Application Example

EP7211-0034 - STO Function

Version: 1.0.0
Date: 2019-11-11

BECKHOFF

Table of contents

1 Foreword

1.1 Notes on the documentation

Intended audience

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

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

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

Origin of the document

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

Currentness

Please check whether you are using the current and valid version of this document. The current version can be downloaded from the Beckhoff homepage at http://www.beckhoff.com/english/download/twinsafe.htm. In case of doubt, please contact Technical Support [▶ 16].

Product features

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

Disclaimer

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

Trademarks

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

Patent Pending

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

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

Delivery conditions

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

1.2 Documentation issue status

Version	Comment
1.0.0	• First release version

1.3 Purpose and area of application

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

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

NOTE

Application samples

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

1.4 Explanation of terms

Name	Explanation
$B10_D$	Mean number of cycles after 10% of the components have dangerously failed
CCF	Failures with a common cause
d_{op}	Mean operating time in days per year
DC_{avg}	Average diagnostic coverage
h_{op}	Mean operating time in hours per day
$MTTF_D$	Mean time to dangerous failure
n_{op}	Mean number of annual actuations
PFH_D	Probability of a dangerous failure per hour
PL	Performance level
PL_r	Required Performance Level
T_{cycle}	Mean time between two successive cycles of the system (given in minutes in the following examples, but can also be given in seconds)
T1	Lifetime of the device (typically 20 years for TwinSAFE devices)
λ_D	Dangerous failure rate given in FIT (failure rate in 10^9 component hours)
T_{10D}	Operating time - maximum operating time for electromechanical components, for example
TwinSAFE SC	The TwinSAFE SC technology (SC - Single Channel) enables a signal from a standard terminal to be packaged in a FSoE telegram and transmitted via the standard fieldbus to the TwinSAFE Logic. As a result, falsifications on the transmission path can be excluded. Within the TwinSAFE Logic, this signal is checked with a further independent signal. This comparison result typically yields an analog value corresponding to a category 3 and PL d. **This technology does not support digital input signals and cannot be used in a single-channel structure (only one TwinSAFE SC channel).**

1.5 Operator's obligation to exercise diligence

The operator must ensure that

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

NOTE

Qualified personnel

For the use of the TwinSAFE components, the personnel must be qualified and take part regularly in training courses.
Training courses on functional safety can be taken at the corresponding certifying bodies such as the TÜV or at the responsible employer's liability insurance associations.
Product training courses for the TwinSAFE components can be booked with the Beckhoff Training Department.

2 Safety instructions

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.

2.2 Operator's obligation to exercise diligence

The operator must ensure that

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

2.3 Description of instructions

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

⚠ DANGER

Serious risk of injury!

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

⚠ WARNING

Risk of injury!

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

⚠ CAUTION

Personal injuries!

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

NOTE

Damage to the environment/equipment or data loss

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

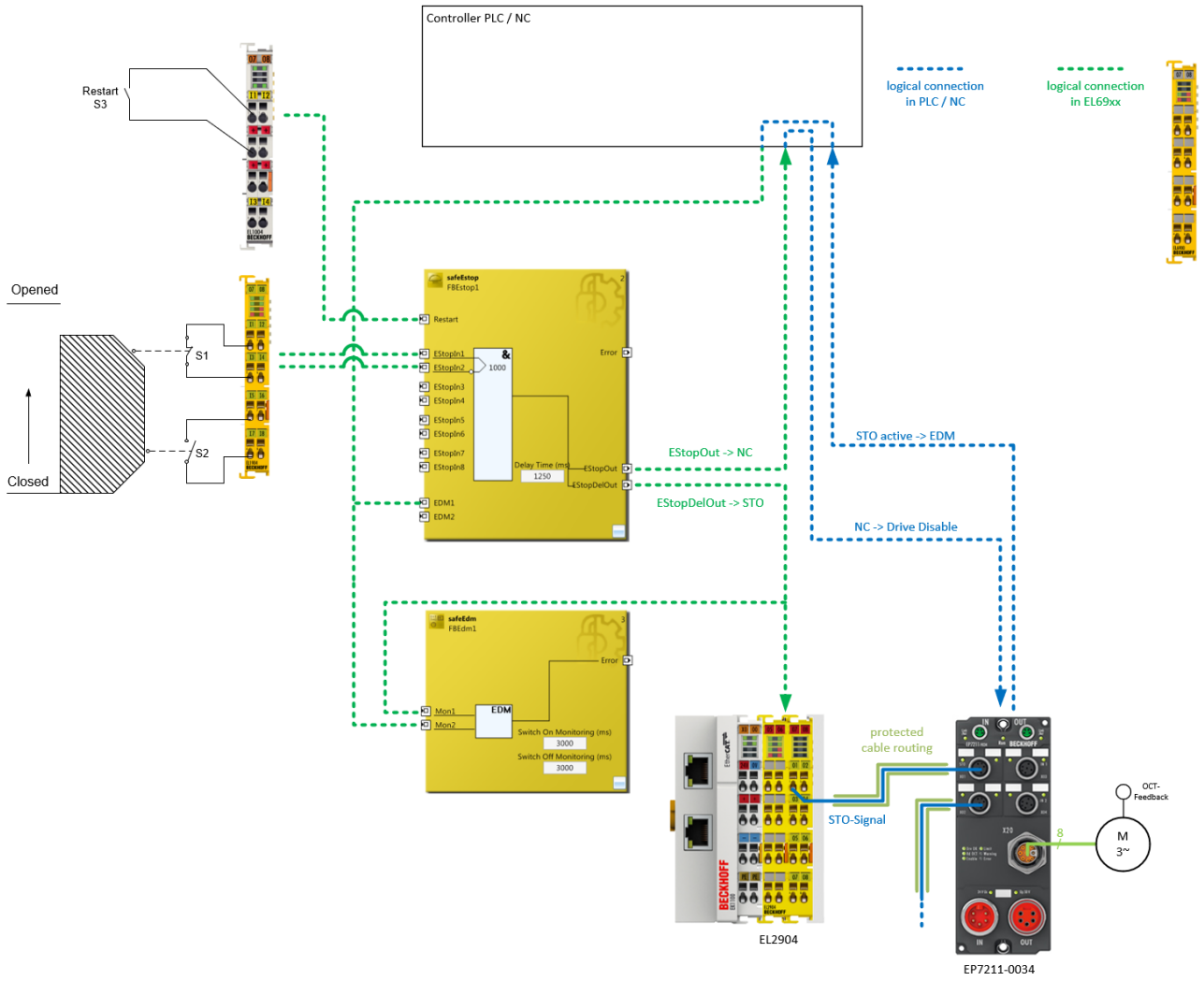
Tip or pointer

This symbol indicates information that contributes to better understanding.

3 STO function with EP7211-0034 (category 3, PL d)

The following application example shows how the EP7211-0034 can be wired together with an EL2904 in order to implement an STO function according to EN 61800-5-2.

A protective door (S1 and S2) and a restart signal (S3) are logically linked on an ESTOP function block. The EStopOut signal is transferred to the NC controller, which can be used within the functional application. The STO input of the EP7211-0034 is operated via the delayed output EStopDelOut. Forwarding this signal to further EP7211-0034 via the second connection is allowed. The EP7211-0034 supplies the information that the STO function is active via the standard controller. This information is transferred to the EDM input of the ESTOP function block and additionally to the EDM function block in order to generate an expectation for this signal.



⚠ CAUTION

Implement a restart lock in the machine!

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

If the risk analysis returns the result that a restart is to be realized in the safety controller, then the restart **must** also be placed on a safe input.

⚠ WARNING

Wiring only with separate sheathed cable

The wiring between the EL2904 and the STO input of the EP7211-0034 must be done with a separate sheathed cable in order to be able to assume a fault exclusion for the cross-circuit or external power supply of the wiring between EL2904 and EP7211-0034. A forwarding of the STO-Signal to further EP7211-0034 must also be done with a separate sheathed cable.

The evaluation of this wiring and the evaluation of whether the fault exclusion is permissible must be done by the machine manufacturer or user.

NOTE

Calculation EP7211-0034

The EP7211-0034 is not taken into account in the calculation of the Performance Level according to DIN EN ISO 13849-1 since it behaves interference-free to the safety function.

The PFH_D value goes into the calculation according to EN 62061 with a value of 0.

3.1 Parameters of the safe input and output terminals

EL1904

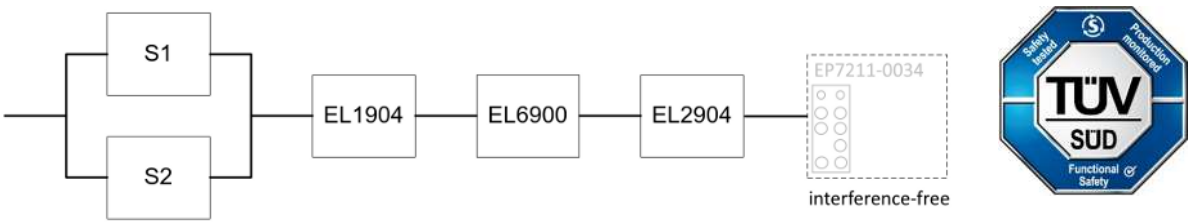
Parameter	Value
Sensor test channel 1 active	Yes
Sensor test channel 2 active	Yes
Sensor test channel 3 active	Yes
Sensor test channel 4 active	Yes
Logic channel 1 and 2	Single Logic
Logic channel 3 and 4	Single Logic

EL2904

Parameter	Value
Current measurement active	No
Output test pulses active	Yes

3.2 Block formation and safety loops

3.2.1 Safety function 1



3.3 Calculation

3.3.1 PFHD / MTTFD / B10D – values

Component	Value
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
EP7211-0034 - PFH_D	0.00
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
Days of operation (d_{op})	230
Hours of operation / day (h_{op})	16
Cycle time (minutes) (T_{cycle})	15 (4x per hour)
Lifetime (T1)	20 years = 175200 hours

3.3.2 Diagnostic Coverage DC

Component	Value
S1/S2 with testing/plausibility	DC_{avg}=99%
EL2904 with testing	DC_{avg}=99%

3.3.3 Calculation of safety function 1

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

From:

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

and:

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

Inserting the values, this produces:

S1:

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

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

S2:

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

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

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

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

produces for

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

S1:

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

S2:

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

The following assumptions must now be made:

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

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

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

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(EL72x1-9014)}$$

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

to:

$$PFH_{ges} = 10\% * \frac{1{,}68E - 09 + 1{,}68E - 09}{2} + 1{,}11E - 09 + 1{,}03E - 09 + 1{,}25E - 09 + 0{,}00 = 3{,}558E - 09$$

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

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

as:

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

with:

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

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

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

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

Hence:

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

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

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 225,2y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 99,00\%$$

⚠ CAUTION

Category

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

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

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

NOTE

Diagnostic coverage

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

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4 Appendix

4.1 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

Beckhoff's branch offices and representatives

Please contact your Beckhoff branch office or representative for local support and service on Beckhoff products!

The addresses of Beckhoff's branch offices and representatives round the world can be found on her internet pages:
http://www.beckhoff.com

You will also find further documentation for Beckhoff components there.

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

Phone:	+49 5246 963 0
Fax:	+49 5246 963 198
e-mail:	info@beckhoff.com

Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline:	+49 5246 963 157
Fax:	+49 5246 963 9157
e-mail:	support@beckhoff.com

Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

Hotline:	+49 5246 963 460
Fax:	+49 5246 963 479
e-mail:	service@beckhoff.com