

## Application Guide

# TwinSAFE

Version: 1.9.1  
Date: 2018-02-05



# BECKHOFF



# Table of contents

<b>1</b>	<b>Foreword</b>	<b>7</b>
1.1	Notes on the documentation	7
1.1.1	Intended audience	7
1.1.2	Origin of the document	7
1.1.3	Currentness	7
1.1.4	Product features	7
1.1.5	Disclaimer	7
1.1.6	Trademarks	7
1.1.7	Patent Pending	8
1.1.8	Copyright	8
1.1.9	Delivery conditions	8
1.2	Safety instructions	8
1.2.1	Delivery state	8
1.2.2	Operator's obligation to exercise diligence	8
1.2.3	Purpose and area of application	9
1.2.4	Description of safety symbols	9
1.2.5	Explanation of terms	10
1.2.6	Documentation issue status	11
<b>2</b>	<b>Circuit examples</b>	<b>12</b>
2.1	ESTOP function variant 1 (Category 3, PL d)	12
2.1.1	Parameters of the safe input and output terminals	12
2.1.2	Block formation and safety loops	13
2.1.3	Calculation	13
2.2	ESTOP function variant 2 (Category 3, PL d)	17
2.2.1	Parameters of the safe input and output terminals	17
2.2.2	Block formation and safety loops	18
2.2.3	Calculation	18
2.3	ESTOP function variant 3 (Category 4, PL e)	23
2.3.1	Parameters of the safe input and output terminals	23
2.3.2	Block formation and safety loops	24
2.3.3	Calculation	24
2.4	ESTOP function variant 4 (Category 4, PL e)	29
2.4.1	Parameters of the safe input and output terminals	29
2.4.2	Block formation and safety loops	30
2.4.3	Calculation	30

<b>2.5</b>	<b>ESTOP function variant 5 (Category 4, PL e)</b>	<b>35</b>
2.5.1	Parameters of the safe input and output terminals	35
2.5.2	Block formation and safety loops	36
2.5.3	Calculation	36
<b>2.6</b>	<b>ESTOP function variant 6 (Category 3, PL d)</b>	<b>41</b>
2.6.1	Parameters of the safe input and output terminals (SIL 2)	41
2.6.2	Block formation and safety loops	42
2.6.3	Calculation	42
<b>2.7</b>	<b>ESTOP function variant 7 (Category 4, PL e)</b>	<b>47</b>
2.7.1	Parameters of the safe input and output terminals	47
2.7.2	Block formation and safety loops	48
2.7.3	Calculation	48
<b>2.8</b>	<b>Protective door function variant 1 (Category 3, PL d)</b>	<b>53</b>
2.8.1	Parameters of the safe input and output terminals	53
2.8.2	Block formation and safety loops	54
2.8.3	Calculation	54
<b>2.9</b>	<b>Protective door function variant 2 (Category 4, PL e)</b>	<b>59</b>
2.9.1	Parameters of the safe input and output terminals	59
2.9.2	Block formation and safety loops	60
2.9.3	Calculation	60
<b>2.10</b>	<b>Protective door function with range monitoring (Category 4, PL e)</b>	<b>65</b>
2.10.1	Parameters of the safe input and output terminals	66
2.10.2	Block formation and safety loops	66
2.10.3	Calculation	67
<b>2.11</b>	<b>Protective door function with guard lock (Category 4, PL e)</b>	<b>72</b>
2.11.1	Parameters of the safe input and output terminals	72
2.11.2	Block formation and safety loops	73
2.11.3	Calculation	73
<b>2.12</b>	<b>Two-hand controller (Category 4, PL e)</b>	<b>79</b>
2.12.1	Parameters of the safe input and output terminals	79
2.12.2	Block formation and safety loops	80
2.12.3	Calculation	80
<b>2.13</b>	<b>Laser scanner (Category 3, PL d)</b>	<b>84</b>
2.13.1	Parameters of the safe input and output terminals	84
2.13.2	Block formation and safety loops	85
2.13.3	Calculation	85

<b>2.14 Light grid (Category 4, PL e)</b>	<b>89</b>
2.14.1 Parameters of the safe input and output terminals	89
2.14.2 Block formation and safety loops	90
2.14.3 Calculation	90
<b>2.15 Safety switching mat / safety bumper (Category 4, PL e)</b>	<b>94</b>
2.15.1 Parameters of the safe input and output terminals	94
2.15.2 Block formation and safety loops	95
2.15.3 Calculation	95
<b>2.16 Muting (Category 4, PL e)</b>	<b>99</b>
2.16.1 Parameters of the safe input and output terminals	99
2.16.2 Block formation and safety loops	100
2.16.3 Calculation	100
<b>2.17 All-pole disconnection of a potential group with downstream non-reactive standard terminals (Category 4, PL e)</b>	<b>105</b>
2.17.1 Notes on prevention of feedback	107
2.17.2 Parameters of the safe input and output terminals	109
2.17.3 Block formation and safety loops	110
2.17.4 Calculation	110
<b>2.18 Single-pole disconnection of a potential group with downstream non-reactive standard terminals with fault exclusion (Category 4, PL e)</b>	<b>115</b>
2.18.1 Notes on prevention of feedback	117
2.18.2 Parameters of the safe input and output terminals	119
2.18.3 Block formation and safety loops	120
2.18.4 Calculation	120
<b>2.19 Networked system (Category 4, PL e)</b>	<b>125</b>
2.19.1 Parameters of the safe input and output terminals	126
2.19.2 Block formation and safety loops	126
2.19.3 Calculation	127
<b>2.20 Drive option AX5801 with SS1 stop function (Category 4, PL e)</b>	<b>131</b>
2.20.1 Parameters of the safe input and output terminals	132
2.20.2 Block formation and safety loops	132
2.20.3 Calculation	132
<b>2.21 Drive option AX5805 with SS2 stop function (Category 4, PL e)</b>	<b>137</b>
2.21.1 Parameters of the safe input and output terminals	137
2.21.2 Block formation and safety loops	138
2.21.3 Calculation	138

<b>2.22 Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (single-channel) (Category 2, PL c)</b>	<b>142</b>
2.22.1 Parameters of the safe input and output terminals	142
2.22.2 Block formation and safety loops	143
2.22.3 Calculation	143
<b>2.23 Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (dual-channel) (Category 3, PL d)</b>	<b>146</b>
2.23.1 Parameters of the safe input and output terminals	146
2.23.2 Block formation and safety loops	146
2.23.3 Calculation	147
<b>2.24 ESTOP function (Category 3, PL d)</b>	<b>149</b>
2.24.1 Parameters of the safe input and output terminals (SIL 2)	150
2.24.2 Block formation and safety loops	150
2.24.3 Calculation	150
<b>2.25 Speed monitoring (Category 3, PL d)</b>	<b>155</b>
2.25.1 Structure and diagnosis	157
2.25.2 FMEA	157
2.25.3 Parameters of the safe output terminal	159
2.25.4 Block formation and safety loops	159
2.25.5 Calculation	159
<b>2.26 Speed monitoring (via IO-link) (Category 3, PL d)</b>	<b>166</b>
2.26.1 Structure and diagnosis	168
2.26.2 FMEA	168
2.26.3 Parameters of the safe output terminal	170
2.26.4 Block formation and safety loops	170
2.26.5 Calculation	170
<b>2.27 STO function with EL72x1-9014 (Category 3, PL d)</b>	<b>176</b>
2.27.1 Parameters of the safe input and output terminals	177
2.27.2 Block formation and safety loops	178
2.27.3 Safety function 1	178
2.27.4 Calculation	178
<b>2.28 STO-Function with IndraDrive (Category 4, PL e)</b>	<b>182</b>
2.28.1 Parameters of the safe input and output terminals	183
2.28.2 Block formation and safety loops	183
2.28.3 Safety function 1	183
2.28.4 Calculation	183
2.28.5 Technical Note from company Bosch Rexroth AG	188

<b>2.29 Temperature measurement with TwinSAFE SC (Category 3, PL d)</b>	<b>192</b>
2.29.1 Diagram of the structure	193
2.29.2 Structure and diagnosis	193
2.29.3 FMEA	193
2.29.4 Parameters of the safe output terminal	195
2.29.5 Block formation and safety loops	195
2.29.6 Calculation	195
<b>2.30 Level measurement with TwinSAFE SC (Category 3, PL d)</b>	<b>202</b>
2.30.1 Diagram of the structure	203
2.30.2 Structure and diagnosis	203
2.30.3 FMEA	203
2.30.4 Parameters of the safe output terminal	205
2.30.5 Block formation and safety-loops	205
2.30.6 Calculation	205
<b>2.31 Pressure measurement with TwinSAFE SC (Category 3, PL d)</b>	<b>212</b>
2.31.1 Diagram of the structure	213
2.31.2 Structure and diagnosis	213
2.31.3 FMEA	213
2.31.4 Parameters of the safe output terminal	215
2.31.5 Block formation and safety-loops	215
2.31.6 Calculation	215
<b>2.32 Monitoring lifting device (Category 3, PL d)</b>	<b>222</b>
2.32.1 Diagram of the structure	223
2.32.2 Structure and diagnosis	223
2.32.3 FMEA	224
2.32.4 Structure within the logic	225
2.32.5 Parameters of the safe output terminal	227
2.32.6 Block formation and safety-loops	228
2.32.7 Calculation	228

<b>3</b>	<b>Planning a safety project with TwinSAFE components</b>	<b>235</b>
3.1	Identifying the risks and hazards	235
3.2	Determining the PL <sub>r</sub> / SIL	236
3.3	Specification of the safety functions	236
3.4	Specification of the measures	236
3.5	Implementation of the safety functions	237
3.6	Proof of achievement of the Performance Level	239
3.7	Validation of the safety functions	239
3.8	Instructions for checking the SF	240
3.9	Acceptance	240
<b>4</b>	<b>Technical report – TÜV SÜD</b>	<b>241</b>
<b>5</b>	<b>Appendix</b>	<b>242</b>
5.1	Beckhoff Support and Service	242
5.1.1	Beckhoff branches and partner companies Beckhoff Support	242
5.1.2	Beckhoff company headquarters	242



# 1 Foreword

## 1.1 Notes on the documentation

### 1.1.1 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.

### 1.1.2 Origin of the document

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

### 1.1.3 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.de/english/download/twinsafe.htm>. In case of doubt, please contact the technical Support (see chapter 5.1 Beckhoff Support and Service)

### 1.1.4 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.

### 1.1.5 Disclaimer

The documentation has been prepared with care. The products described are, however, constantly under development. For that reason the documentation is not in every case checked for consistency with performance data, standards or other characteristics.

In the event that it contains technical or editorial errors, we retain the right to make alterations at any time and without warning.

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.

### 1.1.6 Trademarks

Beckhoff®, TwinCAT®, EtherCAT®, Safety over EtherCAT®, TwinSAFE®, XFC® and XTS® 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.

### 1.1.7 Patent Pending

The EtherCAT Technology is covered, including but not limited to the following patent applications and patents: EP1590927, EP1789857, DE102004044764, DE102007017835 with corresponding applications or registrations in various other countries.

The TwinCAT Technology is covered, including but not limited to the following patent applications and patents: EP0851348, US6167425 with corresponding applications or registrations in various other countries.



EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany

### 1.1.8 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.

### 1.1.9 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
- 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 EL2902. The appropriate parameters, which can be taken from the respective product documentation, must then be used in the calculation.

 <b>Attention</b>	<b>Application samples</b>  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 safety symbols

The following safety symbols are used in these operating instructions. They are intended to alert the reader to the associated safety instructions.

 <b>DANGER</b>	<b>Serious risk of injury!</b>  <b>Failure</b> to follow the safety instructions associated with this symbol directly endangers the life and health of persons.
 <b>WARNING</b>	<b>Caution - Risk of injury!</b>  <b>Failure</b> to follow the safety instructions associated with this symbol endangers the life and health of persons.
 <b>CAUTION</b>	<b>Personal injuries!</b>  <b>Failure</b> to follow the safety instructions associated with this symbol can lead to injuries to persons.
 <b>Attention</b>	<b>Damage to the environment or devices</b>  <b>Failure</b> to follow the instructions associated with this symbol can lead to damage to the environment or equipment.
 <b>Note</b>	<b>Tip or pointer</b>  This symbol indicates information that contributes to better understanding.

### 1.2.5 Explanation of terms

Designation	Explanation
B10 <sub>D</sub>	Mean number of cycles after 10% of the components have dangerously failed
CCF	Failures with a common cause
d <sub>op</sub>	Mean operating time in days per year
DC <sub>avg</sub>	Average diagnostic coverage
h <sub>op</sub>	Mean operating time in hours per day
MTTF <sub>D</sub>	Mean time to dangerous failure
n <sub>op</sub>	Mean number of annual actuations
PFH	Probability of a dangerous failure per hour
PL	Performance Level
PL <sub>r</sub>	Required Performance Level
T <sub>Zyklus</sub>	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 (for TwinSAFE devices typically 20 years)
λ <sub>D</sub>	Dangerous failure rate given in FIT (failure rate in 10 <sup>9</sup> component hours)
T <sub>10D</sub>	Operating time - maximum operating time for e.g. electromechanical components
TwinSAFE SC	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 second independent signal. With this comparison result, an analog value is obtained which has typically a level of category 3 and PL d. This technology does not support digital input signals and cannot be used in a single-channel structure (only one TwinSAFE SC channel).

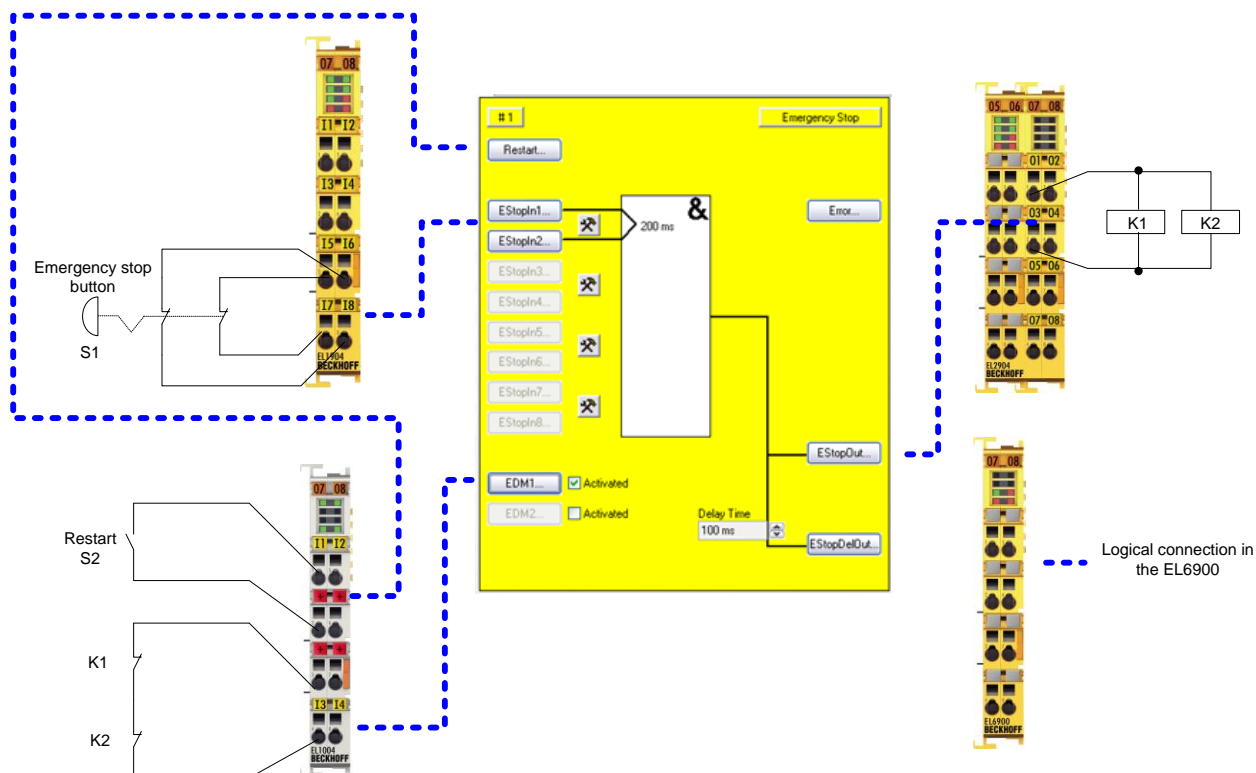
## 1.2.6 Documentation issue status

Version	Comment
1.9.1	<ul style="list-style-type: none"> <li>Note in chapter 2.17 and 2.18 added</li> </ul>
1.9.0	<ul style="list-style-type: none"> <li>Chapter 2.18 updated</li> <li>Chapter 3 Planning a safety project added</li> </ul>
1.8.0	<ul style="list-style-type: none"> <li>TwinSAFE SC examples added</li> <li>Example for Bosch Rexroth IndraDrive drives family</li> <li>Name SIL2 Communication replaced by TwinSAFE SC</li> <li>Examples 2.25 and 2.26 updated</li> <li>General revision of all chapters</li> </ul>
1.7.0	<ul style="list-style-type: none"> <li>Chapter "Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (single channel)" revised</li> <li>Preface updated</li> <li>Chapter "Purpose and area of application" expanded</li> <li>Structure diagram chapters 2.25 and 2.26 updated</li> <li>Chapter 2.27 added</li> <li>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)</li> <li>Note texts added in chapter 2.19</li> </ul>
1.6.2	<ul style="list-style-type: none"> <li>Letter of conformity updated</li> <li>Graphics in chapters 2.25 and 2.26 updated</li> <li>Purpose and area of applications added</li> </ul>
1.6.1	<ul style="list-style-type: none"> <li>Chapters 2.25 and 2.26 added</li> </ul>
1.6.0	<ul style="list-style-type: none"> <li>Chapters 2.17 and 2.18 revised</li> </ul>
1.5.0	<ul style="list-style-type: none"> <li>Company address amended</li> </ul>
1.4.0	<ul style="list-style-type: none"> <li>Chapter 2.24 added</li> <li>Documentation versions added</li> <li>Document origin added</li> <li>Formatting changed</li> </ul>
1.3.1	<ul style="list-style-type: none"> <li>Headers extended with categories and performance levels</li> <li>Note in Chapter 2.6 moved</li> </ul>
1.3.0	<ul style="list-style-type: none"> <li>Terms of delivery removed</li> </ul>
1.2.0	<ul style="list-style-type: none"> <li>Correction to Chapter 2.6</li> </ul>
1.1.0	<ul style="list-style-type: none"> <li>First released version</li> </ul>

## 2 Circuit examples

### 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

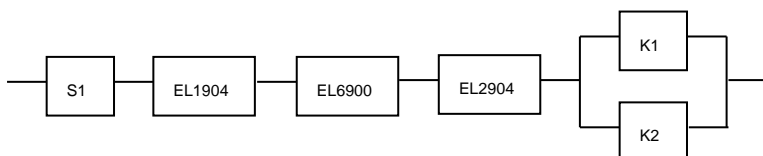
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

##### 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 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
S1 – B10 <sub>d</sub>	100,000
S2 – B10 <sub>d</sub>	10,000,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	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 <sub>avg</sub> =99%
K1/K2 with testing and EDM (actuation 1x per week)	DC <sub>avg</sub> =60%
K1/K2 with testing and EDM (actuation 1x per shift)	DC <sub>avg</sub> =90%

### 2.1.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1 \cdot 21,90} = 45662,1y = 399999120h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 \cdot 21,90} = 593607,3y = 5199997320h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

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

**K1/K2:** actuation 1x per week

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

**K1/K2:** actuation 1x per shift

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

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.

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  $\beta$ -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).

This produces for the calculation of the PFH 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 safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{(MTTF_d(K1))}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 333,98y$$

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

bzw.:

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

**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 attain category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation!

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

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

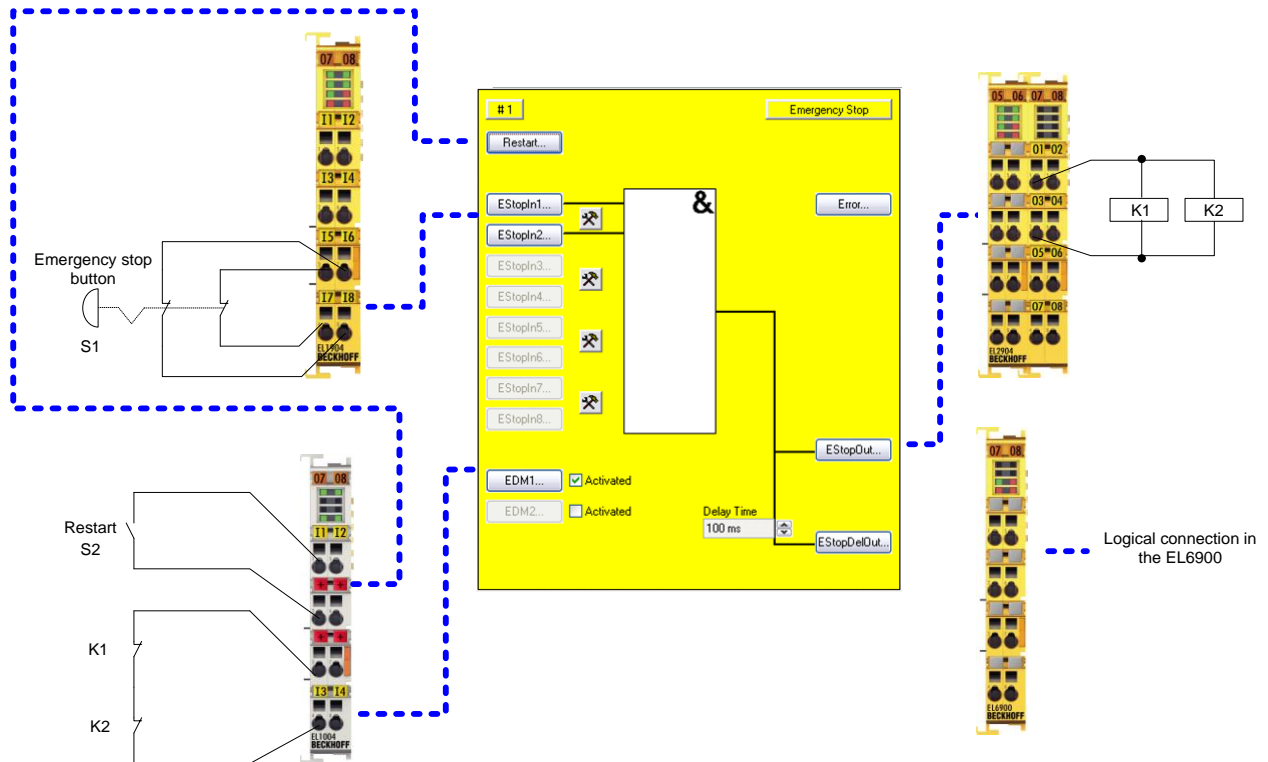
MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC / MTTF <sub>d</sub>	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

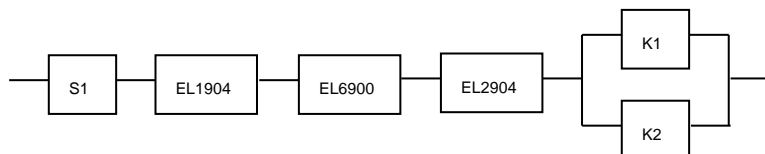
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

#### 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 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
S1 – B10 <sub>d</sub>	100,000
S2 – B10 <sub>d</sub>	10,000,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	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 <sub>avg</sub> =90%
K1/K2 with testing and EDM (actuation 1x per week)	DC <sub>avg</sub> =60%
K1/K2 with testing and EDM (actuation 1x per shift)	DC <sub>avg</sub> =90%

### 2.2.3.3 Calculation for block 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1*21,90} = 45662,1y = 399999120h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

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 100,000 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  $\beta$ -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).

This produces for the calculation of the PFH value for block 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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 333,98y$$

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

bzw.:

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

**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 attain category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation!

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

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

Designation for each channel	MTTF <sub>d</sub>	Range for each channel
low		3 years ≤ MTTF <sub>d</sub> < 10 years
medium		10 years ≤ MTTF <sub>d</sub> < 30 years
high		30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>	Range
none		DC < 60 %
low		60 % ≤ DC < 90 %
medium		90 % ≤ DC < 99 %
high		99 % ≤ DC

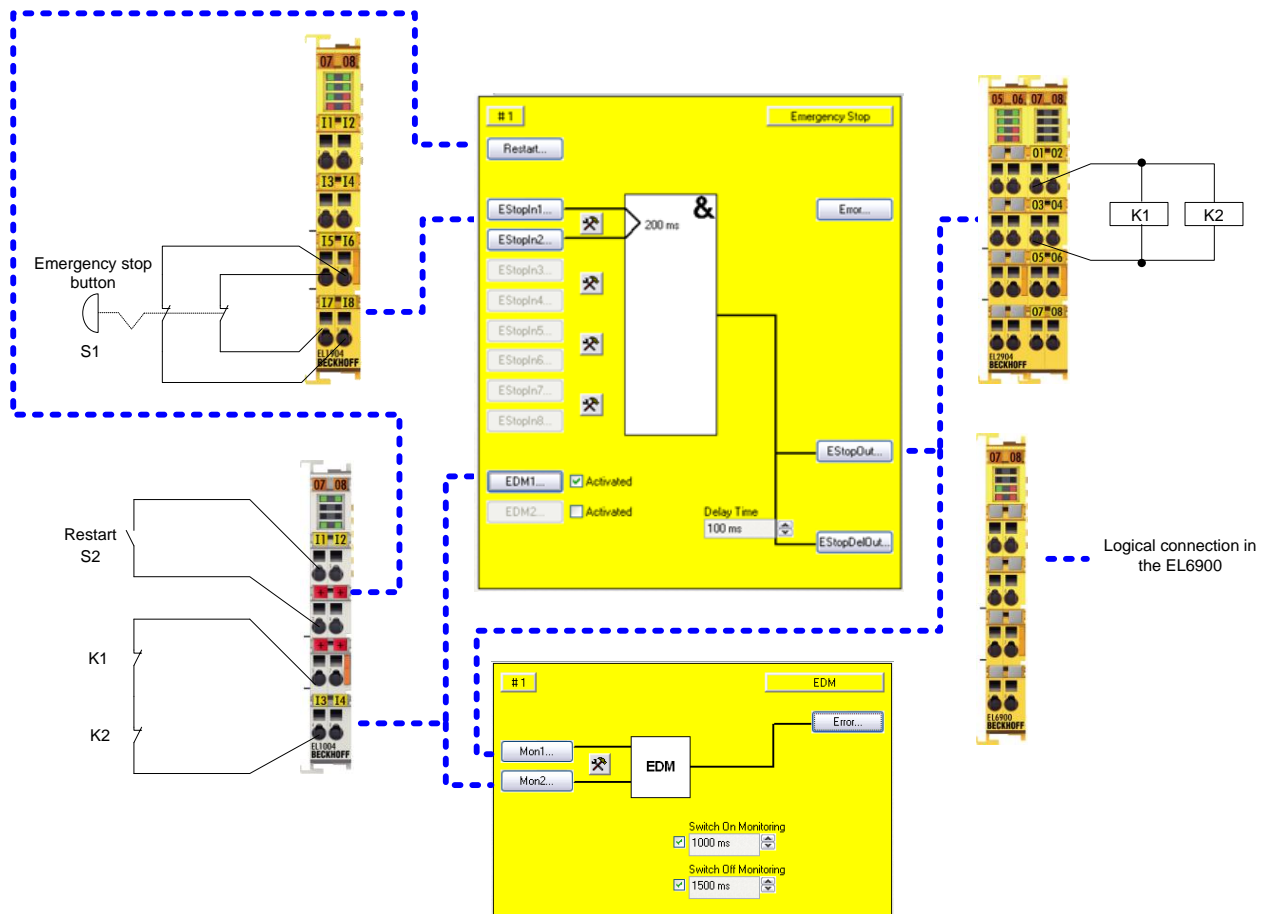
Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e



## 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 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.



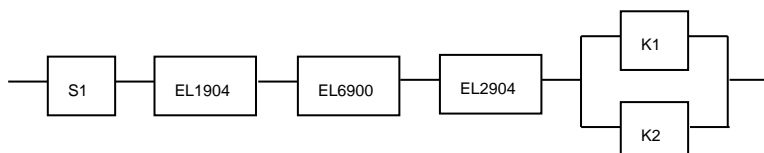
### 2.3.1 Parameters of the safe input and output terminals

#### 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 Block 1****2.3.3 Calculation****2.3.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

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

**2.3.3.2 Diagnostic Coverage DC**

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

### 2.3.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1 * 21,90} = 45662,1y = 399999120h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

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 100,000 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  $\beta$ -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).

This produces for the calculation of the PFH 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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{d ges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 333,98y$$

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

or:

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

**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!

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

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

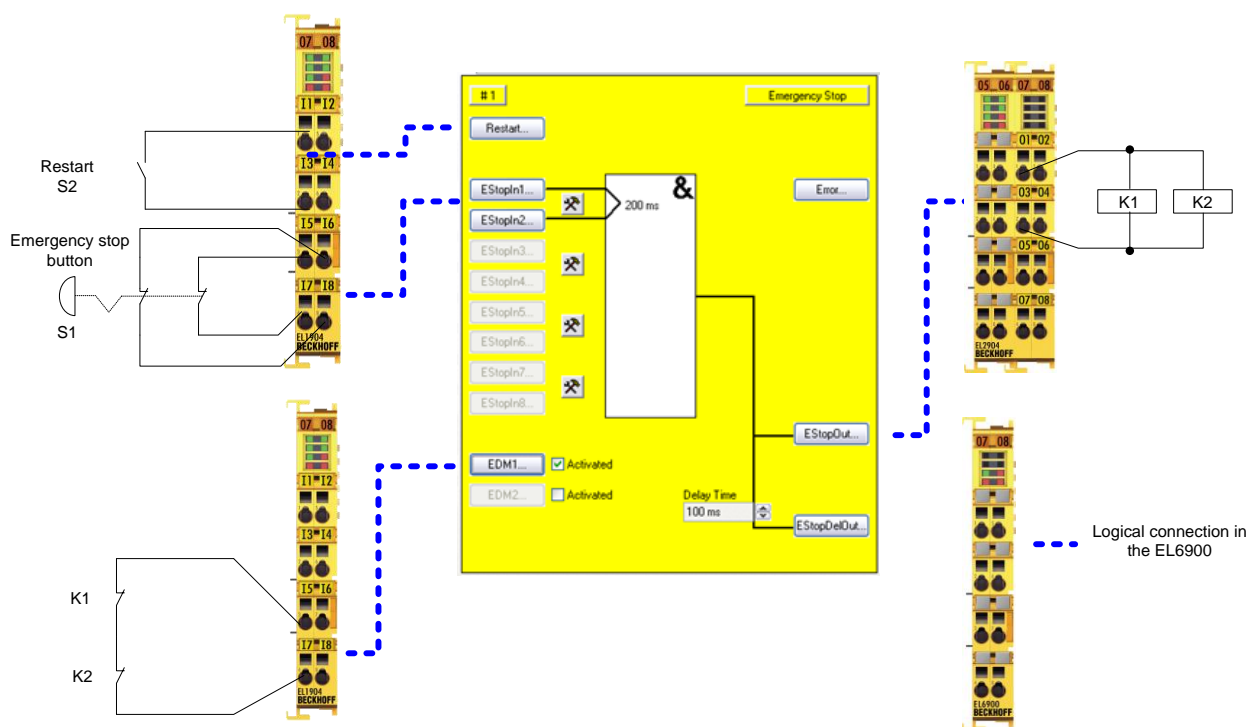
Designation for each channel	MTTF <sub>d</sub>	Range for each channel
low		3 years ≤ MTTF <sub>d</sub> < 10 years
medium		10 years ≤ MTTF <sub>d</sub> < 30 years
high		30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>	Range
none		DC < 60 %
low		60 % ≤ DC < 90 %
medium		90 % ≤ DC < 99 %
high		99 % ≤ DC
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 <sub>d</sub>	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)

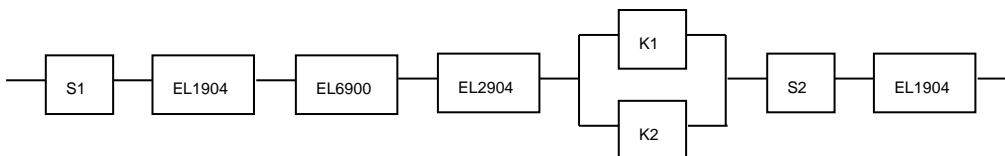
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

#### 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 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.4.3.2 Diagnostic Coverage DC

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

### 2.4.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1 \cdot 21,90} = 45662,1y = 399999120h$$

**S2:**

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

$$MTTF_d = \frac{10000000}{0,1 \cdot 21,90} = 4566210,0y = 4E10h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 \cdot 21,90} = 593607,3y = 5199997320h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

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

**S2:**

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

**K1/K2:** actuation 1x per shift

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

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 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  $\beta$ -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).

This produces for the calculation of the PFH 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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

or:

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

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

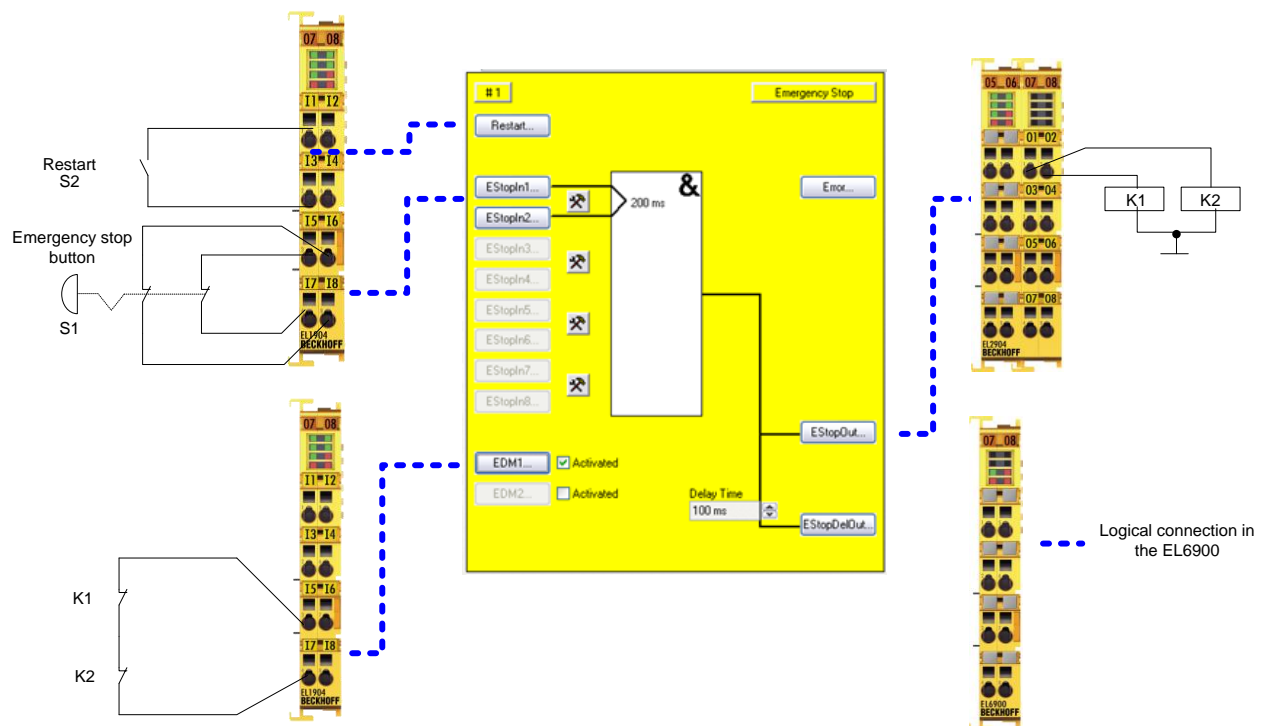
DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

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 <sub>d</sub>	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)

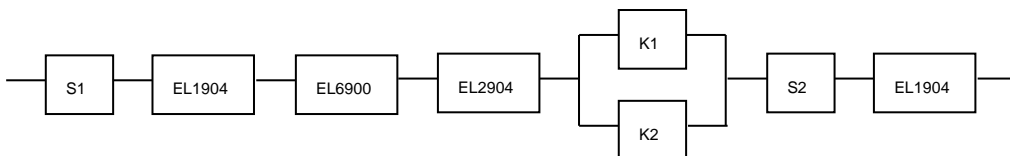
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

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 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.5.3.2 Diagnostic Coverage DC

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

### 2.5.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1 \cdot 21,90} = 45662,1y = 399999120h$$

**S2:**

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

$$MTTF_d = \frac{10000000}{0,1 \cdot 21,90} = 4566210,0y = 4E10h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 \cdot 21,90} = 593607,3y = 5199997320h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

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

**S2:**

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

**K1/K2:** actuation 1x per shift

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

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 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  $\beta$ -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).

This produces for the calculation of the PFH 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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

or:

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

**Note****Category**

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

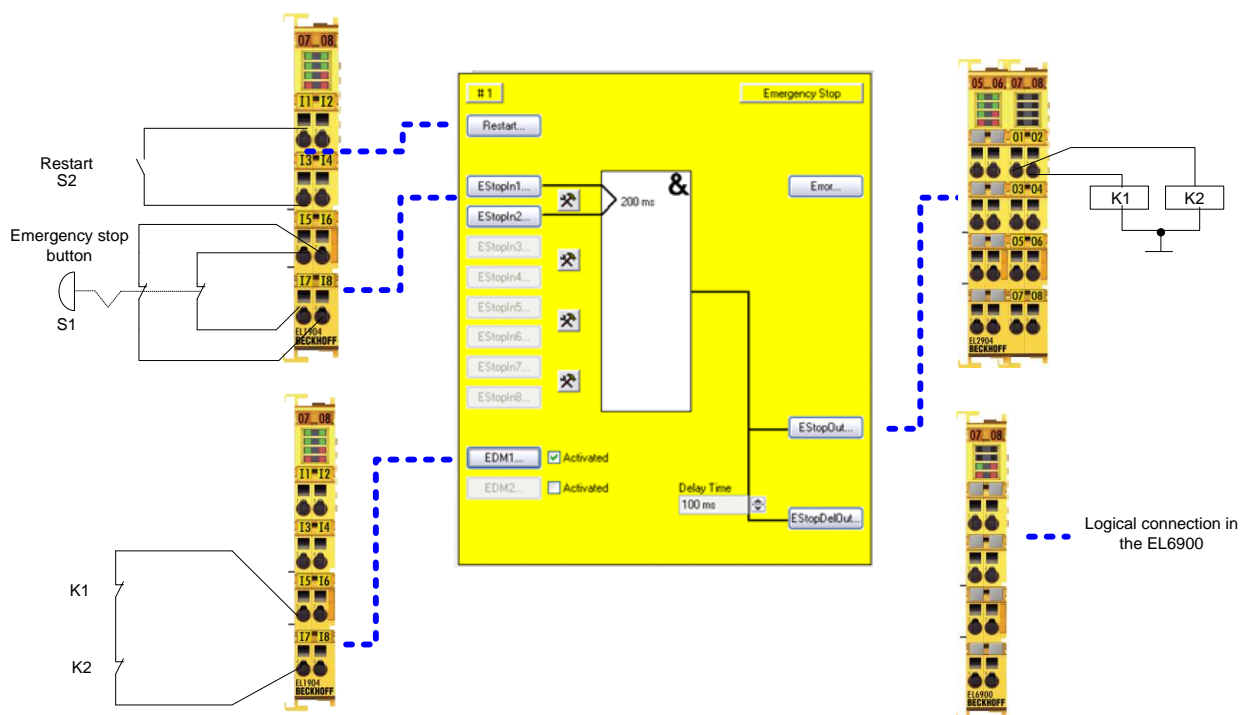
MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years


DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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.



 <b>Note</b>	<p><b>Category</b></p> <p>This structure is possible only up to category 3 at the most on account of a possible sleeping error.</p> <p>Since the EL2904 terminal has only SIL2 in this application, the entire chain has only SIL2!</p>
--	---

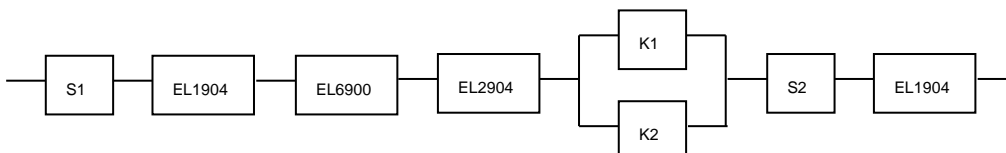
### 2.6.1 Parameters of the safe input and output terminals (SIL 2)

**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 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

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

**2.6.3.2 Diagnostic Coverage DC**

Component	Value
S1 with testing/plausibility	DC <sub>avg</sub> =99%
S2 with plausibility	DC <sub>avg</sub> =90%
K1/K2 without testing and with EDM via a safe input	DC <sub>avg</sub> =90%

### 2.6.3.3 Calculation for safety function 1

Calculation of the PFH 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:**

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

$$MTTF_d = \frac{100000}{0,1 * 21,90} = 45662,1y = 399999120h$$

**S2:**

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

$$MTTF_d = \frac{10000000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

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 100,000 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  $\beta$ -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).

This produces for the calculation of the PFH 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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

**Note****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!

<b>MTTF<sub>d</sub></b>	
<b>Designation for each channel</b>	<b>Range for each channel</b>
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	<b>30 years ≤ MTTF<sub>d</sub> ≤ 100 years</b>

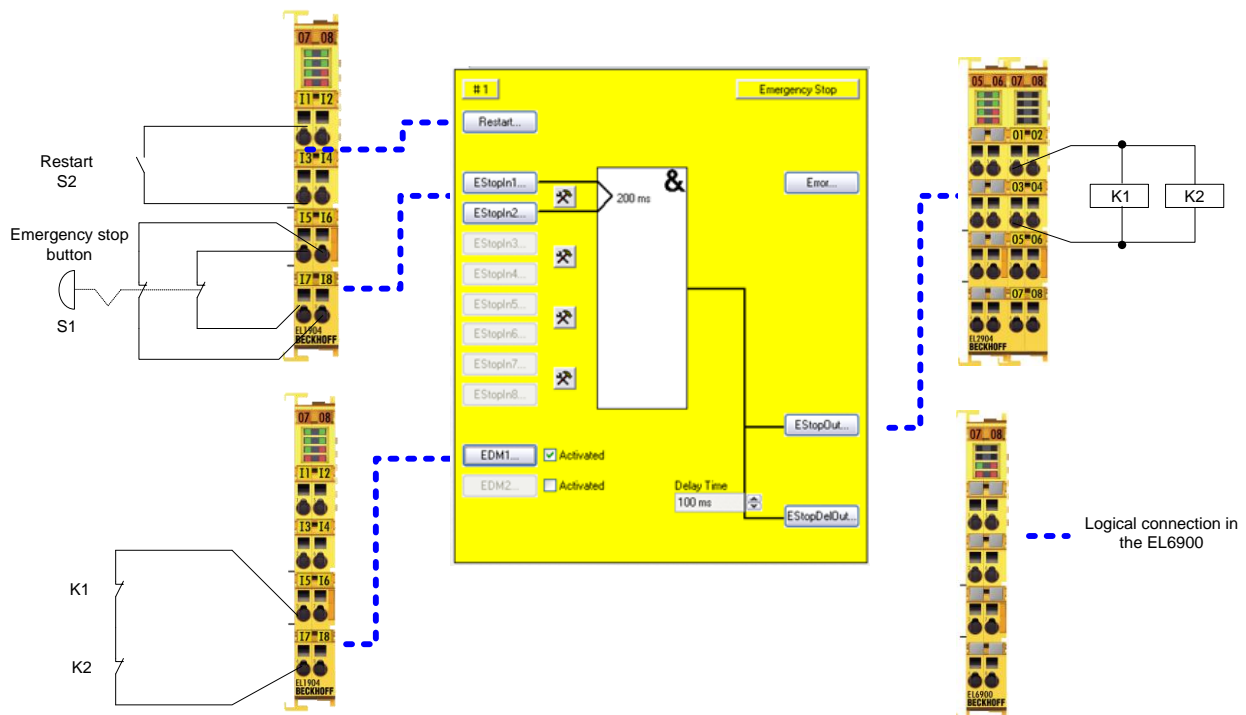
<b>DC<sub>avg</sub></b>	
<b>Designation</b>	<b>Range</b>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
<b>high</b>	<b>99 % ≤ DC</b>

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	<b>none</b>	<b>none</b>	<b>low</b>	<b>medium</b>	<b>low</b>	<b>medium</b>	<b>high</b>
<b>low</b>	a	-	a	b	b	c	-
<b>medium</b>	b	-	b	c	c	d	-
<b>high</b>	-	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

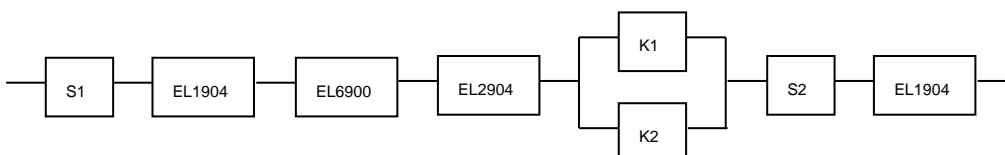
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	not used
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

#### 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 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

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

**2.7.3.2 Diagnostic Coverage DC**

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

### 2.7.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1 * 21,90} = 45662,1y = 399999120h$$

**S2:**

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

$$MTTF_d = \frac{10000000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

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 and direct feedback

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

The following assumptions must now be made:

Safety switch S1: According to BIA report 2/2008, error exclusion to up 100,000 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  $\beta$ -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).

This produces for the calculation of the PFH 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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

or:

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

**Note****Category**

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

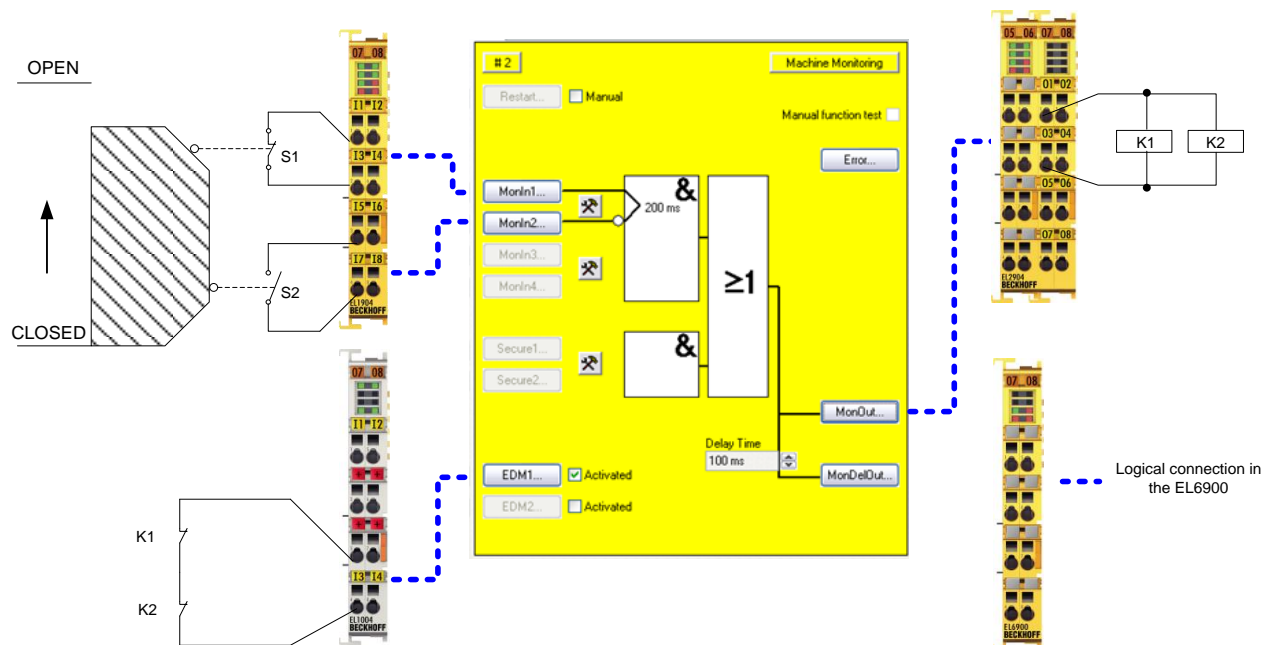
MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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 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.



### 2.8.1 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	Single Logic
Logic channel 3 and 4	Single Logic

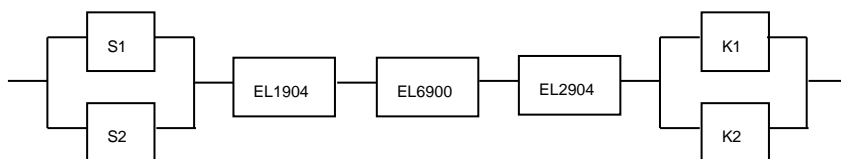
**EL2904**

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes



## 2.8.2 Block formation and safety loops

### 2.8.2.1 Safety function 1



## 2.8.3 Calculation

### 2.8.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.8.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =90%

### 2.8.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{1000000}{0,1 \cdot 14720} = 679,3y = 5951087h$$

**S2:**

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

$$MTTF_d = \frac{2000000}{0,1 \cdot 14720} = 1358,7y = 11902174h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 \cdot 14720} = 883,2y = 7736413h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

$$PFH = \frac{1 - 0,99}{679,3 \cdot 8760} = 1,68E - 9$$

**S2:**

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

**K1/K2:**

$$PFH = \frac{1 - 0,90}{883,2 \cdot 8760} = 1,29E - 8$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

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

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

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

**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 attain category 3, all rising and falling edges must be evaluated together with the time dependence in the controller for the feedback expectation!

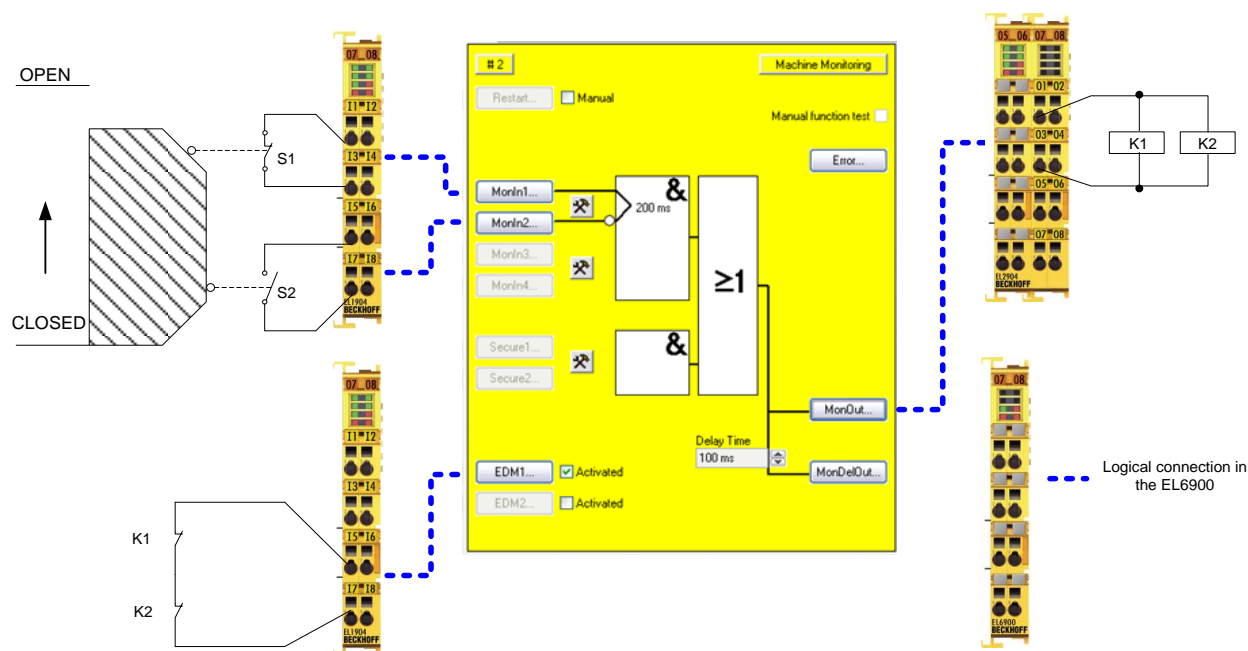
MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	<b>30 years ≤ MTTF<sub>d</sub> ≤ 100 years</b>

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
<b>medium</b>	<b>90 % ≤ DC &lt; 99 %</b>
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.9 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.



### 2.9.1 Parameters of the safe input and output terminals

EL1904 (applies to all EL1904 used)

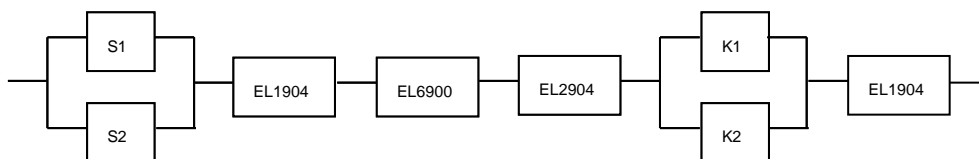
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.9.2 Block formation and safety loops

### 2.9.2.1 Safety function 1



## 2.9.3 Calculation

### 2.9.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.9.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%

### 2.9.3.3 Calculation for block 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{1000000}{0,1 \cdot 14720} = 679,3y = 5951087h$$

**S2:**

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

$$MTTF_d = \frac{2000000}{0,1 \cdot 14720} = 1358,7y = 11902174h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 \cdot 14720} = 883,2y = 7736413h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

$$PFH = \frac{1 - 0,99}{679,3 \cdot 8760} = 1,68E - 9$$

**S2:**

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

**K1/K2:**

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

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 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

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

The MTTF<sub>d</sub> value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} \\ + \frac{1}{MTTF_d(EL1904)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

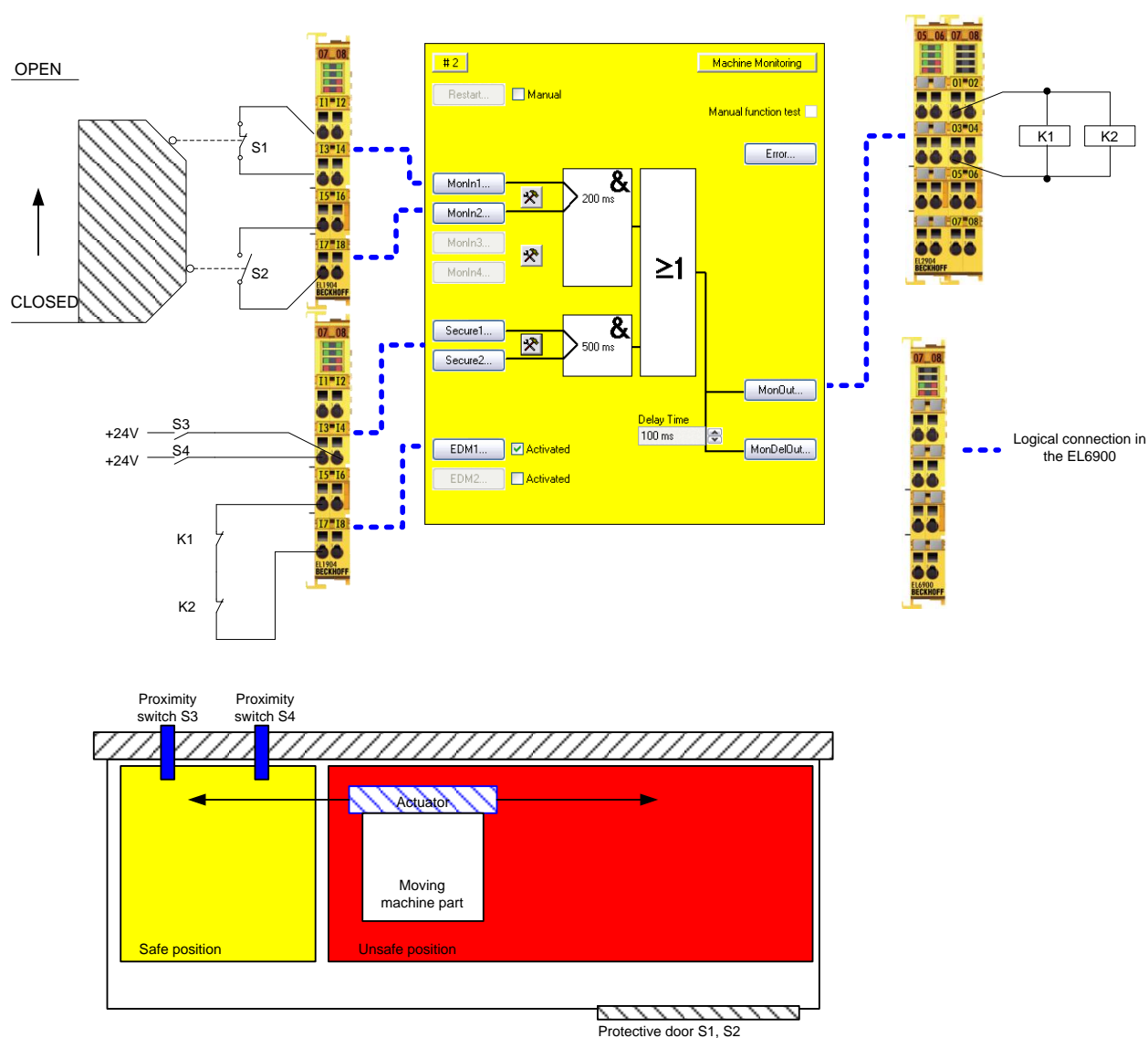
DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.10 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 switches 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.



## 2.10.1 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)

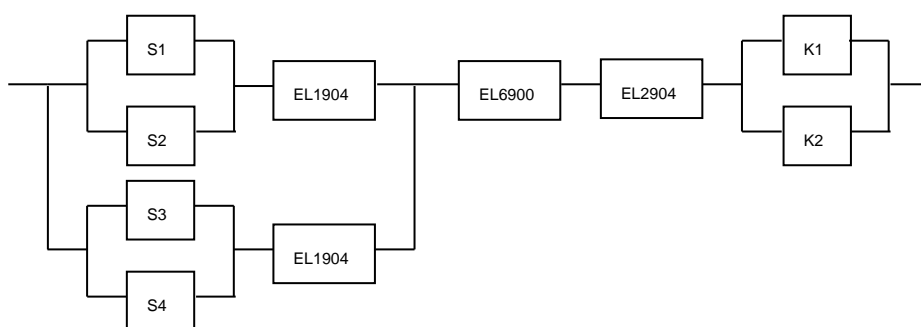
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

### EL2904 (applies to all EL2904 used)

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.10.2 Block formation and safety loops

### 2.10.2.1 Safety function 1



## 2.10.3 Calculation

### 2.10.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.10.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
S3/S4 with without testing / with plausibility	DC <sub>avg</sub> =90%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%

### 2.10.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{1000000}{0,1 * 14720} = 679,3y = 5951087h$$

**S2:**

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

$$MTTF_d = \frac{2000000}{0,1 \cdot 14720} = 1358,7y = 11902174h$$

**S3:**

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

$$MTTF_d = \frac{20000000}{0,1 \cdot 14720} = 13586,9y = 119021739h$$

**S4:**

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

$$MTTF_d = \frac{20000000}{0,1 \cdot 14720} = 13586,9y = 119021739h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 \cdot 21,90} = 883,2y = 7736413h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

$$PFH = \frac{1 - 0,99}{679,3 \cdot 8760} = 1,68E - 9$$

**S2:**

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

**S3/S4:**

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

**K1/K2:**

$$PFH = \frac{1 - 0,99}{883,2 \cdot 8760} = 1,29E - 9$$

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 switches S3/S4 are monitored for plausibility (temporal/logical) and are type A systems according to EN61508 (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 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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

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

Since the portions  $(1 - \beta)^2 * (PFH_{(S1 \setminus S2 \setminus EL1904)} * PFH_{(S3 \setminus S4 \setminus EL1904)}) * T1$  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:

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

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

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

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$



$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{833,2y}} = 177,3y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3} + \frac{99\%}{1358,7} + \frac{90\%}{13586,9} + \frac{90\%}{13586,9} + \frac{99\%}{1028,8} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{833,2} + \frac{99\%}{833,2}}{\frac{1}{679,3} + \frac{1}{1358,7} + \frac{1}{13586,9} + \frac{1}{13586,9} + \frac{1}{1028,8} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{833,2} + \frac{1}{833,2}} = 98,85\%$$

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

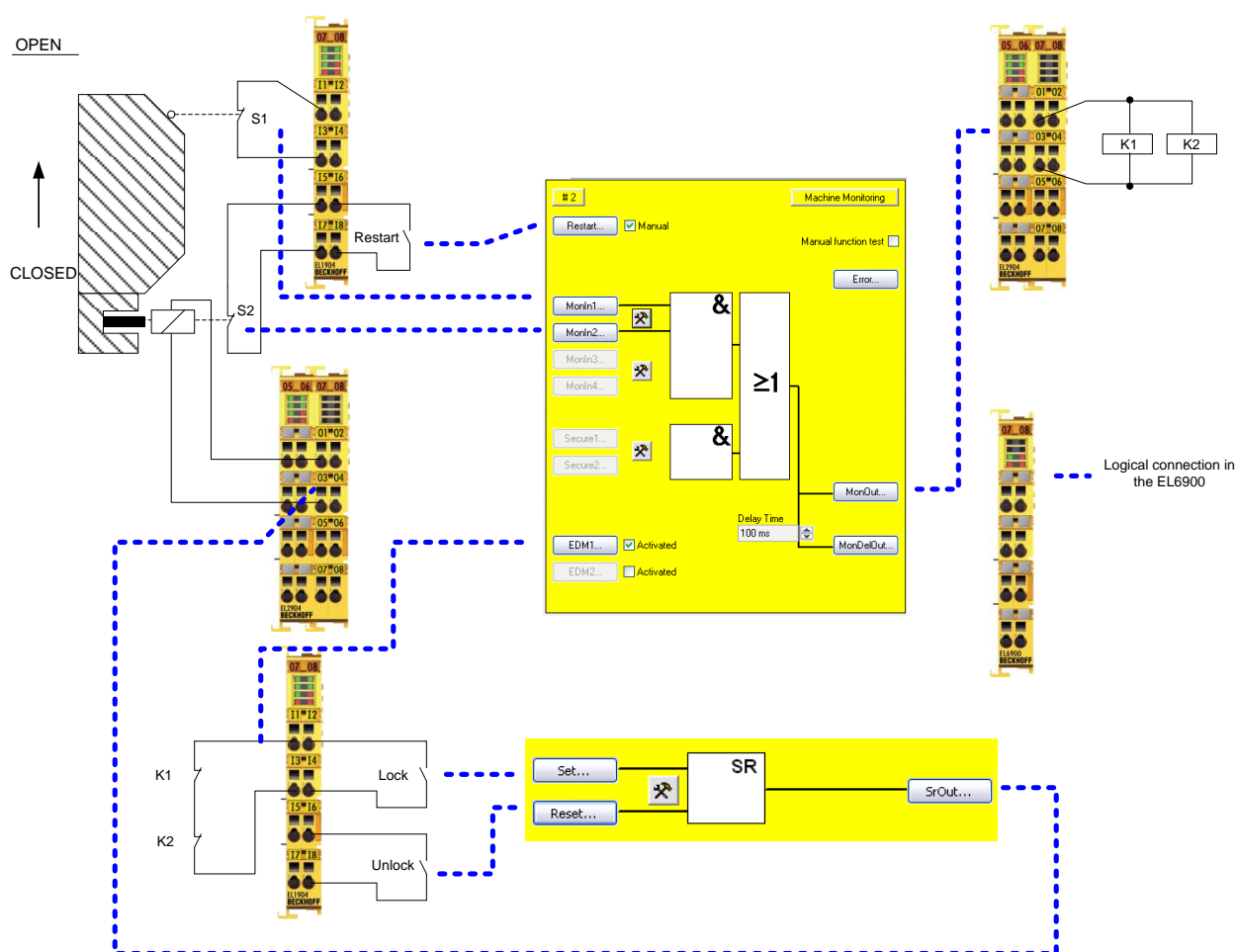
DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.	

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.11 Protective door function with guard lock (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 guard lock is switched via 2 safe inputs in which testing is active. Testing and current measurement is active on the safe output for the guard lock.



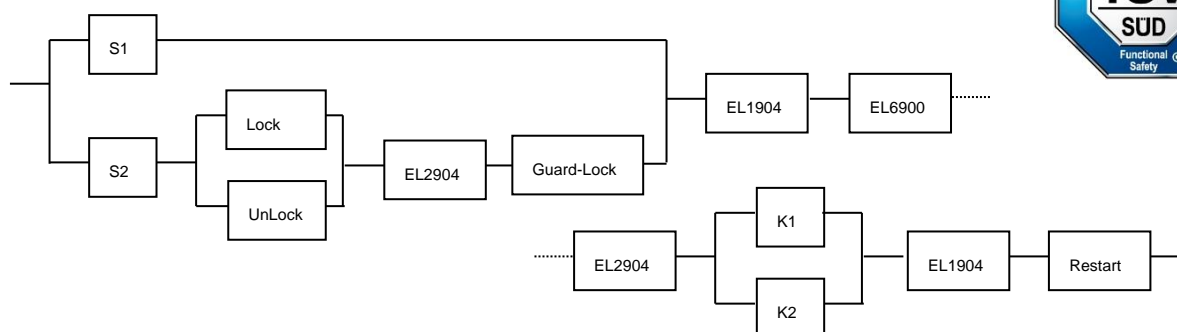
### 2.11.1 Parameters of the safe input and output terminals

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

**2.11.2 Block formation and safety loops****2.11.2.1 Safety function 1****2.11.3 Calculation****2.11.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

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

### 2.11.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing	DC <sub>avg</sub> =90%
S2 with testing and expectation	DC <sub>avg</sub> =99%
Lock/unlock with testing/plausibility	DC <sub>avg</sub> =99%
Restart	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%
Guard Lock	DC <sub>avg</sub> =99%

### 2.11.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{2000000}{0,1 * 14720} = 1358,7y = 11902174h$$

**S2:**

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

$$MTTF_d = \frac{2000000}{0,1 * 14720} = 1358,7y = 11902174h$$

**Lock/Unlock:**

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

$$MTTF_d = \frac{100000}{0,1 * 14720} = 67,9y = 595108h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 883,2y = 7736413h$$

**Restart:**

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

$$MTTF_d = \frac{10000000}{0,1 \cdot 14720} = 6793,5y = 59511060h$$

**Guard lock:**

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

$$MTTF_d = \frac{2000000}{0,1 \cdot 14720} = 1358,7y = 11902173h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

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

**S2:**

$$PFH = \frac{1 - 0,99}{1358,7 \cdot 8760} = 8,40E - 10$$

**Lock/Unlock:**

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

**Restart:**

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

**K1/K2:**

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

**Guard lock:**

$$PFH = \frac{1 - 0,99}{1358,7 \cdot 8760} = 8,40E - 10$$

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 B10d values for K1 and K2 are identical.

The guard lock 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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

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

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:

$$PFH_{(S2\backslash Lock\backslash Unlock\backslash EL2904\backslash Zuhaltung)} = PFH_{(S2)} + \beta * \frac{PFH_{(Lock)} + PFH_{(Unlock)}}{2} + PFH_{(EL2904)} + PFH_{(Zuhaltung)} \\ = 8,4E - 10 + 10\% * \frac{1,68E - 08 + 1,68E - 08}{2} + 1,25E - 09 + 8,4E - 10 = 4,61E - 09$$

$$PFH_{ges} = 10\% * \frac{4,61E - 09 + 8,4E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,29E - 09 + 1,29E - 09}{2} + 1,11E - 09 + 1,68E - 09 = 6,96E - 09$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S2|Lock|Unlock|EL2904|Guardlock)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(Restart)}$$

with:

$$MTTF_d(S1) = \frac{B10_d(S1)}{0,1 * n_{op}}$$

$$MTTF_d(S2) = \frac{B10_d(S2)}{0,1 * n_{op}}$$

$$MTTF_d(Lock) = \frac{B10_d(Lock)}{0,1 * n_{op}}$$

$$MTTF_d(Unlock) = \frac{B10_d(Unlock)}{0,1 * n_{op}}$$

$$MTTF_d(Guard lock) = \frac{B10_d(Guard lock)}{0,1 * n_{op}}$$

$$MTTF_d(K1) = \frac{B10_d(K1)}{0,1 * n_{op}}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_d(S2|Lock|Unlock|EL2904|Guard lock)$$

$$= \frac{1}{\frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(Lock)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(Guard lock)}}$$

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

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

$$DC_{avg} = \frac{\frac{99\%}{57,82} + \frac{99\%}{1358,7} + \frac{99\%}{67,9} + \frac{99\%}{67,9} + \frac{99\%}{913,2} + \frac{99\%}{1358,7} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{883,2} + \frac{99\%}{883,2} + \frac{99\%}{1028,8} + \frac{90\%}{6793,5}}{\frac{1}{57,82} + \frac{1}{1358,7} + \frac{1}{67,9} + \frac{1}{67,9} + \frac{1}{913,2} + \frac{1}{1358,7} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{883,2} + \frac{1}{883,2} + \frac{1}{1028,8} + \frac{1}{6793,5}} = 98,98\%$$

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

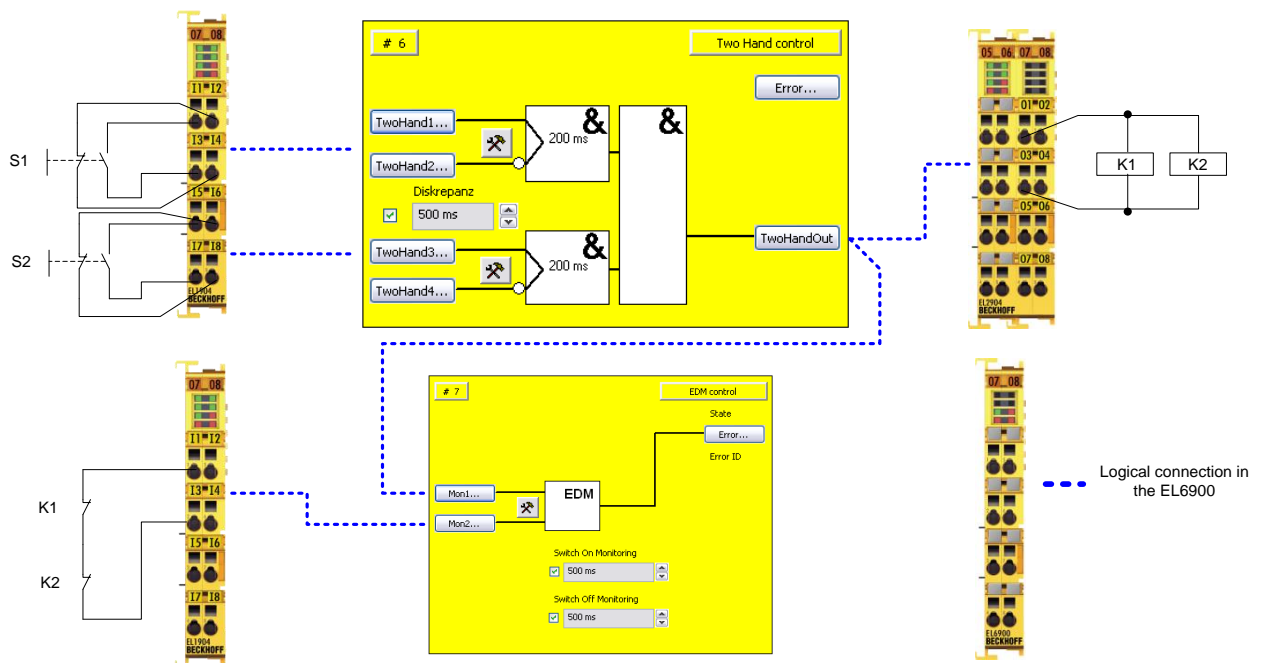
Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e



## 2.12 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.



### 2.12.1 Parameters of the safe input and output terminals

**EL1904 (applies to all EL1904 used)**

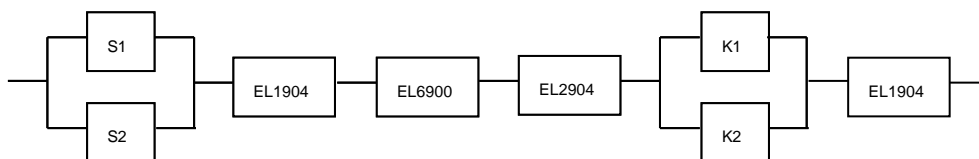
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

**EL2904**

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.12.2 Block formation and safety loops

### 2.12.2.1 Safety function 1



## 2.12.3 Calculation

### 2.12.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.12.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%

### 2.12.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 \cdot 16 \cdot 60}{1} = 220800$$

$$MTTF_d = \frac{20000000}{0,1 \cdot 220800} = 905,8y = 7934783h$$

**K1/K2:**

$$n_{op} = \frac{230 \cdot 16 \cdot 60}{1} = 220800$$

$$MTTF_d = \frac{1300000}{0,1 \cdot 220800} = 58,9y = 515760h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1/S2:**

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

**K1/K2:**

$$PFH = \frac{1 - 0,99}{58,9 \cdot 8760} = 1,93E - 8$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{1,26E - 09 + 1,26E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% \\ * \frac{1,93E - 08 + 1,93E - 08}{2} + 1,11E - 09 = 6,56E - 09$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} \\ + \frac{1}{MTTF_d(EL1904)}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

**Note****Category**

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

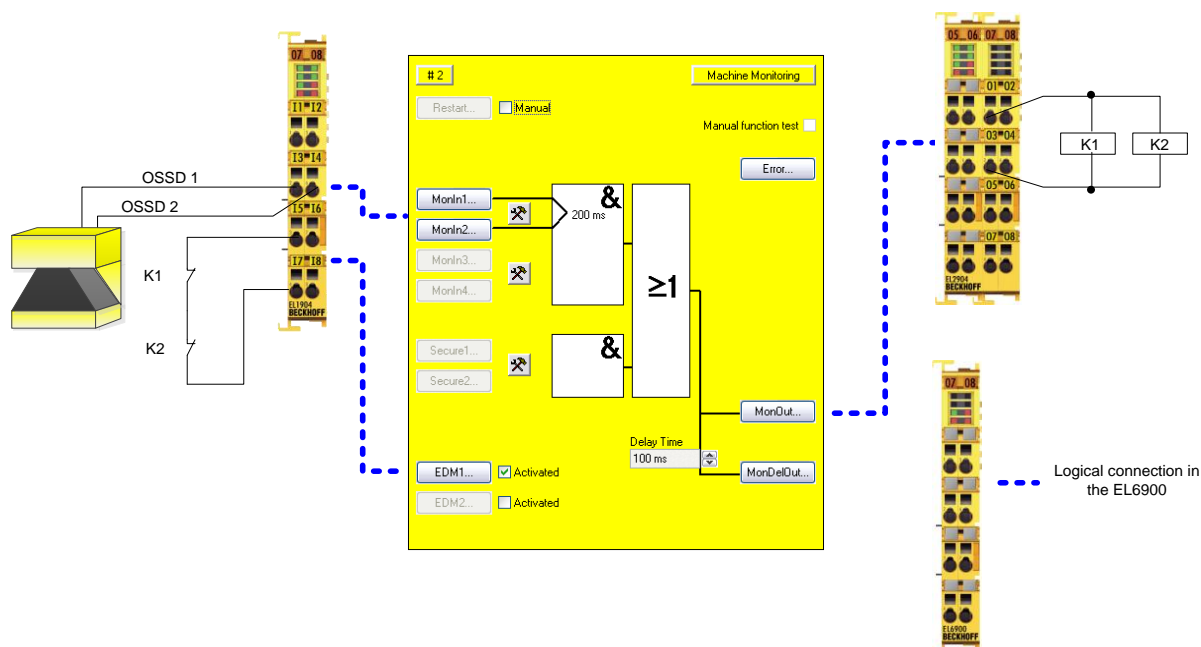
Designation for each channel	MTTF <sub>d</sub>	Range for each channel
low		3 years ≤ MTTF <sub>d</sub> < 10 years
medium		10 years ≤ MTTF <sub>d</sub> < 30 years
high		30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>	Range
none		DC < 60 %
low		60 % ≤ DC < 90 %
medium		90 % ≤ DC < 99 %
high		99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.13 Laser scanner (Category 3, PL d)

The laser scanner has two OSSD outputs (Output Signal Switching Device), which are wired to safe inputs of a 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.



### 2.13.1 Parameters of the safe input and output terminals

#### EL1904 (applies to all EL1904 used)

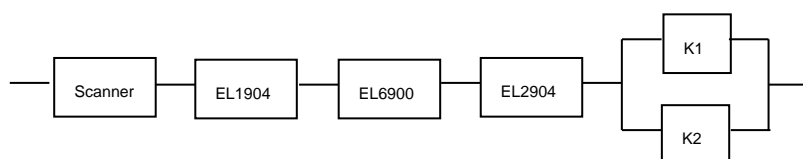
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	OSSD any pulse repetition
Logic channel 3 and 4	Single Logic

#### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.13.2 Block formation and safety loops

### 2.13.2.1 Safety function 1



## 2.13.3 Calculation

### 2.13.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.13.3.2 Diagnostic Coverage DC

Component	Value
OSSD1/2 with testing (by scanner) / plausibility	DC <sub>avg</sub> =90%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%

### 2.13.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 \cdot 16 \cdot 60}{10} = 22080$$

$$MTTF_d = \frac{1300000}{0,1 \cdot 22080} = 588,7y = 5157012h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**K1/K2:**

$$PFH = \frac{1 - 0,99}{588,7 \cdot 8760} = 1,94E - 9$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

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

Since the portion  $(1 - \beta)^2 \cdot (PFH_{(K1)} \cdot PFH_{(K2)}) \cdot T1$  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:

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



The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(Scanner)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

with:

$$MTTF_d(K1) = \frac{B10_d(K1)}{0,1 * n_{op}}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_d(Scanner) = \frac{(1 - DC(Scanner))}{PFH(Scanner)} = \frac{(1 - 0,90)}{7,67E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{6,72E - 04 \frac{1}{y}} = 148,8y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{148,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{588,7y}} = 87,8y$$

$$DC_{avg} = \frac{\frac{90\%}{148,8} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{588,7} + \frac{99\%}{588,7}}{\frac{1}{148,8} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{588,7} + \frac{1}{588,7}} = 94,38\%$$

**Note****Category**

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

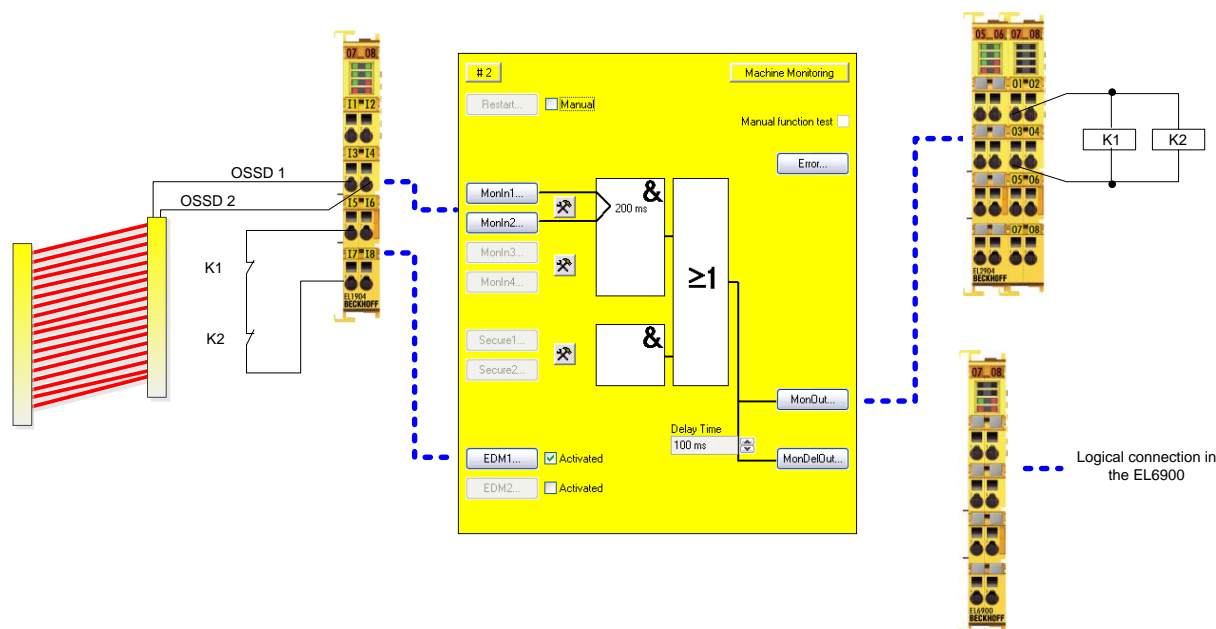
MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
<b>medium</b>	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.14 Light grid (Category 4, PL e)

The light grid 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.



### 2.14.1 Parameters of the safe input and output terminals

#### EL1904

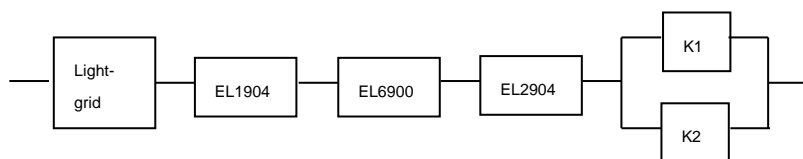
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Asynchronous evaluation OSSD
Logic channel 3 and 4	Single Logic

#### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.14.2 Block formation and safety loops

### 2.14.2.1 Safety function 1



## 2.14.3 Calculation

### 2.14.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

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

### 2.14.3.2 Diagnostic Coverage DC

Component	Value
OSSD1/2 with testing (by light grid) / plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%

### 2.14.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 \cdot 16 \cdot 60}{5} = 44160$$

$$MTTF_d = \frac{1300000}{0,1 \cdot 44160} = 294,4y = 2578944h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**K1/K2:**

$$PFH = \frac{1 - 0,99}{294,4 \cdot 8760} = 3,88E - 9$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

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

Since the portion  $(1 - \beta)^2 \cdot (PFH_{(K1)} \cdot PFH_{(K2)}) \cdot T1$  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:

$$PFH_{ges} = 1,50E - 08 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% \cdot \frac{3,88E - 09 + 3,88E - 09}{2} = 1,88E - 08$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d (Light grid)} + \frac{1}{MTTF_d (EL1904)} + \frac{1}{MTTF_d (EL6900)} + \frac{1}{MTTF_d (EL2904)} + \frac{1}{MTTF_d (K1)}$$

with:

$$MTTF_d(K1) = \frac{B10_d(K1)}{0,1 * n_{op}}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_d(Light grid) = \frac{(1 - DC(Light grid))}{PFH(Light grid)} = \frac{(1 - 0,99)}{1,50E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,31E - 04 \frac{1}{y}} = 76,1y$$

$$MTTF_{d ges} = \frac{1}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{294,4y}} = 51,3y$$

$$DC_{avg} = \frac{\frac{99\%}{76,1} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{588,7} + \frac{99\%}{294,4}}{\frac{1}{76,1} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{588,7} + \frac{1}{294,4}} = 99,0\%$$

**Category**

This structure is possible up to category 4 at the most through the use of the type 4 (category 4) light grid.

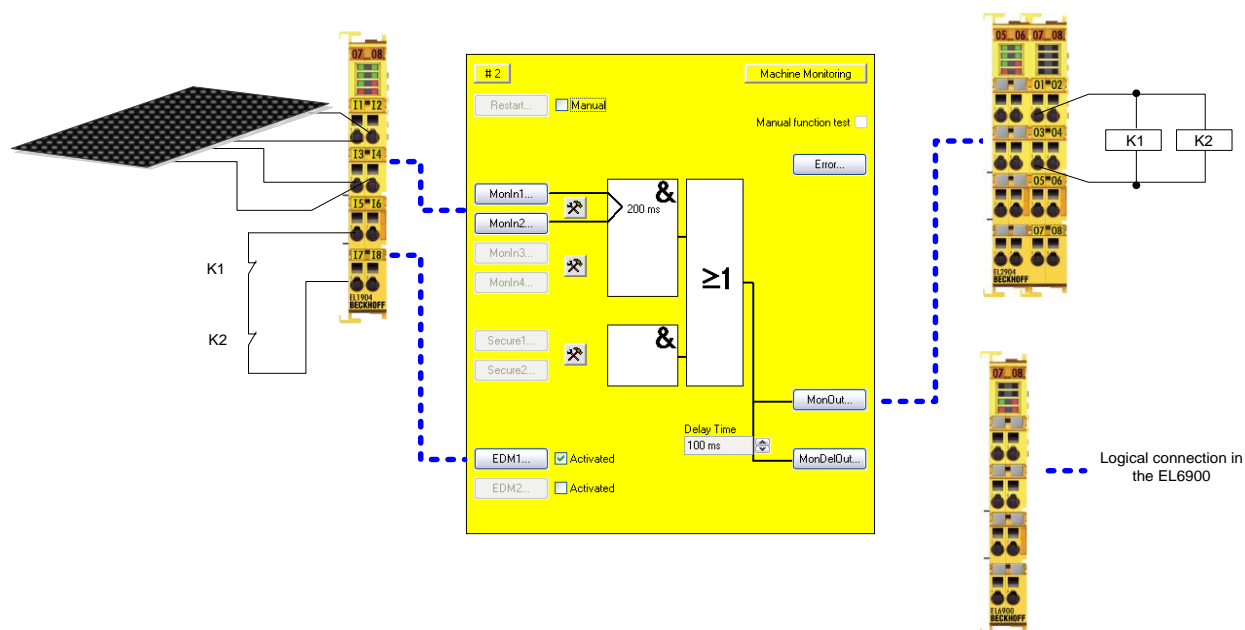
Designation for each channel	MTTF <sub>d</sub>	Range for each channel
low		3 years ≤ MTTF <sub>d</sub> < 10 years
medium		10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>		30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>	Range
none		DC < 60 %
low		60 % ≤ DC < 90 %
medium		90 % ≤ DC < 99 %
<b>high</b>		99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.15 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.



### 2.15.1 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

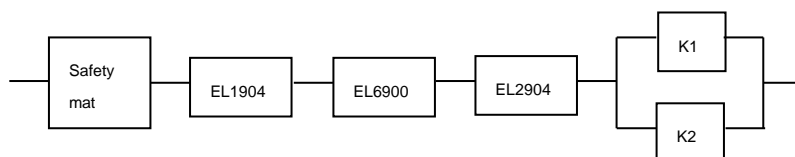
#### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes



## 2.15.2 Block formation and safety loops

### 2.15.2.1 Safety function 1



## 2.15.3 Calculation

### 2.15.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
Switching mat – B10 <sub>d</sub>	6.00E06
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	1 (1x per minute)
Lifetime (T1)	20 years = 175200 hours

### 2.15.3.2 Diagnostic Coverage DC

Component	Value
Switching outputs (mat) with testing/plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%

### 2.15.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 \cdot 16 \cdot 60}{1} = 220800$$

$$MTTF_d = \frac{1300000}{0,1 \cdot 220800} = 58,9y = 515761h$$

**Switching mat:**

$$n_{op} = \frac{230 \cdot 16 \cdot 60}{1} = 220800$$

$$MTTF_d = \frac{6,00E06}{0,1 \cdot 220800} = 271,7y = 2380434h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**K1/K2:**

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

**Switching mat:**

$$PFH = \frac{1 - 0,99}{271,7 \cdot 8760} = 4,20E - 09$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

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

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:

$$PFH_{ges} = 4,20E - 09 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 08 + 1,94E - 08}{2} = 9,53E - 09$$

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

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(Switching mat)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

with:

$$MTTF_d(K1) = \frac{B10_d(K1)}{0,1 * n_{op}}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{271,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y}} = 42,3y$$

$$DC_{avg} = \frac{\frac{99\%}{271,7} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{58,9} + \frac{99\%}{58,9}}{\frac{1}{271,7} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{58,9} + \frac{1}{58,9}} = 99,0\%$$

**Note****Category**

Category 4 is attainable due to the structure of the circuit.

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

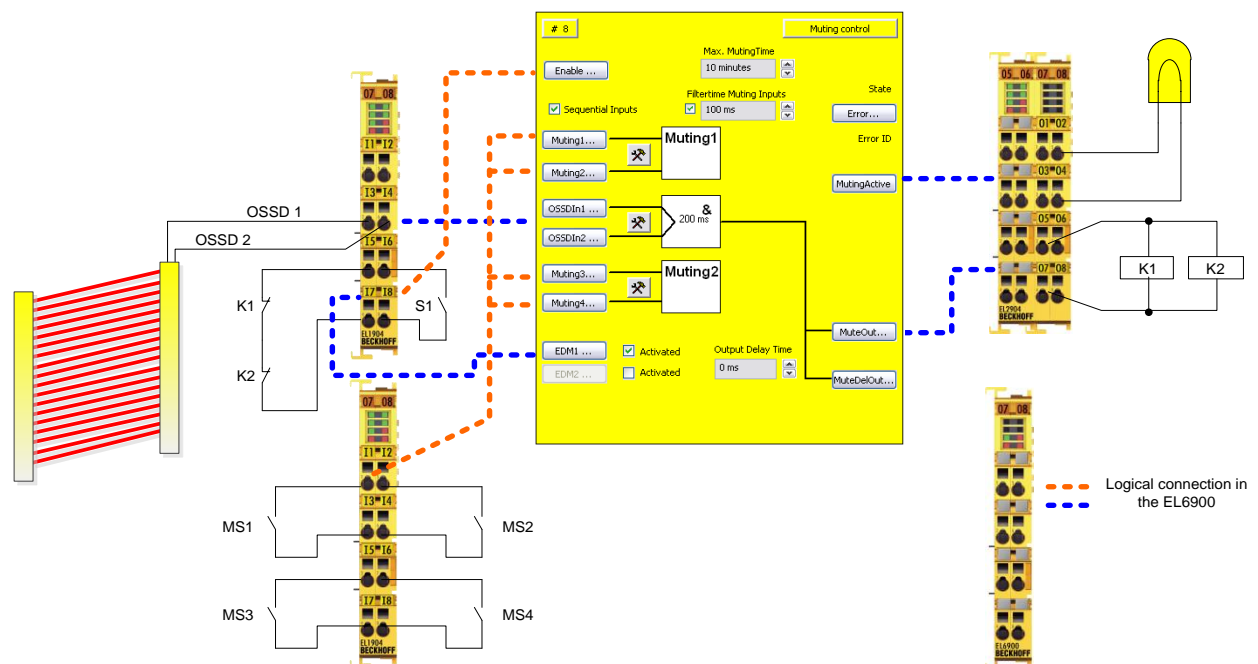
DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.16 Muting (Category 4, PL e)

The light grid 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.



### 2.16.1 Parameters of the safe input and output terminals

#### EL1904 (upper terminal on the drawing)

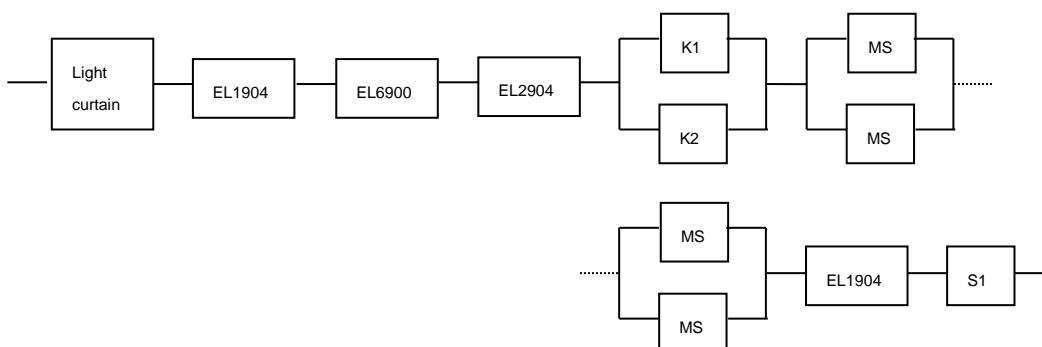
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Asynchronous evaluation OSSD
Logic channel 3 and 4	Single Logic

#### 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

**2.16.2 Block formation and safety loops****2.16.2.1 Safety function 1****2.16.3 Calculation****2.16.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
S1 – B10 <sub>d</sub>	100,000
Light curtain – PFH <sub>d</sub>	1.50E-08
MS1 – B10 <sub>d</sub>	100,000
MS2 – B10 <sub>d</sub>	100,000
MS3 – B10 <sub>d</sub>	100,000
MS4 – B10 <sub>d</sub>	100,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

### 2.16.3.2 Diagnostic Coverage DC

Component	Value
OSSD1/2 with testing (by light curtain) / plausibility	DC <sub>avg</sub> =99%
MS1/2/3/4 with testing/plausibility	DC <sub>avg</sub> =90%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%
S1 with testing	DC <sub>avg</sub> =90%

### 2.16.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_d = \frac{100000}{0,1 * 1840} = 543,5y = 4761060h$$

**K1/K2:**

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_d = \frac{1300000}{0,1 * 1840} = 7065,2y = 61891152h$$

**MS1/MS2/MS3/S4:**

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_d = \frac{100000}{0,1 * 1840} = 543,5y = 4761060h$$

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:**

$$PFH = \frac{1 - 0,90}{543,5 * 8760} = 2,10E - 8$$

**K1/K2:**

$$PFH = \frac{1 - 0,99}{7065,2 * 8760} = 1,62E - 10$$

**MS1/MS2/MS3/S4:**

$$PFH = \frac{1 - 0,90}{543,5 * 8760} = 2,10E - 8$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

$$\begin{aligned} PFH_{ges} = & PFH_{(Lichtvorhang)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} \\ & + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(MS1)} + PFH_{(MS2)}}{2} \\ & + (1 - \beta)^2 * (PFH_{(MS1)} * PFH_{(MS2)}) * T1 + \beta * \frac{PFH_{(MS3)} + PFH_{(MS4)}}{2} \\ & + (1 - \beta)^2 * (PFH_{(MS3)} * PFH_{(MS4)}) * T1 + PFH_{(EL1904)} + PFH_{(S1)} \end{aligned}$$

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:

$$\begin{aligned} PFH_{ges} = & 1,50E - 08 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,62E - 10 + 1,62E - 10}{2} + 10\% \\ & * \frac{2,10E - 08 + 2,10E - 08}{2} + 10\% * \frac{2,10E - 08 + 2,10E - 08}{2} + 1,11E - 09 + 2,10E - 08 \\ = & 4,47E - 08 \end{aligned}$$



The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(Light\ curtain)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(MS1)} + \frac{1}{MTTF_d(MS3)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(S1)}$$

with:

$$MTTF_d(K1) = \frac{B10_d(K1)}{0,1 * n_{op}}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_d(Light\ Curtain) = \frac{(1 - DC(Light\ Curtain))}{PFH(Light\ Curtain)} = \frac{(1 - 0,99)}{1,50E - 08 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,31E - 04 \frac{1}{y}} = 76,1y$$

$$MTTF_d(MS1/MS3) = \frac{(1 - DC(MS1/MS3))}{PFH(MS1/MS3)} = \frac{(1 - 0,90)}{2,10E - 8 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{1,84E - 04 \frac{1}{y}} = 543,6y$$

$$MTTF_{d ges} = \frac{1}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{7065,2y} + \frac{1}{543,6y} + \frac{1}{543,6y} + \frac{1}{1028,8y} + \frac{1}{543,5y}} = 44,0y$$

$$DC_{avg} = \frac{\frac{99\%}{76,1} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{7065,2} + \frac{99\%}{7065,2} + \frac{90\%}{543,6} + \frac{90\%}{543,6} + \frac{90\%}{543,6} + \frac{90\%}{543,6} + \frac{99\%}{1028,8} + \frac{99\%}{543,5}}{\frac{1}{76,1} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{7065,2} + \frac{1}{7065,2} + \frac{1}{543,6} + \frac{1}{543,6} + \frac{1}{543,6} + \frac{1}{543,6} + \frac{1}{1028,8} + \frac{1}{543,5}} = 96,51\%$$

**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 <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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

## 2.17 All-pole disconnection of a potential group with downstream non-reactive 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 (24V 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) is always 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.



**Attention**

### 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**

### Non-reactive standard bus terminals

You can find a list of non-reactive bus terminals in the Beckhoff Information System under <http://infosys.beckhoff.com>.

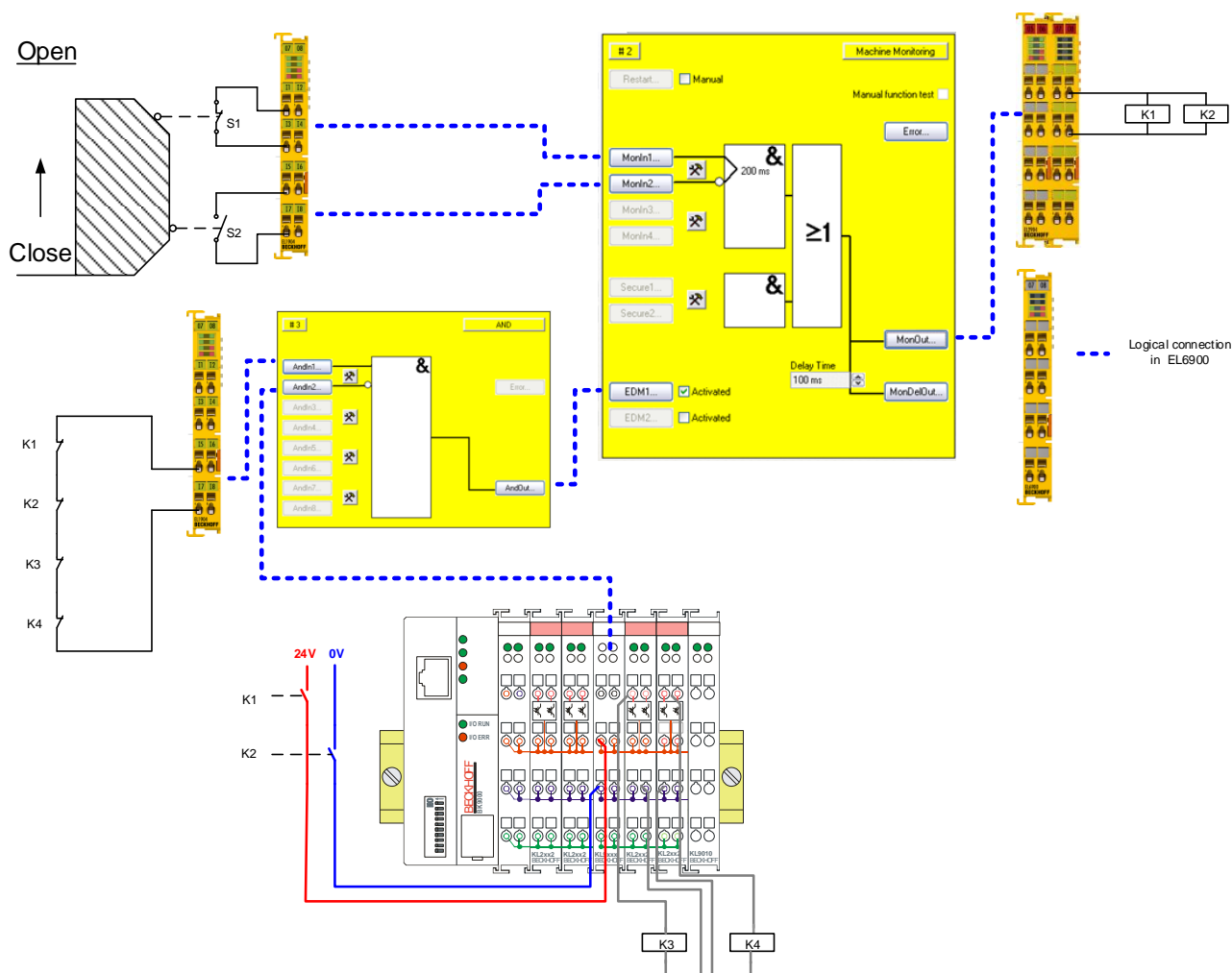
**Attention****Maximum attainable safety level**

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

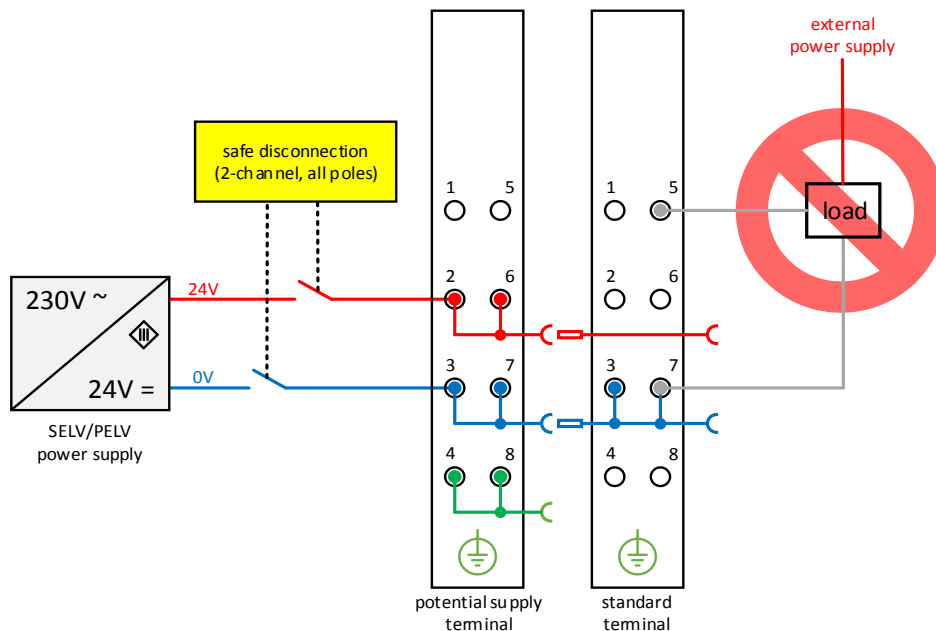
**CAUTION****Time delay**

By switching off the voltage supply of the potential group, the shutdown of the downstream contactors and actuators may be delayed. This delay depends on the downstream actuators, loads and cables and has to be considered by the user in the safety analysis.

## 2.17.1 Notes on prevention of feedback

### 2.17.1.1 No switching of loads with a separate power supply

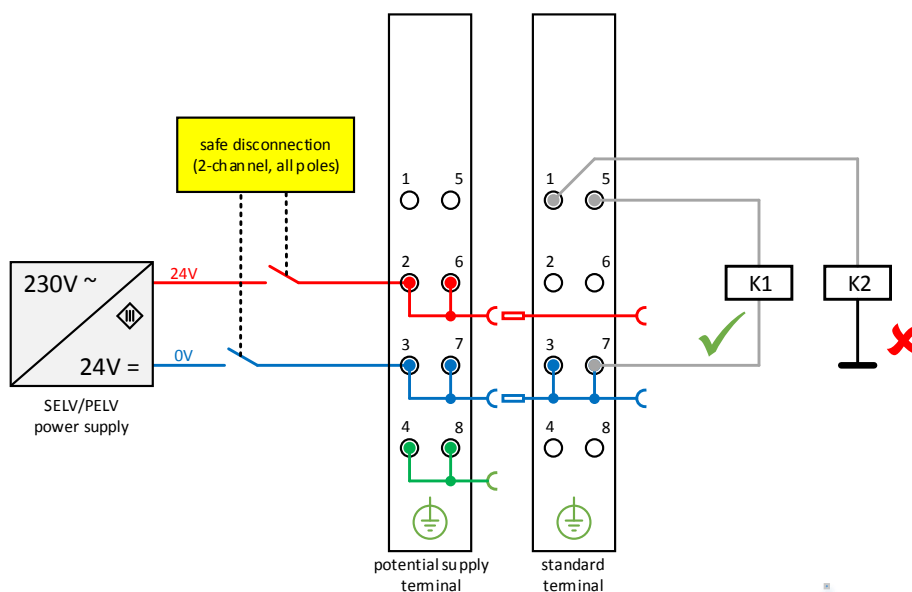
Loads that have their own power supply must not be switched by standard terminals, since in this case feedback via the load cannot be ruled out.



Exceptions to the general requirement are allowed only if the manufacturer of the connected load guarantees that feedback to the control input cannot occur.

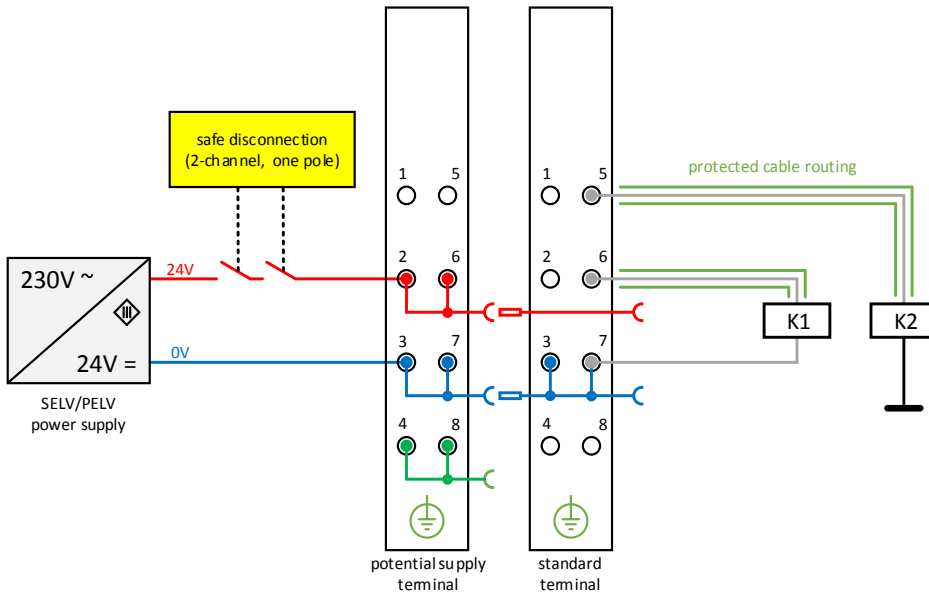
### 2.17.1.2 Option 1: Ground feedback and all-pole disconnection (used in this example)

The ground connection of the connected load must be fed back to the safely switched ground of the respective output terminal or potential group. (In this case: K1 – correct wiring, K2 – incorrect wiring)



### 2.17.1.3 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 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.



Alternative1: Load connection via separate sheathed cables

The non-safely switched potential of the standard terminal may not be conducted together with other potential-conducting cores inside the same sheathed cable.

Alternative2: 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.

Alternative3: Dedicated earth connection per conductor

All conductors connected to the non-safe standard terminals are protected by a separate ground connection.

## 2.17.2 Parameters of the safe input and output terminals

### EL1904 (applies to all EL1904 used)

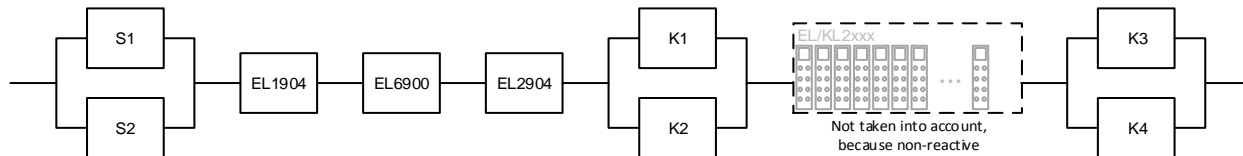
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.17.3 Block formation and safety loops

### 2.17.3.1 Safety function 1



## 2.17.4 Calculation

### 2.17.4.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
S1 – B10 <sub>d</sub>	1,000,000
S2 – B10 <sub>d</sub>	2,000,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
K3 – B10 <sub>d</sub>	1,300,000
K4 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>cycle</sub> )	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

### 2.17.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%
K3/K4 with EDM	DC <sub>avg</sub> =90%



### 2.17.4.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{1000000}{0,1 * 7360} = 1358,7y = 11902212h$$

**S2:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{2000000}{0,1 * 7360} = 2717,4y = 23804424h$$

**K1/K2/K3/K4:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{1300000}{0,1 * 7360} = 1766,3y = 15472788h$$

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:**

$$PFH = \frac{1 - 0,90}{1766,3 * 8760} = 6,46E - 9$$

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 B10d 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{8,40E - 10 + 4,20E - 10}{2} + 1,11E - 9 + 1,03E - 9 + 1,25E - 9 \\ + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} + 10\% * \frac{6,46E - 9 + 6,46E - 9}{2} = 4,16E - 9$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(K3)}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 206,7y$$

$$DC_{avgs} = \frac{\frac{DC}{MTTF_d(S1)} + \frac{DC}{MTTF_d(S2)} + \frac{DC}{MTTF_d(EL1904)} + \frac{DC}{MTTF_d(EL6900)} + \frac{DC}{MTTF_d(EL2904)} + \frac{DC}{MTTF_d(K1)} + \frac{DC}{MTTF_d(K2)} + \frac{DC}{MTTF_d(K3)} + \frac{DC}{MTTF_d(K4)}}{\frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(K2)} + \frac{1}{MTTF_d(K3)} + \frac{1}{MTTF_d(K4)}}$$

$$DC_{avgs} = \frac{\frac{0,99}{1358,7} + \frac{0,99}{2717,4} + \frac{0,99}{1028,8} + \frac{0,99}{1108,6} + \frac{0,99}{913,2} + \frac{0,99}{1766,3} + \frac{0,99}{1766,3} + \frac{0,90}{1766,3} + \frac{0,90}{1766,3}}{\frac{1}{1358,7} + \frac{1}{2717,4} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{1766,3} + \frac{1}{1766,3} + \frac{1}{1766,3} + \frac{1}{1766,3}} = 0,9739 = 97,39\%$$

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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 Tab. 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH <sub>D</sub> )
3	≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.18 Single-pole disconnection of a potential group with downstream non-reactive 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. The testing of the inputs is active and the signals are tested for discrepancy (here 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 feedback signals from 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 NO 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 used must be at the same potential.



**Note**

### Safety consideration

The EL/KL9xxx 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 24V by an SELV/PELV power supply unit with an output voltage limit  $U_{max}$  of 60 V in the event of a fault.



**Attention**

### 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**

### Non-reactive standard bus terminals

You can find a list of non-reactive bus terminals in the Beckhoff Information System under <http://infosys.beckhoff.com>.



## Attention

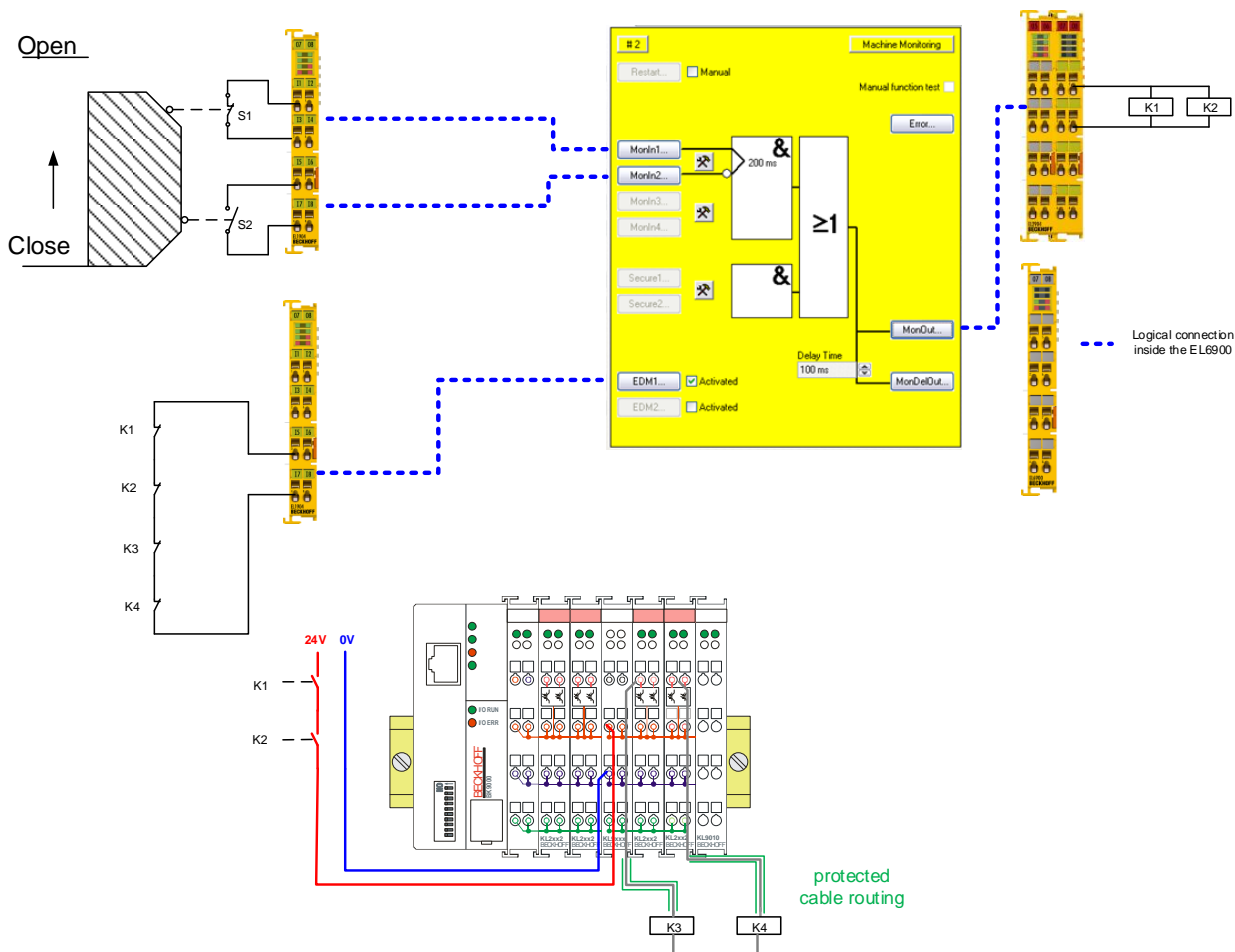
## Maximum attainable safety level

Avoiding feedback through short-circuit fault elimination:

DIN EN ISO 13849-1: max. cat. 4 PL e

IEC 61508: max. SIL3

EN 62061: max. SIL2



## Attention

## Fault exclusion

Due to the fault exclusion "cable short circuit" in the wiring from the non-reactive standard output terminals EL/KL2xxx to the load (here K3, K4), a power supply terminal with diagnostic function is not required anymore. Thus potential supply terminals of type EL/KL9xxx can be used.

The 0 V potentials of the load (here K3, K4) must be identical to the 0 V potential of the voltage supply of the potential group.



**CAUTION**

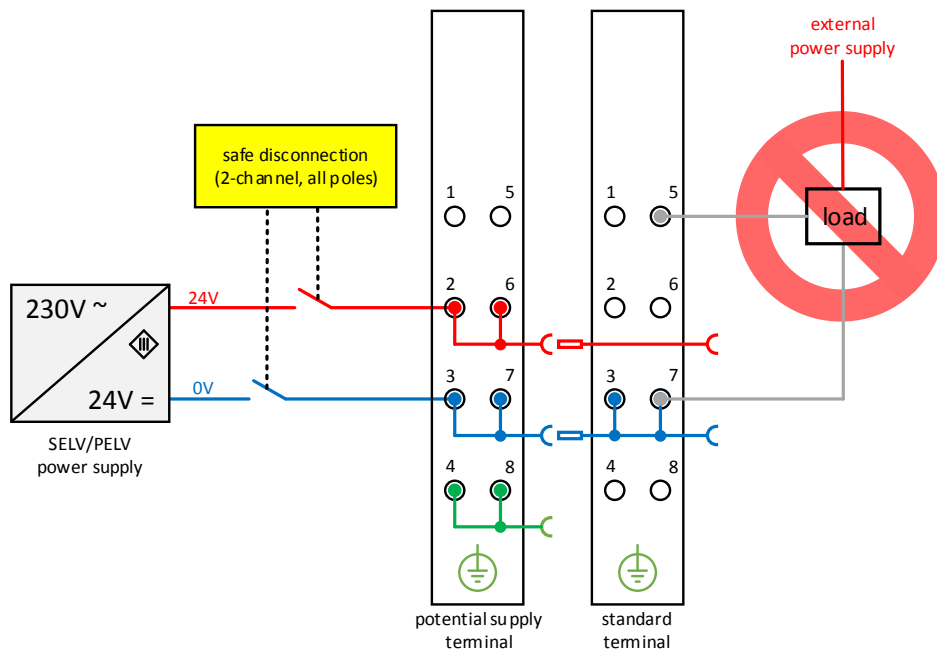
### Time delay

By switching off the voltage supply of the potential group, the shutdown of the downstream contactors and actuators may be delayed. This delay depends on the downstream actuators, loads and cables and has to be considered by the user in the safety analysis.

## 2.18.1 Notes on prevention of feedback

### 2.18.1.1 No switching of loads with a separate power supply

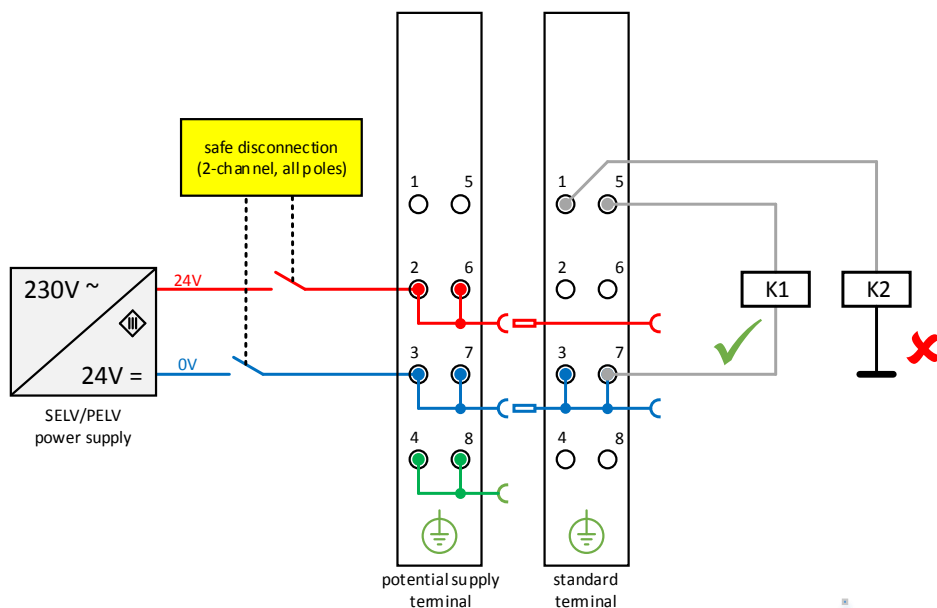
Loads that have their own power supply must not be switched by standard terminals, since in this case feedback via the load cannot be ruled out.



Exceptions to the general requirement are allowed only if the manufacturer of the connected load guarantees that feedback to the control input cannot occur.

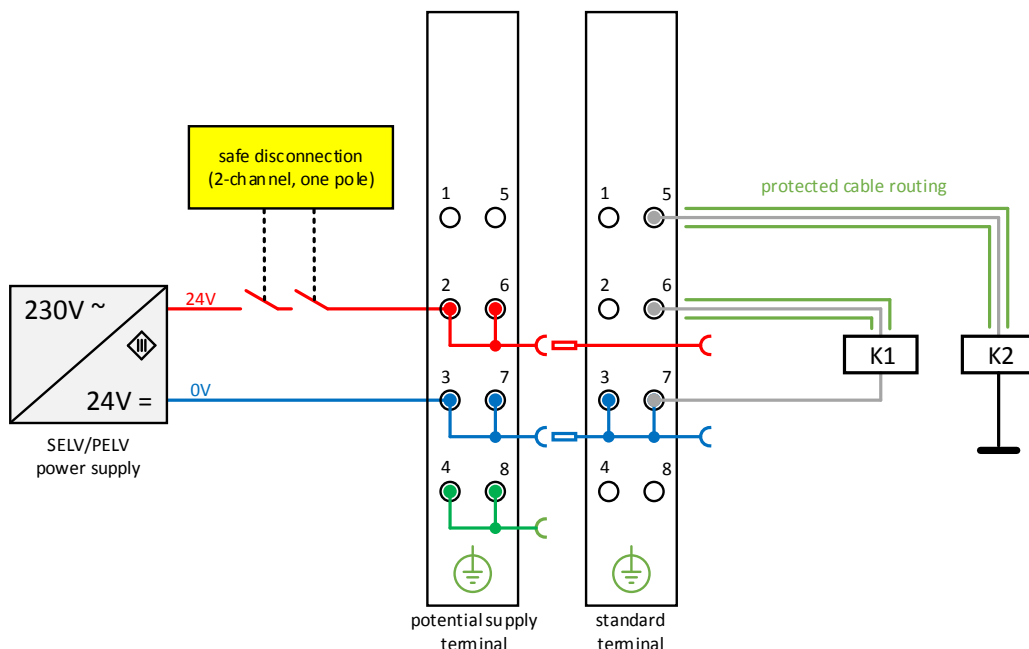
### 2.18.1.2 Option 1: Ground feedback and all-pole disconnection

The ground connection of the connected load must be fed back to the safely switched ground of the respective output terminal or potential group. (In this case: K1 – correct wiring, K2 – incorrect wiring)



### 2.18.1.3 Option 2: Cable short-circuit error exclusion (used here in the 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 cores 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: Cable permanently (fixed) installed and protected against external damage.

All conductors connected to the non-safe standard terminals are permanently fixed and, e.g. protected against external damage by a cable duct or armored pipe.



#### Fault exclusion

The machine manufacturer or the user is solely responsible for the correct execution and evaluation of the applied alternatives.



## 2.18.2 Parameters of the safe input and output terminals

### EL1904 (applies to all EL1904 used)

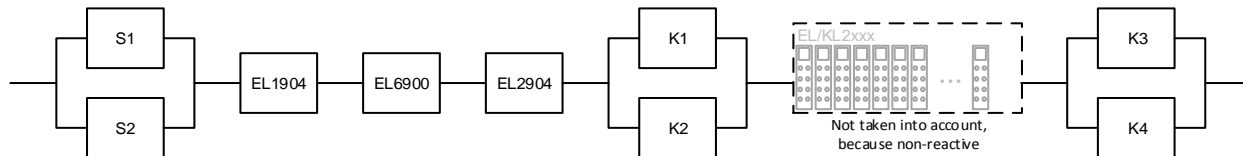
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.18.3 Block formation and safety loops

### 2.18.3.1 Safety function 1



## 2.18.4 Calculation

### 2.18.4.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
S1 – B10 <sub>d</sub>	1,000,000
S2 – B10 <sub>d</sub>	2,000,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
K3 – B10 <sub>d</sub>	1,300,000
K4 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

### 2.18.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
K1/K2 with testing and EDM	DC <sub>avg</sub> =99%
K3/K4 with EDM	DC <sub>avg</sub> =90%

### 2.18.4.3 Calculation for safety function 1

Calculation of the PFH 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:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{1000000}{0,1 * 7360} = 1358,7y = 11902212h$$

**S2:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{2000000}{0,1 * 7360} = 2717,4y = 23804424h$$

**K1/K2/K3/K4:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{1300000}{0,1 * 7360} = 1766,3y = 15472788h$$

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:**

$$PFH = \frac{1 - 0,90}{1766,3 * 8760} = 6,46E - 9$$

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 B10d 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{8,40E - 10 + 4,20E - 10}{2} + 1,11E - 9 + 1,03E - 9 + 1,25E - 9 \\ + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} + 10\% * \frac{6,46E - 9 + 6,46E - 9}{2} = 4,16E - 9$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(K3)}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{d ges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 206,7y$$

$$DC_{avgs} = \frac{\frac{DC}{MTTF_d(S1)} + \frac{DC}{MTTF_d(S2)} + \frac{DC}{MTTF_d(EL1904)} + \frac{DC}{MTTF_d(EL6900)} + \frac{DC}{MTTF_d(EL2904)} + \frac{DC}{MTTF_d(K1)} + \frac{DC}{MTTF_d(K2)} + \frac{DC}{MTTF_d(K3)} + \frac{DC}{MTTF_d(K4)}}{\frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(K2)} + \frac{1}{MTTF_d(K3)} + \frac{1}{MTTF_d(K4)}}$$

$$DC_{avgs} = \frac{\frac{0,99}{1358,7} + \frac{0,99}{2717,4} + \frac{0,99}{1028,8} + \frac{0,99}{1108,6} + \frac{0,99}{913,2} + \frac{0,99}{1766,3} + \frac{0,99}{1766,3} + \frac{0,90}{1766,3} + \frac{0,90}{1766,3}}{\frac{1}{1358,7} + \frac{1}{2717,4} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{1766,3} + \frac{1}{1766,3} + \frac{1}{1766,3} + \frac{1}{1766,3}} = 0,9739 = 97,39\%$$

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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

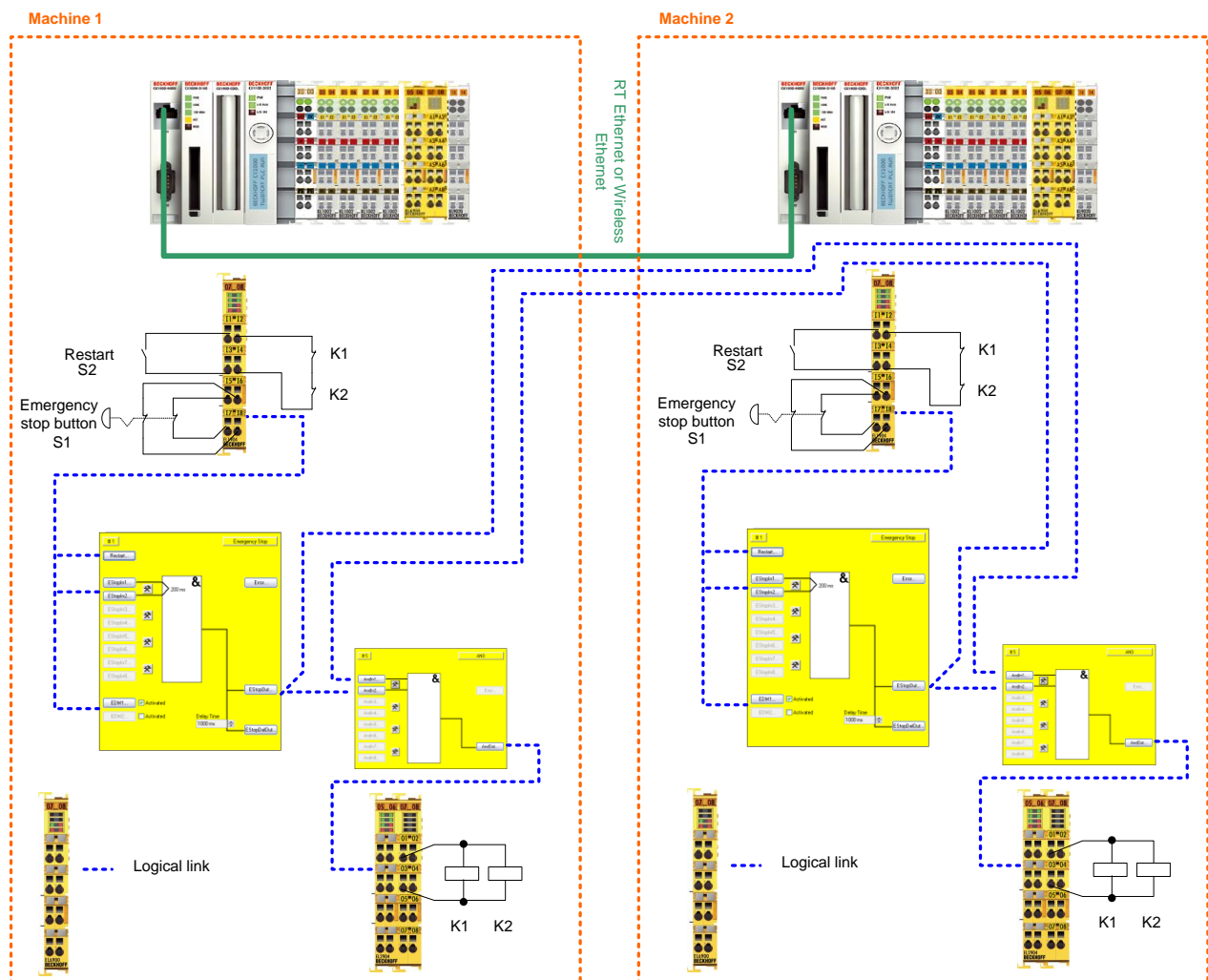
Safety integrity level according to Tab. 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH <sub>D</sub> )
3	≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2 (*)	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

(\*) In accordance with EN62061 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.

## 2.19 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.



### Start / restart

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.

**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.

## 2.19.1 Parameters of the safe input and output terminals

### EL1904 (applies to all EL1904 used)

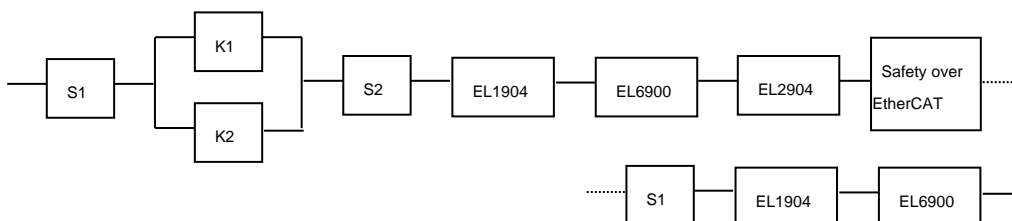
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.19.2 Block formation and safety loops

### 2.19.2.1 Safety function 1





## 2.19.3 Calculation

### 2.19.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
Safety over EtherCAT (FSOE)	1.00E-09
S1 – B10 <sub>d</sub>	1,000,000
S2 – B10 <sub>d</sub>	2,000,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

### 2.19.3.2 Diagnostic Coverage DC

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

### 2.19.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_d = \frac{1000000}{0,1 * 7360} = 1358,7y = 11902212h$$

**S2:**

$$n_{op} = \frac{230 \cdot 8 \cdot 60}{15} = 7360$$

$$MTTF_d = \frac{2000000}{0,1 \cdot 7360} = 2717,4y = 23804424h$$

**K1/K2:**

$$n_{op} = \frac{230 \cdot 8 \cdot 60}{15} = 7360$$

$$MTTF_d = \frac{1300000}{0,1 \cdot 7360} = 1766,3y = 15472788h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

$$PFH = \frac{1 - 0,99}{1358,7 \cdot 8760} = 8,40E - 10$$

**S2:**

$$PFH = \frac{1 - 0,90}{2717,4 \cdot 8760} = 4,20E - 09$$

**K1/K2:** actuation 1x per shift and direct feedback

$$PFH = \frac{1 - 0,99}{1766,3 \cdot 8760} = 6,46E - 10$$

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 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 8,40E - 10 + 10\% * \frac{6,46E - 10 + 6,46E - 10}{2} + 4,20E - 09 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 1,00E - 9 + 8,40E - 10 + 1,11E - 09 + 1,03E - 09 = \mathbf{1,25E - 08}$$

The MTTF<sub>d</sub> value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(S2)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(FSOE)} + \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_d(FSoE) = \frac{(1 - DC(FSoE))}{PFH(FSoE)} = \frac{(1 - 0,99)}{1,00E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{8,76E - 06 \frac{1}{y}} = 1141,6y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1766,3y} + \frac{1}{2717,4y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1358,7y} + \frac{1}{1141,6y} + \frac{1}{1028,8y} + \frac{1}{1108,6y}} = 123,1y$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7} + \frac{99\%}{1766,3} + \frac{99\%}{1766,3} + \frac{90\%}{2717,4} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{1358,7} + \frac{99\%}{1141,6} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6}}{\frac{1}{1358,7} + \frac{1}{1766,3} + \frac{1}{1766,3} + \frac{1}{2717,4} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{1358,7} + \frac{1}{1141,6} + \frac{1}{1028,8} + \frac{1}{1108,6}} = 98,99\%$$

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

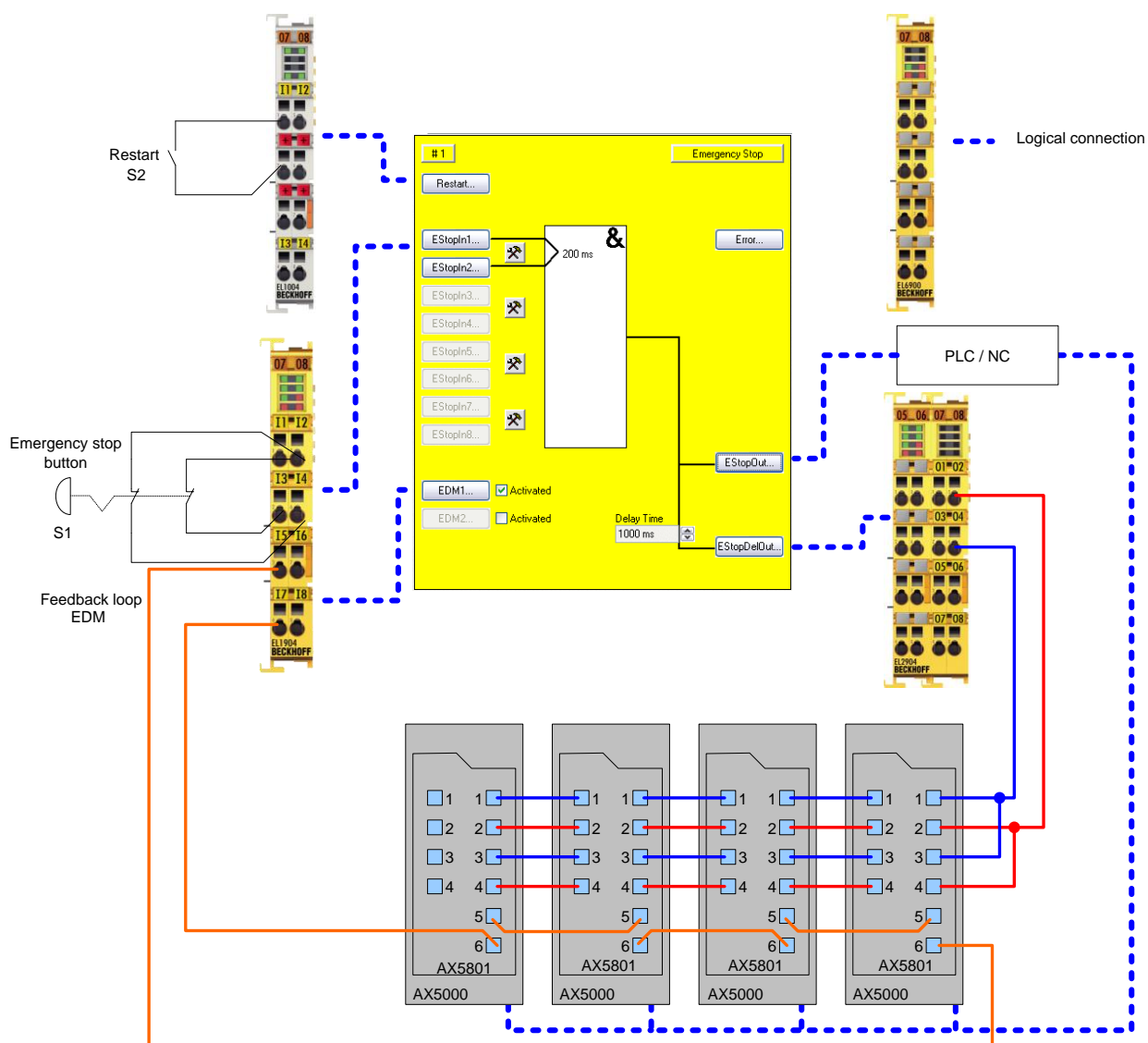
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.

Category	B	1	2	2	3	3	4
DC / MTTF <sub>d</sub>	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

## 2.20 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.



### 2.20.1 Parameters of the safe input and output terminals

**EL1904 (applies to all EL1904 used)**

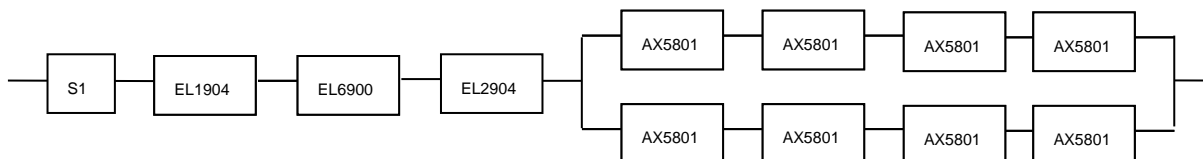
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

**EL2904**

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

### 2.20.2 Block formation and safety loops

### 2.20.2.1 Safety function 1



### 2.20.3 Calculation

#### 2.20.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
AX5801 – B10d	780,000
S1 – B10 <sub>d</sub>	100,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

### 2.20.3.2 Diagnostic Coverage DC

Component	Value
S1 with testing/plausibility	DC <sub>avg</sub> =99%
AX5801	DC <sub>avg</sub> =99%

### 2.20.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_d = \frac{100000}{0,1 * 1840} = 543,5y = 4761060h$$

**AX5801:**

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_d = \frac{780000}{0,1 * 1840} = 4239,1y = 37134516h$$

$$T_{10D} = \frac{B10_D}{n_{op}} = \frac{780000}{1840 \frac{1}{y}} = 423 y$$

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:**

$$PFH = \frac{1 - 0,99}{543,5 * 8760} = 2,10E - 9$$

**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 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  $\beta$ -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).

This produces for the calculation of the PFH 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 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:

$$PFH_{ges} = 2,10E - 09 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{4 * 2,70E - 10 + 4 * 2,70E - 10}{2} = 5,60E - 09$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(AX5801)} + \frac{1}{MTTF_d(AX5801)} + \frac{1}{MTTF_d(AX5801)} + \frac{1}{MTTF_d(AX5801)}$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{543,5y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y}} = 173,8y$$

$$DC_{avg} = \frac{\frac{99\%}{543,5} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1} + \frac{99\%}{4239,1}}{\frac{1}{543,5} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{4239,1} + \frac{1}{4239,1} + \frac{1}{4239,1} + \frac{1}{4239,1} + \frac{1}{4239,1} + \frac{1}{4239,1} + \frac{1}{4239,1} + \frac{1}{4239,1}} = 99,0\%$$

**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!

<b>MTTF<sub>d</sub></b>	
<b>Designation for each channel</b>	<b>Range for each channel</b>
low	$3 \text{ years} \leq \text{MTTF}_d < 10 \text{ years}$
medium	$10 \text{ years} \leq \text{MTTF}_d < 30 \text{ years}$
high	$30 \text{ years} \leq \text{MTTF}_d \leq 100 \text{ years}$

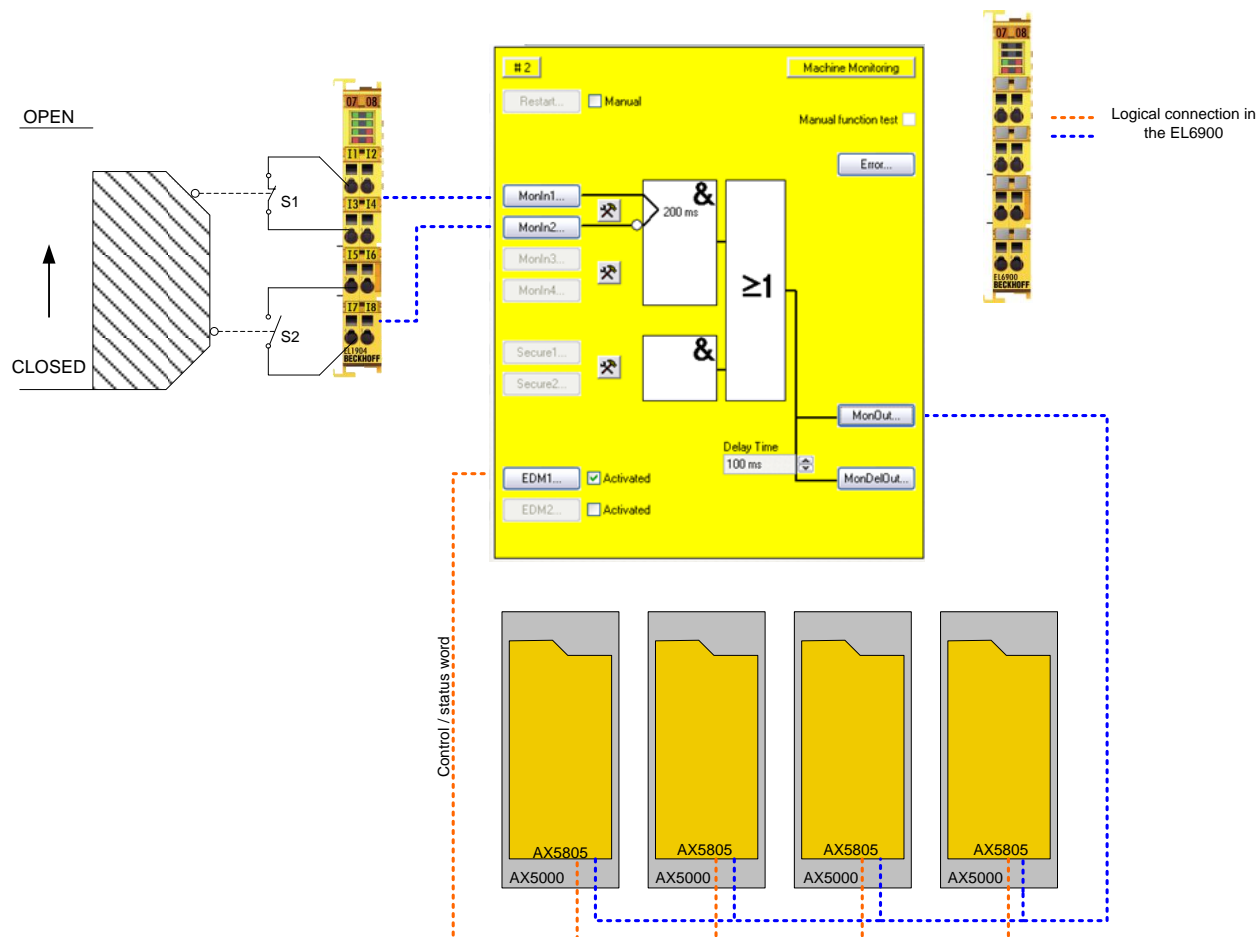
<b>DC<sub>avg</sub></b>	
<b>Designation</b>	<b>Range</b>
none	$\text{DC} < 60 \%$
low	$60 \% \leq \text{DC} < 90 \%$
medium	$90 \% \leq \text{DC} < 99 \%$
high	$99 \% \leq \text{DC}$

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.21 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.



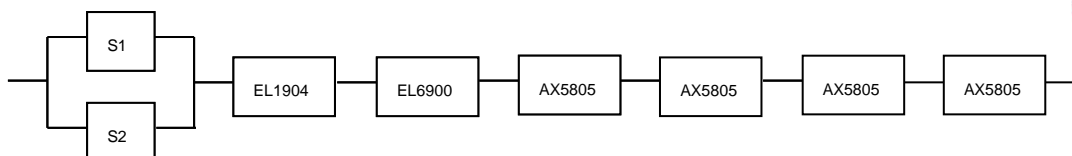
### 2.21.1 Parameters of the safe input and output terminals

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
-	

**2.21.2 Block formation and safety loops****2.21.2.1 Safety function 1****2.21.3 Calculation****2.21.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

Component	Value
EL1904 – PFH	1.11E-09
EL6900 – PFH	1.03E-09
AX5805 – PFH	5.15E-09 (see list of permitted motors)
S1 – B10 <sub>d</sub>	1,000,000
S2 – B10 <sub>d</sub>	2,000,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

**2.21.3.2 Diagnostic Coverage DC**

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%

**2.21.3.3 Calculation for safety function 1**

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

$$n_{op} = \frac{230 \cdot 8 \cdot 60}{60} = 1840$$

$$MTTF_d = \frac{1000000}{0,1 \cdot 1840} = 5434,8y = 47608848h$$

**S2:**

$$n_{op} = \frac{230 \cdot 8 \cdot 60}{60} = 1840$$

$$MTTF_d = \frac{2000000}{0,1 \cdot 1840} = 10869,6y = 95217696h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

$$PFH = \frac{1 - 0,99}{5434,8 \cdot 8760} = 2,10E - 10$$

**S2:**

$$PFH = \frac{1 - 0,99}{10869,6 \cdot 8760} = 1,05E - 10$$

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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

$$PFH_{ges} = \beta \cdot \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 \cdot (PFH_{(S1)} \cdot PFH_{(S2)}) \cdot T1 + PFH_{(EL1904)} + PFH_{(EL6900)} \\ + PFH_{(AX5805)} + PFH_{(AX5805)} + PFH_{(AX5805)} + PFH_{(AX5805)}$$

Since the portions  $(1 - \beta)^2 \cdot (PFH_{(x)} \cdot PFH_{(y)}) \cdot T1$  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:

$$PFH_{ges} = 10\% * \frac{2,10E - 10 + 1,05E - 10}{2} + 1,11E - 09 + 1,03E - 09 + 4 * (5,15E - 09) = 2,28E - 08$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(AX5805)} + \frac{1}{MTTF_d(AX5805)} + \frac{1}{MTTF_d(AX5805)} + \frac{1}{MTTF_d(AX5805)}$$

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 values are available for EL1904, AX5805 and EL6900, the following estimation applies:

$$MTTF_d(ELxxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(AX5805) = \frac{(1 - DC(AX5805))}{PFH(AX5805)} = \frac{(1 - 0,99)}{5,15E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{4,51E - 05 \frac{1}{y}} = 221,7y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{5434,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y}} = 49,8y$$

$$DC_{avg} = \frac{\frac{99\%}{5434,8} + \frac{99\%}{10869,6} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{221,7} + \frac{99\%}{221,7} + \frac{99\%}{221,7} + \frac{99\%}{221,7}}{\frac{1}{5434,8} + \frac{1}{10869,6} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{221,7} + \frac{1}{221,7} + \frac{1}{221,7} + \frac{1}{221,7}} = 99,0\%$$

**Note****Category**

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

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

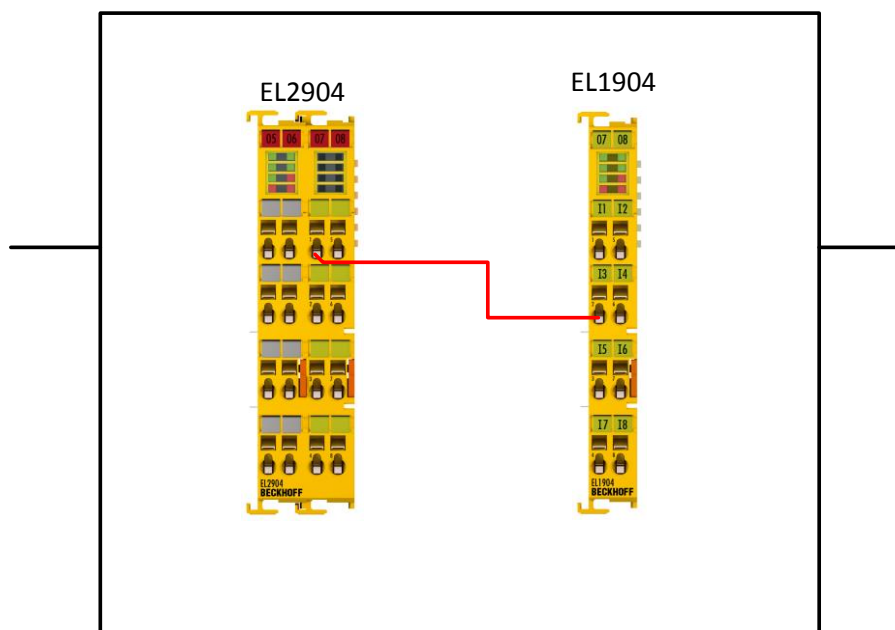
## 2.22 Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (single-channel) (Category 2, PL c)

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. Hence, cyclic checks for cross-circuit and external feed on the cable are not possible.

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



### 2.22.1 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

**2.22.2 Block formation and safety loops****2.22.2.1 Safety function 1****2.22.3 Calculation****2.22.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values**

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

**2.22.3.2 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 <sub>avg</sub> =60%

**2.22.3.3 Calculation for safety function 1**

This produces for the calculation of the PFH value for safety function 1:

$$PFH_{ges} = PFH_{(EL1904)} + PFH_{(EL2904)}$$

to:

$$PFH_{ges} = 1,11E - 09 + 1,25E - 09 = 2,36E - 09$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL2904)}$$

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

$$MTTF_d(ELxxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,60)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,4}{9,72E - 06 \frac{1}{y}} = 41152 y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,60)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,4}{1,1E - 05 \frac{1}{y}} = 36364 y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{41152y} + \frac{1}{36364y}} = 19305 y$$

$$DC_{avg} = \frac{\frac{60\%}{\frac{41152}{1}} + \frac{60\%}{\frac{36364}{1}}}{\frac{1}{41152} + \frac{1}{36364}} = 60\%$$

**Note****Category**

This structure is possible up to category 2 at the most.

**Attention****Attainment of 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 <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
<b>low</b>	<b>60 % ≤ DC &lt; 90 %</b>
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Cat	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.23 Direct wiring of the TwinSAFE outputs to TwinSAFE inputs (dual-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.

### 2.23.1 Parameters of the safe input and output terminals

#### EL1904

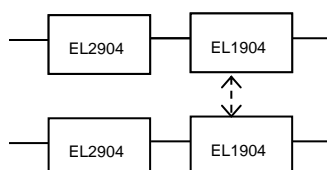
Parameter	Value
Sensor test channel 1 active	No
Sensor test channel 2 active	No
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

#### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	No

### 2.23.2 Block formation and safety loops

#### 2.23.2.1 Safety function 1



### 2.23.3 Calculation

#### 2.23.3.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	8
Cycle time (minutes) (T <sub>Zyklus</sub> )	60 (1x per hour)
Lifetime (T1)	20 years = 175200 hours

#### 2.23.3.2 Diagnostic Coverage DC

Component	Value
EL1904/EL2904	DC <sub>avg</sub> =90%

#### 2.23.3.3 Calculation for safety function 1

This produces for the calculation of the PFH value for block 1:

$$PFH_{ges} = PFH_{(EL1904)} + PFH_{(EL2904)}$$

to:

$$PFH_{ges} = 1,11E - 09 + 1,25E - 09 = \mathbf{2,36E - 09}$$

The MTTF<sub>d</sub> value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_{d(EL1904)}} + \frac{1}{MTTF_{d(EL2904)}}$$

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

$$MTTF_d(ELxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,9)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{9,72E - 06 \frac{1}{y}} = 10288,1y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,9)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,1}{1,1E - 05 \frac{1}{y}} = 9090,9y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{10288,1y} + \frac{1}{9090,9y}} = 4826,3y$$

$$DC_{avg} = \frac{\frac{90\%}{10288,1} + \frac{90\%}{10288,1} + \frac{90\%}{9090,9} + \frac{90\%}{9090,9}}{\frac{1}{10288,1} + \frac{1}{10288,1} + \frac{1}{9090,9} + \frac{1}{9090,9}} = 90\%$$

**Note****Category**

This structure is possible up to category 3 at the most.

MTTF <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

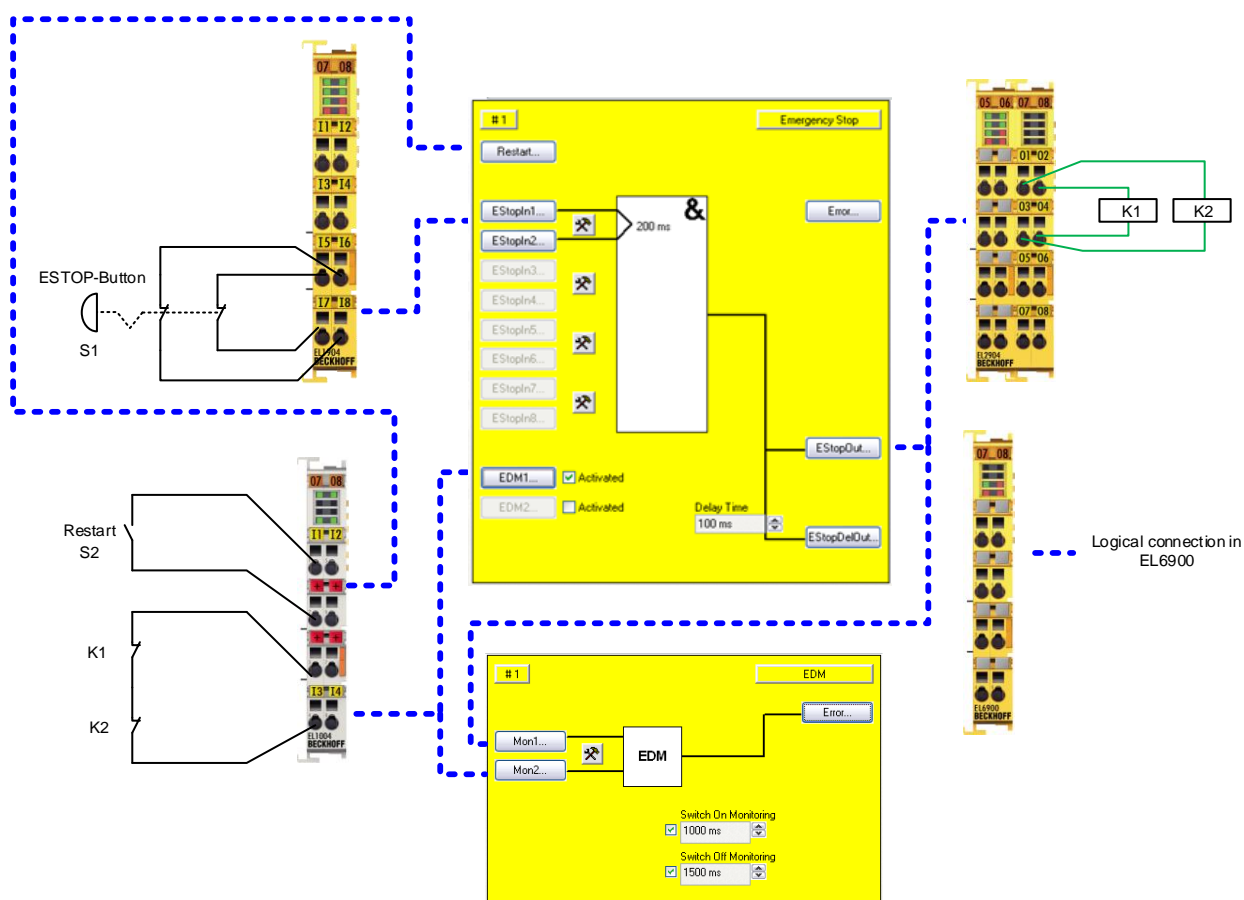
DC <sub>avg</sub>	
Designation	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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

## 2.24 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 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.



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

### EL1904 (applies to all EL1904 used)

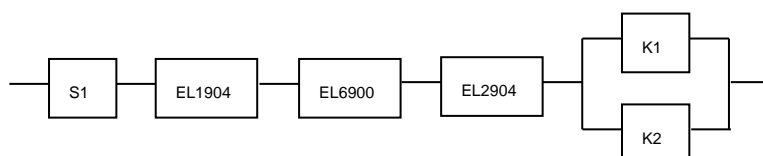
Parameter	Value
Sensor test channel 1 active	-
Sensor test channel 2 active	-
Sensor test channel 3 active	No
Sensor test channel 4 active	No
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	No

## 2.24.2 Block formation and safety loops

### 2.24.2.1 Safety function 1



## 2.24.3 Calculation

### 2.24.3.1 PFH / MTTFd / B10d – values

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



### 2.24.3.2 Diagnostic Coverage DC

Component	Value
S1 with plausibility	DC <sub>avg</sub> =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 <sub>avg</sub> =90%

### 2.24.3.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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:**

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

$$MTTF_d = \frac{100000}{0,1 * 21,90} = 45662,1y = 399999120h$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

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 100,000 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  $\beta$ -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).

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 2,5E - 10 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,92E - 11 + 1,92E - 11}{2} = 3,64E - 09$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

as:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)}$$

with:

$$MTTF_d(S1) = \frac{B10_d(S1)}{0,1 * n_{op}} = 45662,1y$$

$$MTTF_d(K1) = \frac{B10_d(K1)}{0,1 * n_{op}} = 593607,3y$$

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

$$MTTF_d(EL_{xxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:


$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$


$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$


$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

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

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

 <b>CAUTION</b>	<p><b>Category</b></p> <p>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!</p>
---	---

 <b>CAUTION</b>	<p><b>Further measures for attaining Category 3!</b></p> <p>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.</p>
---	--

 <b>CAUTION</b>	<p><b>Implement a restart lock in the machine!</b></p> <p>The restart lock is NOT part of the safety chain and must be implemented in the machine!</p>
---	--

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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

## 2.25 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.

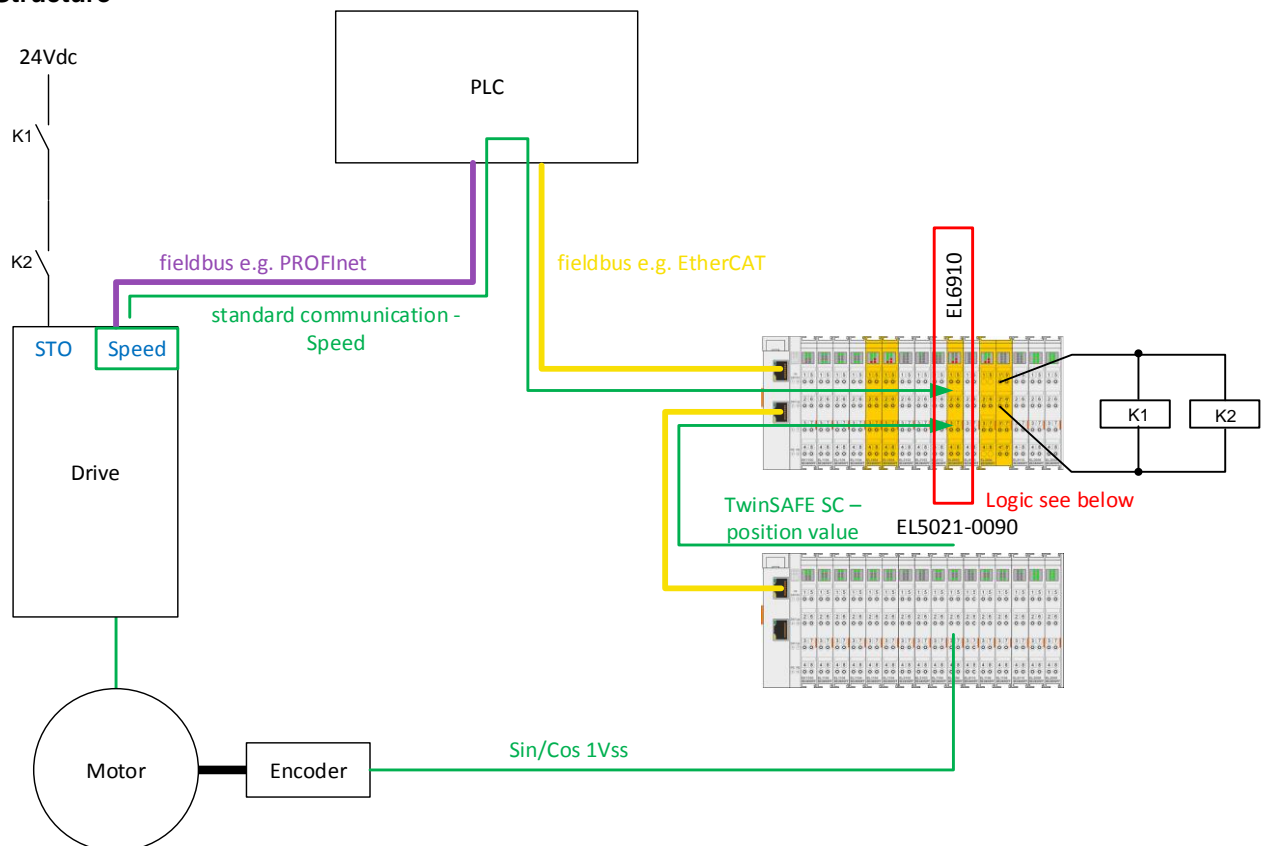
The position and speed signals are transmitted via two different communication paths to the EL6910 TwinSAFE logic and processed there according to the illustrated logic. The Sin/Cos encoder is connected to an EL5021-0090 and the position information is transmitted by TwinSAFE SC communication over EtherCAT. The speed of the drive is transferred to the EL6910 TwinSAFE logic over the standard PROFINET communication (any other fieldbus is also possible) and the standard PLC.

A speed (FB Speed) 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 the FB Compare for equality and monitored by the FB Limit 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 should be within a tolerance band of 10% in order to still to meet the condition of equality. If the current speed value is below the threshold specified in the FB Limit, the STO output is set to logical 1 and the drive can rotate. If the limit is exceeded or if the comparison fails, the output is set to logical 0 and the drive is switched to torque-free or the safety function integrated in the drive is activated. The entire calculation and scaling is 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.

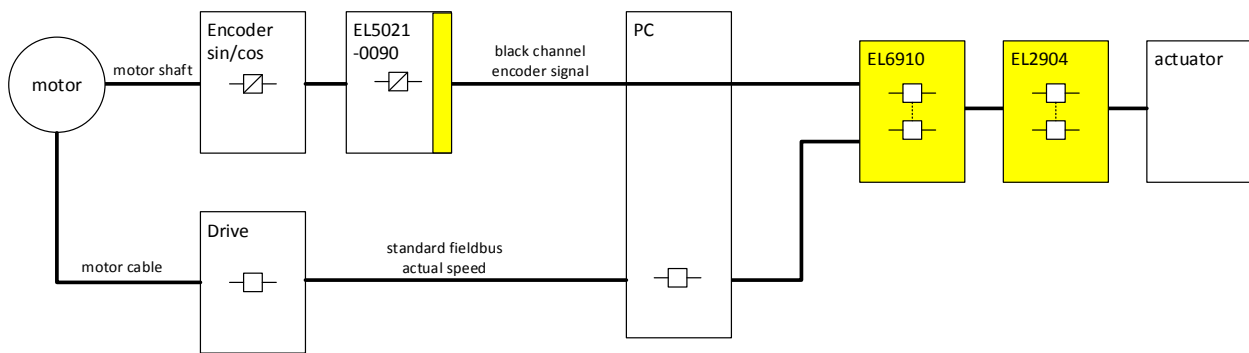
An emergency stop function is additionally implemented by an ESTOP function block (not shown in the diagram for reasons of clarity), which prevents the restart and also takes over the control of contactors K1 and K2.

The IsValid signal of the Compare function block must be used to switch off in case of a fault.

## Structure



## Diagram of the structure



## Logic



### 2.25.1 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 and the encoder a sin/cos signal, which is evaluated by a standard terminal, packaged in a safe telegram (FSoE with changed polynomial - TwinSAFE SC) and transmitted. 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.

### 2.25.2 FMEA

Error assumption	Expectations	Checked
Speed value over e.g. PROFINET itself freezes	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 activated for the speed 0.	
Speed value over EtherCAT and TwinSAFE SC communication freezes	Detected by 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 corrupt value within the TwinSAFE SC communication results in an invalid CRC inside the telegram and thus the immediate cut-off 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 via e.g. PROFINET is corrupted	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	Detected via the second value and the plausibility check in the EL6910 (other fieldbus and TwinSAFE SC communication between EL5021-0090 and EL6910).	
Communication error 61784-3 for standard communication: Corruption	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error 61784-3 for standard communication: Unintentional repetition	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication. In addition, the standard communication watchdog should be activated for the speed 0.	
Communication error 61784-3 for standard communication: Wrong sequence	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Loss	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error 61784-3 for standard communication: Unacceptable delay	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication. In addition, the standard communication watchdog should be activated for the speed 0.	
Communication error 61784-3 for standard communication: Insertion	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error for standard communication: Recurrent memory errors in switches	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	

#### 2.25.2.1 Note about 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.



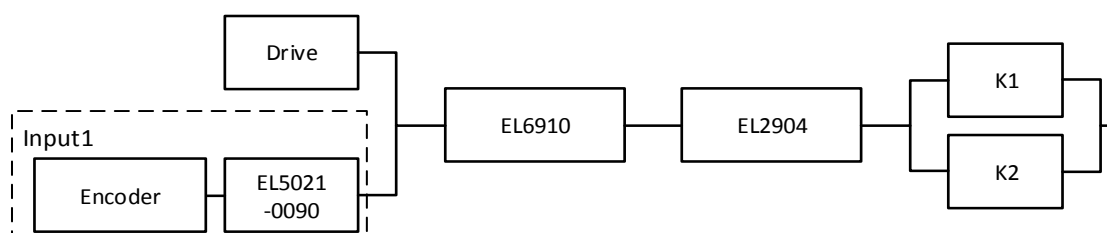
## 2.25.3 Parameters of the safe output terminal

### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.25.4 Block formation and safety loops

### 2.25.4.1 Safety function 1



## 2.25.5 Calculation

### 2.25.5.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6910 – PFH	1.79E-09
Drive MTBF	516,840 (59a)
Encoder – MTTF	549,149
EL5021-0090 - MTBF	1,205,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

### 2.25.5.2 Diagnostic Coverage DC

Component	Value
Drive and encoder with EL5021-0090 and plausibility within the logic	DC <sub>avg</sub> = 90% (alternative in the calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) without testing of the individual channels	DC <sub>avg</sub> = 99%

### 2.25.5.3 Calculation of safety function 1

For clarification, the safety parameter is calculated according to both EN62061 and EN13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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 and MTTF<sub>d</sub> 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:**

$$MTTF_d = 2 * MTBF = 2 * 59 = 1.033.680 \text{ h} = 118\text{y}$$

$$PFH = \frac{1 - DC}{MTTF_d} = \frac{1 - 0,9}{1.033.680 \text{ h}} = 9,67\text{E} - 08$$

**Encoder:**

$$MTTF_d = 2 * MTBF = 2 * 549149 = 1.098.298 \text{ h} = 125\text{y}$$

$$PFH = \frac{1 - DC}{MTTF_d} = \frac{1 - 0,9}{1.098.298 \text{ h}} = 9,10\text{E} - 08$$

**EL5021-0090**

$$MTTF_d = 2 * MTBF = 2 * 1.205.000 \text{ h} = 2.410.000 \text{ h} = 275 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_d} = \frac{1 - 0,9}{2.410.000 \text{ h}} = 4,15 \text{E} - 08$$

**Input subsystem 1**

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL5021-0090)} = 9,10 \text{E} - 08 + 4,15 \text{E} - 08 = 13,25 \text{E} - 08$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607 \text{ y} = 5.199.997.320 \text{ h}$$

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

**K1/K2:** Actuation 1x per week and direct feedback

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

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 B10d values for K1 and K2 are identical.

The input signals from encoder with EL5021-0090 and drive have different measuring methods, provide differently scaled values and are both involved in the safety function. A non-functioning of a channel does not lead to a dangerous situation, but is detected by the comparison of the two values in the TwinSAFE logic and leads to a 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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly. For the input subsystem an estimated value of 2% can be achieved by processing the table to calculate the  $\beta$  factor. In the following calculation, the worst case is assumed to be 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)

This produces for the calculation of the PFH 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  $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1$  are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$PFH_{ges} = 10\% * \frac{13,25E - 08 + 9,67E - 08}{2} + 1,79E - 9 + 1,25E - 9 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 1,146E - 08 + 1,79E - 09 + 1,25E - 9 + 1,92E - 13$$

$$PFH_{ges} = 1,45E - 08$$



#### Note

#### EN 62061

In accordance with EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This restricts the achievable SIL value according to table 5 of EN 62061 to a maximum SIL 2.

Alternative calculation of the MTTF<sub>d</sub> value according to EN13849 for safety function 1 (with the same assumption), with:

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

From the input subsystem, the poorer value is taken (here the combination of encoder and EL5021-0090):

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(Encoder)} + \frac{1}{MTTF_d(EL5021 - 0090)} + \frac{1}{MTTF_d(EL6910)} + \frac{1}{MTTF_d(EL2904)} \\ + \frac{1}{MTTF_d(K1)}$$

with:

If only PFH values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_d(ELxxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637 y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913y$$


$$MTTF_{D ges} = \frac{1}{\frac{1}{125} + \frac{1}{275} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607}} = 69,9 \text{ y}$$


$$DC_{avgs} = \frac{\frac{DC}{MTTF_d(Encoder)} + \frac{DC}{MTTF_d(EL5021-0090)} + \frac{DC}{MTTF_d(Drive)} + \frac{DC}{MTTF_d(EL6910)} + \frac{DC}{MTTF_d(EL2904)} + \frac{DC}{MTTF_d(K1)} + \frac{DC}{MTTF_d(K2)}}{\frac{1}{MTTF_d(Encoder)} + \frac{1}{MTTF_d(EL5021-0090)} + \frac{1}{MTTF_d(Drive)} + \frac{1}{MTTF_d(EL6910)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(K2)}}$$


$$DC_{avgs} = \frac{\frac{0,9}{125} + \frac{0,9}{275} + \frac{0,9}{118} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{125} + \frac{1}{275} + \frac{1}{118} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0207}{0,0228} = 90,78\%$$

Alternatively with DC = 99%

$$DC_{avgs} = \frac{\frac{0,99}{125} + \frac{0,99}{275} + \frac{0,99}{118} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{125} + \frac{1}{275} + \frac{1}{118} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0226}{0,0228} = 99,12\%$$

 <b>CAUTION</b>	<b>Category</b>  This structure is possible up to category 3 at the most.
---	---

 <b>WARNING</b>	<b>Standstill</b>  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.
---	---

 <b>CAUTION</b>	<b>Implement a restart lock in the machine!</b>  The restart lock is NOT part of the safety chain and must be implemented in the machine!
---	---

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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 <sub>d</sub>	
Designation for each channel	Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	<b>30 years ≤ MTTF<sub>d</sub> ≤ 100 years</b>

DC <sub>avg</sub>	
Name	Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
<b>high</b>	<b>99 % ≤ DC</b>
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 <sub>d</sub>	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 Tab. 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH <sub>D</sub> )
3	≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.26 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.

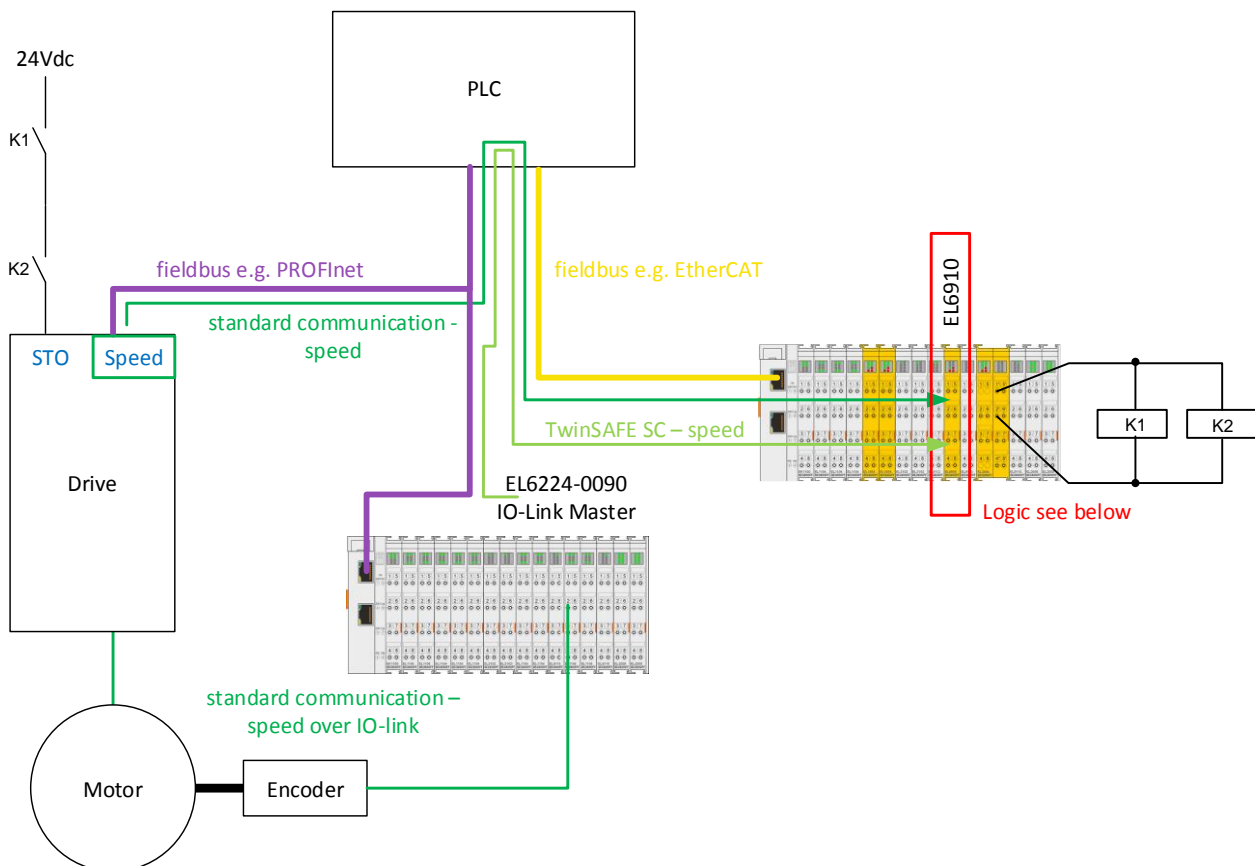
The speed signals are transmitted in two different ways to the EL6910 TwinSAFE logic and processed there according to the illustrated logic. The IO-link encoder is wired to an EL6224-0090 and the speed information is transmitted via TwinSAFE SC communication over PROFINET, for example. The speed of the drive is transferred to the EL6910 TwinSAFE logic over the standard PROFINET communication (any other fieldbus is also possible) and the standard PLC.

The two speeds are scaled by the FB Scale within the safety-related EL6910 logic so that the values match each other. These two speed values are checked by the FB Compare for equality and monitored by the FB Limit for a maximum value. Since the two speed values are never 100% equal at any time, the difference between the two speed values should be within a tolerance band of 10% in order to still to meet the condition of equality. If the current speed value is below the threshold specified in the FB Limit, the STO output is set to logical 1 and the drive can rotate. If the limit is exceeded or if the comparison fails, the output is set to logical 0 and the drive is switched to 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.

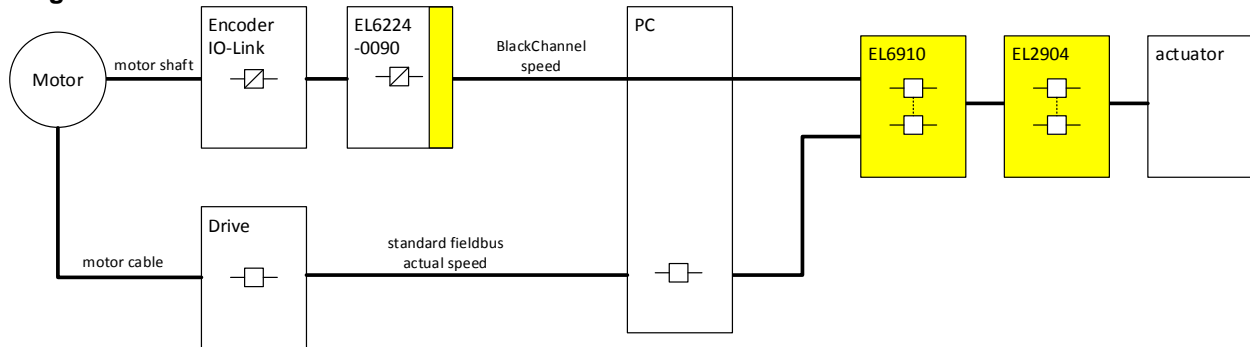
The IsValid signal of the Compare function block must be used to switch off in case of a fault.

### IO-Link structure

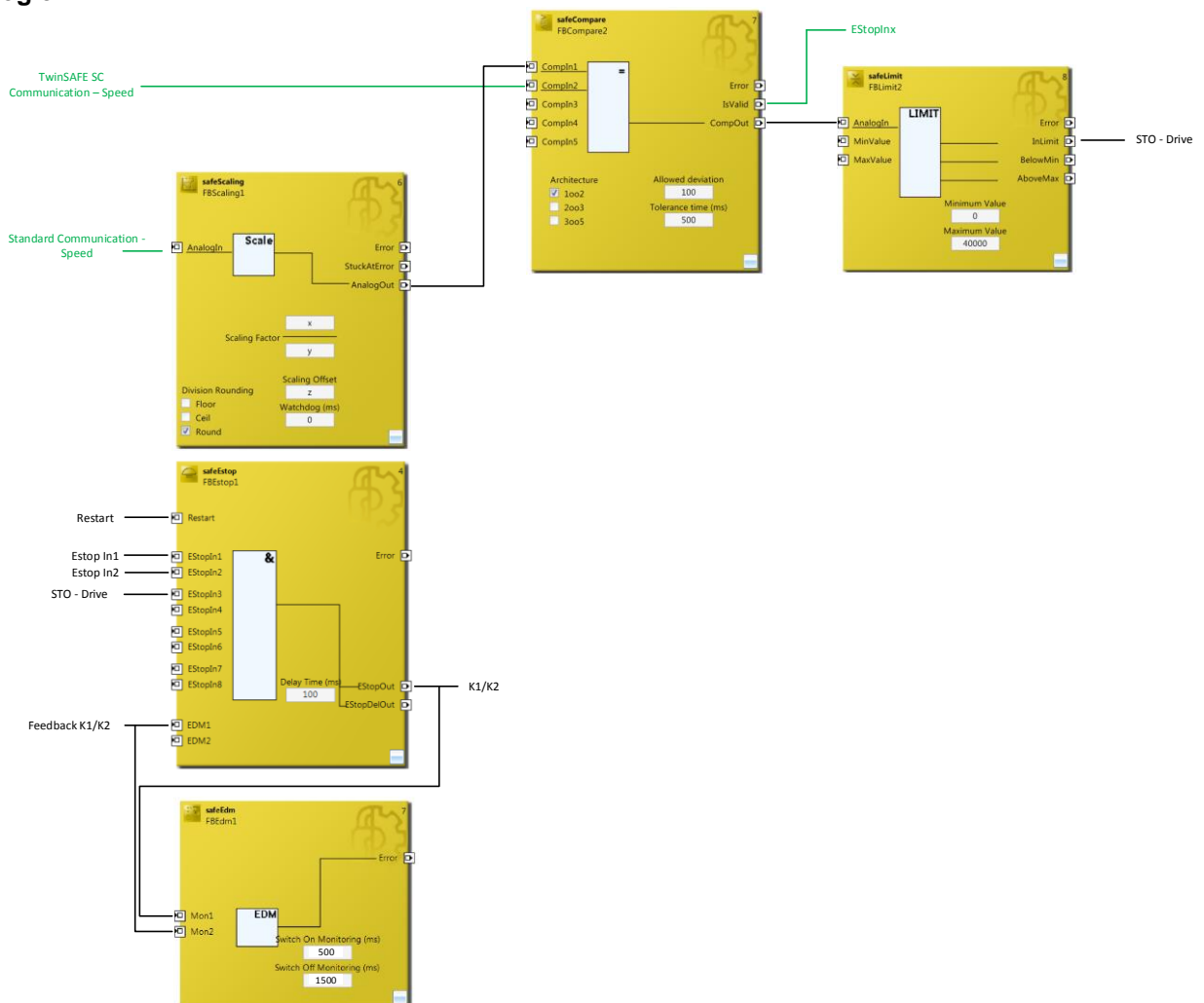




## Diagram of the structure



## logic



### 2.26.1 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 and the encoder an IO-Link signal, which is evaluated by a standard terminal, packaged in a safe telegram (FSoE with changed polynomial - TwinSAFE SC) and transmitted. This terminal (EL6224-0090) supplies a position 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 immediately within the safe logic and lead to the activation of the STO of the drive.

### 2.26.2 FMEA

Error assumption	Expectations	Checked
Speed value over e.g. PROFINET itself freezes	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 activated for the speed 0.	
Speed value over EtherCAT and TwinSAFE SC communication freezes	Detected by 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 corrupt value within the TwinSAFE SC communication results in an invalid CRC inside the telegram and thus the immediate cut-off 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 via e.g. PROFINET is corrupted	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	Detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC communication between EL6224-0090 and EL6910)	
Communication error 61784-3 for standard communication: Corruption	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error 61784-3 for standard communication: Unintentional repetition	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication. In addition, the standard communication watchdog should be activated for the speed 0.	
Communication error 61784-3 for standard communication: Wrong sequence	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Loss	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error 61784-3 for standard communication: Unacceptable delay	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication. In addition, the standard communication watchdog should be activated for the speed 0.	
Communication error 61784-3 for standard communication: Insertion	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error 61784-3 for standard communication: Masquerading	not relevant for standard, only for safety communication.	
Communication error 61784-3 for standard communication: Addressing	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	
Communication error for standard communication: Recurrent memory errors in switches	Detected within the EL6910 via the plausibility check of the speed values with the TwinSAFE SC communication	

### 2.26.2.1 Note about 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.

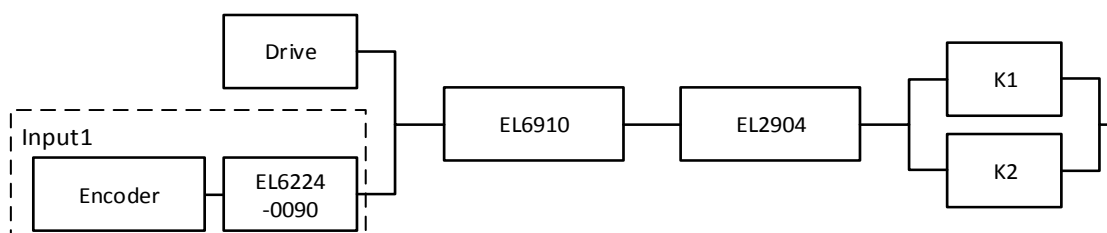
## 2.26.3 Parameters of the safe output terminal

### EL2904

Parameter	Value
Current measurement active	Yes
Output test pulses active	Yes

## 2.26.4 Block formation and safety loops

### 2.26.4.1 Safety function 1



## 2.26.5 Calculation

### 2.26.5.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6910 – PFH	1.79E-09
Drive MTBF	516,840 (59y)
Encoder – MTTF	1.208.880 (138y)
EL6224-0090 - MTBF	1,200,000
K1 – B10 <sub>d</sub>	1,300,000
K2 – B10 <sub>d</sub>	1,300,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zklus</sub> )	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

### 2.26.5.2 Diagnostic Coverage DC

Component	Value
Drive and encoder with EL6224-0090 and plausibility within the logic	DC <sub>avg</sub> = 90% (alternative in the calculation: 99%)
K1/K2 with EDM monitoring (actuation 1x per week and evaluation of all rising and falling edges with monitoring over time) without testing of the individual channels	DC <sub>avg</sub> =99%

### 2.26.5.3 Calculation of safety function 1

For clarification, the safety parameter is calculated according to both EN62061 and EN13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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 and MTTF<sub>d</sub> 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

$$MTTF_d = 2 * MTBF = 2 * 59 = 1.033.680 \text{ h} = 118 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_d} = \frac{1 - 0,9}{1.033.680 \text{ h}} = 9,67 \text{ E} - 08$$

#### Encoder

$$MTTF_d = 2 * MTBF = 2 * 549149 = 1.208.880 \text{ h} = 138 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_d} = \frac{1 - 0,9}{1.208.880 \text{ h}} = 8,27 \text{ E} - 08$$

**EL6224-0090**

$$MTTF_d = 2 * MTBF = 2 * 1.200.000 h = 2.400.000 h = 273y$$

$$PFH = \frac{1 - DC}{MTTF_d} = \frac{1 - 0,9}{2.400.000 h} = 4,17E - 08$$

**Input subsystem 1**

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL6224-0090)} = 8,27E - 08 + 4,17E - 08 = 12,44E - 08$$

**K1/K2:**

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

$$MTTF_d = \frac{1300000}{0,1 * 21,90} = 593607y = 5.199.997.320h$$

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

**K1/K2: Actuation 1x per week**

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

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 B10d values for K1 and K2 are identical.

The input signals from encoder with EL6224-0090 and drive have different measuring methods, provide differently scaled values and are both involved in the safety function. A non-functioning of a channel does not lead to a dangerous situation, but is detected by the comparison of the two values in the TwinSAFE logic and leads to a 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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly. For the input subsystem an estimated value of 2% can be achieved by processing the table to calculate the  $\beta$  factor. In the following calculation, the worst case is assumed to be 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)

This produces for the calculation of the PFH 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  $(1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1$  are smaller than the rest by the power of ten, they are neglected in this and all further calculations for the purpose of simplification.

$$PFH_{ges} = 10\% * \frac{12,44E-08 + 9,67E-08}{2} + 1,79E-9 + 1,25E-9 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$

$$= 1,106E-08 + 1,79E-09 + 1,25E-9 + 1,92E-13$$

$$PFH_{ges} = 1,41E-08$$

**Note****EN 62061**

In accordance with EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This restricts the achievable SIL value according to table 5 of EN 62061 to a maximum SIL 2.

Alternative calculation of the  $MTTF_d$  value according to EN13849 for safety function 1 (with the same assumption), with:

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

From the input subsystem, the poorer value is taken (here the combination of encoder and EL6224-0090):

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(Encoder)} + \frac{1}{MTTF_d(EL6224-0090)} + \frac{1}{MTTF_d(EL6910)} + \frac{1}{MTTF_d(EL2904)}$$

$$+ \frac{1}{MTTF_d(K1)}$$

with:

If only PFH values are available for EL2904 and EL6910, the following estimation applies:

$$MTTF_d(EL_{xxxx}) = \frac{(1 - DC(EL_{xxx}))}{PFH(EL_{xxx})}$$

Hence:

$$MTTF_{d(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E-06 \frac{1}{y}} = 637 y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E-05 \frac{1}{y}} = 913 y$$




$$MTTF_{d ges} = \frac{1}{\frac{1}{138} + \frac{1}{273} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607}} = 73,65 y$$

$$DC_{avgs} = \frac{\frac{DC}{MTTF_d(Encoder)} + \frac{DC}{MTTF_d(EL6224-0090)} + \frac{DC}{MTTF_d(Drive)} + \frac{DC}{MTTF_d(EL6910)} + \frac{DC}{MTTF_d(EL2904)} + \frac{DC}{MTTF_d(K1)} + \frac{DC}{MTTF_d(K2)}}{\frac{1}{MTTF_d(Encoder)} + \frac{1}{MTTF_d(EL6224-0090)} + \frac{1}{MTTF_d(Drive)} + \frac{1}{MTTF_d(EL6910)} + \frac{1}{MTTF_d(EL2904)} + \frac{1}{MTTF_d(K1)} + \frac{1}{MTTF_d(K2)}}$$

$$DC_{avgs} = \frac{\frac{0,9}{138} + \frac{0,9}{273} + \frac{0,9}{118} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{138} + \frac{1}{273} + \frac{1}{118} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0200}{0,0220} = 90,90\%$$

Alternatively with DC=99%

$$DC_{avgs} = \frac{\frac{0,99}{138} + \frac{0,99}{273} + \frac{0,99}{118} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{138} + \frac{1}{273} + \frac{1}{118} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0218}{0,0220} = 99,09\%$$

 <b>CAUTION</b>	<b>Category</b>  This structure is possible up to category 3 at the most.
 <b>WARNING</b>	<b>Standstill</b>  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.
 <b>CAUTION</b>	<b>Implement a restart lock in the machine!</b>  The restart lock is NOT part of the safety chain and must be implemented in the machine!

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	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:

Designation for each channel	MTTF <sub>d</sub>
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

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.

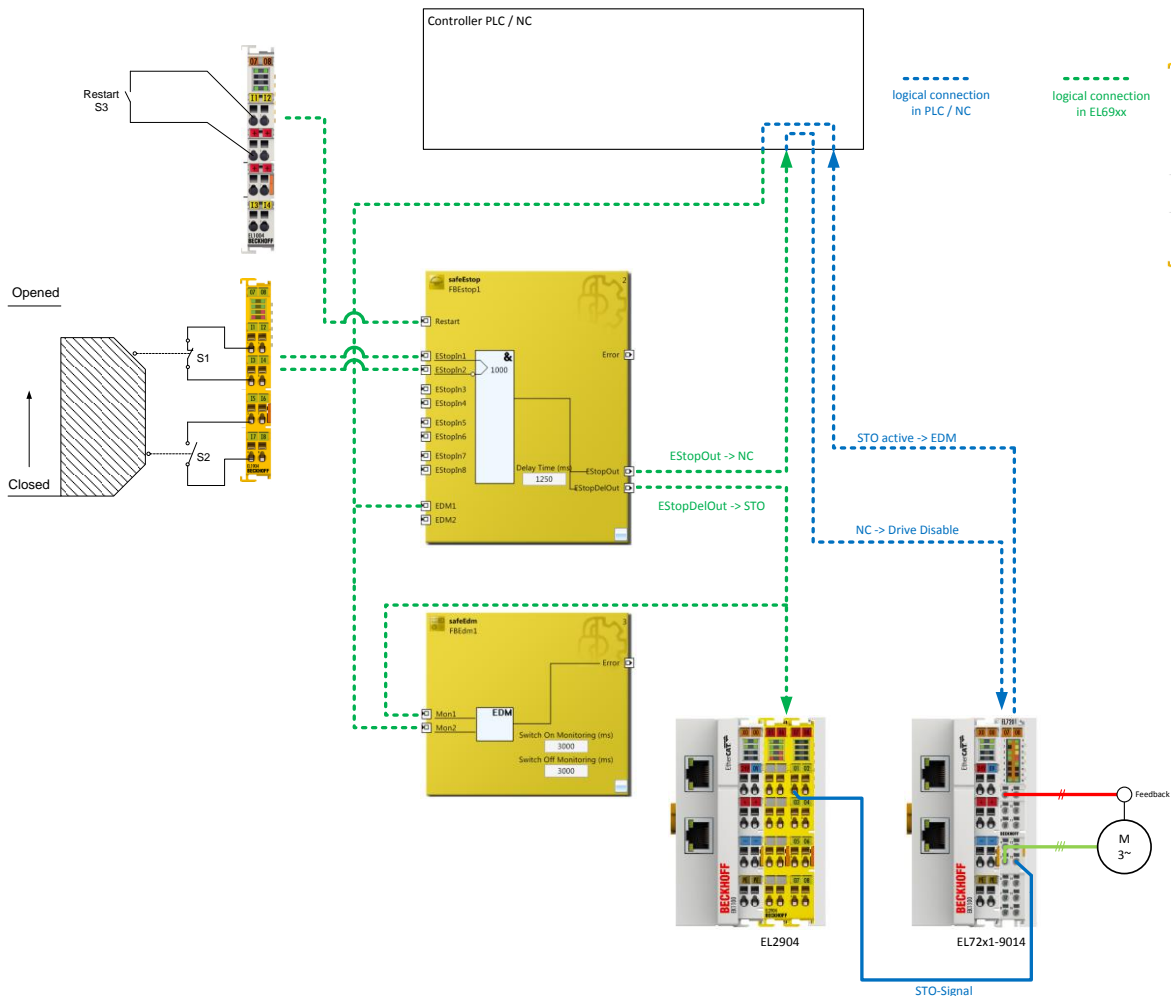
Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e




Safety integrity level according to Tab. 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH <sub>D</sub> )
3	≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.27 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 safety 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.



 <b>CAUTION</b>	<p><b>Implement a restart lock in the machine!</b></p> <p>The restart lock is NOT part of the safety chain and must be implemented in the machine!          If the risk analysis gives the result that a restart has to be done within the safety controller, the restart must also be applied to a safe input.</p>
 <b>WARNING</b>	<p><b>Wiring only inside the control cabinet!</b></p> <p>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.</p>
 <b>Note</b>	<p><b>Calculation EL72x1-9014</b></p> <p>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 non-reactively to the safety function. The PFH value goes into the calculation according to EN 62061 with a value of 0.</p>

### 2.27.1 Parameters of the safe input and output terminals

#### EL1904

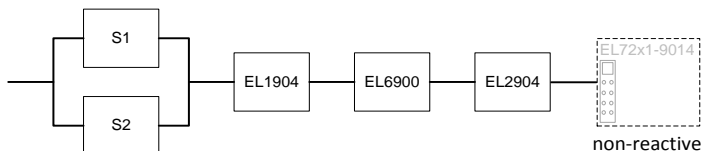
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

#### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

## 2.27.2 Block formation and safety loops

### 2.27.3 Safety function 1



## 2.27.4 Calculation

### 2.27.4.1 PFH / MTTF<sub>d</sub> / B10<sub>d</sub> – values

Component	Value
EL1904 – PFH	1.11E-09
EL2904 – PFH	1.25E-09
EL6900 – PFH	1.03E-09
EL72x1-9014 - PFH	0.00
S1 – B10 <sub>d</sub>	1,000,000
S2 – B10 <sub>d</sub>	2,000,000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

### 2.27.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
EL2904 with testing	DC <sub>avg</sub> =99%

### 2.27.4.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> values:

off:

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

and:

$$MTTF_d = \frac{B10_d}{0,1 \cdot n_{op}}$$

Inserting the values, this produces:

**S1:**

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

$$MTTF_d = \frac{1000000}{0,1 \cdot 14720} = 679,3y = 5951087h$$

**S2:**

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

$$MTTF_d = \frac{2000000}{0,1 \cdot 14720} = 1358,7y = 11902174h$$

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

$$MTTF_d = \frac{1}{\lambda_d}$$

produces for

$$PFH = \frac{0,1 \cdot n_{op} \cdot (1 - DC)}{B10_d} = \frac{1 - DC}{MTTF_d}$$

**S1:**

$$PFH = \frac{1 - 0,99}{679,3 \cdot 8760} = 1,68E - 9$$

**S2:**

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

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  $\beta$ -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).

This produces for the calculation of the PFH value for safety function 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(EL7201-9014)}$$

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:

$$PFH_{ges} = 10\% * \frac{1,68E - 09 + 1,68E - 09}{2} + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 0,00 = 3,558E - 09$$

The  $MTTF_d$  value for safety function 1 (based on the same assumption) is calculated with:

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

for:

$$\frac{1}{MTTF_{d ges}} = \frac{1}{MTTF_d(S1)} + \frac{1}{MTTF_d(EL1904)} + \frac{1}{MTTF_d(EL6900)} + \frac{1}{MTTF_d(EL2904)}$$

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

$$MTTF_d(ELxxxx) = \frac{(1 - DC(ELxxx))}{PFH(ELxxx)}$$

Hence:


$$MTTF_d(EL1904) = \frac{(1 - DC(EL1904))}{PFH(EL1904)} = \frac{(1 - 0,99)}{1,11E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E - 06 \frac{1}{y}} = 1028,8y$$

$$MTTF_d(EL6900) = \frac{(1 - DC(EL6900))}{PFH(EL6900)} = \frac{(1 - 0,99)}{1,03E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E - 06 \frac{1}{y}} = 1108,6y$$

$$MTTF_d(EL2904) = \frac{(1 - DC(EL2904))}{PFH(EL2904)} = \frac{(1 - 0,99)}{1,25E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E - 05 \frac{1}{y}} = 913,2y$$

$$MTTF_{dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 225,2y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3} + \frac{99\%}{1358,7} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2}}{\frac{1}{679,3} + \frac{1}{1358,7} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2}} = 99,00\%$$

 CAUTION	<b>Category</b>  This structure is possible up to category 3 at the most.
--	---

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

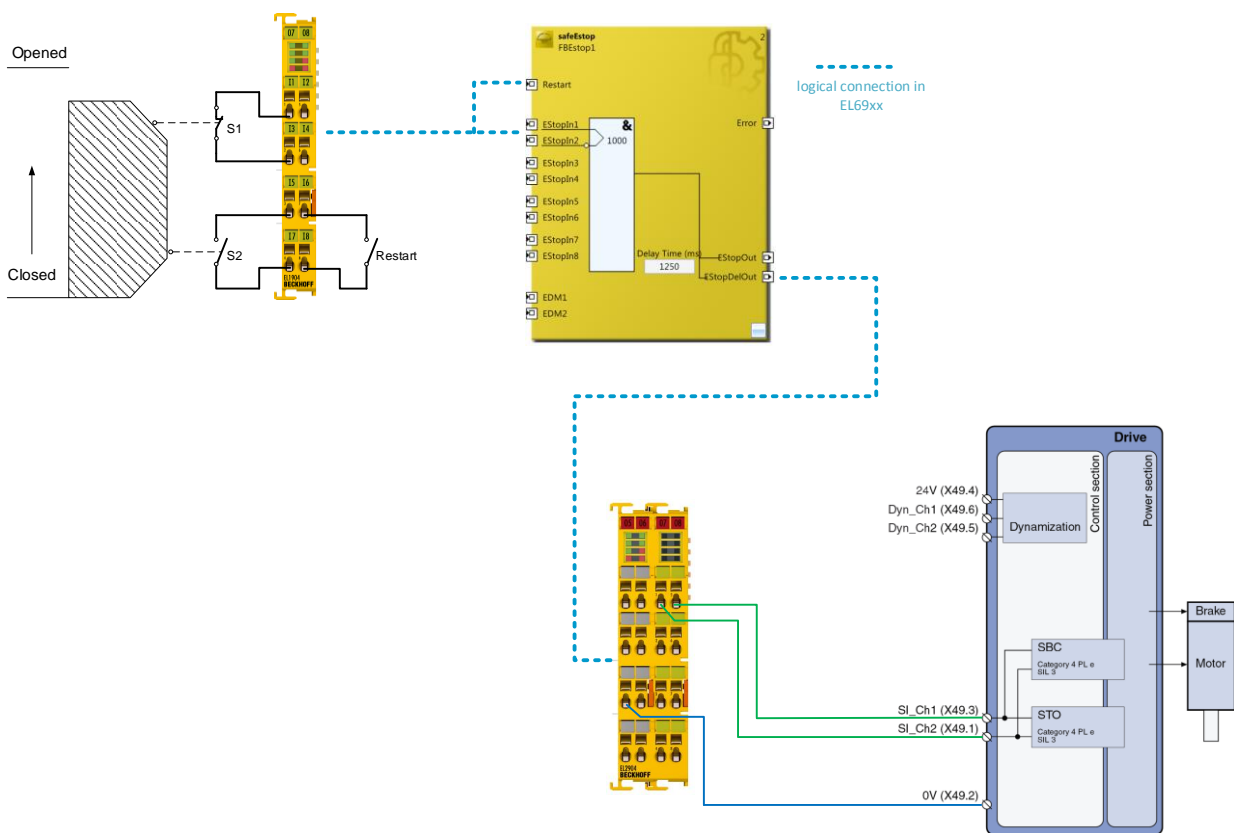
Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

## 2.28 STO-Function with IndraDrive (Category 4, PL e)

The following example shows the use of safe outputs of the EL2904 together with a BOSCH Rexroth IndraDrive drive to realize a STO function on this.

For example, a protective door is wired in two channels to a safe input (here EL1904) together with a restart signal. Within the TwinSAFE logic, these signals are used on an ESTOP module. The delay-switching output of the ESTOP block is used for the two safe outputs of the EL2904. The output EStopOut can be used to electrically stop the drive via the NC control.

One output each of the EL2904 is wired to the STO inputs X49.1 and X49.3 of the Bosch Rexroth IndraDrive. The corresponding GND contact (X49.2) is here, for example, fed back to the EL2904 to show that the EL2904 and the IndraDrive use identical ground potential of the 24V supply.



### Implement a restart lock in the machine!

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



## 2.28.1 Parameters of the safe input and output terminals

### EL1904

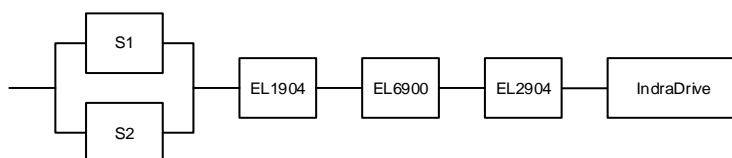
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

## 2.28.2 Block formation and safety loops

### 2.28.3 Safety function 1



## 2.28.4 Calculation

### 2.28.4.1 PFH / MTTFd / B10d – values

Component	Value
EL1904 – PFH	1,11E-09
EL2904 – PFH	1,25E-09
EL6900 – PFH	1,03E-09
Bosch Rexroth IndraDrive <sup>1)</sup> - PFH	0,50E-09
Bosch Rexroth IndraDrive <sup>1)</sup> - MTTF <sub>D</sub>	> 200 years
S1 – B10 <sub>d</sub>	1.000.000
S2 – B10 <sub>d</sub>	2.000.000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

<sup>1)</sup> Please refer to the Bosch Rexroth user documentation

### 2.28.4.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC <sub>avg</sub> =99%
EL2904 with testing	DC <sub>avg</sub> =99%
Bosch Rexroth IndraDrive <sup>1)</sup>	DC <sub>avg</sub> =99%

<sup>1)</sup> Please refer to the Bosch Rexroth user documentation

### 2.28.4.3 Calculation for safety function 1

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> values:

off:

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

and:

$$MTTF_D = \frac{B10_d}{0,1 * n_{op}}$$

Inserting the values, this produces:

**S1:**

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

$$MTTF_D = \frac{1000000}{0,1 * 14720} = 679,3 \text{ y} = 5951087 \text{ h}$$

**S2:**

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

$$MTTF_D = \frac{2000000}{0,1 * 14720} = 1358,7 \text{ y} = 11902174 \text{ h}$$

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:**

$$PFH = \frac{1 - 0,99}{679,3 * 8760} = 1,68E - 9$$

**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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly.

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).

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{1,68E - 09 + 8,40E - 10}{2} + 1,11E - 9 + 1,03E - 9 + 1,25E - 9 + 0,50E - 9$$

$$PFH_{ges} = 4,016E - 09$$



#### Calculation according to EN 62061

According to EN 62061 table 3, this value corresponds to a SIL3.

Alternative calculation of the  $MTTF_D$  value according to EN13849 for safety function 1 (with the same assumption), with:

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

for:

$$\frac{1}{MTTF_{D ges}} = \frac{1}{MTTF_D(S1)} + \frac{1}{MTTF_D(EL1904)} + \frac{1}{MTTF_D(EL6900)} + \frac{1}{MTTF_D(EL2904)} + \frac{1}{MTTF_D(IndraDrive)}$$

with:

$$MTTF_D(S1) = \frac{B10_d(S1)}{0,1 * n_{op}} = 679,3 \text{ y}$$

$$MTTF_D(IndraDrive) = 200 \text{ y}$$

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

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

Hence:

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

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

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

$$MTTF_{D ges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{200y}} = 105,9 \text{ y}$$

$$DC_{avg} = \frac{\frac{99\%}{679,3} + \frac{99\%}{1358,7} + \frac{99\%}{1028,8} + \frac{99\%}{1108,6} + \frac{99\%}{913,2} + \frac{99\%}{200}}{\frac{1}{679,3} + \frac{1}{1358,7} + \frac{1}{1028,8} + \frac{1}{1108,6} + \frac{1}{913,2} + \frac{1}{200}} = 99,00\%$$

**Category**

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

Designation for each channel	MTTF <sub>d</sub>
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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 Tab. 3 EN62061	
Safety integrity level	Probability of a dangerous failure per hour (PFH <sub>D</sub> )
3	≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.28.5 Technical Note from company Bosch Rexroth AG

This technical note is right now only available in German language. Please contact Bosch Rexroth AG in case you need an English translation.



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](http://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.

Firmensitz: Stuttgart, Registrierung: Amtsgericht Stuttgart HRB 23192  
Vorstand: Rolf Najork (Vorsitzender), Dr. Markus Forschner, Dr. Steffen Haack, Dr. Bertram Hoffmann  
Vorsitzender des Aufsichtsrats: Dr. Werner Struth

## 1 Safety Anforderungen

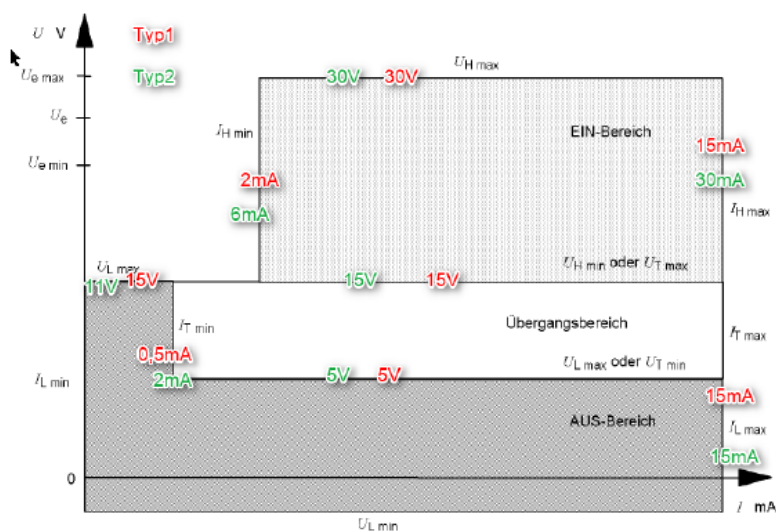
09. März 2017

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
$t_{Lmax}$	1 ms	maximale Low-Zeit des Testpulses
$t_{Lmin}$	20 $\mu$ s	minimale Low-Zeit des Testpulses
$t_{Pmax}$	1 h	maximale Periodendauer der Testpulse
$t_{Pmin}$	500 $\mu$ s	minimale Periodendauer der Testpulse
$t_{Vmax}$	1 s	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{Duty} = t_{PH} / t_P$	90 %	minimales Tastverhältnis der Anwahlsignale
$t_{Halt}$	400 ms	maximale Profilldauer bei einer An- oder Abwahl
$\varphi$	–	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

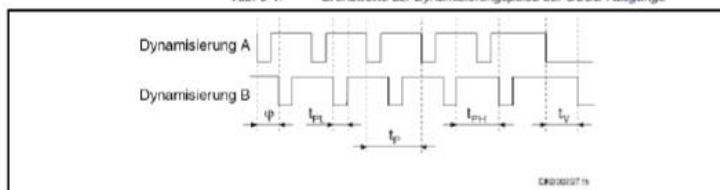
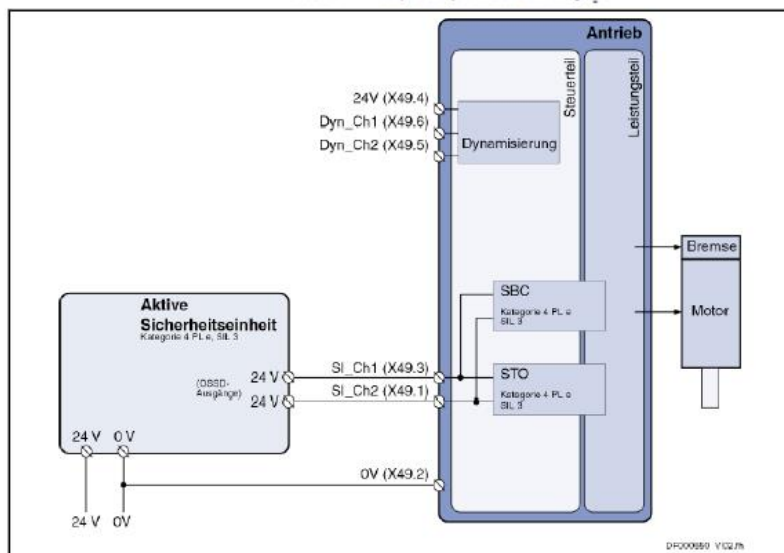


Abb. 5-2: Beispiel für dynamisierte Anwahlsignale





## 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
$t_{D,max}^{(1)} = 1 \text{ s}$	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{D,min} = t_{FH} / t_p = 90 \%$	minimales Tastverhältnis der Anwahlsignale
$t_{D,max} = t_{FH} / t_p = 100 \%$	maximales Tastverhältnis der Anwahlsignale
$t_{PRE} = 400 \text{ ms}$	maximale Prelldauer bei einer An- oder Abwahl
$\varphi^{(1)} = -$	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

<sup>1)</sup> gilt nur bei zweikanaliger Anwahl

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

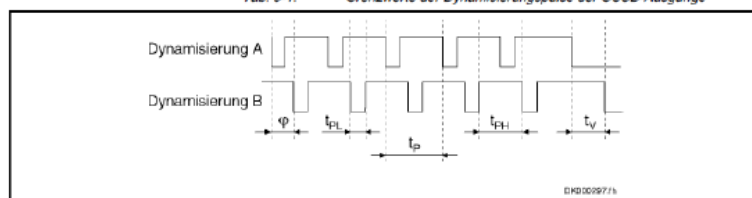


Abb. 5-1: Beispiel für dynamisierte Anwahlsignale

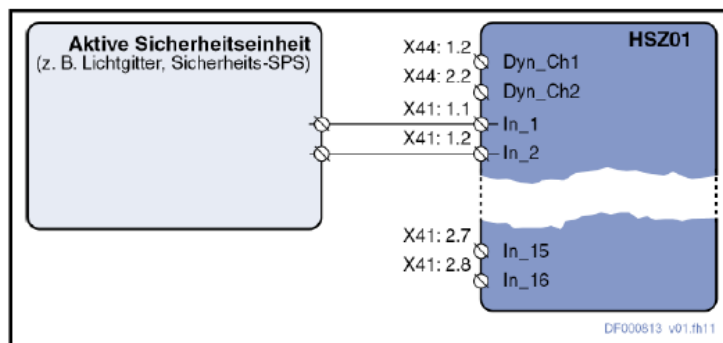


Abb. 5-2: Dynamisierung bei Anwahl über eine aktive Sicherheitseinheit

Diese Bestätigung gilt bis auf Widerruf.

Mit freundlichen Grüßen

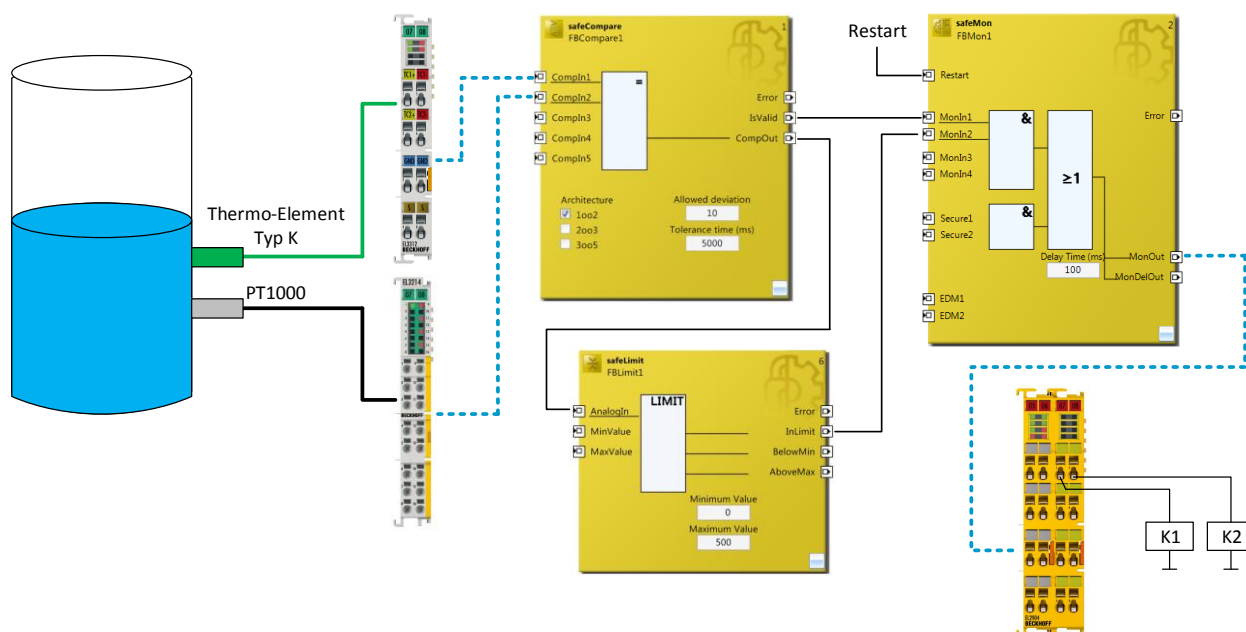
Bosch Rexroth AG (DC-IA/EDY)

## 2.29 Temperature measurement with TwinSAFE SC (Category 3, PL d)

In this example we will show how a temperature measurement with the TwinSAFE SC technology can be realized. For this purpose, two measuring points are equipped with temperature sensors, on the one hand with a thermocouple of type K, which is wired to a standard EtherCAT terminal EL3312, and on the other hand a PT1000 measuring resistor, which is wired to a TwinSAFE SC EtherCAT terminal EL3214-0090.

Within the safe TwinSAFE EL6910 logic, these two signals are compared or plausibilized using a Compare function block. The signal is then checked via the FB limit. The result of the FB limit and the IsValid output of the Compare function block are used to switch off the contactors K1 and K2 via the function block Mon.

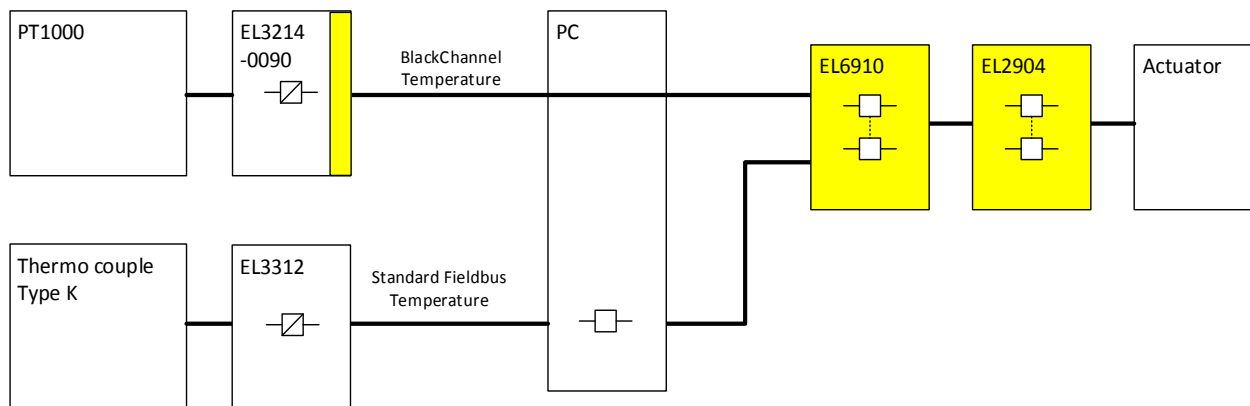
The monitoring of the contactor feedback is not shown in this example for the sake of clarity, but must be considered by the user



### Emergency stop / contactor feedback monitor

In addition to the function shown above, a contactor feedback monitor, e.g. via an EDM function block for K1 and K2 and, if necessary, an emergency stop function must be implemented by the user!

### 2.29.1 Diagram of the structure



### 2.29.2 Structure and diagnosis

The read signals from the two measuring points are standard signals using a different technology. At least one signal is transmitted via the TwinSAFE SC technology to the safe TwinSAFE logic so that falsifications of this signal in the PC or on the transmission path are detected. The check for equality of these two signals, within the permissible tolerances, is performed in the safe TwinSAFE logic.

The individual fault assumptions and associated expectations are listed in the following FMEA table

### 2.29.3 FMEA

Error assumption	Expectations	Checked
Temperature value over standard fieldbus itself freezes	Detected via the second value and the plausibility check in the EL6910.	
Temperature value over TwinSAFE SC communication freezes	Detected by the watchdog within the TwinSAFE SC communication and by the plausibility check in the EL6910.	
Temperature values are copied in succession in the standard PLC	A corrupt value within the TwinSAFE SC communication results in an invalid CRC inside the telegram and thus the immediate switch-off of the group and the outputs	
Temperature value via the standard fieldbus is corrupted	Detected via the second value and the plausibility check in the EL6910.	
There is no longer any connection between the sensor and the EtherCAT terminal	Detected within the EL6910 via the plausibility check with the second temperature value.	
PT1000 supplies an incorrect temperature value	Detected within the EL6910 via the plausibility check with the second temperature value.	
Thermocouple supplies an incorrect temperature value	Detected within the EL6910 via the plausibility check with the second temperature value.	
Communication error 61784-3 for standard communication: Corruption	Is detected via 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	Is detected via the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910.	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Wrong sequence	Is detected via the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Loss	Is detected via 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	Is detected via the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Insertion	Is detected via 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	Is detected via 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	Is detected via the plausibility check of the temperature values and via the TwinSAFE SC communication within the EL6910.	

### 2.29.3.1 Note about 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. This polynomial is sufficiently independent of the polynomial 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.

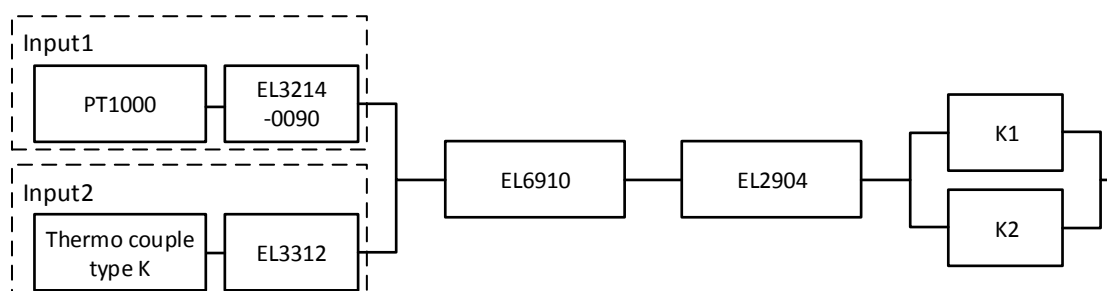
## 2.29.4 Parameters of the safe output terminal

### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

## 2.29.5 Block formation and safety loops

### 2.29.5.1 Safety function 1



## 2.29.6 Calculation

### 2.29.6.1 PFH / MTTF<sub>D</sub> / B10<sub>D</sub> – values

Component	Value
EL2904 – PFH	1,25E-09
EL6910 – PFH	1,79E-09
PT1000 – MTTF <sub>D</sub>	7.618 a (acc. to table C.5 EN ISO 13849-1:2015)
Thermocouple Type K – FIT	1900 (Amount of errors in 10 <sup>9</sup> hours)
EL3214-0090 - MTBF	890.000
EL3312 - MTBF	1.661.253
K1 – B10 <sub>D</sub>	1.300.000
K2 – B10 <sub>D</sub>	1.300.000
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

### 2.29.6.2 Diagnostic Coverage DC

Component	Value
Temperature values over TwinSAFE SC and plausibility check inside the logic	DC <sub>avg</sub> =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 <sub>avg</sub> =99%

### 2.29.6.3 Calculation safety function 1

For clarification, the safety parameter is calculated according to both EN62061 and EN13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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 and MTTF<sub>D</sub> 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:

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

results in:

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

Inserting the values, this produces:

#### PT1000

$$MTTF_D = 7618 \text{ y} = 66.733.680 \text{ h}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{66.733.680 \text{ h}} = 1,50E - 09$$

#### EL3214-0090

$$MTTF_D = 2 * MTBF = 2 * 890.000 \text{ h} = 1.780.000 \text{ h} = 203 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.780.000 \text{ h}} = 5,62E - 08$$

#### Input 1 subsystem

$$PFH_{(Input1)} = PFH_{(PT1000)} + PFH_{(EL3214-0090)} = 1,5E - 09 + 5,62E - 08 = 5,77E - 08$$

#### Thermo couple

$$MTTF_D = \frac{1}{\lambda_D} = \frac{1}{1900 \text{ FIT}} * 10^9 \text{ h} = 526.315 \text{ h} = 60 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{526.315 \text{ h}} = 19,0E - 08$$

#### EL3312

$$MTTF_D = 2 * MTBF = 2 * 1.661.253 \text{ h} = 3.322.506 \text{ h} = 379 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.322.506 \text{ h}} = 3,0E - 08$$

#### Input 2 subsystem

$$PFH_{(Input2)} = PFH_{(Thermocouple)} + PFH_{(EL3312)} = 19,0E - 08 + 3,0E - 08 = 22,0E - 08$$

#### K1/K2

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

$$MTTF_D = \frac{1300000}{0,1 * 21,90} = 593.607 \text{ y} = 5.199.997.320 \text{ h}$$

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 B10d values for K1 and K2 are identical.

The input signals from PT1000 with EL3214-0090 and thermocouple with EL3312 have different measuring methods, provide both temperature values and are both involved in the safety function. A non-functioning of a channel does not lead to a dangerous situation, but is detected by the comparison of the two values in the TwinSAFE logic and leads to a 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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly. For the input subsystem an estimated value of 2% can be achieved by processing the table to calculate the  $\beta$  factor. In the following calculation, the worst case is assumed to be 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)

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{5,77E - 08 + 22,0E - 08}{2} + 1,79E - 9 + 1,25E - 9 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 1,3885E - 08 + 1,79E - 09 + 1,25E - 9 + 1,92E - 13$$

$$PFH_{ges} = 1,693E - 08$$



#### Note

#### EN 62061

In accordance with EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This restricts the achievable SIL value according to table 5 of EN 62061 to a maximum SIL 2.



Alternative calculation of the  $MTTF_d$  value according to EN13849 for safety function 1 (with the same assumption), with:

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

From the input subsystem, the poorer value is taken:

$$\frac{1}{MTTF_{D ges}} = \frac{1}{MTTF_{D (Thermocouple)}} + \frac{1}{MTTF_{D (EL3312)}} + \frac{1}{MTTF_{D (EL6910)}} + \frac{1}{MTTF_{D (EL2904)}} + \frac{1}{MTTF_{D (K1)}}$$

If only PFH values are available for EL2904 and EL6910, the following estimation applies:

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

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637 y$$

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

$$MTTF_{D ges} = \frac{1}{\frac{1}{60} + \frac{1}{379} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593.607}} = 45,5 y$$


$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(PT1000)}} + \frac{DC}{MTTF_{D(EL3214)}} + \frac{DC}{MTTF_{D(TC)}} + \frac{DC}{MTTF_{D(EL3312)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(PT1000)}} + \frac{1}{MTTF_{D(EL3214)}} + \frac{1}{MTTF_{D(TC)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{0,9}{7.618} + \frac{0,9}{203} + \frac{0,9}{60} + \frac{0,9}{379} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{7.618} + \frac{1}{203} + \frac{1}{60} + \frac{1}{379} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0246}{0,0270} = 91,11\%$$

Alternatively with DC=99%

$$DC_{avg} = \frac{\frac{0,99}{7.618} + \frac{0,99}{203} + \frac{0,99}{60} + \frac{0,99}{379} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{7.618} + \frac{1}{203} + \frac{1}{60} + \frac{1}{379} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0268}{0,0270} = 99,26\%$$

 <b>CAUTION</b>	<b>Category</b>  This structure is possible up to category 3 at the most.
---	---

DC=90% for the input subsystem

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
<b>medium</b>	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	<b>none</b>	<b>none</b>	<b>low</b>	<b>medium</b>	<b>low</b>	<b>medium</b>	<b>high</b>
<b>low</b>	a	-	a	b	b	c	-
<b>medium</b>	b	-	b	c	c	d	-
<b>high</b>	-	c	c	d	d	<b>d</b>	e

Alternatively with DC=99% for the input subsystem

Designation for each channel	MTTF <sub>d</sub>
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

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 <sub>d</sub>	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

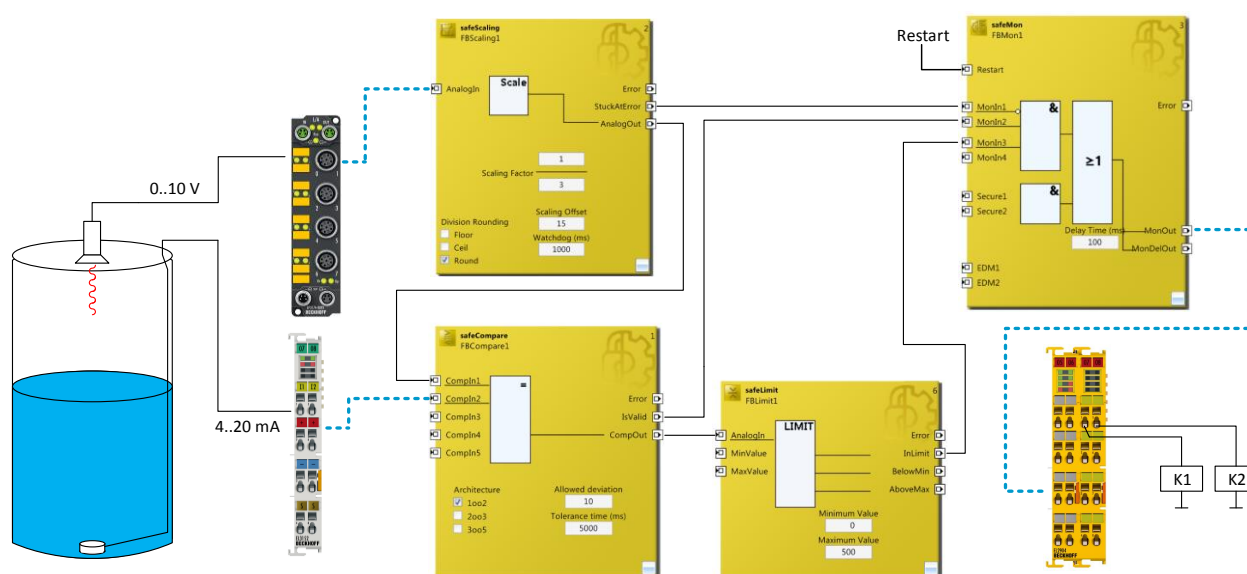
Safety integrity level	Safety integrity level according to Tab. 3 EN62061
3	Probability of a dangerous failure per hour (PFH <sub>D</sub> ) ≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.30 Level measurement with TwinSAFE SC (Category 3, PL d)

In this example we will show how a level measurement with the TwinSAFE SC technology can be realized. Two different measurement methods are used for this purpose. On the one hand an ultrasonic sensor with a 0 - 10 V interface, which is wired to a TwinSAFE SC EtherCAT box EP3174-0092 is used, and on the other hand a level probe with 4-20 mA interface, which is wired to a standard EtherCAT terminal EL3152.

Within the safe TwinSAFE EL6910 logic, these two signals are compared or plausibilized using a Compare function block. The signal from EP3174-0092 is previously scaled via the scale function block so that the two signals have an identical value range. The signal is then checked via the FB limit. The result of the FB limit and the IsValid output of the Compare function block are used to switch off the contactors K1 and K2 via the function block Mon. In addition, the StuckAtError output of the scale function block can also be placed on a Mon input. This means that a freezing of the signal can be detected.

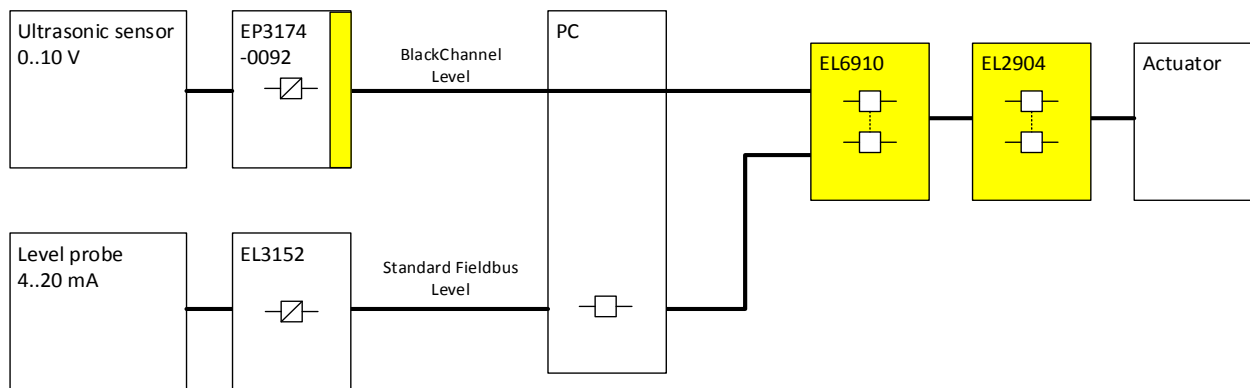
The monitoring of the contactor feedback is not shown in this example for the sake of clarity, but must be considered by the user



### Emergency stop / contactor feedback monitor

In addition to the function shown above, a contactor feedback monitor, e.g. via an EDM function block for K1 and K2 and, if necessary, an emergency stop function must be implemented by the user!

### 2.30.1 Diagram of the structure



### 2.30.2 Structure and diagnosis

The read signals from the two measuring points are standard signals using a different technology. At least one signal is transmitted via the TwinSAFE SC technology to the safe TwinSAFE logic so that falsifications of this signal in the PC or on the transmission path are detected. The check for equality of these two signals, within the permissible tolerances, is performed in the safe TwinSAFE logic.

The individual fault assumptions and associated expectations are listed in the following FMEA table

### 2.30.3 FMEA

Error assumption	Expectations	Checked
Level value over standard fieldbus itself freezes	Detected via the second value and the plausibility check in the EL6910.	
Level value over TwinSAFE SC communication freezes	Detected by the watchdog within the TwinSAFE SC communication and by the plausibility check in the EL6910.	
Level values are copied in succession in the standard PLC	A corrupt value within the TwinSAFE SC communication results in an invalid CRC inside the telegram and thus the immediate switch-off of the group and the outputs	
Level value via the standard fieldbus is corrupted	Detected via the second value and the plausibility check in the EL6910.	
There is no longer any connection between the sensor and the EtherCAT terminal	Detected within the EL6910 via the plausibility check with the second level value.	
Ultrasonic sensor supplies an incorrect level value	Detected within the EL6910 via the plausibility check with the second level value.	
Level probe supplies an incorrect level value	Detected within the EL6910 via the plausibility check with the second level value.	
Communication error 61784-3 for standard communication: Corruption	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Unintentional repetition	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Wrong sequence	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Loss	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Unacceptable delay	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Insertion	Is detected via the plausibility check of the 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	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	
Communication error for standard communication: Recurrent memory errors in switches	Is detected via the plausibility check of the level values and via the TwinSAFE SC communication within the EL6910.	

### 2.30.3.1 Note about 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. This polynomial is sufficiently independent of the polynomial 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.

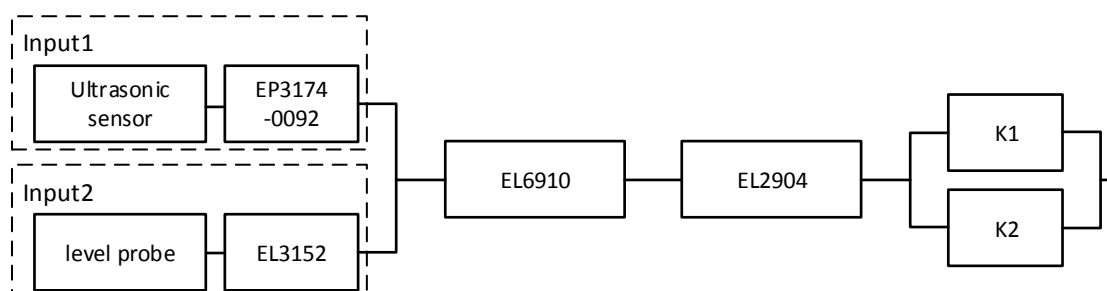
## 2.30.4 Parameters of the safe output terminal

### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

## 2.30.5 Block formation and safety-loops

### 2.30.5.1 Safety function 1



## 2.30.6 Calculation

### 2.30.6.1 PFH / MTTF<sub>D</sub> / B10<sub>D</sub> – values

Component	Value
EL2904 – PFH	1,25E-09
EL6910 – PFH	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 <sub>D</sub>	1.300.000 h
K2 – B10 <sub>D</sub>	1.300.000 h
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

### 2.30.6.2 Diagnostic Coverage DC

Component	Value
Level values over TwinSAFE SC and plausibility check inside the logic	DC <sub>avg</sub> =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 <sub>avg</sub> =99%

### 2.30.6.3 Calculation safety function 1

For clarification, the safety parameter is calculated according to both EN62061 and EN13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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 and MTTF<sub>D</sub> 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:

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

results in

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



Inserting the values, this produces:

#### Ultrasonic sensor

$$MTTF_D = 2 * MTBF = 2 * 195 \text{ y} = 390 \text{ y} = 3.416.400 \text{ h}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.416.400 \text{ h}} = 2,93E - 08$$

#### EP3174-0092

$$MTTF_D = 2 * MTBF = 2 * 600.000 \text{ h} = 1.200.000 \text{ h} = 136 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.200.000 \text{ h}} = 8,33E - 08$$

#### Input 1 subsystem

$$PFH_{(Input1)} = PFH_{(Ultrasonic)} + PFH_{(EP3174-0092)} = 2,93E - 08 + 8,33E - 08 = 11,26E - 08$$

#### Level probe

$$MTTF_D = 2 * MTTF = 2 * 732 \text{ y} = 1.464 \text{ y} = 12.824.640 \text{ h}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{12.824.640 \text{ h}} = 7,79E - 09$$

#### EL3152

$$MTTF_D = 2 * MTBF = 2 * 2.507.303 \text{ h} = 5.014.606 \text{ h} = 572 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{5.014.606 \text{ h}} = 1,99E - 08$$

#### Input 2 subsystem

$$PFH_{(Input2)} = PFH_{(level \text{ probe})} + PFH_{(EL3152)} = 7,79E - 09 + 1,99E - 08 = 2,77E - 08$$

#### K1/K2

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

$$MTTF_D = \frac{1300000}{0,1 * 21,90} = 593.607 \text{ y} = 5.199.997.320 \text{ h}$$

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 B10d values for K1 and K2 are identical.

The input signals from ultrasonic sensor with EP3174-0092 and level probe with EL3152 have different measuring methods, provide both level values and are both involved in the safety function. A non-functioning of a channel does not lead to a dangerous situation, but is detected by the comparison of the two values in the TwinSAFE logic and leads to a 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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly. For the input subsystem an estimated value of 2% can be achieved by processing the table to calculate the  $\beta$  factor. In the following calculation, the worst case is assumed to be 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)

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{11,26E - 08 + 2,77E - 08}{2} + 1,79E - 9 + 1,25E - 9 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 7,015E - 09 + 1,79E - 09 + 1,25E - 9 + 1,92E - 13$$

$$PFH_{ges} = 1,005E - 08$$



#### Note

#### EN 62061

In accordance with EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This restricts the achievable SIL value according to table 5 of EN 62061 to a maximum SIL 2.

Alternative calculation of the  $MTTF_d$  value according to EN13849 for safety function 1 (with the same assumption), with:

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

From the input subsystem, the poorer value is taken:

$$\frac{1}{MTTF_{D ges}} = \frac{1}{MTTF_{D (Ultrasonic sensor)}} + \frac{1}{MTTF_{D (EP3174-0092)}} + \frac{1}{MTTF_{D (EL6910)}} + \frac{1}{MTTF_{D (EL2904)}} + \frac{1}{MTTF_{D (K1)}}$$

If only PFH values are available for EL2904 and EL6910, the following estimation applies:

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

Hence:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637 y$$

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

$$MTTF_{D ges} = \frac{1}{\frac{1}{390} + \frac{1}{136} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593.607}} = 79,46 y$$


$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(UltraSonic)}} + \frac{DC}{MTTF_{D(EP3174)}} + \frac{DC}{MTTF_{D(level probe)}} + \frac{DC}{MTTF_{D(EL3152)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(UltraSonic)}} + \frac{1}{MTTF_{D(EP3174)}} + \frac{1}{MTTF_{D(level probe)}} + \frac{1}{MTTF_{D(EL3152)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{0,9}{390} + \frac{0,9}{136} + \frac{0,9}{1464} + \frac{0,9}{572} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{390} + \frac{1}{136} + \frac{1}{1464} + \frac{1}{572} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0137}{0,0150} = 91,33\%$$

Alternatively with DC=99%

$$DC_{avg} = \frac{\frac{0,99}{390} + \frac{0,99}{136} + \frac{0,99}{1464} + \frac{0,99}{572} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{390} + \frac{1}{136} + \frac{1}{1464} + \frac{1}{572} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,01486}{0,0150} = 99,06\%$$

 <b>CAUTION</b>	<b>Category</b>  This structure is possible up to category 3 at the most.
---	---

DC=90% for the input subsystem

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
<b>medium</b>	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	<b>none</b>	<b>none</b>	<b>low</b>	<b>medium</b>	<b>low</b>	<b>medium</b>	<b>high</b>
<b>low</b>	a	-	a	b	b	c	-
<b>medium</b>	b	-	b	c	c	d	-
<b>high</b>	-	c	c	d	d	<b>d</b>	e

Alternatively with DC=99% for the input subsystem

Designation for each channel	MTTF <sub>d</sub>
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
high	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

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 <sub>d</sub>	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

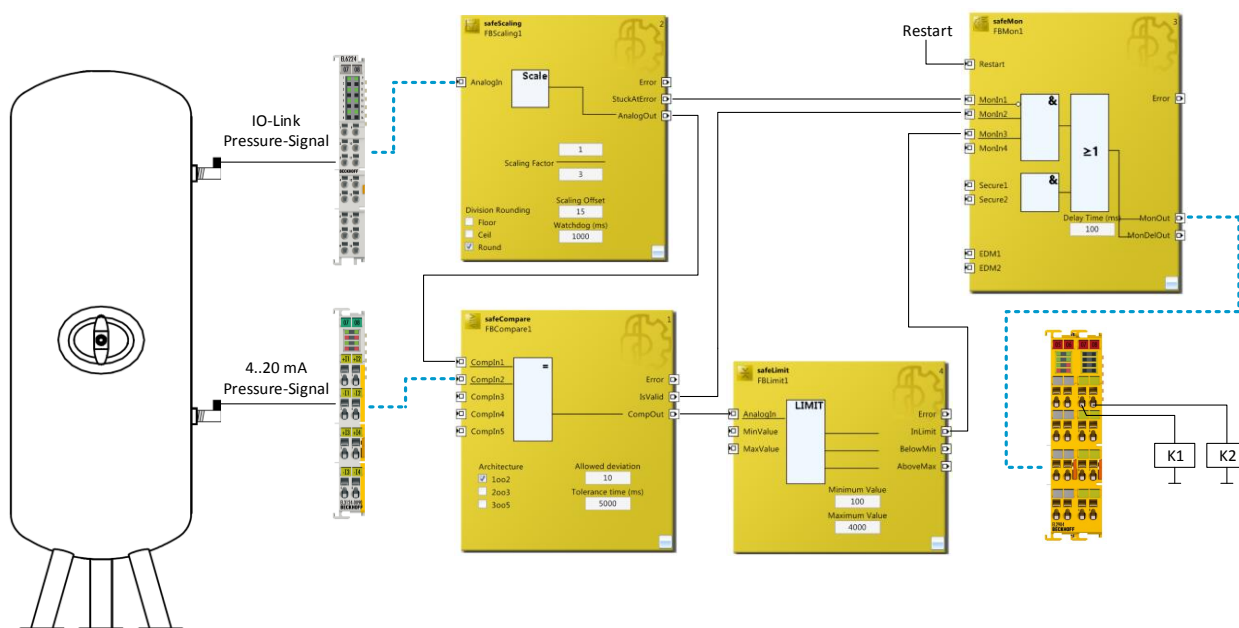
Safety integrity level	Safety integrity level according to Tab. 3 EN62061
3	Probability of a dangerous failure per hour (PFH <sub>D</sub> ) ≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
2	≥ 10 <sup>-7</sup> to < 10 <sup>-6</sup>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.31 Pressure measurement with TwinSAFE SC (Category 3, PL d)

In this example we will show how a pressure measurement with the TwinSAFE SC technology can be realized. For this purpose, two measuring points are equipped with pressure sensors, on the one hand with a pressure sensor with IO-Link interface, which is wired to a standard EtherCAT terminal EL6224, and on the other hand a pressure sensor with 4..20 mA interface, which is wired to a TwinSAFE SC EtherCAT terminal EL3124-0090.

Within the safe TwinSAFE EL6910 logic, these two signals are compared or plausibilized using a Compare function block. The signal from EL6224 is previously scaled via the scale function block so that the two signals have an identical value range. The signal is then checked via the FB limit. The result of the FB limit and the IsValid output of the Compare function block are used to switch off the contactors K1 and K2 via the function block Mon. In addition, the StuckAtError output of the scale function block can also be placed on a Mon input. This means that a freezing of the signal can be detected.

The monitoring of the contactor feedback is not shown in this example for the sake of clarity, but must be considered by the user



### Safety valve (PSV - Pressure Safety Valve)

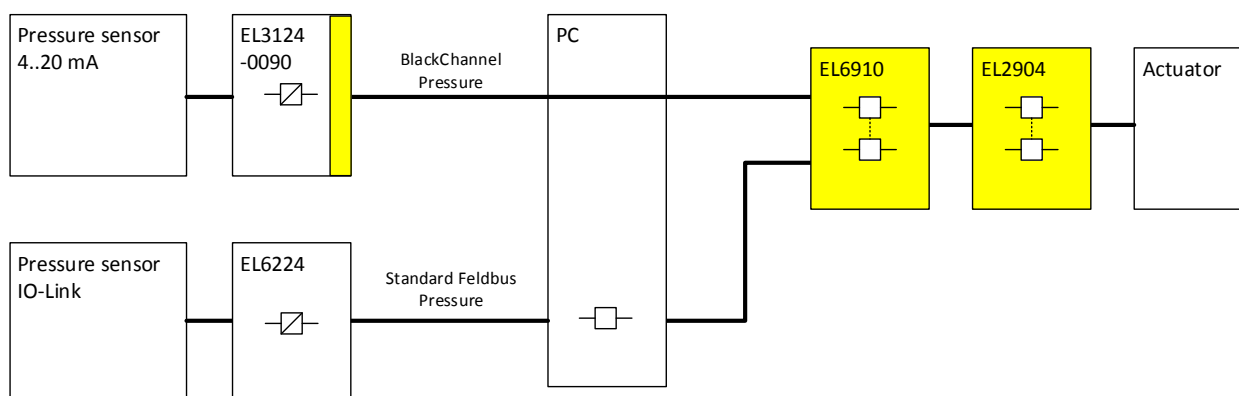
The application shown above cannot be used as a replacement for a safety valve according to the EC Pressure Equipment Directive.



### Emergency stop / contactor feedback monitor

In addition to the function shown above, a contactor feedback monitor, e.g. via an EDM function block for K1 and K2 and, if necessary, an emergency stop function must be implemented by the user!

### 2.31.1 Diagram of the structure



### 2.31.2 Structure and diagnosis

The read signals from the two measuring points are standard signals using a different technology. At least one signal is transmitted via the TwinSAFE SC technology to the safe TwinSAFE logic so that falsifications of this signal in the PC or on the transmission path are detected. The check for equality of these two signals, within the permissible tolerances, is performed in the safe TwinSAFE logic.

The individual fault assumptions and associated expectations are listed in the following FMEA table

### 2.31.3 FMEA

Error assumption	Expectations	Checked
Pressure value over standard fieldbus itself freezes	Detected via the second value and the plausibility check in the EL6910.	
Pressure value over TwinSAFE SC communication freezes	Detected by the watchdog within the TwinSAFE SC communication and by the plausibility check in the EL6910.	
Pressure values are copied in succession in the standard PLC	A corrupt value within the TwinSAFE SC communication results in an invalid CRC inside the telegram and thus the immediate switch-off of the group and the outputs	
Pressure value via the standard fieldbus is corrupted	Detected via the second value and the plausibility check in the EL6910.	
There is no longer any connection between the sensor and the EtherCAT terminal	Detected within the EL6910 via the plausibility check with the second pressure value.	
Pressure sensor (4..20mA) supplies an incorrect pressure value	Detected within the EL6910 via the plausibility check with the second pressure value.	
Pressure sensor (IO-Link) supplies an incorrect pressure value	Detected within the EL6910 via the plausibility check with the second pressure value.	
Communication error 61784-3 for standard communication: Corruption	Is detected via the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910.	

Error assumption	Expectations	Checked
Communication error 61784-3 for standard communication: Unintentional repetition	Is detected via 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	Is detected via the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Loss	Is detected via 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	Is detected via the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Insertion	Is detected via 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	Is detected via 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	Is detected via the plausibility check of the pressure values and via the TwinSAFE SC communication within the EL6910.	

### 2.31.3.1 Note about 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. This polynomial is sufficiently independent of the polynomial 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.



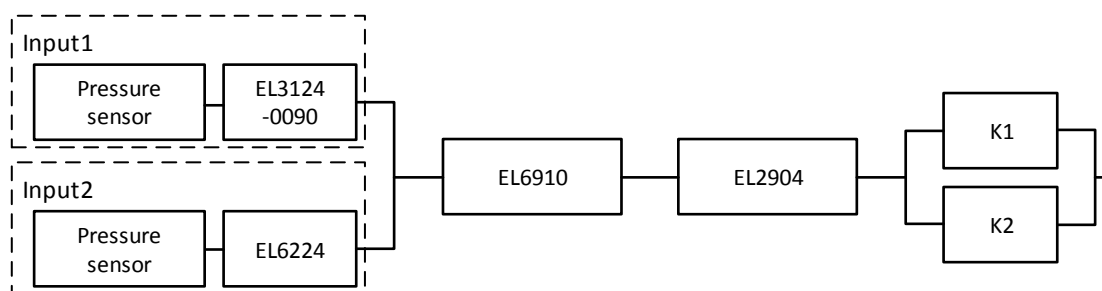
## 2.31.4 Parameters of the safe output terminal

### EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

## 2.31.5 Block formation and safety-loops

### 2.31.5.1 Safety function 1



## 2.31.6 Calculation

### 2.31.6.1 PFH / MTTF<sub>D</sub> / B10<sub>D</sub> – values

Component	Value
EL2904 – PFH	1,25E-09
EL6910 – PFH	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 <sub>D</sub>	1.300.000 h
K2 – B10 <sub>D</sub>	1.300.000 h
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>Zyklus</sub> )	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

### 2.31.6.2 Diagnostic Coverage DC

Component	Value
Pressure values over TwinSAFE SC and plausibility check inside the logic	DC <sub>avg</sub> =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 <sub>avg</sub> =99%

### 2.31.6.3 Calculation safety function 1

For clarification, the safety parameter is calculated according to both EN62061 and EN13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH and MTTF<sub>d</sub> values from the B10<sub>d</sub> 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 and MTTF<sub>D</sub> 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

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

results in

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

Inserting the values, this produces:

#### Pressure sensor 1 (4-20mA)

$$MTTF_D = 2 * MTTF = 2 * 124 \text{ y} = 248 \text{ y} = 2.172.480 \text{ h}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.172.480 \text{ h}} = 4,60E - 08$$

#### EL3124-0090

$$MTTF_D = 2 * MTBF = 2 * 950.000 \text{ h} = 1.900.000 \text{ h} = 216 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.900.000 \text{ h}} = 5,26E - 08$$

#### Input 1 subsystem

$$PFH_{(Input1)} = PFH_{(Pressure\ sensor1)} + PFH_{(EL3124-0090)} = 4,60E - 08 + 5,26E - 08 = 9,86E - 08$$

#### Pressure sensor 2 (IO-Link)

$$MTTF_D = 2 * MTBF = 2 * 1.760.760 \text{ h} = 3.521.520 \text{ h} = 402 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.521.520 \text{ h}} = 2,84E - 08$$

#### EL6224

$$MTTF_D = 2 * MTBF = 2 * 1.607.919 \text{ h} = 3.215.838 \text{ h} = 367 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.215.838 \text{ h}} = 3,11E - 08$$

#### Input 2 subsystem

$$PFH_{(Input2)} = PFH_{(Pressure\ sensor2)} + PFH_{(EL6224)} = 2,84E - 08 + 3,11E - 08 = 5,95E - 08$$

#### K1/K2

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

$$MTTF_D = \frac{1300000}{0,1 * 21,90} = 593.607 \text{ y} = 5.199.997.320 \text{ h}$$

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 B10d values for K1 and K2 are identical.

The input signals from pressure sensor 1 with EL3124-0090 and pressure sensor 2 with EL6224 have different measuring methods, provide both pressure values and are both involved in the safety function. A non-functioning of a channel does not lead to a dangerous situation, but is detected by the comparison of the two values in the TwinSAFE logic and leads to a 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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly. For the input subsystem an estimated value of 2% can be achieved by processing the table to calculate the  $\beta$  factor. In the following calculation, the worst case is assumed to be 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)

This produces for the calculation of the PFH 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:

$$PFH_{ges} = 10\% * \frac{9,86E - 08 + 5,95E - 08}{2} + 1,79E - 9 + 1,25E - 9 + 10\% * \frac{1,92E - 12 + 1,92E - 12}{2} \\ = 7,905E - 09 + 1,79E - 09 + 1,25E - 9 + 1,92E - 13$$

$$PFH_{ges} = 1,094E - 08$$



#### Note

#### EN 62061

In accordance with EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This restricts the achievable SIL value according to table 5 of EN 62061 to a maximum SIL 2.

Alternative calculation of the  $MTTF_d$  value according to EN13849 for safety function 1 (with the same assumption), with:

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

From the input subsystem, the poorer value is taken:

$$\frac{1}{MTTF_{D ges}} = \frac{1}{MTTF_{D (PressureSensor1)}} + \frac{1}{MTTF_{D (EL3124-0090)}} + \frac{1}{MTTF_{D (EL6910)}} + \frac{1}{MTTF_{D (EL2904)}} + \frac{1}{MTTF_{D (K1)}}$$

If only PFH values are available for EL2904 and EL6910, the following estimation applies:

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

Hence:

$$MTTF_{D (EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637 y$$

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

$$MTTF_{D ges} = \frac{1}{\frac{1}{248} + \frac{1}{216} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593.607}} = 88,27 y$$


$$DC_{avg} = \frac{\frac{DC}{MTTF_{D (Pressure 1)}} + \frac{DC}{MTTF_{D (EL3124)}} + \frac{DC}{MTTF_{D (Pressure 2)}} + \frac{DC}{MTTF_{D (EL6224)}} + \frac{DC}{MTTF_{D (EL6910)}} + \frac{DC}{MTTF_{D (EL2904)}} + \frac{DC}{MTTF_{D (K1)}} + \frac{DC}{MTTF_{D (K2)}}}{\frac{1}{MTTF_{D (Pressure 1)}} + \frac{1}{MTTF_{D (EL3124)}} + \frac{1}{MTTF_{D (Pressure 2)}} + \frac{1}{MTTF_{D (EL6224)}} + \frac{1}{MTTF_{D (EL6910)}} + \frac{1}{MTTF_{D (EL2904)}} + \frac{1}{MTTF_{D (K1)}} + \frac{1}{MTTF_{D (K2)}}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{0,9}{248} + \frac{0,9}{216} + \frac{0,9}{402} + \frac{0,9}{367} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{248} + \frac{1}{216} + \frac{1}{402} + \frac{1}{367} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,01512}{0,01654} = 91,41\%$$

Alternatively with DC=99%

$$DC_{avg} = \frac{\frac{0,99}{248} + \frac{0,99}{216} + \frac{0,99}{402} + \frac{0,99}{367} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{248} + \frac{1}{216} + \frac{1}{402} + \frac{1}{367} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,01637}{0,01654} = 98,97\%$$

 <b>CAUTION</b>	<b>Category</b>  This structure is possible up to category 3 at the most.
---	---

DC=90% for the input subsystem

Designation for each channel	MTTF <sub>d</sub> Range for each channel
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	30 years ≤ MTTF <sub>d</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
<b>medium</b>	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>d</sub>	<b>none</b>	<b>none</b>	<b>low</b>	<b>medium</b>	<b>low</b>	<b>medium</b>	<b>high</b>
<b>low</b>	a	-	a	b	b	c	-
<b>medium</b>	b	-	b	c	c	d	-
<b>high</b>	-	c	c	d	d	<b>d</b>	e

Alternatively with DC=99% for the input subsystem

Designation for each channel	MTTF <sub>d</sub>
low	3 years ≤ MTTF <sub>d</sub> < 10 years
medium	10 years ≤ MTTF <sub>d</sub> < 30 years
<b>high</b>	<b>30 years ≤ MTTF<sub>d</sub> ≤ 100 years</b>

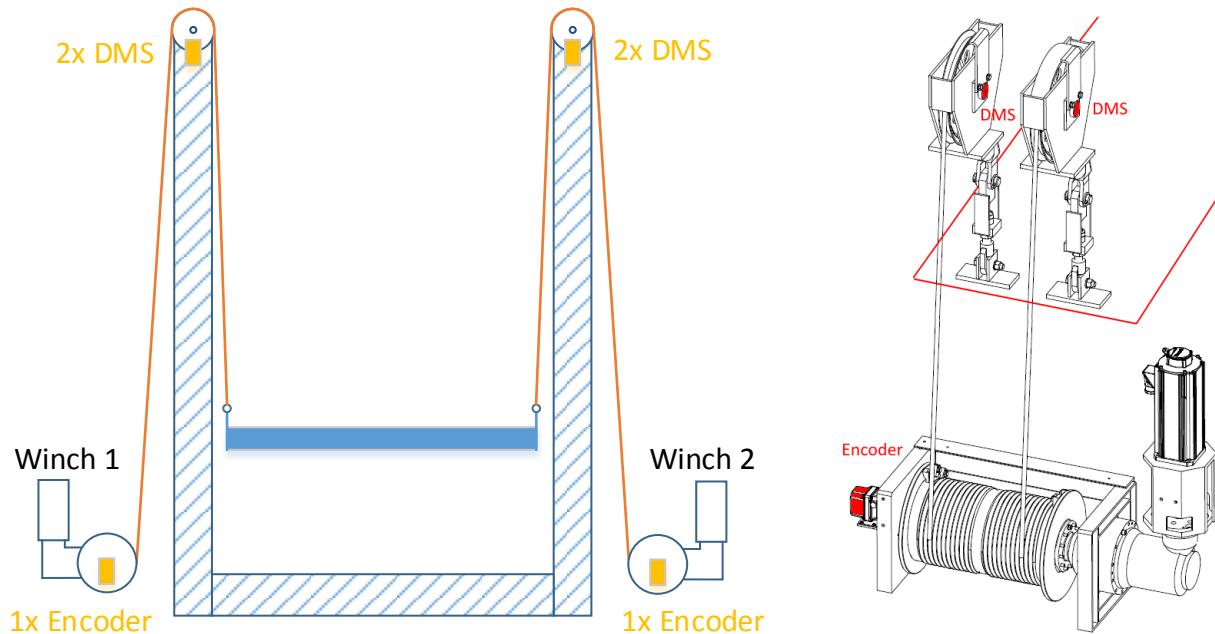
Designation	DC <sub>avg</sub>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
<b>high</b>	<b>99 % ≤ DC</b>
For practical usability, the number of the ranges was limited to four. An accuracy of 5% is assumed for the limit values shown in this table.	

Category	B	1	2	2	3	3	4
DC MTTF <sub>d</sub>	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	Safety integrity level according to Tab. 3 EN62061 Probability of a dangerous failure per hour (PFH <sub>D</sub> )
3	≥ 10 <sup>-8</sup> to < 10 <sup>-7</sup>
<b>2</b>	<b>≥ 10<sup>-7</sup> to &lt; 10<sup>-6</sup></b>
1	≥ 10 <sup>-6</sup> to < 10 <sup>-5</sup>

## 2.32 Monitoring lifting device (Category 3, PL d)

A lifting device consisting of 2 winches with deflection pulleys for moving a lifting table, should be monitored in a safe way. The functions of slack rope detection and overload are to be implemented. There are 2 deflection pulleys with a strain gauge (DMS) sensor on the top of each side of the post, thus in sum 4 strain gauge sensors. One of these two sensors on one side is read with a TwinSAFE SC terminal EL3356-0090. The other strain gauge sensor is wired to an EL3751. This provides a strain gauge 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. For this purpose, after the plausibility check of the EL3751 and EL3356-0090 signals, a limitation of the result is made with the limit FB in the EL6910.

According to the risk and hazard analysis of the customer, this safety function is to be assessed with PL c according to EN 13849-1:2015.

The safety function is built up in a category 3 structure.

### Safety function 2 - Slack rope detection

A slack-rope detection is used to detect whether the lifting sled has been mechanically suspended or is standing on the ground. In either case, a turn off must be done immediately. In addition, it also detects whether a rope is torn.

According to the risk and hazard analysis of the customer, this safety function is to be assessed with PL c according to EN 13849-1:2015.

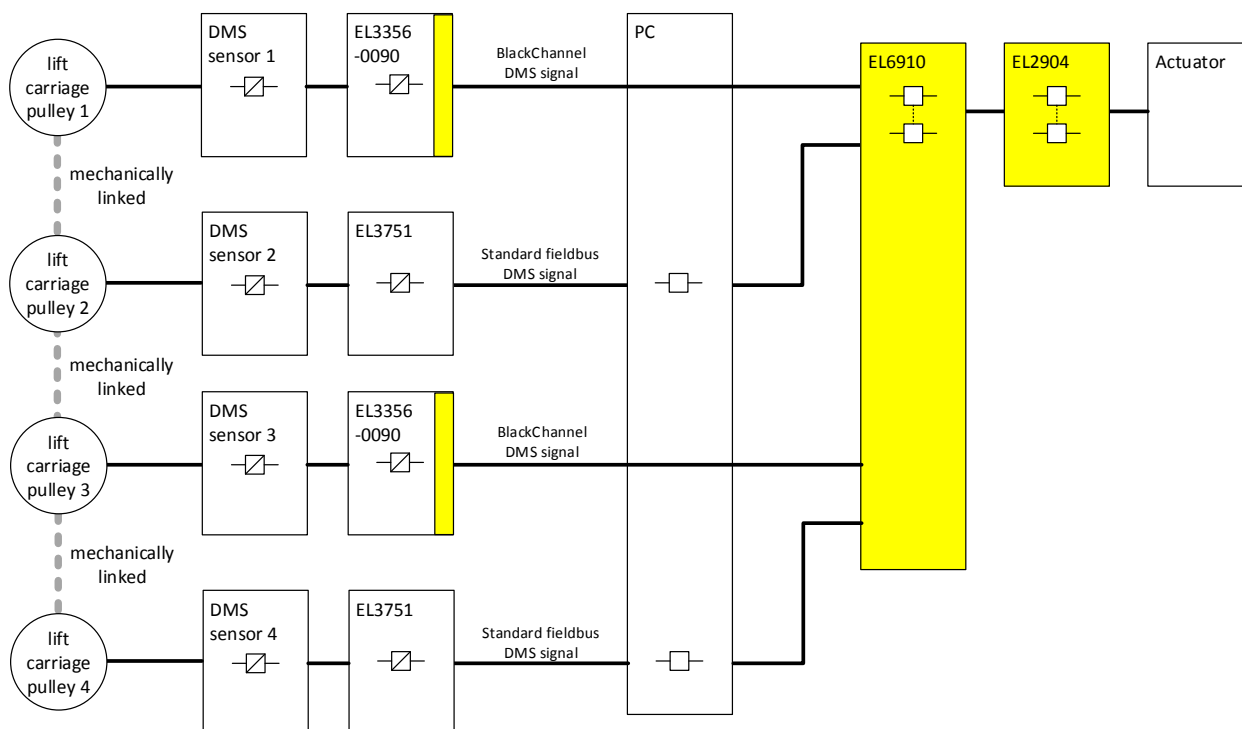
The safety function is built up in a category 3 structure.

### Additional function - without safety requirements

By incremental comparison of the encoder values of winch 1 and 2, a synchronous operation can be checked. This prevents an oblique movement of the lifting sled by the two winches at an early stage.



### 2.32.1 Diagram of the structure



### 2.32.2 Structure and diagnosis

The read-in signals of the strain gauge sensors are standard signals that are recorded differently per side. The first strain gauge sensor is wired to a strain gauge terminal EL3356-0090 which packs the determined weight value into a safe telegram (FSOE with modified polynomial - TwinSAFE SC) and transmits it to the EL6910. The second strain gauge sensor is wired to a terminal EL3751, which performs a strain gauge mV / V measurement. This signal is sent to the EL6910 via the standard communication path. This signal is converted into a weight value before the plausibility check within the safe logic.

The second side of the lifting device with strain gauge sensor 3 and 4 is identical. For the TwinSAFE SC communication of the second EL3356-0090 a different polynomial compared to the first side is used. This is done to detect that the data of both TwinSAFE SC connections is not copied on each other.

### 2.32.3 FMEA

Error assumption	Expectations	Checked
Strain gauge signal over standard fieldbus itself freezes	Detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC Communication between EL3356-0090 and EL6910).	
Strain gauge signal over TwinSAFE SC communication freezes	Detected via the second value and the plausibility check in the EL6910 and via the watchdog within the TwinSAFE SC communication	
Strain gauge values are copied in succession in the standard PLC	A corrupt value within the TwinSAFE SC communication results in an invalid CRC inside the telegram and thus the immediate switch-off of the group and the outputs. The data types of the two strain gauge values have a different length because one of the two is packaged in the TwinSAFE SC telegram (for example, 4 bytes and 11 bytes)	
Strain gauge value via the standard fieldbus is corrupted	Detected via the second value and the plausibility check in the EL6910 (TwinSAFE SC Communication between EL3356-0090 and EL6910).	
There is no longer a mechanical connection between the lifting sled and the winch	Detected within the EL6910 via the plausibility check with the second strain gauge value.	
EL3356-0090 supplies an incorrect strain gauge value	Detected via the plausibility check with the strain gauge value of the EL3751 within the EL6910.	
EL3751 supplies an incorrect strain gauge value	Detected via the plausibility check with the strain gauge value of the EL3356-0090 within the EL6910.	
Communication error 61784-3 for standard communication: Corruption	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Unintentional repetition	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Wrong sequence	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Loss	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Unacceptable delay	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	
Communication error 61784-3 for standard communication: Insertion	Is detected via the plausibility check of the strain gauge 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	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	

Error assumption	Expectations	Checked
Communication error for standard communication: Recurrent memory errors in switches	Is detected via the plausibility check of the strain gauge values and via the TwinSAFE SC communication within the EL6910.	

#### 2.32.3.1 Note about 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. This polynomial is sufficiently independent of the polynomial 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.

#### 2.32.4 Structure within the logic

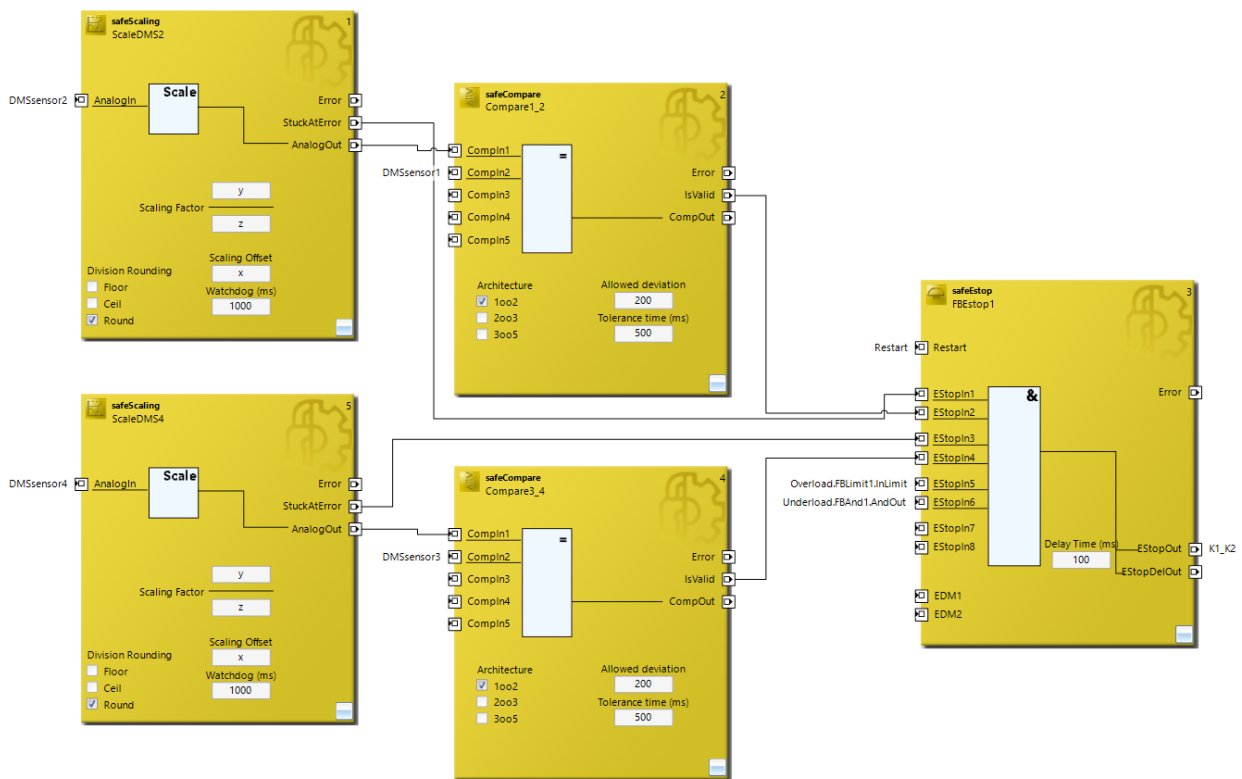
The logic in the EL6910 is divided into 3 parts. In the first section the strain gauge values are scaled and plausibilised. The restart interlock and the shutdown of the contactors K1 and K2 are also included with an ESTOP function block.

In the second section, the total load is determined and monitored via a limit function block to a maximum and minimum. The result is passed to the ESTOP block of the first section.

In the third section, each individual signal is monitored for a minimum value. These 4 signals are linked to the ESTOP block of the first section.

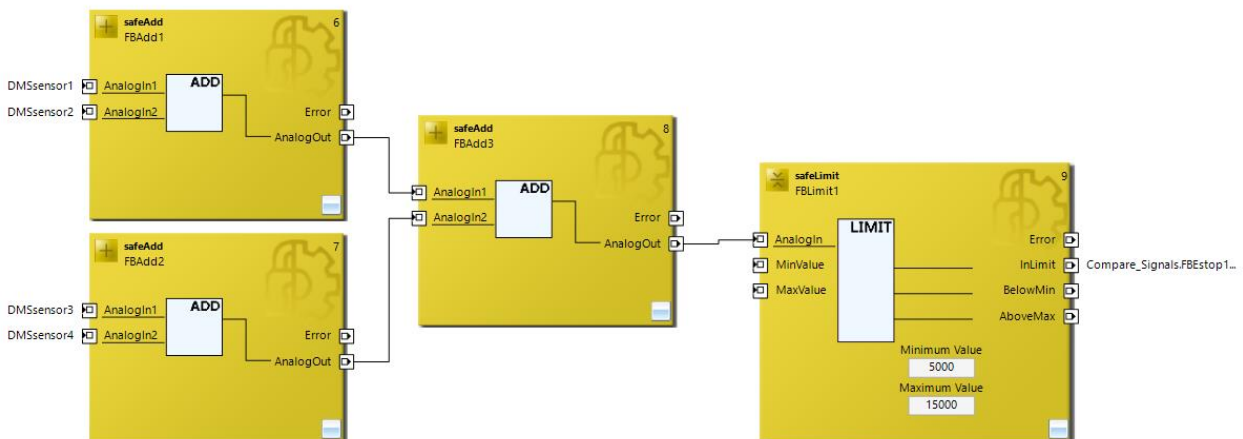
## Section 1

Compare\_Signals

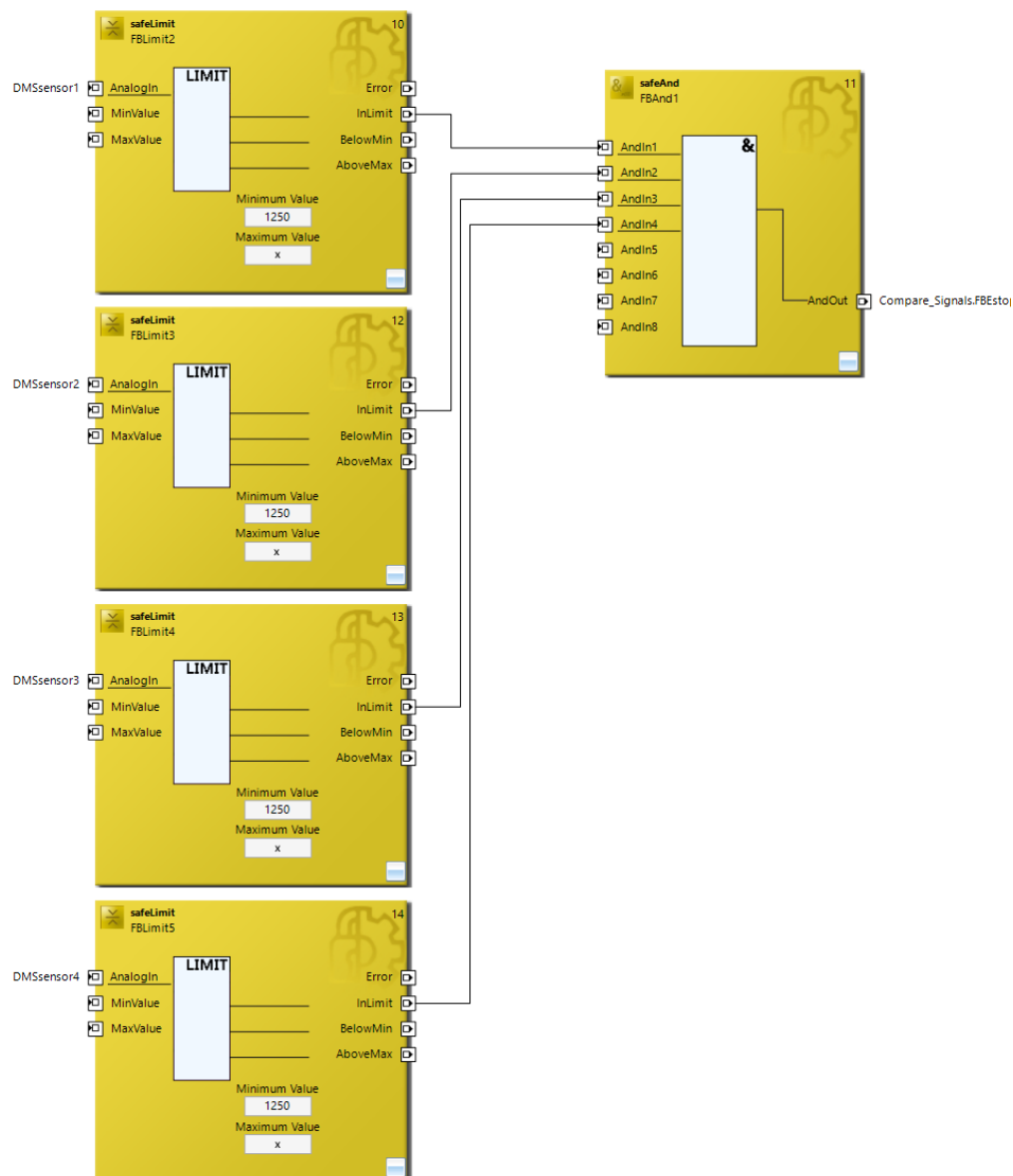


## Section 2

Overload



## Section 3



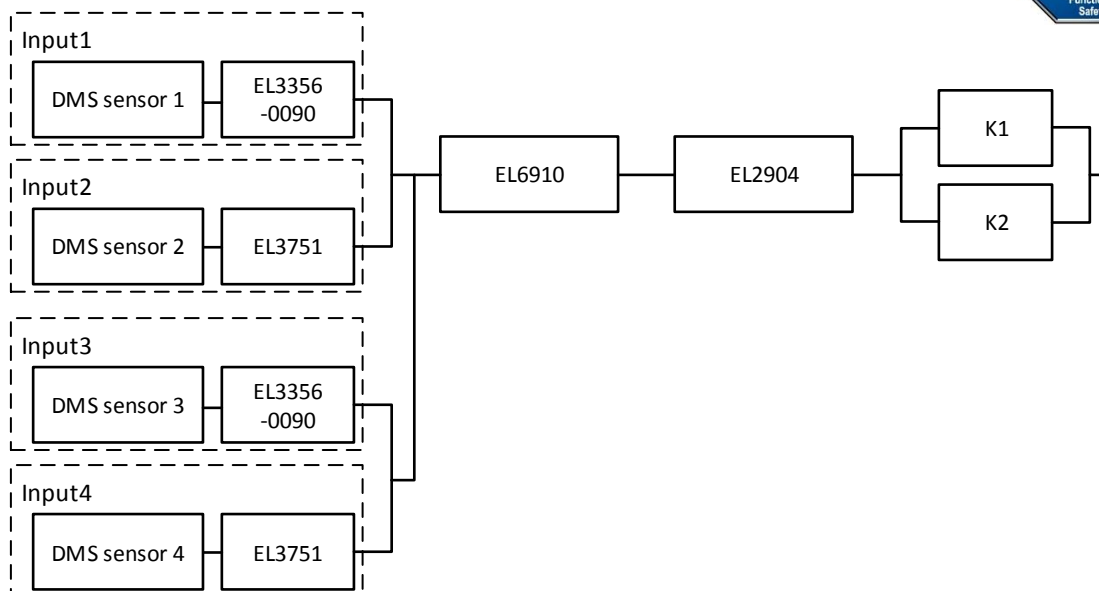
## 2.32.5 Parameters of the safe output terminal

## EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

## 2.32.6 Block formation and safety-loops

### 2.32.6.1 Safety function 1/2



## 2.32.7 Calculation

### 2.32.7.1 PFH / MTTF<sub>D</sub> / B10<sub>D</sub> – values

Component	Value
EL2904 – PFH	1,25E-09
EL6910 – PFH	1,79E-09
Strain gauge Sensor 1-4 – MTTF <sub>D</sub> (AST 3570951.1 KAL/10t/D50d11/L205/1,5mV/V)	160 y (1.401.600 h)
EL3356-0090 - MTBF	780.733 h
EL3751 - MTBF	513.333 h
K1 – B10 <sub>D</sub>	1.300.000 h
K2 – B10 <sub>D</sub>	1.300.000 h
Encoder MTBF	107,5 y (914.700 h)
Days of operation (d <sub>op</sub> )	230
Hours of operation / day (h <sub>op</sub> )	16
Cycle time (minutes) (T <sub>zyklus</sub> )	10080 (1x per week)
Lifetime (T1)	20 years = 175200 hours

### 2.32.7.2 Diagnostic Coverage DC

Component	Value
Strain gauge values over TwinSAFE SC and plausibility check inside the logic	DC <sub>avg</sub> =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 <sub>avg</sub> =99%

### 2.32.7.3 Calculation safety function 1/2

For clarification, the safety parameter is calculated according to both EN62061 and EN13849. Calculation according to one standard is sufficient in practice.

Calculation of the PFH and MTTF<sub>D</sub> values from the B10<sub>D</sub> values:

From:

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

und:

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

Calculation of the PFH and MTTF<sub>D</sub> 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

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

results in

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

Inserting the values, this produces:

#### Strain gauge sensor 1

$$MTTF_D = 1.401.600 \text{ h} = 160 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.401.600 \text{ h}} = 7,13E - 08$$

#### EL3356-0090

$$MTTF_D = 2 * MTBF = 2 * 780.733 \text{ h} = 1.561.466 \text{ h} = 178 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.561.466 \text{ h}} = 6,40E - 08$$

#### Input subsystem 1

$$PFH_{(Input1)} = PFH_{(DMS1)} + PFH_{(EL3356-0090)} = 7,13E - 08 + 6,40E - 08 = 13,53E - 08$$

#### Strain gauge sensor 2

$$MTTF_D = 1.401.600 \text{ h} = 160 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.401.600 \text{ h}} = 7,13E - 08$$

#### EL3751

$$MTTF_D = 2 * MTBF = 2 * 513.333 \text{ h} = 1.026.666 \text{ h} = 117 \text{ y}$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.026.666 \text{ h}} = 9,74E - 08$$

#### Input subsystem 2

$$PFH_{(Input2)} = PFH_{(DMS2)} + PFH_{(EL3751)} = 7,13E - 08 + 9,74E - 08 = 16,87E - 08$$

For input subsystem 3, the values as calculated for input subsystem 1 apply. For input system 4, the values as calculated for input subsystem 2 apply.

#### K1/K2

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

$$MTTF_D = \frac{1300000}{0,1 * 21,90} = 593.607 \text{ y} = 5.199.997.320 \text{ h}$$

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<sub>D</sub> values for K1 and K2 are identical..

The input signals from strain gauge sensor 1 with EL3356-0090 and strain gauge sensor 2 with EL3751 have a different internal structure, have different values (weight value and mV / V value) and are both involved in the safety function. A non-functioning of a channel does not lead to a dangerous situation, but is detected by the comparison of the two values in the TwinSAFE logic and leads to a shutdown. An identical design is used for strain gauge sensors 3 and 4. The sum of the 4 sensors provides the weight value for the overload cut-off. A lowering of the minimum load of a strain gauge sensor leads to slack rope 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 the determination of the CCF and Table F.2 estimation of the CCF factor ( $\beta$ )) with which this  $\beta$  factor can be determined exactly. For the input subsystem an estimated value of 2% can be achieved by processing the table to calculate the  $\beta$  factor. In the following calculation, the worst case is assumed to be 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).

This produces for the calculation of the PFH value for safety function 1 / 2

$$PFH_{DMS\ 1/2} = \beta * \frac{(PFH_{(Input1)} + PFH_{(Input2)})}{2} + (1 - \beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$$

$$PFH_{DMS\ 1/2} = 0,1 * \frac{(13,53E - 08 + 16,87E - 08)}{2} = 1,52E - 08$$

$$PFH_{DMS\ 3/4} = \beta * \frac{(PFH_{(Input3)} + PFH_{(Input4)})}{2} + (1 - \beta)^2 * (PFH_{(Input3)} * PFH_{(Input4)}) * T1$$

$$PFH_{DMS\ 3/4} = 0,1 * \frac{(13,53E - 08 + 16,87E - 08)}{2} = 1,52E - 08$$

$$PFH_{K1/K2} = \beta * \frac{(PFH_{(K1)} + PFH_{(K2)})}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

$$PFH_{K1/K2} = 0,1 * \frac{(1,92E - 12 + 1,92E - 12)}{2} = 1,92E - 13$$

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.

$$PFH_{ges} = PFH_{(DMS\ 1/2)} + PFH_{(DMS\ 3/4)} + PFH_{(EL6910)} + PFH_{(EL2904)} + PFH_{(K1/K2)}$$

$$PFH_{ges} = 1,52E - 08 + 1,52E - 08 + 1,79E - 9 + 1,25E - 9 + 1,92E - 13$$

$$PFH_{ges} = 3,344E - 08$$



**Note**

#### EN 62061

In accordance with EN 62061, the input subsystem is evaluated with an SFF or a DC of 90%. This restricts the achievable SIL value according to table 5 of EN 62061 to a maximum SIL 2.

Alternative calculation of the  $MTTF_D$  value according to EN 13849 for safety function 1 / 2 (with the same assumption), with

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

From the input subsystem, the poorer value is taken:

$$\frac{1}{MTTF_{D ges}} = \frac{1}{MTTF_{D (DMS Sensor 2)}} + \frac{1}{MTTF_{D (EL3751)}} + \frac{1}{MTTF_{D (EL6910)}} + \frac{1}{MTTF_{D (EL2904)}} + \frac{1}{MTTF_{D (K1)}}$$

If only PFH values are available for EL2904 and EL6910, the following estimation applies:

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

Hence:

$$MTTF_{D (EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E - 09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{15,68E - 06 \frac{1}{y}} = 637 y$$

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

$$MTTF_{D ges} = \frac{1}{\frac{1}{160} + \frac{1}{117} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593.607}} = 57,26 y$$


$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}} + \frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}}}{\frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}} = \frac{\frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}} + \frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}}}{\frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Used with DC=90%

$$DC_{avg} = \frac{\frac{0,9}{160} + \frac{0,9}{178} + \frac{0,9}{160} + \frac{0,9}{117} + \frac{0,9}{160} + \frac{0,9}{178} + \frac{0,9}{160} + \frac{0,9}{117} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{160} + \frac{1}{178} + \frac{1}{160} + \frac{1}{117} + \frac{1}{160} + \frac{1}{178} + \frac{1}{160} + \frac{1}{117} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0506388}{0,0559985} = 90,42\%$$

Alternatively with DC=99%

$$DC_{avg} = \frac{\frac{0,99}{160} + \frac{0,99}{178} + \frac{0,99}{160} + \frac{0,99}{117} + \frac{0,99}{160} + \frac{0,99}{178} + \frac{0,99}{160} + \frac{0,99}{117} + \frac{0,99}{637} + \frac{0,99}{913} + \frac{0,99}{593607} + \frac{0,99}{593607}}{\frac{1}{160} + \frac{1}{178} + \frac{1}{160} + \frac{1}{117} + \frac{1}{160} + \frac{1}{178} + \frac{1}{160} + \frac{1}{117} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = \frac{0,0554385}{0,0559985} = 98,99\%$$

 <b>CAUTION</b>	<b>Category</b> This structure is possible up to category 3 at the most.
---	---

DC=90% for the input subsystem

Designation for each channel	MTTF <sub>D</sub> Range for each channel
low	3 years ≤ MTTF <sub>D</sub> < 10 years
medium	10 years ≤ MTTF <sub>D</sub> < 30 years
<b>high</b>	30 years ≤ MTTF <sub>D</sub> ≤ 100 years

Designation	DC <sub>avg</sub> Range
none	DC < 60 %
low	60 % ≤ DC < 90 %
<b>medium</b>	90 % ≤ DC < 99 %
high	99 % ≤ DC
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 <sub>D</sub>	<b>none</b>	<b>none</b>	<b>low</b>	<b>medium</b>	<b>low</b>	<b>medium</b>	<b>high</b>
<b>low</b>	a	-	a	b	b	c	-
<b>medium</b>	b	-	b	c	c	d	-
<b>high</b>	-	c	c	d	d	<b>d</b>	e

Alternatively with DC=99% for the input subsystem

Designation for each channel	MTTF <sub>D</sub>
low	3 years ≤ MTTF <sub>D</sub> < 10 years
medium	10 years ≤ MTTF <sub>D</sub> < 30 years
<b>high</b>	<b>30 years ≤ MTTF<sub>D</sub> ≤ 100 years</b>


Designation	DC <sub>avg</sub>
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
<b>high</b>	<b>99 % ≤ DC</b>
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 <sub>D</sub>	<b>none</b>	<b>none</b>	<b>low</b>	<b>medium</b>	<b>low</b>	<b>medium</b>	<b>high</b>
<b>low</b>	a	-	a	b	b	c	-
<b>medium</b>	b	-	b	c	c	d	-
<b>high</b>	-	c	c	d	d	<b>d</b>	e


 <b>Note</b>	<p><b>Result</b></p> <p>The result with category 3, PL d fulfills or exceeds the requirements of the risk and hazard analysis (PL c).</p>
--	---

## 3 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	<b>Machinery Directive</b>  This description applies only to machines as defined by the Machinery Directive.
--	--

 CAUTION	<b>Standards</b>  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	<b>Type C standard</b>  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.
---	--

### 3.1 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.

## 3.2 Determining the PL<sub>r</sub> / 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 PL<sub>r</sub>* of EN ISO 13849-1. Information on the risk graph can be found in Annex A of EN ISO 13849-1:2015.

## 3.3 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.

## 3.4 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<sub>D</sub>, 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.

### 3.5 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 screenshot shows the 'Download Project Data' dialog box with the 'Login' step selected in the 'Steps' pane. The 'Login' section contains three input fields: 'Username' with the value 'Administrator', 'Serial Number' with the value '00123456', and 'Password' with masked characters. At the bottom right are 'Next' and 'Cancel' buttons.

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 screenshot shows the 'Download Project Data' dialog box with the 'Final Verification' step selected in the 'Steps' pane. The 'Final Verification' section displays a table comparing 'Configured Datasets', 'Online CRC', 'Calculated CRC', and 'Verification Result'. Below the table is a checkbox labeled 'I have manually verified the data shown here and I am aware, that the correct functionality must be tested manually!' which is checked. At the bottom right are 'Next' and 'Cancel' buttons.

Configured Datasets	Online CRC	Calculated CRC	Verification Result
Safe Logic Data	0xA8B4	0xA8B4	✓
Mapping Data	0xB29A	0xB29A	✓
Parameter Data	0x02B0	0x02B0	✓

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.



### 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										
0																				
1																				
2	<b>Documentation for solution</b>  <b>TwinCAT Project18</b> <b>SafetyProject_MachineFeeder</b>																			
3	<b>Project CRC:</b> 0x785F  <b>Programmer:</b>																			
4	Print Name _____			Signature _____			Date _____													
5	<b>Customer:</b>																			
6	Print Name _____			Signature _____			Date _____													
<table border="1"> <tr> <td>Date</td> <td>17.10.2017</td> <td rowspan="3"> <b>BECKHOFF</b>  Beckhoff Automation GmbH </td> <td></td> </tr> <tr> <td>Editor</td> <td>SafetyUser01</td> <td></td> </tr> <tr> <td>Plot</td> <td>17.10.2017</td> <td></td> </tr> </table>											Date	17.10.2017	<b>BECKHOFF</b> Beckhoff Automation GmbH		Editor	SafetyUser01		Plot	17.10.2017	
Date	17.10.2017	<b>BECKHOFF</b> Beckhoff Automation GmbH																		
Editor	SafetyUser01																			
Plot	17.10.2017																			



## 3.6 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 **Fehler! Verweisquelle konnte nicht gefunden werden..**

## 3.7 Validation of the safety functions

Extract from EN ISO 13849-2:2013, Chapter 4.1: validation guidelines.

ISO 13849-1:2006 is still referenced here. The relevant chapters have the same chapter numbers in the current version of EN ISO 13849-1:2015.

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 ISO 13849-1, 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 ISO 13849-1:2006, 4.5):
  - 1. the requirements for the specified category (see ISO 13849-1:2006, 6.2),
  - 2. the measures for controlling and avoiding systematic failures (see ISO 13849-1:2006, Annex G),
  - 3. the software requirements, if applicable (see ISO 13849-1:2006, 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 ISO 13849-1:2006, 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 the validation has to be carried out by a third party.

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

## 3.8 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
- Parameterization check 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
- ...

## 3.9 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
- ...

## 4 Technical report – TÜV SÜD

### KONFORMITÄTSBESTÄTIGUNG LETTER OF CONFIRMATION



Rail

BV89987T

## Applikationshandbuch TwinSAFE (Application guide TwinSAFE)

**Hersteller:**  
Manufacturer:

Beckhoff Automation GmbH & Co. KG  
Huelshorstweg 20  
D-33415 Verl

**Prüfstelle:**  
Test body:

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 gefährdender 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 <sub>d</sub> und DC entsprechend EN ISO 13849-1:2015 Calculation of MTTF <sub>d</sub> 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 1.9.0 Application guide TwinSAFE version 1.9.0

### 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  
2017-10-23

Digital  
unterscriben von  
Guido Neumann  
Datum: 2017.10.23  
17:20:19 +02'00'

G. Neumann  
Technical Certifier

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.

## 5 Appendix

### 5.1 Beckhoff 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.

#### 5.1.1 Beckhoff branches and partner companies Beckhoff Support

Please contact your Beckhoff branch office or partner company for [local support and service](#) on Beckhoff products!

The contact addresses for your country can be found in the list of Beckhoff branches and partner companies: [www.beckhoff.com](http://www.beckhoff.com). You will also find further [documentation](#) for Beckhoff components there.

#### 5.1.2 Beckhoff company headquarters

Beckhoff Automation GmbH & Co.KG  
Huelshorstweg 20  
33415 Verl  
Germany

Phone: + 49 (0) 5246/963-0  
Fax: + 49 (0) 5246/963-198  
E-mail: [info@beckhoff.com](mailto:info@beckhoff.com)  
Web: [www.beckhoff.com](http://www.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:

- world-wide support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline: + 49 (0) 5246/963-157  
Fax: + 49 (0) 5246/963-9157  
E-mail: [support@beckhoff.com](mailto: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 (0) 5246/963-460  
Fax: + 49 (0) 5246/963-479  
E-mail: [service@beckhoff.com](mailto:service@beckhoff.com)