functions

Two-hand control, type III A in PL c

## 3.13.4 Products (options)

	Product
-S1	Button with normally closed (NC) contacts. Required characteristic data: <ul style="list-style-type: none"> <li>Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>
-S2	Button with normally open (NO) contacts. Required characteristic data: <ul style="list-style-type: none"> <li>Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>
-K1	 Safety switchgear <b>safe</b> RELAY: SNZ 1022K Order number: R1.188.3700.0
-T1	Frequency converter with integrated diagnostics and evaluation as PL d. Integrated STO safety function.

## 3.13.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------

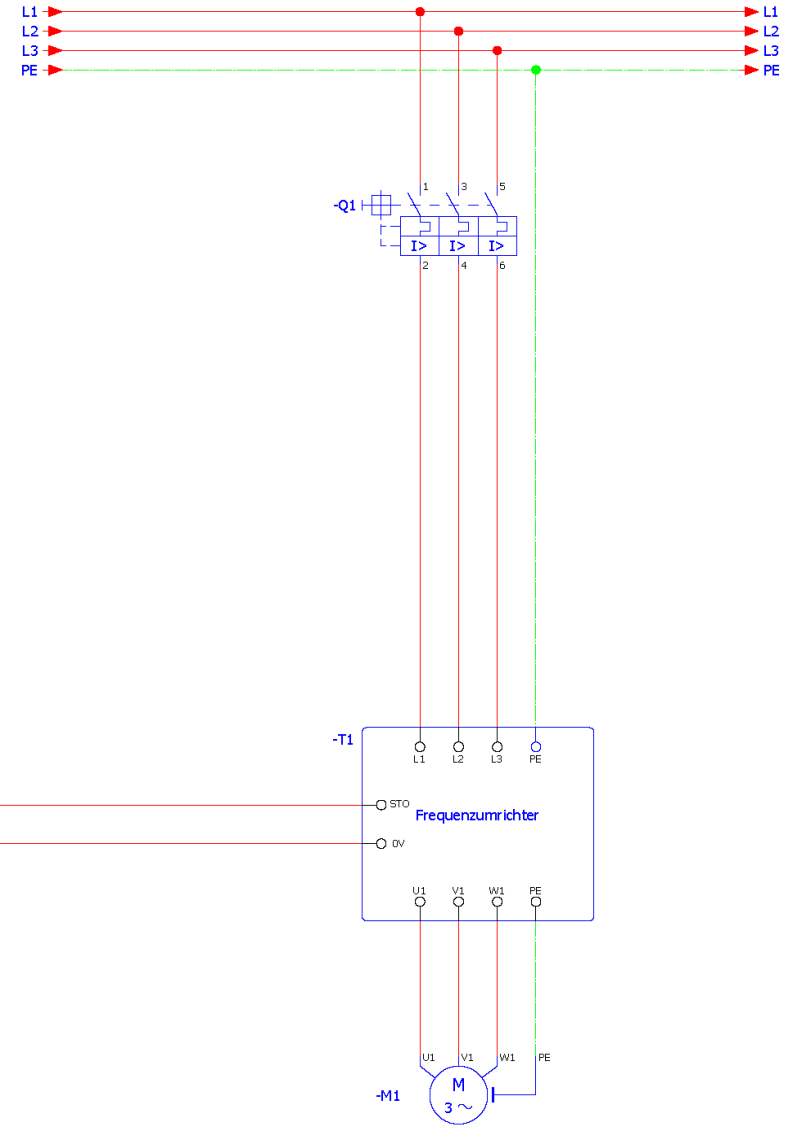
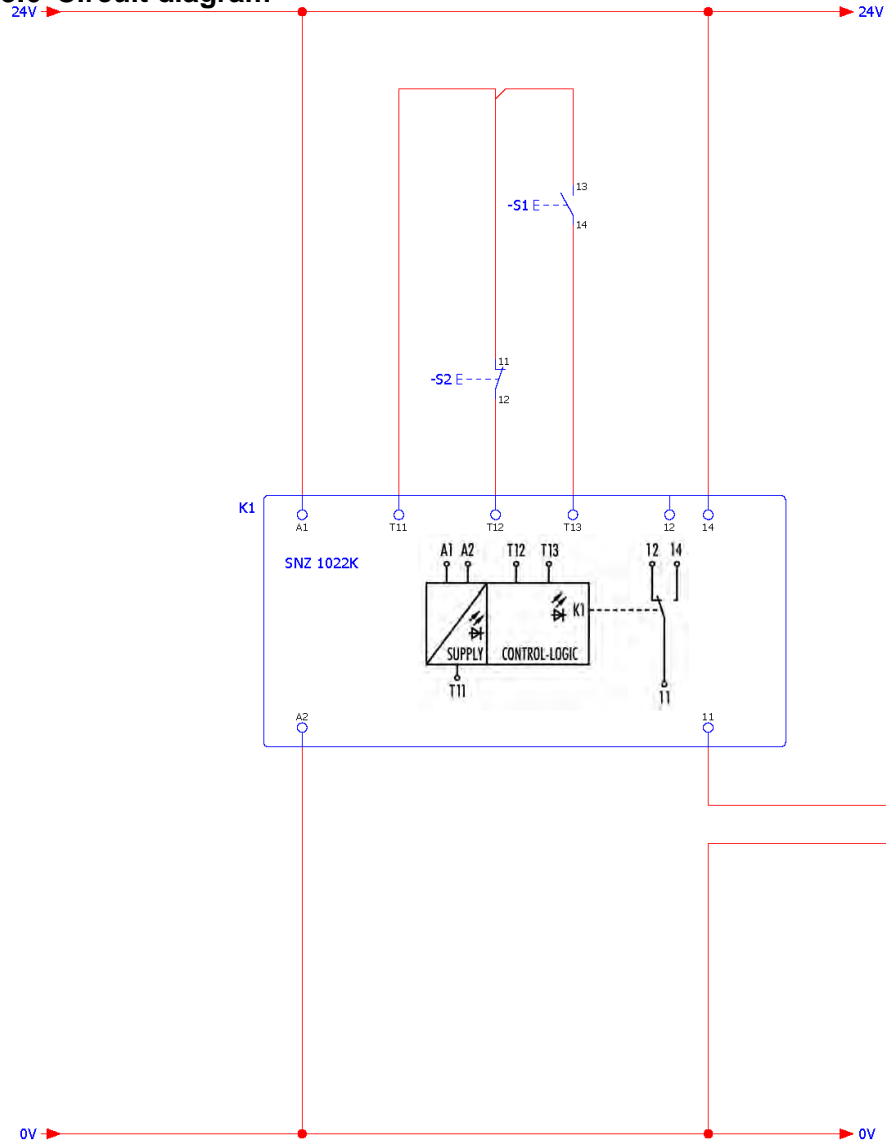


Required data from the device manufacturer		
Respectively $B_{10D}$ ; $T_M$	PL; PFH <sub>D</sub> , $T_M$	PL; PFH <sub>D</sub> , $T_M$
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>CCF not required               <ul style="list-style-type: none"> <li>Cat. 1</li> </ul> </li> <li>DC not required               <ul style="list-style-type: none"> <li><math>n_{op}</math></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>CCF not required               <ul style="list-style-type: none"> <li>Cat. 1</li> </ul> </li> <li>DC not required</li> <li><math>n_{op}</math> not required</li> </ul>	<ul style="list-style-type: none"> <li>CCF not required               <ul style="list-style-type: none"> <li>Cat. 3</li> </ul> </li> <li>DC not required</li> <li><math>n_{op}</math> not required</li> </ul>
Maximum achievable PL		
PL c	PL c	PL d
PL c		

# Safety functions

Two-hand control, type III A in PL c

## 3.13.6 Circuit diagram



### 3.14 Two-hand control, type III C in PL e

#### 3.14.1 Safety function

<b>Safety function</b>	By removing your hands from one or both buttons –S1 / –S2 of the two-hand control device, the drives are stopped. The safe state is achieved if all the drives are de-energised.
<b>Trigger event</b>	Removal of one or both hands from the two-hand control device –S1 / –S2 by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drive is de-energised.

#### 3.14.2 Description

<b>Function</b>	<ul style="list-style-type: none"> <li>• By removing a hand from button –S1: <ul style="list-style-type: none"> <li>• the input circuit –K1:Y11–Y12 on safety switchgear –K1 is closed</li> <li>• the input circuit –K1:Y11–Y14 on safety switchgear –K1 is opened</li> </ul> </li> <li>• By removing a hand from button –S2: <ul style="list-style-type: none"> <li>• the input circuit –K1:Y21–Y22 on safety switchgear –K1 is closed</li> <li>• the input circuit –K1:Y21–Y24 on safety switchgear –K1 is opened</li> <li>• the safety contacts of –K1:11-14 open</li> <li>• the contactors –Q1 and Q2 drop out</li> <li>• the drives are de-energised</li> </ul> </li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by pressing buttons –S1 and –S2 after both have previously not been pressed and the switches have the associated switch positions. The operation must be carried out synchronously.
<b>Restart</b>	The restart function occurs automatically with the manual reset function.  <b>Note: The restart function can depend on other states.</b>
<b>Feedback circuit</b>	The positively-driven normally closed (NC) contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of the safety switchgear –K1.


#### 3.14.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Due to the diversity and redundancy of the switches, each individual fault is detected for each switch.</li> <li>• The switches –S1 and –S2 must be monitored for synchronisation.</li> <li>• Pressing only one of the switches must lead to the safe state. This is ensured by –K1.</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</li> <li>• The contactors have positively-driven feedback contacts. DC = 99%.</li> </ul>

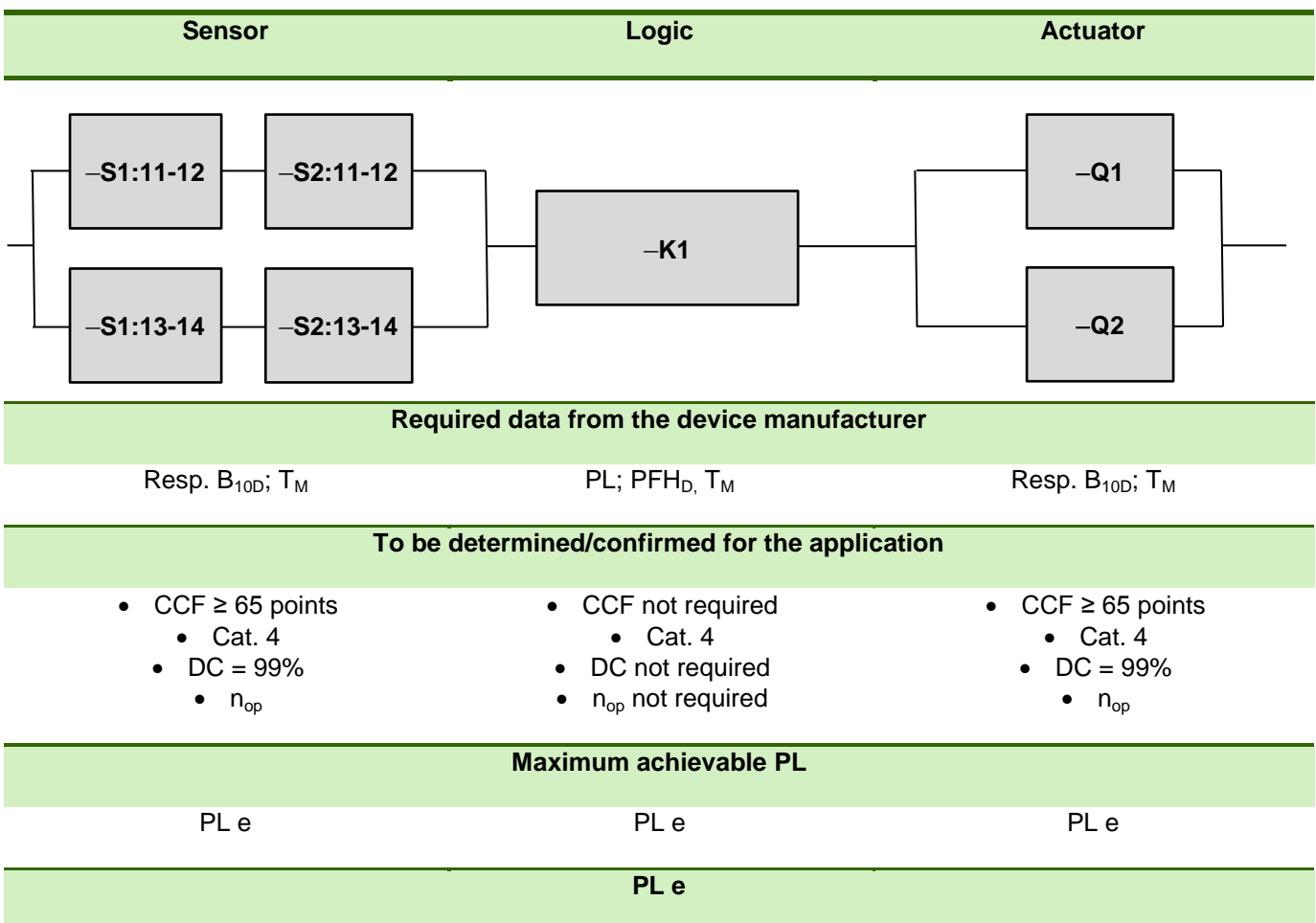
# Safety functions

Two-hand control, type III C in PL e

## 3.14.4 Products (options)

	Product
-S1; -S2	Buttons with normally closed (NC) and normally open (NO) contacts. Necessary characteristic data: <ul style="list-style-type: none"> <li>Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>
-K1	 Safety switchgear <b>safe RELAY: SNZ 4052K</b> Order number: R1.188.0530.1
-Q1; -Q2	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>Contactor with positively-driven feedback contacts</li> <li>Suitable for the expected switching load and frequency</li> <li>Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

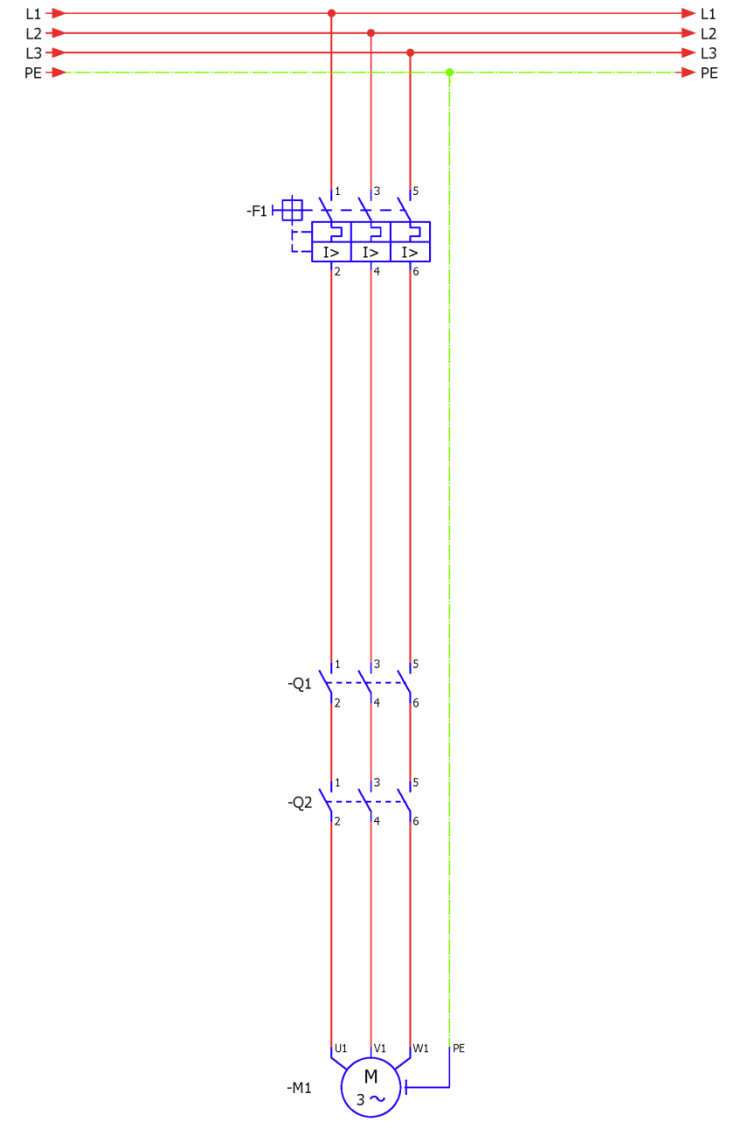
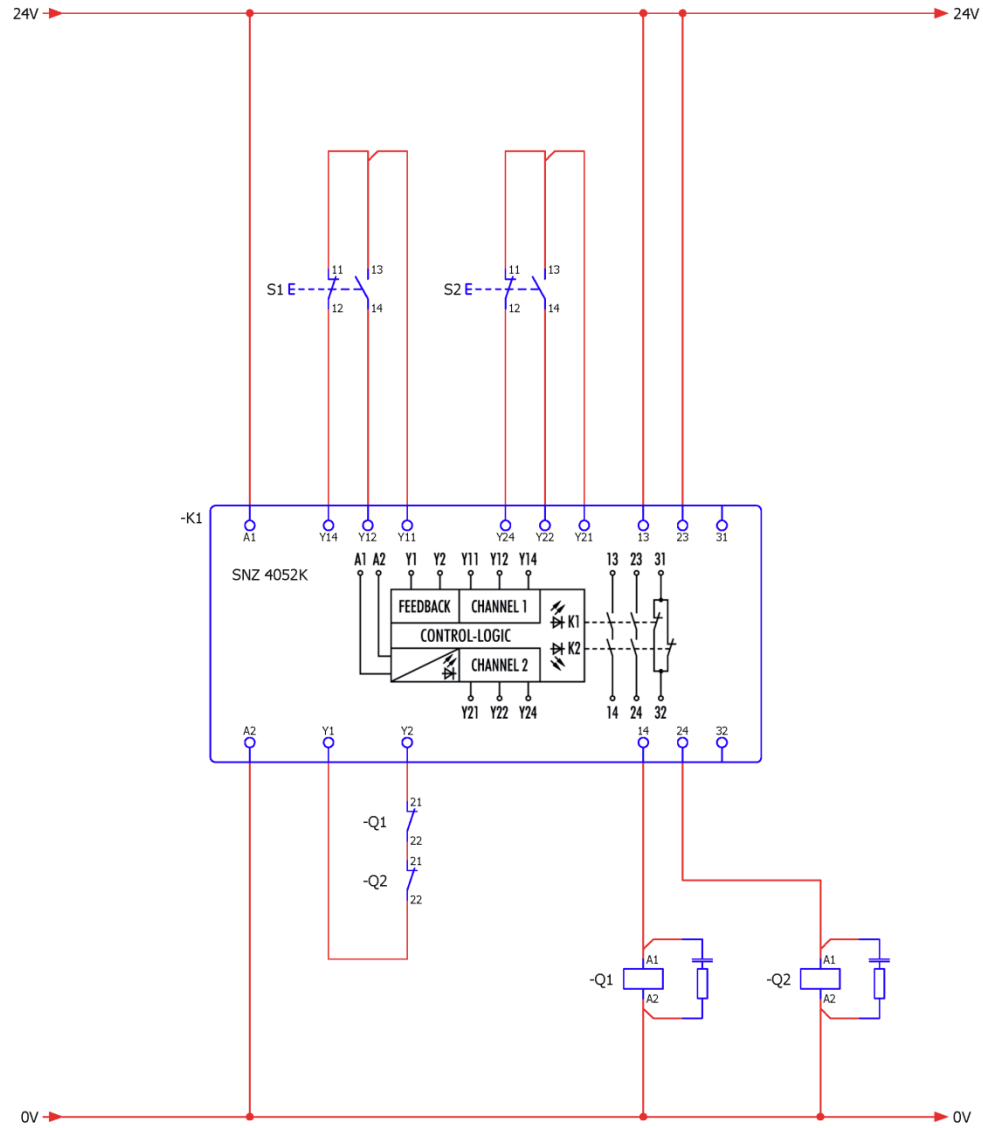
## 3.14.5 Modelling in accordance with EN ISO 13849-1



# Safety functions

Two-hand control, type III C in PL e

## 3.14.6 Circuit diagram



## 3.15 Light curtain/grid, type 2 in PL c

### 3.15.1 Safety function

<b>Safety function</b>	By interrupting the light curtain/grid –B1, all the drives of the system are stopped. The safe state is achieved when all the drives are de-energised.
<b>Trigger event</b>	Interruption of the light curtain/grid –B1 by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

### 3.15.2 Description

<b>Function</b>	By interrupting the light curtain/grid –B1: <ul style="list-style-type: none"> <li>• the OSSD signals are switched off</li> <li>• the two input circuits on safety switchgear –K1 are interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the frequency converter –T1 with STO safety input is de-energised</li> <li>• machine 1 is stopped</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs if the interruption from the light curtain/grid is removed. The design ensures that it is not possible to step behind the light curtain/grid.
<b>Restart</b>	The restart function occurs either by pressing –S2 or by removing the interruption from the light curtain/grid –B1. A restart may only be possible if: <ul style="list-style-type: none"> <li>• light curtain/grid –B1 is not interrupted</li> </ul>
<b>Feedback circuit</b>	Not required here, as –T1 is a device with integrated diagnostics.

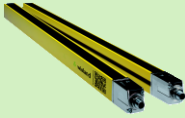

### 3.15.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Monitoring of synchronous time between the input circuits –S12; –S22 by –K.</li> <li>• All faults in the wiring from –B1 to –K1 are detected through using OSSD testing by –B1 as well as synchronous time monitoring by –K1. “Cross comparison with dynamisation and high-performance fault detection” → DC = 99 %.</li> <li>• Protected installation of the cable is not required.</li> <li>• Required for the selection and positioning of the light curtain/grid.</li> <li>• The system reaction time from the interruption of the light curtain/grid until the stoppage of the drives must be determined.</li> <li>• The required design (position, interval, alignment, resolution and length) of the light curtain/grid must be determined. See EN ISO 13855.</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Frequency converter with integrated diagnostics and evaluation as PL d.</li> <li>• Fault exclusion on the wiring from –K1 to –T1 as in the switch cabinet.</li> </ul>

# Safety functions

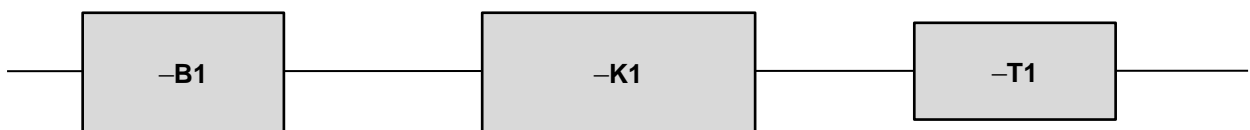
## Light curtain/grid, type 2 in PL c

### 3.15.4 Products (options)

	Product
<b>-B1</b> 	Type 2 safety light grid or curtain <b>sensor</b> PRO: SLC-2xx Order number: R1.512.1800.0 + R1.532.1800.0  <i>Note: With the required data regarding reaction time, resolution and length.</i>
<b>-K1</b> 	Safety switchgear <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>-T1</b>	Frequency converter with integrated diagnostics and evaluation as PL d. Integrated STO safety function.

### 3.15.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------



Required data from the device manufacturer		
PL; PFH <sub>D</sub> , T <sub>M</sub>	PL; PFH <sub>D</sub> , T <sub>M</sub>	PL; PFH <sub>D</sub> , T <sub>M</sub>

To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>CCF not required                             <ul style="list-style-type: none"> <li>Cat. 2</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>CCF not required                             <ul style="list-style-type: none"> <li>Cat. 4</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>CCF not required                             <ul style="list-style-type: none"> <li>Cat. 3</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>

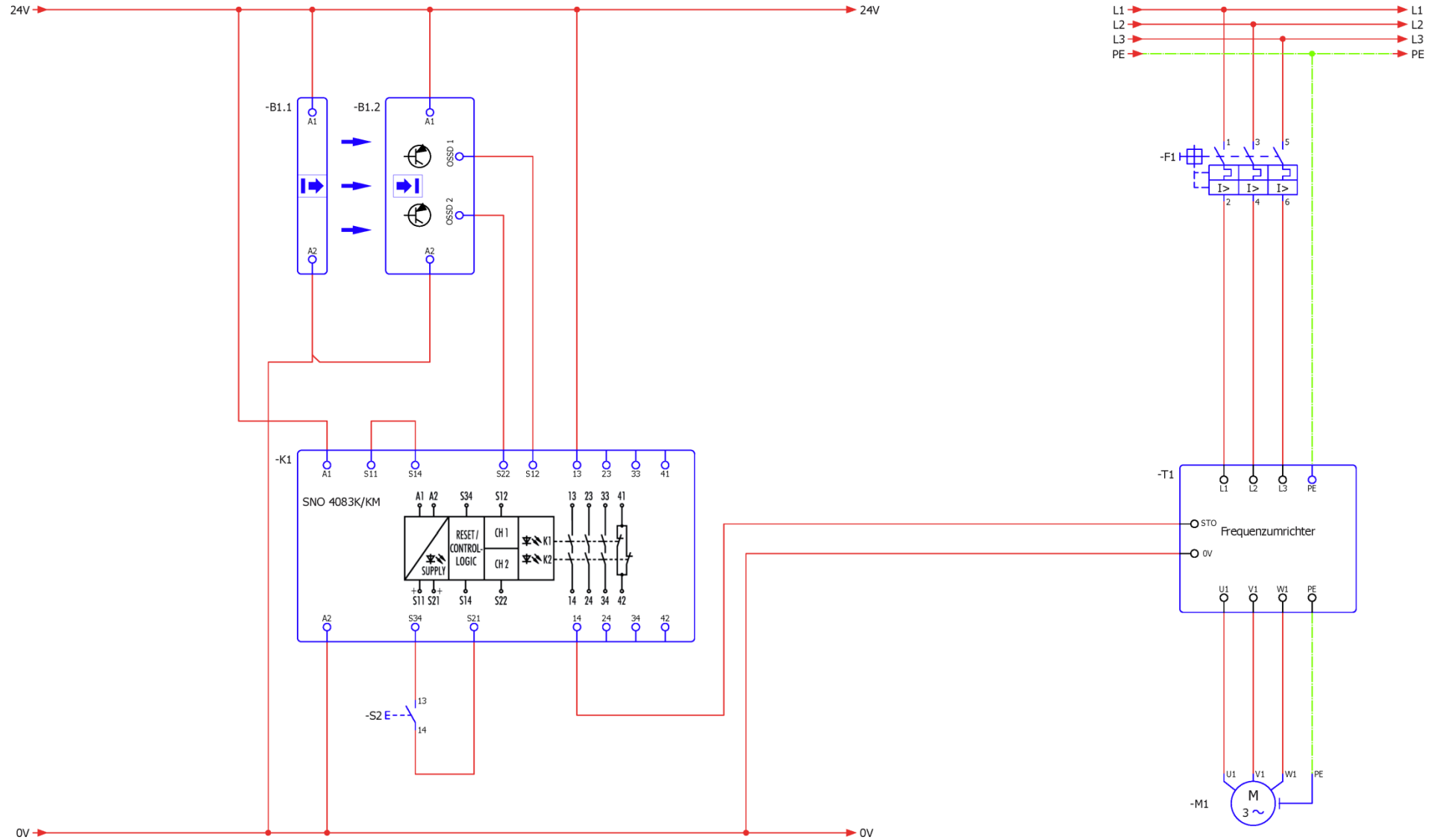
Maximum achievable PL		
PL c	PL e	PL d

PL c		
------	--	--

# Safety functions

Light curtain/grid, type 2 in PL c

## 3.15.6 Circuit diagram





### 3.16 Light curtain/grid, type 4 in PL e

#### 3.16.1 Safety function

<b>Safety function</b>	By interrupting the light curtain/grid –B1, the speed of the drive –M1 is reduced to a safely limited speed (SLS).
<b>Trigger event</b>	Interruption of the light curtain/grid –B1 by the operator.
<b>Reaction</b>	Safely limited speed of –M1 (SLS).
<b>Safe state</b>	The safe state is achieved if –M1 does not move faster than permitted.

#### 3.16.2 Description

<b>Function</b>	By interruption of the light curtain/grid –B1: <ul style="list-style-type: none"><li>• the OSSD signals are switched off</li><li>• the two input circuits on safety switchgear –K1 are interrupted</li><li>• the safety contacts of –K1 open</li><li>• the frequency converter –T1 is switched to a safely limited speed with the SLS safety input</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs if the interruption from the light curtain/grid is removed. It is not possible to step behind the light curtain/grid due to the design.
<b>Restart</b>	The restart function occurs either by pressing –S2 or by removing the interruption from the light curtain/grid –B1. A restart may only be possible if: <ul style="list-style-type: none"><li>• light curtain/grid –B1 is not interrupted</li></ul>
<b>Feedback circuit</b>	Not required here, as –T1 is a device with integrated diagnostics.

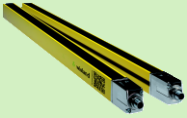

#### 3.16.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"><li>• Monitoring of synchronous time between the input circuits –S12; –S22 by –K.</li><li>• All faults in the wiring from –B1 to –K1 are detected through using OSSD testing by –B1 as well as synchronous time monitoring by –K1. “Cross comparison with dynamisation and high-performance fault detection” → DC = 99 %.</li><li>• Protected installation of the cable is not required.</li><li>• Required for the selection and positioning of the light curtain/grid.</li><li>• The system reaction time from the interruption of the light curtain/grid until the stoppage of the drives must be determined.</li><li>• The required design (position, interval, alignment, resolution and length) of the light curtain/grid must be determined. See EN ISO 13855.</li></ul>
<b>Actuators</b>	Frequency converter with integrated diagnostics and evaluation as PL e.

# Safety functions

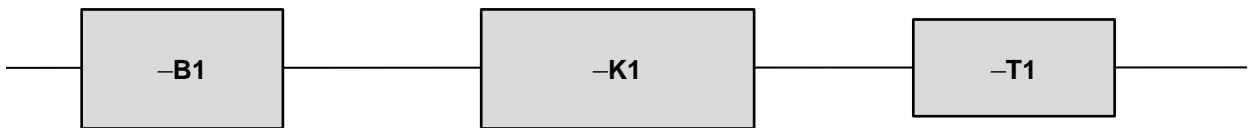
## Light curtain/grid, type 4 in PL e

### 3.16.4 Products (options)

	Product
<b>-B1</b> 	Type 4 safety light grid or curtain <b>sensor</b> PRO: SLC-4xx Order number: R1.541.1800.0 + R1.561.1800.0  <i>Note: With the required data regarding reaction time, resolution and length.</i>
<b>-K1</b> 	Safety switchgear <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>-T1</b>	Frequency converter with integrated diagnostics and evaluation as PL e. Integrated SLS safety function.

### 3.16.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------

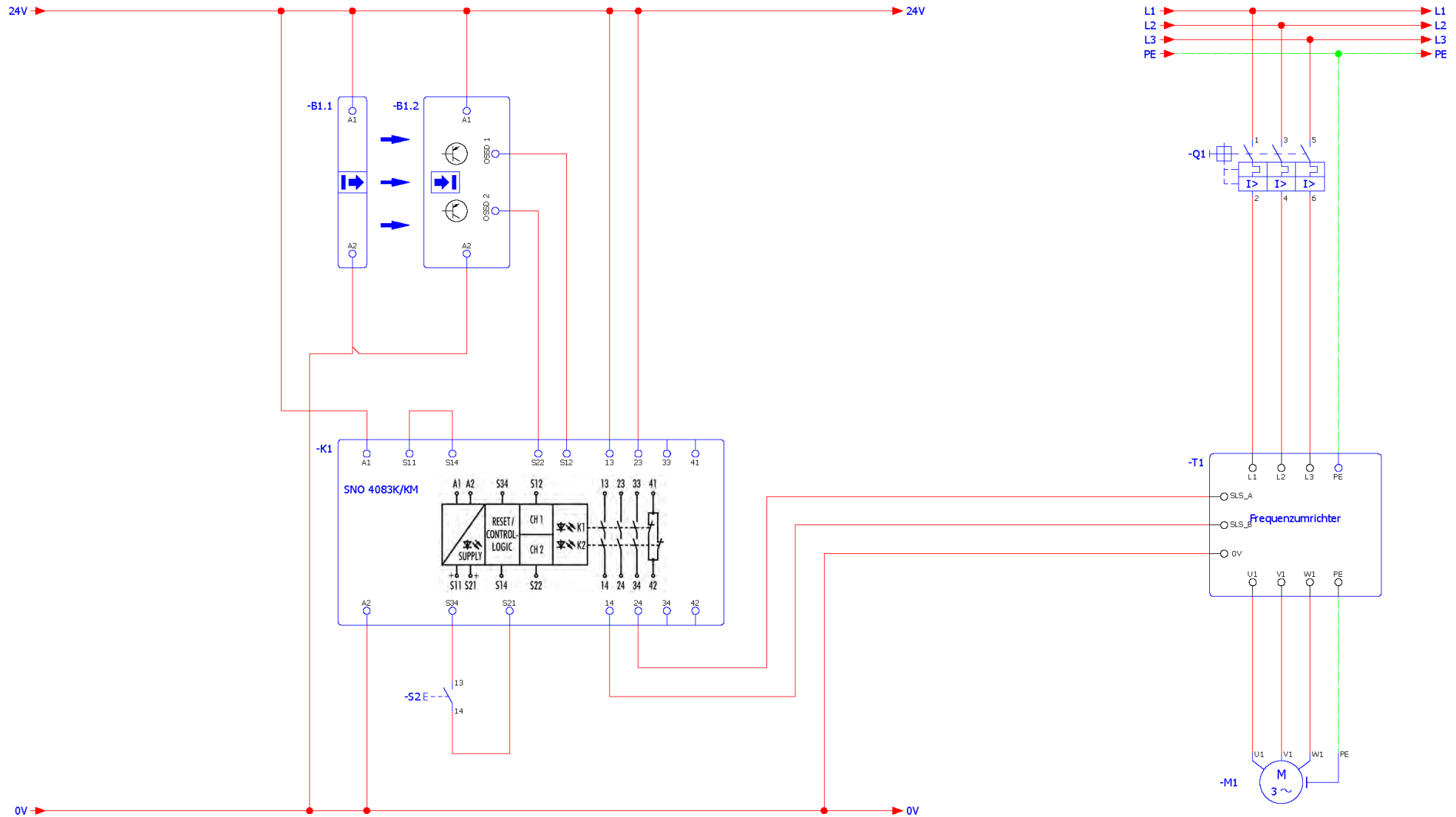


Required data from the device manufacturer		
PL; PFH <sub>D</sub> , T <sub>M</sub>	PL; PFH <sub>D</sub> , T <sub>M</sub>	PL; PFH <sub>D</sub> , T <sub>M</sub>
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>CCF not required                             <ul style="list-style-type: none"> <li>Cat. 4</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>CCF not required                             <ul style="list-style-type: none"> <li>Cat. 4</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>CCF not required                             <ul style="list-style-type: none"> <li>Cat. 4</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>
Maximum achievable PL		
PL e	PL e	PL e
PL e		

# Safety functions

Light curtain/grid, type 4 in PL e

## 3.16.6 Circuit diagram



### 3.17 E-Stop in series – two-channel in PL d

#### 3.17.1 Safety function

<b>Safety function</b>	By pressing one of the emergency stop buttons –S1 or –S2, all the drives of the system are stopped in a controlled way.
<b>Trigger event</b>	Activation of one of the emergency stop buttons by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.17.2 Description

<b>Function</b>	By pressing the emergency stop buttons –S1 or –S2: <ul style="list-style-type: none"> <li>• the input circuit on safety switchgear –K1 is interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the contactors –Q1 and –Q2 drop out</li> <li>• the machine M1 is stopped</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by turning respectively the emergency stop button –S1 or –S2 to release.
<b>Restart</b>	The restart function occurs by pressing –S3. A restart may only be possible if: <ul style="list-style-type: none"> <li>• emergency stop buttons –S1 and –S2 are not pressed</li> <li>• the contactors –Q1 and –Q2 have dropped out</li> </ul>
<b>Feedback circuit</b>	The positively-driven, normally closed contacts of the contactors –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of the safety switchgear –K1.



#### 3.17.3 Safety review

<b>Sensors</b>	Cross-circuits (channel 1 – channel 2) in the input circuit are detected by the different potentials (24V+/0V) of the sensor cables. Not all the faults are detected (0V to 0V / +24V to +24V). An accumulation of faults can lead to a loss of the safety function. DC = 60%.
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</li> <li>• The contactors have positively-driven feedback contacts.</li> <li>• Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.</li> </ul>

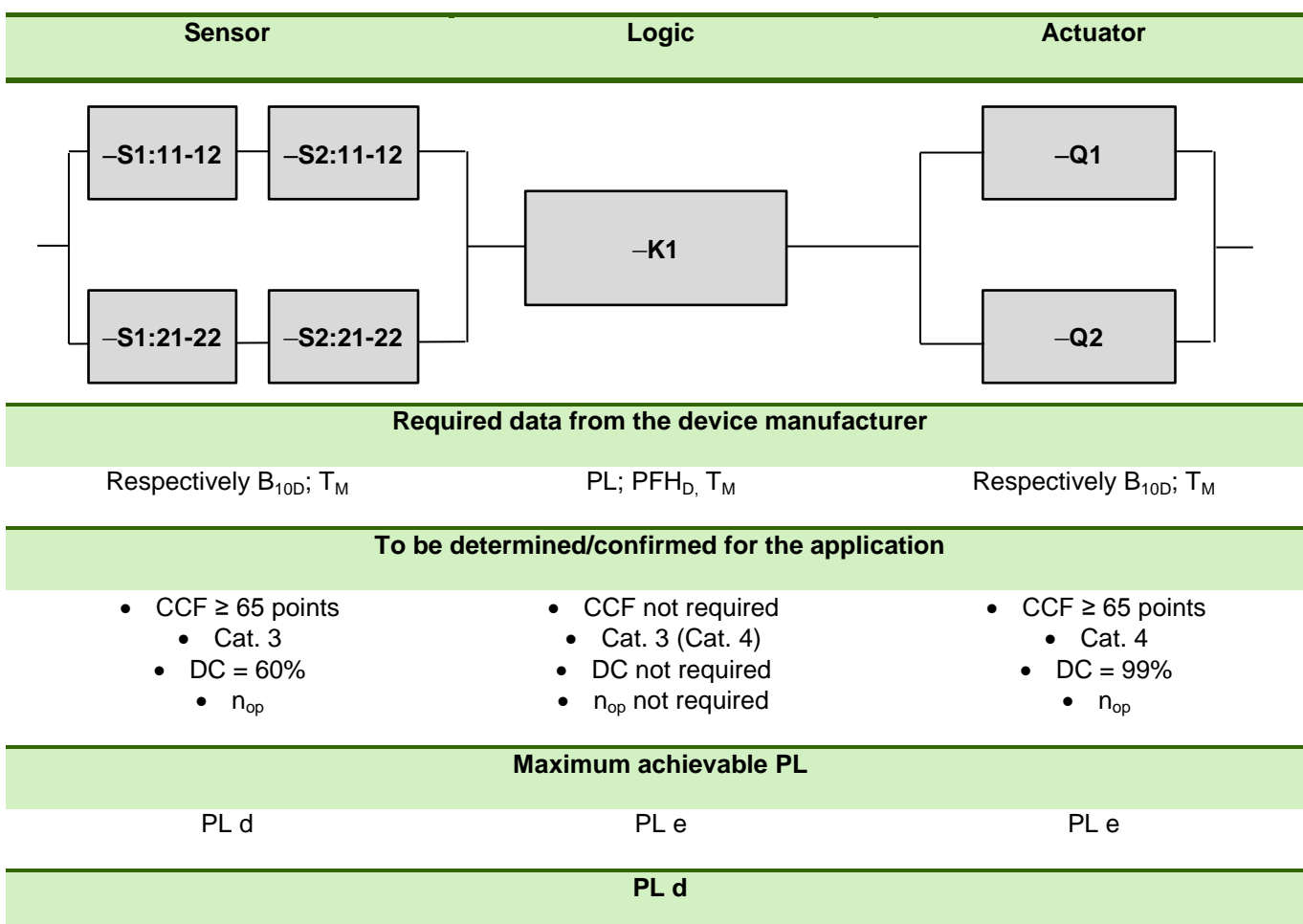
# Safety functions

## E-Stop in series – two-channel in PL d

### 3.17.4 Products (options)

	Product
-S1; -S2 	Emergency stop device (2-channel) with contact block detachment monitoring <b>sensor</b> PRO: SNH-1122 Order number: R1.200.1122.0
-K1 	Safety switchgear <b>safe</b> RELAY: SNO 4003K Order number: R1.188.0500.1
-Q1; -Q2	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

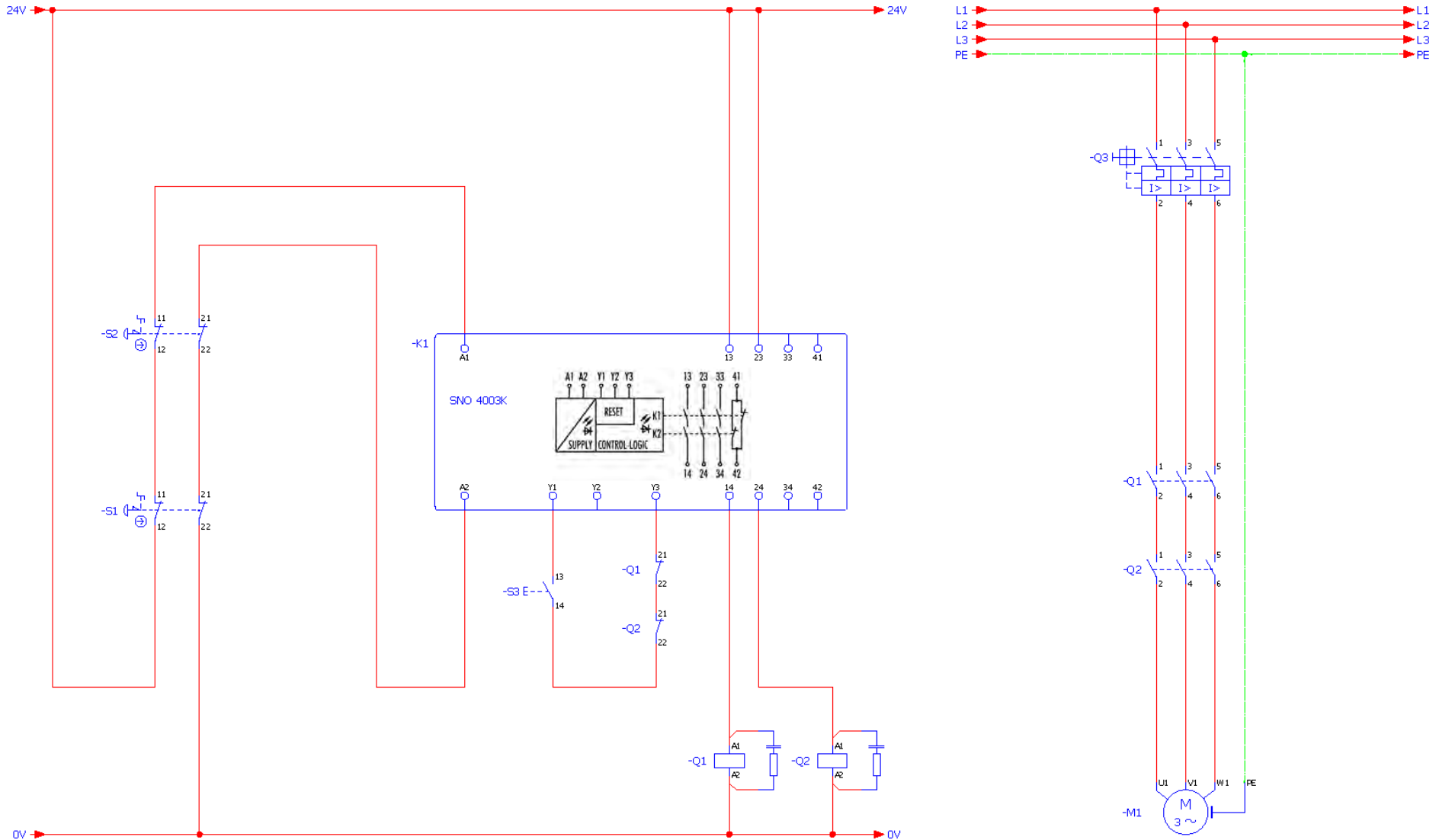
### 3.17.5 Modelling according to EN ISO 13849-1



# Safety functions

E-Stop in series – two-channel in PL d

## 3.17.6 Circuit diagram



### 3.18 E-Stop & door switch, mech. in series, single-channel in PL c

#### 3.18.1 Safety function

<b>Safety function</b>	By opening the door(s) or activating the emergency stop, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of one or several doors or activation of the emergency stop by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

**Note:** *The safety functions of emergency stop and door monitoring can also be modelled separately. Due to the simplicity of the application, a common approach has been selected.*

#### 3.18.2 Description

<b>Function</b>	By opening the door(s) or activating the emergency stop: <ul style="list-style-type: none"><li>• the input circuit on the safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the contactor –Q1 drops out</li><li>• machine 1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door(s) or by releasing the emergency stop. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart function occurs by pressing switch –S2. A restart is only possible if: <ul style="list-style-type: none"><li>• the doors are closed</li><li>• the emergency stop is released</li></ul> It is not possible to step behind the doors due to the design.
<b>Feedback circuit</b>	No monitoring of the contactor




#### 3.18.3 Safety review

<b>Sensors</b>	Faults in the components or wiring are only detected by manual tests. These tests must be carried out at regular intervals. A minimum test frequency of 1x per year must be defined in the documentation.  <b>Note:</b> <i>The use of two-channel switches for doors or emergency stop does not bring any increase in safety due to the expected fault masking (see 4.1.5) and the resulting DC = 0%. A maximum category of Cat. 1 would therefore be possible even with a two-channel configuration.</i>
<b>Actuators</b>	Faults in the components or wiring are only detected by manual tests. These tests must be carried out at regular intervals. A minimum test frequency of 1x per year must be defined in the documentation.

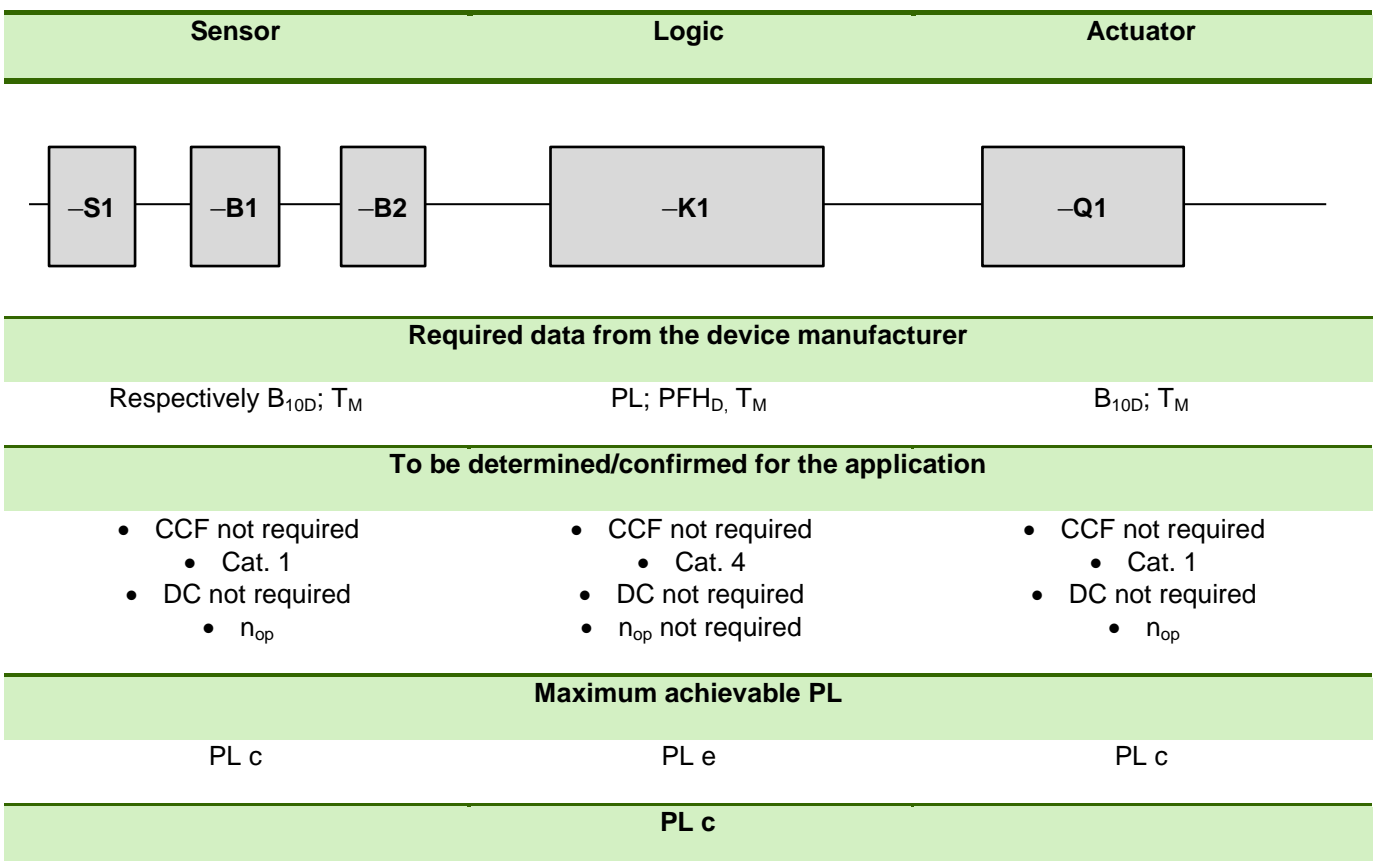
# Safety functions

E-Stop & door switch, mech. in series, single-channel in PL c

## 3.18.4 Products (options)

	Product
-B1; -B2 	Interlocking device type 2 (door switch with separate actuating element) <b>sensor</b> PRO: SMS3x10 Order number: R1.320.3010.0
-S1 	Emergency stop device (1-channel) with contact block detachment monitoring <b>sensor</b> PRO: SNH-1102 Order number: R1.200.1102.0
-K1 	Safety switchgear <b>safe</b> RELAY: SNO 4003K Order number: R1.188.0500.1
-Q1	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

## 3.18.5 Modelling according to EN ISO 13849-1

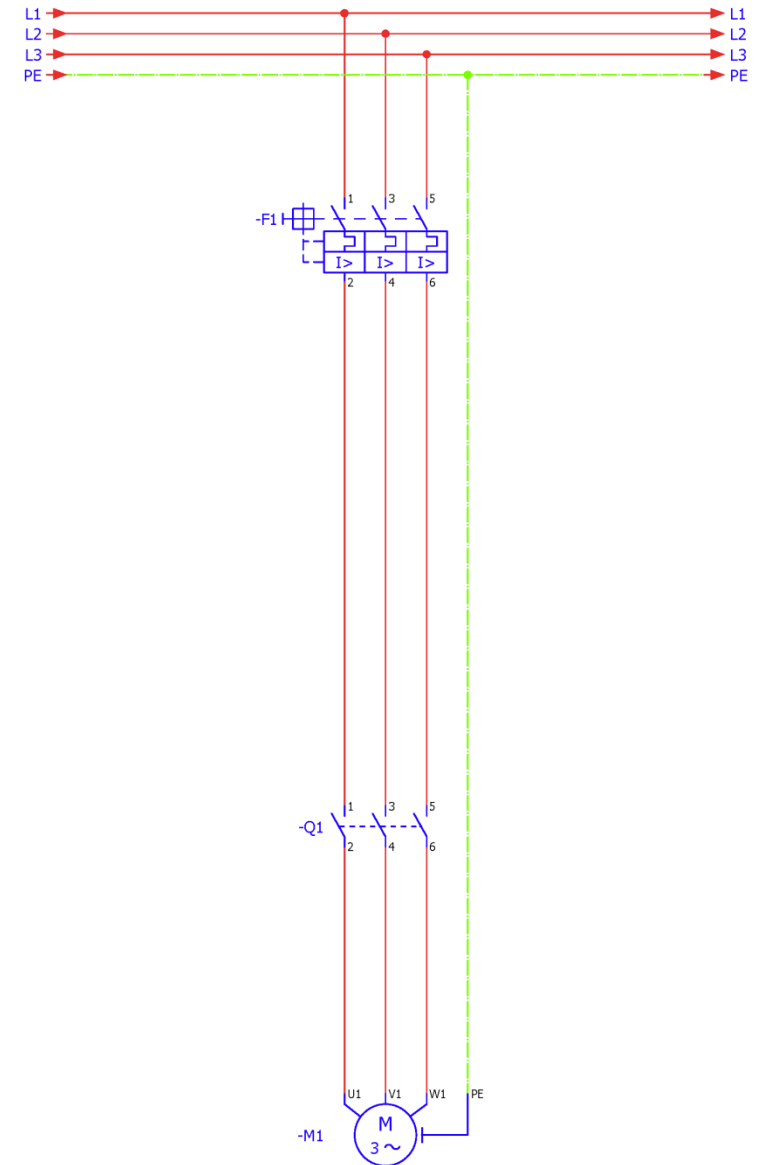
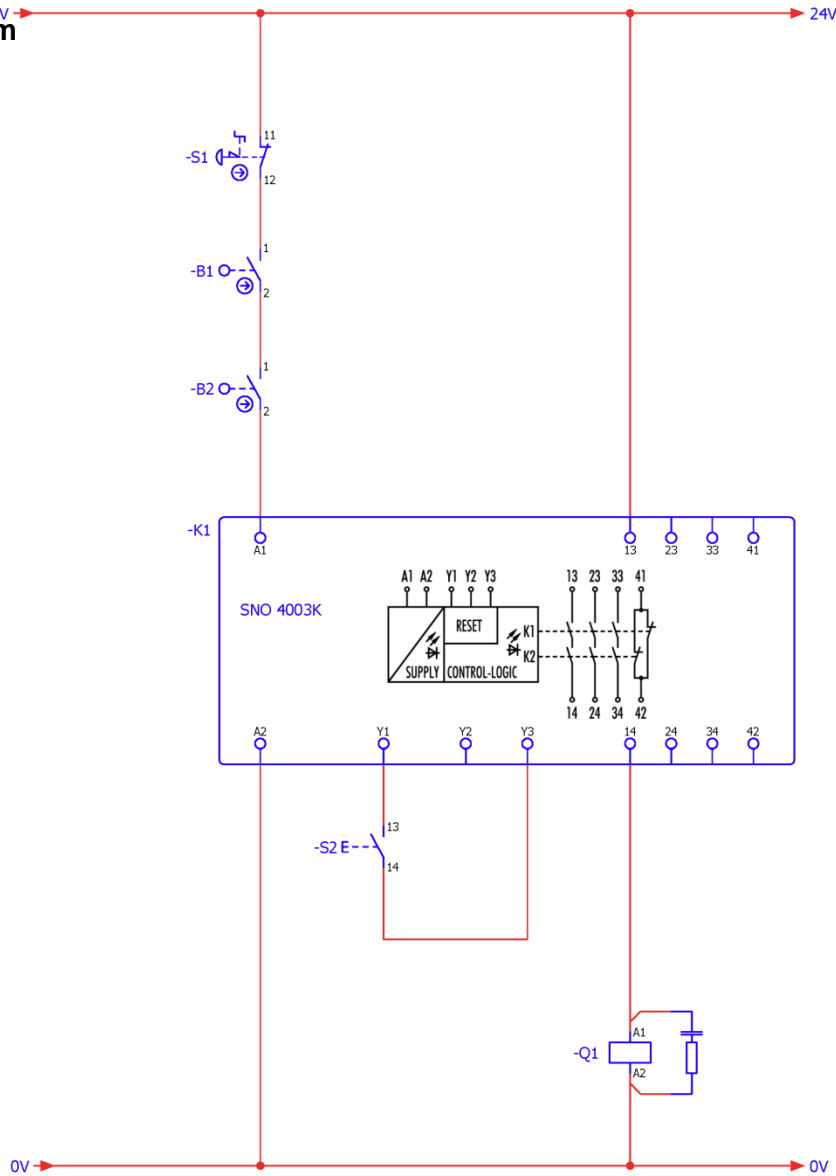




# Safety functions

E-Stop & door switch, mech. in series, single-channel in PL c

## 3.18.6 Circuit diagram



### 3.19 E-Stop & door switch, magnetic in series, two-channel in PL c

#### 3.19.1 Safety function

<b>Safety function</b>	By opening the door(s) or activating the emergency stop, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of one or more doors or activation of the emergency stop by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

**Note:** *The safety functions of emergency stop and door monitoring can also be modelled separately. Due to the simplicity of the application, a common approach has been selected.*

#### 3.19.2 Description

<b>Function</b>	By opening the door(s) or activating the emergency stop: <ul style="list-style-type: none"> <li>• the input circuit on safety switchgear –K1 is interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the contactor –Q1 drops out</li> <li>• machine 1 is stopped</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door(s) or by releasing the emergency stop. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart function occurs by pressing switch –S2. A restart may only be possible if: <ul style="list-style-type: none"> <li>• the doors are closed</li> <li>• the emergency stop is released</li> </ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	No monitoring of the contactor




#### 3.19.3 Safety review

<b>Sensors</b>	<p>Faults in the components or wiring are only detected by manual tests. These tests must be carried out at regular intervals. A minimum test frequency of 1x per year must be defined in the documentation.</p> <p>The use of two-channel switches for doors or emergency stop does not bring any increase in safety due to the expected fault masking (see 4.1.5) and the resulting DC = 0%. A maximum category of Cat. 1 is therefore possible despite the dual-channel design.</p> <p>The dual-channel principle is however still necessary for the sensors as otherwise the positive opening of the magnetic switches is not guaranteed.</p>
<b>Actuators</b>	Faults in the components or wiring are only detected by manual tests. These tests must be carried out at regular intervals. A minimum test frequency of 1x per year must be defined in the documentation.


# Safety functions

## E-Stop & door switch, magnetic in series, two-channel in PL c

### 3.19.4 Products (options)

Product	
-B1; -B2 	Interlocking device type 3 (door switch with magnetic operation) <b>sensor</b> PRO: SMA01xx Order number: R1.100.0113.0
-S1 	Emergency stop device (2-channel) with contact block detachment monitoring <b>sensor</b> PRO: SNH-1122 Order number: R1.200.1122.0
-K1 	Safety switchgear <b>safe</b> RELAY: SNA 4043K/KM Order number: R1.188.3250.0
-Q1	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

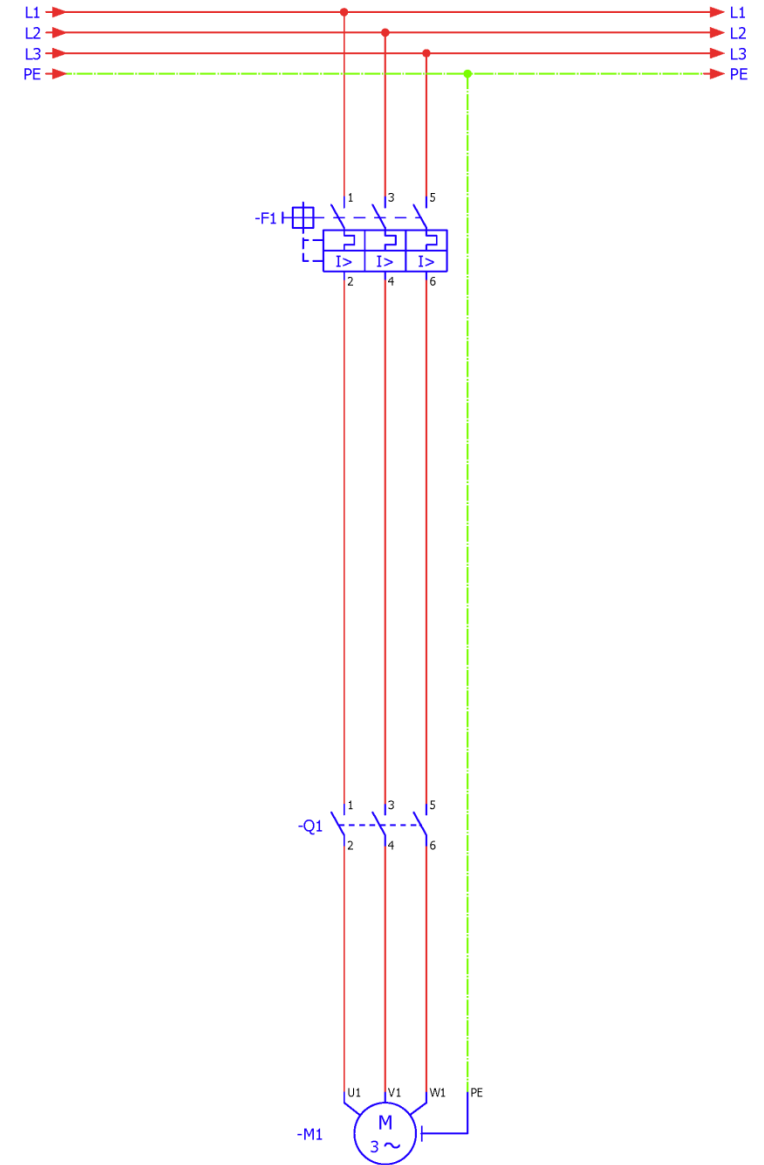
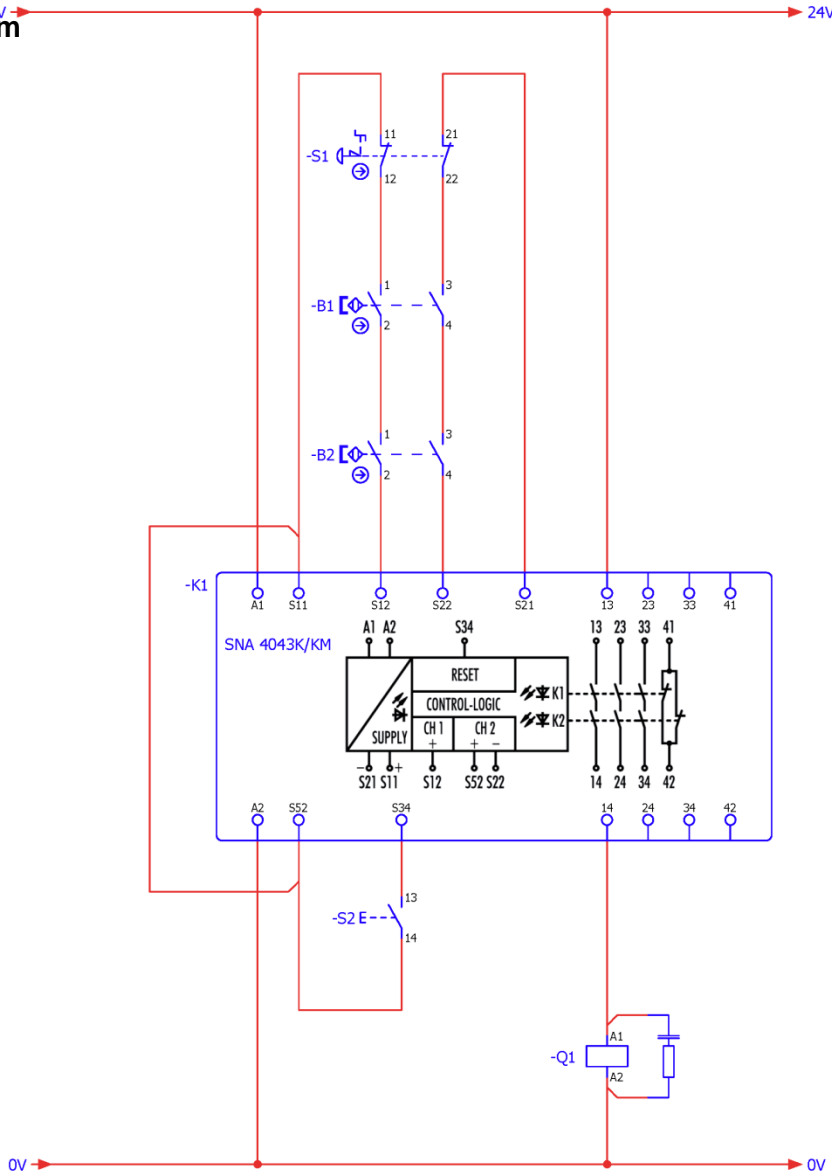
### 3.19.5 Modelling according to EN ISO 13849-1

Sensor	Logic	Actuator
		
Required data from the device manufacturer		
Respectively $B_{10D}$ ; $T_M$	PL; $PFH_D$ ; $T_M$	$B_{10D}$ ; $T_M$
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>• CCF not required                             <ul style="list-style-type: none"> <li>• Cat. 1</li> </ul> </li> <li>• DC not required                             <ul style="list-style-type: none"> <li>• <math>n_{op}</math></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• <math>n_{op}</math> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required                             <ul style="list-style-type: none"> <li>• Cat. 1</li> </ul> </li> <li>• DC not required                             <ul style="list-style-type: none"> <li>• <math>n_{op}</math></li> </ul> </li> </ul>
Maximum achievable PL		
PL c	PL e	PL c
PL c		

# Safety functions

E-Stop & door switch, magnetic in series, two-channel in PL c

## 3.19.6 Circuit diagram



### 3.20 Door switch, magnetic in series – two-channel in PL d

#### 3.20.1 Safety function

<b>Safety function</b>	By opening the door(s), all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of one or more doors by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.20.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch(es) are operated</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the positively-driven contactors –Q1 and –Q2 drop out</li><li>• machine 1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door(s). The door switch(es) (–B1, –B2, –B3) is/are closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart function occurs by closing the door(s). A restart may only be possible if: <ul style="list-style-type: none"><li>• the doors are closed</li><li>• the positively-driven contactors –Q1 and –Q2 have dropped out</li></ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	The positively-driven, normally closed contacts of the contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switchgear –K1.



# Safety functions

## Door switch, magnetic in series – two-channel in PL d

### 3.20.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults and cross-circuits in the input circuit are detected by –K1 through relay potentials (24V+/0V) on the sensor cables.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1.</li> <li>• This would lead to DC = 99% but cannot be implemented due to the series connection. Through the cascading (series connection), an opened door can prevent the fault of another door being detected (fault masking). If it is guaranteed that only one of the doors is used frequently (max. once per hour), up to five further doors can be switched in series and a low or medium DC can be achieved but with a maximum of PL d. In this case, a low DC = 60% can be selected. See ISO/TR 24119.</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</li> <li>• The contactors have positively-driven feedback contacts. DC = 99%</li> </ul>

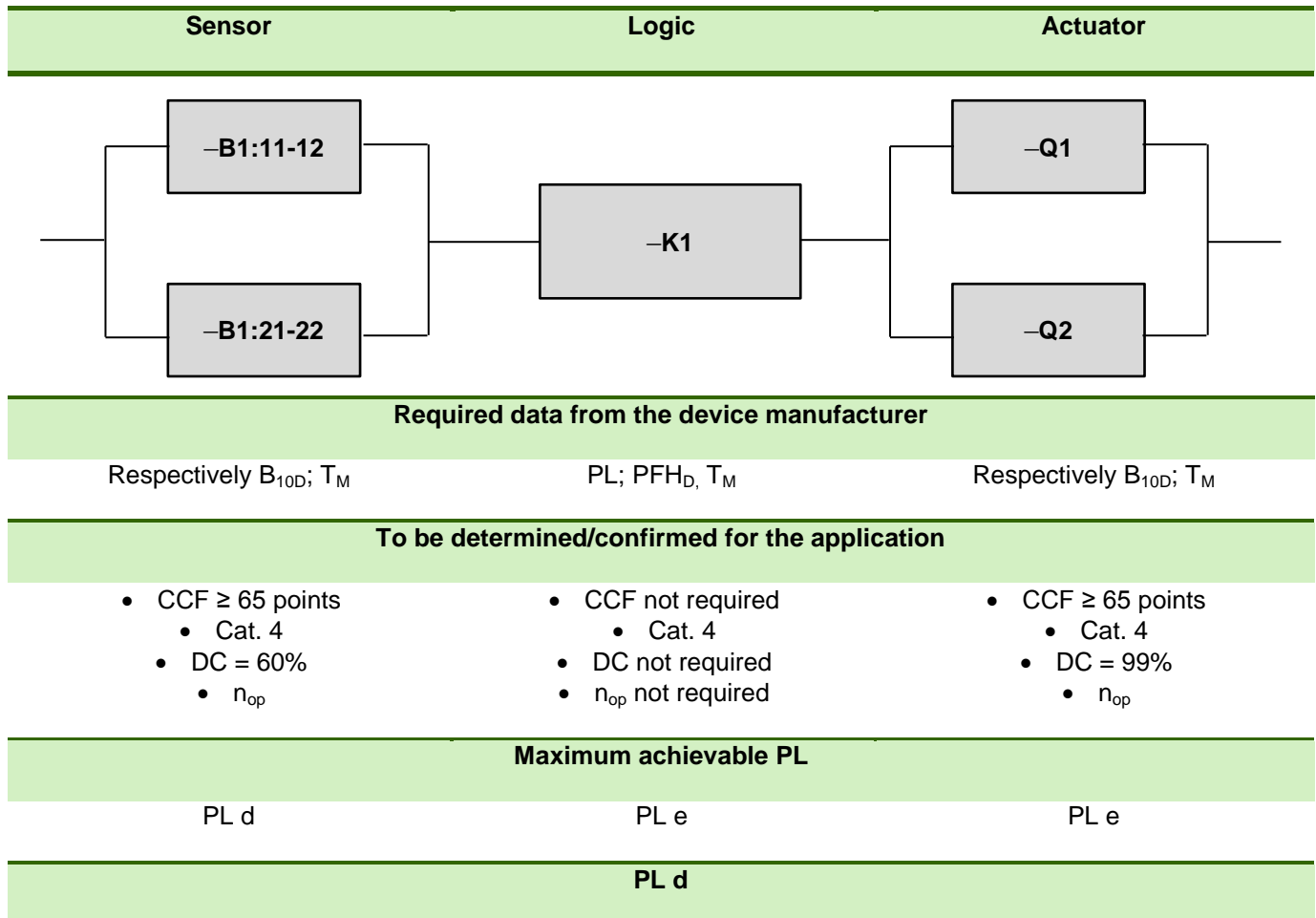
### 3.20.4 Products (options)

	Product
–B1; –B2; –B3 	Interlocking device type 3 (door switch with magnetic operation) <b>sensor</b> PRO: SMA01xx Order number: R1.100.0113.0
–K1 	Safety switchgear <b>safe</b> RELAY: SNA 4043K/KM Order number: R1.188.3250.0
–Q1; –Q2	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

# Safety functions

Door switch, magnetic in series – two-channel in PL d

## 3.20.5 Modelling according to EN ISO 13849-1

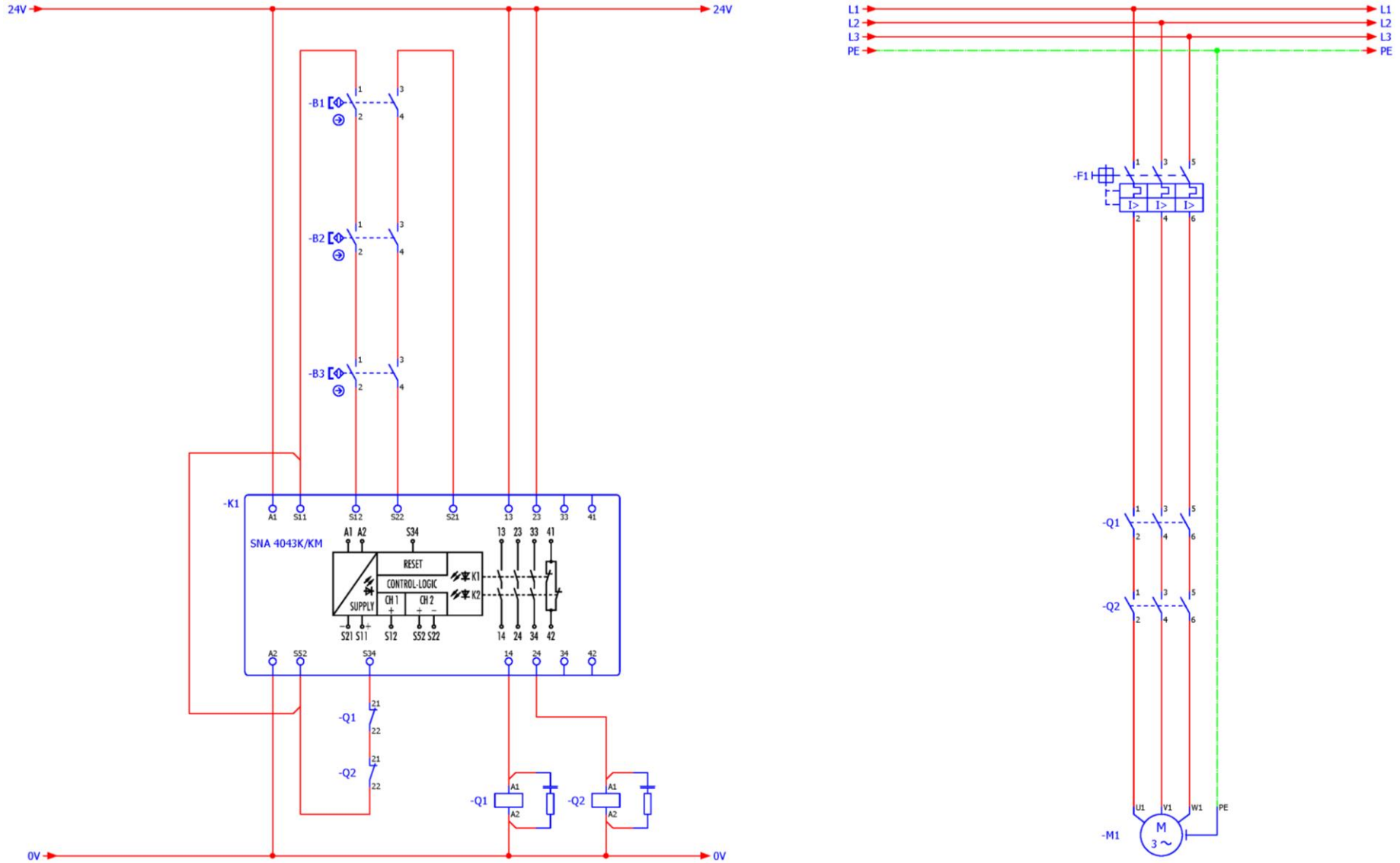


**Note:** For identical sensors –B2 and –B3, the modelling and achievable PL are the same.

# Safety functions

Door switch, magnetic in series – two-channel in PL d

## 3.20.6 Circuit diagram





### 3.21 Door switch, RFID in series – two-channel, equivalent in PL e

#### 3.21.1 Safety function

<b>Safety function</b>	By opening the door(s), all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of one or more doors by the operator.
<b>Reaction</b>	De-energising of the drives via –T1 through the STO safety function.
<b>Safe state</b>	Drives are de-energised.

#### 3.21.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch(es) is/are operated</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the frequency converter –T1 is stopped via STO_A and STO_B</li><li>• machine 1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door(s). The door switch(es) (–B1, –B2) is/are closed. The design ensures that the door(s) cannot open accidentally.
<b>Restart</b>	The restart function occurs by closing the door(s). A restart is only possible if: <ul style="list-style-type: none"><li>• the doors are closed</li></ul> <p>It is not possible to step behind the doors due to the design.</p>



#### 3.21.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"><li>• All door sensors are self-monitoring</li><li>• All sensors have OSSD outputs</li><li>• Cross-circuits between OSSD output signals are detected by the sensor and lead to the safe state of both OSSD outputs in the event of a fault.</li><li>• Short-circuits of the OSSD outputs against 24V or GND are detected by the safety switchgear –K1 or the respective series-connected door sensor using cross comparison.</li><li>• As all the faults are individually diagnosed, fault masking can be ruled out. DC = 99% (cross comparison and high-performance fault detection) can be assumed for all the sensors.</li><li>• It should be noted that the switching times of all the door sensors are added to the respective series-connected door sensor in the sequence (here –B1).</li></ul>
<b>Actuators</b>	<ul style="list-style-type: none"><li>• The frequency converter –T1 is a pre-certified safety module with integrated diagnostics.</li><li>• A feedback circuit is not required.</li></ul>

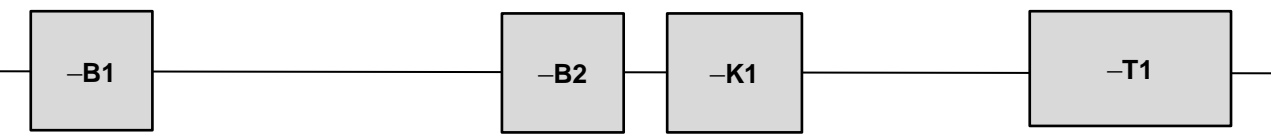
# Safety functions

Door switch, RFID in series – two-channel, equivalent in PL e

### 3.21.4 Products (options)

	Product
-B1; -B2 	Interlocking device type 4 (door switch in RFID technology) <b>sensor</b> PRO: STS01xx Order number: R1.400.0110.0
-K1 	Safety switchgear <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
-T1	Frequency converter with integrated diagnostics and evaluation as PL e. Integrated STO safety function.

### 3.21.5 Modelling according to EN ISO 13849-1

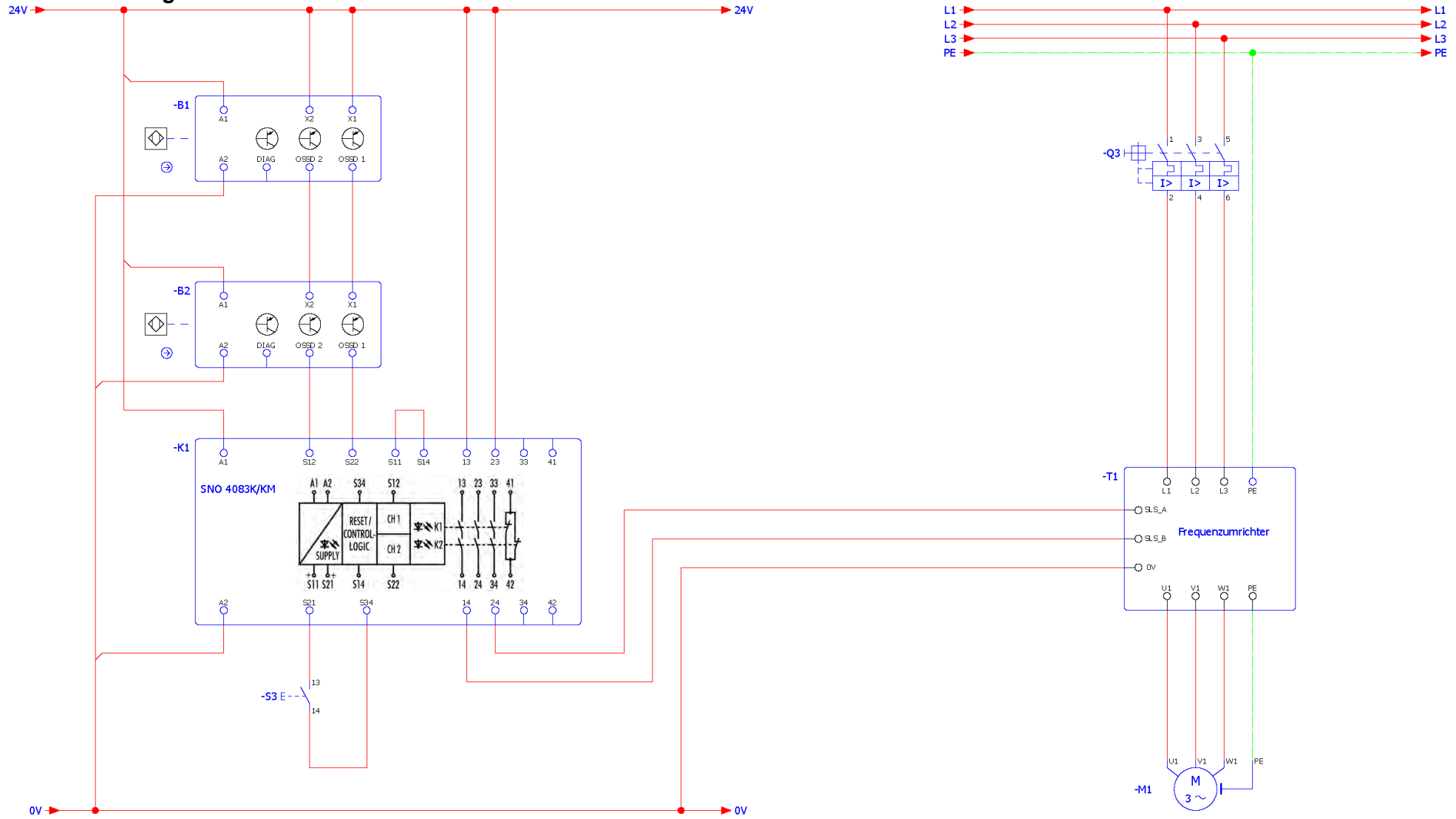
Sensor	Logic	Actuator
		
Required data from the device manufacturer		
PL; PFH <sub>D</sub> , T <sub>M</sub>	Respectively PL; PFH <sub>D</sub> , T <sub>M</sub>	PL; PFH <sub>D</sub> , T <sub>M</sub>
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>• CCF not required               <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required               <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required               <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• n<sub>op</sub> not required</li> </ul>
Maximum achievable PL		
PL e	PL e	PL e
PL e		

**Note:** *The calculation applies to sensor -B1. The modelling is shortened by -B1 for sensor -B2. As the modelling shown represents the worst case, it is adopted for all sensors.*

# Safety functions

Door switch, RFID in series – two-channel, equivalent in PL e

## 3.21.6 Circuit diagram



### 3.22 Door switch, RFID & E-Stop in series (1) – E-Stop –S1 in PL c

#### 3.22.1 Safety function (of emergency stop)

<b>Safety function</b>	The drives are stopped by pressing the emergency stop button –S1.
<b>Trigger event</b>	Activation of the emergency stop actuating element –S1 by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.22.2 Description

<b>Function</b>	By pressing the emergency stop button –S1: <ul style="list-style-type: none"><li>• the input circuit on door switch –B2 is interrupted</li><li>• the OSSD contacts of –B2 open</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the contactors –Q1 and –Q2 drop out and the machine M1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by turning the emergency stop button –S1 to release.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"><li>• emergency stop button –S1 is not pressed</li><li>• the doors –B1 and –B2 are closed</li><li>• the contactors –Q1 and –Q2 have dropped out</li></ul>
<b>Feedback circuit</b>	The positively-driven, normally closed contacts of the contactors –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of safety switchgear –K1.




#### 3.22.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"><li>• All the faults on the emergency stop and its wiring are detected by –B1 or –B2.</li><li>• The emergency stop button has a safeguard against malfunctions. This detects if the actuating element is disconnected from the switch contacts and interrupts one of the electric emergency stop circuits.</li><li>• The diagnosis of line faults between –B2 and –K1 is carried out jointly by –B2 and –K1.</li><li>• It must be expected that the door switch –B1 and the emergency stop –S1 are pressed soon after each other during the work process and that both are activated simultaneously. Fault masking for the emergency stop must thus be expected (initial faults in –S1 are masked by functional –B1 and remain undetected). As –S1 does not have its own integrated diagnostics, DC = none must be assumed for the emergency stop.</li><li>• It should be noted that the switching times of all the door sensors are added to the respective series-connected door sensor and the emergency stop.</li></ul>
----------------	---

### Actuators

- Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.
- The contactors have positively-driven feedback contacts.
- Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.

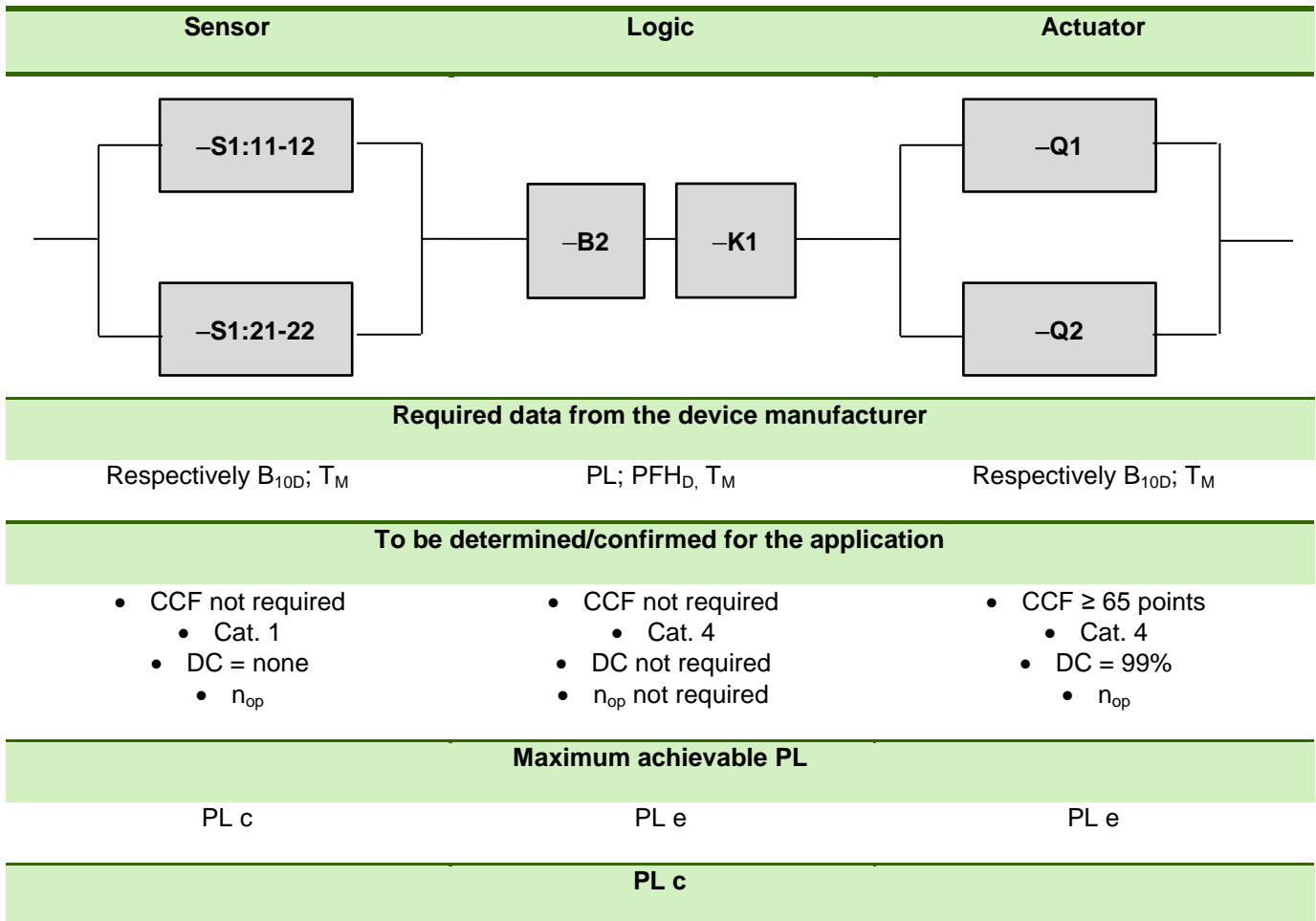
### 3.22.4 Products (options)

	Product
<b>–S1</b> 	Emergency stop device (2-channel) with contact block detachment monitoring <b>sensor PRO: SNH-1122</b> Order number: R1.200.1122.0
<b>–B2</b> 	Interlocking device type 4 (door switch in RFID technology) <b>sensor PRO: STS01xx</b> Order number: R1.400.0110.0
<b>–K1</b> 	Safety switchgear <b>safe RELAY: SNO 4083KM</b> Order number: R1.188.3580.0
<b>–Q1; –Q2</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

# Safety functions

Door switch, RFID & E-Stop in series (1) – E-Stop –S1 in PL c

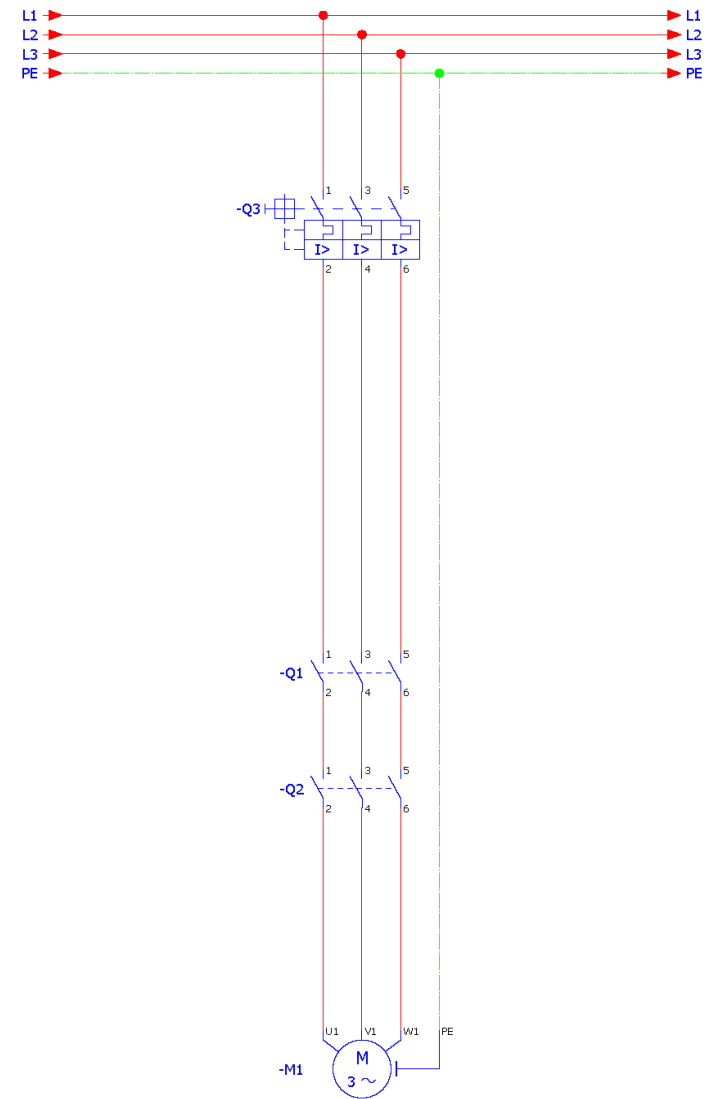
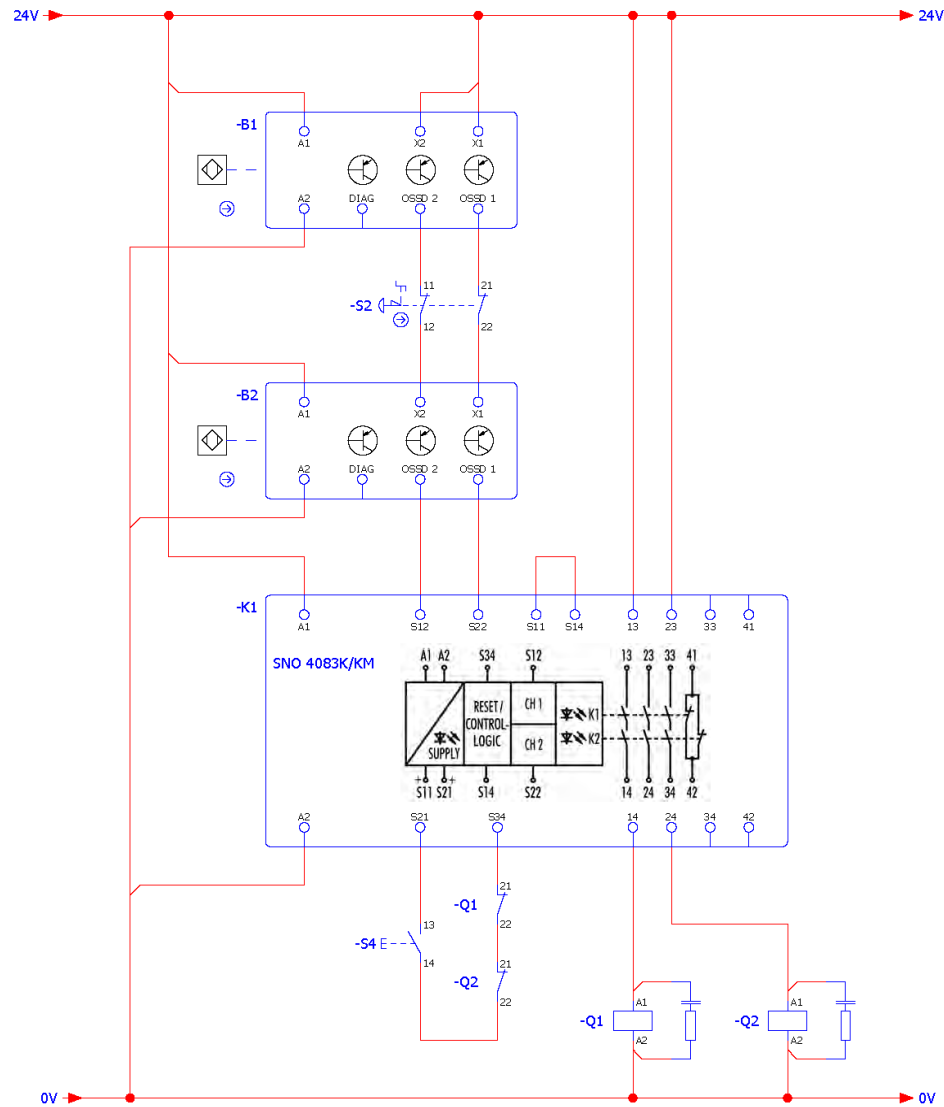
## 3.2.2.5 Modelling according to EN ISO 13849-1



# Safety functions

Door switch, RFID & E-Stop in series (1) – E-Stop –S1 in PL c

## 3.22.6 Circuit diagram



### 3.23 Door switch, RFID & E-Stop in series (1) – Door –B1 in PL e

#### 3.23.1 Safety function (of door 1)

<b>Safety function</b>	By opening door 1 –B1, all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of door 1 –B1 by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

#### 3.23.2 Description

<b>Function</b>	<p>By opening doors 1 –B1:</p> <ul style="list-style-type: none"> <li>• the OSSD contacts of –B1 open</li> <li>• the input circuit on door switch –B2 is interrupted</li> <li>• the OSSD contacts of –B2 open</li> <li>• the input circuit on safety switchgear –K1 is interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the contactors –Q1 and –Q2 drop out</li> <li>• the machine M1 is stopped</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing door 1 –B1.
<b>Restart</b>	<p>The restart function occurs by pressing –S2. A restart may only be possible if:</p> <ul style="list-style-type: none"> <li>• the emergency stop button –S1 is not pressed</li> <li>• the doors –B1 and –B2 are closed</li> <li>• contactors –Q1 and –Q2 have dropped out</li> </ul> <p>It is not possible to step behind the doors due to the design.</p>
<b>Feedback circuit</b>	The positively-driven, normally closed contacts of the contactors –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of safety switchgear –K1.

#### 3.23.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• –B1 is self-monitoring and has OSSD outputs.</li> <li>• Cross-circuits between OSSD output signals are detected by the sensor and lead to the safe state of both OSSD outputs in the event of a fault.</li> <li>• Short-circuits of the OSSD outputs against 24V or GND are detected by safety switchgear –K1 or the respective series-connected door sensor using cross comparison.</li> <li>• Each single fault is detected and leads to the safe state of both OSSDchannels. Fault masking or fault accumulation is thus excluded. DC = 99% can be assumed for –B1 (cross comparison and high-performance fault detection).</li> </ul> <p>It should be noted that the switching times of all the door sensors are added for the respective series-connected door sensor in the sequence (here –B1).</p>
----------------	---





# Safety functions

## Door switch, RFID & E-Stop in series (1) – Door –B1 in PL e

### Actuators

- Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.
- The contactors have positively-driven feedback contacts.
- Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.

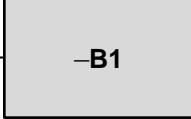
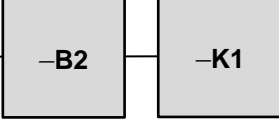
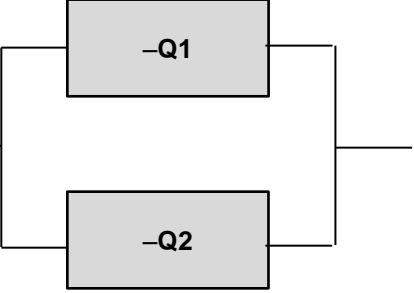
### 3.23.4 Products (options)

	Product
<b>–B1; –B2</b> 	Interlocking device type 4 (door switch in RFID technology) <b>sensor</b> PRO: STS01xx Order number: R1.400.0110.0
<b>–K1</b> 	Safety switchgear <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
<b>–Q1; –Q2</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"><li>• Contactor with positively-driven feedback contacts</li><li>• Suitable for the expected switching load and frequency</li><li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li></ul>

# Safety functions

Door switch, RFID & E-Stop in series (1) – Door –B1 in PL e

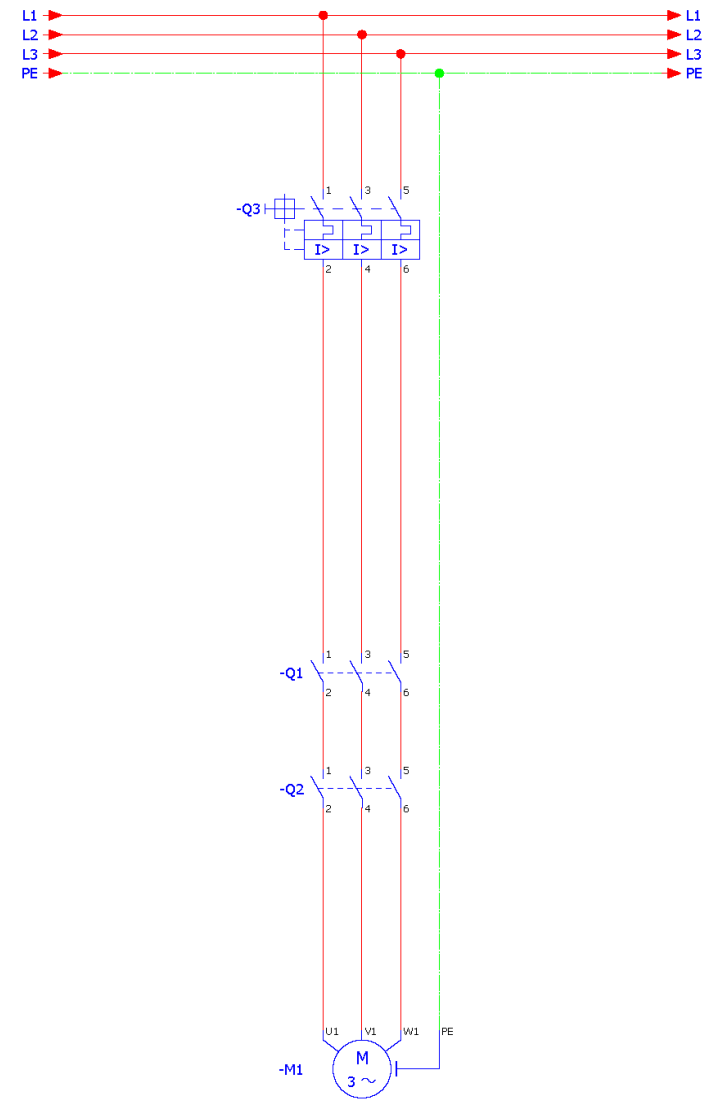
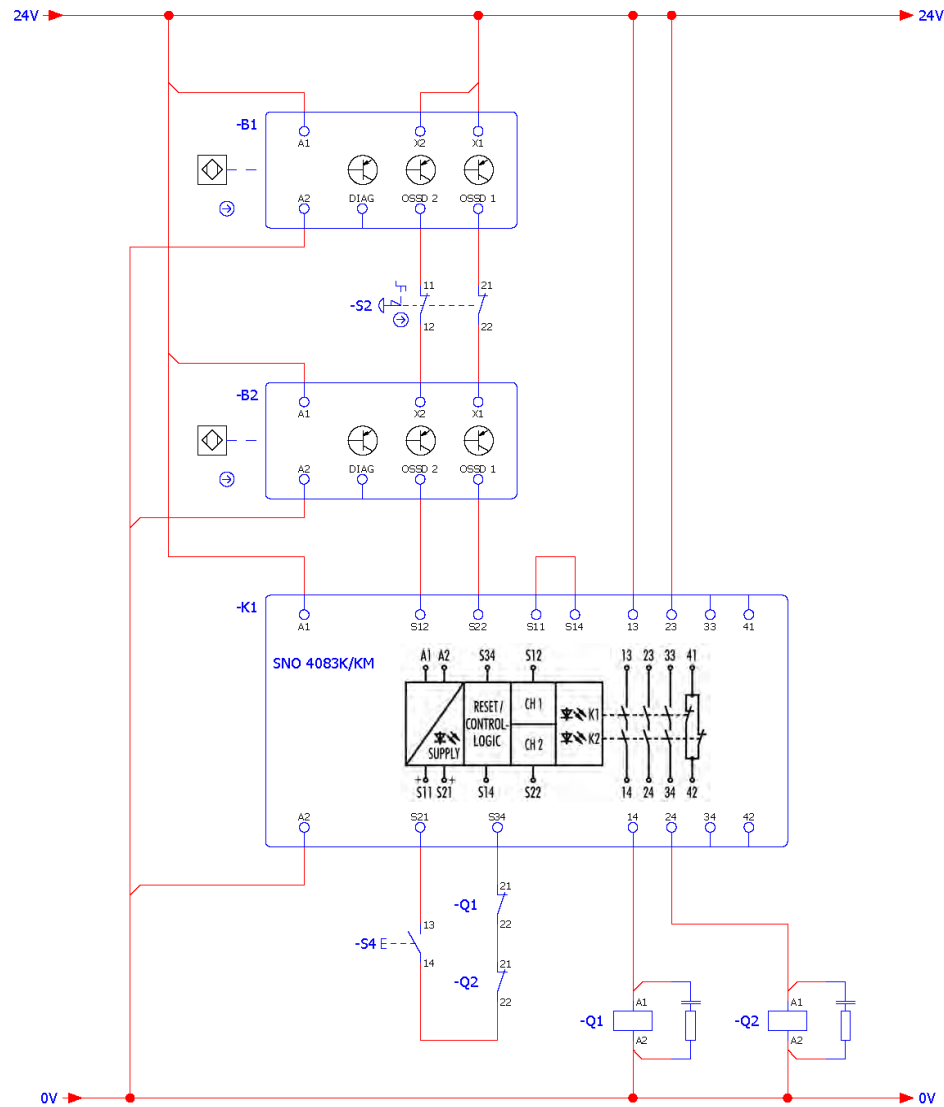
## 3.23.5 Modelling in accordance with EN ISO 13849-1

Sensor	Logic	Actuator
		
Required data from the device manufacturer		
PL; PFH <sub>D</sub> , T <sub>M</sub>	Respectively PL; PFH <sub>D</sub> , T <sub>M</sub>	Respectively B <sub>10D</sub> ; T <sub>M</sub>
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>• CCF not required                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF ≥ 65 points                             <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC = 99%</li> <li>• n<sub>op</sub></li> </ul>
Maximum achievable PL		
PL e	PL e	PL e
<b>PL e</b>		

# Safety functions

Door switch, RFID & E-Stop in series (1) – Door –B1 in PL e

## 3.23.6 Circuit diagram



### 3.24 Door switch, RFID & E-Stop in series (1) – Door –B2 in PL e

#### 3.24.1 Safety function (of door 2)

<b>Safety function</b>	By opening the door(s), all the drives of the installation are stopped / de-energised.
<b>Trigger event</b>	Opening of one or more doors by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.



#### 3.24.2 Description

<b>Function</b>	By opening the door(s): <ul style="list-style-type: none"><li>• the door switch(es) is/are activated</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the contactors –Q1 and –Q2 drop out and the machine M1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door(s). The door switch(es) (–B1, –B2) is/are closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	The restart occurs by closing the door(s). A restart may only be possible if: <ul style="list-style-type: none"><li>• the doors are closed</li></ul> <p>It is not possible to step behind the doors due to the design.</p>

### 3.24.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• All the door sensors are self-monitoring.</li> <li>• All the sensors have OSSD outputs.</li> <li>• Short-circuits of the OSSD outputs against 24V or GND are detected by safety switchgear –K1 or the respective series-connected door sensor using cross comparison.</li> <li>• Cross-circuits between OSSD output signals are detected by the sensor and lead to the safe state of both OSSD outputs in the event of a fault.</li> <li>• As all the faults can be individually diagnosed, fault masking can be excluded. DC = 99% (cross comparison and high-performance fault detection) can be assumed for all the sensors.</li> <li>• It should be noted that the switching times of all the door sensors are added for the respective series-connected door sensor in the sequence (here –B1).</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</li> <li>• The contactors have positively-driven feedback contacts.</li> <li>• Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.</li> </ul>

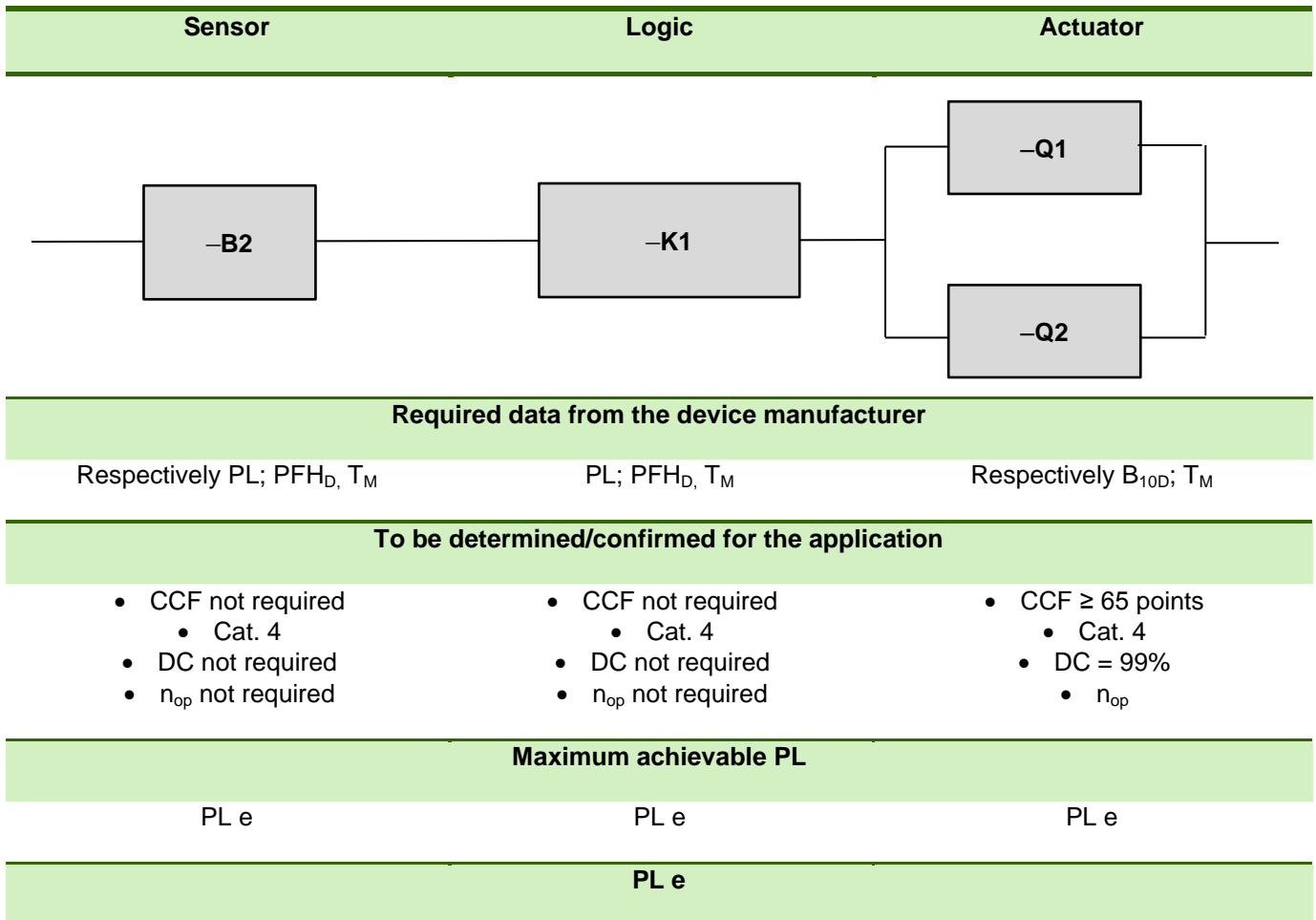
### 3.24.4 Products (options)

		Product
<b>–B2</b>		Interlocking device type 4 (door switch in RFID technology) <b>sensor PRO: STS01xx</b> Order number: R1.400.0110.0
<b>–K1</b>		Safety switchgear <b>safe RELAY: SNO 4083KM</b> Order number: R1.188.3580.0
<b>–Q1; –Q2</b>		Power contactor with the following characteristics: <ul style="list-style-type: none"> <li>• Contactor with positively-driven feedback contacts</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>

# Safety functions

Door switch, RFID & E-Stop in series (1) – Door –B2 in PL e

## 3.24.5 Modelling in accordance with EN ISO 13849-1





## 3.25 Door switch, RFID & E-Stop in series (2) – E-Stop in PL e

### 3.25.1 Safety function (of emergency stop)

<b>Safety function</b>	By pressing the emergency stop button –S1, all the drives of the system are stopped in a controlled way.
<b>Trigger event</b>	Activation of the emergency stop actuating element –S1 by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.

### 3.25.2 Description

<b>Function</b>	By pressing the emergency stop button –S1: <ul style="list-style-type: none"> <li>• the input circuit on door switch –B1 is interrupted</li> <li>• the OSSD contacts of –B1 open</li> <li>• the input circuit on door switch –B2 is interrupted</li> <li>• the OSSD contacts of –B2 open</li> <li>• the input circuit on safety switchgear –K1 is interrupted</li> <li>• the safety contacts of –K1 open</li> <li>• the contactors –Q1 and –Q2 drop out</li> <li>• the machine M1 is stopped</li> </ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by turning the emergency stop button –S1 to release.
<b>Restart</b>	The restart function occurs by pressing –S2. A restart may only be possible if: <ul style="list-style-type: none"> <li>• the emergency stop button –S1 is not pressed</li> <li>• the doors –B1 and –B2 are closed</li> <li>• the contactors –Q1 and –Q2 have dropped out</li> </ul>
<b>Feedback circuit</b>	The positively-driven, normally closed contacts of the contactors –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of safety switchgear –K1.

### 3.25.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults in the input circuit are detected by –B1 on the sensor cables. Cross-circuits are not detected due to the Cat. 3 structure thus “Cross comparison with dynamisation without high-performance fault detection” → DC = 90 %.</li> <li>• The emergency stop button has a safeguard against malfunctions. This detects if the actuating element is disconnected from the switch contacts and interrupts one of the electric emergency stop circuits.</li> <li>• Synchronous time monitoring between the input circuits –S12 and –S22.</li> <li>• It should be noted that the switching times of all the door sensors are added for the respective series-connected door sensor and emergency stop.</li> <li>• The diagnosis of line faults between –B1 and –B2 is carried out jointly by –B1 and –B2.</li> <li>• The diagnosis of line faults between –B2 and –K1 is carried out jointly by –B2 and –K1.</li> </ul>
----------------	---






# Safety functions

## Door switch, RFID & E-Stop in series (2) – E-Stop in PL e

### Actuators

- Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.
- The contactors have positively-driven feedback contacts.
- Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.

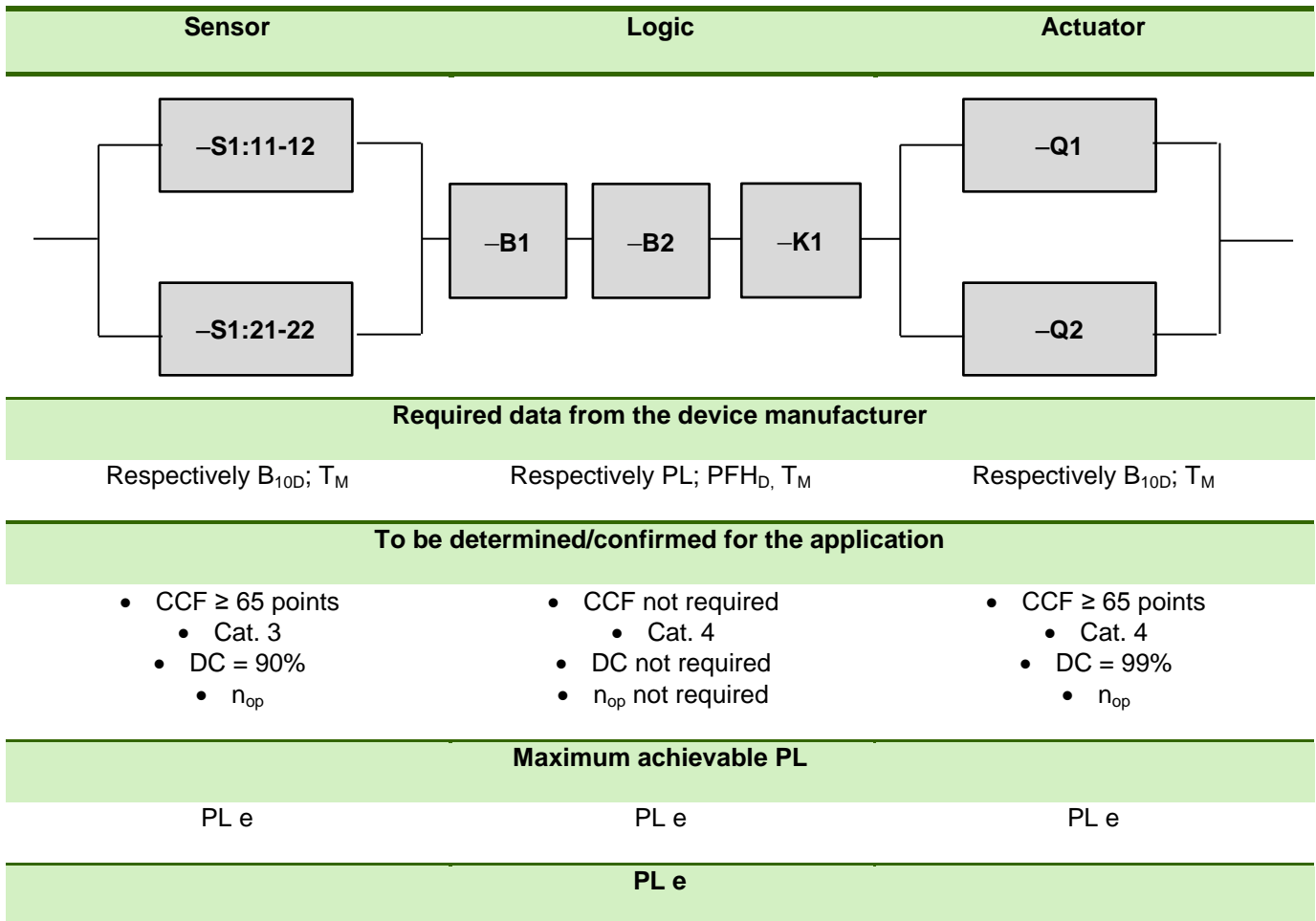
### 3.25.4 Products (options)

	Product
<b>–S1</b> 	Emergency stop device (2-channel) with contact block detachment monitoring <b>sensor PRO</b> : SNH-1122 Order number: R1.200.1122.0
<b>–B1;</b> <b>–B2</b> 	Interlocking device type 4 (door switch in RFID technology) <b>sensor PRO</b> : STS01xx Order number: R1.400.0110.0
<b>–K1</b> 	Safety switchgear <b>safe RELAY</b> : SNO 4083KM Order number: R1.188.3580.0
<b>–T1</b>	Power contactor with the following characteristics: <ul style="list-style-type: none"><li>• Contactor with positively-driven feedback contacts</li><li>• Suitable for the expected switching load and frequency</li><li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li></ul>

# Safety functions

Door switch, RFID & E-Stop in series (2) – E-Stop in PL e

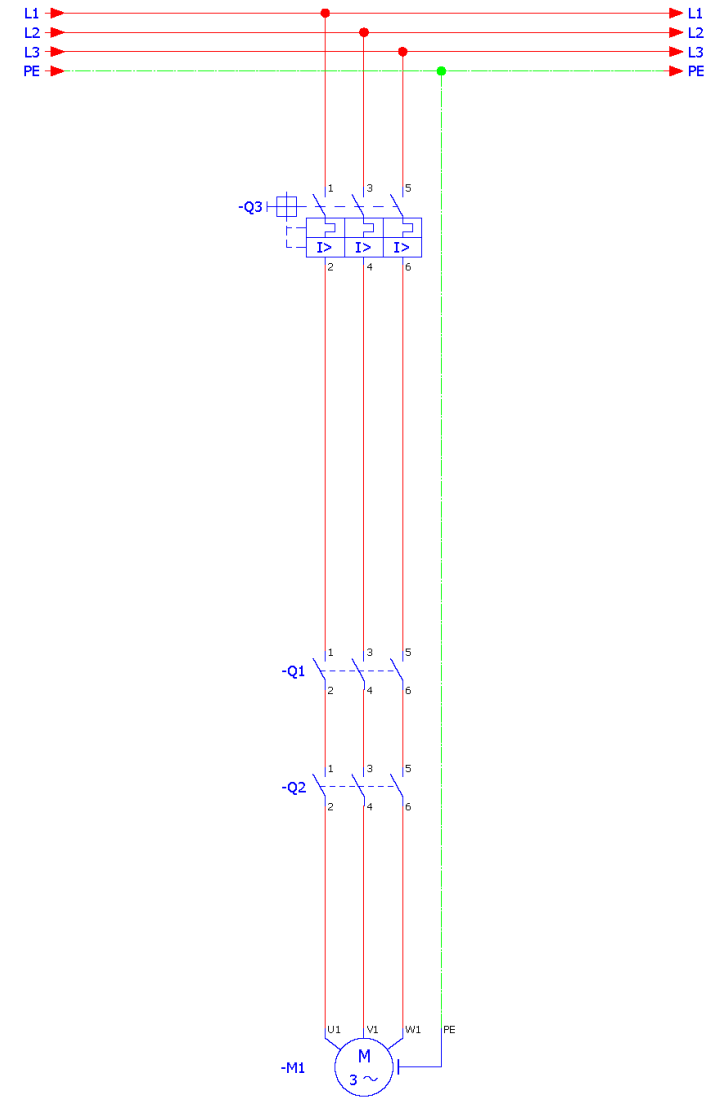
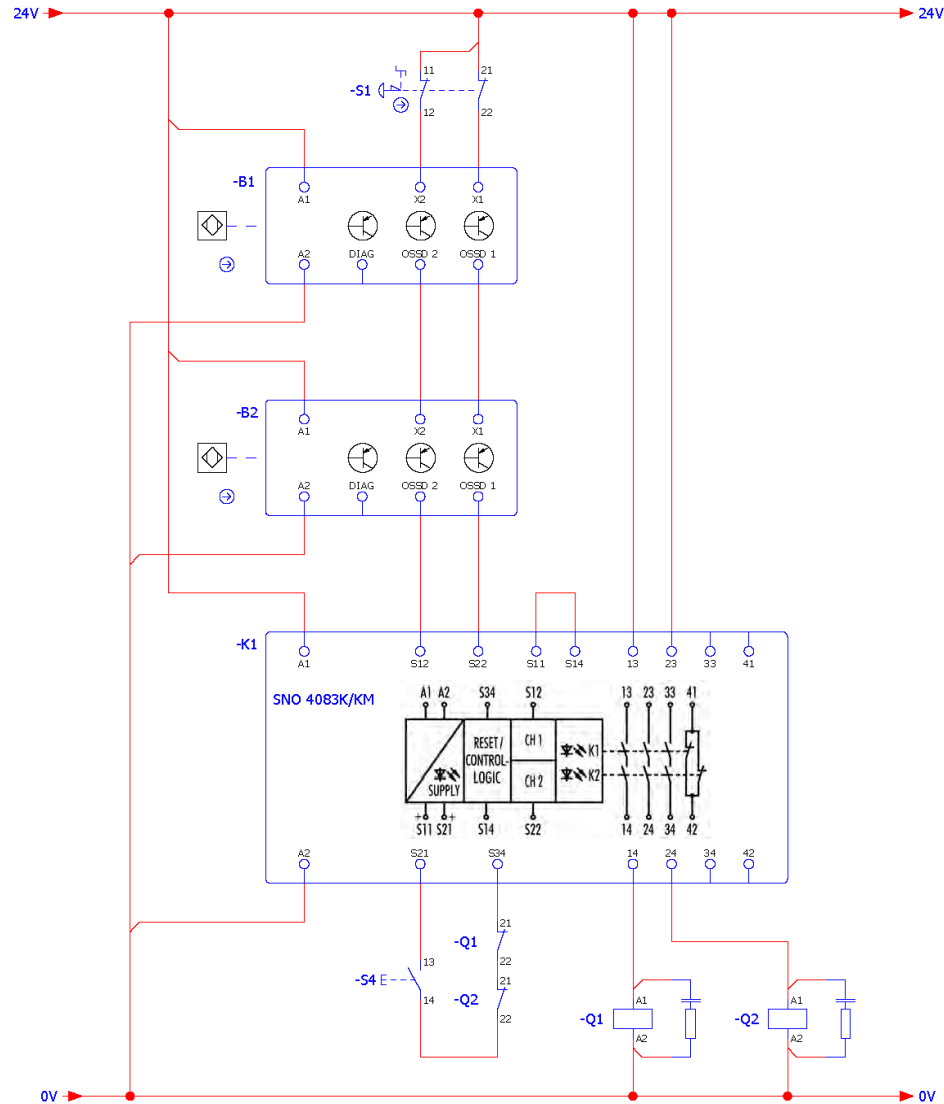
## 3.25.5 Modelling in accordance with EN ISO 13849-1



# Safety functions

Door switch, RFID & E-Stop in series (2) – E-Stop in PL e

## 3.25.6 Circuit diagram



### 3.26 Door switch, RFID & E-Stop in series (2) – Doors in PL e

#### 3.26.1 Safety function (of the doors)

<b>Safety function</b>	By opening the door(s), all the drives of the system are stopped / de-energised.
<b>Trigger event</b>	Opening of one or more doors by the operator.
<b>Reaction</b>	De-energising of the drives.
<b>Safe state</b>	Drives are de-energised.



#### 3.26.2 Description

<b>Function</b>	<p>By opening the door(s):</p> <ul style="list-style-type: none"><li>• the door switch(s) is/are activated</li><li>• the OSSD contacts of –B1 open</li><li>• the input circuit on door switch –B2 is interrupted</li><li>• the OSSD contacts of –B2 open</li><li>• the input circuit on safety switchgear –K1 is interrupted</li><li>• the safety contacts of –K1 open</li><li>• the contactors –Q1 and –Q2 drop out</li><li>• the machine M1 is stopped</li></ul>
<b>Manual reset</b>	The manual reset of the safety function occurs by closing the door(s). The door switch(es) (–B1, –B2) is/are closed. The design ensures that the door(s) cannot close accidentally.
<b>Restart</b>	<p>The restart function occurs by closing the door(s). A restart may only be possible if:</p> <ul style="list-style-type: none"><li>• the doors are closed</li></ul> <p>It is not possible to step behind the doors due to the design.</p>

### 3.26.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• All the door sensors are self-monitoring.</li> <li>• All the sensors have OSSD outputs.</li> <li>• Cross-circuits between OSSD output signals are detected by the sensor and lead to the safe state of both OSSD outputs in the event of a fault.</li> <li>• Short-circuits of the OSSD outputs against 24V or GND are detected by safety switchgear –K1 or the respective series-connected door sensor using cross comparison.</li> <li>• As all the faults can be individually diagnosed, fault masking can be excluded. DC = 99% (cross comparison and high-performance fault detection) can be assumed for all the sensors.</li> <li>• It should be noted that the switching times of all the door sensors are added to the respective series-connected door sensor in the sequence (here –B1).</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• Due to the separate triggering of –Q1 and –Q2 as well as the high-performance diagnostics through reading back of the contacts, it is possible to dispense with protected installation of the cable between –K1 and –Q1 / –Q2.</li> <li>• The contactors have positively-driven feedback contacts.</li> <li>• Direct monitoring (e.g. electric position monitoring of the control valves, monitoring of electromechanical units through positively-driven operation) by –K1. DC = 99%.</li> </ul>

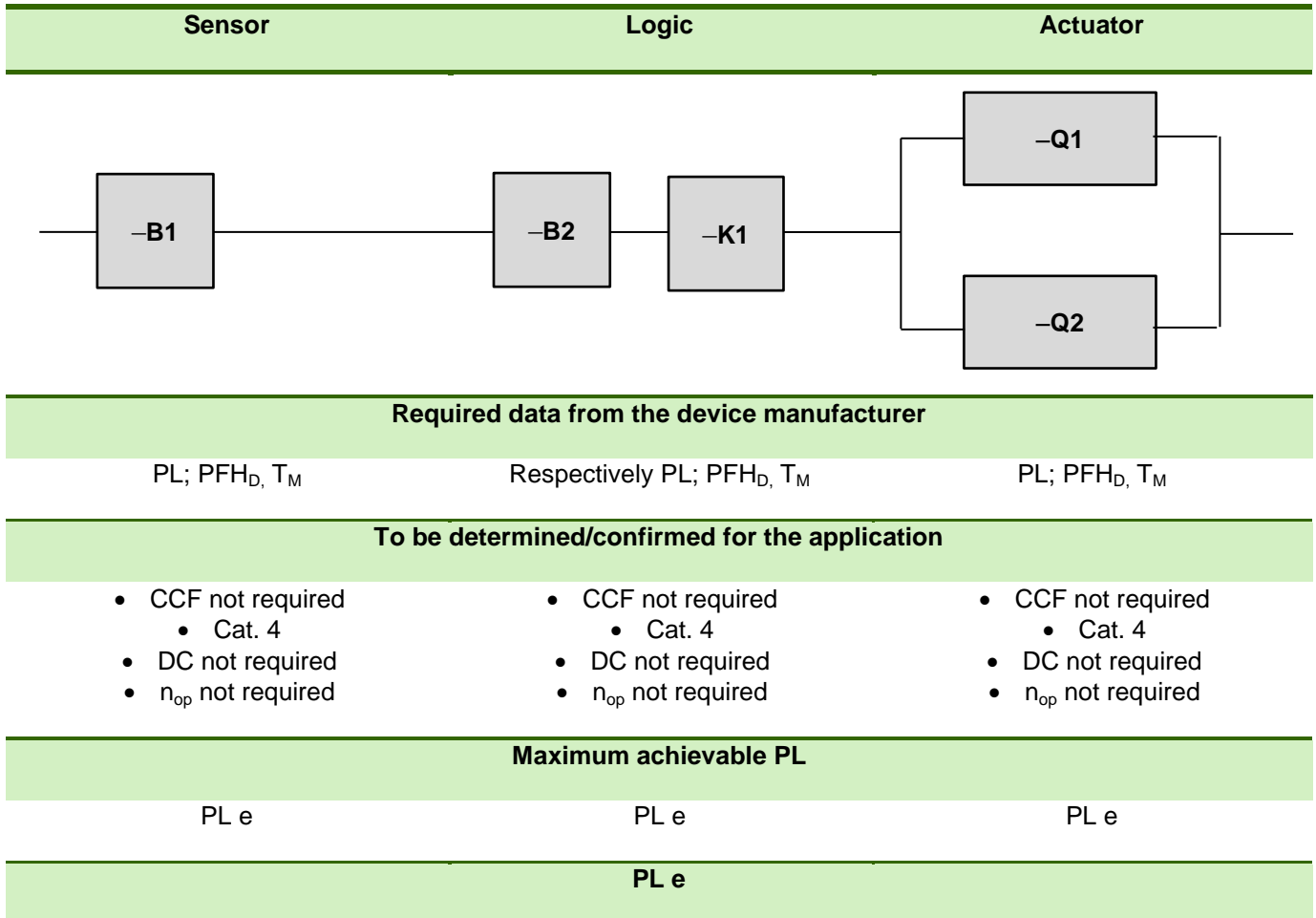
### 3.26.4 Products (options)

		Product
–B1; –B2		Interlocking device type 4 (door switch in RFID technology) <b>sensor</b> PRO: STS01xx Order number: R1.400.0110.0
–K1		Safety switchgear <b>safe</b> RELAY: SNO 4083KM Order number: R1.188.3580.0
–T1	Frequency converter with integrated diagnostics and evaluation as PL e. Integrated STO safety function.	

# Safety functions

Door switch, RFID & E-Stop in series (2) – Doors in PL e

## 3.26.5 Modelling in accordance with EN ISO 13849-1

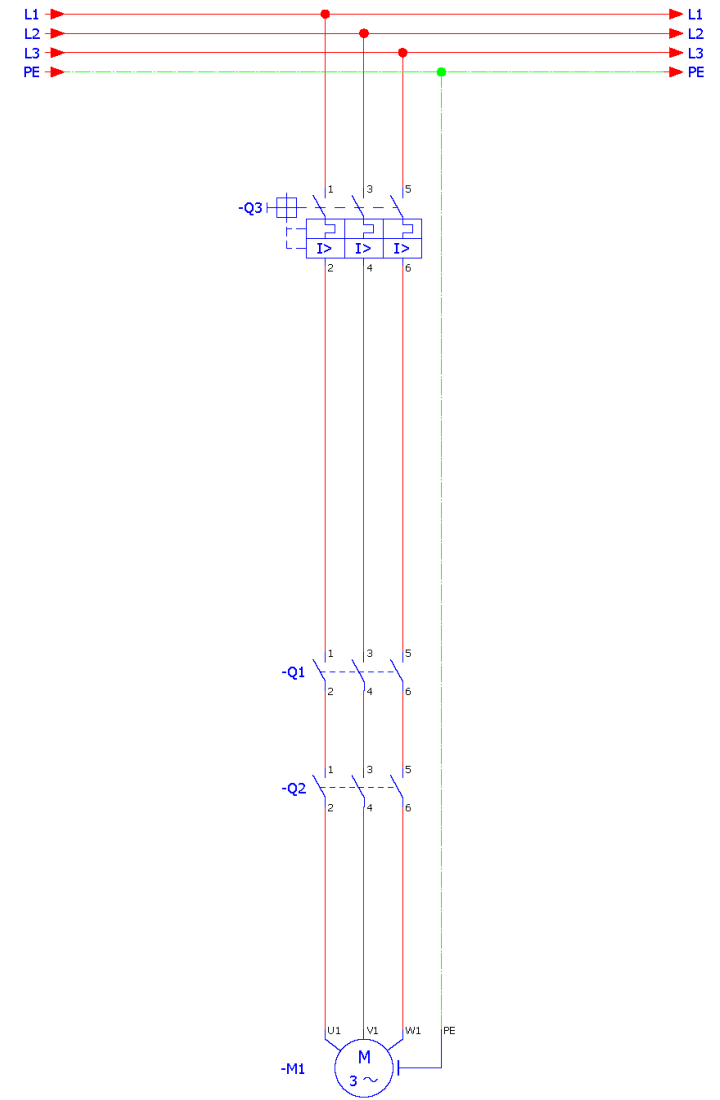
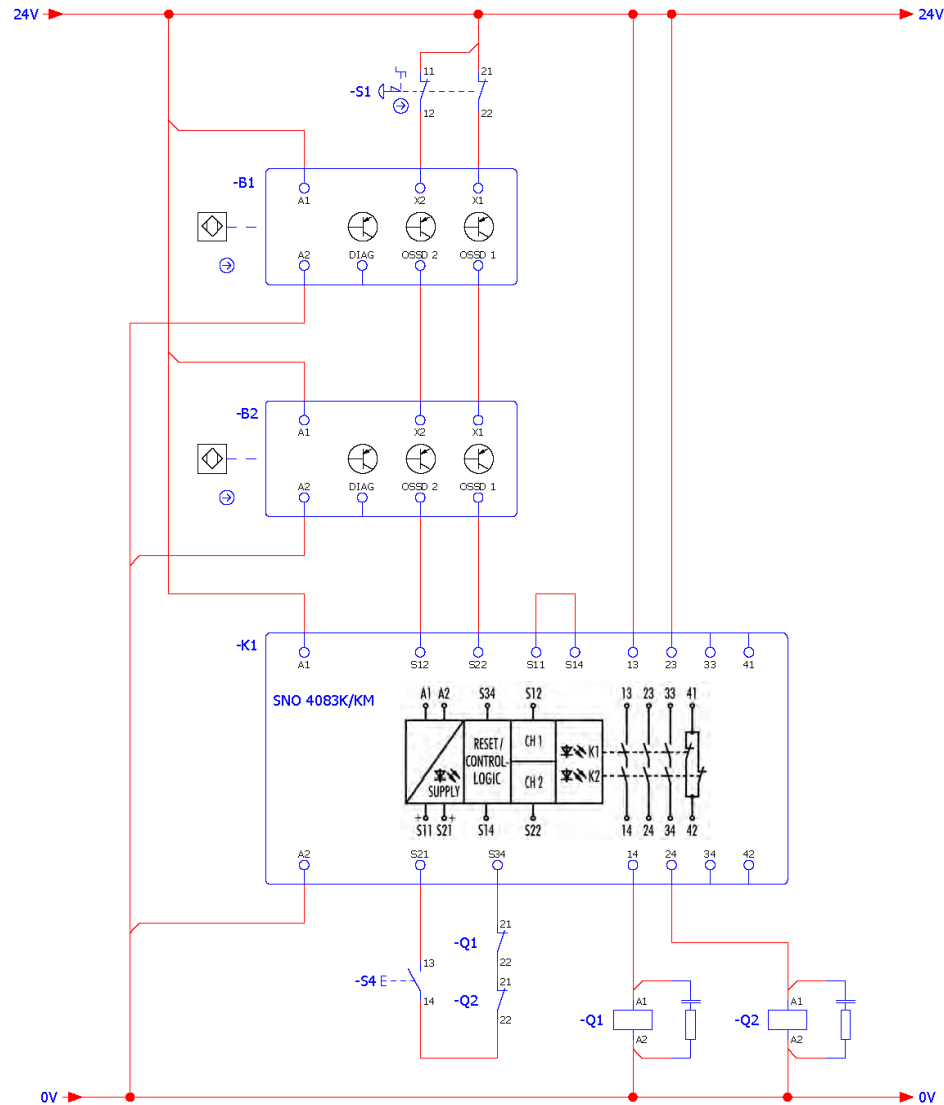


**Note:** *The determination applies to sensor –B1. For sensor –B2, the modelling is shortened by –B1. As the modelling shown represents the worst case, it is assumed for all the sensors.*

# Safety functions

Door switch, RFID & E-Stop in series (2) – Doors in PL e

## 3.26.6 Circuit diagram



### 3.27 Mode selector in PL e

#### 3.27.1 Safety function

<b>Safety function</b>	By operating the mode selector –S1, it is possible to toggle between operating modes.
<b>Trigger event</b>	Operating of the mode selector –S1 by the operator.
<b>Reaction</b>	Change of operating mode.
<b>Safe state</b>	The following two options represent safe states: <ul style="list-style-type: none"><li>• the operating mode displayed on the mode selector is active and all other operating modes are inactive</li><li>• drives are de-energised</li></ul>

**Note:** *The mode selector could also be considered in all the safety functions with which it interacts. This however makes the consideration of the respective safety functions more complex. A separate safety function has therefore been implemented.*

**Warning:** *It must be noted that the PL<sub>r</sub> of this safety function is depending on the PL<sub>r</sub> of the dependent safety functions. In particular, if the change of operating mode is coupled with specific competencies or abilities or if not all the dependent safety functions have the same PL<sub>r</sub>, it is obvious that the PL<sub>r</sub> for this safety function should follow the highest PL<sub>r</sub> of the safety functions involved.*

#### 3.27.2 Description


<b>Function</b>	By operating the mode selector –S1: <ul style="list-style-type: none"><li>• precisely one input circuit on safety switchgear –K1 is closed and all the others are interrupted simultaneously</li><li>• the internal evaluation in –K1 checks for plausibility</li><li>• the operating mode associated with the switch position is activated</li><li>• if a fault is detected, the frequency converter –T1 is stopped via STO_A and STO_B</li></ul>
<b>Manual reset</b>	Not required
<b>Restart</b>	Not required
<b>Feedback circuit</b>	Not required here as –T1 is a device with integrated diagnostics.



### 3.27.3 Safety review

<b>Sensors</b>	<ul style="list-style-type: none"> <li>• Earth faults, cross-circuits and short-circuits against 24V in the input circuit are detected by test pulses on the sensor cables by –K1.</li> <li>• The software checks that always precisely one input is linked with the clock output. If it is detected that no input is linked with clock outputs or if several inputs are linked with the clock output, this is evaluated as an error.</li> <li>• The 1 from the N circuit corresponds to the structure of category 4 as the requirement complies with Cat. 4:</li> <li>• Each single fault is detected at the latest on request and does not lead of a loss of safety.</li> <li>• Fault accumulations do not lead to the loss of safety.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li> </ul>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• The frequency converter –T1 is a pre-certified safety module with integrated diagnostics.</li> <li>• A feedback circuit is not required.</li> </ul>


### 3.27.4 Products (options)

	Product
–S1	Mode selector <ul style="list-style-type: none"> <li>• Lockable in any position</li> <li>• Display of the switch position</li> <li>• Only precisely one output contact is linked with the root contact</li> </ul>
–K1	 Programmable safety controller <b>samos</b> PRO: SP-COP2 Order number: R1.190.1310.0
–T1	Frequency converter with integrated diagnostics and evaluation as PL e. Integrated STO safety function.

# Safety functions

Mode selector in PL e

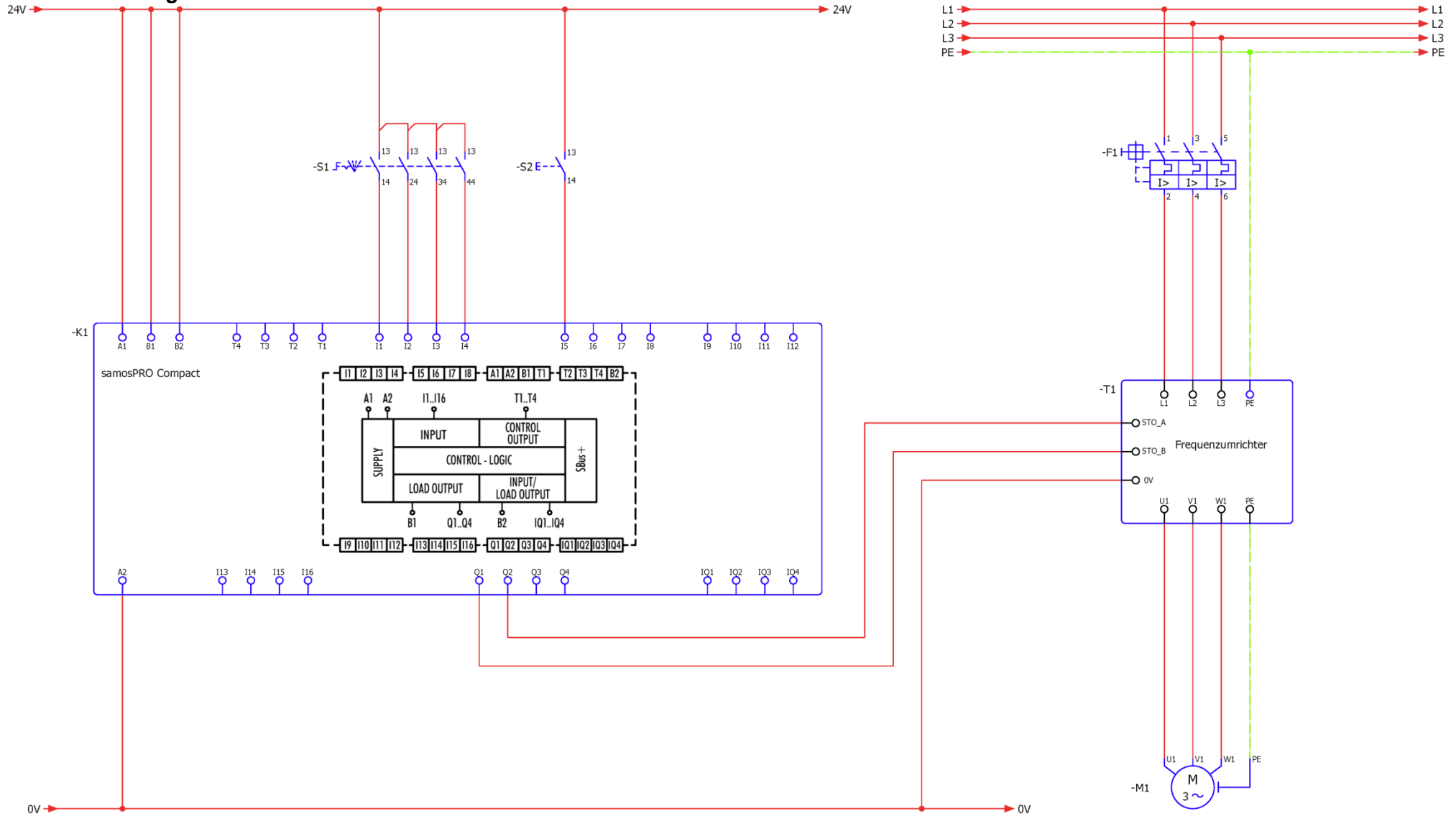
## 3.27.5 Modelling in accordance with EN ISO 13849-1

Sensor	Logic	Actuator
		
Required data from the device manufacturer		
$B_{10D}; T_M$	PL; PFH <sub>D</sub> , $T_M$	$B_{10D}; T_M$
To be determined/confirmed for the application		
<ul style="list-style-type: none"> <li>• CCF <math>\geq</math> 65 points               <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC = 99%               <ul style="list-style-type: none"> <li>• <math>n_{op}</math></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• CCF not required               <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC not required</li> <li>• <math>n_{op}</math> not required</li> </ul>	<ul style="list-style-type: none"> <li>• CCF <math>\geq</math> 65 points               <ul style="list-style-type: none"> <li>• Cat. 4</li> </ul> </li> <li>• DC = 99%               <ul style="list-style-type: none"> <li>• <math>n_{op}</math></li> </ul> </li> </ul>
Maximum achievable PL		
PL e	PL e	PL e
PL e		

# Safety functions

## Mode selector in PL e

### 3.27.6 Circuit diagram



### 3.28 Enabling button in PL e

#### 3.28.1 Safety function

<b>Safety function</b>	<p>When safety door –B1 is opened and the enabling button –S1 is pressed simultaneously, the safely reduced speed of the drive is monitored.</p> <p>The safe state is achieved if the drive moves at maximum with reduced speed or if the drive is stationary when there is no enabling.</p>
<b>Trigger event</b>	Pressing the enabling button when the door is simultaneously opened.
<b>Reaction</b>	Activation of the SLS safety function in the drive and monitoring for reduced speed.
<b>Safe state</b>	<p>Limitation of the traverse speed of the drive to <math>v_{max}=250</math> mm/s (take the appropriate value from the associated C type standard).</p> <p>De-energising of the drive in the event of a fault.</p>



#### 3.28.2 Description

Function	Doors	Enabling button	Mode	STO (–K1:Q2)	SLS (–K1:Q1)
	Closed	Not pressed or panic (fully depressed)	Automatic	ON	ON
	Closed	Enabling	Emergency stop	OFF	OFF
	Opened	Not pressed or panic (fully depressed)	STO	OFF	OFF
	Opened	Enabling	SLS	ON	OFF
<b>Manual reset</b>	<p>The manual reset of the safety function occurs by</p> <ul style="list-style-type: none"> <li>releasing the enabling button –S1 and</li> <li>closing the door(s) and</li> <li>subsequent operation of –S2 (edge monitoring by closing the doors)</li> <li>The manual reset may only be possible if –S1 is not pressed</li> <li>The design ensures that the door cannot close accidentally</li> </ul>				
<b>Restart</b>	<p>The restart function occurs by pressing switch –S2 (again). A restart may only be possible if:</p> <ul style="list-style-type: none"> <li>the doors are closed</li> </ul>				
<b>Feedback circuit</b>	Not required here as –T1 is a device with integrated diagnostics.				

### 3.28.3 Safety review

<b>Sensors</b>	<p>Door switch –B1 and enabling button –S1</p> <ul style="list-style-type: none"> <li>• Earth circuits, cross-circuits and short-circuits against 24V in the input circuit are detected by test pulses on the sensor cables by –K1.</li> <li>• Diagnostics using “Cross comparison with dynamisation and high-performance fault detection” by –K1. DC = 99%.</li> </ul> <p>If the enabling button is pressed when the door is closed (middle position), this is interpreted as a fault and the safe state is initiated.</p>
<b>Actuators</b>	<ul style="list-style-type: none"> <li>• The frequency converter –T1 is a pre-certified safety module with integrated diagnostics.</li> <li>• A feedback circuit is not required.</li> <li>• Fault exclusion on the cabling between –K1 and –T1 as there is fixed wiring within the switch cabinet.</li> </ul>

### 3.28.4 Products (options)

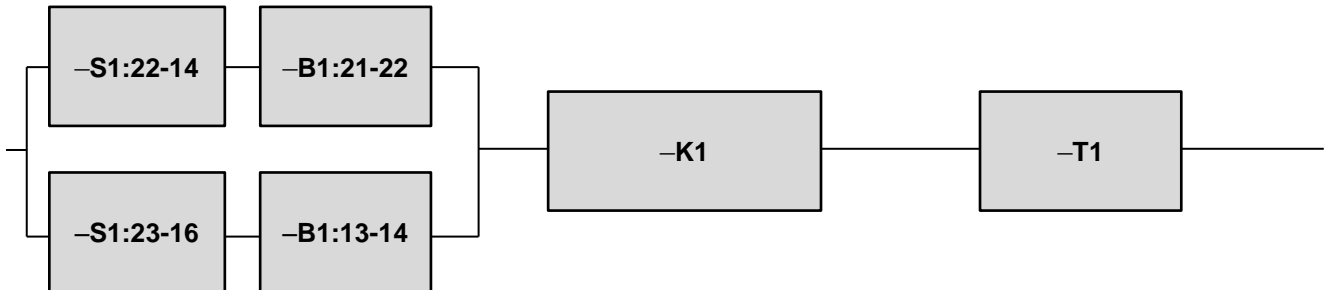
Product	
<b>–B1</b> 	<p>Interlocking device type 3 (door switch with magnetic operation)  <b>samos</b> PRO: SMA01xx                      Order number: R1.100.0113.0</p>
<b>–S1</b>	<p>Enabling button with 3 switch positions.</p> <ul style="list-style-type: none"> <li>• direct opening action of the contact element from middle position to fully depressed position</li> <li>• Self-resetting from the middle position to the deactivated position</li> <li>• Suitable for the expected switching load and frequency</li> <li>• Manufacturer specification of <math>B_{10D}</math> and <math>T_M</math></li> </ul>
<b>–K1</b> 	<p>Programmable safety controller  <b>samos</b> PRO: SP-COP2                      Order number: R1.190.1310.0</p>
<b>–T1</b>	<p>Frequency converter with integrated diagnostics and evaluation as PL e.                      Integrated STO and SLS safety functions.</p>

# Safety functions

Enabling button in PL e

## 3.28.5 Modelling in accordance with EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------



Required data from the device manufacturer		
--	--	--

Respectively  $B_{10D}$ ;  $T_M$

PL;  $PFH_D$ ,  $T_M$

PL;  $PFH_D$ ,  $T_M$

To be determined/confirmed for the application		
--	--	--

- CCF  $\geq$  65 points
  - Cat. 4
- DC = 99%
  - $n_{op}$

- CCF not required
  - Cat. 4
- DC not required
- $n_{op}$  not required

- CCF not required
  - Cat. 4
- DC not required
- $n_{op}$  not required

Maximum achievable PL		
-----------------------	--	--

PL e

PL e

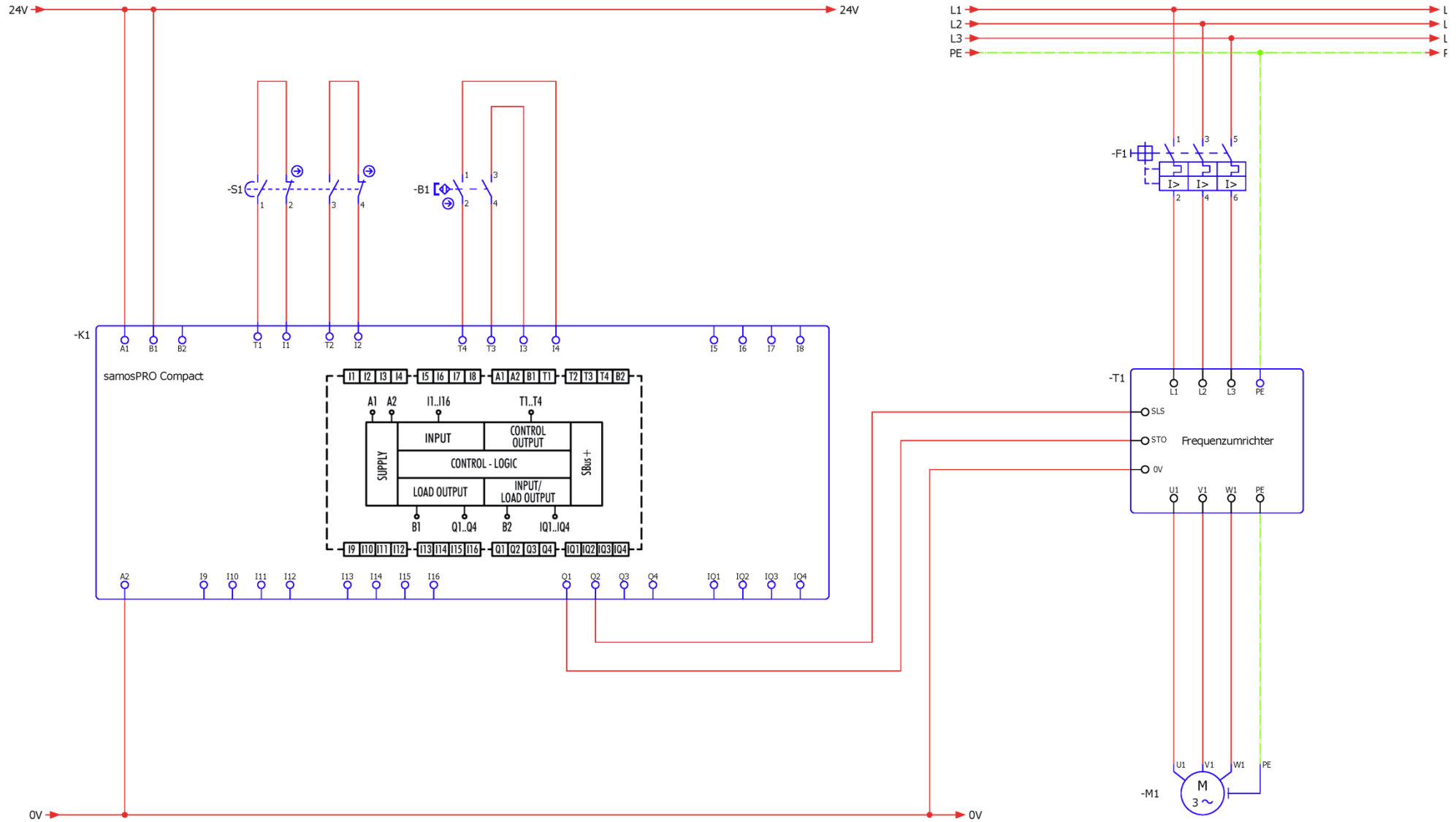
PL e

PL e
------

# Safety functions

Enabling button in PL e

## 3.28.6 Circuit diagram



### 3.29 Door guard with interlocklocking in PL d

#### 3.29.1 Safety function

<b>Safety function</b>	Access to the installation through the movable guard is prevented by an interlocking device with guard locking until the actuators are de-energised and the risk has been sufficiently reduced.
<b>Trigger event</b>	Request for the starting of drive –M1 by the operator by pressing the start button –S2.  <i>Note: The stop function is irrelevant here as movement is the hazard.</i>
<b>Reaction</b>	Guard locking is active.
<b>Safe state</b>	While the drive is running (STO not requested) plus overtravel time $t_{\text{overtravel}}$ , the guard locking is active.

#### 3.29.2 Description



<b>Function</b>	<p>As long as the stopping of the motor –M1 via the operator is not requested via start button –S2:</p> <ul style="list-style-type: none"> <li>• output –K1:Q1 may be switched on (STO not active)</li> <li>• enabling of guard locking –A1 is deactivated via –K1:Q2</li> <li>• guard locking is guaranteed via spring in –A1</li> </ul> <p>Request for the activation by the operator using stop button –S1:</p> <ul style="list-style-type: none"> <li>• opening of the input circuit –K1:I2 for stop request</li> <li>• request for STO function on –T1 using –K1:Q1</li> <li>• start of the time delay <math>t_{\text{overtravel}}</math></li> <li>• activation of –A1 after elapse of <math>t_{\text{overtravel}}</math></li> </ul> <p>Request for the starting of the motor by the operator via start button –S2:</p> <ul style="list-style-type: none"> <li>• closing of the input circuit –K1:I2 for start request</li> <li>• removal of the activation for –A1.1</li> <li>• reading back via –A1:2 or –A1 in the guard locking position</li> <li>• if –A1 in the guard locking position</li> <li>• removal of –K1:Q1 (no more STO request)</li> </ul>
<b>Manual reset</b>	<p>The manual reset of the safety function:</p> <ul style="list-style-type: none"> <li>• occurs by closing the door</li> <li>• removes the activation of –A1.1 via –K1:Q2</li> </ul> <p>The design ensures that it is not possible to step behind the light curtain/grid.</p>
<b>Restart</b>	<p>The restart function occurs either by pressing –S2 or with the manual reset. A restart may only be possible if:</p> <ul style="list-style-type: none"> <li>• the guard locking is confirmed via –A1.2</li> </ul>
<b>Feedback circuit</b>	Not required as –T1 is a device with integrated diagnostics.



### 3.29.3 Safety review

<b>Sensors</b>	The request of the safety function occurs via a logic function in –K1 and can be triggered by any input signal. Here –S1 (stop) and –S2 (start). As the release of –A1 is only possible when the drive is in the safe state, the trigger signal is irrelevant.
<b>Actuators</b>	<p>Required assurances by the manufacturer:</p> <ul style="list-style-type: none"> <li>• A fault exclusion is assumed for the failure of the spring according to EN ISO 13849-2 A.5 (well-tried spring).</li> </ul> <p>Considerations by the machine builder:</p> <ul style="list-style-type: none"> <li>• Due to sufficient dimensioning, a fault exclusion is made for the failure of the bolt. Plausibility is given if used according to the manufacturer's specifications.</li> <li>• The guard locking is a spring-loaded lock which is released by an electromagnet. This electromagnet is controlled by the PLC in PL e.</li> <li>• A fault exclusion is further assumed for the release of the guard locking with no power applied.</li> <li>• The wiring of the cable is assumed as protected from the output of the PLC and thus a fault exclusion is assumed for a short-circuit against 24V.</li> <li>• Due to the numerous fault exclusions, the PL is limited to maximum PL d.</li> </ul> <p>Other:</p> <ul style="list-style-type: none"> <li>• See also EN ISO 14119 G.3.2</li> <li>• If all the points above are met, a mathematical consideration of the guard locking is not required.</li> </ul>

### 3.29.4 Products (options)

	Product
<b>–K1</b> 	Programmable safety controller <b>samos</b> PRO: SP-COP2 Order number: R1.190.1310.0
<b>–A1</b> 	Interlocking device type 2 (door switch with separate actuating element) and spring-loaded guard locking <b>sensor</b> PRO: SIN11xx Order number: R1.310.1150.0  Required assurances by the manufacturer: <ul style="list-style-type: none"> <li>• Well-tried spring according to EN ISO 13849-2 A.5.</li> <li>• During proper use, a fault exclusion is made on the failure of the bolt due to sufficient dimensioning.</li> </ul>

# Safety functions

## Door guard with interlocklocking in PL d

### 3.29.5 Modelling in accordance with EN ISO 13849-1

Sensor	Logic	Actuator
--------	-------	----------



#### Required data from the device manufacturer

omitted	PL; PFH <sub>D</sub> , T <sub>M</sub>	<ul style="list-style-type: none"> <li>Fault exclusion on failure of the actuating element during proper use</li> <li>Use of a well-tried spring</li> </ul>
---------	---------------------------------------	---

#### To be determined/confirmed for the application

omitted	<ul style="list-style-type: none"> <li>CCF not required               <ul style="list-style-type: none"> <li>Cat. 4</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>	<ul style="list-style-type: none"> <li>CCF at least 65 points               <ul style="list-style-type: none"> <li>Cat. 2</li> </ul> </li> <li>DC not required</li> <li>n<sub>op</sub> not required</li> </ul>
---------	--	--

#### Maximum achievable PL

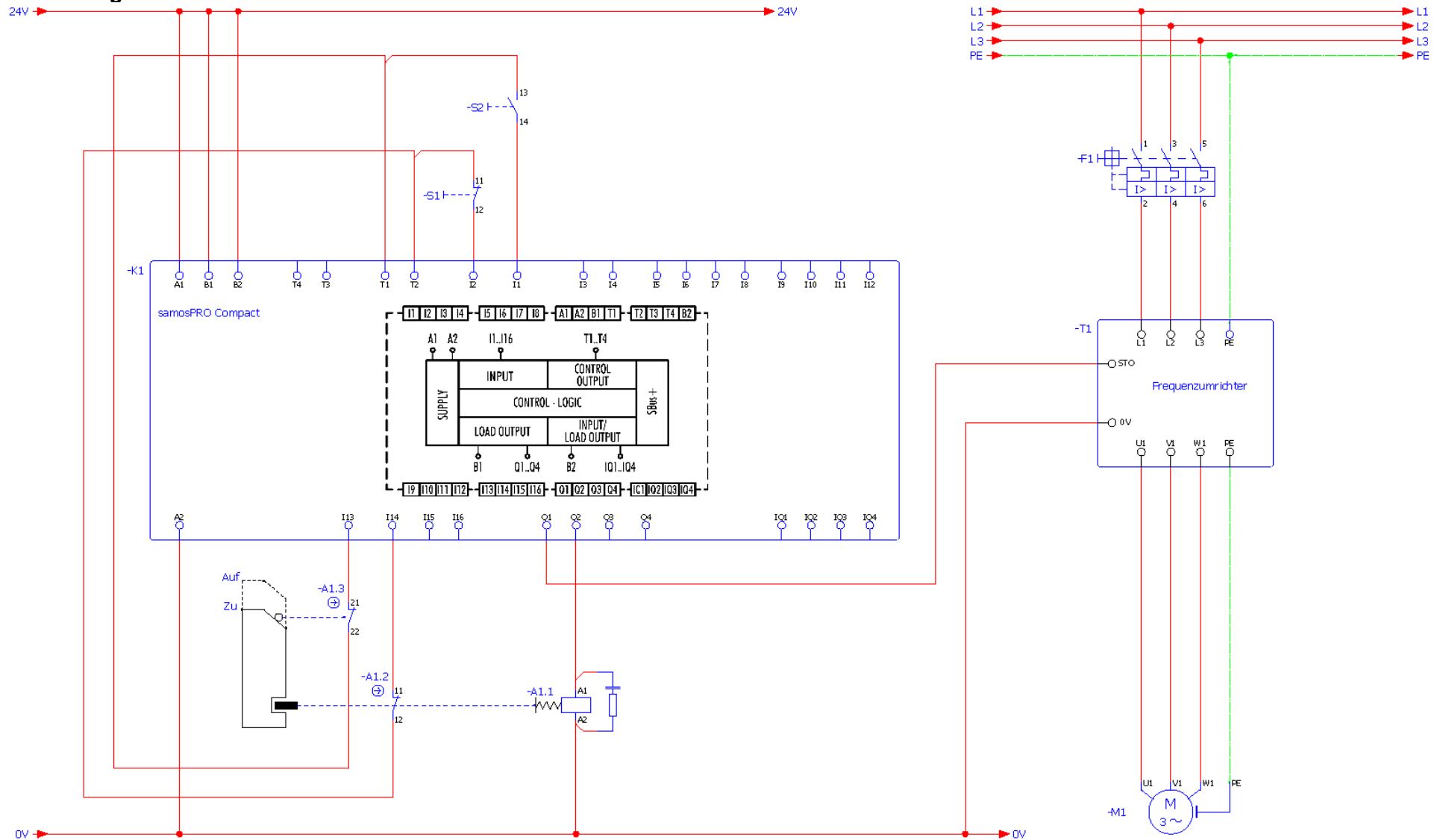
omitted	PL e	PL d
---------	------	------

#### PL d

# Safety functions

Door guard with interlocking in PL d

## 3.29.6 Circuit diagram



### 4 Terms

#### 4.1 Doors and other protective equipment

##### 4.1.1 Separating guards, non separating guards or protective devices fixing location of operators

Separating guards (e.g. doors or flaps) should be selected when there is a risk that the hazard also has an external effect such as in the case of radiation or the risk of ejected parts. Otherwise non-separating protective equipment (e.g. light grid, light curtain) or devices fixing the operator location (e.g. two-hand control device) can be used.

##### 4.1.2 Position monitoring or guard locking

In principle, a distinction is made between two safety functions for access: position monitoring (interlock) and guard lockings. Guard lockings are able to prevent access without a corresponding release (i.e. by locking the doors). The position monitoring only reports the position of the doors (opened or closed).

##### 4.1.3 Coded switches

The use of so-called coded switches has no direct influence on the functional safety. Since EN ISO 14119, the topic has however been explicitly seen as an aspect of manipulation.

The term coding refers to the “number of possible keys” and is divided into 4 levels in accordance with EN ISO 14119.

In most cases, a low coding level (1-9 codes) is ensured for magnetic (type 2) and mechanical (type 1) door switches according to EN ISO 14119. As a consequence, they should be installed so they are covered or inaccessible. Only with a high level of coding can a non-detachable fixing of the actuating element be seen as sufficient to prevent manipulation.

##### 4.1.4 Mechanical position switches

Mechanical position switches are mainly fitted with two electrical contacts and one actuator tongue. Here is the most frequent user error as these switches are used as Cat. 3 or 4 for applications according to PL d or PL e. This is generally speaking an incorrect usage. The reason for this lies in the structure of the switches themselves. They have a mechanical (single-channel) actuator tongue. The tongue activates a (single-channel) plunger in the switch which operates two mechanical contacts. The system thus consists of 3 elements, of which 2 are designed as single-channel.

For use in PL d or PL e, Cat. 3 or 4 would generally be necessary. This requires a complete two-channel system or a fault exclusion on the single-channel components. In the case of the actuator tongue, this can be carried out if necessary by the user, as the user can make this fault exclusion himself with the appropriate installation and environmental conditions (avoidance of corrosion, dirt,...). As regards the internal plunger, this can only be carried out by the manufacturer of the switch. The author is not aware of any manufacturer who would be able to confirm a mechanical fault exclusion for their switch. The direct opening action of the contact element of all mechanical door switches is however confirmed (according to EN ISO 14119).

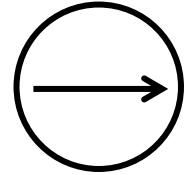
As a consequence, an individual mechanical door switch with direct opening action of the contacts can only be used as Cat.1 up to PL c without further evidence. If a fault exclusion for the actuator tongue is made by the user and documented accordingly, the positive driving of the internal plunger is interpreted as a fault exclusion so that this can lead to a complete mechanical fault exclusion. As a result, the door switch can be used up to Cat. 3, PL d. The restriction to PL d lies in the usual interpretation of the inspection bodies that a PL e cannot be permitted for a single-channel system with a fault exclusion (see 4.3).

### 4.1.5 Series connection of door switches

It has long been known that fault masking can occur when interlinking door switches in series. This is the masking of an error in a switch through an inappropriate work process or by the acknowledgement of a fault in a defective switch through the operation of a functional switch. The standard ISO/TR 24119 describes the problem in detail. The fault masking on the series of door switches is mentioned in particular and the possible diagnostic coverage (DC) is defined as a consequence. See also Chapter 4.4.

### 4.1.6 Direct opening action of a contact element and positively-driven operation

If a movable, mechanical component positively moves another element with it, either through direct contact or through rigid elements, it is called a positively-driven operation. A contact element is directly opened if opening of the switch contacts is carried out immediately by a defined movement of the actuating element through non-elastic elements. Many safety sensors are provided with the symbol for direct opening. It should always be ensured that the hazardous action is signalled with a positive operation and direct opening e.g. the opening of a safety door.



### 4.1.7 NC/NC contact or NC/NO contact or NO/NO contact

The discussion regarding which of the switching principles in two-channel switches is better or safer can be summed up clearly with the statement "It doesn't matter".

There are ultimately two safety principles:

1. Diversity
2. Closed-circuit principle (the de-energised state is the safe state)

In the case of the solution with NC/NO contact, the principle of diversity (1x NC contact; 1x NO contact) comes into effect. In the case of the solution with NC/NC contact and NO/NO contact, the closed-circuit principle is used for both contacts. Both are technically equivalent.

The predominantly interesting fact about the switch is dependent on the type of installation, namely whether the switch is in the active or idle state, provided that the door is closed. It is dependent on whether the positive opening of the switch can have an effect. The aim is to install the switch so that the switch can be positively opened with the opening of the doors.

### 4.1.8 Muting lamp

To clarify whether a muting lamp is required on a light grid or light curtain, a risk assessment is necessary in principle. The standards EN/IEC 61496-1 to 3, EN/IEC 62046 as well as EN ISO 13849-1 name the requirements for this. In the case that the following 3 prerequisites are met, it is possible to dispense with a signal lamp as no additional risks are generated by the muting:

1. ESPE has a muting status signal (on the device) and
2. In the case of muting, the transported material is muted (and not by the carrier or the palette) and
3. The transported material completely prevents access to the hazardous area as long as it is muted.

In all other cases, there can be a necessity for an indicator light. However, even if the risk assessment results in the necessity for an indicator light, the display of the muting function can be interpreted as a request to bypass the protective device in line with foreseeable misuse. Consideration of these two risks can result in a muting light being dispensed with despite a positive result of the risk assessment, if the possible misuse is assessed as the greater risk. In this case, it is advisable to have conclusive proof that points 1 to 3 of the above list are not technically feasible.

### 4.2 Reset or restart

EN ISO 13849-1 makes a distinction for actions or states after the initiation of a stop command and before the restart between:

1. Manual reset function – EN ISO 13849-1, Chap. 5.2.2)
2. Start/restart function – EN ISO 13849-1, Chap. 5.2.3)

The following section explains which of the two functions must be used on a case-by-case basis.

#### 4.2.1 Manual reset and/or restart function?

In general, it should be noted in each individual case that the requirements for the manual reset function and the restart function of the product or C type standards should be observed. They can deviate from the general requirements that are named in the following section.

Example	Stepping behind		Manual reset function	Restart function
	Possible	Safe-guarded <sup>1</sup>		
Emergency stop	-	-	According to EN ISO 13850, the action of the manual reset lies in the release of the emergency stop.	Always required
Separating guard <sup>2</sup>	No	-	If it can be assumed that a hazardous situation will not arise when the doors are locked, it is possible to dispense with a manual reset.	Always required  The restart function can be triggered by the protective device itself (controlling function) provided that the requirements from EN ISO 12100 Chap.6.3.3.2.5 have been met.
Optical protective device <sup>3</sup>	No		If it can be assumed that a hazardous situation will not arise when the protective device is activated, it is possible to dispense with a manual reset.	Always required  The restart function can be triggered by the protective device itself (controlling function) provided that the requirements from EN ISO 12100 Chap.6.3.2.5.3 have been met.
Separating guard <sup>2</sup>	Yes	Yes	If no hazardous situation is assumed when the safety function is requested with protection against access from behind and locked doors, it is possible to dispense with a manual reset in both safety functions.	Always required  The restart function can be triggered by the protective device itself (controlling function) provided that the requirements from EN ISO 12100 Chap.6.3.3.2.5 have been met.
Optical protective device <sup>3</sup>	Yes	Yes	If it can be assumed that a hazardous situation will not arise when the safety function is restored, it is possible to dispense with a manual reset.	Always required  The restart function can be triggered by the protective device itself (controlling function) provided that the requirements from EN ISO 12100 Chap.6.3.2.5.3 have been met.

Example	Stepping behind		Manual reset function	Restart function
	Possible	Safe-guarded <sup>1</sup>		
Separating guard <sup>2</sup> or optical <sup>3</sup> protective device	Yes	No	A manual reset is required in general	Always required

**1** Separate safety function prevents person stepping behind e.g. safety mat, light curtain/grid or scanner

**2** e.g. safety door

**3** e.g. light curtain/grid or scanner

### 4.3 Fault exclusions

If a fault exclusion is made on a component, it no longer appears in the safety review in the following section. This far-reaching consequence requires careful documentation and justification. In EN ISO 13849-2, there are comprehensive lists with possible fault exclusions and the associated requirements. In principle, fault exclusions can be carried out by a component manufacturer or the machine builder themselves. If a fault exclusion is made by the component manufacturer, this fault exclusion is required in written form, ideally within the scope of the product documentation. The reason for this is the technical and legal responsibility for the validity of the statements which otherwise falls back on the machine builder. If the safety function has a single-channel structure and a fault exclusion is made on one of the single-channel elements, the achievable PL is limited to PL d.

### 4.4 Fault masking

Fault masking is an effect which can occur when several devices share a common mechanism for their diagnostic function (see ISO/TR 24119). It can occur that functional devices can mask faults in non-functional devices. In most cases, this is supported by unsuitable process sequences or by the limited diagnostics possibilities of the diagnosis channel.

If fault masking takes place, the capability of the system to detect faults is limited or completely lost. It is usual that the DC must be set to NONE, even in cases when otherwise a DC = HIGH can be used. Consequently, the achievable category and the achievable PL are limited.

The most frequent case is two-channel structures, usually with redundant, potential-free contacts which are switched in series (see 3.19). The diagnosis is carried out by a safety controller in most cases.

### 4.4.1 Variants

Emergency stop	Door switch with potential free contacts	Further sensors	Additional requirements	Note	Max DC [%]	Max PL	Chapter
2+	0	0		The operation of more than one emergency stop must not be expected. Fault masking should therefore not be expected.	99	e	3.17
1+	1+	0		The operation of an emergency stop while a door or a sensor is operated must be expected. Fault masking should therefore be expected.	0	c	3.19
1+	0	1+					
0	2+	0		Dependent on the frequency of operation and number of door switches. See Chapter 4.4.2 and ISO/TR 24119,	0 to 90	c or d	3.20
0	1+	1+	It is ensured through the process that only the sensor or doors are operated at any time.	Fault masking is prevented by the process.	90	d	
Otherwise			Provided that the following requirements are met: <ul style="list-style-type: none"> <li>It is ensured through additional diagnosis (e.g. a third contact and suitable diagnosis that only one sensor/door is operated.</li> <li>The operation of more than one sensor/door switch/emergency stop is evaluated as a fault.</li> <li>All sensors must then be checked individually for the correct function before the process can be continued.</li> </ul>	If the diagnosis is carried out by a non-safety PLC, the diagnosis is part of the safety function. A validation of this diagnosis is part of the validation process of the safety function. In addition, all the changes in the standard PLC software must be evaluated with respect to the influence on diagnosis. The re-validation of the safety function is required.	99	e	
			Otherwise	Fault masking must be assumed.	0	c	

**Table 1: Combinations of sensors and the resulting DC**



### 4.4.2 Series connection of doors – ISO/TR 24119

The ISO/TR 24119 restricts the DC dependent on:

- number of doors
- signal type
- frequency of the operation
- cabling principle
- layout of the switches
- process

The following table displays the simplified approach and the achievable DC level. The standard limits the achievable PL in every case to PL d, even if a higher PL could be achieved based on the DC:

Number of frequently operated doors <sup>1,2</sup>		Number of additional doors <sup>3</sup>	Maximum achievable DC <sup>4</sup>
0	+	2 to 4	medium
		5 to 30	low
		≥ 31	none
1	+	1	medium
		2 to 4	low
		≥ 5	none
≥ 2	+	≥ 1	none

**1** If the frequency is higher than 1x per hour

**2** If more than one operator is able to open doors independently of each other, the “Number of frequently operated doors” must be increased by one

**3** The “Number of additional doors” may be reduced by one if

- the minimum distance between two doors is 5 m or
- if none of the additional doors can be accessed directly

**4** In every case, as far as it is foreseeable that fault masking will occur (e.g. doors are opened simultaneously), the DC must be set to NONE

**Table 2: Simplified DC table from ISO/TR 24119**

## Fault masking

### 4.4.3 Direct fault masking

Figure 5 shows the process of fault masking when a fault in switch B1 is not detected by K1 as it is masked by the functioning switch B2.

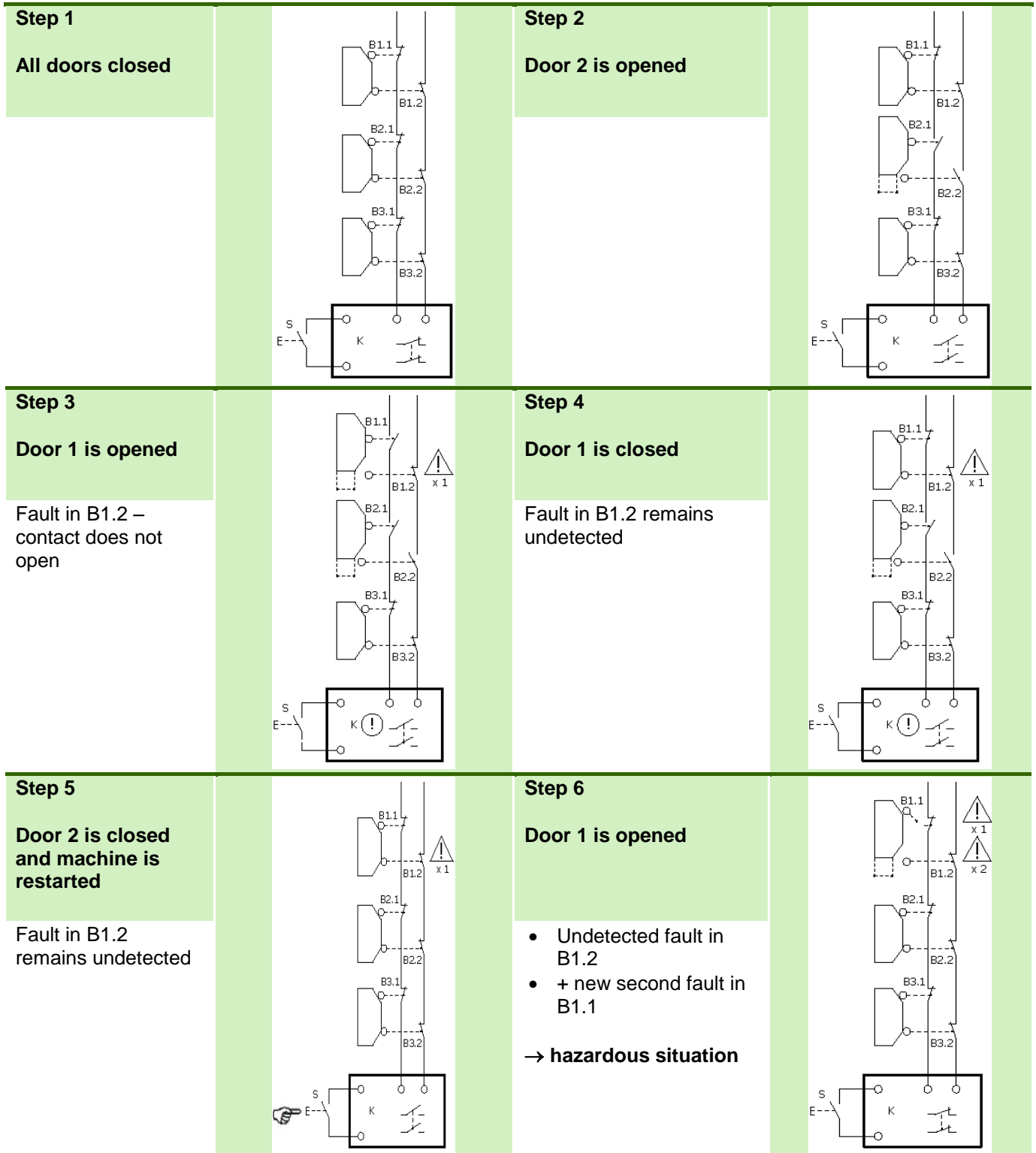


Figure 5: Direct fault masking according to ISO/TR 24119

### 5 Tables & formulae

#### 5.1 Symbols

Symbol	Unit	Meaning
$\beta$	%	Susceptibility to common cause failures
$B_{10}$	-	Number of switching cycles until 10% of the components fail
$B_{10D}$	-	Number of switching cycles until 10% of the components fail dangerously
$C$	1/h	Operating cycles per hour (see also $n_{op}$ )
CCF	-	Common cause failure. 0 to 100 points can be achieved
DC	%	Diagnostic coverage
$DC_{avg}$	%	Average diagnostic coverage (of a subsystem)
$d_{op}$	d/a	Operating days per year
FIT	1/h	Faults in $10^9$ hours
HFT	-	Hardware fault tolerance
$h_{op}$	h/d	Operating hours per day
$\lambda$	1/h	Rate of all failures per hour (= $1/MTTF$ in hours)
$\lambda_D$	1/h	Rate of dangerous failures per hour (= $1/MTTF_D$ in hours)
$\lambda_{DD}$	1/h	Rate of detected dangerous failures per hour
$\lambda_{DU}$	1/h	Rate of undetected dangerous failures per hour
$\lambda_S$	1/h	Rate of safe failures per hour
MTBF	a	Mean time between two failures in years
MTTF	a	Mean time to failure in years (according to Weibull, 62.3% of the devices have failed. See EN/IEC 61810-2)
$MTTF_D$	a	Mean time to dangerous failure in years (according to Weibull, 62.3% of the devices have failed dangerously. See EN/IEC 61810-2)
$n_{op}$	1/a	Switching cycles per year
PFH	1/h	Probability of a dangerous failure per hour (EN/IEC 61508)
$PFH_D$	1/h	Probability of a dangerous failure per hour (EN/IEC 62061 and EN ISO 13849-1)
PL	-	Performance level

## Symbols

Symbol	Unit	Meaning
$PL_r$	-	Required performance level
$P_{TE}$	1/h	Probability of a transmission error in communication (EN/IEC 62061)
RDF	%	Fraction of dangerous failures (VDMA 66413)
SFF	%	Safe failure function (EN/IEC 62061)
SIL	-	Required safety integrity level (EN/IEC 61508 and EN/IEC 62061)
SILCL	-	Safety integrity level claim of a safety function or subsystem (EN/IEC 61508 and EN/IEC 62061)
SRCF		Safety-related control function (corresponds to safety function in EN/IEC 62061)
SRP/CS		Safety-related part of a control system (corresponds to safety function in EN ISO 13849-1)
$T_1$	h or a	Proof test interval. Watch out for the unit! ( $T_1$ corresponds to an "as new" test interval, which usually not feasible, and can therefore be compared to $T_M$ )
$T_2$	h	Diagnosis test interval (this is mostly an automated and frequently repeated test)
$T_{10D}$	a	Operating time in years (after this period, the number of permitted switching cycles is applied for components with mechanical wear)
$T_M$	a	Service life in years (see also $T_1$ )
$t_{\text{cycle}}$	s	Interval between two operations in seconds

## Determination of PL

### 5.2 Determination of PL

#### 5.2.1 Formulae

The validity or usability of formulae is frequently limited to elements, subsystems or the safety function in its entirety. An implementation outside the intended range of application can lead to invalid results.

Formula	Comment	Element	Subsystem	Safety function
$B_{10D} = B_{10}$	Worst-case estimate	X		
$B_{10D} = 2 * B_{10}$	For electronics	X		
$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{cycle}} \cdot 3600 \frac{s}{h}$	Operating frequency	X		
$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}}$		X		
$T_{10D} = \frac{B_{10D}}{n_{op}}$	If $T_{10D} < 20$ years, a note should be made in the manual! $T_{10D}$ is only required for devices with $B_{10}$ or $B_{10D}$	X		
$MTTF_D = MTTF$	Worst-case estimate	X	X	
$MTTF_D = 2 * MTTF$	For electronics (see EN ISO 13849-1 C.5.1)	X	X	
$MTTF = \frac{1}{\lambda} \cong MTBF$	If repair time is negligible (a few days)	X		
$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}}$		X	X	
$MTTF_{D,Ci} = \frac{1}{\sum_{i=1}^n \frac{1}{MTTF_{D,i}}}$	Per channel		X	
$MTTF_{D,tot} = \frac{2}{3} \left[ MTTF_{D,C1} + MTTF_{D,C2} - \frac{1}{\frac{1}{MTTF_{D,C1}} + \frac{1}{MTTF_{D,C2}}} \right]$	Limit values before symmetrisation to 100 (Cat. B to Cat. 3) or 2500 (Cat. 4) years.		X	

## Determination of PL

Formula	Comment	Element	Subsystem	Safety function
$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D,1}} + \frac{DC_2}{MTTF_{D,2}} + \dots + \frac{DC_n}{MTTF_{D,n}}}{\frac{1}{MTTF_{D,1}} + \frac{1}{MTTF_{D,2}} + \dots + \frac{1}{MTTF_{D,n}}}$	Applies to one or two channels. No limit of $MTTF_D$ required		X	
$PFH_D = \sum_i PFH_{D,i}$				X
$PL_{tot} \leq \min_i PL_i$	Requirement for safety function			X
$PL_r \leq PL_{tot}$	Requirement for safety function			X

### 5.2.2 Category requirements

Characteristic	Category				
	B	1	2	3	4
Design must be able to withstand the expected influences according to applicable standards	X	X	X	X	X
Basic safety principle	X	X	X	X	X
Well-tries safety principles		X	X	X	X
Well-tries components		X			
Mean time to dangerous failure – $MTTF_D$	Low to medium	High	Low to high		High
Fault detection (tech.)			X	X	X
Single fault does not lead to hazardous situation				X	X
Consideration of fault accumulation					X
Diagnostic coverage level – $DC_{avg}$	None		Low to medium		High
Measures against CCF			X	X	X
Mainly characterised by	Selection of components		Structure		

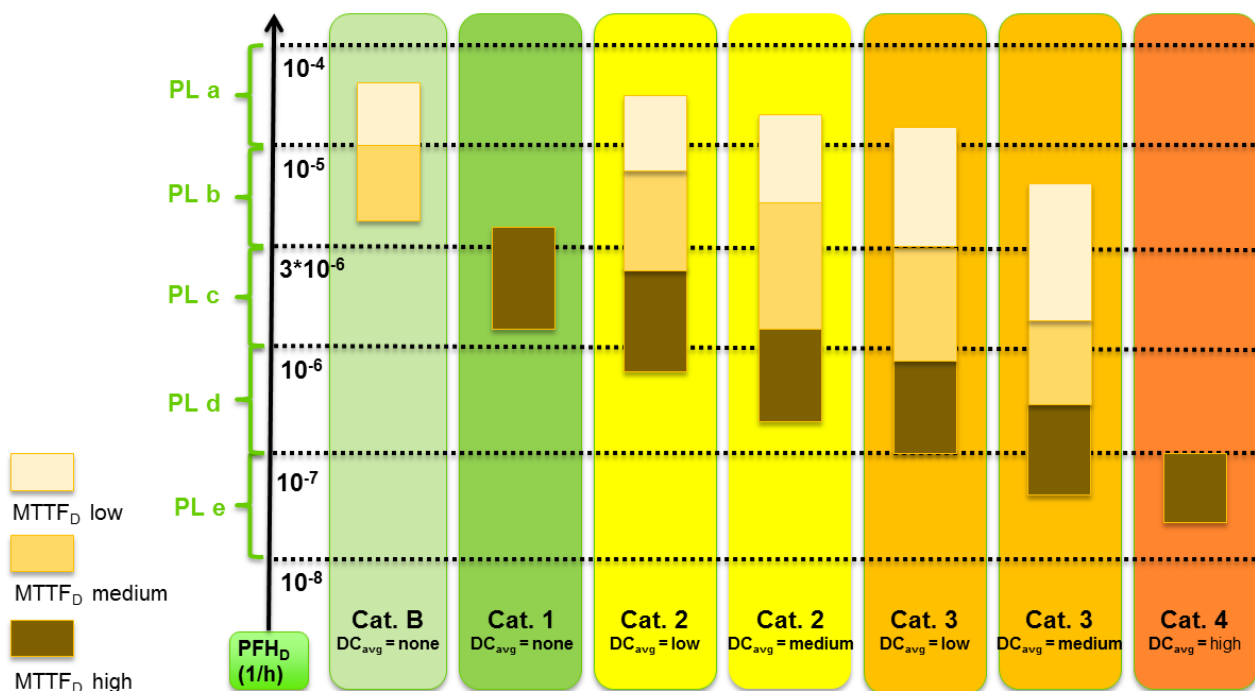
### 5.2.3 Minimum requirements for PFH<sub>D</sub> (EN ISO 13849-1 Table 3)

PL <sub>total</sub>	PFH <sub>D</sub>
A	$10^{-5} \leq PFH_D < 10^{-4}$
B	$10^{-6} \leq PFH_D < 10^{-5}$
C	$10^{-6} \leq PFH_D < 3 * 10^{-6}$
D	$10^{-7} \leq PFH_D < 10^{-6}$
E	$10^{-8} < PFH_D < 10^{-7}$

### 5.2.4 DC ranges (EN ISO 13849-1 Table 5)

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

### 5.2.5 Bar graph (EN ISO 13849-1 Figure 5)



For the detailed table of the correlations, see EN ISO 13849-1 Annex K

**5.2.6 EN ISO 13849-1 Annex K**

MTTF <sub>D</sub>	PFH <sub>D</sub> (1/h) and associated performance level (PL)													
	Cat. B DC <sub>avg</sub> = none		Cat. 1 DC <sub>avg</sub> = none		Cat. 2 DC <sub>avg</sub> = low		Cat. 2 DC <sub>avg</sub> = medium		Cat. 3 DC <sub>avg</sub> = low		Cat. 3 DC <sub>avg</sub> = medium		Cat. 4 DC <sub>avg</sub> = high	
	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL
3.0	3.80 x 10 <sup>-5</sup>	a			2.58 x 10 <sup>-5</sup>	a	1.99 x 10 <sup>-5</sup>	a	1.26 x 10 <sup>-5</sup>	a	6.09 x 10 <sup>-6</sup>	b		
3.3	3.46 x 10 <sup>-5</sup>	a			2.33 x 10 <sup>-5</sup>	a	1.79 x 10 <sup>-5</sup>	a	1.13 x 10 <sup>-5</sup>	a	5.41 x 10 <sup>-6</sup>	b		
3.6	3.17 x 10 <sup>-5</sup>	a			2.13 x 10 <sup>-5</sup>	a	1.62 x 10 <sup>-5</sup>	a	1.03 x 10 <sup>-5</sup>	a	4.86 x 10 <sup>-6</sup>	b		
3.9	2.93 x 10 <sup>-5</sup>	a			1.95 x 10 <sup>-5</sup>	a	1.48 x 10 <sup>-5</sup>	a	9.37 x 10 <sup>-6</sup>	b	4.40 x 10 <sup>-6</sup>	b		
4.3	2.65 x 10 <sup>-5</sup>	a			1.76 x 10 <sup>-5</sup>	a	1.33 x 10 <sup>-5</sup>	a	8.39 x 10 <sup>-6</sup>	b	3.89 x 10 <sup>-6</sup>	b		
4.7	2.43 x 10 <sup>-5</sup>	a			1.60 x 10 <sup>-5</sup>	a	1.20 x 10 <sup>-5</sup>	a	7.58 x 10 <sup>-6</sup>	b	3.48 x 10 <sup>-6</sup>	b		
5.1	2.24 x 10 <sup>-5</sup>	a			1.47 x 10 <sup>-5</sup>	a	1.10 x 10 <sup>-5</sup>	a	6.91 x 10 <sup>-6</sup>	b	3.15 x 10 <sup>-6</sup>	b		
5.6	2.04 x 10 <sup>-5</sup>	a			1.33 x 10 <sup>-5</sup>	a	9.87 x 10 <sup>-6</sup>	b	6.21 x 10 <sup>-6</sup>	b	2.80 x 10 <sup>-6</sup>	c		
6.2	1.84 x 10 <sup>-5</sup>	a			1.19 x 10 <sup>-5</sup>	a	8.80 x 10 <sup>-6</sup>	b	5.53 x 10 <sup>-6</sup>	b	2.47 x 10 <sup>-6</sup>	c		
6.8	1.68 x 10 <sup>-5</sup>	a			1.08 x 10 <sup>-5</sup>	a	7.93 x 10 <sup>-6</sup>	b	4.98 x 10 <sup>-6</sup>	b	2.20 x 10 <sup>-6</sup>	c		
7.5	1.52 x 10 <sup>-5</sup>	a			9.75 x 10 <sup>-6</sup>	b	7.10 x 10 <sup>-6</sup>	b	4.45 x 10 <sup>-6</sup>	b	1.95 x 10 <sup>-6</sup>	c		
8.2	1.39 x 10 <sup>-5</sup>	a			8.87 x 10 <sup>-6</sup>	b	6.43 x 10 <sup>-6</sup>	b	4.02 x 10 <sup>-6</sup>	b	1.74 x 10 <sup>-6</sup>	c		
9.1	1.25 x 10 <sup>-5</sup>	a			7.94 x 10 <sup>-6</sup>	b	5.71 x 10 <sup>-6</sup>	b	3.57 x 10 <sup>-6</sup>	b	1.53 x 10 <sup>-6</sup>	c		
10	1.14 x 10 <sup>-5</sup>	a			7.18 x 10 <sup>-6</sup>	b	5.14 x 10 <sup>-6</sup>	b	3.21 x 10 <sup>-6</sup>	b	1.36 x 10 <sup>-6</sup>	c		
11	1.04 x 10 <sup>-5</sup>	a			6.44 x 10 <sup>-6</sup>	b	4.53 x 10 <sup>-6</sup>	b	2.81 x 10 <sup>-6</sup>	c	1.18 x 10 <sup>-6</sup>	c		
12	9.51 x 10 <sup>-6</sup>	b			5.84 x 10 <sup>-6</sup>	b	4.04 x 10 <sup>-6</sup>	b	2.49 x 10 <sup>-6</sup>	c	1.04 x 10 <sup>-6</sup>	c		
13	8.78 x 10 <sup>-6</sup>	b			5.33 x 10 <sup>-6</sup>	b	3.64 x 10 <sup>-6</sup>	b	2.23 x 10 <sup>-6</sup>	c	9.21 x 10 <sup>-7</sup>	d		
15	7.61 x 10 <sup>-6</sup>	b			4.53 x 10 <sup>-6</sup>	b	3.01 x 10 <sup>-6</sup>	b	1.82 x 10 <sup>-6</sup>	c	7.44 x 10 <sup>-7</sup>	d		
16	7.13 x 10 <sup>-6</sup>	b			4.21 x 10 <sup>-6</sup>	b	2.77 x 10 <sup>-6</sup>	c	1.67 x 10 <sup>-6</sup>	c	6.76 x 10 <sup>-7</sup>	d		
18	6.34 x 10 <sup>-6</sup>	b			3.68 x 10 <sup>-6</sup>	b	2.37 x 10 <sup>-6</sup>	c	1.14 x 10 <sup>-6</sup>	c	5.67 x 10 <sup>-7</sup>	d		
20	5.71 x 10 <sup>-6</sup>	b			3.26 x 10 <sup>-6</sup>	b	2.06 x 10 <sup>-6</sup>	c	1.22 x 10 <sup>-6</sup>	c	4.85 x 10 <sup>-7</sup>	d		
22	5.19 x 10 <sup>-6</sup>	b			2.93 x 10 <sup>-6</sup>	c	1.82 x 10 <sup>-6</sup>	c	1.07 x 10 <sup>-6</sup>	c	4.21 x 10 <sup>-7</sup>	d		
24	4.76 x 10 <sup>-6</sup>	b			2.65 x 10 <sup>-6</sup>	c	1.62 x 10 <sup>-6</sup>	c	9.47 x 10 <sup>-7</sup>	d	3.70 x 10 <sup>-7</sup>	d		
27	4.23 x 10 <sup>-6</sup>	b			2.32 x 10 <sup>-6</sup>	c	1.39 x 10 <sup>-6</sup>	c	8.04 x 10 <sup>-7</sup>	d	3.10 x 10 <sup>-7</sup>	d		
30	4.23 x 10 <sup>-6</sup>	b	3.80 x 10 <sup>-6</sup>	b	2.06 x 10 <sup>-6</sup>	c	1.21 x 10 <sup>-6</sup>	c	6.94 x 10 <sup>-7</sup>	d	2.65 x 10 <sup>-7</sup>	d	9.54 x 10 <sup>-8</sup>	e



# Tables & formulae

## Determination of PL

MTTF <sub>D</sub>	PFH <sub>D</sub> (1/h) and associated performance level (PL)													
	Cat. B DC <sub>avg</sub> = none		Cat. 1 DC <sub>avg</sub> = none		Cat. 2 DC <sub>avg</sub> = low		Cat. 2 DC <sub>avg</sub> = medium		Cat. 3 DC <sub>avg</sub> = low		Cat. 3 DC <sub>avg</sub> = medium		Cat. 4 DC <sub>avg</sub> = high	
	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL
33	4.23 x 10 <sup>-6</sup>	b	3.46 x 10 <sup>-6</sup>	b	1.85 x 10 <sup>-6</sup>	c	1.06 x 10 <sup>-6</sup>	c	5.97 x 10 <sup>-7</sup>	d	2.30 x 10 <sup>-7</sup>	d	8.57 x 10 <sup>-8</sup>	e
36	4.23 x 10 <sup>-6</sup>	b	3.17 x 10 <sup>-6</sup>	b	1.67 x 10 <sup>-6</sup>	c	9.39 x 10 <sup>-7</sup>	d	5.16 x 10 <sup>-7</sup>	d	2.01 x 10 <sup>-7</sup>	d	7.77 x 10 <sup>-8</sup>	e
39	4.23 x 10 <sup>-6</sup>	b	2.93 x 10 <sup>-6</sup>	c	1.53 x 10 <sup>-6</sup>	c	8.40 x 10 <sup>-7</sup>	d	4.53 x 10 <sup>-7</sup>	d	1.78 x 10 <sup>-7</sup>	d	7.11 x 10 <sup>-8</sup>	e
43	4.23 x 10 <sup>-6</sup>	b	2.65 x 10 <sup>-6</sup>	c	1.37 x 10 <sup>-6</sup>	c	7.34 x 10 <sup>-7</sup>	d	3.87 x 10 <sup>-7</sup>	d	1.54 x 10 <sup>-7</sup>	d	6.37 x 10 <sup>-8</sup>	e
47	4.23 x 10 <sup>-6</sup>	b	2.43 x 10 <sup>-6</sup>	c	1.24 x 10 <sup>-6</sup>	c	6.49 x 10 <sup>-7</sup>	d	3.35 x 10 <sup>-7</sup>	d	1.34 x 10 <sup>-7</sup>	d	5.76 x 10 <sup>-8</sup>	e
51	4.23 x 10 <sup>-6</sup>	b	2.24 x 10 <sup>-6</sup>	c	1.13 x 10 <sup>-6</sup>	c	5.80 x 10 <sup>-7</sup>	d	2.93 x 10 <sup>-7</sup>	d	1.19 x 10 <sup>-7</sup>	d	5.26 x 10 <sup>-8</sup>	e
56	4.23 x 10 <sup>-6</sup>	b	2.04 x 10 <sup>-6</sup>	c	1.02 x 10 <sup>-6</sup>	c	5.10 x 10 <sup>-7</sup>	d	2.52 x 10 <sup>-7</sup>	d	1.03 x 10 <sup>-7</sup>	d	4.73 x 10 <sup>-8</sup>	e
62	4.23 x 10 <sup>-6</sup>	b	1.84 x 10 <sup>-6</sup>	c	9.09 x 10 <sup>-7</sup>	d	4.43 x 10 <sup>-7</sup>	d	2.13 x 10 <sup>-7</sup>	d	8.84 x 10 <sup>-8</sup>	e	4.22 x 10 <sup>-8</sup>	e
68	4.23 x 10 <sup>-6</sup>	b	1.68 x 10 <sup>-6</sup>	c	8.17 x 10 <sup>-7</sup>	d	3.90 x 10 <sup>-7</sup>	d	1.84 x 10 <sup>-7</sup>	d	7.68 x 10 <sup>-8</sup>	e	3.80 x 10 <sup>-8</sup>	e
75	4.23 x 10 <sup>-6</sup>	b	1.52 x 10 <sup>-6</sup>	c	7.31 x 10 <sup>-7</sup>	d	3.40 x 10 <sup>-7</sup>	d	1.57 x 10 <sup>-7</sup>	d	6.62 x 10 <sup>-8</sup>	e	3.41 x 10 <sup>-8</sup>	e
82	4.23 x 10 <sup>-6</sup>	b	1.39 x 10 <sup>-6</sup>	c	6.64 x 10 <sup>-7</sup>	d	3.01 x 10 <sup>-7</sup>	d	1.35 x 10 <sup>-7</sup>	d	5.79 x 10 <sup>-8</sup>	e	3.08 x 10 <sup>-8</sup>	e
91	4.23 x 10 <sup>-6</sup>	b	1.25 x 10 <sup>-6</sup>	c	5.88 x 10 <sup>-7</sup>	d	2.61 x 10 <sup>-7</sup>	d	1.14 x 10 <sup>-7</sup>	d	4.94 x 10 <sup>-8</sup>	e	2.74 x 10 <sup>-8</sup>	e
100	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.47 x 10 <sup>-8</sup>	e
110	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.23 x 10 <sup>-8</sup>	e
120	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.03 x 10 <sup>-8</sup>	e
130	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.87 x 10 <sup>-8</sup>	e
150	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.61 x 10 <sup>-8</sup>	e
160	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.50 x 10 <sup>-8</sup>	e
180	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.33 x 10 <sup>-8</sup>	e
200	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.19 x 10 <sup>-8</sup>	e
220	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.08 x 10 <sup>-8</sup>	e
240	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	9.81 x 10 <sup>-9</sup>	e
270	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	8.67 x 10 <sup>-9</sup>	e
300	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	7.76 x 10 <sup>-9</sup>	e
330	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	7.04 x 10 <sup>-9</sup>	e

# Tables & formulae

## Determination of PL

MTTF <sub>D</sub>	PFH <sub>D</sub> (1/h) and associated performance level (PL)													
	Cat. B DC <sub>avg</sub> = none		Cat. 1 DC <sub>avg</sub> = none		Cat. 2 DC <sub>avg</sub> = low		Cat. 2 DC <sub>avg</sub> = medium		Cat. 3 DC <sub>avg</sub> = low		Cat. 3 DC <sub>avg</sub> = medium		Cat. 4 DC <sub>avg</sub> = high	
	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL	PFH <sub>D</sub>	PL
360	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	6.44 x 10 <sup>-9</sup>	e
390	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	5.94 x 10 <sup>-9</sup>	e
430	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	5.38 x 10 <sup>-9</sup>	e
470	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	4.91 x 10 <sup>-9</sup>	e
510	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	4.52 x 10 <sup>-9</sup>	e
560	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	4.11 x 10 <sup>-9</sup>	e
620	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	3.70 x 10 <sup>-9</sup>	e
680	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	3.37 x 10 <sup>-9</sup>	e
750	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	3.05 x 10 <sup>-9</sup>	e
820	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.79 x 10 <sup>-9</sup>	e
910	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.51 x 10 <sup>-9</sup>	e
1000	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.28 x 10 <sup>-9</sup>	e
1100	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	2.07 x 10 <sup>-9</sup>	e
1200	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.90 x 10 <sup>-9</sup>	e
1300	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.75 x 10 <sup>-9</sup>	e
1500	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.51 x 10 <sup>-9</sup>	e
1600	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.42 x 10 <sup>-9</sup>	e
1800	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.26 x 10 <sup>-9</sup>	e
2000	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.13 x 10 <sup>-9</sup>	e
2200	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	1.03 x 10 <sup>-9</sup>	e
2300	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	9.85 x 10 <sup>-10</sup>	e
2400	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	9.44 x 10 <sup>-10</sup>	e
2500	4.23 x 10 <sup>-6</sup>	b	1.14 x 10 <sup>-6</sup>	c	5.28 x 10 <sup>-7</sup>	d	2.29 x 10 <sup>-7</sup>	d	1.01 x 10 <sup>-7</sup>	d	4.29 x 10 <sup>-8</sup>	e	9.06 x 10 <sup>-10</sup>	e

**5.2.7 CCF table (EN ISO 13849-1 Table F.1)**

<b>Measure against CCF</b>		<b>Points</b>
<b>Separation Disconnection</b>	1. Physical separation between the signal paths e.g.: <ul style="list-style-type: none"> <li>• separation of the wiring/piping;</li> <li>• detection of short-circuits and interruptions in cables through dynamic testing;</li> <li>• separate screening of the signal path of each channel;</li> <li>• adequate creepage distances and clearances on printed circuits</li> </ul>	<b>15</b>
<b>Diversity</b>	2. Different technologies/design or physical principles are used e.g.: <ul style="list-style-type: none"> <li>• first channel in programmable electronics and second channel electromechanical hardwired,</li> <li>• different initiation of safety function for each channel e.g.</li> <li>• pressure and temperature,</li> <li>• measurement of distance and pressure,</li> <li>• digital and analogue,</li> <li>• components from different manufacturers.</li> </ul>	<b>20</b>
<b>Draft Application Experience</b>	3.1 Protection against overvoltage, excess pressure, overcurrent etc.	<b>15</b>
	3.2 Components used are well-tried.	<b>5</b>
<b>Assessment Analysis</b>	4. Have the results of the failure mode and effects analysis been taken into account in order to avoid failures developing due to a common cause?	<b>5</b>
<b>Competence Training</b>	5. Have designers/installers been trained to recognise the reasons and effects of common cause failures?	<b>5</b>
<b>Environment</b>	6.1 Protection against contamination and electromagnetic influence (EMC) against CCF in compliance with the proper standards.  Fluid systems:                      Filtering of the fluid medium, prevention of the ingress of dirt, water extraction from compressed air e.g. in compliance with the requirements of the manufacturer for the purity of the medium.  Electric systems:                      Has the system been tested as regards electromagnetic immunity e.g. relevant standards for CCF?  In the case of combined fluid and electric systems, both aspects should be taken into account.	<b>25</b>
	6.2 Other influences  Have all the requirements as regards insensitivity to all relevant environmental conditions such as temperature, shock, vibration, humidity (e.g. as defined in the relevant standards) been taken into account?	<b>10</b>
<b>Total CCF</b>	<b>Total number of points (<math>65 \leq CCF \leq 100</math>) required for Cat. 2 to Cat. 4. For each listed measure, only the full score or nothing can be claimed.</b>	

## DC measures

### 5.3 DC measures

#### 5.3.1 Input (EN ISO 13849-1 Table E.1)<sup>1</sup>

Measures for input	DC min	DC max	Comment
Cyclical testing/dynamisation	90%	90%	Periodic generation of a signal change with monitoring of the result
Plausibility test e.g. use of normally open and normally closed mechanically linked contacts	99%	99%	
Cross comparison <ul style="list-style-type: none"> <li>without dynamisation</li> </ul>	0%	99%	Manual initiation of the test
Cross comparison <ul style="list-style-type: none"> <li>with dynamisation</li> <li>without high-performance fault detection</li> </ul>	90%	90%	Comparison of inputs or outputs without short-circuit detection (for multiple inputs/outputs)
Cross comparison <ul style="list-style-type: none"> <li>with dynamisation</li> <li>with high-performance fault detection</li> </ul>	99%	99%	<ul style="list-style-type: none"> <li>Position detection of the slide valve</li> <li>Cross comparison of signals and intermediate values with short-circuit detection (for multiple inputs/outputs)</li> <li>Detection of static faults (e.g. with the help of safety modules) and timed and logic program monitoring</li> <li>Dynamic cross comparison of independent position or speed information</li> </ul>
Indirect monitoring (e.g. monitoring by pressure switch, electric position monitoring by drive elements)	90%	99%	<ul style="list-style-type: none"> <li>Position transducer or limit switch on the actuators instead of on the control elements</li> <li>Valve monitoring by pressure switch</li> </ul>
Direct monitoring (e.g. electric position monitoring of control valves, monitoring of electromechanical units through positively-driven operation)	99%	99%	<ul style="list-style-type: none"> <li>Position monitoring directly on the control element</li> <li>Position monitoring directly on the slide valve</li> <li>Position monitoring by positively-driven read back contacts (antivalent normally closed contacts)</li> <li>Signal monitoring through read back e.g. using optocouplers</li> </ul>
Fault detection through the process (e.g. FMEA, not sufficient for PL e)	0%	99%	Failure of the process control which is noticeable <ul style="list-style-type: none"> <li>through malfunction,</li> <li>damage of the work piece or machine parts,</li> <li>interruption or delay to the process,</li> </ul> without immediately representing a hazard.
Monitoring of properties	60%	60%	<ul style="list-style-type: none"> <li>Monitoring of response times, signal strengths of analogue signals (e.g. resistance, capacity)</li> </ul>

<sup>1</sup> *The wording and details vary between different local editions of ISO 13849-1. The above entries reflect a combination of several versions of the table.*

### 5.3.2 Logic (EN ISO 13849-1 Table E.1)<sup>2</sup>

Measures for logic	DC min	DC max	Comment
Indirect monitoring (e.g. monitoring by pressure switch, electric position monitoring by drive elements)	90%	99%	<ul style="list-style-type: none"> <li>Position transducer or limit switch on the actuators instead of on the control elements</li> </ul>
Direct monitoring (e.g. electric position monitoring of control valves, monitoring of electromechanical units through positively-driven operation)	99%	99%	<ul style="list-style-type: none"> <li>Signal monitoring through read back e.g. using optocouplers</li> </ul>
Fault detection through the process	0%	99%	<ul style="list-style-type: none"> <li>Failure of the process control which is noticeable through malfunction,</li> <li>damage of the work piece or machine parts,</li> <li>interruption or delay to the process,</li> <li>without immediately representing a hazard.</li> </ul>
Simple timed monitoring of the program run (e.g. timer as a watchdog with trigger signals in the logic program)	60%	60%	<ul style="list-style-type: none"> <li>Timer as watchdog with trigger signals in the logic program</li> </ul>
Timed and logic monitoring of the program run through a watchdog whereby the test equipment carries out a plausibility test of the logic response	90%	90%	<ul style="list-style-type: none"> <li>Through a watchdog, whereby the test equipment carries out a plausibility test of the logic response</li> </ul>
Self-test on startup to find hidden faults in parts of the logic (e.g. program and data memory, input/output connections, interfaces)	90%	90%	<ul style="list-style-type: none"> <li>Detection of hidden faults in the program and data memory,</li> <li>Input/output connections, interfaces</li> </ul>
Testing the possible reactions of the monitoring device e.g. watchdog) by the main channel after startup or whenever the safety function is required or whenever an external signal is requested by an input device	90%	90%	<ul style="list-style-type: none"> <li>Test of the possible reactions of the watchdog</li> </ul>
Dynamic principles (all logic modules require a status change ON-OFF-ON if the safety function is requested) e.g. interlocking circuits in relay technology	99%	99%	
Invariant memory: signature with single word length (8 bit)	90%	90%	

<sup>2</sup> *The wording and details vary between different local editions of ISO 13849-1. The above entries reflect a combination of several versions of the table.*

## DC measures

Measures for logic	DC min	DC max	Comment
Invariant memory: signature with double word length (16 bit)	99%	99%	
Variant memory: RAM test through use of redundant data e.g. flags, markers, constants, timers and cross comparison of this data	60%	60%	
Variant memory: test of the legibility and writability of the memory cells used	60%	60%	
Variant memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. "Galpat" or "Abraham")	99%	99%	
Processing unit: Self-test through software	60%	90%	
Processing unit: Coded processing	90%	99%	
Fault detection through the process (DC dependent on the application; this measure is alone sufficient for the required PL e)	0%	99%,	

### 5.3.3 Output (EN ISO 13849-1 Table E.1)<sup>3</sup>

Measures for output	DC min	DC max	Comment
Monitoring of the outputs by a channel without dynamic test	0%	99%	Dependent on how often a signal change is carried out by the application
Cross comparison <ul style="list-style-type: none"> <li>without dynamisation</li> </ul>	0%	99%	Manual initiation of the test
Cross comparison <ul style="list-style-type: none"> <li>with dynamisation</li> <li>without high-performance fault detection</li> </ul>	90%	90%	Comparison of inputs or outputs without short-circuit detection (for multiple inputs/outputs)
Cross comparison <ul style="list-style-type: none"> <li>with dynamisation</li> <li>with high-performance fault detection</li> </ul>	99%	99%	<ul style="list-style-type: none"> <li>Position detection of the slide valve</li> <li>Cross comparison of signals and intermediate values with short-circuit detection (for multiple inputs/outputs), detection of static faults (e.g. with the help of safety modules) and timed and logic program monitoring</li> </ul>
Indirect monitoring (e.g. monitoring by pressure switch, electric position monitoring by drive elements)	90%	99%	<ul style="list-style-type: none"> <li>Position transducer or limit switch on the actuators instead of on the control elements</li> <li>Valve monitoring by pressure switch</li> </ul>
Direct monitoring (e.g. electric position monitoring of control valves, monitoring of electromechanical units through positively-driven operation)	99%	99%	<ul style="list-style-type: none"> <li>Position monitoring directly on the control element</li> <li>Position monitoring directly on the slide valve</li> <li>Position monitoring by positively-driven read back contacts (antivalent normally closed contacts)</li> <li>Signal monitoring through read back e.g. using optocouplers</li> </ul>
Fault detection through the process (e.g. FMEA, not sufficient for PL e)	0%	99%	Failure of the process control which is noticeable through malfunction, damage of the work piece or machine parts, interruption or delay to the process, without immediately representing a hazard.
Redundant shutdown path <ul style="list-style-type: none"> <li>with monitoring of one of the actuators either by the logic or the test equipment</li> </ul>	99%	99%	

<sup>3</sup> The wording and details vary between different local editions of ISO 13849-1. The above entries reflect a combination of several versions of the table.

### 5.4 Safety principles

#### 5.4.1 Basic safety principles – Mechanical (EN ISO 13849-2 Table A.1)

Basic safety principle Mechanical	Comments
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature.
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, sticking, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply manufacturer's application notes, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components/systems.
Use of de-energization principle	<p>The safe state is obtained by a release of energy. See primary action for stopping in ISO 12100:2010, 6.2.11.3.</p> <p>Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3.</p> <p>Consider different modes, e.g. operation mode, maintenance mode.</p> <p><b>IMPORTANT</b> — This principle is not to be followed when loss of energy would create a hazard, e.g. release of workpiece caused by loss of clamping force.</p>
Proper fastening	For the application of screw locking, consider manufacturer's application notes. Overloading can be avoided and adequate resistance to release can be achieved by applying adequate torque loading technology.
Limitation of the generation and/or transmission of force and similar parameters	<p>Examples are break pin, break plate, and torque-limiting clutch.</p> <p><b>IMPORTANT</b> — This principle is not to be followed when the continued integrity of components is essential to maintain the required level of control.</p>
Limitation of range of environmental parameters	Examples are temperature, humidity and pollution at the installation place. See Clause 10 and consider manufacturer's application notes.
Limitation of speed and similar parameters	Consider, e.g. the speed, acceleration, deceleration required by the application.
Protection against unexpected start-up	<p>Consider unexpected start-up caused by stored energy and after power supply restoration for different modes (operation mode, maintenance mode, etc.).</p> <p>Special equipment for release of stored energy can be necessary.</p> <p>Special applications, e.g. to keep energy for clamping devices or ensure a position, need to be considered separately.</p>



## Safety principles

---

<b>Basic safety principle Mechanical</b>	<b>Comments</b>
Simplification	Avoid unnecessary components in the safety-related system.
Separation	Separation of safety-related functions from other functions.
Proper lubrication	Consider the need for lubrication devices, information on lubricants and lubrication intervals.
Proper prevention of the ingress of fluids and dust	Consider IP rating (see IEC 60529).

### 5.4.2 Well-trying safety principles – Mechanical (EN ISO 13849-2 Table A.2)

Well tried safety principle Mechanical	Remarks
Use of carefully selected materials and manufacturing	Selection of suitable material, adequate manufacturing methods and treatments related to the application.
Use of components with oriented failure mode	The predominant failure mode of a component is known in advance and always the same. See ISO 12100:2010, 6.2.12.3.
Overdimensioning/safety factor	The safety factors are given in standards or by good experience in safety-related applications.
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed for changing the position.
Increased OFF force	A safe position/state is obtained by an increased OFF force in relation to ON force.
Carefully selection, combination, arrangement, assembly and installation of components/system related to the application	—a
Carefully selection of fastening related to the application	Avoid relying only on friction.
Positive mechanical action	To achieve positive mechanical action, all moving mechanical components required to perform the safety function shall inevitably move connected components, e.g. a cam directly opens the contacts of an electrical switch rather than relying on a spring. See ISO 12100:2010, 6.2.5.
Multiple parts	Reducing the effect of faults by multiplying parts, e. g. where a fault of one spring (of many springs) does not lead to a dangerous condition.

Well tried safety principle Mechanical	Remarks
Use of wellf the effect of failures using seve	<p>A welld range of reaction time</p> <ul style="list-style-type: none"> <li>• use of carefully selected materials, manufacturing methods (e. g. presetting and cycling before use) and treatments (e. g. rolling and shot-peening),</li> <li>• sufficient guidance of the spring, and – sufficient safety factor for fatigue stress (i. e. with high probability a fracture will not occur). Welltreatments (e. g. rolling and shot-peening), rings, a d</li> <li>• use of carefully selected materials, manufacturing methods (e. g. presetting and cycling before use) and treatments (e. g. rolling and shot-peening),</li> <li>• sufficient guidance of the spring,</li> <li>• clearance between the turns less than the wire diameter when unloaded,</li> <li>• sufficient force after a fracture(s) is maintained (i. e. a fracture(s) will not lead to a dangerous condition).</li> </ul> <p>NOTE Compression springs are preferred.</p>
Limited range of force and similar parameters	<p>Determine the necessary limitation in relation to the experience and application. Examples are break pin, break plate, and torque-limiting clutch.</p> <p>IMPORTANT the necessary limitation in relation to the experience and application. Examples are break pin, break plate, and torque-limiting clutch.imit</p>
Limited range of speed and similar parameters	<p>Decide the necessary limitation in relation to the experience and application. Examples for limitations are centrifugal governor; safe monitoring of speed or limited displacement.</p>
Limited range of environmental parameters	<p>Decide the necessary limitations. Examples on parameters are temperature, humidity, pollution at the installation. See clause 10 and consider manufacturer's application notes.</p>
Limited range of reaction time, limited hysteresis	<p>Decide the necessary limitations.</p> <p>Consider e. g. spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.</p>

### 5.4.3 Basic safety principles – Pneumatic (EN ISO 13849-2 Table B.1)

Basic safety principle Pneumatic	Comments
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e. g. stress, durability, elasticity, friction, wear, corrosion, temperature.
Correct dimensioning and shaping	Consider e. g. stress, strain, fatigue, surface roughness, tolerances, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply manufacturer's application notes, e. g. catalogue sheets, installation instructions, specifications and use of good engineering practice in similar components/systems.
Use of de-energisation principle	<p>The safe state is obtained by release of energy to all relevant devices. See primary action for stopping in ISO 12100:2010, 6.2.11.3.</p> <p>Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3.</p> <p>Consider different modes, e. g. operation mode, maintenance mode. This principle shall not be used in some applications, e. g. where the loss of pneumatic pressure will create an additional hazard.</p>
Proper fastening	For the application of e. g. screw locking, fittings, gluing, clamp ring, consider manufacturer's application notes. Overloading can be avoided by applying adequate torque loading technology.
Pressure limitation	Examples are pressure relief valve, pressure reducing/control valve.
Speed limitation/ speed reduction	An example is the speed limitation of a piston by a flow valve or a throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration and separation of solid particles and water in the fluid.
Proper range of switching time	Consider, e. g. the length of pipework, pressure, exhaust capacity, force, spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.
Withstanding environmental conditions	<p>Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e. g. temperature, humidity, vibration, pollution. See clause 8 and consider manufacturer's specification/application notes.</p>

## Safety principles

---

Basic safety principle Pneumatic	Comments
Protection against unexpected start tha	<p>Consider unexpected start-up caused by stored energy and after power supply restoration for different modes, e.g. operation mode, maintenance mode.</p> <p>Special equipment for the release of stored energy can be necessary (see ISO 14118:2000, 5.3.1.3).</p> <p>Special applications (e.g. to keep energy for clamping devices or ensure a position) need to be considered separately..</p>
Simplification	Reduce the number of components in the safety-related system.
Proper temperature range	To be considered throughout the whole system.
Separation	Separation of the safety throughout the system. ty-related system.

### 5.4.4 Well-ried safety principles – Pneumatic (EN ISO 13849-2 Table B.2)

Well-ried safety principle Pneumatic	Comments
Over-dimensioning/safety factor	The safety factor is given in standards or by good experience in safety-related applications.
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position.
Increased OFF force	One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to ON position (a safety factor).
Valve closed by load pressure	These are generally seat valves, e. g. poppet valves, ball valves. Consider how to apply the load pressure in order to keep the valve closed even if e. g. the spring closing the valve breaks.
Positive mechanical action	The positive mechanical action is used for moving parts inside pneumatic components, see also Table A.2.
Multiple parts	See Table A.2.
Use of well-ried spring	See Table A.2.
Speed limitation/speed reduction by resistance to defined flow	Examples are fixed orifice, fixed throttle.
Force limitation/force reduction	This can be achieved by a well-ried pressure relief valve which is e. g. equipped with a well-ried spring, correctly dimensioned and selected.
Appropriate range of working conditions	The limitation of working conditions, e. g. pressure range, flow rate and temperature range should be considered.
Proper avoidance of contamination of the fluid	Consider high degree of filtration and separation of solid particles and water in the fluid.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents un-allowed movements.
Limited hysteresis	For example increased friction will increase the hysteresis. Combination of tolerances will also influence the hysteresis.

### 5.4.5 Basic safety principles – Hydraulic (EN ISO 13849-2 Table C.1)

Basic safety principle Hydraulic	Comments
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to e. g. stress, durability, elasticity, friction, wear, corrosion, temperature, hydraulic fluid.
Correct dimensioning and shaping	Consider e. g. stress, strain, fatigue, surface roughness, tolerances, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply manufacturer's application notes, e. g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components/ systems.
Use of detion of implementation n	The safe state is obtained by release of energy to all relevant devices. See primary action for stopping in ISO 12100:2010, 6.2.11.3. Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3. Consider different modes, e. g. operation mode, maintenance mode. This principle shall not be used in some applications, e. g. where the loss of hydraulic pressure will create an additional hazard.
Proper fastening	For the application of e. g. screw locking, fittings, gluing, clamp ring, consider manufacturer's application notes. Overloading can be avoided by applying adequate torque loading technology.
Pressure limitation	Examples are pressure relief valve, pressure reducing/control valve.
Speed limitation / speed reduction	An example is the speed limitation of a piston by a flow valve or a throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration/separation of solid particles/water in the fluid. Consider also an indication of the need of filter–service.
Proper range of switching time	Consider e. g. the length of pipework, pressure, evacuation relief capacity, spring tiredness, friction, lubrication, temperature/viscosity, inertia during acceleration and deceleration, combination of tolerances.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e. g. temperature, humidity, vibration, pollution. See clause 10 and consider manufacturer's specification and application notes.
Protection against unexpected start–up	Consider unexpected start–up caused by stored energy and after power supply restoration for different modes, e. g. operation mode, maintenance mode. Special equipment for release of stored energy may be necessary. Special applications, (e. g. keep energy for clamping devices or ensure a position) need to be considered separately.
Simplification	Reduce the number of components in the safety–related system.
Proper temperature range	To be considered throughout the whole system.
Separation	Separation of safety–related functions from other functions.

### 5.4.6 Well-ried safety principles – Hydraulic (EN ISO 13849-2 Table C.2)

Well-ried safety principle Hydraulic	Comments
Over-dimensioning/safety factor	The safety factor is given in standards or by good experience in safety-related applications.
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position.
Increased OFF force	One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to ON position (a safety factor).
Valve closed by load pressure	Examples are seat and cartridge valves. Consider how to apply the load pressure in order to keep the valve closed even if, e. g. the spring closing the valve, breaks.
Positive mechanical action	The positive mechanical action is used for moving parts inside hydraulic components, see also Table A.2.
Multiple parts	See Table A.2.
Use of well-ried spring	See Table A.2.
Speed limitation/speed reduction by resistance to defined flow	Examples are fixed orifices, fixed throttles.
Force limitation/force reduction	This can be achieved by a well-ried pressure relief valve which is, e. g. equipped with a well-ried spring, correctly dimensioned and selected.
Appropriate range of working conditions	The limitation of working conditions, e. g. pressure range, flow rate and temperature range should be considered.
Monitoring of the condition of the fluid	Consider high degree of filtration/separation of solid particles/water in the fluid. Consider also the chemical/physical conditions of the fluid. Consider an indication of the need of filter-service.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents un-allowed movements.
Limited hysteresis	For example increased friction will increase the hysteresis. A combination of tolerances will also influence the hysteresis.



### 5.4.7 Basic safety principles – Electrical (EN ISO 13849-2 Table D.1)

Basic safety principle Electrical	Comments
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to e. g. stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, dielectric rigidity.
Correct dimensioning and shaping	Consider e. g. stress, strain, fatigue, surface roughness, tolerances, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply manufacturer's application notes, e. g. catalogue sheets, installation instructions, specifications, and use of good engineering practice.
Correct protective bonding	One side of the control circuit, one terminal of the operating coil of each electromagnetic operated device or one terminal of other electrical device is connected to the protective bonding circuit [(see IEC 60204-1:2005, 9.4.3.1).
Insulation monitoring	Use of isolation monitoring device which either indicates an earth fault or interrupts the circuit automatically after an earth fault (see IEC 60204-1:2005, 6.3.3).
Use of defor insulation monitorin	<p>A safe state is obtained by def power separationlevant devices, e. g. by using of normally closed (NC) contact for inputs (push–buttons and position switches) and normally open (NO) contact for relays (see also ISO 12100:2010, 6.2.11.3).</p> <p>Exceptions may exist in some applications, e. g. where the loss of the electrical supply will create an additional hazard. Time delay functions may be necessary to achieve a system safe state (see IEC 60204-1:2005, 9.2.2).</p>
Transient suppression	Use of a suppression device (RC, diode, varistor) parallel to the load, but not parallel to the contacts. NOTE A diode increases the switch off time.
Reduction of response time	Minimise delay in deponse time by a diode. (RC element, d
Compatibility	Use components compatible with the voltages and currents used.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e. g. temperature, humidity, vibration and electromagnetic interference (EMI) (see clause 10).
Secure fixing of input devices	Secure input devices, e. g. interlocking switches, position switches, limit switches, proximity switches, so that position, alignment and switching tolerance is maintained under all expected conditions, e. g. vibration, normal wear, ingress of foreign bodies, temperature. See ISO 14119:1998, Clause 5.
Protection against unexpected start–up	Prevent unexpected start–up, e. g. after power supply restoration (see ISO 12100:2010, 6.2.11.4, ISO 14118, IEC 60204-1).

## Safety principles

---

<b>Basic safety principle</b> <b>Electrical</b>	<b>Comments</b>
Protection of the control circuit	The control circuit should be protected in accordance with IEC 60204-1:2005, 7.2 and 9.1.1.
Sequential switching for circuit of serial contacts of redundant signals	To avoid the common mode failure of the welding of both contacts, the switching on and off does not happen simultaneously, so that one contact always switches without current.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e. g. temperature, humidity, vibration and electromagnetic interference (EMI) (see clause 10).

### 5.4.8 Well-trying safety principles – Electrical (EN ISO 13849-2 Table D.2)

Well-trying safety principle Electrical	Comments
Positive mechanically linked contacts	Use of positively mechanically linked contacts for, e.g. monitoring function in Category 2, 3, and 4 systems (see EN 50205, IEC 60947-4-1:2001, Annex F, IEC 60947-5-1:2003 + A1:2009, Annex L).
Fault avoidance in cables	To avoid short circuit between two adjacent conductors: – use cable with shield connected to the protective bonding circuit on each separate conductor, or – in flat cables, use of one earthed conductor between each signal conductors.
Separation distance	Use of sufficient distance between position terminals, components and wiring to avoid unintended connections.
Energy limitation	Use of a capacitor for supplying a finite amount of energy, e. g. in timer application.
Limitation of electrical parameters	Limitation in voltage, current, energy or frequency resulting, e. g. in torque limitation, hold-to-run with displacement/time limited, reduced speed, to avoid leading to an unsafe state.
No undefined states	Avoid undefined states in the control system. Design and construct the control system so that during normal operation and all expected operating conditions its state, e. g. its output(s) can be predicted.
Positive mode actuation	Direct action is transmitted by the shape (and not by the strength) with no elastic elements, e. g. spring between actuator and the contacts, (see ISO 14119:1998, 5.1, ISO 12100:2010, 6.2.5).
Failure mode orientation	Wherever possible, the device/circuit should fail to the safe state or condition.
Oriented failure mode	Oriented failure mode components or systems should be used wherever practicable (see ISO 12100:2010, 6.2.12.3).
Over-dimensioning	Derate components when used in safety circuits, e. g. by : – current passed through switched contacts should be less than half their rated current, – the switching frequency of components should be less than half their rated value, and – total number of expected switching operation shall be ten times less than the device's electrical durability. NOTE Derating can depend on the design rationale.
Minimise possibility of faults	Separate safety-related functions from the other functions.
Balance complexity/simplicity	Balance should be made between: – complexity to reach a better control, and – simplify to have a better reliability.

### 5.5 Hazards (EN ISO 12100 Table B.1)

Type or group	Origin	Possible consequences	Subclause of ISO 12100
<b>Mechanical hazards</b>	<ul style="list-style-type: none"> <li>acceleration, deceleration</li> <li>angular parts</li> <li>approach of a moving element to a fixed part</li> <li>cutting parts</li> <li>elastic elements</li> <li>falling objects</li> <li>gravity</li> <li>height from the ground</li> <li>high pressure</li> <li>instability</li> <li>kinetic energy</li> <li>machinery mobility</li> <li>moving elements</li> <li>rotating elements</li> <li>rough, slippery surface</li> <li>sharp edges</li> <li>stored energy</li> <li>vacuum</li> </ul>	<ul style="list-style-type: none"> <li>being run over</li> <li>being thrown</li> <li>crushing</li> <li>cutting or severing</li> <li>drawing-in or trapping</li> <li>entanglement</li> <li>friction or abrasion</li> <li>impact</li> <li>injection</li> <li>shearing</li> <li>slipping, tripping and falling</li> <li>stabbing or puncture</li> <li>suffocation</li> </ul>	<ul style="list-style-type: none"> <li>6.2.2.1</li> <li>6.2.2.2</li> <li>6.2.3 a)</li> <li>6.2.3 b)</li> <li>6.2.6</li> <li>6.2.10</li> <li>6.3.1</li> <li>6.3.2</li> <li>6.3.3</li> <li>6.3.5.2</li> <li>6.3.5.4</li> <li>6.3.5.5</li> <li>6.3.5.6</li> <li>6.4.1</li> <li>6.4.3</li> <li>6.4.4</li> <li>6.4.5</li> </ul>
<b>Electrical hazards</b>	<ul style="list-style-type: none"> <li>arc</li> <li>electromagnetic phenomena</li> <li>electrostatic phenomena</li> <li>live parts</li> <li>insufficient distance to live parts under high voltage</li> <li>overload</li> <li>parts which have become live under fault conditions</li> <li>short-circuit</li> <li>thermal radiation</li> </ul>	<ul style="list-style-type: none"> <li>burn</li> <li>chemical effects</li> <li>effects on medical implants</li> <li>electrocution</li> <li>falling, being thrown</li> <li>fire</li> <li>projection of molten particles</li> <li>(electric) shock</li> </ul>	<ul style="list-style-type: none"> <li>6.2.9</li> <li>6.3.2</li> <li>6.3.3.2</li> <li>6.3.5.4</li> <li>6.4.4</li> <li>6.4.5</li> </ul>
<b>Thermal hazards</b>	<ul style="list-style-type: none"> <li>explosion</li> <li>flame</li> <li>objects or materials with a high or low temperature</li> <li>radiation from heat sources</li> </ul>	<ul style="list-style-type: none"> <li>burn</li> <li>dehydration</li> <li>discomfort</li> <li>frostbite</li> <li>injuries caused by radiation of heat sources</li> <li>scald</li> </ul>	<ul style="list-style-type: none"> <li>6.2.4 b)</li> <li>6.2.8 c)</li> <li>6.3.2.7</li> <li>6.3.3.2.1</li> <li>6.3.4.5</li> </ul>
<b>Noise hazards</b>	<ul style="list-style-type: none"> <li>cavitation phenomena</li> <li>exhaust system</li> <li>gas leaking at high speed</li> <li>manufacturing process (stamping, cutting etc.)</li> <li>moving parts</li> <li>scraping surfaces</li> <li>unbalanced rotating parts</li> <li>whistling pneumatics</li> <li>worn parts</li> </ul>	<ul style="list-style-type: none"> <li>discomfort</li> <li>loss of awareness</li> <li>loss of balance</li> <li>permanent hearing loss</li> <li>stress</li> <li>tinnitus</li> <li>tiredness</li> <li>any other (e.g. mechanical, electrical) problems as a consequence of an interference with speech communication or with acoustic signals</li> </ul>	<ul style="list-style-type: none"> <li>6.2.2.2</li> <li>6.2.3 c)</li> <li>6.2.4 c)</li> <li>6.2.8 c)</li> <li>6.3.1</li> <li>6.3.2.1 b)</li> <li>6.3.2.5.1</li> <li>6.3.3.2.1</li> <li>6.3.4.2</li> <li>6.4.3</li> <li>6.4.5.1 b) and c)</li> </ul>

# Tables & formulae

## Hazards (EN ISO 12100 Table B.1)

Type or group	Origin	Possible consequences	Subclause of ISO 12100
<b>Vibration hazards</b>	<ul style="list-style-type: none"> <li>cavitation phenomena</li> <li>misalignment of moving parts</li> <li>mobile equipment</li> <li>scraping surfaces</li> <li>unbalanced rotating parts</li> <li>whistling pneumatics</li> <li>worn parts</li> </ul>	<ul style="list-style-type: none"> <li>discomfort</li> <li>lower-back morbidity</li> <li>neurological disorder</li> <li>osteo-articular disorder</li> <li>trauma of the spine</li> <li>vascular disorder</li> </ul>	6.2.2.2 6.2.3 c) 6.2.8 c) 6.3.3.2.1 6.3.4.3 6.4.5.1 c)
<b>Radiation hazards</b>	<ul style="list-style-type: none"> <li>ionising radiation source</li> <li>low-frequency electromagnetic radiation</li> <li>optical radiation (infrared, visible and ultraviolet); including laser</li> <li>high-frequency electromagnetic radiation</li> </ul>	<ul style="list-style-type: none"> <li>burn</li> <li>damage to eyes and skin</li> <li>effects on reproductive capability</li> <li>mutation</li> <li>headache, insomnia etc.</li> </ul>	6.2.2.2 6.2.3 c) 6.3.3.2.1 6.3.4.5 6.4.5.1 c)
<b>Material/substance hazards</b>	<ul style="list-style-type: none"> <li>aerosol</li> <li>biological and microbiological (viral or bacterial) agent</li> <li>combustible</li> <li>dust</li> <li>explosive</li> <li>fibres</li> <li>flammable material</li> <li>fluid</li> <li>fumes</li> <li>gas</li> <li>mist</li> <li>oxidiser</li> </ul>	<ul style="list-style-type: none"> <li>breathing difficulties, suffocation</li> <li>cancer</li> <li>corrosion</li> <li>effects on reproductive capability</li> <li>explosion</li> <li>fire</li> <li>infection</li> <li>mutation</li> <li>poisoning</li> <li>sensitisation</li> </ul>	6.2.2.2 6.2.3 b) 6.2.3 c) 6.2.4 a) 6.2.4 b) 6.3.1 6.3.3.2.1 6.3.4.4 6.4.5.1 c) 6.4.5.1 g)
<b>Ergonomical hazards</b>	<ul style="list-style-type: none"> <li>access</li> <li>design or location of indicators and visual display units</li> <li>design, location or identification of control devices</li> <li>effort</li> <li>flicker, dazzling, shadow and stroboscopic effects</li> <li>local lighting</li> <li>mental overload/underload</li> <li>posture</li> <li>repetitive activities</li> <li>visibility</li> </ul>	<ul style="list-style-type: none"> <li>discomfort</li> <li>fatigue</li> <li>musculoskeletal disorder</li> <li>stress</li> <li>any other (e.g. mechanical, electrical) problems as a consequence of human error</li> </ul>	6.2.2.1 6.2.7 6.2.8 6.2.11.8 6.3.2.1 6.3.3.2.1
<b>Hazards associated with the environment in which the machine is used</b>	<ul style="list-style-type: none"> <li>dust and fog</li> <li>electromagnetic disturbance</li> <li>lightning</li> <li>moisture</li> <li>pollution</li> <li>snow</li> <li>temperature</li> <li>water</li> <li>wind</li> <li>lack of oxygen</li> </ul>	<ul style="list-style-type: none"> <li>burn</li> <li>mild disorder</li> <li>slipping, falling</li> <li>suffocation</li> <li>any other problems as a consequence of the effects caused by the sources of the hazards on the machine or parts of the machine</li> </ul>	6.2.6 6.2.11.11 6.3.2.1 6.4.5.1 b)
<b>Combination of hazards</b>	e.g. repetitive activity + effort + high ambient temperature	<ul style="list-style-type: none"> <li>e.g. dehydration, loss of awareness, heatstroke</li> </ul>	—

## Protective devices

### 5.6 Protective devices

#### 5.6.1 Forces

The question of possible forces is relevant for the design of protective devices. EN ISO 14119 provides good guidelines for this Table I.1.

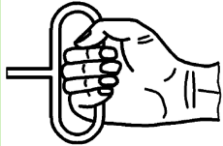
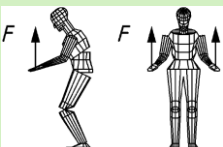
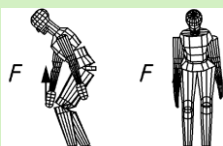
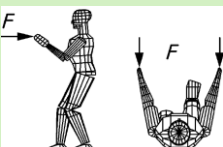
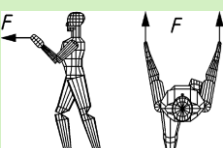
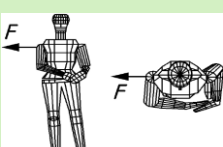
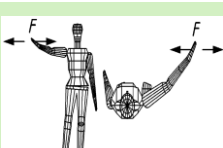
Direction of force	Body posture	Application of force	Value of force [N]	
	Horizontal pulling (dragging)	Sitting	One-handed	600
	Vertically upwards	Standing, torso and legs bent, feet next to each other	Two-handed, horizontal grip	1400
	Vertically upwards	Free standing	One-handed, horizontal grip	1200
	Horizontal, parallel to the body's backward plane of symmetry, pulling	Standing upright, feet next to each other or step position	Two-handed, vertical grip	1100
	Horizontal, parallel to the body's forward plane of symmetry, pushing	Standing, feet next to each other or step position	Two-handed, vertical grip	1300
	Horizontal, away from the body's plane of symmetry	Standing, torso bent sideways	Shoulder pressed against lateral metal plate	1300
	Horizontal, in line with the body's plane of symmetry	Standing, feet next to each other	One-handed, vertical grip	700

Table 3: EN ISO 14119 - Table I.1

## Protective devices

### 5.6.2 Safety distances

The determination of the safety distance of a protective device occurs by means of DIN EN ISO 13857 and depends on the following parameters:

- Direction of approach
- Height of the hazardous area
- Affected limbs
- Presence of children
- Height of the protection zone
- Resolution of the optical protective device
- Stop time of the safety function

As the evaluation of a range of formulae and tables is necessary for this, please download our calculation aid in the form of an MS Excel table. This can be downloaded at <http://wie.li/safetytools>

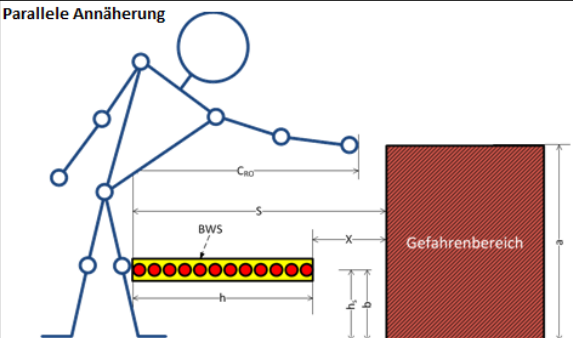
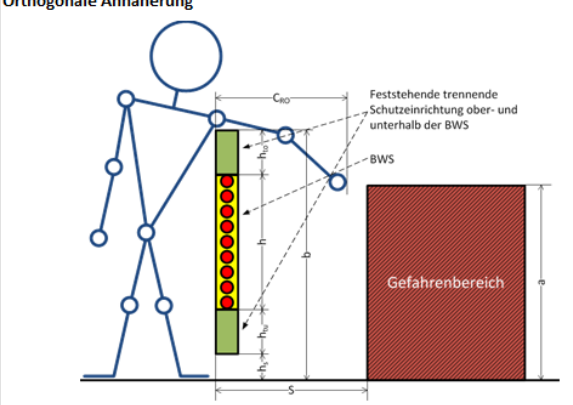

	A	B	C	D	E	F		
1	<b>Berechnung des Abstandes zur Gefahrenquelle bei Verwendung von optoelektronischen Sicherheitssensoren (BWS)</b>							
2	<b>Vorgabewerte</b>							
3	Annäherungsrichtung	a	Parallel					
4	Höhe des Gefährdungsbereichs		800 mm					
5	Betroffene Gliedmaßen		obere Gliedmaßen					
6	Kinder anwesend	KI	Ja					
7	Höhe festst. trennende Schutzeinrichtung oberhalb der BWS	h <sub>to</sub>	0 mm					
8	Höhe festst. trennende Schutzeinrichtung unterhalb der BWS	h <sub>tu</sub>	0 mm					
9	Unterkante des Schutzbereichs	h <sub>s</sub>	200 mm					
10	Sensortyp		SLC...-1200					
11	Bauhöhe der BWS	h	1200 mm					
12	Auflösung der BWS	d	40 mm					
13	Reaktionszeit BWS	t <sub>1</sub>	8,0 ms					
14	Reaktionszeit Auswärtiger	t <sub>2</sub>	11,6 ms					
15	Stopp-Zeit der Aktoren	t <sub>3</sub>	100,0 ms					
16	<b>Zwischenergebnisse</b>							
17	Maximale Höhe der Unterkante des Schutzbereichs	h <sub>max</sub>	1000 mm					
18	Mindest Höhe der Oberkante des Schutzbereichs	h <sub>min</sub>	0 mm					
19	Höhe Oberkante Schutzbereich	b	200 mm					
20	Anzunehmende Annäherungsgeschwindigkeit	K	1.600 mm/s					
21	Zuschlag für Eindringabstand	C <sub>RT</sub>	850 mm					
22	Zuschlag für Übergreifen	C <sub>RO</sub>	0 mm					
23	Zuschlag bei Anwesenheit von Kindern	C <sub>Kind</sub>	75 mm					
24	Minimum abhängig von Sensorauflösung	S <sub>1</sub>						
25		S <sub>2</sub>	1116 mm					
26		S <sub>3</sub>	1116 mm					
27	<b>Ergebnisse</b>							
28	Mindestabstand	S	1116 mm					
29	Reaktionszeit	T	0,120 s					
30	Erforderliches Sensordetektionsvermögen	d <sub>min</sub>	63 mm					
31	Maximaler Abstand zwischen Schutzfeld und Gefährdungsbereich	X	63 mm					
32	Sensorauflösung geeignet für Detektion von		Körper					
33	Strahlhöhe OK		OK					
34	Sensordetektionsvermögen OK		OK					

Figure 6: Safety distances - Screenshot of an Excel table

### 5.6.3 Access protection and anti-crawl protection

Different values are named in the standards for the permitted dimensions of the openings.

Standard	Access / safeguard	Dimensions [mm]	Prevents access of
EN ISO 13857	Slotted openings	180	Adult <sup>1</sup>
	Square or round openings	240	Adult <sup>1</sup>
EN ISO 11161	Distance between separating guard and floor	200	Adult <sup>1</sup>
EN ISO 13855	Vertical protection field (light curtain/grid) with beam at the bottom	300	Adult <sup>1</sup>
	Vertical protection field (light curtain/grid) with beam at the bottom	200	Children or groups of visitors

<sup>1</sup> Persons of 14 years and over are considered adults.



### 5.7 Actuators

#### 5.7.1 Safe drive functions

Safe drive functions are available nowadays for many frequency converters. The simpler functions such as STO, SS1 and parts of SLS can also be implemented with external solutions. Examples are shown in Chapter 3. The column “Examples for applications” is intended as a suggestion for the use of safety functions, many of which were still not practically feasible 5 years ago.

Abbreviation	EN	Function	Examples for applications
STO	Safe torque off	Motor does not receive any energy which can generate a rotating movement; stop category 0 according to EN 60204-1	Prevention of the unexpected startup of dangerous movements during configuration, setup and fault rectification.
SS1	Safe stop 1	Motor slows down; monitoring of brake ramp and STO after a stoppage or STO after a delay period has elapsed; stop category 1 according to EN 60204-1	Shutting down as quickly as possible when triggering a protective device e.g. <ul style="list-style-type: none"> <li>• opening of a safety door,</li> <li>• occurrence of imbalances in the system</li> </ul>
SS2	Safe stop 2	Motor slows down; monitoring of brake ramp and SOS after a stoppage or SOS after a delay period has elapsed; stop category 2 according to EN 60204-1	<ul style="list-style-type: none"> <li>• Workpiece measurement while maintaining position,</li> <li>• Retaining loads on the vertical axis</li> </ul>
SOS	Safe operating stop	Motor is stationary and resists external forces.	<ul style="list-style-type: none"> <li>• Setup mode on machining centres</li> <li>• Manual measurement during the machining</li> </ul>
SLA	Safely-limited acceleration	The exceeding of the acceleration limit is prevented.	<ul style="list-style-type: none"> <li>• When transporting open fluid containers</li> <li>• Limitation of the mechanical inertia forces on the workpiece or bracket</li> </ul>
SAR	Safe acceleration range	The acceleration of the motor is kept within specified limit values.	See SLA
SLS	Safely-limited speed	The exceeding of a speed limit value is prevented.	<ul style="list-style-type: none"> <li>• Setup mode on machining centres</li> <li>• Threading of material on calendar rolls</li> </ul>

# Tables & formulae

## Actuators

Abbreviation	EN	Function	Examples for applications
SSR	Safe speed range	The speed of the motor is kept within specified limit values.	See SLS and SSM
SLT	Safely-limited torque	The exceeding of a torque/force limit value is prevented.	<ul style="list-style-type: none"> <li>• Force limitation on closing edges of power-operated doors and gates</li> <li>• Prevention of the dragging in of operating personnel into winding machines</li> </ul>
STR	Safe torque range	The torque of the motor is maintained within specified limit values.	See SLT
SLP	Safely-limited position	The exceeding of a position limit value is prevented.	<ul style="list-style-type: none"> <li>• Zone partitioning on a machine in the production and loading area</li> <li>• Limitation of a travel range</li> <li>• Replacement of electromechanical limit switches</li> <li>• Limitation of the range of robotic arms</li> </ul>
SLI	Safely-limited increment	The motor is moved by a specified increment and then stops.	<ul style="list-style-type: none"> <li>• Setup mode on machining centres</li> <li>• Movement-limited typing on printing machines</li> </ul>
SDI	Safe direction	The unintentional direction of movement of the motor is prevented.	<ul style="list-style-type: none"> <li>• Preventing machine parts from moving towards the personnel.</li> <li>• Preventing entry points on rollers.</li> </ul>
SMT	Safe motor temperature	The exceeding of a motor temperature limit value is prevented.	<ul style="list-style-type: none"> <li>• Prevention of unacceptable high temperatures in potentially explosive areas</li> <li>• Fire protection</li> </ul>
SBC	Safe brake control	Safe control of an external brake.	Vertical axis applications
SCA	Safe CAM	While the motor position is in a specified range, a safe output signal is generated.	<ul style="list-style-type: none"> <li>• Replacement of position sensors</li> <li>• Monitoring of press cycles</li> <li>• Position limiting of robot axes</li> </ul>
SSM	Safe speed monitor	While the motor torque is lower than a specified value, a safe output signal is generated.	<ul style="list-style-type: none"> <li>• Fan monitoring</li> <li>• Monitoring of gases</li> <li>• Motion monitoring of lasers</li> </ul>

# Tables & formulae

## Actuators

### 5.7.2 Safe speeds

Currently there is no uniform assessment when a movement is considered hazardous. The following standards name speeds or step increments and can serve as reference points. Since additional complex conditions sometimes exist for the respective cases, the text in the standard should be checked for suitability for the respective application. Speeds are indicated in mm/s or m/min in the standards. For better comparability, they are converted here to mm/s.

Standard and machine type	Criteria						Function	Limit	Required measures			
	General	Impact	Crushing	Shearing	Capture	Vector movement			Movement / hazard	Manual operation of the direction	Enabling / inching device	Two-hand control
EN ISO 16090-1 - Machining centres, Milling machines, Transfer machines	X						SLS	33 mm/s	X	X		Standstill 2 rotations after stop command or braking distance less than 4 mm
	X					No		50 U/min	X	X		
	X							83 mm/s	X	X		
		X						250 mm/s	X	X		
		X						Gap > 300 mm	417 mm/s	X	X	
	X					Yes	Stretching	SLS 83 mm/s		X		Standstill 5 rotations after stop command
								SLI 10 mm				
EN ISO 10218 - Robots	X					Yes	SLI	4 mm	X	X		Maximum span hub 4 mm
EN ISO 23125 - Machine tools - Turning machines	X						SLS	250 mm/s		X		
	X						SLI	6 mm		X		
	X						SLS	33 mm/s		X		Small turning machines
						No		100 mm/s		X	(X)	
							Stretching	167 mm/s				
						SLI 4 mm						Maximum span hub 4 mm
							SLS	4 mm/s				

# Tables & formulae

## Actuators

Standard and machine type	Criteria						Function	Limit	Required measures			
	General	Impact	Crushing	Shearing	Capture	Vector movement			Movement / hazard	Manual operation of the direction	Enabling / inching device	Two-hand control
EN 1010-1 - Printing and paper converting machines	X						SLI	25 mm		X		
							SLS	17 mm/s				
	X						SLI	75 mm		X		
							SLS	83 mm/s				
		X					SLI	333 mm/s		X		
							SLS	333 mm/s				
EN ISO 11161 - Integrated manufacturing systems				X			SLI	33 mm/s		X		
		X	X		X		SLS	250 mm/s		X		
							SLS	10 mm/s		X		
EN ISO 13128 - Safety of machine tools - Milling machines							SLI	10 mm		X		Standstill 2 rotations after stop command
	X						SLS	33 mm/s				
	X					Yes	SLS	83 mm/s	X	X		Standstill 5 rotations after stop command
		X					SLS	250 mm/s		X		

## 6 Standards and references

In the context of this document, the EN version of the standard is quoted where it exists. If it does not exist, the ISO or IEC version is used. Tables that have been completely taken from standards represent a special case. Frequently the ISO or IEC version is referenced and often an obsolete version is used. The text of the corresponding EN is indicated for legibility.

The EN version of the standards itself can generally not be acquired directly and thus the respective national version should be used (e. g. from British Standards or Irish Standards). In other EU countries, the corresponding national adaptations must be used. The CE column stands for standards with relevance to an EU conformity declaration.

European standard / reference	Title	CE <sup>1</sup>	International equivalence
EN 1010-1+A1:2010	Safety of machinery - Safety requirements for the design and construction of printing and paper converting machines	X	<i>Not available as ISO or IEC standard</i>
2006/42/EC (published in document: 2006 L 157/24)	Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC	X	2006/42/EC
EN ISO 10218-1:2011	Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots	X	ISO 10218-1:2011
EN ISO 11161:2010	Safety of machinery - Integrated manufacturing systems - Basic requirements	X	ISO 11161:2007 + Amd 1:2010
EN ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction	X	ISO 12100:2010
EN 13128:2001 +A2:2009	Safety of machine tools - Milling machines (including boring machines)	X	<i>Not available as ISO or IEC standard</i>
EN ISO 13849-1:2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	X	ISO 13849-1:2015
EN ISO 13849-2:2012	Safety of machinery - Safety-related parts of control systems - Part 2: Validation	X	ISO 13849-2:2012
EN ISO 13850:2015	Safety of machinery - Emergency stop function - Principles for design	X	ISO 13850:2015
EN ISO 13855:2010	Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body	X	ISO 13855:2010
EN ISO 13857:2008	Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs	X	ISO 13857:2008



European standard / reference	Title	CE <sup>1</sup>	International equivalence
prEN ISO 14118:2016	Safety of machinery - Prevention of unexpected start-up		ISO/DIS 14118:2016
EN ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection	X	ISO 14119:2013
ISO/TR 24119: 2015 <i>Not available as EN standard</i>	Safety of machinery - Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts		ISO/TR 24119: 2015
prEN ISO 16090-1:2015	Machine tools safety - Machining centres, Milling machines, Transfer machines - Part 1: Safety requirements		ISO/DIS 16090-1.2:2015
EN ISO 23125:2015	Machine tools - Safety - Turning machines	X	ISO 23125:2015
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	X	IEC 60204-1:2005
EN 60529/A2:2013	Degrees of protection provided by enclosures (IP Code)		IEC 60529 AMD 2:2013
EN 60947-4-1/A1:2012	Low-voltage switchgear and controlgear - Part 4-1: Contactors and motor-starters - Electromechanical contactors and motor-starters		IEC 60947-4-1 AMD 1:2012
EN 60947-5-1/A1:2009	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices		IEC 60947-5-1:2003 + A1:2009
EN 61496-1:2013	Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests	X	IEC 61496-1:2012
EN 61508 parts 1-7:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems		IEC 61508 parts 1-7:2010
EN 61810-2:2011	Electromechanical elementary relays - Part 2: Reliability		IEC 61810-2:2011
EN 61810-3:2015 <i>(replaces EN 50205)</i>	Electromechanical elementary relays - Part 3: Relays with forcibly guided		IEC 61810-3:2015
EN 62061/A2:2015	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	X	IEC 62061 AMD 2:2015

**1** Listed in the journal of at least one EU directive requesting a CE declaration.

---

## 7 Notes

### 7.1 Copyright

This work is protected by copyright. Any rights derived from the copyright are retained by Wieland Electric GmbH. Duplication of the work or part of this work is only permitted within the limits of the statutory provisions of the copyright law. Any change or curtailment of the work is prohibited without the express written approval of Wieland Electric GmbH.

### 7.2 Liability

As far as nothing else is agreed from the following provisions, we are liable in the event of a breach of contractual and non-contractual duties according to the appropriate legal requirements.

We assume liability for compensation in the event of intent and gross negligence, irrespective of the legal grounds. In the case of simple negligence, we are only liable for damages arising from loss of life, bodily injury or damage to health or for damages resulting from the violation of an essential contractual obligation (an obligation whose fulfilment only enables the proper implementation of the contract and on whose compliance the contract partner relies); in this case, our liability is however limited to the compensation of the foreseeable damage that typically occurs.

## Index

$\lambda$ .....	131	Table A.1 .....	144
2006 L 157/24 .....	165	Table A.2 .....	146
2006/42/EG .....	9	Table B.1 .....	148
2006/42/EU .....	165	Table B.2 .....	150
Access protection .....	160	Table C.1 .....	151
Annex K .....	136	Table C.2 .....	152
Anti-crawl protection .....	160	Table D.1 .....	153
Avoidability .....	11	Table D.2 .....	155
B <sub>10</sub> .....	131	EN ISO 14119	
B <sub>10D</sub> .....	131	Table I.1 .....	158
Bar graph .....	135	Enabling button .....	116
Betriebssicherheitsverordnung .....	9	E-Stop	
BetrSichV .....	9	PL c .....	24, 82, 92
block circuit diagram .....	15	PL d .....	27, 76
Bumper .....	59	PL e .....	30
C .....	131	Series connection .....	76, 82, 92
Calendar rolls .....	161	EU Commission .....	9
Category .....	134	EU Journal .....	9
CCF .....	20, 131, 134	Fan monitoring .....	162
Table .....	139	Fault accumulation .....	134
Coded switches .....	124	Fault exclusions .....	127
C-Type standard .....	11	Fault masking .....	127
DC .....	19, 129, 131	Fire protection .....	162
Input .....	140	FIT .....	131
Logic .....	141	Fluid containers .....	161
Measures .....	140	Force limitation .....	162
Output .....	143	Forces .....	158
Ranges .....	135	Formulae .....	131
DC <sub>avg</sub> .....	131	Frequency of exposure to hazard .....	11, 12
Diagnostic coverage .....	131	Frequency of use .....	18
Direct opening action .....	125	Guard	
Directive .....	9	Guard locking .....	124
Door monitoring		non separating .....	124
Guard locking .....	120	separating .....	124
PL c .....	34, 79, 82	Guards .....	124
PL c/d .....	37, 41	harmonised standards .....	9
PL d .....	13, 55, 85	Hazard	
PL e .....	45, 49, 52, 89, 96, 100, 104, 108	Possibility of avoiding .....	12
Series connection .....	79, 82, 85, 89, 96, 100, 104, 108	Probability of occurrence .....	12
d <sub>op</sub> .....	131	Hazards .....	9, 11
Dragging in .....	162	Combination .....	157
Duration of exposition .....	12	Electrical .....	156
EE-Stop		Environmental .....	157
PL c .....	79	Ergonomical .....	157
Series connection .....	79	Material .....	157
EN ISO 12100		Mechanical .....	156
Figure 1 .....	11	Noise .....	156
Table B.1 .....	156	Radiation .....	157
EN ISO 13849-1		Substances .....	157
Figure 5 .....	135	Table .....	156
Table 3 .....	135	Thermal .....	156
Table 5 .....	135	Vibration .....	157
Table E.1 .....	140, 141, 143	HFT .....	131
Table F.1 .....	139	h <sub>op</sub> .....	131
Table K.1 .....	136	inherently safe design .....	11
EN ISO 13849-2		ISO/TR 24119	
		Table 1 .....	129



Laser .....	162	Safe stop 2 .....	161
Laws .....	9	Safe torque off .....	161
Light curtain/grid		Safely-limited speed .....	161
PL c .....	70	Safety distances .....	159
PL e .....	73	Safety Integrity Level .....	132
Typ 2 .....	70	Safety matchaltmatte .....	55
Typ 4 .....	73	Safety principles .....	134, 144
Machinery directive .....	9, 165	Basic .....	134
Manual reset function .....	13	Basic – Elektrical .....	153
MD .....	9	Basic – Hydraulicalcal .....	151
Mechanical position switches .....	124	Basic – Mechanical .....	144
Mode selector .....	112	Basic – Pneumatical .....	148
MTBF .....	131	Well-ried – Elektrical .....	155
MTTF .....	131	Well-ried – Hydraulical .....	152
MTTF <sub>D</sub> .....	18, 19, 131	Well-ried – Mechanical .....	146
Muting .....	125	Well-ried – Pneumatical .....	150
Muting lamp .....	125	Safety related part of a control system .....	12
n <sub>op</sub> .....	131	Safety review .....	14
Operating days .....	14, 131	Series connection .....	125
Operating hours .....	14	Severity of injury .....	11, 12
Performance Level .....	14	SIL .....	132
PFH .....	131	SILCL .....	132
PFH <sub>D</sub> .....	20, 131	Single fault .....	134
Minimum requirements .....	135	SLS .....	161
PL .....	20, 131	SRP/CS .....	12
PL <sub>r</sub> .....	14, 132	SS1 .....	161
Position limiting .....	162	SS2 .....	13, 161
Position monitoring .....	124	Standards .....	9
positively-driven operation .....	125	Typ C .....	10
ProdSG .....	9	Start/restart function .....	126
Produktsicherheitsgesetz .....	9	Step mat .....	55
Proof-Test-Intervall .....	132	STO .....	161
Protective equipment .....	124	Subsystem .....	18
fixing location .....	124	Symbols .....	131
P <sub>TE</sub> .....	132	T <sub>1</sub> .....	132
RDF .....	132	T <sub>10D</sub> .....	132
Reaction .....	13	T <sub>2</sub> .....	132
References .....	165	Tables .....	131
Reset .....	126	t <sub>cycle</sub> .....	132
Restart .....	13, 126	technical protection measures .....	11
risk analysis .....	11	T <sub>M</sub> .....	20, 132
risk assessment .....	11	Trigger event .....	13
risk graph .....	11	Two-hand-control	
Risk reduction .....	11	PL c .....	64
Rollers .....	162	PL e .....	67
Safe drive functions .....	161	Vertical axis .....	162
Safe speeds .....	163	Well-ried components .....	134
Safe state .....	13	Well-ried safety principles .....	134
Safe stop 1 .....	161	Winding machines .....	162

# Value-added-service

One reaches into the other - Support by Wieland



# wieland

### On-site service provision

Wieland Electric also provides support for the entire service life of machines by offering direct, on-site services, including:

- Risk assessment
- Verification and validation
- Commissioning check
- Stoptime measurement
- Periodic inspections of light grids
- Inspections before and during operation
- Programming support



Applikationshandbuch - DIGITAL

Use our comprehensive support for standard-compliant creation of your risk assessment.



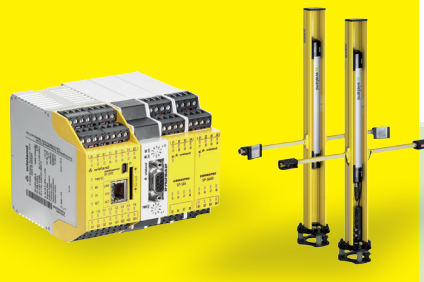
### Flexibility and plug-in ease

Save time and money thanks to flexibility, modular design, and plug-in ease – across all life phases of the machine.



### Safety

Make your machine safe – with solutions from Wieland.



### Process reliability + communication

Increase process reliability and communicate with your machines worldwide.





**USA**  
**Wieland Electric Inc.**  
**North America**  
2889 Brighton Road  
Oakville, Ontario L6H 6C9  
Phone +1 905 8298414  
Fax +1 905 8298413  
[www.wielandinc.com](http://www.wielandinc.com)



**CANADA**  
**Wieland Electric Inc.**  
**North America**  
2889 Brighton Road  
Oakville, Ontario L6H 6C9  
Phone +1 905 8298414  
Fax +1 905 8298413  
[www.wieland-electric.ca](http://www.wieland-electric.ca)



**GREAT BRITAIN**  
**Wieland Electric Ltd.**  
Riverside Business Centre,  
Walnut Tree Close  
GB-Guildford/Surrey GU1 4UG  
Phone +44 1483 531213  
Fax +44 1483 505029  
[sales.uk@wieland-electric.com](mailto:sales.uk@wieland-electric.com)  
[www.wieland.co.uk](http://www.wieland.co.uk)



**FRANCE**  
**Wieland Electric SARL.**  
Le Cérame, Hall 6  
47, avenue des Genottes  
CS 48313,  
95803 Cergy-Pontoise Cedex  
Phone +33 1 30320707  
Fax +33 1 30320714  
[info.france@wieland-electric.com](mailto:info.france@wieland-electric.com)  
[www.wieland-electric.fr](http://www.wieland-electric.fr)



**SPAIN**  
**Wieland Electric S.L.**  
C/ Maria Auxiliadora 2, bajos  
E-08017 Barcelona  
Phone +34 93 2523820  
Fax +34 93 2523825  
[ventas@wieland-electric.com](mailto:ventas@wieland-electric.com)  
[www.wieland-electric.es](http://www.wieland-electric.es)



**ITALY**  
**Wieland Electric S.r.l.**  
Via Edison, 209  
I-20019 Settimo Milanese  
Phone +39 02 48916357  
Fax +39 02 48920685  
[info.italy@wieland-electric.com](mailto:info.italy@wieland-electric.com)  
[www.wieland-electric.it](http://www.wieland-electric.it)



**BELGIUM & GD LUXEM-  
BOURG**  
**ATEM-Wieland Electric NV**  
Bedrijvenpark De Veert 4  
B-2830 Willebroek  
Phone +32 3 8661800  
Fax +32 3 8661828  
[info.belgium@wieland-electric.com](mailto:info.belgium@wieland-electric.com)  
[www.wieland-electric.be](http://www.wieland-electric.be)



**DENMARK**  
**Wieland Electric A/S**  
Vallørækken 26  
DK-4600 Køge  
Phone +45 70 266635  
Fax +45 70 266637  
[sales.denmark@wieland-electric.com](mailto:sales.denmark@wieland-electric.com)  
[www.wieland-electric.dk](http://www.wieland-electric.dk)



**SWITZERLAND**  
**Wieland Electric AG**  
Harzachstrasse 2b  
CH-8404 Winterthur  
Phone +41 52 2352100  
Fax +41 52 2352119  
[info.swiss@wieland-electric.com](mailto:info.swiss@wieland-electric.com)  
[www.wieland-electric.ch](http://www.wieland-electric.ch)



**POLAND**  
**Wieland Electric Sp. z o.o.**  
Św. Antoniego 8  
62-080 Swadzim  
Phone +48 61 2225400  
Fax +48 61 8407166  
[office@wieland-electric.pl](mailto:office@wieland-electric.pl)  
[www.wieland-electric.pl](http://www.wieland-electric.pl)



**CHINA**  
**Wieland Electric Trading**  
Unit 2703 International Soho City  
889 Renmin Road,  
Huang Pu District  
PRC-Shanghai 200010  
Phone +86 21 63555833  
Fax +86 21 63550090  
[info-shanghai@wieland-electric.com](mailto:info-shanghai@wieland-electric.com)  
[www.wieland-electric.cn](http://www.wieland-electric.cn)



**JAPAN**  
**Wieland Electric Co, Ltd.**  
Nisso No. 16 Bldg. 7F  
3-8-8 Shin-Yokohama,  
Kohoku-ku  
Yokohama 222-0033  
Phone +81 45 473 5085  
Fax. +81 45 470 5408  
[info-japan@wieland-electric.com](mailto:info-japan@wieland-electric.com)



**GERMANY**  
**Headquarters**  
**Wieland Electric GmbH**  
Brennerstraße 10 – 14  
D-96052 Bamberg  
Phone +49 951 9324-0  
Fax +49 951 9324-198  
[info@wieland-electric.com](mailto:info@wieland-electric.com)  
[www.wieland-electric.de](http://www.wieland-electric.de)

**Sales partners:**

**You can reach us worldwide in more than 70 countries.  
Find the contact address at: [www.wieland-electric.com](http://www.wieland-electric.com)**

Subject to technical changes without notice!  
**gesis<sup>®</sup>, RST<sup>®</sup>, GST<sup>®</sup>, GST18<sup>®</sup>, podis<sup>®</sup>, samos<sup>®</sup>, and saris<sup>®</sup>**  
are registered trademarks of Wieland Electric GmbH

**contacts  
are  
green.**