

Documentation | EN

Application Guide TwinSAFE

Examples for the calculation of safety parameters for safety functions

Safety over
EtherCAT 

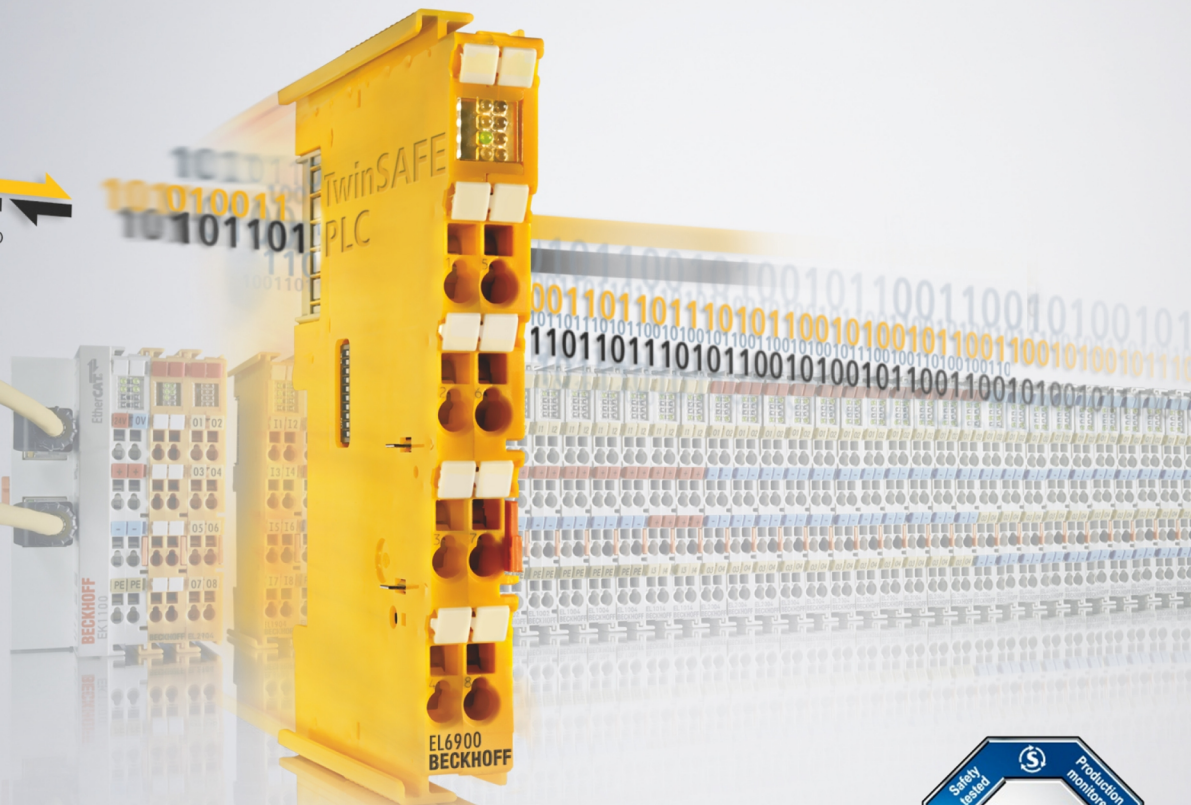


Table of contents

1	Foreword	9
1.1	Notes on the documentation.....	9
1.2	Safety instructions	10
1.2.1	Delivery state	10
1.2.2	Operator's obligation to exercise diligence	11
1.2.3	Purpose and area of application	11
1.2.4	Description of instructions.....	12
1.2.5	Explanation of terms	13
1.3	Documentation issue status	14
2	ESTOP functions	15
2.1	ESTOP function variant 1 (category 3, PL d)	15
2.1.1	Parameters of the safe input and output terminals	15
2.1.2	Block formation and safety loops.....	16
2.1.3	Calculation	16
2.2	ESTOP function variant 2 (category 3, PL d)	21
2.2.1	Parameters of the safe input and output terminals	21
2.2.2	Block formation and safety loops.....	22
2.2.3	Calculation	22
2.3	ESTOP function variant 3 (category 4, PL e)	27
2.3.1	Parameters of the safe input and output terminals	27
2.3.2	Block formation and safety loops.....	28
2.3.3	Calculation	28
2.4	ESTOP function variant 4 (category 4, PL e)	33
2.4.1	Parameters of the safe input and output terminals	33
2.4.2	Block formation and safety loops.....	34
2.4.3	Calculation	34
2.5	ESTOP function variant 5 (category 4, PL e)	39
2.5.1	Parameters of the safe input and output terminals	39
2.5.2	Block formation and safety loops.....	40
2.5.3	Calculation	40
2.6	ESTOP function variant 6 (category 3, PL d)	45
2.6.1	Parameters of the safe input and output terminals (SIL 2)	45
2.6.2	Block formation and safety loops.....	46
2.6.3	Calculation	46
2.7	ESTOP function variant 7 (category 4, PL e)	51
2.7.1	Parameters of the safe input and output terminals	51
2.7.2	Block formation and safety loops.....	52
2.7.3	Calculation	52
2.8	EK1960 digital inputs and outputs (category 4, PL e)	57
2.8.1	Parameters of the safe input and output modules	58
2.8.2	Block formation and safety loops.....	58
2.8.3	Calculation	59
2.9	EK1960 digital inputs / relay outputs (category 4, PL e).....	63
2.9.1	Parameters of the safe input and output modules	64

2.9.2	Block formation and safety loops.....	64
2.9.3	Calculation	65
2.10	ESTOP function (category 3, PL d)	69
2.10.1	Parameters of the safe input and output terminals (SIL 2)	69
2.10.2	Block formation and safety loops.....	70
2.10.3	Calculation	70
3	Access functions.....	74
3.1	Protective door function variant 1 (category 3, PL d)	74
3.1.1	Parameters of the safe input and output terminals	74
3.1.2	Block formation and safety loops.....	75
3.1.3	Calculation	75
3.2	Protective door function variant 2 (category 4, PL e)	79
3.2.1	Parameters of the safe input and output terminals	79
3.2.2	Block formation and safety loops.....	80
3.2.3	Calculation	80
3.3	Protective door function with range monitoring (Category 4, PL e)	84
3.3.1	Parameters of the safe input and output terminals	85
3.3.2	Block formation and safety loops.....	85
3.3.3	Calculation	86
3.4	Protective door function with tumbler (Category 4, PL e).....	91
3.4.1	Parameters of the safe input and output terminals	91
3.4.2	Block formation and safety loops.....	92
3.4.3	Calculation	92
3.5	Two-hand controller (Category 4, PL e)	98
3.5.1	Parameters of the safe input and output terminals	98
3.5.2	Block formation and safety loops.....	99
3.5.3	Calculation	99
3.6	Laser scanner (category 3, PL d)	103
3.6.1	Parameters of the safe input and output terminals	103
3.6.2	Block formation and safety loops.....	104
3.6.3	Calculation	104
3.7	Light curtain (Category 4, PL e).....	108
3.7.1	Parameters of the safe input and output terminals	108
3.7.2	Block formation and safety loops.....	109
3.7.3	Calculation	109
3.8	Safety switching mat / safety bumper (Category 4, PL e)	113
3.8.1	Parameters of the safe input and output terminals	113
3.8.2	Block formation and safety loops.....	114
3.8.3	Calculation	114
3.9	Muting (Category 4, PL e)	118
3.9.1	Parameters of the safe input and output terminals	118
3.9.2	Block formation and safety loops.....	119
3.9.3	Calculation	119
3.10	EK1960 safety mat inputs / digital outputs (category 2, PL d).....	124
3.10.1	Parameters of the safe input and output modules	125
3.10.2	Block formation and safety loops.....	125

3.10.3	Calculation	126
3.11	EP1957 OSSD sensor for protective door (Category 4, PL e)	130
3.11.1	Parameters of the safe input and output modules	131
3.11.2	Block formation and safety loops	131
3.11.3	Calculation	132
4	Potential groups	135
4.1	All-pole disconnection of a potential group with downstream interference-free standard terminals (Category 4, PL e)	135
4.1.1	Notes on prevention of feedback	137
4.1.2	Parameters of the safe input and output terminals	138
4.1.3	Block formation and safety loops	139
4.1.4	Calculation	139
4.2	Single-pole disconnection of a potential group with downstream interference-free standard terminals with fault exclusion (Category 4, PL e)	144
4.2.1	Notes on prevention of feedback	146
4.2.2	Parameters of the safe input and output terminals	147
4.2.3	Block formation and safety loops	148
4.2.4	Calculation	148
4.3	EL2911 potential group with interference-free standard terminals (Category 4, PL e).....	153
4.3.1	Notes on prevention of feedback	154
4.3.2	EL2911 parameters	156
4.3.3	Block formation and safety loops	156
4.3.4	Calculation	157
4.4	EPP potential group with EPP9022-9060 (Category 4, PL e)	161
4.4.1	Notes on prevention of feedback	164
4.4.2	EL2911 parameters	166
4.4.3	Block formation and safety loops	166
4.4.4	Calculation	167
5	STO/SS1 functions	171
5.1	AX8xxx-x1xx STO function (Category 4, PL e)	171
5.1.1	Parameters of the safe input and output modules	172
5.1.2	Block formation and safety loops	172
5.1.3	Calculation	172
5.2	Drive option AX5801 with SS1 stop function (Category 4, PL e).....	177
5.2.1	Parameters of the safe input and output terminals	178
5.2.2	Block formation and safety loops	178
5.2.3	Calculation	179
5.3	STO function with EL72x1-9014 (category 3, PL d)	183
5.3.1	Parameters of the safe input and output terminals	184
5.3.2	Block formation and safety loops	184
5.3.3	Calculation	185
5.4	STO function with IndraDrive (category 4, PL e)	189
5.4.1	Parameters of the safe input and output terminals	190
5.4.2	Block formation and safety loops	190
5.4.3	Calculation	190
5.4.4	Technical Note from Bosch Rexroth AG	194

6	Safe Motion functions	198
6.1	Drive option AX5805 with SS2 stop function (Category 4, PL e).....	198
6.1.1	Parameters of the safe input and output terminals	198
6.1.2	Block formation and safety loops	199
6.1.3	Calculation	199
7	Analog value processing with TwinSAFE SC	203
7.1	Speed monitoring (category 3, PL d).....	203
7.1.1	Structure and diagnosis	205
7.1.2	FMEA.....	206
7.1.3	Parameters of the safe output terminal.....	207
7.1.4	Block formation and safety loops.....	208
7.1.5	Calculation	208
7.2	Speed monitoring (via IO-Link) (category 3, PL d)	214
7.2.1	Structure and diagnosis	215
7.2.2	FMEA.....	216
7.2.3	Parameters of the safe output terminal.....	217
7.2.4	Block formation and safety loops.....	218
7.2.5	Calculation	218
7.3	Temperature measurement with TwinSAFE SC (category 3, PL d).....	224
7.3.1	Schematic diagram of the configuration	225
7.3.2	Structure and diagnosis	225
7.3.3	FMEA.....	225
7.3.4	Parameters of the safe output terminal.....	226
7.3.5	Block formation and safety loops.....	227
7.3.6	Calculation	227
7.4	Level measurement with TwinSAFE SC (category 3, PL d)	233
7.4.1	Schematic diagram of the configuration	234
7.4.2	Structure and diagnosis	234
7.4.3	FMEA.....	234
7.4.4	Parameters of the safe output terminal.....	235
7.4.5	Block formation and safety loops.....	236
7.4.6	Calculation	236
7.5	Pressure measurement with TwinSAFE SC (category 3, PL d)	242
7.5.1	Schematic diagram of the configuration	243
7.5.2	Structure and diagnosis	243
7.5.3	FMEA.....	243
7.5.4	Parameters of the safe output terminal.....	244
7.5.5	Block formation and safety loops.....	245
7.5.6	Calculation	245
7.6	Monitoring of lifting device (category 3, PL d)	251
7.6.1	Structural image structure.....	252
7.6.2	Structure and diagnosis	252
7.6.3	FMEA.....	253
7.6.4	Structure within the logic.....	254
7.6.5	Parameters of the safe output terminal.....	256
7.6.6	Block formation and safety loops.....	257

7.6.7	Calculation	257
8	Application-specific scenarios	264
8.1	Networked system (Category 4, PL e).....	264
8.1.1	Parameters of the safe input and output terminals	265
8.1.2	Block formation and safety loops	265
8.1.3	Calculation	266
8.2	Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (1-channel) (Category 2, PL c)	270
8.2.1	Parameters of the safe input and output terminals	270
8.2.2	Block formation and safety loops	271
8.2.3	Calculation	271
8.3	Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (2-channel) (Category 3, PL d)	274
8.3.1	Parameters of the safe input and output terminals	274
8.3.2	Block formation and safety loops	274
8.3.3	Calculation	275
9	Connection of PROFIsafe	277
9.1	Safe speed monitoring with PROFIsafe encoder (category 4, PL e).....	277
9.1.1	FMEA	279
9.1.2	Configuration in the engineering environment	279
9.1.3	Parameters of the safe output terminal	287
9.1.4	Block formation and safety loops	287
9.1.5	Calculation of safety function 1 (without drive)	288
9.1.6	Calculation of safety function 2 (with drive)	291
9.2	Safe area monitoring with PROFIsafe laser scanner (category 3, PL d).....	295
9.2.1	Configuration in the engineering environment	296
9.2.2	Parameters of the safe input and output terminal	306
9.2.3	Block formation and safety loops	307
9.2.4	Calculation of safety function 1	307
9.3	Safe control of an ABB robot via PROFIsafe (category 3, PL d)	311
9.3.1	FMEA	313
9.3.2	Configuration in the engineering environment	313
9.3.3	Parameters of the safe input terminal	321
9.3.4	Block formation and safety loops	322
9.3.5	Calculation of safety function 1	322
10	Planning a safety project with TwinSAFE components	326
10.1	Identifying the risks and hazards	326
10.2	Determining the PLr / SIL	327
10.3	Specification of the safety functions	327
10.4	Specification of the measures	327
10.5	Implementation of the safety functions	327
10.6	Proof of achievement of the Performance Level	330
10.7	Validation of the safety functions	330
10.8	Instructions for checking the SF	330
10.9	Acceptance	331
11	Technical report – TÜV SÜD	332
12	Support and Service	333

1 Foreword

1.1 Notes on the documentation

Intended audience

This description is only intended for the use of trained specialists in control and automation engineering who are familiar with the applicable national standards.

It is essential that the following notes and explanations are followed when installing and commissioning these components.

The responsible staff must ensure that the application or use of the products described satisfy all the requirements for safety, including all the relevant laws, regulations, guidelines and standards.

Origin of the document

This original documentation is written in German. All other languages are derived from the German original.

Currentness

Please check whether you are using the current and valid version of this document. The current version can be downloaded from the Beckhoff homepage at <http://www.beckhoff.com/english/download/twinsafe.htm>. In case of doubt, please contact Technical Support [▶ 333].

Product features

Only the product features specified in the current user documentation are valid. Further information given on the product pages of the Beckhoff homepage, in emails or in other publications is not authoritative.

Disclaimer

The documentation has been prepared with care. The products described are subject to cyclical revision. For that reason the documentation is not in every case checked for consistency with performance data, standards or other characteristics. We reserve the right to revise and change the documentation at any time and without prior announcement. No claims for the modification of products that have already been supplied may be made on the basis of the data, diagrams and descriptions in this documentation.

Trademarks

Beckhoff®, TwinCAT®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered trademarks of and licensed by Beckhoff Automation GmbH. Other designations used in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owners.

Patent Pending

The EtherCAT Technology is covered, including but not limited to the following patent applications and patents: EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702 with corresponding applications or registrations in various other countries.



EtherCAT® and Safety over EtherCAT® are registered trademarks and patented technologies, licensed by Beckhoff Automation GmbH, Germany.

Copyright

© Beckhoff Automation GmbH & Co. KG, Germany.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited.

Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

Delivery conditions

In addition, the general delivery conditions of the company Beckhoff Automation GmbH & Co. KG apply.

1.2 Safety instructions

1.2.1 Delivery state

All the components are supplied in particular hardware and software configurations appropriate for the application. Modifications to hardware or software configurations other than those described in the documentation are not permitted, and nullify the liability of Beckhoff Automation GmbH & Co. KG.

1.2.2 Operator's obligation to exercise diligence

The operator must ensure that

- the TwinSAFE products are only used as intended (see chapter Product description);
- the TwinSAFE products are only operated in sound condition and in working order.
- the TwinSAFE products are operated only by suitably qualified and authorized personnel.
- the personnel is instructed regularly about relevant occupational safety and environmental protection aspects, and is familiar with the operating instructions and in particular the safety instructions contained herein.
- the operating instructions are in good condition and complete, and always available for reference at the location where the TwinSAFE products are used.
- none of the safety and warning notes attached to the TwinSAFE products are removed, and all notes remain legible.

1.2.3 Purpose and area of application

The Application Guide provides the user with examples for the calculation of safety parameters for safety functions according to the standards DIN EN ISO 13849-1 and EN 62061 or EN 61508:2010 (if applicable), such as are typically used on machines.

In the examples an EL1904 is taken as an example for a safe input or an EL2904 for a safe output. This is to be considered an example; of course other safe inputs or outputs can be used, such as an EP1908 or an EL2912. The appropriate parameters, which can be taken from the respective product documentation, must then be used in the calculation.

NOTE

Application samples

These samples provide the user with example calculations. They do not release him from his duty to carry out a risk and hazard analysis and to apply the directives, standards and laws that need to be considered for the application.

1.2.4 Description of instructions

In these operating instructions the following instructions are used.
These instructions must be read carefully and followed without fail!

DANGER

Serious risk of injury!

Failure to follow this safety instruction directly endangers the life and health of persons.

WARNING

Risk of injury!

Failure to follow this safety instruction endangers the life and health of persons.

CAUTION

Personal injuries!

Failure to follow this safety instruction can lead to injuries to persons.

NOTE

Damage to the environment/equipment or data loss

Failure to follow this instruction can lead to environmental damage, equipment damage or data loss.



Tip or pointer

This symbol indicates information that contributes to better understanding.

1.2.5 Explanation of terms

Name	Explanation
B_{10D}	Mean number of cycles after 10% of the components have dangerously failed
CCF	Failures with a common cause
d_{op}	Mean operating time in days per year
DC_{avg}	Average diagnostic coverage
h_{op}	Mean operating time in hours per day
$MTTF_D$	Mean time to dangerous failure
n_{op}	Mean number of annual actuations
PFH_D	Probability of a dangerous failure per hour
PL	Performance level
PL_r	Required Performance Level
T_{cycle}	Mean time between two successive cycles of the system (given in minutes in the following examples, but can also be given in seconds)
T1	Lifetime of the device (typically 20 years for TwinSAFE devices)
λ_D	Dangerous failure rate given in FIT (failure rate in 10^9 component hours)
T_{10D}	Operating time - maximum operating time for electromechanical components, for example
TwinSAFE SC	<p>The TwinSAFE SC technology (SC - Single Channel) enables a signal from a standard terminal to be packaged in a FSoE telegram and transmitted via the standard fieldbus to the TwinSAFE Logic. As a result, falsifications on the transmission path can be excluded. Within the TwinSAFE Logic, this signal is checked with a further independent signal. This comparison result typically yields an analog value corresponding to a category 3 and PL d.</p> <p>This technology does not support digital input signals and cannot be used in a single-channel structure (only one TwinSAFE SC channel).</p>

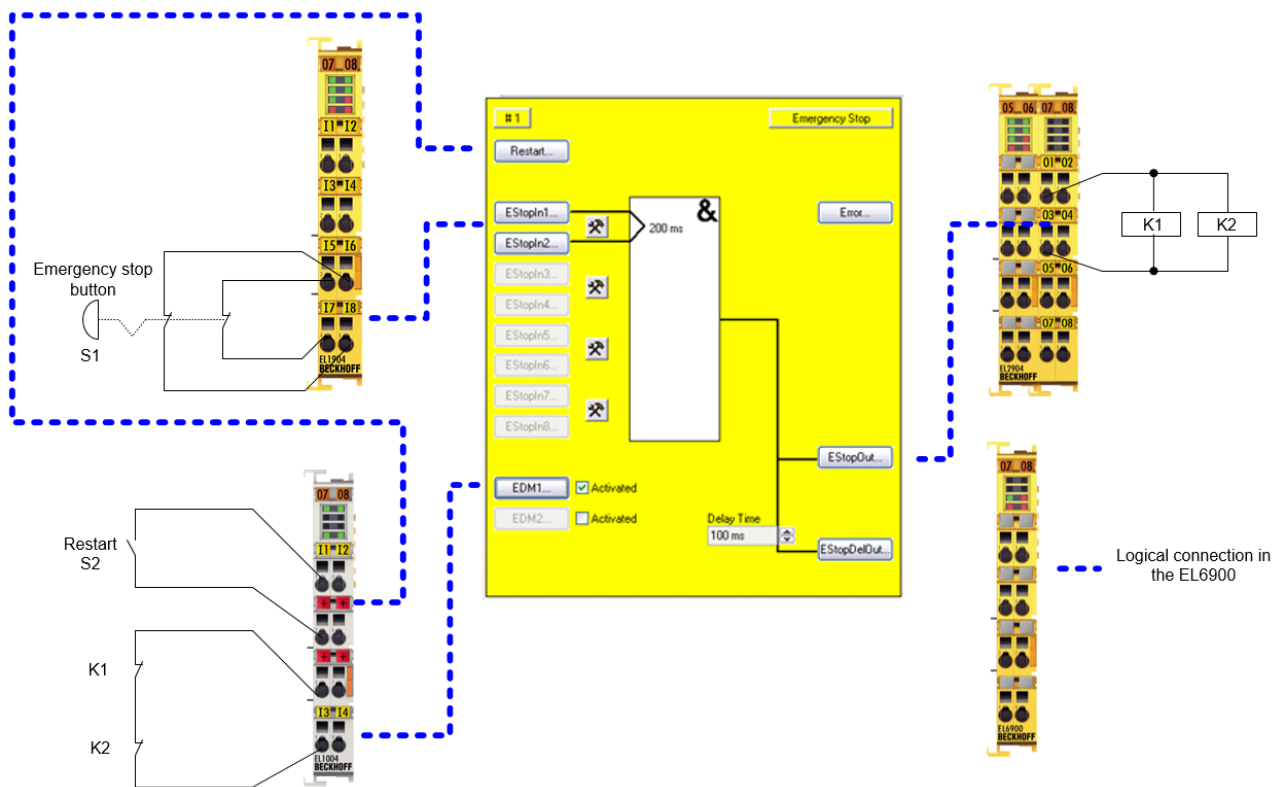
1.3 Documentation issue status

Version	Comment
3.1.0	<ul style="list-style-type: none"> Chapter <i>Planning a safety project with TwinSAFE components</i> added
3.0.0	<ul style="list-style-type: none"> PROFIsafe examples added Document structure revised Confirmation of conformity updated
2.2.0	<ul style="list-style-type: none"> EPP9022-9060 example updated
2.1.0	<ul style="list-style-type: none"> Migration Examples AX8xxx, EL2911, EP1957 and EPP9022-9060 added Information on training courses added Confirmation of conformity updated
2.0.0	<ul style="list-style-type: none"> EK1960 examples added Calculation in chapter 2.26 corrected
1.9.1	<ul style="list-style-type: none"> Note added in chapter 2.17 and 2.18
1.9.0	<ul style="list-style-type: none"> Chapter 2.18 revised Chapter <i>Planning a safety project</i>, added
1.8.0	<ul style="list-style-type: none"> TwinSAFE SC examples added Example for Bosch Rexroth IndraDrive drive family Designation <i>SIL2 communication</i> replaced with <i>TwinSAFE SC</i> Examples 2.25 and 2.26 updated General revision of all chapters
1.7.0	<ul style="list-style-type: none"> Chapter <i>Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (single channel)</i> revised Foreword updated Chapter <i>Purpose and area of application</i> expanded Structure diagram chapters 2.25 and 2.26 updated Chapter 2.27 added Chapters 2.2.3.2, 2.3.3.2, 2.4.3.2, 2.5.3.2, 2.7.3.2 and 2.19.3.2. substantiated (notes on direct / indirect reading back removed) Note texts added in chapter 2.19
1.6.2	<ul style="list-style-type: none"> Confirmation of conformity updated Graphics in chapters 2.25 and 2.26 updated Chapter <i>Purpose and area of application</i> added
1.6.1	<ul style="list-style-type: none"> Chapters 2.25 and 2.26 added
1.6.0	<ul style="list-style-type: none"> Chapters 2.17 and 2.18 revised
1.5.0	<ul style="list-style-type: none"> Chapter 2.24 added Documentation versions added Document origin added Formatting changed
1.4.0	<ul style="list-style-type: none"> Headers extended with categories and performance levels Note in Chapter 2.6 moved
1.3.0	<ul style="list-style-type: none"> Terms of delivery removed
1.2.0	<ul style="list-style-type: none"> Correction to Chapter 2.6
1.1.0	<ul style="list-style-type: none"> First released version

2 ESTOP functions

2.1 ESTOP function variant 1 (category 3, PL d)

The emergency stop button is connected via two normally closed contacts to an EL1904 safe input terminal. The testing and the monitoring of the discrepancy of the two signals are activated. The restart and the feedback signal are wired to standard terminals and are transferred to TwinSAFE via the standard PLC. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



2.1.1 Parameters of the safe input and output terminals

EL1904

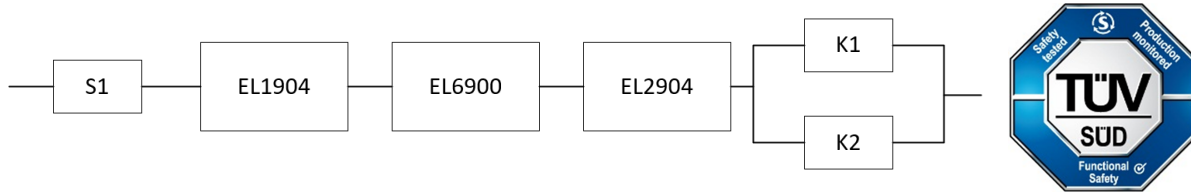
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

2.1.2 Block formation and safety loops

2.1.2.1 Safety function 1



2.1.3 Calculation

2.1.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week) (7 days, 24 hours)
Lifetime (T1)	20 years = 175200 hours

2.1.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM (actuation 1x per week)	DC _{avg} =60%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =90%

2.1.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_d values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

K1/K2

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

K1/K2 actuation 1x per week

$$PFH = \frac{1 - 0,60}{593607,3 * 8760} = 7,69E - 11$$

K1/K2 actuation 1x per shift

$$PFH = \frac{1 - 0,90}{593607,3 * 8760} = 1,92E - 11$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10d values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely

determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E-11 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{7,96E-11 + 7,96E-11}{2} = 3,42E-09$$

in the case of actuation 1x per week

or

$$PFH_{ges} = 2,5E-11 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-11 + 1,92E-11}{2} = 3,42E-09$$

in the case of actuation 1x per shift

The MTTF_D value for block 1 (based on the same assumption) is calculated with:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E-06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{60\%}{593607,3y} + \frac{60\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,96\%$$

or:

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,99\%$$

⚠ CAUTION**Measures for attaining category 3!**

This structure is possible up to category 3 at the most, since an error in the feedback path of the relays may be undiscovered. In order to achieve category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation!

⚠ CAUTION**Implement a restart lock in the machine!**

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

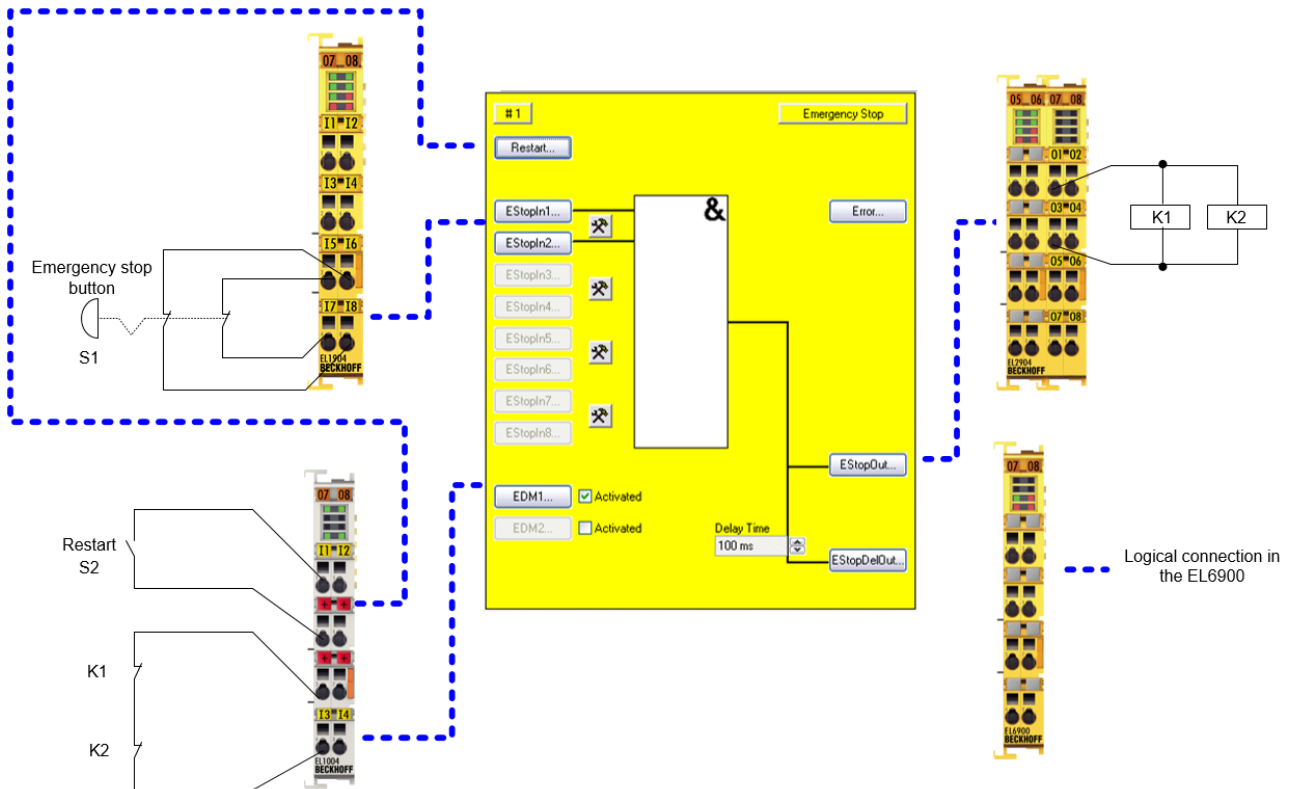
NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.2 ESTOP function variant 2 (category 3, PL d)

The emergency stop button is connected via two normally closed contacts to an EL1904 safe input terminal. The testing of the two signals is activated. The signals are **not** tested for discrepancy. The restart and the feedback signal are wired to standard terminals and are transferred to TwinSAFE via the standard PLC. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



2.2.1 Parameters of the safe input and output terminals

EL1904

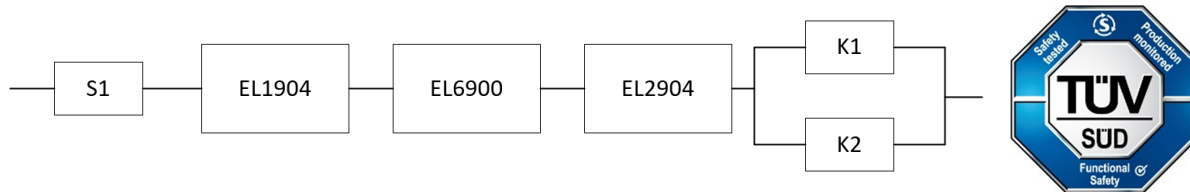
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

2.2.2 Block formation and safety loops

2.2.2.1 Safety function 1



2.2.3 Calculation

2.2.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.2.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing / without plausibility	DC _{avg} =90%
K1/K2 with testing and EDM (actuation 1x per week)	DC _{avg} =60%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =90%

2.2.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,90}{45662,1 * 8760} = 2,50E - 10$$

K1/K2: actuation 1x per week

$$PFH = \frac{1 - 0,60}{593607,3 * 8760} = 7,69E - 11$$

K1/K2: actuation 1x per shift

$$PFH = \frac{1 - 0,90}{593607,3 * 8760} = 1,92E - 11$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 10 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{7,96E - 11 + 7,96E - 11}{2} = 3,65E - 09$$

in the case of actuation 1x per week

or

$$PFH_{ges} = 2,5E - 10 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 11 + 1,92E - 11}{2} = 3,65E - 09$$

in the case of actuation 1x per shift

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{60\%}{593607,3y} + \frac{60\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,89\%$$

or:

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,92\%$$

⚠ CAUTION**Measures for attaining category 3!**

This structure is possible only up to category 3 at the most on account of a possible sleeping error. In order to achieve category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation.

⚠ CAUTION**Implement a restart lock in the machine!**

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE**Diagnostic coverage**

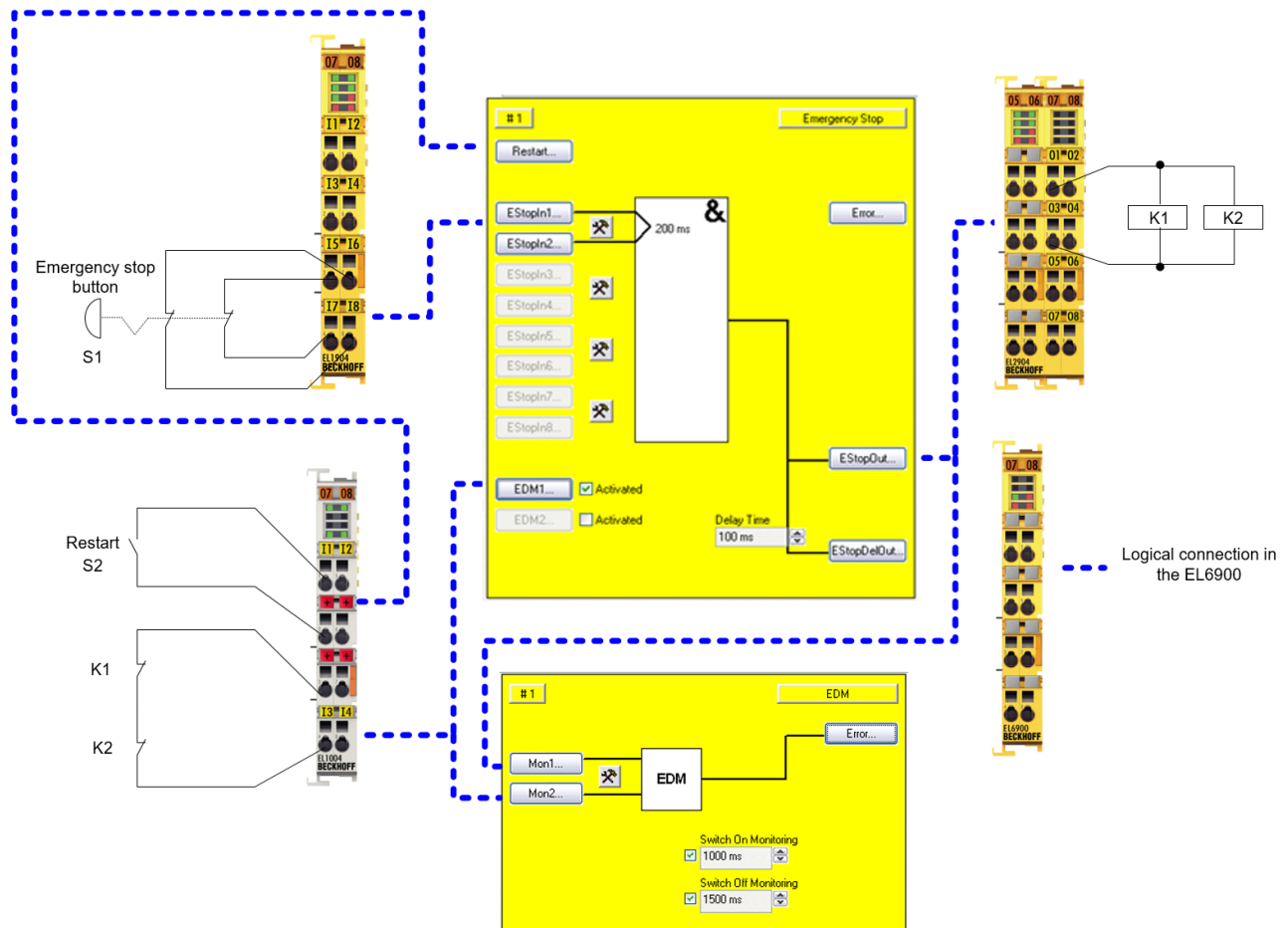
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.3 ESTOP function variant 3 (category 4, PL e)

The emergency stop button is connected via two normally closed contacts to an EL1904 safe input terminal. The testing of the two signals is activated. These signals are checked for discrepancy. The restart and the feedback signal are wired to standard terminals and are transferred to TwinSAFE via the standard PLC. Furthermore, the output of the ESTOP function block and the feedback signal are wired to an EDM function block. This checks that the feedback signal assumes the opposing state of the ESTOP output within the set time.

The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



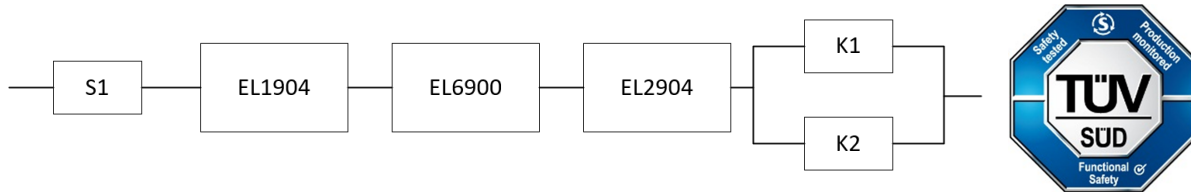
2.3.1 Parameters of the safe input and output terminals

EL1904

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

2.3.2 Block formation and safety loops**2.3.2.1 Safety function 1****2.3.3 Calculation****2.3.3.1 PFHD / MTTFD / B10D – values**

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.3.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM (actuation 1x per week)	DC _{avg} =90%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =99%

2.3.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

K1/K2: actuation 1x per week

$$PFH = \frac{1 - 0,90}{593607,3 * 8760} = 1,92E - 11$$

K1/K2: actuation 1x per shift

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10d values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 11 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 11 + 1,92E - 11}{2} = 3,42E - 09$$

in the case of actuation 1x per week

or

$$PFH_{ges} = 2,5E - 11 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} = 3,42E - 09$$

in the case of actuation 1x per shift

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,99\%$$

or:

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 99,00\%$$

⚠ CAUTION

Measures for attaining category 4!

This structure is possible up to category 4 at the most. In order to attain category 4, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation!

⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

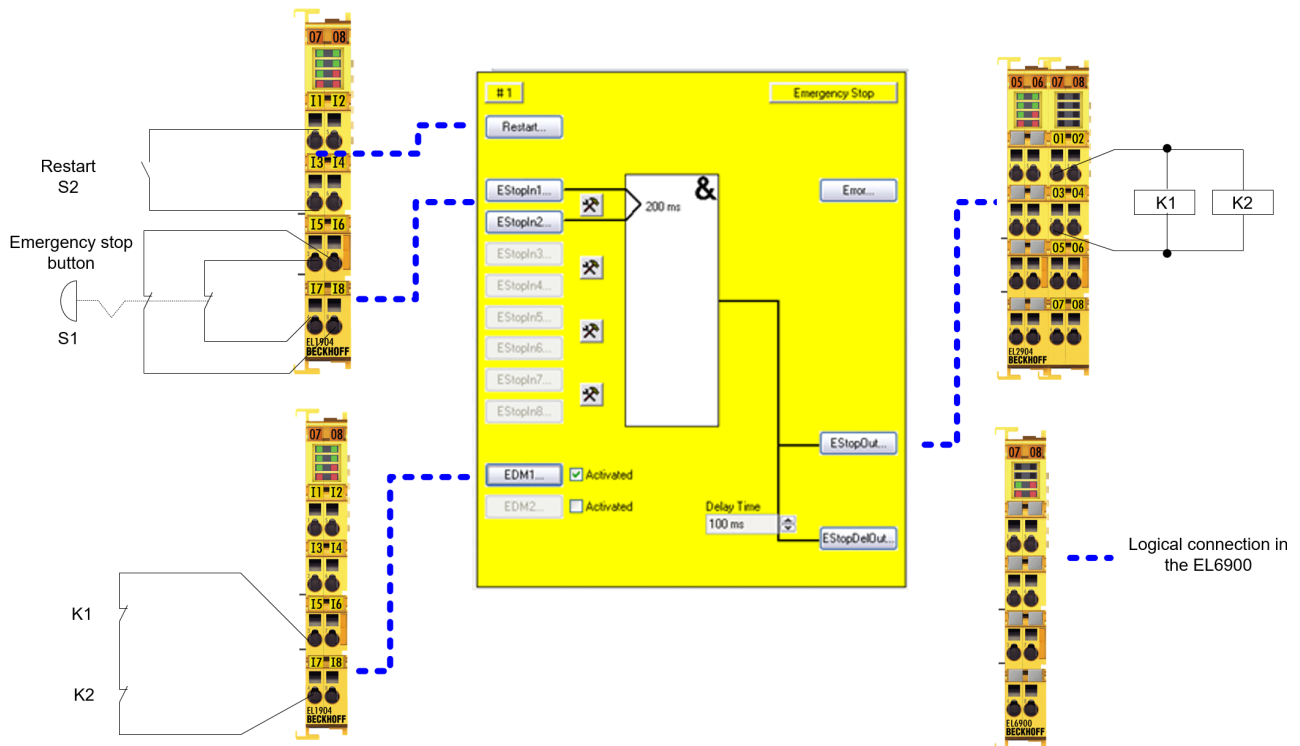
Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.4 ESTOP function variant 4 (category 4, PL e)

The emergency stop button with two normally closed contacts, the restart and the feedback loop are connected to safe channels of an EL1904 input terminal. The testing of the signals is activated. The two emergency stop signals are tested for discrepancy. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



2.4.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

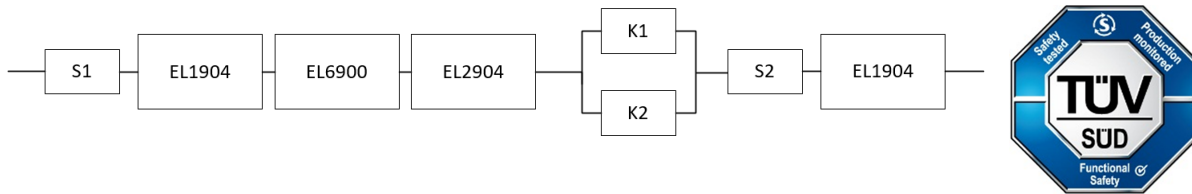
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

2.4.2 Block formation and safety loops

2.4.2.1 Safety function 1



2.4.3 Calculation

2.4.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.4.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
S2 with plausibility	DC _{avg} =90%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =99%

2.4.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{10.000.000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

S2:

$$PFH = \frac{1 - 0,90}{4566210,0 * 8760} = 2,50E - 12$$

K1/K2: actuation 1x per shift

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the $B10_D$ values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 \\ + PFH_{(S2)} + PFH_{(EL1904)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 11 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} + 2,5E - 12 + 1,11E - 09 = 4,53E - 09$$

in the case of actuation 1x per shift

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,99\%$$

or:

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 99,00\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC

Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

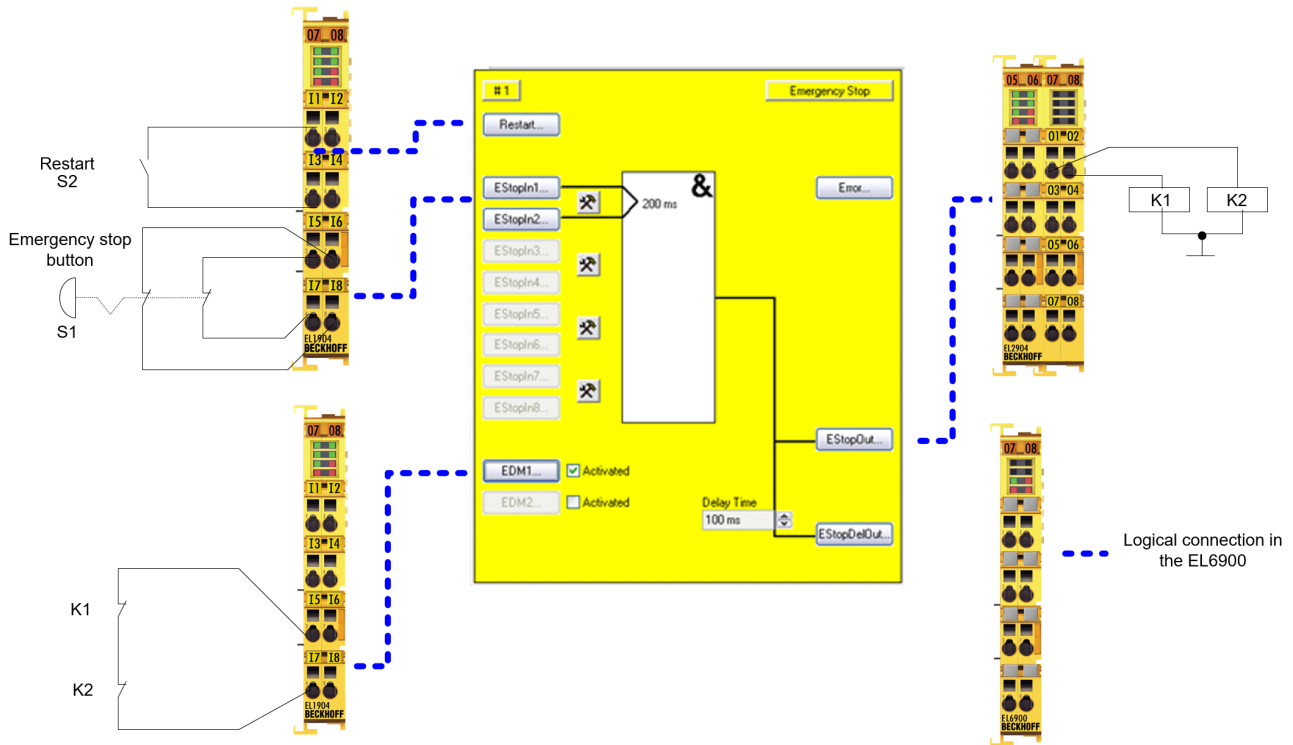
NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.5 ESTOP function variant 5 (category 4, PL e)

The emergency stop button with two normally closed contacts, the restart and the feedback loop are connected to safe channels of an EL1904 input terminal. The testing of the signals is activated. The two emergency stop signals are tested for discrepancy. Contactors K1 and K2 are wired to different output channels. The A2 connections of the two contactors are fed together to ground. The current measurement of the output channels is deactivated for this circuit. The testing of the outputs is active.



2.5.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

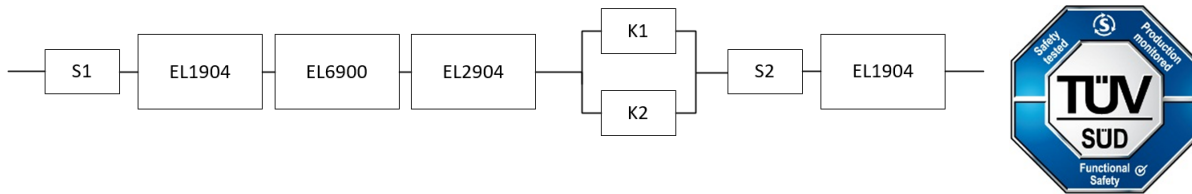
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

2.5.2 Block formation and safety loops

2.5.2.1 Safety function 1



2.5.3 Calculation

2.5.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.5.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
S2 with plausibility	DC _{avg} =90%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =99%

2.5.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_d values from the B10_d values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{10.000.000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

S2:

$$PFH = \frac{1 - 0,90}{4566210,0 * 8760} = 2,50E - 12$$

K1/K2: actuation 1x per shift

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10d values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 \\ + PFH_{(S2)} + PFH_{(EL1904)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 11 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} + 2,5E - 12 + 1,11E - 09 = 4,53E - 09$$

in the case of actuation 1x per shift

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,99\%$$

or:

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 99,00\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC

Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

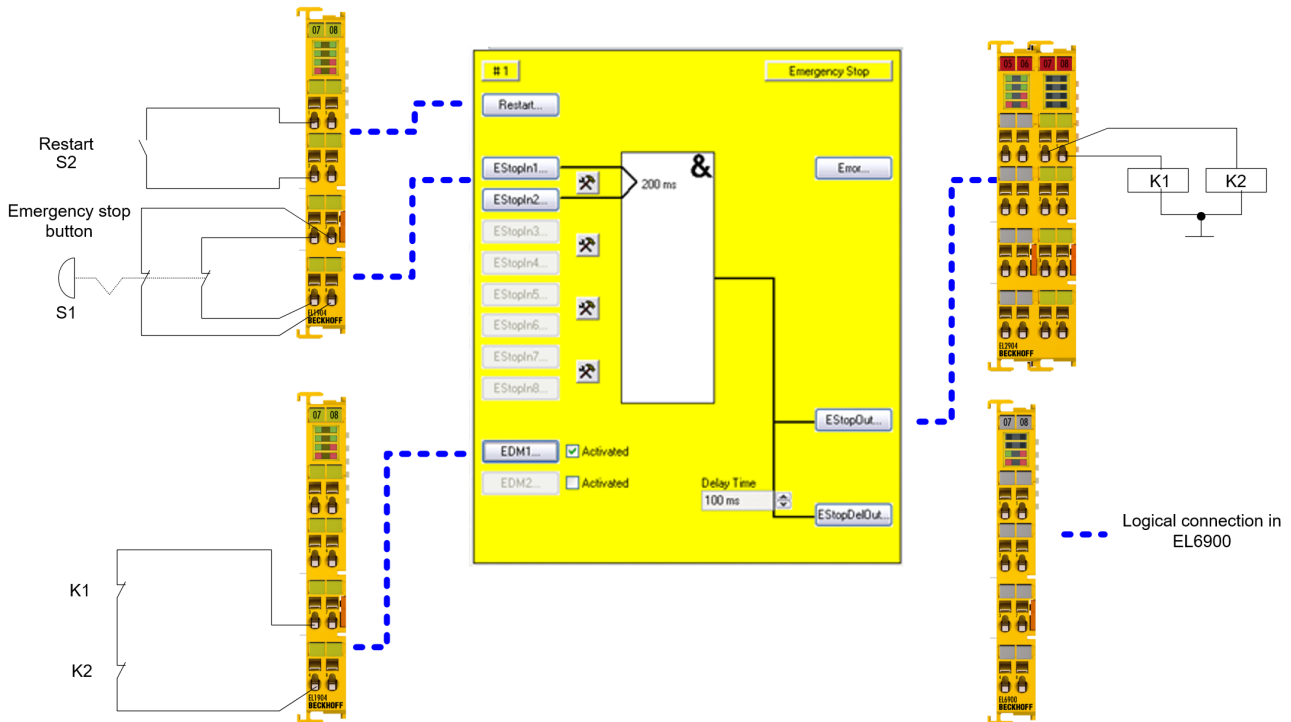
NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.6 ESTOP function variant 6 (category 3, PL d)

The emergency stop button with two normally closed contacts, the restart and the feedback loop are connected to safe channels of an EL1904 input terminal. The testing of the signals is activated. The two emergency stop signals are tested for discrepancy. Contactors K1 and K2 are wired to different output channels. The A2 connections of the two contactors are fed together to ground. The current measurement of the output channels is deactivated for this circuit. The testing of the outputs is not active.



⚠ CAUTION

Category

This structure is possible only up to category 3 at the most on account of a possible sleeping error. Since the EL2904 terminal has only SIL2 in this application, the entire chain has only SIL2!

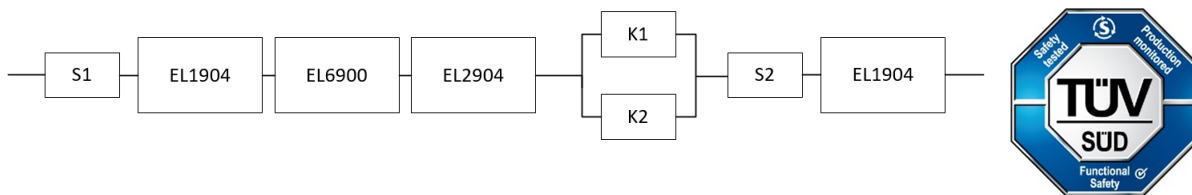
2.6.1 Parameters of the safe input and output terminals (SIL 2)

EL1904 (applies to all EL1904 used)

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	No

2.6.2 Block formation and safety loops**2.6.2.1 Safety function 1****2.6.3 Calculation****2.6.3.1 PFHD / MTTFD / B10D – values**

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.6.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
S2 with plausibility	DC _{avg} =90%
K1/K2 without testing and with EDM via a safe input	DC _{avg} =90%

2.6.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{10.000.000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

S2:

$$PFH = \frac{1 - 0,90}{4566210,0 * 8760} = 2,50E - 12$$

K1/K2: actuation 1x per shift

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 11 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} + 2,5E - 12 + 1,11E - 09 = 4,53E - 09$$

in the case of actuation 1x per shift

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,99\%$$

⚠ CAUTION**Category**

This structure is possible only up to category 3 at the most on account of a possible sleeping error.
Since the EL2904 terminal has only SIL2 in this application, the entire chain has only SIL2!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

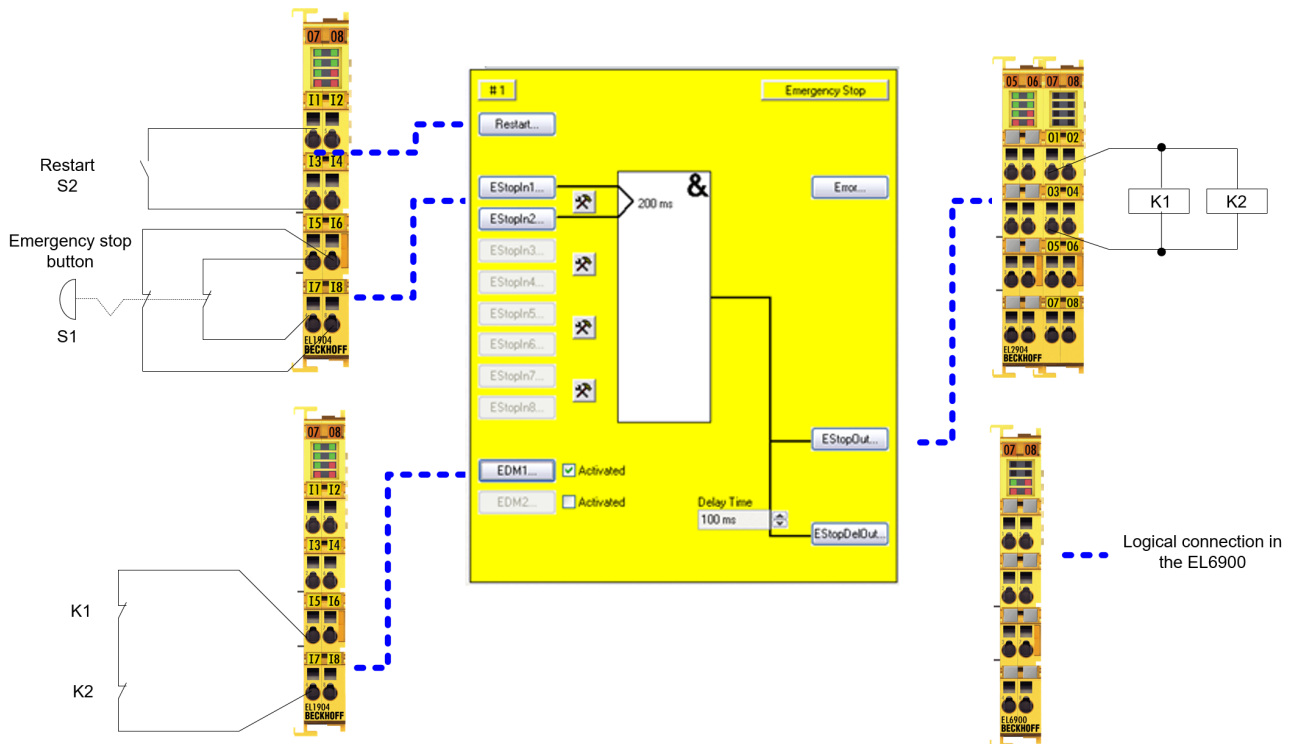
NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.7 ESTOP function variant 7 (category 4, PL e)

The emergency stop button with two normally closed contacts, the restart and the feedback loop are connected to safe channels of an EL1904 input terminal. The testing of the emergency stop button is deactivated on both channels. The sensor test is activated for the restart button and the feedback loop. The two emergency stop signals are tested for discrepancy. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



2.7.1 Parameters of the safe input and output terminals

1. EL1904

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	not used
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

2. EL1904

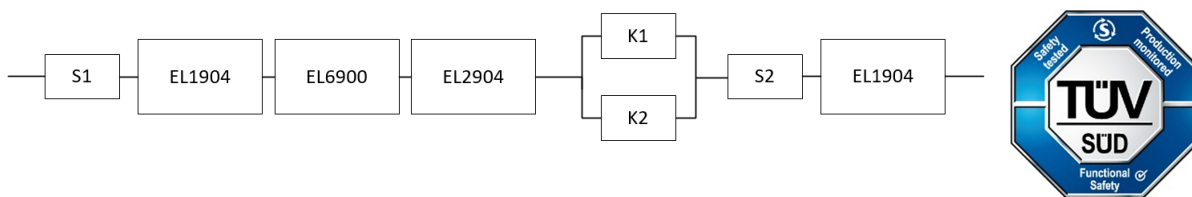
Parameter	Value
Sensor test channel 1 active	not used
Sensor test channel 2 active	not used
Sensor test channel 3 active	Yes
Sensor test channel 4 active	not used
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

2.7.2 Block formation and safety loops

2.7.2.1 Safety function 1



2.7.3 Calculation

2.7.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.7.3.2 Diagnostic Coverage DC

Component	Value
S1 with plausibility	DC _{avg} =90%
S2 with testing	DC _{avg} =90%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =99%

2.7.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{10.000.000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,90}{45662,1 * 8760} = 2,50E - 10$$

S2:

$$PFH = \frac{1 - 0,90}{4566210,0 * 8760} = 2,50E - 12$$

K1/K2: actuation 1x per shift

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the $B10_D$ values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 \\ + PFH_{(S2)} + PFH_{(EL1904)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 10 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} + 2,5E - 12 + 1,11E - 09 = 4,75E - 09$$

in the case of actuation 1x per shift

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 * \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 * \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,94\%$$

or:

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,95\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC

Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

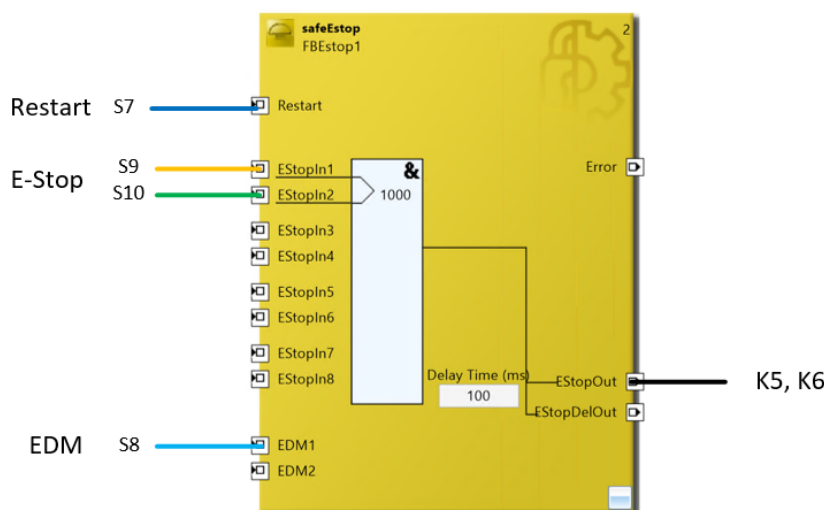
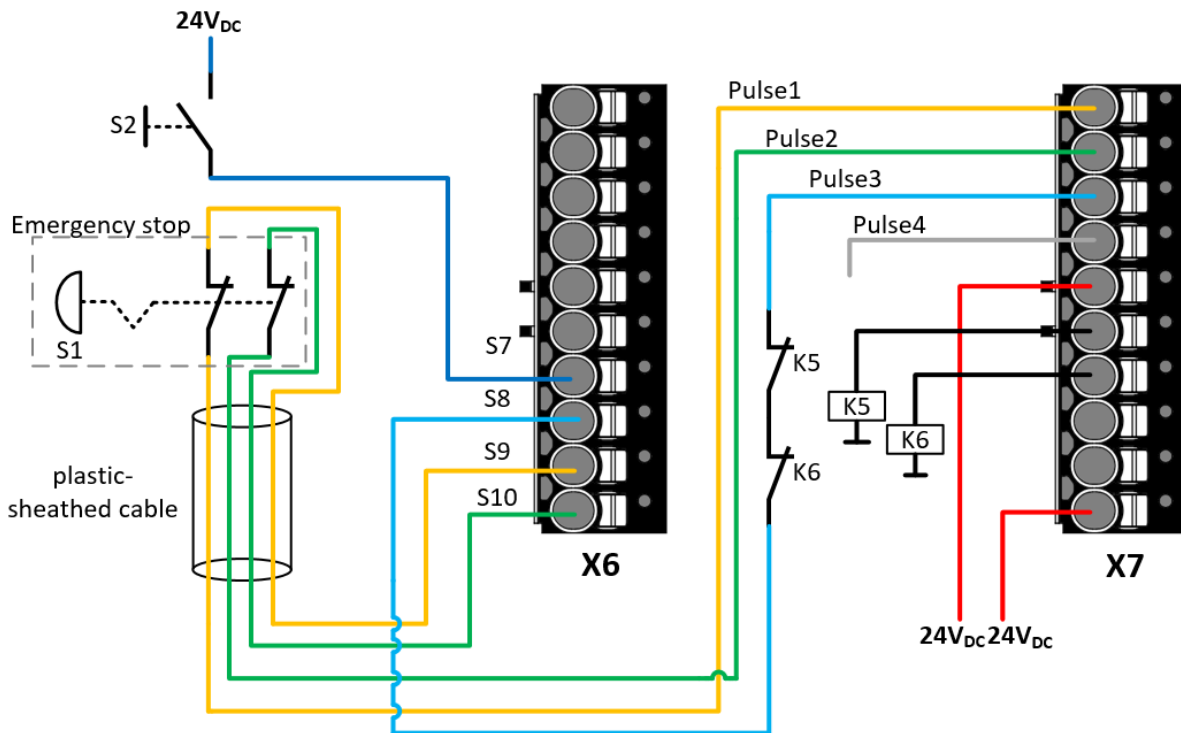
Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

2.8 EK1960 digital inputs and outputs (category 4, PL e)

The emergency stop button S1 is wired with two normally closed contacts to safe inputs S9 and S10 on the 10-pole X6 connector. The first output group on the 10-pole X7 connector is configured as a clock source (for FSOUT module 3, the parameter *Diag TestPulse for Inputs active* is set to TRUE). For inputs S9 and S10, the parameter *Channel x.Test pulse Diag Mode* is configured based on the corresponding clock sources.

Contactors K5 and K6 are wired to outputs 7.5 and 7.6 on the second output module on X7. Terminal A2 of the contactors is wired to the common ground of the 24 V_{DC} supply of terminal X7. The feedback loops of the two contactors are wired in series from pulse 3 to input S8.

Restart S2 is wired to safe input S7 without testing. A restart option must be available for the application, although this is not included in the calculation.



2.8.1 Parameters of the safe input and output modules

EK1960

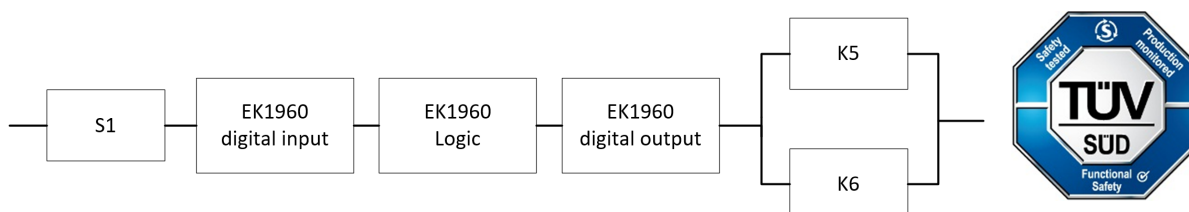
Parameter	Value
FSOUT module 3 (X7.1 – X7.4)	-
8020:01 ModuloDiagTestPulse	0x00
8020:02 MultiplierDiagTestPulse	0x02
8020:03 Standard Outputs active	FALSE
8020:04 Diag Testpulse active	TRUE
8020:05 Diag Testpulse for Inputs active	TRUE
FSOUT Module 4 (X7.5 – X7.8)	-
8030:01 ModuloDiagTestPulse	0x00
8030:02 MultiplierDiagTestPulse	0x02
8030:03 Standard Outputs active	FALSE
8030:04 Diag Testpulse active	TRUE
8030:05 Diag Testpulse for Inputs active	FALSE
FSIN Module 4	-
80A1:04 Channel 2.InputFilterTime	0x000C
80A1:05 Channel 2.DiagTestPulseFilterTime	0x0002
80A1:06 Channel 2.Testpulse Diag Mode	(X7.3) Testpulse Detection Output Module 3.Channel 3
FSIN Module 5	-
80B1:01 Channel 1.InputFilterTime	0x000C
80B1:02 Channel 1.DiagTestPulseFilterTime	0x0002
80B1:03 Channel 1.Testpulse Diag Mode	(X7.1) Testpulse Detection Output Module 3.Channel 1
80B1:04 Channel 2.InputFilterTime	0x000C
80B1:05 Channel 2.DiagTestPulseFilterTime	0x0002
80B1:06 Channel 2.Testpulse Diag Mode	(X7.2) Testpulse Detection Output Module 3.Channel 2

ESTOP FB Parameter

Parameter	Value
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (Port EStopIn1/EStopIn2)	1000
Safe Inputs After Disc Error	TRUE

2.8.2 Block formation and safety loops

2.8.2.1 Safety function 1



2.8.3 Calculation

2.8.3.1 PFHD / MTTF_D / B10_D – values

Component	Value
EK1960 digital input – PFH _D	6.40E-11
EK1960 safety mat input - PFH _D	8.84E-10
EK1960 logic – PFH _D	5.18E-09
EK1960 digital output – PFH _D	1.50E-10
EK1960 relay output (cat. 4, two-channel) - PFH _D	1.46E-09 (actuation 1x per hour)
EK1960 relay – B10 _D	1,500,000 (DC13 24 V _{DC} and I _{max} ≤ 2 A)
S1 – B10 _D	100,000
K5 – B10 _D	1,300,000
K6 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

● Safety-over-EtherCAT communication

i The PFH_D value of the Safety-over-EtherCAT (FSoE) communication is included in the PFH_D value of the EK1960 logic component.

2.8.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing and plausibility check	DC _{avg} =99%
K5/K6 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with temporal monitoring) with testing	DC _{avg} =99%

2.8.3.3 Calculation of safety function 1

Calculation of the performance level according to EN ISO 13849-1:2015

Calculation of the MTTF_D values from the B10_D values

From:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662y$$

K5/K6

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607y$$

The total $MTTF_D$ value is calculated based on the following formula:

$$\frac{1}{MTTF_{D_{ges}}} = \sum_{i=1}^n \frac{1}{MTTF_{D_n}}$$

as:

$$\frac{1}{MTTF_{D_{ges}}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EK1960-Input)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Output)}} + \frac{1}{MTTF_{D(K5)}}$$

If only PFH_D values are available for EL1960 components, the following estimation applies:

$$MTTF_{D(EK1960-xxx)} = \frac{(1 - DC_{(EK1960-xxx)})}{PFH_{(EK1960-xxx)}}$$

Hence:

$$MTTF_{D(EK1960-Input)} = \frac{(1 - DC_{(EK1960-Input)})}{PFH_{D(EK1960-Input)}} = \frac{(1 - 0,99)}{6,40E - 11 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{5,60E - 07 \frac{1}{y}} = 17836y$$

$$MTTF_{D(EK1960-Logic)} = \frac{(1 - DC_{(EK1960-Logic)})}{PFH_{D(EK1960-Logic)}} = \frac{(1 - 0,99)}{5,18E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{4,54E - 05 \frac{1}{y}} = 220y$$

$$MTTF_{D(EK1960-Output)} = \frac{(1 - DC_{(EK1960-Output)})}{PFH_{D(EK1960-Output)}} = \frac{(1 - 0,99)}{1,50E - 10 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,31E - 06 \frac{1}{y}} = 7610y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{593607y}} = 210y$$

$$DC_{avg} = \frac{\frac{99\%}{45662y} + \frac{99\%}{17836y} + \frac{99\%}{220y} + \frac{99\%}{7610y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

NOTE

Category
 This structure is possible up to category 4 at the most.

⚠ CAUTION

Implement a restart lock in the machine!
 The restart lock is **NOT** part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Calculation of PFH_D values according to EN 62061

assuming that S1, K5 and K6 are single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH_D = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH_D = \frac{1 - 0,99}{45662 * 8760} = 2,50E - 11$$

K5/K6:

$$PFH_D = \frac{1 - 0,99}{593607 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100,000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K5 and K6 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K5 and K6 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{D_{ges}} = PFH_{D(S1)} + PFH_{D(EK1960-Input)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Output)} \\ + \beta * \frac{PFH_{D(K5)} + PFH_{D(K6)}}{2} + (1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{D_{ges}} = 2,5E - 11 + 6,40E - 11 + 5,18E - 09 + 1,50E - 10 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 5,42E - 09$$

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

NOTE

Safety integrity level

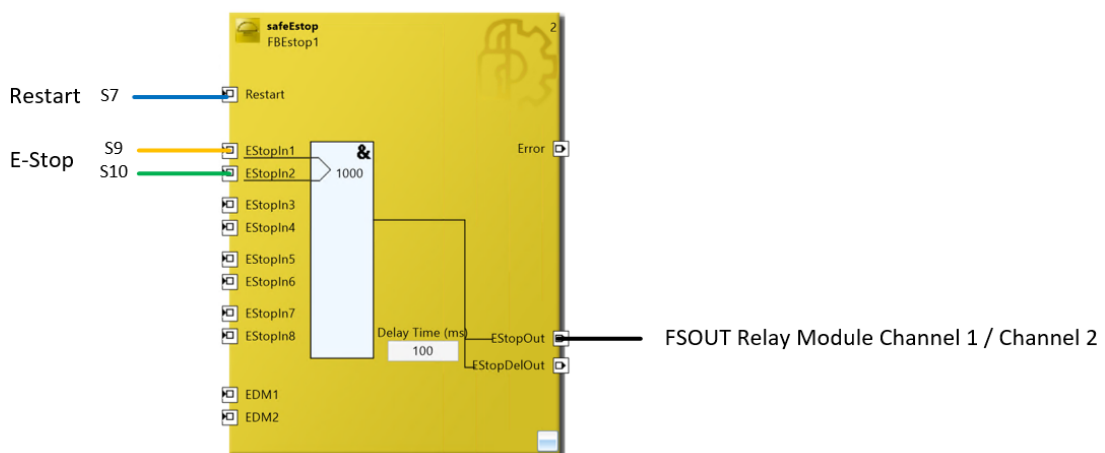
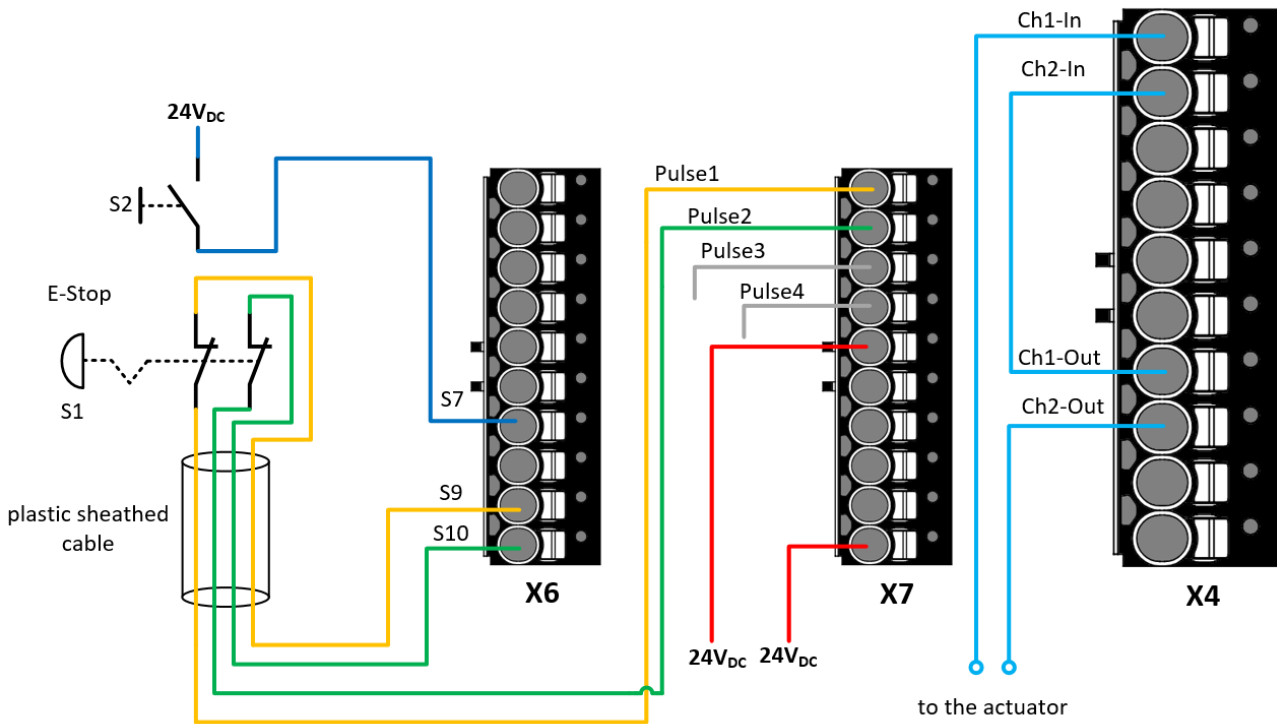
The application meets the requirements of safety integrity level SIL3 according to EN 62061.

2.9 EK1960 digital inputs / relay outputs (category 4, PL e)

The emergency stop button S1 is wired with two normally closed contacts to safe inputs S9 and S10 on the 10-pole X6 connector. The first output group on the 10-pole X7 connector is configured as a clock source (for FSOUT module 3, the parameter *Diag TestPulse for Inputs active* is set to TRUE). For inputs S9 and S10, the parameter *Channel x.Test pulse Diag Mode* is configured based on the corresponding clock sources.

The relay outputs Channel 1 and Channel 2 are connected in series and can then be used for safety-related functions (e.g. to transmit an emergency stop message to an upstream or downstream machine). The EDM is not wired to the ESTOP input, because the relay module performs the EDM monitoring, and in case of an error it reports a module error for the relay module. The application can then respond to this module error, or the TwinSAFE group can be configured such that a module error leads to a Com error.

Restart S2 is wired to safe input S7 without testing. A restart option must be available for the application, although this is not included in the calculation.



2.9.1 Parameters of the safe input and output modules

EK1960

Parameter	Value
FSOUT module 3 (X7.1 – X7.4)	-
8020:01 ModuloDiagTestPulse	0x00
8020:02 MultiplierDiagTestPulse	0x02
8020:03 Standard Outputs active	FALSE
8020:04 Diag Testpulse active	TRUE
8020:05 Diag Testpulse for Inputs active	TRUE
FSOUT relay module	-
8060:03 Standard Outputs active	FALSE
FSIN Module 5	-
80B1:01 Channel 1.InputFilterTime	0x000C
80B1:02 Channel 1.DiagTestPulseFilterTime	0x0002
80B1:03 Channel 1.Testpulse Diag Mode	(X7.1) Testpulse Detection Output Module 3.Channel 1
80B1:04 Channel 2.InputFilterTime	0x000C
80B1:05 Channel 2.DiagTestPulseFilterTime	0x0002
80B1:06 Channel 2.Testpulse Diag Mode	(X7.2) Testpulse Detection Output Module 3.Channel 2

ESTOP FB Parameter

Parameter	Value
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (Port EStopIn1/EStopIn2)	1000
Safe Inputs After Disc Error	TRUE

NOTE

Module error in the relay module

In case of an EDM error, a module error of the relay module is reported. This module then enters the safe, switched-off state. The error acknowledgement can take place via the signal *FSOUT Relais Module.Err Ack*.

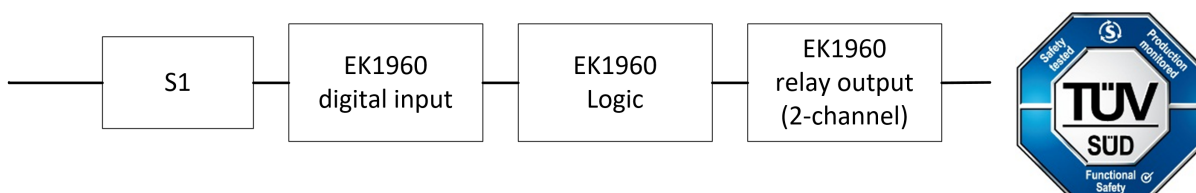
NOTE

Switching frequency

To achieve PL e, the relay outputs must be activated at least once per month. This example assumes a switching frequency of 1x per week.

2.9.2 Block formation and safety loops

2.9.2.1 Safety function 1



2.9.3 Calculation

2.9.3.1 PFHD / MTTF_D / B10_D – values

Component	Value
EK1960 digital input – PFH _D	6.40E-11
EK1960 safety mat input - PFH _D	8.84E-10
EK1960 logic – PFH _D	5.18E-09
EK1960 digital output – PFH _D	1.50E-10
EK1960 relay output (cat. 4, two-channel) - PFH _D	1.46E-09 (actuation 1x per hour)
EK1960 relay – B10 _D	1,500,000 (DC13 24 V _{DC} and I _{max} ≤ 2 A)
S1 – B10 _D	100,000
K5 – B10 _D	1,300,000
K6 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

i Safety-over-EtherCAT communication

The PFH_D value of the Safety-over-EtherCAT (FSoE) communication is included in the PFH_D value of the EK1960 logic component.

2.9.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing and plausibility check	DC _{avg} =99%
Two-channel relay output with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges) with testing	DC _{avg} =99%

2.9.3.3 Calculation of safety function 1

Calculation of the performance level according to EN ISO 13849-1:2015:

Calculation of the MTTF_D values from the B10_D values.

From:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662y$$

Relay

Both $B10_D$ and PFH_D values are specified for the relay. In this case, the inferior of the two values is used to calculate the $MTTF_D$ value (in this case the PFH_D value – see below).

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.500.000}{0,1 * 21,90} = 684.931y$$

The total $MTTF_D$ value is calculated based on the following formula:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EK1960-Input)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Relay)}}$$

If only PFH_D values are available for EL1960 components, the following estimation applies:

$$MTTF_{D(EK1960-xxx)} = \frac{(1 - DC_{(EK1960-xxx)})}{PFH_{(EK1960-xxx)}}$$

Hence:

$$MTTF_{D(EK1960-Input)} = \frac{(1 - DC_{(EK1960-Input)})}{PFH_{D(EK1960-Input)}} = \frac{(1 - 0,99)}{6,40E - 11 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{5,60E - 07 \frac{1}{y}} = 17836y$$

$$MTTF_{D(EK1960-Logic)} = \frac{(1 - DC_{(EK1960-Logic)})}{PFH_{D(EK1960-Logic)}} = \frac{(1 - 0,99)}{5,18E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{4,54E - 05 \frac{1}{y}} = 220y$$

$$MTTF_{D(EK1960-Relay)} = \frac{(1 - DC_{(EK1960-Relay)})}{PFH_{D(EK1960-Relay)}} = \frac{(1 - 0,99)}{1,46E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,28E - 05 \frac{1}{y}} = 781y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{781y}} = 169y$$

$$DC_{avg} = \frac{\frac{99\%}{45662y} + \frac{99\%}{17836y} + \frac{99\%}{220y} + \frac{99\%}{781y}}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{781y}} = 99,00\%$$

NOTE

Category
 This structure is possible up to category 4 at the most.

⚠ CAUTION

Implement a restart lock in the machine!
 The restart lock is **NOT** part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Calculation of PFH_D values according to EN 62061:

with the assumption that S1 is single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH_D = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH_D = \frac{1 - 0,99}{45662 * 8760} = 2,50E - 11$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100,000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{Dges} = PFH_{D(S1)} + PFH_{D(EK1960-Input)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Relay)}$$

to:

$$PFH_{Dges} = 2,5E - 11 + 6,40E - 11 + 5,18E - 09 + 1,46E - 09 \\ = 6,73E - 09$$

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

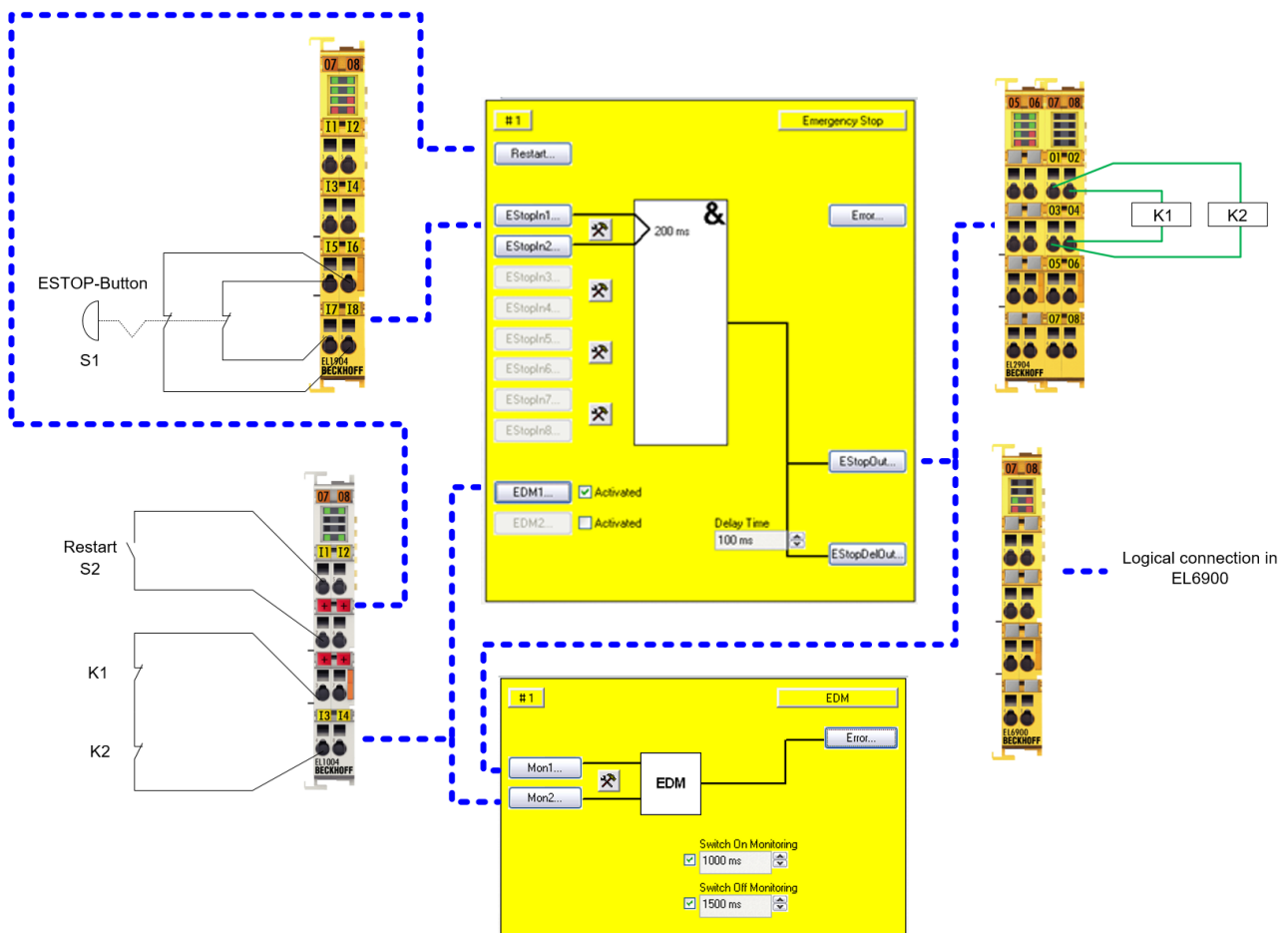
NOTE**Safety integrity level**

The application meets the requirements of safety integrity level SIL3 according to EN 62061.

2.10 ESTOP function (category 3, PL d)

The emergency stop button is connected via two normally closed contacts to an EL1904 safe input terminal. The testing of both signals is switched off. These signals are tested for discrepancy inside the ESTOP function block. The restart and the feedback signal from the contactors K1 and K2 are wired to standard terminals and are transferred to TwinSAFE via the standard PLC. Furthermore, the output of the ESTOP function block and the feedback signal are wired to an EDM function block. This checks that the feedback signal assumes the opposing state of the ESTOP output within the set time.

Contactors K1 and K2 are wired to different output channels. The A2 connections of the two contactors are fed back to the EL2904. The current measurement of the output channels is deactivated for this circuit. The testing of the outputs is similarly inactive.



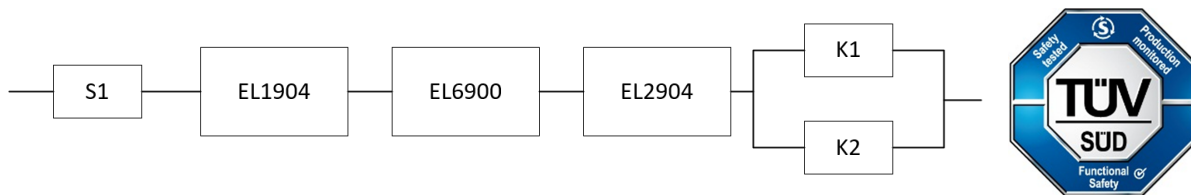
2.10.1 Parameters of the safe input and output terminals (SIL 2)

EL1904 (applies to all EL1904 used)

Parameter	Value
Sensor test channel 1 active	-
Sensor test channel 2 active	-
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	No

2.10.2 Block formation and safety loops**2.10.2.1 Safety function 1****2.10.3 Calculation****2.10.3.1 PFHD / MTTF_D / B10_D – values**

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
S2 – B10 _D	10,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

2.10.3.2 Diagnostic Coverage DC

Component	Value
S1 with plausibility	DC _{avg} =90%
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =90%

2.10.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that S1, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,90}{45662,1 * 8760} = 2,50E - 10$$

K1/K2: Actuation 1x per week and indirect feedback

$$PFH = \frac{1 - 0,90}{593607,3 * 8760} = 1,92E - 11$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,5E - 10 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 11 + 1,92E - 11}{2} = 3,65E - 09$$

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,92\%$$

⚠ CAUTION

Category

This structure is possible only up to category 3 at the most on account of a possible sleeping error. Since the EL2904 terminal has only SIL2 in this application, the entire chain has only SIL2!

⚠ CAUTION

Further measures for attaining Category 3!

This structure is possible up to category 3 at the most. In order to attain category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation! This is achieved via the implemented EDM function block.

⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

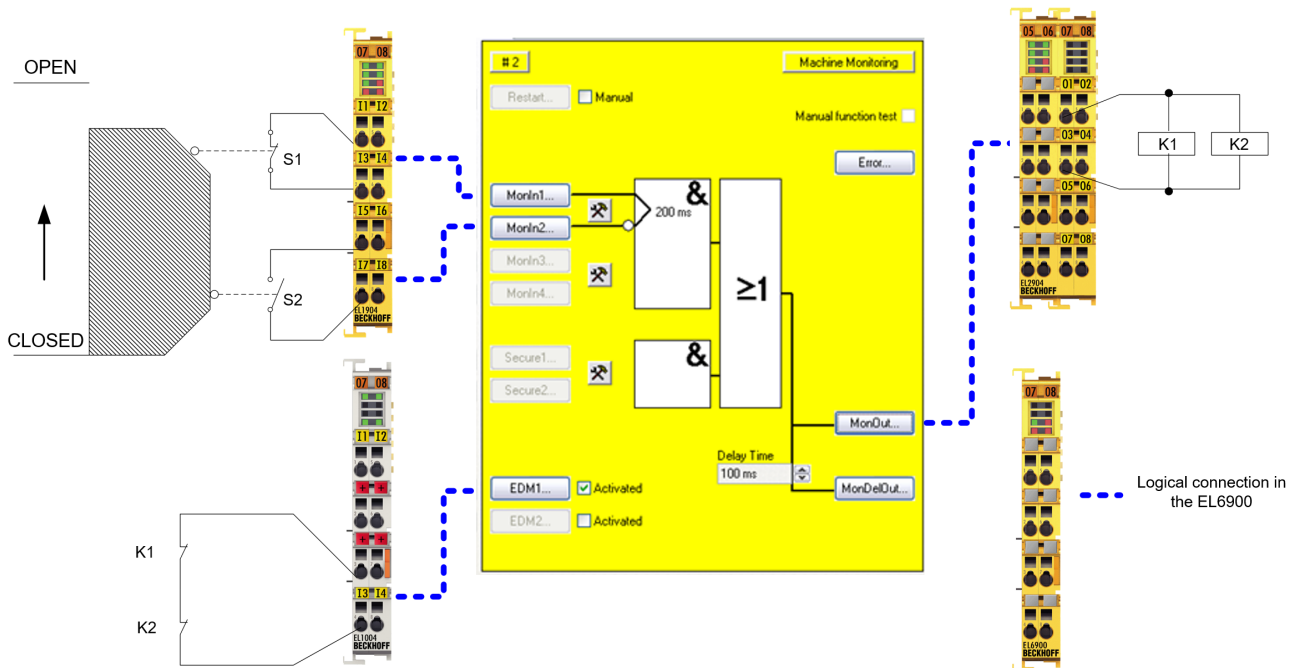
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3 Access functions

3.1 Protective door function variant 1 (category 3, PL d)

The protective door uses a combination of normally closed and normally open contacts on the safe inputs of an EL1904. The testing of the inputs is active and the signals are tested for discrepancy (200 ms). The feedback loop is read in via a standard input and transferred to TwinSAFE via the standard PLC. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.1.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

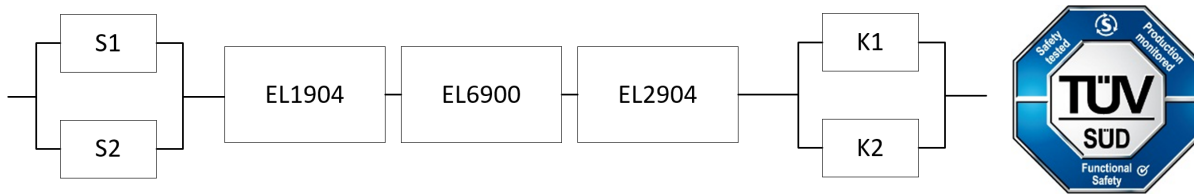
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.1.2 Block formation and safety loops

3.1.2.1 Safety function 1



3.1.3 Calculation

3.1.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

3.1.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =90%

3.1.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1 * 14720} = 679,3y = 5951087h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0,1 * 14720} = 883,2y = 7736413h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{679,3 * 8760} = 1,68E - 09$$

S2:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

K1/K2:

$$PFH = \frac{1 - 0,90}{883,2 * 8760} = 1,29E - 08$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{1,68E - 09 + 1,68E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,29E - 08 + 1,29E - 08}{2} = 4,85E - 09$$

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y}} = 179,4y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{883,2y} + \frac{90\%}{883,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y}} = 96,26\%$$

⚠ CAUTION

Measures for attaining category 3!

This structure is possible only up to category 3 at the most on account of a possible sleeping error. In order to achieve category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

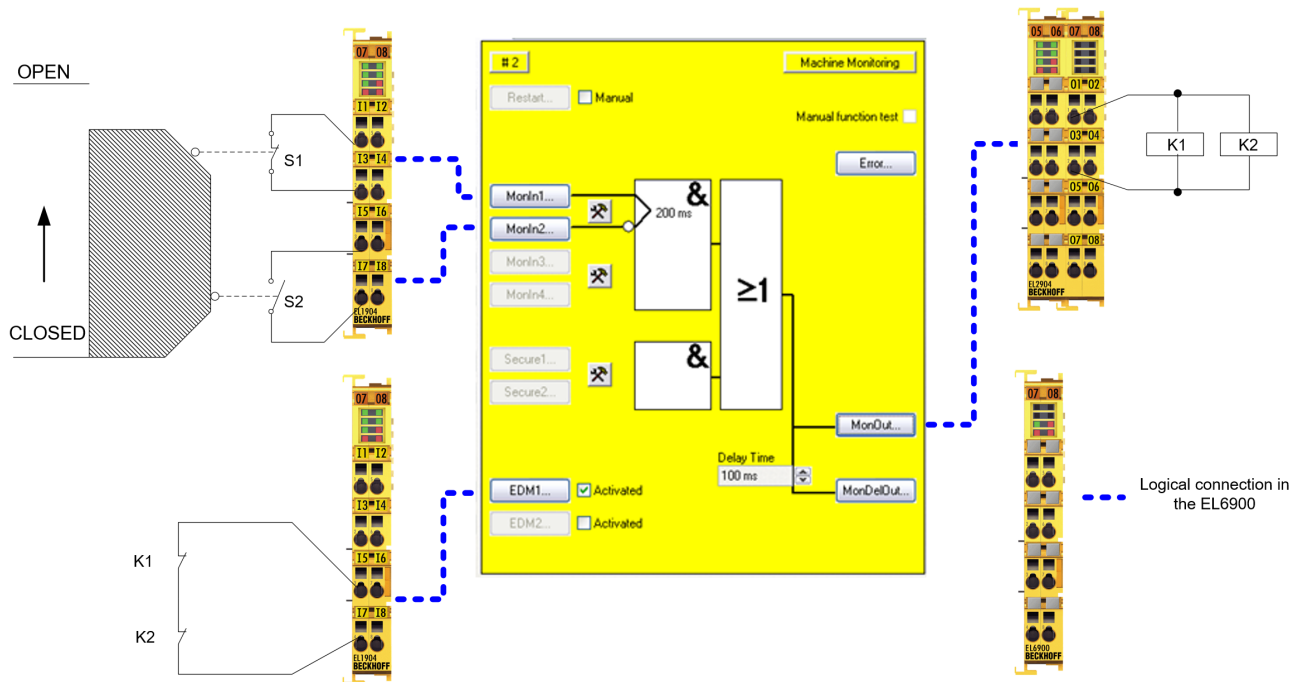
Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.2 Protective door function variant 2 (category 4, PL e)

The protective door uses a combination of normally closed and normally open contacts on the safe inputs of an EL1904. The testing of the inputs is active and the signals are tested for discrepancy (200 ms). The feedback loop is read in via a safe input. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.2.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

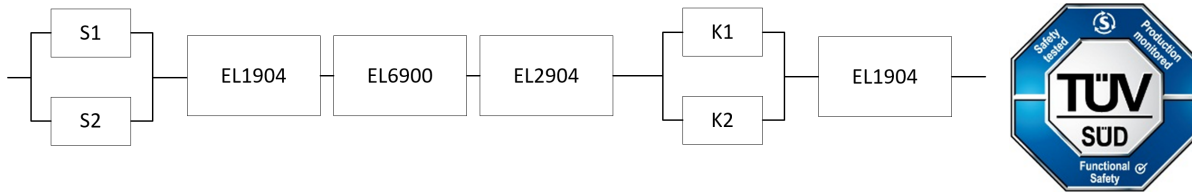
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.2.2 Block formation and safety loops

3.2.2.1 Safety function 1



3.2.3 Calculation

3.2.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

3.2.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%

3.2.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1 * 14720} = 679,3y = 5951087h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0,1 * 14720} = 883,2y = 7736413h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{679,3 * 8760} = 1,68E - 09$$

S2:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

K1/K2:

$$PFH = \frac{1 - 0,99}{883,2 * 8760} = 1,29E - 09$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(EL1904)}$$

Since the portions $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{1,68E - 09 + 1,68E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,29E - 09 + 1,29E - 09}{2} + 1,11E - 09 = 4,80E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(EL1904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{1028,8y}} = 152,7y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{883,2y} + \frac{99\%}{883,2y} + \frac{99\%}{1028,8y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y} + \frac{1}{1028,8y}} = 99,0\%$$

NOTE

Category
 This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

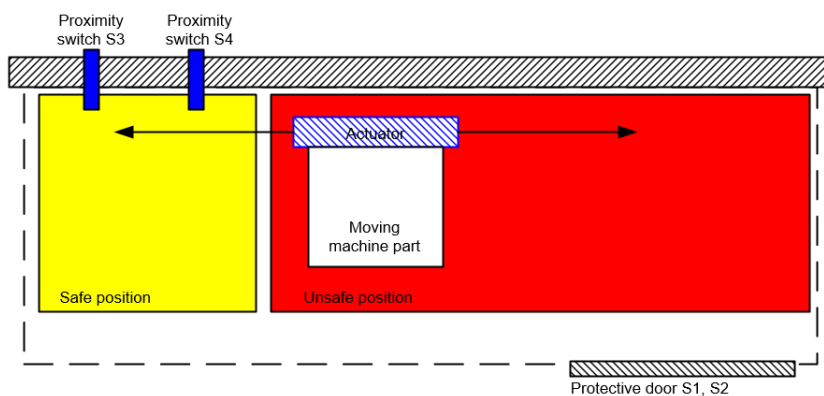
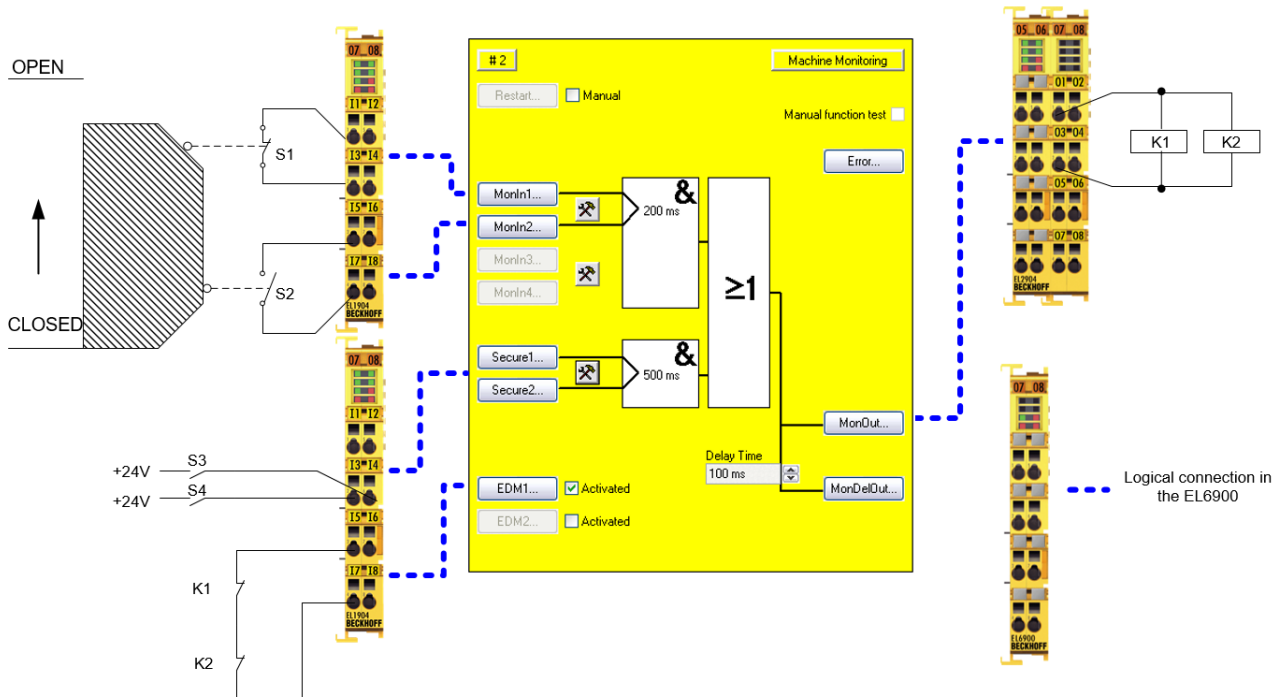
Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.3 Protective door function with range monitoring (Category 4, PL e)

The protective door uses a combination of normally closed and normally open contacts on the safe inputs of an EL1904. The testing of the inputs is active and the signals are tested for discrepancy (200 ms). The feedback loop is read in via a safe input. The proximity sensors S3 and S4 are wired to safe inputs and detect, for example, when a dangerous machine part is in a safe position so that the protective door may be opened when the machine is running. The testing of these inputs is deactivated so that the static 24 V voltage of the sensors can be used.

The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.3.1 Parameters of the safe input and output terminals

EL1904 (upper EL1904 on the drawing)

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL1904 (lower EL1904 on the drawing)

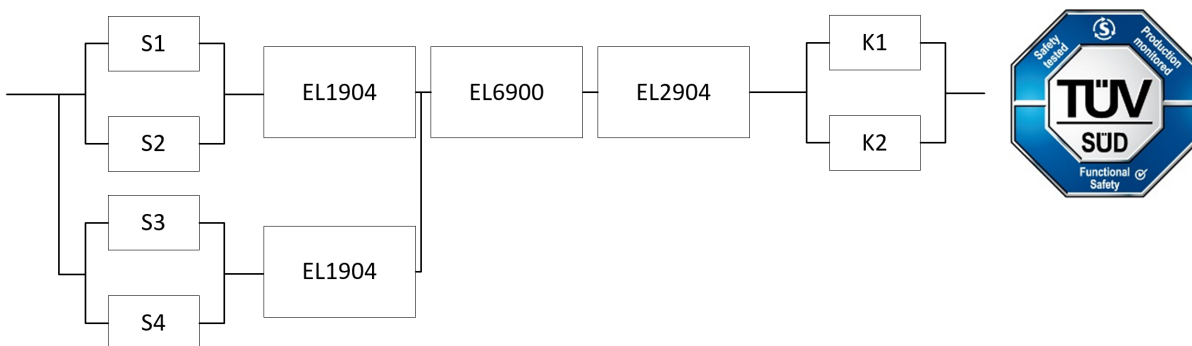
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904 (applies to all EL2904 used)

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.3.2 Block formation and safety loops

3.3.2.1 Safety function 1



3.3.3 Calculation

3.3.3.1 PFHD / MTTF_D / B10_D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
S3 – B10 _D	20,000,000
S4 – B10 _D	20,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

3.3.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
S3/S4 with without testing / with plausibility	DC _{avg} =90%
K1/K2 with testing and EDM	DC _{avg} =99%

3.3.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1 * 14720} = 679,3y = 5951087h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

S3:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{20.000.000}{0,1 * 14720} = 13586,9y = 119021739h$$

S4:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{20.000.000}{0,1 * 14720} = 13586,9y = 119021739h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0,1 * 14720} = 883,2y = 7736413h$$

and the assumption that S1, S2, S3, S4, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{679,3 * 8760} = 1,68E - 09$$

S2:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

S3/S4:

$$PFH = \frac{1 - 0,90}{13586,9 * 8760} = 8,4E - 10$$

K1/K2:

$$PFH = \frac{1 - 0,99}{883,2 * 8760} = 1,29E - 09$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

The proximity sensors S3/S4 are monitored for plausibility (temporal/logical) and are type A systems according to EN 61508 (simple components whose behavior under error conditions is fully known). The safe position is driven to once per shift.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the $B10_D$ values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1/S2/EL1904)} + PFH_{(S3/S4/EL1904)}}{2} + (1 - \beta)^2 * (PFH_{(S1/S2/EL1904)} * PFH_{(S3/S4/EL1904)}) * T1 + PFH_{(EL6900)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(S1/S2/EL1904)} * PFH_{(S3/S4/EL1904)}) * T1$ and $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{(S1/S2/EL1904)} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + PFH_{(EL1904)} = 10\% * \frac{1,68E-09 + 8,4E-10}{2} + 1,11E-09 = 1,24E-09$$

$$PFH_{(S3/S4/EL1904)} = \beta * \frac{PFH_{(S3)} + PFH_{(S4)}}{2} + PFH_{(EL1904)} = 10\% * \frac{8,4E-10 + 8,4E-10}{2} + 1,11E-09 = 1,19E-09$$

$$PFH_{ges} = 10\% * \frac{1,24E-09 + 1,19E-09}{2} + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,29E-09 + 1,29E-09}{2} = 2,53E-09$$

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(S3)} = \frac{B10_{D(S3)}}{0,1 * n_{op}}$$

$$MTTF_{D(S4)} = \frac{B10_{D(S4)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y}} = 179,4y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{90\%}{13586,9y} + \frac{90\%}{13586,9y} + \frac{99\%}{1028,8y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{883,2y} + \frac{99\%}{883,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{13586,9y} + \frac{1}{13586,9y} + \frac{1}{1028,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y}} = 98,85\%$$

NOTE

Category

This structure is possible up to category 4 at the most. The monitoring of sensors S3 and S4 must be temporarily and logically programmed.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

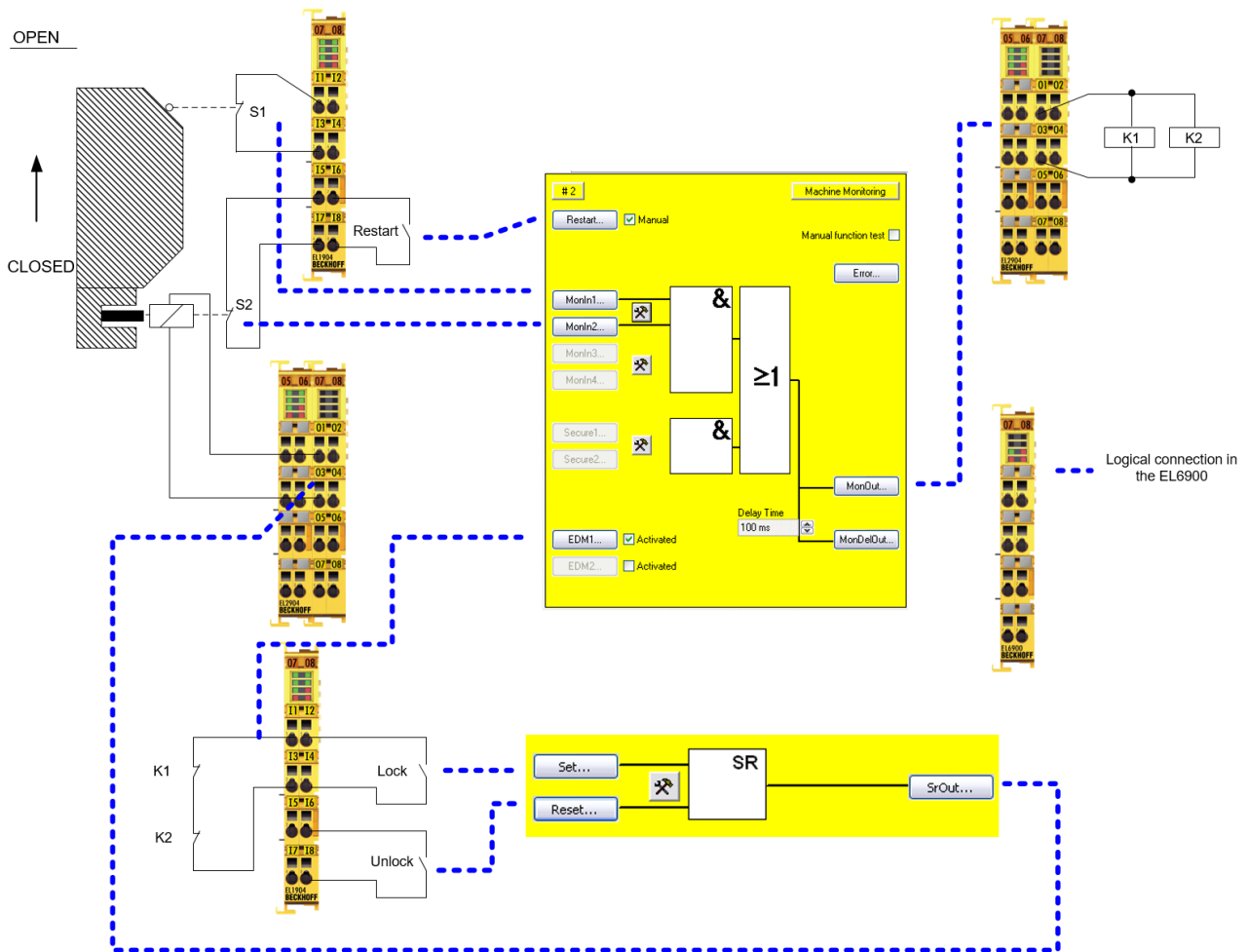
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.4 Protective door function with tumbler (Category 4, PL e)

The protective door has two contacts, S1 'door closed' and S2 'door closed and locked', which are wired to safe inputs of an EL1904. The testing of the inputs is active. Checking of the signals for discrepancy cannot take place, because there is no temporal relationship between the signals. The feedback loop and the restart signal are read in via a safe input. The testing of the inputs is active here also. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.

The tumbler is switched via 2 safe inputs in which testing is active. Testing and current measurement is active on the safe output for the tumbler.



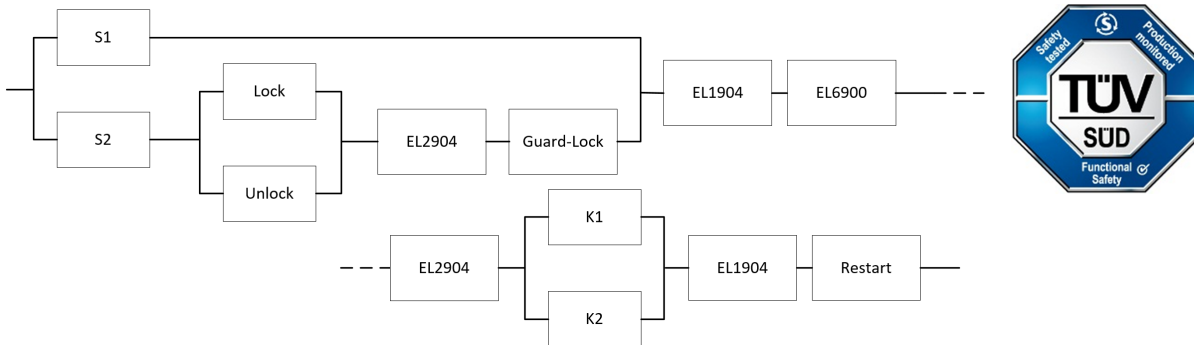
3.4.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904 (applies to all EL2904 used)

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.4.2 Block formation and safety loops**3.4.2.1 Safety function 1****3.4.3 Calculation****3.4.3.1 PFHD / MTTFD / B10D – values**

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	2,000,000
S2 – B10 _D	2,000,000
Restart - B10 _D	10,000,000
Lock – B10 _D	100,000
Unlock – B10 _D	100,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Tumbler (guard lock) - B10 _D	2,000,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

3.4.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing	DC _{avg} =90%
S2 with testing and expectation	DC _{avg} =99%
Lock/unlock with testing/plausibility	DC _{avg} =99%
Restart	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%
Tumbler	DC _{avg} =99%

3.4.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

Lock/Unlock:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{100.000}{0,1 * 14720} = 67,9y = 595108h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0,1 * 14720} = 883,2y = 7736413h$$

Restart:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{10.000.000}{0,1 * 14720} = 6793,5y = 59511060h$$

Tumbler:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

and the assumption that S1, S2, S3, S4, K1, K2 and the tumbler are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,90}{1358,7 * 8760} = 8,40E - 09$$

S2:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

Lock/Unlock:

$$PFH = \frac{1 - 0,99}{67,9 * 8760} = 1,68E - 08$$

Restart:

$$PFH = \frac{1 - 0,90}{6793,5 * 8760} = 1,68E - 09$$

K1/K2:

$$PFH = \frac{1 - 0,99}{883,2 * 8760} = 1,29E - 09$$

Tumbler:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

The following assumptions must now be made:

The door switches S1/S2 must both be actuated. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The tumbler is mechanically connected to the switch S2 in such a way that a separation of the coupling is impossible.

The restart is monitored, so that a signal change is only valid once the door is closed.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S2/Lock/Unlock/EL2904/GuardLock)} + PFH_{(S1)}}{2} + (1 - \beta)^2 * (PFH_{(S2/Lock/Unlock/EL2904/GuardLock)} * PFH_{(S1)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(EL1904)} + PFH_{(Restart)}$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{(S2//Lock/Unlock/EL2904/GuardLock)} = PFH_{(S2)} + \beta * \frac{PFH_{(Lock)} + PFH_{(Unlock)}}{2} + PFH_{(EL2904)} + PFH_{(GuardLock)}$$

$$= 8,4E - 10 + 10\% * \frac{1,68E - 08 + 1,68E - 08}{2} + 1,25E - 09 + 8,4E - 10 = 4,61E - 09$$

$$PFH_{ges} = 10\% * \frac{4,61E - 09 + 8,4E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09$$

$$+ 10\% * \frac{1,29E - 09 + 1,29E - 09}{2} + 1,11E - 09 + 1,68E - 09$$

$$= 6,96E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S2/Lock/Unlock/EL2904/GuardLock)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(Restart)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(Lock)} = \frac{B10_{D(Lock)}}{0,1 * n_{op}}$$

$$MTTF_{D(Unlock)} = \frac{B10_{D(Unlock)}}{0,1 * n_{op}}$$

$$MTTF_{D(GuardLock)} = \frac{B10_{D(GuardLock)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 * \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(S2/Lock/Unlock/EL2904/GuardLock)} = \frac{1}{\frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(Lock)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(GuardLock)}}}$$

$$= \frac{1}{\frac{1}{1358,7y} + \frac{1}{67,9y} + \frac{1}{913,2y} + \frac{1}{1358,7y}} = 57,82y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{57,82y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{1028,8y} + \frac{1}{6793,5y}} = 44,41y$$

$$DC_{avg} = \frac{\frac{99\%}{57,82y} + \frac{99\%}{1358,7y} + \frac{99\%}{67,9y} + \frac{99\%}{67,9y} + \frac{99\%}{913,2y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{883,2y} + \frac{99\%}{883,2y} + \frac{99\%}{1028,8y} + \frac{90\%}{6793,5y}}{\frac{1}{57,82y} + \frac{1}{1358,7y} + \frac{1}{67,9y} + \frac{1}{67,9y} + \frac{1}{913,2y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y} + \frac{1}{1028,8y} + \frac{1}{6793,5y}}$$

$$= 98,98\%$$

NOTE

Category
This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

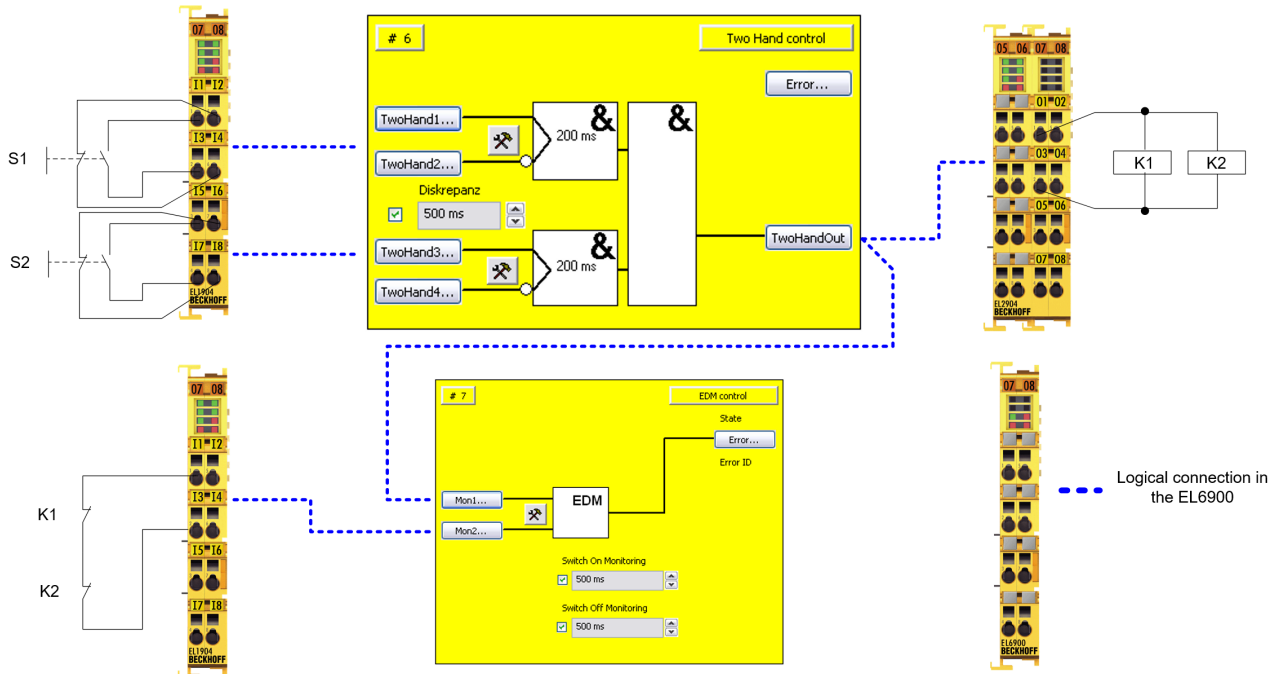
Diagnostic coverage
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.5 Two-hand controller (Category 4, PL e)

The two-hand buttons each consist of a combination of normally closed and normally open contacts on safe inputs of an EL1904. The testing of the inputs is active and the signals are tested for discrepancy (200 ms). In addition, the synchronous actuation of the two buttons is activated with a monitoring time of 500 ms.

The feedback loop is read in via a safe input. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.5.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

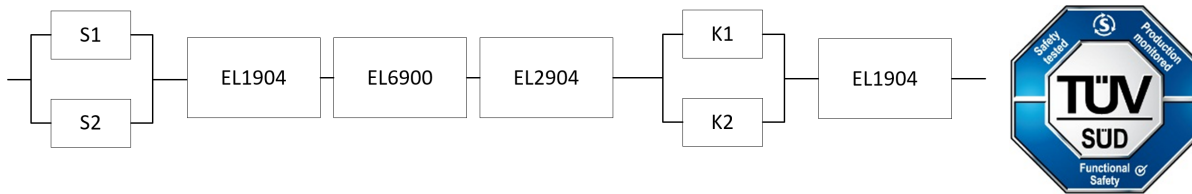
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.5.2 Block formation and safety loops

3.5.2.1 Safety function 1



3.5.3 Calculation

3.5.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	20,000,000
S2 – B10 _D	20,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	1 (1x per minute)
Lifetime (T1)	20 years = 175200 hours

3.5.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%

3.5.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1/S2:

$$n_{op} = \frac{230 * 16 * 60}{1} = 220.800$$

$$MTTF_D = \frac{20.000.000}{0,1 * 220.800} = 905,8y = 7.934.783h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{1} = 220.800$$

$$MTTF_D = \frac{1.300.000}{0,1 * 220.800} = 58,9y = 515.760h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1/S2:

$$PFH = \frac{1 - 0,99}{905,8y * 8760} = 1,26E - 09$$

K1/K2:

$$PFH = \frac{1 - 0,99}{58,9y * 8760} = 1,94E - 08$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} \\ + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(EL1904)}$$

Since the portions $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{1,26E - 09 + 1,26E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 08 + 1,94E - 08}{2} + 1,11E - 09 \\ = 6,56E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(EL1904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{905,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y} + \frac{1}{1028,8y}} = 45,4y$$

$$DC_{avg} = \frac{\frac{99\%}{905,8y} + \frac{99\%}{905,8y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{58,9y} + \frac{99\%}{58,9y} + \frac{99\%}{1028,8y}}{\frac{1}{905,8y} + \frac{1}{905,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y} + \frac{1}{58,9y} + \frac{1}{1028,8y}} = 99,0\%$$

NOTE

Category
 This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

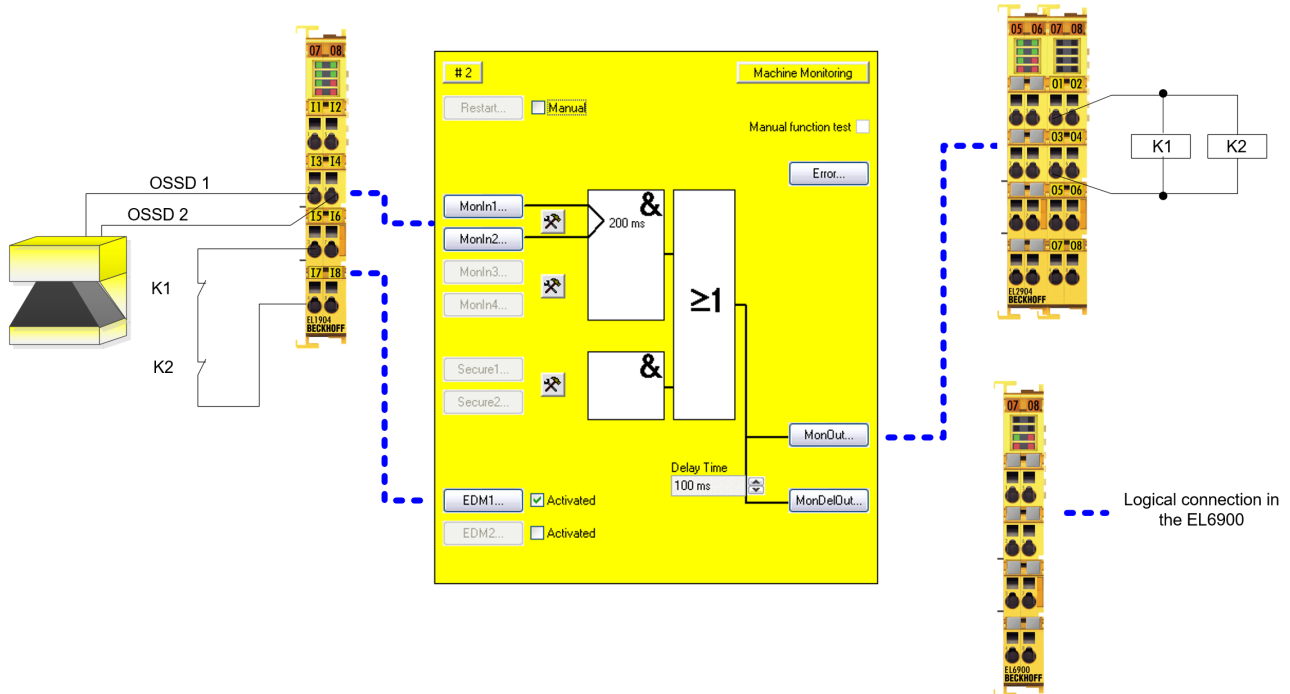
NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.6 Laser scanner (category 3, PL d)

The laser scanner has two OSSD outputs (Output-Signal-Switching-Device), which are wired to safe inputs of an EL1904. The testing of the inputs is not active, since the OSSD outputs carry out their own test. Furthermore, the signals are checked for discrepancy (200 ms). The feedback loop is read in via a safe input. Testing is active for this input. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.6.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

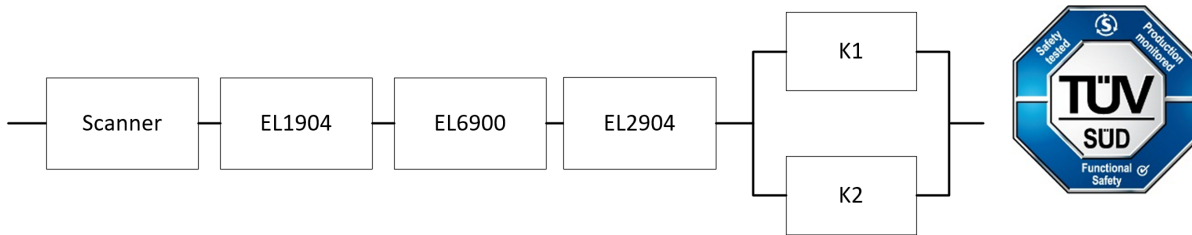
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	OSSD arbitrary types of pulse
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.6.2 Block formation and safety loops

3.6.2.1 Safety function 1



3.6.3 Calculation

3.6.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
Laser scanner – PFH _D	7.67E-08
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10 (6x per hour)
Lifetime (T1)	20 years = 175200 hours

3.6.3.2 Diagnostic Coverage DC

Component	Value
OSSD1/2 with testing (by scanner) / plausibility	DC _{avg} =90%
K1/K2 with testing and EDM	DC _{avg} =99%

3.6.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10} = 22.080$$

$$MTTF_D = \frac{1.300.000}{0,1 * 22.080} = 588,7y = 5.157.012h$$

and the assumption that K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

K1/K2:

$$PFH = \frac{1 - 0,99}{588,7y * 8760} = 1,94E - 09$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(Scanner)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 7,67E - 08 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 09 + 1,94E - 09}{2} = 8,03E - 08$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(Scanner)} = \frac{(1 - DC_{(Scanner)})}{PFH_{(Scanner)}} = \frac{(1 - 0,90)}{7,67E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{6,72E - 04 \frac{1}{y}} = 148,8y$$

In accordance with the limitation of the $MTTF_D$ to 100 years for components with a category 3 structure (for category 4 the limit is 2500 years) introduced in EN ISO 13849-1, the value is limited to 100 years for the further processing of the $MTTF_D$ of the scanner.

$$MTTF_{D(Scanner)} = 100y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{100y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{588,7y}} = 68,2y$$

$$DC_{avg} = \frac{\frac{90\%}{100} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{588,7} + \frac{99\%}{588,7}}{\frac{1}{100} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{588,7} + \frac{1}{588,7}} = 93,5\%$$

NOTE

Category

This structure is possible up to category 3 at the most through the use of the type 3 (category 3) laser scanner.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Area
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

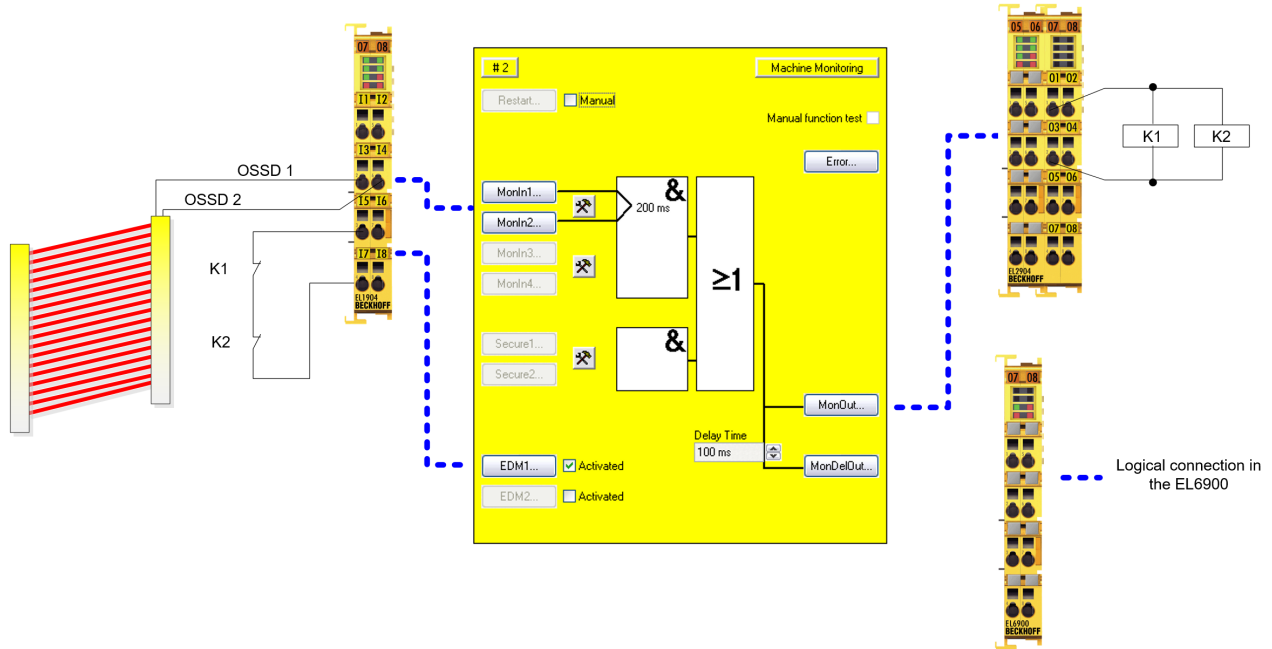
Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.7 Light curtain (Category 4, PL e)

The light curtain has two OSSD outputs (Output-Signal-Switching-Device), which are wired to safe inputs of an EL1904. The testing of the inputs is not active, since the OSSD outputs carry out their own test. Furthermore, the signals are checked for discrepancy (200 ms). The feedback loop is read in via a safe input. Testing is active for this input. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.7.1 Parameters of the safe input and output terminals

EL1904

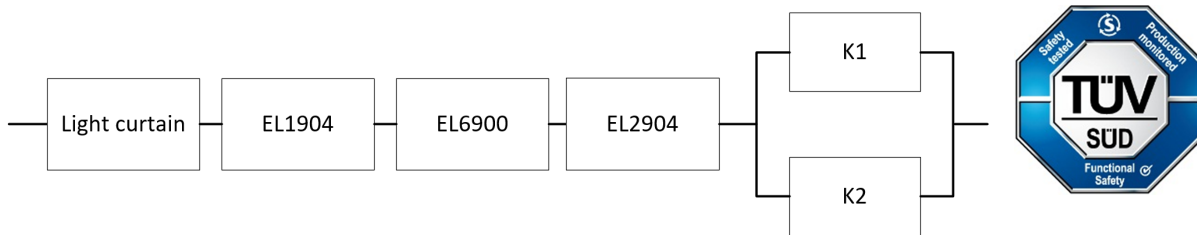
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Asynchronous evaluation OSSD
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.7.2 Block formation and safety loops

3.7.2.1 Safety function 1



3.7.3 Calculation

3.7.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
Light curtain – PFH _D	1.50E-08
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	5 (12x per hour)
Lifetime (T1)	20 years = 175200 hours

3.7.3.2 Diagnostic Coverage DC

Component	Value
OSSD1/2 with testing (by light curtain) / plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%

3.7.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{5} = 44.160$$

$$MTTF_D = \frac{1.300.000}{0,1 * 44.160} = 294,4y = 2.578.944h$$

and the assumption that K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

K1/K2:

$$PFH = \frac{1 - 0,99}{294,4y * 8760} = 3,88E - 09$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(Lightcurtain)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 1,50E - 08 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{3,88E - 09 + 3,88E - 09}{2} = 1,88E - 08$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Lightcurtain)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(Lightcurtain)} = \frac{(1 - DC_{(Lightcurtain)})}{PFH_{(Lightcurtain)}} = \frac{(1 - 0,99)}{1,50E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,31E - 04 \frac{1}{y}} = 76,1y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{294,4y}} = 51,3y$$

$$DC_{avg} = \frac{\frac{99\%}{76,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{294,4y} + \frac{99\%}{294,4y}}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{294,4y} + \frac{1}{294,4y}} = 99,00\%$$

NOTE

Category

This structure is possible up to category 4 at the most through the use of the type 4 (category 4) light curtain.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

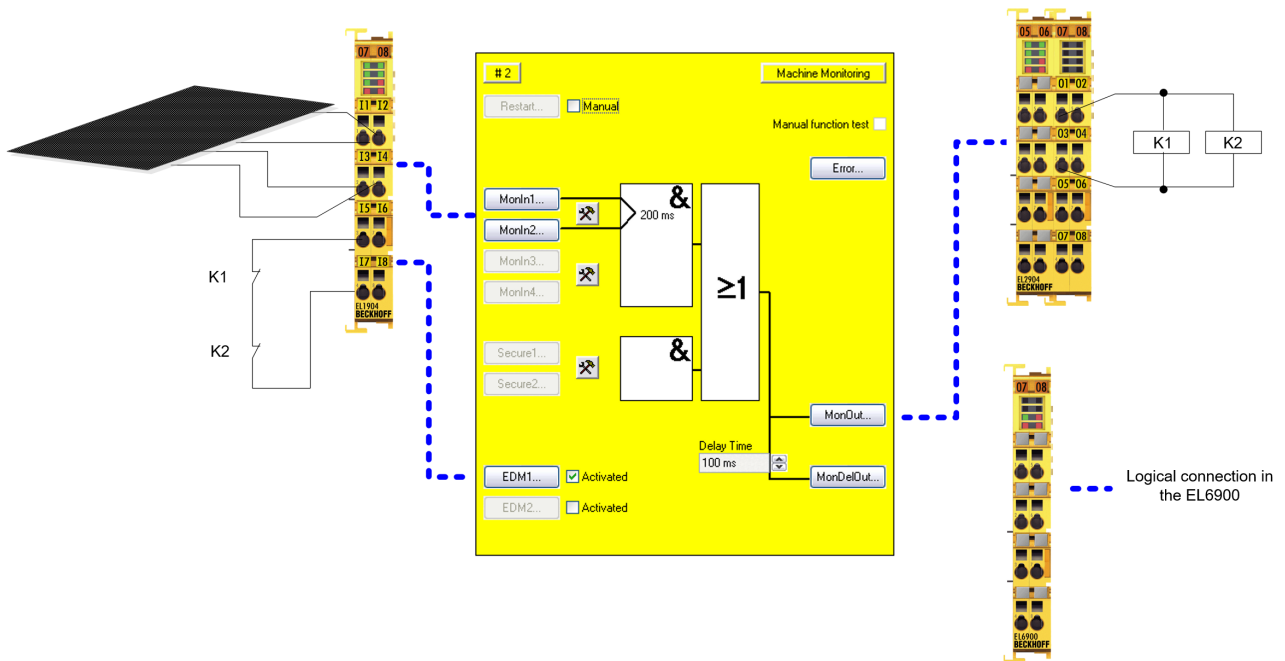
Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.8 Safety switching mat / safety bumper (Category 4, PL e)

Safety switching mats or safety bumpers work according to the cross-circuit principle. The contact surfaces of the device are wired to safe inputs of an EL1904. The testing of the inputs is active and the signals are tested for discrepancy (200 ms). As soon as a cross-circuit between the signals is detected (safety mat is stepped on), a logical 0 is signaled by the EL1904 input terminal. If the cross-circuit is no longer present, a logical 1 is signaled. The feedback loop is read in via a safe input. The testing of the input is active here also. The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.



3.8.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

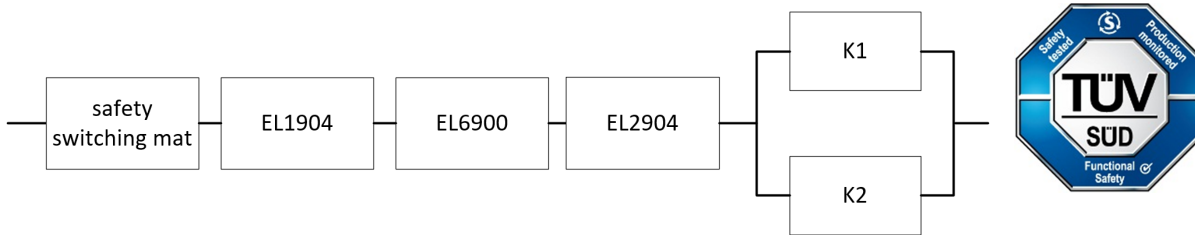
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Cross-circuit is not a module error
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.8.2 Block formation and safety loops

3.8.2.1 Safety function 1



3.8.3 Calculation

3.8.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
Safety switching mat – B10 _D	6.00E06
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	1 (1x per minute)
Lifetime (T1)	20 years = 175200 hours

3.8.3.2 Diagnostic Coverage DC

Component	Value
Switching outputs (mat) with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%

3.8.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_d values from the B10_d values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{1} = 220.800$$

$$MTTF_D = \frac{1.300.000}{0,1 * 220.800} = 58,9y = 515.760h$$

Safety mat:

$$n_{op} = \frac{230 * 16 * 60}{1} = 220.800$$

$$MTTF_D = \frac{6,00E06}{0,1 * 220.800} = 271,7y = 2.380.434h$$

and the assumption that K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

K1/K2:

$$PFH = \frac{1 - 0,99}{58,9y * 8760} = 1,94E - 08$$

Safety mat:

$$PFH = \frac{1 - 0,99}{271,7y * 8760} = 4,20E - 09$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(SafetyMat)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 4,20E - 09 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 08 + 1,94E - 08}{2} = 9,53E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SafetyMat)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{271,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y}} = 42,3y$$

$$DC_{avg} = \frac{\frac{99\%}{271,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{58,9y} + \frac{99\%}{58,9y}}{\frac{1}{271,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y} + \frac{1}{58,9y}} = 99,00\%$$

NOTE

Category
 This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

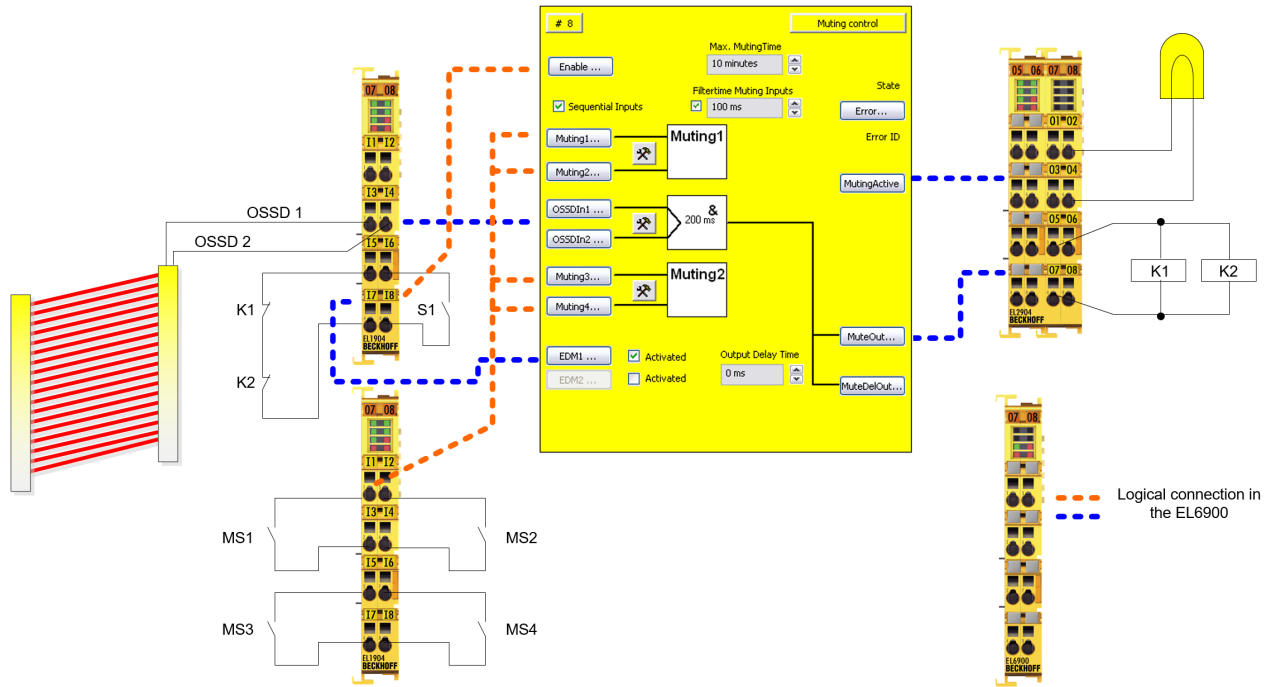
Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.9 Muting (Category 4, PL e)

The light curtain has two OSSD outputs (Output-Signal-Switching-Device), which are wired to safe inputs of an EL1904. The testing of the inputs is not active, since the OSSD outputs carry out their own test. Furthermore, the signals are checked for discrepancy (200 ms). The feedback loop is read in via a safe input. The muting switches and the enable switch are also wired to safe inputs. Testing is active for these inputs.

The contactors K1 and K2 are connected in parallel to a safe output. The muting lamp is also wired to a safe output. Current measurement and testing of the output are active for this circuit.



3.9.1 Parameters of the safe input and output terminals

EL1904 (upper terminal on the drawing)

Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Asynchronous evaluation OSSD
Logic channel 3 and 4	Single Logic

EL1904 (lower terminal on the drawing)

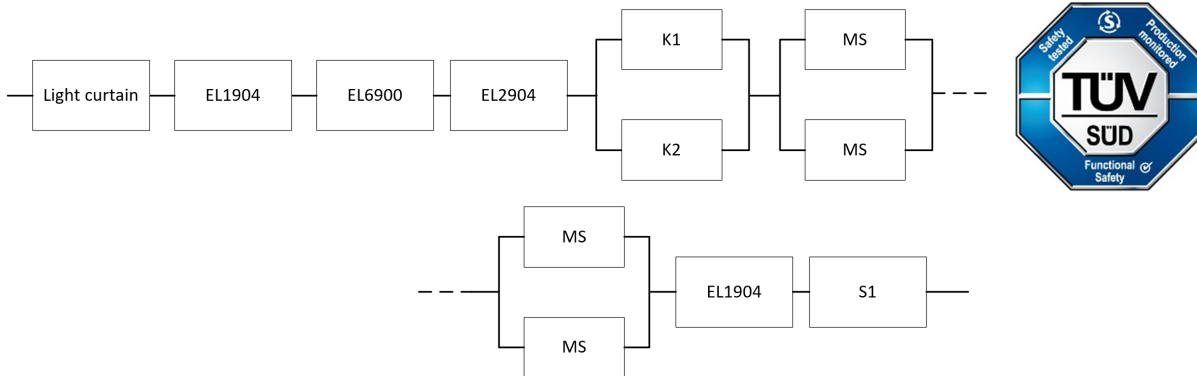
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

3.9.2 Block formation and safety loops

3.9.2.1 Safety function 1



3.9.3 Calculation

3.9.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	100,000
Light curtain – PFH _D	1.50E-08
MS1 – B10 _D	100,000
MS2 – B10 _D	100,000
MS3 – B10 _D	100,000
MS4 – B10 _D	100,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

3.9.3.2 Diagnostic Coverage DC

Component	Value
OSSD1/2 with testing (by light curtain) / plausibility	$DC_{avg}=99\%$
MS1/2/3/4 with testing/plausibility	$DC_{avg}=90\%$
K1/K2 with testing and EDM	$DC_{avg}=99\%$
S1 with testing	$DC_{avg}=90\%$

3.9.3.3 Calculation of safety function 1

Calculation of the PFH_D and $MTTF_D$ values from the $B10_D$ values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0,1 * 1840} = 543,5y = 4761060h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{1.300.000}{0,1 * 1840} = 7065,2y = 61891152h$$

MS1/MS2/MS3/S4:

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0,1 * 1840} = 543,5y = 4761060h$$

and the assumption that S1, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,90}{543,5 * 8760} = 2,10E - 08$$

K1/K2:

$$PFH = \frac{1 - 0,99}{7065,2 * 8760} = 1,62E - 10$$

MS1/MS2/MS3/S4:

$$PFH = \frac{1 - 0,90}{543,5 * 8760} = 2,10E - 08$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(Lightcurtain)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

$$+ \beta * \frac{PFH_{(MS1)} + PFH_{(MS2)}}{2} + (1 - \beta)^2 * (PFH_{(MS1)} * PFH_{(MS2)}) * T1 + \beta * \frac{PFH_{(MS3)} + PFH_{(MS4)}}{2} + (1 - \beta)^2 * (PFH_{(MS3)} * PFH_{(MS4)}) * T1$$

$$+ PFH_{(EL1904)} + PFH_{(S1)}$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 1,50E - 08 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,62E - 10 + 1,62E - 10}{2} + 10\% * \frac{2,10E - 08 + 2,10E - 08}{2}$$

$$+ 10\% * \frac{2,10E - 08 + 2,10E - 08}{2} + 1,11E - 09 + 2,10E - 08$$

$$= 4,47E - 08$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Lightcurtain)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

$$+ \frac{1}{MTTF_{D(MS1)}} + \frac{1}{MTTF_{D(MS3)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(S1)}}$$

with:

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(Lightcurtain)} = \frac{(1 - DC_{(Lightcurtain)})}{PFH_{(Lightcurtain)}} = \frac{(1 - 0,99)}{1,50E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,31E - 04 \frac{1}{y}} = 76,1y$$

$$MTTF_{D(MS1/MS3)} = \frac{(1 - DC_{(MS1/MS3)})}{PFH_{(MS1/MS3)}} = \frac{(1 - 0,90)}{2,10E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{1,84E - 04 \frac{1}{y}} = 543,6y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{7065,2y} + \frac{1}{543,6y} + \frac{1}{543,6y} + \frac{1}{1028,8y} + \frac{1}{543,5y}} = 44,0y$$

$$DC_{avg} = \frac{\frac{99\%}{76,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{7065,2y} + \frac{99\%}{7065,2y} + \frac{90\%}{543,6y} + \frac{90\%}{543,6y} + \frac{90\%}{543,6y} + \frac{90\%}{543,6y} + \frac{99\%}{1028,8y} + \frac{99\%}{543,5y}}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{7065,2y} + \frac{1}{7065,2y} + \frac{1}{543,6y} + \frac{1}{543,6y} + \frac{1}{543,6y} + \frac{1}{543,6y} + \frac{1}{1028,8y} + \frac{1}{543,5y}} = 96,51\%$$

NOTE

Category

This structure is possible up to category 4 at the most through the use of the type 4 (category 4) light curtain.

MTTF_D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

Diagnostic coverage

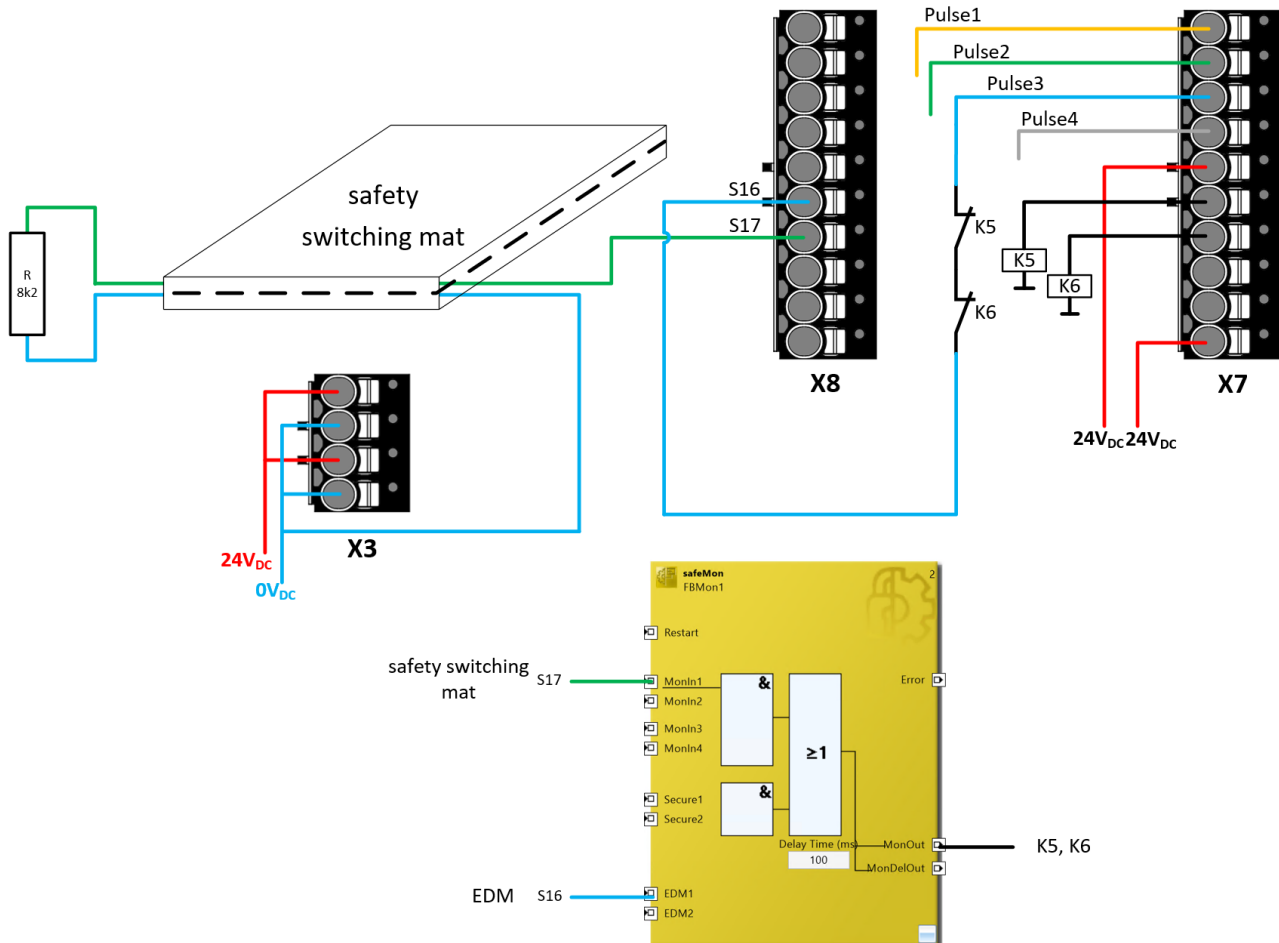
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.10 EK1960 safety mat inputs / digital outputs (category 2, PL d)

The safety mat is wired to safe input S17 (or 8.7) on the X8 10-pole connector. The first output group on the 10-pole X7 connector is configured as a clock source (for FSOUT module 3, the parameter *Diag TestPulse for Inputs active* is set to TRUE). For input S16, the parameter *Channel x.Testpulse Diag Mode* is configured based on the corresponding clock source.

Contactors K5 and K6 are wired to outputs 7.5 and 7.6 on the second output module on X7. Terminal A2 of the contactors is wired to the common ground of the 24 V_{DC} supply of terminal X7. The feedback loops of the two contactors are wired in series from pulse 3 to input S16 (or 8.6).



⚠ CAUTION

Safety mat wiring

Only safety mats that operate according to the principle of resistance change (resistance value: 8k Ω) are supported. The ground connection of the safety mat must be connected to the ground of the EK1960 supply voltage according to the above drawing.

3.10.1 Parameters of the safe input and output modules

EK1960

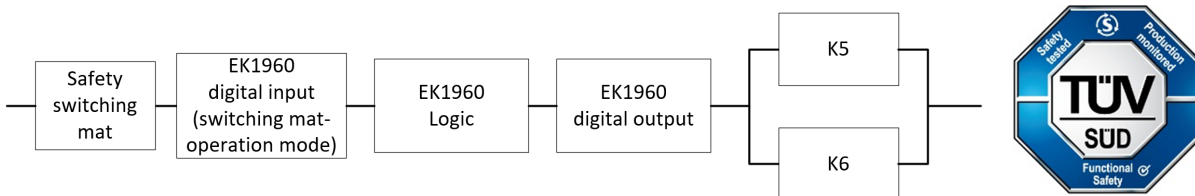
Parameter	Value
FSOUT module 3 (X7.1 – X7.4)	-
8020:01 ModuloDiagTestPulse	0x00
8020:02 MultiplierDiagTestPulse	0x02
8020:03 Standard Outputs active	FALSE
8020:04 Diag Testpulse active	TRUE
8020:05 Diag Testpulse for Inputs active	TRUE
FSOUT Module 4 (X7.5 – X7.8)	-
8030:01 ModuloDiagTestPulse	0x00
8030:02 MultiplierDiagTestPulse	0x02
8030:03 Standard Outputs active	FALSE
8030:04 Diag Testpulse active	TRUE
8030:05 Diag Testpulse for Inputs active	FALSE
FSIN Module 8 (X8.5 – X8.6)	-
80E1:04 Channel 2.InputFilterTime	0x0014
80E1:05 Channel 2.DiagTestPulseFilterTime	0x0002
80E1:06 Channel 2.Testpulse Diag Mode	(X7.3) Testpulse Detection Output Module 3.Channel 3
FSIN Module 9 (X8.7 – X8.8)	-
80F0:03 Input Mode	Bumper Mode Channel 1 (1)
80F1:01 Channel 1.InputFilterTime	0x0014
80F1:02 Channel 1.DiagTestPulseFilterTime	0x0002
80F1:03 Channel 1.Testpulse Diag Mode	External test pulses (0)

MON FB parameter

Parameter	Value
Reset Time (ms) (Port EDM1)	1000

3.10.2 Block formation and safety loops

3.10.2.1 Safety function 1



3.10.3 Calculation

3.10.3.1 PFHD / MTTFD / B10D – values

Component	Value
EK1960 digital input – PFH _D	6.40E-11
EK1960 safety mat input - PFH _D	8.84E-10
EK1960 logic – PFH _D	5.18E-09
EK1960 digital output – PFH _D	1.50E-10
Safety mat – B10 _D	6,000,000
K5 – B10 _D	1,300,000
K6 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

● Safety-over-EtherCAT communication

i The PFH_D value of the Safety-over-EtherCAT (FSoE) communication is included in the PFH_D value of the EK1960 logic component.

3.10.3.2 Diagnostic Coverage DC

Component	Value
Safety mat with testing	DC _{avg} =90%
K5/K6 with EDM monitoring (actuation 1x per hour and evaluation of all rising and falling edges with temporal monitoring) with testing	DC _{avg} =99%

3.10.3.3 Calculation of safety function 1

Calculation of the performance level according to EN ISO 13849-1:2015:

Calculation of the MTTF_D values from the B10_D values.

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

Safety switching mat:

$$n_{op} = \frac{230 * 16 * 60}{60} = 3680$$

$$MTTF_{D(SwitchingMat)} = \frac{6.000.000}{0,1 * 3680} = 16304y$$

K5/K6:

$$n_{op} = \frac{230 * 16 * 60}{60} = 3680$$

$$MTTF_D = \frac{1.300.000}{0,1 * 3680} = 3532y$$

The total $MTTF_D$ value is calculated based on the following formula:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SwitchingMat)}} + \frac{1}{MTTF_{D(EK1960-InputSwitchingMat)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Output)}} + \frac{1}{MTTF_{D(K5)}}$$

If only PFH_D values are available for EL1960 components, the following estimation applies:

$$MTTF_{D(EK1960-xxx)} = \frac{(1 - DC_{(EK1960-xxx)})}{PFH_{(EK1960-xxx)}}$$

Hence:

$$MTTF_{D(EK1960-InputSwitchingMat)} = \frac{(1 - DC_{(EK1960-InputSwitchingMat)})}{PFH_{D(EK1960-InputSwitchingMat)}} = \frac{(1 - 0,90)}{8,84E - 10 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{7,74E - 06 \frac{1}{y}} = 12913y$$

$$MTTF_{D(EK1960-Logic)} = \frac{(1 - DC_{(EK1960-Logic)})}{PFH_{D(EK1960-Logic)}} = \frac{(1 - 0,99)}{5,18E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{4,54E - 05 \frac{1}{y}} = 220y$$

$$MTTF_{D(EK1960-Output)} = \frac{(1 - DC_{(EK1960-Output)})}{PFH_{D(EK1960-Output)}} = \frac{(1 - 0,99)}{1,50E - 10 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,31E - 06 \frac{1}{y}} = 7610y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{16304y} + \frac{1}{12913y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{3532y}} = 196y$$

$$DC_{avg} = \frac{\frac{90\%}{16304y} + \frac{90\%}{12913y} + \frac{99\%}{220y} + \frac{99\%}{7610y} + \frac{99\%}{3532y} + \frac{99\%}{3532y}}{\frac{1}{16304y} + \frac{1}{12913y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{3532y} + \frac{1}{3532y}} = 98,76\%$$

NOTE

Category
 This structure is possible up to category 2 at the most.

⚠ CAUTION

Implement a restart lock in the machine!
 The restart lock is **NOT** part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Calculation of PFH_D values according to EN 62061:

assuming that the safety mat, K5 and K6 are all single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH_D = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Safety switching mat:

$$PFH_D = \frac{1 - 0,90}{16304 * 8760} = 7,00E - 10$$

K5/K6:

$$PFH_D = \frac{1 - 0,99}{3532 * 8760} = 3,23E - 10$$

The following assumptions must now be made:

Relays K5 and K6 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K5 and K6 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{Dges} = PFH_{D(SwitchingMat)} + PFH_{D(EK1960-InputSwitchingMat)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Output)} + \beta * \frac{PFH_{D(K5)} + PFH_{D(K6)}}{2} + (1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{Dges} = 7,00E - 10 + 8,84E - 10 + 5,18E - 09 + 1,50E - 10 + 10\% * \frac{3,23E - 10 + 3,23E - 10}{2} = 6,94E - 09$$

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

NOTE

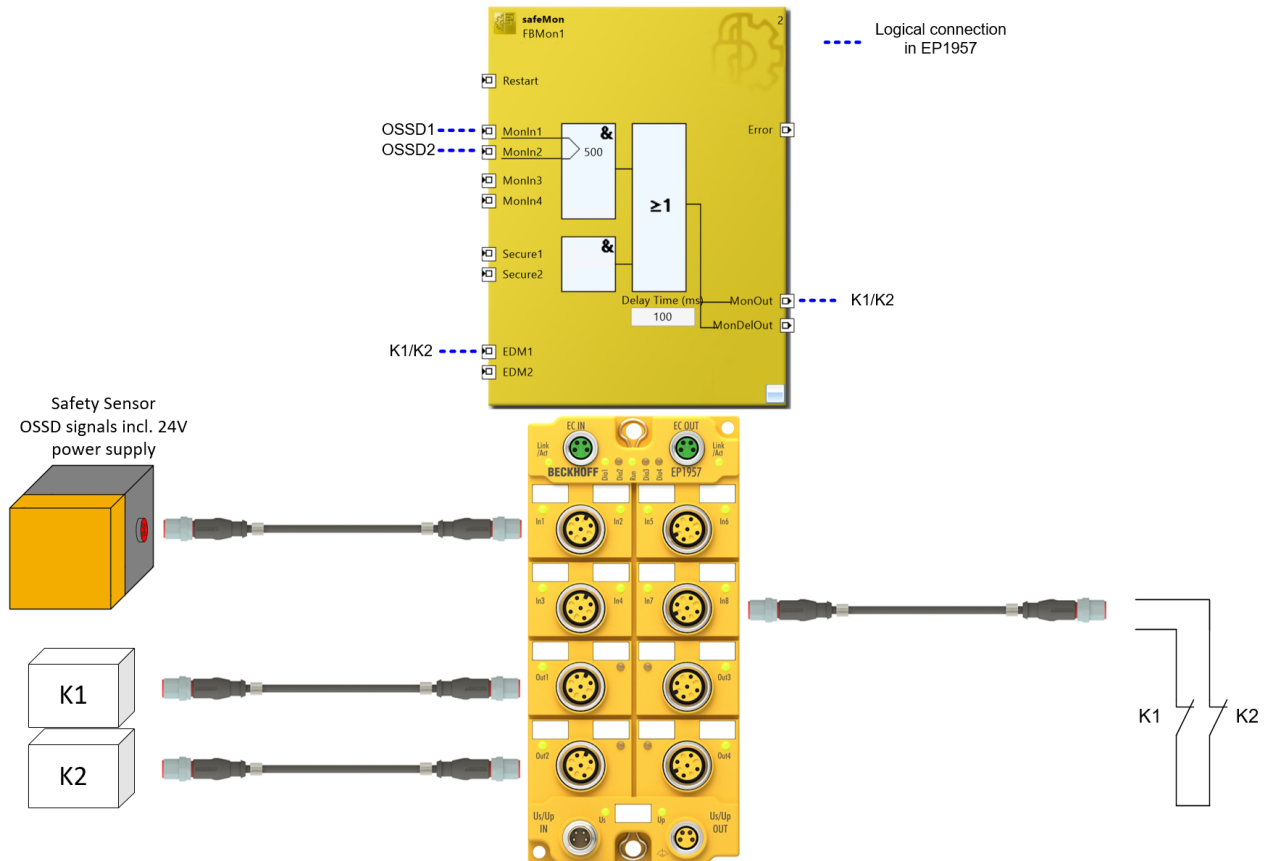
Safety integrity level

The application meets the requirements of safety integrity level SIL2 according to EN 62061, since the maximum achievable SIL for the safety mat input is limited to SIL 2.

3.11 EP1957 OSSD sensor for protective door (Category 4, PL e)

The OSSD Safety Sensor (in this case, for example, a proximity limit switch with a defined behavior under error conditions (PDDDB) according to EN 60947-5-3) is connected to the EP1957 via an M12 connection and can be used, for example, for a protective door application. The power supply is on pins 1 and 3 of the M12 connection (PowerModeA). The sensor checks the wiring between the sensor and the EP1957 by means of test pulses on the two OSSD channels and switches both OSSD signals to the safe state in case of error. The two OSSD inputs are monitored for discrepancy within the logic.

The two actuators K1 and K2 are switched according to the protective door state. The feedback loop of the two actuators is wired to a safe input. The test pulses are activated for this input.



3.11.1 Parameters of the safe input and output modules

EP1957

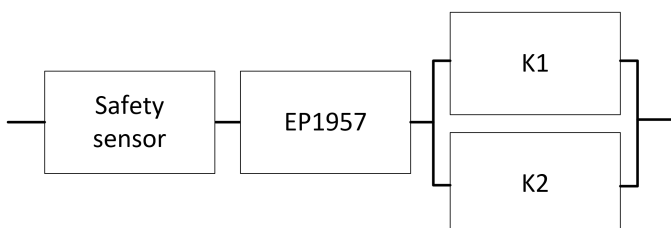
Parameter	Value
FSOUT Module 1 Settings Common	-
8000:04 Diag Testpulse active	TRUE
8000:07 Module Fault Link active	TRUE
FSOUT Module 2 Settings Common	-
8010:04 Diag Testpulse active	TRUE
8010:07 Module Fault Link active	TRUE
FSIN Module 1 Settings Common	-
8040:04 Diag Testpulse active	FALSE
8040:05 Module Fault Link active	TRUE
8040:0C Input Power Mode	PowerMode A: Pin1(+) / Pin3(-)
FSIN Module 1 Settings Channel	-
8041:01 Channel 1.InputFilterTime	0x000A (1ms)
8041:02 Channel 1.DiagTestPulseFilterTime	0x0002 (0.2 ms)
8041:04 Channel 2.InputFilterTime	0x000A (1ms)
8041:05 Channel 2.DiagTestPulseFilterTime	0x0002 (0.2 ms)
FSIN Module 4 Settings Common	-
8070:04 Diag Testpulse active	TRUE
8070:05 Module Fault Link active	TRUE
8070:0C Input Power Mode	Diag TestPulse
FSIN Module 4 Settings Channel	-
8071:01 Channel 1.InputFilterTime	0x000A (1ms)
8071:02 Channel 1.DiagTestPulseFilterTime	0x0002 (0.2 ms)

MON FB parameter

Parameter	Value
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (port MonIn1/MonIn2)	500
Safe Inputs After Disc Error	TRUE

3.11.2 Block formation and safety loops

3.11.2.1 Safety function 1



3.11.3 Calculation

3.11.3.1 PFHD / MTTFD / B10D – values

Component	Value
EP1957 – PFH _D	6.50E-09
Safety sensor – PFH _D (certified according to EN 60947-5-3 and EN ISO 13849)	1.00E-08 (Cat. 4 / PL e)
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

3.11.3.2 Diagnostic Coverage DC

Component	Value
Safety sensor with OSSD outputs	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%

3.11.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

K1/K2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0,1 * 7360} = 1766,3y = 15472788h$$

and the assumption that K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

K1/K2

$$PFH = \frac{1 - 0,99}{1766,3 * 8760} = 6,46E - 10$$

The following assumptions must now be made:

The contactors K1 und K2 are both connected to the safety function. The non-functioning of a contactor does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through contactor contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(SafetySensor)} + PFH_{(EP1957)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 1,00E - 08 + 6,50E - 09 + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} = 1,66E - 08$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SafetySensor)}} + \frac{1}{MTTF_{D(EP1957)}} + \frac{1}{MTTF_{D(K1)}}$$

If only PFH_D values are available for EP1957 and safety sensor, the following estimation applies:

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

Hence:

$$MTTF_{D(EP1957)} = \frac{(1 - DC_{(EP1957)})}{PFH_{(EP1957)}} = \frac{(1 - 0,99)}{6,50E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{5,69E - 05 \frac{1}{y}} = 175y$$

$$MTTF_{D(SafetySensor)} = \frac{(1 - DC_{(SafetySensor)})}{PFH_{(SafetySensor)}} = \frac{(1 - 0,99)}{1,00E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{8,76E - 05 \frac{1}{y}} = 114y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{114y} + \frac{1}{175y} + \frac{1}{1766,3y}} = 66y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(SafetySensor)}} + \frac{DC}{MTTF_{D(EP1957)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(SafetySensor)}} + \frac{1}{MTTF_{D(EP1957)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

$$DC_{avg} = \frac{\frac{99\%}{114y} + \frac{99\%}{175y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y}}{\frac{1}{114y} + \frac{1}{175y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 99,00\%$$

NOTE

Category
This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

NOTE

Safety integrity level
The application meets the requirements of safety integrity level SIL3 according to EN 62061.

4 Potential groups

4.1 All-pole disconnection of a potential group with downstream interference-free standard terminals (Category 4, PL e)

The protective door uses a combination of normally closed and normally open contacts on the safe inputs of an EL1904. The testing of the inputs is active and the signals are tested for discrepancy (200 ms). The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.

The diagnostic information from the KL/EL9110 (24 V is present on the power contacts) is negated, ANDed with the feedback signals from contactors K1, K2, K3 and K4 and applied to the EDM input.

The supply to the power contacts (24 V and also 0 V) of the potential group is switched off with the NO contacts of contactors K1 and K2. The 0 V potentials of the load employed (in this case K3 and K4) must always be fed back to the potential group.

NOTE

Safety consideration

The EL/KL9110 and EL/KL2xxx terminals used are not an active part of the safety controller. Accordingly, the safety level attained is defined only through the higher-level safety controller. The standard terminals are **not** incorporated in the calculation.

The external wiring of the standard terminals can lead to limitations in the maximum attainable safety levels.

NOTE

Power supply unit requirements

The standard terminals must be supplied with 24 V by an SELV/PELV power supply unit with an output voltage limit U_{max} of 60 V in the event of a fault.

⚠ CAUTION

Prevention of feedback

Feedback can be prevented by various measures (see further information below):

- No switching of loads with a separate power supply
- Ground feedback and all-pole disconnection (**used in this example**)
or
cable short-circuit fault exclusion (separate sheathed cable, wiring only inside control cabinet, dedicated earth connection per conductor)

NOTE

Interference-free Bus Terminals

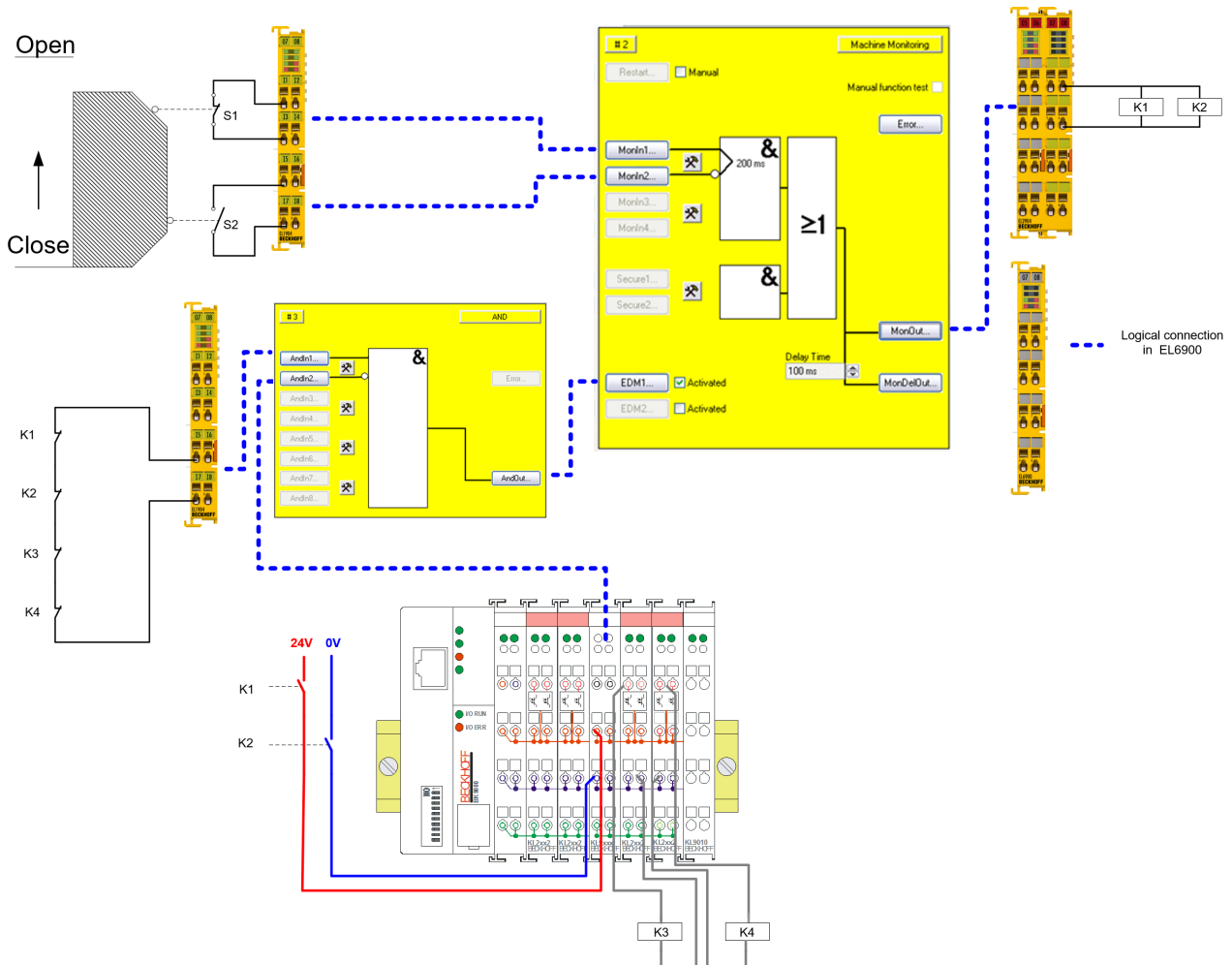
A list of the interference-free Bus Terminals can be found in the Beckhoff Information System under <http://infosys.beckhoff.de>.

NOTE

Maximum attainable safety level

Avoid feedback through ground feedback and all-pole disconnection:

- DIN EN ISO 13849-1: max. cat. 4 PL e
- IEC 61508: max. SIL3
- EN 62061: max. SIL3



⚠ CAUTION

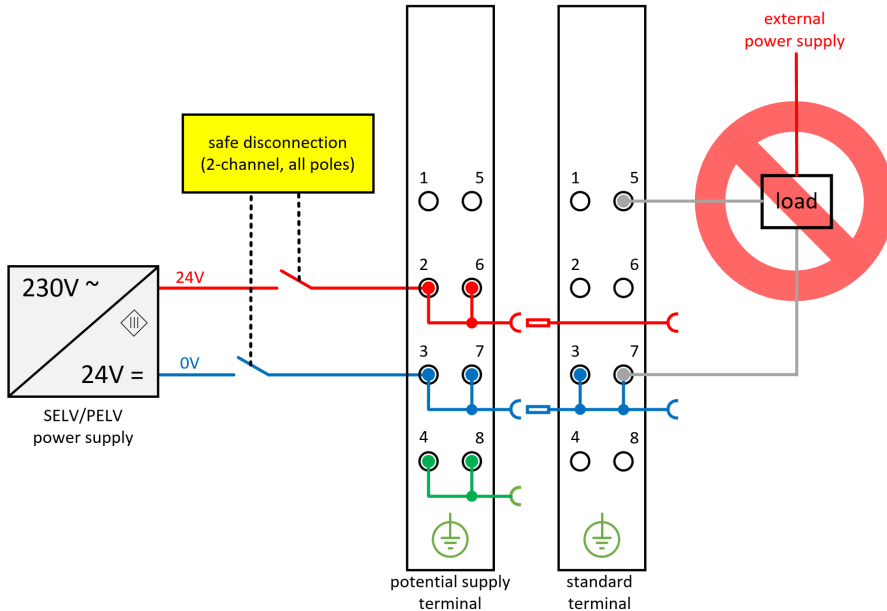
Time delay

Switching off the power supply for the potential group can delay the shutdown of the downstream contactors and actuators. This delay depends on the downstream actuators, loads and lines and must be taken into account by the user in the safety assessment.

4.1.1 Notes on prevention of feedback

4.1.1.1 No switching of loads with a separate power supply

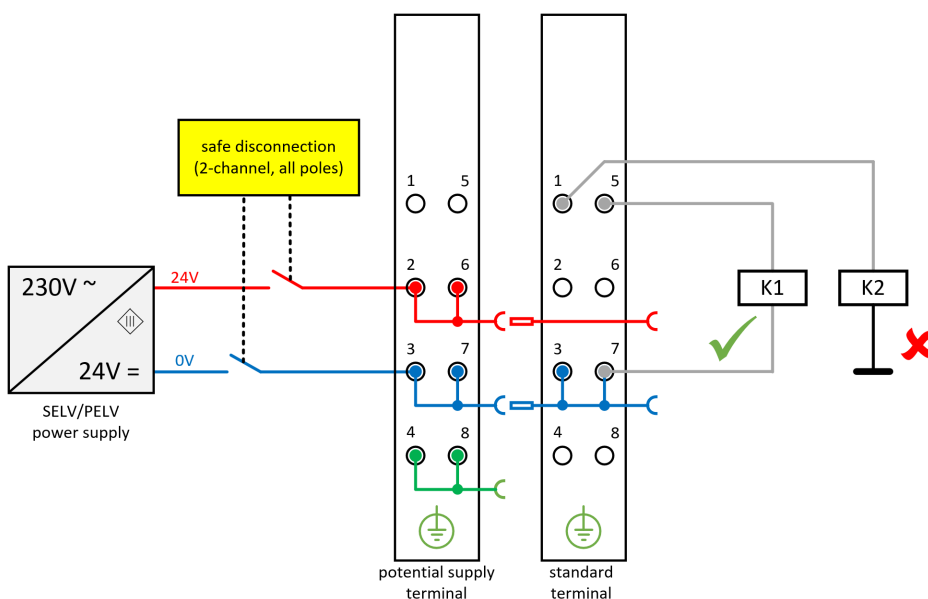
Loads that have their own power supply must not be switched by standard terminals, since in this case feedback via the load cannot be ruled out.



Exceptions to the general requirement are allowed only if the manufacturer of the connected load guarantees that feedback to the control input cannot occur.

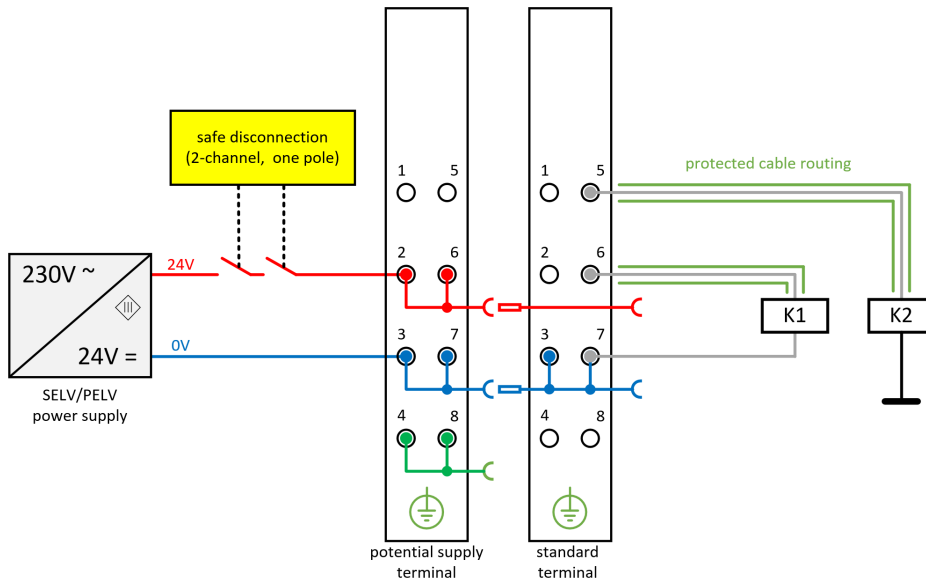
4.1.1.2 Option 1: Ground feedback and all-pole shutdown (used in this example)

The ground connection of the connected load must be fed back to the safely switched ground of the respective output terminal or potential group. (Here: K1 – correct wiring, K2 – incorrect wiring)



4.1.1.3 Option 2: Cable short-circuit fault exclusion

If option 1 from chapter 2.17.1.2 is not feasible, the ground feedback and all-pole disconnection can be dispensed with if the danger of feedback due to a cable short-circuit can be excluded by other measures. The following measures can be implemented as an alternative.



- Alternative 1: Load connection via separate sheathed cables
The non-safely switched potential of the standard terminal may not be conducted together with other potential-conducting lines inside the same sheathed cable
- Alternative 2: Wiring only inside the control cabinet
All loads connected to the non-safe standard terminals must be located in the same control cabinet as the terminals. The cables are routed entirely inside the control cabinet.
- Alternative 3: Dedicated earth connection per conductor
All conductors connected to the non-safe standard terminals are protected by a separate ground connection.
- Alternative 4: Permanent (fixed) wiring, protected from external damage
All conductors connected to the non-safe standard terminals are permanently installed and protected from external damage, e.g. through a cable duct or an armored conduit.

⚠ CAUTION

Fault exclusion

The machine manufacturer or the user is solely responsible for the correct execution and evaluation of the applied alternatives.

4.1.2 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

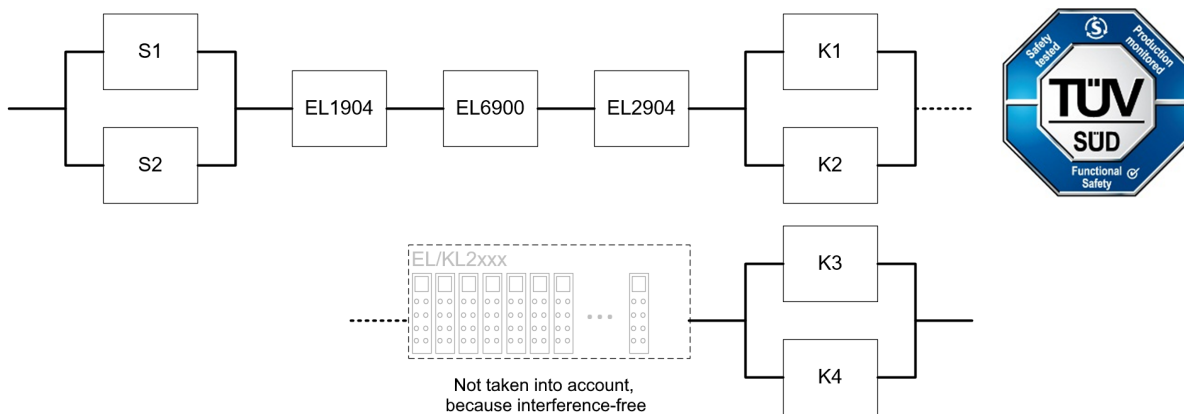
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

4.1.3 Block formation and safety loops

4.1.3.1 Safety function 1



4.1.4 Calculation

4.1.4.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
K3 – B10 _D	1,300,000
K4 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

4.1.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%
K3/K4 with EDM	DC _{avg} =90%

4.1.4.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0,1 * 7360} = 1358,7y = 11902212h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0,1 * 7360} = 2717,4y = 23804424h$$

K1/K2/K3/K4:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0,1 * 7360} = 1766,3y = 15472788h$$

and the assumption that S1, S2, K1, K2, K3 and K4 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0,99}{1358,7 * 7360} = 8,40E - 10$$

S2

$$PFH = \frac{1 - 0,99}{2717,4 * 8760} = 4,20E - 10$$

K1/K2

$$PFH = \frac{1 - 0,99}{1766,3 * 8760} = 6,46E - 10$$

K3/K4

$$PFH = \frac{1 - 0,90}{1766,3 * 8760} = 6,46E - 09$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

The contactors K1, K2, K3 und K4 are all connected to the safety function. The non-functioning of a contactor does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1, K2, K3 and K4 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through contactor contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1 - \beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{8,40E - 10 + 4,20E - 10}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} + 10\% * \frac{6,46E - 09 + 6,46E - 09}{2} = 4,16E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K3)}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 206,7y$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 97,39\%$$

NOTE

Category

This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	$\geq 10^{-8} \text{ to } < 10^{-7}$
2	$\geq 10^{-7} \text{ to } < 10^{-6}$
1	$\geq 10^{-6} \text{ to } < 10^{-5}$

4.2 Single-pole disconnection of a potential group with downstream interference-free standard terminals with fault exclusion (Category 4, PL e)

The protective door uses a combination of normally closed and normally open contacts on the safe inputs of an EL1904. Testing of the inputs is active, and the signals are checked for discrepancy (200 ms in this case). The contactors K1 and K2 are connected in parallel to the safe output. Current measurement and testing of the output are active for this circuit.

The feedback signals of the contactors K1, K2, K3 and K4 are applied to the EDM input.

Only the 24 V supply to the power contacts of the potential group is switched off with the make contacts of contactors K1 and K2. The 0 V connection of the power contacts is fed directly back to the 0 V of the power supply.

The 0 V potentials of all loads and devices that are used have to be at or connected to the same potential.

NOTE

Safety consideration

The EL/KL9110 and EL/KL2xxx terminals used are not an active part of the safety controller. Accordingly, the safety level attained is defined only through the higher-level safety controller. The standard terminals are **not** incorporated in the calculation.

The external wiring of the standard terminals can lead to limitations in the maximum attainable safety levels.

NOTE

Power supply unit requirements

The standard terminals must be supplied with 24 V by an SELV/PELV power supply unit with an output voltage limit U_{\max} of 60 V in the event of a fault.

⚠ CAUTION

Prevention of feedback

Feedback can be prevented by various measures (see further information below):

- No switching of loads with a separate power supply
 - Ground feedback and all-pole disconnection
 - or
 - cable short-circuit fault exclusion (separate sheathed cable, wiring only inside control cabinet, dedicated earth connection per conductor)
- (used in this example)**

NOTE

Interference-free Bus Terminals

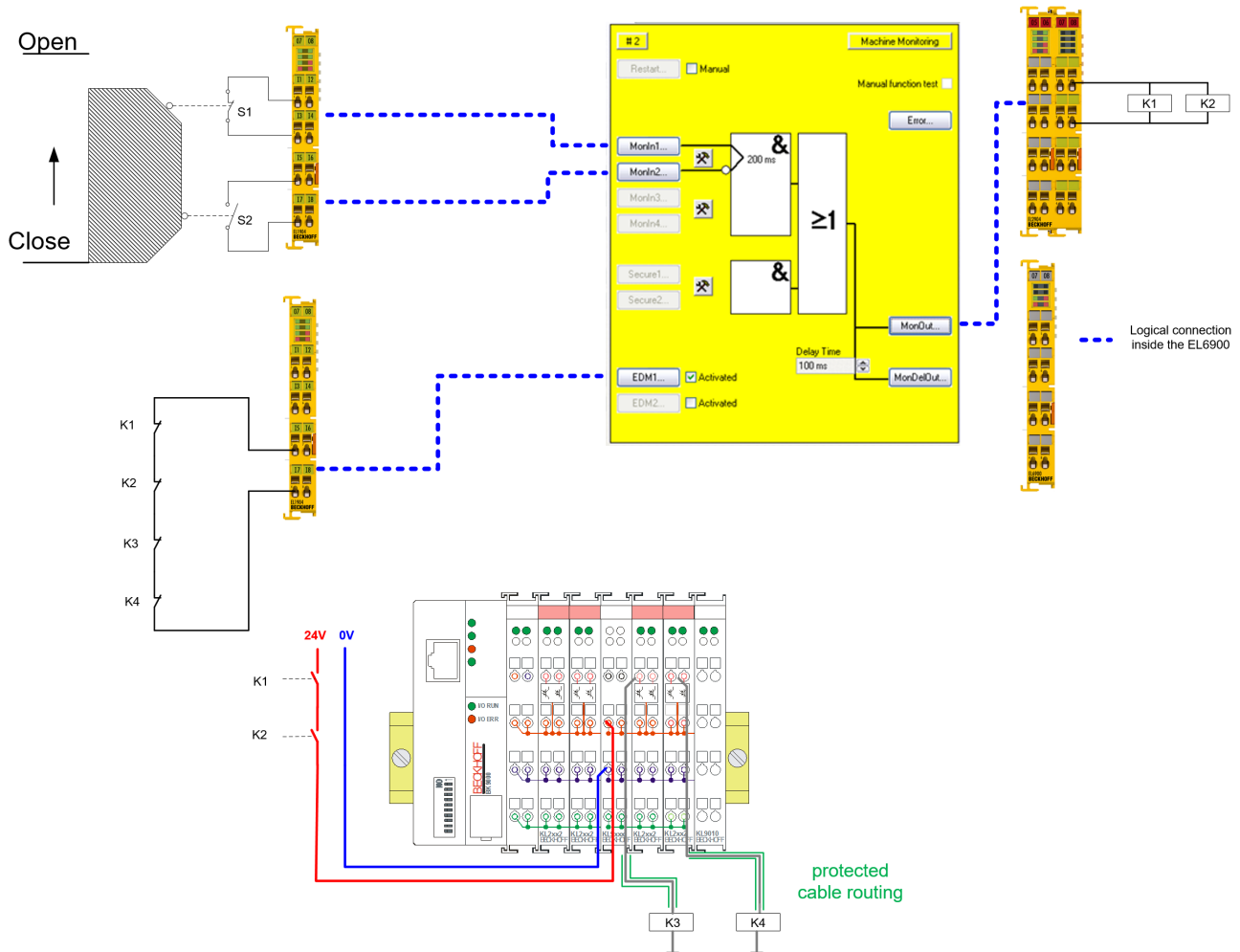
A list of the interference-free Bus Terminals can be found in the Beckhoff Information System under <http://infosys.beckhoff.de>.

NOTE

Maximum attainable safety level

Avoiding feedback through short-circuit fault exclusion:

- DIN EN ISO 13849-1: max. cat. 4 PL e
- IEC 61508: max. SIL3
- EN 62061: max. SIL2



NOTE

Fault exclusion

Due to the "line short circuit" fault exclusion in the wiring from the interference-free standard output terminals EL/KL2xxx to the load (K3, K4 in this case), a power feed terminal with diagnostic function is not required in this case. Power feed terminals of type EL/KL9xxx can therefore be used.

The 0 V potentials of the load (K3, K4 in this case) have to be identical to the 0 V potential of the power supply for the potential group.

⚠ CAUTION

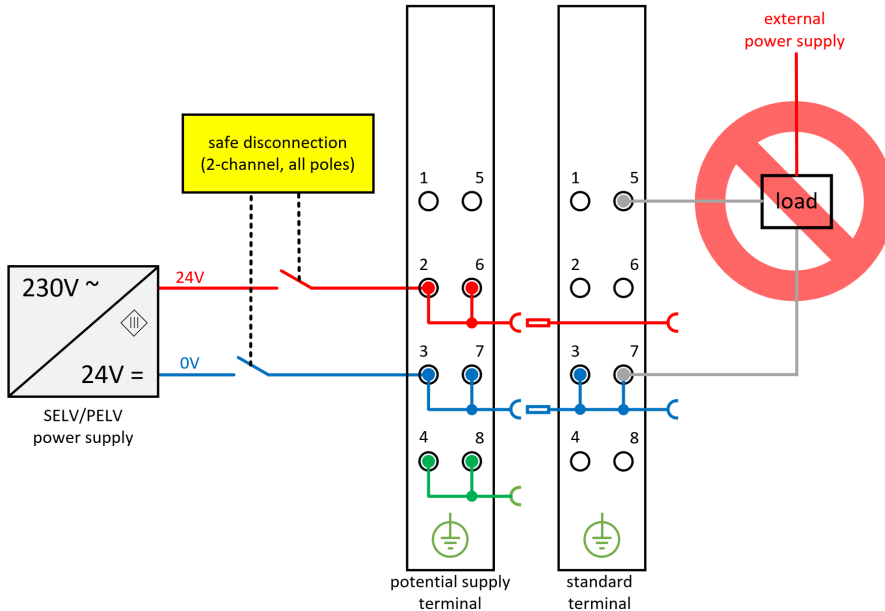
Time delay

Switching off the power supply for the potential group can delay the shutdown of the downstream contactors and actuators. This delay depends on the downstream actuators, loads and lines and must be taken into account by the user in the safety assessment.

4.2.1 Notes on prevention of feedback

4.2.1.1 No switching of loads with a separate power supply

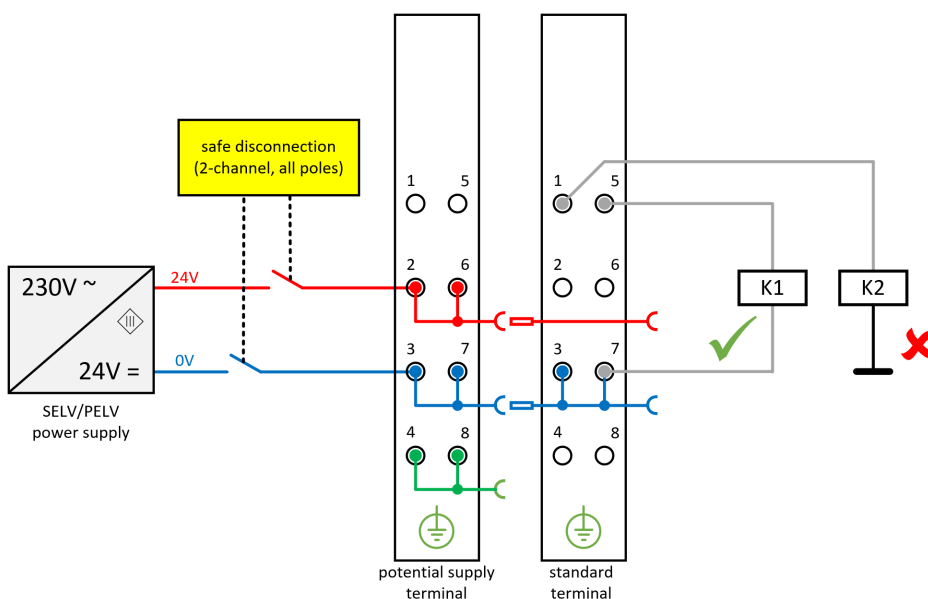
Loads that have their own power supply must not be switched by standard terminals, since in this case feedback via the load cannot be ruled out.



Exceptions to the general requirement are allowed only if the manufacturer of the connected load guarantees that feedback to the control input cannot occur.

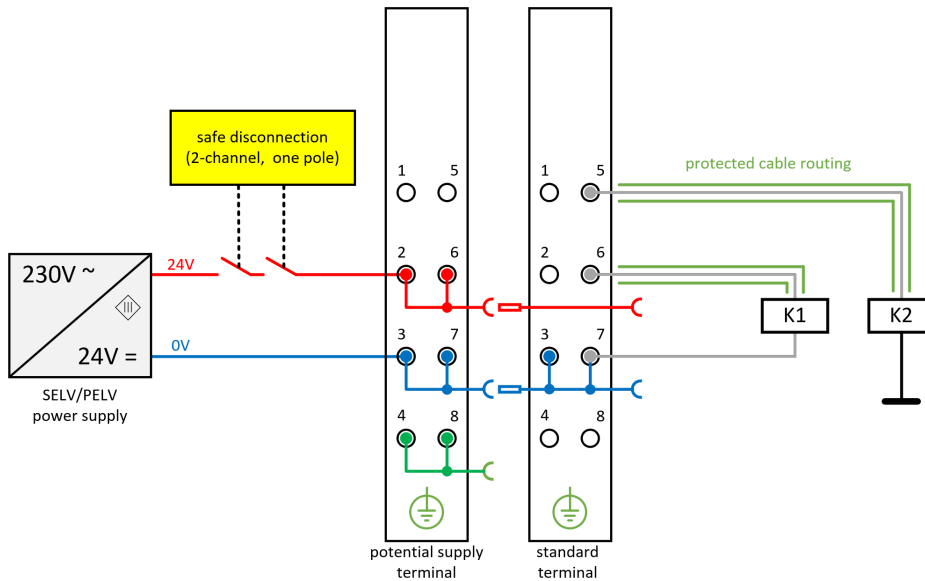
4.2.1.2 Option 1: Ground feedback and all-pole disconnection

The ground connection of the connected load must be fed back to the safely switched ground of the respective output terminal or potential group. (Here: K1 – correct wiring, K2 – incorrect wiring)



4.2.1.3 Option 2: Cable short-circuit error exclusion (used in this example)

If option 1 from chapter 2.18.1.2 is not feasible, the ground feedback and all-pole disconnection can be dispensed with if the danger of feedback due to a cable short-circuit can be excluded by other measures. The following measures can be implemented as an alternative.



- Alternative 1: Load connection via separate sheathed cables
The non-safely switched potential of the standard terminal may not be conducted together with other potential-conducting lines inside the same sheathed cable
- Alternative 2: Wiring only inside the control cabinet
All loads connected to the non-safe standard terminals must be located in the same control cabinet as the terminals. The cables are routed entirely inside the control cabinet.
- Alternative 3: Dedicated earth connection per conductor
All conductors connected to the non-safe standard terminals are protected by a separate ground connection.
- Alternative 4: Permanent (fixed) wiring, protected from external damage
All conductors connected to the non-safe standard terminals are permanently installed and protected from external damage, e.g. through a cable duct or an armored conduit.

⚠ CAUTION

Fault exclusion

The machine manufacturer or the user is solely responsible for the correct execution and evaluation of the applied alternatives.

4.2.2 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

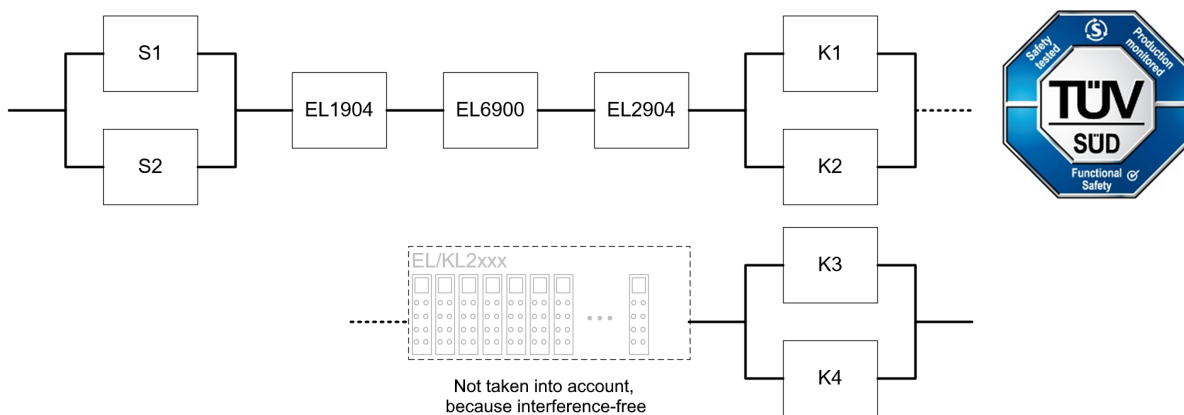
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

4.2.3 Block formation and safety loops

4.2.3.1 Safety function 1



4.2.4 Calculation

4.2.4.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
K3 – B10 _D	1,300,000
K4 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

4.2.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K1/K2 with testing and EDM	DC _{avg} =99%
K3/K4 with EDM	DC _{avg} =90%

4.2.4.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0,1 * 7360} = 1358,7y = 11902212h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0,1 * 7360} = 2717,4y = 23804424h$$

K1/K2/K3/K4:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0,1 * 7360} = 1766,3y = 15472788h$$

and the assumption that S1, S2, K1, K2, K3 and K4 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,40E - 10$$

S2

$$PFH = \frac{1 - 0,99}{2717,4 * 8760} = 4,20E - 10$$

K1/K2

$$PFH = \frac{1 - 0,99}{1766,3 * 8760} = 6,46E - 10$$

K3/K4

$$PFH = \frac{1 - 0,90}{1766,3 * 8760} = 6,46E - 09$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

The contactors K1, K2, K3 und K4 are all connected to the safety function. The non-functioning of a contactor does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1, K2, K3 and K4 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through contactor contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1 - \beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{8,40E - 10 + 4,20E - 10}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 \\ + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} + 10\% * \frac{6,46E - 09 + 6,46E - 09}{2} \\ = 4,16E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K3)}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 206,7y$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 97,39\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC

Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	$\geq 10^{-8} \text{ to } < 10^{-7}$
2 ^(*)	$\geq 10^{-7} \text{ to } < 10^{-6}$
1	$\geq 10^{-6} \text{ to } < 10^{-5}$

(*) In accordance with EN 62061 chapter 6.7.7.2, SILCL is restricted to a maximum of SIL2 in relation to structural constraints for a subsystem that has an HFT of 0 and for which fault exclusions have been applied to faults that could lead to a dangerous failure.

4.3 EL2911 potential group with interference-free standard terminals (Category 4, PL e)

The protective door uses a combination of NC and NO contacts and is wired to safe inputs of the EL2911. Testing of the inputs is active, and the signals are checked for discrepancy (500 ms in this case). The 24 V supply of the power contacts of the potential group is switched off at the safe output. The 0 V connection of the power contacts is fed directly back to the 0 V of the power supply of the EL2911.

The EL2911 monitors a feedback to the 24 V_{DC} to the power contacts and enters the module error state as soon as a voltage higher than 5 V is read in the switched-off state.

The feedback loop of the contactors K3 and K4 is connected to a safe input of the EL2911.

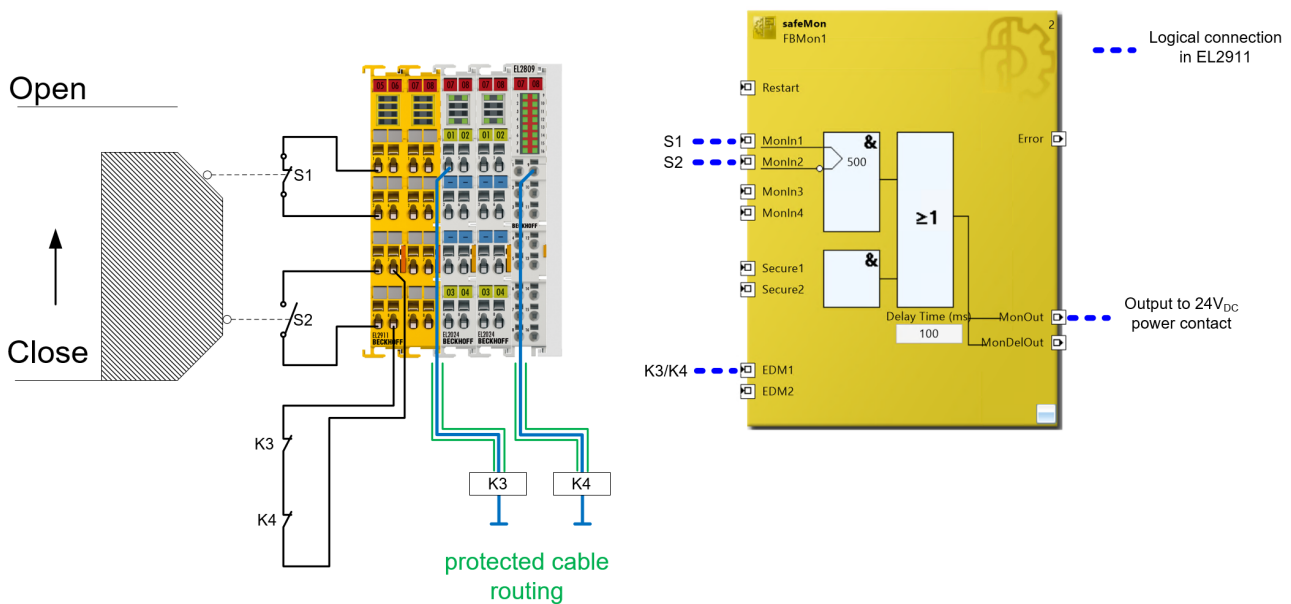
The 0 V potentials of all loads and devices that are used have to be at or connected to the same potential.

NOTE

Safety consideration

The EL2xxx terminals used are not an active part of the safety controller. Accordingly, the safety level attained is defined only through the higher-level safety controller. The standard terminals are **not** incorporated in the calculation, but they must be interference-free.

The external wiring of the standard terminals can lead to limitations in the maximum attainable safety levels.



⚠ CAUTION

Power supply unit requirements

The standard terminals must be supplied with 24 V_{DC} by an SELV/PELV power supply unit with an output voltage limit U_{max} of 36 V in the event of a fault.

⚠ CAUTION

Prevention of feedback

Feedback can be prevented by various measures (see further information below):

- No switching of loads with a separate power supply
- Cable short-circuit fault exclusion (separate non-metallic sheathed cable, wiring only inside control cabinet, dedicated earth connection per conductor, fixed installation)

⚠ CAUTION

Interference-free EtherCAT Terminals

In the potential group connected through the EL2911, only interference-free standard terminals must be used. A list of the interference-free EtherCAT Terminals can be found in the Beckhoff Information System under <http://infosys.beckhoff.de>.

⚠ CAUTION

Maximum attainable safety level

Avoiding feedback through short-circuit fault exclusion:
 DIN EN ISO 13849-1: max. cat. 4 PL e
 IEC 61508: max. SIL3
 EN 62061: max. SIL2

⚠ CAUTION

Potential 0V

The 0 V potentials of the load (in this case K3, K4) must be identical to the 0 V potential of the power supply of the EL2911.

⚠ CAUTION

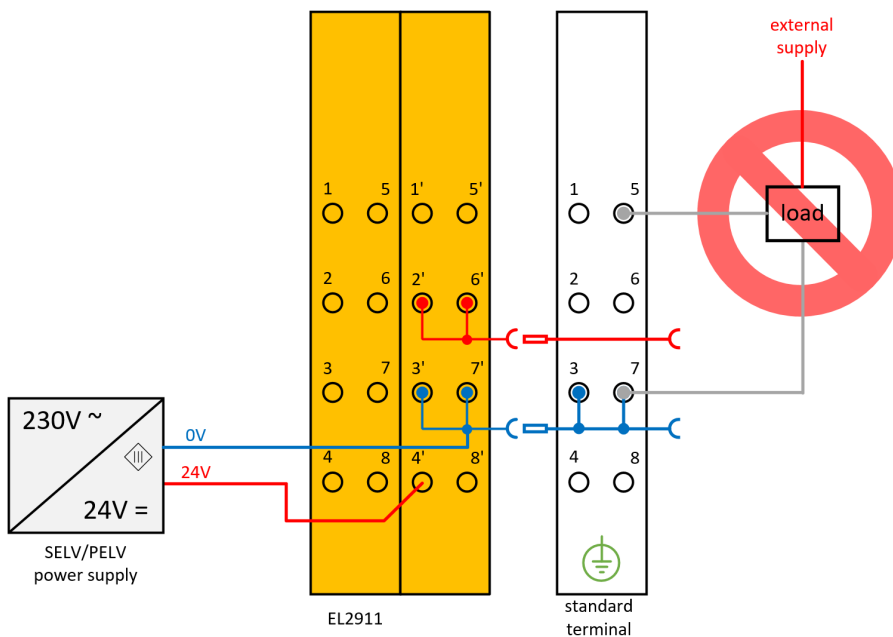
Time delay

Switching off the power supply for the potential group can delay the shutdown of the downstream contactors and actuators. This delay depends on the downstream actuators, loads and lines and must be taken into account by the user in the safety assessment.

4.3.1 Notes on prevention of feedback

4.3.1.1 No switching of loads with a separate power supply

Loads that have their own power supply must not be switched by standard terminals, since in this case feedback via the load cannot be ruled out.

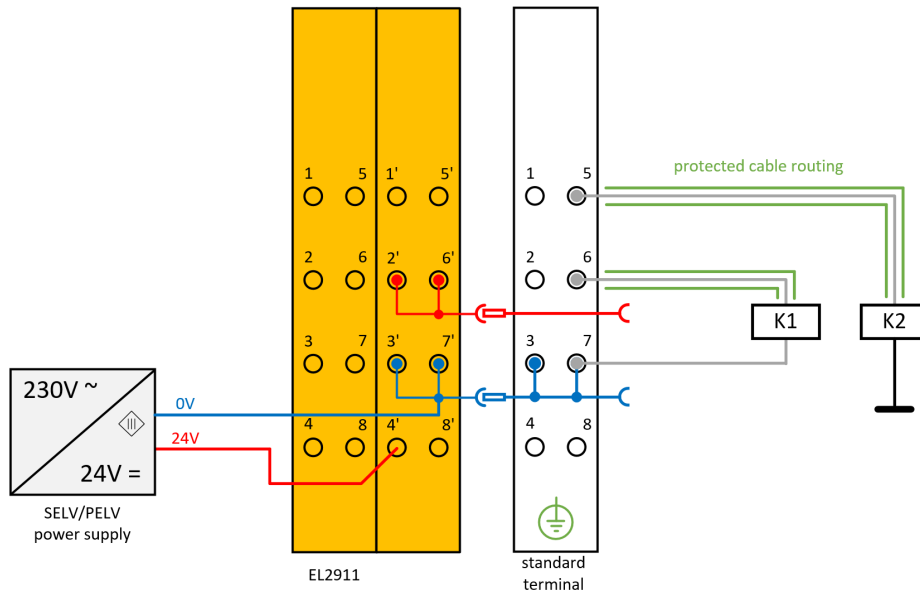


⚠ CAUTION

Manufacturer's data
 Exceptions to the general requirement are allowed only if the manufacturer of the connected load guarantees that feedback to the control input cannot occur.

4.3.1.2 Cable short-circuit fault exclusion

The danger of feedback on account of a cable short-circuit must be ruled out through further measures. The following measures can be implemented as an alternative.



- Alternative 1: Load connection via separate sheathed cables
 The non-safely switched potential of the standard terminal may not be conducted together with other potential-conducting lines inside the same sheathed cable
- Alternative 2: Wiring only inside the control cabinet
 All loads connected to the non-safe standard terminals must be located in the same control cabinet as the terminals. The cables are routed entirely inside the control cabinet.
- Alternative 3: Dedicated earth connection per conductor
 All conductors connected to the non-safe standard terminals are protected by a separate ground connection.
- Alternative 4: Permanent (fixed) wiring, protected from external damage
 All conductors connected to the non-safe standard terminals are permanently installed and protected from external damage, e.g. through a cable duct or an armored conduit.

⚠ CAUTION

Fault exclusion
 The machine manufacturer or the user is solely responsible for the correct execution and evaluation of the applied alternatives.

4.3.2 EL2911 parameters

EL2911

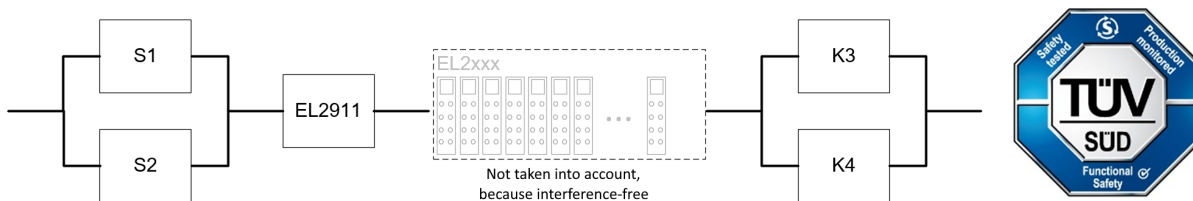
Parameter	Value
FSOUT Settings Common	-
0x8000:04 – Diag Testpulse active	TRUE
0x8000:12 – Output Cross Circuit Detection Delay	1000 ms
FSIN Settings Common	-
0x8010:02 - MultiplierDiagTestPulse	0x01
0x8010:04 – Diag TestPulse active	TRUE
FSIN Settings Channel	-
0x8011:01 – Channel 1.InputFilterTime	0x0014 (2 ms)
0x8011:02 – Channel 1.DiagTestPulseFilterTime	0x0002 (0.2 ms)
0x8011:04 – Channel 2.InputFilterTime	-
0x8011:05 – Channel 2.DiagTestPulseFilterTime	-
0x8011:07 – Channel 3.InputFilterTime	0x0014 (2 ms)
0x8011:08 – Channel 3.DiagTestPulseFilterTime	0x0002 (0.2 ms)
0x8011:0A – Channel 4.InputFilterTime	0x0014 (2 ms)
0x8011:0B – Channel 4.DiagTestPulseFilterTime	0x0002 (0.2 ms)

FB MON

Parameter	Value
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (port MonIn1/MonIn2)	500
Safe Inputs After Disc Error	TRUE

4.3.3 Block formation and safety loops

4.3.3.1 Safety function 1



4.3.4 Calculation

4.3.4.1 PFHD / MTTFD / B10D – values

Component	Value
EL2911 – PFH _D	4.50E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K3 – B10 _D	1,300,000
K4 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

4.3.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K3/K4 with EDM	DC _{avg} =90%

4.3.4.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0,1 * 7360} = 1358,7y = 11902212h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0,1 * 7360} = 2717,4y = 23804424h$$

K3/K4:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0,1 * 7360} = 1766,3y = 15472788h$$

and the assumption that S1, S2, K3 and K4 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,40E - 10$$

S2

$$PFH = \frac{1 - 0,99}{2717,4 * 8760} = 4,20E - 10$$

K3/K4

$$PFH = \frac{1 - 0,90}{1766,3 * 8760} = 6,46E - 09$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

The contactors K3 und K4 are both connected to the safety function. The non-functioning of a contactor does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K3 and K4 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through contactor contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL2911)} \\ + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1 - \beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{8,40E - 10 + 4,20E - 10}{2} + 4,50E - 09 + 10\% * \frac{6,46E - 09 + 6,46E - 09}{2} \\ = 5,21E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}}$$

If only PFH_D values are available for EL2911, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL2911)} = \frac{(1 - DC_{(EL2911)})}{PFH_{(EL2911)}} = \frac{(1 - 0,99)}{4,50E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{3,94E - 05 \frac{1}{y}} = 253y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{253y} + \frac{1}{1766,3y}} = 190y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(K3)}} + \frac{DC}{MTTF_{D(K4)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}} + \frac{1}{MTTF_{D(K4)}}$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{253y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{253y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 97,35\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC

Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2 ^(*)	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

(*) In accordance with EN 62061 chapter 6.7.7.2, SILCL is restricted to a maximum of SIL2 in relation to structural constraints for a subsystem that has an HFT of 0 and for which fault exclusions have been applied to faults that could lead to a dangerous failure.

4.4 EPP potential group with EPP9022-9060 (Category 4, PL e)

The protective door uses a combination of NC and NO contacts and is wired to safe inputs of the first EL2911 (1). Testing of the inputs is active, and the signals are checked for discrepancy (500 ms in this case). The 24 V supply Up of the potential group is switched off at the safe output of the second EL2911 (2). The 0 V connection is fed directly back to the 0 V of the power supply of the EL2911. The 0 V potentials of the two EL2911s are at the same potential or are bridged.

The feedback loop of the contactors K3 and K4 is connected to a safe input of the EL2911.

The 0 V potentials of all loads and devices that are used have to be at or connected to the same potential.

Diagnostics

No fault exclusion can be used for the EtherCAT p cable because Us and Up are located in a common sheathed cable and there is no dedicated earth connection per cable.

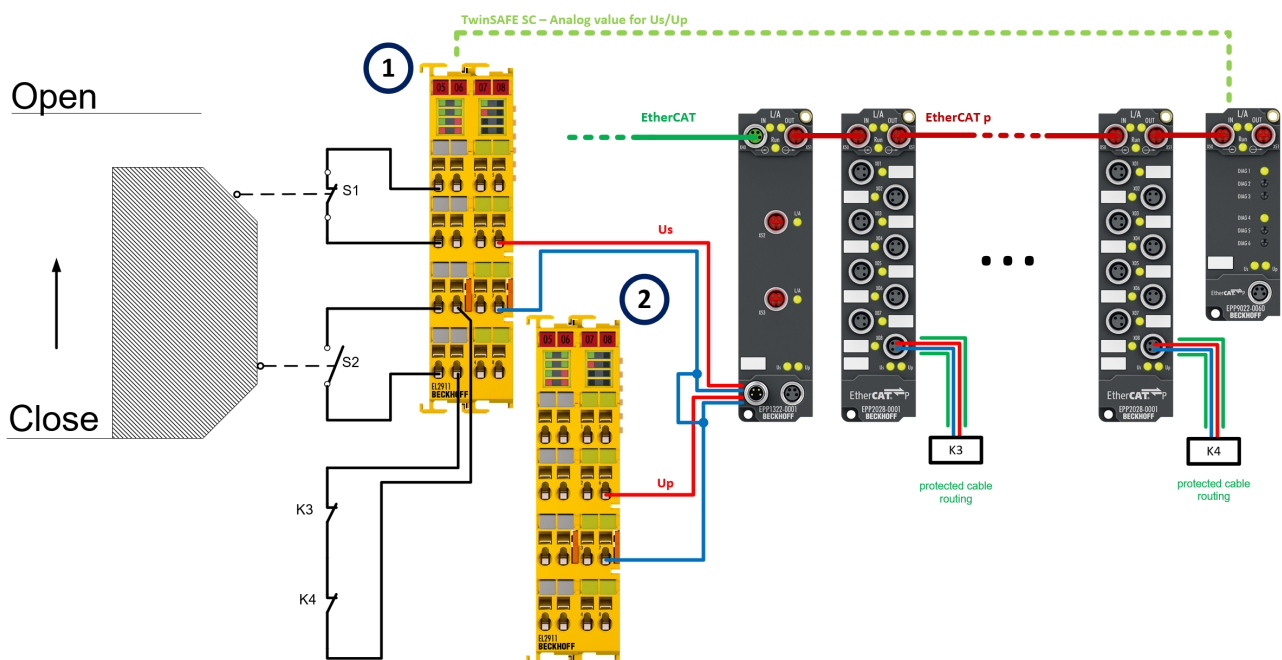
Firstly, for diagnosis of whether there is a feedback or cross-circuit on the EtherCAT p cable, the voltages Us and Up are measured by the EPP9022-9060 EtherCAT p Box and transmitted by TwinSAFE SC as an analog value to the EL2911. Corruption of the analog signals on the communication path is thus ruled out. Secondly, the EL2911 monitors a feedback to the 24 V_{DC} of the safe output and enters the module error state as soon as a voltage higher than 5 V is read in the switched-off state.

NOTE

Safety consideration

The EPP2xxx boxes used are not an active part of the safety controller. Accordingly, the safety level attained is defined only through the higher-level safety controller. The standard boxes are **not** incorporated in the calculation.

The external wiring of the standard boxes can lead to limitations in the maximum attainable safety level (See also [Notes on prevention of feedback \[▶ 164\]](#)).



⚠ CAUTION

Power supply unit requirements

The standard terminals must be supplied with 24 V_{DC} by an SELV/PELV power supply unit with an output voltage limit U_{max} of 36 V in the event of a fault.

⚠ CAUTION**Prevention of feedback**

Feedback can be prevented by various measures (see further information below):

- No switching of loads with a separate power supply
- Cable short-circuit fault exclusion (separate non-metallic sheathed cable, wiring only inside control cabinet, dedicated earth connection per conductor, fixed installation)

⚠ CAUTION**Maximum safety response time**

The maximum time for detecting a fault (Fault Detection Time) occurs when detecting of a fault by reading the feedback circuits of the contactors K3 and K4, as this time is typically very much longer than detection by reading back the voltages on the EL2911 and the EPP9022-9060. The time is set in the safety logic and should be set large enough to enable fast error detection, but so that the availability of the machine is also ensured.

The Fault Reaction Time results from the input filter time of the EL2911 (the safe input to which the feedback loop is connected), double the cycle time of the logic program running on the EL2911 (can also be read from the CoE objects) and the release time of the contactors K3 and K4 after the voltage at the output of the EL2911 has been switched off. The time is strongly dependent on the actuators employed.

These two times added together result in the Safety Response Time.

$$\begin{aligned} \text{SafetyResponseTime} &= \text{FaultDetectionTime} + \text{FaultReactionTime} \\ &= \text{EDMtime} + \text{InputfilterTimeEL2911} + 2 * \text{LogicCycleTime} + \text{SwitchOffTimeAktuators} \end{aligned}$$

This Safety Response Time must be referred to and checked by the user or machine manufacturer for the safety assessment of his application.

Safety application

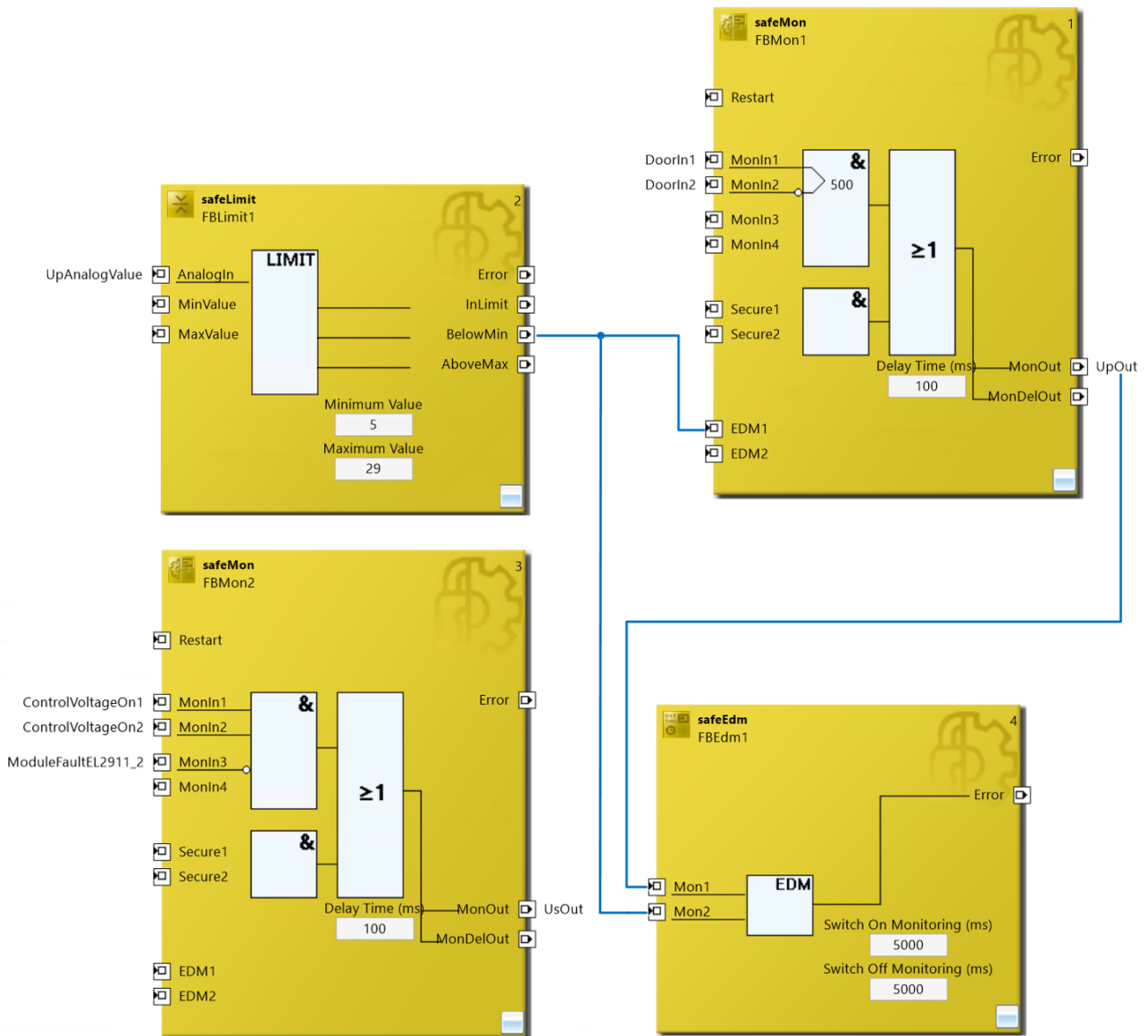
If the safe output of the EL2911 (2) for Up is switched off, the analog value for Up transmitted via TwinSAFE SC must signal a value smaller than 5 V. If this is not the case, both EL2911 outputs (1) + (2) must be switched off. This is implemented, for example, via an EDM function block, which is programmed in a TwinSAFE group with the outputs Us and Up and thus switches off the entire group and all outputs configured within it in case of error.

Furthermore, in the case of a module error, the EL2911 (2) for Up and the EL2911 (1) for Us must be switched off.

⚠ CAUTION**Implementation of the safety application**

The user or machine manufacturer is solely responsible for the correct implementation and testing of the safety application.

Example of a safety application



NOTE

Feedback loop

For clarity the feedback loop of the actuators K3 and K4 is not shown, but it must be taken into account by the user.

NOTE

Maximum attainable safety level

Avoiding feedback through short-circuit fault exclusion:
 DIN EN ISO 13849-1: max. cat. 4 PL e
 IEC 61508: max. SIL3
 EN 62061: max. SIL2

NOTE

Potential 0 V

The 0 V potentials of the load (in this case K3, K4) must be identical to the 0 V potential of the power supply of both EL2911s.

⚠ CAUTION

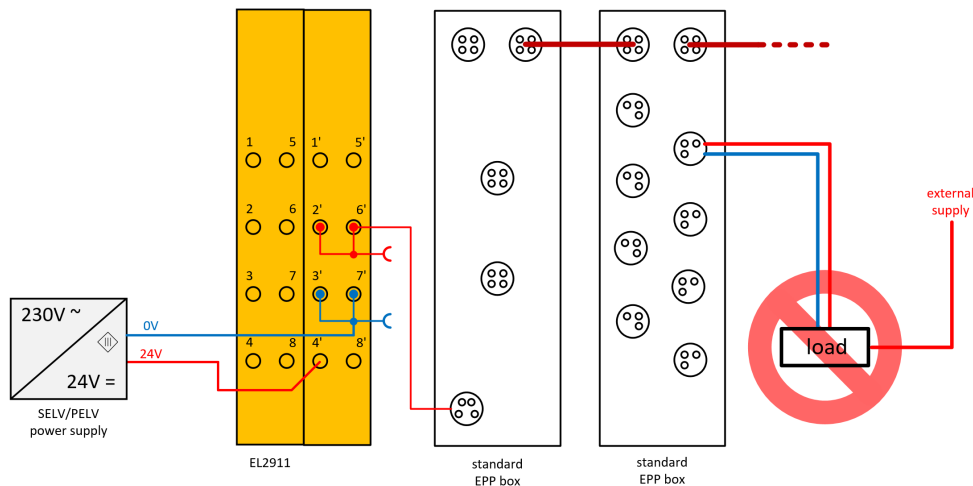
Time delay

Switching off the power supply for the potential group can delay the shutdown of the downstream contactors and actuators. This delay depends on the downstream actuators, loads and lines and must be taken into account by the user in the safety assessment.

4.4.1 Notes on prevention of feedback

4.4.1.1 No switching of loads with a separate power supply

Loads that have their own power supply must not be switched by standard boxes, since in this case feedback via the load cannot be ruled out.



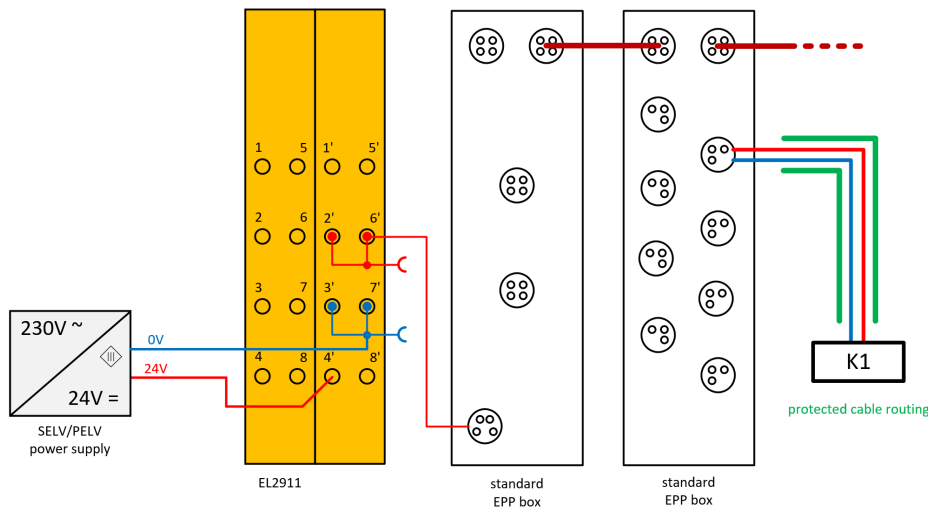
⚠ CAUTION

Manufacturer's data

Exceptions to the general requirement are allowed only if the manufacturer of the connected load guarantees that feedback to the control input cannot occur.

4.4.1.2 Cable short-circuit fault exclusion

The danger of feedback on account of a cable short-circuit must be ruled out through further measures. The following measures can be implemented as an alternative.



- Alternative 1: Load connection via separate sheathed cables
The non-safely switched potential of the standard terminal may not be conducted together with other potential-conducting lines inside the same sheathed cable
- Alternative 2: Wiring only inside the control cabinet
All loads connected to the non-safe standard terminals must be located in the same control cabinet as the terminals. The cables are routed entirely inside the control cabinet.
- Alternative 3: Dedicated earth connection per conductor
All conductors connected to the non-safe standard terminals are protected by a separate ground connection.
- Alternative 4: Permanent (fixed) wiring, protected from external damage
All conductors connected to the non-safe standard terminals are permanently installed and protected from external damage, e.g. through a cable duct or an armored conduit.

⚠ CAUTION

Fault exclusion
The machine manufacturer or the user is solely responsible for the correct execution and evaluation of the applied alternatives.

4.4.2 EL2911 parameters

EL2911 (applies to all EL2911s)

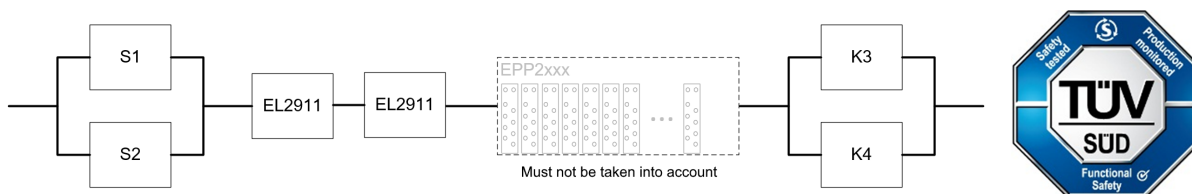
Parameter	Value
FSOUT Settings Common	-
0x8000:04 – Diag Testpulse active	TRUE
0x8000:12 – Output Cross Circuit Detection Delay	1000 ms
FSIN Settings Common	-
0x8010:02 - MultiplierDiagTestPulse	0x01
0x8010:04 – Diag TestPulse active	TRUE
FSIN Settings Channel	-
0x8011:01 – Channel 1.InputFilterTime	0x0014 (2 ms)
0x8011:02 – Channel 1.DiagTestPulseFilterTime	0x0002 (0.2 ms)
0x8011:04 – Channel 2.InputFilterTime	-
0x8011:05 – Channel 2.DiagTestPulseFilterTime	-
0x8011:07 – Channel 3.InputFilterTime	0x0014 (2 ms)
0x8011:08 – Channel 3.DiagTestPulseFilterTime	0x0002 (0.2 ms)
0x8011:0A – Channel 4.InputFilterTime	0x0014 (2 ms)
0x8011:0B – Channel 4.DiagTestPulseFilterTime	0x0002 (0.2 ms)

FB MON

Parameter	Value
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (port MonIn1/MonIn2)	500
Safe Inputs After Disc Error	TRUE

4.4.3 Block formation and safety loops

4.4.3.1 Safety function 1



4.4.4 Calculation

4.4.4.1 PFHD / MTTFD / B10D – values

Component	Value
EL2911 – PFH _D	4.50E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K3 – B10 _D	1,300,000
K4 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

4.4.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
K3/K4 with EDM	DC _{avg} =90%

4.4.4.3 Calculation of safety function 1

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0,1 * 7360} = 1358,7y = 11902212h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0,1 * 7360} = 2717,4y = 23804424h$$

K3/K4:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0,1 * 7360} = 1766,3y = 15472788h$$

and the assumption that S1, S2, K3 and K4 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,40E - 10$$

S2

$$PFH = \frac{1 - 0,99}{2717,4 * 8760} = 4,20E - 10$$

K3/K4

$$PFH = \frac{1 - 0,90}{1766,3 * 8760} = 6,46E - 09$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

The contactors K3 und K4 are both connected to the safety function. The non-functioning of a contactor does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K3 and K4 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through contactor contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL2911)} + PFH_{(EL2911)} \\ + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1 - \beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{8,40E - 10 + 4,20E - 10}{2} + 4,50E - 09 + 4,50E - 09 + 10\% * \frac{6,46E - 09 + 6,46E - 09}{2} \\ = 9,71E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}}$$

If only PFH_D values are available for EL2911, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL2911)} = \frac{(1 - DC_{(EL2911)})}{PFH_{(EL2911)}} = \frac{(1 - 0,99)}{4,50E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{3,94E - 05 \frac{1}{y}} = 253y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{253y} + \frac{1}{253y} + \frac{1}{1766,3y}} = 108y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(K3)}} + \frac{DC}{MTTF_{D(K4)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}} + \frac{1}{MTTF_{D(K4)}}$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{253y} + \frac{99\%}{253y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{253y} + \frac{1}{253y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 98,00\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC

Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2 ^(*)	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

(*) In accordance with EN 62061 chapter 6.7.7.2, SILCL is restricted to a maximum of SIL2 in relation to structural constraints for a subsystem that has an HFT of 0 and for which fault exclusions have been applied to faults that could lead to a dangerous failure.

5 STO/SS1 functions

5.1 AX8xxx-x1xx STO function (Category 4, PL e)

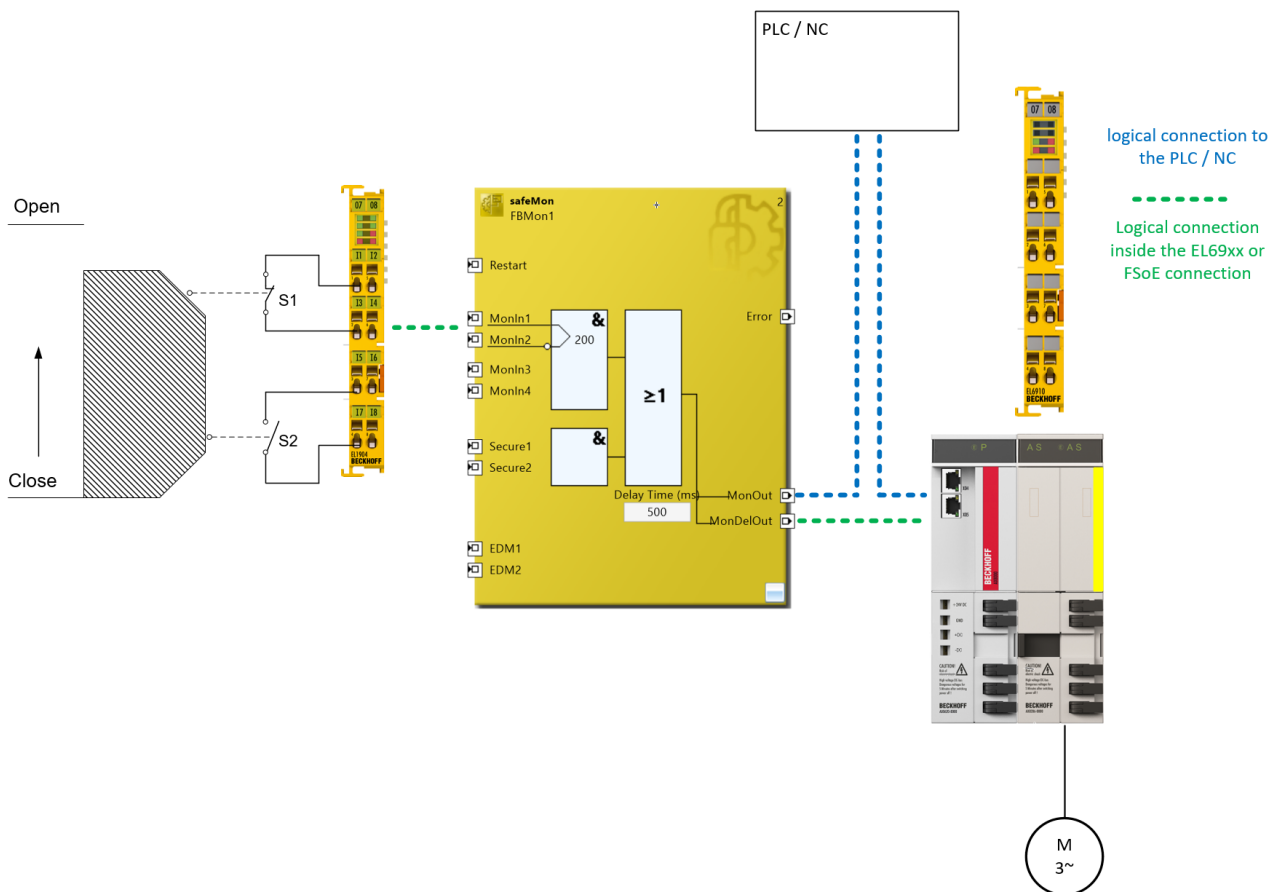
The protective door is wired with an NC/NO contact combination to safe inputs of an EL1904. The test pulses of the inputs are activated. Within the TwinSAFE logic the protective door is connected to an FB Mon and the directly switching output is used to inform the NC controller that, for example in 500 ms, an STO will be executed and a stop ramp is therefore to be driven.

After 500 ms, for example, the AX8xxx-x1xx will be informed via the delayed-switching output that STO is to be activated.

In this example it is assumed that, with the opening of the door and the delayed switching of the AX8xxx-x1xx, the machine is in a safe state after STO before the hazard point can be reached by the user.

The machine manufacturer must assess the machine and the application.

If another application is to be executed on the drive, this can be implemented through a customer-specific logic application on the AX8xxx-x1xx.



5.1.1 Parameters of the safe input and output modules

EL1904

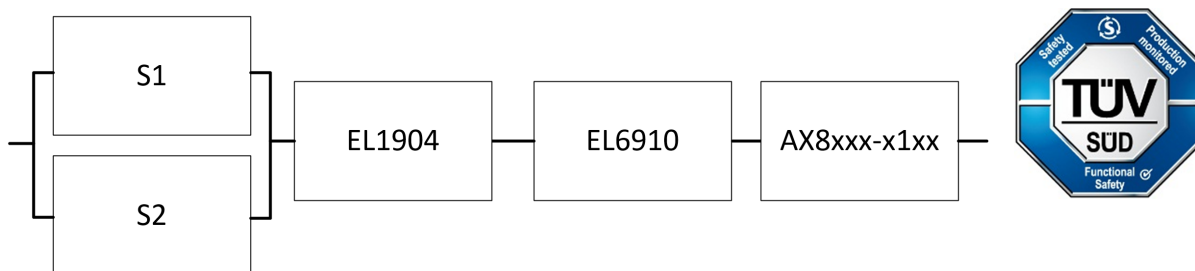
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	-
Sensor test channel 4 active	-
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

MON FB parameter

Parameter	Value
Discrepancy Time (ms) (port MonIn1/MonIn2)	200
Safe Inputs After Disc Error	TRUE
MON Delay Time	500

5.1.2 Block formation and safety loops

5.1.2.1 Safety function 1



5.1.3 Calculation

5.1.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL6910 – PFH _D	1.79E-09
AX8xxx-x1xx - PFH _D	3.04E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

5.1.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing and plausibility check	DC _{avg} = 99%
AX8xxx-x1xx STO function	DC _{avg} > 99%

5.1.3.3 Calculation of safety function 1

Calculation of the performance level according to EN ISO 13849-1:2015

Calculation of the MTTF_D values from the B10_D values

From:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1 * 14720} = 679y$$

S2

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358y$$

The total MTTF_D value is calculated based on the following formula:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}$$

If only PFH_D values are available for EL1904, EL6910 and AX8xxx-x1xx, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(A\bar{X}8xxx-x1.xx)} = \frac{(1 - DC_{(A\bar{X}8xxx-x1.xx)})}{PFH_{D(A\bar{X}8xxx-x1.xx)}} = \frac{(1 - 0,99)}{3,04E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{2,66E - 05 \frac{1}{y}} = 375y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679y} + \frac{1}{1028y} + \frac{1}{637y} + \frac{1}{375y}} = 149y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL1904)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(A\bar{X}8xxx-x1.xx)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(A\bar{X}8xxx-x1.xx)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{679y} + \frac{99\%}{1358y} + \frac{99\%}{1028y} + \frac{99\%}{637y} + \frac{99\%}{375y}}{\frac{1}{679y} + \frac{1}{1358y} + \frac{1}{1028y} + \frac{1}{637y} + \frac{1}{375y}} = 99,00\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

⚠ CAUTION**Implement a restart lock in the machine!**

The restart lock is **NOT** part of the safety chain and must be implemented in the machine!

MTTF_D

Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC

Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Calculation of PFH_D values according to EN 62061

with the assumption that S1 and S2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH_D = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH_D = \frac{1 - 0,99}{679 * 8760} = 1,68E - 09$$

S2:

$$PFH_D = \frac{1 - 0,99}{1358 * 8760} = 8,41E - 10$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100,000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{Dges} = \beta * \frac{PFH_{D(S1)} + PFH_{D(S2)}}{2} + (1 - \beta)^2 * (PFH_{D(S1)} * PFH_{D(S2)}) * T1 + PFH_{D(EL1904)} + PFH_{D(EL6910)} + PFH_{D(AX8xxx-x1xx)}$$

Since the portion $(1 - \beta)^2 * (PFH_{D(S1)} * PFH_{D(S2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{Dges} = 10\% * \frac{1,68E - 09 + 8,41E - 10}{2} + 1,11E - 09 + 1,79E - 09 + 3,04E - 09$$

$$= 6,07E - 09$$

Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

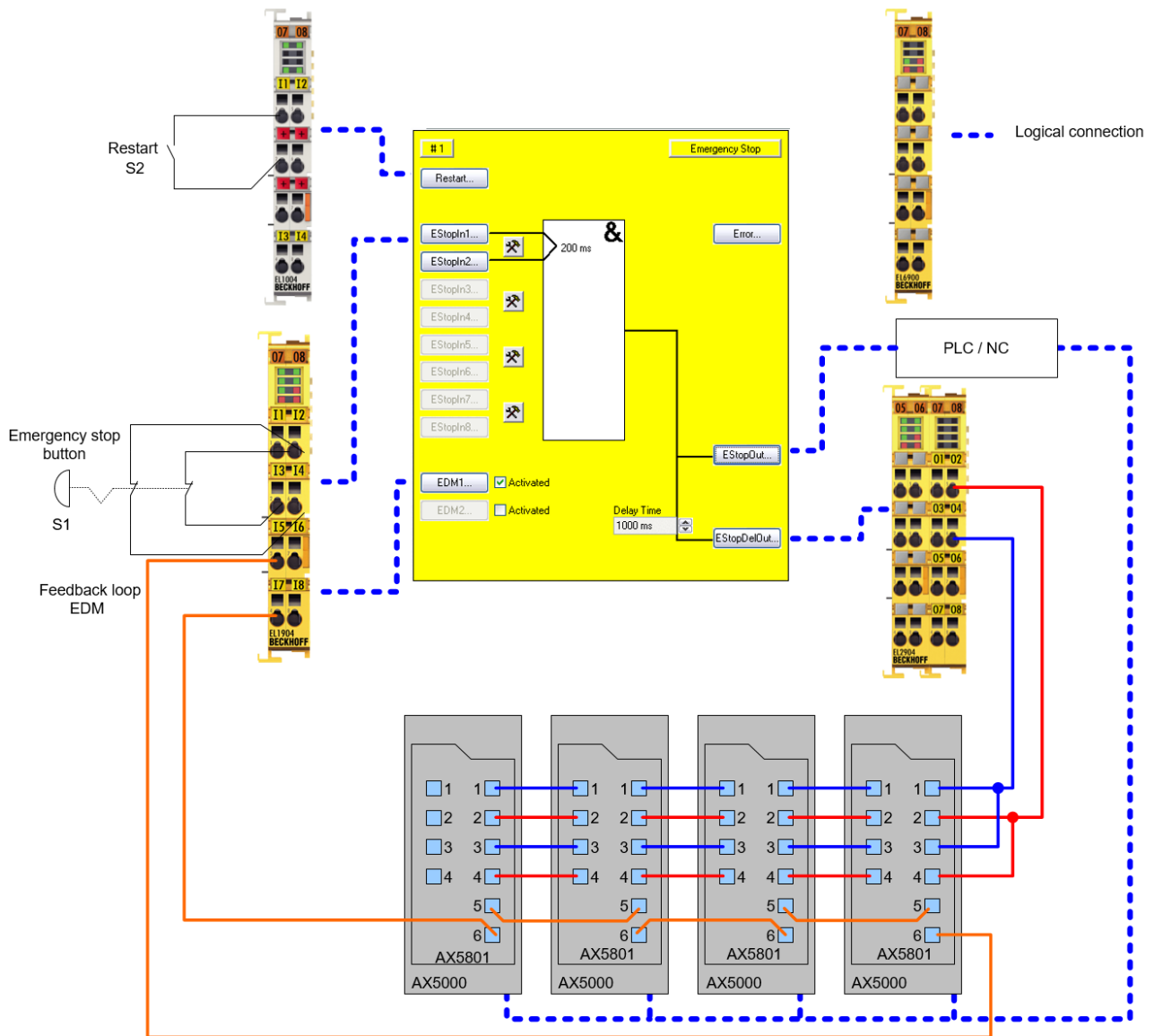
NOTE**Safety integrity level**

The application meets the requirements of safety integrity level SIL3 according to EN 62061.

5.2 Drive option AX5801 with SS1 stop function (Category 4, PL e)

By activating the emergency stop button inputs EStopIn1 and EStopIn2 of FB ESTOP are switched to state “0”, resulting in outputs EStopOut and EStopDelOut of FB ESTOP being switched to state “0”. As a result, a quick stop command is issued to the PLC and therefore the AX5000 via EtherCAT. The output EStopDelOut of the ESTOP FB ensures that, after the expiry of a specified delay time (in this case e.g. 1000 ms), the 24 V supply of the safety option AX5801 is interrupted and the internal relays of the AX5801 are thus de-energized. The two channels (motors) are switched torque-free via the internal switch-off paths of the AX5000.

Testing and checking for discrepancy are activated for the input signals. The testing of the outputs is also active. The relays of the 4 AX5801 option cards are wired in parallel to a safe output of the EL2904. The feedback loops are wired in series to a safe input. The restart signal is wired to a non-safe input.



5.2.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

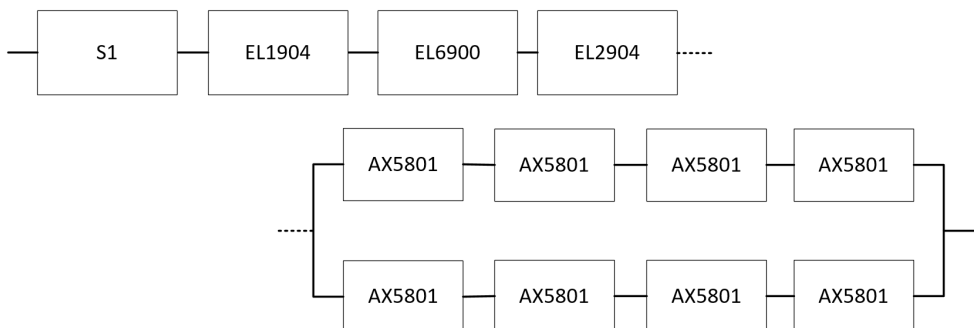
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

5.2.2 Block formation and safety loops

5.2.2.1 Safety function 1



5.2.3 Calculation

5.2.3.1 PFHD / MTTF_D / B10_D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
AX5801 – B10 _D	780,000
S1 – B10 _D	100,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

5.2.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
AX5801	DC _{avg} =99%

5.2.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0,1 * 1840} = 543,5y = 4761060h$$

AX5801:

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{780.000}{0,1 * 1840} = 4239,1y = 37134516h$$

$$T_{10D} = \frac{B10_D}{n_{op}} = \frac{780.000}{1840} = 423y$$

and the assumption that S1 is single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{543,5 * 8760} = 2,10E - 09$$

AX5801:

$$PFH = \frac{1 - 0,99}{4239,1 * 8760} = 2,70E - 10$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{4 * PFH_{(AX5801)} + 4 * PFH_{(AX5801)}}{2} + 4 * (1 - \beta)^2 * (PFH_{(AX5801)} * PFH_{(AX5801)}) * T1$$

Since the portion $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 2,10E - 09 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{4 * 2,70E - 10 + 4 * 2,70E - 10}{2} = 5,60E - 09$$

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(AX5801)} = \frac{B10_{D(AX5801)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{543,5y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y}} = 173,8y$$

$$DC_{avg} = \frac{\frac{99\%}{543,5y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y}}{\frac{1}{543,5y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y}} = 99,00\%$$

NOTE**Category**

This structure is possible up to category 4 at the most.

⚠ CAUTION**Implement a restart lock in the machine!**

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF_D

Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC

Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE**Diagnostic coverage**

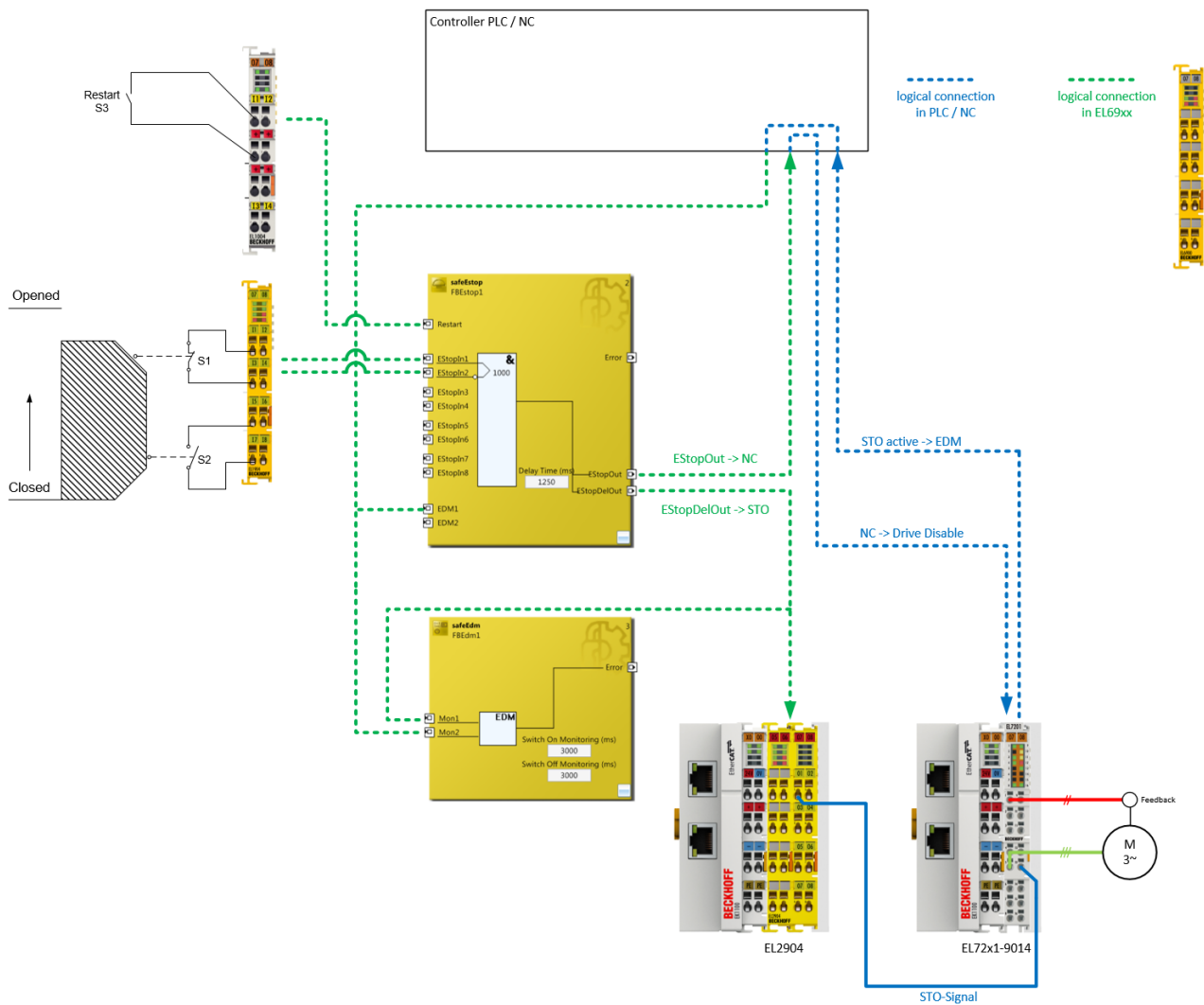
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

5.3 STO function with EL72x1-9014 (category 3, PL d)

The following application example shows how the EL72x1-9014 can be wired together with an EL2904 in order to implement an STO function according to EN 61800-5-2.

A protective door (S1 and S2) and a restart signal (S3) are logically linked on an EStop function block. The EStopOut signal is transferred to the NC controller, with which, for example, the Enable signal of the EL72x1-9014 can be switched. The STO input of the EL72x1-9014 is operated via the delayed output EStopDelOut. The EL72x1-9014 supplies the information that the STO function is active via the standard controller. This information is transferred to the EDM input of the EStop function block and additionally to the EDM function block in order to generate an expectation for this signal.



⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

If the risk analysis returns the result that a restart is to be realized in the safety controller, then the restart **must** also be placed on a safe input.

⚠ WARNING**Wiring only inside the control cabinet**

The wiring between the EL2904 and the STO input of the EL72x1-9014 must be located in the same control cabinet in order to be able to assume a fault exclusion for the cross-circuit or external power supply of the wiring between EL2904 and EL72x1-9014.

The evaluation of this wiring and the evaluation of whether the fault exclusion is permissible must be done by the machine manufacturer or user.

NOTE**Calculation EL72x1-9014**

The EL72x1-9014 is not taken into account in the calculation of the Performance Level according to DIN EN ISO 13849-1 since it behaves interference-free to the safety function.

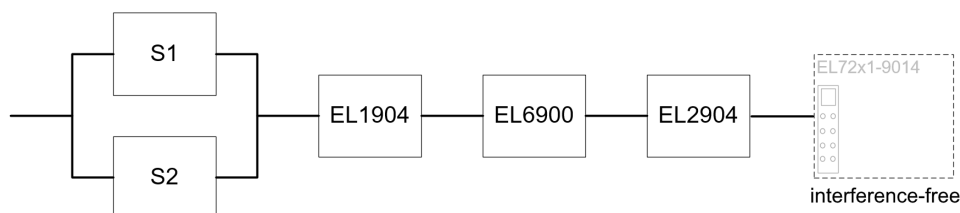
The PFH_p value goes into the calculation according to EN 62061 with a value of 0.

5.3.1 Parameters of the safe input and output terminals**EL1904**

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

5.3.2 Block formation and safety loops**5.3.2.1 Safety function 1**

5.3.3 Calculation

5.3.3.1 PFHD / MTTF_D / B10_D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
EL72x1-9014 - PFH _D	0.00
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

5.3.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
EL2904 with testing	DC _{avg} =99%

5.3.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1 * 14720} = 679,3y = 5951087h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

and the assumption that S1 and S2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{679,3 * 8760} = 1,68E - 09$$

S2:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(EL72x1-9014)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{1,68E - 09 + 1,68E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 0,00 = 3,558E - 09$$

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL6900 and EL2904, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 225,2y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 99,00\%$$

⚠ CAUTION**Category**

This structure is possible up to category 3 at the most.

MTTF_D

Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC

Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE**Diagnostic coverage**

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

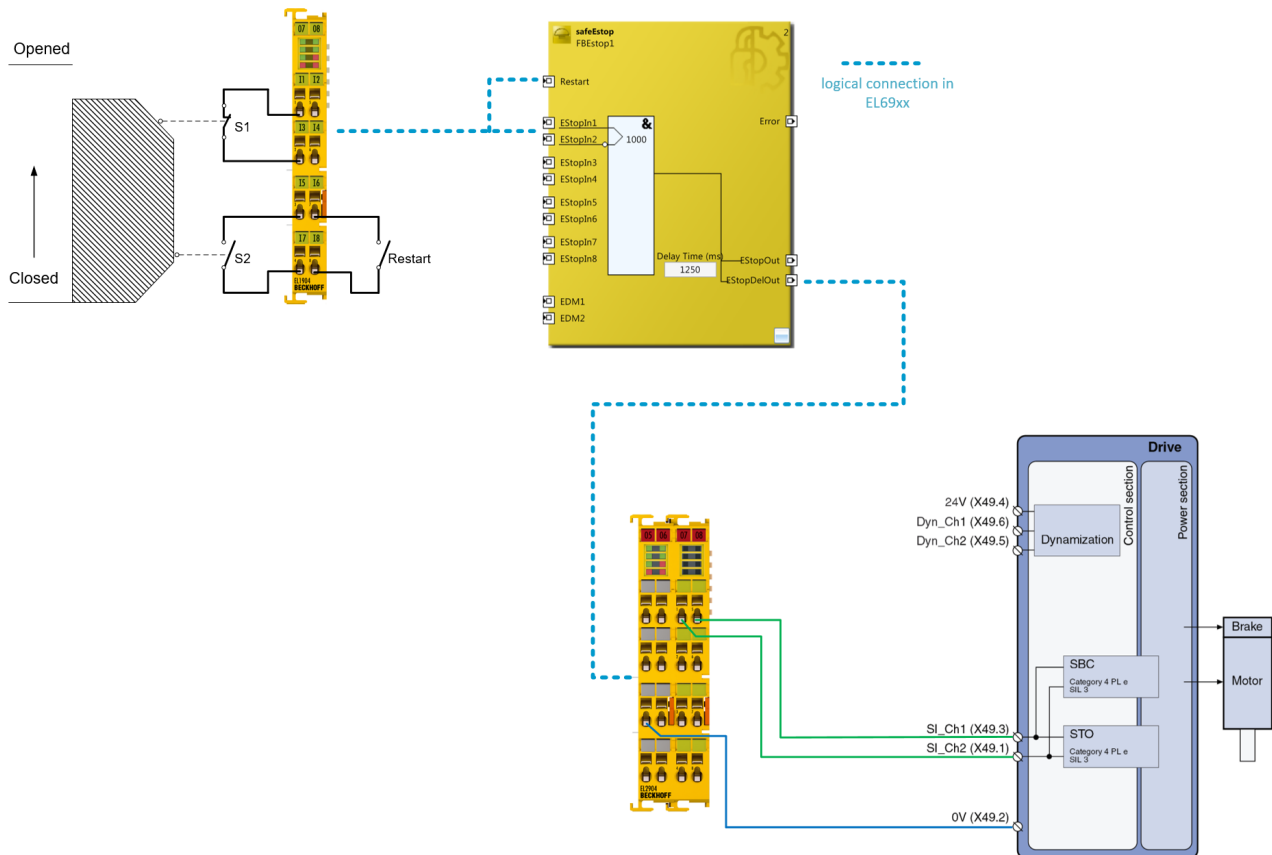
Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

5.4 STO function with IndraDrive (category 4, PL e)

The following example shows the application of the safe EL2904 outputs in conjunction with a BOSCH Rexroth IndraDrive for realizing an STO function on this drive.

As an example, a protective door is wired to a safe input (in this case EL1904) together with a restart signal in two-channel mode. Within the TwinSAFE Logic, these signals are used at an ESTOP function block. Switching of the ESTOP function block is delayed and is used for the two safe EL2904 outputs. The EStopOut output can be used to stop the drive electrically via the NC controller .

One output of the EL2904 is wired to STO input X49.1 of the Bosch Rexroth IndraDrive, the other output is wired to X49.3. The corresponding GND connection (X49.2) is taken back to the EL2904 to illustrate that the EL2904 and the IndraDrive use the same ground potential of the 24 V supply.



⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is **NOT** part of the safety chain and must be implemented in the machine!

5.4.1 Parameters of the safe input and output terminals

EL1904

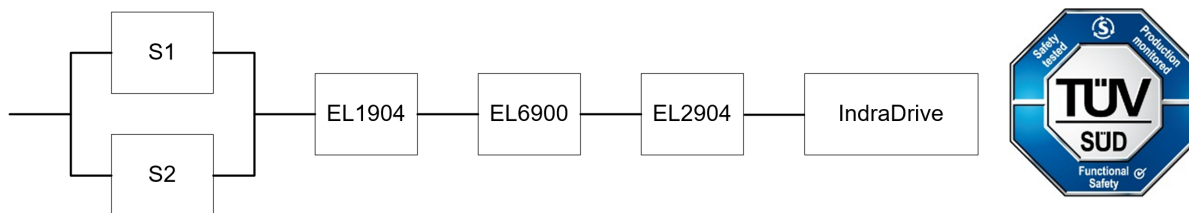
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

5.4.2 Block formation and safety loops

5.4.2.1 Safety function 1



5.4.3 Calculation

5.4.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
Bosch Rexroth IndraDrive ¹⁾ - PFH _D	0.50E-09
Bosch Rexroth IndraDrive ¹⁾ - MTTFD	> 200 years
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

¹⁾ Please note the information provided in the Bosch Rexroth user documentation

5.4.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%
EL2904 with testing	DC _{avg} =99%
Bosch Rexroth IndraDrive ¹⁾	DC _{avg} =99%

¹⁾ Please note the information provided in the Bosch Rexroth user documentation

5.4.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1 * 14720} = 679,3y = 5951087h$$

S2:

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1 * 14720} = 1358,7y = 11902174h$$

and the assumption that S1 and S2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{679,3 * 8760} = 1,68E - 09$$

S2:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,4E - 10$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(IndraDrive)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{1,68E-09 + 8,40E-10}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09 + 0,50E-09 = 4,016E-09$$

NOTE

Calculation according to EN 62061

This value corresponds to SIL3, according to EN 62061, Table 3.

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(IndraDrive)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(IndraDrive)} = 200y$$

If only PFH_D values are available for EL1904, EL6900 and EL2904, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09 * \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E-06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09 * \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E-06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{200y}} = 105,9y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{200y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{200y}} = 99,00\%$$

NOTE

Category
This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

5.4.4 Technical Note from Bosch Rexroth AG



Technical Note

Bosch Rexroth AG
Postfach 1357
97803 Lohr am Main
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr am Main
Tel. +49 9352 18-0
Fax +49 9352 18-8400
www.boschrexroth.com

09. März 2017

Sehr geehrte Damen und Herren,

Folgend bestätigen wir Ihnen die Anwendungsbedingungen für die sichere Anwahl von Sicherheitsfunktionen unseres IndraDrive.

Die Anwendungsbedingungen gelten für die IndraDrive Antriebsfamilien Cs, C/M, Mi, ML mit folgenden Sicherheitsoptionen

- L3, L4: Anwahl über Klemme X49 des Steuerteils
- S4, S5: Anwahl über Klemme X41 des Sicherheitszonenmoduls HSZ01

Die Installations- und Projektierungshinweise in der Kundendokumentation sind zu beachten.

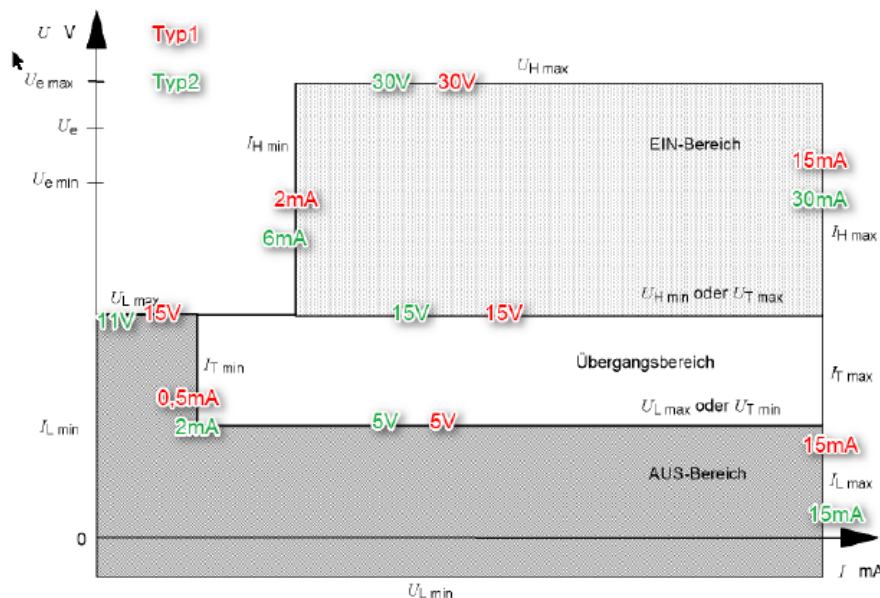
1 Safety Anforderungen

09. März 2017
Seite 2 von 4

Die Anforderungen von Kat.4 Ple nach EN 13849 bzw. SIL 3 gemäß EN 61062 sind für die sichere Anwahl der Sicherheitsfunktionen des Antriebssystems IndraDrive gegeben, wenn die Ansteuereinheit (z.B EL2904 Fa. Beckhoff) folgende Anwendungsbedingungen erfüllt:

1.1 Elektrische Anforderungen

Die sicheren Eingänge verhalten sich konform zur IEC61131-2, Typ 2 (Sicherheitsoption L3, L4) bzw. Typ 1 (Sicherheitsoption S4, S5). Entsprechend muss der Ausgang der aktiven Ansteuereinheit folgende Pegel für das Low-Signal einhalten. Im einfachen Fall liegt das Low-Signal vor, wenn die Ausgangsspannung <5V und der Leckstrom Ausgangstufe <0,5mA ist.



1.2 Durch Testungen des Ausgangs der Ansteuereinheit werden folgende Fehler aufgedeckt.

- Kurzschluss der Anwahlsignale mit 24 V
- Kurzschluss zwischen den beiden Anwahlsignalen

Dies entspricht dem Verhalten von OSSD-Ausgängen

2 Funktionale Anforderungen an die Anwahl (für Verfügbarkeit)

09. März 2017
Seite 3 von 4

Folgende funktionale Anforderungen an die Testimpulse der aktiven Ansteuereinheit müssen erfüllt sein.

2.1 Anforderung IndraDrive mit Sicherheitsoption L3/L4

Zweikanalige Anwahl über Klemme X49 (Eingang nach IEC 61131-2, Typ 2)

Dynamisierungspulse der OSSD-Ausgänge folgende Grenzwerte einhalten:

	Wert	Erklärung
$t_{PL,max}$	1 ms	maximale Low-Zeit des Testpulses
$t_{PL,min}$	20 μ s	minimale Low-Zeit des Testpulses
$t_{P,max}$	1 h	maximale Periodendauer der Testpulse
$t_{P,min}$	500 μ s	minimale Periodendauer der Testpulse
$t_{V,max}$	1 s	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{D,min} = t_{PH} / t_P$	90 %	minimales Tastverhältnis der Anwahlsignale
$t_{PH,max}$	400 ms	maximale Preldauer bei einer An- oder Abwahl
φ	-	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

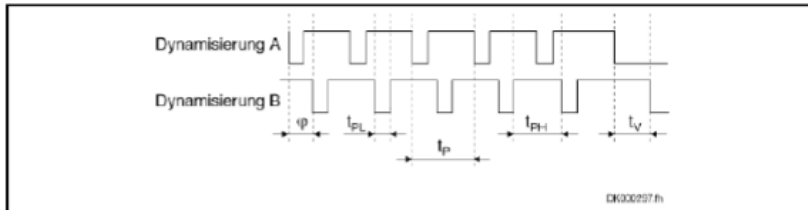
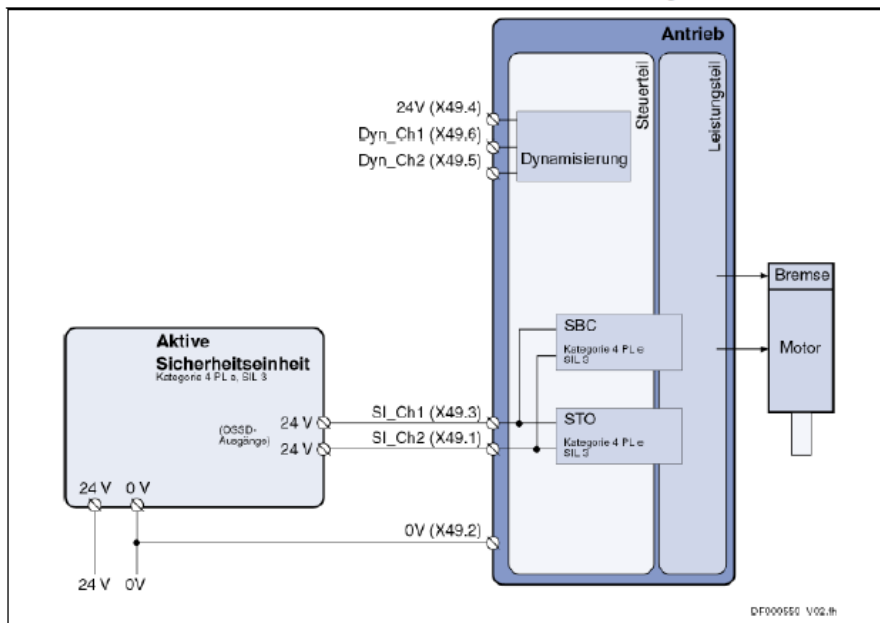


Abb. 5-2: Beispiel für dynamisierte Anwahlsignale



2.2 Anforderung IndraDrive mit Sicherheitsoption S4, S5

Zweikanalige Anwahl über Klemme X41 des Sicherheitszonenmoduls HSZ01 (Eingang nach IEC 61131-2, Typ 1)

09. März 2017
Seite 4 von 4

Grenzwert	Erklärung
$t_{PL,max} = 1 \text{ ms}$	maximale Low-Zeit des Testpulses
$t_{PL,min} = 0 \text{ ms}$	minimale Low-Zeit des Testpulses
$t_{V,max}^{1)} = 1 \text{ s}$	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{C,min} = t_{PH} / t_P = 90 \%$	minimales Tastverhältnis der Anwahlsignale
$t_{C,max} = t_{PH} / t_P = 100 \%$	maximales Tastverhältnis der Anwahlsignale
$t_{P,rel} = 400 \text{ ms}$	maximale Prelldauer bei einer An- oder Abwahl
$\phi^{1)} = -$	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

¹⁾ gilt nur bei zweikanaliger Anwahl
Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

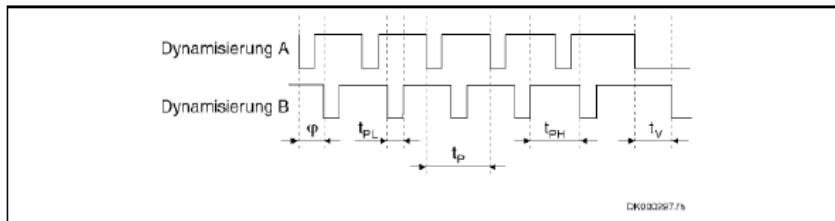


Abb. 5-1: Beispiel für dynamisierte Anwahlsignale

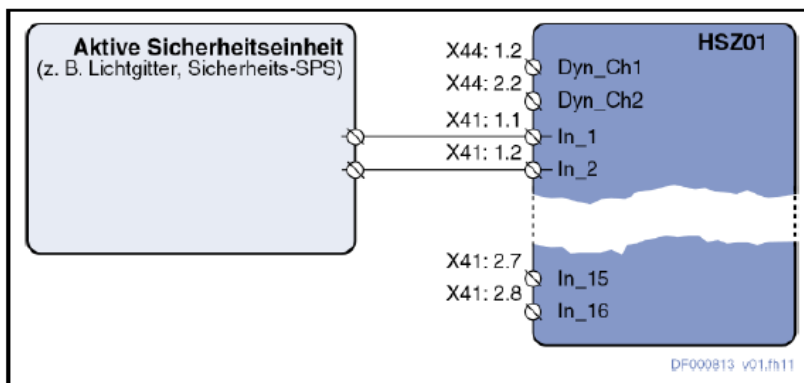


Abb. 5-2: Dynamisierung bei Anwahl über eine aktive Sicherheitseinheit

Diese Bestätigung gilt bis auf Widerruf.

Mit freundlichen Grüßen

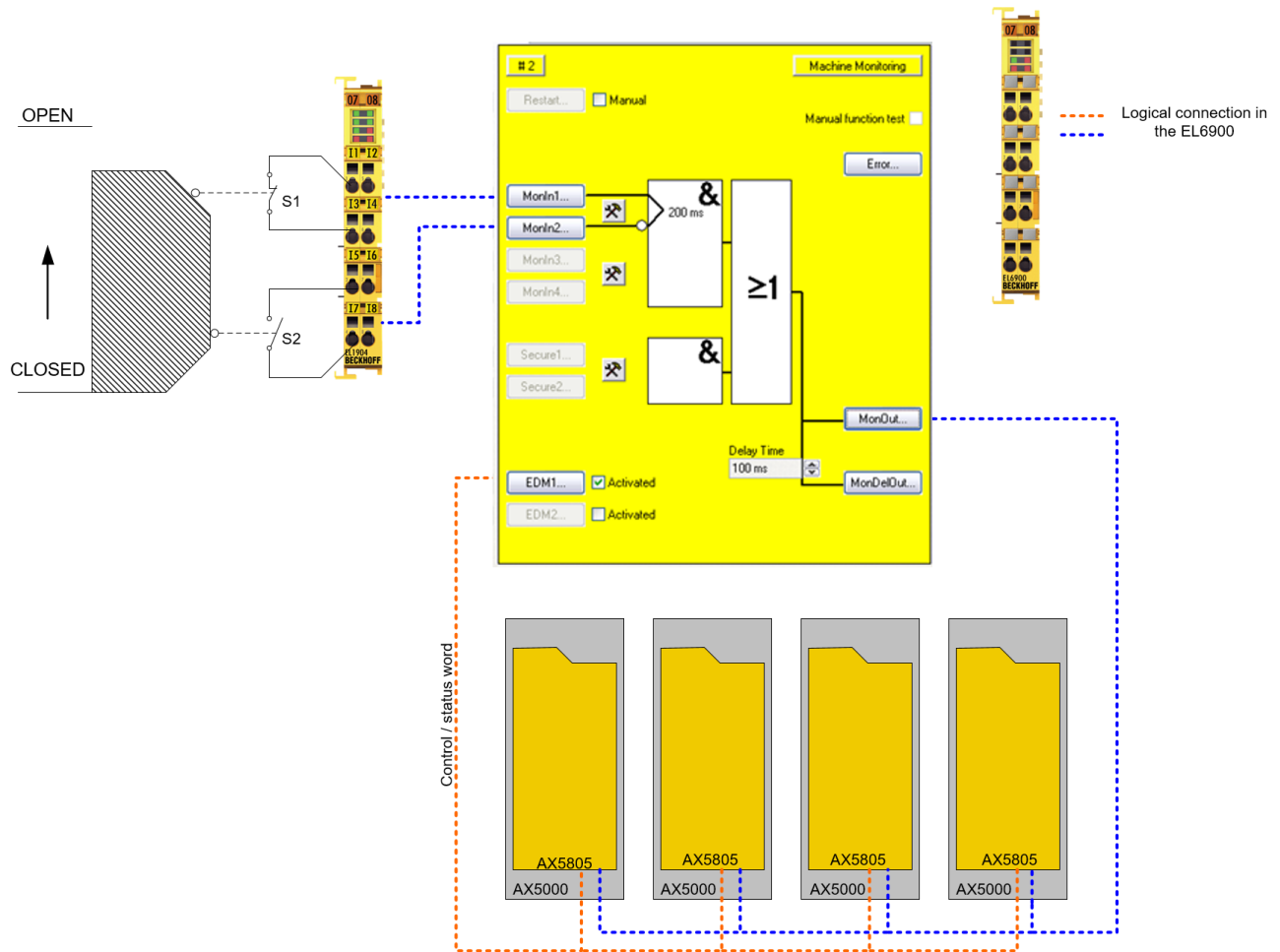
Bosch Rexroth AG (DC-IA/EDY)

6 Safe Motion functions

6.1 Drive option AX5805 with SS2 stop function (Category 4, PL e)

The protective door is connected with a combination of normally closed and normally open contacts to an EL1904 safe input terminal. Testing and checking for discrepancy are activated for the input signals. The output is linked on the AX5805.

The feedback signals are checked via the control and status word returned by the drive option.



6.1.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

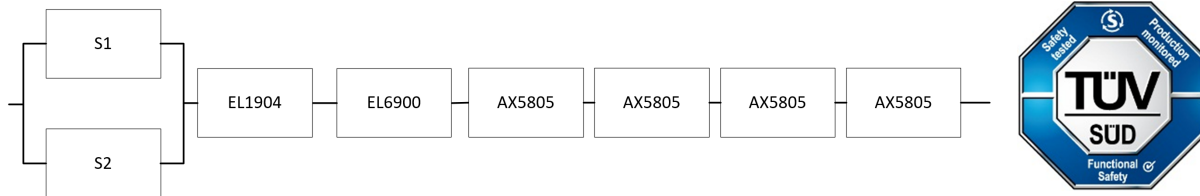
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

AX5805

Parameter	Value
-	

6.1.2 Block formation and safety loops

6.1.2.1 Safety function 1



6.1.3 Calculation

6.1.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL6900 – PFH _D	1.03E-09
AX5805 – PFH _D	5.15E-09 (see list of approved motors)
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

6.1.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC _{avg} =99%

6.1.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{1.000.000}{0,1 * 1840} = 5434,8y = 47608848h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{2.000.000}{0,1 * 1840} = 10869,6y = 95217696h$$

and the assumption that S1 and S2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{5434,8 * 8760} = 2,10E - 10$$

S2:

$$PFH = \frac{1 - 0,99}{10869,6 * 8760} = 1,05E - 10$$

The following assumptions must now be made:

The door switches S1/S2 are always actuated in opposite directions. Since the switches have different values, but the complete protective door switch consists of a combination of normally closed and normally open contacts and both switches must function, the poorer of the two values (S1) can be taken for the combination!

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains a table with which this β -factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(AX5805)} + PFH_{(AX5805)} + PFH_{(AX5805)} + PFH_{(AX5805)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{2,10E - 10 + 1,05E - 10}{2} + 1,11E - 09 + 1,03E - 09 + 4 * 5,15E - 09 = 2,28E - 08$$

Calculation of the $MTTF_D$ value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, AX5805 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(AX5805)} = \frac{(1 - DC_{(AX5805)})}{PFH_{(AX5805)}} = \frac{(1 - 0,99)}{5,15E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{4,51E - 05 \frac{1}{y}} = 221,7y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{5434,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y}} = 49,8y$$

$$DC_{avg} = \frac{\frac{99\%}{5434,8y} + \frac{99\%}{10869,6y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y}}{\frac{1}{5434,8y} + \frac{1}{10869,6y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y}} = 99,00\%$$

NOTE

Category
 This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

7 Analog value processing with TwinSAFE SC

7.1 Speed monitoring (category 3, PL d)

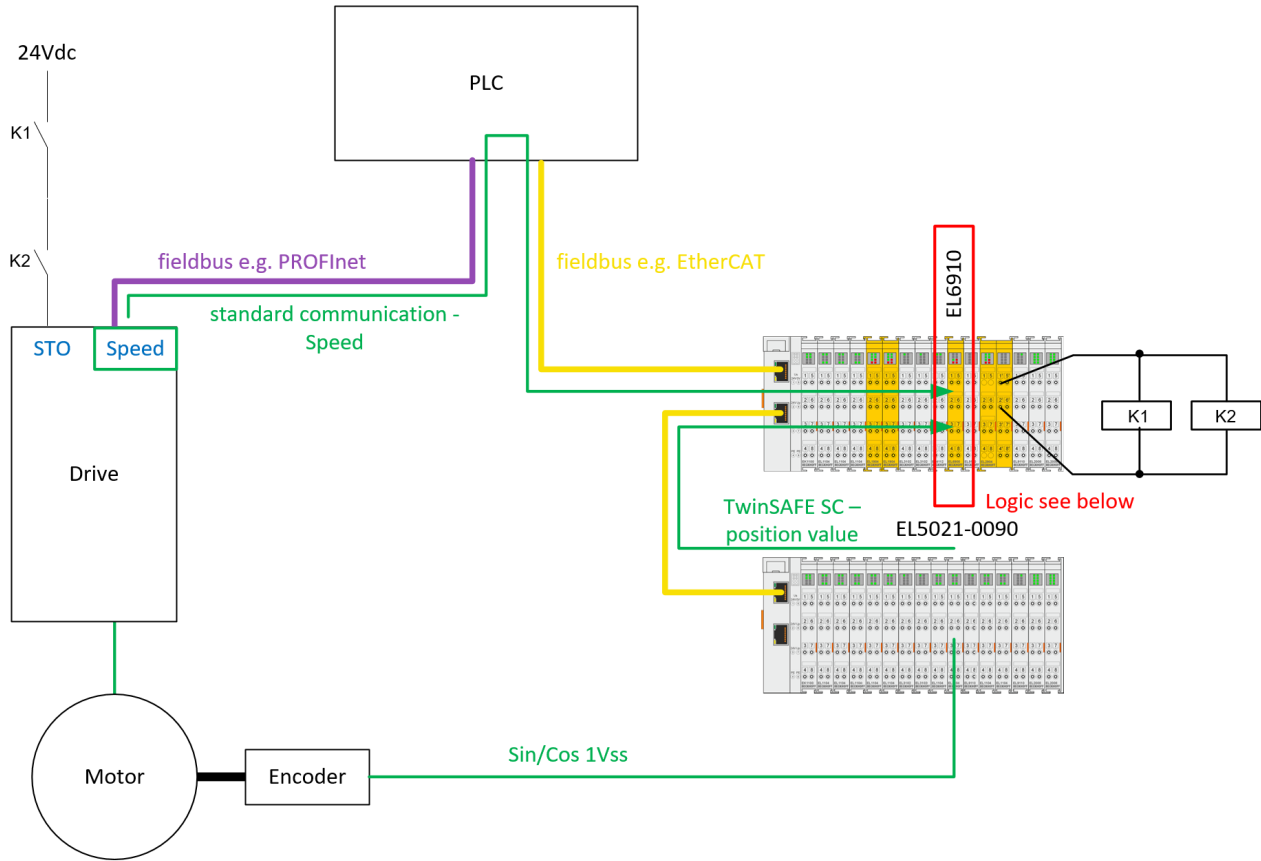
The speed of a drive is to be monitored. This drive has a safety function (in this case, for example, STO), which is activated via a corresponding input. This input is conducted through one working contact of each of two contactors. The position and speed signals are transmitted via two different communication paths to the EL6910 TwinSAFE Logic and processed there according to the illustrated logic. The sin/cos encoder is wired to an EL5021-0090, and the position information is transferred via TwinSAFE SC communication and EtherCAT. The drive speed is also transferred to the EL6910 TwinSAFE Logic, via the standard PROFINET communication (any other fieldbus is also possible) and the standard PLC.

A speed (Speed FB) is calculated from the position value within the safety-related EL6910 logic. The speed of the drive is scaled via the FB so that the value matches the calculated speed. These two speed values are checked by a Compare FB for equality and monitored by a Limit FB for a maximum value. Since the two speed values (one calculated directly and the other calculated in the safety-related EL6910 logic) are never 100% equal at any time, the difference between the two speed values must lie within the tolerance band of 10% in order to still meet the condition of equality. If the current speed value lies below the threshold specified in the Limit FB, the STO output is set to logical 1 and the drive can rotate. If the limit is exceeded or the comparison is invalid, the output is set to logic 0, and the drive is switched torque-free or the safety function integrated in the drive is activated. The entire calculation and scaling are performed at the SIL3/PL e safety level in the safety-related EL6910 logic. Using this method, a safety-related result is created from two non-safety-related signals.

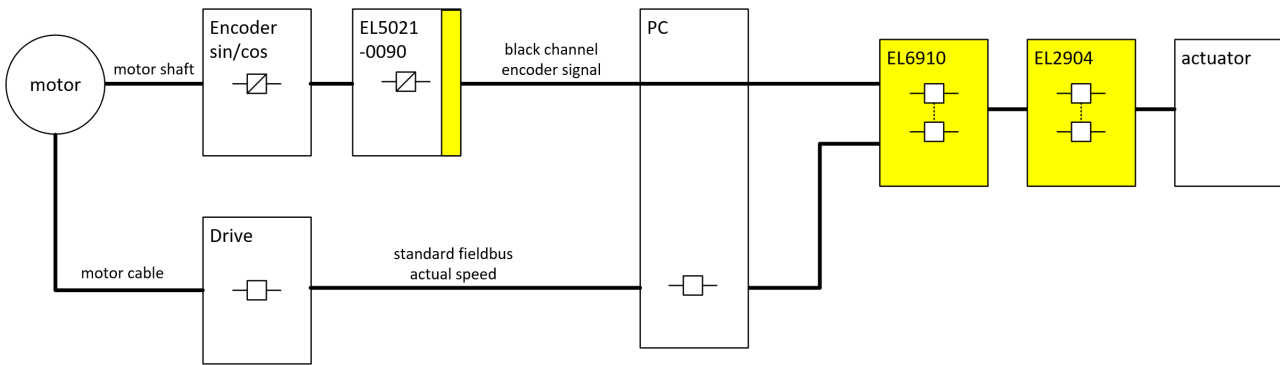
An emergency stop function is additionally implemented by an ESTOP function block (not shown in the diagram for reasons of clarity), which prevents the restart and also takes over the control of contactors K1 and K2.

The IsValid signal of the Compare function block must be used for shutdown in the event of a fault.

Structure



Structural image structure



Logic



7.1.1 Structure and diagnosis

The input signals from the drive and the encoder are standard signals, which are dynamic and different. The drive supplies a speed value, the encoder supplies a sin/cos signal, which is evaluated by a standard terminal and packed and transmitted in a safe telegram (FSoE with modified polynomial - TwinSAFE SC).

This terminal (EL5021-0090) supplies a position value that is converted within the safe logic to a speed value, then scaled and compared with the speed value of the drive. Equality means in this case that the difference signal lies within the tolerance window of 10%.

The encoder signal is transmitted via the standard fieldbus using the black channel principle. This value is checked for plausibility against the drive speed that is transmitted via the standard fieldbus. Errors in one of the two channels are detected by means of the comparison of the two diverse speed and position signals within the safe logic and lead to the activation of STO of the drive.

7.1.2 FMEA

Error assumption	Expectations	Checked
The speed value, e.g. via PROFINET, freezes	This is detected via the second value and the plausibility check in the EL6910 (other fieldbus and TwinSAFE SC communication between EL5021-0090 and EL6910). In addition, the standard-communication watchdog should be enabled for speed 0.	
Speed value via EtherCAT and TwinSAFE SC communication freezes	This is detected via the watchdog within the TwinSAFE SC communication. Plausibility check: Dynamic speed values are also expected when the motor is started.	
Speed values are copied in succession in the standard PLC	A distorted value within the TwinSAFE SC communication leads to an invalid CRC within the telegram and thus to immediate shutdown of the group and the outputs. The data types of the two speed values have a different length (e.g. 4 bytes and 11 bytes)	
Speed value is distorted, e.g. via PROFINET	This is detected via the second value and the plausibility check in the EL6910 (other fieldbus and TwinSAFE SC communication between EL5021-0090 and EL6910)	
There is no longer any connection between the motor and the encoder	Detected within the EL6910 via the plausibility check with the speed value of the drive. Plausibility check: Dynamic speed values are also expected when the motor is started.	
Encoder supplies an incorrect position value	Detected within the EL6910 via the plausibility check with the speed value of the drive	
Drive supplies incorrect speed value	This is detected via the second value and the plausibility check in the EL6910 (other fieldbus and TwinSAFE SC communication between EL5021-0090 and EL6910)	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Corruption	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unintentional repetition	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910. In addition, the standard-communication watchdog should be enabled for speed 0.	
Communication error 61784-3 for standard communication: Wrong sequence	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Loss	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unacceptable delay	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910. In addition, the standard-communication watchdog should be enabled for speed 0.	
Communication error 61784-3 for standard communication: Insertion	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error for standard communication: Recurrent memory errors in switches	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	

7.1.2.1 Note on TwinSAFE SC communication:

The TwinSAFE SC communication uses the identical mechanisms for error detection as the Safety-over-EtherCAT communication, the difference being that a different polynomial is used to calculate the checksum and this polynomial is sufficiently independent of the polynomial previously used for Safety-over-EtherCAT.

The identical mechanisms are active, such as the black channel principle (bit error probability 10^{-2}).

The quality of the data transmission is not crucial, because ultimately all transmission errors are detected via the comparison in the safe logic, since this would lead to inequality.

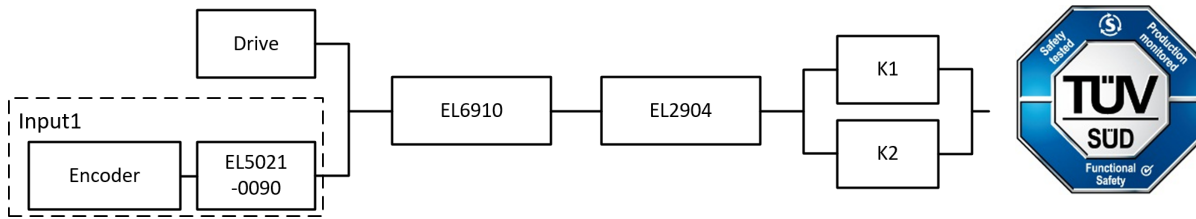
7.1.3 Parameters of the safe output terminal

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

7.1.4 Block formation and safety loops

7.1.4.1 Safety function 1



7.1.5 Calculation

7.1.5.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
Drive – MTBF	516,840 (59a)
Encoder – MTTF	549,149
EL5021-0090 - MTBF	1,205,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

7.1.5.2 Diagnostic Coverage DC

Component	Value
Drive and encoder with EL5021-0090 and plausibility within the logic	DC _{avg} =90% (alternatively in calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

7.1.5.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN 13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Calculation of the PFH_D and MTTF_D values from the MTBF values:

Note: Repair times can be neglected, therefore the following applies:

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

with

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

Drive

$$MTTF_D = 2 * MTBF = 2 * 59y = 1.033.680h = 118y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.033.680h} = 9,67E - 08$$

Encoder

$$MTTF_D = 2 * MTTF = 2 * 549149h = 1.098.298h = 125y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.098.298h} = 9,10E - 08$$

EL5021-0090

$$MTTF_D = 2 * MTBF = 2 * 1.205.000h = 2.410.000h = 275y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.410.000h} = 4,15E - 08$$

Input subsystem 1

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL5021-0090)} = 9,10E - 08 + 4,15E - 08 = 13,25E - 08$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct feedback

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The input signals from the encoder with EL5021-0090 and drive have different measuring procedures, deliver differently scaled values and are both involved in the safety function. A malfunction of a channel does not lead to a dangerous situation, but is detected by comparing the two values in the TwinSAFE Logic and leads to shutdown.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the input subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Drive)}}{2} + (1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Antrieb)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$PFH_{ges} = 10\% * \frac{13,25E - 08 + 9,67E - 08}{2} + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 1,45E - 08$$

NOTE

EN 62061

According to EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This limits the maximum SIL value that can be achieved to 2, according to table 5 of EN 62061.

Alternative calculation of the MTTF_D value for safety function 1 according to EN 13849 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

The inferior value is taken from the input subsystem (in this case a combination of encoder and EL5021-0090):

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL5021-0090)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 69,9y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL5021-0090)}} + \frac{DC}{MTTF_{D(Drive)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL5021-0090)}} + \frac{1}{MTTF_{D(Drive)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

$$DC_{avg} = \frac{\frac{90\%}{125y} + \frac{90\%}{275y} + \frac{90\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 90,78\%$$

Alternatively with DC = 99%

$$DC_{avg} = \frac{\frac{99\%}{125y} + \frac{99\%}{275y} + \frac{99\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ CAUTION

Category

This structure is possible up to category 3 at the most.

⚠ WARNING

Standstill

When the motor is stopped, an error such as the freezing of an encoder signal is detected only if a movement is requested. The machine manufacturer or user must take this into account.

⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC / MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Alternative with DC = 99% for the input subsystem:

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC / MTTFD	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

7.2 Speed monitoring (via IO-Link) (category 3, PL d)

The speed of a drive is to be monitored. This drive has a safety function (in this case, for example, STO), which is activated via a corresponding input. This input is conducted through one working contact of each of two contactors.

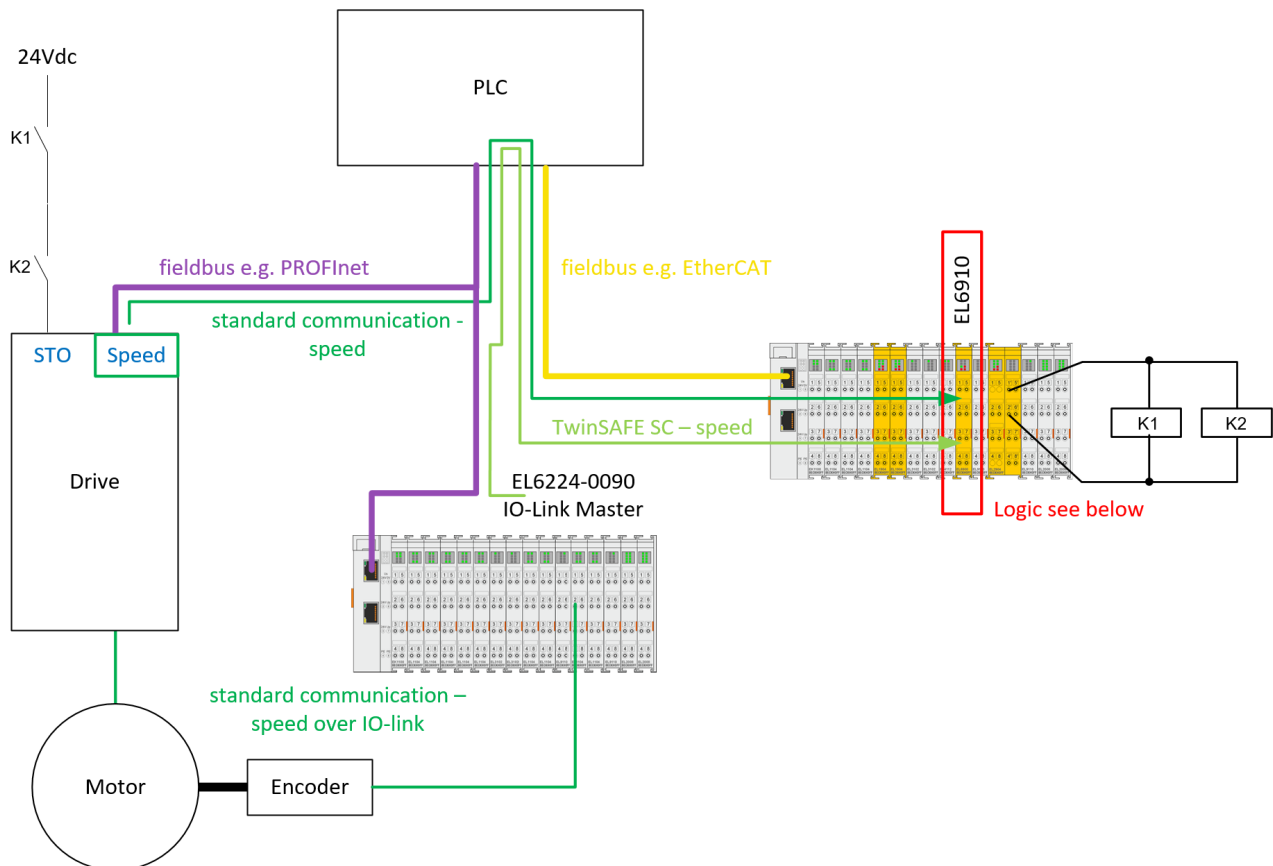
The speed signals are transmitted in two different ways to the EL6910 TwinSAFE Logic and processed according to the logic shown. The IO-Link encoder is wired to an EL6224-0090, and the speed information is transmitted via a TwinSAFE SC communication. The drive speed is also transferred to the EL6910 TwinSAFE Logic, via the standard PROFINET communication (any other fieldbus is also possible) and the standard PLC.

The two speeds are scaled by the Scale FB within the safety-related EL6910 logic so that the values match each other. These two speed values are checked by a Compare FB for equality and monitored by a Limit FB for a maximum value. Since the two speed values are never 100% equal at any time, the difference between the two speed values must lie within the tolerance band of 10% in order to still meet the condition of equality. If the current speed value lies below the threshold specified in the Limit FB, the STO output is set to logical 1 and the drive can rotate. If the limit is exceeded or the comparison is invalid, the output is set to logic 0, and the drive is switched torque-free or the safety function integrated in the drive is activated. The entire calculation and scaling are performed at the SIL3/PL e safety level in the safety-related EL6910 logic. Using this method, a safety-related result is created from two non-safety-related signals.

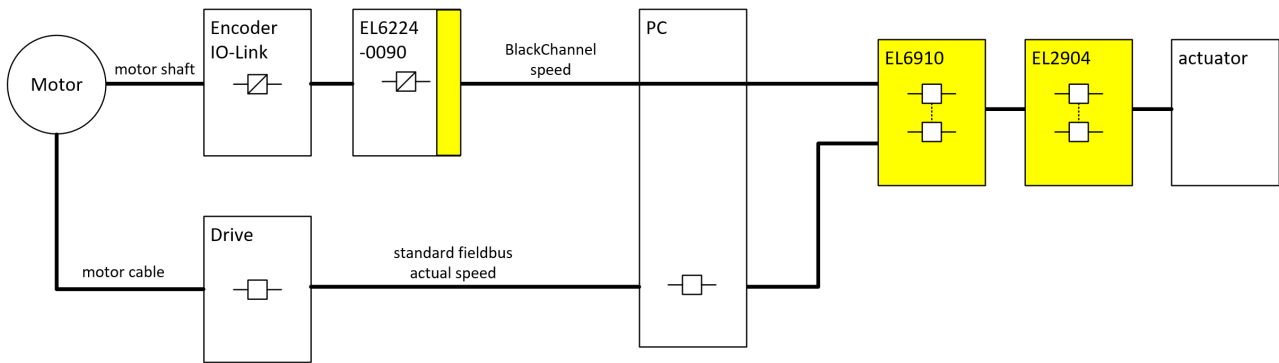
An emergency stop function is additionally implemented by an ESTOP function block (not shown in the diagram for reasons of clarity), which prevents the restart and also takes over the control of contactors K1 and K2.

The IsValid signal of the Compare function block must be used for shutdown in the event of a fault.

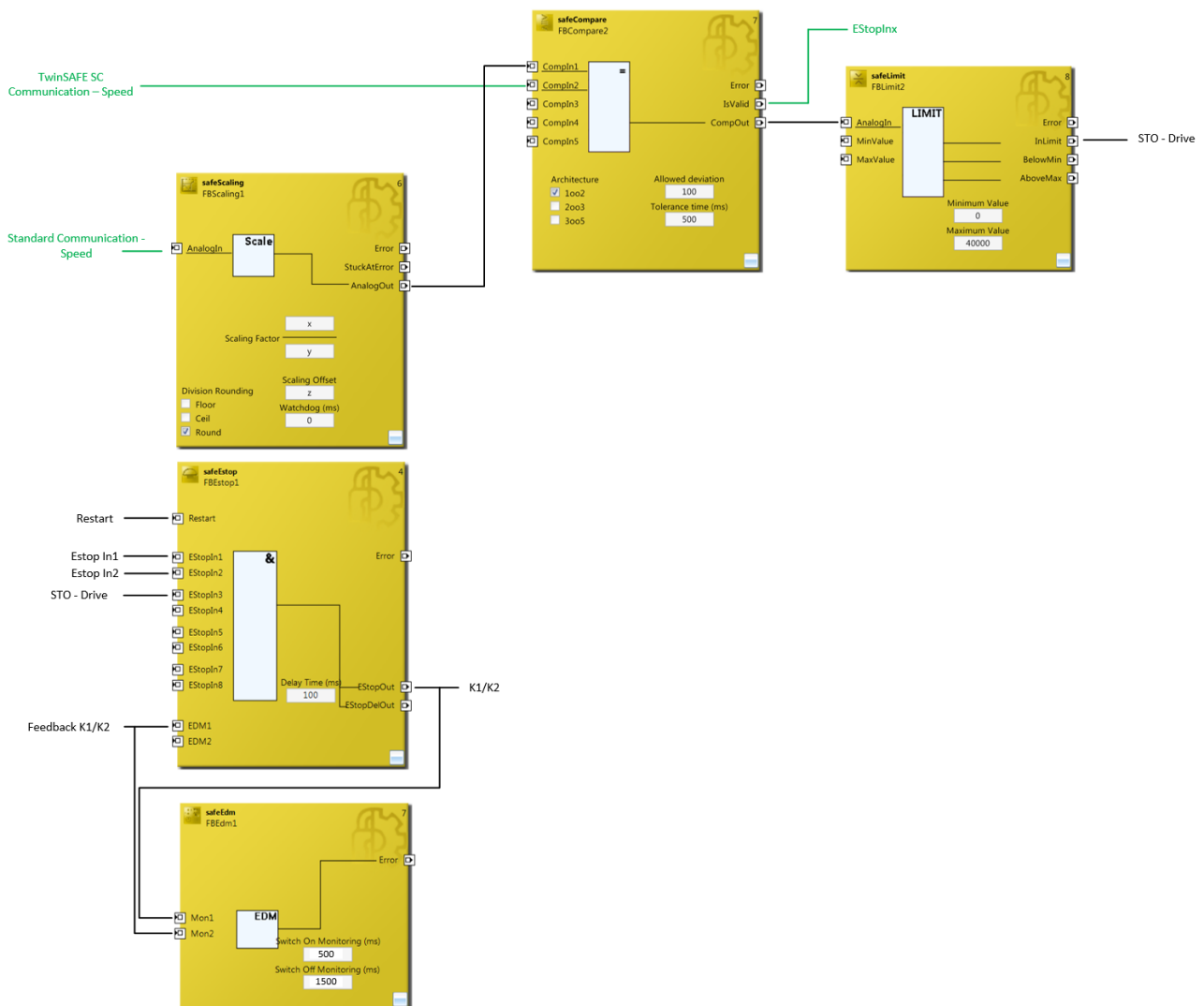
IO-link structure



Structural image structure



Logic



7.2.1 Structure and diagnosis

The input signals read from the drive and the encoder are standard signals, but they are very different. The drive supplies a speed value, the encoder supplies an IO-Link signal, which is evaluated by a standard terminal and packed and transmitted in a safe telegram (FSoE with modified polynomial - TwinSAFE SC). This terminal (EL6224-0090) supplies a speed value that is scaled within the safe logic and compared with the speed value of the drive. Equality means in this case that the difference signal lies within the tolerance window of 10%.

The IO-link encoder signal is transmitted via the standard fieldbus using the black channel principle. This value is checked for plausibility against the drive speed that is transmitted via the standard fieldbus. Errors in one of the two channels are detected by comparing the two diverse speed signals within the safe logic and lead to the activation of STO of the drive.

7.2.2 FMEA

Error assumption	Expectations	Checked
The speed value, e.g. via PROFINET, freezes	This is detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC communication between EL6224-0090 and EL6910). In addition, the standard-communication watchdog should be enabled for speed 0.	
Speed value via EtherCAT and TwinSAFE SC communication freezes	This is detected via the watchdog within the TwinSAFE SC communication. Plausibility check: Dynamic speed values are also expected when the motor is started.	
Speed values are copied in succession in the standard PLC	A distorted value within the TwinSAFE SC communication leads to an invalid CRC within the telegram and thus to immediate shutdown of the group and the outputs The data types of the two speed values have a different length (e.g. 4 bytes and 11 bytes)	
Speed value is distorted, e.g. via PROFINET	This is detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC communication between EL6224-0090 and EL6910)	
There is no longer any connection between the motor and the encoder	Detected within the EL6910 via the plausibility check with the speed value of the drive Plausibility check: Dynamic speed values are also expected when the motor is started.	
Encoder supplies an incorrect position value	Detected within the EL6910 via the plausibility check with the speed value of the drive	
Drive supplies incorrect speed value	This is detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC communication between EL6224-0090 and EL6910)	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Corruption	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unintentional repetition	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910. In addition, the standard-communication watchdog should be enabled for speed 0.	
Communication error 61784-3 for standard communication: Wrong sequence	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Loss	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unacceptable delay	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910. In addition, the standard-communication watchdog should be enabled for speed 0.	
Communication error 61784-3 for standard communication: Insertion	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	
Communication error for standard communication: Recurrent memory errors in switches	This is detected through the plausibility check of the speed values together with the TwinSAFE SC communication within the EL6910	

7.2.2.1 Note on TwinSAFE SC communication:

The TwinSAFE SC communication uses the identical mechanisms for error detection as the Safety-over-EtherCAT communication, the difference being that a different polynomial is used to calculate the checksum and this polynomial is sufficiently independent of the polynomial previously used for Safety-over-EtherCAT.

The identical mechanisms are active, such as the black channel principle (bit error probability 10^{-2}).

The quality of the data transmission is not crucial, because ultimately all transmission errors are detected via the comparison in the safe logic, since this would lead to inequality.

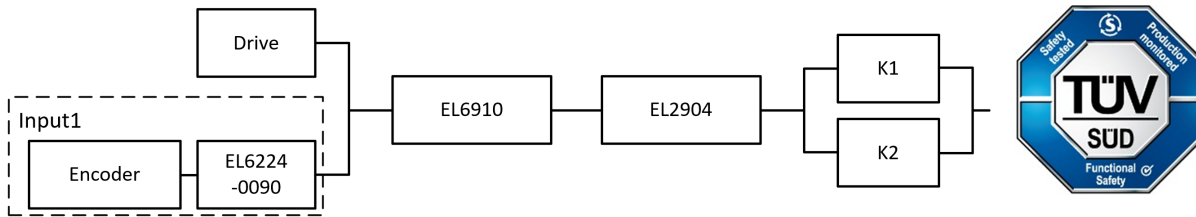
7.2.3 Parameters of the safe output terminal

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

7.2.4 Block formation and safety loops

7.2.4.1 Safety function 1



7.2.5 Calculation

7.2.5.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
Drive – MTBF	516,840 (59y)
Encoder – MTTF	1,208,880 (138y)
EL6224-0090 - MTBF	1,200,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

7.2.5.2 Diagnostic Coverage DC

Component	Value
Drive and encoder with EL6224-0090 and plausibility within the logic	DC _{avg} =90% (alternatively in calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

7.2.5.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN 13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Calculation of the PFH_D and MTTF_D values from the MTBF values:

Note: Repair times can be neglected, therefore the following applies:

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

with

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

Drive

$$MTTF_D = 2 * MTBF = 2 * 59y = 1.033.680h = 118y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.033.680h} = 9,67E - 08$$

Encoder

$$MTTF_D = 2 * MTTF = 2 * 1.208.880h = 2.417.760h = 276y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.417.760h} = 4,13E - 08$$

EL6224-0090

$$MTTF_D = 2 * MTBF = 2 * 1.200.000h = 2.400.000h = 273y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.400.000h} = 4,17E - 08$$

Input system 1

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL6224-0090)} = 4,13E - 08 + 4,17E - 08 = 8,30E - 08$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct feedback

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The input signals from the encoder with EL6224-0090 and drive have different measuring procedures, deliver differently scaled values and are both involved in the safety function. A malfunction of a channel does not lead to a dangerous situation, but is detected by comparing the two values in the TwinSAFE Logic and leads to shutdown.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the input subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Drive)}}{2} + (1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Antrieb)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$PFH_{ges} = 10\% * \frac{8,30E - 08 + 9,67E - 08}{2} + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 1,2E - 08$$

NOTE

EN 62061

According to EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This limits the maximum SIL value that can be achieved to 2, according to table 5 of EN 62061.

Alternative calculation of the MTTF_D value for safety function 1 according to EN 13849 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

The inferior value is taken from the input subsystem (in this case the drive):

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Antrieb)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 89,7y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6244-0090)}} + \frac{DC}{MTTF_{D(Antrieb)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6244-0090)}} + \frac{1}{MTTF_{D(Antrieb)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

$$DC_{avg} = \frac{\frac{90\%}{276y} + \frac{90\%}{273y} + \frac{90\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{276y} + \frac{1}{273y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,30\%$$

Alternatively with DC = 99%

$$DC_{avg} = \frac{\frac{99\%}{276y} + \frac{99\%}{273y} + \frac{99\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{276y} + \frac{1}{273y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ CAUTION

Category

This structure is possible up to category 3 at the most.

⚠ WARNING

Standstill

When the motor is stopped, an error such as the freezing of an encoder signal is detected only if a movement is requested. The machine manufacturer or user must take this into account.

⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Alternative with DC = 99% for the input subsystem:

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC / MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

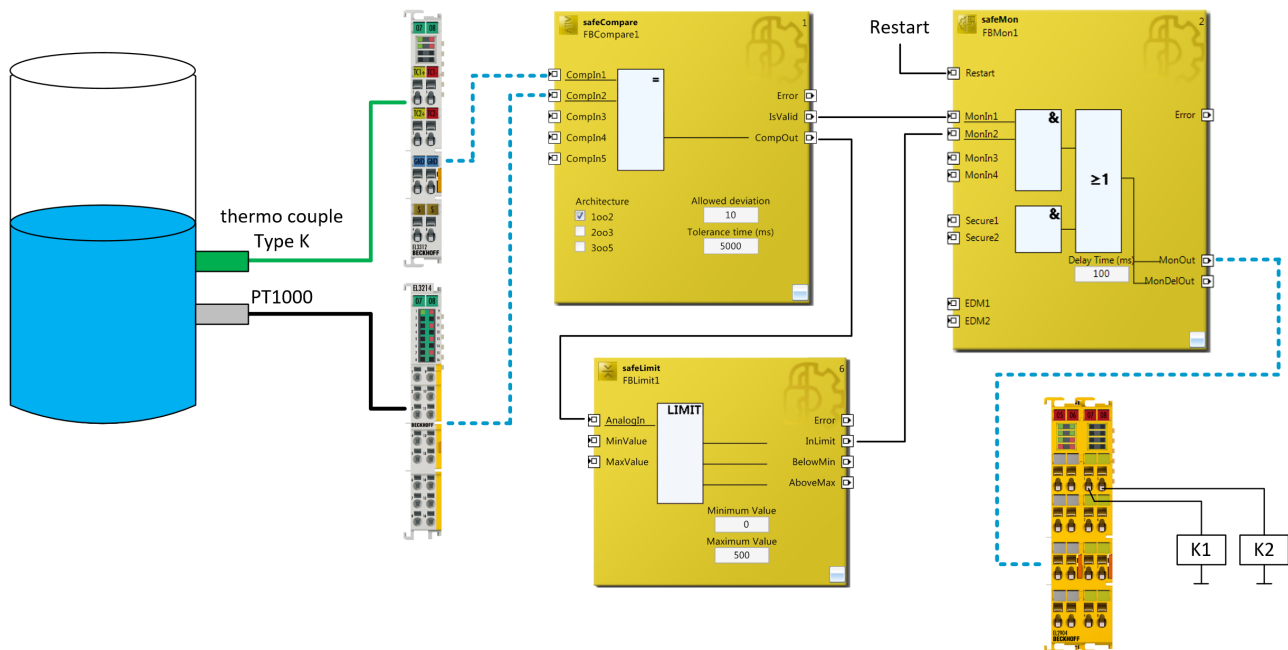
Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

7.3 Temperature measurement with TwinSAFE SC (category 3, PL d)

This example shows how a temperature measurement can be realized with the TwinSAFE SC technology. To this end, two measuring points are equipped with temperature sensors, one with a type K thermocouple wired to a standard EL3312 EtherCAT Terminal and the other with a PT1000 measuring resistance wired to an EL3214-0090 TwinSAFE SC EtherCAT Terminal.

These two signals are compared or checked for plausibility by means of a Compare function block within the safe EL6910 TwinSAFE Logic. The signal is then checked via the Limit function block. The result of the Limit function block and the IsValid output of the Compare function block is used to switch off contactors K1 and K2 via the function block Mon.

To keep things clear the contactor control is not shown in this example, but the user should keep it in mind.

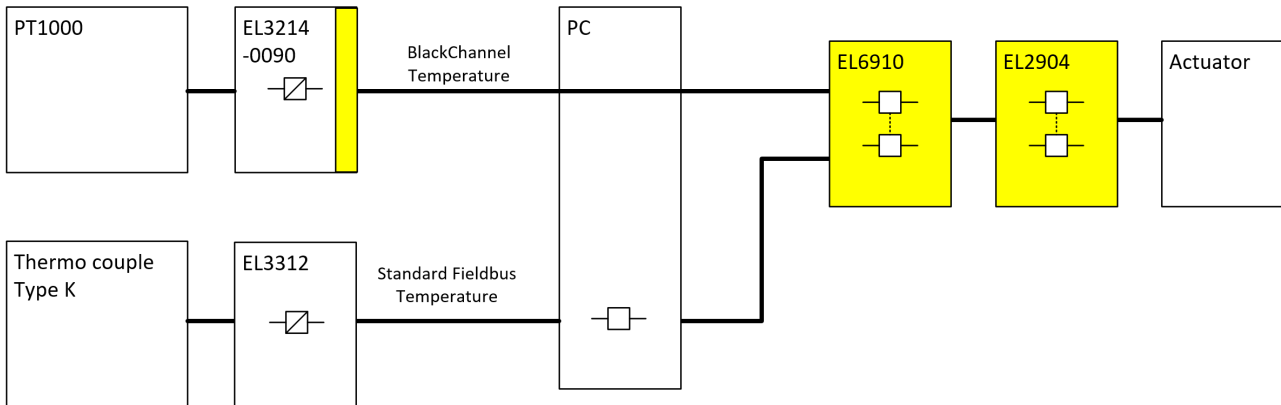


⚠ CAUTION

Emergency stop / contactor monitoring

In addition to the function shown above, contactor monitoring, e.g. via an EDM function block for K1 and K2, and possibly an emergency stop function, must be implemented by the user!

7.3.1 Schematic diagram of the configuration



7.3.2 Structure and diagnosis

The signals that are read at the two measuring points are standard signals, which use different technologies. At least one signal is transmitted via the TwinSAFE SC technology to the safe TwinSAFE Logic, so that distortions of this signal are detected in the PC or on the communication path. The test for equality of these two signals, within the permissible tolerances, is carried out in the safe TwinSAFE Logic.

The individual error assumptions and associated expectations are listed in the following FMEA table.

7.3.3 FMEA

Error assumption	Expectations	Checked
Temperature value via the standard fieldbus freezes	The value is detected by the second value and via the plausibility check in the EL6910.	
Temperature value via the TwinSAFE SC communication freezes	This is detected via the watchdog within the TwinSAFE SC communication and via the plausibility check in the EL6910.	
Temperature values are copied to each other in the standard PLC	A distorted value within the TwinSAFE SC communication leads to an invalid CRC within the telegram and thus to immediate shutdown of the group and the outputs.	
Temperature value via standard fieldbus is distorted	The value is detected by the second value and via the plausibility check in the EL6910.	
The connection between the sensor and the EtherCAT Terminal has been lost	This is detected via the plausibility check with the second temperature value within the EL6910.	
PT1000 delivers incorrect temperature value	This is detected via the plausibility check with the second temperature value within the EL6910.	
Thermocouple delivers incorrect temperature value	This is detected via the plausibility check with the second temperature value within the EL6910.	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Corruption	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unintentional repetition	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Wrong sequence	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Loss	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unacceptable delay	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Insertion	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	
Communication error for standard communication: Recurrent memory errors in switches	This is detected through the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910	

7.3.3.1 Note on TwinSAFE SC communication:

The TwinSAFE SC communication uses the identical mechanisms for error detection as the Safety-over-EtherCAT communication, the difference being that a different polynomial is used to calculate the checksum and this polynomial is sufficiently independent of the polynomial previously used for Safety-over-EtherCAT.

The identical mechanisms are active, such as the black channel principle (bit error probability 10^{-2}).

The quality of the data transmission is not crucial, because ultimately all transmission errors are detected via the comparison in the safe TwinSAFE Logic, since this would lead to inequality.

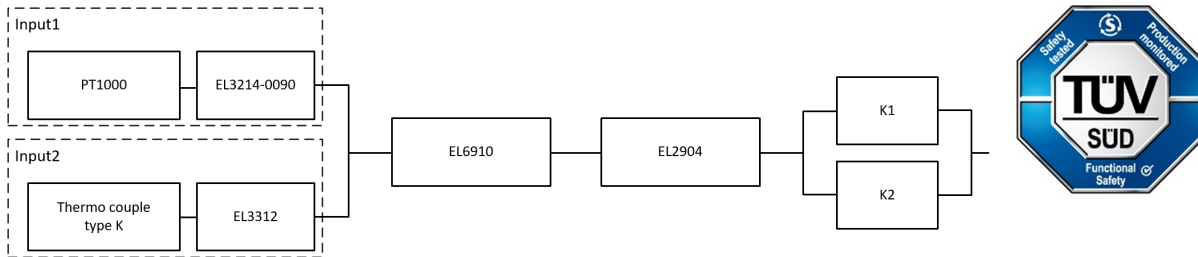
7.3.4 Parameters of the safe output terminal

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

7.3.5 Block formation and safety loops

7.3.5.1 Safety function 1



7.3.6 Calculation

7.3.6.1 PFHD / MTTFD / B10D – values

Component	Value
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
PT1000 – MTTFD	7,618 a (according to Table C.5 EN ISO 13849-1:2015)
Thermocouple type K – FIT	1900 (number of errors in 10 ⁹ hours)
EL3214-0090 - MTBF	890,000
EL3312 - MTBF	1,661,253
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

7.3.6.2 Diagnostic Coverage DC

Component	Value
Temperature values via TwinSAFE SC and plausibility check within the logic	DC _{avg} =90% (alternatively in calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

7.3.6.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN 13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTFD values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Calculation of the PFH_D and MTTF_D values from the MTBF values:

Note: Repair times can be neglected, therefore the following applies:

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

with

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

PT1000

$$MTTF_D = 7618y = 66.733.680h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{66.733.680h} = 1,50E - 09$$

EL3214-0090

$$MTTF_D = 2 * MTBF = 2 * 890.000h = 1.780.000h = 203y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.780.000h} = 5,62E - 08$$

Input system 1

$$PFH_{(Input1)} = PFH_{(PT1000)} + PFH_{(EL3214-0090)} = 1,50E - 09 + 5,62E - 08 = 5,77E - 08$$

Thermocouple

$$MTTF_D = \frac{1}{\lambda_D} = \frac{1}{1900FIT} * 10^9 h = 526.315h = 60y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{526.315h} = 19,0E - 08$$

EL3312

$$MTTF_D = 2 * MTBF = 2 * 1.661.253h = 3.322.506h = 379y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.322.506h} = 3,0E - 08$$

Input system 2

$$PFH_{(Input2)} = PFH_{(ThermoCouple)} + PFH_{(EL3312)} = 19,0E - 08 + 3,0E - 08 = 22,0E - 08$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct feedback

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The input signals from PT1000 with EL3214-0090 and thermocouple with EL3312 use different measuring procedures. Both provide a temperature value and are involved in the safety function. A malfunction of a channel does not lead to a dangerous situation, but is detected by comparing the two values in the TwinSAFE Logic and leads to shutdown.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the input subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{5,77E - 08 + 22,0E - 08}{2} + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} = 1,693E - 08$$

NOTE

EN 62061

According to EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This limits the maximum SIL value that can be achieved to 2, according to table 5 of EN 62061.

Alternative calculation of the MTTF_D value for safety function 1 according to EN 13849 (under the same assumption)

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

The inferior value is taken from the input subsystem:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(ThermoCouple)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 45,5y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(PT1000)}} + \frac{DC}{MTTF_{D(EL3214)}} + \frac{DC}{MTTF_{D(Thermocouple)}} + \frac{DC}{MTTF_{D(EL3312)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(PT1000)}} + \frac{1}{MTTF_{D(EL3214)}} + \frac{1}{MTTF_{D(Thermocouple)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{90\%}{7618y} + \frac{90\%}{203y} + \frac{90\%}{60y} + \frac{90\%}{379y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{7618y} + \frac{1}{203y} + \frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,11\%$$

Alternatively with DC = 99%

$$DC_{avg} = \frac{\frac{99\%}{7618y} + \frac{99\%}{203y} + \frac{99\%}{60y} + \frac{99\%}{379y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{7618y} + \frac{1}{203y} + \frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ CAUTION

Category
This structure is possible up to category 3 at the most.

DC=90% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Alternative with DC = 99% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC / MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

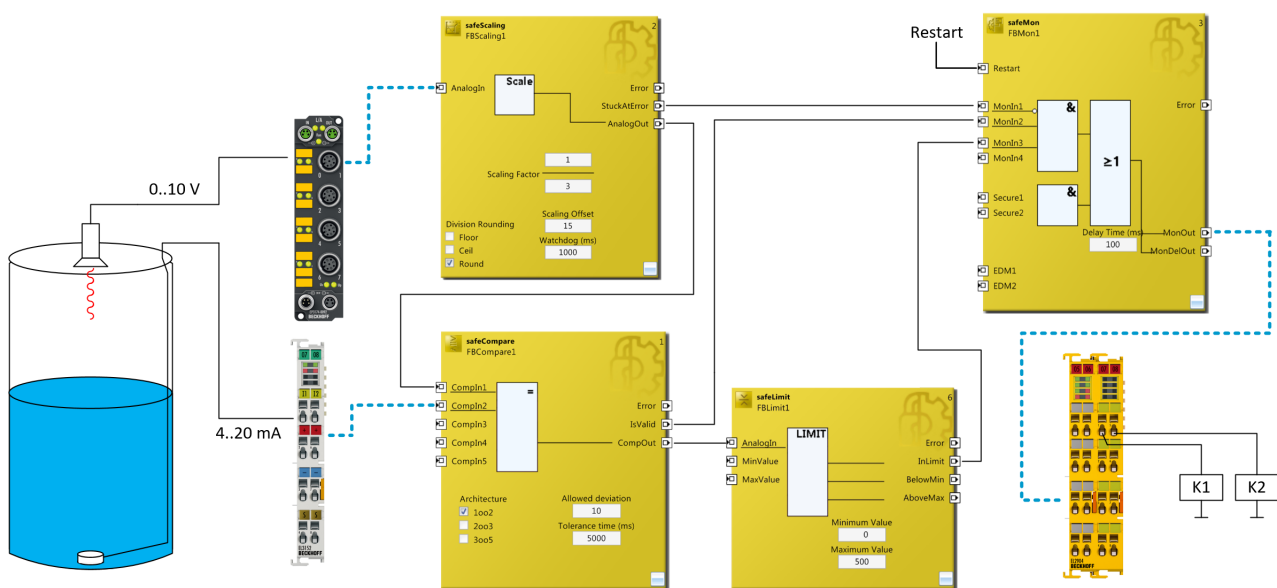
Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

7.4 Level measurement with TwinSAFE SC (category 3, PL d)

This example shows how a level measurement of a container can be realized with the TwinSAFE SC technology. Two different measuring methods are used for this purpose. One is an ultrasonic sensor with a 0 - 10 V interface, which is wired to a TwinSAFE SC EtherCAT Box EP3174-0092, is used, and the other is a level probe with a 4-20 mA interface, which is wired to a standard EL3152 EtherCAT Terminal.

These two signals are compared or checked for plausibility by means of a Compare function block within the safe EL6910 TwinSAFE Logic. The signal from the EP3174-0092 is scaled by the Scale function block first so that both signals have an identical value range. The signal is then checked via the Limit function block. The result of the Limit function block and the IsValid output of the Compare function block is used to switch off contactors K1 and K2 via the function block Mon. In addition, the StuckAtError output of the Scale function block can be connected to a Mon input. Freezing of the signal can be detected with this configuration.

To keep things clear the contactor control is not shown in this example, but the user should keep it in mind.

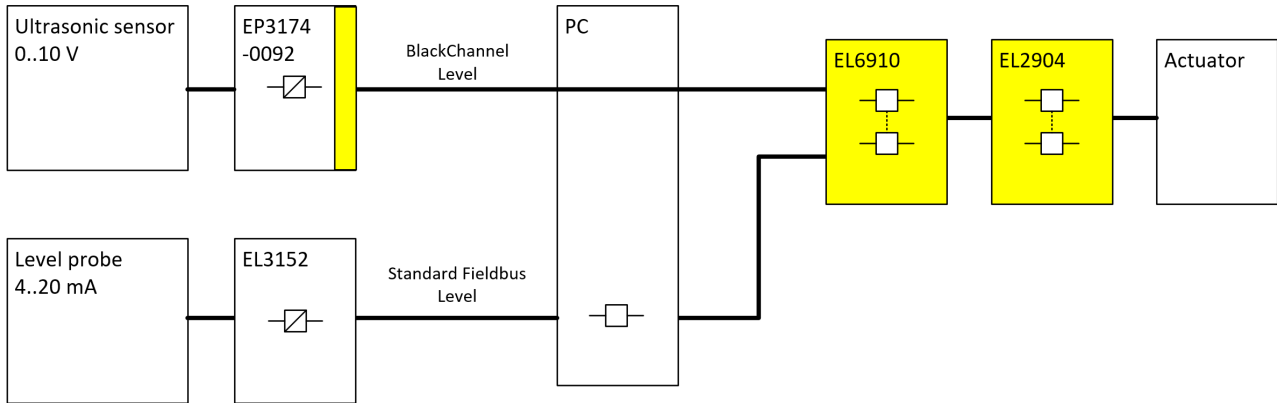


⚠ CAUTION

Emergency stop / contactor monitoring

In addition to the function shown above, contactor monitoring, e.g. via an EDM function block for K1 and K2, and possibly an emergency stop function, must be implemented by the user!

7.4.1 Schematic diagram of the configuration



7.4.2 Structure and diagnosis

The signals that are read at the two measuring points are standard signals, which use different technologies. At least one signal is transmitted via the TwinSAFE SC technology to the safe TwinSAFE Logic, so that distortions of this signal are detected in the PC or on the communication path. The test for equality of these two signals, within the permissible tolerances, is carried out in the safe TwinSAFE Logic.

The individual error assumptions and associated expectations are listed in the following FMEA table.

7.4.3 FMEA

Error assumption	Expectations	Checked
Filling level value via the standard fieldbus freezes	The value is detected by the second value and via the plausibility check in the EL6910.	
Filling level value via the TwinSAFE SC communication freezes	This is detected via the watchdog within the TwinSAFE SC communication and via the plausibility check in the EL6910.	
Filling level values are copied to each other in the standard PLC	A distorted value within the TwinSAFE SC communication leads to an invalid CRC within the telegram and thus to immediate shutdown of the group and the outputs.	
Filling level value via standard fieldbus is distorted	The value is detected by the second value and via the plausibility check in the EL6910.	
The connection between the sensor and the EtherCAT Terminal has been lost	This is detected via the plausibility check with the second filling level value within the EL6910.	
Ultrasonic sensor supplies incorrect filling level value	This is detected via the plausibility check with the second filling level value within the EL6910.	
Level probe supplies incorrect filling level value	This is detected via the plausibility check with the second filling level value within the EL6910.	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Corruption	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unintentional repetition	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Wrong sequence	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Loss	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unacceptable delay	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Insertion	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	
Communication error for standard communication: Recurrent memory errors in switches	This is detected through the plausibility check of the filling level values and via the TwinSAFE SC communication within the EL6910	

7.4.3.1 Note on TwinSAFE SC communication:

The TwinSAFE SC communication uses the identical mechanisms for error detection as the Safety-over-EtherCAT communication, the difference being that a different polynomial is used to calculate the checksum and this polynomial is sufficiently independent of the polynomial previously used for Safety-over-EtherCAT.

The identical mechanisms are active, such as the black channel principle (bit error probability 10^{-2}).

The quality of the data transmission is not crucial, because ultimately all transmission errors are detected via the comparison in the safe TwinSAFE Logic, since this would lead to inequality.

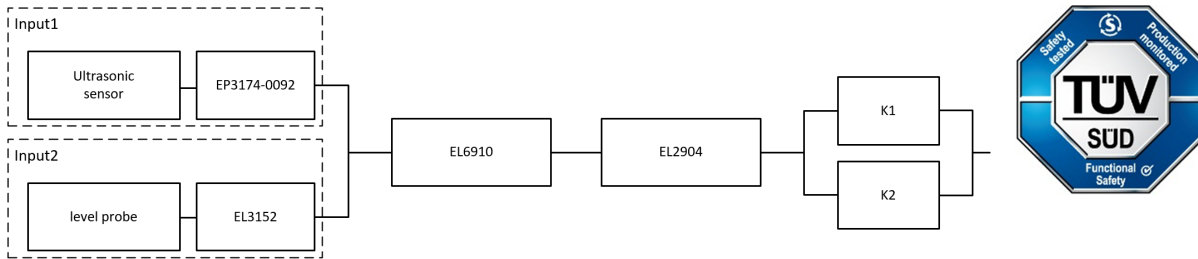
7.4.4 Parameters of the safe output terminal

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

7.4.5 Block formation and safety loops

7.4.5.1 Safety function 1



7.4.6 Calculation

7.4.6.1 PFHD / MTTFD / B10D – values

Component	Value
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
Ultrasonic sensor – MTBF	195 a (1,708,200 h)
Level probe – MTTF	732 a (6,412,320 h)
EP3174-0092 - MTBF	600,000 h
EL3152 - MTBF	2,507,303 h
K1 – B10 _D	1,300,000 h
K2 – B10 _D	1,300,000 h
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

7.4.6.2 Diagnostic Coverage DC

Component	Value
Filling level values via TwinSAFE SC and plausibility check within the logic	DC _{avg} =90% (alternatively in calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

7.4.6.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN 13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Calculation of the PFH_D and MTTF_D values from the MTBF values:

Note: Repair times can be neglected, therefore the following applies:

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

with

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

Ultrasonic sensor

$$MTTF_D = 2 * MTBF = 2 * 195y = 390y = 3.416.400h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.416.400h} = 2,93E - 08$$

EP3174-0092

$$MTTF_D = 2 * MTBF = 2 * 600.000h = 1.200.000h = 136y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.200.000h} = 8,33E - 08$$

Input system 1

$$PFH_{(Input1)} = PFH_{(Ultrasonic)} + PFH_{(EP3174-0092)} = 2,93E - 08 + 8,33E - 08 = 11,26E - 08$$

Level probe

$$MTTF_D = 2 * MTBF = 2 * 732y = 1.464y = 12.824.640h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{12.824.640h} = 7,79E - 09$$

EL3152

$$MTTF_D = 2 * MTBF = 2 * 2.507.303h = 5.014.606h = 572y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{5.014.606h} = 1,99E - 08$$

Input system 2

$$PFH_{(Input2)} = PFH_{(Level Probe)} + PFH_{(EL3152)} = 7,79E - 09 + 1,99E - 08 = 2,77E - 08$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct feedback

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The input signals from the ultrasonic sensor with EP3174-0092 and the level probe with EL3152 use different measuring procedures. Both provide a filling level and are involved in the safety function. A malfunction of a channel does not lead to a dangerous situation, but is detected by comparing the two values in the TwinSAFE Logic and leads to shutdown.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where $\beta = 10\%$. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the input subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)} \\ + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{11,26E - 08 + 2,77E - 08}{2} + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 1,005E - 08$$

NOTE**EN 62061**

According to EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This limits the maximum SIL value that can be achieved to 2, according to table 5 of EN 62061.

Alternative calculation of the MTTF_D value for safety function 1 according to EN 13849 (under the same assumption)

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

The inferior value is taken from the input subsystem:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(UltraSonicSensor)}} + \frac{1}{MTTF_{D(EP3174-0092)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 79,46y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(UltraSonic)}} + \frac{DC}{MTTF_{D(EP3174-0092)}} + \frac{DC}{MTTF_{D(LevelProbe)}} + \frac{DC}{MTTF_{D(EL3152)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(UltraSonic)}} + \frac{1}{MTTF_{D(EP3174-0092)}} + \frac{1}{MTTF_{D(LevelProbe)}} + \frac{1}{MTTF_{D(EL3152)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{90\%}{390y} + \frac{90\%}{136y} + \frac{90\%}{1464y} + \frac{90\%}{572y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{1464y} + \frac{1}{572y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,33\%$$

Alternatively with DC = 99%

$$DC_{avg} = \frac{\frac{99\%}{390y} + \frac{99\%}{136y} + \frac{99\%}{1464y} + \frac{99\%}{572y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{1464y} + \frac{1}{572y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ CAUTION

Category

This structure is possible up to category 3 at the most.

DC=90% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Alternative with DC = 99% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

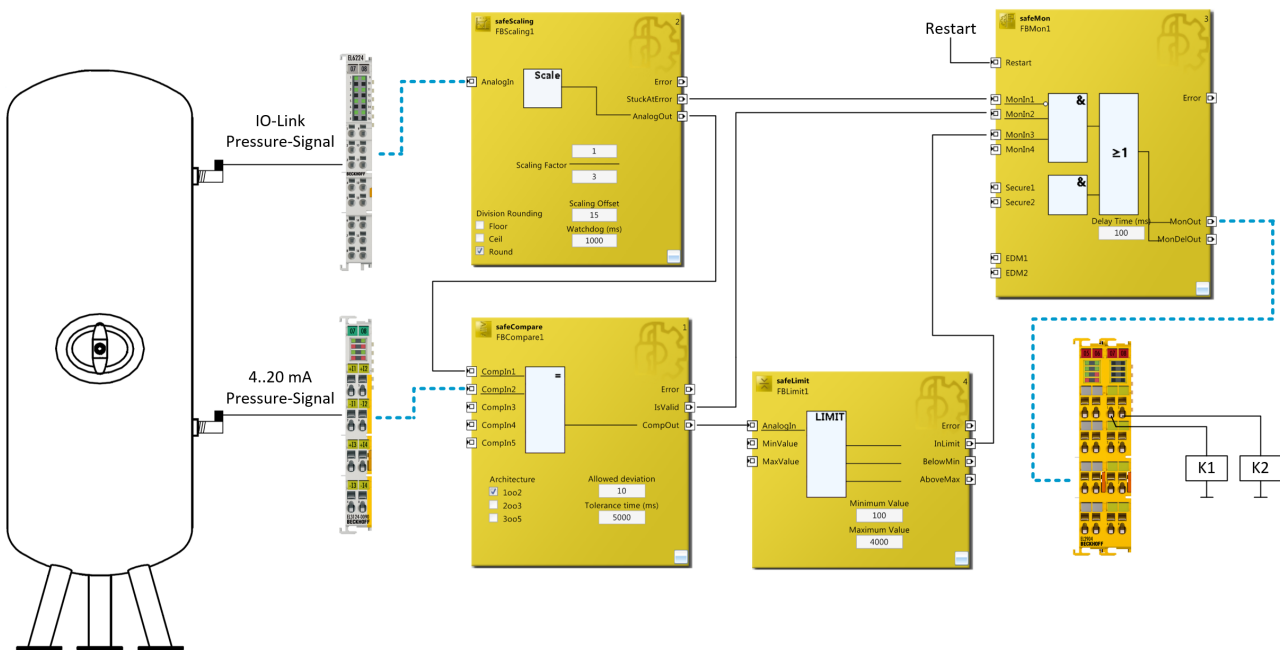
Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

7.5 Pressure measurement with TwinSAFE SC (category 3, PL d)

This example shows how a pressure measurement of a container can be realized with the TwinSAFE SC technology. To this end, two measuring points are equipped with pressure sensors, one with a pressure sensor with IO-Link interface wired to a standard EL6224 EtherCAT Terminal and the other with a pressure sensor with 4-20 mA interface wired to an EL3124-0090 TwinSAFE SC EtherCAT Terminal.

These two signals are compared or checked for plausibility by means of a Compare function block within the safe EL6910 TwinSAFE Logic. The signal from the EP6224 is scaled by the Scale function block first so that both signals have an identical value range. The signal is then checked via the Limit function block. The result of the Limit function block and the IsValid output of the Compare function block is used to switch off contactors K1 and K2 via the function block Mon. In addition, the StuckAtError output of the Scale function block can be connected to a Mon input. Freezing of the signal can be detected with this configuration.

To keep things clear the contactor control is not shown in this example, but the user should keep it in mind.



⚠ WARNING

Pressure safety valve (PSV)

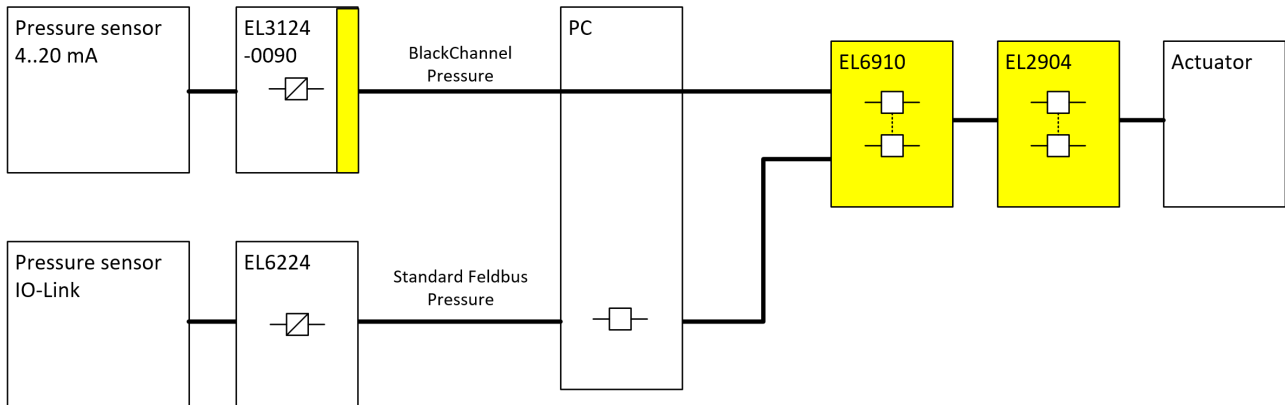
The application shown above cannot be used as a replacement for a pressure safety valve according to the EC Pressure Equipment Directive.

⚠ CAUTION

Emergency stop / contactor monitoring

In addition to the function shown above, contactor monitoring, e.g. via an EDM function block for K1 and K2, and possibly an emergency stop function, must be implemented by the user!

7.5.1 Schematic diagram of the configuration



7.5.2 Structure and diagnosis

The signals that are read at the two measuring points are standard signals, which use different technologies. At least one signal is transmitted via the TwinSAFE SC technology to the safe TwinSAFE Logic, so that distortions of this signal are detected in the PC or on the communication path. The test for equality of these two signals, within the permissible tolerances, is carried out in the safe TwinSAFE Logic.

The individual error assumptions and associated expectations are listed in the following FMEA table.

7.5.3 FMEA

Error assumption	Expectations	Checked
Pressure value via the standard fieldbus freezes	The value is detected by the second value and via the plausibility check in the EL6910.	
Pressure value via the TwinSAFE SC communication freezes	This is detected via the watchdog within the TwinSAFE SC communication and via the plausibility check in the EL6910.	
Pressure values are copied to each other in the standard PLC	A distorted value within the TwinSAFE SC communication leads to an invalid CRC within the telegram and thus to immediate shutdown of the group and the outputs.	
Pressure value via standard fieldbus is distorted	The value is detected by the second value and via the plausibility check in the EL6910.	
The connection between the sensor and the EtherCAT Terminal has been lost	This is detected via the plausibility check with the second pressure value within the EL6910.	
Pressure sensor (4..20 mA) supplies incorrect pressure value	This is detected via the plausibility check with the second pressure value within the EL6910.	
Pressure sensor (IO-Link) supplies incorrect pressure value	This is detected via the plausibility check with the second pressure value within the EL6910.	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Corruption	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unintentional repetition	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Wrong sequence	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Loss	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unacceptable delay	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Insertion	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	
Communication error for standard communication: Recurrent memory errors in switches	This is detected through the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910	

7.5.3.1 Note on TwinSAFE SC communication:

The TwinSAFE SC communication uses the identical mechanisms for error detection as the Safety-over-EtherCAT communication, the difference being that a different polynomial is used to calculate the checksum and this polynomial is sufficiently independent of the polynomial previously used for Safety-over-EtherCAT.

The identical mechanisms are active, such as the black channel principle (bit error probability 10^{-2}).

The quality of the data transmission is not crucial, because ultimately all transmission errors are detected via the comparison in the safe TwinSAFE Logic, since this would lead to inequality.

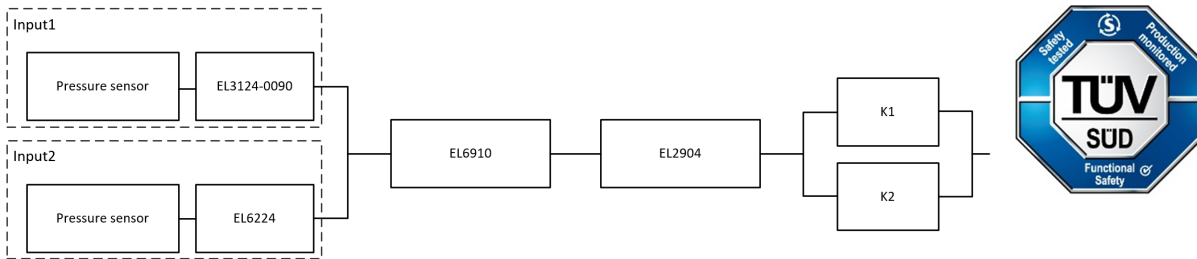
7.5.4 Parameters of the safe output terminal

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

7.5.5 Block formation and safety loops

7.5.5.1 Safety function 1



7.5.6 Calculation

7.5.6.1 PFHD / MTTFD / B10D – values

Component	Value
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
Pressure sensor 1 (4-20 mA) – MTTF	124 a (1,086,240 h)
Pressure sensor 2 IO-Link – MTTF	201 a (1,760,760 h)
EL3124-0090 - MTBF	950,000 h
EL6224 - MTBF	1,607,919 h
K1 – B10 _D	1,300,000 h
K2 – B10 _D	1,300,000 h
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

7.5.6.2 Diagnostic Coverage DC

Component	Value
Pressure values via TwinSAFE SC and plausibility check within the logic	DC _{avg} =90% (alternatively in calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

7.5.6.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN 13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTFD_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Calculation of the PFH_D and MTTF_D values from the MTBF values:

Note: Repair times can be neglected, therefore the following applies:

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

with

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

Pressure sensor 1 (4-20 mA)

$$MTTF_D = 2 * MTBF = 2 * 124y = 248y = 2.172.480h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.172.480h} = 4,60E - 08$$

EL3124-0090

$$MTTF_D = 2 * MTBF = 2 * 950.000h = 1.900.000h = 216y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.900.000h} = 5,26E - 08$$

Input system 1

$$PFH_{(Input1)} = PFH_{(PressureSensor1)} + PFH_{(EL3124-0090)} = 4,60E - 08 + 5,26E - 08 = 9,86E - 08$$

Pressure sensor 2 (IO-Link)

$$MTTF_D = 2 * MTBF = 2 * 1.760.760h = 3.521.520h = 402y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.521.520h} = 2,84E - 08$$

EL6224

$$MTTF_D = 2 * MTBF = 2 * 1.607.919h = 3.215.838h = 367y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.215.838h} = 3,11E - 08$$

Input system 2

$$PFH_{(Input2)} = PFH_{(PressureSensor2)} + PFH_{(EL6224)} = 2,84E - 08 + 3,11E - 08 = 5,95E - 08$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct feedback

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The input signals from pressure sensor 1 with EL3124-0090 and pressure sensor 2 with EL6224 use different measuring procedures. Both supply a pressure value and are involved in the safety function. A malfunction of a channel does not lead to a dangerous situation, but is detected by comparing the two values in the TwinSAFE Logic and leads to shutdown.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the input subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ and $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 10\% * \frac{9,86E - 08 + 5,95E - 08}{2} + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} = 1,094E - 08$$

NOTE

EN 62061

According to EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This limits the maximum SIL value that can be achieved to 2, according to table 5 of EN 62061.

Alternative calculation of the MTTF_D value for safety function 1 according to EN 13849 (under the same assumption)

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

The inferior value is taken from the input subsystem:

$$\frac{1}{MTTF_{D_{ges}}} = \frac{1}{MTTF_{D(PressureSensor)}} + \frac{1}{MTTF_{D(EL3124-0090)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 88,27y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Pressure1)}} + \frac{DC}{MTTF_{D(EL3124-0090)}} + \frac{DC}{MTTF_{D(Pressure2)}} + \frac{DC}{MTTF_{D(EL6224)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Pressure1)}} + \frac{1}{MTTF_{D(EL3124-0090)}} + \frac{1}{MTTF_{D(Pressure2)}} + \frac{1}{MTTF_{D(EL6224)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{90\%}{248y} + \frac{90\%}{216y} + \frac{90\%}{402y} + \frac{90\%}{367y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{402y} + \frac{1}{367y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,41\%$$

Alternatively with DC = 99%

$$DC_{avg} = \frac{\frac{99\%}{248y} + \frac{99\%}{216y} + \frac{99\%}{402y} + \frac{99\%}{367y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{402y} + \frac{1}{367y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ CAUTION

Category
This structure is possible up to category 3 at the most.

DC=90% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Alternative with DC = 99% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

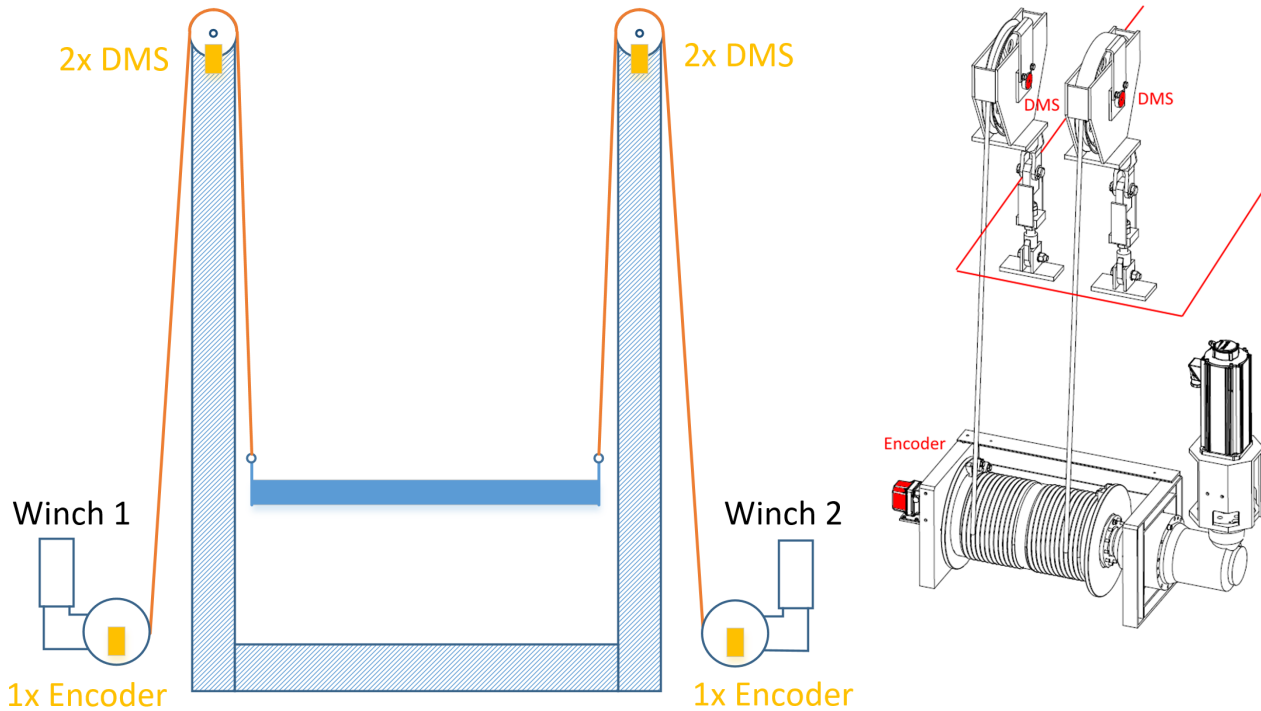
Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Safety integrity level according to Table 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH _D)
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

7.6 Monitoring of lifting device (category 3, PL d)

A lifting device, consisting of two winches with deflection rollers for moving a lifting table, is to be monitored from a safety point of view. The functions "slack rope detection" and "overload" are to be realized. Two deflection rollers, each with an SG sensor, are mounted at the top of the posts on each side, i.e. there are four SG sensors in total. One of these two sensors of one side is read in with a TwinSAFE SC terminal EL3356-0090. The other SG sensor is wired to an EL3751. This provides an SG mV/V signal, which must be converted into a weight value in the safe logic so that it can be compared with the value of the EL3356-0090.



Safety function 1 - Overload

A maximum permissible payload is specified for the lifting device. This must be monitored. After the plausibility check of the signals of the EL3751 and EL3356-0090, the result is limited with the limit function block in the EL6910.

Based to the customer's risk and hazard analysis, this safety function must be evaluated with PL c according to EN 13849-1:2015.

The safety function is set up in a category 3 structure.

Safety function 2 - Slack rope detection

Slack rope detection is used to detect whether the lifting slide has got stuck mechanically somewhere or is on the floor. In both cases, the system must be switched off immediately. In addition, it also detects whether a rope has snatched.

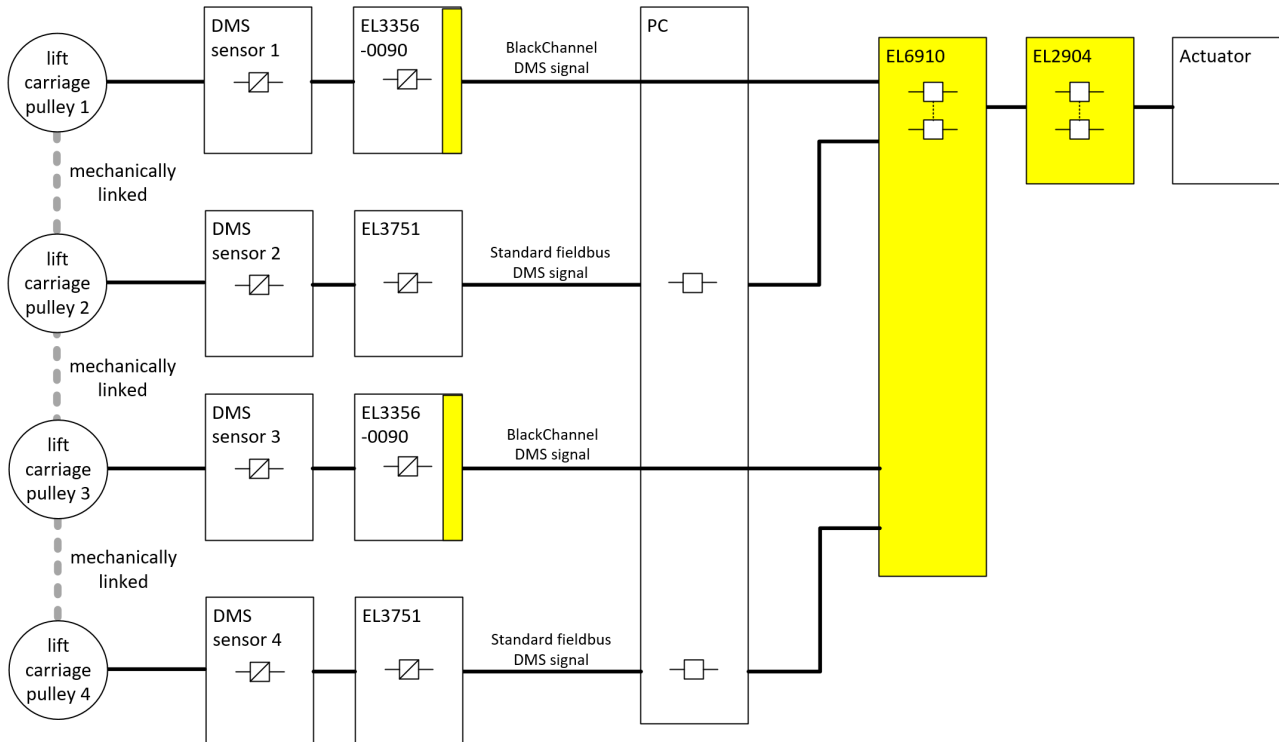
Based to the customer's risk and hazard analysis, this safety function must be evaluated with PL c according to EN 13849-1:2015.

The safety function is set up in a category 3 structure.

Additional function - without safety requirements

Synchronism can be checked by incremental comparison of the encoder values of winch 1 and 2. This prevents the lifting slide from being pulled sideways by the two winches at an early stage.

7.6.1 Structural image structure



7.6.2 Structure and diagnosis

The read-in signals of the SG sensors are standard signals, which are recorded differently on each side. The first SG sensor is wired to an EL3356-0090 SG terminal, which packs the determined weight value into a safe telegram (FSoE with modified polynomial - TwinSAFE SC) and transmits it to the EL6910. The second SG sensor is wired to an EL3751 terminal, which performs an SG mV/V measurement. This signal is sent to the EL6910 via the standard communication path. This signal is converted to a weight value within the safe logic before the plausibility check.

The same procedure is used for the second side of the lifting unit with SG sensors 3 and 4. A different polynomial is used for the TwinSAFE SC communication of the second EL3356-0090 compared to the first side. This enables detection of situations where the data of the two TwinSAFE SC connections have been copied to each other.

7.6.3 FMEA

Error assumption	Expectations	Checked
SG signal via standard fieldbus freezes	This is detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC communication between EL3356-0090 and EL6910).	
SG signal via TwinSAFE SC communication freezes	This is detected via the second value and the plausibility check in the EL6910 and via the watchdog within the TwinSAFE SC communication.	
SG values are copied to each other in the standard PLC	A distorted value within the TwinSAFE SC communication leads to an invalid CRC within the telegram and thus to immediate shutdown of the group and the outputs. The data types of the two SG values have a different length, since one of the two is packed in the TwinSAFE SC telegram (e.g. 4 bytes and 11 bytes)	
SG signal via standard fieldbus is distorted	This is detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC communication between EL3356-0090 and EL6910)	
Mechanical connection between lifting slide and winch no longer exists	This is detected via the plausibility check with the second SG signal within the EL6910.	
EL3356-0090 delivers incorrect SG value	This is detected via the plausibility check with the SG value of the EL3751 within the EL6910	
EL3751 returns incorrect SG value	This is detected via the plausibility check with the SG value of the EL3356-0090 within the EL6910	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Corruption	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unintentional repetition	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Wrong sequence	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Loss	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Unacceptable delay	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Insertion	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	
Communication error for standard communication: Recurrent memory errors in switches	This is detected through the plausibility check of the SG values together with the TwinSAFE SC communication within the EL6910	

7.6.3.1 Note on TwinSAFE SC communication:

The TwinSAFE SC communication uses the identical mechanisms for error detection as the Safety-over-EtherCAT communication, the difference being that a different polynomial is used to calculate the checksum and this polynomial is sufficiently independent of the polynomial previously used for Safety-over-EtherCAT.

The identical mechanisms are active, such as the black channel principle (bit error probability 10^{-2}).

The quality of the data transmission is not crucial, because ultimately all transmission errors are detected via the comparison in the safe logic, since this would lead to inequality.

7.6.4 Structure within the logic

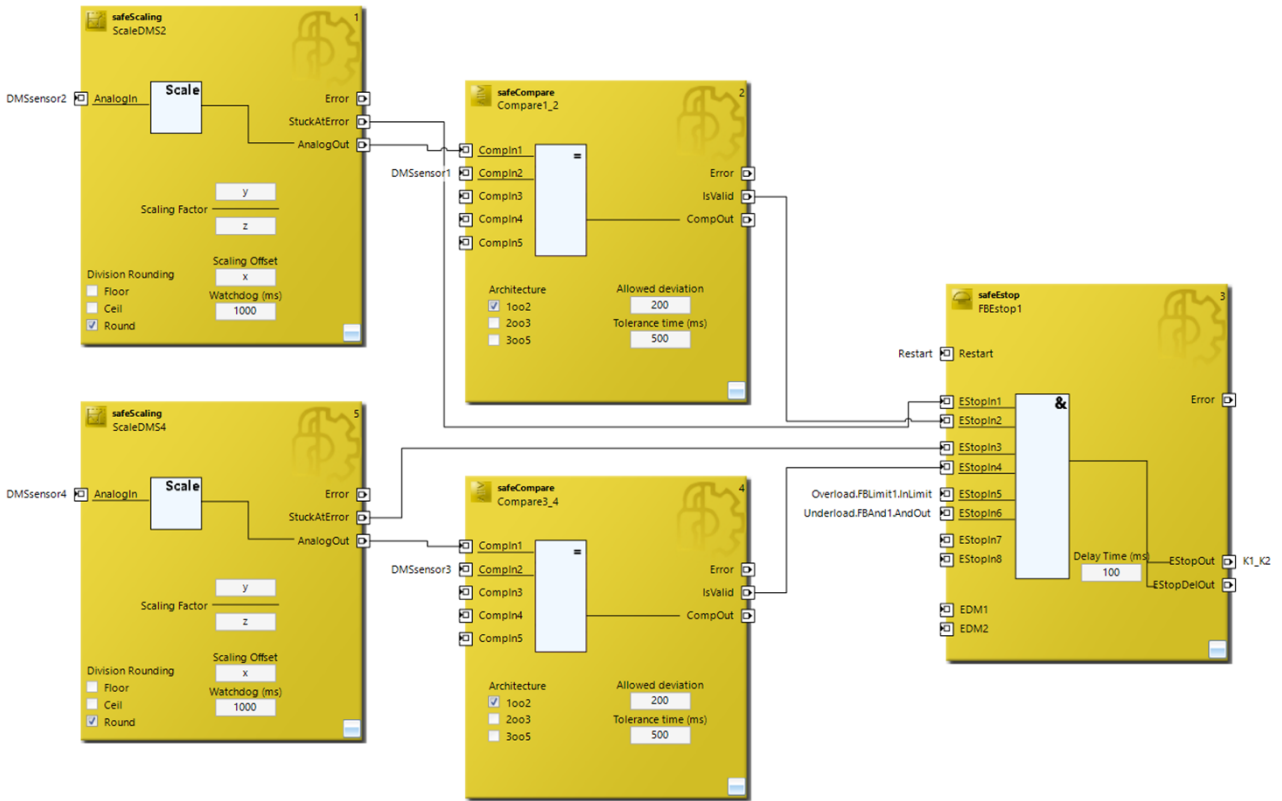
The logic in the EL6910 is divided into three parts. In the first section, the SG values are scaled and verified. It also contains the restart lock and the shutdown of contactors K1 and K2 via an ESTOP function block.

In the second section, the total load is determined and compliance with maximum and minimum values is monitored via a limit function block. The result is transferred to the ESTOP function block of the first section.

In the third section, each individual signal is monitored for compliance with a minimum value. These four signals are ANDed and linked to the ESTOP function block of the first section.

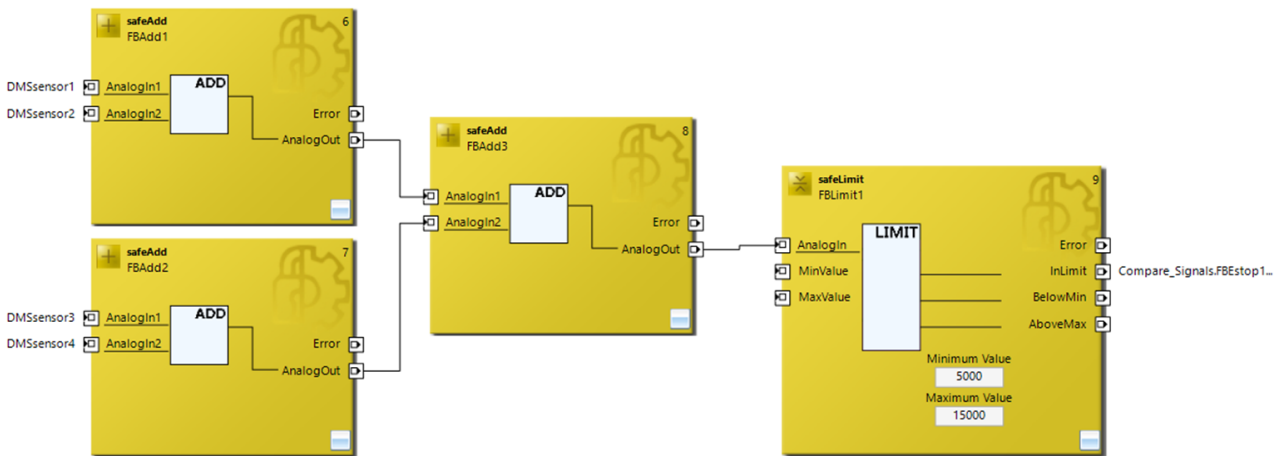
Section 1

Compare_Signals

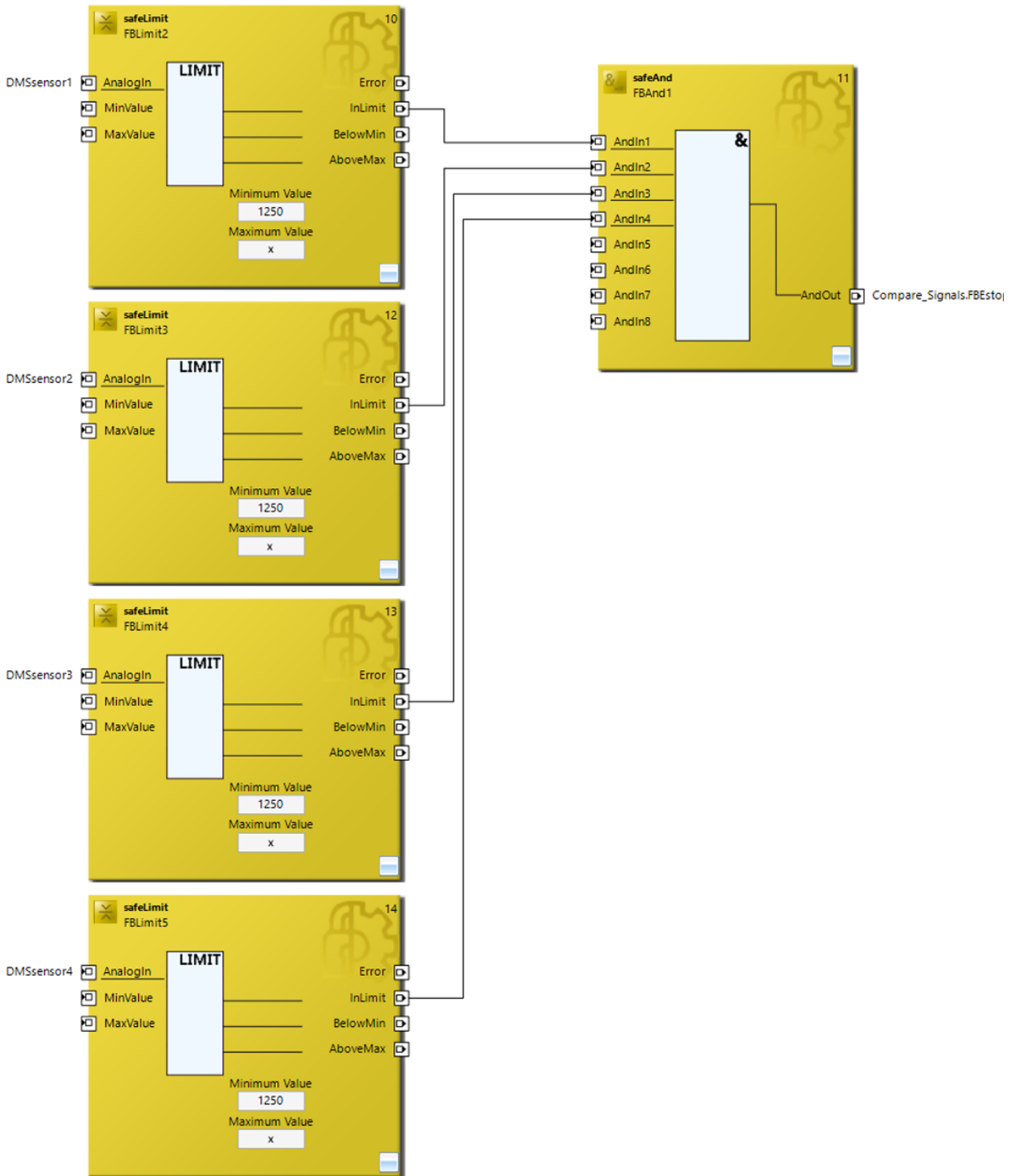


Section 2

Overload



Section 3



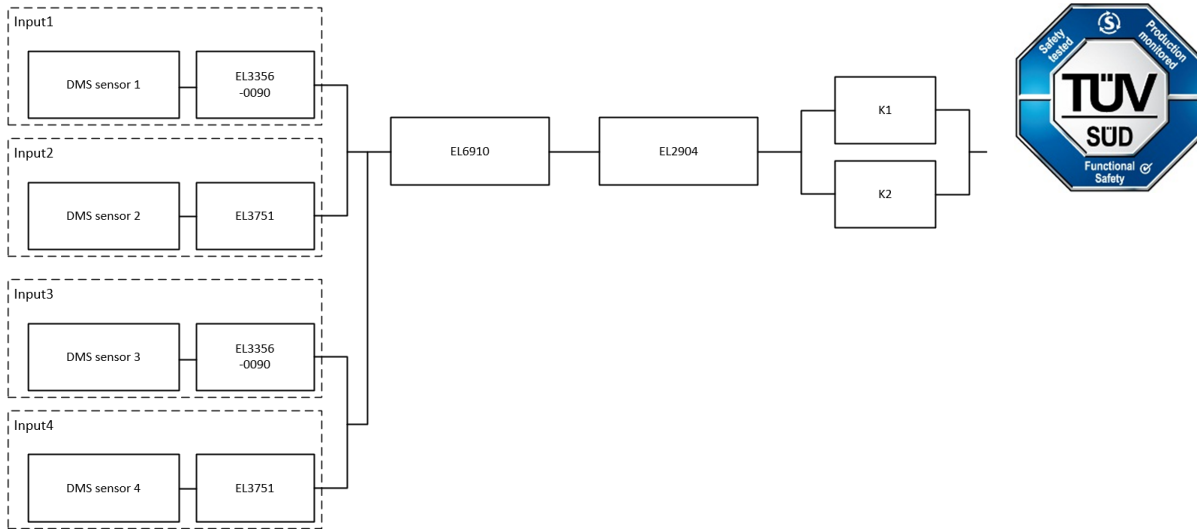
7.6.5 Parameters of the safe output terminal

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

7.6.6 Block formation and safety loops

7.6.6.1 Safety function 1/2



7.6.7 Calculation

7.6.7.1 PFHD / MTTFD / B10D – values

Component	Value
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
SG sensors 1-4 – MTTF _D (AST 3570951.1 CAL/10t/D50d11/L205/1.5 mV/V)	160 y (1,401,600 h)
EL3356-0090 - MTBF	780,733 h
EL3751 - MTBF	513,333 h
K1 – B10 _D	1,300,000 h
K2 – B10 _D	1,300,000 h
Encoder MTBF	107.5 y (914,700 h)
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

7.6.7.2 Diagnostic Coverage DC

Component	Value
SG values via TwinSAFE SC and plausibility check within the logic	DC _{avg} =90% (alternatively in calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

7.6.7.3 Calculation of safety function 1/2

For clarity, the safety factor is calculated according to EN 62061 as well as EN 13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Calculation of the PFH_D and MTTF_D values from the MTBF values:

Note: Repair times can be neglected, therefore the following applies:

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

with

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

SG sensor 1

$$MTTF_D = 1.401.600h = 160y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.401.600h} = 7,13E - 08$$

EL3356-0090

$$MTTF_D = 2 * MTBF = 2 * 780.733h = 1.561.466h = 178y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.561.466h} = 6,40E - 08$$

Input system 1

$$PFH_{(Input1)} = PFH_{(DMS1)} + PFH_{(EL3356-0090)} = 7,13E - 08 + 6,40E - 08 = 13,53E - 08$$

SG sensor 2

$$MTTF_D = 1.401.600h = 160y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.401.600h} = 7,13E - 08$$

EL3751

$$MTTF_D = 2 * MTBF = 2 * 513.333h = 1.026.666h = 117y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{1.026.666h} = 9,74E-08$$

Input system 2

$$PFH_{(Input2)} = PFH_{(DMS2)} + PFH_{(EL3751)} = 7,13E-08 + 9,74E-08 = 16,87E-08$$

For input system 3 the values calculated for input system 1 apply. For input system 4 the values calculated for input system 2 apply.

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct feedback

$$PFH = \frac{1-0,99}{593607,3 * 8760} = 1,92E-12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

The input signals from SG sensor 1 with EL3356-0090 and SG sensor 2 with EL3751 have a different internal structure, supply different values (weight value and mV/V value) and are both involved in the safety function. A malfunction of a channel does not lead to a dangerous situation, but is detected by comparing the two values in the TwinSAFE Logic and leads to shutdown. An identical configuration is used for SG sensors 3 and 4. The sum of the four sensors provides the weight value for the overload shut down. If the value of an SG sensor falls below a minimum load value, the slack rope shutdown feature is triggered.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the input subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1 / 2

$$PFH_{(DMS1/2)} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$$

$$= 10\% * \frac{13,53E-08 + 16,87E-08}{2} = 1,52E-08$$

$$PFH_{(DMS3/4)} = \beta * \frac{PFH_{(Input3)} + PFH_{(Input4)}}{2} + (1-\beta)^2 * (PFH_{(Input3)} * PFH_{(Input4)}) * T1$$

$$= 10\% * \frac{13,53E-08 + 16,87E-08}{2} = 1,52E-08$$

$$PFH_{(K1/K2)} = \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

$$= 10\% * \frac{1,92E-12 + 1,92E-12}{2} = 1,92E-13$$

Since the portions $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$\begin{aligned} PFH_{ges} &= PFH_{(DMS1/2)} + PFH_{(DMS3/4)} + PFH_{(EL6910)} + PFH_{(EL2904)} + PFH_{(K1/K2)} \\ &= 1,52E - 08 + 1,52E - 08 + 1,79E - 09 + 1,25E - 09 + 1,92E - 13 \\ &= 3,344E - 08 \end{aligned}$$

NOTE

EN 62061

According to EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This limits the maximum SIL value that can be achieved to 2, according to table 5 of EN 62061.

Alternative calculation of the $MTTF_D$ value for safety function 1 / 2 according to EN 13849 (under the same assumption)

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

The inferior value is taken from the input subsystem:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(DMSsensor2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 57,26y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}} + \frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}}}{\frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}} + \frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}}}} + \frac{\frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{90\%}{160y} + \frac{90\%}{178y} + \frac{90\%}{160y} + \frac{90\%}{117y} + \frac{90\%}{160y} + \frac{90\%}{178y} + \frac{90\%}{160y} + \frac{90\%}{117y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}}} = 90,42\%$$

Alternatively with DC = 99%

$$DC_{avg} = \frac{\frac{99\%}{160y} + \frac{99\%}{178y} + \frac{99\%}{160y} + \frac{99\%}{117y} + \frac{99\%}{160y} + \frac{99\%}{178y} + \frac{99\%}{160y} + \frac{99\%}{117y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}}} = 99,00\%$$

⚠ CAUTION

Category

This structure is possible up to category 3 at the most.

DC=90% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

Alternative with DC = 99% for the input subsystem

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC / MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

NOTE

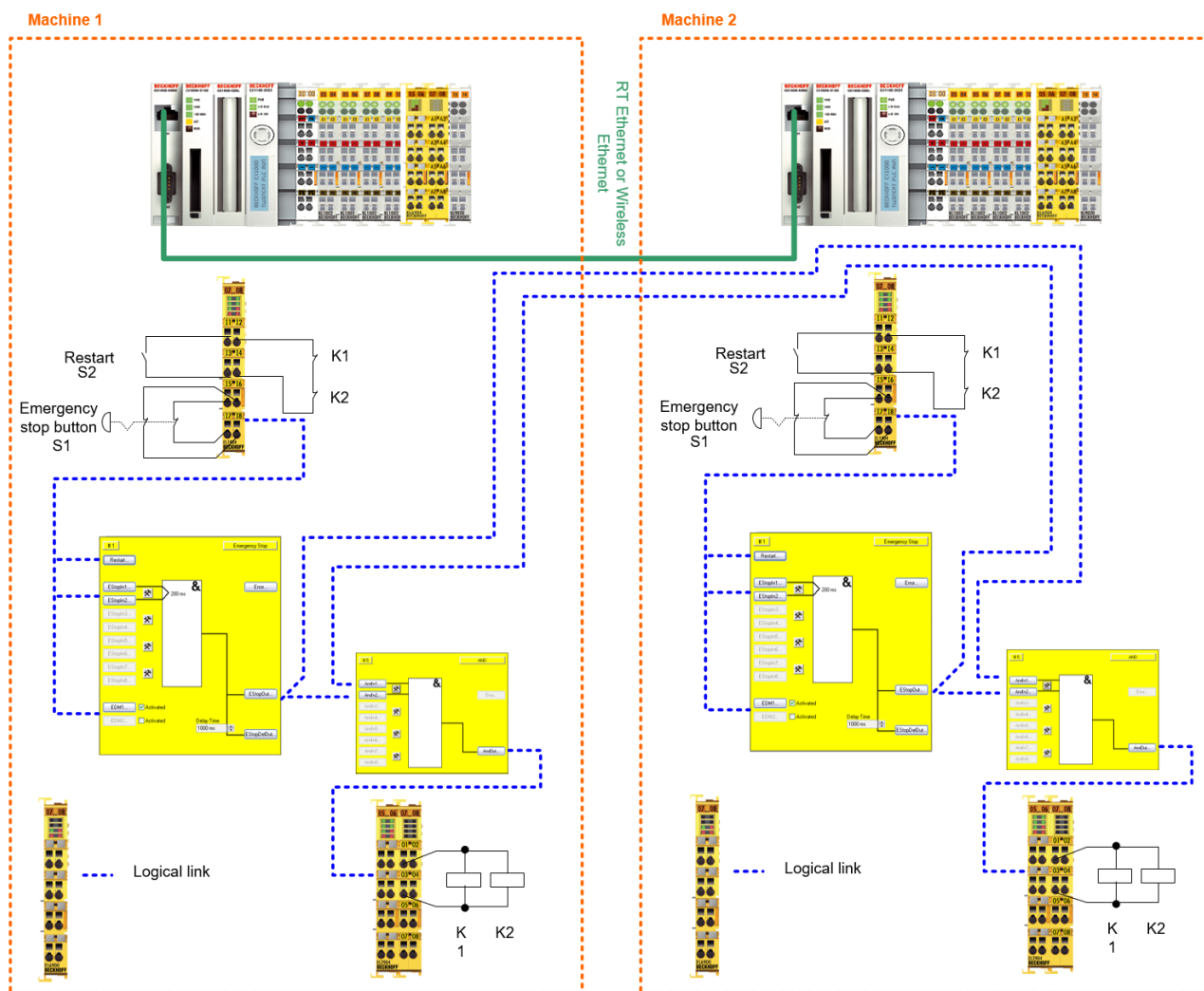
Result
 The result with category 3, PL d meets or exceeds the requirements of the risk and hazard analysis (PL c).

8 Application-specific scenarios

8.1 Networked system (Category 4, PL e)

2 plants are connected via Ethernet here. The path can also be implemented by a Wireless Ethernet connection. Each station switches the outputs K1 / K2 on only if the second machine does not signal an emergency stop. The signals from the emergency stop button, the restart and the feedback loop are wired to safe inputs. The output of the ESTOP block is linked to an AND function block and additionally signaled to the respective other machine via the network. The ESTOP output of the respective other machine is linked to the AND function block and the output of the AND gate then switches the contactors on the safe output terminal.

Testing and checking for discrepancy are activated for the input signals. The testing of the outputs is also active.



NOTE

Start / restart

If a machine has more than one operating station, measures must be provided to ensure that the initiation of commands from different operating stations does not lead to a hazardous situation.

NOTE

Contactor monitoring

If the result of the risk and hazard analysis shows that a contactor check is necessary when switching the contactors of the respective remote controller, this is to be done using an EDM function block.

8.1.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

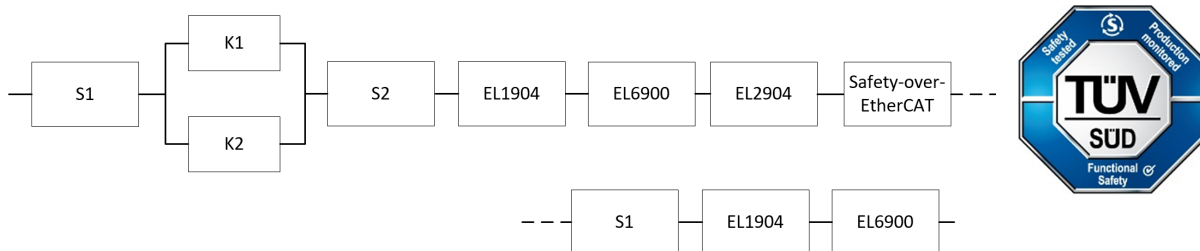
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

8.1.2 Block formation and safety loops

8.1.2.1 Safety function 1



8.1.3 Calculation

8.1.3.1 PFHD / MTTF_D / B10_D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
EL6900 – PFH _D	1.03E-09
Safety-over-EtherCAT (FSoE) – PFH _D	1.00E-09
S1 – B10 _D	1,000,000
S2 – B10 _D	2,000,000
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

8.1.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC _{avg} =99%
S2 with plausibility	DC _{avg} =90%
K1/K2 with testing and EDM (actuation 1x per shift)	DC _{avg} =99%

8.1.3.3 Calculation of safety function 1

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0,1 * 7360} = 1358,7y = 11902212h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0,1 * 7360} = 2717,4y = 23804424h$$

K1/K2:

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0,1 * 7360} = 1766,3y = 15472788h$$

and the assumption that S1, S2, K1 and K2 are each single-channel:

$$MTTF_D = \frac{1}{\lambda_D}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0,99}{1358,7 * 8760} = 8,40E - 10$$

S2:

$$PFH = \frac{1 - 0,90}{2717,4 * 8760} = 4,20E - 09$$

K1/K2: actuation 1x per shift and direct feedback

$$PFH = \frac{1 - 0,99}{1766,3 * 8760} = 6,46E - 10$$

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100000 cycles is possible, provided the manufacturer has confirmed this. If no confirmation exists, S1 is included in the calculation as follows.

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains a table with which this β-factor can be precisely determined. Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(S1)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(FSOE)} + PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)}$$

Since the portion $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ is smaller than the rest by the power of ten, it is neglected in this and all further calculations for the purpose of simplification.

to:

$$PFH_{ges} = 8,40E - 10 + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} + 4,20E - 09 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 1,00E - 09 + 8,40E - 10 + 1,11E - 09 + 1,03E - 09 = 1,25E - 08$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{D_{ges}}} = \sum_{i=1}^n \frac{1}{MTTF_{D_n}}$$

as:

$$\begin{aligned} \frac{1}{MTTF_{D_{ges}}} &= \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} \\ &+ \frac{1}{MTTF_{D(FSoE)}} + \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} \end{aligned}$$

with:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

If only PFH_D values are available for EL1904, EL2904 and EL6900, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(FSoE)} = \frac{(1 - DC_{(FSoE)})}{PFH_{(FSoE)}} = \frac{(1 - 0,99)}{1,00E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{8,76E - 06 \frac{1}{y}} = 1141,6y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1766,3y} + \frac{1}{2717,4y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1141,6y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y}} = 123,1y$$

$$\begin{aligned} DC_{avg} &= \frac{\frac{99\%}{1358,7y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y} + \frac{90\%}{2717,4y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{1141,6y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y}}{\frac{1}{1358,7y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{2717,4y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1141,6y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y}} \\ &= 98,99\% \end{aligned}$$

NOTE

Category
This structure is possible up to category 4 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	DC < 60 %
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

Diagnostic coverage
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

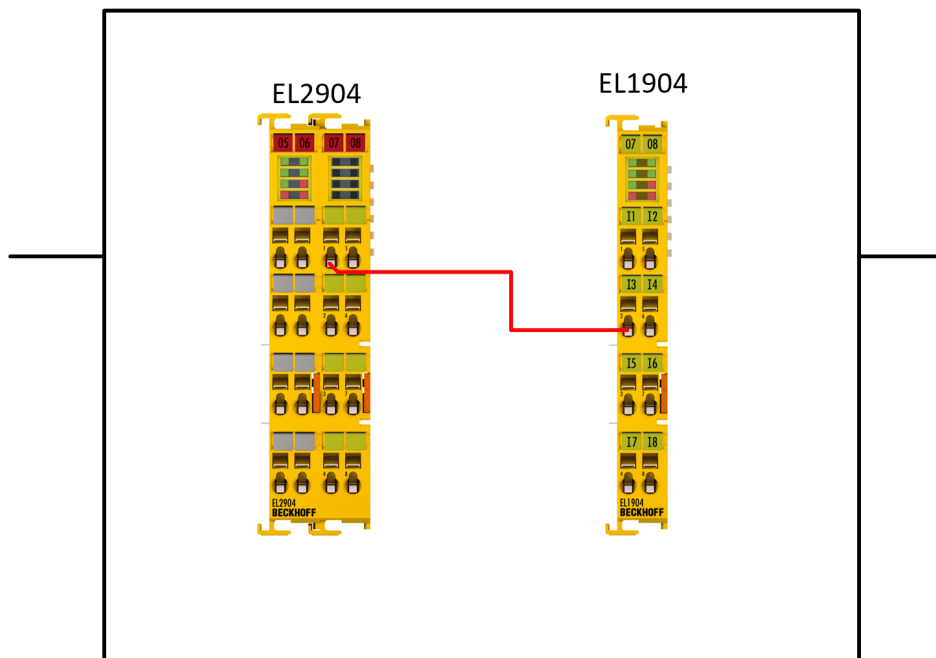
8.2 Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (1-channel) (Category 2, PL c)

The output of an EL2904 is wired directly to a safe input of an EL1904; the test pulses and current measurement of the outputs and the sensor test of the inputs are thereby deactivated. This means that no cyclic tests are possible for cross-circuits and external feed on the line.

On account of their high internal diagnostics, the EL2904 and EL1904 are to be evaluated as individual components with Category 2, SIL2 and PL d, since only a single-channel structure is used externally. The total performance level of output and input is to be evaluated with PL c at the most on account of chapter 6.2.5 DIN EN ISO 13849-1:2016-06.

The test setup required for Category 2 is integrated in the EL2904. When switching on the output of the EL2904, a check is performed to ascertain whether 24 V are actually read back. When switching off, a check is performed to ascertain whether 0 V are actually read back. If an error is detected, the EL2904 enters the error state, which is also signaled to the higher level safety controller. This module error of the EL2904 must be evaluated in the machine controller. To do this the parameter *ModuleFault is ComError* is to be switched on for the connection to the EL2904, as a result of which the TwinSAFE group switches to the safe state and signals a ComError in the event of a module error.

Cat.2, PL c



8.2.1 Parameters of the safe input and output terminals

EL1904

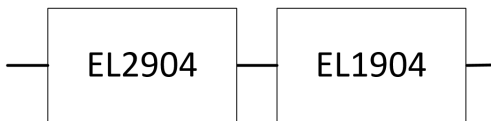
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	No

8.2.2 Block formation and safety loops

8.2.2.1 Safety function 1



8.2.3 Calculation

8.2.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

8.2.3.2 Diagnostic Coverage DC

Component	Value
EL1904/EL2904 On account of the internal diagnostics of the terminals (such as monitoring of the field voltage, temperature, etc.) and the checking of the EL2904 for the correctness of the switched output each time the signal state changes	DC _{avg} =60%

8.2.3.3 Calculation of safety function 1

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(EL1904)} + PFH_{(EL2904)}$$

to:

$$PFH_{ges} = 1,11E - 09 + 1,25E - 09 = 2,36E - 09$$

Calculation of the $MTTF_D$ value for safety function 1:

$$\frac{1}{MTTF_{D_{ges}}} = \sum_{i=1}^n \frac{1}{MTTF_{D_n}}$$

as:

$$\frac{1}{MTTF_{D_{ges}}} = \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL2904)}}$$

If only PFH_D values are available for EL1904 and EL2904, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,60)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,4}{9,72E - 06 \frac{1}{y}} = 41152y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,60)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,4}{1,1E - 05 \frac{1}{y}} = 36364y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{41152y} + \frac{1}{36364y}} = 19305y$$

$$DC_{avg} = \frac{\frac{60\%}{41152y} + \frac{60\%}{36364y}}{\frac{1}{41152y} + \frac{1}{36364y}} = 60\%$$

NOTE

Category

This structure is possible up to category 2 at the most.

⚠ CAUTION

Achieving the safety level

For the Attainment of the safety level the user must ensure that a testing of the wiring is carried out within his application and will be done 100 times more often than the safety function is called.

MTTF _D	
Designation for each channel	Range for each channel
low	$3 \text{ years} \leq \text{MTTF}_D < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_D < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_D \leq 100 \text{ years}$

DC	
Name	Range
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

8.3 Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (2-channel) (Category 3, PL d)

Two outputs of an EL2904 are wired directly to two safe inputs of an EL1904; the test pulses and current measurement of the outputs and the sensor test of the inputs are thereby deactivated. On the input side, both signals are checked for discrepancy within the TwinSAFE Logic. Hence, both signals are checked for their value, but no tests are active on the cable, so that possible external feeds are detected when switching the outputs.

8.3.1 Parameters of the safe input and output terminals

EL1904

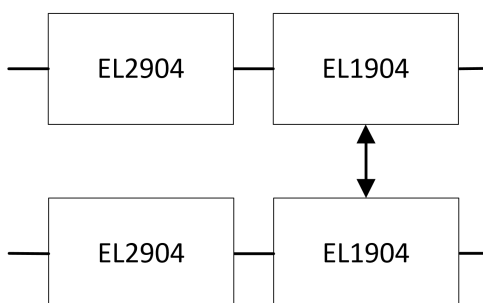
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	No

8.3.2 Block formation and safety loops

8.3.2.1 Safety function 1



8.3.3 Calculation

8.3.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH _D	1.11E-09
EL2904 – PFH _D	1.25E-09
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	8
Cycle time (minutes) (T _{cycle})	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

8.3.3.2 Diagnostic Coverage DC

Component	Value
EL1904/EL2904	DC _{avg} =90%

8.3.3.3 Calculation of safety function 1

It follows for the calculation of the PFH_D value for safety function 1:

$$PFH_{ges} = PFH_{(EL1904)} + PFH_{(EL2904)}$$

to:

$$PFH_{ges} = 1,11E - 09 + 1,25E - 09 = 2,36E - 09$$

Calculation of the MTTF_D value for safety function 1 (under the same assumption):

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

as:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL2904)}}$$

If only PFH_D values are available for EL1904 and EL2904, the following estimation applies:

$$MTTF_{D(ELxxx)} = \frac{(1 - DC_{(ELxxx)})}{PFH_{(ELxxx)}}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,90)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{9,72E - 06 \frac{1}{y}} = 10288,1y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,90)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{1,1E - 05 \frac{1}{y}} = 9090,9y$$

$$MTTF_{D_{ges}} = \frac{1}{\frac{1}{10288,1y} + \frac{1}{9090,9y}} = 4826,3y$$

$$DC_{avg} = \frac{\frac{90\%}{10288,1y} + \frac{90\%}{10288,1y} + \frac{90\%}{9090,9y} + \frac{90\%}{9090,9y}}{\frac{1}{10288,1y} + \frac{1}{10288,1y} + \frac{1}{9090,9y} + \frac{1}{9090,9y}} = 90\%$$

NOTE

Category

This structure is possible up to category 3 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9 Connection of PROFI-safe

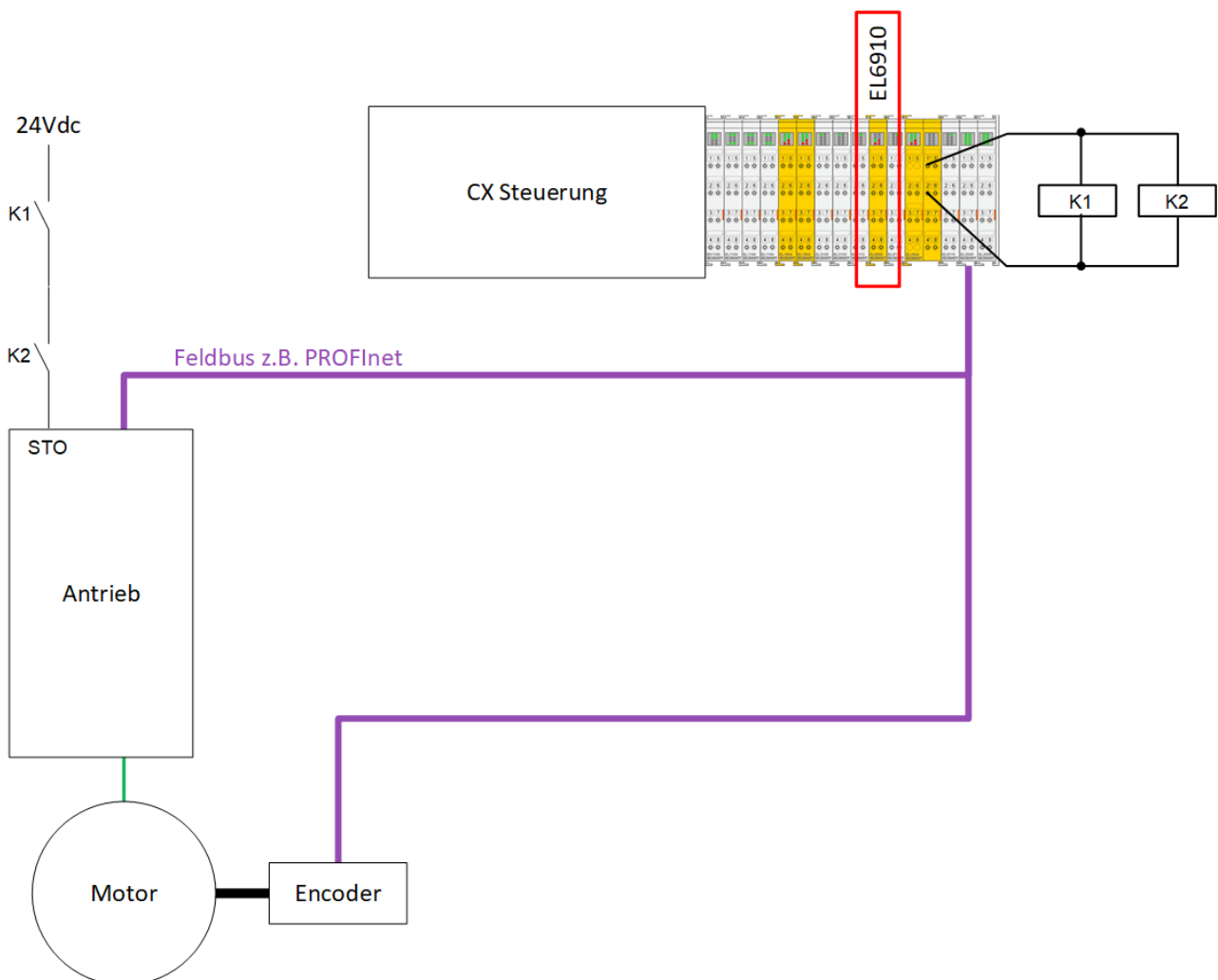
9.1 Safe speed monitoring with PROFI-safe encoder (category 4, PL e)

The speed of a drive is to be monitored. This drive has a safety function (in this case, for example, STO), which is activated via a corresponding input. This input is/these inputs are conducted via a NO contact of two contactors. A safe absolute rotary encoder from TR-Electronic is used to safely measure the speed. It is certified for applications up to Performance Level e. The safety-relevant data is transmitted via PROFINet with the help of PROFI-safe. The speed data is transmitted via the safety-relevant protocol PROFI-safe to the EL6910 as the PROFI-safe master and monitored there with the help of the available pre-certified function blocks for analog value processing.

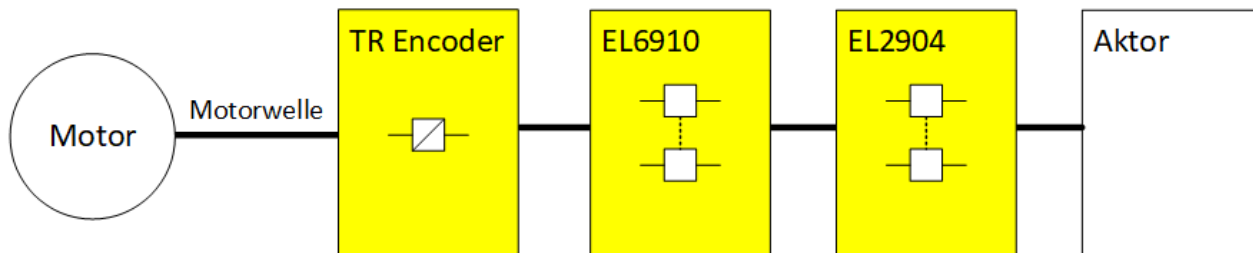
If the current speed value lies below the threshold specified in the Limit FB, the STO output is set to logical 1 and the drive can rotate. If the limit is exceeded, the output is set to logic 0 and the drive is switched torque-free or the safety function integrated in the drive is activated. The entire calculation and scaling are performed at safety level SIL3/PL e in the safety-related EL6910 logic.

An ESTOP function block also implements an emergency stop function (not shown in the graph to reduce complexity), which prevents restarting and also assumes control of the contactors K1 and K2.

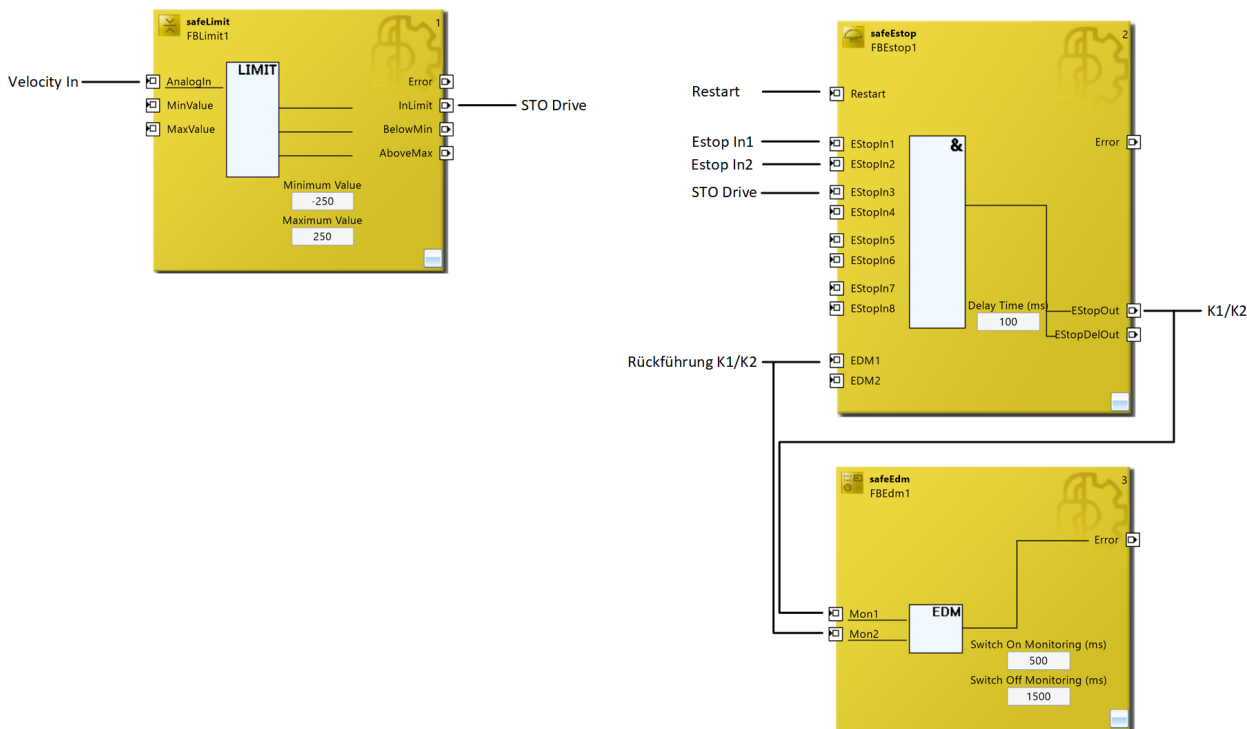
Structure



Structure diagram configuration



Logic



Correct configuration of the overall system

The following restrictions apply when transmitting PROFIsafe within EtherCAT.

PROFIsafe telegram only via E-bus and PROFINET/PROFIBUS

On account of the PROFIsafe policy, the use of PROFIsafe is permitted only via the PROFIBUS and PROFINET fieldbuses or via a backplane bus, in this case for example the E-bus. The use of PROFIsafe via other fieldbuses is impermissible for reasons connected with patent law. This must be ensured through the use of the EL9930 segment end terminal.

The following Siemens AG patents are relevant according to the PROFIsafe profile:

- EP1267270-A2 Method for data transfer
- WO00/045562-A1 Method and device for determining the reliability of data carriers
- WO99/049373-A1 Shortened data message of an automation system
- EP1686732 Method and system for transmitting protocol data units
- EP1802019 Identification of errors in data transmission
- EP1921525-A1 Method for operation of a safety-related system
- EP13172092.2 Method and system for detection of errors

Depending on the architecture of the application, appropriate measures must therefore be taken. Details of the correct configuration of the overall system with regard to PROFIsafe can be found in the documentation for the EL6910 and EL9930.

Use of external safe encoders

Further requirements must be met when using an external encoder.

⚠ CAUTION
<p>Use of external safe encoders</p> <p>When using an external safe encoder, the current version of the documentation must always be observed. Here you will find all the requirements for assembly, operation and repair, which must be met so that the encoder can be used correctly in a safety-relevant application.</p>

9.1.1 FMEA

Error assumption	Expectations	Checked
Speed value freezes	The speed in the encoder is determined safely (Performance Level e) and transmitted safely via PROFIsafe. Freezing of the telegram is detected via the watchdog of the safe communication protocol.	
Speed value is falsified	The speed in the encoder is determined safely (Performance Level e) and transmitted safely via PROFIsafe. Falsification of the telegram is detected via the safe communication protocol.	
There is no longer any connection between the motor and the encoder	<p>Can be detected via a plausibility check with a standard drive signal. Thus, both the standard speed of the drive can be used for a plausibility check as well as a Boolean information about whether the drive should be rotating. Alternatively, the position signal of the safe telegram can be used as the input signal of the function block safeScaling in order to be able to detect this error case with the help of the output <i>StuckAtError</i> (e.g. in combination with the evaluation of the information as to whether the drive is being actively decelerated).</p> <p>Plausibility check: Dynamic speed values are also expected when the motor is started.</p>	

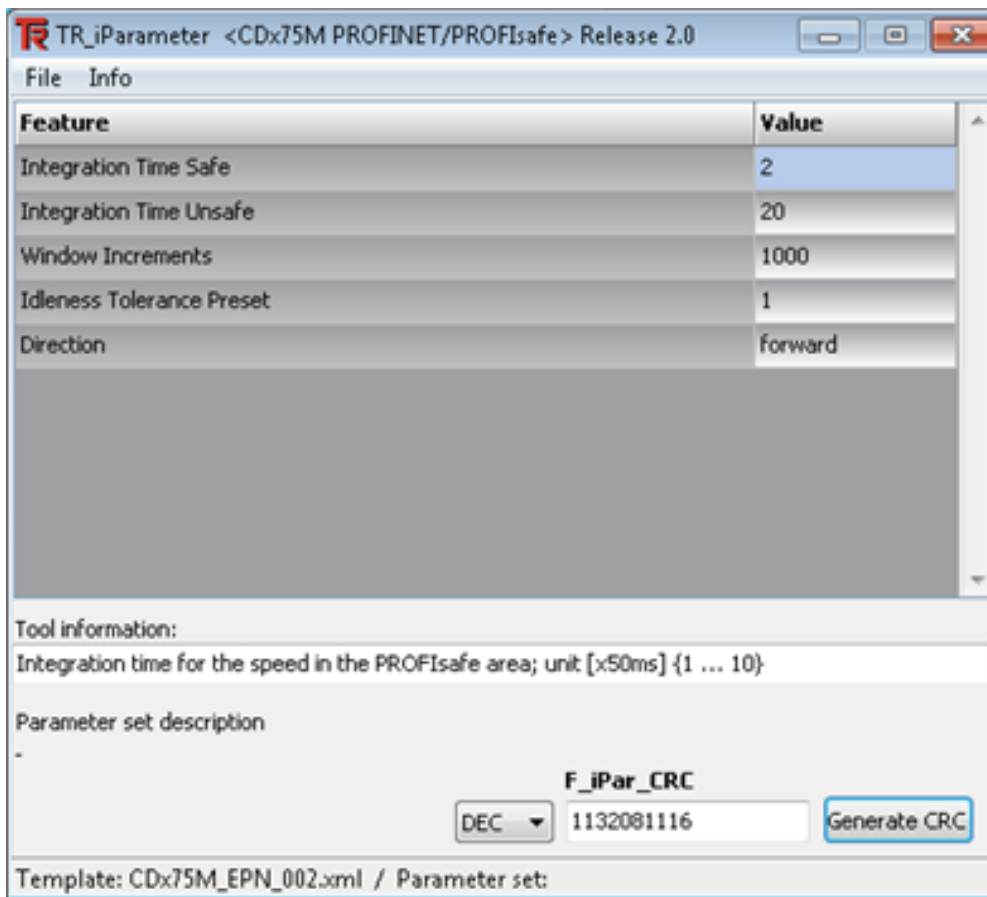
9.1.2 Configuration in the engineering environment

In addition to the connection of TwinSAFE components, the additional connection of an encoder via PROFIsafe/PROFINet is considered in the context of this application example. All necessary configuration steps for the implementation are described in detail below.

For the configuration of the safety-relevant parameters of the encoder, an additional application is required to perform the parameterization of the device and to determine the CRC checksum of the iParameters, which ultimately has to be additionally configured within TwinCAT.

9.1.2.1 Encoder configuration

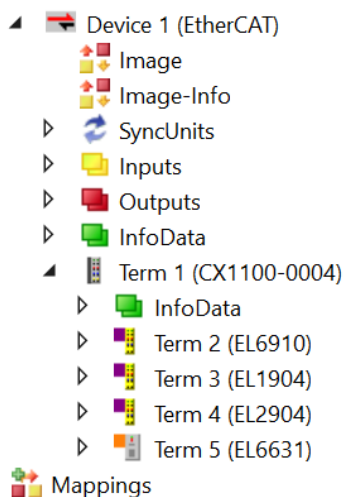
An additional application is required for the parameterization of the encoder. The current version can be obtained from the manufacturer's website.



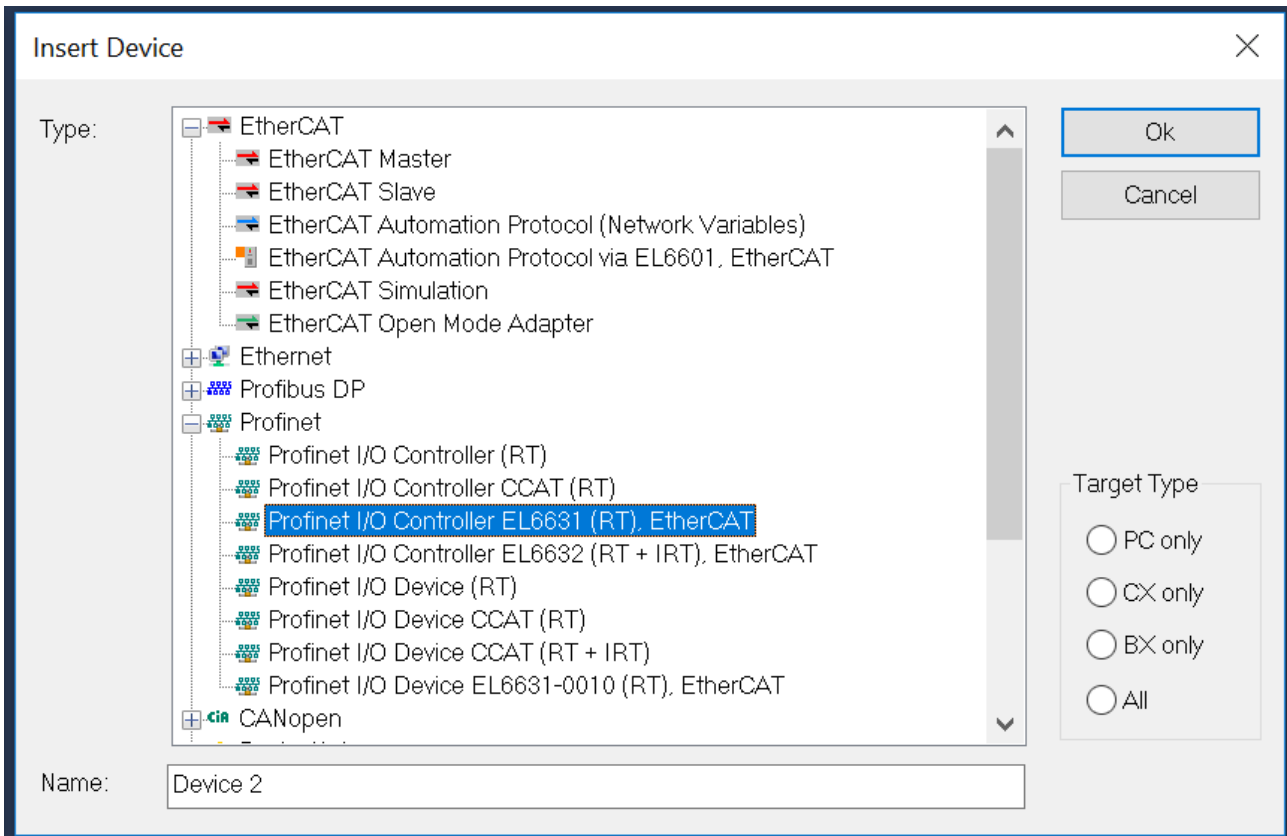
Here the necessary parameters have to be configured according to the application, so that the CRC checksum can be calculated correctly (**F_iPar_CRC** in the illustration).

9.1.2.2 Configuration of TwinCAT I/O

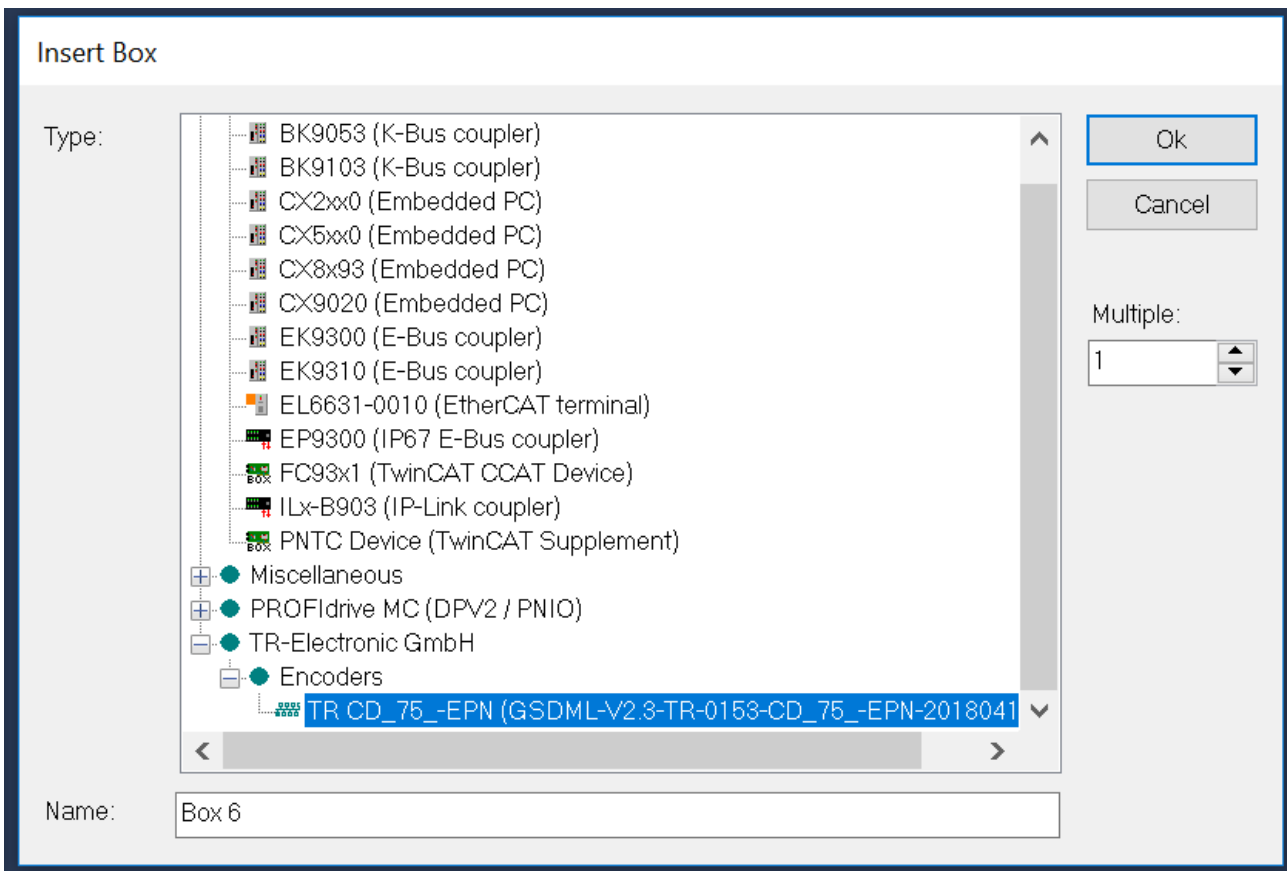
First, a new TwinCAT project is created and the EtherCAT segment is configured.



In addition, the configuration of the PROFINet segment is generated by adding a PROFINet I/O controller.



In the same way as the configuration of the EtherCAT segment, an automatic scan can also be initiated in the case of the PROFINet controller or the configuration can be generated manually. In this way, the encoder can also be added manually.



The following information must be observed for the successful use of the encoder via PROFIsafe.

⚠ CAUTION**Data type WORD!**

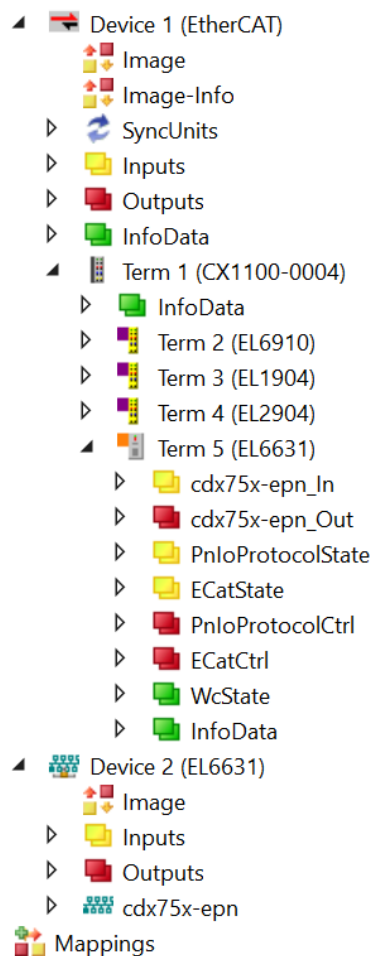
An additional configuration may have to be done when using WORD data types within the process image.

If no EL9930 is used within the configuration to limit the PROFIsafe segment, the swapping of the high and low byte portions must be configured as part of the I/O configuration of the PROFIsafe device for the signals with WORD data type contained in the process image. This is done by checking the *Swap LOBYTE and HIBYTE* checkbox directly on the data values (on the *Flags* tab).

⚠ CAUTION**iParameters**

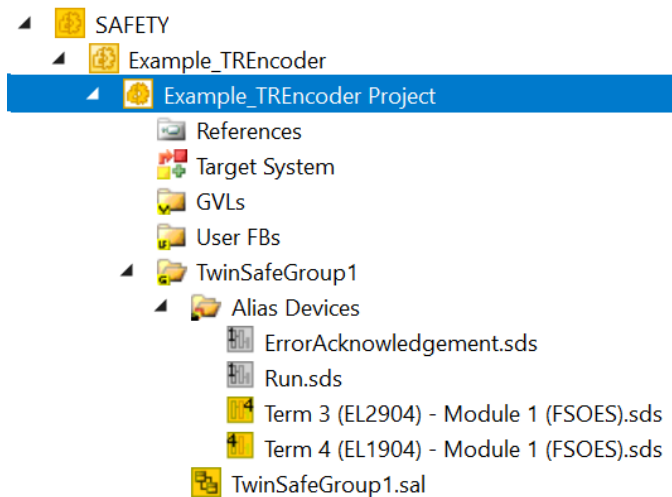
The identical iParameters as on the *Alias Device* must be configured on the PROFIsafe I/O device so that communication can start correctly.

You can then continue with the configuration of the safety project. At this point, the following initial situation is assumed.

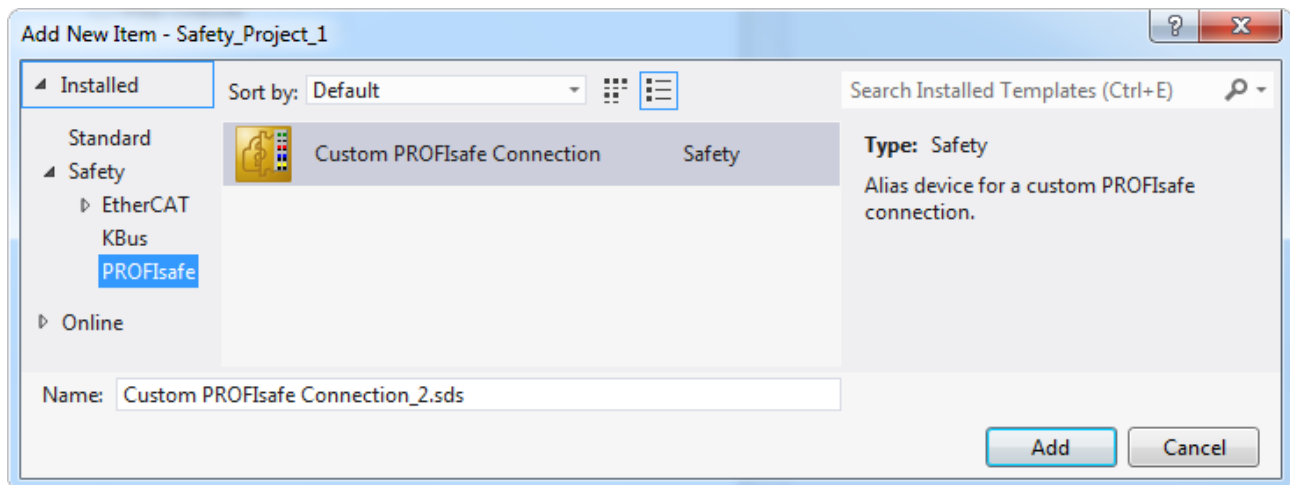


9.1.2.3 Configuration of TwinCAT safety project connections

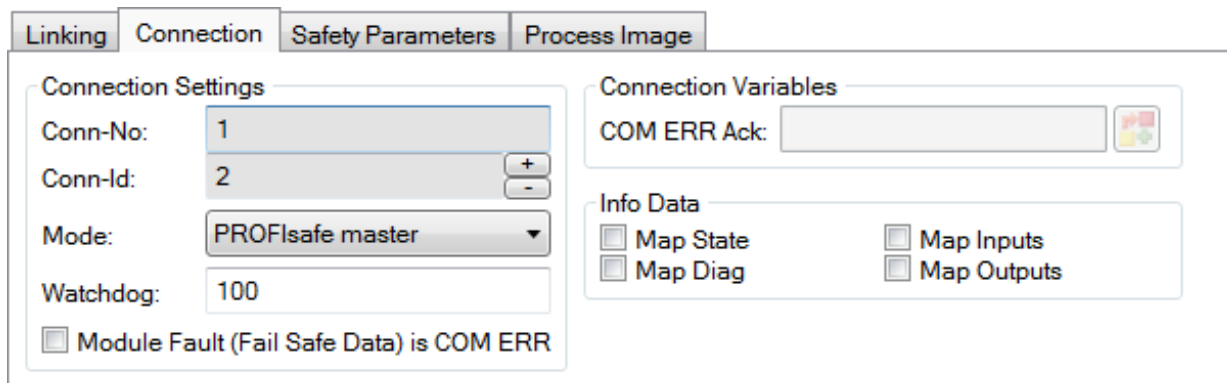
Before configuring the PROFIsafe connection, a safety project is created first and the required alias devices for the available EtherCAT components are imported. In addition, the target system is mapped to the EL6910 of the EtherCAT segment (via the *Target System* node).



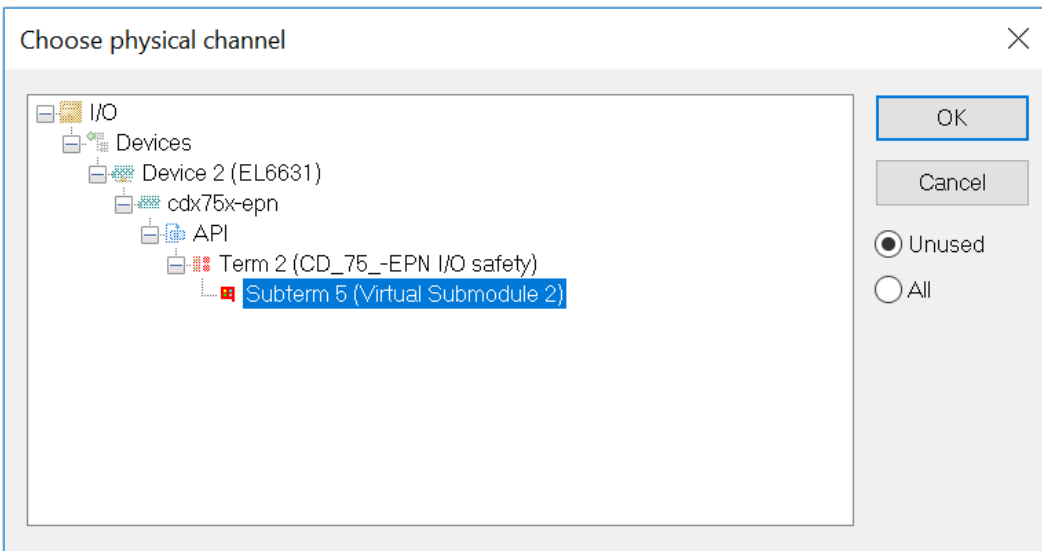
You can then continue with the configuration of the PROFIsafe connection to the TR encoder. This connection is implemented as usual via an *Alias Device*. A *Custom PROFIsafe Connection* can be created via the context menu of the node *Alias Devices* selecting *Add* and *New* item....



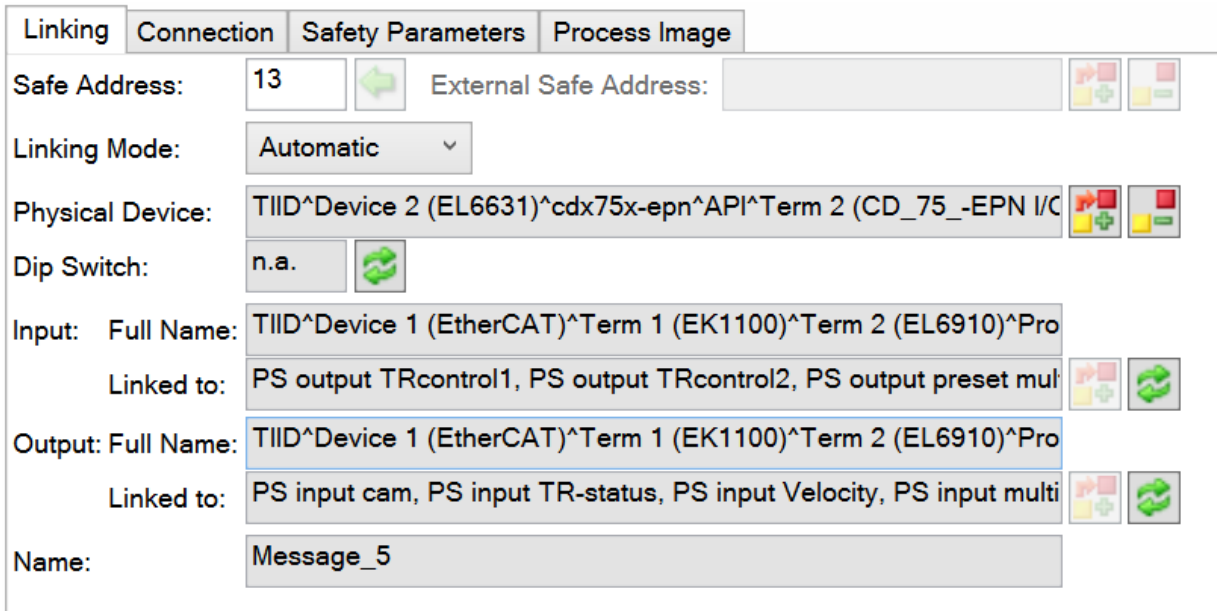
After opening the Alias Device, *PROFIsafe Master* must first be selected as the mode of the connection on the *Connection* tab.



On the *Linking* tab, the linking mode must be set to *Automatic* so that the TR encoder considered here can be selected via the *Map to Physical Device* button.



In addition to mapping to the physical device, the safe address of the encoder must also be entered on the *Linking* tab (13 in this example).



If all settings have been made correctly, the safe process image of the encoder can be viewed on the *Process Image* tab (with the entry *Velocity*, which is relevant in this example).

Linking Connection Safety Parameters Process Image

Inputs

Message Size: 14 Bytes (10 Bytes Safe Data)

Name	Type	Size	Position
PS input TR-status[4]	BIT	0.1	2.4
PS input TR-status[5]	BIT	0.1	2.5
PS input TR-status[6]	BIT	0.1	2.6
PS input TR-status[7]	BIT	0.1	2.7
PS input TR-status[8]	BIT	0.1	3.0
PS input TR-status[9]	BIT	0.1	3.1
PS input TR-status[10]	BIT	0.1	3.2
PS input TR-status[11]	BIT	0.1	3.3
PS input TR-status[12]	BIT	0.1	3.4
PS input TR-status[13]	BIT	0.1	3.5
PS input TR-status[14]	BIT	0.1	3.6
PS input TR-status[15]	BIT	0.1	3.7
PS input Velocity	INT	2.0	4.0
PS input multiturn	INT	2.0	6.0
PS input singleturn	INT	2.0	8.0

Edit

Outputs

Message Size: 12 Bytes (8 Bytes Safe Data)

Name	Type	Size	Position
PS output TRcontrol1[0]	BIT	0.1	0.0
PS output TRcontrol1[1]	BIT	0.1	0.1
PS output TRcontrol1[2]	BIT	0.1	0.2
PS output TRcontrol1[3]	BIT	0.1	0.3
PS output TRcontrol1[4]	BIT	0.1	0.4
PS output TRcontrol1[5]	BIT	0.1	0.5
PS output TRcontrol1[6]	BIT	0.1	0.6
PS output TRcontrol1[7]	BIT	0.1	0.7
PS output TRcontrol1[8]	BIT	0.1	1.0
PS output TRcontrol1[9]	BIT	0.1	1.1
PS output TRcontrol1[10]	BIT	0.1	1.2
PS output TRcontrol1[11]	BIT	0.1	1.3
PS output TRcontrol1[12]	BIT	0.1	1.4
PS output TRcontrol1[13]	BIT	0.1	1.5
PS output TRcontrol1[14]	BIT	0.1	1.6
PS output TRcontrol1[15]	BIT	0.1	1.7

Edit

The *Safety Parameters* tab provides the parameters for the PROFIsafe master connection.

Linking Connection Safety Parameters Process Image

Name	R/W	Current Value	I/O Treeltem Value	Default Value
F_Check_Seq_Nr	R/W	0 (0)	0 (0)	0 (0)
F_Check_iPar	R/W	0 (0)	0 (0)	0 (0)
F_SIL	R/W	SIL3 (2)	SIL3 (2)	SIL3 (2)
F_CRC_Length	R	3-Byte-CRC (0)	3-Byte-CRC (0)	3-Byte-CRC (0)
F_Block_ID	R	0 (0)	1 (1)	1 (1)
F_Par_Version	R	V2-mode (1)	V2-mode (1)	V2-mode (1)
F_Source_Add	R/W	0x0001 (1)	0x0001 (1)	0x0001 (1)
F_Dest_Add	R/W	0x000D (13)	0x0001 (1)	0x0001 (1)
F_WD_Time	R/W	0x0064 (100)	0x007D (125)	0x007D (125)
F_iPar_CRC	R/W	0x00000000 (0)	0x437A2FDC (1132081116)	0x437A2FDC (1132081116)
F_Par_CRC	R	0x5863 (22627)	0x4289 (17033)	0x4289 (17033)

Edit Set Current to Default Value Set Current to I/O Treeltem Value Get I/O Treeltem Values Update I/O Treeltem

Fig. 1: Safety Parameter Encoder

All parameters for the PROFIsafe connection must be set correctly here. These include the two addresses *F_Source_Add* (target system) and *F_Dest_Add* (safe address of PROFIsafe device). In addition, the CRC of the *iParameters* must be configured. This can be taken from the additional application for configuring the encoder (see section *Encoder Configuration*)

In the case of a PROFIsafe device, the parameters must be set both within the Alias Device and directly for the device in the I/O configuration. The reading of the data from the I/O device and the transfer to the I/O device can be initiated via the corresponding buttons on the *Safety Parameters* tab. Both data must match for a PROFIsafe connection to be successfully established.

Parameter	Description
F_Check_Seq_Nr	Setting (0/1) to indicate whether the sequence number of the connection should be checked.
F_Check_iPar	Setting (0/1) to indicate whether the parameterization should take place via an iPar server.
F_SIL	Selecting the required SIL level (SIL1, SIL2, SIL3, NoSIL)
F_CRC_Length	Display of the CRC length
F_Block_ID	always 0
F_Par_Version	PROFIsafe version used (typically V2 mode)
F_Source_Add	Setting the PROFIsafe source address
F_Dest_Add	Setting the PROFIsafe destination address
F_WD_Time	Setting the watchdog time
F_iPar_CRC	i-parameter(s) for the PROFIsafe slave
F_Par_CRC	Calculated CRC across all parameters

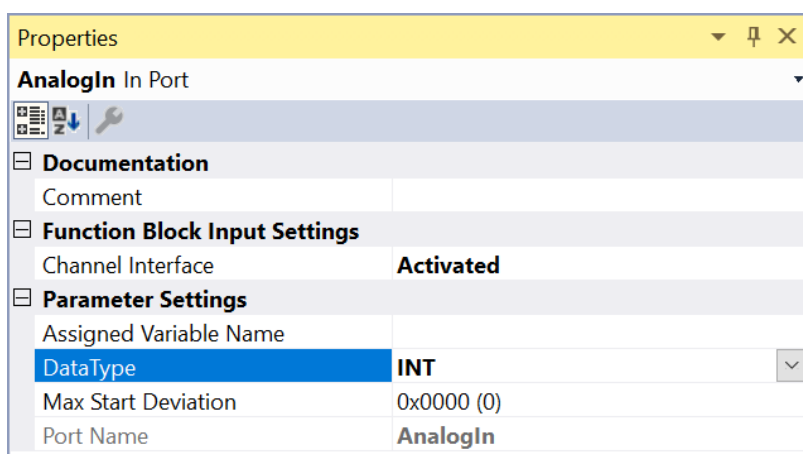
After completion of the configuration of the parameters, they must be transferred to the I/O configuration by clicking the button *Update IO TreeItem* final.

After completion of the configuration of the connections, you can continue with the implementation of the actual safety function.

9.1.2.4 Implementing a TwinCAT safety project

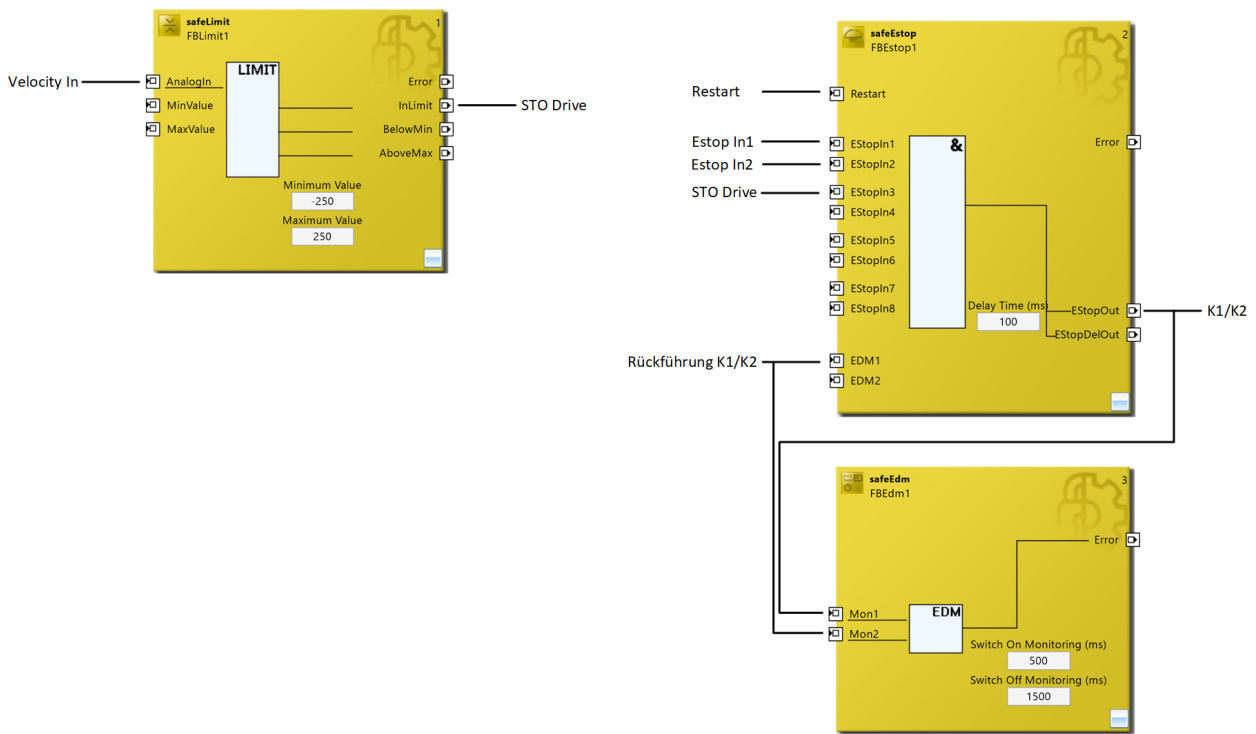
In the context of the safety function for monitoring the speed of a drive considered in this example, the safe speed value received via PROFIsafe is used to compare it to a specified limit value and to react appropriately if this limit value is exceeded.

A *safeLimit* function block is used to check the speed value. The speed value received via PROFIsafe is a 16-bit integer value (see *the Process Image* tab of the *Alias Device* for the PROFIsafe connection). Accordingly, the data type of the input *AnalogIn* must be configured as *INT* for the inserted *safeLimit* function block.



The input can then be linked to the *Velocity* signal of the PROFIsafe connection.

The *InLimit* signal resulting from the *safeLimit* function block indicates whether the speed is below the configured maximum limit. It can be used further to additionally evaluate a possibly existing emergency stop switch with a *safeEstop* function block, for example.



As the illustration shows, the *EstopOut* output of the *safeEstop* function block switches the two contactors *K1* and *K2*, which in turn control the *STO* safety function of the drive. The feedback from the contactors is used as an *EDM* input of the *safeEstop* function block.

In addition to the function blocks already described, a *safeEdm* function block is used to check the correct behavior of the contactors *K1* and *K2*. Here, the time intervals for the switch-on and switch-off check are configured according to the contactors used.

9.1.3 Parameters of the safe output terminal

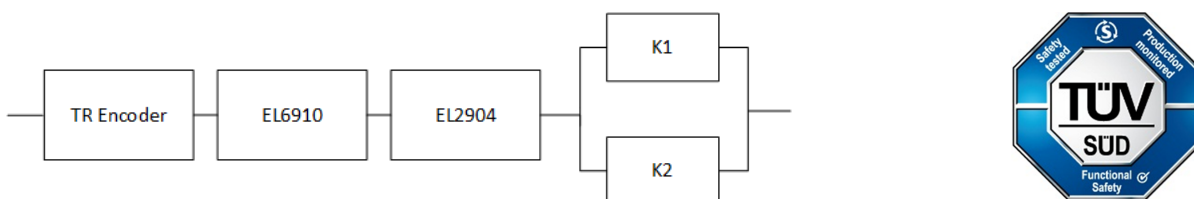
EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

9.1.4 Block formation and safety loops

9.1.4.1 Safety function 1 (without drive)

Safety function 1 considers the safety loop starting from the TR encoder to the contactors *K1*/*K2* for the application example described so far. The downstream *STO* inputs are not considered in this safety function.



9.1.4.2 Safety function 2 (with drive)

Safety function 2 considers the safety loop starting from the TR encoder for the application example described so far. The STO functionality is controlled by safe communication. For this purpose, a drive with corresponding characteristic safety values is assumed within the context of the calculation.



9.1.5 Calculation of safety function 1 (without drive)

9.1.5.1 PFHD / MTTFD / B10D – values

Component	Value
TR Encoder ¹⁾ – PFH _D	1.46E-09
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

¹⁾ Please note the information provided in the current user documentation

9.1.5.2 Diagnostic Coverage DC

Component	Value
TR Encoder ¹⁾	DC _{avg} =95%
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) with testing of the individual channels	DC _{avg} =99%

¹⁾ Please note the information provided in the current user documentation

9.1.5.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN ISO 13849-1. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 1x per week and direct read back

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the output subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = PFH_{(Encoder)} + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$PFH_{ges} = 1,46E - 09 + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 09 + 1,94E - 09}{2}$$

$$PFH_{ges} = 4,69E - 09$$

The MTTF_D value according to EN 13849 for safety function 1 is calculated with:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

to:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

If only PFH_D values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

The value of the encoder can be taken from the current user documentation:

$$MTTF_{d(Encoder)} = 421y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{421y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 198y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

$$DC_{avg} = \frac{\frac{95\%}{421} + \frac{99\%}{637} + \frac{99\%}{913} + \frac{99\%}{593607} + \frac{99\%}{593607}}{\frac{1}{421} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = 97,12\%$$

⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Area
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.1.6 Calculation of safety function 2 (with drive)

9.1.6.1 PFHD / MTTFD / B10D – values

Component	Value
TR Encoder ¹⁾ – PFH _D	1.46E-09
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
AX8xxx-x1xx – PFH _D	3.04E-09
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

¹⁾ Please note the information provided in the current user documentation

9.1.6.2 Diagnostic Coverage DC

Component	Value
TR Encoder ¹⁾	DC _{avg} =95%
AX8xxx-x1xx STO function	DC _{avg} >99%

¹⁾ Please note the information provided in the current user documentation

9.1.6.3 Calculation of safety function 2

It follows for the calculation of the PFH_D value for safety function 2:

$$PFH_{ges} = PFH_{(Encoder)} + PFH_{(EL6910)} + PFH_{(AX8xxx-x1xx)}$$

$$PFH_{ges} = 1,46E - 09 + 1,79E - 09 + 3,04E - 09$$

$$PFH_{ges} = 6,29E - 09$$

The MTTF_D value according to EN 13849 for safety function 1 is calculated with:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

to:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}$$

with:

If only PFH_D values exist for AX8xxx-x1xx and EL6910, the following estimation applies:

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(AX8xxx-x1xx)} = \frac{(1 - DC_{(AX8xxx-x1xx)})}{PFH_{D(AX8xxx-x1xx)}} = \frac{(1 - 0,99)}{3,04E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{2,66E - 05 \frac{1}{y}} = 375y$$

Fig. 2:

The value of the encoder can be taken from the current user documentation:

$$MTTF_{d(Encoder)} = 421y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{421y} + \frac{1}{637y} + \frac{1}{375y}} = 151y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(AX8.xxx-x1.xx)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8.xxx-x1.xx)}}$$

$$DC_{avg} = \frac{\frac{95\%}{421} + \frac{99\%}{637} + \frac{99\%}{375}}{\frac{1}{421} + \frac{1}{637} + \frac{1}{375}} = 97,56\%$$

⚠ CAUTION

Implement a restart lock in the machine!
 The restart lock is NOT part of the safety chain and must be implemented in the machine!

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Area
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

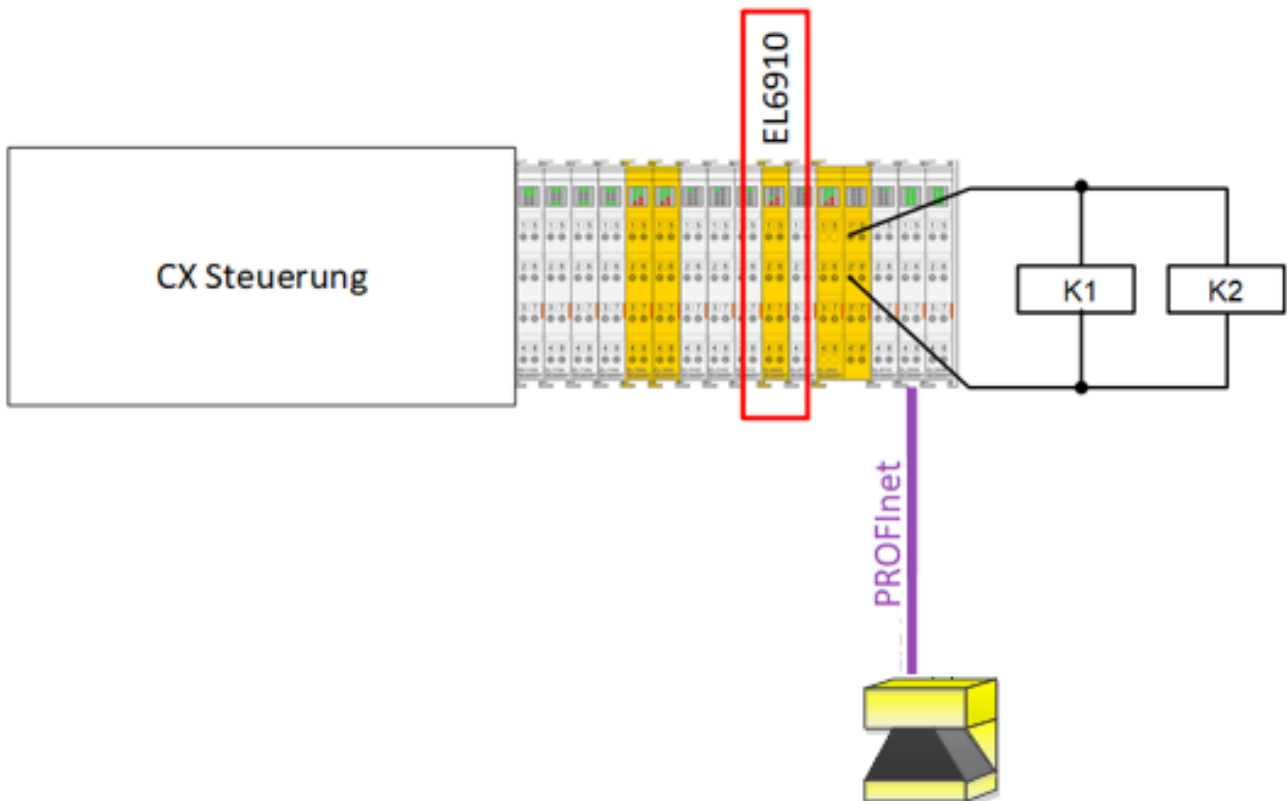
9.2 Safe area monitoring with PROFI-safe laser scanner (category 3, PL d)

The hazard area of a machine is to be monitored by means of a safety laser scanner. This hazard can be switched off by two contactors. The contactors are connected to an output of an EL2904. A microScan3 safety laser scanner from SICK is used for safe area monitoring. It is certified for applications up to Performance Level d. The relevant data are transmitted via the safety-relevant protocol PROFI-safe to the EL6910 as the PROFI-safe master and monitored there with the help of the available pre-certified function blocks.

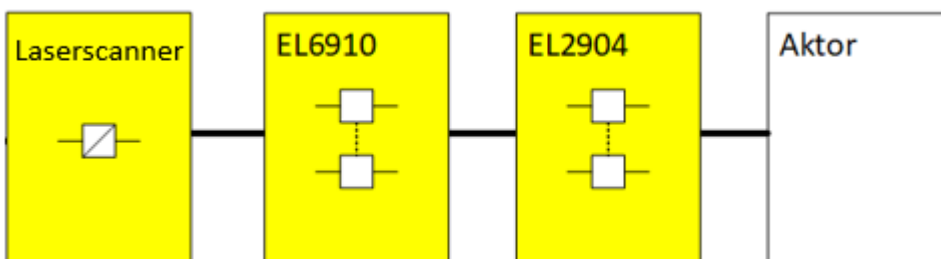
If the two switch-off paths of the set monitoring case (two signals within the PROFI-safe protocol) signal logic 1, then the protective field is free and the two contactors are switched on. If the protective field is occupied, the two switch-off paths signal logic 0 and the contactors are switched off. The entire evaluation is carried out in the safety-related logic EL6910 at the safety level SIL3 / PL e.

Any necessary restart lock can be realized via the reset input of the fbMon. The feedback loop is read in via a safe input. Testing is active for this input.

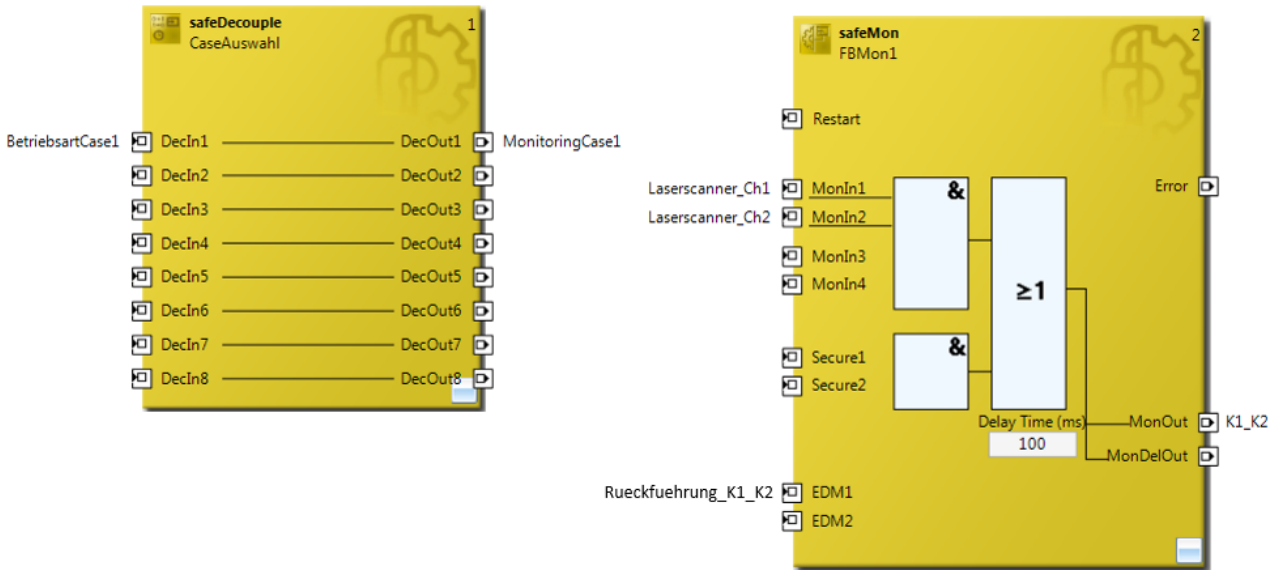
Structure



Structure diagram configuration



Logic



Correct configuration of the overall system

The following restrictions apply when transmitting PROFIsafe within EtherCAT.

PROFIsafe telegram only via E-bus and PROFINET/PROFIBUS

On account of the PROFIsafe policy, the use of PROFIsafe is permitted only via the PROFIBUS and PROFINET fieldbuses or via a backplane bus, in this case for example the E-bus. The use of PROFIsafe via other fieldbuses is impermissible for reasons connected with patent law. This must be ensured through the use of the EL9930 segment end terminal.

The following Siemens AG patents are relevant according to the PROFIsafe profile:

- EP1267270-A2 Method for data transfer
- WO00/045562-A1 Method and device for determining the reliability of data carriers
- WO99/049373-A1 Shortened data message of an automation system
- EP1686732 Method and system for transmitting protocol data units
- EP1802019 Identification of errors in data transmission
- EP1921525-A1 Method for operation of a safety-related system
- EP13172092.2 Method and system for detection of errors

Depending on the architecture of the application, appropriate measures must therefore be taken. Details of the correct configuration of the overall system with regard to PROFIsafe can be found in the documentation for the EL6910 and EL9930.

Use of external safe sensors

Further requirements must be observed when using an external safe sensor.

⚠ CAUTION

Use of external safe sensors

When using an external safe sensor, the current version of the documentation must always be observed. Here you will find all the requirements for assembly, operation and repair, which must be met so that the sensor can be used correctly in a safety-relevant application.

9.2.1 Configuration in the engineering environment

In addition to the connection of TwinSAFE components, the additional connection of a safety laser scanner via PROFIsafe/PROFINet is considered in the context of this application example. All necessary configuration steps for the implementation are described in detail below.

An additional application is required to configure the safety laser scanner. This determines the range of functions of the safety laser scanner, the communication settings in PROFINET/PROFI-safe and the CRC checksum of the iParameters, which ultimately has to be additionally configured within TwinCAT.

9.2.1.1 Configuration of safety laser scanners

An additional application is required to configure the safety laser scanner. The current version can be obtained from the manufacturer's website.

The screenshot shows the TwinCAT configuration software interface. The navigation tree on the left includes sections like 'Übersicht', 'Konfiguration', 'Diagnose', and 'Service'. The main window displays the following information:

- Projekt:** Projektname, Applikationsname, Benutzername.
- Geräteinformation:** Name (microscan3), Typenschlüssel (MICS3-CBAZ55PZ1), Funktionsumfang der Konfiguration im Projekt (1.0), Funktionsumfang der Konfiguration im Gerät (1.0), Seriennummer (18040525/18040525), Funktionsumfang des Geräts (1.0).
- Verbindung:** Verbindungsstatus (Verbunden), Typ (1-1).
- Prüfsummen:**
 - Prüfsumme der Konfiguration im Projekt (Funktion 0x432C28AA und Netzwerk)
 - Prüfsumme der Konfiguration im Gerät (Funktion 0x432C28AA und Netzwerk)
 - Prüfsumme der Konfiguration im Projekt (Funktion 0x52332444)
 - Prüfsumme der Konfiguration im Gerät (Funktion 0x52332444)
- Systemstatus:** Applikationsstatus (Gestartet), Letzte Meldung (Keine Meldungen vorhanden), Konfigurationsdatum Gerät (30.05.2018 13:42:51), Synchronisation (Verifiziert).

On the right, there is a 'Messdaten' section with a circular scan diagram and an 'Anzeige' section showing a scanner unit and a display with a green checkmark and the label 'F_iPar_CRC'.

Here the necessary functions and parameters have to be configured according to the application, so that the CRC checksum can be calculated correctly (F_iPar_CRC in the illustration).

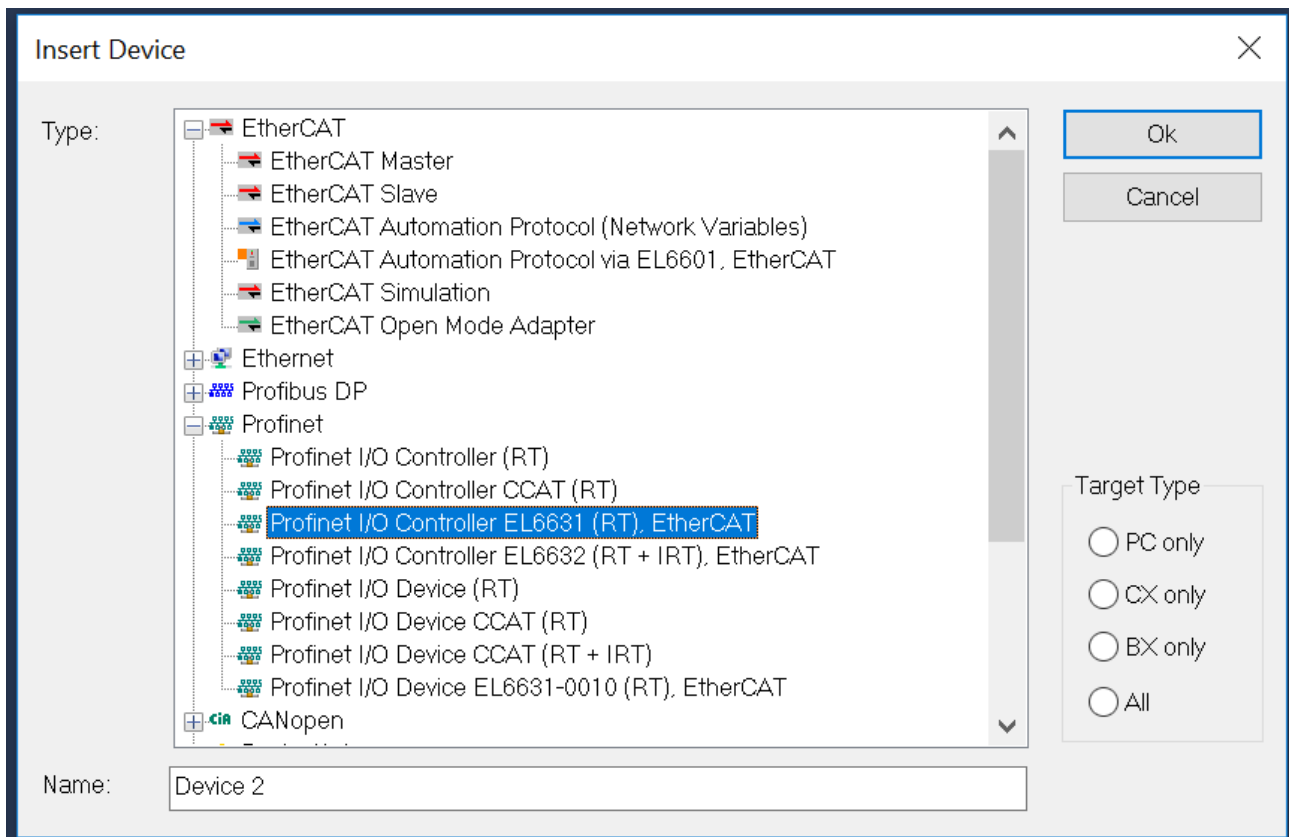
9.2.1.2 Configuration of TwinCAT I/O

The current GSDML file of the safety laser scanner must be inserted into the Profinet device directory under TwinCAT\3.1\Config\Io\Profinet prior to starting the TwinCAT configuration.

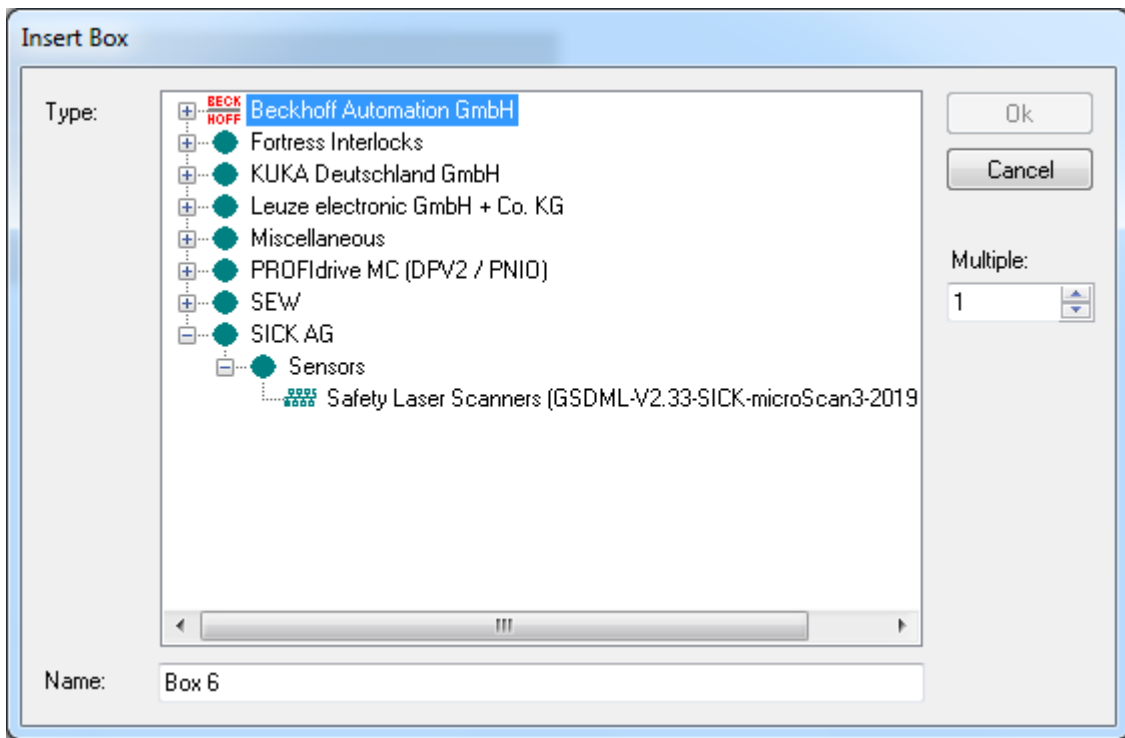
Subsequently, a new TwinCAT project is created and the EtherCAT segment is configured.

- Image
 - Image-Info
 - SyncUnits
 - Inputs
 - Outputs
 - InfoData
 - Term 1 (CX1100-0004)
 - InfoData
 - Term 2 (EL6910)
 - Term 3 (EL1904)
 - Term 4 (EL2904)
 - Term 5 (EL6631)
- Mappings

In addition, the configuration of the PROFINet segment is generated by adding a PROFINet I/O controller.



In the same way as the configuration of the EtherCAT segment, an automatic scan can also be initiated in the case of the PROFINet controller or the configuration can be generated manually. In this way, the Sick laser scanner can also be added manually.



The following information must be observed for the successful use of the Sick laser scanner via PROFIsafe.

⚠ CAUTION

Data type WORD!

An additional configuration may have to be done when using WORD data types within the process image.

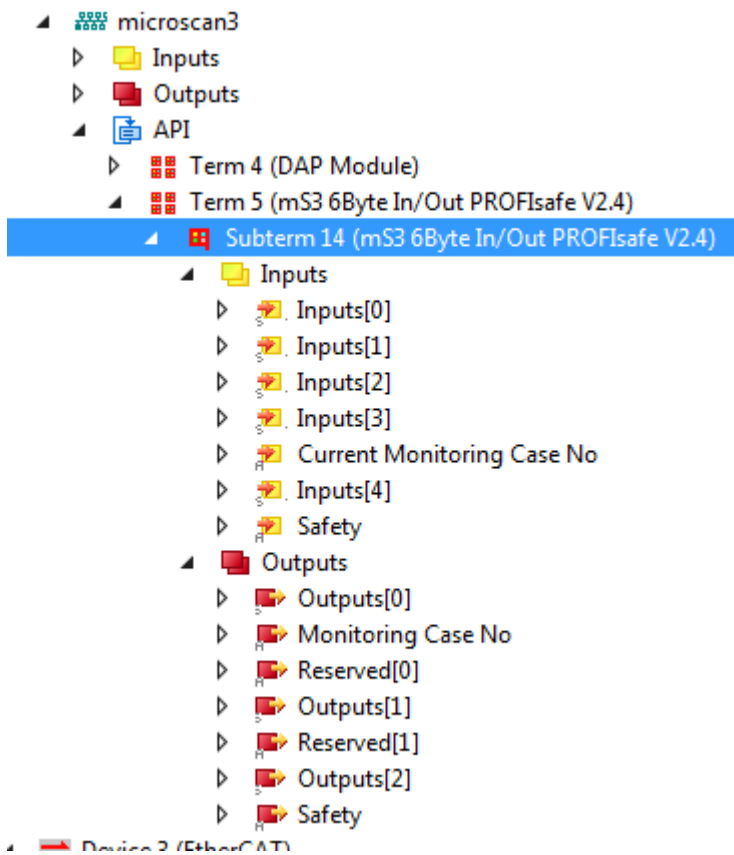
If no EL9930 is used within the configuration to limit the PROFIsafe segment, the swapping of the high and low byte portions must be configured as part of the I/O configuration of the PROFIsafe device for the signals with WORD data type contained in the process image. This is done by checking the *Swap LOBYTE and HIBYTE* checkbox directly on the data values (on the *Flags* tab).

⚠ CAUTION

iParameter

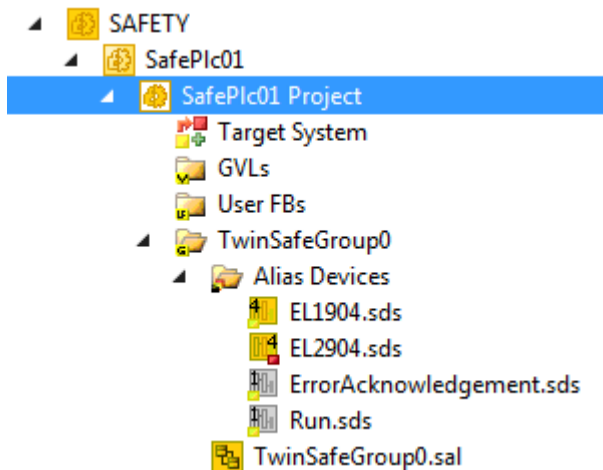
The identical iParameters as on the *Alias Device* must be configured on the PROFIsafe I/O device so that communication can start correctly.

You can then continue with the configuration of the safety project. At this point, the following initial situation is assumed.

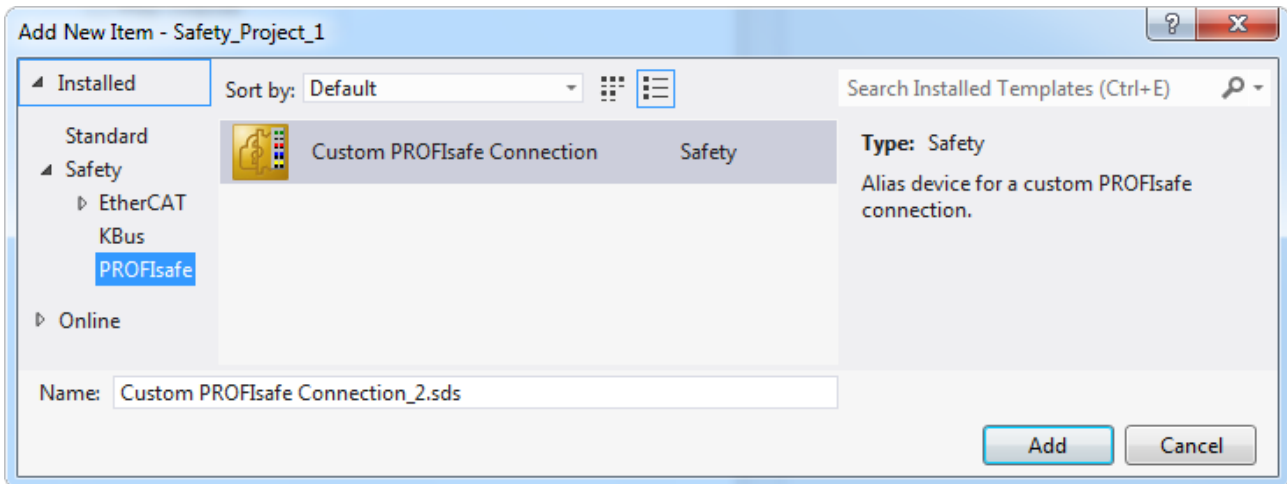


9.2.1.3 Configuration of TwinCAT safety project connections

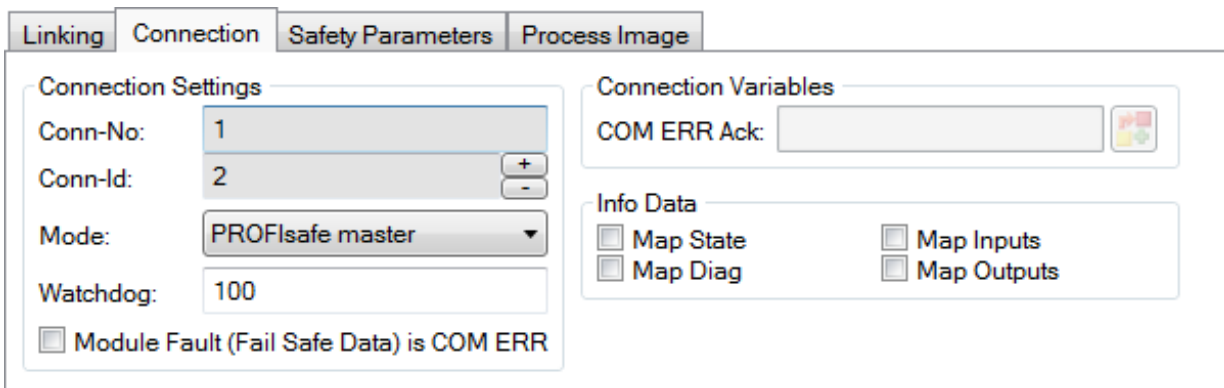
Before configuring the PROFIsafe connection, a safety project is created first and the required alias devices for the available EtherCAT components are imported. In addition, the target system is mapped to the EL6910 of the EtherCAT segment (via the *Target System* node).



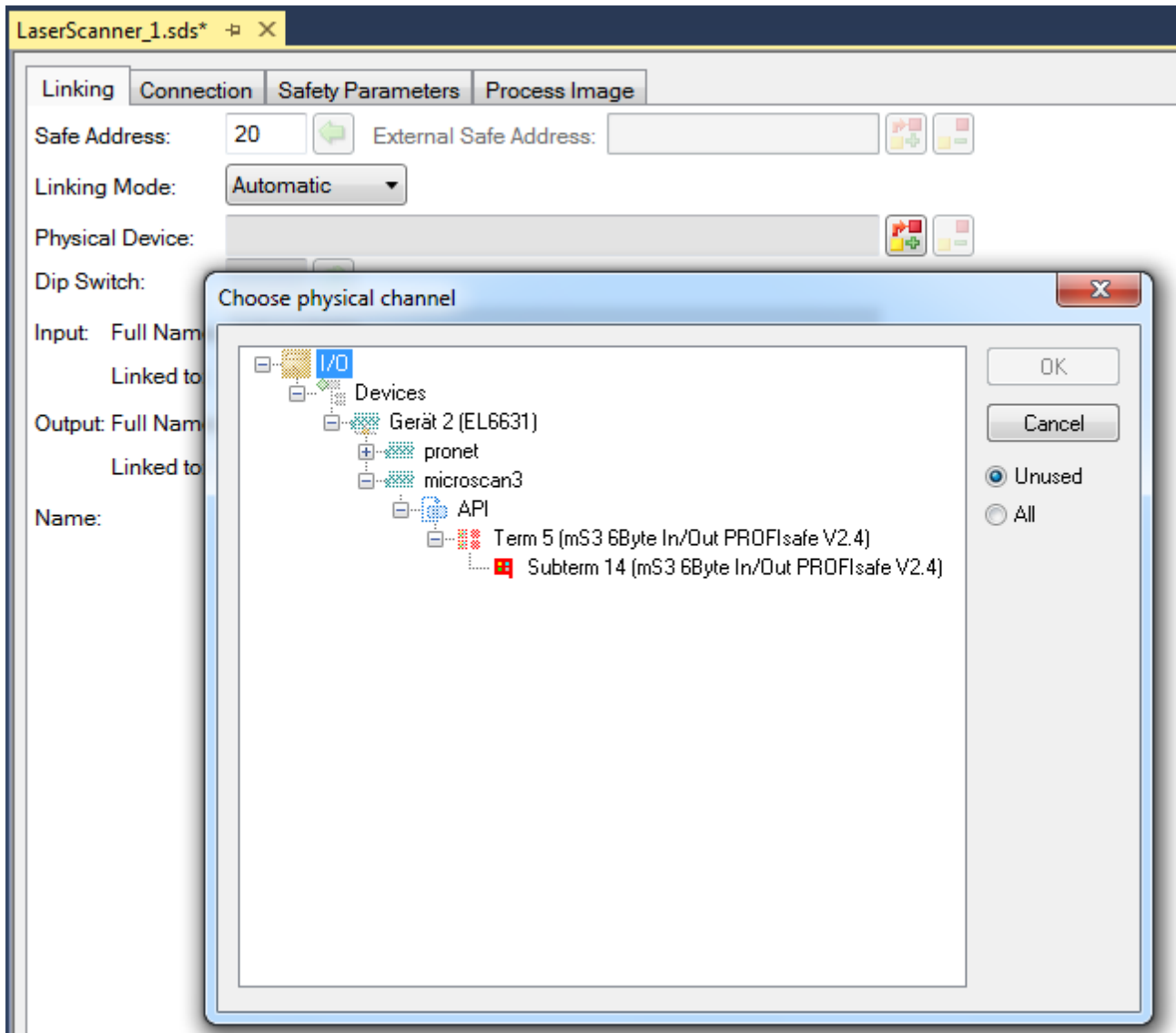
You can then continue with the configuration of the PROFIsafe connection to the safety laser scanner. This connection is implemented as usual via an *Alias Device*. A *Custom PROFIsafe Connection* can be created via the context menu of the node *Alias Devices* selecting *Add* and *New* item....



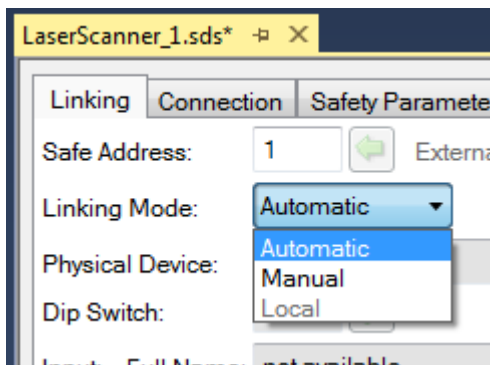
After opening the Alias Device, *PROFIsafe Master* must first be selected as the mode of the connection on the *Connection* tab.



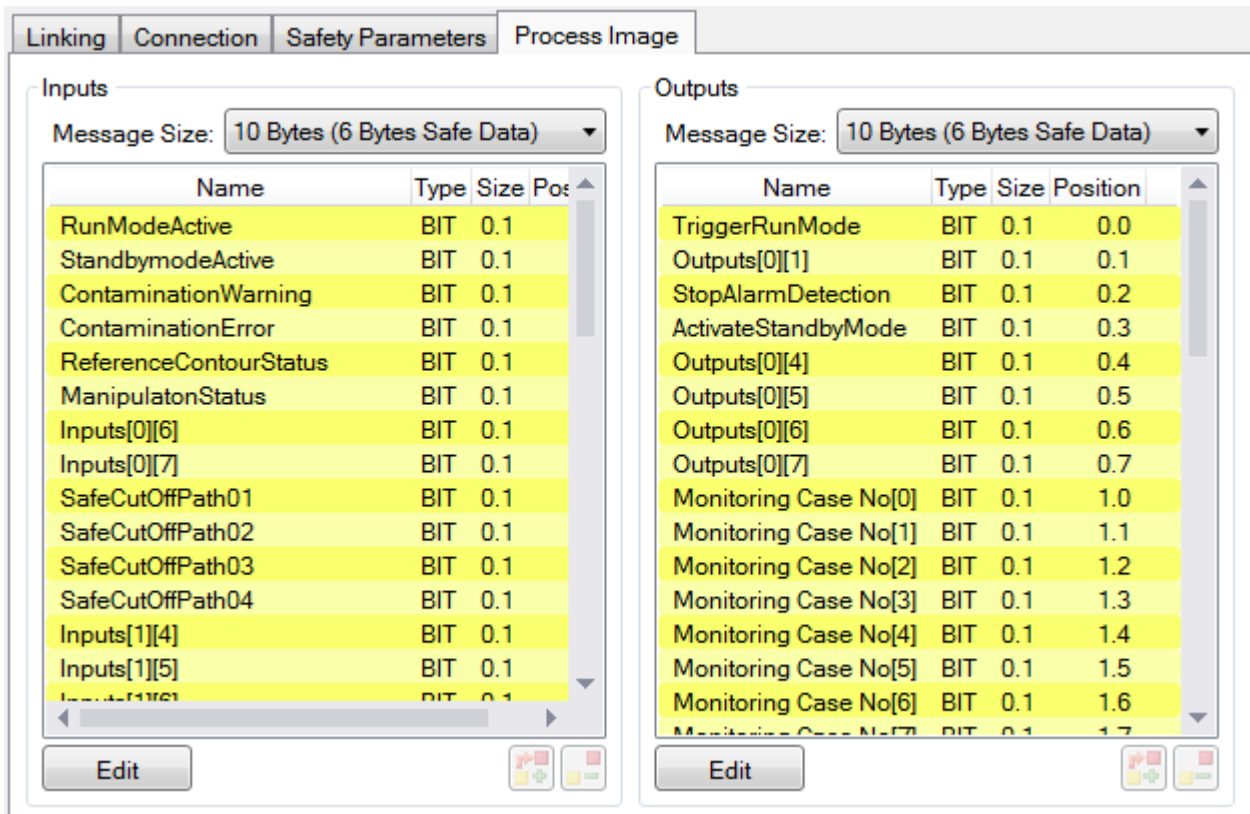
On the *Linking* tab, the Linking mode must be set to *Automatic* so that the Sick safety laser scanner considered here can be selected via the *Map to Physical Device* button.



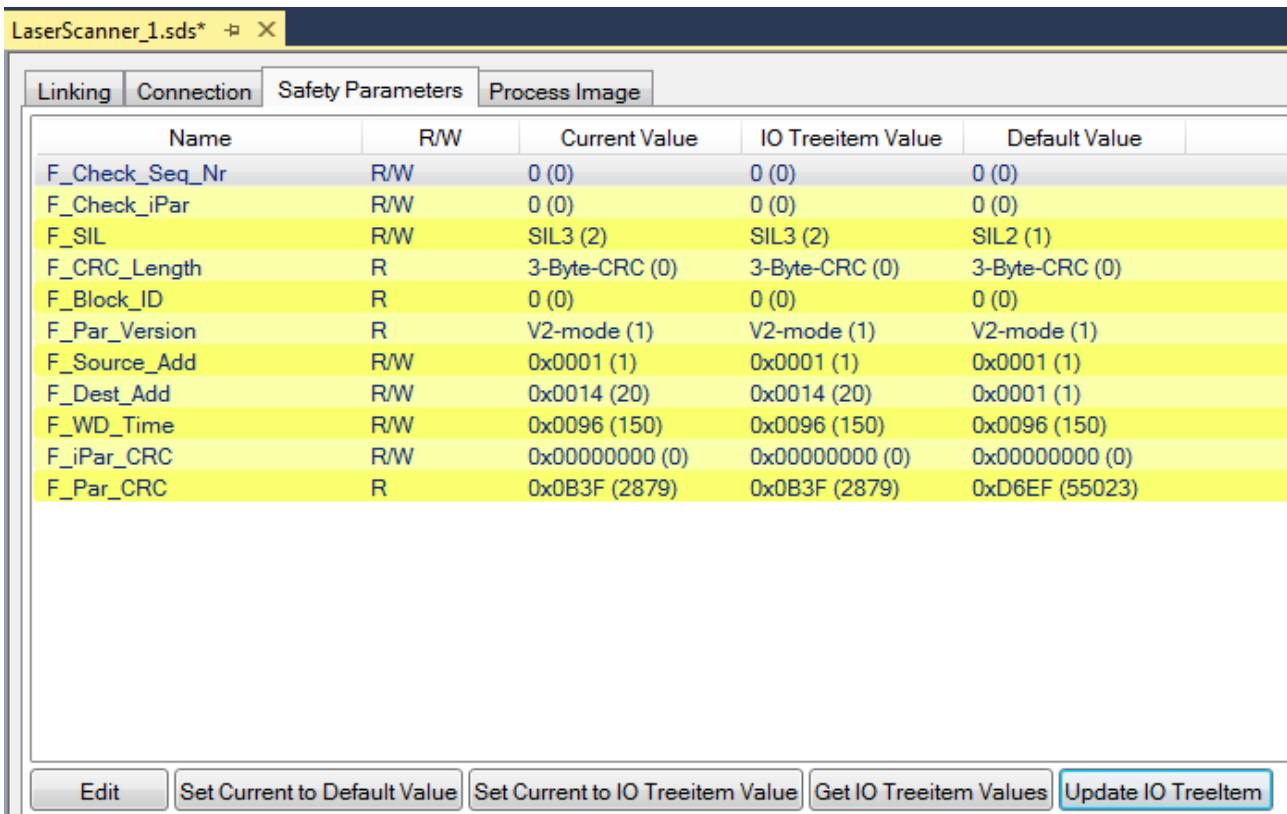
In addition to mapping to the physical device, the safe address of the safety laser scanner must also be entered on the *Linking* tab (20 in this example).



If all settings have been made correctly, the safe process image of the safety laser scanner can be viewed on the *Process Image* tab. The names can be adapted via the Edit button. The assignment of the interface as well as the description of the individual signals must be taken from the manufacturer's latest documentation.



The *Safety Parameters* tab provides the parameters for the PROFI-safe master connection.



All parameters for the PROFI-safe connection must be set correctly here. These include the two addresses *F_Source_Add* (target system) and *F_Dest_Add* (safe address of PROFI-safe device). In addition, the CRC of the *iParameters* must be configured. This can be taken from the additional application for configuring the safety laser scanner (see section *Encoder Configuration*).

In the case of a PROFIsafe device, the parameters must be set both within the Alias Device and directly for the device in the I/O configuration. The reading of the data from the I/O device and the transfer to the I/O device can be initiated via the corresponding buttons on the *Safety Parameters* tab. Both data must match for a PROFIsafe connection to be successfully established.

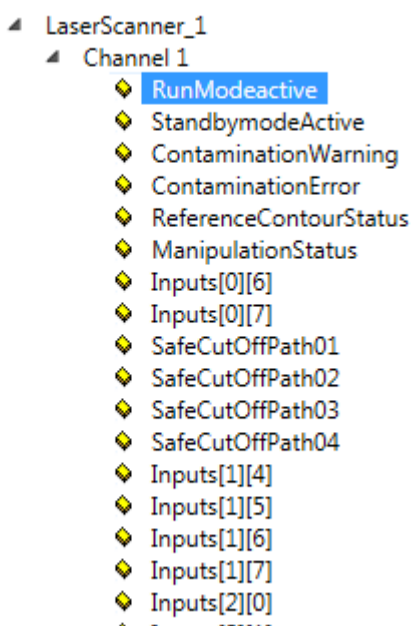
Parameter	Description
F_Check_Seq_Nr	Setting (0/1) to indicate whether the sequence number of the connection should be checked.
F_Check_iPar	Setting (0/1) to indicate whether the parameterization should take place via an iPar server.
F_SIL	Selecting the required SIL level (SIL1, SIL2, SIL3, NoSIL)
F_CRC_Length	Display of the CRC length
F_Block_ID	always 0
F_Par_Version	PROFIsafe version used (typically V2 mode)
F_Source_Add	Setting the PROFIsafe source address
F_Dest_Add	Setting the PROFIsafe destination address
F_WD_Time	Setting the watchdog time
F_iPar_CRC	i-parameter(s) for the PROFIsafe slave
F_Par_CRC	Calculated CRC across all parameters

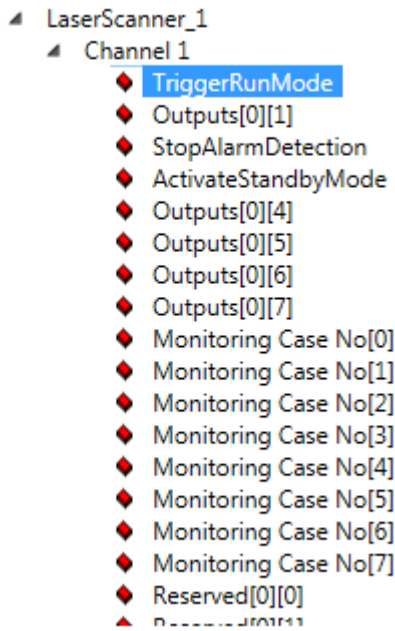
After completion of the configuration of the parameters, they must be transferred to the I/O configuration by clicking the button *Update IO TreeItem* final.

After completion of the configuration of the connections, you can continue with the implementation of the actual safety function.

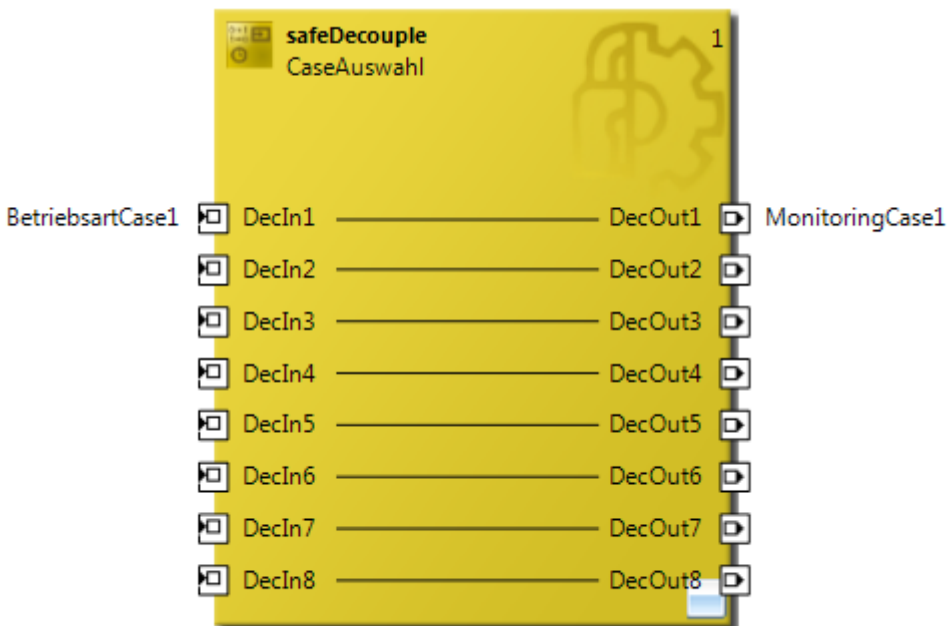
9.2.1.4 Implementing a TwinCAT safety project

The safe process image received via PROFIsafe is used within the scope of the safety function for area monitoring by means of a safety laser scanner considered in this example. The inputs that absolutely must be evaluated as well as the outputs to be switched on arise from the configuration of the safety laser scanner.

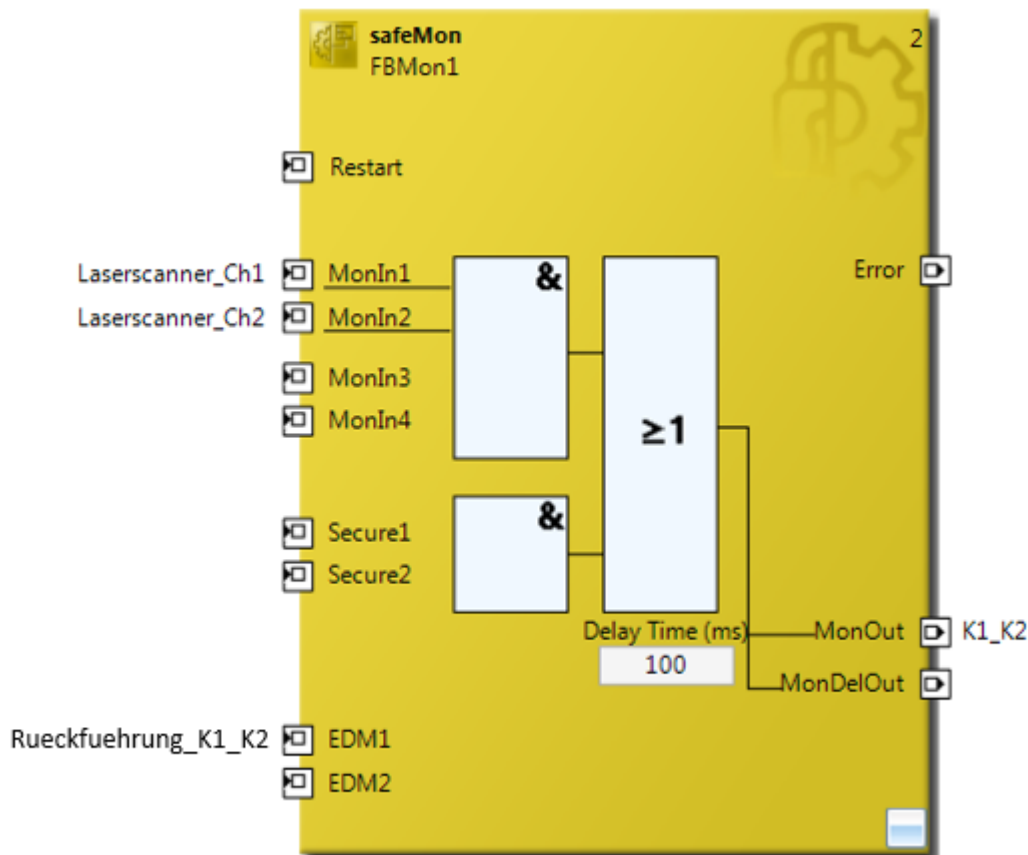




In this example, the monitoring case 1 is switched on without any further condition by means of the *safeDecoupler* function block.



The safety laser scanner monitors the hazard area parameterized in the device and sends the result of the monitoring in the signals switch-off paths 01 and 02. These two signals are evaluated by means of the *safeMon* function block. The switch-off paths are logic 1 if the hazard area is free and monitored in a safety-oriented manner.



As the illustration shows, with logic 1 at the inputs *MonIn1* and *MonIn2* and *EDM1*, the two contactors *K1* and *K2*, which execute the safety function, are switched via the output *MonOut* of the function block *safeMon*. The feedback from the contactors is used as the *EDM1* input of the function block *safeMon*.

Any necessary restart lock can be realized via the reset input of the function block *safeMon*.

9.2.2 Parameters of the safe input and output terminal

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

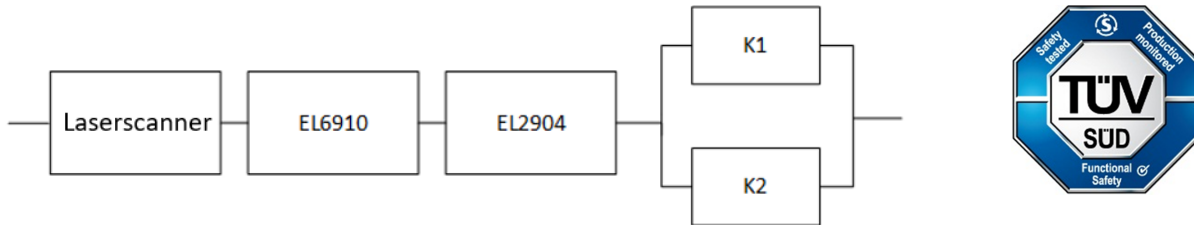
EL1904

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

9.2.3 Block formation and safety loops

9.2.3.1 Safety function 1

Safety function 1 considers the safety loop from the safety laser scanner to the contactors K1/K2 for the application example described so far.



9.2.4 Calculation of safety function 1

9.2.4.1 PFHD / MTTFD / B10D – values

Component	Value
Laser scanner ¹⁾ – PFH _D , SIL, Cat, PL	8E-08, SIL 2, Cat. 3, PL d
EL2904 – PFH _D	1.25E-09
EL6910 – PFH _D	1.79E-09
K1 – B10 _D	1,300,000
K2 – B10 _D	1,300,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10 (6x per hour)
Lifetime (T1)	20 years = 175200 hours

¹⁾ Please note the information provided in the current user documentation

9.2.4.2 Diagnostic Coverage DC

Component	Value
Laser scanner with testing (by scanner) ¹⁾	DC _{avg} =90%
K1/K2 with EDM monitoring with testing of the individual channels	DC _{avg} =99%

¹⁾ Please note the information provided in the current user documentation

9.2.4.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN ISO 13849-1. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{10} = 22.080$$

$$MTTF_D = \frac{1.300.000}{0,1 * 22.080} = 588,7y = 5.157.012h$$

and the assumption that K1 and K2 are each single-channel:

K1/K2: Actuation 10/hour and direct read back

$$PFH = \frac{1 - 0,99}{588,7y * 8760} = 1,94E - 09$$

The following assumptions must now be made:

Relays K1 and K2 are both connected to the safety function. The non-functioning of a relay does not lead to a dangerous situation, but it is discovered by the feedback. Furthermore, the B10_D values for K1 and K2 are identical.

There is a coupling coefficient between the components that are connected via two channels. Examples are temperature, EMC, voltage peaks or signals between these components. This is assumed to be the worst-case estimation, where β = 10%. EN 62061 contains tables (Table F.1: Criteria for determining the CCF, and Table F.2: Estimation of the CCF factor(β)), which can be used to determine the β factor precisely. For the output subsystem, an estimated value of 2% can be achieved if the table for calculating the β factor is modified accordingly. In the following calculation, the worst case is assumed with 10%.

Further, it is assumed that all usual measures have been taken to prevent both channels failing unsafely at the same time due to an error (e.g. overcurrent through relay contacts, overtemperature in the control cabinet).

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = PFH_{(Scanner)} + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Since the portions $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$PFH_{ges} = 8E - 08 + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 09 + 1,94E - 09}{2} = 8,32E - 08$$

The MTTF_D value according to EN 13849 for safety function 1 is calculated with:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

to:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

with:

If only PFH_D values exist for scanners, EL2904 and EL6910, the following estimation applies:

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(Scanner)} = \frac{(1 - DC_{(Scanner)})}{PFH_{(Scanner)}} = \frac{(1 - 0,90)}{8E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = 142y$$

In accordance with the limitation of the MTTFD to 100 years for components with a category 3 structure (for category 4 the limit is 2500 years) introduced in EN ISO 13849-1, the value is limited to 100 years for the further processing of the MTTFD of the scanner.

$$MTTF_{D(Scanner)} = 100y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{100y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{588y}} = 69,6y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Scanner)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}$$

$$DC_{avg} = \frac{\frac{90\%}{100} + \frac{99\%}{637} + \frac{99\%}{913} + \frac{99\%}{588} + \frac{99\%}{588}}{\frac{1}{100} + \frac{1}{637} + \frac{1}{913} + \frac{1}{588} + \frac{1}{588}} = 93,4\%$$

⚠ CAUTION

Implement a restart lock in the machine!
 The restart lock is NOT part of the safety chain and must be implemented in the machine!

NOTE

Category
 This structure is possible up to category 3 at the most through the use of the type 3 (category 3) laser scanner.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF_D ≤ 100 years

DC	
Name	Area
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage
 For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

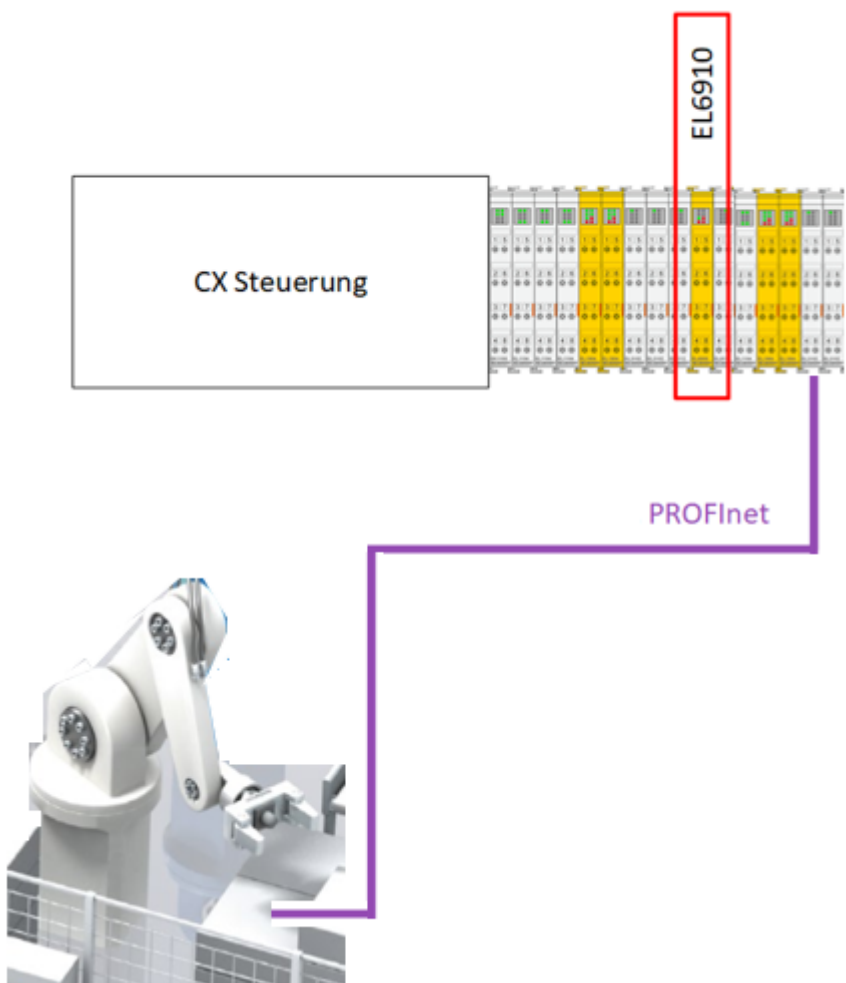
Category	B	1	2	2	3	3	4
DC / MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.3 Safe control of an ABB robot via PROFI-safe (category 3, PL d)

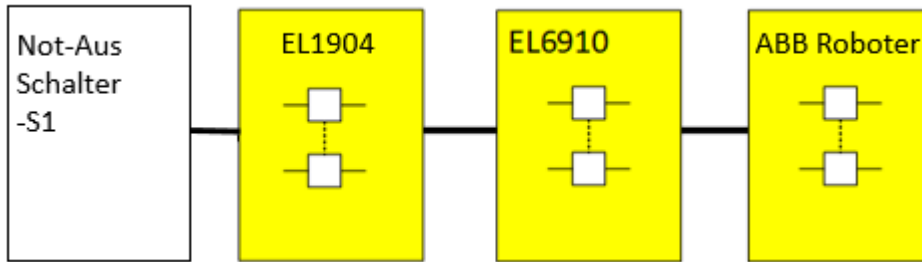
An ABB robot is connected to a TwinSAFE controller as a PROFI-safe device. The ABB robot with the *SafeMove* functionality is certified for applications up to Performance Level d. The safety-relevant data are transmitted via PROFINet with the help of PROFI-safe. The emergency stop is transmitted to the robot from the EL6910 as PROFI-safe master via the safety-relevant protocol PROFI-safe. The robot is configured to perform a category-0 stop. The safe state is signaled back to the EL6910 via the PROFI-safe connection, where it is further processed with the available pre-certified function blocks.

The example considers the emergency stop safety function. The emergency stop switch is wired to an EL1904 in a two-channel configuration with two normally closed contacts. The testing of the signals is activated. The input signals are monitored for discrepancy. The entire evaluation is carried out in the safety-related logic EL6910 at the safety level SIL 3 / PL e.

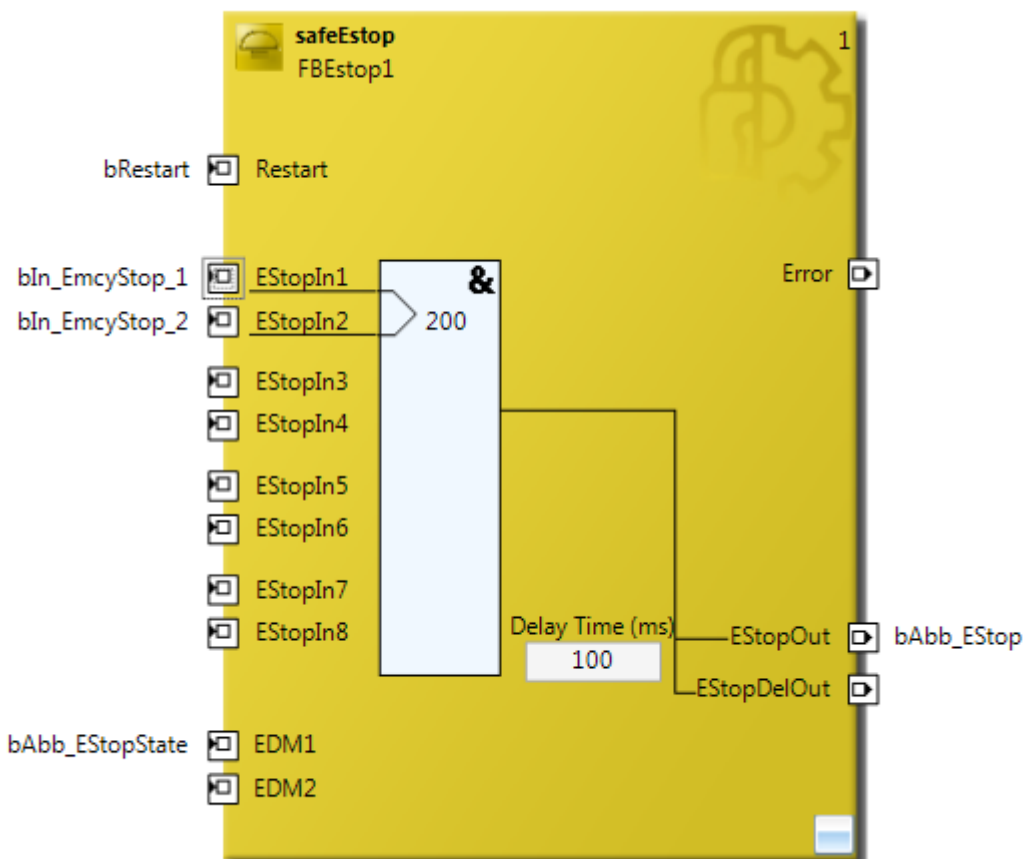
Structure



Structure diagram configuration



Logic



Correct configuration of the overall system

The following restrictions apply when transmitting PROFIsafe within EtherCAT.

PROFIsafe telegram only via E-bus and PROFINET/PROFIBUS

i On account of the PROFIsafe policy, the use of PROFIsafe is permitted only via the PROFIBUS and PROFINET fieldbuses or via a backplane bus, in this case for example the E-bus. The use of PROFIsafe via other fieldbuses is impermissible for reasons connected with patent law. This must be ensured through the use of the EL9930 segment end terminal.

The following Siemens AG patents are relevant according to the PROFIsafe profile:

- EP1267270-A2 Method for data transfer
- WO00/045562-A1 Method and device for determining the reliability of data carriers
- WO99/049373-A1 Shortened data message of an automation system
- EP1686732 Method and system for transmitting protocol data units
- EP1802019 Identification of errors in data transmission
- EP1921525-A1 Method for operation of a safety-related system
- EP13172092.2 Method and system for detection of errors

Depending on the architecture of the application, appropriate measures must therefore be taken. Details of the correct configuration of the overall system with regard to PROFI-safe can be found in the documentation for the EL6910 and EL9930.

Use of external PROFI-safe robots

Further requirements must be observed when using an external PROFI-safe robot.

CAUTION

Use of external PROFI-safe robots

When using an external PROFI-safe robot, the current version of the documentation must always be observed. Here you will find all the requirements for assembly, operation and repair, which must be met so that the robot can be used correctly in a safety-relevant application.

9.3.1 FMEA

Use of external PROFI-safe robots

Further requirements with regard to FMEA must also be observed when using an external PROFI-safe robot.

CAUTION

Use of external PROFI-safe robots

When using an external PROFI-safe robot, the current version of the documentation must always be observed. Here you will find all the requirements for assembly, operation and repair, which must be met so that the robot can be used correctly in a safety-relevant application.

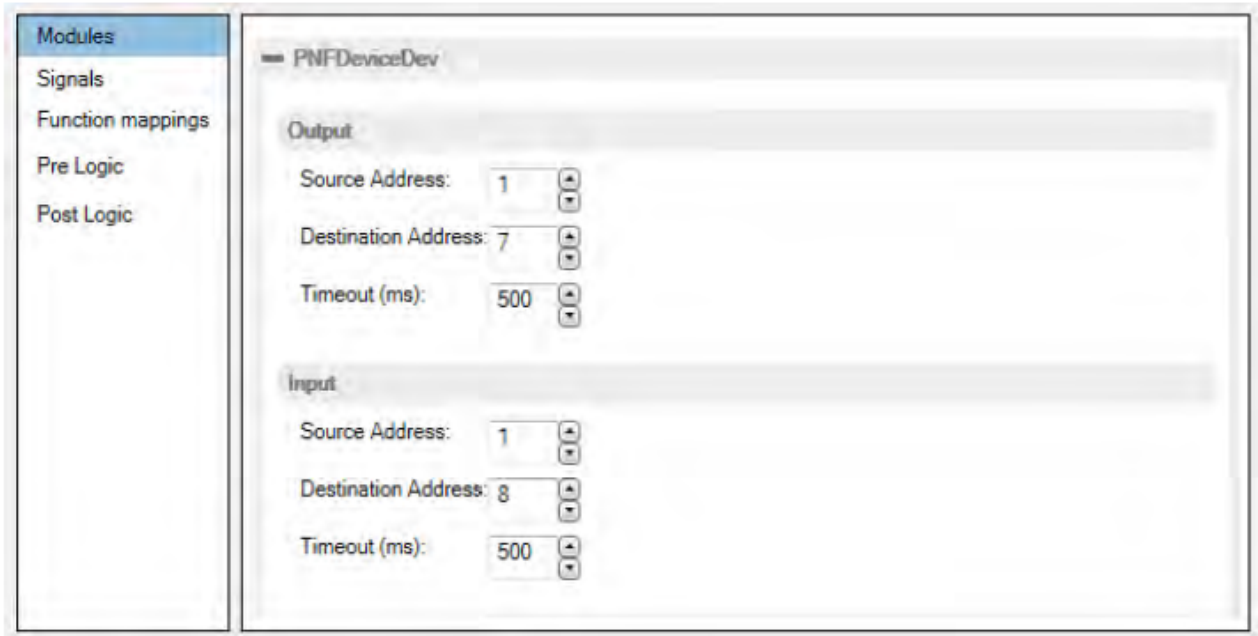
9.3.2 Configuration in the engineering environment

In addition to the connection of TwinSAFE components, the additional connection of an encoder via PROFI-safe/PROFINet is considered in the context of this application example. All necessary configuration steps for the implementation are described in detail below.

For the configuration of the safety-relevant parameters of the encoder, an additional application is required to perform the parameterization of the device and to determine the CRC checksum of the iParameters, which ultimately has to be additionally configured within TwinCAT.

9.3.2.1 Robot configuration

An additional application is required to configure the robot. The current version can be obtained from the manufacturer's website.



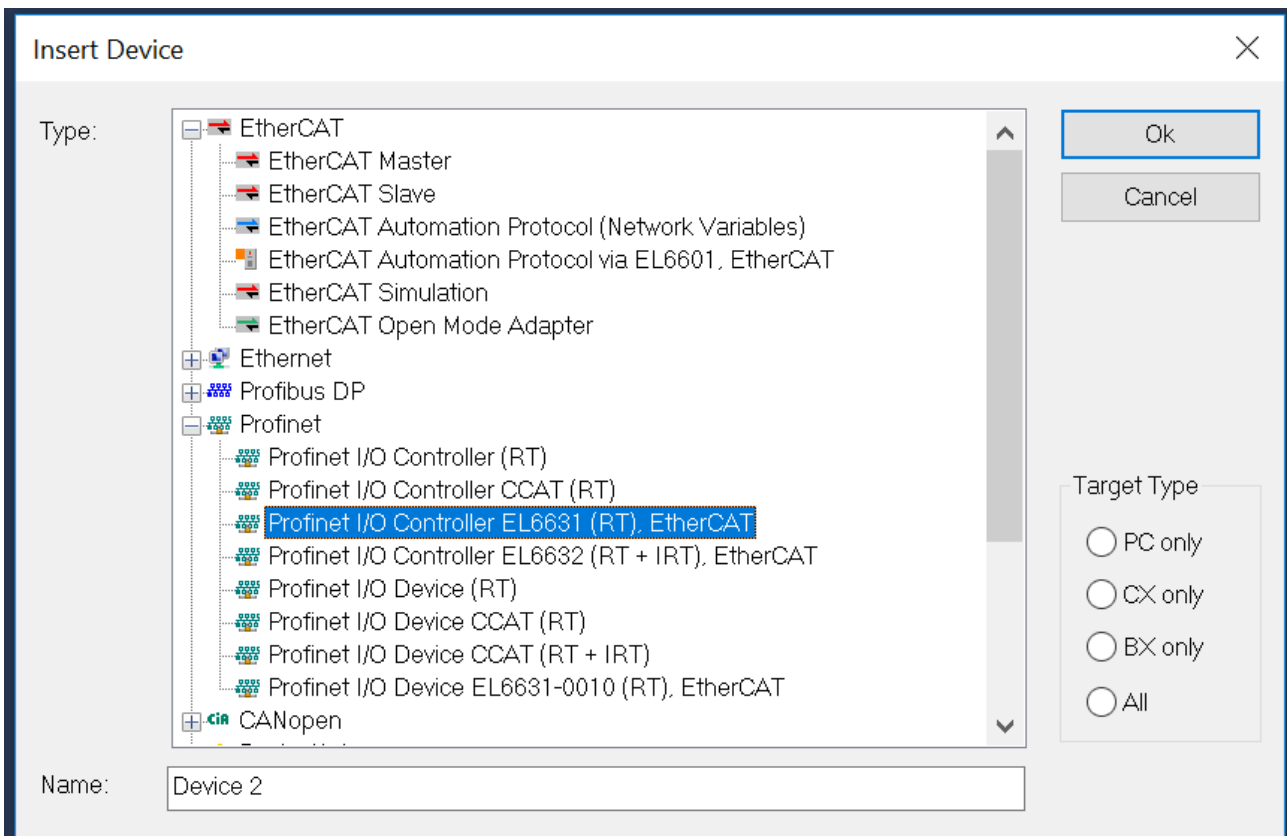
Here the necessary functions and parameters have to be configured according to the application, so that, for example, the CRC checksum can be calculated correctly. Security-oriented communication is only possible if the settings of the safe process images match.

9.3.2.2 Configuration of TwinCAT I/O

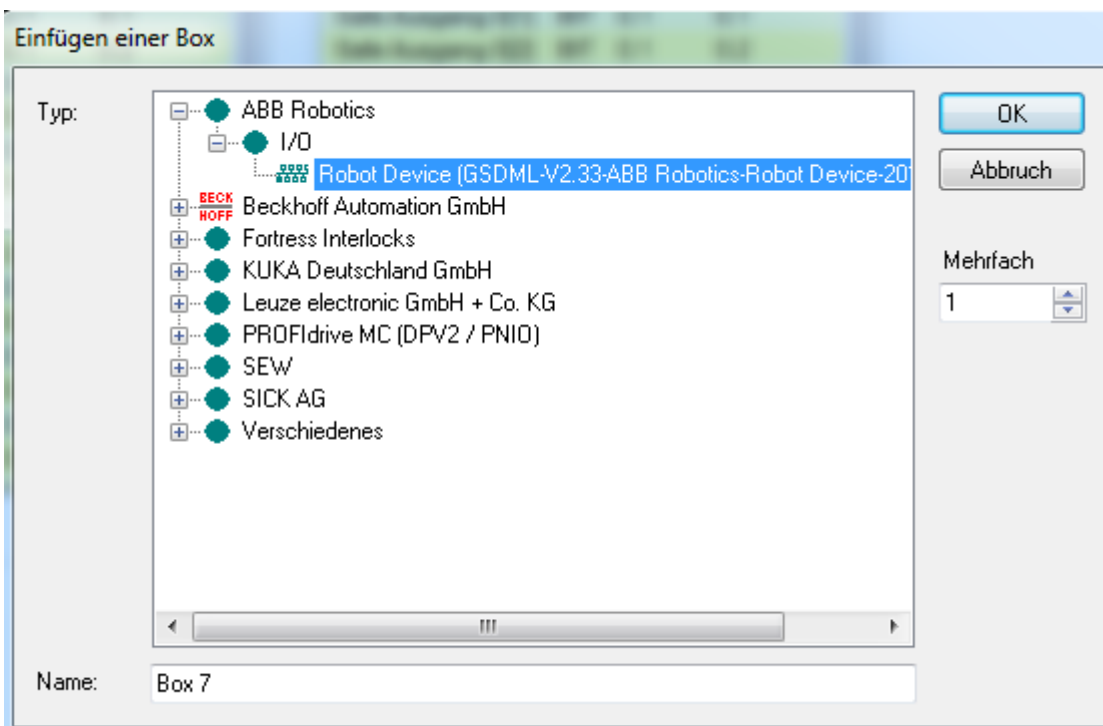
First, a new TwinCAT project is created and the EtherCAT segment is configured.

- Device 1 (EtherCAT)
 - Image
 - Image-Info
 - SyncUnits
 - Inputs
 - Outputs
 - InfoData
 - Term 1 (CX1100-0004)
 - InfoData
 - Term 2 (EL6910)
 - Term 3 (EL1904)
 - Term 4 (EL2904)
 - Term 5 (EL6631)
 - Mappings

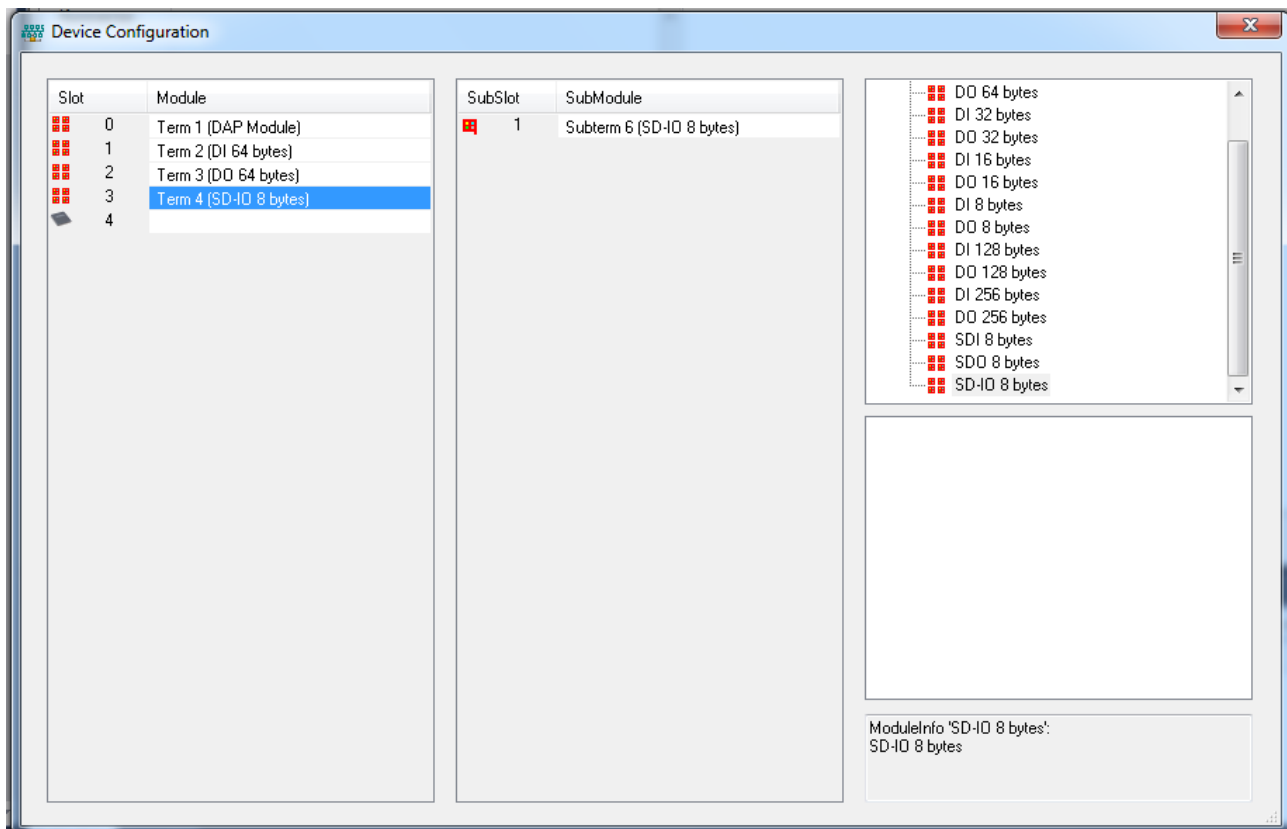
In addition, the configuration of the PROFINet segment is generated by adding a PROFINet I/O controller.



In the same way as the configuration of the EtherCAT segment, an automatic scan can also be initiated in the case of the PROFINet controller or the configuration can be generated manually. In this way, the ABB robot can also be added manually.



The device configuration must be extended by the PROFIsafe safety module.



The following information must be observed for the successful use of the ABB robot via PROFIsafe.

⚠ CAUTION

Data type WORD!

An additional configuration may have to be done when using WORD data types within the process image.

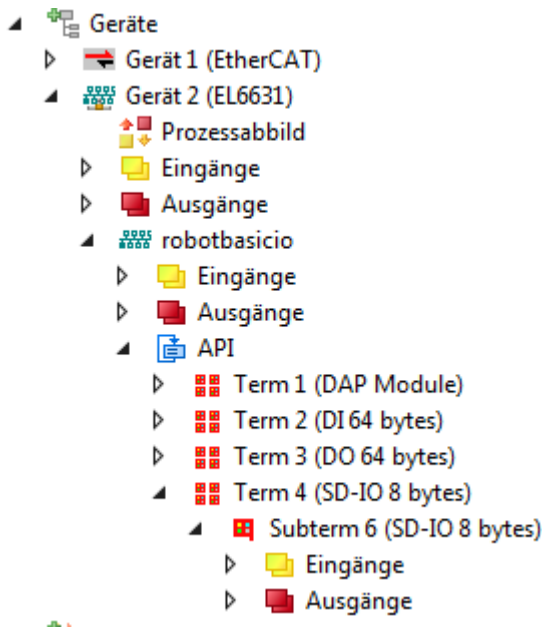
If no EL9930 is used within the configuration to limit the PROFIsafe segment, the swapping of the high and low byte portions must be configured as part of the I/O configuration of the PROFIsafe device for the signals with WORD data type contained in the process image. This is done by checking the *Swap LOBYTE* and *HIBYTE* checkbox directly on the data values (on the *Flags* tab).

⚠ CAUTION

iParameters

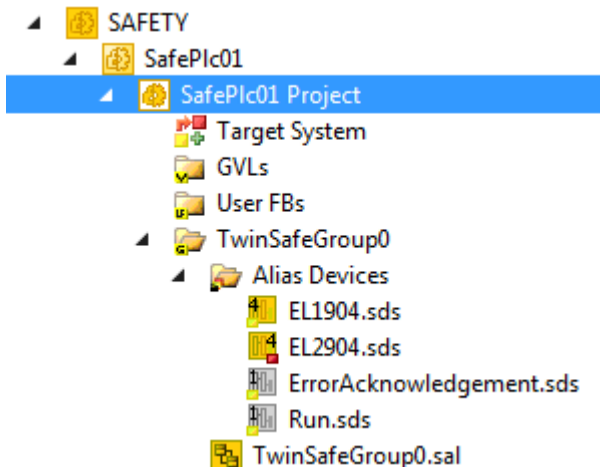
The identical iParameters as on the *Alias Device* must be configured on the PROFIsafe I/O device so that communication can start correctly.

You can then continue with the configuration of the safety project. At this point, the following initial situation is assumed.

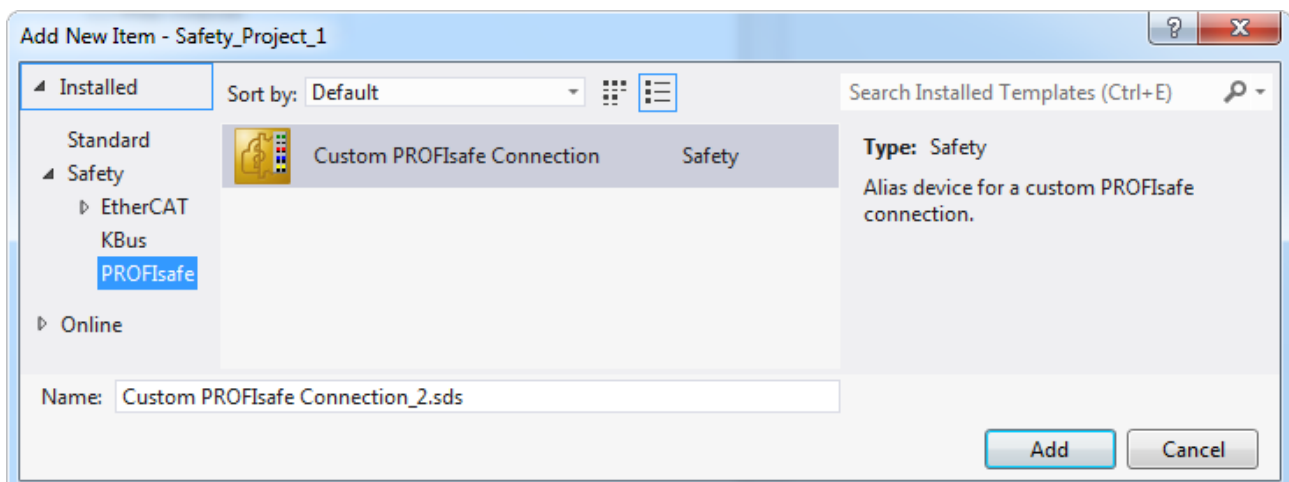


9.3.2.3 Configuration of TwinCAT safety project connections

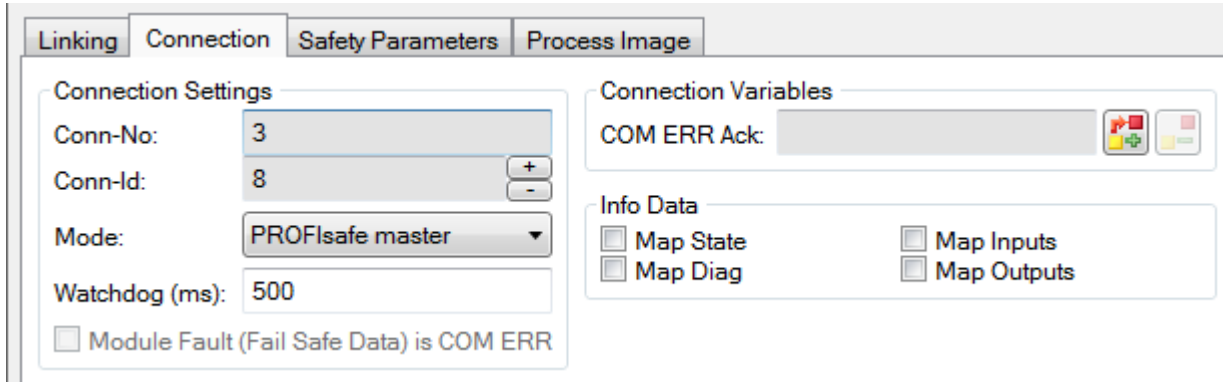
Before configuring the PROFIsafe connection, a safety project is created first and the required alias devices for the available EtherCAT components are imported. In addition, the target system is mapped to the EL6910 of the EtherCAT segment (via the *Target System* node).



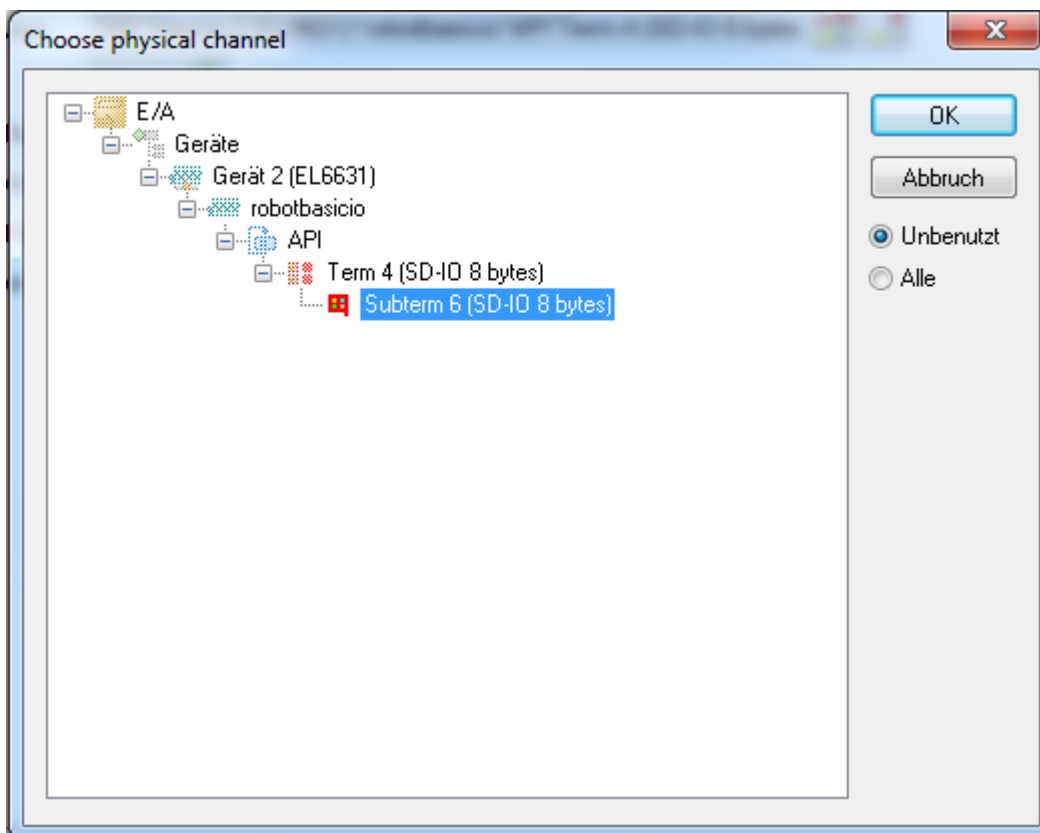
You can then continue with the configuration of the PROFIsafe connection to the ABB robot. This connection is implemented as usual via an *Alias Device*. A *Custom PROFIsafe Connection* can be created via the context menu of the node *Alias Devices* selecting *Add* and *New* item....



After opening the Alias Device, *PROFIsafe Master* must first be selected as the mode of the connection and the watchdog for the communication on the *Connection* tab.



On the *Linking* tab, the linking mode must be set to *Automatic* so that the ABB robot considered here can be selected via the *Map to Physical Device* button.



In addition to mapping to the physical device, the safe address of the encoder must also be entered on the *Linking* tab (21 in this example).

Linking | **Connection** | Safety Parameters | Process Image

Safe Address: External Safe Address:

Linking Mode: **Automatic**

Physical Device: TIID^Device 2 (EL6631)^robotbasicio^API^Term 4 (SD-IO 8 bytes)

Dip Switch: n.a.

Input: Full Name: TIID^Device 1 (EtherCAT)^Term 1 (EK1200)^Term 2 (EL6910)^Pi
 Linked to: Safe Ausgang 0, Safe Ausgang 1, Safe Ausgang 2, Safe Ausgang 3

Output: Full Name: TIID^Device 1 (EtherCAT)^Term 1 (EK1200)^Term 2 (EL6910)^Pi
 Linked to: Safe Eingang 0, Safe Eingang 1, Safe Eingang 2, Safe Eingang 3

Name:

If all settings have been made correctly, the safe process image of the ABB robot can be set on the *Process Image* tab and edited according to the setting from the robot's application tool.

Linking | Connection | **Safety Parameters** | Process Image

Inputs

Message Size: **12 Bytes (8 Bytes Safe Data)**

Name	Type	Size	Position
Robot_ES_Active	BIT	0.1	0.0
Safe Eingang 0[1]	BIT	0.1	0.1
Safe Eingang 0[2]	BIT	0.1	0.2
Safe Eingang 0[3]	BIT	0.1	0.3
Safe Eingang 0[4]	BIT	0.1	0.4
Safe Eingang 0[5]	BIT	0.1	0.5
Safe Eingang 0[6]	BIT	0.1	0.6
Safe Eingang 0[7]	BIT	0.1	0.7
Safe Eingang 1[0]	BIT	0.1	1.0
Safe Eingang 1[1]	BIT	0.1	1.1
Safe Eingang 1[2]	BIT	0.1	1.2
Safe Eingang 1[3]	BIT	0.1	1.3
Safe Eingang 1[4]	BIT	0.1	1.4
Safe Eingang 1[5]	BIT	0.1	1.5
Safe Eingang 1[6]	BIT	0.1	1.6
Safe Eingang 1[7]	BIT	0.1	1.7

Outputs

Message Size: **12 Bytes (8 Bytes Safe Data)**

Name	Type	Size	Position
Robot_ES_Req	BIT	0.1	0.0
Safe Ausgang 0[1]	BIT	0.1	0.1
Safe Ausgang 0[2]	BIT	0.1	0.2
Safe Ausgang 0[3]	BIT	0.1	0.3
Safe Ausgang 0[4]	BIT	0.1	0.4
Safe Ausgang 0[5]	BIT	0.1	0.5
Safe Ausgang 0[6]	BIT	0.1	0.6
Safe Ausgang 0[7]	BIT	0.1	0.7
Safe Ausgang 1[0]	BIT	0.1	1.0
Safe Ausgang 1[1]	BIT	0.1	1.1
Safe Ausgang 1[2]	BIT	0.1	1.2
Safe Ausgang 1[3]	BIT	0.1	1.3
Safe Ausgang 1[4]	BIT	0.1	1.4
Safe Ausgang 1[5]	BIT	0.1	1.5
Safe Ausgang 1[6]	BIT	0.1	1.6
Safe Ausgang 1[7]	BIT	0.1	1.7

The *Safety Parameters* tab provides the parameters for the PROFIsafe master connection. If necessary, the values must be adapted to the application with the help of the Edit button.

Linking Connection Safety Parameters Process Image					
Name	R/W	Current Value	IO Treeitem Value	Default Value	
F_Check_Seq_Nr	R/W	0 (0)	0 (0)	0 (0)	
F_Check_iPar	R/W	0 (0)	0 (0)	0 (0)	
F_SIL	R/W	SIL2 (1)	SIL2 (1)	SIL2 (1)	
F_CRC_Length	R	3-Byte-CRC (0)	3-Byte-CRC (0)	3-Byte-CRC (0)	
F_Block_ID	R	0 (0)	0 (0)	0 (0)	
F_Par_Version	R	V2-mode (1)	V2-mode (1)	V2-mode (1)	
F_Source_Add	R/W	0x0001 (1)	0x0001 (1)	0x0001 (1)	
F_Dest_Add	R/W	0x0015 (21)	0x0015 (21)	0x0001 (1)	
F_WD_Time	R/W	0x01F4 (500)	0x01F4 (500)	0x01F4 (500)	
F_iPar_CRC	R/W	0x00000000 (0)	0x00000000 (0)	0x00000000 (0)	
F_Par_CRC	R	0xC2A1 (49825)	0xC2A1 (49825)	0x9223 (37411)	

All parameters for the PROFIsafe connection must be set correctly here. These include the two addresses F_Source_Add (target system) and F_Dest_Add (safe address of PROFIsafe device). In addition, the CRC of the *iParameters* must be configured. This can be taken from the additional application for configuring the robot (see section *Robot Configuration*)

In the case of a PROFIsafe device, the parameters must be set both within the Alias Device and directly for the device in the I/O configuration. The reading of the data from the I/O device and the transfer to the I/O device can be initiated via the corresponding buttons on the *Safety Parameters* tab. Both data must match for a PROFIsafe connection to be successfully established.

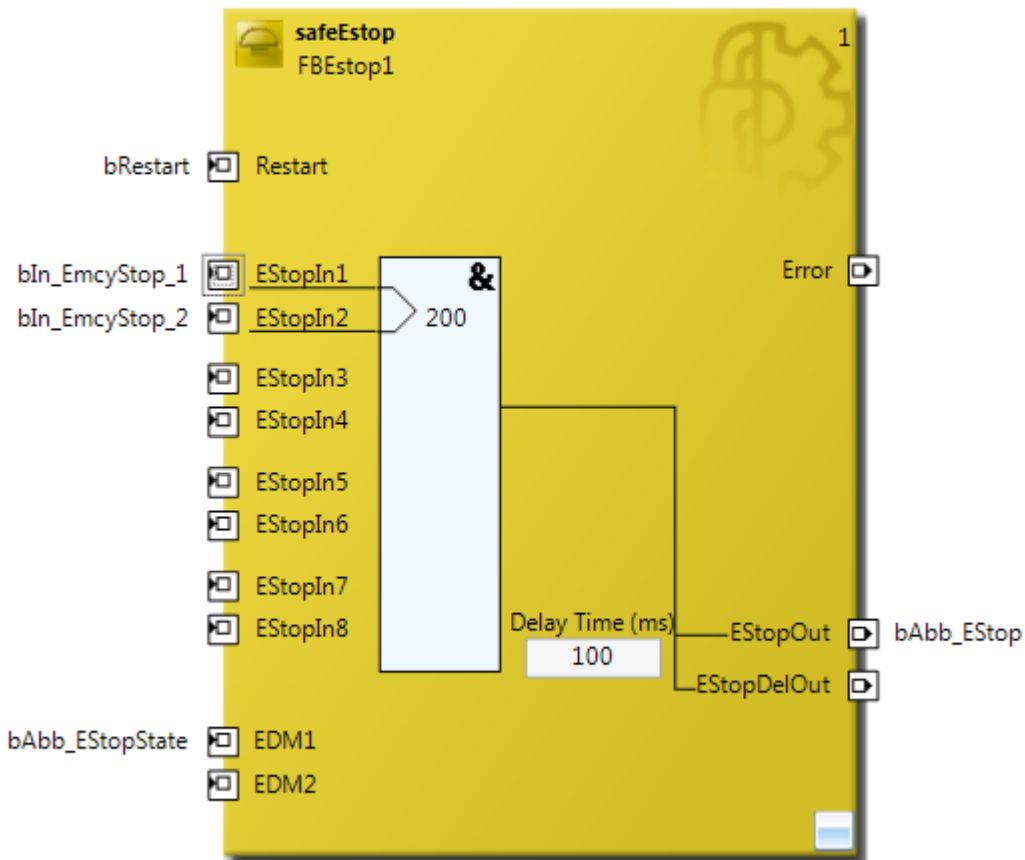
Parameter	Description
F_Check_Seq_Nr	Setting (0/1) to indicate whether the sequence number of the connection should be checked.
F_Check_iPar	Setting (0/1) to indicate whether the parameterization should take place via an iPar server.
F_SIL	Selecting the required SIL level (SIL1, SIL2, SIL3, NoSIL)
F_CRC_Length	Display of the CRC length
F_Block_ID	always 0
F_Par_Version	PROFIsafe version used (typically V2 mode)
F_Source_Add	Setting the PROFIsafe source address
F_Dest_Add	Setting the PROFIsafe destination address
F_WD_Time	Setting the watchdog time
F_iPar_CRC	i-parameter(s) for the PROFIsafe slave
F_Par_CRC	Calculated CRC across all parameters

After completion of the configuration of the parameters, they must be transferred to the I/O configuration by clicking the button *Update IO Treeitem* final.

After completion of the configuration of the connections, you can continue with the implementation of the actual safety function.

9.3.2.4 Implementing a TwinCAT safety project

Within the context of the safety function considered in this example, an emergency stop switch with 2 normally closed contacts is read in safely via an EL1904 in a 2-channel configuration. Testing of the inputs is activated. The inputs are evaluated via the safeEstop function block with discrepancy monitoring activated.



As the illustration shows, the signal for controlling the ABB robot via PROFIsafe is switched via the *EStopOut* output of the *safeEstop* function block. The feedback from the ABB robot is used as an *EDM* input of the *safeEstop* function block.

9.3.3 Parameters of the safe input terminal

EL1904

Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

9.3.4 Block formation and safety loops

9.3.4.1 Safety function 1

Safety function 1 considers the safety loop from the emergency stop switch S1 to the ABB robot for the application example described so far.



9.3.5 Calculation of safety function 1

9.3.5.1 PFHD / MTTFD / B10D – values

Component	Value
ABB robot, SafeMove function ¹⁾ – PFH _D , PL, MTTF _D , DC _{avg}	1.19E-07, PL d, 52y, medium
EL1904 – PFH _D	1.11E-09
EL6910 – PFH _D	1.79E-09
S1 – B10 _D	100,000
Days of operation (d _{op})	230
Hours of operation / day (h _{op})	16
Cycle time (minutes) (T _{cycle})	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

¹⁾ Please note the information provided in the current user documentation

9.3.5.2 Diagnostic Coverage DC

Component	Value
ABB robot, SAFEMove function ¹⁾	DC _{avg} = 90%
S1 with testing/plausibility	DC _{avg} = 99%

¹⁾ Please note the information provided in the current user documentation

9.3.5.3 Calculation of safety function 1

For clarity, the safety factor is calculated according to EN 62061 as well as EN ISO 13849-1. Calculation according to one standard is sufficient in practice.

Calculation of the PFH_D and MTTF_D values from the B10_D values:

From:

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

and:

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

produces for

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

Inserting the values, this produces:

S1:

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

and the assumption that S1 is single-channel:

S1: Actuation 1x per week and direct read back

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

It follows for the calculation of the PFH_D value for safety function 1

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6910)} + PFH_{(Roboter)}$$

$$PFH_{ges} = 2,5E - 11 + 1,11E - 9 + 1,79E - 9 + 1,19E - 7 = 1,22E - 7$$

The MTTF_D value according to EN 13849 for safety function 1 is calculated with:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^n \frac{1}{MTTF_{Dn}}$$

to:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(Roboter)}}$$

with:

If only PFH_D values are available for EL1904 and EL6910, the following estimation applies:

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

Hence:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637y$$

The value of the robot can be taken from the current user documentation:

$$MTTF_{D(Roboter)} = 52y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{637y} + \frac{1}{52y}} = 45,88y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(EL1904)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(Roboter)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(Roboter)}}$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{637y} + \frac{90\%}{52y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{637y} + \frac{1}{52y}} = 91\%$$

⚠ CAUTION

Implement a restart lock in the machine!

The restart lock is NOT part of the safety chain and must be implemented in the machine!

NOTE

Category

Due to the safety data of the robot used, this structure is possible up to Category 3 at the most.

MTTF _D	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF _D < 10 years
medium	10 years ≤ MTTF _D < 30 years
high	30 years ≤ MTTF _D ≤ 100 years

DC	
Name	Area
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE

Diagnostic coverage

For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC \ MTTF _D	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

10 Planning a safety project with TwinSAFE components

This chapter provides an overview of the general planning process for a safety project using TwinSAFE components.

⚠ CAUTION

Machinery Directive

This description applies only to machines as defined by the Machinery Directive.

⚠ CAUTION

Standards

The relevant standards must be available to the user. The following description cannot replace the standard. Typically, the current version of EN ISO 13849-1 and EN ISO 13849-2 or EN 62061 should be available as a minimum. Further useful information can be found in IFA report 2/2017.

NOTE

Type C standard

Before you start the following process, you should check whether a type C standard is available for your machine. If this is the case, please follow the steps and instructions given there. If no type C standard is available, you can use the process described below as a guide for the steps to be performed.

10.1 Identifying the risks and hazards

DIN EN ISO 12100 defines an *iterative process for risk minimization*, for eliminating hazards or for reducing the risk at machines. It describes the process of risk minimization in a three-step method. In the first step, the machine should be designed to be inherently safe. If this is not possible, technical protective measures can be taken to minimize the risk. In the last step, user information about the residual risk can be provided.

In the first step, the risks and hazards and thus the safety functions must be identified. Machine manufacturers require precise knowledge of the operation of their machine in order to identify risks and hazards. Referring to Annex B of EN ISO 12100:2010 is helpful for this purpose.

This risk and hazard analysis should be carried out by persons with knowledge in different areas (mechanics, electrics, hydraulics, software, maintenance, ...). All operating modes and conditions must be taken into account, including commissioning, maintenance/servicing, normal operation and decommissioning. The reasons for or against a particular decision should also be documented. Make sure that your arguments and justifications are understandable and conclusive.

In this context, it is particularly important to note that safety measures must not yet be taken into account when assessing the risk.

When all persons involved in the process agree with the result of the analysis, it should be signed by all involved.

10.2 Determining the PLr / SIL

For each safety function (SF) of the machine identified in the risk and hazard analysis, the machine manufacturer or user must determine the required Performance Level or SIL Level.

The SIL level is determined based on the description in Annex A of EN 62061

The performance level is determined based on the risk graph for determining the PLr, according to EN ISO 13849-1. Information on the risk graph can be found in Annex A of EN ISO 13849-1:2015.

10.3 Specification of the safety functions

For each safety function identified, it is necessary to specify how the risk should be reduced in accordance with the EN ISO 12100 *strategy for risk reduction*.

Risks and hazards whose residual risk is to be reduced by inherently safe design or user information must be specified, but are not part of this description.

The following explanations refer only to safety functions, the residual risk of which is to be reduced by technical protective measures.

For these safety functions, the *iterative design process for safety-related parts of the control system (SRP/CS)* is carried out in accordance with EN ISO 13849-1:2015.

10.4 Specification of the measures

The machine manufacturer should compile a detailed description of each identified safety function (SF) whose residual risk is to be reduced by means of technical protection measures. This description contains information about the hazard, the type of measures taken to reduce the hazard and the required Performance Level or SIL Level for this safety function.

For each SF, the description of the measures must include the category according to EN ISO 13849-1 and the components to be used, together with their safety parameters (MTTF_D, DC, CCF, SFF).

Information on operating states and characteristics is required. These include the operating modes, the cycle time, the response times or process safety time, the ambient conditions, the frequency of execution, the operating times, the behavior of the machine in the event of energy loss and more. More detailed information on this can be found in chapter 5.2 of EN 62061 and chapter 5 of EN ISO 13849-1:2015.

The machine manufacturer must specify and document the description of the safety-related program for the TwinSAFE Logic, since it forms the basis for the implementation. In addition to selecting the TwinSAFE components, the function blocks to be used and the sensors and actuators, the parameterization of the components must also be specified, since this can influence the maximum achievable Performance Level.

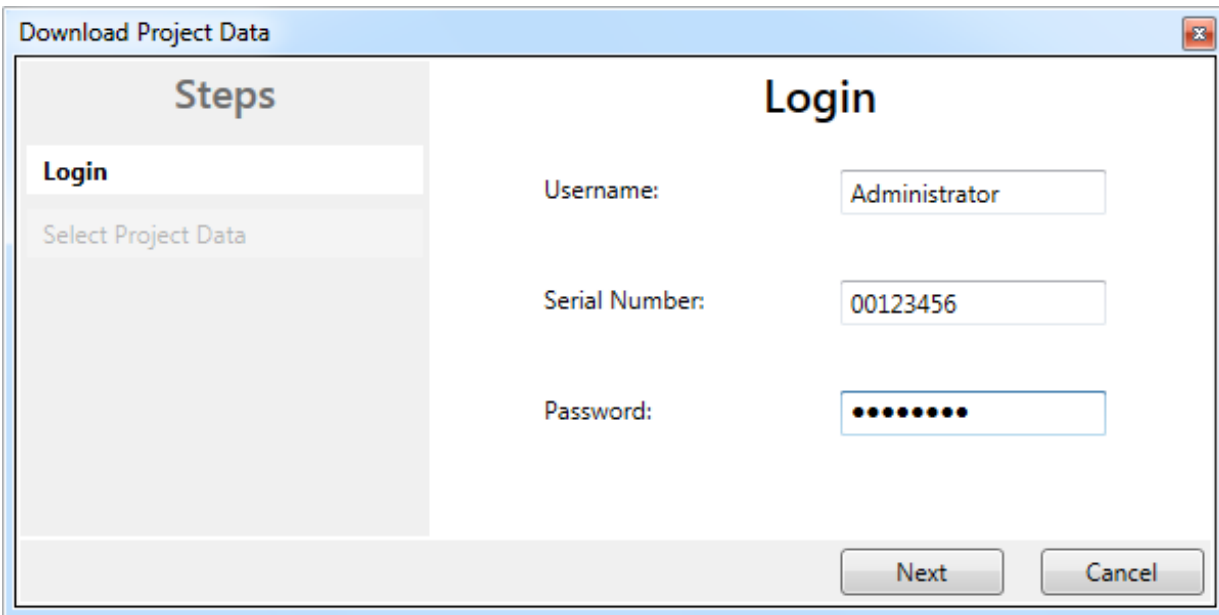
Examples for the implementation of safety functions and the parameterization of the TwinSAFE components can be found in this manual.

10.5 Implementation of the safety functions

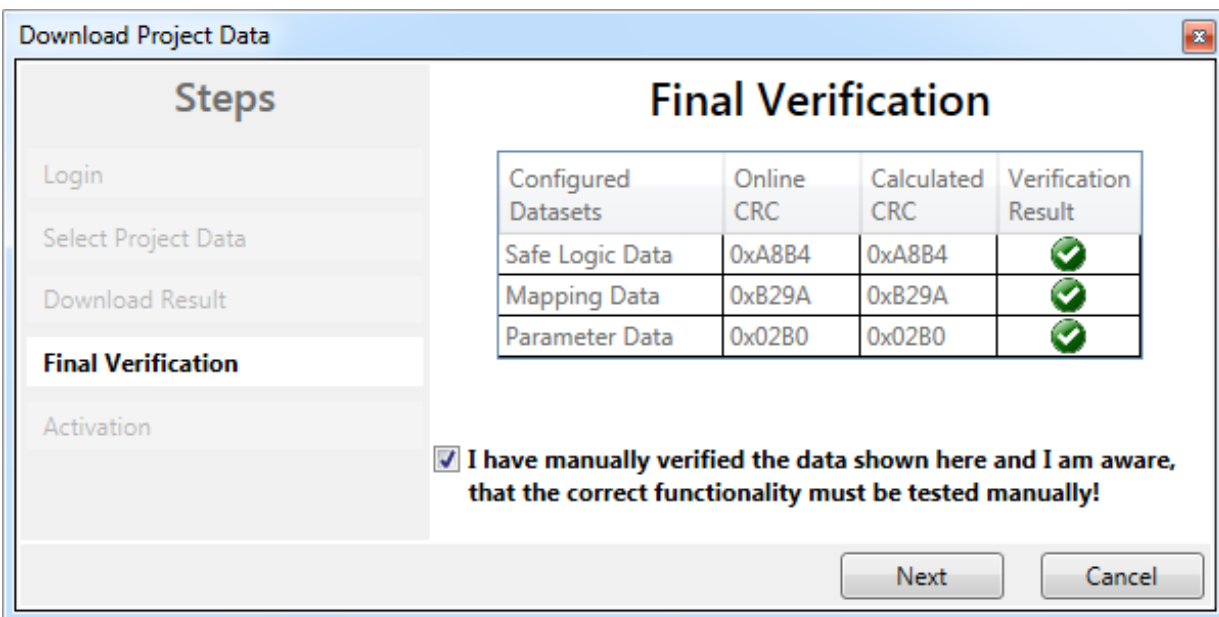
The function blocks are configured in TwinCAT according to the specified safety functions. Predefined function blocks are available for the typical safety functions, which can be interconnected in a graphical editor. Safe input and output components provide the interface to sensors and actuators.

Once the entire safety logic and the parameterization of the safe inputs and outputs have been implemented, a download to the TwinSAFE logic can take place.



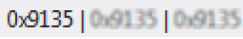
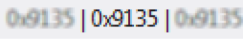
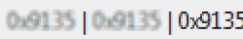
A valid user name and password must be provided for the download, together with the serial number of the device.



The download of the safety program is verified by comparing the CRC of the loaded project (online CRC) and the calculated CRC from the Safety Editor (offline CRC). The comparison is carried out by TwinCAT on the one hand and by the user on the other. The user confirms the comparison by ticking the checkbox and re-entering the password.



The Safety CRC toolbar in TwinCAT can be used at any time to check whether the online CRC matches the offline CRC, i.e. whether data has been changed in the editor or on the TwinSAFE logic. The following table is taken from the EL6910 documentation.

Icon	Name	Description
 CRCs:	CRC Toolbar	Left-click on the toolbar to initiate an update of the CRCs by the user. Red icon: CRCs are different
 CRCs:	CRC Toolbar	Green icon: All CRCs are identical
 0x9135 0x9135 0x9135	Online CRC	CRC of the safety project on the EL6910. This value is read online by the terminal. In the absence of an ADS connection to the EL6910, this value is displayed with 0x---- .
 0x9135 0x9135 0x9135	Downloaded CRC	CRC of the safety project that was loaded last. If no safety project is loaded when the TwinCAT project is opened, the value is displayed with 0x---- .
 0x9135 0x9135 0x9135	Offline CRC	CRC of the current safety project, as stored in the safety editor. A CRC is displayed, if the stored project is valid. If the project is invalid, 0x---- is displayed as CRC.

⚠ CAUTION

Checking the checksums

The user must verify that the online CRC and the offline CRC match. This is the only way to ensure that a download was carried out after the project was created or modified.

Once all specified safety functions have been implemented in the TwinSAFE logic, the implemented logic is printed.

In addition to the entire logic, the parameters and the safety addresses of all safety components used, the printout also contains the calculated project checksum, which is shown on the cover sheet. The programmer and the customer can document the acceptance of the safety functions with date and signature on the cover sheet.

A	B	C	D	E	F	G	H	I	J	
<p>Documentation for solution</p> <p>TwinCAT Project18</p> <p>SafetyProject_MachineFeeder</p> <p>Project CRC: 0x785F</p> <p>Programmer:</p> <p>Print Name _____ Signature _____ Date _____</p> <p>Customer:</p> <p>Print Name _____ Signature _____ Date _____</p>										
Date	17.10.2017	BECKHOFF		Beckhoff Automation GmbH						
Editor	SafetyUser01									
Plot	17.10.2017									

10.6 Proof of achievement of the Performance Level

Once the safety project for the identified safety functions (SF) has been realized, the Performance Level achieved for these SFs is calculated and verified. Examples for such calculations and verifications can be found in this manual in chapter 2.

10.7 Validation of the safety functions

Extract from EN ISO 13849-2:2013, Chapter 4.1: validation guidelines.

The referenced chapters have already been changed over to the chapter numbers of EN ISO 13849-1:2015, although EN ISO 13849-1:2006 is still referenced in EN ISO 13849-2:2013.

The purpose of the validation procedure is to confirm that the design of the safety-related parts of the control system (SRP/CS) supports the specification of the safety requirements of the machines.

The validation must show that each SRP/CS meets the requirements of EN ISO 13849-1:2015, particularly with regard to:

- a) the specified safety characteristics of the safety functions, as intended by the design;
- b) the requirements for the specified Performance Level (see EN ISO 13849-1:2015, 4.5):
 1. the requirements for the specified category (see EN ISO 13849-1:2015, 6.2),
 2. the measures for controlling and avoiding systematic failures (see EN ISO 13849-1:2015, Annex G),
 3. the software requirements, if applicable (see EN ISO 13849-1:2015, 4.6), and
 4. the ability to provide a safety function under the expected conditions;
- c) the ergonomic design of the user interface, e.g. to discourage the user to act in a dangerous manner by circumventing the SRP/CS (see EN ISO 13849-1:2015, 4.8).

The validation should be carried out by persons who not involved in the SRP/CS design.

NOTE "Independent person" does not necessarily mean that a test by a third party is necessary.

Further information about the validation can be found in EN ISO 13849-2:2013, for example in Figure 1, *overview of the validation procedure*, and in EN ISO 13849-1:2015.

10.8 Instructions for checking the SF

All implemented safety functions (SF) have to be checked for correctness. This includes both normal operation and the function in the event of a fault. Some of the test cases can be read from the defined safety function with its described measures for risk minimization. For each function, the possible fault scenarios must be defined and checked accordingly. This information must be recorded in a test specification or acceptance protocol.

- The following list shows some fault scenarios to be considered:
- Discrepancy error of two safe inputs
- Line interruption of the fieldbus used
- Feedback (EDM) error of the actuators
- Failure of the power supply
- Cross-circuit / external feed / line interruption in the wiring
- Violation of a defined limit, e.g. speed limit for axis functions and checking of the defined error behavior
- ...

The validation must also ensure that all hazards identified by the risk assessment are covered by appropriate measures and that these measures have actually been implemented.

This applies especially to the life cycle phases of installation/assembly and maintenance. It must be ensured that any necessary changes or extensions to the safety project are only made after the design engineer (machine manufacturer) has been notified and the safety specification has been changed by the manufacturer. A check to see whether an extension of the test specification is necessary must also be carried out. This applies in particular to machines that are assembled and put into operation at the end customer's premises.

The test must cover the following points as a minimum:

- I/O Check of the safe inputs and outputs
- Verification of the parameterization of all safety components (watchdog times, sensor tests, FSoE address, etc.)
- Check of the safety functions during normal operation
- Check of the safety functions in the event of an error
- Check of the safe drive functions during normal operation
- Check of the safe drive functions outside the defined safety limits
- Check of the safe drive functions in the event of a power failure
- ...

10.9 Acceptance

The following list contains points which are required for the acceptance of the safety project. This list is not exhaustive. These points must be checked after the initial start-up and after each software modification of the TwinSAFE project.

- Implementation or changes only by qualified personnel
- Printout of the TwinSAFE project
- Checking of the entire safety project for correctness according to the previous chapter
- Comparison of the online CRC of the TwinSAFE project with the offline CRC to ensure that a download took place after the changes to the safety project
- Implementation and printout of the acceptance protocol
- Signature by programmer and customer
- This information should be added to the machine documentation
- ...

11 Technical report – TÜV SÜD

KONFORMITÄTSBESTÄTIGUNG LETTER OF CONFIRMATION



BV89987T

Applikationshandbuch TwinSAFE (Application guide TwinSAFE)

Hersteller:
Manufacturer:

Prüfstelle:
Test body:

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
D-33415 Verl

TÜV SÜD RAIL GmbH
Rail Automation
Barthstr. 16
D-80339 München

1. Allgemein / General

Das "Applikationshandbuch TwinSAFE" zeigt die Berechnungen der sicherheitsrelevanten Kennwerte bezüglich der Wahrscheinlichkeit gefährbringender zufälliger Hardwareausfälle (MTTFd und PFH) nach EN 61508 bzw. EN ISO 13849-1.

The "Application guide TwinSAFE" shows calculations of the safety relevant parameters of the probability of dangerous random hardware failures (MTTFd and PFH) according to EN 61508 respectively EN ISO 13849-1.

2. Prüfgrundlagen / Test bases

Berechnung des MTTF _d und DC entsprechend EN ISO 13849-1:2015 Calculation of MTTF _d and DC in accordance with EN ISO 13849-1:2015
Berechnung des PFH entsprechend EN 61508:2010 Calculation of PFH in accordance with EN 61508:2010
Applikationshandbuch TwinSAFE Version 3.0.0 Application guide TwinSAFE version 3.0.0

3. Zusammenfassung / Summary

Die Applikationsbeispiele des "Applikationshandbuch TwinSAFE" der Firma Beckhoff Automation GmbH & Co. KG wurden von der TÜV SÜD Rail GmbH, Rail Automation, überprüft und bestätigt.

The application examples in the "Application guide TwinSAFE" were checked and confirmed by TÜV SÜD Rail GmbH, Rail Automation.

TÜV SÜD Rail GmbH
2020-07-20

Digital unterschrieben
von Guido Neumann
Datum: 2020.07.20
12:46:21 +02'00'

G. Neumann
Technical Certifier

Digital unterschrieben
von Thomas Kreten
Datum:
2020.07.20
12:22:59 +02'00'

T. Kreten
Project Leader

Diese Bestätigung wurde auf Grundlage einer TÜV-internen technischen Beurteilung erstellt.
Diese enthält das Ergebnis einer einmaligen Untersuchung an dem zur Prüfung vorgelegten Erzeugnis.

This confirmation was created on basis of a TÜV internal technical review report.
It includes the result of a one-time examination of the product submitted for examination.

12 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

Beckhoff's branch offices and representatives

Please contact your Beckhoff branch office or representative for [local support and service](#) on Beckhoff products!

The addresses of Beckhoff's branch offices and representatives round the world can be found on her internet pages:

<http://www.beckhoff.com>

You will also find further [documentation](#) for Beckhoff components there.

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

Phone: +49 5246 963 0
Fax: +49 5246 963 198
e-mail: info@beckhoff.com

Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline: +49 5246 963 157
Fax: +49 5246 963 9157
e-mail: support@beckhoff.com

Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

Hotline: +49 5246 963 460
Fax: +49 5246 963 479
e-mail: service@beckhoff.com

More Information:

www.beckhoff.de/english/twinsafe/default.htm

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
Phone: +49 5246 9630
info@beckhoff.com
www.beckhoff.com

