wieland

safety SERVICE

SAFETY MANUAL

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

Contents

Contents

Illustrations

Contents
Overview of Safety Functions

	PL	Cat	Series connection	Emergency stop	Two-hand	Acknowledgment button	Operating mode selection switch	Door switch, mechanical	Door switch, magnetic	Door switch, RFID	Pressure-sensitive mat / bumper	Light grid / light curtain	Door locking function	Pneumatic valve, STO	Relay, STO	Frequency converter, STO	Frequency converter, SS2	Frequency converter, SLS	Time delay	Section
EMERGENCY stop & door switch, mechanically in series, 1-channel in PL c	c)	1	X	X				X							X					3.18
EMERGENCY stop & door switch, magnetic in series, 2-channel in PL c	c)	1	X	X					X						X					3.19
Magnetic door switches in series – 2-channel in PL d	d	3	X						X						X					3.20
RFID door switch in series – 2-channel, equivalent in PL e	e	4	X							X						X				3.21
Door switch, RFID & emergency stop in series (1) – emergency stop –S1 in PL c	c)	1	X	X						X					X					3.22
Door switch, RFID & emergency stop in series (1) – door –B1 in PL e	e	4	X	X						X					X					3.23
Door switch, RFID & emergency stop in series (1) – door –B2 in PL e	e	4	X	X						X					X					3.24
Door switch, RFID & emergency stop in series (2) – emergency stop in PL e	e	3	X	X						X					X					3.25
Door switch, RFID & emergency stop in series (2) – door in PL e	e	4	X	X						X					X					3.26
Operating mode selection switch in PL e	e	4					X									X				3.27
Acknowledgment button in PL e	e	3				X		X								X				3.28
Door locking in PL d	d	2											X						X	3.29

Foreword

1   Foreword

With this application manual, we offer you a realistic, practical aid for drafting your safety solutions. Example solutions for your day-to-day machine applications let you profit from our experience. Wieland has been involved in electronic connection technology since 1910, making us a pioneer in this sector. As manufacturer of safety controls and safety sensor systems, Wieland grants you 30 years of experience in these areas. Our experts in training, consultancy and technical support are always on hand for you. Our knowledge is yours to leverage.

The present Version 2 updates the examples and deals with new topics such as new aspects of the emergency stop thematic and the use of electrical components with software, without safety levels Lock Out, Tag Out and HRC.

On-site service provision

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

- Risk assessment
- Verification and validation
- Commissioning checks
- Stop time measurement
- Periodic inspections of light grids
- Inspections before and during operation
- Programming support
- CSE Certified Safety Engineer in accordance with EN ISO 13849 by SGS-TÜV Saar

2   Introduction

2.1   Safety Technology – Laws and Standards

Since ratification of the Machinery Directive (MRL) in 1993, the EU Commission has adopted this framework for application throughout Europe. Machines must be safe. In this context, safe means machinery is not permitted to introduce any hazards to humans or the environment. In certain areas, the framework is still more restrictive; machinery must not pose hazards to even the production means or manufactured products. The Machinery Directive has wrought significant change since 1993, while itself undergoing a number of updates and adaptations. The current applicable version is Directive 2006/42/EC, published in the EU Official Journal under number 2006 L 157/24. The individual EU countries have found different approaches to integrating the Directive into their national laws.
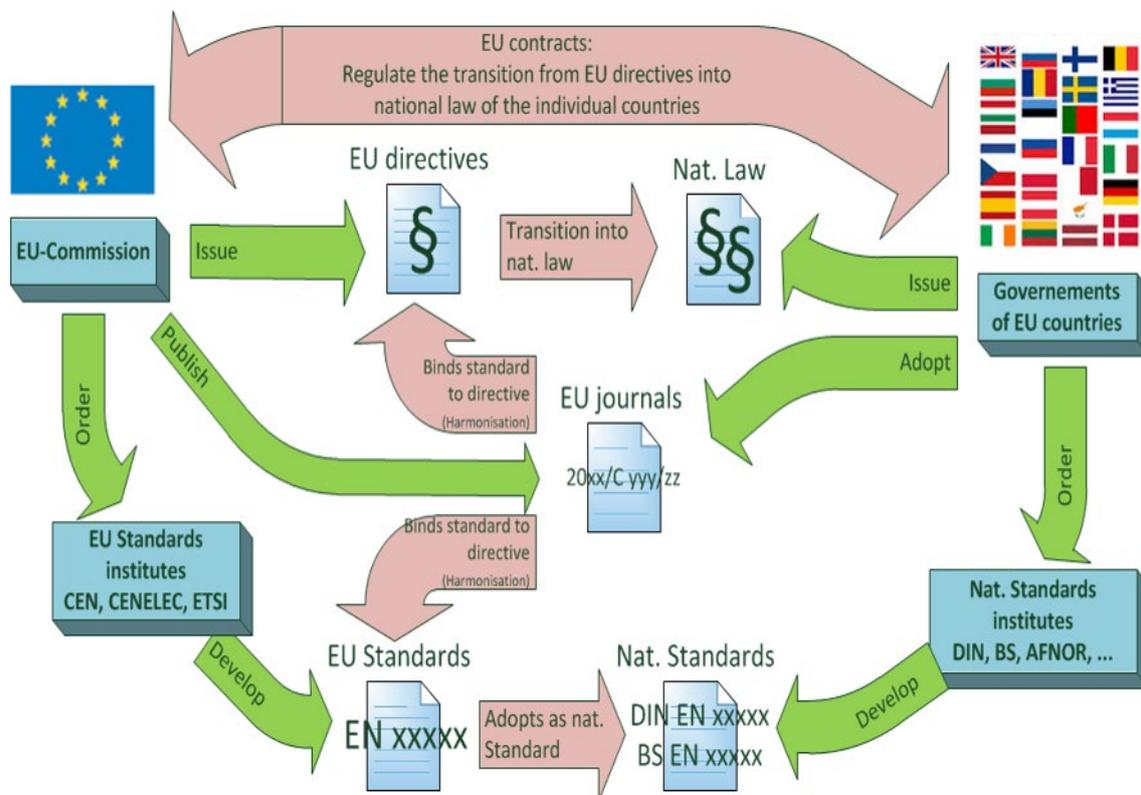
Illustration 1: Europe – Standards and Laws

Even though this results in different shapes and forms, the content is always the same. In Germany, the Machinery Directive is implemented into national legislation through several laws and regulations. Of particular note are:

- Product Safety Act – ProdSG
- Industrial Safety Regulations – BetrSichV

And even though formally, only German laws are valid in Germany, just as only their national laws apply in the other European countries, it is helpful to know that all EU countries have laws with the same content that are oriented to the Machinery Directive. Thus, it is enough to know and follow the European directives in order to fulfill the important legal requirements in the other EU countries as well.

The special European feature of harmonized standards has proven itself as particularly helpful. In Europe, standards can be tied to directives by means of an official communication, the EU Official Journal. This provides whoever applies the corresponding standard with legal certainty. Those who use a harmonized standard can assume they maintain legal compliance within the standard's scope of validity. This is not to say standards amount to technical laws, especially since solutions other than those described in the standards must always remain open; yet in fulfilling the standards, the specific text of the law is no longer of concern. Currently there are nearly 800

standards listed as harmonized for the Machinery Directive alone; in particular, for many hazardous machines. Of the general standards, EN ISO 12100 and EN ISO 13849-1 stand out as most important and are explained in more detail below. Because research into standards proven difficult for many due to lack of access to standards databases, the attached standards overview should serve as helpful at the least for type B standards, which cover hazards, aspects and technologies. Yet one must always bear in mind, standards are subject to a continual updating process. Typical update periods run from 3 to 5 years, meaning that regularly checking the currency of an applied standard is urgently recommended. Even though they were not actually designed for the purpose, online shops of standards publishers like Beuth (http://www.beuth.de/de), ISO (http://www.iso.org/iso/home/store) and IEC (https://webstore.iec.ch) serve well as no-cost, always up-to-date research sources.

Illustration 2: Overview of essential safety technology standards

② Scheme of standards according ISO/TR 22100-1: 2016

GENERAL PRINCIPLES FOR DESIGN – RISK ASSESSMENT & RISK REDUCTION
EN ISO 12100 (TYPE-A STANDARD)

Type-B Standards related to: hazards

NOISE

- Determination of emission sound pressure levels at a workstation
EN ISO 11200 to 11205

- Determination of sound power & energy levels
EN ISO 3741, 3743-1, 3744, 3745, 3746, 3747

- Determination of sound power levels by sound intensity
EN ISO 9614 series

- Insulation performances of enclosures
EN ISO 11546 series

- Insulation performances of cabins
EN ISO 11957

- Declaration & verification of noise emission
EN ISO 4871

SUBSTANCES

- Evaluation of emission of airborne hazardous substances
ISO 29042 series

- Reduction of risks to health from hazardous substances
ISO 14123-1 & -2

- Hygiene requirements
EN ISO 14159

THERMAL HAZARDS

- Human responses to contact with surfaces
EN ISO 13732-1 & -3

FIRE HAZARDS

- Fire prevention and protection
EN ISO 19353

ELECTRICAL HAZARDS

- Protection against electric shock
EN 60204-1

VIBRATION & SHOCK

- Whole body vibration
ISO 2631 series

- Hand-arm vibration
EN ISO 13753

- Hand-held & hand-guided machinery
EN ISO 20643

ERGONOMICS

- Access openings
EN ISO 15534

- Anthropometric requirements for workstations
EN ISO 14738

- Computer manikins and body templates
EN ISO 15536-1

RADIATION HAZARDS

- Lasers and laser-related equipment - Generals
EN ISO 11145

Type-B Standards related to: aspects and technology

DIMENSIONS & DISTANCES

- Gaps to avoid crushing
EN ISO 13854

- Minimum distances
EN ISO 13855

- Safety distances
EN ISO 13857

- Permanent means of access
EN ISO 14122 series

ALARMS & WARNINGS

- Design principles for safety signs
ISO 3864-1

- Registered safety signs
EN ISO 7010

- Auditory danger signals
EN ISO 7731

- Visual, acoustic and tactile signals
EN 61310-1

POWER SOURCE

- Electrical equipment
EN 60204-1

- Pneumatic equipment
EN ISO 4414

- Hydraulic equipment
EN ISO 4413

CONTROL SYSTEMS

- Avoidance of unexpected start-up
EN ISO 14118

- Design of safety-related parts of control systems
EN ISO 13849-1

- Validation of safety-related parts of control systems
EN ISO 13849-2

- Emergency stop function
EN ISO 13850

SAFETY DEVICES

- Guards
EN ISO 14120

- Interlocking devices
EN ISO 14119

- Series connection of doors
EN ISO/TR 24119

- Two-hand control devices
EN ISO 13851

- Electro-sensitive protective equipment
EN 61496 series

- Detection of persons
EN 62046

- Pressure-sensitive protective devices
EN ISO 13856 series

ASSEMBLY OF MACHINERY

- Integrated manufacturing systems
EN ISO 11161

2.2 What will make my machine safe?

The basis of any safety technology is a risk assessment of the machine. Here, harmonized standards for the specific machine type – the C-standards – are helpful. If there is no appropriate C-standard, or only one that does not apply to all aspects of the machine, EN ISO 12100 comes into play. This explains how the boundaries of the machine are determined, which hazards need to be taken into account and how the risk estimation and risk evaluation are to be performed (see Figure 3).

The risk evaluation is usually conducted with a risk graph. In this context, the most well-known risk graph is EN ISO 13849-1 (see Figure 4, Page 11), which presents only an approximate classification of severity of injuries, hazard exposure frequency and hazard avoidability. Other risk graphs are equally applicable.

Risk reduction is only addressed in the second step. It must be kept in mind, risk reduction measures carry an explicit priority here. According to EN ISO 12100, inherently safe design must always be applied first. In most cases, these types of solutions are also the most cost-effective. If risk levels cannot be adequately reduced by inherently safe design, technical protective measures can be applied. Their effectiveness and suitability must also be evaluated as described in EN ISO 13849. Only when technical measures do not adequately reduce risk either can user information be used as final option. However, this can be extremely comprehensive, since they open possibilities to thoroughly document safe operation and correspondingly training of the operator.

2.3 The safety function

If the risks have been identified and evaluated and technical protective measures should be employed to reduce them, EN ISO 13849-1 is then applied. Here, the first step in implementation is always formulation


Illustration 3: Risk assessment

of the safety function, frequently referred to with the abbreviation SRP/CS (Safety related part of a control system). In practice, the term "subsystem" is often used with the same meaning. The particular safety function must be selected so it will reduce the risk to an acceptable level. When formulating the protective function, it is helpful to clearly designate the *Trigger event*, the *Reaction* and the *Safe state*. In general, several elements are used to realize the safety function, with a 3-stage implementation as typical. The situation is captured by sensor technology, identified as *Input* in EN ISO 13849-1, that detects the hazardous state. The logical processing is run in *Logic*. The reaction is realized through the *Output*, or, the actuator technology, and leads to a safe state. In most cases, the individual elements serve not just one, but several, safety functions. For instance, the same contactor can be used for safety-oriented switching of an emergency stop safety function or a safety function that monitors access to a hazard area. Likewise, the same safety logic applies in both cases. Only the *Input* will be different in these two cases; specifically, one an emergency stop switch and one a light grid or light curtain.

Each of the applications presented in this manual demonstrate a complete safety function; however, depending on the example, the focus can be on either the *Input* or *Output* side. If the number of in- and outputs is not the limiting element and there are no special requirements for diagnosis of the sensors and actuators, most examples can be

Introduction

The safety function

varied without any problems by simply putting the desired in- and output components together. Wherever possible, concrete products are referred to. Thus, the key safety data are to be taken as examples. In contrast to some standards and collections of examples, requirements that are to be fulfilled by the machine builder are specifically stated. This primarily concerns fault exclusions and their conditions.

Calculations related to safety technology are typically done with calculation tools such as, e.g., Sistema; therefore, they are not given any special consideration in this document. Instead, only the entry parameters needed for calculations are presented.

S: Severity of injury
S1 Slight injury
S2 Severe injury, including death

F: Frequency and/or duration of exposure to hazard
F1 Seldom to often and/or brief exposure duration
F2 Frequent to constant and/or lengthy exposure

P: Possibility for preventing the hazard
P1 Possible under certain conditions
P2 Hardly possible

Likelihood of hazard occurring
If the likelihood is low, PL_r can be reduced by one level
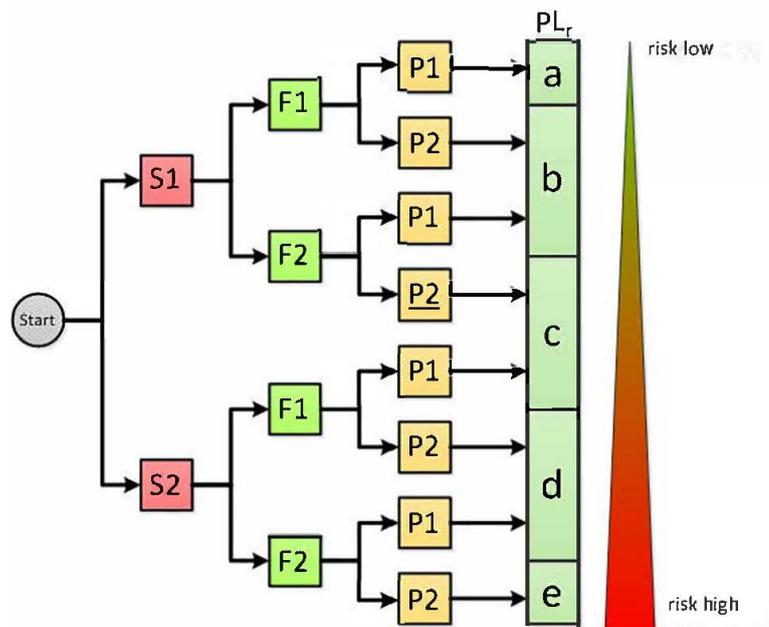
Illustration 4: EN ISO 13849-1 risk graph

Because the individual safety function examples were deliberately kept short, a more comprehensive example, with all of its steps, is presented at the start in 3.1. Furthermore, unfortunately it is not possible to depict every possible combination of sensors, logic and actuators. On the other hand, normally the respective aspects from many of the safety function examples presented below can be put together with little effort by suitable combinations of individual subsystems for sensor, logic and actuator. Thus, in most cases the sensors of one safety function can be combined with the actuators of another one without a problem. An overview of the individual functions and their main aspects is presented in *Overview of Safety Functions* on Page 5.

3 Safety functions

3.1 Door switch, magnetic – SS2 in PL d

3.1.1 Problem

In a work area, the drive may present a hazard for the worker. Thus, the work area is equipped with a safety fence and a protective door with door sensor –B1. Because calibrating the drive position is time-consuming, a safe stop with live energy (SS2) is performed instead of one without energy. Frequency converter –T1 with integrated SS2 is used here. To function correctly, the frequency converter needs certain information about drive position, which is detected by rotary encoder –B11. Safety controller –K1 is used as safety logic.

3.1.2 Safety function

Safety function	When door –B1 is closed, drive –T1 is brought to a stop in a controlled manner. Safe state is reached when the drive axis pauses at the current position.
Trigger event	Opening protective doors –B1
Reaction	Activation of safety function SS2 in drive control –T1 and prevention of unintended restart
Safe state	Safe drive standstill and position hold.

3.1.3 Description

Function	By opening protective door –B1: • Input circuit is interrupted at safety switching device –K1 • frequency converter –T1 activates SS2 • frequency converter –T1 monitors standstill via rotary encoder –B11 • If there is a malfunction, frequency converter –T1 triggers an STO.
Manual reset function	Because it is not possible to go behind protective doors –B1, manual reset is initiated by closing doors –B1.
Start/restart function	The start/reset function is automatically initiated when the doors are closed or via a separate start command.

3.1.4 Safety assessment

Sensor technology	• Ground faults and cross shorts in the input circuit are detected by –K1 through test impulses on the sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99% • Synchronization time monitoring between input circuits –K1:I1 and –K1:I2
Actuator technology	Because it is a certified safety component, the actuator technology needs no special monitoring.

3.1.5 Frequencies

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

Annual operating days	d_{op}	365
Operating hours per day	h_{op}	16
Interval between two accesses into hazard area in hours	t_{Cycle}	4

3.1.6 Determination of performance level PL$_r$

PL$_r$ is determined per the EN ISO 13849-1 risk graph Abbildung 4 (Page 11). A detailed reason should follow for the parameters for which a low risk is assumed. To an extent, product standards (C standards) and the category to be applied have already determined PL$_r$. In such cases, this should be documented.

| PL$_r$	PL d
Reason for parameter selection	F1: A frequency of every 4 hours is considered as rare. Troubleshooting and remediation take only a few minutes (< 5 minutes).
Are there requirements from the C standards	No

Safety functions

Door switch, magnetic – SS2 in PL d

3.1.7 Realization

Selection of the necessary components needed for the safety function and modeling of the equivalent circuit:

Input	Logic	Output

Data required from device manufacturer		
B_{10D}; T_M	PL; PFH_D, T_M	PL; PFH_D, T_M for –T1 and –B11

To determine/confirm for application		
Cat. 4, DC, CCF, n_{op}		
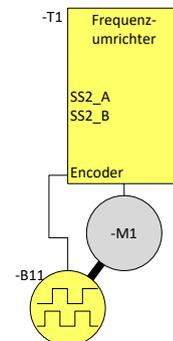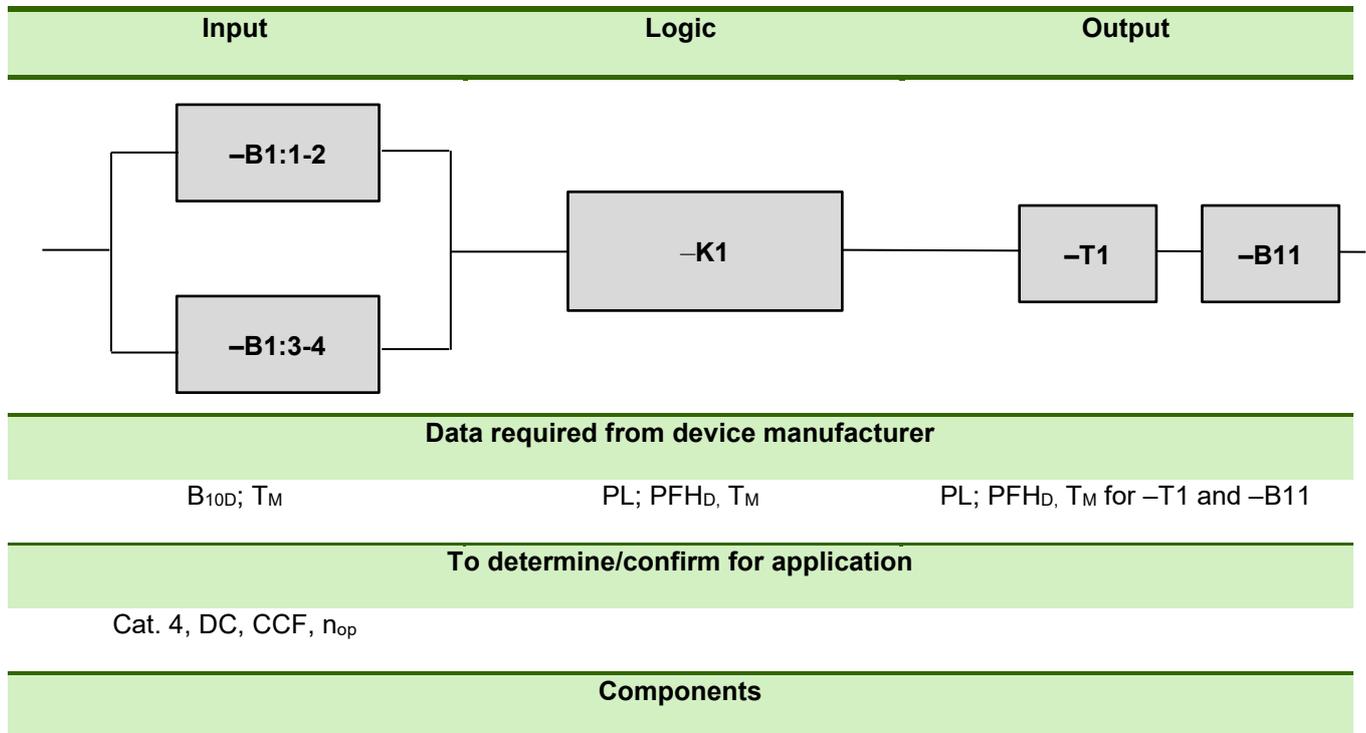
Components		

3.1.8 Products

Determination of key data for the components used based on manufacturer documentation.

	Product
–B1	Locking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0 Key data: • B_{10D} = 10,000,000 • T_M = 20 years
–K1	Programmable safety controller *samos* PRO: SP-COP2, article number: R1.190.1310.0 Key data: • PL = PL e • PFH_D = 1.3 x 10^{-9} • T_M = 20 years
–T1	Safe frequency converter with integrated diagnosis and an evaluation as PL e. Integrated SS2 safety function. Key data: • PL = PL e • PFH_D =7.79 x 10^{-10} • T_M = 20 years
–B11	Safe rotary encoder (for connection to –T1) Key data: • PL = PL d • PFH_D =2.16 x 10^{-8} • T_M = 20 years

Safety functions

Door switch, magnetic – SS2 in PL d

3.1.9
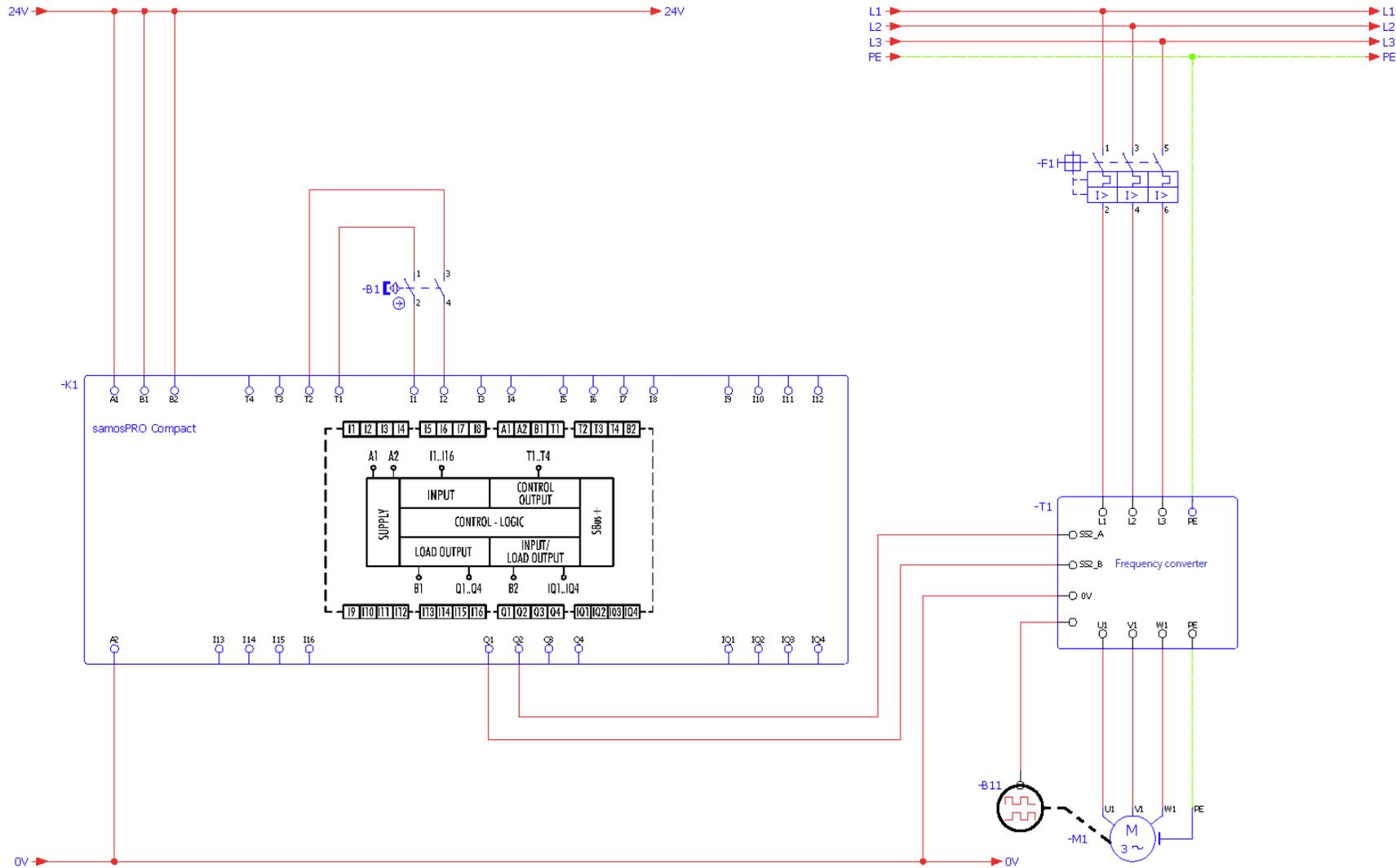
Safety functions

Door switch, magnetic – SS2 in PL d

3.1.10 Determination of the MTTF$_D$ of the individual subsystem channels – input based on frequency of use

For components on which wear is dependent on frequency of use, the MTTF$_D$ is determined over 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$_{op}$	$n_{\mathrm{op}} = \dfrac{d_{\mathrm{op}} \cdot h_{\mathrm{op}}}{t_{\mathrm{zyklus}}} \cdot 3600 \dfrac{s}{h}$ **1,460**	
Determine MTTF$_D$	MTTF$_D$	$MTTF_{\mathrm{D}} = \dfrac{B_{10D}}{0{,}1 \cdot n_{\mathrm{op}}}$ **68,493**	

Safety functions

Door switch, magnetic – SS2 in PL d

3.1.11 Determination of DC for subsystem input

Determine DC for subsystem. Ideally, based on EN ISO 13849-1 Appendix E.

Subsystem	Input			
Values per EN ISO 13849-1 Appendix E or through values determined by FMEA	Components	DC		Justification
	–B1	**99**	**%**	**Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance)**
Determine DC_{avg} (no restriction of MTTF$_D$ to 100 or, say, 2500 years)	DC_{avg}	$DC_\mathrm{avg} \; = \; \dfrac{\dfrac{DC_1}{MTTF_{D,1}} + \dfrac{DC_2}{MTTF_{D,2}} + \; ... \; + \dfrac{DC_n}{MTTF_{D,n}}}{\dfrac{1}{MTTF_{D,1}} + \dfrac{1}{MTTF_{D,2}} + \; ... \; + \dfrac{1}{MTTF_{D,n}}}$ **99**		
DC description (high / average / low / none)	DC_{avg}	**High**		

3.1.12 Determination of MTTF$_D$ for subsystem input

For the subsystem input from the MTTF$_D$ values of the individual components, determine the MTTF$_D$ of the subsystem.

Subsystem	Input			
Manufacturer data or calculated values	Components	MTTF$_D$	T$_{10D}$	
	–B1	**68,493**	**6,849**	Years
MTTF$_D$ channel 1	MTTF$_{D,C1}$	$MTTF_{D,Ci} = \dfrac{1}{\sum_{i=1}^{n} \dfrac{1}{MTTF_{D,i}}}$ **68,493**		
MTTF$_D$ channel 2	MTTF$_{D,C2}$	**68,493**		
If 2 channels (limit channels to 100 or 2500 years)	MTTF$_{D,ges}$	$MTTF_{D,ges} = \dfrac{2}{3}\left[MTTF_{D,C1} + MTTF_{D,C2} - \dfrac{1}{\dfrac{1}{MTTF_{D,C1}} + \dfrac{1}{MTTF_{D,C2}}} \right]$ **2,500**		
MTTF$_{D,ges}$	MTTF$_{D,ges}$	**2,500**		

3.1.13 Determination of CCF for subsystem input

If a Category 2 or higher is used for the subsystem and not all the elements can be classified with the PL values from the manufacturer, the CCF for the subsystem must be determined.

Measures against CCF	For electronics	Points	Fulfilled?
Separation between signal paths	Clearance and creepage distances on printed circuits	15	**15**
Diversity	E.g., different processors	20	**0**
Protection against overvoltage, overpressure…	Protection against overvoltage (e.g., fuses, power supply units)	15	**15**
Use of validated components		5	**0**
FMEA in development	FMEA during Conception of the System	5	**5**
Competence/education	Certification measures	5	**5**
Protection from contamination and EMC	EMC check	25	**25**
Other influences (temperature, shock, etc.)	Maintains environmental conditions per product specifications	10	**10**
Total CCF	Sum of points tallies ($65 \leq CCF \leq 100$):		**75**

3.1.14 Determination of PL and PFH_D for subsystem input

With the determined data, the PL and PFH_D can be determined for the subsystem input based on EN ISO 13849-1 Appendix K (see Section 5.2.6).

Subsystem	Input	
Dependent on subsystem	Determined values (ISO 13849-1 Appendix K)	
$MTTF_{D,ges}$	2,500	Years
DC_{avg}	99	%
Category	4	
PL	e	
PFH_D	9.06×10^{-10}	1/h
CCF fulfilled?	Yes	Fulfilled?
T_M	20 years	Years

3.1.15 Determination of PL and PFH$_D$ for subsystem logic

Because the subsystem logic is a pre-certified component, no data need to be determined.

Subsystem	Logic – SPS –K1	
Dependent on subsystem	Manufacturer data	
Category	**4**	
PL	**PL e**	
PFH$_D$	**1.1 x 10^{-9}**	1/h
T$_M$	**20 years**	Years

3.1.16 Determination of PL and PFH$_D$ for subsystem output

The subsystem output consists of two pre-certified components. These can be considered either as separate subsystems or as shown here, combined into a single subsystem.

Subsystem	Output				
Values per manufacturer specification	Components	PL	PFH$_D$	Cat	T$_M$
	–T1	**e**	**7.79 x 10^{-10}**	**4**	**20**
	–B11	**d**	**2.16 x 10^{-8}**	**3**	**20**
Determine PFH$_D$	PFH$_D$	**PFH$_D$ = 7.79 x 10^{-10} + 2.16 x 10^{-8}** **= 2.24 x 10^{-8}**		$PFH_D = \sum_i PFH_{D,i}$	
Determine PL	PL	$PL \leq \min_i PL_i$ Also take into account PL limit for PFH$_D$ **PL d**			
Determine Cat.	Cat	$Cat \leq \min_i Cat_i$ **Cat. 3**			

Safety functions

Subsystem	Output	
Dependent on subsystem	Determined data	
Category	3	
PL	PL d	
PFH_D	2.24×10^{-8}	1/h
T_M	20	Years

3.1.17 Determination of total PL

Based on the previously determined subsystem values, the total PL is determined. Then whether the resulting PL is sufficient for the required PL is determined.

Input	Logic	Output

Determined data for subsystems		
• PL e • $PFH_D = 9{,}06 \times 10^{-10}$ • CCF = 75 – fulfilled	• PL e • $PFH_D = 1.1 \times 10^{-9}$ • No CCF required	• PL d • $PFH_D = 2{,}24 \times 10^{-8}$ • No CCF required
Cat. 4	**Cat. 4**	**Cat. 3**
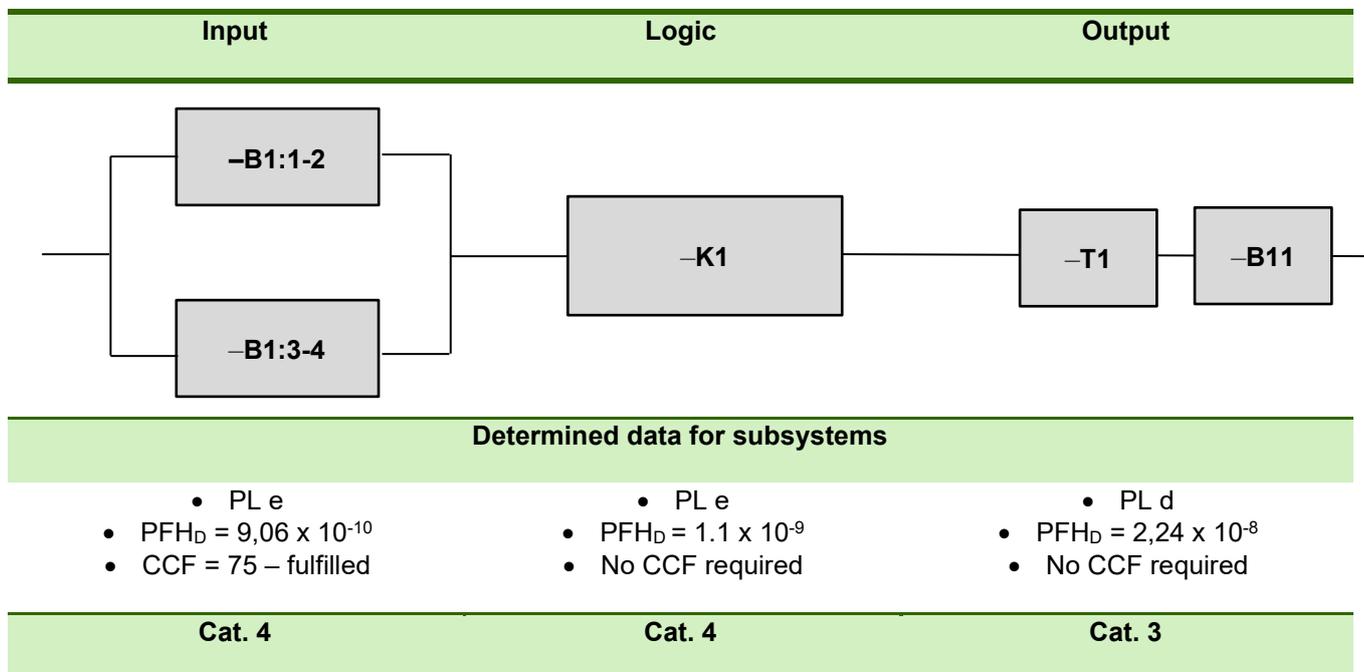
Safety functions

Door switch, magnetic – SS2 in PL d

Summary		
Required performance level	PL_r	**PL d**
CCF fulfilled for all subsystems?	Fulfilled?	**Yes**
Category requirements from C-standards fulfilled for all subsystems?	Fulfilled?	**No requirements**
Determine PFH$_{D,ges}$	PFH$_{D,ges}$	$$PFH_D = \sum_i PFH_{D,i}$$ **2.45 x 10^{-8}**
PFH$_D$ sufficient up to (requirement from EN ISO 13849-1 Table 3 – See 5.2.3).	PL$_{PFHD}$	**PL e**
Determine PL$_{ges}$ based on PL of subsystems and requirements from EN ISO 13849-1 Table 3.	PL$_{ges}$	$$PL_{ges} \leq \min_i PL_i$$ **PL d**
PL$_r \leq$ PL?	Fulfilled?	**Yes**

3.2 EMERGENCY stop – 1-channel in PL c

3.2.1 Safety function

Safety function	When the emergency stop button –S1 is actuated, all drives in the system are brought to a controlled standstill.
Trigger event	One of the emergency stop buttons is actuated by the operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.2.2 Description

Function	By actuating the emergency stop button –S1: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactor –Q1 is switched off • Motor –M1 is stopped
Manual reset function	The safety function manual reset is initiated when emergency stop button –S1 is rotated to unlock it.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Emergency stop button –S1 is not actuated
Feedback circuit	No feedback circuit used

3.2.3 Safety assessment

Sensor technology	• Ground faults on the sensor line in the input circuit are detected by –K1. • The emergency stop button is equipped with a malfunction safeguard. The safeguard detects when the actuator is triggered by the switch contacts and interrupts the electrical emergency stop circuit.
Actuator technology	• As entailed by EN ISO 13849-2, the actuator technology is a validated component.

Safety functions

EMERGENCY stop – 1-channel in PL c

wieland

3.2.4 Products (options)

		Product
–S1		Emergency stop control device (1-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1102 article number: R1.200.1102.0
–K1		Safety switching device *safe* RELAY: SNO 4003K article number: R1.188.0500.1
–Q3		Power contactor with the following properties: • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.2.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
B_{10D}; T_M	PL; PFH_D, T_M	B_{10D}; T_M

To determine/confirm for application		
• No CCF required • Cat. 1 • No DC required • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• No CCF required • Cat. 1 • No DC required • n_{op}

Maximum attainable PL		
PL c	PL e	PL c

PL c

Safety functions

wieland
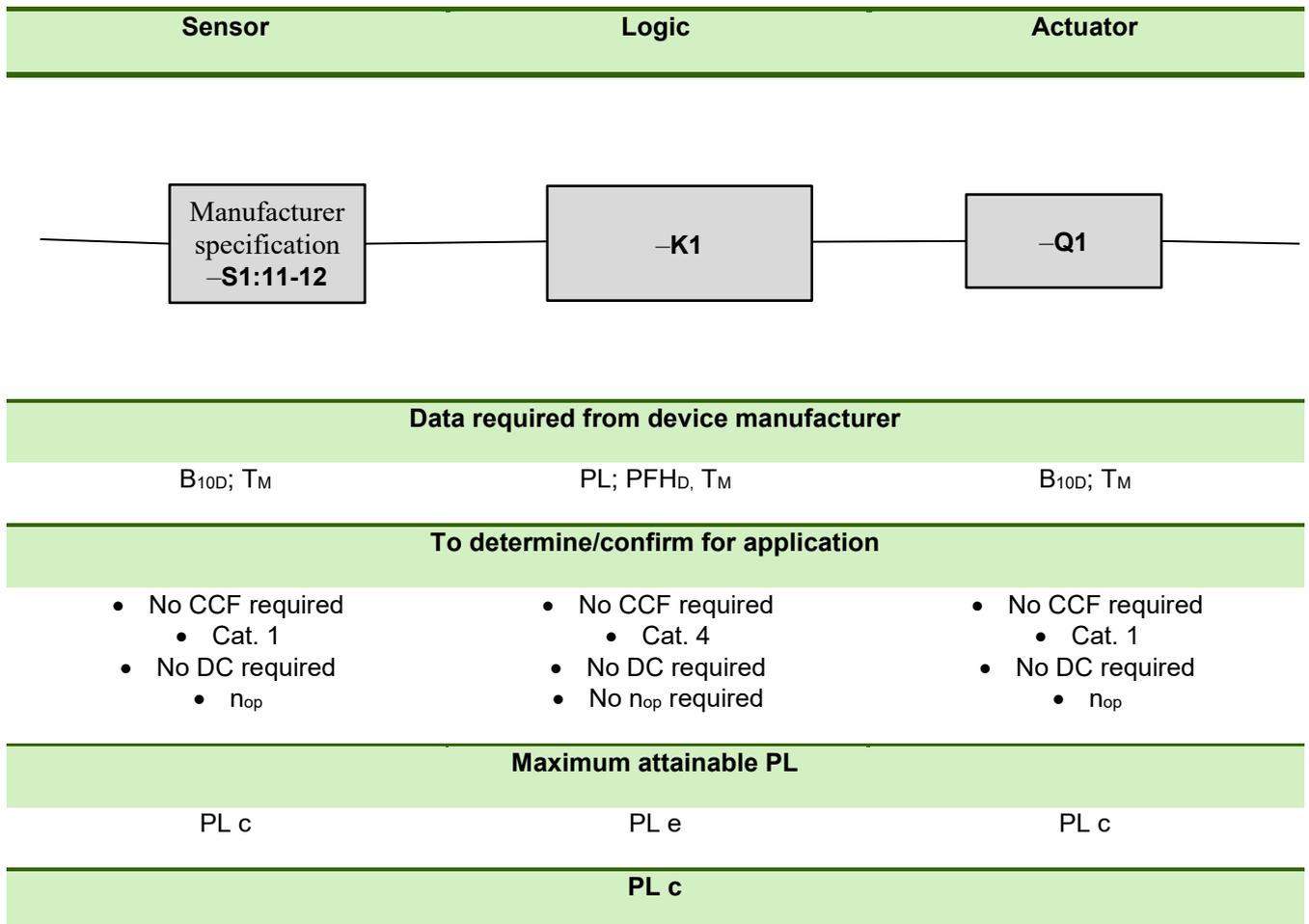
3.2.6 Circuit diagram
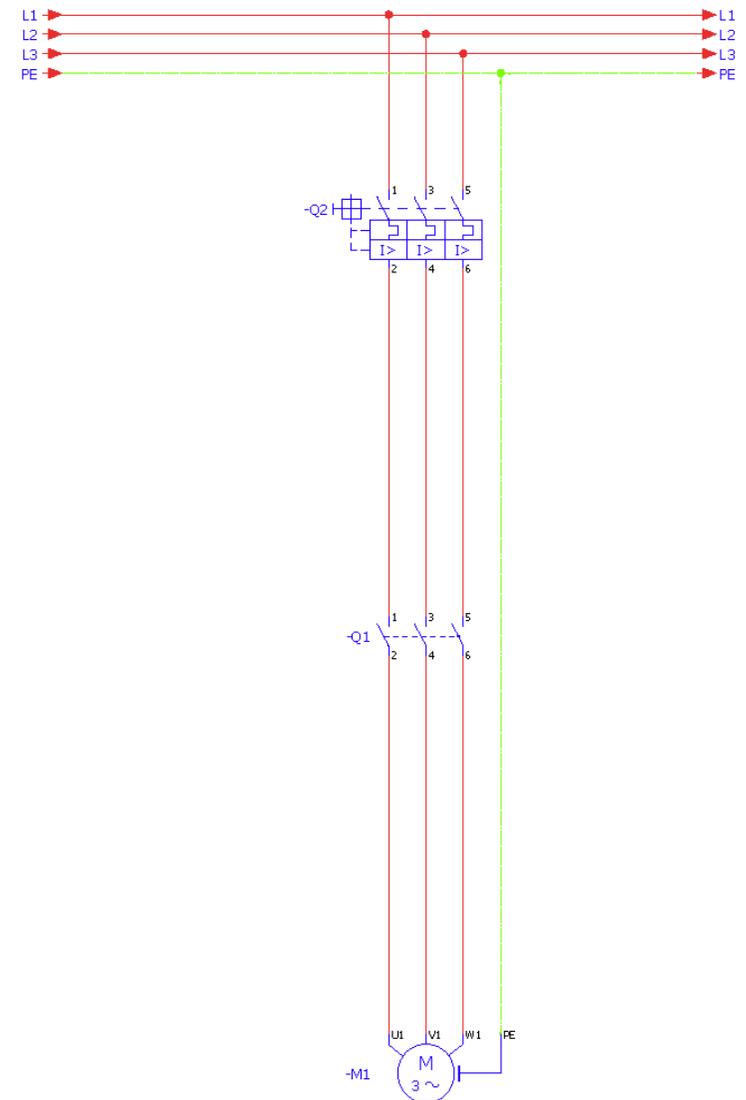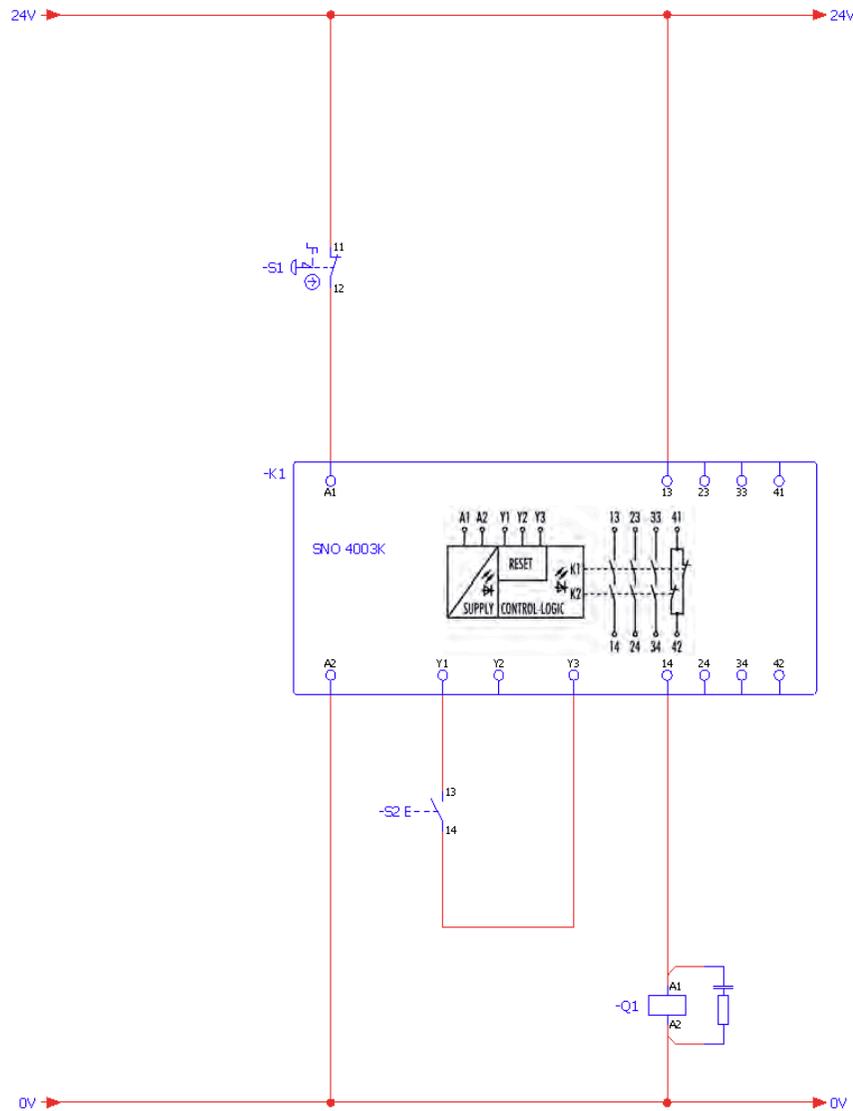
3.3   EMERGENCY stop – 2-channel in PL d

3.3.1   Safety function

Safety function	When the emergency stop button –S1 is actuated, all drives in the system are brought to a controlled standstill.
Trigger event	One of the emergency stop buttons is actuated by the operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.3.2   Description

Function	By actuating the emergency stop button –S1: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • FU –T1 with safety input STO is disconnected from power • Machine 1 is stopped.
Manual reset function	The safety function manual reset is initiated when emergency stop button –S1 is rotated to unlock it.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Emergency stop button –S1 is not actuated
Feedback circuit	Not needed here, since –T1 is a device with integrated diagnosis.

3.3.3   Safety assessment

|	
Sensor technology	• Ground faults in the input circuit are detected by –K1 through test impulses on the sensor lines. Because of the structure Cat. 3, cross shorts are not detected; thus "Cross comparison with dynamization, without high quality fault detection" → DC = 90 % • The emergency stop button is equipped with a malfunction safeguard. This feature detects when the actuator is triggered by the switch contacts and interrupts the electrical emergency stop circuit. • Synchronization time monitoring between input circuits –S12 and –S22
Actuator technology	• Frequency converter with integrated diagnosis and an evaluation as PL d. • STO input classified as PL d. • Faults excluded on wiring from –K1 to –T1 because it is in control cabinet

3.3.4 Products (options)

|		Product
–S1		Emergency stop control device (2-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1122 article number: R1.200.1122.0
–K1		Safety switching device *safe* RELAY: SNO 4062KM article number: R1.188.0720.2
–T1		Safe frequency converter with integrated diagnosis and an evaluation as PL d. Integrated STO safety function.

3.3.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	PL; PFH_D, T_M

To determine/confirm for application		
• CCF ≥ 65 points • Cat. 3 • DC = 90% • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• No CCF required • Cat. 3 • No DC required • No n_{op} required

Maximum attainable PL		
PL d	PL e	PL d

PL d

Safety functions

EMERGENCY stop – 2-channel in PL d

wieland

3.3.6   Circuit diagram

3.4 EMERGENCY stop – 2-channel, cross short circuit detection in PL e

3.4.1 Safety function

Safety function	When the emergency stop button –S1 is actuated, all drives in the system are brought to a controlled standstill.
Trigger event	One of the emergency stop buttons –S1 is actuated by the operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.4.2 Description

Function	By actuating the emergency stop button –S1: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off. • Machine M1 is stopped.
Manual reset function	The safety function manual reset is initiated when emergency stop button –S1 is rotated to unlock it.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Emergency stop button –S1 is not actuated • Contactors –Q1 and –Q2 are switched off
Feedback circuit	The positively driven NC contacts of contactor –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of –K1.

3.4.3 Safety assessment

Sensor technology	• Ground faults and cross shorts in the input circuit are detected by –K1 through test impulses on the sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99% • The emergency stop button is equipped with a malfunction safeguard. This feature detects when the actuator is triggered by the switch contacts and interrupts the electrical emergency stop circuit. • Synchronization time monitoring between input circuits –K1:S12 and –K1:S22
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

3.4.4 Products (options)

	Product
–S1	Emergency stop control device (2-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1122 article number: R1.200.1122.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

EMERGENCY stop – 2-channel, cross short circuit detection in PL e

3.4.5   Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Manufacturer specification −S1:11-12

Manufacturer specification −S1:21-22

−K1

−Q1

−Q2

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
  • Cat. 4
 • DC = 99%
  • n_{op}
	• No CCF required
	  • Cat. 4
	 • No DC required
	 • No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		 • DC = 99%
		  • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e
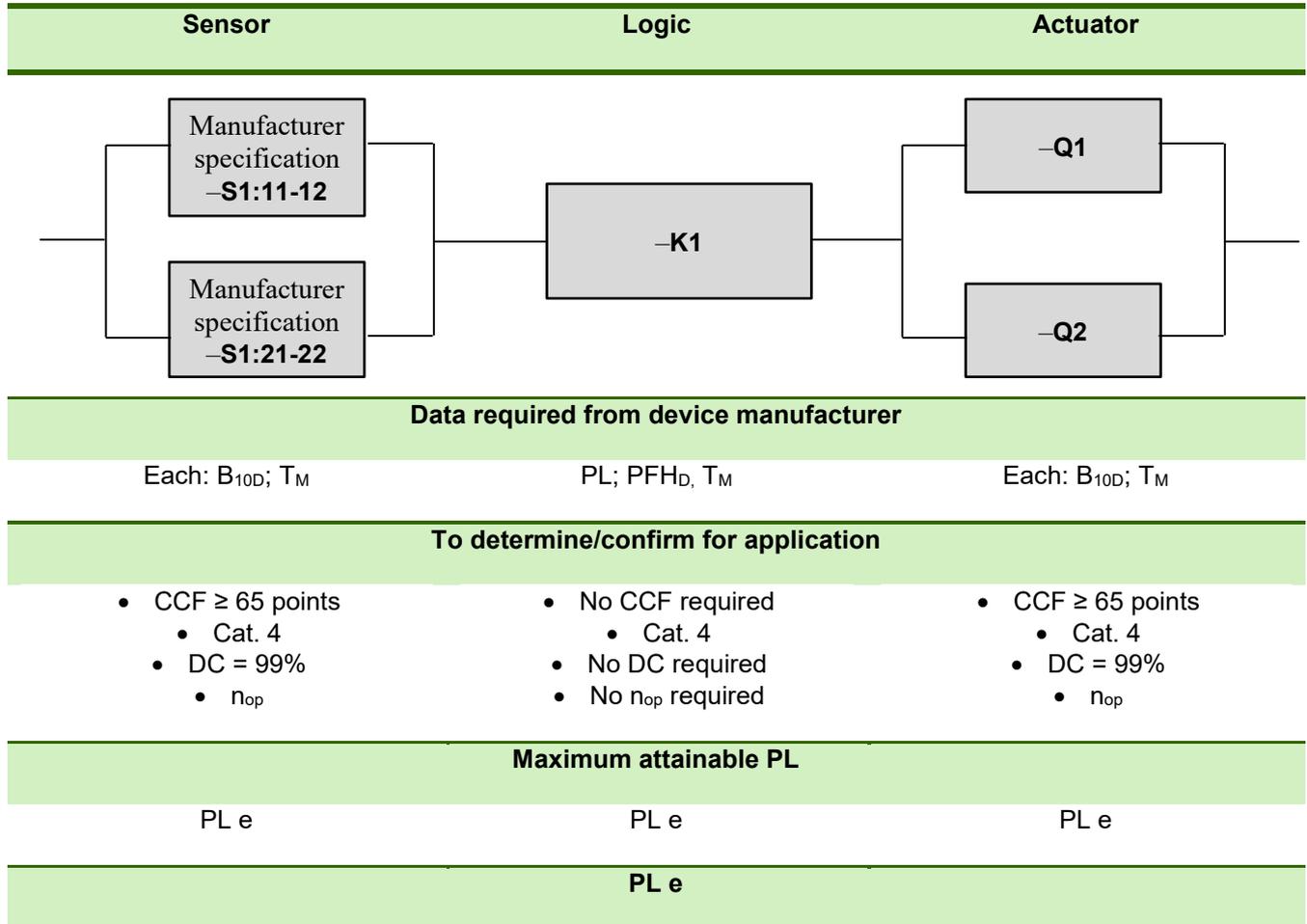
Safety functions

EMERGENCY stop – 2-channel, cross short circuit detection in PL e

3.4.6 Circuit diagram
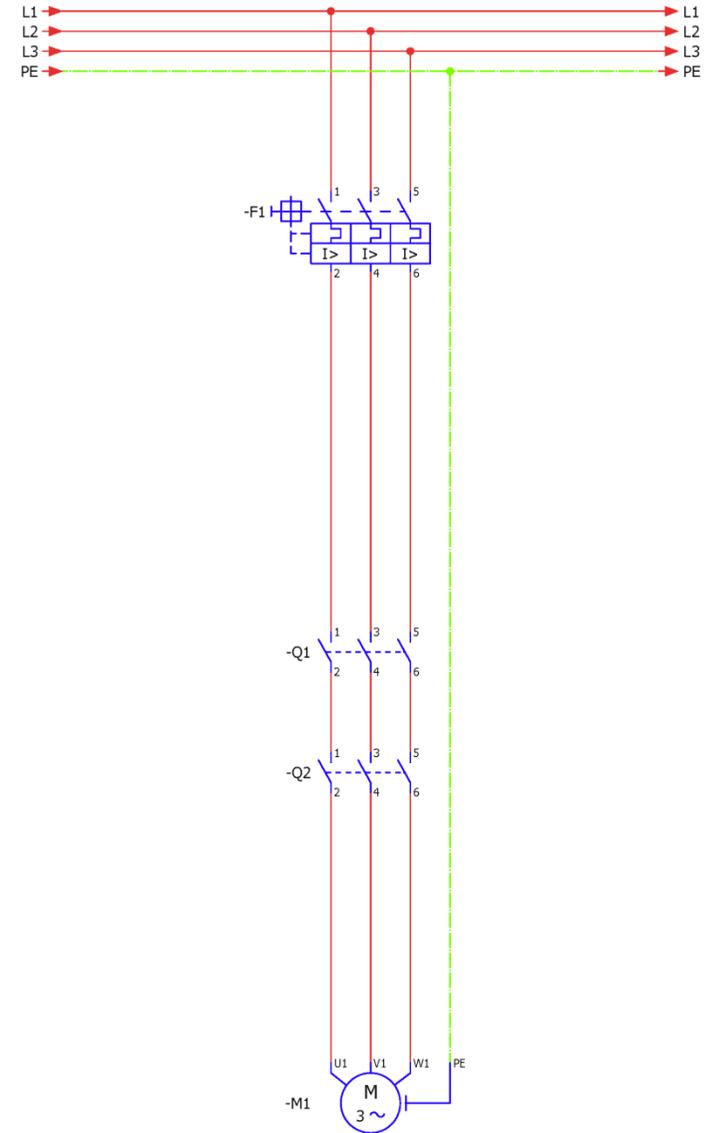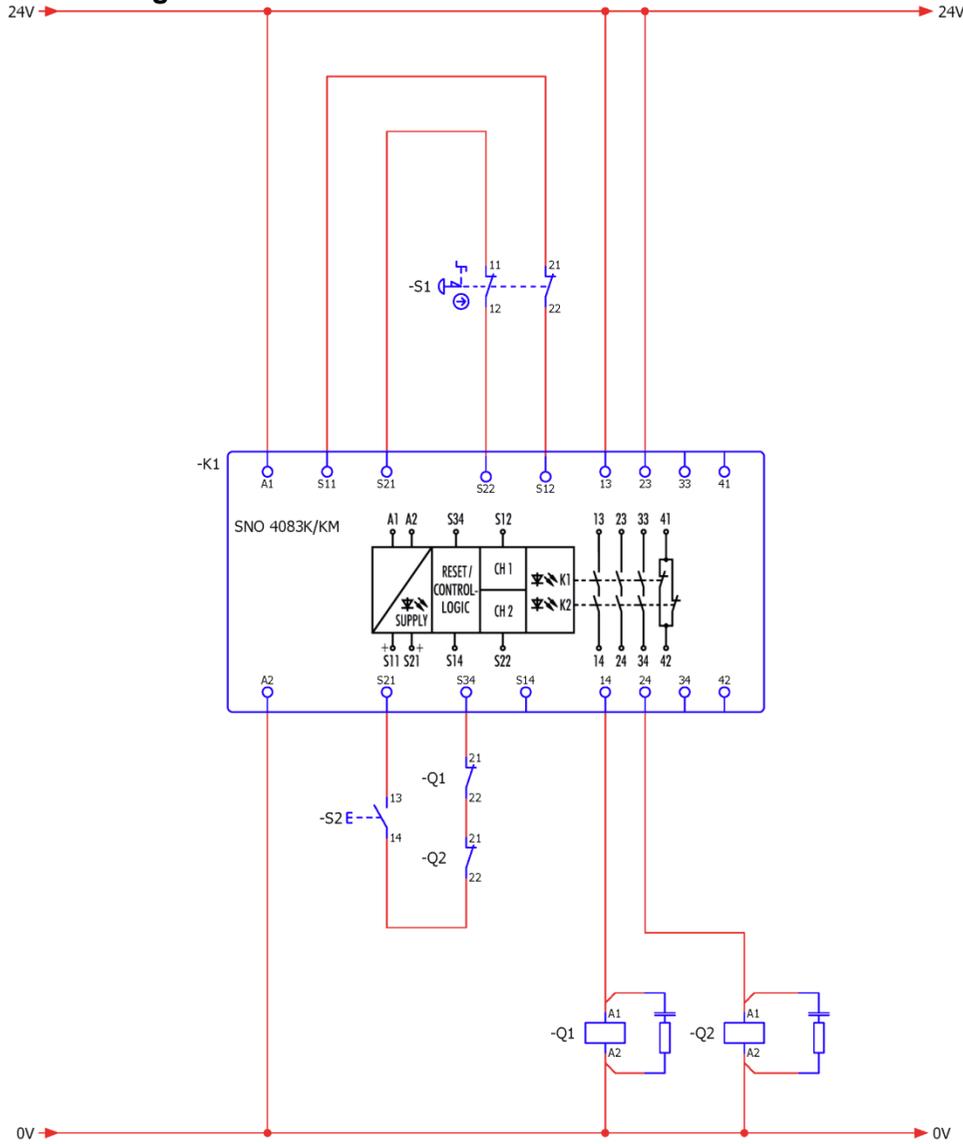
3.5 Door switch, mechanical – 1-channel in PL c

3.5.1 Safety function

Safety function	When the door is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	A door is opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.5.2 Description

Function	By opening the door(s): • Door switch is actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactor –Q1 is switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door. Door switch –B1 is closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door(s). Start/restart must only be possible when: • The doors are closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contact of contactor –Q1 is monitored in the feedback circuit of safety switch device –K1.

3.5.3 Safety assessment

Sensor technology	• Ground faults on the sensor line in the input circuit are detected by –K1. • A fault may lead to loss of the safety function. DC = None • Faults are first recognized during the next test cycle (manual).
Actuator technology	The contactor is equipped with a positively driven feedback contact. DC = 99%. However, no reaction to faults is possible and in Cat. 1, no DC is required.

3.5.4 Products (options)

		Product
–B1		Locking device, design 2 (door switch with separate actuator) *sensor* PRO: SMS3x10 article number: R1.320.3010.0
–K1		Safety switching device *safe* RELAY: SNO 4003K article number: R1.188.0500.1
–Q1		Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.5.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
B_{10D}; T_M	PL; PFH_D, T_M	B_{10D}; T_M

To determine/confirm for application		

• No CCF required
  • Cat. 1
• DC = None
  • n_{op}
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• No CCF required
		  • Cat. 1
		• DC = None
		  • n_{op}

Maximum attainable PL		
PL c	PL e	PL c

PL c
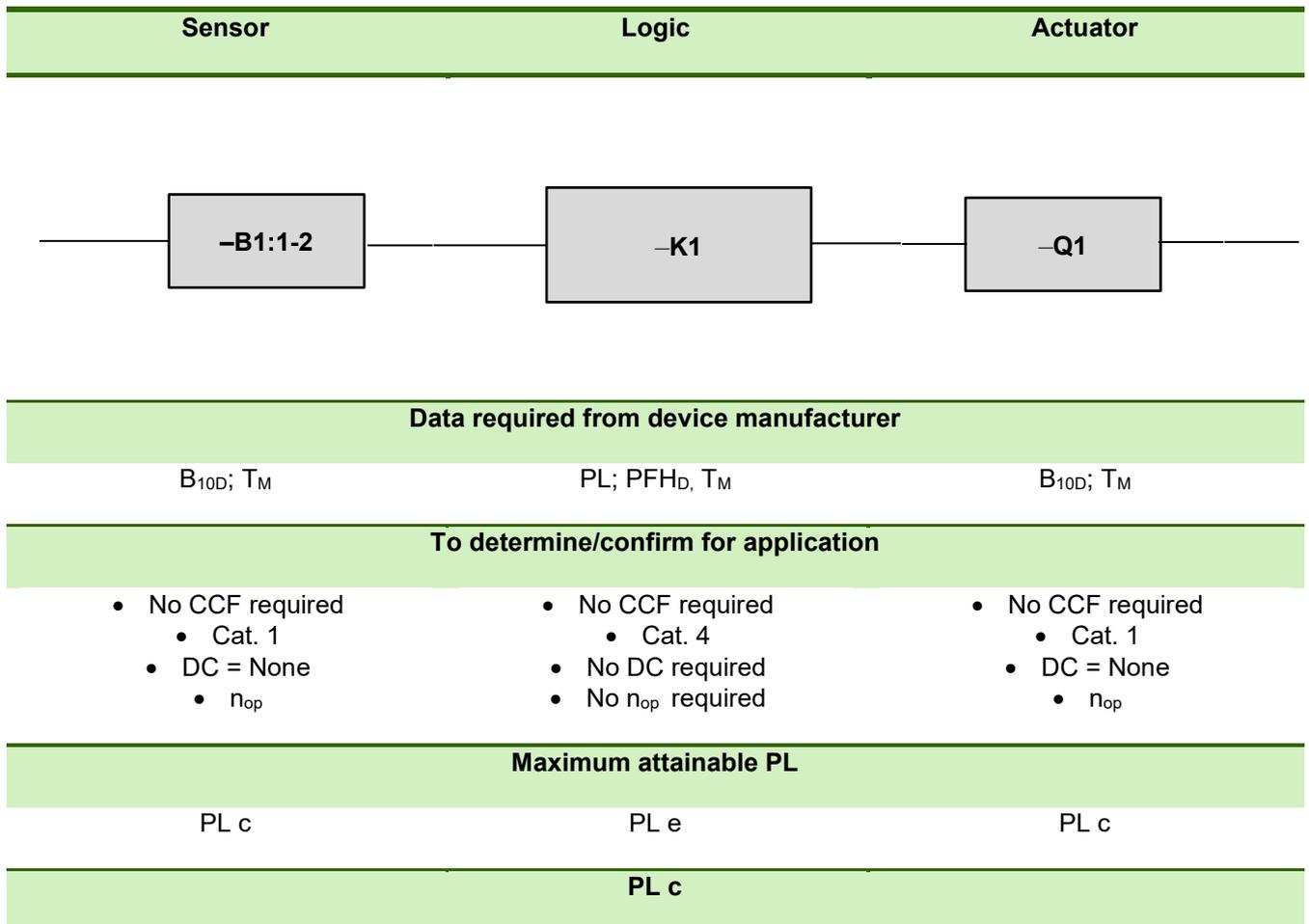
Safety functions

**Door switch, mechanical – 1-channel in PL c**

3.5.6 Circuit diagram
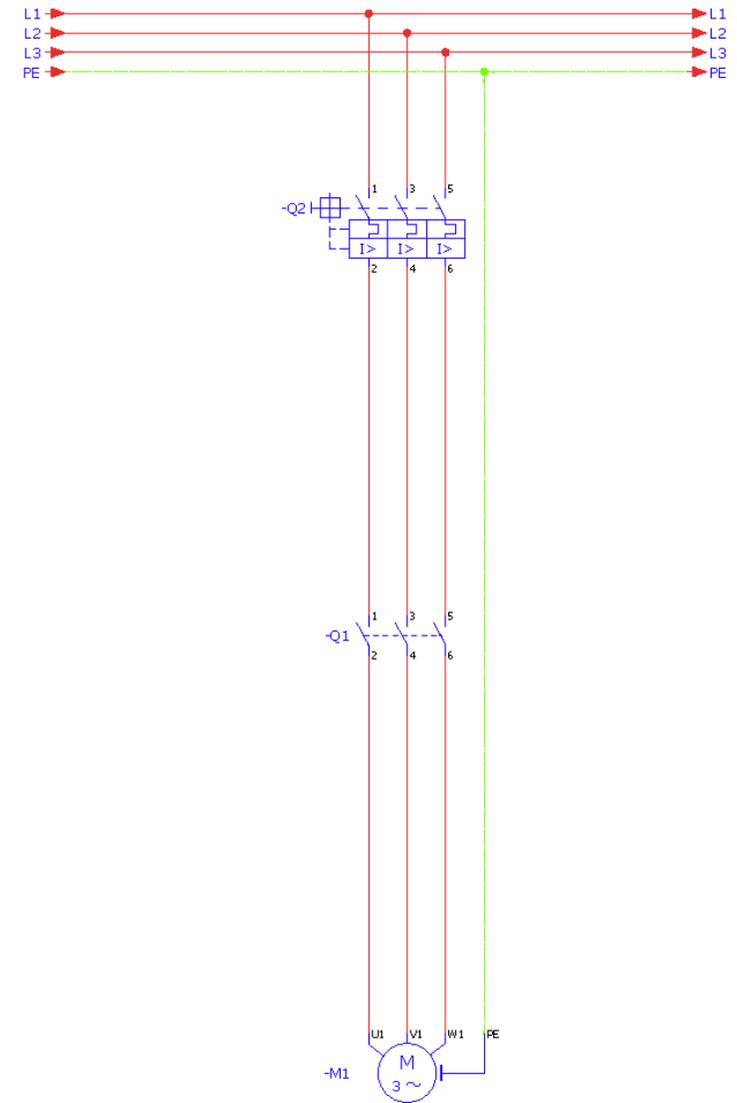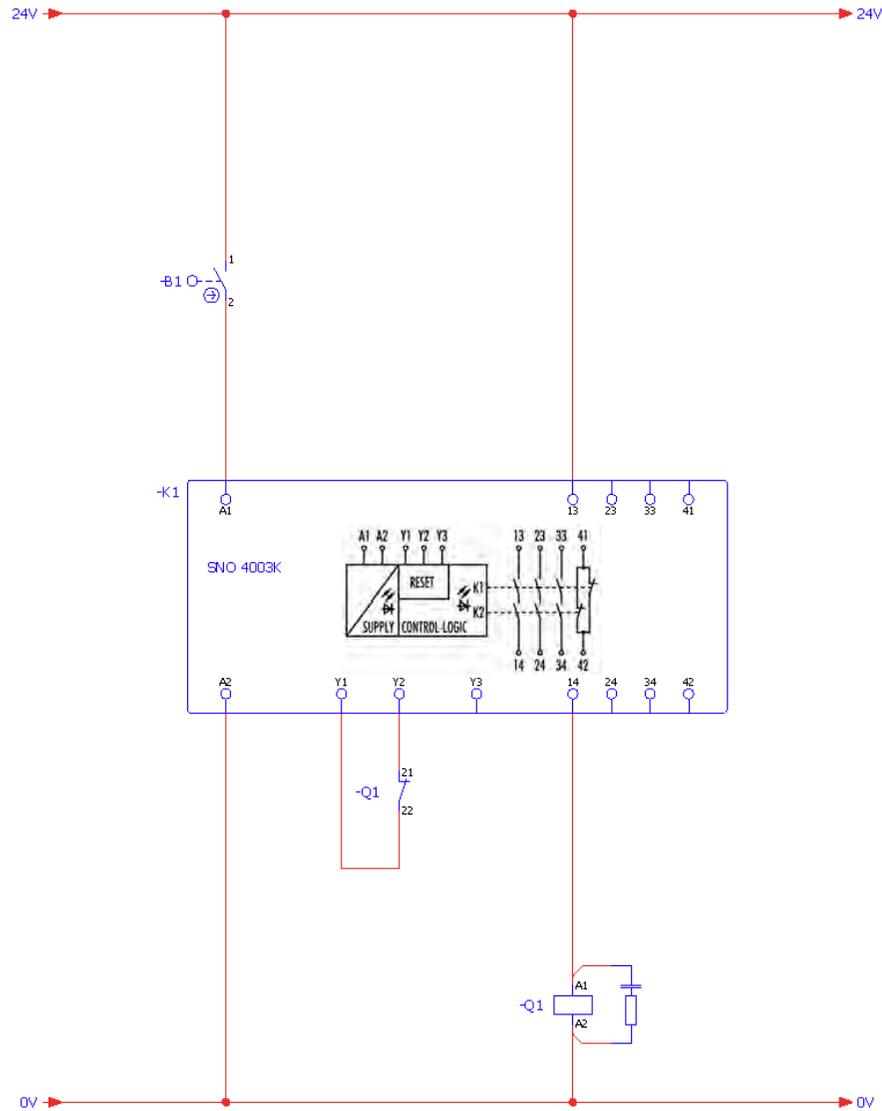
3.6 Door switch, mechanical – 2-channel equivalent in PL c/d

3.6.1 Safety function

Safety function	When the door is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Door opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.6.2 Description

Function	By opening the door(s): • Door switch is actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door. Door switch –B1 is closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door. Start/restart must only be possible when: • The doors are closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.6.3 Safety assessment

| Sensor technology	• Ground faults and cross shorts in the input circuit are detected by –K1 through test impulses on the sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. Fault exclusions: • Fault exclusion upon actuator breakage by machine builder. Normally, at minimum the installation requirements according to the instructions of the switch manufacturer apply here. • Fault exclusion upon mechanical switch failure. Normally, at minimum the installation requirements according to the instructions of the switch manufacturer apply here. • If these fault exclusions are used, Cat. 4 can be achieved, but the PL is restricted to PL d. • If the exclusions are not possible, Cat. 1 is the maximum that can be reached.
Actuator technology	Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. The contactors are equipped with positively driven feedback contacts. DC = 99%

3.6.4 Products (options)

|		Product
–B1		Interlocking device, design 2 (door switch with separate actuator) *sensor* PRO: SMS2x20 article number: R1.320.2020.0
–K1		Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–Q1; –Q2		Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Door switch, mechanical – 2-channel equivalent in PL c/d

3.6.5 Modeling per EN ISO 13849-1
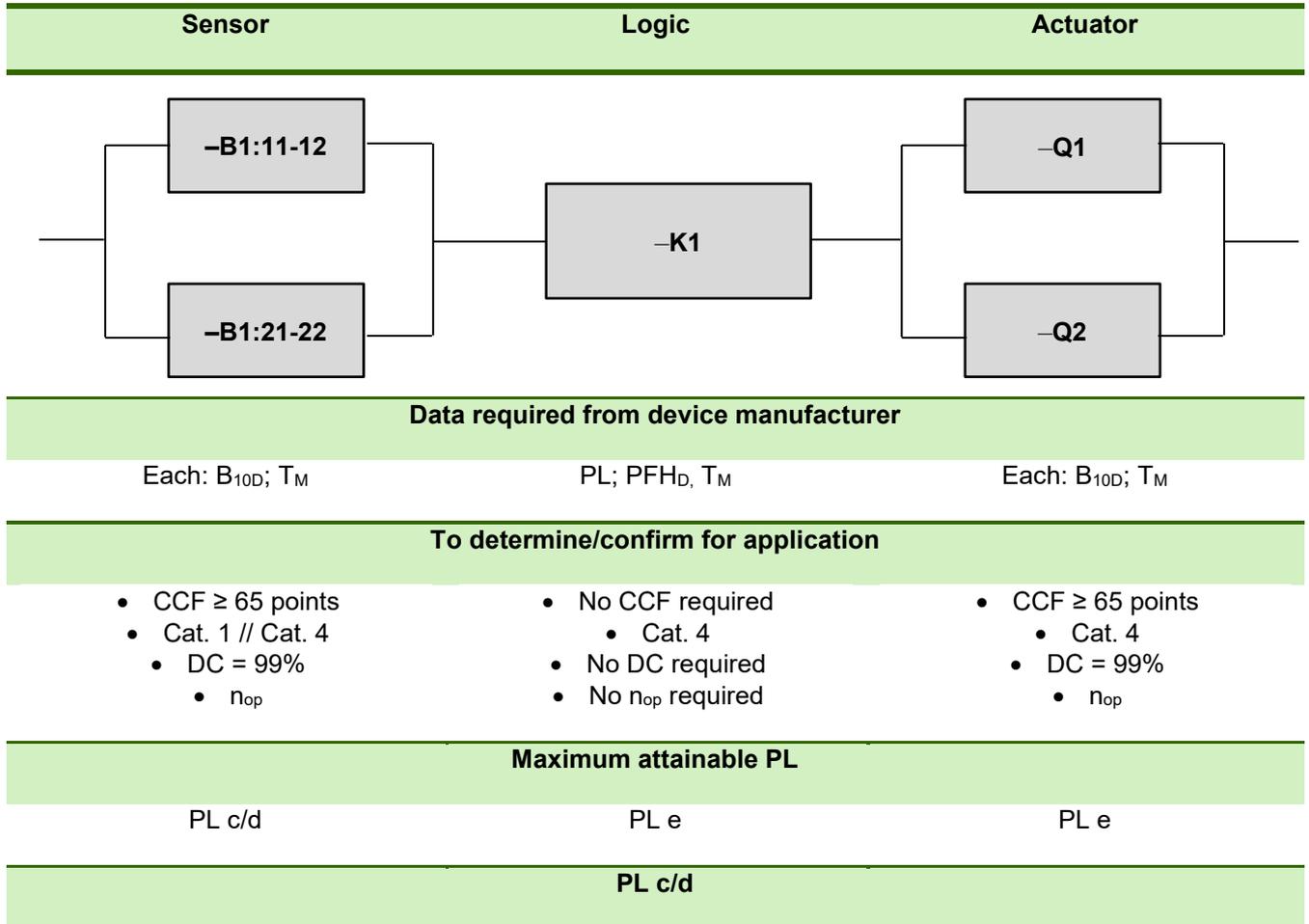
Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		
• CCF ≥ 65 points • Cat. 1 // Cat. 4 • DC = 99% • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• CCF ≥ 65 points • Cat. 4 • DC = 99% • n_{op}

Maximum attainable PL		
PL c/d	PL e	PL e

PL c/d

3.6.6 Circuit diagram
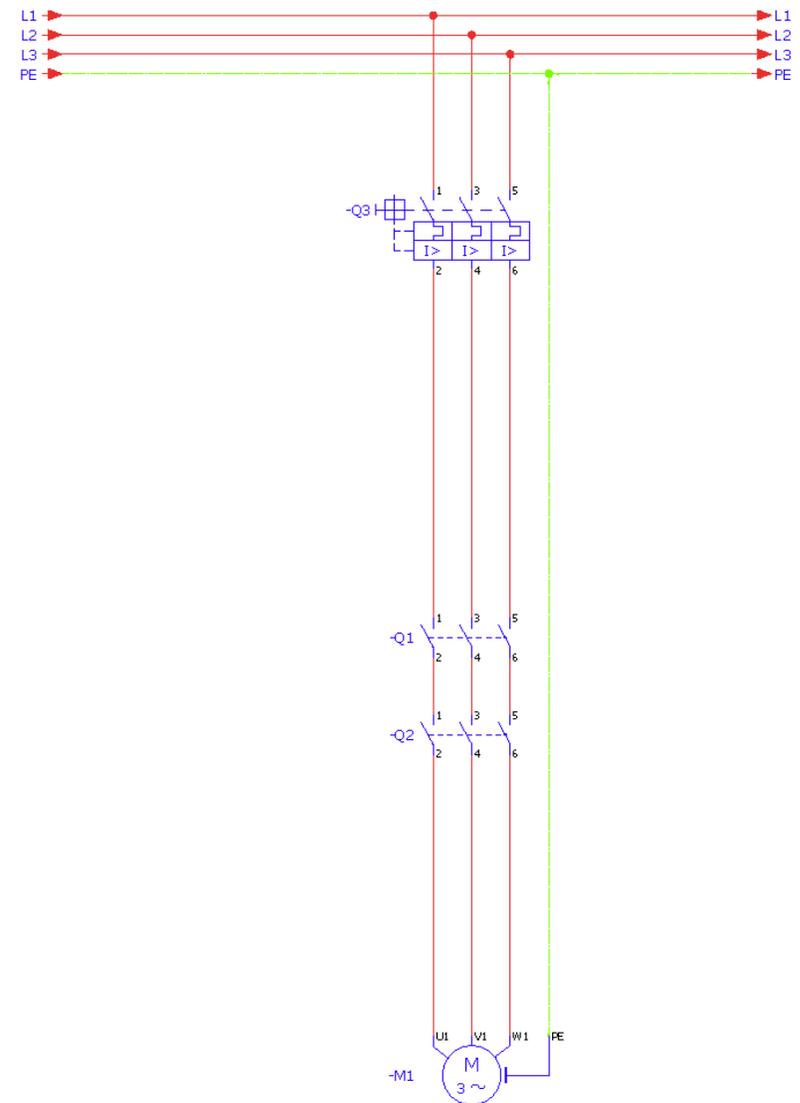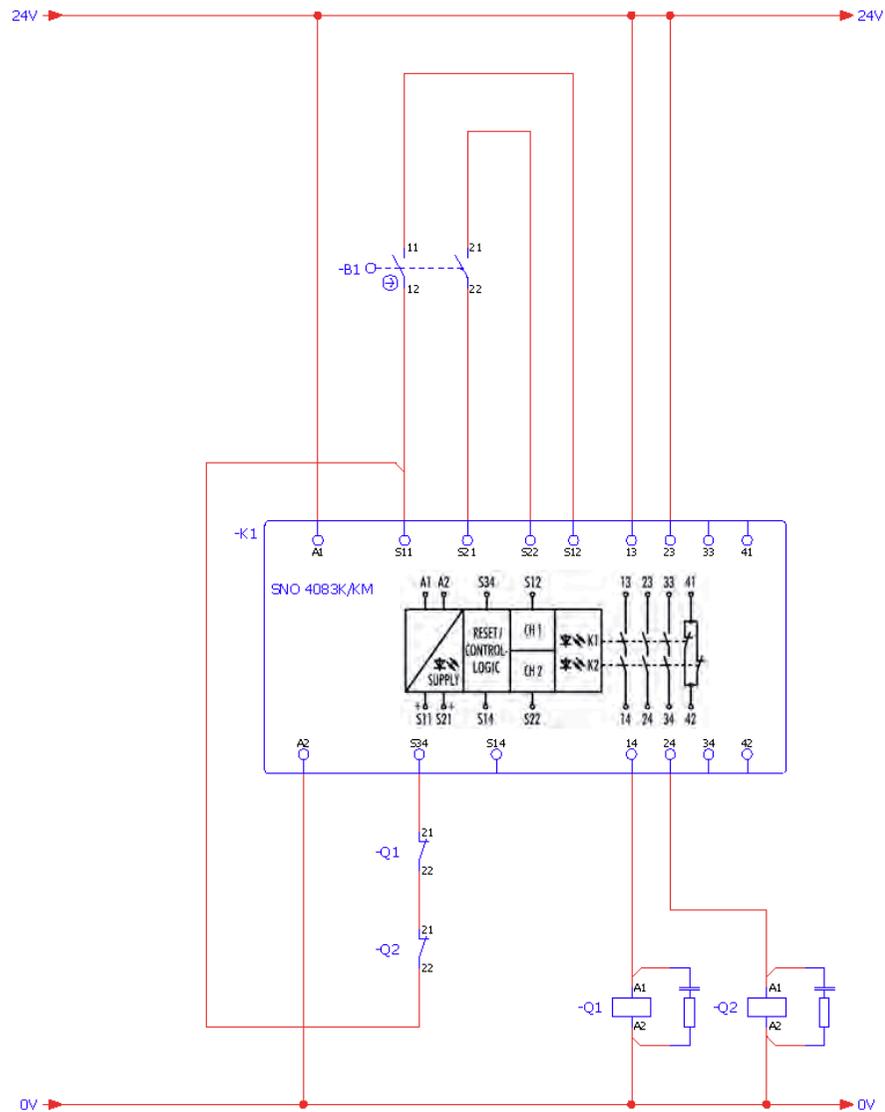
3.7 Door switch, mechanical – 2-channel antivalent in PL c/d

3.7.1 Safety function

Safety function	When the door is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Door opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.7.2 Description

Function	By opening the door(s): • Door switch is actuated • Input circuit is interrupted/closed at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door. Door switch –B1 is closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door. Start/restart must only be possible when: • The doors are closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

Safety functions

Door switch, mechanical – 2-channel antivalent in PL c/d

3.7.3 Safety assessment

|	
Sensor technology	• Ground faults, cross shorts and short circuits to 24 VDC in the input circuit are detected by –K1 through differing potentials on the two sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. Fault exclusions: • Fault exclusion upon actuator breakage by machine builder. Normally, at minimum the installation requirements according to the instructions of the switch manufacturer apply here. • Fault exclusion upon mechanical switch failure. Normally, at minimum the installation requirements according to the instructions of the switch manufacturer apply here. • If these fault exclusions are made, Cat. 4 can be achieved, but the PL is restricted to PL d. • If the exclusions are not possible, Cat. 1 is the maximum that can be reached.
Actuator technology	Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. The contactors are equipped with positively driven feedback contacts. DC = 99%

3.7.4 Products (options)

	Product
–B1	Interlocking device, design 2 (door switch with separate actuator) *sensor* PRO: SMS2x40 article number: R1.320.2040.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Door switch, mechanical – 2-channel antivalent in PL c/d

3.7.5 Modeling per EN ISO 13849-1
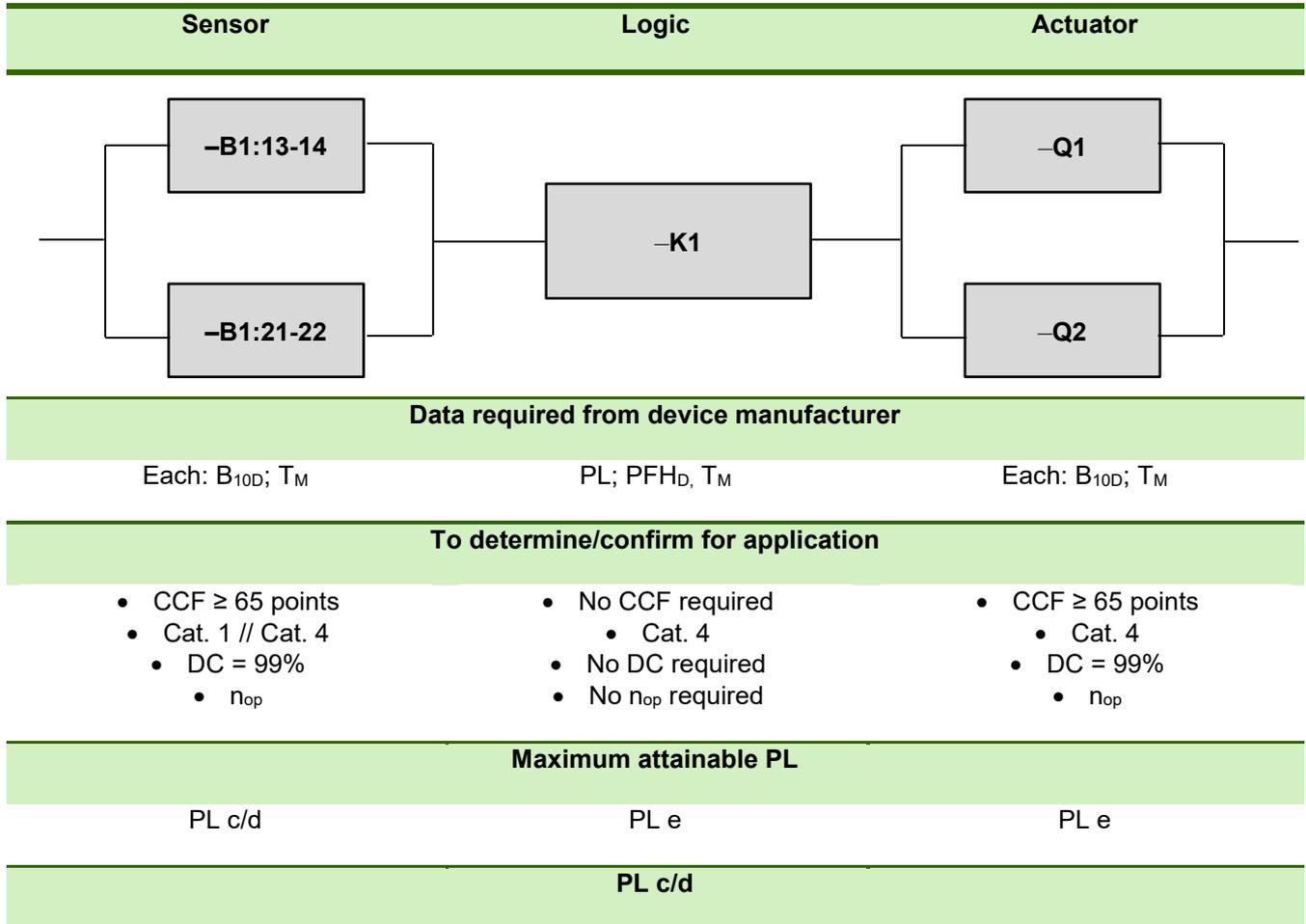
Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		
• CCF ≥ 65 points • Cat. 1 // Cat. 4 • DC = 99% • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• CCF ≥ 65 points • Cat. 4 • DC = 99% • n_{op}

Maximum attainable PL		
PL c/d	PL e	PL e

PL c/d

3.7.6 Circuit diagram

SNO 4083KM

-K1

-B1

-Q1

-Q2

-F1

-M1
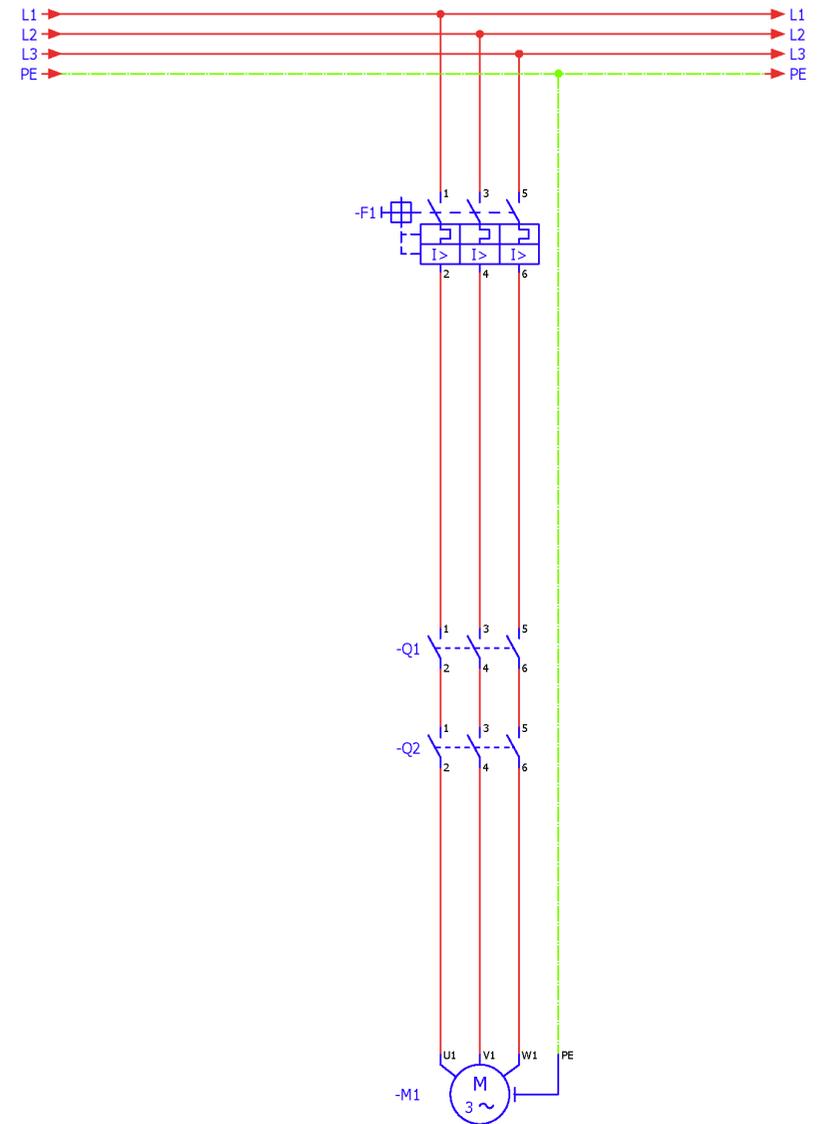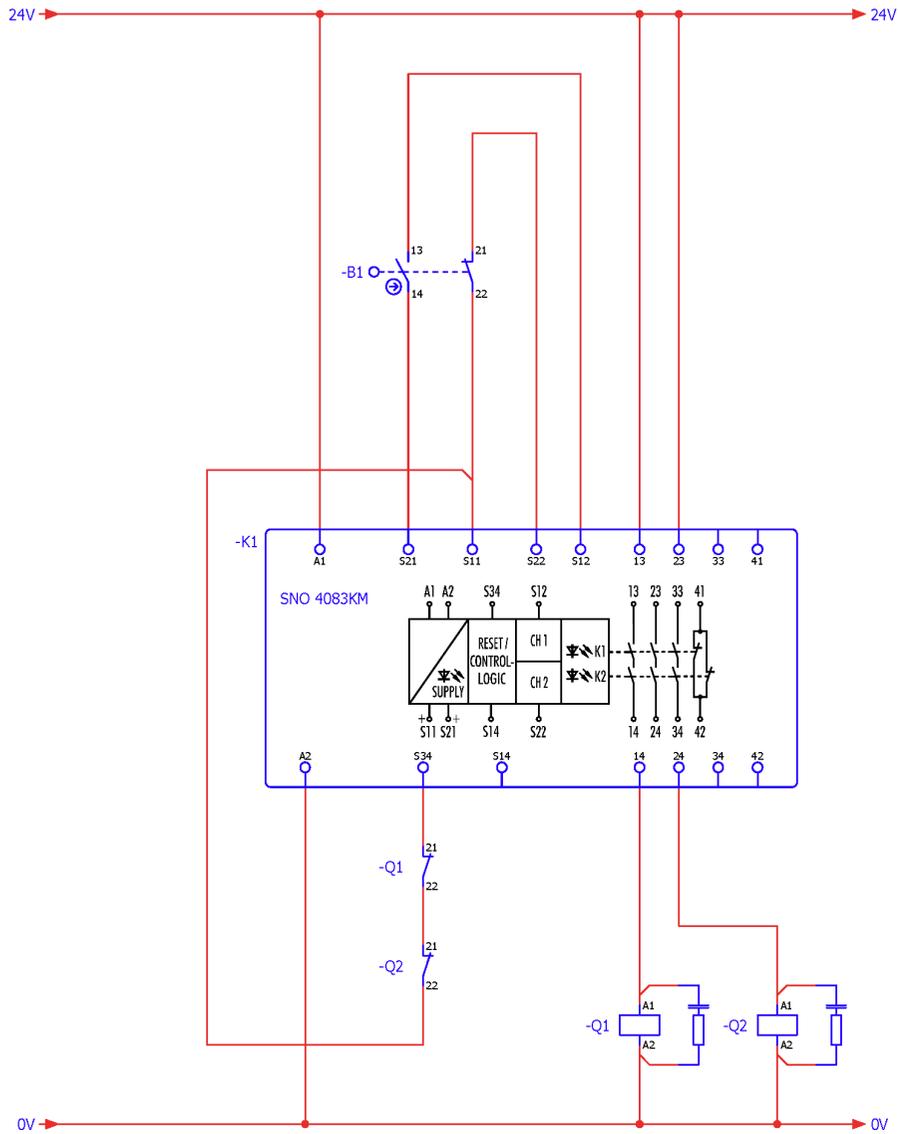
3.8   Door switch, mechanical & magnetic – each 1-channel in PL e

3.8.1   Safety function

Safety function	When the door is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Door opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.8.2   Description

Function	By opening the door(s): • Door switch –B1 is actuated • Door switch is –B2 is actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door. Door switches –B1 and –B2 are closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door. Start/restart must only be possible when: • The door is closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.8.3 Safety assessment

Sensor technology	• Ground faults, cross shorts and short circuits to 24 V in the input circuit are detected by –K1 through test impulses on the sensor lines. • Because of the diverse redundancy, a single fault does not lead to loss of safety. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99%
Actuator technology	Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. The contactors are equipped with positively driven feedback contacts. DC = 99%

3.8.4 Products (options)

|	**Product**
–B1	Interlocking device, design 2 (door switch with separate actuator) and spring-actuated locking device *sensor* PRO: SIN11xx article number: R1.310.1150.0 *Note: Since this requirement frequently appears in combination with door closures, a door switch with spring-actuated locking is appropriate here. If no locking is required, a type without locking can be used; e.g., SMS3x10; article number: R1.320.3010.0.*
–B2	Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–K1	Safety switching device *safe* RELAY: SNO 4063K/KM article number: R1.188.1280.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Door switch, mechanical & magnetic – each 1-channel in PL e

3.8.5 Modeling per EN ISO 13849-1
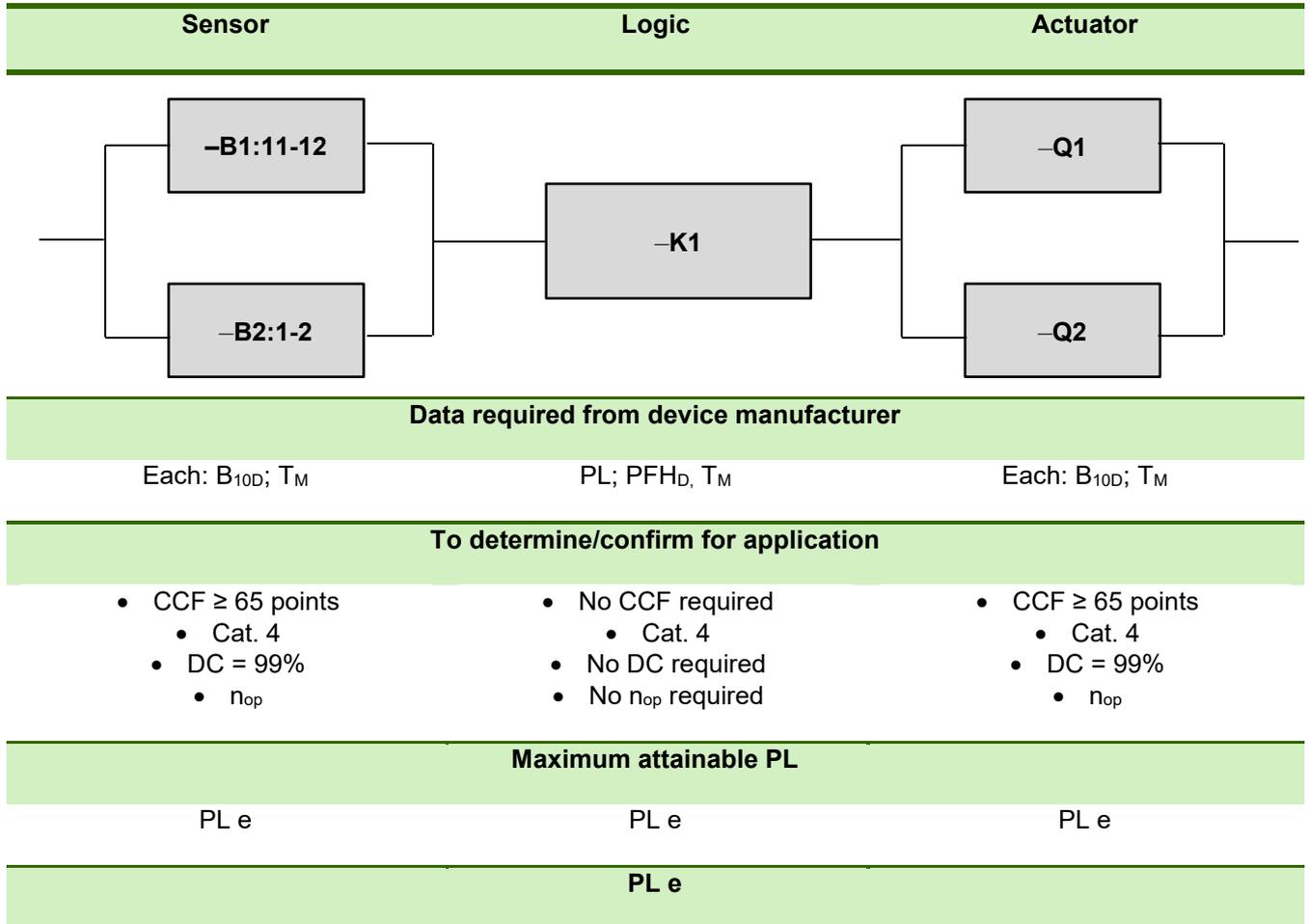
Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
  • Cat. 4
• DC = 99%
  • n_{op}
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		• DC = 99%
		  • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e

Safety functions

3.8.6   Circuit diagram
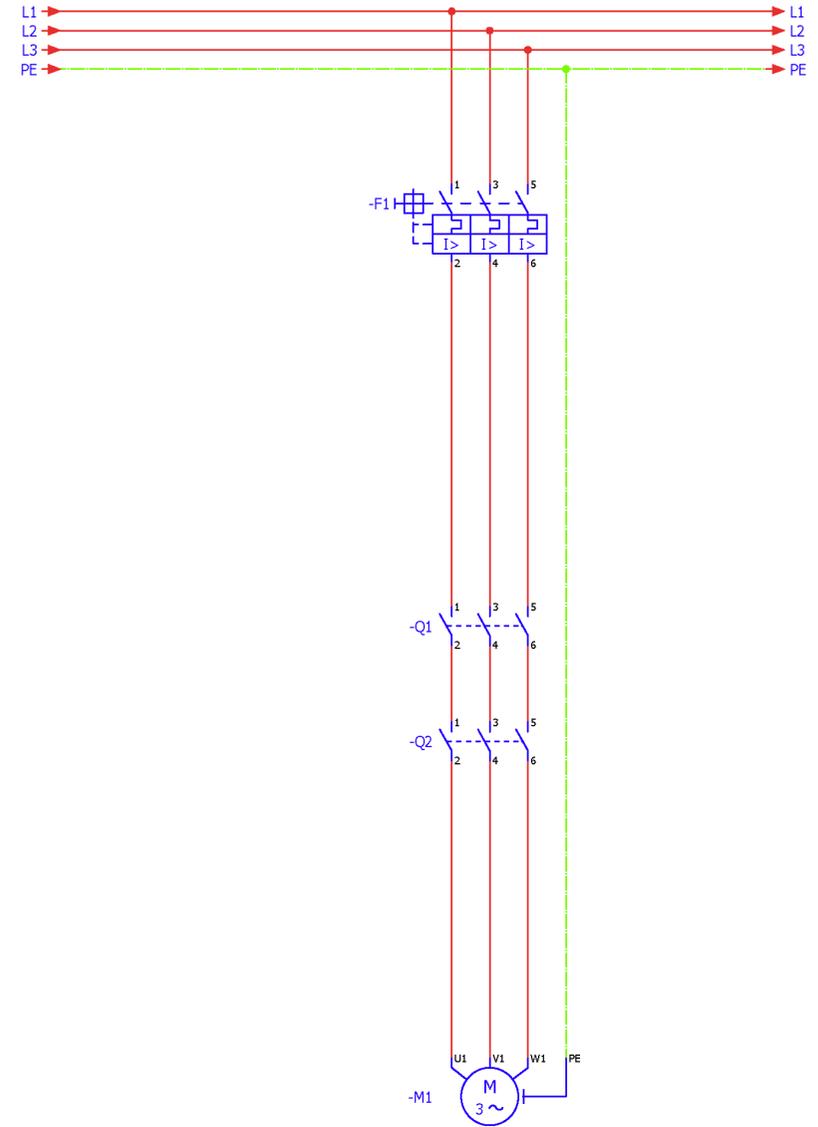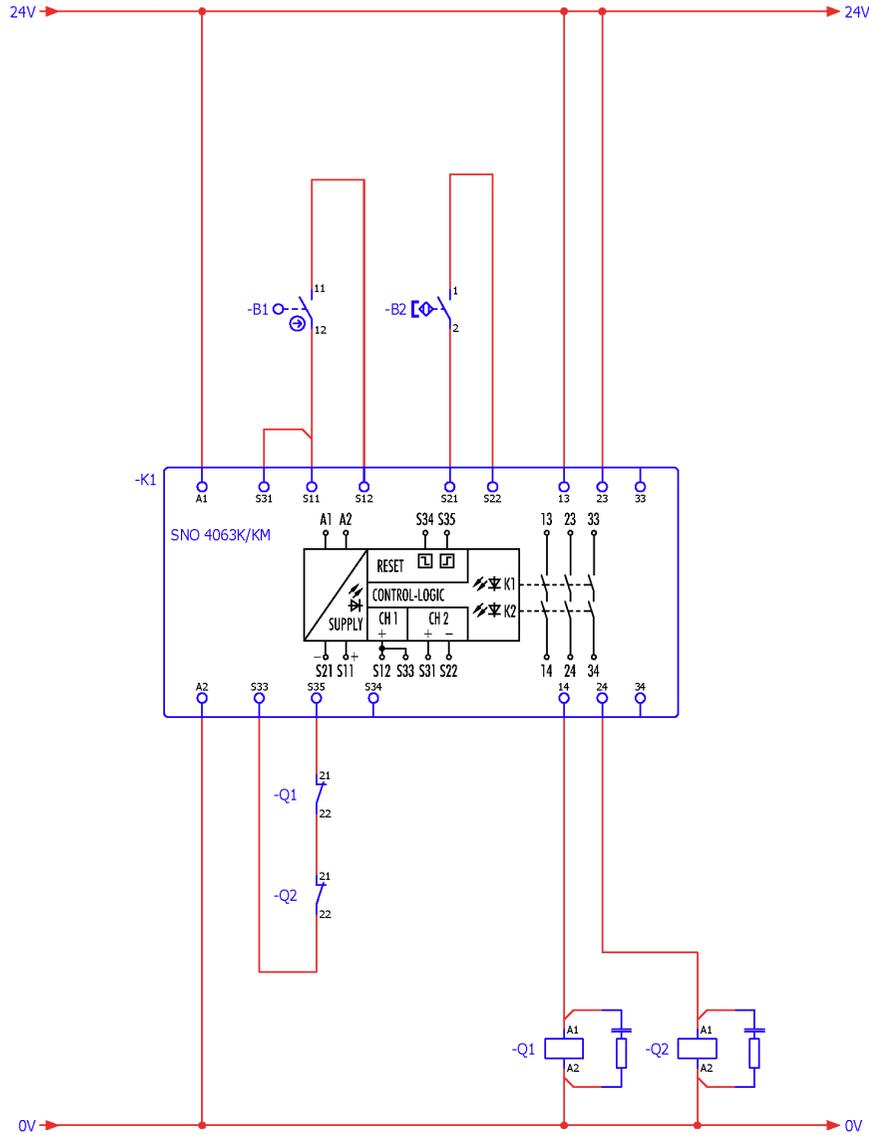
3.9   Door switch, magnetic – 2-channel, equivalent in PL e

3.9.1   Safety function

Safety function	When the door is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Door opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.9.2   Description

Function	By opening the door(s): • Door switch –B1 is actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door. Door switch –B1 is closed. The constructive design ensures that the door cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door. Start/restart must only be possible when: • The door is closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.9.3   Safety assessment

|	
Sensor technology	• Ground faults, cross shorts and short circuits to 24 V in the input circuit are detected by –K1 through test impulses on the sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99%
Actuator technology	Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. The contactors are equipped with positively driven feedback contacts. DC = 99%

Safety functions

Door switch, magnetic – 2-channel, equivalent in PL e

3.9.4 Products (options)

		Product
–B1		Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–K1		Safety switching device *safe* RELAY: SNA 4043K/KM article number: R1.188.3250.0
–Q1; –Q2		Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.9.5 Modeling per EN ISO 13849-1
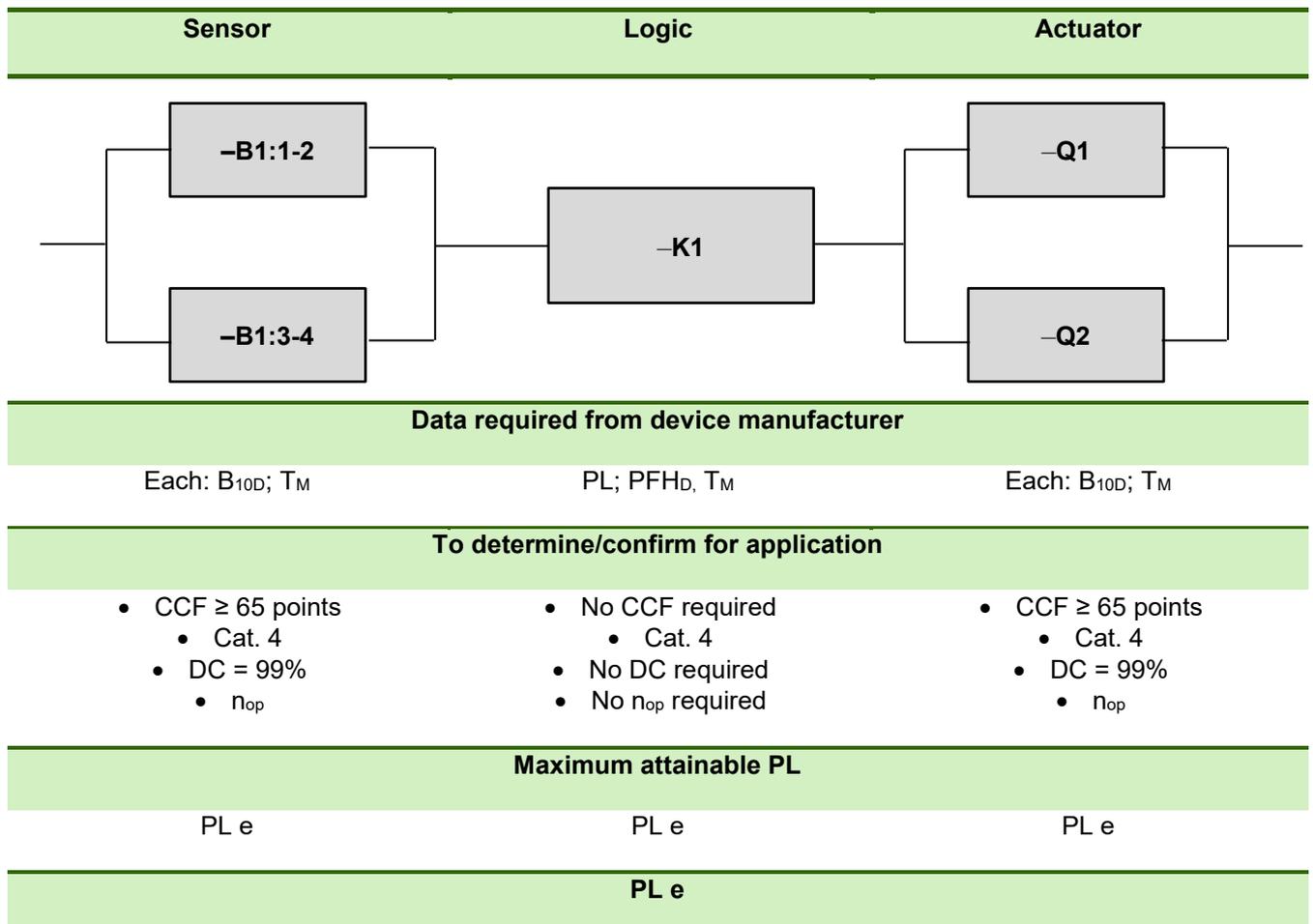
Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
  • Cat. 4
  • DC = 99%
    • n_{op}
	• No CCF required
	  • Cat. 4
	  • No DC required
	  • No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		  • DC = 99%
		    • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e

wieland

3.9.6   Circuit diagram
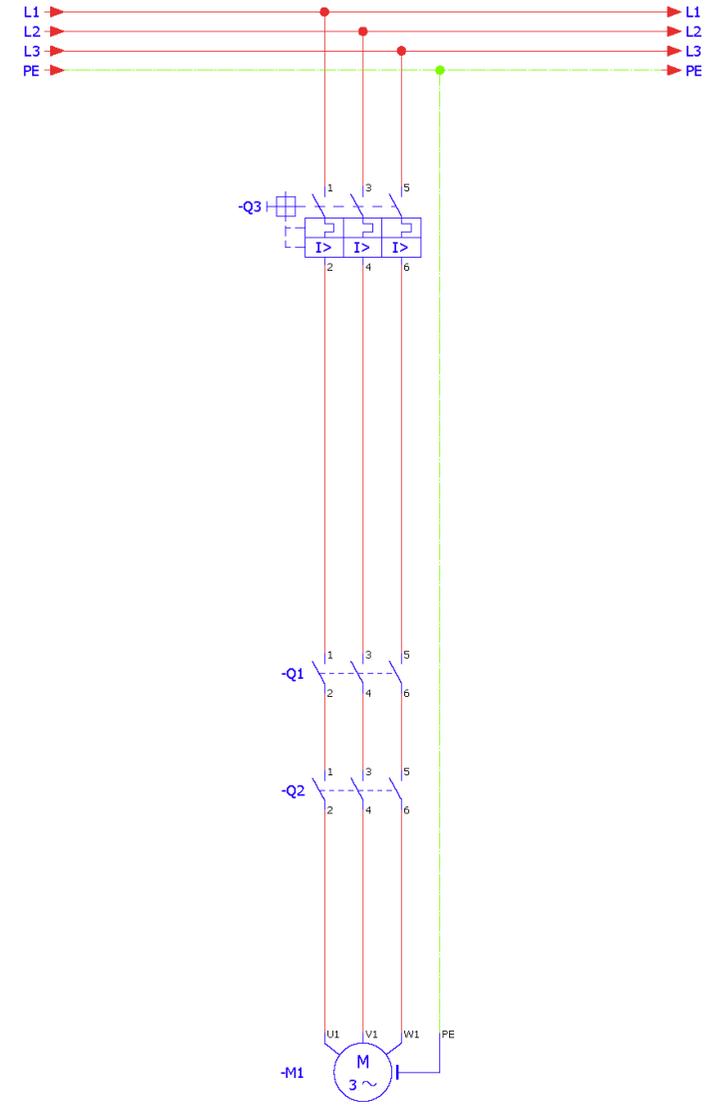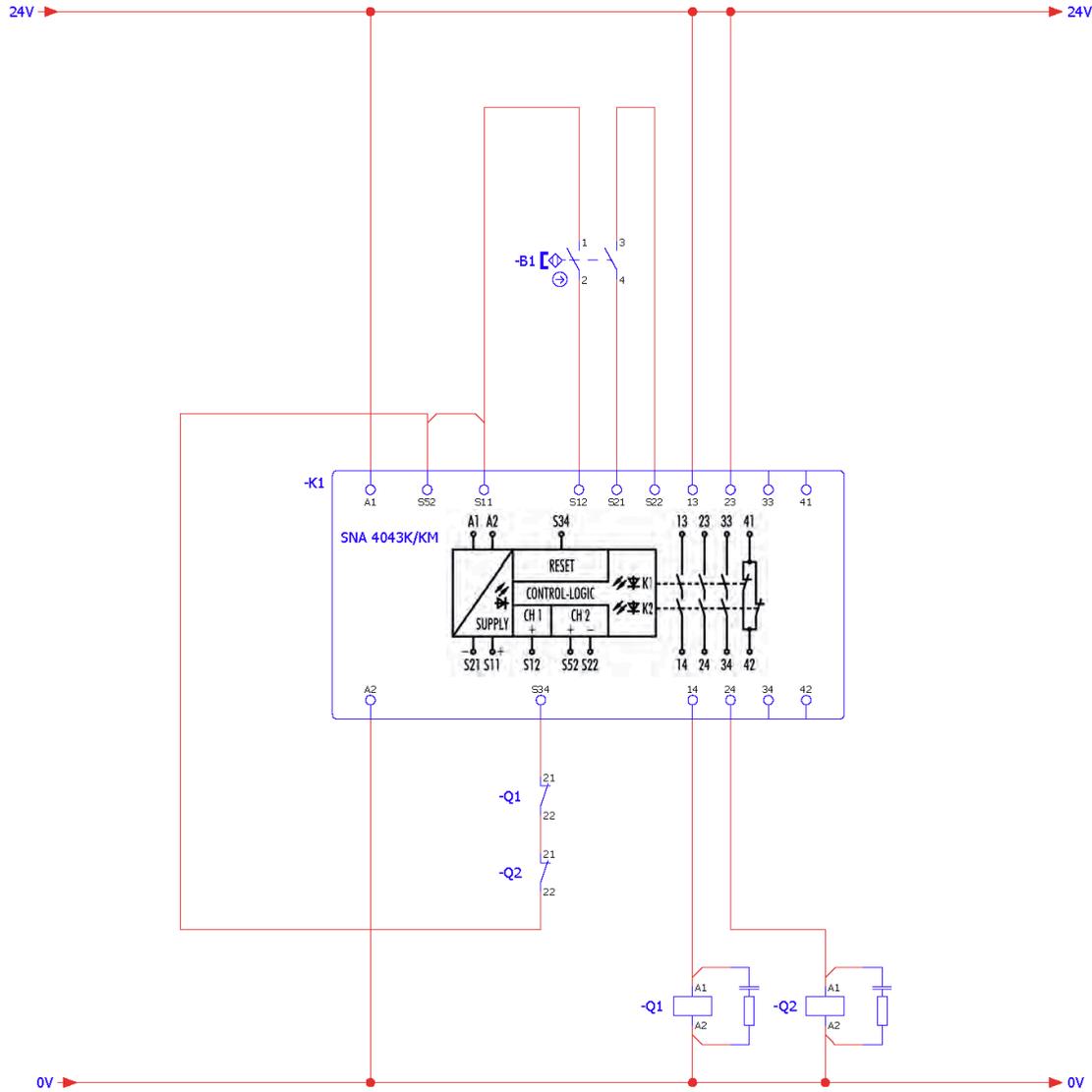
3.10 Door switch, magnetic – 2-channel antivalent in PL e

3.10.1 Safety function

Safety function	When the door is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Door opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.10.2 Description

Function	By opening the door(s): • Door switch –B1 is actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door. Door switch –B1 is closed. The constructive design ensures that the door cannot close accidentally.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • The door is closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.10.3 Safety assessment

|	
Sensor technology	• Ground faults, cross shorts and short circuits to 24 V in the input circuit are detected by –K1 through antivalent signals on the sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99%
Actuator technology	Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. The contactors are equipped with positively driven feedback contacts. DC = 99%

Safety functions

Door switch, magnetic – 2-channel antivalent in PL e

3.10.4 Products (options)

	Product
–B1	Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM Article number: R1.188.3580.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.10.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		
• CCF ≥ 65 points • Cat. 4 • DC = 99% • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• CCF ≥ 65 points • Cat. 4 • DC = 99% • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e

3.10.6 Circuit diagram

3.11 Magnetic door switch and pressure-sensitive mat – cross circuit in PL d

3.11.1 Safety function

Safety function	When door –B1 is opened or pressure-sensitive mat –S1 (safety mat) is stepped on, all drives in the system are disconnected from power. The safety function can only be reset after pressure-sensitive mat –S1 has been released.
Trigger event	Operator opens door –B1 or steps on pressure-sensitive mat –S1
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.11.2 Description

Function	By opening the door –B1: • The two channels from –B1 are opened • Input circuit –K1:3-3 and –K1:4-4 is opened • Safety contact –K1:Q1 opens • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped. By stepping on pressure-sensitive mat –S1: • Both circuits from –S1 are short circuited against each other • The short circuit is input circuit –K1:T1-I1 and –K1:T2-I2 is detected by –K1 • Safety contact –K1:Q1 opens • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	Manual reset of the safety function is actuated by closing door –B1. Preconditions for restart: • Hazard area must be cleared • Pressure-sensitive mat –S1 must not be actuated • The constructive design ensures that door –B1 cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door. Start/restart must only be possible when: • Door –B1 is closed • Pressure-sensitive mat –S1 is not actuated • Positively driven contactors –Q1 and –Q2 are switched off.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.11.3 Safety assessment

Sensor technology	Door switch –S1 and pressure-sensitive mat –S1 • Ground faults, cross shorts and short circuits to 24 V in the input circuit of –B1 and –S1 are detected by –K1 through test impulses on the sensor lines. • –B1: Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99% • –S1: Diagnosis through "Cross comparison with dynamization, without high quality fault detection" by –K1. DC = 90%
Actuator technology	Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. The contactors are equipped with positively driven feedback contacts. DC = 99%

3.11.4 Products (options)

	Product
–B1	Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–S1	Short circuiting pressure-sensitive mat with the requirements: • Must be adequate for anticipated loads • Number of electrical switching cycles must be adequate for anticipated frequency of use • Manufacturer specification from B_{10D} and T_M as well as the achievable category Normally, the use of this type of pressure-sensitive mat is limited to PL d, Cat. 3 by the manufacturer.
–K1	Programmable safety controller *samos* PRO: SP-COP2, article number: R1.190.1310.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Magnetic door switch and pressure-sensitive mat – cross circuit in PL d

3.11.5 Modeling per EN ISO 13849-1
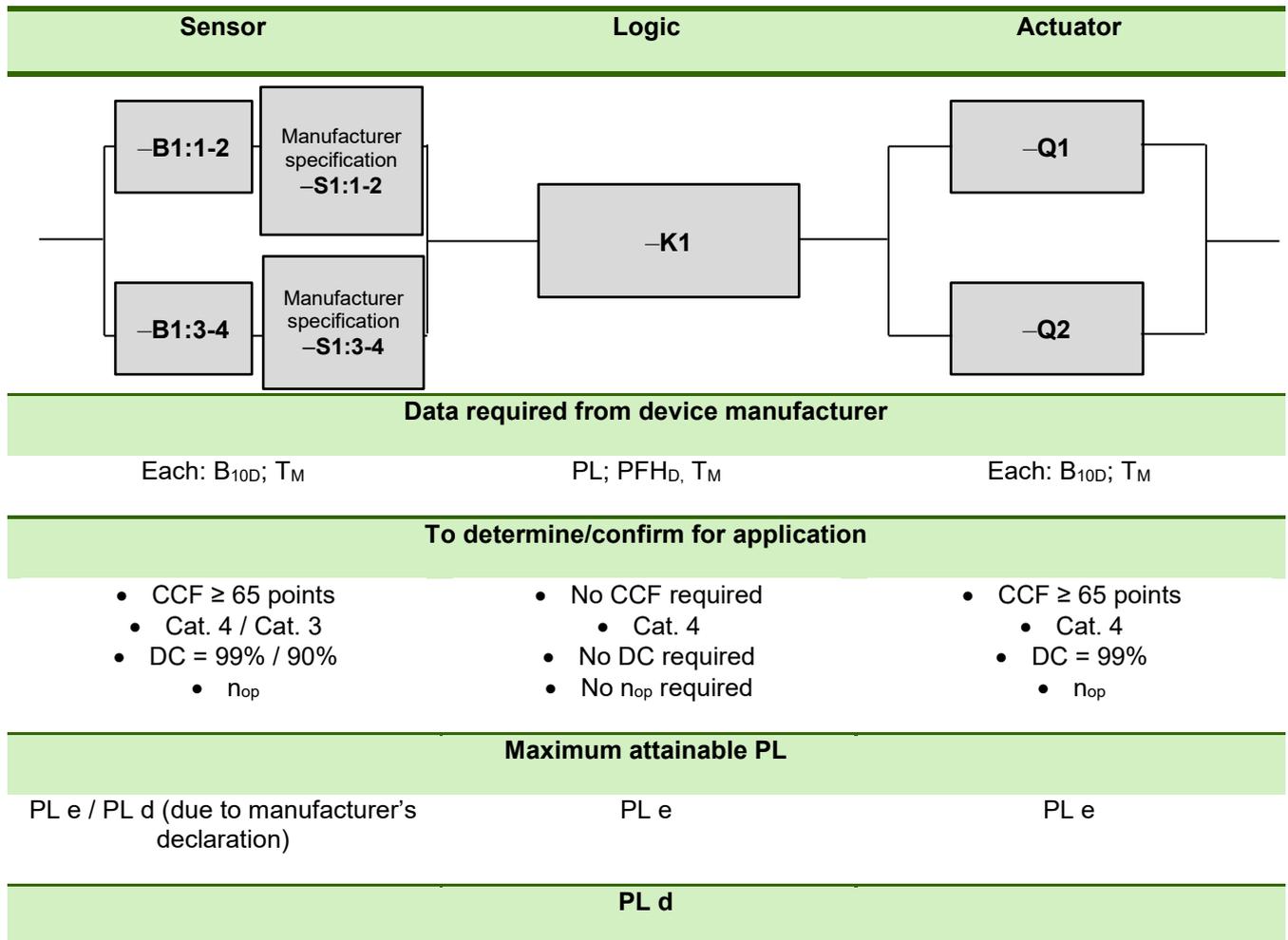
Sensor	Logic	Actuator
−B1:1-2 / Manufacturer specification **−S1:1-2** ; **−B1:3-4** / Manufacturer specification **−S1:3-4**	**−K1**	**−Q1** ; **−Q2**

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		
• CCF ≥ 65 points • Cat. 4 / Cat. 3 • DC = 99% / 90% • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• CCF ≥ 65 points • Cat. 4 • DC = 99% • n_{op}

Maximum attainable PL		
PL e / PL d (due to manufacturer's declaration)	PL e	PL e

PL d

Safety functions

Magnetic door switch and pressure-sensitive mat – cross circuit in PL d

3.11.6 Circuit diagram
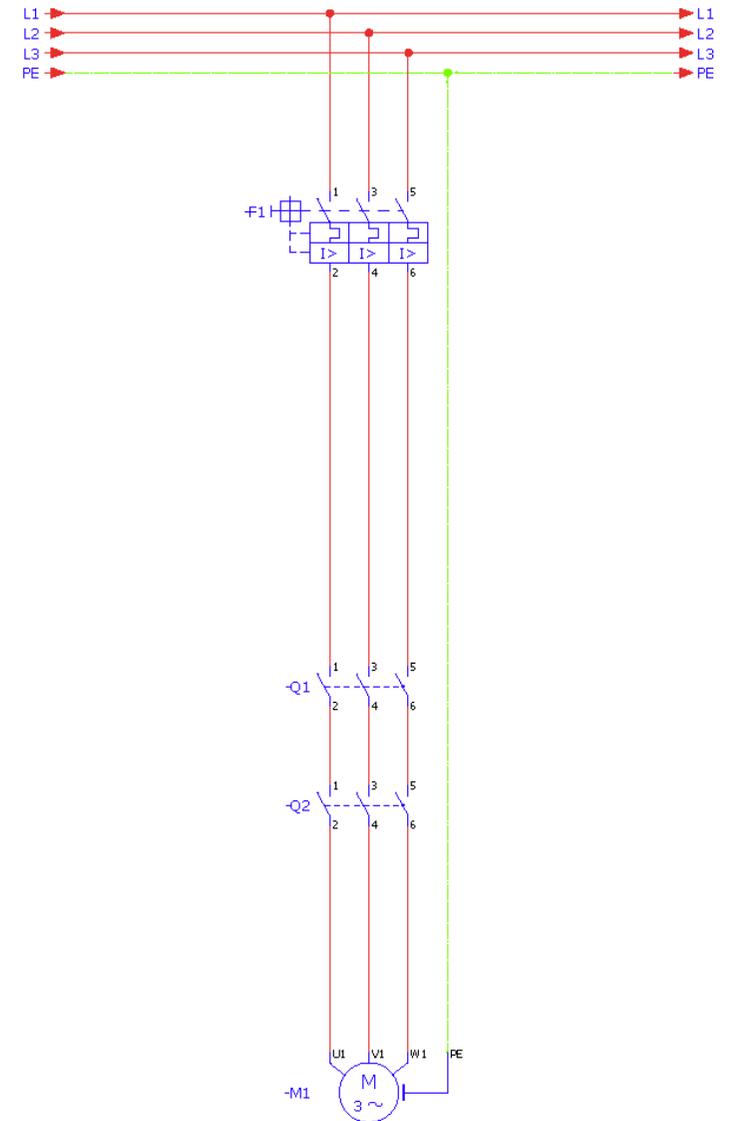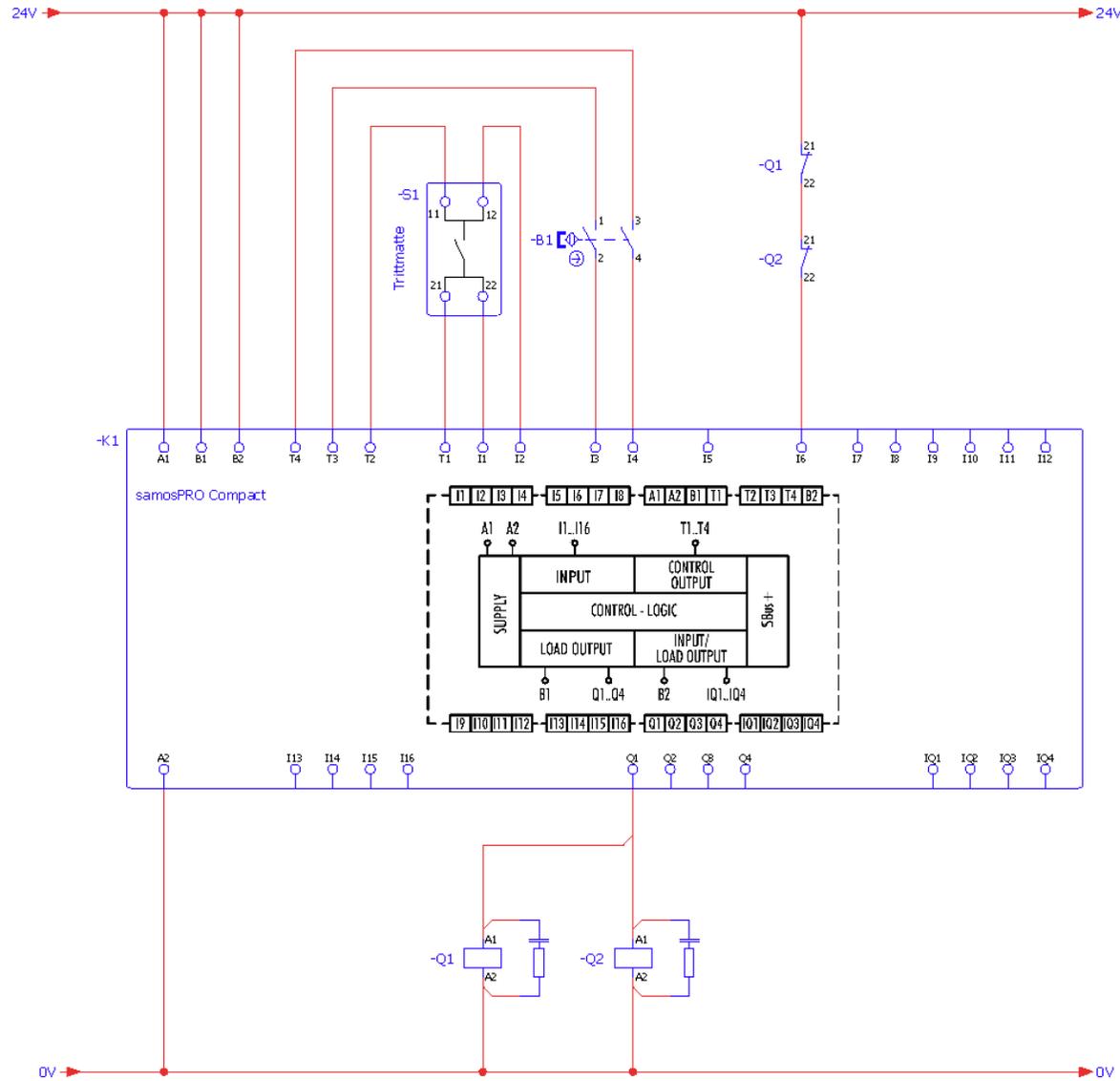
3.12 Bumper, 1-channel – positive opening in PL d

3.12.1 Safety function

Safety function	Actuating bumper –B4 (safety strip) brings pneumatic drive –M1 of the system to a standstill.
Trigger event	Bumper –B4 actuated by operator.
Reaction	Power to pneumatic drive –M1 disconnected
Safe state	Drive –M1 is depressurized and disconnected from power. *Note: It is assumed that the depressurized state of the cylinder is the safe state. In case of vertical installation, often the pressurized state of –M1 is the safe state, because then no independent lowering is expected. Then the pneumatic diagram must be correspondingly adapted.*

3.12.2 Description

Function	By actuating bumper –B4: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Magnets –Q2:14 and –Q2:12 are disconnected from power • Valve –Q2 moves to its middle position and depressurizes –M1. • Drive –M1 is stopped. • In addition, –Q1 is disconnected from power. As a result, –Q3 and –Q4 are also without power and –M1 depressurizes through –Q3 and –Q4. • Valves –Q1, –Q3 and –Q4 do not switch at all or switch only rarely in operating mode, because usually an entire group of valves is switched off through –Q1.
Manual reset function	The manual reset of the safety function is actuated by the release of bumper –B4.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Bumper –B4 is not actuated
Feedback circuit	• Position switch –B1 at –Q1 is used to directly read back the valve position. • During the process sequence, position switches –B2 and –B3 are monitored by –K1. The process position is specified through additional inputs at –K1

3.12.3 Safety assessment

Sensor technology	• Ground faults, and short circuits to 24 VDC in the input circuit are detected by –K1 through test impulses on the sensor lines. • The sensors are positively opening and are classified and certified as Cat: 3 by the manufacturer. • The signals are evaluated by an input of at least Cat. 3 at –K1. • The bumper manufacturer instructions must be observed. Normally, protected wiring installation is required. • DC = 90%

Actuator technology	Diagnosis of –Q1 through –B1
	   • Direct monitoring → DC = 99%
	
	Diagnosis of –Q2 through –B2 and –B3
	   • Indirect monitoring at end of –M1 path → DC = 90%
	
	Diagnosis of –Q3 and –Q4 through –B2 and –B3
	   • Only indirect and at end of –M1 path.
	   • Only possible at certain times
	   • E.g., switching on the machine or shift change.
	Possible test process
	   • Move –M1 to left end position
	   • Lock –Q3 and –Q4
	   • –Q2 in position: Clockwise
	   • –M1 must not leave the end position. Detection by –B2 or –B3
	   • Check the other end position in the same way
	   • If movement away from the end position is detected, it can be ended by –Q2.
	   • If tests are run at least 1x per month: DC = 90% (for comparison, see also CNB/M/11.050/R/E Rev. 05 from 2011-10-18)

Bumper, 1-channel – positive opening in PL d

3.12.4 Products (options)

	Product
–B4	Bumper with positively opened contact and lock, Cat. 3 / PL d by manufacturer.
–K1	Programmable safety controller *samos* PRO: SP-COP2, Article number: R1.190.1310.0
–Q1	2/3 way valve with the following properties: • Electrical pilot control • Neutral position venting • Reset via mechanically validated spring • Suitable for anticipated use • Manufacturer specification from B_{10D} and T_M
–Q2	5/3 way valve with the following properties: • Electrical pilot control • Neutral position venting • Reset via mechanically validated spring • Suitable for anticipated use • Manufacturer specification from B_{10D} and T_M
–Q3, –Q4	Pneumatic 2/3 way valve with the following properties: • Pneumatic actuation • Neutral position venting • Reset via mechanically validated spring • Suitable for anticipated use • Manufacturer specification from B_{10D} and T_M
–B1 to –B3	Position switch with the following properties: • Switch contact in open position when valve/cylinder in non-actuated position

Safety functions

Bumper, 1-channel – positive opening in PL d

3.12.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

−B4	−K1	−Q2 −Q1 −Q3 −Q4

Data required from device manufacturer		
PL; PFH_D, T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• No CCF required
  • Cat. 3
• No DC required
• No n_{op} required
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 3
		• −Q1: DC = 99%
		• −Q2; −Q3; −Q4: each DC = 90%
		  • n_{op}

Maximum attainable PL		
PL d	PL e	PL e

PL d
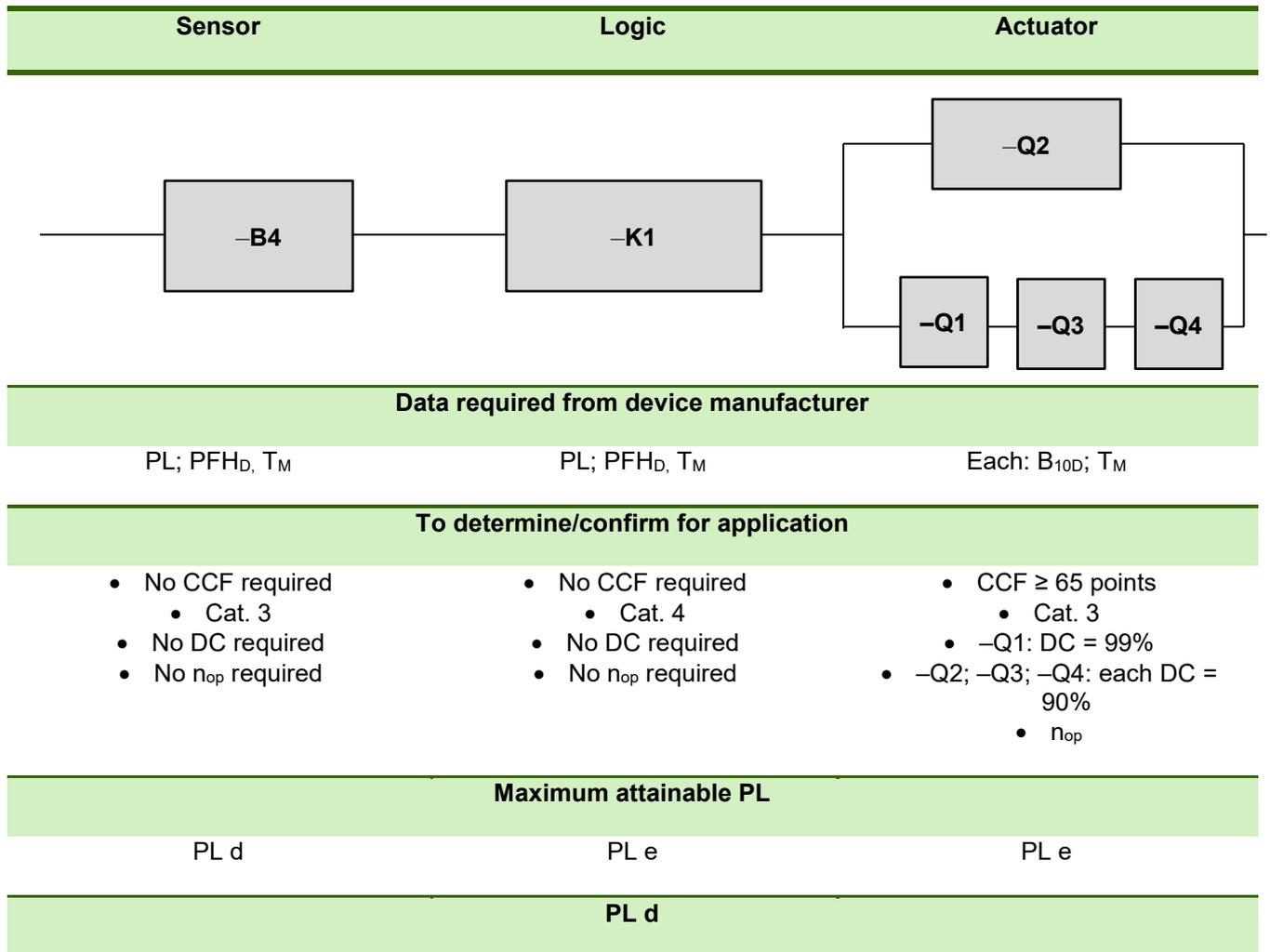
Note 1: *In many cases, n_{op} will have a different value for each of the elements, because the valve does not switch each time the bumper is actuated; in normal operation, often it switches more often than the bumper.*

Note 2: *As an alternative, reading back −B1 to −B3 can also be done through standard controls. However, when this option is used, the diagnosis is part of the standard control program and must be taken into account when CCF is determined. The standard controls do not contribute mathematically to the determination of PL and PFH_D. The diagnosis result is to be transferred to −K1 by the software. In the end, the safety technology aspects of the standard control program also must be validated. Particular attention must be given to the requisite validation after every change to the standard control program.*

Safety functions

Bumper, 1-channel – positive opening in PL d

3.12.6 Circuit diagram
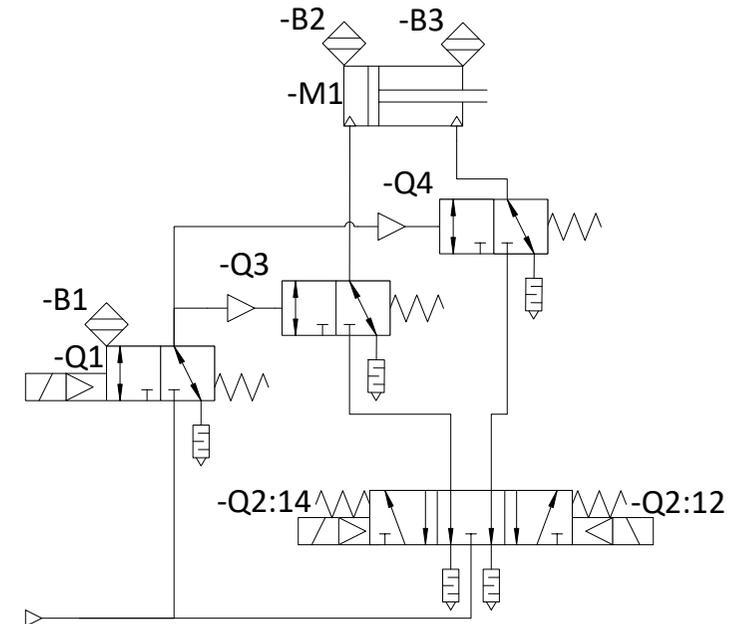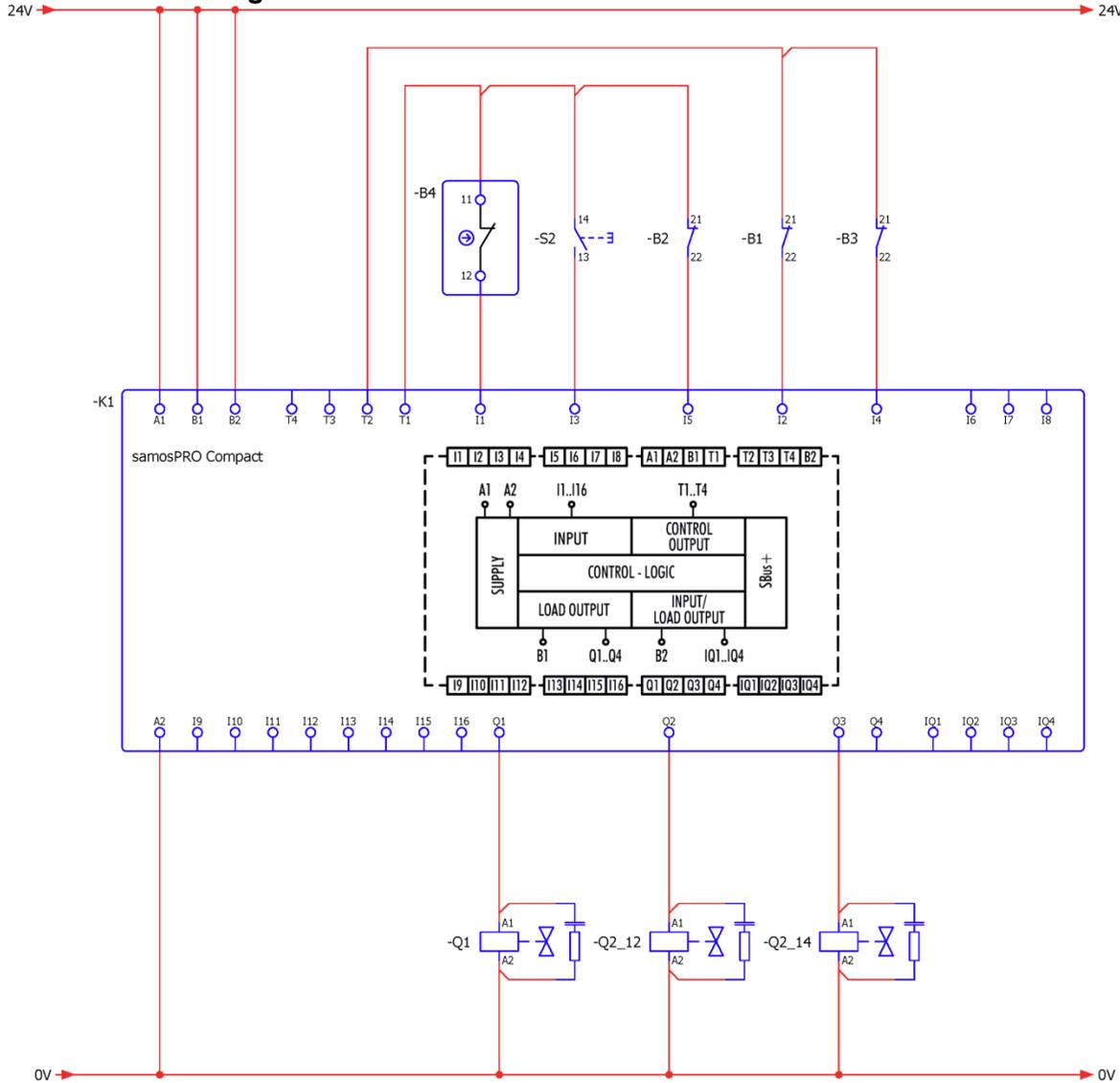
3.13 Two hand, type III A in PL c

3.13.1 Safety function

Safety function	Removing hands from one or both buttons –S1 / –S2 of the two-hand operation device brings drive –T1 to a stop.
Trigger event	Operator removes one or both hands from two-hand operation device –S1 / –S2.
Reaction	Drive –M1 disconnected from power.
Safe state	Drive –M1 is without power.

3.13.2 Description

Function	By removing hands from buttons –S1 and –S2: • Input circuit –K1:T11–T12 is closed at safety switching device–K1 • Input circuit –K1:T11–T13 is interrupted at safety switching device –K1 • –K11:11-14 safety contacts are opened • STO requested at frequency converter –T1 • Machine M1 is stopped.
Manual reset function	The manual reset of the safety function is initiated by actuating buttons –S1 and –S2 after both buttons were not previously actuated and the switches had the associated switch position.
Start/restart function	The start/restart function is automatically performed along with the manual reset. *Note: The start/restart function can depend on other states.*
Feedback circuit	Not needed here, since –T1 is a device with integrated diagnosis.

3.13.3 Safety assessment

Sensor technology	A single fault may lead to loss of safety.
Actuator technology	Frequency converter with integrated diagnosis and an evaluation as PL d.

Note: *If switches with NC and NO contacts are used for –S1 and –S2, only the NO contact of one button and the NC contact of the other should be used. Wiring contacts of one switch in series or in parallel with those of the other will result in fault masking. Then, an initial fault will not be detected under any circumstances.*

3.13.4 Products (options)

		Product
–S1		Button, NC design. Required key data: • Manufacturer specification from B_{10D} and T_M
–S2		Button, NO design. Required key data: • Manufacturer specification from B_{10D} and T_M
–K1		Safety switching device *safe* RELAY: SNZ 1022K rticle number: R1.188.3700.0
–T1		Safe frequency converter with integrated diagnosis and an evaluation as PL d. Integrated STO safety function.

3.13.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	PL; PFH_D, T_M

To determine/confirm for application		

• No CCF required
  • Cat. 1
• No DC required
  • n_{op}
	• No CCF required
	  • Cat. 1
	• No DC required
	• No n_{op} required
		• No CCF required
		  • Cat. 3
		• No DC required
		• No n_{op} required

Maximum attainable PL		
PL c	PL c	PL d
PL c		

Safety functions

3.13.6 Circuit diagram

Safety functions

3.14 Two hand, type III C in PL e

3.14.1 Safety function

Safety function	Removing hands from one or both buttons –S1 / –S2 of the two-hand operation device brings drives to a stop. Safe state is reached when all drives are completely without power.
Trigger event	Operator removes one or both hands from two-hand operation device –S1 / –S2.
Reaction	Drives disconnected from power
Safe state	Drive is completely without power.

3.14.2 Description

Function	• By removing hand from button –S1: • Input circuit –K1:Y11–Y12 is closed at safety switching device –K1 • Input circuit –K1:Y11–Y14 is opened at safety switching device –K1 • By removing hand from button –S2: • Input circuit –K1:Y21–Y22 is closed at safety switching device –K1 • Input circuit –K1:Y21–Y24 is opened at safety switching device –K1 is opened • –K11:11-14 safety contacts are opened • Contactors –Q1 and –Q2 are switched off • Drives have no power.
Manual reset function	The manual reset of the safety function is initiated by actuating buttons –S1 and –S2 after both buttons were not previously actuated and the switches had the associated switch position. Actuation must be synchronous.
Start/restart function	The start/restart function is automatically performed along with the manual reset. *Note: The start/restart function can depend on other states.*
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.14.3 Safety assessment

Sensor technology	• Because of the diversity and redundancy of the switches, a single fault does not lead to loss of safety. • The synchronization of switches –S1 and –S2 must be monitored • Actuation of just one button must result is safe state. This is ensured by –K1.
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. DC = 99%

3.14.4 Products (options)

	Product

| –S1; –S2		Each button with NC and NO contacts. Required key data: • Manufacturer specification from B_{10D} and T_M
–K1		Safety switching device *safe* RELAY: SNZ 4052K article number: R1.188.0530.1
–Q1; –Q2		Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.14.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
 • Cat. 4
 • DC = 99%
  • n_{op}
	• No CCF required
	 • Cat. 4
	 • No DC required
	 • No n_{op} required
		• CCF ≥ 65 points
		 • Cat. 4
		 • DC = 99%
		  • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e
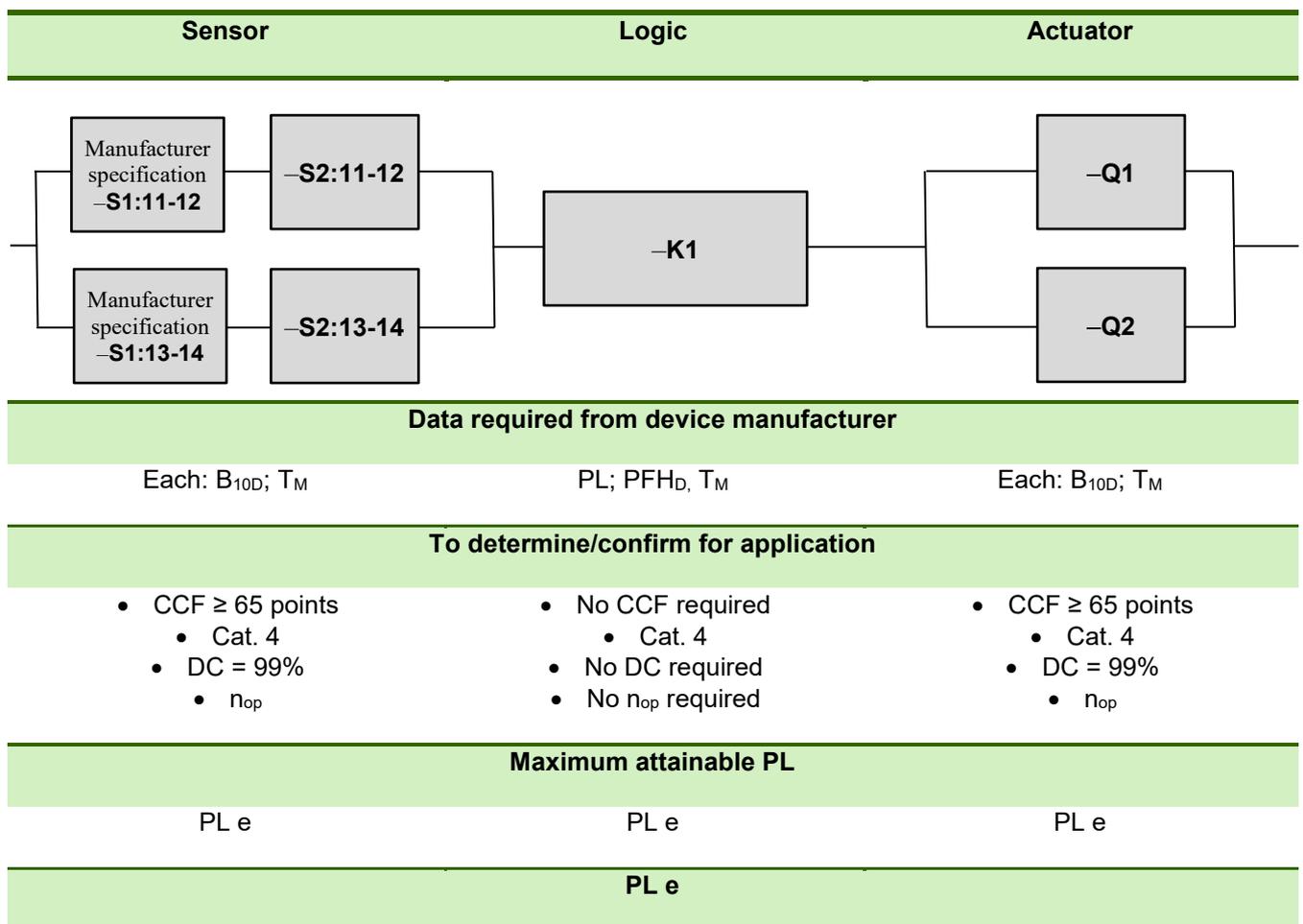
Safety functions

Two hand, type III C in PL e

3.14.6 Circuit diagram
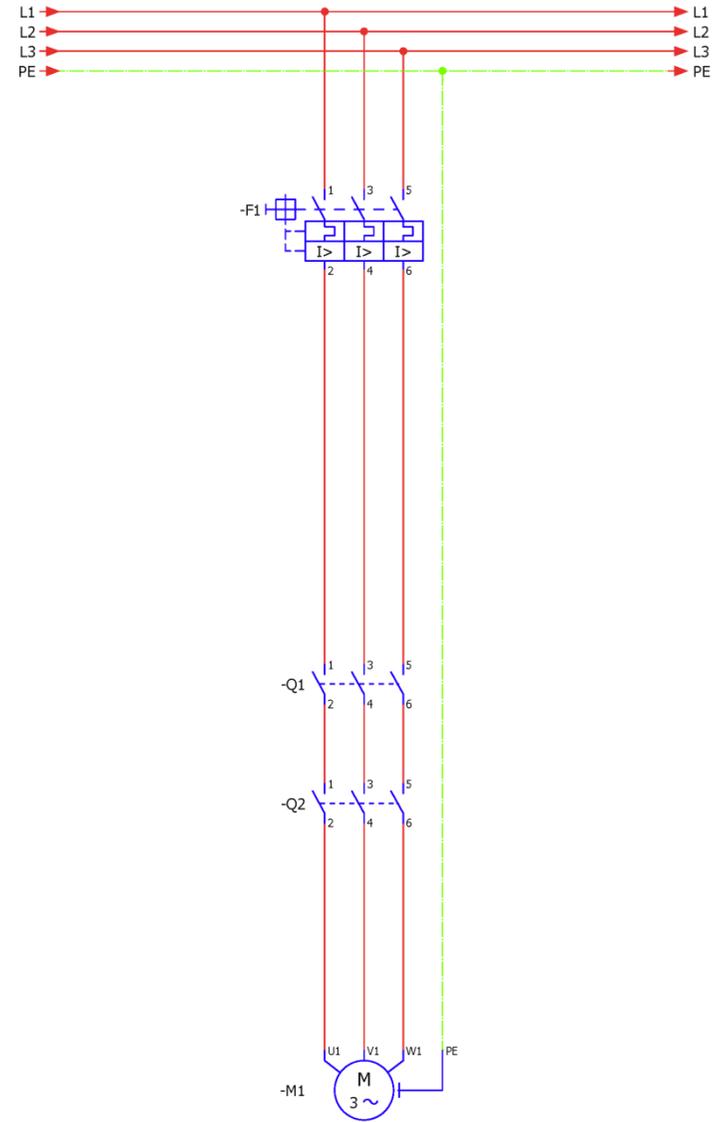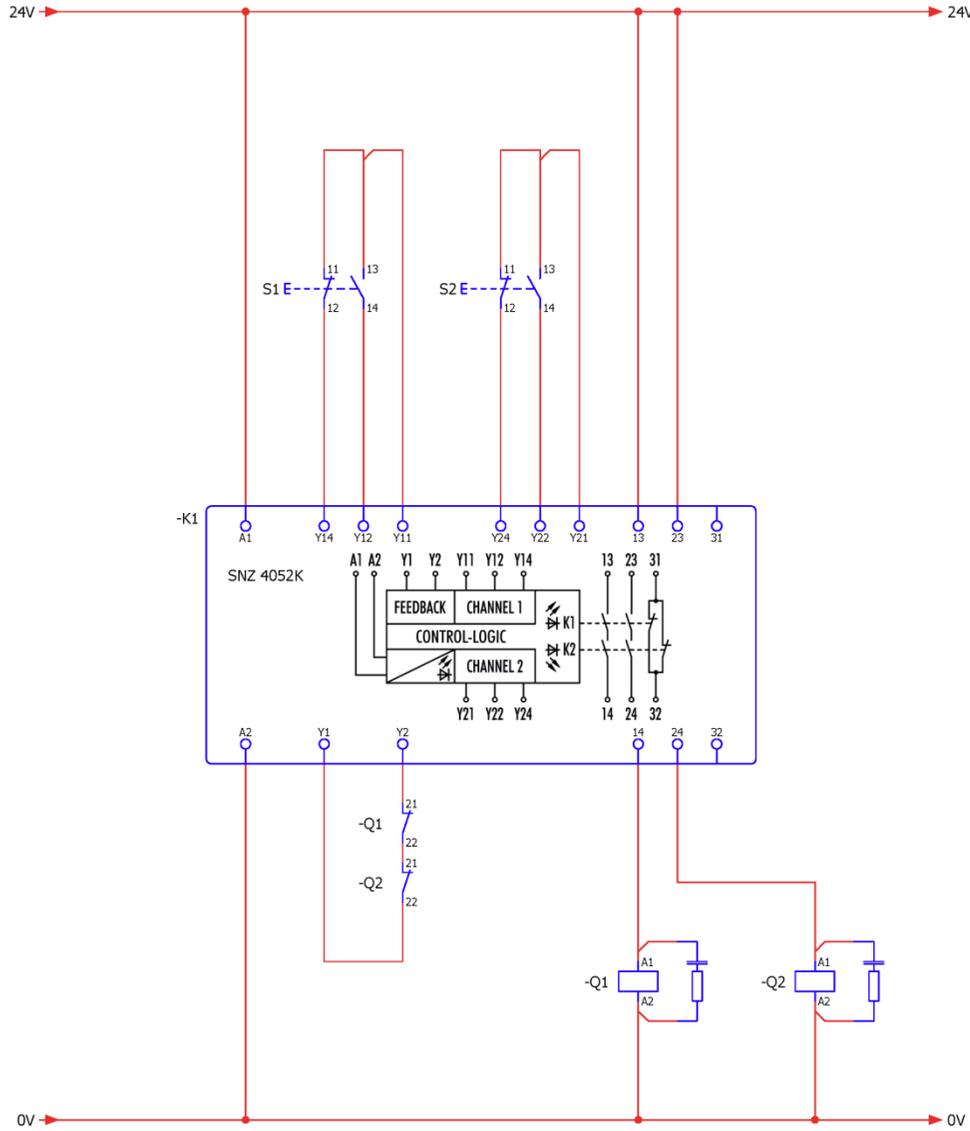
3.15 Light curtain/grid, type 4 in PL e

3.15.1 Safety function

Safety function	When light curtain/grid –B1 is interrupted, the speed of drive –M1 is reduced to a safe limited speed (SLS).
Trigger event	Light curtain/grid –B1 interrupted by operator.
Reaction	–M1 set to safe limited speed (SLS).
Safe state	Safe state is reached when –M1 is not moving faster than permitted.

3.15.2 Description

Function	When light curtain/grid –B1 is interrupted: • The OSSD signals switch off • The two input circuits at safety switching device –K1 are interrupted • –K1 safety contacts are opened • Frequency converter –T1 with safety input SLS switched to safe limited speed state
Manual reset function	The manual reset of the safety function is actuated by release of light the curtain/grid. The constructive design ensures no access behind the light curtain/grid is possible.
Start/restart function	The start/restart function is initiated either by actuating –S2 or releasing light curtain/grid –B1. Start/restart must only be possible when: • Light curtain/grid –B1 is not interrupted
Feedback circuit	Not needed here, since –T1 is a device with integrated diagnosis.

3.15.3 Safety assessment

Sensor technology	• Synchronization time monitoring between input circuits –S12; –S22 through –K1 • Any wiring faults from –B1 to –K1 are detected by OSSD testing through –B1 and synchronization time monitoring by –K1. "Cross comparison with dynamization and high quality fault detection" → DC = 99 % • No protected installation of the wiring is required. • Selecting and positioning the light curtain/grid requires • Determination of system reaction time from interruption of the light curtain/grid until the drives have been stopped • Determination of the necessary arrangement (placement, distance, alignment, resolution and length) of the light curtain/grid. See also EN ISO 13855
Actuator technology	Frequency converter with integrated diagnosis and an evaluation as PL e.

Safety functions

Light curtain/grid, type 4 in PL e

3.15.4 Products (options)
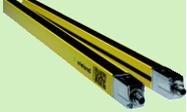
	Product
–B1	Type 4 safety light grid or curtain **sensor** PRO: SLC-4xx article number: R1.541.1800.0 + R1.561.1800.0 *Note: With the required data regarding reaction time, resolution and length.*
–K1	Safety switching device **safe** RELAY: SNO 4083KM article number: R1.188.3580.0
–T1	Safe frequency converter with integrated diagnosis and an evaluation as PL e. Integrated SLS safety function.

3.15.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
PL; PFH_D, T_M	PL; PFH_D, T_M	PL; PFH_D, T_M

To determine/confirm for application		

• No CCF required
   • Cat. 4
 • No DC required
 • No n_{op} required
	• No CCF required
	   • Cat. 4
	 • No DC required
	 • No n_{op} required
		• No CCF required
		   • Cat. 4
		 • No DC required
		 • No n_{op} required

Maximum attainable PL		
PL e	PL e	PL e

PL e
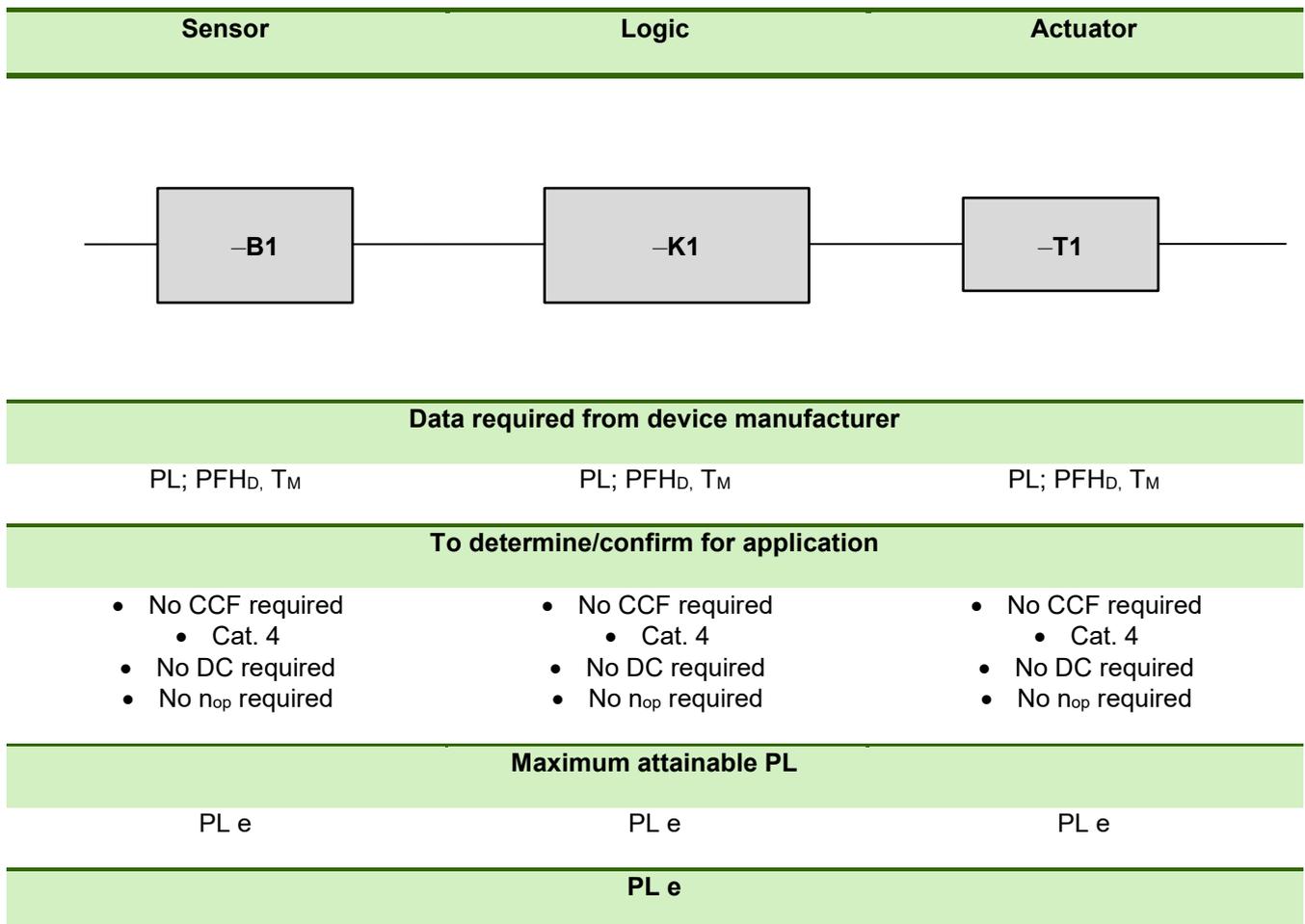
Safety functions

Light curtain/grid, type 4 in PL e

3.15.6 Circuit diagram
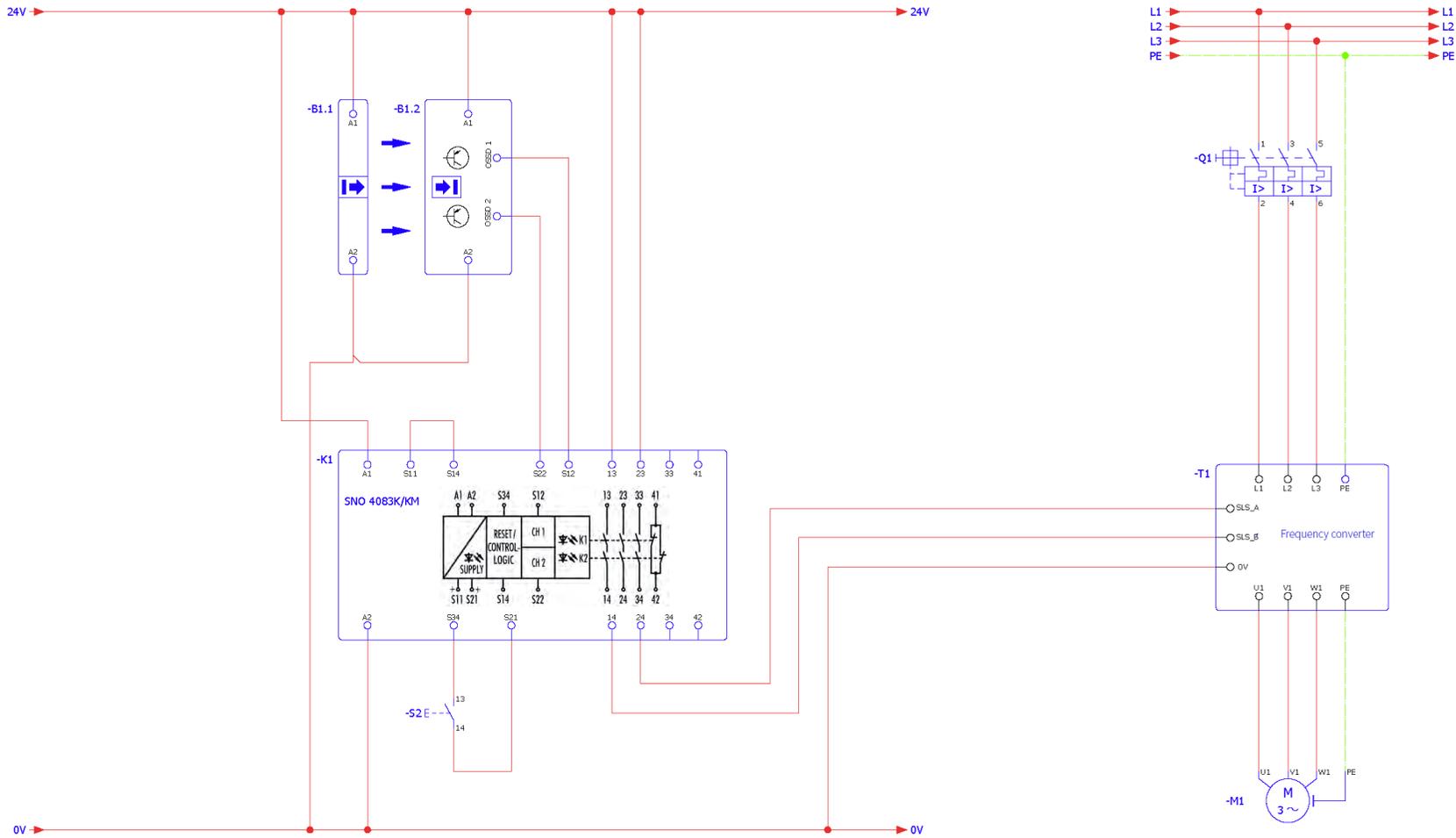
Safety functions

3.16 EMERGENCY stop in series – 2-channel in PL d

3.16.1 Safety function

Safety function	When one of the emergency stop buttons –S1 or –S2 is actuated, all drives in the system are brought to a controlled standstill.
Trigger event	One of the emergency stop buttons is actuated by the operator.
Reaction	Hazardous movements brought to a stop.
Safe state	Drives have no power.

3.16.2 Description

Function	By actuating the emergency stop button –S1 or –S2: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off. • Machine M1 is stopped.
Manual reset function	The safety function manual reset is initiated when emergency stop button –S1 or –S2 is rotated to unlock it.
Start/restart function	The start/restart function is initiated by actuating –S3. Start/restart must only be possible when: • Emergency stop button –S1 and –S2 are not actuated • Contactors –Q1 and –Q2 are switched off
Feedback circuit	The positively driven NC contacts of contactor –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of –K1.

3.16.3 Safety assessment

|	
Sensor technology	Cross shorts (channel 1 – channel 2) in the input circuit are detected through the differing potentials (+24 V / 0 V) in the sensor lines. Not all faults (0 V to 0 V / +24 V to +24 V); are detected; an accumulation of faults can lead to loss of the safety function. DC = 60% Although two buttons are wired in series, they are still two functionally independent safety functions. Depending on the approach used, faults in one sensor can be concealed; nonetheless, they cannot impair the function of the other sensor.
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

Safety functions

EMERGENCY stop in series – 2-channel in PL d

3.16.4 Products (options)

		Product
–S1; –S2		Emergency stop control device (2-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1122 article number: R1.200.1122.0
–K1		Safety switching device *safe* RELAY: SNO 4003K article number: R1.188.0500.1
–Q1; –Q2		Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.16.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
  • Cat. 3
  • DC = 60%
    • n_{op}
	• No CCF required
	  • Cat. 3 (Cat. 4)
	  • No DC required
	  • No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		  • DC = 99%
		    • n_{op}

Maximum attainable PL		
PL d	PL e	PL e

PL d

3.16.6 Circuit diagram

3.17 EMERGENCY stop & door switch, mechanically in series, 1-channel in PL c

3.17.1 Safety function

Safety function	When the door(s) are opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Opening one or more doors or actuating emergency stop by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

Note: *The emergency stop and door monitoring safety functions can also be modeled separately. Because of the simplicity of this application, modeling them together was selected here. This, then, is a worst-case appraisal. In any case, the PFHd value of the individual function is lower than is determined here.*

3.17.2 Description

Function	By opening the door or pressing emergency stop: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactor –Q1 is switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door(s) or unlocking emergency stop. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is initiated by actuating switch –S2. Start/restart must only be possible when: • The doors are closed • Emergency stop is unlocked The constructive design prevents access behind the doors.
Feedback circuit	No contactor monitoring

3.17.3 Safety assessment

Sensor technology	Faults in the components or wiring are only detected by manual tests, which should be performed regularly. A minimum test frequency of 1x per year is specified in the documentation. *Note: Because of anticipated fault masking and the resulting DC = 0%, use of 2-channel switches for doors or emergency stop (see 4.1.5) does not bring any gain in safety. Thus, even with 2-channel wiring, a maximum Cat. 1 is possible.*
Actuator technology	Faults in the components or wiring are only detected by manual tests, which should be performed regularly. A minimum test frequency of 1x per year is specified in the documentation.

Safety functions

EMERGENCY stop & door switch, mechanically in series, 1-channel in PL c

3.17.4 Products (options)

	Product
–B1; –B2	Locking device, design 2 (door switch with separate actuator) *sensor* PRO: SMS3x10 article number: R1.320.3010.0
–S1	Emergency stop control device (1-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1102 article number: R1.200.1102.0
–K1	Safety switching device *safe* RELAY: SNO 4003K article number: R1.188.0500.1
–Q1	Power contactor with the following properties: • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.17.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	B_{10D}; T_M

To determine/confirm for application		
• No CCF required • Cat. 1 • No DC required • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• No CCF required • Cat. 1 • No DC required • n_{op}

Maximum attainable PL		
PL c	PL e	PL c

PL c		
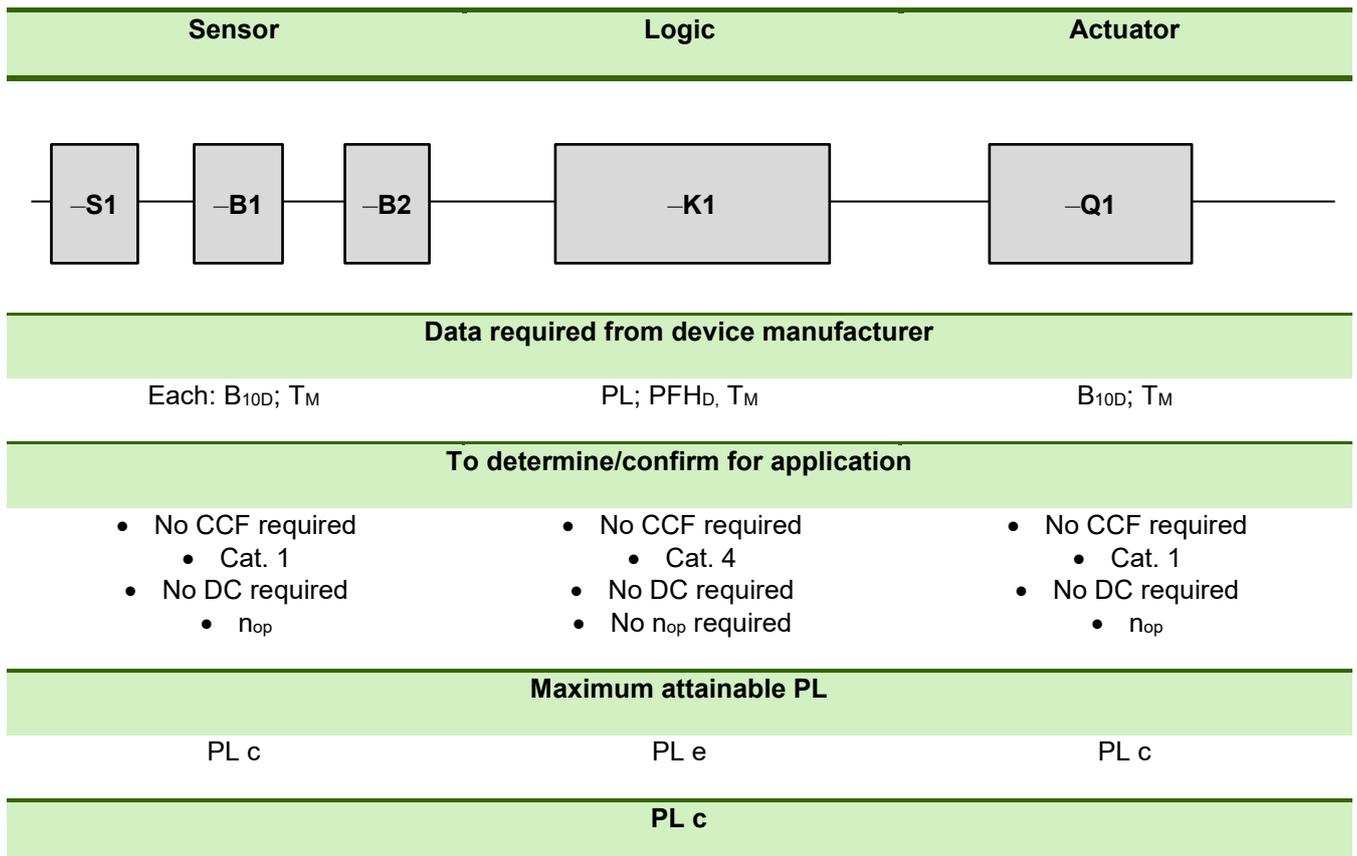
Safety functions

EMERGENCY stop & door switch, mechanically in series, 1-channel in PL c

3.17.6 Circuit diagram
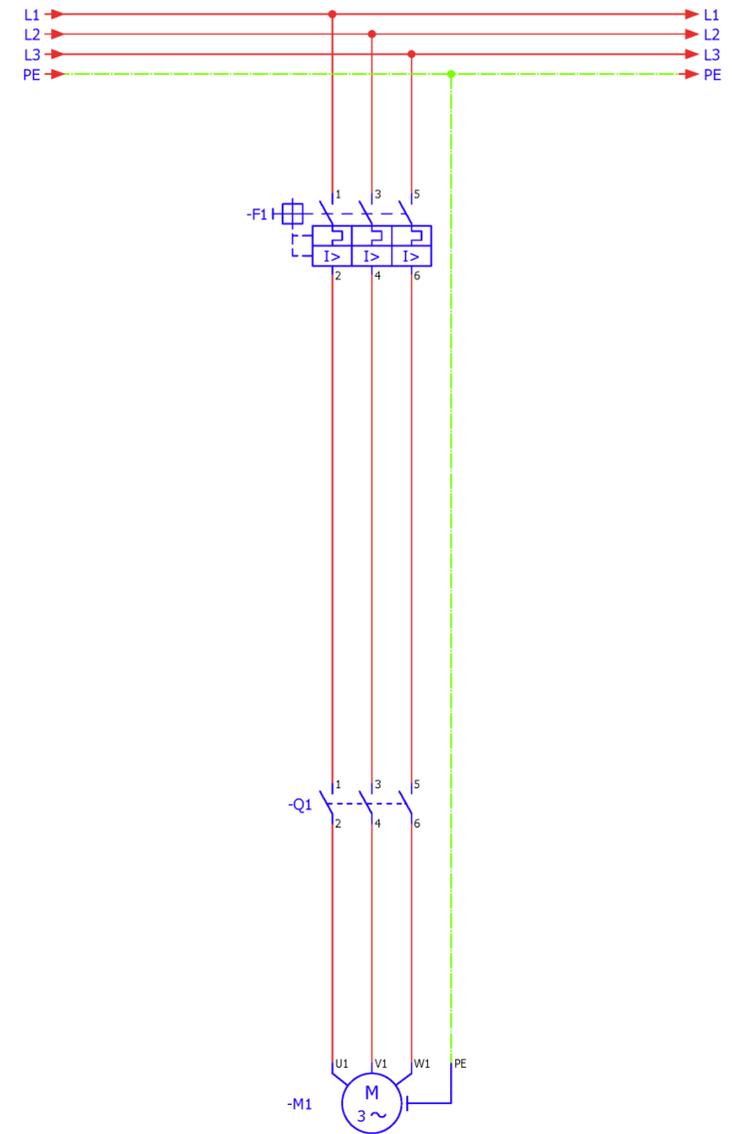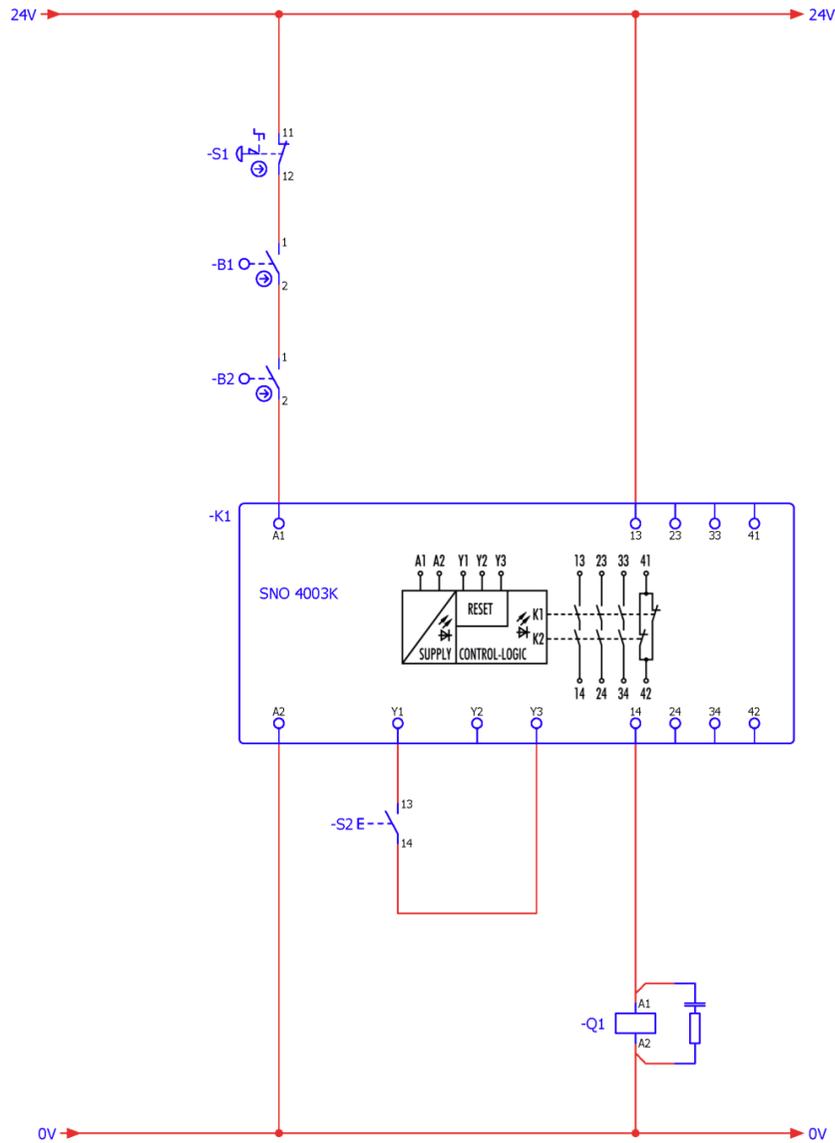
3.18 EMERGENCY stop & door switch, magnetic in series, 2-channel in PL c

3.18.1 Safety function

Safety function	When the door(s) are opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Opening one or more doors or actuating emergency stop by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

Note: ***The emergency stop and door monitoring safety functions can also be modeled separately. Because of the simplicity of this application, modeling them together was selected here.***

3.18.2 Description

Function	By opening the door or pressing emergency stop: • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactor –Q1 is switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door(s) or unlocking emergency stop. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is initiated by actuating switch –S2. Start/restart must only be possible when: • The doors are closed • Emergency stop is unlocked The constructive design prevents access behind the doors.
Feedback circuit	No contactor monitoring

3.18.3 Safety assessment

Sensor technology	Faults in the components or wiring are only detected by manual tests, which should be performed regularly. A minimum test frequency of 1x per year is specified in the documentation. Because of anticipated fault masking and the resulting DC = 0%, use of 2-channel switches for doors or emergency stop (see 4.1.5) does not bring any gain in safety. Thus, even with 2-channel wiring, a maximum Cat. 1 is possible. 2 channels, however, are needed for the sensors; otherwise, the positively opening characteristic of the magnetic switch is not guaranteed.
Actuator technology	Faults in the components or wiring are only detected by manual tests, which should be performed regularly. A minimum test frequency of 1x per year is specified in the documentation.

3.18.4 Products (options)

	Product
–B1; –B2	Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–S1	Emergency stop control device (2-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1122 article number: R1.200.1122.0
–K1	Safety switching device *safe* RELAY: SNA 4043K/KM article number: R1.188.3250.0
–Q1	Power contactor with the following properties: • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

3.18.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	B_{10D}; T_M

To determine/confirm for application		
• No CCF required • Cat. 1 • No DC required • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• No CCF required • Cat. 1 • No DC required • n_{op}

Maximum attainable PL		
PL c	PL e	PL c

PL c
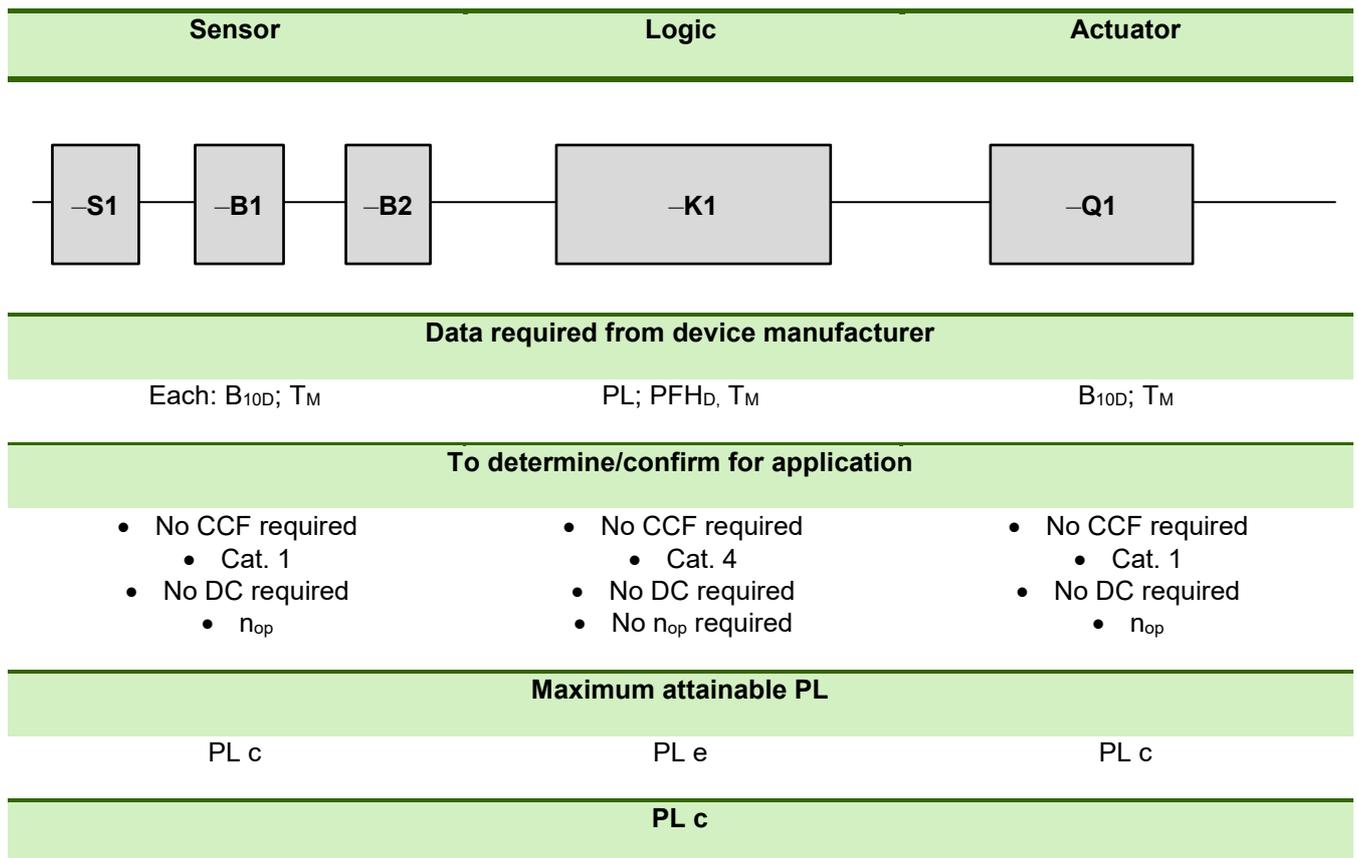
EMERGENCY stop & door switch, magnetic in series, 2-channel in PL c

3.18.6 Circuit diagram
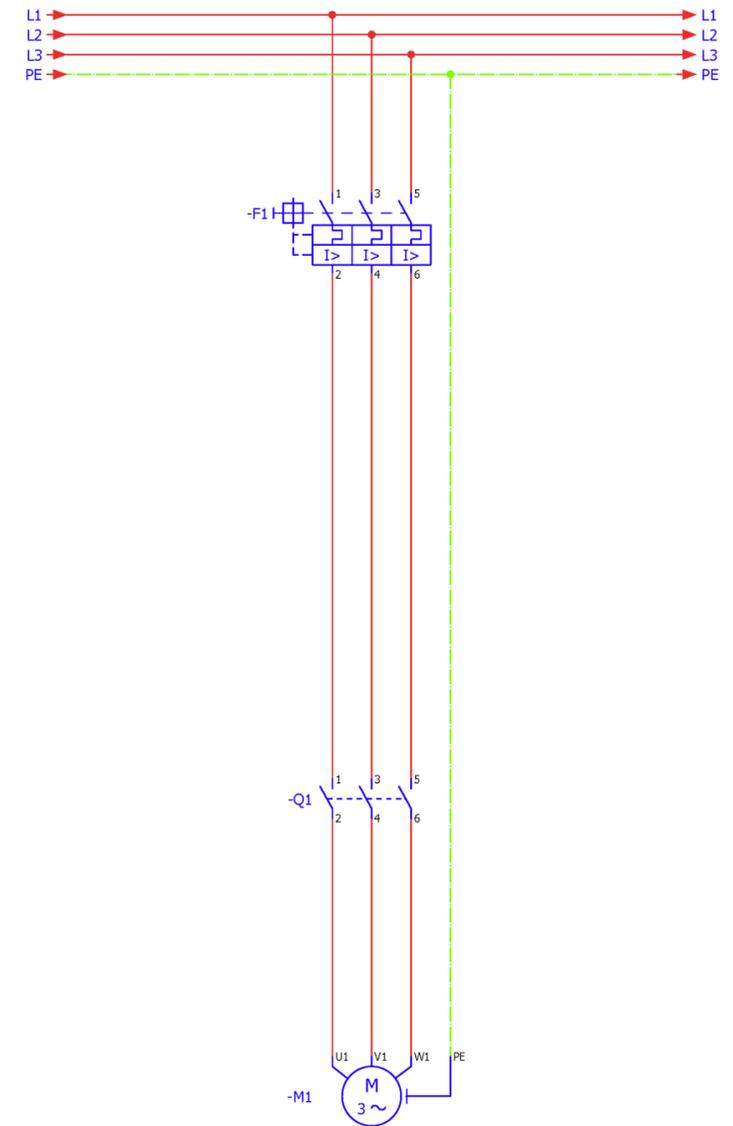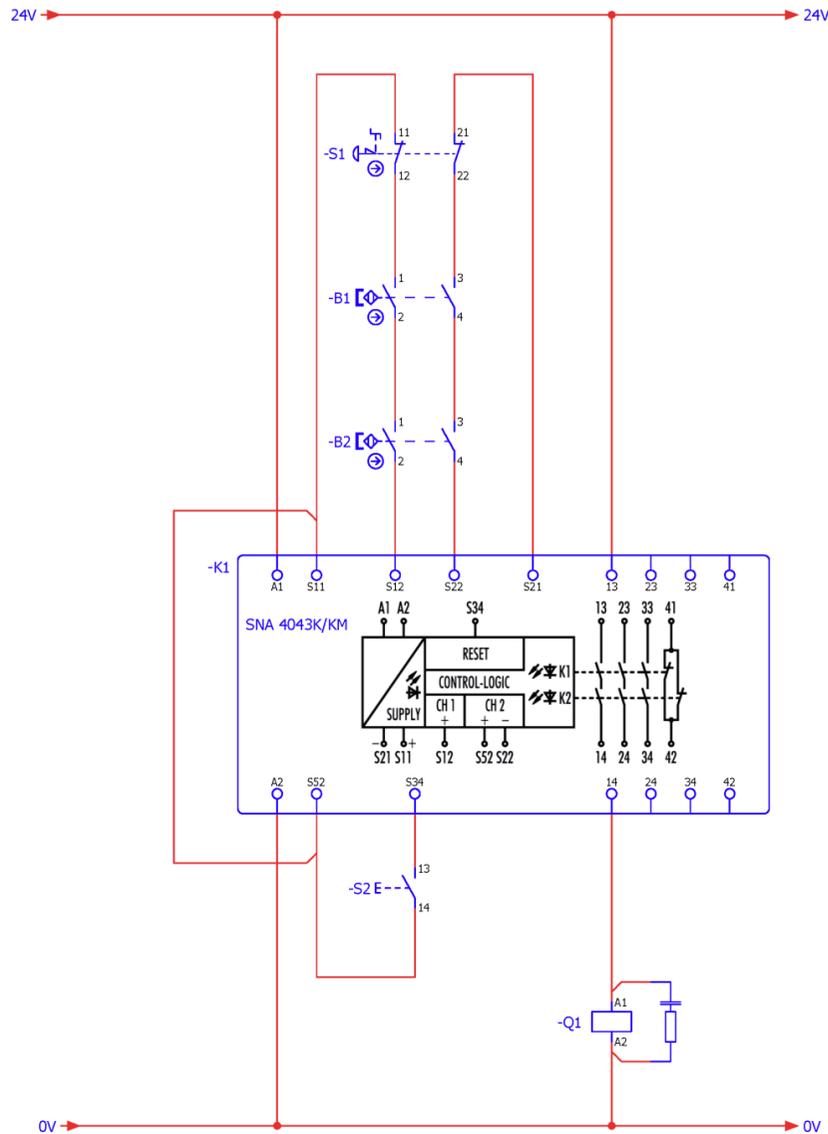
3.19 Magnetic door switches in series – 2-channel in PL d

3.19.1 Safety function

Safety function	When the door(s) are opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	One or more doors are opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.19.2 Description

Function	By opening the door(s): • Door switch(es) are actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Positively driven contactors –Q1 and –Q2 are switched off. • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door(s). The door switches (–B1, –B2, –B3) are closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door(s). Start/restart must only be possible when: • The doors are closed • Positively driven contactors –Q1 and –Q2 are switched off. The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactors –Q1 and –Q2 are monitored in the feedback circuit of safety switch device –K1.

3.19.3 Safety assessment

Sensor technology	• Ground faults and cross shorts in the input circuit are detected by –K1 through the relay's intrinsic potentials (24V+/0V) on the sensor lines. • Diagnosis through "Cross comparison and high quality fault detection" by –K1. This itself would lead to DC = 99%; but because of the series wiring, cannot be realized. Because of the cascading (wiring in series), an open door can prevent a fault in another door from being detected (fault masking). If it is guaranteed that only one of the doors is frequently actuated (a maximum 1x per hour), up to 5 additional doors can be wired in series and a medium or low DC is attainable, up to a maximum PL d. Here, DC = low = 60% is assumed. See also ISO/TR 24119.
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –Q1 and –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. DC = 99%

3.19.4 Products (options)

|	Product
–B1; –B2; –B3	Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–K1	Safety switching device *safe* RELAY: SNA 4043K/KM article number: R1.188.3250.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Magnetic door switches in series – 2-channel in PL d

3.19.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
  • Cat. 4
• DC = 60%
  • n_{op}
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		• DC = 99%
		  • n_{op}

Maximum attainable PL		
PL d	PL e	PL e

PL d
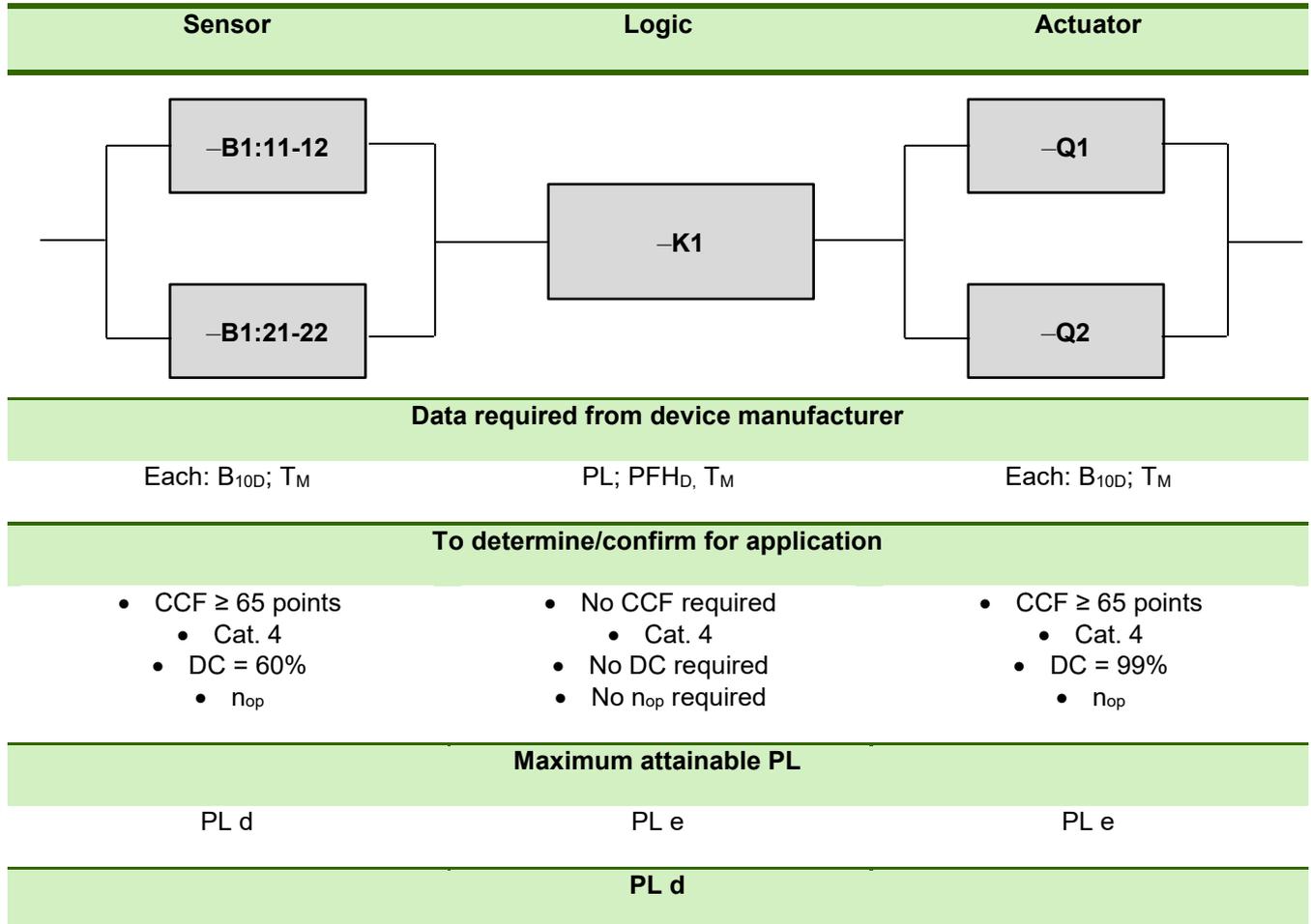
Note: *For sensors –B2 and –B3, the modeling and the attainable PL are identical – as long as sensors of the same design are used.*

Safety functions

Magnetic door switches in series – 2-channel in PL d

3.19.6 Circuit diagram
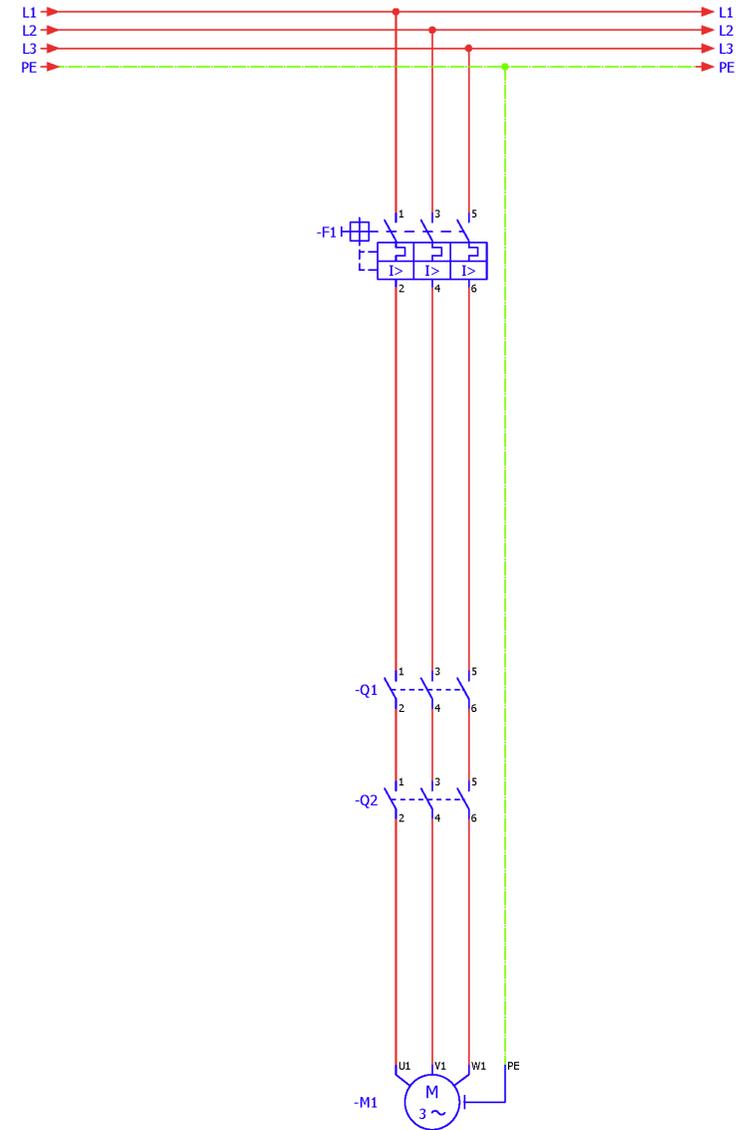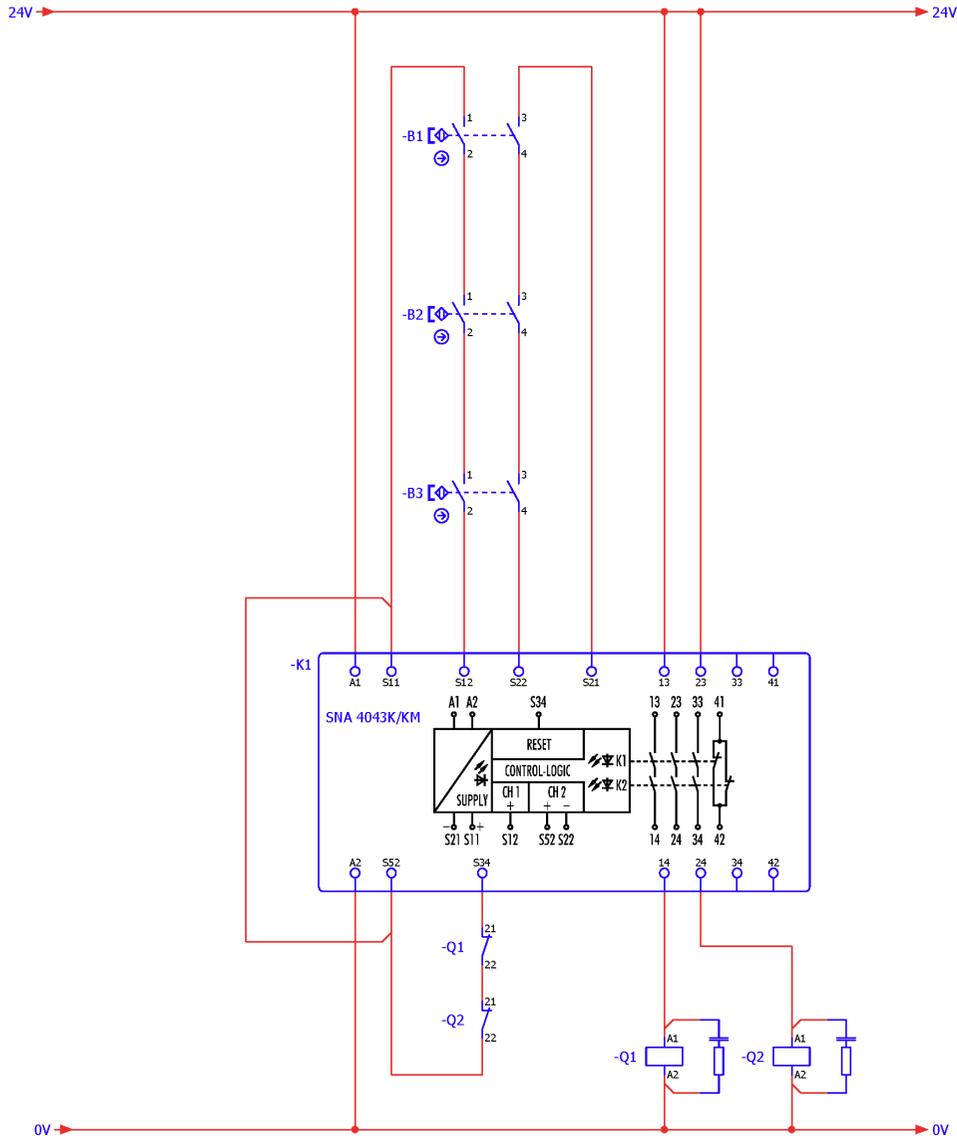
3.20 RFID door switch in series – 2-channel, equivalent in PL e

3.20.1 Safety function

Safety function	When the door(s) are opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	One or more doors are opened by operator.
Reaction	Power to drives disconnected through –T1 by means of STO.
Safe state	Drives have no power.

3.20.2 Description

Function	By opening the door(s): • Door switch(es) are actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Frequency converter –T1 shut down through STO_A and STO_B • Machine 1 is stopped.
Manual reset function	The safety function is manually reset by closing the door(s). Door switches (–B1, –B2) are closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door(s). Start/restart must only be possible when: • The doors are closed The constructive design prevents access behind the doors.

3.20.3 Safety assessment

Sensor technology	• All door sensors are self-monitoring. • All senors have OSSD outputs • Cross shorts between OSSD output signals are detected by the sensor and if there is a fault, cause both OSSD outputs to shut down. • Short circuits to 24 V or GND in the OSSD outputs are detected by safety switching device –K1 or the respective downstream door sensor through cross comparison. • Because all faults are diagnosed individually, fault masking (masking) is excluded. A DC = 99% (cross comparison and high quality fault detection) can be assumed for all sensors. • Keep in mind that the switching times of all door sensors add up for the respective upstream door sensor in the series (here, –B1).
Actuator technology	• Frequency converter –T1 is a pre-certified safety component with integrated diagnosis. • No feedback circuit is required.

Safety functions

RFID door switch in series – 2-channel, equivalent in PL e

3.20.4 Products (options)

	Product
–B1; –B2	Interlocking device, design 4 (RFID door switch) *sensor* PRO: STS01xx article number: R1.400.0110.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–T1	Safe frequency converter with integrated diagnosis and an evaluation as PL e. Integrated STO safety function.

3.20.5 Modeling per EN ISO 13849-1

Sensor	*Logic*	*Actuator*

Data required from device manufacturer		
PL; PFH_D, T_M	Each: PL; PFH_D, T_M	PL; PFH_D, T_M

To determine/confirm for application		

• No CCF required
  • Cat. 4
• No DC required
• No n_{op} required
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• No CCF required
		  • Cat. 4
		• No DC required
		• No n_{op} required

Maximum attainable PL		
PL e	PL e	PL e

PL e

Note: The determination applies to sensor –B1. If there is an internal fault, sensor –B2 can prevent transmission of the signals from sensor –B1. Thus, it contributes to the likelihood of failure of this safety function.

RFID door switch in series – 2-channel, equivalent in PL e

3.20.6 Circuit diagram
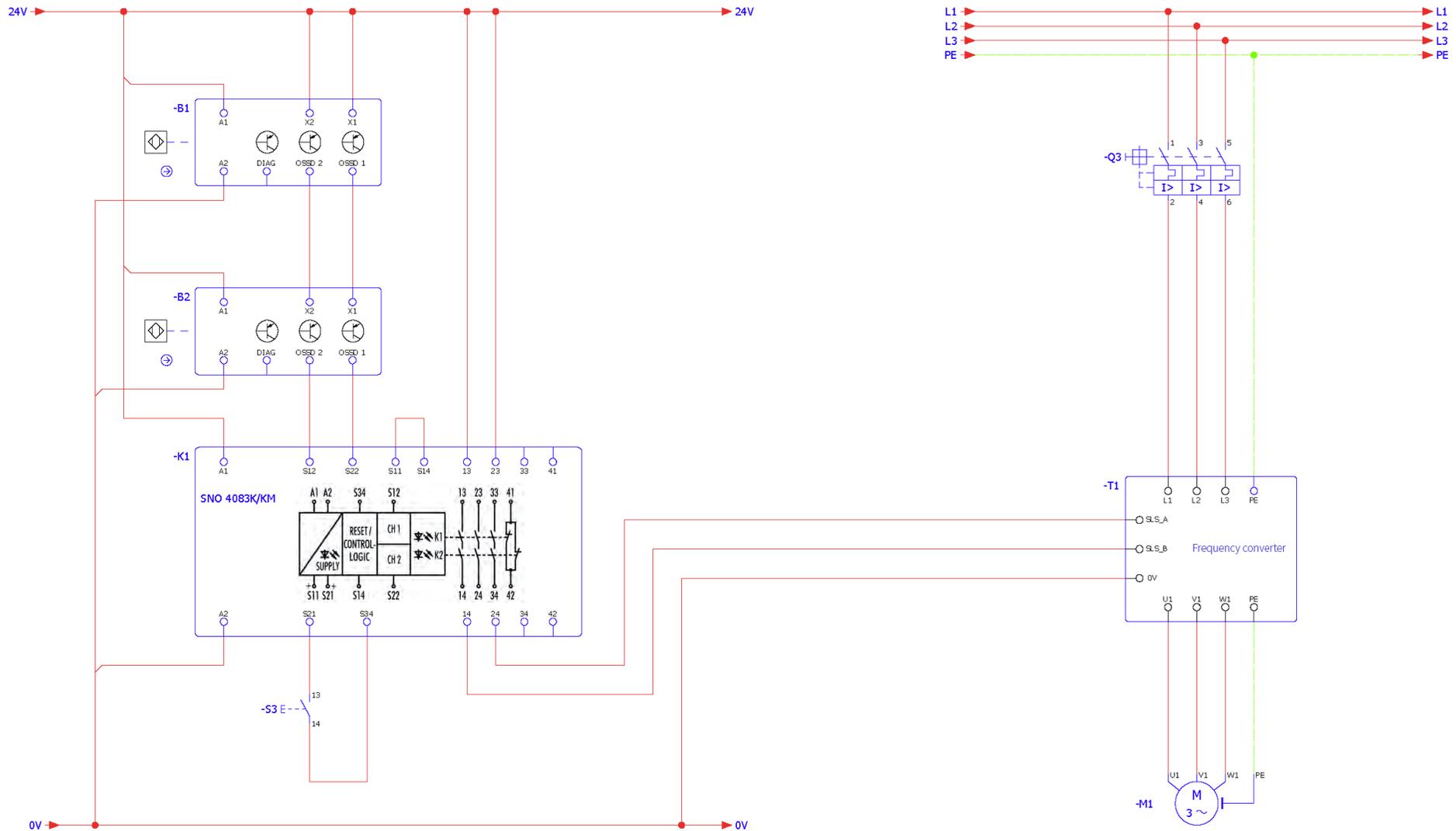
3.21 Door switch, RFID & emergency stop in series (1) – emergency stop –S1 in PL c

3.21.1 Safety function (of emergency stop)

Safety function	When the emergency stop button –S1 is actuated, all drives are brought to a stop.
Trigger event	One of the emergency stop buttons –S1 is actuated by the operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.21.2 Description

Function	By actuating the emergency stop button –S1: • Input circuit is interrupted at door switch –B2 • OSSD contacts from –B2 open • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off and machine –M1 is stopped.
Manual reset function	The safety function manual reset is initiated when emergency stop button –S1 is rotated to unlock it.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Emergency stop button –S1 is not actuated • Doors –B1 and –B2 are closed. • Contactors –Q1 and –Q2 are switched off
Feedback circuit	The positively driven NC contacts of contactor –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of –K1.

Safety functions

3.21.3 Safety assessment

|	
Sensor technology	• All faults on the emergency stop and its wiring are detected by –S1 or –B2. • The emergency stop button is equipped with a malfunction safeguard. This feature detects when the actuator is triggered by the switch contacts and interrupts the electrical emergency stop circuit. • Diagnosis of faults in the line between –B2 and –K1 is done jointly by –B1 and –B2 • During normal operation, it can be expected that door switch –B1 and emergency stop –S1 will be actuated in close succession and so are activated at the same time. Thus, fault masking for the emergency stop can be expected (initial faults in –S1 concealed by functioning –B1 and remain undetected). Because –S1 does not have its own integrated diagnosis, DC = none is to be assumed for the emergency stop. • Keep in mind that the switching times of all door sensors add up for the respective upstream door sensor.
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

3.21.4 Products (options)

	Product
–S1	Emergency stop control device (2-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1122 article number: R1.200.1122.0
–B2	Interlocking device, design 4 (RFID door switch) *sensor* PRO: STS01xx article number: R1.400.0110.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

3.21.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator
Manufacturer specification – **S1:11-12** / Manufacturer specification – **S1:21-22**	**–B2** **–K1**	**–Q1** / **–Q2**

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• No CCF required
  • Cat. 1
• DC = None
  • n_{op}
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		• DC = 99%
		  • n_{op}

Maximum attainable PL		
PL c	PL e	PL e

PL c		

wieland

3.22 Door switch, RFID & emergency stop in series (1) – door –B1 in PL e

3.22.1 Safety function (of door 1)

Safety function	When door 1 –B1 is opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	Door 1 –B1 opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.22.2 Description

Function	By opening door 1 –B1: • OSSD contacts of –B1 open • Input circuit is interrupted at door switch –B2 • OSSD contacts from –B2 open • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off. • Machine M1 is stopped.
Manual reset function	Manual reset of the safety function is actuated by closing door 1 –B1
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Emergency stop button –S1 is not actuated • Doors –B1 and –B2 are closed. • Contactors –Q1 and –Q2 are switched off The constructive design prevents access behind the doors.
Feedback circuit	The positively driven NC contacts of contactor –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of –K1.

Safety functions

3.22.3 Safety assessment

Sensor technology	• –B1 is self-monitoring and is equipped with OSSD outputs • Cross shorts between OSSD output signals are detected by the sensor and if there is a fault, cause both OSSD outputs to shut down. • Short circuits to 24 V or GND in the OSSD outputs are detected by safety switching device –K1 or the respective downstream door sensor through cross comparison. • Each individual fault is detected and causes both OSSD channels to be switched off. This exclude fault masking (masking) or fault accumulation. A DC = 99% (cross comparison and high quality fault detection) can be assumed for –B1. Keep in mind that the switching times of all door sensors add up for the respective upstream door sensor in the series (here, –B1).
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

3.22.4 Products (options)

	Product
–B1; –B2	Interlocking device, design 4 (RFID door switch) *sensor* PRO: STS01xx article number: R1.400.0110.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Door switch, RFID & emergency stop in series (1) – door –B1 in PL e

3.22.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
PL; PFH_D, T_M	Each: PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• No CCF required
   • Cat. 4
• No DC required
• No n_{op} required
	• No CCF required
	   • Cat. 4
	• No DC required
	• No n_{op} required
		• CCF ≥ 65 points
		   • Cat. 4
		• DC = 99%
		   • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e
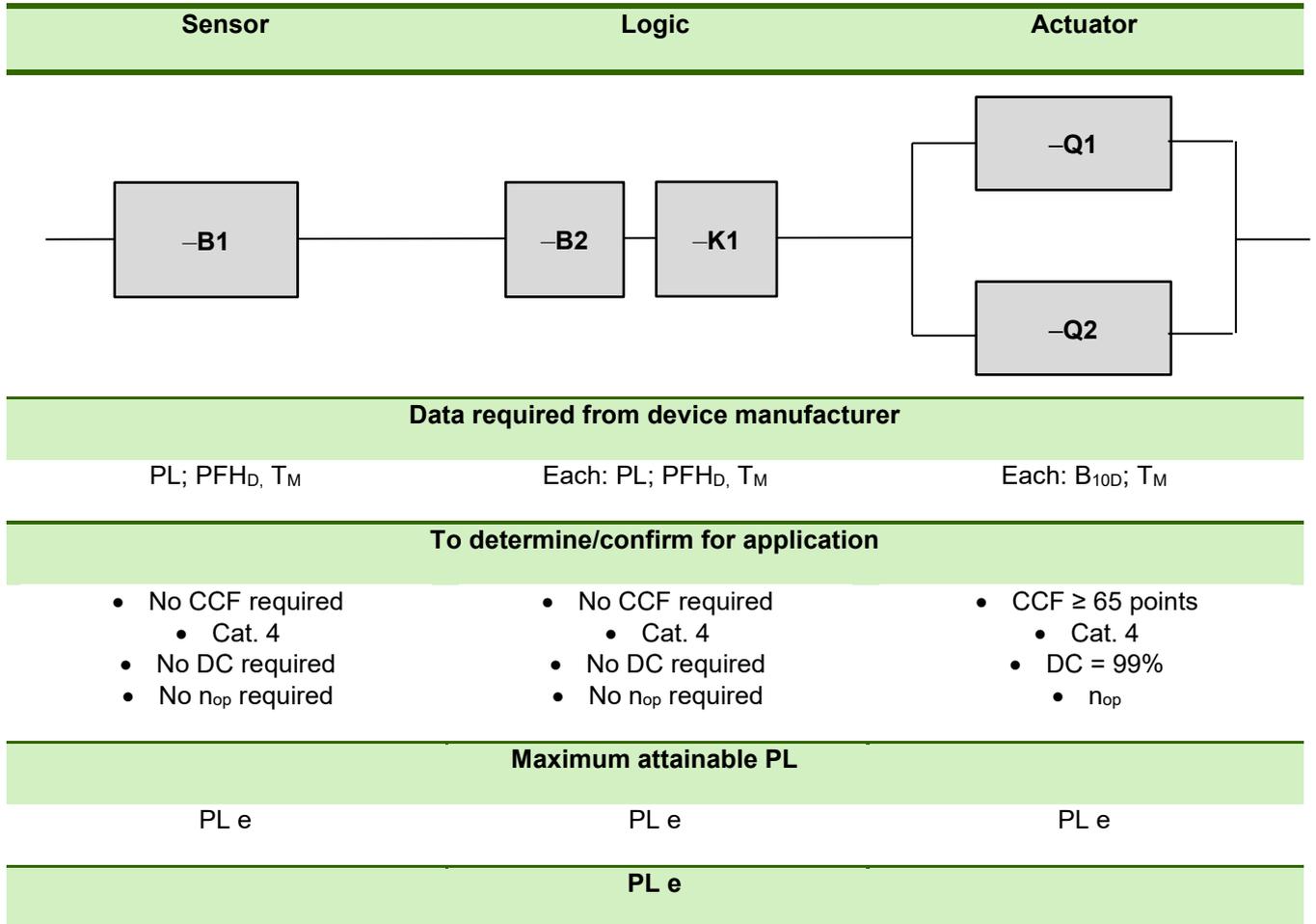
Safety functions

Door switch, RFID & emergency stop in series (1) – door –B1 in PL e

3.22.6 Circuit diagram
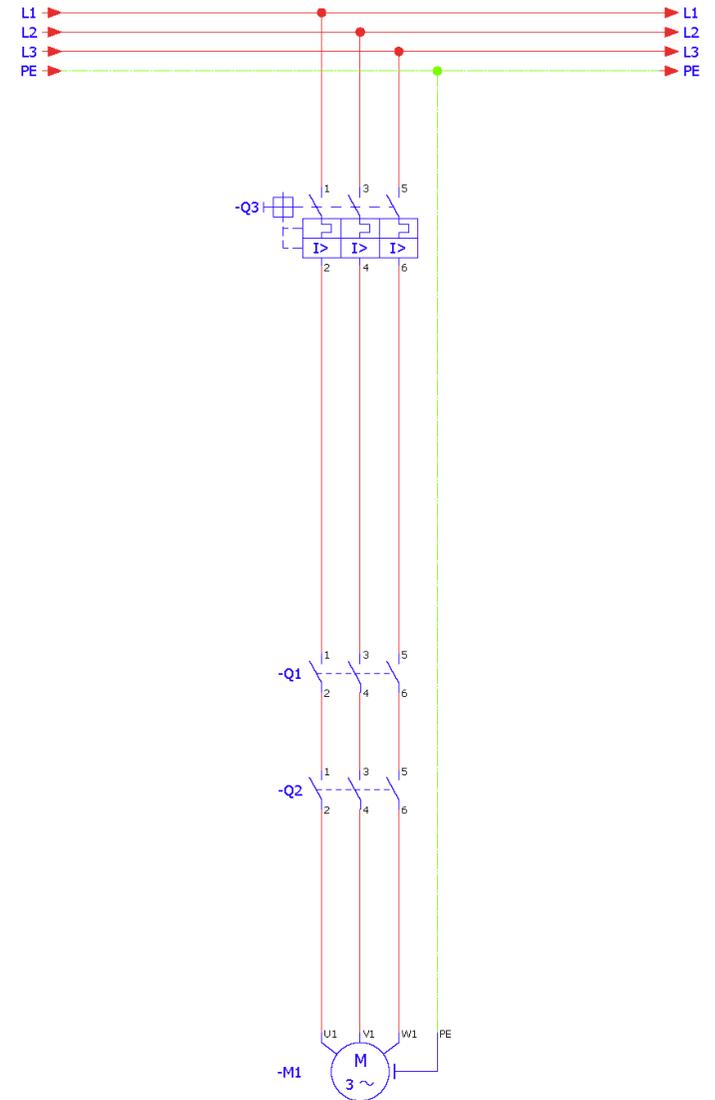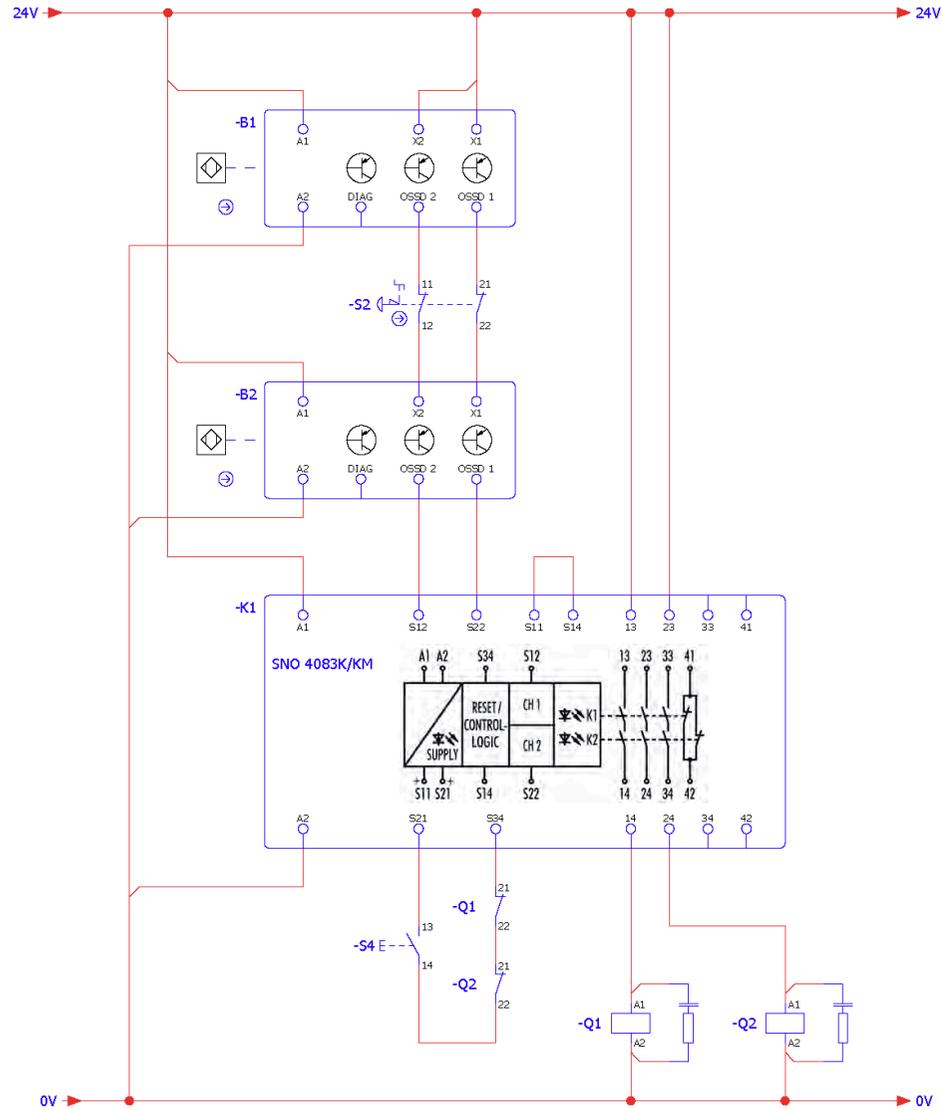
3.23 Door switch, RFID & emergency stop in series (1) – door –B2 in PL e

3.23.1 Safety function (of door 2)

Safety function	When the door(s) are opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	One or more doors are opened by operator.
Reaction	Power supply to drives is disconnected
Safe state	Drives have no power.

3.23.2 Description

Function	By opening the door(s): • Door switch(es) are actuated • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off and machine –M1 is stopped.
Manual reset function	The safety function is manually reset by closing the door(s). Door switches (–B1, –B2) are closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door(s). Start/restart must only be possible when: • The doors are closed The constructive design prevents access behind the doors.

3.23.3 Safety assessment

Sensor technology	• All door sensors are self-monitoring. • All senors have OSSD outputs • Cross shorts between OSSD output signals are detected by the sensor and if there is a fault, cause both OSSD outputs to shut down. • Short circuits to 24 V or GND in the OSSD outputs are detected by safety switching device –K1 or the respective downstream door sensor through cross comparison. • Because all faults are diagnosed individually, fault masking (masking) is excluded. A DC = 99% (cross comparison and high quality fault detection) can be assumed for all sensors. • Keep in mind that the switching times of all door sensors add up for the respective upstream door sensor in the series (here, –B1).
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

3.23.4 Products (options)

	Product
–B2	Interlocking device, design 4 (RFID door switch) *sensor* PRO: STS01xx article number: R1.400.0110.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–Q1; –Q2	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Door switch, RFID & emergency stop in series (1) – door –B2 in PL e

3.23.5 Modeling per EN ISO 13849-1
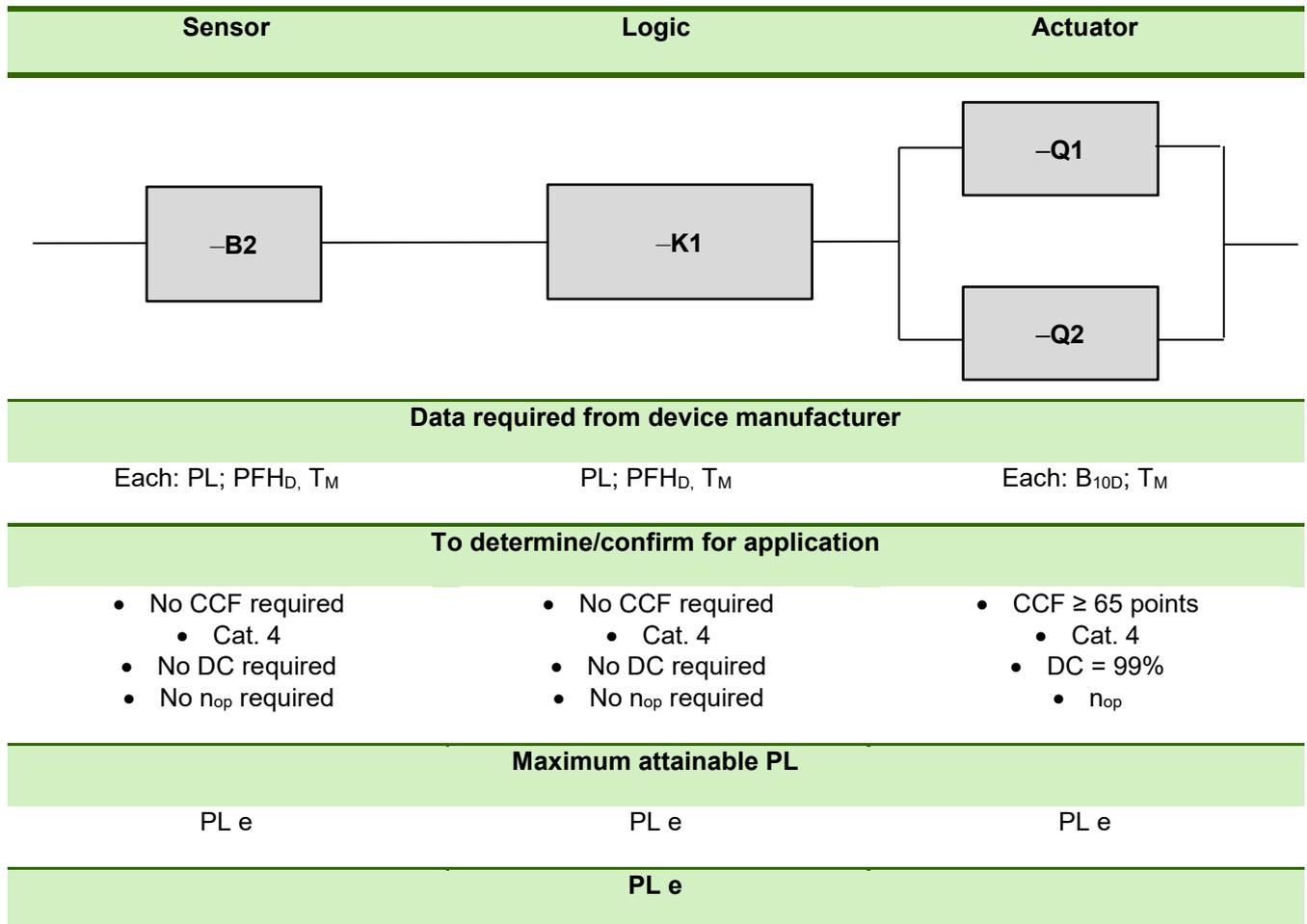
Sensor	Logic	Actuator

Data required from device manufacturer		
Each: PL; PFH_D, T_M	PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		
- No CCF required - Cat. 4 - No DC required - No n_{op} required	- No CCF required - Cat. 4 - No DC required - No n_{op} required	- CCF ≥ 65 points - Cat. 4 - DC = 99% n_{op}

Maximum attainable PL		
PL e	PL e	PL e
PL e		

3.23.6 Circuit diagram
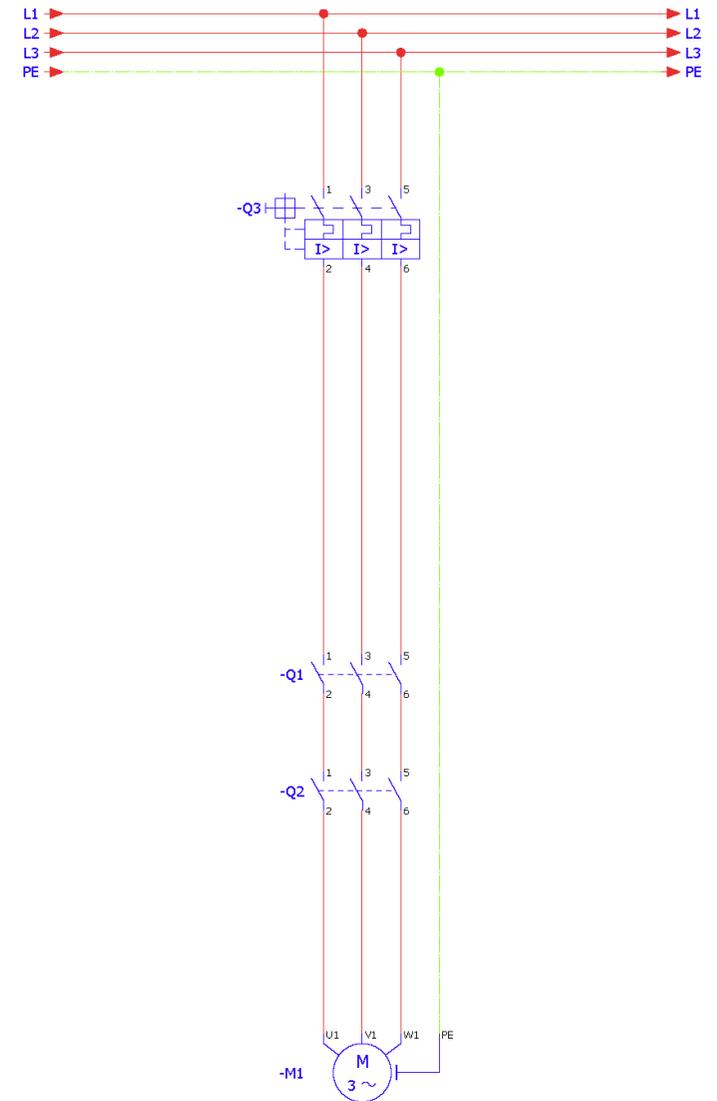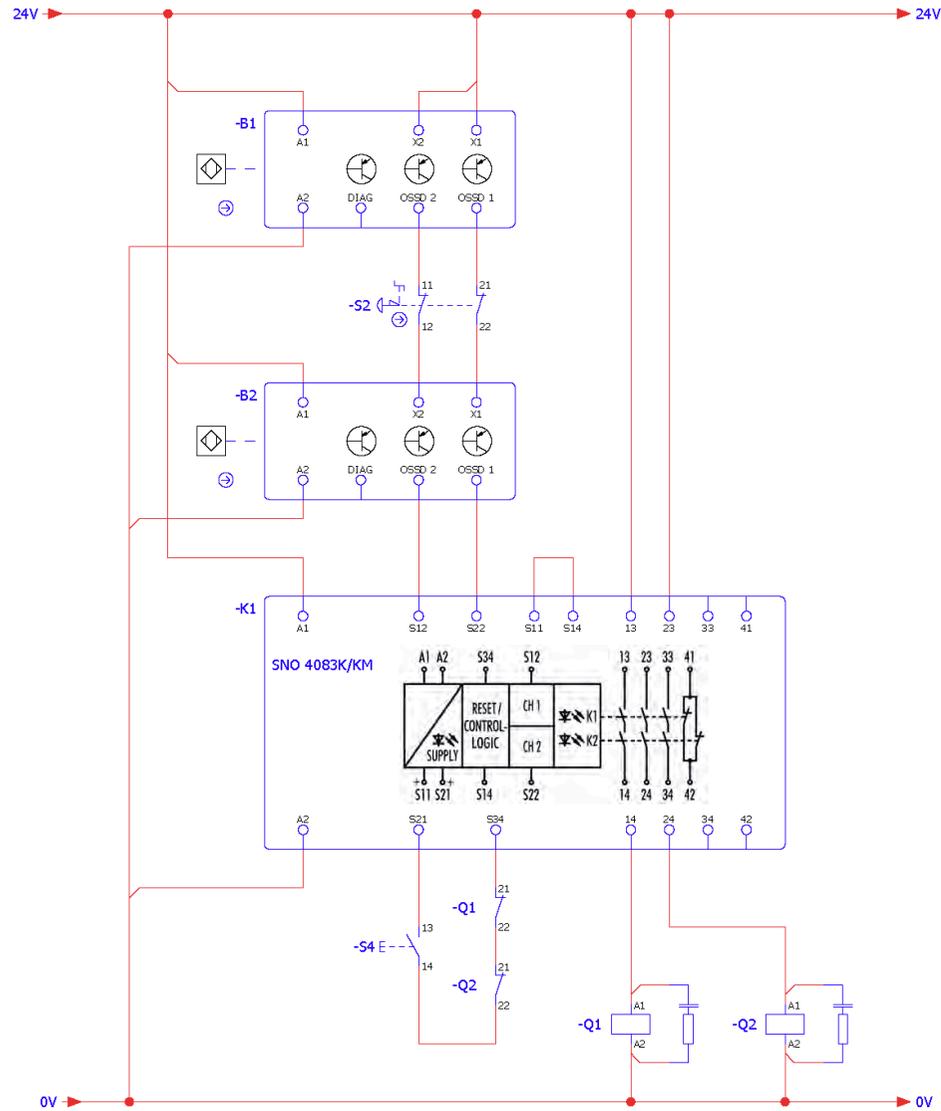
3.24 Door switch, RFID & emergency stop in series (2) – emergency stop in PL e

3.24.1 Safety function (of emergency stop)

Safety function	When the emergency stop button –S1 is actuated, all drives in the system are brought to a controlled standstill.
Trigger event	One of the emergency stop buttons –S1 is actuated by the operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.24.2 Description

Function	By actuating the emergency stop button –S1: • Input circuit is interrupted at door switch –B1 • OSSD contacts of –B1 open • Input circuit is interrupted at door switch –B2 • OSSD contacts from –B2 open • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off. • Machine M1 is stopped.
Manual reset function	The safety function manual reset is initiated when emergency stop button –S1 is rotated to unlock it.
Start/restart function	The start/restart function is initiated by actuating –S2. Start/restart must only be possible when: • Emergency stop button –S1 is not actuated • Doors –B1 and –B2 are closed. • Contactors –Q1 and –Q2 are switched off
Feedback circuit	The positively driven NC contacts of contactor –Q1: 21-22 and –Q2: 21-22 are monitored in the feedback circuit of –K1.

3.24.3 Safety assessment

Sensor technology	• Ground faults in the input circuit are detected on the sensor lines by –B1. Because of the structure Cat. 3, cross shorts are not detected; thus "Cross comparison with dynamization, without high quality fault detection" → DC = 90 % • The emergency stop button is equipped with a malfunction safeguard. This feature detects when the actuator is triggered by the switch contacts and interrupts the electrical emergency stop circuit. • Synchronization time monitoring between input circuits –S12 and –S22 • Keep in mind that the switching times of all door sensors add up for the respective upstream door sensor. • Diagnosis of faults in the line between –B1 and –B2 is done jointly by –B1 and –B2 • Diagnosis of faults in the line between –B2 and –K1 is done jointly by –B1 and –B2
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

3.24.4 Products (options)

	Product
–S1	Emergency stop control device (2-channel) with integrated malfunction safeguard *sensor* PRO: SNH-1122 article number: R1.200.1122.0
–B1; –B2	Interlocking device, design 4 (RFID door switch) *sensor* PRO: STS01xx article number: R1.400.0110.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–T1	Power contactor with the following properties: • Contactor with positively driven feedback contacts • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M

Safety functions

Door switch, RFID & emergency stop in series (2) – emergency stop in PL e

3.24.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Manufacturer specification – **S1:11-12**	–B1 –B2 –K1	–Q1
Manufacturer specification – **S1:21-22**		–Q2

Data required from device manufacturer		
Each: B_{10D}; T_M	Each: PL; PFH_D, T_M	Each: B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
   • Cat. 3
 • DC = 90%
   • n_{op}
	• No CCF required
	   • Cat. 4
	 • No DC required
	 • No n_{op} required
		• CCF ≥ 65 points
		   • Cat. 4
		 • DC = 99%
		   • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e
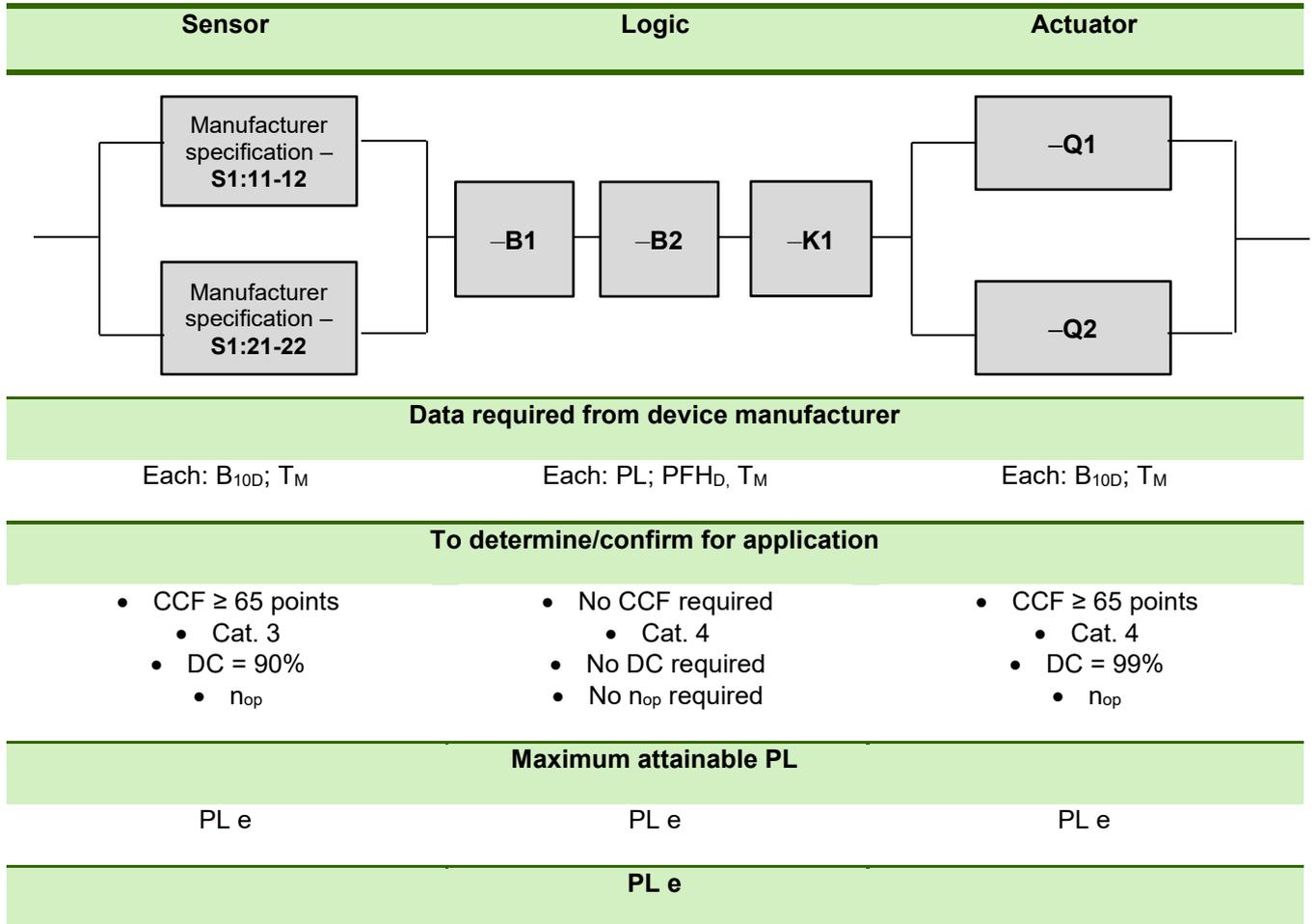
Safety functions

Door switch, RFID & emergency stop in series (2) – emergency stop in PL e

3.24.6 Circuit diagram
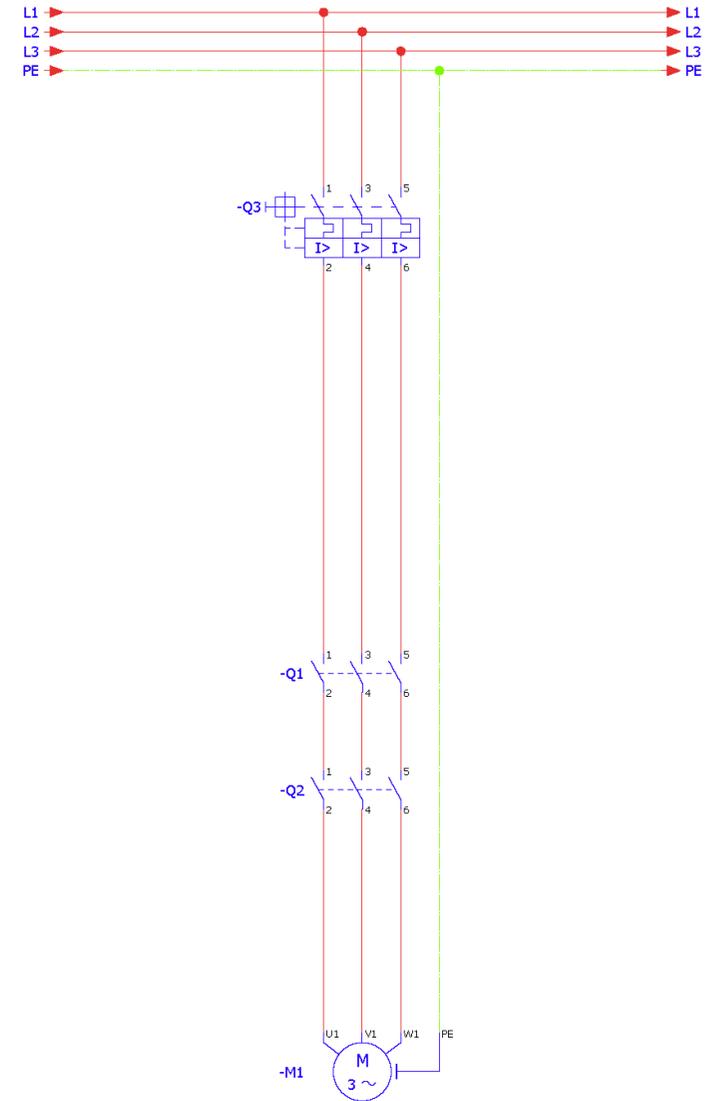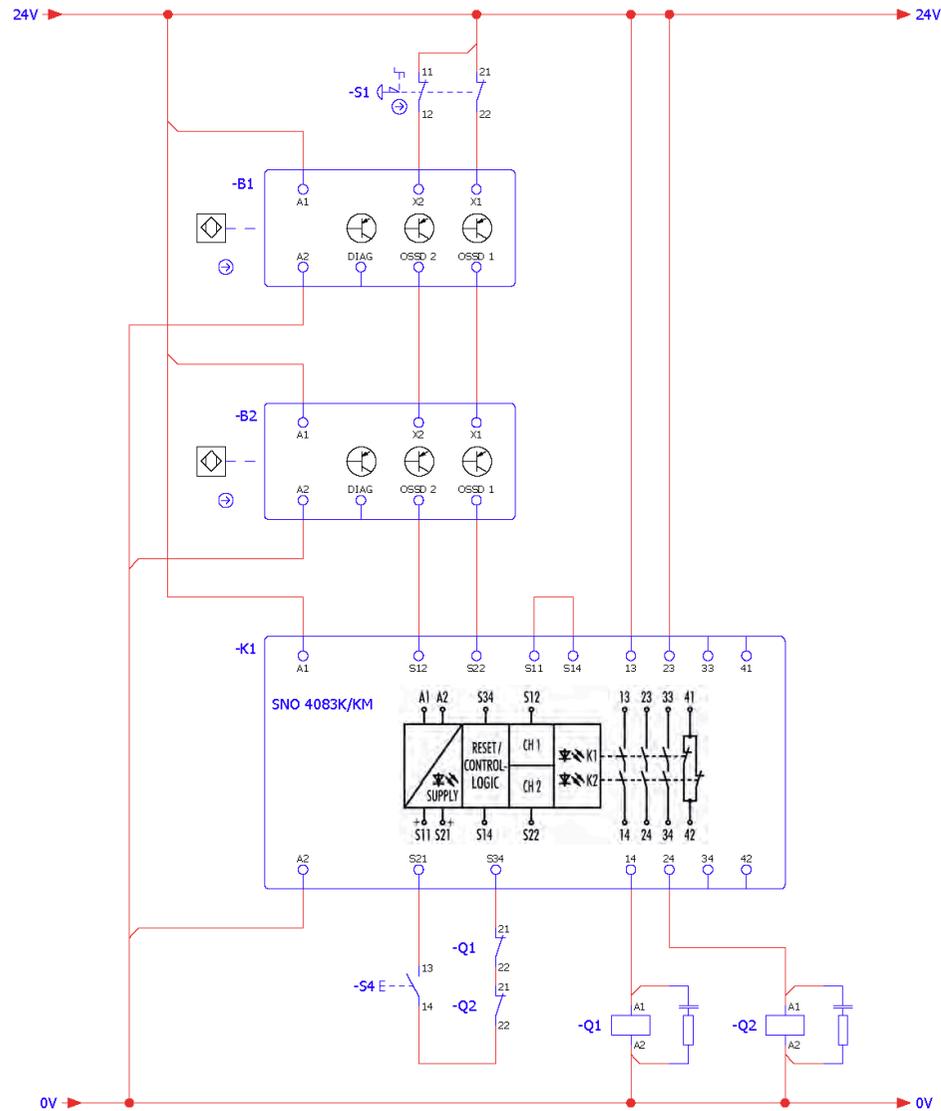
3.25 Door switch, RFID & emergency stop in series (2) – door in PL e

3.25.1 Safety function (of doors)

Safety function	When the door(s) are opened, all drives in the system are brought to a stop and disconnected from power.
Trigger event	One or more doors are opened by operator.
Reaction	Power supply to drives is disconnected.
Safe state	Drives have no power.

3.25.2 Description

Function	By opening the door(s): • Door switch(es) are actuated • OSSD contacts of –B1 open • Input circuit is interrupted at door switch –B2 • OSSD contacts from –B2 open • Input circuit is interrupted at safety switching device –K1 • –K1 safety contacts are opened • Contactors –Q1 and –Q2 are switched off. • Machine M1 is stopped.
Manual reset function	The safety function is manually reset by closing the door(s). Door switches (–B1, –B2) are closed. The constructive design ensures that the door(s) cannot close accidentally.
Start/restart function	The start/restart function is actuated by closing the door(s). Start/restart must only be possible when: • The doors are closed The constructive design prevents access behind the doors.

Safety functions

3.25.3 Safety assessment

Sensor technology	• All door sensors are self-monitoring. • All senors have OSSD outputs • Cross shorts between OSSD output signals are detected by the sensor and if there is a fault, cause both OSSD outputs to shut down. • Short circuits to 24 V or GND in the OSSD outputs are detected by safety switching device –K1 or the respective downstream door sensor through cross comparison. • Because all faults are diagnosed individually, fault masking (masking) is excluded. A DC = 99% (cross comparison and high quality fault detection) can be assumed for all sensors. • Keep in mind that the switching times of all door sensors add up for the respective upstream door sensor in the series (here, –B1).
Actuator technology	• Due to the separate actuation of –Q1 and –Q2, along with the high quality diagnosis by reading back the contacts, a protected wiring installation between –K1 and –Q1 / –Q2 is not needed. • The contactors are equipped with positively driven feedback contacts. • Direct monitoring (e.g., electrical position monitoring of control valves; monitoring of electromechanical units via positive guidance) through –K1. DC = 99%

3.25.4 Products (options)

	Product
–B1; –B2	Interlocking device, design 4 (RFID door switch) *sensor* PRO: STS01xx article number: R1.400.0110.0
–K1	Safety switching device *safe* RELAY: SNO 4083KM article number: R1.188.3580.0
–T1	Safe frequency converter with integrated diagnosis and an evaluation as PL e. Integrated STO safety function.

Safety functions

Door switch, RFID & emergency stop in series (2) – door in PL e

3.25.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

Data required from device manufacturer		
PL; PFH_D, T_M	Each: PL; PFH_D, T_M	PL; PFH_D, T_M

To determine/confirm for application		

• No CCF required
  • Cat. 4
• No DC required
• No n_{op} required
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• No CCF required
		  • Cat. 4
		• No DC required
		• No n_{op} required

Maximum attainable PL		
PL e	PL e	PL e

PL e
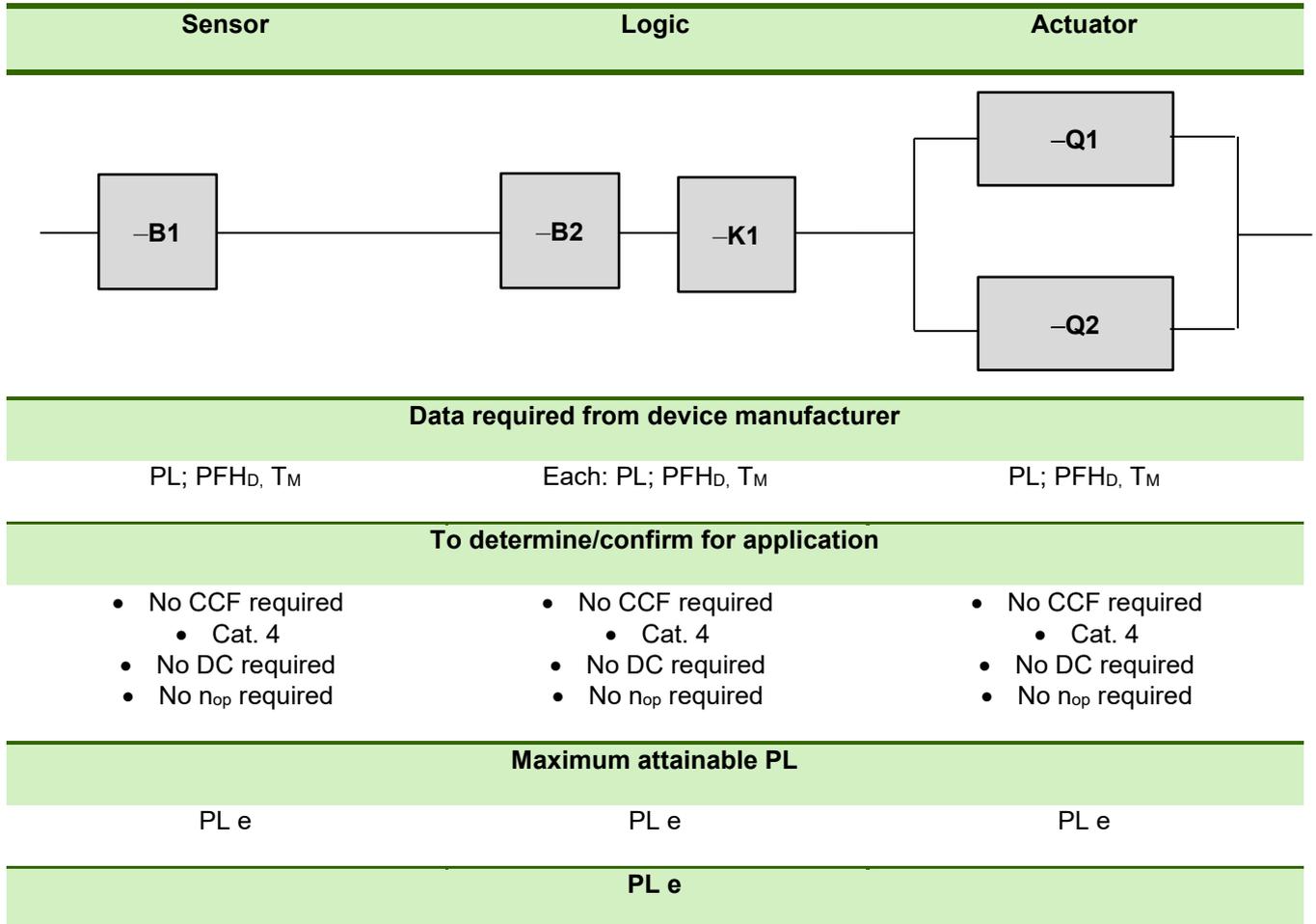
Note: *The determination applies to sensor –B1. For sensor –B2, modeling is shortened by –B1. Because the modeling that is shown represents the worst-case scenario, it is taken for all sensors.*

Safety functions

wieland

3.25.6 Circuit diagram

3.26 Operating mode selection switch in PL e

3.26.1 Safety function

Safety function	A fault in the operating mode selection switch must not lead to unintended switching.
Trigger event	Implausible operating mode selection signal is present.
Reaction	Machine is stopped -> mode "off."
Safe state	The following options represent safe state: • The operating mode shown on the mode selection switch is active and all other modes are inactive. • Operating mode "off" is active (no operation possible)

Note: *The operating mode selection switch can also can be included in consideration of all safety functions with safety that depends on presence of the correct operating mode. However, this does make consideration of the respective safety functions more complex. For this reason, separate displays were selected here.*

Caution: *Note that the PL_r of this safety function is dependent on the PL_r of the dependent safety function. Especially when the change of operating modes is coupled with certain authorizations or competencies or not all safety functions have the same PL_r, it is obvious that the PL_r for this safety function should be oriented to the highest PL_r of the safety function involved.*

3.26.2 Description

Function	By actuating operating mode selection switch –S1: • Exactly one input circuit on safety switching device –K1 is closed; at the same time, all others are interrupted • The internal evaluation on –K1 checks for plausibility • The operating mode indicated by the switch position is activated • If a fault is detected, frequency converter –T1 is stopped through STO_A and STO_B
Manual reset function	Not required
Start/restart function	Not required
Feedback circuit	Not needed here, since –T1 is a device with integrated diagnosis.

3.26.3 Safety assessment

Sensor technology	• Ground faults, cross shorts and short circuits to 24 V in the input circuit are detected by –K1 through plausibility checks on the sensor lines. • The software checks that exactly one input is active at any given time. If it is detected, that no input is active or several are, it is evaluated as a fault. • The 1 from N circuit corresponds to the system behavior of Category 4. • Each individual fault is detected by the request at the latest and does not cause loss of safety. • Fault accumulations do not cause loss of safety • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99%
Actuator technology	• Frequency converter –T1 is a pre-certified safety component with integrated diagnosis. • No feedback circuit is required.

3.26.4 Products (options)

	Product
–S1	Operating mode selection switch • Can be closed from any position • Switch position display • Exactly one output contact connected with the root contact in each case
–K1	Programmable safety controller *samos* PRO: SP-COP2, article number: R1.190.1310.0
–T1	Safe frequency converter with integrated diagnosis and an evaluation as PL e. Integrated STO safety function.

Safety functions

Operating mode selection switch in PL e

3.26.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator
−S1	−K1	−T1

Data required from device manufacturer		
B_{10D}; T_M	PL; PFH_D, T_M	B_{10D}; T_M

To determine/confirm for application		

• CCF ≥ 65 points
  • Cat. 4
• DC = 99%
  • n_{op}
	• No CCF required
	  • Cat. 4
	• No DC required
	• No n_{op} required
		• CCF ≥ 65 points
		  • Cat. 4
		• DC = 99%
		  • n_{op}

Maximum attainable PL		
PL e	PL e	PL e

PL e

Safety functions

3.26.6 Circuit diagram
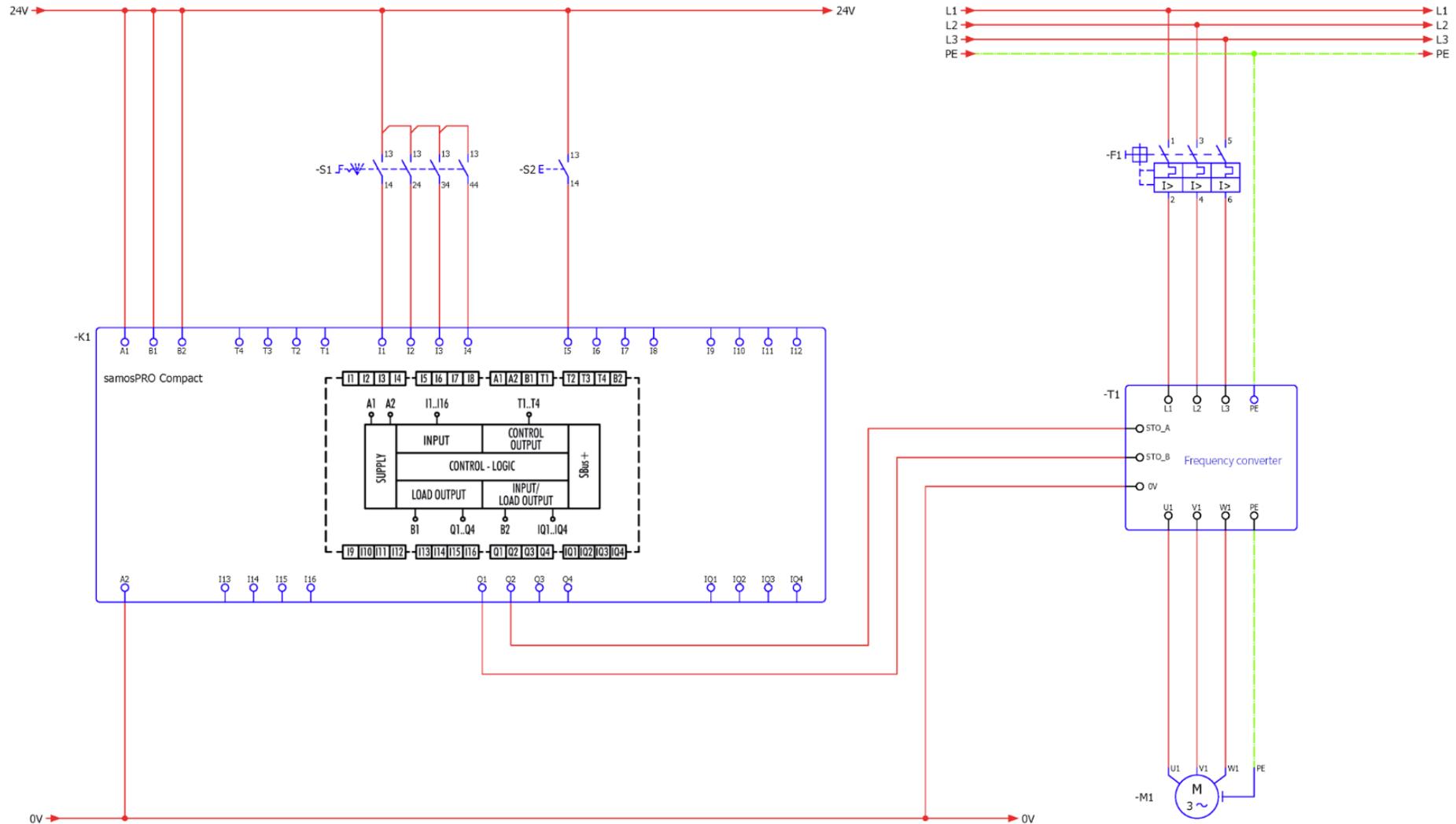
3.27 Acknowledgment button in PL e

3.27.1 Safety function

Safety function	When safety door –B1 is open and if acknowledgment button –S1 has not been actuated, the machine is prevented from starting. Pressing the acknowledgment button activates an additional safety function (safe reduced drive speeds). Safe state has been reached when the drive moves at a reduced speed; or when the drive is stationary because there is no acknowledgment.
Trigger event	Acknowledgment button not actuated while door open at same time Note: Stopping the machine by pushing button to end can be considered as a separate safety function.
Reaction	Prevention of unexpected start-up
Safe state	Stop drive In case of fault, disconnect drive from power

3.27.2 Description

Function	Door	Acknowledgment button	Mode	STO (–K1:Q2)	SLS (–K1:Q1)
	Closed	Not actuated or panic (button pushed completely to end)	Automatic	On	On
	Closed	Acknowledgment	Initiate emergency stop	Off	Off
	Open	Not actuated or panic (button pushed completely to end)	STO	Off	Off
	Open	Acknowledgment	SLS	On	Off
Manual reset function	Safety function manual reset is initiated by: • Releasing acknowledgment button –S1 and • Closing door(s) and • Actuating –S2 (edge monitoring after door is closed) • The constructive design ensures that the door cannot close accidentally				
Start/restart function	The start/restart function is initiated by actuating (again) switch –S2. Start/restart must only be possible when: • The door is closed				
Feedback circuit	Not needed here, since –T1 is a device with integrated diagnosis.				

3.27.3 Safety assessment

Sensor technology	Door switch –B1 and acknowledgment button –S1
	• Ground faults, cross shorts and short circuits to 24 V in the input circuit are detected by –K1 through test impulses on the sensor lines. • Diagnosis through "Cross comparison with dynamization and high quality fault detection" by –K1. DC = 99% If the acknowledgment button is actuated while the door is closed (middle position), it is interpreted as a fault and safe state is initiated.
Actuator technology	• Frequency converter –T1 is a pre-certified safety component with integrated diagnosis. • No feedback circuit is required. • Fault exclusion on wiring between –K1 and –T1, due to fixed installation inside control cabinet.

3.27.4 Products (options)

	Product
–B1	Interlocking device, design 3 (magnetic door switch) *sensor* PRO: SMA01xx, Article Number: R1.100.0113.0
–S1	Acknowledgment button with 3 switching positions • Positive opening from middle position to full end position • Self-reset from middle position to non-pressed position • Suitable for anticipated switching load and frequency. • Manufacturer specification from B_{10D} and T_M
–K1	Programmable safety controller *samos* PRO: SP-COP2, article number: R1.190.1310.0
–T1	Safe frequency converter with integrated diagnosis and an evaluation as PL e. Integrated STO and SLS safety functions.

3.27.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator

```
┌─────────┐  ┌─────────┐
│ −S1:22-14│  │ −B1:21-22│
└─────────┘  └─────────┘        ┌─────────┐      ┌─────────┐
                                │   −K1   │      │   −T1   │
┌─────────┐  ┌─────────┐        └─────────┘      └─────────┘
│ −S1:23-16│  │ −B1:13-14│
└─────────┘  └─────────┘
```

Data required from device manufacturer		
Each: B_{10D}; T_M	PL; PFH_D, T_M	PL; PFH_D, T_M

To determine/confirm for application		
• CCF ≥ 65 points • Cat. 4 • DC = 99% • n_{op}	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• No CCF required • Cat. 4 • No DC required • No n_{op} required

Maximum attainable PL		
PL e	PL e	PL e

PL e

3.27.6 Circuit diagram

3.28 Door locking in PL d

3.28.1 Safety function

Safety function	Access to the system through the movable separating protective equipment is prevented by locking until the actuators are completely without power, so the risk has been adequately minimized.
Trigger event	Once an operator requests to start drive –M1 by actuating the start button –S2, the locking device can no longer be opened.
Reaction	Locking active
Safe state	When drive is running (STO not requested) plus run-on time t_{run-on}, the locking is active. In this state, the locking device is a simple mechanical component. Now, a flow of energy to rescind the locking must be prevented.

3.28.2 Description

Function	Hold motor –M1 via operator, not as requested through start button –S2: • Output –K1:Q1 must not be switched on (STO not active) • Release for locking –A1 switched off through –K1:Q2 • Locking ensured by spring in –A1 Request for release by operator, using stop button –S1: • Open input circuit –K1:I2 for stop request • Request STO on –T1 through –K1:Q1 • Start of time delay t_{run-on} • After t_{run-on}, –A1 released Motor start requested from operator, through –S2: • Close input circuit –K1: 12 for start request • Removal of release –A1.1 • Readout through -A1:2; whether –A1 actually in lock position • When –A1 in locking position • Removal of –K1:Q1 (no STO request any more)
Manual reset function	The safety function manual reset is initiated by: • Closing the door • Removing release of –A1.1 through –K1:Q2
Start/restart function	The start/restart function is initiated either by actuating –S2 or by manual reset. Start/restart must only be possible when: • Door closure confirmed through –A1.2
Feedback circuit	Not needed, since –T1 is a device with integrated diagnosis.

3.28.3 Safety assessment

Sensor technology	The safety function is initiated according to a logic function in –K1 and can be triggered by an arbitrary input signal. Here: –S1 (stop) and –S2 (start). Because –A1 can only be unlocked when the drive is in safe state, the trigger signal is irrelevant.
Actuator technology	Assurances required through manufacturer: • If a spring breaks, a fault exclusion per EN ISO 13849-2 A.5. is accepted (validated spring). Observations by machine builder: • Because of adequate dimensioning, a fault exclusion for breakage of the bolt was made. This was plausibilized through proper use as per manufacturer instructions. • The locking involves a spring that is unlocked by an electromagnet. The electromagnet is actuated in PL e of the SPS. • A fault exclusion was also adopted for an unlocking of the lock without any power. • Installation of the lead from the SPS output is ranked as protected; hence, a fault exclusion for a short circuit to 24 V. • Because of the numerous fault exclusions, the PL is restricted to a maximum PL d. Other: • Also compare EN ISO 14119 G.3.2 • If all the above points have been fulfilled, no calculatory scrutiny of the locking device is necessary.

3.28.4 Products (options)

	Product
–K1	Programmable safety controller *samos* PRO: SP-COP2, article number: R1.190.1310.0
–A1	Interlocking device, design 2 (door switch with separate actuator) and spring-actuated locking device *sensor* PRO: SIN11xx article number: R1.310.1150.0 Assurances required through manufacturer: • Given proper use and thanks to generous dimensioning, a fault exclusion can be assigned to breakage of a bolt

Safety functions

Door locking in PL d

3.28.5 Modeling per EN ISO 13849-1

Sensor	Logic	Actuator
	−K1	−A1

Data required from device manufacturer		
Omitted	PL; PFH_D, T_M	• Fault exclusion upon actuator breakage during approved use •

To determine/confirm for application		
Omitted	• No CCF required • Cat. 4 • No DC required • No n_{op} required	• CCF at least 65 points • Cat. 2 • No DC required • No n_{op} required

Maximum attainable PL		
Omitted	PL e	PL d

PL d		

Safety functions

3.28.6 Circuit diagram
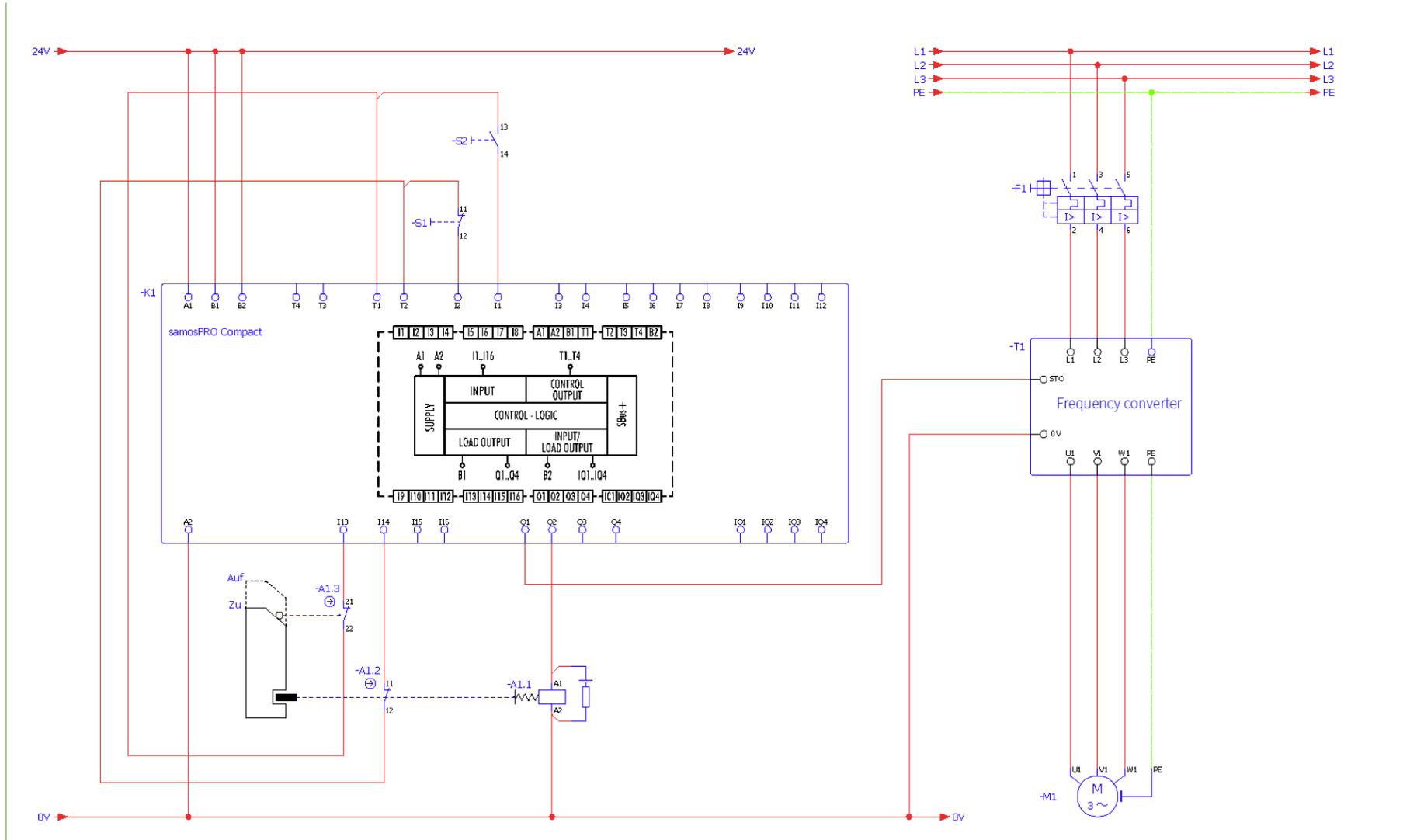
4 Safety aspects

4.1 Doors and other safety devices

4.1.1 Separating protective equipment, non-separating protective equipment or remote-hold

If there is a danger that the hazard also extends outwardly, separating protective equipment (e.g., doors or flaps) should be chosen. Therefore, definitely where radiation or the risk of parts being ejected to outside the hazard zone are concerned. Otherwise, non-separating protective equipment (e.g., light curtain, light grid) or remote-hold protective equipment (e.g., two-hand controls) are options.

4.1.2 Position monitoring or locking closed

Basically, a decision is made between two safety functions for access areas: position monitoring (interlock) and interlock with guard locking. Locking guards are able to prevent access without a required release (in plain terms: locking the door). Position monitoring only reports the door position (open or closed).

4.1.3 Coded switches

The use of coded switches has no direct influence on functional security. However, since EN ISO 14119, the subject has been noted as an aspect of manipulation.

Coding refers to a "multiplicity of keys" and in EN ISO 14119, is divided into 4 levels.

For magnetic (design 2) and mechanical (design 1) door locks, according to EN ISO 14119, usually a minimal level of codings is provided (1-9 codings). Consequently, these should be installed where they are hidden or cannot be reached. Only with higher coding can an insoluble fastening of the actuator be ensured as adequate to prevent manipulation.

4.1.4 Mechanical position switch

Mechanical position switches are usually equipped with two electrical contacts and a switch tongue. With these switches, the most frequent mistake a user makes is to use them as Cat. 3 or Cat. 4 for applications per PL d or PL e. As a general rule, this is improper use. The reason for this lies in the construction of the switch itself. They are equipped with a mechanical (1-channel) switch tongue. The switch tongue actuates a (1-channel) plunger within the switch, which then actuates two mechanical contacts. Thus, the switch consists of 3 elements of which 2 are 1-channel.

For use in PL d or PL e applications, Cat. 3 or Cat. 4 would be required throughout. These categories call for a complete 2-channel construction or a fault exclusion on the 1-channel components. For the switch tongue, the exclusion can in some cases be designated by the user under own authority if installation and environmental conditions (avoidance of corrosion, dust, etc.) are suitable. Only the switch manufacturer can assign an exclusion for the plunger. The author is not aware of any manufacturer who would confirm a mechanical fault exclusion for their switch. However, direct opening action is approved for all mechanical door switches (per EN ISO 14119).

Consequently, without further verification, a single mechanical door switch with direct opening contacts can only be used as Cat. 1 up to PL C. If the user takes a fault exclusion for the switch tongue and provides documentation verifying that the direct opening action of the internal switch tongue is interpreted as a fault exception, a complete mechanical fault exception can result. In this case, the door switch can be used up to Cat. 3, PL d. The limitation to PL d is due to the typical interpretation of the testing body that with one fault exclusion, no PL e will be permitted for a 1-channel system (see 4.3).

4.1.5 Door switches in series

It has been known for some time now that chaining door switches can result in fault masking. This is the masking of a fault in one switch by an unsuitable work process or by acknowledging a fault in a defective switch by actuating a functional switch. ISO/TR 24119 describes the problem in detail. There, fault detection in chained door switches

is treated in depth and the resulting possible diagnostic degrees of coverage (DC) are defined. See also Section 4.6.

4.1.6   Direct opening and forced actuation

"Forced actuation" refers to a movable mechanical component directly causing another component to move, either by direct contact or through rigid parts. A contact element is direct opening when the switch contacts are directly opened by a defined movement of the actuating element through non-elastic parts. Many safety sensors are provided with the symbol for direct opening action. It should always be kept in mind that the action presenting the hazard is signaled by forced actuation and direct opening action. In other words, e.g., the opening of a protective door.
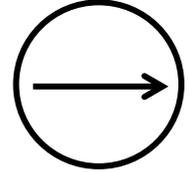
4.1.7   Opener/opener or opener/closer or closer/closer

The discussion of which of the switching principles is for 2-channel switches is better or safer is summed up with a simple: "It doesn't matter!"

Ultimately, it comes down to two safety principles:

1. Diversity
2. De-energize to trip principle

For the solution opener/closer, the diversity principle (1x opener, 1x closer) comes to bear. For the opener/opener and closer/closer solutions, the de-energize to trip principle is applied on both contacts. Technically, they are equivalent.

Relevance for the switch lies primarily in the type of installation; i.e., whether the switch is in actuated or non-actuated state as long as the door is closed Whether the forced opening of the switch can be effected, in turn, depends on this. The goal is to install the switch so when the door is opened, the switch is forcibly actuated.

4.1.8   Muting lamp

A risk assessment is required to clarify whether a muting lamp on a light grid or light curtain is needed. Standards EN/IEC 61496-1 to 3, EN/IEC 62046 and EN ISO 13849-1 state the requirements for this. Since the muting does not create any additional risks, a signal lamp can be omitted if 3 prerequisites are fulfilled:

1. BWS is equipped with a muting status symbol (on the device) and
2. In the muting is used, it will be through the transport good (and not through the carrier or pallet) and
3. The transport good prevents access to the hazard area throughout the muting.

In all other cases, a signal lamp may be necessary. However, even when the risk assessment results in the necessity of a signal lamp, the display of the muting function can be interpreted as a prompt to circumvent the protective equipment in the sense of foreseeable misuse. Weighing these two risks may conclude that despite risk assessment results indicating otherwise, a signal lamp should be omitted, if potential misuse is evaluated as the greater risk. In this case, conclusive verification that points 1 to 3 as outlined above are technically unfeasible is advised.

4.2   Reset or restart

EN ISO 13849-1 differentiates between actions and states after a stop command is issued and before restart as follows:

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

Which of the two functions should be applied in particular cases is explained below.

4.2.1   Manual reset and/or start/restart function?

In general, the requirements applicable to product and C-standards for manual reset and start/restart in each individual case are decisive. These can deviate from the general requirements stated below.

Example	Entering behind		Manual reset function	Start/reset function
	Poss-ible	Sec-ured[1]		
Emergency stop	-	-	According to EN ISO 13850, after an emergency stop, the manual reset action is enabled after the emergency stop is unlocked.	This is always required.
Separating protective equipment[2]	No	-	If no hazardous situation can arise when a door is locked, a manual reset can be omitted.	This is always required. The start/restart function can be initiated by the protective equipment itself (control function) as long as the requirements of EN ISO 12100 Sect. 6.3.3.2.5 are fulfilled.
Separating protective devices[3]	No		If no hazardous situation can arise when a protective device is locked, a manual reset can be omitted.	This is always required. The start/restart function can be initiated by the protective equipment itself (control function) as long as the requirements of EN ISO 12100 Sect. 6.3.2.5.3 are fulfilled.
Separating protective equipment[2]	Yes	Yes	If no hazards are caused by the required access prevention safety function or while a door is secured, a manual reset can be omitted for both safety functions.	This is always required. The start/restart function can be initiated by the protective equipment itself (control function) as long as the requirements of EN ISO 12100 Sect. 6.3.3.2.5 are fulfilled.
Separating protective devices[3]	Yes	Yes	If no hazardous situation can arise when a protective device is locked, a manual reset can be omitted.	This is always required. The start/restart function can be initiated by the protective equipment itself (control function) as long as the requirements of EN ISO 12100 Sect. 6.3.2.5.3 are fulfilled.
Separating[2] or optical[3] protective equipment	Yes	No	In most cases, manual reset is required.	This is always required.

1   Access barrier by means of separate safety function; e.g., safety mat, light curtain/grid or scanner.
2   E.g., safety doors
3   E.g., light curtain/grid or scanner

4.3 Aspects of emergency stop

4.3.1 Regarding the definition of an emergency stop function:

Such definitions crop up in a number of places in the European standards. For example, shutdown in emergencies is defined as: Function that should prevent or minimize hazards to persons, damage to the machine or during operation. Further, these emergencies are described as hazardous situations during normal machine operation that are caused by human intervention or a faulty function. Caution: All other hazardous situations are foreseeable and are not secured by an emergency stop!

Which, according to this definition, are not within the scope of responsibility of an emergency stop function:

- To keep the machine motionless during troubleshooting, cleaning or maintenance work
- As protective measure during loading or unloading
- To keep the machine stopped while the operator distances himself
- To establish complete separation from power in electrical devices to allow them to be worked on
- To brake drives under maximum delay, which could cause damage (and accompanying new hazardous situations).

Use of an emergency stop function for these purposes also results in significantly increased accumulation of requirements for which the designer may have not equipped the function for. With this type of connection, it is possible that due to connection of the involved switching elements, the function no longer reaches the performance level and ultimately, failure of this function becomes a risk.

4.3.2 Series switching of emergency stop switches:

An electrical series switch array of several switches which then allows an evaluation at one or more inputs yields a certain savings potential compared to the variant in which each switch individually delivers the evaluation at inputs. What does such a series circuit mean regarding its suitability for an emergency stop performance level?

Faults – especially due to wear – may emerge in such a circuit; their effects must be precisely considered.

ISO/TR24119 addresses just this situation and investigates exactly if and how faults can arise in such applications. This involves safety-critical faults; i.e., those faults that either can lead to failure of the safety function or reduce the performance level of a safety function permanently and undetected. The key property of such circuits lies in, fault detection is first performed at the electrical "end" of the series circuit. Thus, the circuit unit that could detect the fault only "sees" the sum of all faults. And right here lies the problem. ISO/TR24119 points out how individual faults develop in succession and in certain cases can conceal each other, so fault detection is impossible.

This fault masking is especially possible when several switch contacts are actuated (opened) at the same time. In this case, fault masking must be expected; the performance level of the circuit would fall back to PL c because at this performance level, no fault detection is required.

Whether such simultaneous actuation should be assumed must be decided very carefully and in concert with the designer in each individual case. In example circuit 8.2.29 in IFA Report 2/2017, this simultaneous actuation is exempted. No reasoning is presented for this decision. There are no European rulings on this subject.

Attention!

In ISO/TR24119, the attainable performance level when the switches are simultaneously actuated is limited to PL c. Yet the performance level is restricted even for non-simultaneous actuation! This restriction, then, is dependent on the number of switches, how frequently they are actuated and the form of wiring.

4.3.3 Minimum performance level requirement from EN13850: The emergency stop function should reach at least PL c!

Under EN 13850 4.1.5.1, PL c or SIL 1 is the minimum requirement for an emergency stop function. As defined, the emergency stop function is intended to prevent unexpected hazard events and to control situations arising from human behavior. This complicates application of classical risk evaluation methods: How high is a risk that I cannot foresee? For this reason, the minimum requirement per a PL or SIL is applied in EN13850. In a concrete application, higher PLs or SILs can be resorted to at any time; in type C standards too, something else can be defined. Still, according to this definition, it is difficult to go below this minimum requirement. If a machine for which its most dangerous hazard must be secured by PL a or PL b control technology, whether this can also apply to the emergency stop function demands close consideration. In a question to the DIN NA 060-48-02 AA (German mirror committee for ISO 13850), it was determined that requiring the emergency stop to have a higher PL than the remaining machine safety functions was not the intent of the standards makers.

4.3.4 Requirements from the C-standards – on the category too

Requirements for the emergency stop function are imposed by different regulations: Machinery Directive, EN13850, EN60204-1 and in many cases from type C standards for specific machine categories.

Examples:

Alternatively, EN23125 requires PL c and Category 1 per EN 138491-1 or Category 1 or 3 (hard-wired or software-equipped) per EN954 for the emergency stop function for machine tools.

Regardless of the reference to the invalid EN954-1, be advised that requirements for PL and category are presented here.

4.3.5 Regular actuation

In order to detect faults in the emergency stop operating devices or their wiring, usually it is necessary to trigger a state change of the operating device. This safety function requirement which is in most cases met by, e.g, a two-hand circuit, needs particular attention when deployed for an emergency stop function. If all ran as intended, this function would never be actuated. Thus, the function's actuation frequency would be under 1x per year. So it would not be possible to determine a required or the actual attained performance level. This would exceed the EN13849 application scope. To preclude this problem, the emergency stop function must be actuated at regular intervals of less than one year. This would shift responsibility for the required safety function minimum frequency and fault detection to the machine operator. A way for which is not foreseen by EN13849; yet there are no known alternatives

4.3.6 What is reset (turn, pull out or key, etc., unlocking)?

Is reset of an emergency stop command the unlocking (pulling out) the actuator or confirming the emergency stop function on the control panel?

Which of the following actions is safety-relevant:

- Do I confirm the triggered emergency off as acknowledged?

- Or do I confirm the emergency off, which now may no longer be triggered, as acknowledged?

- Or do I confirm that the hazard has been resolved and the machine is now ready to be started?

The third actuation form is definitely relevant to safety. This actuation has the obvious condition than it can only be initiated under full overview of the hazard area. On larger systems, however, this is not possible from the central control panel. So best is, set confirmation at the switch on which the emergency off was triggered. This is precisely what EN13850 requires for a reset: that it not restart the machine, but only enable start-up.

4.3.7   Selective activation/deactivation of emergency off operating devices

One subject that is only approached with extreme caution: Can/should/must the emergency off be deactivated? This is a nuanced topic, since in an actual emergency situation, the operator would only take a short glance at which knob to press, and then actuate the closest knob and expect some immediate reaction. Thus, EN13850 does allow this activation/deactivation on detachable and wireless operating stations, but only under strict limitations. These conditions are:

At least one emergency off device, hard-wired (stationary), must be available on the mm at all times.

Also, at least one of the following measures were deployed to prevent mix-ups between active and inactive emergency off devices:

-Changing device color by illuminating active emergency stop device

-Automatic (self-actuating) coverage of inactive emergency off device. Where this is inexpedient, a manually actuated coverage can be used as long as this function stays fastened to the operating station,

-Measures for proper storage of detachable and wireless operating station.

The machine operating instructions must clearly state the measures used to prevent mix-up between active and inactive emergency off devices. Proper handling of these measures must be explained.

4.3.8   Safety collar

Whether or not a safety collar is allowed on an emergency off is a recurring topic for discussion. EN ISO 13850 states:

The emergency off device must be designed to be easily actuated by operating personnel and any persons who need to use it. This can be a press-button that is easily actuated by the palm of a hand. (Author's note: Once again, here is a translation difficulty: In the standards, the English "push-button" is an reflexive translation for "Drucktaster," even though a switch and not a button is referred to.)

Measures to prevent unintended actuation of an emergency off device must not create risk of hindering actuation or detract from access to the emergency off device. No such measures are permitted to impair visibility of an emergency off device or its actuator

Also consider: The emergency stop device must be designed to prevent unintended actuation.

As far as possible, unintended actuation must prevented by layout rather than constructive measures.

Triggering an emergency off device must not be obstructed. Several options are available as available as preventive measures:

- Locating emergency stop devices distanced from foreseeable heavily occupied areas

- Selection of the emergency stop device type

Aspects of emergency stop

- Selection of appropriate dimensions and form of the emergency stop device, or

- Attachment of the emergency stop device in a recessed surface of the surrounding operating station.

Use of a safety collar is avoided except when necessary to prevent unintended actuation where no other measures are practicable.

A safety collar must not have any sharp corners or edges or rough surfaces that may cause injury. Corners and edges must be deburred and touch surfaces must be smooth.

For hand-actuated emergency stop devices, measures against unintended actuation must not obstruct or hinder actuation by palm of hand from any and all foreseeable positions of the machine operator and others who must be able to actuate it.

In this section of the standard, a veritable procession of safety collars are as far as possible invalidated – only to be accepted shortly thereafter. In particular, the option of a recessed installation of the emergency stop device brings the search for an explicit guideline from the standard to end.

In sum, safety collars should not be used except when no other option is effective.

So far, so good. When might such a safety collar be required?

First to consider is where and in what situations an emergency stop is intended for in the first place. The Machinery Directive only sets general requirements for one or several emergency off control devices for each machine, unless the dangerous machine motions of the machine cannot be brought to a standstill faster by the device function than by an operation stop (handheld machinery also needs no emergency stop). Not much is said over device arrangement and design.

EN13850 is more substantial here, requiring an emergency off at every operating station, on in- and outputs and at loading and unloading stations. Yet all these requirements are subject to the results of a risk assessment.

This type of formulation and convolution in the standard allows the conclusion that perhaps the standards committee could not agree on a clear statement, or that stating a specific solution would not be technically advantageous. What this leaves is just as much freedom as it does aversion: Everything depends on the risk assessment. Whether with or without safety collar, recessed mounting or no emergency stop at all. These decisive questions are left to designers and their risk assessments. Only they can decide which version best suits the specific situation. If the designer concludes that an emergency stop with safety collar better reduces risks than one that is soon manipulated during operation, because it restricts machine uptime, this variant is permitted!

The same deliberations apply to the ultimate form of the safety collar. Current opinions on the market about different forms, and sometimes even test specimens, have no relevance within the context of the European regulations Neither do translations of standards that contradict the published standard texts have any sway on the European level. On the other hand, there is no reason to turn to these detours when a risk assessment is applied as described above.

4.3.9 Working area

The desire to divide the emergency stop function of a larger system and designate separate working areas is common. Due to process technology, sometimes it is more advantageous not to stop an entire system and separate it from power. De-energizing in particular is sometimes problematic and is associated with difficulties when restarting after a hazardous situation is resolved. Of course safety always takes priority during emergency stop, but if one is found, a solution that ensures a safe state in sections of the machine without completely de-energizing the entirety is permitted under certain circumstances.

4.3.10 Recommended fault safeguard (not standard-compliant, but state-of-the-art).

The contact blocks of an emergency off switch are normally mechanically latched with the retaining block. This is a solid connection that will withstand all the environmental conditions described in the relevant standards. Still, in some cases it is recommended to monitor the correct positioning of the contact blocks and mechanical actuator. This is accomplished by fault monitoring, as realized by an additional contact. This contact opens when the contact block is triggered by a purely mechanical part of the switch. Installation errors or loads due to environmental conditions exceeding the standards, especially UV radiation, may cause such malfunctions.

4.4 LoTo (Lockout/Tagout)

The "Lockout/Tagout" method (LoTo) describes the procedure for safely controlling hazardous energies (mechanical, electrical, hydraulic, pneumatic, chemical, thermal, etc.) during necessary employee intervention on a machine.

Depending on how it is implemented, the effectiveness of LoTo depends on organizational measures. According to European legal interpretations, organizational measures are only permitted when hazard due to unsafe construction, intrinsic measures or technical measures can be sufficiently reduced (see also EN ISO 12100:2010 Fig. 1).

4.4.1 Legal framework

By Wtshymanski – Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=38891175

The lockout/tagout method originated in the USA. In that country, technical regulations established by the Occupational Safety and Health Administration (OSHA – US work safety organization) serve as legal foundation. The lockout/tagout method has found increasing use in Germany. European legislation does **not** prescribe any obligation here; but there do exist special legal requirements that would most readily be satisfied by a lockout/tagout program.

Germany: Industrial Safety Regulations 2015 (BetrSichV)

Art. 8 Safety measures for hazards due to energies, start-up and shutdown … (3) Control devices that affect safe use of work equipment must in particular ... be secured against unintended or unauthorized actuation (4) It must only be possible to set work equipment in motion deliberately. Where required, start-up must be safely and reliably prohibited.

Art. 10 Maintenance and modification of work equipment … (3) The employer must meet all required measures to ensure maintenance work can be safely performed. In particular ... 3. The work area must be secured during maintenance work, ... 6. Hazards due to movable or raised work equipment or its parts and hazardous energies or substances are to be avoided, ... 9. Required warning and hazard notices specifically identifying maintenance work must be available at the work equipment,

(4): If technical safety measures required for normal operation are wholly or completely disabled during maintenance work or if such work must be conducted while hazards due to energies still exist, the safety of those involved must be secured by other suitable measures throughout such work.

USA (OSHA – OCCUPATIONAL SAFETY & HEALTH ADMINISTRATION)

OSHA 29 CFR 1910.147 requires employers to implement a program or procedure to control hazardous energy sources (lockout/tagout) on machines and systems. This requirement stipulates attaching suitable blocking devices and identification on hazardous machine energy sources or deactivating machines or devices by other means.

Safety aspects

Fault exclusions

Such measures can prevent unexpected reactivation of energy, accidental machine startup or release of retained energy, thus reducing risk of personal injury.

4.4.2   Lockout / tagout process

The lockout/tagout process is based on:

1. Creation of a process/procedure for energy control (LoTo)
   Generation/documentation of guidelines for switching off hazardous energy sources that define the purpose and scope of the LoTo method

2. Determination of all energy control points
   Listing of all energy control points and their identification; such as valves, switches or plugs, etc., to which permanent tags must be affixed.

3. Provision of the requisite barriers and shutoffs, with their identification
   The lockout/tagout devices defined in the LoTo procedure must be provided. These include valve shutoffs, padlocks, tags, labels, lock boxes, lock stations, etc.

4. Employee training
   Employees must be instructed in the LoTo process so they are familiar with these hazardous energy sources and can use the correct LoTo procedure.

4.4.3   General function of LoTo method:

Wtshymanski [CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons

To isolate and disable an energy source, both a locking device and lockout/tagout materials (warning signage) must be used to lock the energy source and warn others that maintenance work is being performed on the system, before the system is reactivated. Each employee who will work on the machine must apply lockout and/or tagout material to the energy-isolating device. All employees are obligated to gain proficiency with this program and heed the specified process.

4.5   Fault exclusions

If a component is designated with a fault exclusion, it is no longer taken into account in any following safety considerations. The far-reaching consequences, the, necessitate careful documentation and justification. EN ISO 13849-2 contains comprehensive lists about possible fault exclusions and their associated requirements. Both a component manufacturer and the machine engineer may designate fault exclusions. If a fault exclusion is claimed by the component manufacturer, the exclusion must take written form without exception, ideally within the product documntation. This mandate is because of technical and juristic responsibility for the validity of such claims, which otherwise would transfer to the machine engineer. A fundamental restriction must be considered for fault exclusions. If a 1-channel structure is used for a safety function and a fault exclusion has been stated for one of the 1-channel elements, the maximum permissible PL is PL e.

4.6 Fault masking

Fault masking is an effect that can occur when the function of several devices is monitored by the same mechanism (see ISO/TR 24119). In this scenario, functional devices may conceal faults in non-functioning devices. This is mostly facilitated by unsuitable process flows or by restricted diagnosis possibilities of the diagnosis channel.

Safety aspects

Fault masking

When any faults are masked, the system's ability to detect faults is impaired or disabled completely. Typically, the DC must then be set to NONE, even in cases where a DC = HIGH would have been possible otherwise. In turn, attainable categories and PLs are also restricted.

This most often occurs with 2-channel structures, typically with redundant potential-free contacts, that are arranged in series (see 3.19). Here, the diagnosis is usually conducted by a safety control.

Safety aspects

Fault masking

4.6.1 Variants

Emergency stop	Door lock with potential-free contacts	Additional sensors	Additional requirements	Note	Max DC [%]	Max PL	Section
2+	0	0		Actuation from more than one emergency stop must not be expected. Thus, no fault masking is anticipated.	99	e	3.17
1+	1+	0		Actuation of emergency stop while a door or a sensor is actuated is expected. Thus, fault masking is anticipated.	0	c)	3.19
1+	0	1+					
0	2+	0		Dependent on actuation frequency and number of door switches. See also Section 4.6.2 and ISO/TR 24119	0 thru 90	c or d	3.20
0	1+	1+	As conditioned by the process, more than the sensor or door cannot be actuated at any given time.	Fault masking is prevented by the process.	90	d	

Otherwise			If the following requirements are fulfilled:
			
			• An additional diagnosis (e.g., a third contact and suitable) ensures only one sensor/door is actuated at a time
			• Actuation of more than one sensor/door lock/emergency-stop)
			  • Evaluated as fault
			  • Then, the function of each sensor must be checked before the process is continued.
				Whenever a diagnosis is conducted by a non-safety SPS, it is part of the SPS section of the safety function. Thus is a validation of this diagnosis part of the safety function validation process. Further, any changes to the standard SPS software must be checked for their effect on diagnoses and new safety validation is required.	99	e	

Otherwise				Fault masking must be assumed.	0	c	

Table 1: Combination of sensors and resulting DC

4.6.2 Wiring doors in series – ISO/TR 24119

ISO/TR 24119 restricts DCdepending on:
- Number of doors
- Signal type
- Actuation frequency
- Wiring principle
- Arranging switches
- Process

The following table shows a simplified approach and attainable DC level. In each case, the standard restricts attainable performance level to PL d, even when the DC would indicate a higher PL:

Number of frequently actuated doors: [1, 2]		Number of additional doors: [3]	Maximum attainable DC [4]
0	+	2 to 4	Medium
		5 to 30	Low
		≥ 31	None
1	+	1	Medium
		2 to 4	Low
		≥ 5	None
≥ 2	+	≥ 1	None

1   *When the frequency is higher than 1x per hour*
2   *When more than one operator is able to independently open doors, the number of frequently actuated doors must be increased by one.*
3   *The number of additional doors can be decreased by one if:*
- *The minimum distance between two doors is 5 m or*
- *When no other door can be directly reached*
4   *In any case, if potential fault masking is foreseen (e.g., doors opened simultaneously), the DC must be set to NONE.*

Table 2: Simplified DC table from ISO/TR 24119

4.6.3   Direct fault masking

Abbildung 5 Indicates fault masking process for a typical case of faults in switch –B1 that are not detected by –K1 because they are concealed by a functioning switch –B2.

1. Step **All doors closed**		2. Step **Door 2 is opened**	
3. Step **Door 1 is opened** Fault in B1.2 – contact does not open		4. Step **Door 1 is closed** Fault in B1.2 remains concealed	
5. Step **Door 2 is closed and machine is restarted** Fault in B1.2 remains concealed		6. Step **Door 1 is opened** • Undetected fault in B1.2 • + New 2nd fault in B1.1 → **Hazardous situation.**	
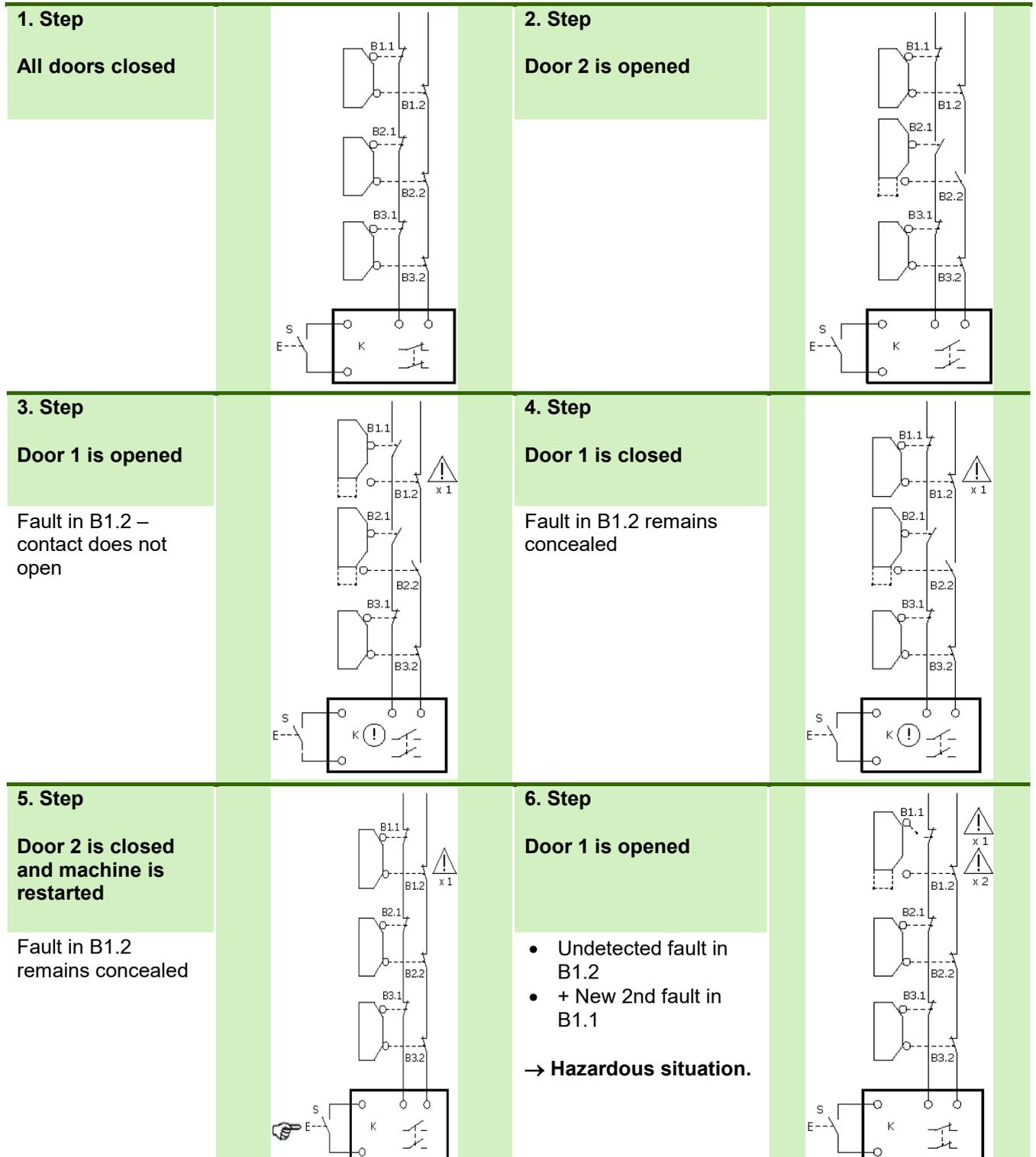
Illustration 5: Direct fault masking per ISO/TR 24119

4.7 Non-secured electronics and software

Standard electronic components; i.e., programmable or embedded electronics

- without safety technological evaluation by the manufacturer and
- consequently, with no key values for safety-relevant functions

are viewed critically in EN ISO 13849-1 and their use is prohibited in most cases. The only exceptions are for when diverse elements in two channels are used. According to EN ISO 13849-1 Sect. 4.6.2 , the requirements for specification, design, coding and testing of the safety-relevant embedded software (firmware) fulfill up to PL e virtually automatically. Thus, electronic components can be used on a microcontroller basis in safety-relevant applications even though they were not originally intended for such purposes. However, there are additional requirements on the user-programmed software and parameterization. Irrespective of these requirements, safety-technological hardware evaluations (category, $MTTF_D$, DC, CCF) must be conducted in every case.

4.8 Human/robot "Cooperation/Collaboration/Coexistence" (HRC)

4.8.1 Definitions of terms

Cobot: Conjunction of the words "Collaboration" and "Robot"; describes robots designed for direct interaction with humans.

HRC: Human-Robot Collaboration (HRC) refers to a situation wherein humans and robots share a work area without any separating safety equipment.

4.8.2 Human-robot working scenarios

Modern manufacturing processes in today's production systems use different, flexible interaction forms to meet the current application. Collaboration between humans and robots takes different forms, depending on the degree of automation. However, the application itself determines how closely human and cobot can work together without safety barriers. Thus, the "C" in HRC can have different meanings: *Coexistence, Cooperation, Collaboration*

Coexistence		• Humans work near robot work area • No overlap between work areas • **No** physical contact exists • Robot work area secured by locked, separating protective equipment
Cooperation		• Humans and robots work in same work area, but at separate times. • **No** physical contact exists • Work areas secured by non-separating protective equipment
Collaboration		• Humans and robots work closely together (same work area) • Physical contact **is possible and sometimes necessary** • Work areas secured by robot-specific safety functions
Image source: www.baua.de/Mensch-Roboter-Interaktion		
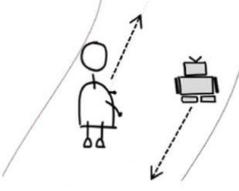
Safety aspects

Human/robot "Cooperation/Collaboration/Coexistence" (HRC)

When designing HRC applications, appropriate robot safety principles must be selected and deployed to ensure a safe work environment for all personnel. EN ISO 10218-1 describes safety measures for robots that can be applied on collaborative operation.

4.8.3 Safety principles for HRC operation

1. Safety-evaluation monitored stop When the common work area is entered, all robot drives are immediately stopped (STO or SOS). If no persons are in the collaboration area, the robots work autonomously.
2. Manual control The robots can be manually operated by the operator via a manual control device (with acknowledgment device) at safely reduced speed. As soon as the acknowledgment device is released, the robot stops.
3. Speed and distance monitoring Proximity of personnel is reliably detected and robot movements are slowed or stopped. (safe distances between operator and robot maintained dynamically)
4. Power and force limitation
   Hazards caused by robots are controlled/regulated by limiting energy or force. Certain load characteristics must not be exceeded during contact between human and robots/tools. These parameters for power, force, and ergonomics need to be determined by a risk assessment. Additional information and instructions (body regions, biometric limit values, etc.) for operating collaborative robots is provided by ISO/TS 15066 (Robots and robotic devices – Collaborative robots).

Regardless of the specific human-robot interaction (coexistence, cooperation, collaboration), the system manufacturer must provide safety measures that ensure operating personnel are protected at all times. This requires the C-standards for robotic systems and integration (EN ISO 10128-2) or Machinery Directive 2006/42/EC.

The **entire** HRC application/system must be .considered here. This includes not only the robots, but also the end effectors employed (grippers, cameras, etc.) as well as workpieces, apparatus, protective equipment and so on.

Applications like coexistence and cooperation have already been established in robotics for some time. They are usually secured by detection solutions such as light barriers or safety mats. These devices are often supplemented by corresponding safety functions in the robot controls, which prevent a robot from moving into the forbidden zone. Because in coexistence or cooperation scenarios, humans and robots largely operate separately, conventional industrial robots can be used here

When contact is not, cannot or should not be completely avoided, at very least an attempt should be made to limit the forces and pressures (see 5.8) which may be exerted on humans by robots. Force/torque sensors located in the joints of the cobot that stop the collaborative robot if force and pressure limits are exceeded are one readily available means to do so. Special protective covers that use sensors to react to pressure and contact could also be used.

Tables & formulas

5 Tables & formulas

5.1 Symbols

Symbol	Unit	Meaning
β	%	Likelihood of faults compared to actual faults with same cause
B_{10}	-	Number of switching cycles until 10% of components fail
B_{10D}	-	Number of switching cycles until 10% of components fail and present hazard
C	1/h	Operating cycles per hour (see also n_{op})
CCF	-	Common cause faults 0 to 100 point range
DC	%	Diagnostic degree of coverage
DC_{avg}	%	Average diagnostic degree of coverage (of a subsystem)
d_{op}	d/a	Annual operating days
FIT	1/h	Faults in 10^{-9} hours
HFT	-	Hardware fault tolerance
h_{op}	h/d	Operating hours per operating day
λ	1/h	Rate of all faults per hour (= 1/MTTF in hours)
λ_D	1/h	Rate of hazardous faults per hour (= $1/MTTF_D$ in hours)
λ_{DD}	1/h	Rate of detected hazardous faults per hour
λ_{DU}	1/h	Rate of undetected hazardous faults per hour
λ_S	1/h	Rate of non-hazardous faults per hour
MTBF	a	Average time between two faults in years
MTTF	a	Average time until fault in years *(per Weibull, 62.3% of all devices than fail. See EN/IEC 61810-2)*
$MTTF_D$	a	Average time until hazardous fault in years *(per Weibull, 62.3% of all devices than fail. See EN/IEC 61810-2)*
n_{op}	1/a	Annual switching cycles
PFH	1/h	Probability of a hazardous fault per hour (EN/IEC 61508)
PFH_D	1/h	Probability of a hazardous fault per hour (EN/IEC 62061 and EN ISO 13849-1)
PL	-	Performance level

Tables & formulas

Symbols

Symbol	Unit	Meaning
PL_r	-	Required performance level
P_{TE}	1/h	Probability of a transmission fault in communication (EN/IEC 62061)
RDF	%	Portion of hazardous faults (VDMA 66413)
SFF	%	Portion of safe faults (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 a subsystem (EN/IEC 61508 and EN/IEC 62061)
SRCF		Safety-related control function *(corresponds to safety functions in EN/IEC 62061)*
SRP/CS		Safety-related part of a control system *(corresponds to safety functions in EN ISO 13849-1)*
T_1	h or a	Test intervals. Pay attention to units! *(T_1 corresponds to a "like new" test interval; because it is not feasible in most cases, it can be replaced with T_M)*
T_2	h	Diagnostic test interval *(this is a mainly automatic and frequently recurring test)*
T_{10D}	a	Service life in years *(after this time, the number of permissible switching cycles for components with mechanical locking expires)*
T_M	a	Operating life in years *(see also T_1)*
t_{Cycle}	s	Time between two actuations in seconds

5.2 Performance level determination

5.2.1 Formulas

The validity/applicability of formulas is often limited by the totality of elements, subsystems or safety functions. Applications outside the intended application scope can yield invalid results.

Formula	Comment	Item	Subsystem	Safety function
$B_{10D} = B_{10}$	Worst-case estimate	X		
$B_{10D} = B_{10} 2 *$	For electronics	X		
$n_{op} = \dfrac{d_{op} \cdot h_{op}}{t_{zyklus}} \cdot 3600 \dfrac{s}{h}$	Actuation frequency	X		
$MTTF_D = \dfrac{B_{10D}}{0,1 \cdot n_{op}}$		X		
$T_{10D} = \dfrac{B_{10D}}{n_{op}}$	If $T_{10D} <$ 20 years, It must be noted 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	
$MTTF = \dfrac{1}{\lambda} \cong MTBF$	When repair time is irrelevant (a few days)	X		
$DC = \dfrac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}}$		X	X	
$MTTF_{D,Ci} = \dfrac{1}{\sum_{i=1}^{n} \dfrac{1}{MTTF_{D,i}}}$	Per channel		X	
$MTTF_{D,ges} = \dfrac{2}{3}\left[MTTF_{D,C1} + MTTF_{D,C2} - \dfrac{1}{\dfrac{1}{MTTF_{D,C1}} + \dfrac{1}{MTTF_{D,C2}}} \right]$	Limit values to 100 (Cat. B to Cat. 3) or 2500 (Cat. 4) before symmetrizing.		X	

Tables & formulas

Performance level determination

Formula	Comment	Item	Subsystem	Safety function
$DC_{avg} = \dfrac{\frac{DC_1}{MTTF_{D,1}} + \frac{DC_2}{MTTF_{D,2}} + \cdots + \frac{DC_n}{MTTF_{D,n}}}{\frac{1}{MTTF_{D,1}} + \frac{1}{MTTF_{D,2}} + \cdots + \frac{1}{MTTF_{D,n}}}$	Valid for one and two channels. No limitation of $MTTF_D$ required		X	
$PFH_D = \displaystyle\sum_i PFH_{D,i}$				X
$PL_{ges} \leq \min_i PL_i$	Requirements for safety functions			X
$PL_r \leq PL_{ges}$	Requirements for safety functions			X

5.2.2 Requirements for categories

Feature	Category				
	B	1	2	3	4
Design must withstand influences expected per applicable standards	X	X	X	X	X
Basic safety principles	X	X	X	X	X
Validated safety principles		X	X	X	X
Validated 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 safety				X	X
Consideration of fault accumulation					X
Degree of diagnosis coverage – DC$_{avg}$	None		Low to medium		High
Measures against CCF			X	X	X
Mainly characterized by	Component selection	Structure			

Tables & formulas

Performance level determination

5.2.3 Minimum requirement for PFH$_D$ (EN ISO 13849-1 Table 3)

PL$_{ges}$	PFH$_D$
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	$PFH_D < 10^{-7}$

5.2.4 DC areas (EN ISO 13849-1 Table 5)

Name	Area
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

5.2.5 Bar chart (EN ISO 13849-1 Figure 5)
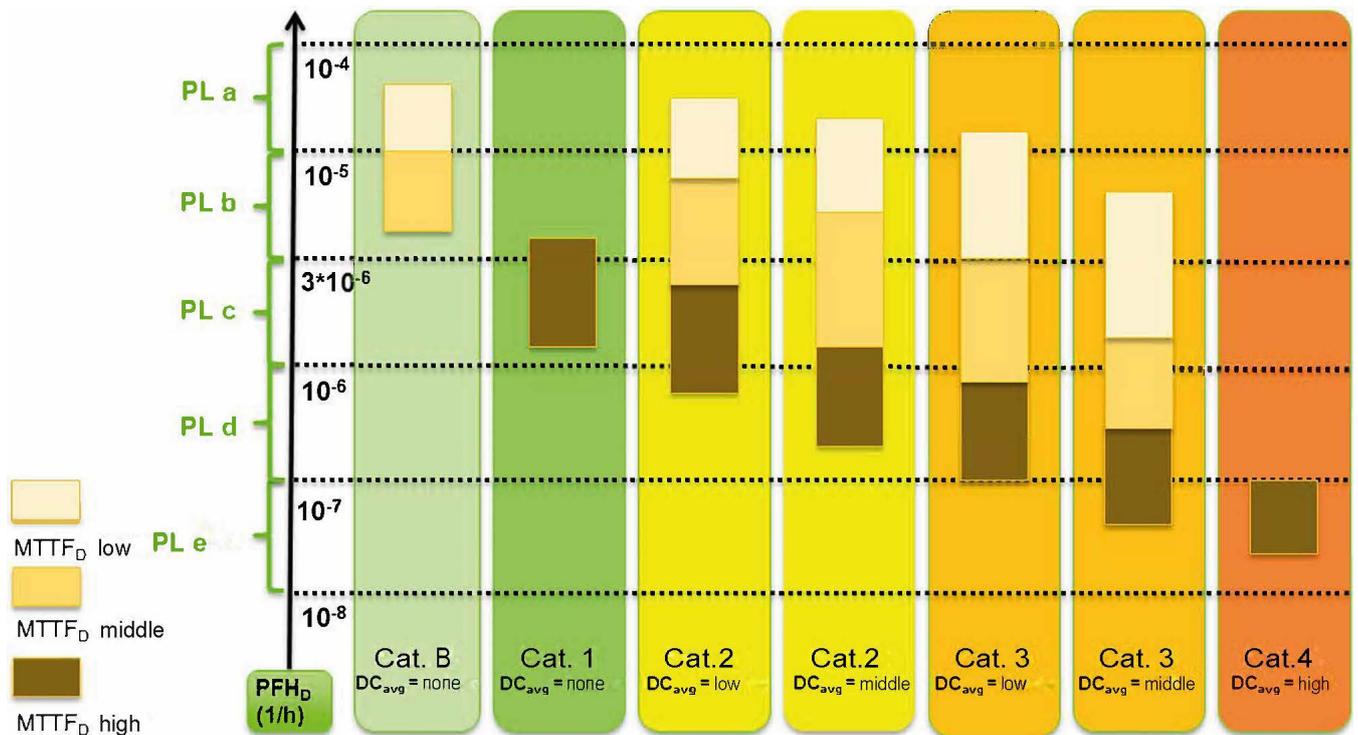
For a detailed table of the relations, see EN ISO 13849-1 Appendix K

Performance level determination

5.2.6   EN ISO 13849-1 Appendix K

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

Tables & formulas

Performance level determination

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

Column group header: **PFH$_D$ (1/h) and corresponding performance level (PL)**

Tables & formulas

Performance level determination

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

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

Measures against CCF		Points
Separation	1. Physical separation between signal paths; e.g.: • Separation between wiring / wire conduits • Short circuit detection and cable interruptions by dynamic test • Separate signal path shielding per channel • Adequate clearance and creepage distances on printed circuits.	**15**
Diversity	2. Different technologies and designs or physical principles are used; e.g.: • The first channel in the programmable electronics and the second channel are hard-wired • Type of initiation • Pressure and temperature • Distance and pressure measurements • Digital and analog • Components from different manufacturers	**20**
Application design experience	3.1 Protection against overvoltage, overpressure, overcurrent etc.	**15**
	3.2 Use of validated components	**5**
Evaluation analysis	4. Are the results of a failure type and effect analysis taken into account during development to prevent failures resulting from common causes?	**5**
Educating competence	5. Are designers/assemblers sufficiently educated to recognize the causes and effects resulting from common cause faults?	**5**
Environment	6.1 Prevention of contamination and electromagnetic influence (EMC) in accord with the appropriate standards. Fluid systems: Filtering pressure mediums, prevention of contamination incursion, dewatering compressed air: e.g., in compliance with manufacturer requirements for pressure medium purity. Electrical systems: Was the electromagnetic immunity of the system specifically checked, e.g., for CCF as specified in the applicable standards? Both aspects should be considered for combined fluid and electrical systems.	**25**
	6.2 Other influences Were all requirements for immunity against all relevant environmental conditions like temperature, shock, vibration, humidity, etc. (e.g., as described in the applicable standards) taken into account?	**10**
Total CCF	**Total points ($65 \leq CCF \leq 100$) required for Cat. 2 to Cat. 4. No partial points are permitted.**	

5.3 DC measures

5.3.1 Entry (EN ISO 13849-1 Table E.1)

Measure – Entry	DC min	DC max	Comment
Cyclical testing/dynamization	90%	90%	Periodic generation of a signal change with monitoring of the results
Plausibility check; e.g., use of closer/opener contacts of direct-opened relays	99%	99%	
Cross comparison • Without dynamization	0%	99%	Manual test initiation
Cross comparison • With dynamization • Without high quality fault detection	90%	90%	Comparison of inputs or outputs without short circuit detection (for multiple in-/outputs)
Cross comparison • With dynamization • With high quality fault detection	99%	99%	• Capturing valve actuator position • Cross comparison of signal and intermediate values with short circuit detection (for multiple in-/outputs) • Recognition of static faults (e.g., by using safety components) and temporal and logical program monitoring • Position or speed information gained separately from cross comparison
Independent monitoring (e.g., monitoring via pressure switch, electrical drive element position monitoring, etc.)	90%	99%	• Position encoder or end switch on actuators instead of control elements • Valve monitoring via pressure switch
Direct monitoring (e.g., electrical control valve position monitoring; monitoring electromechanical units through forced guidance)	99%	99%	• Position monitoring directly on control element • Position monitoring directly on valve actuator • Position monitoring via forced feedback contacts (antivalent opener contacts) • Signal monitoring via feedback; e.g., via optocouplers
Fault detection by the process (e.g., FMEA; insufficient for PL e)	0%	99%	Process control failure made evident by: • Faulty function • Damage to workpiece or machine parts • Process interruption or delay without presenting immediate hazards.
Monitoring properties	60%	60%	• Monitoring response times, analog signal strength (e.g., resistance, capacity)

Tables & formulas

DC measures

5.3.2   Logic (EN ISO 13849-1 Table E.1)

Measure – logic	DC min	DC max	Comment
Independent monitoring (e.g., monitoring via pressure switch, electrical drive element position monitoring, etc.)	90%	99%	• Position encoder or end switch on actuators instead of control elements
Direct monitoring (e.g., electrical control valve position monitoring; monitoring electromechanical units through forced guidance)	99%	99%	• Signal monitoring via feedback; e.g., via optocouplers
Fault detection by the process	0%	99%	• Process control failure made evident by: Faulty function • Damage to workpiece or machine parts • Process interruption or delaywithout presenting immediate hazards.
Simple temporal program runtime monitoring (e.g., time element as watchdog, with trigger signals in logic program)	60%	60%	• Time element as watchdog, with trigger signals in logic program
Temporal and logical program runtime monitoring by the watchdog, whereby the test setup conducts plausibility tests of the actions by the logic	90%	90%	• Through a watchdog, whereby the test setup conducts plausibility tests of the actions by the logic
Self test at start-up to find concealed faults in sections of the logic (e.g., program and data memory, in- and output terminals, interfaces)	90%	90%	• Detection of concealed faults in program and data memory, • in- and output terminals, interfaces
Test of the monitoring device (e.g., watchdog) reaction possibilities through the main channel after start-up, or whenever the safety function is requested, or whenever an external signal requests the function through an input device	90%	90%	• Test of the watchdog reaction possibilities
Dynamic principles (all logic components require a state change ON-OFF-ON when the safety function is requested) e.g, locking circuits in relay technology	99%	99%	
Invariant memory: Basic signature word width (8-bit)	90%	90%	
Invariant memory: Doubled signature word width (16-bit)	99%	99%	

Page **145** from **179**

Tables & formulas

DC measures

5.3.2   Logic (EN ISO 13849-1 Table E.1)

Measure – logic	DC min	DC max	Comment
Independent monitoring (e.g., monitoring via pressure switch, electrical drive element position monitoring, etc.)	90%	99%	• Position encoder or end switch on actuators instead of control elements
Direct monitoring (e.g., electrical control valve position monitoring; monitoring electromechanical units through forced guidance)	99%	99%	• Signal monitoring via feedback; e.g., via optocouplers
Fault detection by the process	0%	99%	• Process control failure made evident by: Faulty function • Damage to workpiece or machine parts • Process interruption or delaywithout presenting immediate hazards.
Simple temporal program runtime monitoring (e.g., time element as watchdog, with trigger signals in logic program)	60%	60%	• Time element as watchdog, with trigger signals in logic program
Temporal and logical program runtime monitoring by the watchdog, whereby the test setup conducts plausibility tests of the actions by the logic	90%	90%	• Through a watchdog, whereby the test setup conducts plausibility tests of the actions by the logic
Self test at start-up to find concealed faults in sections of the logic (e.g., program and data memory, in- and output terminals, interfaces)	90%	90%	• Detection of concealed faults in program and data memory, • in- and output terminals, interfaces
Test of the monitoring device (e.g., watchdog) reaction possibilities through the main channel after start-up, or whenever the safety function is requested, or whenever an external signal requests the function through an input device	90%	90%	• Test of the watchdog reaction possibilities
Dynamic principles (all logic components require a state change ON-OFF-ON when the safety function is requested) e.g, locking circuits in relay technology	99%	99%	
Invariant memory: Basic signature word width (8-bit)	90%	90%	
Invariant memory: Doubled signature word width (16-bit)	99%	99%	

Tables & formulas

DC measures

Measure – logic	DC min	DC max	Comment
Variant memory: RAM test using redundant data: e.g., flags, markers, constants, timer and cross comparison of this data	60%	60%	
Variant memory: Legibility and writability of 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 by process (DC depends on application; this measure alone does not suffice for PL e!)	0%	99%	

Tables & formulas
DC measures

5.3.3 Output (EN ISO 13849-1 Table E.1)

Measure – output	DC min	DC max	Comment
Monitoring outputs through one channel without dynamic tests	0%	99%	Depending on how often the application initiates a signal change
Cross comparison • Without dynamization	0%	99%	Manual test initiation
Cross comparison • With dynamization • Without high quality fault detection	90%	90%	Comparison of inputs or outputs without short circuit detection (for multiple in-/outputs)
Cross comparison • With dynamization • With high quality fault detection	99%	99%	• Capturing valve actuator position • Cross comparison of signal and intermediate values with short circuit detection (for multiple in-/outputs); detection of static faults (e.g., by using safety components) and temporal and logical program monitoring
Independent monitoring (e.g., monitoring via pressure switch, electrical drive element position monitoring, etc.)	90%	99%	• Position encoder or end switch on actuators instead of control elements • Valve monitoring via pressure switch
Direct monitoring (e.g., electrical control valve position monitoring; monitoring electromechanical units through forced guidance)	99%	99%	• Position monitoring directly on control element • Position monitoring directly on valve actuator • Position monitoring via forced feedback contacts (antivalent opener contacts) • Signal monitoring via feedback; e.g., via optocouplers
Fault detection by the process (e.g., FMEA; insufficient for PL e)	0%	99%	Process control failure made evident by faulty function, damage to workpiece or machine parts, process interruption or delay without presenting immediate hazards.
Redundant circuit path • With actuator monitoring via logic and test setup	99%	99%	

Tables & formulas

5.4 Safety principles

5.4.1 Basics – Mechanical (EN ISO 13849-2 Table F.1)

Basic mechanical safety principles	Remarks
Use of suitable materials and appropriate manufacturing processes	Selection of materials and manufacturing/treatment processes covering, e.g, voltages, durability, elasticity, friction, wear, corrosion, temperature
Proper dimensioning and design	Consideration of, e.g, tension, expansion, fatigue, surface roughness, deviation limits, snagging, production processes
Suitable selection, combination, arrangement, assembly of components/systems	Consideration of manufacturer application instructions, e.g, catalog pages, installation instructions, specifications as well as of proven technical experience with similar components/systems.
Energy isolation principle	Safe state is reached after energy is deactivated. See significant aspects of shutdown process in ISO 12100:2010, 6.2.11.3. Energy is supplied to initiate a mechanical movement. See significant aspects of start-up process in ISO 12100:2010, 6.2.11.3. Consideration of different operation modes; e.g., operating mode, maintenance mode. IMPORTANT – This principle must not be used when loss of energy gives rise to a hazard; e.g., release of a tool due to loss of clamping force.
Suitable fastening	When using screw retention, follow manufacturer use instructions. Overloads can be prevented and an appropriate resistance against connections loosening can be achieved by using a suitable torque limitation procedure.
Limiting force generation and/or transfer and similar parameters	Examples include shear pins, shear plates and torque limitation couplings, etc. IMPORTANT – This principle must not be applied where component integrity is essential to maintain the required control level
Limiting range of environmental parameters	Examples of these parameters include temperature, humidity contamination, etc., at installation site. See Section 10; observe manufacturer use instructions.
Suitable reaction time	Focus on reduction of spring force, friction, lubrication, temperature inertia under acceleration and deceleration as well as combinations of tolerance limits

Tables & formulas

Safety principles

Basic mechanical safety principles	Remarks
Protection against unexpected start-up	Consideration of unexpected start-up caused by retained energy and after energy supply is restored, for different operation modes like operating mode, maintenance mode, etc. Additional equipment for discharging retained energy may be necessary. Particular applications, e.g., to maintain energy for clamping devices or to secure a position, require especial attention
Simplification	Avoidance of unnecessary components in safety-related systems
Separation	Separation of safety-related functions from other functions
Suitable lubrication	Observation of required lubrication equipment, specifications and intervals
Suitable protection against penetration of liquid and dust	Observation of IP protection type (see EN/IEC 60529)

Tables & formulas

5.4.2   Validated – Mechanical (EN ISO 13849-2 Table A.2)

Validated mechanical safety principles	Remarks
Application of judiciously selected materials and manufacturing processes	Selection of materials and of manufacturing and handling processes appropriate for the respective application
Use of components with specified failure behavior	The predominant behavior of a failed component is known in advance and is always the same. See ISO 12100:2010, 6.2.12.3
Overdimensioning / safety factor	Safety factors specified in the standards or drawn from experience with safety-related applications are to be applied.
Secured position	The movable element of a component is mechanically secured in a safe position (friction alone is insufficient). Force must be applied to move the element from its secured position.
Increased OFF force	A safe position or state is achieved by raising the OFF force compared to the ON force.
Careful selection, combination, arrangement, assembly and installation of components/systems for the respective application	—
Careful selection of mounting method for the respective application	Avoidance of mounting/fastening by friction alone
Direct-opened mechanical switches	To achieve mechanically direct action, all moving mechanical elements required to execute a safety function must force connected components to move in concert; e.g., a cam that directly opens the contacts of an electrical switch instead of a connection using a spring (see ISO 12100:2010, 6.2.5).
Parts redundancy	Confining effect of failures by using several identical parts working in parallel, e.g., a fault impairing one of several springs will not cause a hazard.
Reduced reaction time and hysteresis range	Determination of necessary limits. Focus on reduction of spring force, friction, lubrication, temperature, inertia under acceleration and deceleration as well as combinations of tolerance limits

Tables & formulas

Safety principles

Validated mechanical safety principles	Remarks
Use of validated springs (See also Table A.3)	A validated spring requires: • Use of carefully selected materials, manufacturing processes (e.g., static and dynamic setting before application) and handling processes (e.g., milling, shot peening); • adequate spring guidance and support and • sufficient safety factor to cover sustained loads (i.e., to minimize likelihood of breaks). • Validated compression springs can also be employed. • Use of carefully selected materials, manufacturing processes (e.g., static and dynamic setting before application) and handling processes (e.g., milling, shot peening); • adequate spring guidance and support and • spacing smaller than spring wire diameter between coils of unloaded springs and • adequate strength is maintained after one or more breaks (i.e., breaks do not cause hazardous situations). *NOTE: Pressure springs are preferred.*
Reduced range of force and other parameters	Determination of essential limits based on experience and the respective application. Examples include shear pins, shear plates and torque limitation couplings, etc. **IMPORTANT – This principle must not be applied where component integrity is essential to maintain the required control level.**
Reduced range of speed and other parameters	Determination of essential limits based on experience and the respective application. Examples include centrifugal governors, secure speed monitoring and travel limitation.
Reduced travel limitation range	Determination of necessary limits. Examples include temperature, humidity, contamination during installation, etc. See Section 10; observe manufacturer use instructions.

Tables & formulas

Safety principles

5.4.3 Basics – Pneumatics (EN ISO 13849-2 Table B.1)

Basic pneumatic safety principles	Remarks
Use of suitable materials and manufacturing processes	Selection of materials and manufacturing/handling processes taking into account, e.g., tensions, durability, elasticity, friction, wear, corrosion, temperature
Correct dimensioning and design	Consideration, e.g., of tension, stretching, fatigue, surface roughness, tolerance limits and manufacturing processes
Suitable selection, combination, arrangement, assembly and installation of components/systems	Consideration of manufacturer's use instructions; e.g., catalog pages, installation instructions, specifications as well as of proven technical experience with similar components/systems.
Energy isolation principle	Safe state is reached after energy is deactivated on all relevant equipment. See significant aspects of shutdown process in ISO 12100:2010, 6.2.11.3.
	Energy is supplied to initiate a mechanical movement See significant aspects of start-up process in ISO 12100:2010, 6.2.11.3.
	Consideration of different operation modes; e.g., operating mode, maintenance mode.
	This principle must never be used where loss of pneumatic pressure would lead to additional hazard.
Suitable fastening	When using, e.g., screw retention, armatures, adhesives, or clamping rings, follow manufacturer use instructions.
	Overloads can be prevented by using a suitable torque limitation procedure.
Pressure limitation	Examples include pressure limitation valves and pressure-reduction or pressure-regulating valves
Speed limitation/restriction	One example is the use of a flow valve or choke valve to limit piston speed.
Sufficient measures to prevent contamination of fluids	Consideration of filtration and separation of solids and water from operating fluids
Appropriate switching time range	Consideration of, e.g., length of hoses/piping, pressure, discharge capacity, force, spring force restriction, friction, lubrication, temperature, inertia under acceleration and deceleration as well as the interplay of tolerance limits.
Resistance to environmental conditions	Design of system for work in all anticipated environments and under all foreseeable unfavorable conditions; e.g., temperature, humidity, vibration, contamination. See Section 10; observe manufacturer use instructions and specifications.

Tables & formulas

Safety principles

Basic pneumatic safety principles	Remarks
Protection against unexpected start-up	Consideration of unexpected start-up caused by retained energy and after energy supply is restored, for different operation modes like operating mode, maintenance mode, etc. Additional equipment for discharging retained energy may be necessary (see ISO 14118, 5.3.1.3). Particular applications (e.g., to maintain energy for clamping devices or to secure a position) require especial attention.
Simplification	Avoidance of unnecessary components in safety-related systems
Suitable temperature range	This must be considered throughout the system.
Separation	Separation of safety-related functions from other functions (e.g, logical separation)

5.4.4   Validated – Pneumatics (EN ISO 13849-2 Table B.2)

Validated pneumatic safety principles	Remarks
Overdimensioning / safety factor	The safety factors are specified in the standards or draw on experience with safety-related applications.
Secured position	The movable element of a component is mechanically secured in one of the possible positions (friction alone is insufficient). Force must be applied to move the element from its position.
Increased OFF force	One solution is to have the area ratio for moving a valve slide to safe position (OFF position) is significantly greater than the area ratio for its movement to the ON position (a safety factor).
By the load pressure of a closing valve	Generally, this means seat valves; e.g., ball seat valves or ball valves. Factor in how sufficient load pressure is to be applied to keep the valve closed even if, e.g., the valve closing spring breaks.
Mechanically forced components	Mechanically forced action is used for the movable parts within a pneumatic components. See also Table A.2.
Parts redundancy	See Table A.2.
Use of validated springs	See Table A.2.
Speed limitation/restriction through a resistance to reaching a set volume flow.	Examples are fixed orifices and fixed throttles.
Force limitation/restriction	This can be achieved through a validated pressure limitation valve that is, e.g., equipped with a validated spring and was correctly dimensioned and selected.
Suitable operating condition range	Limitation of operating conditions; e.g., pressure, volume flow and temperature ranges should be taken into account.
Suitable contamination prevention for operating fluids	Consideration of necessity for highly effective filtration and separation of solids and water from operating fluids.
Adequately dimensioned positive overlap in gate valves	The positive overlap ensures the stop function and prevents impermissible movements.
Hysteresis limitation	Hysteresis is increased by, e.g., greater friction and through the interplay of tolerance limits.

Tables & formulas

Safety principles

5.4.5   Basics – Hydraulics (EN ISO 13849-2 Table C.1)

Basic hydraulic safety principles	Remarks
Use of suitable materials and manufacturing processes	Selection of materials and manufacturing/handling processes taking into account, e.g., tensions, durability, elasticity, friction, wear, corrosion, temperature, hydraulic fluid.
Correct dimensioning and design	Consideration, e.g., of tension, stretching, fatigue, surface roughness, tolerance limits and manufacturing processes.
Suitable selection, combination, arrangement, assembly and installation of components/systems	Application of manufacturer's use instructions; e.g., catalog pages, installation instructions, specifications as well as of proven technical experience with similar components/systems.
Energy isolation principle	• Safe state is reached after energy is deactivated on all relevant equipment. See significant aspects of shutdown process in ISO 12100:2010, 6.2.11.3. • Energy is supplied to initiate a mechanical movement See significant aspects of start-up process in ISO 12100:2010, 6.2.11.3. • Consideration of different operation modes; e.g., operating mode, maintenance mode. • This principle must never be used in applications where loss of pneumatic pressure would lead to additional hazard.
Suitable fastening	When using, e.g., screw retention, armatures, adhesives, or clamping rings, follow manufacturer use instructions. Overloads can be prevented by using a suitable torque limitation procedure.
Pressure limitation	Examples include pressure limitation valves and pressure-reduction or pressure-regulating valves.
Speed limitation/restriction	One example is the use of a flow valve or choke valve to limit piston speed.
Sufficient measures to prevent contamination of fluids	Consideration of filtration/separation of solids/water from operating fluids. A display/indication notifying of necessity for filter change is also to be taken into account.
Appropriate switching time range	Consideration of, e.g., length of hoses/piping, pressure, discharge capacity, spring force restriction, friction, lubrication, temperature/viscosity, inertia under acceleration and deceleration as well as the interplay of tolerance limits.

5.4.6 Validated – Hydraulics (EN ISO 13849-2 Table C.2)

Validated hydraulic safety principles	Remarks
Overdimensioning / safety factor	The safety factors are specified in the standards or draw on experience with safety-related applications.
Secured position	The movable element of a component is mechanically secured in one of the possible positions (friction alone is insufficient). Force must be applied to move the element from its position.
Increased OFF force	One solution is to have the area ratio for moving a valve slide to safe position (OFF position) is significantly greater than the area ratio for its movement to the ON position (a safety factor).
By the load pressure of a closing valve	Example are seat valves and cartridge valves. Factor in how sufficient load pressure is to be applied to keep the valve closed even if, e.g., the valve closing spring breaks.
Mechanically forced components	Mechanically forced action is used for the movable parts within a hydraulic components. See also Table A.2.
Parts redundancy	See Table A.2.
Use of validated springs	See Table A.2.
Speed limitation/restriction through a resistance against a set volume flow	Examples are fixed orifices and fixed throttles.
Force limitation/restriction	This can be achieved through a validated pressure limitation valve that is, e.g., equipped with a validated spring and was correctly dimensioned and selected.
Suitable operating condition range	Limitation of operating conditions; e.g., pressure, volume flow and temperature ranges should be taken into account.
Monitoring fluid status	Consideration of a highly effective filtration/separation of solids/water from operating fluids. The chemical/physical state of the fluids must also be considered. Consideration of a display/indication notifying of necessity for filter change.
Adequately dimensioned positive overlap in piston slide valves	The positive overlap ensures the stop function and prevents impermissible movements.
Hysteresis limitation	Hysteresis is increased by, e.g., greater friction. The interplay of tolerance limits also influences hysteresis.

5.4.7 Basics – Electrical (EN ISO 13849-2 Table D.1)

Basic electrical safety principles	Remarks
Use of suitable materials and manufacturing processes	Selection of materials and manufacturing/handling processes taking into account, e.g., tensions, durability, elasticity, friction, wear, corrosion, temperature, hydraulic fluid.
Correct dimensioning and design	Consideration, e.g., of tension, stretching, fatigue, surface roughness, tolerance limits and manufacturing processes.
Suitable selection, combination, arrangement, assembly and installation of components/systems	Consideration of manufacturer's use instructions; e.g., catalog pages, installation instructions, specifications as well as application of proven technical experience.
Correct protective ground connection	A side of the control current circuit, a terminal of each electromagnetically actuated device or a terminal of other electrical devices is connected to a protective ground (see IEC 60204-1:2005, 9.4.3.1).
Isolation monitoring	Am isolation monitoring device that either displays a ground fault or independently interrupts the circuit after a ground fault must be used (see IEC 60204-1:2005, 6.3.3.)
Energy isolation principle	Safe state is achieved once all important devices are separated from the energy source; e.g., through use of a normally closed contact (NC) for inputs (push-button and position switches) and a normally open contact (NO)for relays (see also ISO 12100:2010, 6.2.11.3). Exceptions are possible in some cases; e.g., when failure of electrical supply results in an additional hazard. Time delay functions may be required to achieve safe state for the system (see IEC 60204-1:2005, 9.2.2).
Power surge suppression	Equipment to suppress power surges (RC elements, diodes, varistors) must be used in parallel with the applied load, but never parallel with the contacts. *NOTE: A diode will increase switchoff time.*
Reduction of response time	Minimization of delay when switching off components used for switching.
Compatibility	Use of components suitable for the applied voltages and currents.
Guard locking for input devices	The input devices must be secured; e.g., through locking circuits, position switches, boundary position switches, proximity switches, etc., so position, alignment and switching tolerances are maintained under all expected conditions, such as vibration, typical wear, temperature and penetration of foreign bodies. See ISO 14119: 1998, Sect. 5.
Protection against unexpected start-up	Prevention of unexpected start-up; e.g., after power supply is restored (see ISO 12100:2010, 6.2.11.4, ISO 14118, IEC 60204-1).

Tables & formulas

Safety principles

Basic electrical safety principles	Remarks
Protection of control circuit	The control circuit should be protected according to IEC 60204-1:2005, 7.2 and 9.1.1.
Sequential switching in circuits with series connection of redundant signals	To prevent common-cause faults due to welded contacts, switching on and off never occur at the same time, so a contact always switches without power.

5.4.8 Validated – Electrical (EN ISO 13849-2 Table C.1)

Validated electrical safety principles	Remarks
Mechanically linked contacts	Use of mechanically linked contacts; e.g., for monitoring functions 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).
Cable fault prevention	To prevent short circuits between two adjacent lines, either: • Use cables with shielding that is connected to the protective ground system on each individual line, or • For ribbon cables, use a protective ground between all signal lines.
Distances between electrical lines	Application of a sufficient distance between connection terminals, components and lines to prevent unintended connection.
Energy restriction	A capacitor is to be used for the supply of restricted amounts of energy; e.g., where time control is used.
Limitation of electrical parameters	Limitation of voltage, current, energy or frequency to restrict movement; e.g., through torque limits, staggered/temporary running and speed restrictions to prevent unsafe states.
Prevention of undefined states	Undefined states in the control system must be prevented. The control system must be designed so that during normal operation and under all expected operating conditions, control system status; e.g., in- and outputs, can be determined in advance.
Direct actuation mode	Direct actuation is accomplished through positive locking (not forced fitting) with no elastic elements; i.e., no use of springs between actuator and contacts (see ISO 14119:1998, 5.1, ISO 12100:2010, 6.2.5).
Status alignment during failures	As far as possible, all devices/circuits must transition to a safe state or safe movements whenever there is a failure.
Controlled failure	Wherever feasible, components or systems for which failure types and behavior is known in advance are to be used (see ISO 12100:2010, 6.2.12.3).
Overdimensioning	Components used in safety circuits must be underloaded; e.g., by: • The current conducted through the switch contacts must be less than half the rated current, • The component switching frequency should be less than half the rated switching frequency and • The total number of expected switchings should be at most 10% of what the electrical device is designed for. NOTE: Underloading can depend on expedient design.
Restriction of potential faults	Separation of safety-related functions from other functions

Tables & formulas

Safety principles

Validated electrical safety principles	Remarks
Balance between complexity/simplicity	A balance should be established between: • Complexity of equipment needed to improve control and • Simplicity of equipment needed to improve reliability

Tables & formulas

5.5 Hazards (EN ISO 12100 Table B.1)

Group type	Origin	Possible consequences	ISO 12100 section
Mechanical hazards	- Acceleration, braking - Sharp parts - Proximity of moving part to stationary part - Cutting part - Elastic elements - Falling objects - Gravity - Height from ground - High pressure - Structural stability - Kinetic energy - Machine movability - Moving parts - Rotating parts - Rough, slippery surfaces - Sharp edges - Retained energy - Vacuum	- Being run over - Being ejected - Crushing - Cutting or severing - Pulling in or catching - Grasping - Chafing or abrading - Impact - Penetration of pressurized operating media - Shearing - Slipping, stumbling and falling - Piercing or puncturing - Suffocation	6.2.2.1 6.2.2.2 6.2.3 a) 6.2.3 b) 6.2.6 6.2.10 6.3.1 6.3.2 6.3.3 6.3.5.2 6.3.5.4 6.3.5.5 6.3.5.6 6.4.1 6.4.3 6.4.4 6.4.5
Electrical hazards	- Electric arc - Electromagnetic processes - Electromagnetic processes - Live electrical parts - Insufficient distance from live high voltage parts - Overload - Parts in faults state have become live - Short circuit - Heat radiation	- Combustion - Chemical reaction - Effects on medical implants - Lethal electric shock - Falling, ejection - Fire - Ejection of molten parts (electrical) shock	6.2.9 6.3.2 6.3.3.2 6.3.5.4 6.4.4 6.4.5
Thermal hazards	- Explosion - Flame - Objects or materials at higher or lower temperatures - Radiation from heat sources	- Combustion - Dehydration - Discomfort - Frostbite - Injuries due to radiation from heat sources - Scalding	6.2.4 b) 6.2.8 c) 6.3.2.7 6.3.3.2.1 6.3.4.5
Noise hazards	- Cavitation phenomena; - De-pressurizing system - Gas leaking at high speed - Manufacturing process)(stamping, cutting, etc.) - Moving parts - Scraping surfaces - Unbalanced rotating parts - Whistling pneumatics - Worn parts	- Discomfort - Loss of awareness - Loss of balance; - Permanent hearing loss - Stress - Tinnitus - Fatigue - Any other (e.g, mechanical electrical) as a consequence of an interference with speech communication or with acoustic signals.	6.2.2.2 6.2.3 c) 6.2.4 c) 6.2.8 c) 6.3.1 6.3.2.1 b) 6.3.2.5.1 6.3.3.2.1 6.3.4.2 6.4.3 6.4.5.1 b) and c)

Tables & formulas

Group type	Origin	Possible consequences	ISO 12100 section
Vibration hazards	• Cavitation phenomena; • Misalignment of moving parts • Mobile equipment • Scraping surfaces • Unbalanced rotating parts • Vibrating equipment • Worn parts	• Discomfort • Low-back morbidity • Neurological disorder • Osteo-articular disorder • Trauma of the spine • Vascular disorder	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)
Radiation hazards	• Ionizing radiation source • Low frequency electromagnetic radiation • Optical radiation (infrared, visible and ultraviolet), including laser • High frequency electromagnetic radiation	• Burns • Damage to eyes and skin • Effects on reproductive capability • Mutation • Headache, insomnia, etc.	6.2.2.2 6.2.3 c) 6.3.3.2.1 6.3.4.5 6.4.5.1 c)
Material/substance hazards	• Aerosol • Biological and microbiological (viral or bacterial) agent • Combustible • Dust • Explosive • Fiber • Flammable material • Fluid • Fume • Gas • Mist • Oxidizer	• Breathing difficulties, suffocation • Cancer • Corrosion • Effects on reproductive capability • Explosion • Fire • Infection • Altered genetics • Poisoning • Sensation	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)
Ergonomic hazards	• Access • Design or location of indicators and visual display units • Design, location or identification of control devices • Effort • Flicker, dazzling, shadow, stroboscopic effect; • Local lighting • Mental overload/underload • Posture • Repetitive activity • Visibility	• Discomfort • Fatigue • Musculoskeletal disorder • Stress • Any other (e.g., mechanical, electrical) as a consequence of human error.	6.2.2.1 6.2.7 6.2.8 6.2.11.8 6.3.2.1 6.3.3.2.1
Hazards associated with the environment in which the machine was used	• Dust and fog • Electromagnetic disturbance • Lightning • Moisture • Pollution • Snow • Temperature • Water • Wind • Lack of oxygen.	• Burns • Slight disease • Slipping, falling • Suffocation • Any other as a consequence of the effect caused by the sources of the hazards on the machine or parts of the machine.	6.2.6 6.2.11.11 6.3.2.1 6.4.5.1 b)
Combination of hazards	• E.g., repetitive activity + effort + high environmental temperature	• E.g., dehydration, loss of awareness, heat stroke	—

5.6 Protective equipment

5.6.1 Forces

The question of potential force is relevant to the conception of safety equipment. EN ISO 14119, Table I.1, gives a good starting point for this subject.

Force direction		Posture	Type of power transmission	Force unit [N]
	Horizontal pulling (tugging)	Sitting	One-handed	600
	Vertically upward	Standing, torso and legs bent, feet next to each other	Two-handed; horizontal grip	1400
	Vertically upward	Standing; free	One-handed; horizontal grip	1200
	Horizontal, parallel to sagittal plane toward rear, pulling	Standing upright, feet next to each other or step position	Two-handed; vertical grip	1100
	Horizontal, parallel to sagittal plane toward front, pushing	Standing, feet next to each other or step position	Two-handed; vertical grip	1300
	Horizontal, away from sagittal plane	Standing; torso bent sideways	Shoulder pressed against lateral metal plate	1300
	Horizontal, normal to sagittal plane	Standing feet next to each other	One-handed; vertical grip	700
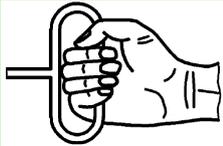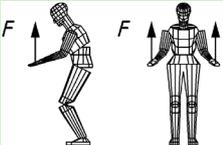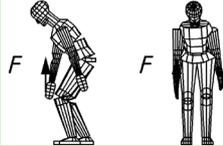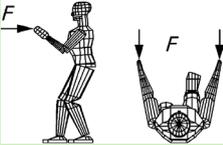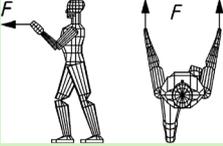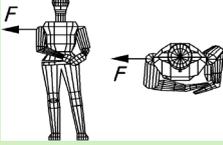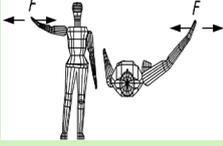
Table 3: EN ISO 14119 – Table I.1

Tables & formulas

Protective equipment

5.6.2 Safety distances

Safety distances for protective equipment are determined based on DIN EN ISO 13857 and depend on the following parameters:

- Proximity sensing devices
- Height of hazard area
- Affected limbs
- Presence of children
- Height of protective field
- Triggering optical protective equipment
- Safety function stop time

5.6.3 Access and sneak-by protection

The standards specify different values for permissible opening dimensions.

Standard	Access/safeguarding	Size [mm]	Prevents access
EN ISO 13857	Slot-shaped openings	180	Adult[1]
	Square or circular openings	240	Adult[1]
EN ISO 11161	Gap between separating protective equipment and floor	200	Adult[1]
EN ISO 13855	Vertical protective field (light curtain/grid) with bottom beam	300	Adult[1]
	Vertical protective field (light curtain/grid) with bottom beam	200	Children or visitor groups

[1] *Persons aged 14 years and older are viewed as adults.*

Tables & formulas

5.7   Actuator technology

5.7.1   Safe drive functions

Today, safe drive functions are available for many frequency converters. Some of the simpler functions, such as STO, SS1 and to an extent, SLS, can also be implemented with external solutions. See also the examples in Section 3. The column for example applications is intended to stimulate use of safety functions viewed by many as impracticable as little as 5 years ago.

Abbreviation	EN	DE	Function	Examples for applications
STO	Safe Torque Off	Sicher abge-schaltetes Moment	Motor disconnected from any energy that might cause rotational movement; stop category 0 per EN 60204-1	Prevention of unexpected start-up of hazardous movements during setup, commissioning and troubleshooting
SS1	Safe Stop 1	Sicherer Stopp 1	Motor decelerated, braking ramp monitored, STO after standstill or STO after a set delay time expires; stop category 1 per EN 60204-1	Bring about standstill as quickly as possible after safety equipment is triggered. E.g.: • Opening a protective door • Imbalance of rotating parts occurs in the system
SS2	Safe Stop 2	Sicherer Stopp 2	Motor decelerated, braking ramp monitored, SOS after standstill or SOS after a set delay time expires; stop category 2 per EN 60204-1	• Measurement on workpiece under position maintenance • Maintain load on vertical axis.
SOS	Safe Operating Stop	Sicherer Betriebshalt	Motor at full stop and resists external forces.	• Setup mode at processing centers, • Manual measurement during processing.
SLA	Safety-Limited Acceleration	Sicher begrenzte Beschleuni-gung	Exceeding an acceleration limit value is prevented.	• During transport of open fluid containers, • Mechanical inertial load restricted to workpiece or mount.
SAR	Safe Acceleration Range	Sicherer Beschleuni-gungsbereich	Motor acceleration kept within specified limit values.	See SLA

Tables & formulas

Actuator technology

Abbreviation	EN	DE	Function	Examples for applications
SLS	Safely-Limited Speed	Sicher begrenzte Geschwindig-keit	Exceeding a speed limit value is prevented.	• Setup mode at processing centers. • Threading of material on calendar rolls.
SSR	Safe Speed Range	Sicherer Geschwindig-keitsbereich	Motor speed kept within specified limit values.	See SLS and SSM
SLT	Safely-Limited Torque	Sicher begrenztes Moment	Exceeding torque/force limit value is prevented.	• Force limitation at closing edges of force-actuated doors and gates, • Prevention of persons being drawn in by winding machines.
STR	Safe Torque Range	Sicherer Momenten-bereich	Motor torque kept within specified limit values.	See SLT
SLP	Safely-Limited Position	Sicher begrenzte Position	Exceeding a position limit value is prevented.	• Area division at a machine into manufacturing and loading areas, • Limitation of a travel range, • Use of electromechanical end switches, • Limited reach distance for robot arms.
SLI	Safely-limited increment	Sicher begrenztes Schrittmaß	The motor is run for a specified interval and then stops.	• Setup mode at processing centers, • Travel-limited jogging on print machine
SDI	Safe direction	Sichere Bewegungs-richtung	Unexpected direction of motor movement prevented	• Prevents machine parts from moving toward/into people. • Prevention of entrapment and pull-in points on rollers.

Tables & formulas

Actuator technology

Abbreviation	EN	DE	Function	Examples for applications
SMT	Safe Motor Temperature	Sichere Motor-temperatur	Exceeding a motor temperature limit value is prevented	• Prevention of impermissibly high temperatures in Ex areas, • Fire protection
SBC	Safe Brake Control	Sichere Bremsen-ansteuerung	Safe control of an external brake	Vertical axis applications
SCA	Safe CAM	Sichere Nocken	A safe output signal is generated when the motor is in a specified area.	• Replacement of position sensors, • Pressing cycle monitoring • Robot axis position limitation.
SSM	Safe Speed Monitoring	Sichere Geschwindig-keitsüber-wachung	A safe output signal is generated when the motor speed is below a specified area.	• Fan monitoring • Gas mixture monitoring • Laser movement monitoring

Tables & formulas

Actuator technology

5.7.2 Safe speeds

At this time, there are no uniform evaluations from which to identify a movement as nonhazardous. The following standards state speeds or increments and can serve as starting points. Because of the complexity of factors in every individual case, the text of a standard should be carefully checked to ensure its applicability. In the standard texts, both mm/s or m/min are used to denote speeds. Here, all speed values are expressed in mm/s for easier comparability.

Standard and Machine type	Criteria							Function	Limit	Required measures			
	General	Impact	Crushing	Shearing	Entrapment	Vector movement	Movement / hazard			Manual operation of direction	Consent/jogging	Two-hand	Other measures
EN ISO 16090-1: Machining centers, milling machines, transfer machines	X							SLS	33 mm/s	X	X		Standstill 2 rotations after stop command or stopping distance less than 4 mm
	X					No			50 rpm	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		SLS	83 mm/s		X		Standstill 5 rotations after stop command
								SLI	10 mm				
							Clamping	SLI	4 mm	X	X		Maximum clamp/lift 4 mm
EN ISO 10218: Robots	X					Yes		SLS	250 mm/s		X		
EN ISO 23125: Safety – Turning machines	X							SLI	6 mm		X		
	X								33 mm/s		X		
	X					No		SLS	100 mm/s		X	(X)	Small turning machines
									167 mm/s				Large turning machines and linear axes
							Clamping	SLI	4 mm				Maximum clamp/lift 4 mm
								SLS	4 mm/s				

Tables & formulas

Actuator technology

Standard and machine type	Criteria							Function	Limit	Required measures			
	General	Impact	Crushing	Shearing	Entrapment	Vector movement	Movement / hazard			Manual operation of direction	Acknowledgement/logging circuit	Two-hand	Other measures
EN 1010-1: Printing and paper converting machines	X							SLI	25 mm		X		
								SLS	17 mm/s		X		
	X						Hazard not significantly increased	SLI	75 mm		X		
								SLS	83 mm/s		X		
		X					Transport of rolls	SLS	333 mm/s		X		
EN ISO 11161: Integrated manufacturing systems				X				SLS	33 mm/s		X		
		X	X		X				250 mm/s		X		
							Presses		10 mm/s		X		
EN ISO 13128: Safety of machine tools – Milling machines	X							SLI	10 mm		X		Standstill 2 rotations after stop command
								SLS	33 mm/s				
	X					Yes		SLS	83 mm/s	X	X		Standstill 5 rotations after stop command
		X							250 mm/s		X		

5.8 Biometric limit values

5.8.1 Pressures and forces per DIN ISO/TS 15066:2017

Limit values for quasi-static pressures (crushing/squeezing) or transient forces (impact) corresponding to body regions. Potential collisions to especially endangered employee head and throat areas must be avoided.
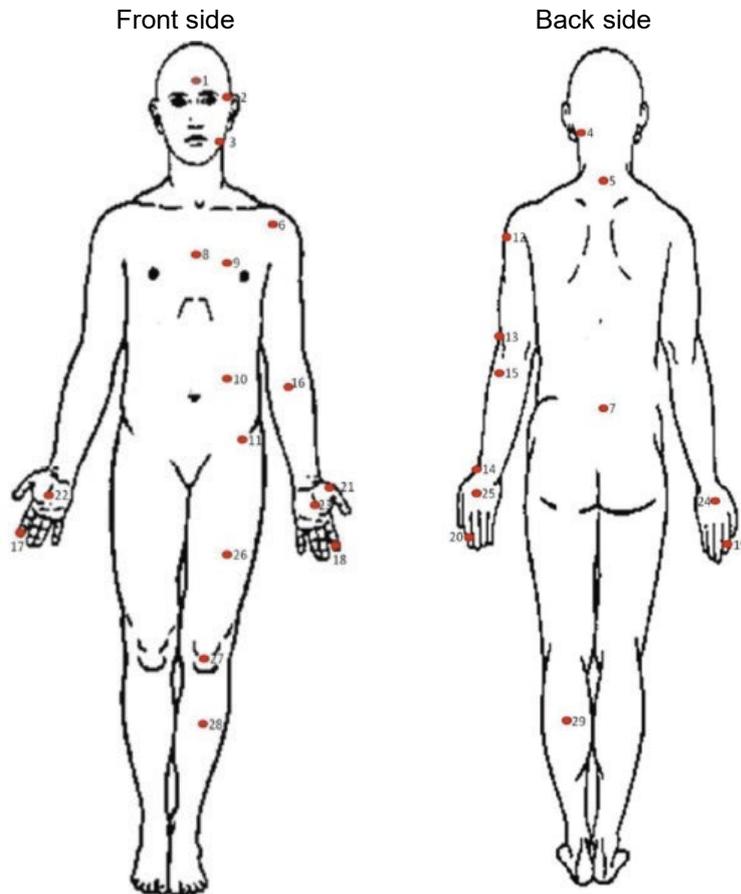
Illustration 6: Model body(DIN ISO/TS 15066:2017)

Body region	Specific body region		Quasi-static contact		Transient contact	
			Maximum permissible pressure	Maximum permissible force	Factor for maximum permissible pressure	Factor for maximum permissible force
			p_s [N/cm^2]	N	P_T	F_T
Cranium and forehead	1	Center of forehead	130	130	Not applicable	Not applicable
	2	Temples	110	130	Not applicable	Not applicable
Face	3	Masticatory muscles	110	65	Not applicable	Not applicable
Throat	4	Throat muscles	140	150	2	2

Tables & formulas

Body region		Specific body region	Quasi-static contact		Transient contact	
			Maximum permissible pressure	Maximum permissible force	Factor for maximum permissible pressure	Factor for maximum permissible force
			p_s [N/cm^2]	N	P_T	F_T
	5	Machine mobility	210	150	2	2
Back and shoulders	6	Shoulder joint	160	210	2	2
	7	Fifth lumbar vertebra	210	210	2	2
Ribcage	8	Sternum	120	140	2	2
	9	Pectoral muscle	170	140	2	2
Abdomen	10	Abdominal muscle	140	110	2	2
Pelvis	11	Pelvic bone	210	180	2	2
Shoulder and elbow joints	12	Deltoid muscle	190	150	2	2
	13	Shoulder joint	220	150	2	2
Forearm and wrist	14	Radius	190	160	2	2
	15	Forearm muscles	180	160	2	2
	16	Arm nerves	180	160	2	2
Hand and finger	17	Index fingertip D	300	140	2	2
	18	Index fingertip ND	270	140	2	2
	19	Index finger joint D	280	140	2	2
	20	Index finger joint ND	220	140	2	2
	21	Ball of thumb	200	140	2	2
	22	Palms, surface D	260	140	2	2
	23	Palms, surface ND	260	140	2	2

Body region	Specific body region		Quasi-static contact		Transient contact	
			Maximum permissible pressure	Maximum permissible force	Factor for maximum permissible pressure	Factor for maximum permissible force
			p_s [N/cm^2]	N	P_T	F_T
	24	Back of hand D	200	140	2	2
	25	Back of hand ND	190	140	2	2
Thigh and knee	26	Thigh musculature	250	220	2	2
	27	Kneecap	220	220	2	2
Lower leg	28	Shin	220	130	2	2
	29	Calf muscle	210	130	2	2

Illustration 7: Biomechanical limit values (DIN ISO/TS 15066:2017)

Standards and references

6 Standards and references

To the extent that they exist, this document quotes from the EN version of the standard; if it does not exist, the ISO or IEC version is used as source. Complete tables taken from standards sources are an exception. Here, ISO or IEC versions – often outmoded – are often referenced. To improve legibility, the corresponding DIN is given in places.

Usually, the EN version of the standard cannot be directly acquired and so the corresponding DIN variation is referenced. In other EU countries, the corresponding national adaptations are to be used. The column "CE" contains standards relevant to CE mark compliance.

German standard / reference	Title – German (where available)	CE[1]	International equivalences
2006/42/EC *(published in document: 2006 L 157/24)*	DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (new revision)	X	2006/42/EC
BetrSichV (2015)	Industrial Safety Regulations		*(implementation of part of 2006/42/EC)*
DIN EN 1010-1:2010	Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines	X	EN 1010-1:2004+A1:2010 *(not available as ISO or IEC)*
DIN EN 60204-1:2006/AC:2010	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	X	IEC 60204-1:2005
DIN EN 60529:2014	Degrees of protection provided by enclosures		IEC 60529 AMD 2:2013
DIN EN 60947-4-1:2014	Low-voltage switchgear and controlgear – Part 4-1: Contactors and motor-starters – Electromechanical contactors and motor-starters		IEC 60947-4-1 AMD 1:2012
DIN EN 60947-5-1:2010	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
DIN EN 61496-1:20140	Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests	X	IEC 61496-1:201208
DIN EN 61508 Part 1-7:2011	Functional safety of electrical/electronic/programmable electronic safety-related systems		IEC 61508 Parts 1-7:2010

Standards and references

German standard / reference	Title – German (where available)	CE[1]	International equivalences
DIN EN 61810-2:2012	Electromechanical elementary relays – Part 2: Reliability		IEC 61810-2:2011
DIN EN 61810-3:2016 *(replaces EN 50205)*	Electromechanical elementary relays – Part 3: Relays with forcibly guided (mechanically linked) contacts		IEC 61810-3:2015
DIN EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems	X	IEC 62061 AMD 2:2015
DIN EN ISO 10218-1:2012	Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots	X	ISO 10218-1:2011
DIN EN ISO 11161:2010	Safety of machinery – Integrated manufacturing systems – Basic requirements	X	ISO 11161:2007 + Amd 1:2010
DIN EN ISO 12100:2011	Safety of machinery – General principles for design – Risk assessment and risk reduction	X	ISO 12100:2010
DIN EN ISO 13849-1:2016	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design	X	ISO 13849-1:2015
DIN EN ISO 13849-2:2013	Safety of machinery – Safety-related parts of control systems – Part 2: Validation	X	ISO 13849-2:2012
DIN EN ISO 13850:2015	Safety of machinery – Emergency stop function – Principles for design	X	ISO 13850:2015
DIN EN ISO 13855:2010	Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body	X	ISO 13855:20082010
DIN EN ISO 13857:2008	Safety of machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs	X	ISO 13857:2008
DIN EN ISO 14118:2016	Safety of machinery – Prevention of unexpected start-up		ISO/DIS 14118:2016
DIN EN ISO 14119:2014-03	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection	X	ISO 14119:2013
DIN EN ISO 16090-1:2016, draft	Machine tools safety – Machining centers, Milling machines, Transfer machines – Part 1: Safety requirements		ISO/DIS 16090-1.2:2015

German standard / reference	Title – German (where available)	CE[1]	International equivalences
DIN EN ISO 23125:2015	Machine tools – Safety – Turning machines	X	ISO 23125:2015
DIN EN ISO EN 13128:2009	Safety of machine tools – Milling machines (including boring machines)	X	EN 13128:2001 +A2:2009 *(not available as ISO or IEC)*
DIN ISO/TS 15066:2017	Robots and robotic devices – Collaborative robots		ISO/TS 15066:2016 *(no EN equivalent)*
ISO/TR 24119: 2015 *(no DE equivalent)*	Safety of machinery – Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts		ISO/TR 24119: 2015
OSHA 29 CFR 1910.147 *(no DE equivalent)*	Occupational Safety and Health Standards – General Environmental Controls – The control of hazardous energy (lockout/tagout)		OSHA 29 CFR 1910.147
ProdSG	Product Safety Act		*(Part of 2006/42/EC)*

1 Is listed in the Official Journal as harmonized with at least one EU Directive with CE relevance.a

7   Notes

7.1   Copyright

7.2   Liability

Unless stated otherwise in these General Sales Conditions including the following provisions, we shall be liable for any breach of contractual and non-contractual duties according to the relevant statutory provisions.

We shall be liable for compensation – regardless for which legal reason – in cases of intent or gross negligence. We shall be liable for compensation – regardless for which legal reason – in cases of intent or gross negligence. In cases of ordinary negligence, we shall only be liable for damages arising from injury to life, body or health, for damages arising from violation of an essential contractual obligation (obligation, which makes the proper implementation of the contract possible at all and the adherence to which the contractual partner relies on and may rely on regularly); in this case, however, our liability shall be limited to the reimbursement of the foreseeable, typically occurring damage.

Index

Index

Index

Index

wieland

HEADQUARTERS

Wieland Electric GmbH

Brennerstraße 10 – 14

96052 Bamberg · Germany

Phone +49 951 9324-0
Fax   +49 951 9324-198
info@wieland-electric.com

0424.1 MC 04/23

Represented in over 70 countries worldwide:

www.**wieland**-electric.com